Law, Governance and Technology Series 77

Akanksha Bisoyi

Blockchain and Legitimacy

The Rule of Law by Design

Springer

Law, Governance and Technology Series

Volume 77

The *Law, Governance and Technology Series* is intended to attract manuscripts arising from an interdisciplinary approach in law, artificial intelligence and information technologies. The idea is to bridge the gap between research in IT law and IT-applications for lawyers developing a unifying techno-legal perspective. The series will welcome proposals that have a fairly specific focus on problems or projects that will lead to innovative research charting the course for new interdisciplinary developments in law, legal theory, and law and society research as well as in computer technologies, artificial intelligence and cognitive sciences. In broad strokes, manuscripts for this series may be mainly located in the fields of the Internet law (data protection, intellectual property, Internet rights, etc.), Computational models of the legal contents and legal reasoning, Legal Information Retrieval, Electronic Data Discovery, Collaborative Tools (e.g. Online Dispute Resolution platforms), Metadata and XML Technologies (for Semantic Web Services), Technologies in Courtrooms and Judicial Offices (E-Court), Technologies for Governments and Administrations (E-Government), Legal Multimedia, and Legal Electronic Institutions (Multi-Agent Systems and Artificial Societies).

Akanksha Bisoyi

Blockchain and Legitimacy

The Rule of Law by Design

Springer

Akanksha Bisoyi
School of Social Sciences and Technology
Technical University of Munich
Munich, Bayern, Germany

ISSN 2352-1902 ISSN 2352-1910 (electronic)
Law, Governance and Technology Series
ISBN 978-3-031-98711-3 ISBN 978-3-031-98712-0 (eBook)
https://doi.org/10.1007/978-3-031-98712-0

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Foreword

The discourse surrounding Distributed Ledger Technologies (DLTs) has often been characterized by effervescence, a familiar pattern when novel technological paradigms emerge. For some time now, DLTs, most famously exemplified by blockchains, have captured the collective imagination, oscillating wildly between breathless hype and dismissive skepticism. Yet, beyond the ephemeral shimmer of technological novelty lie profound questions about governance, trust, and the very architecture of our legal and social orders. The lessons Akanksha Bisoyi invites us to consider in this monograph focus on but extend far beyond the specifics of DLTs; they speak more broadly to the perennial challenge of navigating the relationship between law and technology, mainly when innovation seems to unlock unprecedented possibilities while simultaneously generating novel normative effects that test the foundational assumptions upon which our legal systems rest.

To appreciate the significance of Akanksha Bisoyi's contribution, it is instructive to briefly retrace the trajectory of the technology itself. The initial innovation underpinning blockchain was not a singular invention sprung ex nihilo but rather a remarkable feat of recombinant innovation. It ingeniously integrated several pre-existing technological components into a novel configuration: the cryptographically secured chain-of-blocks data structure, drawing inspiration from Haber and Stornetta's work on tamper-proof timestamping; Proof-of-Work consensus mechanisms, with roots in efforts to combat email spam and later formalized in cryptography; established methods of digital signatures and public key cryptography for secure ownership; timestamping mechanisms building directly on earlier cryptographic work; and peer-to-peer networking principles exemplified by predecessors like BitTorrent. Precursors like David Chaum's eCash, Wei Dai's b-money, and Nick Szabo's Bit Gold laid conceptual groundwork. This recombination, however, was not merely technical; it was animated by a potent socio-technical aspiration: the creation of systems capable of fostering trust and coordinating action without reliance on traditional, centralized intermediaries. The advent of cryptocurrencies, spearheaded by Bitcoin, demonstrated a functional model of decentralized trust, a paradigm shift that directly confronted assumptions deeply embedded within

state-guaranteed legal orders. It showed that building functional, coordinated systems without a central authority was possible.

Following this initial wave, a second tide of innovation sought to extend the logic of DLTs from the realm of value transfer to the domain of law itself, primarily through the concept of "smart contracts". The idea was tantalizing: could legal agreements be rendered self-executing, encoded directly into the immutable ledger? This prospect elicited sharply divided reactions. On one side, a form of "crypto-legalism" emerged, suggesting that technology itself could, or perhaps should, become the law—that legal principles ought to adapt to the inherent affordances and constraints of the technological medium. Proponents envisioned a world of automated enforcement and radically reduced ambiguity. Conversely, a critical response, primarily from within the legal profession, maintained that technology must yield to the established precepts and enduring values of the law. From this perspective, DLTs and smart contracts must be molded to fit within existing legal structures, ensuring compatibility with fundamental principles that safeguard fairness, justice, and due process. As the practical implementation of smart contracts encountered significant hurdles, revealing complexities unforeseen in initial theoretical formulations, it became increasingly apparent that neither pole of this dichotomy offered a complete or satisfactory path forward. The moment grew ripe for a third way, one capable of transcending the binary opposition between technological determinism and legal conservatism.

Enter Akanksha Bisoyi's contribution. Her signal contribution lies in operationalizing the concept of "Law by Design"—an idea focused on proactively embedding legal values into technology from the outset—and applying it specifically to the challenges posed by DLTs, using the Rule of Law itself as the foundational normative framework. Moving beyond reactive approaches that focus solely on the outcomes or effects of technology after deployment, her methodology directs attention to the crucial, formative stages: the *purpose* driving a technology's creation and the *design* and *deployment* processes themselves. She argues for establishing a coherent set of high-order Rule of Law values—such as transparency, accountability, fairness, and contestability—to proactively shape the technological architecture and the accompanying legal regulation as these systems evolve. This framework provides a sophisticated toolset for navigating the tensions between technological affordances and legal requirements, offering a principled alternative to the rigidities of crypto-legalism and the limitations of purely technology-critical legal reactions.

The framework developed in this book holds immense promise for steering the future development of DLTs and other emerging digital technologies. This approach serves multiple purposes by embedding values at the core of technological design and governance. It can guide the development of principled and socially conscious technologies, acts as a benchmark against which existing and future laws and regulations can be evaluated, and fosters a mutual shaping of law and technology. Significantly, it moves beyond the binary debates of "law versus technology" to create a synergy that enables both to flourish. In practical terms, this vision has vast implications across healthcare, insurance, and public administration sectors, where DLTs are already being explored as transformative tools.

Yet, the effects of "Law by Design" can ripple outward when normative aspirations trigger ideas that can be translated into novel recombinations or innovations in technologies. A fitting example is the journey of the art project *BeeCoin* by the Berlin-based artist collective KUNSTrePUBLIK/ZK/U. It began with a bold question: *What if the health of bees could create real economic value?* The idea was to link data from living beehives—their weight, temperature, and activity—to a new digital currency. This currency would reward actions that support bee populations, turning care for the environment into a form of wealth. But as the project evolved, its focus shifted. Rather than just creating a new kind of money, the artists asked a more profound question: *What if bees could have a voice in the decisions that affect them?* This question led to BeeDAO—a decentralized organization where both humans and bees are members. Humans join as *Beeholders*, using unique tokens to propose and vote on projects. The bees "participate" through their data, which reflects the state of their environment.

Just as proactive value-driven engagement has created bitcoin, new ideas might spring from a value-sensitive engagement from a Rule of Law perspective. Therefore, readers should engage with the following pages not as a conclusion but as an invitation. The arc of the normative effects of DLTs remains unwritten, its trajectory shaped by our choices at the drawing board and in the legislature. This book's concepts and tools can help us enter an open and productive conversation to ensure the arc bends toward justice.

Law, Innovation and Legal Design at the Technical University of Munich
Munich, Germany
April 2025

Christian Djeffal

Preface

The book 'Blockchain and Legitimacy: The Rule of Law by Design' is about questioning and examining the legitimacy, accountability, and contestability of blockchain-based mechanisms. This work aims to add key insights for a better understanding of the intersection between law and technology, which influence and shape the development of blockchain technology or the broader framework of code-driven technologies.

Here, I start with the question: *Can the rule of law shape, guide, and influence the design and implementation of blockchain technology in a legitimate manner?* How can the function and role of 'the rule of law' provide substantial guidance in setting design goals and choices to configure blockchain? How can we reach harmony between the rule of law and blockchain?

With the blockchain influencing the 'traditional' social construction, the code embedded within the technology has an impact on our lives, not only enormously but also more effectively than what the law aims to achieve. Since code can potentially shape people's behavior in a democracy, its implications must be within the bounds of the rule of law. The utilization of blockchain and smart contracts challenges key tenets of the rule of law, such as protecting fundamental rights like privacy and ensuring the effectiveness of checks and balances, such as robust judicial oversight. It provides the designers and developers working with blockchain technology a unique opportunity not only to create 'blockchain lite' applications primarily focused on enhancing commerce and governance but also to design for 'blockchain heavy' applications explicitly aimed at safeguarding human rights, particularly in combatting corruption and electoral fraud.

In this book, I argue that the technical attributes of blockchain technology may result in *crypto-legalism*, which typically portrays a sort of 'unthinking' rigid adherence to rules that are imposed on the users or individuals through codes without any reflective consideration. In order to chalk out the characteristics of the code rules regulating user behavior and to understand whether these code rules are compatible with the rule of law, I employ various notions from the philosophical study of technology as well as the design theory to provide a perspective on the concepts of affordance, technological intentionality, and technological mediation.

Even though code is not law, it is prudent to be concerned about techno(code)-regulation similar to the conventional system because code as law must be evaluated by reflecting on the techno-regulation effects anent the freedom and individual autonomy in comparison to the balance affected by the rule of law. One of the rule of law standards is legal certainty, which is contrary to the domain of computational science which is bereft of scientific certainty; ergo, if a code that does not adhere to such values making it 'not legitimate', should not, in fact, be implemented. Given the unparalleled efficiency of code in enforcing regulations, it is crucial that the *ex-ante* and *ex-post* rule of law standards that guarantee legitimacy and allow for contestability must be considered at equal footing with the conventional legislation since the code embedded within the technology is the manifestation of the intentions which can either be for the purposes of fostering the rule of law or circumventing it.

The rule of law may not ensure a perfectively just social order, but it certainly puts some restrictions on those who govern. The underlying principle is that 'the rule of law is the fulcrum of normative legal orders'. It prevents arbitrary governance and, when conditions are met, demands responsible citizenship by respecting the law. With the ushering in of technology regulation, the base requires to be overhauled and its emphasis adjusted. However, its spirit remains crucial, and in the context of technology regulation, laws authorizing technological use must be clearly defined and administered in accordance with their terms.

I put forward in this book that there is a need to design and implement the technology in accordance with the rule of law. While incorporating specific legal features 'by design' is possible, applying the same to the rule of law is not forthright since it may not be feasible to automate multi-dimensional socio-legal requirements.

In order to frame the notion of the rule of law for the purposes of shaping the blockchain, I have utilized the conceptualization of legality and legalism, that is, the rule of law and the rule by law, in consonance with the legal-theoretical frameworks of Fuller's 'inner morality of law' and related legisprudential theories which lay down the rule of standards that the characteristics of the legal rules must possess. While legalism relies on the source of the law that is based on the will of the sovereign, legality adopts a more rational approach and looks for substantiation of necessary prerequisites in a rule-making process. Legalism, due to its rigid adherence to rules, is at one extreme, while legality is positioned at the other extreme and aims to align the normative construct of law with the principles that legitimize sovereign power in the rule of law environment.

The theoretical instruments such as Fullerian principles and legisprudential principles are conducive to shaping the *ex-ante* and *ex-post* evaluation of various normative rule-making processes, which is essential to examine in order to draw a parallel between the issues that undermine the legitimacy of legal rules and the issues that may be present in the privately programmed code. The idea is to incorporate their rule of law standards into the design phase as a means to address and reduce the 'illegitimacies' associated with the characteristics of the code embedded in the blockchain (*crypto-legalism*). Therefore, I have used the concept of the rule of law to examine and analyze the 'purpose' behind the blockchain to understand the

influence, motivations, and aspirations of the 'figure' behind programming the conceptual notions into the technology and also whether the code rule embedded within the technology, written for the 'purpose' is valid and legitimate and what is the characteristics of such a code rule and does it follow the rule of law procedural norms such as the principles of legality and legitimacy.

It is essential to recognize here that while there are numerous conceptions (thin and thick) of the rule of law, I have primarily employed the thin conception of the rule of law. This framework enables to understand and examine the characteristics of legal rules and subsequently apply this knowledge to the domain of the rule of code, aiming to create a congruence between the two subjects. My inquiry revolves around the premise that just as legal rules governing human behavior must comply with the substantive and formal procedural norms, the same requirement should be imposed on the technology that influences our behavior and conduct. To find an answer to why the technological artifacts that govern us should adhere to the procedural standards in addition to the material notions of the rule of law, I have chosen Fuller's principles of legality, in conjunction with the legisprudential principles, as a foundation for my analysis.

This book emphasizes on identifying as well as facilitating the integration of the key values of legal protection within the technological system. Given the focus is on blockchain applications for humanitarian purposes and public administration purposes, I have deliberated material notions such as transparency, accountability, and protection of human rights as well as the rule of law affordances *vis-à-vis crypto-legalistic* characteristics of blockchain artifacts that are at play in these code-driven technologies.

Finally, it must be noted here that while this book examines and focuses on blockchain as the primary technology, the findings and conclusions drawn from this work are relevant and applicable across all forms of DLT. Additionally, the insights from the narrative drawn here can be applied more broadly to all code-driven technological artifacts. I acknowledge the significant environmental implications associated with blockchain usage. Keeping this concern at the forefront, the book has been designed in a manner that allows for navigation and adaptability, ensuring that the design standards, State choices, and the normative reference points or the rule of law affordances identified in this study can be extended to other code-driven architectures and technologies, facilitating a holistic understanding of their impacts and applications.

Munich, Germany Akanksha Bisoyi

Acknowledgments

I express my sincere gratitude and indeptedness to Professor Dr. Christian Djeffal, Professorship of Law, Innovation and Legal Design, Technical University of Munich who has supported me in this endeavour since inception and helped me to develop an interdisciplinary approach to the topic which has finally culminated into 'Blockchain and Legitimacy: The Rule of Law by Design'. His guidance, support, and expert advice have been invaluable in improving the research work at every stage, but for which this book would not have perhaps been in the present form. I also put on record my gratitude to Professor Dr. Rolf H. Weber, University of Zurich, for his invaluable inputs and comments during the development stage of this monograph.

I have received many thought-provoking inputs and ideas while interacting with academicians, researchers and participants in different fora, which have helped me to finalise the content.

My colleagues at the Department of Science, Technology, and Society have been very supportive and have kept me motivated during this journey. My heartfelt thanks are due to all of them.

Special thanks are also due to my parents, Bipina and Jayashri Bisoyi, who taught the first lessons on the value of hard work, passion, and aspirations. Your constant motivation has helped a lot to complete this book.

Last but not the least, I also express my sincere thanks to the publisher, Springer and its editors for their valuable support when it mattered most.

Competing Interests The author has no competing interests to declare that are relevant to the content of this manuscript.

Contents

Abbreviations

AI	Artificial Intelligence
DAO	Decentralized autonomous organization
DBMS	Database Management System
DLT	Distributed Ledger Technology
GDPR	General Data Protection Regulation
HTML	Hypertext Markup Language
ICO	Initial coin offering
ICT	Information and Communication Technology
ISO	International Organisation of Standardisation
ISP	Internet Service Provider
NatSpec	Ethereum Natural Language Specification Format
UNCITRAL	United Nations Commission on International Trade Law
WEF	World Economic Forum
WWF	World Wildlife Fund

Chapter 1
Introduction

While blockchain, by design, ought to promote transparency, equality, and non-discrimination, it can also be used to evade essential obligations imposed by traditional law, thus threatening the rule of law framework upon which the conventional legal systems are grounded. This raises questions about the legitimacy, accountability, and contestability of blockchain-based mechanisms, especially since blockchain-based technological artifacts are being increasingly employed for democratic e-governance, delivery of public services, and humanitarian activities.

The blockchain establishes and enforces a set of new rules and norms without relying on any external legal authority or institution, resulting in the creation of a novel regulatory framework called *lex cryptographica* or the rule of code.[1] The blockchain-based applications such as smart contracts and DAOs can create self-executing and self-regulating systems of governance and coordination among the users of a blockchain network.[2] It effectively functions as a private regulatory framework whose operation is independent of the language, territory, or body of conventional law. Currently, societal governance is, by and large, enforced by institutions and bureaucratic systems based on legal principles and hierarchy. In contrast, blockchain-based applications rely on *lex cryptographica* to govern economic and social activities, potentially shifting power from traditional legal and regulatory frameworks to decentralized blockchain networks.

As the blockchain influences 'traditional' social constructions, with the code shaping people's behavior in a democracy, it must be within the bounds of the rule of law. However, the technical attributes of blockchain technology may result in *crypto-legalism,* which typically portrays rigid adherence to rules that are imposed on the users or individuals through codes without any reflective considerations. In order to comprehensively understand how the behavior of a user is enabled and

[1] Wright and De Filippi (2015), p. 4.

[2] Wright and De Filippi (2015), pp. 3–4.

A. Bisoyi, *Blockchain and Legitimacy*, Law, Governance and Technology Series 77, https://doi.org/10.1007/978-3-031-98712-0_1

constrained by the code embedded in the blockchain, the various notions from the philosophical study of technology and the design theory are employed to provide a perspective on this question focusing on the concepts of inscription, affordance, and technological mediation, which will facilitate in chalking out the characteristics of the code rules regulating the user behavior and whether these code rules are compatible with the rule of law.

Given the unparalleled efficiency of code in enforcing regulations, it is essential to have *ex-ante* and *ex-post* rule of law standards that guarantee legitimacy and allow for contestability, similar to the responsibilities placed on the public legislators. Though the rule of law may not ensure a perfectively just social order; it certainly restrains those who govern. The underlying principle is 'the rule of law is the fulcrum of normative legal orders'.[3] In the context of technology regulation, laws authorizing technological use must be clearly defined and administered in accordance with their terms.[4]

A technological artifact needs to be designed and implemented in accordance with the rule of law. While incorporating specific legal features 'by-design' is possible, applying the same to the rule of law is not forthright since it may not be feasible to automate multi-dimensional socio-legal requirements. In this book, a design exploratory method has been adopted to explore the question: *can the rule of law shape, guide, and influence the design and implementation of blockchain technology in a legitimate manner?* The idea is to employ the concept of the rule of law to examine and analyze the 'purpose' behind the blockchain implementation and understand the influence, motivations, and aspirations behind programming the conceptual notions into the technology. Various characteristics of the rule of code are also examined to understand whether the rule of code embedded within the blockchain artifact, written for the 'purpose', is valid and legitimate and whether it would follow the rule of law procedural norms.

The book is structured mainly into three parts. Part I discusses the relationship between the blockchain and the rule of law. It begins with the functional understanding of the blockchain, the normative effect of the technology on law, the approaches that have been in place to shape the blockchain, and the opportunities and risks presented to the rule of law by the blockchain (Chap. 2). Understanding this aspect acknowledges the need to develop a study that employs the appropriate approach to design and implement the technology from the perspective of the rule of law.

The next step is to explore the standards and values of the rule of law and their influence on the formulation of a 'legitimate' legal rule. The concept of the *rule by law* and the *rule of law* that aligns with the notion of legalism and legality is investigated to comprehend the essential requirements for making a legal norm valid, lawful, and legitimate. This facilitates the establishment of certain rule of law standards and values, which sets the stage for their potential implementation in the

[3] Brownsword (2016), p. 36.

[4] Brownsword (2019), p. 132.

blockchain realm to reduce the 'illegitimacies' arising from the artifact (Chap. 3). To understand the negative ramifications and illegitimacies that may occur due to the use of technology, the interplay between blockchain and the rule of law as two distinct regulatory environments is investigated through the concept of 'code is law' and the 'code of law'. It explores the critical points of friction or harmony that emerge from the interaction between the blockchain (*lex cryptographica*) and the rule of law (Chap. 4).

Part I ends with acknowledging the relationship between blockchain code and law to that of 'Tom and Jerry' and emphasizes that just focusing on one level, either macro or micro level, would not be sufficient to legitimize the technology—not only the purpose behind the conceptual rules for using the technology should be justified but also the command code rules which make this (justified) purpose possible, should also be legitimized. This outlines the need to study the blockchain artifact at the micro level, that is, at the programming stage, from the standpoint of the philosophical study of technology and the theory of design in order to comprehend the human-technology interaction and examine how the rule of code impacts the behavior of the users, and what are the similarities and dissimilarities, if any, in characteristics between the rule of code embedded in the blockchain and law.

Part II deals with the design of the rule of code and covers normative foundations of design in blockchain artifacts, *crypto-legalism,* and legitimacy standards for blockchain. This part starts with the exploration of the blockchain, wherein it examines how the technological artifact shapes, guides, and influences user behavior (Chap. 5). It facilitates appreciating the technological design issues from a normative standard perspective and mediating how one might knowingly aspire to produce legitimate normative architectures.

The discussions in Chap. 5 lead to examining the rule-fetish representation of the rule of code-based blockchain infrastructure, demonstrating how the characteristics of the rule of code embedded in the blockchain architecture formulate the notion of *crypto-legalism* (Chap. 6). This chapter endeavors to elucidate congruities between legalism within the legal domain and technological normativity, aiming to seamlessly incorporate the cushioning effects of the former into the latter. The deliberations raise the question: whether the coding rules in blockchain architecture or the rule of code adhere to the standards of the rule of law or not, rendering them legitimate or otherwise.

The aforesaid inquiry leads to the examination of the legitimacy standards for blockchain code, focusing on normative *ex-post* and *ex-ante* standards for technology implementation and code production within the blockchain (Chap. 7). The aim of the inquiry is to answer whether the standards that legitimize legal rules in compliance with the rule of law can be applied in the design realm to legitimize the rule of code.

The objective of such an exercise is to explore how the principles of the rule of law can be integrated with the commercial purpose of the code to counter the negative impacts of *crypto-legalism*. Therefore, Part III focuses on the translation of the rule of law standards and values into the design and implementation of blockchain technology and explores the notion of the rule of law by design, blockchain choices

and the State decisions, and the rule of law affordances. This part delves into the exploration of how the standards and values of the rule of law can be reflected in technological architecture by conceptualizing the by-design notion to understand its nuances and formulating 'the rule of law by design' approach (Chap. 8). In order to not just focus on the formal aspects and to have a panoramic understanding of the technology and its design choices, Chap. 9 has been formulated to guide the State decisions in deciphering the purpose for which the technology is to be employed. The motivation and aspirations for the implementation of the technology ought to be in compliance with the material notions, ensuring that the substantive standards or the thick notion of the rule of law are upheld in both design and application. The formulation of the rule of law by design approach facilitates understanding what the State may intend for a particular blockchain application to afford for a particular usage, which must result in an *ex-post* legitimacy such that the technological affordances follow the rule of law. Furthermore, this approach provides a fresh perspective on plotting the characteristics of *crypto-legalism* onto the rule of law values, using the Fullerian standards of legality, which helps in developing the relationship between the rule of law standards and values and the affordances that can assist in immersing their aspirations into the design of the rule of code (Chap. 10).

Finally, the book ends with a conclusion highlighting the relevance as well as the necessity of the rule of law in blockchain systems, the State decisions, and formulation of the affordances to be embedded into the artifact.

References

Brownsword R (2016) Technological management and the rule of law. Law Innov Technol 8:1

Brownsword R (2019) The ideal of legality and the rule of law. In: Law, technology and society: reimagining the regulatory environment. Routledge, p 132

Wright A, De Filippi P (2015) Decentralized Blockchain technology and the rise of Lex Cryptographia. https://doi.org/10.2139/ssrn.2580664

Part I
Blockchain and the Rule of Law: Concepts and Relationships

Chapter 2
Understanding Blockchain and Its Normative Implications

2.1 Concepts and Origin of Blockchain

Blockchain is a technology that can reshape the world by enabling a distributed immutable digital ledger of transactions that is validated using a consensus mechanism. As a trustless trust[1] artifact and a confidence machine,[2] blockchain has the potential to provide a low-cost mutual-trust mechanism to enforce transactions and smart contracts. Technically, blockchain is an assortment of technologies[3] to record, store, and process data—its core technological features being a decentralized and distributed infrastructure, cryptographic and immutability attributes, and trustless nature. As such, a blockchain is typically associated with multi-party maintenance, cross-validation, tamper-resistant, byzantine fault-tolerant, and transparent platform that can facilitate a self-enclosed space for social, political, and economic coordination among diverse and potentially non-cooperative agents.

A distinctive feature of blockchain architecture is that, unlike traditional computational systems, it does not have central administration and control functions. Instead, it consists of a chain of blocks that seeks to craft an egalitarian institution with a peer-to-peer network. Since blockchain is a technology of governance that can challenge the role of the State,[4] its technical architecture and socio-technical enforcement are crucial for enhancing trust in the democratic society.[5] Following the principle of direct reciprocity among the users, blockchain permits management and control functions to be performed within the system without third-party entities or trusted intermediaries such as the State. Moreover, this technology establishes

[1] Werbach (2016). https://youtu.be/Uj342yXUkCc?feature=shared.

[2] De Filippi et al. (2020), p. 6.

[3] Mallard et al. (2014), p. 4.

[4] Atzori (2017), pp. 47–50.

[5] Goossens (2021), p. 87.

A. Bisoyi, *Blockchain and Legitimacy*, Law, Governance and Technology Series 77, https://doi.org/10.1007/978-3-031-98712-0_2

and enforces a set of new rules and norms without relying on any external legal authority or institution, resulting in the creation of a novel regulatory framework called *lex cryptographica* that is based on the idea that 'code is law'. In this framework, blockchain-based applications such as smart contracts and DAOs can create self-executing and self-regulating systems of governance and coordination among the users of a blockchain network.[6] It, therefore, challenges the traditional notions of law, as its operation is independent of the language, territory, or body of conventional law.

Blockchain, by design, promotes transparency, equality, and non-discrimination; however, it might also be used to evade essential obligations imposed by traditional law due to its pseudo-anonymous nature,[7] thus directly threatening the rule of law framework upon which the conventional legal systems are grounded. This raises questions about the legitimacy, accountability, and contestability of blockchain-based mechanisms, especially since the instant technology is being (proposed to be) employed for democratic e-governance, delivery of public services, and humanitarian activities. We must, therefore, understand the notions and intentions behind the development of blockchain technology, the features that 'make' such a technology to be employed by the States and democratic institutions, its normative implications, and its effects on the law and society as a whole, to investigate and analyze the approaches laid down to shape the technology and to regulate it.

The creation of blockchain has been compared to the advent of a revolution since this technology supposedly has the potential to obviate the essentiality of traditionally trusted third-party intermediaries and the middlemen, which includes all conventional institutions and individuals who serve as mediators of those 'social constructions' and 'representations',[8] and are the key economic and regulatory actors. These developments seemingly free individuals from social constructs or representations, allowing for direct interaction and a seamless connection with the diverse nature of the world.

The ideas and ideals of blockchain transpired during the decline in public confidence in institutions,[9] which resulted in the direct effect of the growing importance of the societal functions that depend on numbers and algorithms.[10] These developments ostensibly liberate the citizens from social constructs or representations, allowing for direct interaction and a seamless connection with the diverse nature of the world.[11] It allows collective groups and social institutions to be more adaptable and encourages increased participation, potentially transforming the functioning of corporate bodies and democratic organizations. The blockchain technology's

[6] Wright and De Filippi (2015), p. 4.

[7] De Filippi et al. (2022a), pp. 359, 366.

[8] Searle (1995), p. 2.

[9] Casey and Vigna (2018). https://www.technologyreview.com/2018/04/09/3066/in-blockchain-we-trust/.

[10] Faria (2019), pp. 120–123.

[11] Rouvroy and Stiegler (2015). https://journals.openedition.org/socio/1251.

eventual impact 'on society may be as significant as foundational events such as the creation of the Magna Carta'.[12] This technology is thus seen as an entirely novel socio-economic paradigm.

Since hype is an unavoidable component of any technological revolution, much hype also surrounds the potential of blockchain, as it is hailed as a solution to nearly every issue facing humanity.

'Sustaining innovations' are those that simply enhance the performance of products that are already in the market, while 'disruptive technologies' typically perform poorly at first but bring an entirely different value proposition, resulting in subsequent large-scale adoption.[13] Blockchain falls into the latter category as it is widely considered to be radically disruptive[14] and 'to fundamentally shift the way in which the society operates'.[15] This idea was extended through metaphors of 'better horse' and 'new car'.[16] A 'better horse' represents an improved version of something known', while a 'new car' signifies a disruptive innovation that introduces entirely novel concepts. The use of blockchain in 'digital cash', a known concept, is an example of a 'better horse'; a blockchain as a 'new car' introduces the notion of *programmable money*, allowing for the customization of currency parameters such as usage rights, conditions, and future actions like expiration or redistribution.

While blockchain was born out of the metaphor of 'better horse', it is currently evolving and transcending into the concept of 'new car' since blockchain is 'nearly there' to 'programmable money' in the form of welfare payments, employee reimbursements, insurance claims, and conditional donations.

As said, blockchain was initially created to provide technical infrastructure for Bitcoin,[17] the 'better horse' of digital money. Nakamoto boldly claimed that

> this electronic case system, fully peer-to-peer, requires no trusted third party. Banks would have no control over the system, and neither would the States; instead, it would be run by everyone.[18]

In 2009, it did not seem much, and nobody knew that blockchain would come up this way, much beyond being a by-product of cryptocurrency. Ironically, the term 'blockchain' doesn't even figure in Nakamoto's paper. Instead of being a completely new and unique technology, blockchain is better understood as an innovative blend of existing mechanisms.

---

[12] Mulligan (2016), p. 65.

[13] Christensen et al. (2018), pp. 1044, 1047, 1050–1052, 1068.

[14] Walport (2016), p. 8.

[15] Wright and De Filippi (2015), p. 2.

[16] Swan and De Filippi (2017), p. 8.

[17] While blockchain as a concept originated in the 1970s, the technological breakthrough came only after Nakamoto published the landmark paper in 2008 and created the Bitcoin social network, developing the first block, the genesis block, in 2009. Since then, this technology has gained momentum with the introduction and implementation of the distributed peer-to-peer timestamp server, which generates computational evidence for the chronological order of transactions.

[18] Nakamoto (2008), p. 1.

The roots of blockchain can be found in a long-standing debate in political philosophy about power and where it should be positioned. Ou stated that 'bitcoin anarchy is a feature, not a bug. Sometimes it's good to have no human governance'.[19] According to Tasca and Piselli, the *leitmotiv* of the entire debate has been synthesized as follows: 'In blockchains, anarchy is the worst form of governance'.[20] The same values of libertarianism and anarchy, come to think of it, were even invoked prior to Bitcoins' popularity. Back in 1996, Barlow warned that

> cyberspace does not live within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature, and it grows through our collective actions.[21]

Whilst the difficulty of regulating cyberspace, that is, its 'unregulability'[22] by public authorities, has been debunked in the literature for some time, the contemporaneous development of blockchain technology has integrated into this declaration and caused it to assume renewed substance. However, blockchain can actually be a great tool to reduce the 'anarchist' tendencies by inducing the rule of law concepts into the code architecture.[23]

In 1992, Timothy C. May predicted that individuals and organizations would soon have the ability to communicate and engage online completely anonymously, enabled by new cryptographic methods, eliminating the need for a trusted third party or State involvement.[24] According to Hacker et al., the blockchain realm denotes 'an epitome of competing political, legal, and social frames'.[25] Different narratives, which can sometimes develop into well-established ideologies, are advocated by technology enthusiasts and a growing community of specialists that emerges alongside the advancement of this innovative technology. During these 'liminal' periods, the narrative often contends with established communities that have historically controlled the 'value-generation' process during prior technological transitions. These initial liminal phases are characterized by 'framing struggles', in which the benefits of the new technology and its community of specialists are presented and challenged against the existing framework.[26] This dynamic is especially pertinent in the context of blockchain and its emphasis on decentralization, which sets it apart from the dominance of centralized platforms towards a more decentralized paradigm. In the ongoing discourse, proponents of centralization advocate concentrating power among a select few, while advocates of

[19] Bitcoin's Anarchy Is a Feature, Not a Bug (2018). https://www.bloomberg.com/view/articles/2018-03-14/bitcoin-blockchain-demonstrates-the-value-of-anarchy.

[20] Tasca and Piselli (2019), p. 27.

[21] Barlow (2019), p. 5.

[22] Lessig (1999b), p. 514.

[23] This can be seen in the later chapters.

[24] May (1992). https://activism.net/cypherpunk/crypto-anarchy.html.

[25] Hacker et al. (2019), p. 13.

[26] Hacker et al. (2019), p. 14.

decentralization argue for distributing power among the masses.[27] Ultimately, the debate over centralization versus decentralization[28] revolves around defining the proper relationship between the State and individuals, often framed as a clash of opposing values between the State's authority and individual rights.

It is now widely accepted that democratic governments possess limited powers and that individuals retain certain inalienable rights. Many Western philosophers aim to create a society where each individual can exercise their own decision-making within an established set of legal rights and responsibilities while having a minimum dependence on the arbitrary power of their rulers.[29] An examination of the views of the members of blockchain communities, who resonate with such democratic principles and values, uncovers two pivotal insights often overlooked by traditional analysis of the 'end of history'[30] thesis. Firstly, it becomes apparent that the threat to the liberal-democratic order, as conceptualized by Fukuyama,[31] doesn't solely emanate from authoritarian politicians and governmental entities; equally subversive are the radically innovative models of governance and decentralized decision-making originating within the technological sphere of the blockchain. Secondly, the challenge posed by blockchain communities to the liberal-democratic framework is significant in that it stems not from anti-democratic intentions but rather from actors who perceive the democratic structures and processes as inadequate in terms of fairness and democracy. The increase in corruption within the public administration, coupled with a lack of transparency and accountability as well as arbitrary exercise of power by the State, has prompted the members of the community to advocate for the return to the radical decentralization of the state of nature.[32] By conceptualizing fresh avenues for community-led governance, blockchain enthusiasts aspire to introduce unconventional systems of social and political structuring that prioritize decentralization and focus on leveraging digital technologies to facilitate collective decision-making processes that may not be possible within conventional, non-digital frameworks.[33]

[27] Pollicino and De Gregorio (2021).

[28] This debate is not new; it harkens back to one of the profound philosophical debates in Western history between Thomas Hobbes and John Locke. Hobbes and Locke arrive at contrasting perspectives on the ideal relationship between the State and individuals. Hobbes commended centralization as inherently beneficial: citizens must relinquish their rights to a powerful central authority to avoid chaos and violence. In contrast, Locke viewed centralized government as flawed and susceptible to corruption, advocating for a balance with decentralization, ensuring the many can challenge the power of the few. In the field of public opinion, Locke won this argument.

[29] Watkins (1948).

[30] Marks (2017).

[31] Fukuyama (2012), p. 14.

[32] Owen (2015), pp. 24–29.

[33] Tozzi (2019), p. 194.

2.1.1 Functional Understanding of Blockchain Technology

> [W]ithout a functional understanding of the technology itself, it is impossible to appreciate how the language of the law variously captures, clarifies, distorts, and obfuscates the nature of the encrypted machine.[34]

Blockchain is a type of distributed ledger technology, which is a decentralized form of recordkeeping that can store many kinds of information, ranging from monetary transactions to land titles or even digital identities. Such a range of applications is endowed with blockchain being constituted of a cryptographic, secure database distributed on many computers combined with decentralized consensus mechanisms with cryptographic verification.

Ghiro et al. offer a definition of blockchain as 'a distributed ledger that records transactions in a tamper-proof way, ensuring immutability, transparency, and anonymity',[35] highlighting that these three elements are the key to distinguishing blockchain from other distributed ledger technologies. It is also defined as 'a system for achieving consensus about the state of a shared data structure among a set of mutually distrusting parties',[36] where the focus is on the problem of consensus in distributed systems and how blockchain solves it using various mechanisms, such as proof-of-work,[37] proof-of-stake,[38] and byzantine fault tolerance.[39]

Blockchain technology is distinguished by two ingredients—the first one is that it provides a response to the 'missing link' of the digital system, allowing the introduction of 'counterparts' of uncopiable digital goods that are verified and tracked in a network book (ledger); and the second, that it is an undertaking characterized by (joint) participation.[40]

Blockchain is a digital infrastructure with the governance of the architecture being decentralized, where the data is replicated across various nodes. The distributed storage of data offers numerous benefits such as (1) it prevents a single centralized party tampering with the data; (2) there is no master copy, hence no single point of failure, reducing the chances of a possible attack succeeding; and (3) there is less

---

[34] Gill (2018), p. 442.

[35] Ghiro et al. (2021), p. 9.

[36] Werbach (2018), p. 14.

[37] See Dimitropoulos (2020), pp. 1155–1156. In the proof-of-work mechanism, the miner is required to 'proof' their work to propose a new block, which entails dedicating substantial computational power to solve complex algorithmic hash puzzles based on hash function properties. The first miner to propose a block receives incentives to be part of and operate in the network, which are called "block rewards".

[38] See Dimitropoulos (2020), pp. 1156–1157. In proof-of-stake, the influence of each validator's vote is determined by the magnitude of their deposited stake. This mechanism functions by having a set of validators take turns proposing and voting on successive blocks. Validators risk losing their stake if their proposed block is not added to the blockchain, incentivizing them to vote on blocks containing exclusively legitimate transactions.

[39] This mechanism has been explained in this chapter below.

[40] Maxwell et al. (2017), p. 79.

risk of a denial-of-service attack.[41] Disintermediation is the technology's related promise. Due to this very structure, blockchains are widely considered to decentralize and disintermediate economic and legal relations. When 'data' is transferred through blockchain networks, the traditional intermediaries (the State) responsible for verifying and validating transactions, that is, human-based institutions, may become obsolete.[42] As a consequence, the society's institutional framework may evolve into a computational model, reducing the reliance on traditional human-operated physical establishments.

2.1.1.1 Decentralized Architecture

The 'decentralized' technological architecture of blockchain is claimed to be incongruous with the traditional 'State' centralized architectures. But what does it mean for the system to be decentralized? It is an awkward term that is often rushed over without careful thinking. It also does not mean that its center has been removed, creating a void. Technically, the blockchain does not have a single, authoritative administrator. Instead, it is a system in which power is held by a large number of separate parties. Many different actors influence important decisions regarding the blockchain.

Power or decision making may take different forms, depending on a system. It might mean a formal right to vote on specific actions, such as a shareholder's right to vote on whether a corporation will merge with another.[43] It might also mean less formal influence over a decision-making process, such as a large family's discussion of where to go for vacation next year. It might also mean, simply, the inability of a single actor to dictate the policies of others or exercise their power arbitrarily, such as world order under a system of sovereign nation-states.

The fact remains that it is rare to see a fully centralized or fully decentralized system. Instead, most systems combine elements of centralization with elements of decentralization. Even the most centralized governments nowadays tend to have a large number of people involved in decision-making. Even the most decentralized ones give citizens a final say on only a small portion of the workings of government, with the rest being delegated to representatives and administrative bodies. Just as with democracy, the degree of decentralization within the blockchain can be overstated—it is imperative to separate the narrative of decentralization and disintermediation, fact from fiction. Blockchains can be centralized at both the software and the hardware levels. First, one may have a blockchain that runs on very few nodes, all of which can be located in the same room. Another important source of centralization is the software itself—even when the technology is highly decentralized at the hardware level (at the application layer or macro level), it can still be centralized

[41] Bacon et al. (2018), pp. 12–13.

[42] Swan and De Filippi (2017), p. 4.

[43] Van der Elst and Lafarre (2019), pp. 111–137.

at the software governance level[44] (at the infrastructure layer or micro level). When protocol maintenance is managed by a single party or small group of programmers, designers or developers, cumulatively referred to as the 'figure' henceforth, decentralization is hardly a given. Even the most well-known blockchains, such as Ethereum, can be considered as centralized since a few individuals dominate the software development process.[45]

When decentralization occurs, it presents many potential advantages. For one, political philosophers have argued that decentralization promotes freedom and equality.[46] In democracies, citizens can vote how they like, and their votes all count equally.[47] Of course, the reality is more complex than this; even in a well-functioning democracy, powerful or wealthy citizens may exert a disproportionate influence over politicians and their policies. But the basic principle—the decentralized systems promise to grant participants a greater degree of freedom and equality—is a plausible one. Decentralized systems also benefit from being able to aggregate the knowledge and ideas of the many.

Instead of relying on a central decision-maker's wisdom on how a system should be run, decentralized systems rely on the collective wisdom of the masses. To the extent that these masses have better knowledge about relevant information, they should be able to make more informed decisions than a single authority. Notably, blockchain aims to solve the Byzantine Generals Problem, a classic problem in computer science dating back to the early 1980s, which questions how distributed computer systems can achieve consensus without depending on a central authority while also being resilient to attacks from malicious actors.[48] It hypothesizes a scenario that involves three divisions of the Byzantine army, each led by an independent general situated outside an enemy city. To coordinate an attack, the three generals must agree on a common plan of action. However, communication between them is limited to messengers, and there is a traitor among them attempting to disrupt the consensus by either deceiving them into premature attacks or withholding crucial information to prevent coordinated action. The blockchain resolves this dilemma through a probabilistic mechanism.[49] It mandates that information transmitted across a network of computers be transparent and verifiable through complex mathematical problems requiring substantial computational resources to solve. This mechanism makes it challenging for potential attackers to manipulate a shared database with false data unless they have a command over a majority of the computational power within the network.[50] Consequently, blockchain protocols guarantee the validity of transactions and prevent duplicate entries in the shared ledger, which

[44] De Filippi (2019), pp. 3–5.

[45] Efe et al. (2018), p. 24.

[46] Treisman (2007).

[47] Jacob (2021), p. 61.

[48] Lamport et al. (1982), p. 382; Lamport (1983), p. 668.

[49] Nakamoto (2008), pp. 6–8.

[50] Nakamoto (2008), pp. 6–8.

enables users to coordinate transactions in a decentralized manner without relying on a trusted intermediary to authenticate and approve each transaction.[51]

2.1.1.2 Distributive Ledger

According to the ISO standards, 'a distributed ledger is a ledger that is shared across a set of DLT nodes and synchronized between the DLT nodes using a consensus mechanism'.[52] Any participant in the network can maintain a representation of the ledger that matches all the others.

The blockchains are logically centralized, that is, there is only one ledger, but organizationally decentralized, insinuating that many entities maintain copies of that ledger. Computers directly participating in a blockchain network, often called full nodes, constantly communicate to remain synchronized. Though maintaining synchronization, called consensus mechanism, is the hard part, such consensus protocol provides consistency to the ledgers in the blockchain network. Consensus is established when the protocol can ensure that each node adds the same blocks to its local version of the blockchain. The fact that all network users follow the protocol's pre-determined rules in deciding how to update the ledger can be considered the source of trust in the system. Indeed, trust in technology is said to replace trust in humans. It is the essence of the consensus mechanism that users can have confidence that a certain outcome is reached before it is effectively reached because of the characteristics of automatically executing and enforcing the 'immutable' encoded rules without any third-party interference once the pre-defined requirements have been fulfilled.

2.1.1.3 Cryptography

Another distinctive architectural element of blockchain that instills trust is cryptography, as they 'enforce decisions based on the difficulty of reversing cryptographic mathematical transformations'.[53] In the past, too, cryptography has served as a tool to hide political and military information, tracing back to the era of Julius Caesar, where he communicated by employing a simple cipher known as the 'Caesar cipher'[54] or 'Caesar shift'.[55] In blockchain, there are two cryptographic tools that are particularly important: public key infrastructure (PKI) and hash functions. Cryptography is an inherently political tool, as it 'rearranges power: it configures

[51] Meiklejohn and Orlandi (2015), p. 127.

[52] Distributed ledger is defined at point 3.23 of ISO 22739:2024 (En). See ISO (2024). https://www.iso.org/obp/ui/en/#iso:std:iso:22739:ed-2:v1:en:term:3.54.

[53] Finck (2018), p. 28; Rogaway (2015), pp. 10–17.

[54] This involved shifting the alphabet three places to the right and wrapping the last three letters (X, Y, Z) back onto the first three letters.

[55] Luciano and Prichett (1987), p. 3.

who can do what, from what'.[56] The use of PKI underlines that transactions on a blockchain are pseudonymous in nature.[57] While the information stored on the ledger is usually encrypted, metadata about the accounts involved in transactions is usually not. It is, accordingly, relatively straightforward to link such pseudonymous identities belonging to the same individual through the statements they make. However, when in wrongful hands, such a tool can be used for malicious purposes such as infringement of data protection rights of an individual, since 'calculative' linking of pseudonymous information results in the identification of the person.[58] This is one of the reasons why blockchain is considered to promote 'alegality'[59] by design since such systems are capable of facilitating and encouraging actions that are outside the boundaries of the law through their technological affordances.

2.1.1.4 Immutable Character

Though blockchains are conventionally branded as 'immutable', they are not immutable at the application layer;[60] however, at the micro level, the code embedded in the blockchain is still considered immutable. Indeed, various participants can collude to alter the current state of the ledger, similar to in a democracy, where wealthy and powerful citizens may conspire to influence the State and their policies. Although amending the ledger is not impossible, it is extremely hard and unlikely. There are no technical solutions, aside from compromising the integrity of the entire system that would allow for the reversal of a transfer.[61] In fact, blockchain is an 'ongoing chain of hash-based proof-of-work'.[62] Any change to the blockchain network is extremely difficult, even through human intervention. It is for that reason that it is preferable to refer to distributed ledgers as 'tamper-evident'. Through their 'tamper-evident' nature, blockchains freeze the information entered or code programmed, and the smart contracts' execution in the future cannot be halted even when users change their minds.[63]

---

[56] Rogaway (2015), p. 1.

[57] Tao Feng et al. (2019), pp. 2, 12; De Filippi et al. (2022b), p. 2.

[58] Zyskind and Nathan (2015), pp. 180–184.

[59] Gavin Wood, who is one of the co-founders of Ethereum, proposed this term in the blockchain space back in 2014. The term aimed to advance the notion that decentralized blockchain-based systems can be likened to natural forces.

[60] Walch (2016), p. 713.

[61] Werbach and Cornell (2017), pp. 331, 335.

[62] Nakamoto (2008), p. 1.

[63] De Filippi and Hassan (2016). https://firstmonday.org/ojs/index.php/fm/article/view/7113/5657.

2.1.1.5 Off-Chain and On-Chain Governance

Blockchain-based systems operate under the governance of two distinct sets of rules: the 'legal code' which speaks of the off-chain governance, encompassing rules imposed by external entities onto the community using the blockchain, where these rules may include national laws, contractual agreements, technology standards, and other regulations, and the 'technical code' relating to the on-chain governance which entails the rules and decision-making mechanisms directly encoded into the foundational infrastructure of a blockchain-based system.[64] On-chain governance is not easily circumvented since it operates within the system itself, enforcing algorithmic rules encoded directly into its architecture. While the legal code is considered 'extrinsic', allowing for rule-breaking, the technical code is 'intrinsic', triggering an error message upon any breach.[65] Where off-chain governance necessitates elements of trust beyond technological solutions involving nodes, miners, developers, and institutional entities, on-chain governance primarily relies on integrating technological assurances into the technical framework of the blockchain.

The replicated structure and decentralized management of blockchain echo the hypothesis that the involved parties cannot be trusted, so the ledger must not be held or administered in a centralized fashion. The removal of the human or institutional third-party forms a core value proposition of blockchain networks which provides 'trustless trust' as participants do not need to know or rely on each other when exchanging value, ensuring complete confidence without the need for intermediaries.[66] Rather than relying on trust in humans or institutions, blockchain-based transactions are powered by trust in technology. For instance, a smart contract is essentially a code on the blockchain that functions like a traditional legal contract, free from the potential corruption of a human agent. This allows the parties involved to structure their relationships more effectively in a self-executing manner, eliminating ambiguities often associated with verbal or written agreements.

Relying on source code allows interested parties to simulate the execution of a contract and model its performance before actually implementing it.[67] However, importantly, this doesn't remove trust; it just changes the instance in which it is placed. Human decision-making cannot be replaced completely since humans are still required to design and write codes, maintain protocols, and reach an agreement on the terms of a smart contract.

The 'trustless trust' narrative is anchored in what game theory maps as the problem of cooperation.[68] The problem of trust is traditionally solved by parties' incentives to maintain their reputation or by relying on trusted third parties, such as the

[64] Werbach (2018), p. 487.

[65] Lehdonvirta and Ali (2016), pp. 40, 41; Werbach (2018), p. 137.

[66] Hoffman (2014). https://www.linkedin.com/pulse/20141117154558-1213-the-future-of-the-bitcoin-ecosystem-and-trustless-trust-why-i-invested-in-blockstream.

[67] Sklaroff (2017), p. 263.

[68] North (1990).

State and its legal system. Blockchains promise to replace these mechanisms with their technical protocol.[69] From this perspective, blockchains serve as technological artifacts that substitute for the necessity of trust between organizations. This explains why, to some, blockchains are an ideology rather than a technology, expressing the preference for a world where trust is put into cryptography rather than humans. As such, blockchains now serve a trust function previously performed by the rule of law, which anchors the capacity and legitimacy of legal systems in effectively addressing cooperation issues.[70] It is worthwhile not only to determine how the law should react to this new technology but also because replacing trust generated by the legal system with a machine-based trust may have lasting implications for the rule of law.

It may be reiterated that blockchains do not make trust disappear; they just substitute 'trust in humans and institutions (the State)' with 'trust in technology'. The tentative outcome of this ideology of trusting technology is a lack of control by the centralized State authorities. While the participants have to abide by the rules contained in the protocol, the technology affords the benefits of a tamper-resistant, 'trustless' database devoid of the need to have any overseeing entity. Indeed, the rules and principles comprised in blockchain code are not a product of the technology itself but, rather, of the humans who create it, that is the 'figure'. Software is, accordingly, never neutral but reflects the objectives and beliefs of those who use it as a means of expression.[71] Trusting a blockchain or blockchain-based application ultimately requires trust in the collectivity of individuals, the 'figure', who architect or code programs, as well as in the procedures that govern their behavior and manage their accountability—or the absence of such norms and institutions.

2.1.2 Public, Private, or Permissioned Blockchain

Based on the activities performed by the blockchains and how they are configured to control the access and design objectives by the 'figure', blockchains can be categorized as public, private, or permissioned. Public or permissionless blockchains are accessible and offer anonymity, allowing individuals to participate in the network without revealing their identities or consenting to specific system rules or terms of use. The sole requirement for participants is adherence to the rules encoded in the algorithm.[72] In principle, all network members are equal and enjoy the same rights to read, write, and audit all the activities without authorization. All participants agree to a single version of data, and a trusted third party or a central intermediary, who would verify and guarantee the accuracy of transactions, is not required.

[69] Pereira et al. (2019), p. 94.

[70] Yeung (2017), pp. 12–13.

[71] Balkin (1998).

[72] Low and Mik (2020), p. 139.

This consensus achieved with delegation of power of control (decentralization) is based on the premise that most network participants are non-malicious. Indeed, blockchain is a 'trust machine', representing a 'shift from trusting people to trusting math',[73] allowing for 'trust by computation'[74] across a decentralized network. Unlike a public blockchain, which is completely decentralized in nature, private and permissioned blockchains operate quite differently, restricting participation to identified participants who adhere and subscribe to predefined system code rules. These rules, often equated with 'terms of use' or 'master agreements', dictate the eligibility criteria for joining the system and how it operates and are designed in a manner where the technology tends to impose certain constraints on users concerning reading, writing, and accessing the information by trusted entities in the network.[75] Such permissions are granted depending on the sensitivity of the data processed by the blockchain.[76] Since participants are already identified and obligated to follow specific rules, there's no necessity for the system to be 'trustless'. This means their consensus algorithms don't require code designed to prevent selfish actions. Typically, a structured governance procedure is followed, where coders are identifiable, and their code is rigorously vetted before integration into the system. Instead of relying solely on technology, non-compliant participants are subject to legal accountability. Essentially, the system hinges on traditional trust mechanisms.[77]

Technology often influences our behavioral patterns through a backdoor mechanism, creating a deep-rooted understanding that allows us to interact with it effectively.[78] In the case of a blockchain-based application, the 'figure' is the one with the ability to enforce normative effects on the users and the society, that is, regulate and govern the behavior of the users by either restricting or inviting their actions,[79] regardless of whether such regulation or action is lawful or unlawful, through the code embedded in the blockchain. The blockchain's unique attributes, such as 'decentralization, transnationality, tamper-resistance, pseudonymity, lack of coercion, trustless-ness, and operational autonomy',[80] when working in unison, make it impenetrable by the conventional legal system—thus the blockchain technology can be said to challenge the existing legal orders in which it functions.[81] This renders certain activities conducted through blockchain networks beyond the scope of legal recognition or comprehension. Thus, blockchain technology can be seen as 'alegal',

[73] De Filippi et al. (2020), p. 6.

[74] Antonopoulos (2014). http://radar.oreilly.com/2014/02/bitcoin-security-model-trust-by-computation.html.

[75] Guegan (2017), pp. 4–5.

[76] Peck (2017), p. 38.

[77] Low and Mik (2020), p. 140.

[78] Hildebrandt (2008), p. 178.

[79] See this chapter, Sect. 2.2 for further explanation.

[80] De Filippi and Wright (2018).

[81] De Filippi et al. (2022a), p. 358.

creating and establishing a new normative order by facilitating activities that are neither legal nor illegal and are distinct from alegal actions.[82]

2.2 Normative Effects of Blockchain Code on Law

The typical pattern throughout human history has been that new technologies and discoveries create new architectures,[83] where every technology is a reflection of unabridged visualization of the world and identifies themselves with their own suite of impressions, symbols, and similes.[84] De Filippi compares blockchain to 'Plantoid' to draw out its features, which, according to her,

> illustrates its ability to create 'blockchain-based lifeforms', that is, algorithmic entities that are (1) autonomous, (2) self-sustainable, and (3) capable of reproducing themselves, through a combination of blockchain-based code and human interactions[85]

and thus presenting blockchain as a living instrument with the capability to grow in society. From a cursory glance at the fictional framework of the blockchain (each technology involves both a functional and fictional dimension),[86] its intentions, impressions, and principles appear to be closely associated with those of digitization. In a way, the idea of creating laws, institutions, frameworks for governance, and subject positions by programming and coding of algorithms by the blockchain community has an equivalence with the idea of digitization, which is broadly based on 'governance by numbers', an ideology introduced by Alain Supiot.[87] This philosophy, almost a dogma, came into existence at the intersection of communism and ultraliberalism. That means it is an intersectional outcome of, on the one hand, the dream of a 'society without heteronomy',[88] which considers the law and the State as mechanisms of power that violate individual sovereignty, and on the other hand, the belief and deep trust in the power of numbers and computational ability as the basis of society, law and subjectivity and ultimately, the belief in the likelihood of coding them.[89] Essentially, the philosophies and principles that are promoted by blockchain start where the 'governance by numbers' ideology ends or when the 'exhaustion' of public trust in institutions creeps in.[90] Further, blockchain drives in newer perceptions of the society and self and influences the imaginary bases of our societal norms

[82] Wood (2015). https://www.youtube.com/watch?v=Zh9BxYTSrGU.

[83] Garcia (2009).

[84] Baudrillard (1968), p. 39; Feenberg (2012).

[85] De Filippi (2017), p. 51.

[86] Musso (2021), p. 83; Becker (2022), p. 113.

[87] Supiot (2015) and Mennicken and Salais (2022).

[88] Supiot (2015), p. 408.

[89] Supiot (2015), pp. 175, 244.

[90] Vigna and Casey (2019), p. 23.

with its claim to possess the ability to obviate the need for a trusted third party 'intermediary' to free the individual from any institutional constraints.

Blockchain is not just a technology but also a social and political phenomenon that challenges the existing paradigms of governance and regulation. It brings in the new normative architecture of 'alegality' by design, which was initially introduced to transcend and circumvent the central authorities. This intriguing perspective has been further expanded by framing it within Lindahl's concept of 'alegal acts', which denotes acts that defy conventional legal categorization due to their inherent strangeness or incomprehensibility within existing legal frameworks.[91] The intentional design aspect of the technology is emphasized here—particularly blockchain technology, which is overlooked in Lindahl's analysis of 'alegal acts' with respect to how the blockchain can be designed to support or facilitate such alegal acts. Thus, blockchain technology embodies a form of political activism, challenging established legal orders and advocating for alternative normative orders.

As smart contracts, decentralized organizations, algorithms, and source code become more prevalent in our daily lives, we may witness the rise of *algorithmic governance*.[92] This new normative system has the potential to regulate society more efficiently, decreasing the costs of law enforcement and providing a more customized set of rules tailored to each citizen. Additionally, these rules can be continuously updated based on individual preferences and profiles.[93] Thus, there arises a normative question regarding whether existing code-based regulations could and should supersede human judgment in decision-making, along with the ethical and political implications therein.[94] Blockchain technology is poised to revolutionize legal discussions concerning the fundamental components of legal systems, including substantive law, legal frameworks, and legal ethos. This is why enthusiasts argue that blockchain is designed to embark on a mission to counter the very foundational principles of a society governed by law;[95] that is, blockchain supposedly encodes a consensually and forge-proof vision of the world, a 'truth that's more reliable than any truth we have ever seen'[96] and paves way for a new legal regime where the code assumes the role of a symbolic referent and concurrently, abolishes the need for the mentioned bond of faith.

The widespread utilization and acceptance of smart contracts facilitate individuals in creating and establishing personalized legal systems where they are free to choose and enforce their own rules.[97] Thus, blockchain has the potential to facilitate the establishment of a decentralized alternative to the existing legal system. This alternative would involve (code) rules interacting autonomously, ensuring reliability

[91] Lindahl (2013), pp. 697, 730.

[92] Wright and De Filippi (2015), p. 41.

[93] Wright and De Filippi (2015), p. 41.

[94] De Filippi and Hassan (2016). https://firstmonday.org/ojs/index.php/fm/article/view/7113/5657.

[95] Walport (2016).

[96] Vigna and Casey (2019), p. 20.

[97] Wright and De Filippi (2015), p. 40; Kaeseberg (2019), p. 107.

and predictability without reliance on third-party institutions for enforcement. Unlike conventional legal systems, which impose provisions that are universal and applicable to everyone regardless of their informed consent, this new paradigm allows individuals the freedom to choose from a defined range of provisions that better align with their preferences and needs. As such, individuals could even have the option to engage with multiple regulatory frameworks simultaneously, arbitrarily transitioning between them based on situational factors and contingencies.[98]

Contrary to centralized organizations, where decision-making is top-down, decentralized organizations encode decision-making directly into source code.[99] By enhancing coordination and trust, blockchain enables novel forms of collective action, addressing issues like opacity and corruption inherent in the decision-making of many organizations.[100] While large hierarchical organizations suffer from centralization, delegated decision-making, and regulatory capture, blockchain technology aims to mitigate these flaws. Blockchain-based decentralized organizations are being used to facilitate individuals and machines to coordinate through codified smart contracts, bypassing the need for traditional business structures. The interactions within decentralized organizations, predefined by smart contracts, are in the form of affordances and constraints, fostering trust through code transparency and auditability.[101]

In essence, decentralized organizations whose operations can be scrutinized by millions of eyes, afford everyone to have access to the 'truth-realities'[102] of a blockchain determined by algorithms. In fact, only supposedly harmoniously coded algorithms at the pedestal of the blockchain need to be trusted. The impact of this phenomenal power of code is two-pronged. One, it serves as a cornerstone for programming a number of life-governing legal applications. For instance, instead of traditional institutions regulating motor accidents, self-driving (autonomous) cars could be coordinated and managed through advanced algorithms that have the potential to significantly decrease accident rates on the road. If a collision is forthcoming, an ethical algorithm could swiftly evaluate the contextual setting and determine the best course of action based on factors such as the number and reputation of individuals or objects at risk and the system's designed-in optimization criteria, thus minimizing the accident's impact. This would necessitate instilling a set of moral standards and ethical precepts in these artifact's algorithms,[103] although the same may ultimately fail without human involvement. And two, it challenges the traditional institutions or human agents with regard to not only their trust potential but also the necessity of their service by providing a regulatory space, who conventionally perform as the messengers of a society's underlying (truth-)vision of the

[98] Weber (2018), p. 701.

[99] Wright and De Filippi (2015), p. 16.

[100] De Filippi and Mauro (2014).

[101] De Filippi (2017), p. 53.

[102] Becker (2022), p. 113.

[103] Wright and De Filippi (2015), p. 41, see footnote 152.

world. In other words, in addition to supporting or complementing the law, code can also serve to circumvent or bypass the law, as evidenced in the case of Napster,[104] which offered a platform for users to share music files.

Code may also introduce new rules which have little or nothing to do with existing laws. For example, many Peer-to-Peer (P2P) file-sharing protocols incorporate requirements in their code mandating users to share content before accessing more, thus enforcing a form of collaborative behavior among users. However, the influence of code in shaping online behavior extends beyond this aspect. Particularly significant in this regard is the role of Graphical User Interfaces, extensively examined in fields like Human-Computer Interaction and Science and Technology Studies, to scrutinize their social and political ramifications.[105]

2.2.1 Lex Cryptographica

In the blockchain, the new code rules encoded with 'values and principles' assume the role of customary law and govern the behavior of the users rather than the conventional law—as *lex cryptographica*. *Lex cryptographica* is characterized as

> the law that is no longer legitimized by a culturally established symbolic referent which it no longer needs to be as there is no longer a need for recognition or belief: by programming the code, the parties to a smart contract are making law, implying—or rather coding—the values they take to be fundamental.[106]

Zou focuses on the political and social dimensions of law, leading to his interpreting *lex cryptographica* as 'a system of algorithmic control that entails 'order without law' in its architectural design'.[107] These definitions illustrate that *lex cryptographica* has created a new form of law that is self-sufficient in terms of regulating and organizing itself, which does not rely on any external referent or recognition; is autonomous and anti-representational, and disrupts the cultural and symbolic aspects of conventional law, thus challenging the system. Wright and De Filippi alternatively describe *lex cryptographica* as 'rules administered through self-executing smart contracts and decentralized (autonomous) organizations'.[108] Hacker uses this definition to raise concerns regarding the 'non-regulatability' of blockchain, where he defined *lex cryptographica* as

> the private and mostly technical framework that effectively governs a blockchain, and which consists in an amorphous and highly decentralized set of socio-technical agencements, supporting a range of application protocols, that sit on top of the transportation layer

[104] Ku (2002), p. 263.

[105] Kannabiran et al. (2011), p. 695.

[106] Becker (2022), p. 113.

[107] Zou (2020), p. 645.

[108] Wright and De Filippi (2015), p. 4; De Filippi and Wright (2018), pp. 48–49, 144.

> of the Internet network (the TCP/IP stack) and cannot be linked to a central note that can be easily identified, and eventually regulated, by a national or international legal framework.[109]

Therefore, *lex cryptographica* is instituted primarily by a new quasi-legal structure of smart contracts, which are being deployed to regulate and initiate multifold trustless trust relationships. This law or legal framework created by blockchain demonstrates to what extent it introduces a displacement of the conventional law and the symbolic and imaginary basis on which it is based. By utilizing more complex systems of smart contracts and decentralized organizations, this technology can be employed to create and establish rules and frameworks for organizations, formal entities, and the State institutions. When designed to incorporate human feedback, it can also embody community values and society norms, which are then automatically enforced through self-executing code.[110]

Lex cryptographica not only uncouples itself from traditional symbolic referent as its legal legitimacy but also progresses to emancipate from artificial geographical and political territories. Essentially, *lex cryptographica* claims that any sort of attachment to a traditional corpus or territory is no longer necessary, nor does it require to be legitimized by a culturally established symbolic referent as there is no longer a need for recognition or belief. The idea of law draws its legitimacy from the decentralized and algorithmic establishment[111] since decentralized organizations function based on defined rules and protocols established by smart contracts and code,[112] independent of the conventional system. The 'governance by numbers' ideology was the first to move forward towards making the law territory agnostic by substituting the traditional approach of defining law based on territorial jurisdiction with a focus on the utility of their legal content.[113]

In pursuit of a 'matter-free existence', digitization, considered as the initial step, has already taken off. As early as 2014, Estonia introduced an e-residency program, which envisages a virtual residency, which is supposed to be 'an international passport to the virtual world'.[114] While this passport essentially represents an entry ticket to the Estonian economy, e-citizens remain generally bound by their 'national identity' and, as such, remain tied to the corpus as well as to the body of the nation ('biological citizenship').[115] Blockchain-based subjectivity, however, is conceived as purely virtual and code- or else data-based, and thus independent of any institutional pre-definition. As such, the individual identity is no longer solely dependent on legal citizenship or physical presence in a country. Instead, the transnational, digitized individual acquires a 'self-sovereign identity'. This empowers individuals to manage their identity-related information independently, without the need to rely

[109] Hacker et al. (2019), p. 15.

[110] Wright and De Filippi (2015), p. 50.

[111] Finck (2018), p. 80.

[112] Wright and De Filippi (2015), p. 15.

[113] Mennicken and Salais (2022); Supiot (2008), p. 151.

[114] Sullivan and Burger (2017), pp. 470, 472.

[115] Heinemann and Weiß (2016), p. 8.

on any trusted authority or intermediary,[116] fostering trust and enabling secure sharing of information with multiple independent parties across wide networks.

The individual subjects draw their power, depending on their legal pursuits, to define the rules on a case-to-case basis—rules that are automated, peer-to-peer, and globally operative to legitimize their own existence. To that extent, individuals are bound by code alone or *lex cryptographica,* which stands on an 'acephalous and fluid foundation',[117] which implicitly means that it is individually negotiable, and various terms, conditions, and provisions of law depend on the retrospective transactional context or on the membership of the chosen 'cloud community'. From that perspective, the subject is envisaged as not only being disconnected from the heteronomous sovereignty of the State and law but also from the heteronomy of its own body. This thought on *lex cryptographica* begins with the idea of 'decentralized government service', which comes from the notion that residing in a specific geographic area should not confine individuals to specific government services, and ends with the plans for 'personal thinking blockchains', in the sense of 'mind files', that is,

> the recording of every 'transaction' in the sense of capturing every thought and emotion of every entity, human and machine, encoding and archiving this activity into life-logging blockchains.[118]

2.2.2 Social and Political Implications

As with every other technology, blockchain is also not neutral. It is a technical artifact with a particular *architecture*, which inevitably has both social and political implications, as it facilitates certain actions and behaviors more than others. *Lex cryptographica* produces a normative effect through the utilization of programming languages, depending on the political intention of the 'figure'. This includes, for instance, the implementation of smart contracts either to facilitate hourly or daily payment for employees, with taxes being automatically sent to government entities in real-time, or to promptly and automatically verify State death records and allocate assets from a testator's estate, including sending taxes to relevant agencies without the requirement of probate administration.[119] The conception that blockchain technology should take the place of the State and law is largely 'misguided'. The success of blockchain largely depends on their acceptance and recognition in the real world, and to have a pragmatic impact, the artifacts must be compliant with the prevailing legal frameworks.[120] Thus, establishing and administering a

[116] Wang and De Filippi (2020), pp. 28, 33.

[117] Becker (2022), p. 113.

[118] Swan (2015), pp. 43, 47.

[119] Wright and De Filippi (2015), p. 12.

[120] Finck (2018), pp. 85–86.

completely virtual and body-less, text-less, and State-less social life through blockchains appears to be highly improbable, unrealistic, and utopian or rather dystopian. This negativity, however, has not deterred the growing recognition of blockchain technology in certain applications in legal-political contexts. For example, the government of the Zug region in Switzerland conducted an experiment using a blockchain prototype to issue government identity cards for voting in their direct democracy.[121] There are also situations where a government is unreliable, and blockchains offer solutions. The United Nations has implemented programs that provide individuals with a digital identity that can be verified with eye scans, allowing individuals to receive funds and food.[122] These applications, thus, have a significant impact on the fundamental rights of individuals which forms the essence of the rule of law framework.

Due to the impact of blockchain technology on the fundamental rights of individuals, it seems that the rule of law and *lex cryptographica* are intended to function alongside each other—the rule of law exists outside the blockchain while the *lex cryptographica* governs within the blockchain. Therefore, in the absence of State-imposed justice, code embedded in blockchain can create an equivalent in both determining the rules and ensuring that they are enforced.[123]

2.2.3 Enabling a New Normativity

As has been postulated, the blockchain protocol, with its embedded code, replaces the traditional legal order. This technology is conducive to partially supplanting and/or supplementing the legal order whilst also being a 'target' of law and regulation, with the regulatory State asserting its sovereign power.[124] The blockchain enables a new normativity of decentralized governance, where the rules are embedded in the code and enforced by the network rather than by human authorities or institutions. De Filippi calls this 'the rule of code' and contrasts it with the rule of law, which is based on the authority and legitimacy of the State and the legal system.[125]

This assertion of 'code taking the shaping of law' is not novel, but flows from the famous equation, 'code is law', coined by Lessig in the late 1990s.[126] The seminal work of Lessig explores how, in cyberspace, code complements or even substitutes law as a normative order. Due to smart contracts based on blockchain technology

[121] Zug Digital ID: Blockchain Case Study for Government Issued Identity' (Consensys, 2018). https://consensys.io/blockchain-use-cases/government-and-the-public-sector/zug.

[122] Juskalian (2018); Dimitropoulos (2022), p. 328; Coppi and Fast (2019).

[123] Schrepel (2020), pp. 368–370.

[124] Yeung (2019), p. 207.

[125] De Filippi and Wright (2018) and De Filippi et al. (2022b).

[126] Lessig (1999a), p. 3.

and their self-executing nature, the two components of that equation seem to converge even further. De Filippi and Hassan reversed the equation, claiming that 'law is code', that is, that law itself can be codified and defined as technological code –

> As a result of these technological advances, the lines between what constitutes a legal or technological rule becomes more blurred. Since smart contracts can be used as both a support and as a replacement to legal contracts.[127]

They presented four phases that led to the origination of the normative order of 'law turning in code':

> The first phase involves the process of digitizing information —turning paper and ink into computer-readable information. The second phase consists in bringing automation to decision-making processes. The third phase involves the incorporation of legal rules into code on the one hand and the emergence of regulation by code on the other. The fourth phase —which is just beginning— involves a new approach to regulation, the code-ification of law, which entails an increasing reliance on code not only to enforce legal rules but also to draft and elaborate these rules. .....today, code is also used by the public sector as a regulatory mechanism…. mostly related to the ability to automate the law and to enforce rules and regulations a priori, i.e., before the fact.[128]

Blockchain is, therefore, argued to have the potential to reinforce and complicate this tendency of imposing normativity as it enables code to run autonomously, with very limited third-party intervention, and to produce real effects in terms of value transfers.[129] Unlike traditional legal rules that are only enforceable after the fact (*ex-post*), regulation by code can proactively restrict individual actions, ensuring compliance before any potential violation takes place (*ex-ante*). In other words, code-based regulation prevents people from violating technical rules even before they have the chance to act.

As the effects of the smart contracts are indelibly written in the relevant code, the parties can easily bypass the traditionally necessary, contractual safeguards. This process would condition both modalities of negotiation and stipulation of the contract and the whole system of guarantee prescribed by the national or international contract law system, which encompasses principles, such as *bona fide*, or institutions, such as *force majeure*, and the hardship clause, or of vitiating factors. Thus, smart contracts represent the mere implementation of legal and technical rules into the code of a particular infrastructure or device. The trustless nature of blockchain doesn't directly ensure enforcement of these rules, except for the fact that it eliminates the necessity for a trusted intermediary to mediate any transactions. What distinguishes blockchain from other technologies is that programs stored on a blockchain are designed to supplant traditional legal contracts. They are no longer merely auxiliary mechanisms for enforcing existing legal frameworks; rather, their code is intended to function as the law itself. Consequently, as more contractual terms or legal rules are encoded as smart contracts instead of traditional legal

[127] De Filippi and Hassan (2016). https://firstmonday.org/ojs/index.php/fm/article/view/7113/5657.

[128] De Filippi and Wright (2018), pp. 193–204.

[129] Yeung (2019), p. 13.

agreements, blockchain evolves into a regulatory technology[130]—a tool capable of defining, incorporating, and enforcing legal or contractual provisions through code independent of the existence of underlying legal rules.

However, translating legal regulations (referred to as 'wet code') into technical specifications (referred to as 'dry code') is often challenging.[131] Legal language is inherently open to interpretation and adaptable, allowing for case-by-case application to unforeseen circumstances. It intentionally maintains ambiguity to facilitate flexible application. A robust regulatory framework emerges from the convergence of numerous legal provisions, incorporating various limitations and exceptions to accommodate the complexity and unpredictability of human society. Conversely, technical code operates on rigid, formalized principles, necessitating well-defined categories and precise specifications of methods and conditions in advance.[132] Despite the fundamental disparities that subsist between these two typologies, there is a growing trend to translate legal rules into technical rules for incorporation into technological hardware or software, although enforcement of code can be stringent and intrusive. Poorly designed regulation by code may inadvertently work against the interests of those it aims to regulate. The decentralized nature of blockchain technology, along with the capabilities of smart contract code, which enable the creation of autonomous, self-sufficient, and potentially unstoppable DAOs, also presents new challenges concerning legal accountability and regulatability. Therefore, legal systems must devise methods to regulate code to mitigate its potentially disruptive effects.

Without any exaggeration, it can be said that the conditions engraved in the smart contract are 'alive' with the capability to self-execute without any requirement of human intervention, akin to the notion of blockchain as a 'plantoid',[133] exhibiting characteristics reminiscent of a living entity. To illustrate, blockchain-enabled smart contracts can be utilized to automatically verify decentralized online identity and digital criminal records to assess and determine whether an individual meets specific preconditions for gun ownership—who can and who cannot own or use guns; and those meeting the criteria will be allowed to purchase a gun, whereas those who fail to meet these requirements would be denied from completing the purchase.[134] This illustration shows that smart contracts are just waiting for triggers for the encoded rules. These are not 'some' passive instructions coded for contracting parties to execute; rather, it can be said, by drawing parallels with human agents, smart contracts are more akin to 'autonomous agents' which 'live' inside the execution

[130] Yeung (2008), p. 88.

[131] De Filippi and Hassan (2016), https://firstmonday.org/ojs/index.php/fm/article/view/7113/5657.

[132] De Filippi and Hassan (2016), https://firstmonday.org/ojs/index.php/fm/article/view/7113/5657.

[133] De Filippi (2017), p. 51.

[134] Wright and De Filippi (2015), p. 36.

environment, ready to perform or execute a specific piece of code when nudged by a transaction.[135]

Additionally, there may be instances where the code can be applied to establish a concatenation of technological configurations that might potentially restrict the exercise or assertion of property rights of individuals concerning a specific object. For example,

> access to the property can be programmatically limited to specific users or devices, or even be limited to a person who is identified in a record on a blockchain. When brought to the extreme, every piece of property could be tied to a potential kill switch, whereby property could be disabled or divested remotely through the simple click of a button or a computer algorithm, resulting in property ownership vanishing. In such a world, property ownership could vanish, replaced by a web of temporary leasehold interests governed by contracts.[136]

Thus, the code implements changes to the laws governing the blockchain realm.

There is a mix of volunteer and paid software developers who write and update the code, determining how to revise the code through informal processes based on a general sense of consensus, without being governed by any fixed legal or organizational guidelines.[137] Furthermore, some individuals who contribute to shaping the code do not actually write it—these may include people reviewing it or doing research and making recommendations about the policy and technical goals of the system. In this context, Walch has used the term developer to encompass

> those making decisions about the policy choices, to be embedded in the code, how best technically to manifest these choices, and then actually crafting, and reviewing the code to achieve those policy and technical choices.[138]

Within this group of contributors, importantly, not all participants are equal. For instance, in open-source software ventures such as public blockchain, a cadre of core developers typically spearhead the software development trajectory.[139] This means that, these individuals serve as the leading figures and decision-makers concerning the code and manifest power differently from that of rank-and-file developers. In the Bitcoin framework, core developers possess the capability to broadcast emergency messages to all network nodes and are the sole individuals with privileged access, enabling them to implement actual modifications to the software code,[140] while other developers can suggest and propose changes, but the same can only be incorporated by a core developer. Additionally, prominent developers play a pivotal role in shaping how blockchains are perceived by both the State and the broader public.[141]

---

[135] Ethereum Foundation Blog (2015). https://blog.ethereum.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology.

[136] Wright and De Filippi (2015), p. 35.

[137] Bayern (2014), p. 108.

[138] Walch (2019).

[139] Wahab et al. (2024), p. 287; Bosu et al. (2019), p. 2636.

[140] Simonite (2014), p. 21.

[141] Renwick and Gleasure (2021), p. 16.

Within the blockchain realm, the code is at once a rule and reality where normativity impacts the descriptiveness.[142] The blockchain technologies, such as cryptocurrencies, can shape our social reality by creating and enforcing rules through code. Since blockchain can facilitate a fundamental shift in authority from State-administered legal frameworks to decentralized systems governed by code-based rules and protocols,[143] the *lex cryptographica* poses a significant threat to the traditional distribution of social and economic power.[144] This shift could diminish the role of intermediaries, who traditionally managed and influenced the actions of diverse individuals.[145] Such changes intersect profoundly with the rule of law, a cornerstone of democratic societies, where centralized authorities, such as the State, are responsible for regulating individual behavior by interpreting laws, adjudicating disputes, and ensuring compliance with regulations. Therefore, not only may this technology be a target of law and regulation,[146] but it may also be used as an alternative to or displacement of law and legal ordering.[147]

Given the greater degree of autonomy that characterizes these systems, it becomes imperative to regulate the technology or shape the artifact in such a manner that it does not transgress the rule of law. This raises an important question: can some of the basic principles and philosophies of the rule of law be absorbed into the rule of code? While achieving complete absorption may be an aspiration, even a limited adaptation warrants serious consideration.

To explore this incorporation, one must study the procedural rules and substantive constraints applicable to traditional (centralized) governance structures. These elements not only require adaptation to accommodate the newer technological innovations but also necessitate careful examination of how these rules can be enforced, short of formalizing a sovereign authority with coercive power.

2.3 Approaches to Shape Blockchain

Altering the characteristics of the blockchain code through legal means is a considerably challenging process. While it may seem challenging, it is not impossible—law can or must be employed as an instrument in guiding, influencing, and shaping the attributes of blockchain code in a much more tangible manner. Law as a tool can profoundly shape and influence the process of technological change and its diffusion at numerous levels. Law can be used as a weapon in the initial 'framing

[142] Reijers and Coeckelbergh (2018), p. 103.
[143] De Filippi and Wright (2018), p. 7.
[144] Yeung (2019), pp. 207–208.
[145] Wright and De Filippi (2015), p. 4.
[146] Butenko and Larouche (2015), p. 52.
[147] Liu et al. (2020), p. 205.

struggles',[148] by the proponents or the opponents of new technology in order to establish regulatory barriers to curtail the spread of the new technology or, on the contrary, to eliminate existing strategic barriers put in place by the incumbents. Hacker et al. add to it and say that legal change can be actively promoted in order to facilitate the development of the new technology and its rapid diffusion into various other fields of economic and social activity.[149] The logic here is to encourage innovation by providing the main actors of technological change with the legal capabilities for organizing new processes of new value generation. Some even go far as suggesting discounts to the application of existing regulatory norms and 'outdated' values that had so far animated risk regulation, as these may jeopardize the expected rent from the application of the blockchain technology and, thus, affect the pace of its diffusion.[150] At this initial period of the development of the technology, it is natural to generate debates over whether there should be more regulation or less.

2.3.1 Regulatory Sandboxes

Instead of embarking on extensive legal reforms to regulate blockchain-based systems comprehensively, which could necessitate a significant restructuring of the legal framework or even the underlying infrastructure and political setup of these systems, the policies should utilize the principles of 'functional equivalence and regulatory equivalence' as an alternative approach to integrating these systems into the legal framework.[151] Functional equivalence involves assessing how the functions of a specific artifact (e.g., a paper document) could be replicated using a different type of artifact (e.g., an electronic document) within a particular legal context (e.g., contract law). This approach efficiently addresses the lack of legality of the latter type—that is, actions not yet accounted for by the law but easily could be, as expanding legal boundaries to encompass them would not significantly alter legal content or fundamentally challenge the legal framework. The concept of functional equivalence has already been applied in certain laws, such as the UNCITRAL Model Law for Electronic Commerce,[152] which equates paper-based documents with electronic documents for contracting purposes. Regulatory equivalence takes this a step further by examining the objectives of a legal or regulatory provision (e.g., auditing to verify creditworthiness) to determine the conditions under which the same objective could be achieved through alternative technological means (e.g., using fully collateralized smart contracts to mitigate counterparty risk). Regulatory

[148] Lianos (2019), pp. 329–410.

[149] Hacker et al. (2019), pp. 3–24.

[150] Parenti et al. (2022), p. 71; Bagby et al. (2019), p. 419.

[151] De Filippi et al. (2022a), p. 368.

[152] UNCITRAL Model Law on Electronic Commerce (1996) with additional article 5 bis as adopted in 1998.

equivalence is pertinent in the context of legality gaps because it allows for the inclusion of objects or activities outside the legal framework, provided they contribute to achieving equivalent objectives or purposes as certain legal provisions.

To evaluate if novel applications of blockchain technology can adhere to current regulatory standards (functional equivalence) or offer comparable levels of protection to advance existing policy goals (regulatory equivalence), policymakers globally should promote the establishment of 'regulatory sandboxes'[153] more extensively. These sandboxes, commonly utilized in finance, provide a controlled setting for early-stage enterprises to test technological innovations or business models while being exempted from prevailing financial regulations (e.g., protection for novice investors) and legal obligations (e.g., safeguarding customer interests) within this environment. This would involve more frequent intervention of regulatory authorities, in diverse forms. Such sandboxes would enable the State to learn from the experiences of blockchain developers and users and to adapt the legal rules accordingly. Hacker advocates for a more interdisciplinary and participatory approach to blockchain regulation, involving not only lawyers and technologists but also social scientists, ethicists, and civil society actors. He states that

> it is not only limited to the classic command and control or risk-based approaches to regulation and the application of 'hard' law; it may also consist of a broad communicative effort, aiming to steer the activity of the various communities of experts, nudging the development of the technology towards an approach that is more compatible with the existing regulatory values that is regulation by design.[154]

To grasp the potential benefits of regulatory sandboxes in establishing functional and regulatory equivalence, let us consider ICOs. The expenses and regulatory complexities associated with adhering to securities regulations frequently discourage numerous projects from pursuing them. However, through carefully crafted technological innovations, transparency can be ensured, significantly diminishing investor risk. This could warrant the implementation of a less stringent regulatory framework for all initiatives that embrace such solutions.[155]

According to Agamben, a strategy in response to alegality involves the concept of 'inclusion by exclusion', which connotes that by intentionally exempting certain activities through legal exemptions, the legal system both broadens its jurisdiction to cover these activities and commits to non-interference as long as they comply with the exemptions.[156] This approach, while allowing for the development of a burgeoning private legal framework for blockchain systems (*lex cryptographica*), is recognized to have inherent constraints. This private legal framework will still delineate an internal realm and an unregulated external domain.

[153] De Filippi et al. (2022a), p. 369.

[154] Hacker et al. (2019).

[155] Collomb et al. (2019), p. 263.

[156] Agamben (1998), p. 22.

This regulatory sandbox approach can, further, be supplemented by the 'blockchain legal integration' approach,[157] which views that blockchain as a technology should be compatible and consistent with the existing legal framework and aligned and coordinated with the relevant laws and regulations of different jurisdictions. The proponents of this approach argue that legal integration offers several benefits, such as complementarity, improvement of the legal system, and certainty.[158] The blockchain can enhance and support the legal system by providing additional tools and mechanisms that can improve the functionality and quality of legal services and processes. For example, the technology can enable the creation and verification of digital identities, the authentication and certification of documents and records, and the automation and optimization of workflows and procedures.

2.3.2 Architecture of Control

Since blockchain technology is capable of governing, restricting, and influencing the behavior of users and individuals, it becomes more important to regulate the technology by perceiving it as an 'architecture of control'.[159] This connotes that while blockchain enables decentralization, transparency, and trust, it also requires regulation to address the potential risks and challenges associated with its use.[160] However, the law has not yet established a mechanism to regulate the blockchain system as an architecture. Despite the ongoing discussion regarding the possibility of equating smart contracts with traditional contracts,[161] there have only been a few legislative interventions concerning either their qualification or penetrating effects of this architecture on contract law. The only legislative interventions to date, with blockchain as an artifact, have been in relation to some categories of subjects, such as the promoters of initial offerings and assets such as tokens and their qualification. This raises questions as to whether the law is capable of reaffirming its primacy over the blockchain system and the value it promotes or whether it is the particular configuration of the blockchain system that exercises a certain restraint or is capable of regulating the behavior of individuals.

Indeed, the concept of technology capable of regulating is not novel. The example of the overpasses of the Long Island roadway system, which were planned by architect Moses, having the maximum height that prevented the transit of buses and coaches, known to be used by people of the lower classes, to Manhattan, is

[157] Donovan (2019).

[158] Deloitte (2022). https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Tax/dttl-tax-global-blockchain-wp-sept-2022.pdf.

[159] Du et al. (2024).

[160] Habib et al. (2022), p. 341.

[161] O'Shields (2017), p. 177.

emblematic in this regard.[162] Thus, engineering technology lent itself to the realization of a policy of social exclusion. In the same way, Latour affirmed the technological artifacts in some examples: speed bumps or cars, which do not start unless the seatbelts are buckled, have prescriptive capacity, operating like silent traffic cops.[163] Therefore, irrespective of whether technologies are complex information technological architecture or simple functionality, it is capable of modifying and reorienting the scope of permitted actions and, in so doing, contribute to the regulation of individual behavior. In fact, many cases could be imagined or have indeed been reported where devices produce outcomes that seem to contradict fundamental legal values. Corkery and Silver-Greenberg presented an example in which the starter interrupt devices can impede vehicles, affecting those that are actively running, those that debtors rely on for essential transportation to work, or those that are urgently required in specific situations, such as medical emergencies, where a patient needs to reach an emergency room quickly.[164] Since the automatic blocking of a car triggers harsh consequences in all three situations, either by causing accidents, by making earnings impossible, or by putting human lives at risk, the legitimacy of the blocking needs to be critically examined, especially if the payment has only been overdue for a very short period of time. Some of these concerns can be addressed by technical safeguards, as the devices can be designed so that they do not block cars while they are currently being driven, and all creditors can be given a certain number of one-off codes to manually override the devices so that they effectively enjoy a period of grace.[165] In fact, such modifications are increasingly incorporated into the best practice guidelines of the industry. Technical safeguards, however, cannot entirely replace legal value judgments, at least when the respective conflict is of a situational nature. Thus, two questions are signified here: in what way can the law take precedence over technological code to protect public policy interests? What means can be employed to override the code?[166]

2.3.3 The Rule of Code

Blockchain code, like the law, not only modifies individual behavior directly, but it also does so indirectly; it conditions other modalities, which in turn, condition it, thus making it essential to understand the dynamics between code embedded with the technology and law to be able to soundly regulate blockchain. In this regard, one of the approaches that are often propounded is ‘the rule of code’,[167] which views

[162] Winner (1980), p. 121.

[163] Latour (1994), pp. 33–40.

[164] Corkery and Silver-Greenberg (2014); Raskin (2017), p. 305.

[165] Möslein (2019a), p. 331.

[166] Möslein (2019b), pp. 275–288.

[167] De Filippi and Wright (2018).

blockchain as a new form of law based on the code that runs on the blockchain network. This approach is often attributed to Lessig, who refers to the architecture of the Internet and its potential to impose certain regulatory effects on Internet users: by weighing certain value principles, that architecture sets the terms on which the Internet can be used and thereby defines what is possible in that space. Lessig explored the implications of the computer code on the values of the rule of law, democracy, privacy, and freedom in the digital age.[168]

In the blockchain domain, several scholars have highlighted the myriad challenges and opportunities the rule of code presents for the legal system.[169] Because of the ongoing conversation regarding the potential benefits, challenges, and risks of the rule of code approach for the legal system, there lies an opportunity to investigate how the blockchain, or its code, can be shaped 'legitimately' to deal with the potential challenges and risks.

Möslein, in his paper 'Conflicts of Laws and Codes',[170] raises the question, 'can law, or at least private law, effectively be substituted in its entirety by the blockchain?'. The functional similarities of code and law, and of digital and legal jurisdiction, may indeed seem increasingly striking due to the advances in blockchain technology; however, the actual concern should be that, in substance, both sets of rules are, by no means, necessarily congruent as they may lead to different substantive results. Conflicts arise whenever technologically codified rules differ from the applicable legal rules or whenever both sets of rules, even if their substance agrees in principle, are applied in different ways. Therefore, the two equations seem to be misleading in both cases: instead of 'code is law' or 'law is code', the accurate identifier would rather be 'code vs. law'. Further related questions to consider are—what occurs when there is a conflict between code and law? How should we address situations when code does not equate to law?[171] The primary challenge lies in delineating the limits of digital jurisdictions and establishing new principles to address conflicts between law and codes.[172]

2.3.4 Architecture of Trust

Another way to approach the shaping of blockchain is to perceive it from the framework of a 'new architecture of trust'.[173] This approach explores how the blockchain can create a new kind of trust in the digital world. The argument is that trust is not eliminated by the blockchain but rather transformed into a different form and

[168] Lessig (1999a), pp. 123–125; Lessig (2006); Zou (2020), p. 647.

[169] Hassan and De Filippi (2017), De Filippi and Hassan (2016) and De Filippi et al. (2022b).

[170] Möslein (2019b), p. 279.

[171] Wu (2003), p. 707.

[172] Möslein (2019b), p. 275.

[173] Werbach (2018).

proposes a framework for understanding and regulating blockchain based on four modes of trust: peer-to-peer, Leviathan, intermediary, and distributed. Peer-to-peer trust relies on direct interactions and social norms, while Leviathan trust depends on the authority and legitimacy of a central entity; intermediary trust involves a third party that facilitates transactions and ensures compliance, while distributed trust emerges from a network of nodes that follow a common protocol and verify each other. Blockchain architecture, 'just how it is now', enables peer-to-peer and distributed trust while challenging Leviathan and intermediary trust by creating a shared and secure record of transactions that is verified by the network participants, thus creating a gap within the artifact to be said to have a 'legitimate' architecture. The perspective is supported by the notion that despite the potential for smart contracts and decentralized organizations to assume numerous roles traditionally held by law and the States, the widespread implementation of blockchain applications is not expected to eradicate the necessity of these centralized institutions. Instead, it is likely to create a shift in the dynamics between law and technological infrastructure, necessitating the development of new regulatory frameworks to effectively govern society.[174]

Moreover, due to the blockchain not being controlled by a single well-defined entity, together with the extreme fragmentation of the nodes of the network, it becomes difficult for traditional legal systems to directly regulate the architecture.[175] In a space where decentralized data and organizations thrive, the number of chokepoints that facilitate and regulate data flow will significantly decrease, posing challenges for government control and oversight. However, it is important to recognize that powerful intermediaries are likely to persist, continuing to play a crucial role in this evolving environment. De Filippi and Wright illustrate a series of draconian measures[176] that the States and governmental entities might resort to, if threatened, aimed at regulating the emerging online environment and maintaining control and authority over the blockchain habitat. Firstly, ISPs can be pressurized to block encrypted data flowing through their networks, effectively halting any transmission related to or from decentralized organizations. Secondly, regulations can be enacted mandating online intermediaries, like search engines, to refrain from 'intentionally' indexing blockchain-based applications, thus driving such technology towards unregulatable 'dark' markets. Thirdly, centralized authorities can attempt to stifle illegal blockchain-based entities by prosecuting software developers or users associated with them. Fourthly, hardware manufacturers can be compelled to modify their products intentionally, either by breaking encryption capabilities or incorporating tracking measures to prevent certain uses. These actions would constitute a significant abuse of governmental power and would likely impede the economic benefits offered by permissionless blockchain technology. By imposing restrictions on software developers, governments would essentially dictate the code they are

[174] Wright and De Filippi (2015), p. 51.

[175] Möslein (2019a), pp. 333–335.

[176] Wright and De Filippi (2015), p. 51.

permitted to program. Similarly, laws mandating the production of compromised hardware to thwart encryption would infringe upon basic human rights by limiting citizens' ability to safeguard their privacy. Consequently, the implementation of blockchain technology in this particular manner could potentially mirror the trajectory of the original internet, initially celebrated as a symbol of individual freedom and empowerment but now serving as a tool for surveillance and control alongside its facilitation of free speech.

Möslein argues that even if public authorities decide to deprive a smart contract of legal validity, thereby removing the guarantee of its enforcement before a court of law, this will not discourage the use of the technology by individual users.[177] Rather, the enforcement of the contract would be ensured by the very same code by which it was enacted. Once signed, a smart contract seeks to fulfill the terms and conditions it contains because the parties, in their contractual autonomy, have previously decided to forfeit the guarantee supplied by the legal order. Therefore, the main regulatory tool in the case of blockchain is considered to be the underlying technological architecture: What has the system been programmed to do, and what is the purpose behind the programming? What kind of information will it receive and verify?

Some of these questions are answered at different functional levels. This forecasts two points: first, the interaction between law and architecture can be adversarial: when architecture promotes a value that conflicts with those espoused by the law, the latter may accept or reject it, and second, the greater the decentralization of the architecture, the less effective the government's power to regulate: regulating open-source software is far more difficult than regulating proprietary software.[178] As a result, much of the regulation has to be baked into the architecture of the system. Consequently, a *lex cryptographica* emerges from this, where the 'figure' has to develop norms that will be embedded into the programs, that is, applications, code scripts, or smart contracts, they develop on the blockchain. In such a situation, public authorities could seek to impose behavioral obligations on the physical persons behind the terminal, but given the obvious enforcement difficulties, the blockchain system could decide to refuse them *en bloc*.[179]

However, before imposing any obligations on the individuals responsible for the blockchain technology, it is important to identify such a 'physical person' as no single party has the ability to control the execution of the code embedded in the blockchain. In this regard, De Filippi and Wright raised a fundamental question:

> How can the law determine who is in charge of and who is responsible for the activities of these new organizations?[180]

To answer this question, they put forward certain measures. Firstly, they suggested to adopt 'the nearest person theory' and proposed that

[177] Möslein (2019a), pp. 336–337.

[178] Lessig (1999a), pp. 507–518.

[179] Möslein (2019b), pp. 283–284.

[180] Wright and De Filippi (2015), p. 55.

> the creator of a decentralized autonomous organization should be held jointly liable for any foreseeable damages it might cause under product liability law.[181]

This response presupposes that it is always possible to pinpoint the creators of a DAO. However, such an organization might actually be formed by numerous anonymous individuals, potentially numbering in the hundreds or even thousands, or by other DAOs. Secondly, they recommended that

> the users of a decentralized autonomous organization should be held vicariously liable for the services they are paying for if they in some way can control and receive direct or indirect financial benefit from the decentralized autonomous organization's operation.[182]

However, imposing responsibility on users raises concerns about causation. It would be unjust to attribute liability to a user for actions of a third party that the user was unaware of or had no valid grounds to anticipate might result in harm to another individual. Thirdly, they suggested that

> the decentralized autonomous organization itself should be held liable for its own misdemeanors.[183]

Considering the characteristics of blockchain-enabled smart contracts, it is exceedingly challenging to seek compensation or secure an injunction against a DAO unless such provisions have been explicitly incorporated into the contract or the organizational framework of the DAOs.

2.3.5 By Design Approach

A fairly recent approach that has gained momentum in filling the gaps of the technological artifact and shaping the technology in compliance and adherence to the law is the 'by-design' methodology. In contemporary scholarship, the 'by design' concept is positioned at the intersection of law, philosophy, and technology. It is developed through two notions: 'value-sensitive design' and 'compliance by design'. The 'value sensitive design' approach acknowledges that by embedding particular values into a system, architectural design choices can create opportunities or barriers for specific social and political viewpoints.[184] In the case of the 'compliance by design' approach, legal norms are applied straightforwardly through the design of socio-technical systems.[185] This approach concentrates on techno-regulation by law with the thought that it will improve the methods of transferring norms between domains. Extending these concepts, Hildebrandt speaks of 'legal

[181] Wright and De Filippi (2015), p. 55.
[182] Wright and De Filippi (2015), p. 55.
[183] Wright and De Filippi (2015), p. 55.
[184] Friedman (1996), p. 16.
[185] Casanovasabc et al. (2017).

protection by design',[186] wherein fundamental values are considered in the design processes and technologies, particularly concerning transparency and contestability of design features.

Lessig views that

> to regulate a new technology is not a technocratic operation: it requires the active defense of a positive choice of values between those embedded in the different practices involved in the emergence of this new technology.[187]

Therefore, when discussing the future of technology law, Nemitz[188] and Hildebrandt[189] refer to democratic principles, the rule of law, and human rights by design. Ultimately what matters is not 'only' compliance with the law but the kinds of constitutional safeguards that it affords, regardless of the substantive content of its rules.

This approach does not warrant the implementation of legal norms but puts a spotlight on the issue of legal protection by addressing that the legal values are not winnowed out from the technological environment, which is essential for diagnosing whether democratic values have been ingrained into the architecture. This provides the opportunity to appraise and afford a benchmark that is considered legitimate, and that can be channeled into the production of digital artifacts. It also steers us to take a pragmatic view of code embedded in the blockchain—about its development, production, and intended function. Crepaldi, also advocates for this approach implicitly when he concludes that 'the study of the method and the design of meta-rules (code rules) for blockchains'[190] is a necessity.

The 'by-design' approach, traditionally used to study the infrastructure of 'technology' solely, has yet to be employed for the architecture of blockchain specifically. This approach can be drawn in to comprehend and tweak the blockchain technical fortress in order to shape the technology 'legitimately' by determining what design choices the 'figure' makes and the purpose behind the design choices from the outset. It flags the question- 'how does the blockchain code enable and constrain an individual's behavior?'

2.4 Blockchain from the Rule of Law Perspective

From the earlier discussions on the features of the technology and its normative implications on society and law, it can be well comprehended why blockchain technology is being pushed as a revolutionary idea. If blockchain technology is able to realize its anticipated potential partially, then it will find its deployment in many key

[186] Hildebrandt (2015), p. 181.

[187] Lessig (1999a), p. 239. Lessig (2006), p. 345.

[188] Nemitz (2021), p. 237.

[189] Hildebrandt (2015).

[190] Crepaldi (2019), pp. 189–193.

infrastructures, ranging from property records to payment to voting systems, enabling our most fundamental social infrastructure, which is the rule of law.[191] Specifically, in the developing regions of the world where governments are, in principle, the main providers of public goods, including justice, security, health, and education, there is often a deficit of trust owing to corruption, nepotism, and the notorious lack of resources.[192] These governments will, in fact, be among the 'key users' of the new technology as blockchains eliminate the necessity to place personal confidence in a certain intermediary, leading to improving the efficiency of the government and restoring public trust in the administration of legal institutions.

In recent years, the discourse surrounding blockchain either highlights the potential of this technology in democratic e-governance and delivery of public services or focuses on the effects that the code embedded in the blockchain has introduced in the law of contracts and on models of governance architecture. However, there are not enough scholarly works on the multi-faceted relationship between the rule of law and blockchain, which advances the function of law as an enabler to promote blockchain from 'the rule of law' perspective. In this context, it becomes imperative to present the opportunities for employing blockchain for the purposes of upholding the rule of law and risks incurred to the rule of law values due to this technology, as well as the impact of *lex cryptographica* on the fundamental rights of individuals, which is a vital facet of the rule of law philosophy.

Understanding these dynamics is necessary to comprehend the state of the art of the blockchain from the rule of law perspective so as to facilitate the framing of critical questions and understand the rationale behind the inquiry: the necessity for conducting a comprehensive study into the interactions between blockchain and the principles of legal governance.

2.4.1 Opportunities and Risks for the Rule of Law

Sociologists have long recognized the potential for technological architecture to influence the social landscape, albeit in ways that are often less conspicuous than traditional methods[193] of public policy implementation.[194] Governments would utilize intelligent technology to eradicate the many harmful by-products associated with modern industrialized life. Therefore, as a technological solution to fulfill the global commitment of strengthening the rule of law-based society, technologists advocate that blockchain, due to its potential in the area of data integrity, data

[191] Walch (2015), p. 837.

[192] Wilheim (2020), pp. 9, 10.

[193] Regulatory literature primarily emphasized efforts to advance social policy objectives by modifying individual behavior. This has predominantly been achieved through conventional policy tools such as directives, market forces, information dissemination, and fostering agreement, all aimed at altering the external factors affecting individual choices.

[194] Hood and Margetts (2007).

quality, transparency, and efficiency, can assist in realizing a utopian framework encompassing freedom, equality, fraternity, and world peace.[195] Blockchain has been widely used for cryptocurrencies, such as Bitcoin, but it also has many other potential applications in various fields and sectors. Its industrial usability, as well as its capacity to surpass humans in key sectors, seems to have become a new phenomenon. Given that data storage and processing is decentralized and distributed, blockchain technology finds immense use in applications related to human rights such as humanitarian aid, human trafficking supply-chain management, logistics, land properties, electricity, government payments, and smart contracts since the different actors involved in each process would benefit from the distributed ledger.[196] Similarly, blockchain's data processing efficiency and data security features make it eminently suitable for social control of elections and document maintenance and control and regulation of processes relating to public administration.[197]

The prime motive for introducing blockchain-based applications is to ensure that public officials do not manipulate the distribution of public resources. Other important considerations are reducing the cost of operation, eliminating fraud, and ensuring error-free, transparent transactions between government agencies and citizens. For example, a blockchain-based secure land registry or a public procurement system provides citizens with their rightful share of public resources and entitlements without bureaucratic hassles. Applying blockchain technology in public services also improves data storage and processing, leading to smart contracts and eliminating bureaucratic processes. Additionally, the technology has the capability to enhance transparency, accountability, and participation in democratic processes and institutions by facilitating secure and verifiable voting systems, which can prevent fraud, manipulation, and coercion and increase voter turnout and confidence.[198] Blockchain also enables decentralized and participatory governance models, such as liquid democracy, which can allow citizens to delegate their votes to others or vote directly on issues according to their preferences and expertise. It can support civil society and social movements by providing platforms for fundraising, organizing, and campaigning without the need for intermediaries or censorship.

The embryonic development of blockchain in the area of the rule of law facilitates the protection and promotion of human rights, especially the right to privacy, freedom of expression, and access to information. This technology can provide a secure and anonymous way of storing and sharing personal and sensitive data without the risk of surveillance, hacking, or identity theft by creating self-sovereign identities with blockchain.[199] Using unique biometric information such as fingerprint and iris scans diminishes the importance of physical identity documents. Since an individual would be able to prove his or her identity with the information on a

[195] Busstra (2020), p. 31; Hughes (2017), p. 654.

[196] Ølnes and Jansen (2018), pp. 1–10.

[197] Berryhill et al. (2024), p. 28.

[198] G'sell and Martin-Bariteau (2022), Hughes (2017) and Rodriguez (2021).

[199] Grech et al. (2021), p. 5.

blockchain, employers cannot exploit the victims by confiscating the physical document. Thus, the exploitative value of physical documents ceases to have any meaning. In fact, the need for a physical document can be dispensed with by creating a 'virtual identity' on the blockchain. The immutability of the blockchain makes it nearly impossible to forge identification details to transport victims over borders illegally, and reduces the vulnerability of the refugees who are without any physical documents to trafficking.[200] When identification details are stored in a distributed and immutable ledger on the blockchain, human trafficking will be traceable and preventable and will also increase the probability of prosecuting the traffickers.[201] By creating a self-sovereign identity, the individual is empowered to control how much, when, and with whom to share his or her personal identification data. With self-sovereign designs built on blockchain technology, the role of intermediaries and centralized databases is done away with, and self-controlled peer-to-peer data sharing is possible. However, issues with respect to the privacy of a person must be addressed. Moreover, how the principles of the 'right to be forgotten' can be incorporated into the design of a self-sovereign identity system built around an immutable blockchain structure must be addressed since the technology freezes all the information that has entered into it.

Blockchain can also enable the creation and distribution of uncensorable and unalterable content, such as journalism, activism, and art, which can challenge the status quo and expose human rights violations. One example of this is the Uyghur Pulse project, which aims to use blockchain to preserve and share the cultural heritage and identity of the Uyghur people, who are facing persecution and oppression by the Chinese government in Xinjiang. This project allows users to upload and access various types of content, such as photos, videos, music, and stories, that reflect the Uyghur culture and history and such content is stored on a decentralized network that is resistant to censorship and manipulation.[202] Similarly, Bellingcat, which is an independent investigative journalism platform, uses open source and digital tools, including blockchain, to uncover and verify information about various topics, such as war crimes, corruption, and human rights abuses. This platform uses blockchain to ensure the authenticity and integrity of the evidence and data that it collects and publishes, as well as to protect the anonymity and security of its sources and contributors. Till now, Bellingcat has exposed and challenged many cases of misinformation and propaganda by the authorities and the media.[203]

Another application of this technology is the facilitation of the verification and documentation of human rights abuses, such as torture, trafficking, and genocide, by using digital evidence, such as photos, videos, and testimonies that can be authenticated and preserved on the blockchain. One of the critical requirements of forensic investigations is that evidence is not modified while collecting, processing,

[200] Seyedsayamdost and Vanderwal (2020), p. 943.

[201] #Blockchain4Humanity (2018). https://press.un.org/en/2018/pi2224.doc.htm.

[202] Ekman (2021).

[203] Crumpler (2021).

or storing. Blockchain provides a consensus and distributed network model for immutable data storage and processing capability in which the same cannot be altered once a record is created. Thus, a decentralized and 'de-trusted' blockchain may be an effective solution to the problem of data loss and forgery observed in a centralized storage system. Since the data is stored in a network of dispersed computers and all transactions are updated with the timestamp in all the nodes on a real-time basis, it provides more reliable information for judicial examination.[204] Since transactions are stored and verified in a distributed ledger via a consensus algorithm, blockchain can be applied to certify the authenticity and legitimacy of the procedures used to collect, process, and store electronic evidence. This would broadly address issues pertaining to trust, integrity, data security, and transparency. For digital forensics, a private blockchain can be put in place to ensure the integrity of evidence.[205] Expectedly, blockchain solutions are being applied for intrusion detection as well as forensic evidence gathering.[206]

However, blockchain technology also entails some human rights risks and dilemmas, such as the potential for abuse, misuse, and harm, which will inherently hurt the rule of law since human rights cannot be protected without a strong rule of law as it is the implementation mechanism for human rights, turning them from principles to reality. The technology can be used for malicious and criminal purposes, such as money laundering, terrorism, and cyberattacks, which can threaten the security and well-being of individuals and communities. Such acts, thus, negatively affect the rights of the individuals, which refers to the thick definition of the rule of law that, according to Lord Bingham, embraces the entire code of rights contained in the European Convention on Human Rights, essentially on the ground that they are to be regarded as the basic entitlements of a human being.[207] Therefore, any abuse or harm to human rights was, in fact, a violation of the rule of law.

The Silk Road crypto-market case exemplifies how blockchain or cryptocurrency can be used for illegal purposes, such as the trafficking of human beings and drugs. The site not only allowed the purchase of merchandise (drugs) with cryptocurrency such as Bitcoin but also hid the internet user's identity.[208] Studies on the Silk Road crypto marketplace indicate the extent of its impact and the way it has entrenched into the sale and consumption of illegal and prescription narcotics.[209] Participants in illegal trades, inter alia narcotics, and human trafficking often prefer Silk Road because it allows the participant to remain anonymous and to protect their identity by using on-screen pseudonyms. Such anonymity reduces personal risks, stealthy product delivery, and the opportunity to develop personal connections with vendors using stealth modes of contact and forum activity. Human traffickers also

[204] Wu and Zheng (2020), pp. 7–10.

[205] Lone and Mir (2019), p. 44; Tian et al. (2019), p. 151.

[206] Brotsis et al. (2019).

[207] Bingham (2007), pp. 66–84.

[208] Martin (2013), p. 351.

[209] Van Hout and Bingham (2014), p. 183.

use such cryptocurrencies to settle financial transactions and to pay websites for online classified ads to lure victims. The US National Center for Missing and Exploited Children has said that the majority of child sex trafficking cases referred to them involve ads on Backpage.[210] In 2015, with an aim to stop this crime, the credit card companies stopped using their services on Backpage, leaving Bitcoin as the only mode of payment.[211]

Cryptocurrency has become increasingly popular among transnational criminals due to its decentralized nature, anonymity, speed of transaction, ease of use, global outreach, and, above all, lack of adequate regulations. However, the immutable nature of the transaction and digital footprint may provide vital electronic evidence to law enforcement agencies, which might deter cybercriminals. Further, transnational criminal activities using cryptocurrency or blockchain can be decreased with the support of technology. Blockchain can be used, with public consultations and international organization cooperation, in supply chain management to curb, for example, modern-day slavery and violation of fundamental rights. In a supply chain, transparency, trackability, accountability, and integrity are the key ingredients, all of which can be addressed through blockchain. By deploying this technology, all transactions are visible and can be tracked through the immutable ledger in real-time. This prevents fraud and errors and reduces the risk of data loss.[212] The World Wildlife Fund (WWF) has successfully launched a project to combat modern-day slavery and human rights abuse in the fishing industry.[213] While blockchain has the potential to tackle modern-day slavery within supply chains, this by itself is not an absolute panacea. It does not remove the need for proper due diligence and checks to ensure that the source data is legitimate. It relies on all parties' commitment to ethical practices and to ensure that there are no gaps in the source data provided to the blockchain.

All the above blockchain applications have an impact on the rule of law, whether it is being used for public services in the government administration or employed for the purposes of human rights. When the blockchain is used in government operations such as digital identity management, supply chain traceability, and voting systems, its main motivation is to improve transparency, efficiency, and

[210] Reuters (2017). https://www.reuters.com/article/usa-trafficking-lawsuits-idUSL1N1F-S1EA. New Scientist (2017). https://www.newscientist.com/article/2145355-ai-uses-bitcoin-trail-to-find-and-help-sex-trafficking-victims/.

[211] US Department of Justice Office of Public Affairs (2022). https://www.justice.gov/opa/pr/fbi-announces-results-nationwide-sex-trafficking-operation.

[212] Deloitte (2023). https://www2.deloitte.com/us/en/pages/operations/articles/blockchain-supply-chain-innovation.html.

[213] The World Wildlife Fund (WWF) in Australia, Fiji and New Zealand, in partnership with US-based software company ConsenSys, technology implementer TraSeable and tuna fishing and processing company Sea Quest Fiji Ltd., launched a pilot project in January using blockchain to track tuna 'from bait to plate'. The purpose of this project is to combat the modern slavery and human rights abuses that plague the fishing industry by recording the journey of each tuna fish to ensure that they are not sourced from illegal fishing boats prone to slave labour. See Boulais (2019), p. 1.

accountability in such services. These applications can be said to facilitate upholding the rule of law by ensuring that the government processes are transparent and verifiable, reducing opportunities for corruption and arbitrary exercise of power by public officials. Similarly, when employed for the benefit of vulnerable populations or for securing the fundamental rights of individuals, it can be said there is an impact on the rule of law since the rule of law and human rights mutually reinforce each other, and the rule of law provides the foundation for the protection, promotion, and realization of human rights.

Though blockchain has a lot of potential for protecting and promoting the rule of law, it is also capable of transgressing legal obligations and being employed for malicious purposes. This is in line with—'while these systems might bring new promises of increased transparency and accountability if improperly governed, we might incur the risk of losing some of the basic tenets of a democratic society'.[214] This implies that certain tenets of the rule of law, particularly accountability, transparency, legal certainty, and legitimacy, cannot be taken for granted. A conscious and strategic choice must be taken to 'enforce or restrict certain user behavior' through the design and implementation of blockchain technology, such that it aligns with the values and principles of the rule of law.

2.4.2 Lex Cryptographica and the Rule of Law

Blockchain is regulated by *lex cryptographica*, which are rules governed through 'self-executing' smart contracts and decentralized infrastructure. These rules dominate the rule of law within the blockchain artifact, which results in the subsistence of two environments, divergent from each other, drawing on the argument of Nozick and Nagel.[215] On the one side, there exists an environment outside the blockchain where the rule of law applies, and on the other side, inside the blockchain, an environment persists where the *lex cryptographica* applies. In both these environments, the rule of law remains to be in the application within the blockchain, and the *lex cryptographica* also has an influence outside the blockchain, however, as an exception to the source. Nevertheless, within the blockchain, the State conserves its monopoly to the extent that no other entity is challenging it but is no longer able to exercise it in all spaces.[216] Due to the paucity of conventional application of the rule of law within the blockchain, there are questions regarding the degree of protection of fundamental rights by the rule of law outside the blockchain infrastructure. This ineffectiveness of the rule of law is offset by the emergence of the *lex cryptographica* environment, in which technology protects fundamental rights and not the State. In that sense, the State is deprived of its cardinal function of protecting fundamental

[214] De Filippi (2019), p. 9.

[215] Nozick and Nagel (1974).

[216] Schrepel (2019a), p. 117; Spinello (2001), p. 137.

and human rights, particularly visible individual rights (e.g., freedom of opinion, right to privacy) and collective rights (e.g., freedom of press and freedom of association). This points to the issue of whether the technology has the competence to create an equivalency with the rule of law or State-imposed justice in the absence of it regarding the determination, regulation, and enforcement of the rules.[217]

According to the natural law theory, certain fundamental rights pre-exist in the legislation,[218] and when we take this analogy to the blockchain environment, it reflects that fundamental rights within the rule of law may also be considered to subsist within the *lex cryptographica*. This approach can also be viewed as conforming to the legal positivism theory to the degree that the presence of fundamental rights under the rule of law may be transported to the blockchain environment. However, the blockchain environment 'as it is now' cannot be expected to determine legal standards and values, as can be envisaged under the rule of law environment. In other words, the *lex cryptographica* system does not allow for any 'one' fundamental right to be held superior to the others, which is in contradistinction to the rule of law environment, where centralized authorities and courts exist to regulate the supremacy of the law. This expresses the difference between the legal rules and values enforced by the rule of law and the 'cryptographic order' produced by the *lex cryptographica*, which means that users can only implement their rights if the technology enables it.

It is tricky to identify the rights in the blockchain as 'fundamental rights' since the *lex cryptographica* significantly influences the competence to implement what is referred to as 'fundamental rights', making the entire analogy to the rule of law theories flawed. Subsequently, such an interface leads to the question regarding the enforcement of the rights with the *lex cryptographica*. This can be understood by taking the example of smart contracts utilized in the arbitration mechanisms, where the cryptographic rules allow for certain rights to be implemented by technically warranting that the transaction is accomplished with the pre-determined amount being transferred 'in return' to the blockchain and with the addendum that in case of non-compliance by one of the parties, the amount would be automatically released.[219] Such a blockchain application can be enforced to strengthen property rights, which is one of the fundamental rights. However, there is a lacuna in the blockchain artifact since the technology only allows protection of the rights of the users who are participants of the smart contract, and thus, in case of a third user inflicting damage, there is no mechanism to claim compensation as the identity of such a user is confidential. Moreover, within the blockchain environment, a user can claim compensation for wrongdoing but may not get the actual compensation without having those financial contributions already deposited in the smart contract.

Within the *lex cryptographica* system, when a network user publishes information on the blockchain in violation of the right to privacy of another user, causing

[217] Schrepel (2018), p. 281.

[218] Moore (1958), p. 277.

[219] Schrepel (2019a), p. 117.

harm to that user, it is neither possible to erase the information nor unveil the offender's identity. For example, even if photographs of a user are published in the blockchain environment without prior informed consent by a third party, causing the privacy of the user to be violated, these third-party violations cannot be easily punished within the *lex cryptographica* system. As such, the State fails to deliver justice in the blockchain environment, and hence, the scope of protection of the fundamental rights granted by the State in the technological system is questioned.

Therefore, when users decide to use blockchain, it formulates a new social contract where they concur on not receiving compensation or justice even if there is a violation of the fundamental rights by a third party. In a manner, blockchain shifts the State's duty of protecting the right to privacy to the citizens or the users themselves, but at the same time, it obliterates the limits imposed on other rights by public authorities. However, safeguarding their right to privacy on the blockchain might become complicated for the users, since simply protecting in the online environment may be inadequate. This means that when the photographs of the users are published on the blockchain, the online environment interferes with the offline world, steering the users to protect themselves not only in the online environment but also in the offline world.

Here and now, users are unable to depart from the rule of law environment if they want to stay a member of the democratic society. To patch up the rule of law environment, they have the freedom of speech and expression to voice their opinions. However, the *lex cryptographica* creates a new archetype where users are offered the choice of departing the rule of law, to an extent for a part of their activities, and entering the blockchain environment. In such an environment, the rights allowed by the technology are made 'almost' absolute, which results in generating friction between them, which connotes that under the *lex cryptographica* system, there is no balance, for instance, between the two fundamental rights, freedom of expression and right to privacy, that can be achieved. A balance between these two fundamental rights can be attained by the implementation of the rule of law, where law could be enforced *a posteriori* to remedy the infringement of one of the rights. However, under the influence of *lex cryptographica,* the first user making use of its rights obtains a 'first-mover' advantage over the others. If the first user employs his or her freedom of expression against the second user, the information cannot be erased or deleted from the blockchain once it is published, regardless of whether the information infringes the right to privacy of the other user or not. Likewise, if the second user moves first to protect his or her privacy by using blockchain to interact in the online environment, the first user will be stripped of the information related to the identity, actions, and behavior of the second user and henceforth would not be able to exercise his or her freedom of expression against the second user. This is one of the reasons why blockchain is promoted since it provides protection against infringement of the users' right to privacy as compared to the rule of law environment. Therefore, blockchain-enabled 'self-sovereign' identity services are being developed that empower users to control their identities and their data.

Lex cryptographica system creates a new-found recognition of Rousseau's social contract with the desire for the rule of law, where the State cannot impose its

monopoly of justice, and hence a new trade-off is proffered to the users. The users are provided a choice to utilize a blockchain application contingent on two factors that is one, which fundamental rights they desire the most, and second, infringement of which rights they are consenting to accept due to the lack of limitations on each of them. In the rule of law environments, the limitations vary depending on the situation and the decisions of the governments and central entities as to what they deem 'right'; but that is not the case in the blockchain environment, courtesy of the decentralized architecture of the technology where there is no central authority empowered to pursue changes to the *lex cryptographic* rules. As such, depending on the trust of the citizens in the State to protect their rights and establish a balance between the rights in the rule of law environment, they may espouse to join the *lex cryptographica* system since the origin of blockchain is from an anti-State credo which vows to succeed where the State failed.[220]

If the citizens choose to employ the blockchain, there may be certain trade-offs to be made between the protection of fundamental rights and the use of services offered by the technology. One can perceive this today also, when we as individuals are trading out our right to privacy in exchange for online services. Blockchain will take this praxis of trade-off and highlight its acceptance among the population. Since within the *lex cryptographica* system, the fundamental rights are of absolute in nature, which may cause, for example, the user's freedom of expression to infringe the rights of others, it will emphasize on the values that the users respect if they keep the services on the technology. Moreover, there is a direct link between the utility of the technology and its key features, such as pseudonymity or immutability, resulting in potential violations of fundamental rights. As such, the trade-off between fundamental rights and the utility derived from the services will become more visible.

Outside the blockchain environment, the rule of law regulates fundamental rights with certain limitations. In essence, it regulates an environment that is not considered apt for all individuals where some would prefer to employ absolute freedoms regardless of whether it causes significant harm to others. However, blockchain questions this model where some fundamental rights are guaranteed absolute power while others are left vulnerable. Therefore,

> if and when blockchain technology will manage to impregnate itself into the very fabric of society, some of today's legal, social, and political institutions might need to accommodate new technological constructs operated by market forces and code-based rules.[221]

Since the *lex cryptographica* system provides functionality to replace the core responsibilities of the State, that is, acting in accordance with the rule of law as a principle of governance mechanism, by the technology, which may not be acceptable to the State, there needs to be a 'schema' which would, to a certain extent would make the technology uphold the rule of law and be admissible by the State.

[220] Schrepel (2019b), pp. 322–323.

[221] De Filippi (2019), p. 5.

References

Agamben G (1998) Homo Sacer: Sovereign Power and Bare Life (trans: Daniel Heller-Roazen). Stanford University Press, p 7

Atzori M (2017) Blockchain technology and decentralized governance: is the state still necessary? J Governance Regul 6:45

Bacon J et al (2018) Blockchain demystified: a technical and legal introduction to distributed and centralized ledgers. Richmond J Law Technol 25:1

Bagby JW et al (2019) An emerging political economy of the Blockchain: enhancing regulatory opportunities. UMKC Law Rev 88:419

Balkin JM (1998) Cultural software: a theory of ideology. Yale University Press, London

Barlow JP (2019) A declaration of the Independence of cyberspace. Duke Law Technol Rev 18:5

Baudrillard J (1968) Le Système Des Objets. Gallimard, Paris, p 39

Bayern SJ (2014) Of bitcoins, independently wealthy software, and the zero-member LLC. Northwest Univ Law Rev 108:1485

Becker K (2022) Blockchain matters—Lex Cryptographia and the displacement of legal Symbolics and imaginaries. Law Critique 33:113

Berryhill J et al (2018) Blockchains unchained: blockchain technology and its use in the public sector. OECD Working Papers on Public Governance, p 28

Bingham T (2007) The rule of law. Cambridge Law J 66:84

'Bitcoin's Anarchy Is a Feature, Not a Bug' (Bloomberg.Com, 14 March 2018). https://www.bloomberg.com/view/articles/2018-03-14/bitcoin-blockchain-demonstrates-the-value-of-anarchy

Bosu A et al (2019) Understanding the motivations, challenges and needs of Blockchain software developers: a survey. Empir Softw Eng 24:2636

Boulais O (2019) Exploring provenance of tuna using distributed ledgers. Viral Communications, p 1

Brotsis S et al (2019) Blockchain solutions for forensic evidence preservation in IoT environments. In: IEEE Conference on Network Softwarization (NetSoft). Paris, France

Busstra M (2020) Designing for good: blockchain technology and human rights. Intergovernmental Organisations In-house Counsel Journa, p 31

Butenko A, Larouche P (2015) Regulation for innovativeness or regulation of innovation? Law Innov Technol 7:52

Casanovasabc P et al (13 December 2017) Legal Compliance by Design (LCbD) and through Design (LCtD): Preliminary Survey (2049 CEUR Workshop Proceedings, 1st Workshop on Technologies for Regulatory Compliance (TERECOM 2017), Luxembourg, https://ddd.uab.cat/record/189386

Casey MJ, Vigna P (2018) In Blockchain we trust. MIT Technol Rev 121:10, 23

Christensen MC et al (2018) Disruptive innovation: an intellectual history and directions for future research. J Manag Stud 55:1043–1078

Collomb A et al (2019) Blockchain technology and financial regulation: a risk-based approach to the regulation of ICOs. Eur J Risk Regul 10:263

Coppi G, Fast L Blockchain and Distributed Ledger Technologies in the Humanitarian Sector. HPG Commissioned Report 2019

Corkery M, Silver-Greenberg J (24 September 2014) Miss a Payment? Good Luck Moving That Car. New York Times

Crepaldi M (2019) Why Blockchains Need the Law: Secondary Rules as the Missing Piece of Blockchain Governance. In: 17th International Conference on Artificial Intelligence and Law (ICAIL '19), pp 189–193

Crumpler W (2021) The human rights risks and opportunities in blockchain. center for strategic and international studies. https://www.csis.org/analysis/human-rights-risks-and-opportunities-blockchain

De Filippi P (2017) Plantoid—the birth of a Blockchain-based lifeform. In: Catlow R et al (eds) Artists re: thinking the Blockchain. Torque & Furtherfield, Leeds, p 51

De Filippi P (2019) Blockchain Technology and Decentralized Governance: The Pitfalls of a Trustless Dream. Decentralized Thriving: Governance and Community on the Web 3.0, hal-02445179
De Filippi P, Hassan S (2016) Blockchain Technology as a Regulatory Technology: From Code Is Law to Law Is Code. 21 First Monday. https://doi.org/10.5210/fm.v21i12.7113
De Filippi P, Mauro R (2014) Ethereum: the decentralised platform that might displace today's institutions. Internet Policy Rev 25
De Filippi P, Wright A (2018) Blockchain and the law: the rule of code. Harvard University Press, Cambridge
De Filippi P et al (2020) Blockchain as a confidence machine: the problem of Trust & Challenges of governance. Technol Soc 62
De Filippi P et al (2022a) The Alegality of Blockchain technology. Polic Soc 41:358
De Filippi P et al (2022b) Blockchain Technology and the Rule of Code: Regulation via Governance, hal-03883249
Dimitropoulos G (2020) The law of Blockchain. Wash Law Rev 95:1117
Dimitropoulos G (2022) The use of Blockchain by international organizations: effectiveness and legitimacy. Polic Soc 41:328
Donovan A (2019) Blockchain: developing regulatory approaches for the use of technology in legal services. Legal Services Board UK, London
Du Z et al (2024) Blockchain-based access control architecture for multi-domain environments. Pervasive Mobile Computing 98:101878
Efe Gencer A et al (2018) Decentralization in bitcoin and Ethereum networks. In: Meiklejohn S, Sako K (eds) Financial cryptography and data security. Springer, Cham, p 24. https://doi.org/10.1007/978-3-662-58387-6
Ekman A (2021) China's blockchain and cryptocurrency ambitions: the first-mover advantage. European Union Institute for Security Studies (EUISS)
Faria I (2019) Trust, reputation and ambiguous freedoms: financial institutions and subversive libertarians navigating Blockchain, markets, and regulation. J Cult Econ 12:2, 119
Feenberg A (2012) Questioning technology. Routledge, London
Feng T et al (2019) Research on privacy enhancement scheme of Blockchain trans-actions. Secur Priv 2:1
Finck M (2018) Blockchain regulation and governance in Europe. Cambridge University Press, Cambridge, p 28
Friedman B (1996) Value-Sensitive Design. Interactions 3:16
Fukuyama F (2012) China and east Asian democracy: the patterns of history. J Democr 23:1, 14
Garcia M (2009) The patterns of architecture. John Wiley & Sons, New Jersy
Ghiro L et al (2021) What is a Blockchain? A definition to clarify the role of the Blockchain in the internet of things
Gill L (2018) Law, metaphor, and the encrypted machine. Osgoode Hall Law J 55:440
Goossens J (2021) Challenges and opportunities of Blockchain and smart contracts for democracy in the distributed, algorithmic state. In: Pollicino O, De Gregorio G (eds) Blockchain and public law: global challenges in the era of decentralisation. Edward Elgar Publishing, Cheltenham, p 76
Grech A et al. (2021) Blockchain, self-sovereign identity and digital credentials: promise versus praxis in education. Front Blockchain 4:5
G'sell F, Martin-Bariteau F (2022) The impact of blockchains for human rights, democracy, and the rule of law. Council of Europe
Guegan D (2017) Public Blockchain versus Private Blockchain. halshs-01524440
Habib G et al (2022) Blockchain technology: benefits, challenges, applications, and integration of Blockchain technology with cloud computing. Future Internet 14:341
Hacker P et al (2019) Regulating Blockchain: techno-social and legal challenges- an introduction. In: Hacker P et al (eds) Regulating Blockchain: techno-social and legal challenges. Oxford University Press, Oxford, p 13

Hassan S, De Filippi P (2017). Field Actions Science Reports) The expansion of algorithmic governance: from code is law to law is code. J Field Actions:88
Heinemann T, Weiß GM (2016) Biotechnologische Grenzregime. An Der Grenze-Die Biotechnologische Überwachung von Migration. p 8
Hildebrandt M (2008) A vision of ambient law. Regulating Technol 175:178
Hildebrandt M (2015) The public (s) Onlife: a call for legal protection by design. In: Floridi L (ed) The Onlife manifesto: being human in a Hyperconnected era. Springer, Cham, p 181
Hood C, Margetts H (2007) The tools of government in the digital age. Bloomsbury Publishing
Hughes K (2017) Blockchain, the greater good, and human and civil rights. Metaphilosophy 48:654
ISO (2024). https://www.iso.org/obp/ui/en/#iso:std:iso:22739:ed-2:v1:en:term:3.54
Jacob D (2021) Every vote counts: equality, autonomy, and the moral value of democratic decision-making. Res Publica 21:1
Juskalian R (2018) Inside the Jordan Refugee Camp That Runs on Blockchain. MIT Technology Review
Kaeseberg T (2019) The code-Ification of law and its potential effects. Computer Law Rev Int 20:107
Kannabiran G et al (2011) How HCI Talks about Sexuality: Discursive Strategies, Blind Spots, and Opportunities for Future Research. In: SIGCHI Conference on Human Factors in Computing Systems, p 695
Ku RRS (2002) The creative destruction of copyright: Napster and the new economics of digital technology. University of Chicago Law Review 69:263
Lamport L (1983) The weak byzantine generals problem. J Assoc Comput Mach 30:1, 668
Lamport L et al (1982) The byzantine generals problem. ACM Trans Program Lang Syst 4:382
Latour B (1994) On technical mediation - philosophy, sociology, genealogy. Common Knowledge 3:29
Lehdonvirta V, Ali R (2016) Governance and regulation, distributed ledger technology: beyond Blockchain. UK Government Office for Science, London, p 40
Lessig L (1999a) Code and other Laws of cyberspace. Basic Books, New York, p 3. https://lessig.org/images/resources/1999-Code.pdf
Lessig L (1999b) The law of the horse: what cyber law might teach. Harv Law Rev 113:501
Lessig L (2006) Code Version 2.0. Basic Books, New York. https://tigerprints.clemson.edu/cgi/viewcontent.cgi?article=1183&context=cheer
Lianos I (2019) Blockchain competition–gaining competitive advantage in the digital economy: competition law implications. In: Hacker P et al (eds) Regulating Blockchain: techno-social and legal challenges. Oxford University Press, Oxford, pp 329–410
Lindahl H (2013) We and Cyberlaw: the spatial Unity of constitutional orders. Indiana J Global Legal Stud 20:697
Liu HY et al (2020) Artificial intelligence and legal disruption: a new model for analysis. Law Innov Technol 12:205
Lone A, Mir R (2019) Forensic-chain: blockchain based digital forensics chain of custody with PoC in hyperledger composer. Digit Investig 28:44
Low KF, Mik E (2020) Pause the Blockchain legal revolution. Int Comp Law Q 69:135
Luciano D, Prichett G (1987) Cryptology: from Caesar ciphers to public-key cryptosystems. Coll Math J 18:2
Mallard et al (2014) The paradoxes of distributed trust: peer-to-peer architecture and user confidence in bitcoin. J Peer Production:1
Marks S (2017) The end of history? Reflections on some international legal theses. In: Simpson G (ed) The nature of international law. Routledge, London
Martin J (2013) Lost on the silk road: online drug distribution and the 'cryptomarket'. Criminol Crim Jus 14:351
Maxwell D et al (2017) Story blocks: reimagining narrative through the Blockchain. Convergence 23:1
May T (1992) The Crypto Anarchist Manifesto. https://activism.net/cypherpunk/crypto-anarchy.html

Meiklejohn S, Orlandi C (2015) Privacy-enhancing overlays in bitcoin. In: Brenner M et al (eds) Financial cryptography and data security. Spring-er, Cham, p 127
Mennicken A, Salais R (2022) The new politics of numbers: an introduction. Springer, Cham
Moore MS (1958) A natural law theory of interpretation. South Calif Law Rev 58:277
Möslein F (2019a) Legal boundaries of Blockchain technologies: smart contracts as self-help? In: De Franceschi A, Reiner SR (eds) Digital revolution–new challenges for law. C.H. Beck and Nomos, Frankfurt, p 331
Möslein F (2019b) Conflicts of Laws and Codes: defining the boundaries of digital jurisdictions. In: Hacker P et al (eds) Regulating Blockchain: techno-social and legal challenges. Oxford University Press, Oxford, pp 275–288
Mulligan C (2016) Applications in government. In: Walport M (ed) Distributed ledger technology: beyond block chain. Government Office for Science, London
Musso P (2021) Technique et Politique: Diabolique et Symbolique. Pistes Revue de philosophie contemporaine Éthique, Politique, Philosophie Des Techniques 1:83
Nakamoto (2008) A peer-to-peer electronic cash system. Bitcoin 4:15. https://bitcoin.org/bitcoin.pdf
Nemitz P (2021) Democracy through law - the transatlantic reflection group and its manifesto in defence of democracy and the rule of law in the age of “artificial intelligence”. Eur Law J 29:237
North DC (1990) Institutions, institutional change and economic performance. Cambridge University Press, Cambridge
Nozick R, Nagel T (1974) Anarchy, state, and Utopia. vol 5038: Basic Books
O’Shields R (2017) Smart contracts: legal agreements for the Blockchain. N C Bank Inst 21:177
Ølnes S, Jansen A (2018) Blockchain technology as infrastructure in public sector: an analytical framework. In 19th annual international conference on digital government research: governance in the data age. Article 77, pp 1–10
Owen T (2015) Disruptive power: the crisis of the state in the digital age. Oxford University Press, Oxford, pp 24–29
Parenti C et al (2022) A smart governance diffusion model for Blockchain as an anti-corruption tool in smart cities. J Smart Cities Soc 1:71
Peck ME (2017) Blockchain world - do you need a Blockchain? This chart will tell you if the technology can solve your problem. IEEE Spectr 54:38
Pereira J et al (2019) Blockchain-based platforms: De-centralized infrastructures and its boundary conditions. Technol Forecast Soc Chang 146:94
Pollicino O, De Gregorio G (2021) Blockchain and public law: global challenges in the era of decentralisation. Edward Elgar Publishing, Cheltenham
Raskin M (2017) The law and legality of smart contracts. Georgetown Law Technol Rev 1:305
Reijers W, Coeckelbergh M (2018) The Blockchain as a narrative technology: investigating the social ontology and normative configurations of cryptocurrencies. Philos Technol 31:103
Renwick R, Gleasure R (2021) Those who control the code control the rules: how different perspectives of privacy are being written into the code of Blockchain systems. J Inf Technol 36:16
Rodriguez A (2021) Blockchain and its impact on human rights. In: Rodriguez A et al (eds) Legal challenges in the new digital age. Brill Nijhoff
Rogaway P (2015) The Moral Character of Cryptographic Work. IACR Cryptol. ePrint Arch. 2015/1162
Rouvroy A, Stiegler B (2015) Le Régime de Vérité Numérique. De La Gouvernementalité Algorithmique à Un Nouvel État de Droit. Socio La Nouvelle Revue Des Sciences Sociales:113. https://journals.openedition.org/socio/1251
Schrepel T (2018) Is Blockchain the death of antitrust law? The Blockchain antitrust paradox. Georgetown Law Technol Rev 3:281
Schrepel T (2019a) Collusion by Blockchain and smart contracts. Harvard J Law Technol 33:117
Schrepel T (2019b) Libra: a concentrate of "Blockchain antitrust". Mich Law Rev Online 118:322–323

Schrepel T (2020) Anarchy, state, and Blockchain utopia: rule of law versus Lex Cryptographia. In: Bernitz U et al (eds) General principles of EU law and the EU digital order. Kluwer Law International, Alphen aan den Rijn
Searle JR (1995) The construction of social reality, vol 2. Free Press, Washington, p 2
Seyedsayamdost E, Vanderwal P (2020) From good governance to governance for good: blockchain for social impact. J Int Dev 32:943
Simonite T (2014) Meet the man who really built bitcoin. MIT Technology Rev 117:21
Sklaroff JM (2017) Smart contracts and the cost of inflexibility. Univ Penn Law Rev 166:263
Spinello RA (2001) Code and moral values in cyberspace. Ethics Inf Technol 3:137
Sullivan C, Burger E (2017) E-residency and Blockchain. Comp Law Security Rev 33:470
Supiot A (2008) L'inscription Territoriale Des Lois. Esprit:151
Supiot A (2015) La Gouvernance Par Les Nombres. Fayard, Munkebo
Swan M (2015) Blockchain: blueprint for a new economy. O'Reilly Media, Inc, Sebastopol, p 43, 47
Swan M, De Filippi P (2017) Towards a philosophy of Blockchain. Metaphilosophy 48:5
Tasca P, Piselli R (2019) The Blockchain paradox. In: Hacker P et al (eds) Regulating Blockchain: techno-social and legal challenges. Oxford University Press, Oxford, p 27
Tian Z et al (2019) Block-DEF: a secure digital evidence framework using Blockchain. Inf Sci 491:151
Tozzi C (2019) Decentralizing democracy: approaches to consensus within Blockchain communities. Teknokultura: Revista de Cultura Digital y Movimientos Sociales 16:181
Treisman D (2007) The architecture of government: rethinking political decentralization. Cambridge University Press, Cambridge
Van Hout MC, Bingham T (2014) Responsible vendors, intelligent consumers: silk road, the online revolution in drug trading. Int J Drug Policy 25:183
Van der Elst C, Lafarre A (2019) Blockchain and smart contracting for the shareholder community. Eur Bus Organ Law Rev 20:111
Vigna P, Casey MJ (2019) The truth machine: the Blockchain and the future of everything. Picador, New York, p 23
Wahab AA et al (2024) Examining the software developers' perception in open-source software of Blockchain project using association rules mining. In: Zakaria HN et al (eds) Computing and informatics. 9th international conference, ICOCI 2023. Malaysia 13–24 September 2023. Springer, Cham, p 287
Walch A (2015) The bitcoin Blockchain as financial market infrastructure: a consideration of operational risk. NYU J Legislation Public Policy 18:837
Walch A (2016) The path of the Blockchain lexicon (and the law). Rev Banking Financ Law 36:713
Walch A (2019) In code(rs) we trust: software developers as fiduciaries in public Blockchains. In: Hacker P et al (eds) Regulating Blockchain: techno-social and legal challenges. Oxford, 2019; online edn, Oxford Academic, p 61
Walport M (2016) Distributed ledger technology: beyond Blockchain. Government Office for Science, London, p 5
Wang F, De Filippi P (2020) Self-sovereign identity in a globalized world: credentials-based identity systems as a driver for economic inclusion. Front Blockchain 2:28, 33
Watkins F (1948) The political tradition of the west: a study in the development of modern liberalism. Harvard University Press, Cambridge
Weber RH (2018) Rose is a rose is a rose is a rose–what about code and law? Comp Law Secur Rev 34:701
Werbach KD (2016) Trustless trust. https://youtu.be/Uj342yXUkCc?feature=shared
Werbach KD (2018) The Blockchain and the new architecture of trust. MIT Press, Cambridge
Werbach K, Cornell N (2017) Contracts ex Machina. Duke Law J 67:313
Wilhelm A (2020) Rule of Law 2.0: Blockchain Technology and the Development of Legal Institutions in Africa. 22 Recht in Afrika, p 9, 10
Winner L (1980) Do Artifacts have politics? Daedalus 109:1, 121

Wright A, De Filippi P (2015) Decentralized Blockchain Technology and the Rise of Lex Cryptographia. https://doi.org/10.2139/ssrn.2580664
Wu T (2003) When code isn't law. Va Law Rev 89:679
Wu H, Zheng G (2020) Electronic evidence in the blockchain era: new rules on authenticity and integrity. Comput Law Secur Rev 36:7–10
Yeung K (2008) Towards an understanding of regulation by design. In: Brownsword R, Yeung K (eds) Regulating technologies: legal futures, regulatory frames and technological fixes. Hart Publishing, London, p 79
Yeung K (2017) Blockchain, transactional security and the promise of automated law enforcement: the withering of freedom under law? TLI Think! Paper 58/2017
Yeung K (2019) Regulation by Blockchain: the emerging Battle for supremacy between the code of law and code as law. Mod Law Rev 82:207
Zou M (2020) Code, and other Laws of Blockchain. Oxf J Leg Stud 40:645
'Zug Digital ID: Blockchain Case Study for Government Issued Identity' (Consensys, 2018). https://consensys.io/blockchain-use-cases/government-and-the-public-sector/zug
Zyskind G, Nathan O (2015) Decentralizing Privacy: Using Blockchain to Protect Personal Data. IEEE Security and Privacy Workshops. pp 180–184

Chapter 3
The Rule of Law Philosophy and Design Standards

3.1 The Rule of Law Philosophy

Blockchain's technical attributes have led to a new normative order, that is, the *lex cryptographica,* thus giving way to the emergence of the new rule of code, which has the potential to create another regulatory environment, co-existing in parallel with the rule of law such that to a certain extent, the *lex cryptographica* has a significant impact on the fundamental rights of the individuals. As such, there is a necessity to consider the re-factoring of the *lex cryptographica* framework based on the standards and values of the rule of law by comprehending and investigating the true purpose behind the code rules of the blockchain application as well as the validity and legitimacy of the characteristics of code governing human behavior and the actual enforcement of these rules, so that the purpose behind the rule of code and the code rules themselves adhere to the rule of law values and standards.

The influence of the rule of law pertains not to the intrinsic nature of law, its core values, or its foundational principles but rather to its functioning and the manner in which it is executed. That is why the rule of law is a fabrique—'a delicately woven fabric that binds us together and a production of those bonds'.[1] Since the law has the power to intermingle everywhere and connects everything, such as persons, things, acts, and words, its 'shallowness' characteristics is one peculiar feature that adds up to its grandeur, and this is why the rule of law makes up for an instrument of significance to be employed to study the blockchain architecture. The rule of law is a dynamic concept, and a productive ingredient as has been established by its ability to adjust and afford a vocabulary sufficient to express and address the changing demands of different historical and political responsiveness while upholding its essential core. It is multifaceted in nature and has a critical role in fostering stability, predictability, and fairness in society.

[1] Latour (2010), p. 280.

A. Bisoyi, *Blockchain and Legitimacy*, Law, Governance and Technology Series 77, https://doi.org/10.1007/978-3-031-98712-0_3

3.1.1 A Modern Positive View

The rule of law is an implied philosophy of modern positive law. The expression 'the rule of law' is usually attributed to Professor Albert Venn Dicey, a constitutional theorist.[2] Although the idea of 'the rule of law' has been traced back to Aristotle, who, in a modern English translation, refers to the rule of law, with the literal translation being—'it is better for the law to rule than one of the citizens…. so even the guardians of the laws are obeying the laws',[3] the influence of Dicey's book was such that the concepts associated with the rule of law prevailed like never before.

Prior to Dicey, Fuller made a point that—'be you never so high, the law is above you'.[4] In a way, the rule of law envisages that no one is above the law, and all are subject to the same set of laws in the same jurisdictions.

Given that multiple divergent and contradictory concepts of the rule of law had been floated, Krygier provides a significant takeaway—'the rule of law now means so many different things to so many different people',[5] with Waldron further asserting how it is so 'essentially contested'.[6] There is also a propensity to use the rule of law as a brief description of the positive facets of any given political system.[7] The principle of the rule of law

> is one of the ideals of our political morality, and it refers to the ascendency of law as such and of the institutions of the legal system in a system of governance.[8]

The rule of law is 'the name commonly given to the state of affairs in which a legal system is legally good in shape'.[9] As a notion that gives rise to a 'rampant divergence of understandings', the rule of law is extraordinarily elusive and analogous to the concept of the 'good' in the sense that 'everyone is for it, but have contrasting convictions about what it is'.[10]

The rule of law enables modern societies to have a stable and transparent system to resolve conflicts between citizens within a community. It is called the 'rule' because, in doubtful or unforeseen cases, it is a guide or norm for their decision.[11] It is a teleological concept that ought to be appreciated based on its ideas and purposes, essentially, for how it is supposed to serve good.

---

[2] Dicey introduced this phrase in his book, 'An Introduction to the Study of the Law of the Constitution'. Dicey (1915), p. 193.

[3] Aristotle (2009).

[4] Fuller (1732).

[5] Krygier (2016), p. 200.

[6] Waldron (2017), p. 137.

[7] Raz (2017), p. 210.

[8] Waldron (2016). https://plato.stanford.edu/archives/fall2023/entries/rule-of-law/.

[9] Finnis (2011), p. 270.

[10] Tamanaha (2004), p. 3.

[11] Raz (2017), p. 218.

Further, the rule of law must not be merely considered as a tool for limitation, curbing, or constraints but rather as an apparatus to include further positive dimensions. We can posit that the rule of law can be perceived as a 'positive' instrument for defining the affordances that may guide and critique the development of the blockchain and assess the protection of the rule of law norms when deploying the technology for usage such that it remains within the perimeter of the rule of law to an extent, regardless of their intended commercial objectives.

It can be generally noted that a notion of the rule of law is very significant for its potential to prevent the arbitrary use of power. However, the fundamental basis of the rule of law has been misinterpreted and distorted in many countries. It has been propagated to be tantamount to 'the rule by law' or 'rule by the law', or even 'law by the rules', which facilitates authoritarian governments to enforce their totalitarian rules disregarding the intended meaning of the rule of law.[12] The subtle difference between the rule of law and the rule by law is that while the former is both an instrument of public policy and an instrument of protection, the latter is simply an instrument to achieve the goals of the stated public policy. The rule by law is a core determinant of legalism, bringing a contrast to the rule of law, which emphasizes the principle of legality coupled with legitimacy.[13]

The values of the rule of law are not absolute, but nevertheless, they are largely beneficial. The rule of law has typically been promoted as an important component of a solution to all sorts of problems, notwithstanding the fact that many contemporary rule of law intelligentsia and reformers too often start the other way around. Instead of starting with a solution that focuses 'on the end' rather than 'the means', it is prudent to start with the problem and determine a solution for the same.[14] As the focus is on power and its *modus operandi*, the rule of law, in a sense, becomes problematic by virtue of its potential for manipulation and exploitation and not for its mere existence. Yet, the rule of law in its right connotation is an integral part of any democratic society and the concept of the rule of law is invoked in a multitude of circumstances which can be differentiated according to varying conceptualization.

The endeavors to explain a taxonomy of the various notions of the rule of law, which portray the present-day deliberations, have led to the recognition of the 'thinner and thicker version of formal, substantive, and procedural perspectives'.[15] The distinction is often made between a thin and thick version, which is contingent upon the way conditions tilt towards formal or substantive. In the case of substantive conceptions, protecting liberty, equality as well as fundamental rights, human rights, including social and cultural rights, are given more weightage and considered as necessary components of the rule of law. In the case of the formal conceptions, the rule of law affords importance to the enacted laws and other formal requirements

[12] Holovaty (2006), p. 214.

[13] Under Sect. 3.2, I will explore the concept of the rule of law and rule by law in depth to bring out the essence of legality and legalism and how it contrasts in legal forum. This exploration will find its meaning in deriving a parallelism with the rule of code characteristics.

[14] Krygier (2011), p. 72.

[15] MacCormick (2005). Waldron (2011), p. 3.

that can limit the legitimacy of legal rules;[16] it is a legal system constituted and enforced by the government institutions, typically distinguished by features such as clarity, foreseeability, non-contradictoriness, non-retroactivity, generality, and stability. The procedural conceptions, however, emphasize the roles performed by the judiciary and legal procedures in the law-making process, thereby shaping legal protection, where attention is on the right to dispute against the State[17] and the procedural conditions that enable disputation and debate as crux to the rule of law.[18] This conception of formal, procedural, and substantive formulation of the rule of law ought to be introduced into the blockchain architecture to develop an analogy between technology and the rule of the law environment in terms of both, first, building up a resonance between the rule of code embedded in the blockchain and the legal norms at the micro level, and second, prioritizing the substantive values of the rule of law at the macro level, that is the protection of fundamental rights and human rights when deploying the blockchain. The first aspect is about how the rule of code 'ought' to be programmed within the circumference of the rule of law, that is, does it conform to the formal requirements as well as procedural principles of the rule of law by which code norms 'ought' to be administered, such that the rule of code norms are legitimate; The second aspect answers what choices and decisions must the State deliberate upon when employing the blockchain for public purposes, to guarantee respect for human rights.

It is imperative to acknowledge that during recent years due to globalization and deregulation, there are international and transnational public actors as well as hybrid and private actors with great power over State authorities and private citizens. The rule of law doctrine should be and can also be extended to the private stakeholders, especially in cases where the role of the private organizations has an impact on the public interests or individual rights. As such, the rule of law may also be applied to the 'figure' who has power concentrated in its hands to develop and deploy blockchain in order to avoid an 'unjust' arbitrary exercise of power, which is more towards fulfilling the commercial objective and less towards protecting the ethos of the rule of law.

A notable aspect of the rule of law is that we realize its significance only when it is flouted. It functions as the mainstay of 'liberalism of fear'.[19] This means that the rule of law supports the notion that human beings should have the capability to make as many decisions as they can without any discrimination or bias, as long as these decisions are in sync with the liberties of other human beings.

The rule of law empowers citizens with crucial information and security and provides a basis for legitimate expressions, by facilitating them to gather information about each other, by coordinating their actions with them, and providing certain security and predictability in their transactions. As the root source of information,

[16] Wintgens (2002a).

[17] Dicey (1915), p. 200.

[18] Waldron (2011), pp. 5–7.

[19] Shklar (1989).

security, and predictability, the rule of law could be the foundation of 'civil' relations between the State and its citizens and among citizens themselves. It provides the citizens with the necessary strength to rely upon the State and the law, without being suspicious or fearful.[20] From this perspective, the positive accomplishment of the rule of law is not merely a legal outcome but a social one, meaning how the law affects subjects is more important than other considerations as everywhere with the rule of law. As the gap between law in books and in actions is ever so often large, filled with different things in different places at different times, it is a matter of comparative social exploration and theorization to determine what might be best in particular societies.

Essentially, what people expect from the rule of law, and what it can provide through successful interpretation, is first, an acceptable shield against uncertainties, surprises, and the worst fears that are generated due to the arbitrary exercise of power, and second, adequate and commonly interpretable prompts which assists citizens to orient their behavior so as to interact with the fellow citizens with confidence and mutual understanding. The rule of law can act as an instrumental tool in the design and implementation of blockchain technology and its rule of code, which is capable of regulating individuals' behavior by constraining and allowing their actions, and hence, the primary question is: *can the rule of law shape, guide and influence the design and implementation of blockchain technology, in a legitimate manner?*

3.1.2 'Legitimacy' in 'the Rule of Law'

Legitimacy encompasses a multitude of interpretations. Various actors within the international system, such as activists, academics, politicians, the press, judges, and bureaucrats, attribute different meanings to this word. The diversity of these meanings and the frequent usage of the word itself make it a challenging concept to categorize systematically. Having said so, legitimacy can be said to be a multidimensional social construct that can be justified on the grounds of 'tradition, charisma, and legality'[21] and is ultimately determined by the subjectivity of the individuals.[22] Suchman has broadly defined it as

> a generalized perception or assumption that the actions of an entity are desirable, proper, or appropriate within some socially constructed system of norms, values, beliefs, and definitions.[23]

In other words, legitimacy can be described as the property of a rule or rule-making institution that inherently encourages compliance from individuals who believe that

[20] Krygier (2008), p. 12.

[21] Weber (2009), p. 61.

[22] Suchman (1995), p. 571.

[23] Suchman (1995), p. 574.

the rule or institution was established and functions in alignment with widely accepted principles of the right process. According to Franck, legitimacy relies on four essential attributes: determinacy (easily ascertainable normative content or transparency), symbolic validation (approval from authority), coherence (consistency or general applicability), and adherence (compliance within an organized hierarchy of rules).[24] This suggests the existence of objectively verifiable criteria that aid in understanding why rules are followed and, consequently, why the system functions effectively. The internal features of law are central to its power to promote commitment since

> law is about rules, about prescription, about normativity; in all conceptions, law is a normative enterprise, the rules prescribing what ought and ought not to be done.[25]

By conferring authority and acceptability upon the normative order, legitimacy sets a standard for assessing the relevance and acceptability of legal norms and practices within the broader political context. However, one cannot assume that what is *legal* is necessarily *legitimate*.[26] A rule or entity that is legal but lacks legitimacy is unlikely to maintain its position over the long term.

When the law is said to be 'legitimate', it means that it can generate fidelity to the rule of law itself and not merely to specific rules. To create 'legitimacy', Fuller's criteria of legality must also be met substantially. These criteria are essential for establishing norms that qualify as 'law'. Merely meeting these criteria is not adequate to uphold the rule of law or specific legal rules, shared understandings and rules that meet the criteria of legality must also be consistently reinforced through a robust adherence to legality in practice, which becomes the core of 'legal' legitimacy. Hence, legitimacy emphasizes the necessity of an inclusive practice that conforms to the criteria of legality to establish and uphold legal norms.[27] Such a perspective reveals the inherent weakness of many customary or treaty rules. This weakness does not stem from the lack of enforcement or other attributes of 'hard' law but rather from a legitimacy deficit resulting from limited participation in norm development and insufficient attention to the requirements of legality.[28] If a legal rule does not have a basis in shared understandings and only weakly or imperfectly aligns with the criteria of legality, it will not generate fidelity to the rule of law and will not be employed in determining appropriate behavior.

The concept of 'legal' legitimacy can, thus, be understood as a characteristic of an action, rule, actor, or system that indicates a legal obligation to adhere to or support that action, rule, actor, or system. Legitimacy is often directly equated with legal validity to the exclusion of questions of moral justifiability.[29] It is recognized that legitimacy is particularly significant due to its inherent self-justification within

[24] Franck (1990), p. 24, 26.

[25] Brownsword (2015), p. 19.

[26] Dyzenhaus (1999).

[27] Brunnée and Toope (2010), p. 54.

[28] Brunnée and Toope (2010), p. 55.

[29] Beetham (1991), p. 4.

a functioning legal system. Once something becomes legally legitimate, a compelling reason for compliance is created, even in the face of conflicting moral considerations.[30]

Questions of legal validity directly impact broader concepts of morality and order. In the positivist tradition, exemplified notably by Kelsen and Hart, asserting that a law is legally valid means claiming that it has been created in compliance with the correct legal procedure. According to Kelsen, the test for positive validity could be conducted recursively until a non-legal fundamental norm for a legal system, known as the 'Basic Norm (*Grundnorm*)', could be reached, for which authority is 'presupposed'.[31] Kelsen articulates a 'principle of legitimacy', which pertains to the persistence of a norm's legal validity until its replacement or repeal in accordance with the legal order that produced it.[32] He also made a firm distinction between the 'is' and the 'ought' of the law.[33] According to him, the 'is'-ness of the law is derived from one foundational 'Basic Norm'. This foundational norm cultivates a hierarchical structure of normative rules, resembling a pyramid procedural structure where the validity of all legal rules that are derived from such systems are guaranteed by the 'Basic Norm'. He asserts that 'what law is' must be differentiated from 'what law ought to be (*das richtige Recht*)'. According to Kelsen, a principled assessment of the law is carried out by describing its normative content, considering the deductive reasoning that ascertains the interrelationships between various legal norms,[34] thus emphasizing the systematic coherence of the legal order.

In contrast, for Hart, the validity of law is ultimately linked to a 'rule of recognition' as the rule of recognition is a social fact rather than a norm.[35] Hart refrains from 'purely' normative statements and defines the nature of law in terms of social interactions. He defines primary legal rules as those that define which conducts are prescribed and permitted or which are proscribed, and secondary legal rules as those that specify the ability to identify, amend, or decide primary legal rules. His 'Ultimate Rule of Recognition' is based on the 'internal aspects of legal rules' wherein law is the 'union of primary and secondary rules'.[36] His 'concept of law' underscores law as a multifaceted system of social acceptance, explaining the interaction between regulative and constitutive rules[37] by defining primary and secondary rules.

In simple terms, for a positivist, a norm is considered legally legitimate if it is established and continues to exist in compliance with the appropriate legal

[30] Raz (1975), pp. 38–48.

[31] Kelsen (2017), pp. 110–122.

[32] Kelsen (2017), pp. 117–118.

[33] Kelsen (1991).

[34] Kelsen (2017), pp. 110–112.

[35] Hart (1961), pp. 100–110.

[36] Hart (1961), p. 80 and chp. 5.

[37] In Chap. 5, Sect. 5.5, this aspect will be further discussed in the context of constitutive and regulative normativity in technological design.

procedures, where the correctness of these procedures ultimately stems from a basic norm or from societal consensus. Actions carried out in accordance with such norms can be regarded as having legitimacy.

Legitimacy has a 'specific, legal meaning'[38] in international law scholarship, which goes beyond tests for validity. Drawing on Fuller's work, an 'interactional account' of legitimacy is constructed in which adherence to eight criteria of legality (generality, promulgation, non-retroactivity, clarity, non-contradiction, not asking the impossible, constancy and congruence between rules and official action) 'produces a law that is legitimate in the eyes of the person to whom it is addressed'.[39] Adhering to the criteria of legality creates a sense of legitimacy by creating communities of practice, generating shared understandings and moral obligations to comply with the law. Fulfilling these criteria is considered morally valuable, reflecting a commitment to autonomous actor choices, diversity, and communication processes.[40] Franck has also highlighted the importance of considering how rules are formulated, interpreted, and implemented in addition to their properties since 'focus on the properties of rules… is not a self-sufficient account of the socialization process'.[41] The law comes into existence when norms that fulfill the criteria of legality are integrated into actual practice.

3.1.2.1 Bases of Legitimacy

The bases of legitimacy pertain to the grounds on which the object is determined to be legitimate.[42] The moral duty to adhere to a rule can be influenced by various factors that collectively or individually determine the validity of the rule such that it enhances or reduces the legitimacy of a given norm. These factors formulate the bases of legitimacy, which can be distinguished between first, procedural legitimacy, that is, the process through which the rule is established; second, substantive legitimacy, that is, the objectives it fulfills; and third, outcome legitimacy, the results it generates.[43]

Procedural legitimacy refers to the mechanisms through which power is granted and exercised.[44] It emphasizes the formal validity of power, centering on the secondary rules governing the creation, modification, and annulment of laws. Legitimacy, as conceptualized by positivists, embodies a significant manifestation of procedural legitimacy. Law is the ultimate embodiment of procedural legitimacy, asserting an obligation to comply regardless of its content. The procedural approach may

[38] Brunnée and Toope (2010), p. 54, 3.

[39] Brunnée and Toope (2010), p. 27.

[40] Brunnée and Toope (2010), pp. 9, 28–33.

[41] Franck (1988), pp. 712–713.

[42] Franck (1990), pp. 17–18. Hurd (2007), pp. 66–73. Clark (2005), pp. 18–19.

[43] Thomas (2014), p. 749.

[44] Friedman (1977), p. 139.

specifically focus on the correctness of the procedure as assessed against procedural rules,[45] which in turn may reflect a specific substantive aim (e.g., the rule of law). However, it refrains from questioning the desirability of a given substantive objective.

Substantive legitimacy is primarily concerned with the purpose served by the object being legitimized. This form of legitimacy is most commonly associated with justice or substantive fairness. It can also be seen in pieces of literature that aim to evaluate or support existing rules or institutions based on considerations of human rights,[46] development,[47] global welfare,[48] or trade liberalization.

The distinction between input and output-based forms of legitimacy is often discussed in the context of analyzing the 'democratic deficit' in the EU. Input-oriented legitimacy, according to Scharpf, pertains to the normative ideal of 'government by the people', focusing on representation, participation, and transparency.[49] His articulation of input legitimacy does not need to be read as purely procedural, being strongly concerned with promoting sovereignty and self-government as values in their own right. The procedural aspect of input legitimacy can further be classified as 'throughput legitimacy', which is defined by specific qualities of the rules and procedures by which binding decisions are made, including the quality of participation, checks and balances, and mechanisms for collective decision-making.[50] In contrast, output legitimacy refers to 'government for the people', deriving legitimacy from its ability to solve collective problems. Input legitimacy encompasses procedural and substantive considerations in decision-making, while output legitimacy is validated based on the practical consequences of such decision-making.[51] Some refer to this broader understanding of output legitimacy as outcome-based or effectiveness-based legitimacy, which judges the system seeking legitimacy based on a given set of desirable outcomes.

3.1.2.2 What Law Ought to Be

A general understanding of legal rules suggests the leadership of non-binary standards applicable to rules, and hence, it is not sensible to explain law as a system of rules. The integrity of law is essential more than just consistency for coherence, which is intrinsic to law,[52] as it introduces moral standards into the law. These moral standards could even be transpired from previous legal decisions and legislations.

[45] Hurd (2007), p. 71.

[46] Petersmann (2000), p. 19.

[47] Fakhri (2009).

[48] Cottier (2009), p. 9.

[49] Scharpf (1999), p. 11.

[50] Bekkers and Edwards (2007), pp. 44–45.

[51] Hurd (2007), pp. 66–67.

[52] Dworkin (1986).

Rather than concentrating on logical coherence to understand legal systems, this approach to law is hermeneutical, emphasizing that any decision requires interpretation and needs creativity as well as meticulousness. This includes exploration of the interrelationship between various distinct and interrelated concepts such as 'validity, content, normativity, and legitimacy'.[53] Since modern law centers around legal text and the script, the printing machine shapes the necessary conditions to have a legal system, and the emphasis on their interpretation has gained prominence in the contemporary legal discourse. More so, written text is the 'externalization and objectification of the spoken word, bringing about the need for interpretation'.[54] As printed text-based law is used for mediation, its utility may be apparent to many lawyers to merit further exploration. However, the legal craft would profit from the realization that printing as a technology has serious implications on the nature, the scope, and the content of the jurisdiction. The invention of the script and the printing press spread the reach of legal rules far and wide, not just limiting to face-to-face relationships but also preparing a conducive environment for cross-border politics and jurisdictions. While the script provokes a linear understanding of time due to the necessity of reading from beginning to end, the printing press promotes 'rationalization and systematization' so as to endure the text content.[55] Another remarkable feature of written law is its ability to address the unescapable sense of delay arising out of the complexity of the legal system and the time-and-distance gap between the law and the individual or user.[56]

The notion that constitutional safeguards can be interpreted, applied, and grounded on the basis of the 'framers' intention' or on the 'clear meaning' of the text is difficult to hold since it is argued that it is not possible to claim what the author of the text actually meant since the text does not speak for itself.[57] Of course, it does not mean that legal texts can be and are being interpreted in an *ad-hoc* manner depending upon the readers' response. Rather, it indicates that legal texts could be interpreted in a restricted manner so as not to allow any potential interpretation that would make the text redundant, even though it may open up new possibilities for fresh applications involving creative realization. While being dynamic and autonomous, written law depends on legal doctrine, it also affords continuity and flexibility while applying the law.[58] Various rule of law values, such as legal certainty, justice, and effectiveness, so desirable considering the ever-changing nature of the social and technological infrastructure in modern society, are strengthened by such continuity and flexibility emanating from the interpretation of written law.

This discussion opens the door for deliberation and initiates a conversation in the realm of technology, specifically when dealing with coded architectures like

[53] Priel (2011), p. 8.

[54] Ihde (1990), pp. 80–84.

[55] Hildebrandt (2008a), p. 184.

[56] Hildebrandt (2008b), p. 169.

[57] Strauss (2010). Kay (2009), p. 703.

[58] Hildebrandt (2008a), p. 187.

blockchain, regarding the written code norms and its characteristics—what 'is' the characteristics of the code norm and what 'ought' to be the characteristics—as well as build up an argument concerning the intention behind the enactment of the written code norms within the blockchain artifact.

3.2 The Rule by Law *Vis-à-Vis* the Rule of Law

The rule by law, a core determinant of legalism, is often misunderstood with the concept of legality, which is one of the 'indispensable' constituents of the rule of law. The notion of 'legality' stipulates that the rules proclaimed must be fabricated to echo the substantive legitimacy of the norms and certain ideals such as proportionality, as well as safeguards.[59] On the contrary, legalism is only bothered about whether the rule has been enacted by a legitimate institution or not, without worrying about its contents or substantive effects. It is evident that legality is not the same as legalism, or 'the rule of law' cannot be drawn parallel to 'the rule by law'.

3.2.1 Legalism

Legalism asserts that adequate legal justification is required for State interventions such that these interventions attain legitimacy, which denotes that for the interventions to be lawful and legitimate, regardless of their content, it must be dependent on the pre-existing legal rules. When developed in a comprehensive manner, legalism could furnish values such as reliability, comprehensibility, foreseeability, and certainty and even cope with Fuller's principles of 'inner morality of law',[60] that is, generality, publicity, prospectivity, intelligibility, consistency, practicability, stability, and congruency.

3.2.1.1 Strong Legalism and Weak Legalism

Legalism is 'a pre-requisite of free government'[61] and is, in essence, an *ex-post* doctrine that asks all government actions to be respectful towards rules and rights. This formulation of legalism aligns with Wintgens's concept of 'weak' legalism rather than 'strong' legalism. Weak legalism is interpreted as a conception in which rules persist to be the instrument *de règle* for regulatory activities, while the probability for their *ad-hoc* interpretation is concurrently restricted, necessitating

[59] Fuller (1964), pp. 33–44.

[60] Fuller (1964).

[61] MacCormick (1989), p. 184.

justifying the limitation by the law of individual freedom.[62] In other words, it outlines the normative position where the development process of the rules is curtailed to the limit of non-arbitrariness, and at the same time, those rules are framed on an *ad rem* premise for regulating behaviors. The concept of weak legalism has been propounded with a view that certain measures of legalism, such as respect for 'law as law', is essential for society to function effectively, and it ought to be comprehended normatively as a required component of legality and not as something antagonistic.[63]

Strong legalism is a strategy in itself. The strategic character is normative, wherein

> timelessness and instrumentalism mutually support one another and make values or ends lose their contingent character, failing which the whole construction would vanish under the pervasive weight of contingency.[64]

Contingency is, however, mitigated by arguing that they reflect reality through the merger of representation-reproduction and representation-construction, which promotes legal certainty. The 'stronger' version of legalism also represents the condition of 'heteronomy' where the action is influenced and dominated by an external sovereign and contradicts the objectives of coherent interpretation and action as well as its autonomy.[65] To put it simply, where strong legalism indicates the manifestation of an authoritative sovereign and does not investigate about the 'how' and 'why' of enacting a specific rule, weak legalism allows the removal of the 'veil of sovereignty' to pursue the rationale behind this act.[66] In other words, it can be said that strong legalism subverts legality, whereas weak legalism, although a deficient ingredient, is imperative to legality. Thus, a new rule cannot be justified and enacted on the basis of the 'bare sovereign power' of the legislator since the legislator cannot claim to instrumentalize natural law or social contract.

In the absence of any safeguards against arbitrary rule, legalism essentially portrays the 'stronger' version of the notion. The strong legalism is

> the ethical attitude that holds moral conduct to be a matter of rule-following, and moral relationships to consist of duties and rights determined by rules.[67]

This ethical interpretation is denominated as *the morality of duty* by Fuller. It establishes essential rules that are crucial for maintaining an orderly society, or else any society aiming for specific objectives is likely to miss its intended targets.[68] The consequence of such an approach is a culmination of moral force since it ensues normalization and systemization of behavior in a society, which fosters some sort of

---

[62] Wintgens (2016), p. 220.

[63] MacCormick (1989), p. 184.

[64] Wintgens (2016), p. 159.

[65] MacCormick (1989), p. 192.

[66] Wintgens (2016), p. 220. MacCormick (1989), p. 179.

[67] Shklar (1986), p. 1.

[68] Fuller (1964), pp. 5–6.

behavioral predictability effectuating moral certainty that has been contended to be a sought-after aspiration for developing an enduring pluralist society.[69]

The hierarchy of power under strong legalism, in most cases, does not permit the subordinate to seek answers from the superior. In contrast, the hierarchy of power under weak legalism enables the same and, if justifiable, reverses the hierarchy of power itself. Though such proposals for reversal would be overlooked from the notion of strong legalism, the philosophy of legisprudence does provide conceptual anatomy for legitimizing this temporal reversal. This means that legisprudence, while requiring a valid source of the norm, also calls for the justification of the proposed legal norm through rigorous reasoning and rationalization by lawmakers.[70] The principles of legisprudence, which steer the manner in which the ruler behaves, notwithstanding the politics involved in the substantial formulation of the norm, become the basis of such rationalization. Legal norms or lawful justifications for specific limitations on freedom should be established before the promulgation of any law and can be used *ex-post* to test the efficacy of the hierarchy of power.

Where strong legalism focuses primarily on the validity of the normative source, specifically with regards to the sovereign following its own proposed norm, legisprudence propounds that while strong legalism is essential, it alone is inadequate to establish legitimacy. The sovereign must be bound by the core philosophy of the norm, and at the same time, it must also proactively legitimize its proposed norms. This is the type of validity that blurs the distinction between procedural formal (*ex-ante*) and substantive (*ex-post*) legitimacy to an extent; specific procedural formal traits exemplified in the principles of legisprudence constrain the substantive content of the norm. Thus, an additional active layer of legitimation is required for understanding 'legitimacy'. That means the sovereign is bound not only by the general principles of law that are applicable to all individuals, such as adherence to the rule of law, but also by the specific rules it proposes to enact. These rules must reflect specific procedural attributes that constrain the breadth of substantial scope of those rules. The probability of the notion of strong legalism to be abused as prioritizing heteronomy undermines not only the principles of legality that are characteristic of the rule of law but also the critical appreciation and application of the rule of law itself. When we apply these arguments to the blockchain infrastructure, they facilitate in understanding the characteristics of the rule of code from a legalistic perspective—whether the characteristics resonate with the 'strong' version of legalism or the 'weak' version—and as such, try to articulate to what extent does the blockchain architecture 'as it is now' falls under the periphery of the rule of law—what 'is' versus what 'ought' to be.

According to the solipsistic view of law, legalism functions independently from the societal structures that shape its existence and is manifested as a distinct system of rules and practices. As a system, since the law is 'self-contained, auto generative,

[69] Shklar (1986), p. 64.

[70] Wintgens (2016), p. 145.

and clean'[71] and embraces the legislations or the products of the politics, which are often unscrupulous, legalism applies them as per its own *sui generis* processes and institutions and vocabulary. This conceptualization already brings in an emotion of congruity with the blockchain code framework, *lex cryptographica,* which formulates 'a new and foundational mode of configuring reality'.[72]

The legislators, as sovereign actors, produce law by *epistemologizing* and transforming practical reasons with theoretical reasonings—identification and working with the 'verity'. Legalism as a 'verity' remains unquestioned because, in terms of law and legal practice, the 'verity is just is', and this 'verity' is asserted as an immutable reality. This perspective is passed from the political space, where legislators are the 'only' authorities who can ponder over the essence of the norm. As the legislator is primarily a political actor rather than a legal one, at least not in the sense a judge is, the legislature is fundamentally a matter of politics that revolves around making choices. After legislators finalize one of the choices between various possibilities and enact it into law, it turns into a 'veracious' knowledge element within the 'science of law'.[73] The extra-legal attributes associated with this law are extraneous to the legal scholars who observe its application within their domain. As a result of safeguarding law from irrelevant factors, legal thinking has become detached from historical thoughts and experiences.[74] Thus, one ought to think of a law that is 'there' and bring in the view of positivism.

The positivistic view of law talks about law being 'just there',[75] and it is not to be questioned by the citizens or the legal practitioners regarding how it got 'there'. The matter of relevancy here is the validity of the law and not our concurrence or otherwise with the essence and applicability of the law. The 'veracity' of a specified legal norm is attained from its legal acceptability, genuineness, and legitimacy of its genesis in relation to approved processes and players, and the desirability of the essence of law needs to be considered separately from its 'veracity-ness'.[76] Conceptually speaking, this stance is linked to 'strong' legalism, which splits the legal order between what it means (internal to the system) and what is not law (external to the system).[77] In fact, examining what should be considered as 'law' and what should not is one of the core characteristics of legal positivism. Drawing on the solipsistic conceptualization, the lawyers use the knowledge provided from somewhere 'out there' as an instrument to realize specific legal objectives.[78] Maintaining a 'neutral' position towards the crux of the rules, the lawyers routinely control and influence those rules in line with the mechanism of legal reasoning.

---

[71] Bankowski and MacCormick (2000), p. 46.

[72] Swan and De Filippi (2017), p. 8.

[73] Wintgens (2006), p. 5.

[74] Shklar (1986), p. 3.

[75] Bankowski (1989), p. 289.

[76] Wintgens (2016), p. 186.

[77] Wintgens (2002b), p. 20.

[78] Wintgens (2016), p. 140.

There is the legisprudential abstraction that endeavors to cultivate weak legalism under which constancy of rules is considered essential, provided that the rules can be justified, and their formulation meets the specified standard;[79] it handles the rationality and justification of legislation. It may be said that legisprudence is an approach that shifts the philosophy of law towards the *ex-ante* reasoning of legislators and away from the *ex-post* reasoning of the lawyers and judges. This approach focuses on the actions of the legislator and lays down the principles that enable restraining those who legislate to capitulate to strong legalism tenets.[80]

The 'stronger' version of legalism provides a structure for applying established rules or principles rather than for formulating those rules themselves.[81] Synthesizing the theoretical means of legitimation in 'positivism and jusnaturalism', it has been identified that

> strong legalism consists of conjugation of five characteristics – representationalism, timelessness, concealed instrumentalism, etatism, and the scientific method of study of law.[82]

From a jusnaturalistic perspective,

> the creation of law is based on the knowledge of natural law, which is to say that the norm creation is a matter of knowledge and, as a consequence, is an application of jusnaturalistic principles.[83]

In a way, it can be said that positive legal rules, which are observed in a sovereign legislative body, are creations of the knowledge of natural law, which affords a cognitive foundation and is pre-existent with respect to positive law. These natural laws attain the value of positive law through legislation.

The sovereign's will is, therefore, the only and ultimate source of law because the 'will of the sovereign' stamps a proposition from the legislators so as to transform it into a legal rule. The institutionalization of political space as the unique source of legal rules, then leads to the institutionalization of law that does not require any justification. Hence, there is no law beyond the State, and all laws find their origin in the State. According to *etatism*, the State is the sole source of law and has the power to legitimize any legal norms it declares.[84] Strong legalism posits that the establishment of a legitimate State necessarily leads to the emergence of legitimate norms. As long as the original source from which law can be promulgated is *a priori* legitimate, the law is *de facto* legitimate and, therefore, ought to be followed.

Under strong legalism, the sovereign assumes the role of a 'general proxy' for the enforcement of rules. Consequently, the legislative actions undertaken are 'in effect' legitimate by virtue of their effective implementation. The concept of

---

[79] Wintgens (2002a), p. 2.

[80] Wintgens (2016), p. 297.

[81] Wintgens (2016), p. 139.

[82] The study of these characteristics will facilitate sketching the attributes of the rule of code embedded in the blockchain artifact and make a comparison with the legal norms.

[83] Wintgens (2002b), pp. 10–11.

[84] Wintgens (2016), pp. 170, 172. Wintgens (2017).

sovereignty, therefore, releases the sovereign from the requirement to give any justification for his rulings and hence has created the phenomenon of 'one-shot legitimation'. Under the *proxy theory of legitimization*, the sovereign created by the subjects, based on the social contracts, holds the final power within the political space they are establishing and has the 'proxy power' to legitimate the normative contents of the law that will limit the subject's freedom. The operationalization of political space involves legislation that entails the imposition of 'external limitations on freedom'.[85]

According to the *proxy theory of legitimization*, any external limitation is legitimate or validated by its very existence. Limiting freedom in terms of 'external limitations on freedom', preceded by an initial consent grounded on the social contract, means once the subjects consent and enter into a social contract, they outsource their rights to the sovereign and delimit their 'absolute freedom', in which the subjects agree to all limits enforced by the sovereign.[86] The assertion mechanism of the social contract renders the subject to be the author of these limitations,[87] such that the individuals are not allowed to think about it, rather, they ought to conduct as per the applicable rules. This is the crux of the *proxy theory of legitimation*. It is an *a priori* limitation in the sense that neither the subject nor the sovereign is aware of under what conceptions his freedom will be limited.[88] Within the blockchain environment, the community provides a *one-shot legitimization* to the 'figure' who is the programmer of code when, first, there is an attribute in the plasticity of code norms to create a seemingly infinite number of conditions and programs that allow and restrict behavior through technological normativity, second, there is a protection of the private practices through legally authorized trade secrecy & confidentiality requirements, and third, there is a submission to the *sui generis* obscurantism of code norm.

'Representationalism' is the most relevant component in the blockchain environment[89] and is behind the strong legalism mechanism according to which law is 'just there'. On a 'representationalism' view, 'law is held to be a representation of reality', whose foundation lies in the reproduction, that is, the 'structure of reality' and construction, that is, a 'more active role in structuring reality'.[90]

In the context of law, the dynamic operation in this form of representation is the foundation of positive law that makes natural law present in its own particular way. It may be said that representation realism is most closely connected to realism. With representation-construction, the dynamics of the relationships are reversed, according to which concepts have no ontological value; rather, they are simply human constructs, defined by the sovereign. There needs to be a proactive definitive

[85] Wintgens (2016), chp. 6.

[86] Wintgens (2016), p. 204.

[87] Wintgens (2016), p. 208.

[88] Wintgens (2016), p. 207.

[89] This aspect will be discussed in depth in Chap. 6, Sect. 6.1.1.

[90] Wintgens (2016), pp. 208–209.

intervention by the sovereign, or else the laws of nature will not make sense; its representation within positive law can only occur through the sovereign's constructive intervention. The equivocality at the core of the relationship between representation-reproduction (precept of the eternal laws) and representation-construction (the materialized constructs defined by the sovereign) can be called 'the naturalization of positive law'.[91]

Even though distinctions lie between representation-reproduction and representation-construction, it can be ascertained how legalism's representation of reality is not the former but the latter. In other words, the construction is naturalized; it looks as if it were real—the naturalization fuses the construction with what is real or 'out there'. The striking correlation is that the representation in the blockchain environment is, to a greater degree, more cemented as compared to what the situation is in the context of a 'stronger' version of legalism since it is not a mere belief that 'the rules present reality' because the rule of code within the blockchain environment does not simply represent reality, rather is an active constituent or at least a participant.

Another element of strong legalism is 'timelessness or a-temporality', which emanates from the notion that 'law is a representation of reality', which represents 'law as it is'.[92] The collaboration between representation-reproduction and representation-construction amounts to manipulation of the concept of time and representationalism, leading to the reality being represented *ex-ante*. This collaboration is considered to be true and genuine, thus putting a veil over the constructivist intervention. This also means that the political space is not a natural datum and retains its existence as long as it is in compliance with the 'cognitively universal content of the clauses of the social contract'.[93] which are the true principles of public law. Consequently, the political space is, something that is valid, independent of human recognition, as it should be. Thus, the social contract can be perceived as the outcome of having access to reality and be deemed as a representation-reproduction that signifies the genuine tenets of the political right and their universal or a-temporal validity.

The etymology of legal rules at the constitution level and their validity is derived from the political space as it comes into existence. However, their participation in the 'a-temporal character or timelessness' of the contract itself causes a tension between contingency and a-temporality. Moreover, the tacit consent (the people's will which is articulated by the sovereign) has to be 'unveiled' and recognized by the contingent laws rather than reflect upon it since the norms created from 'the will of the sovereign' resemble the façade of timelessness.[94] The concept of 'a-temporality' of norms resonates with the rule of code's immutability

[91] Wintgens (2016), pp. 150–151.

[92] Wintgens (2016). pp. 151–153.

[93] Rousseau (1997), p. 152.

[94] Wintgens (2016), pp. 155–156, 157.

characteristics, and the approach developed to cope with the timelessness in legislating becomes relevant when drawing parallel with the blockchain mechanism.

The last element of strong legalism flows from the notion of 'the veil of sovereignty', which is used as a concealment tool to hide the legislator's values and resolutions. While values and goals must be selected, these choices cannot be justified through rational methods. This element is referred to as 'concealed instrumentalism', which is an ingredient of legalism that separates law and politics.[95]

The values and resolutions of the legislature remain in the political domain, camouflaged by the a-temporality of law. As can be evinced in textualism, the value judgments and instrumentalism in law can be concealed by excluding references to reality and value choices. Further, a-temporality conceals choice such that it evolves into a strategic plan to convert chaotic politics into something with rational reasoning and lawful elements. The notion of 'concealment instrumentalism' can also be found within the blockchain environment where there are, for example, the anti-competition laws drawing a veil on the rule of code to protect the economic benefits and commercial purposes of the corporation.

In other words, under the proxy theory of legitimation, as identified above through the characteristics of strong legalism, the subjects are required to grant a 'general proxy' to the sovereign, which consequently issues a limitation of their freedom or norms whereby the subject will act on *conceptions about freedom* instead of *conceptions of freedom*, whenever the sovereign desires. *Ipso facto*, the sovereign is bestowed with the legitimate authority to substitute *conceptions about freedom* for *conceptions of freedom* and can legitimately convert any propositional content into a norm.[96] This theory resonates well within the blockchain system, wherein the 'figure' assumes the role of the 'general proxy' and subjects the users to the rigid and immutable rule of code embedded in the technology to restrictions on their behavior by navigating their actions on *conceptions about freedom*, determined by the 'figure' themselves, and according to them, such code rules are legitimized by virtue of them producing such 'true' rule of code.

3.2.1.2 Trade-off Model Theory

To reduce the effect of strong legalism, the trade-off model theory was propounded by Wintgens, which does justice to freedom that is 'the principium of the organization of political space'.[97] It is not feasible to operationalize the concept of freedom unless it is related to a notion of freedom that renders action both possible and essential.

Freedom comes before the institution of the State. The first variant of freedom that can be deduced is the *state of nature* deriving from the situation where there is

[95] Wintgens (2016), p. 158.

[96] Wintgens (2016), p. 219.

[97] Wintgens (2016), p. 124.

no State. Therefore, such origin is a self-referential beginning, which indicates that freedom is a principium at *terminus a quo*. As a principium, it is both the beginning and the principle of action.[98] No action is possible without freedom at the beginning, and as a principle, it is mere behavior, and as such, action requires a reflective or rational choice. It may be discerned that freedom as principium is a thought-provoking abstract concept as it is not constituted with deductive reasoning, though the thesis is not arbitrary. This idea is reflexive because freedom is meaningful only when practiced in freedom, which speaks to the view that "freedom from freedom' makes no sense'.[99] As such, it can be inferred that there is a second variant of freedom that resonates with the perspective that 'freedom as the guiding idea or Leitmotiv in politics and law'.[100] This variant requires respecting the reflexive nature of freedom and continuously bringing justice to it, in addition to just respecting freedom at the beginning. It is, therefore, not enough to organize 'just' the freedom of others such that the legal norms limit the principium freedom for certain individuals or groups. The proposed norm constraining the principium freedom should not be justified but be rejected *a priori*, unless and until its imposition is adequately justified.

As per the notion of *freedom as principium,* it is not a legitimate exercise of power to make the citizens follow the rules, merely due to the rules being 'just there', like in the case of strong legalism. Despite the existence of any teleological value, it only displays the arbitrary exercise of sovereignty.[101] The conception of what freedom is, is not subjective to individuals and should not be interfered with and interpreted in line with the legislator's political agenda. Individual freedom is treated as supreme; therefore, the idea of substantive freedom of an individual always precedes over the external view of the State.[102]

Therefore, under the trade-off model, the subjects only trade-off *conceptions of freedom* for *conceptions about freedom* when substantial justification has been provided by the sovereign:

> Any A, therefore, will act on a conception about freedom C in situation S because the sovereign has justified this substitution.[103]

This means that there must be a rationale for the substitution of *conceptions about freedom* for *conceptions of freedom*—no rule can be deemed legitimate without proper justification. Under this model, the substitution is no more a *one-shot legitimation* of the sovereign's ruling; rather every limitation of freedom must be justified, which also makes up the core of legisprudential abstraction. There is no 'general proxy' under weak legalism that regulates the *conception of freedom* of individuals and unilaterally issues a limitation on the same; instead, it imposes a

[98] Aristotle (2009), pp. 31–34.

[99] Wintgens (2016), p. 125.

[100] Wintgens (2016), p. 207.

[101] Wintgens (2006), p. 10.

[102] Wintgens (2016), pp. 254–257.

[103] Wintgens (2016), p. 219.

critique of the *a priori* legitimation of law on the 'general proxy'. Under the trade-off model, legitimation of the law is required, which includes justification for preferring to act on a *conception about freedom* over a *conception of freedom*.[104] Such justification must, therefore, include reasons for assuming *a priori* that all external limitations of freedom are legitimate or justified under the proxy theory. According to the requirement of a justification of the external limitation of freedom, the chain of legitimation is reversed in that the unilateral nature of the proxy is to be complemented with the rationale provided by the sovereign to its subjects on the imposition of the external limitations.

In the case of a stronger version of legalism, the presence of the subject starts fading away as their moral autonomy evanesces due to the proxy consenting to the sovereign. The rudimentary error is that, in the proxy theory of legitimation, any *conception about freedom* under a general proxy is placed in a hierarchically superior position to any *conception of freedom*. This results in competition and incompatibility with the *conception about freedom*.[105] However, such a presumption would lead to failure of the political and legal system and thus jeopardizing the moral autonomy of the subject *qua* subject. Therefore, for the external limitations to be legitimate, the *conception about freedom* ought to be weighed against moral autonomy and also be justified, that is validated with reasoning. In case the conceptions about freedom do not satisfy the requirements or the design standards, the creation of the rule cannot be considered legitimate.

Wintgens, under his theory of legisprudence, has laid down, to some degree, design standards for legal rule formulation in terms of the test for the justification of limitation of freedom in order to mitigate legalism in the legal sphere, which is, first, failure of social interaction, second, insufficiency of weaker alternatives, third, justification for imposing an external limitation at a particular time, and fourth, justification with regards to the entire legal system. These standards commensurate with the four principles of legisprudence, which are 'the principle of alternativity, the principle of normative density, the principle of temporality, and the principle of coherence',[106] which translate or operationalize into duties *seriatim* that the legislator must consider when formulating a new legal norm. These standards intend to make the legal rule less legalistic and bring it closer to the aspect of legality, that is, the transition from legalism to legality is compatible with the principles of legality and henceforth adhere to the rule of law. Therefore, the concept of legality is worth examining, especially, what entails to fall within the circumference of the principle of legality, and what are the design standards for the legal rule formulation under this concept.

[104] Wintgens (2016), p. 220.

[105] Wintgens (2016), p. 221.

[106] Wintgens (2016), p. 284.

3.2.2 Legality: An Aspirational Concept

In contrast to legalism, legality, which is nested within the rule of law, is not 'only' confined to the requirement of a legal competence to perform governmental interventions. While strong legalism is at one extreme end of the spectrum, legal scholarship with ingredients of flexibility and discretion lies at the opposite end.[107] In between lies the legality, considered as an aspirational concept.

Since the constitution and limitation of law are rooted in the interplay of justice, legal certainty, and reasonability, a judicious conception of legality requires that the law constitutes as well as limits the competencies for governmental intervention. As the demands of justice, certainty, and purposiveness limit the resulting balancing acts, the circularity that permeates into legal development is neither vicious nor complacent, rather, it is virtuous and productive. Instead of promoting legal thoughts in a mechanical manner, it fosters insightfulness and judicious legal decision-making. For instance, if fundamental rights are infringed upon, the balancing act will entail the competent authorities to investigate the legitimacy of the proposed norm, the essentiality of the intervention, and its proportionality in relation to the norm. The balancing act will also require investigating the legal attributes that not only make such interventions predictable and disputable but also lay down necessary legal safeguards. Thus, in this case, the legal ground both constitutes and limits a specific governmental competence.[108] Legality is at variance from legalism in the sense that it looks for proportionality in justice, grounds for legal certainty, purpose of legal intervention, and requirement of effective remedies. On the contrary, legalism synthesizes all this to properly enacted laws, which may or may not protect the subjects making them susceptible to government interventions driven by 'the rule by law' and not 'the rule of law'. Legalism does not provide the individual subjects any viable answer against the arbitrary rule of the sovereign that practices 'the rule by law'.

The rule by law is essentially about self-binding, something akin to authoritarianism prevalent during the eighteenth century, but the rule of law is much beyond that. Legality, which is a strand of the rule of law, is the amalgamation of purpose-binding, not simply self-binding, and the imposition of checks and balances. The resulting 'modern laws' are characterized by, one, laws that are visible and intelligible to those whom the sovereign intends to rule and are constituted by democratic legislations (self-rule due to transparency and accountability), two, the subjects have the power to defy those laws and can exercise their autonomy (disobedience), and three, such legal norms are open to interpretation and as a consequence, if found violative, can be litigated against (contestability in line with the due process rights).[109] Therefore, the effective remedies that establish the rule of law in a State determine the protections offered by the principle of legality. Such protections can

[107] Bankowski (1989), p. 289.

[108] Hildebrandt (2013), p. 357.

[109] Hildebrandt (2015), p. 10.

be in the form of safeguarding fundamental rights, which play an essential role in averting the rule of law from retrogressing into the concept of rule by law.

Some authors enunciate that the collaboration between the heteronomous nature of legalism with legality *ad-rem*, or the threshold between principles and virtues of duties and aspiration, can ameliorate the individuals' legal access.[110] Legality requires a compatible amalgamation of the rules along with their considered interpretation, with the apt response that varies according to the circumstances. It is occasionally apposite for the subjects to *mindlessly* follow a rule, like a robot; on other occasions, it is incumbent upon the subjects to act *mindfully* of their own volition to determine their own behavior and reaction by mulling over what the rule means. While the former approach is representative of the 'stronger' version of legalism, the 'weak' version broadly represents legality.

Earlier discussions show that legality is conspicuously different from legalism and is neither a purely formal nor a purely substantive conception of law.[111] It is not limited, as a concept, to law's positivity, nor to its instrumentality nor its fundamental morality. The objective of the balancing act in relation to the legality principle is defined by the concept of proportionality, which talks about decisions borne out of inconsistent procedures. The decisions under the rule of law are not the outcome of a singular inner monologue, as these are not creations of any single individual. The balancing act requires that all the relevant voices are heard and taken into account in a confrontational debate, regardless of acceptance or rejection of a particular view. Since the idea of law is antinomian, the effect of prevalent legal conditions is often contingent upon incompatible conditions of justice, certainty, instrumentality, and morality. In other words, pertinent and relevant interpretation of the legal conditions is the product of a decision that must be firmed up after careful consideration of alternate viewpoints on the interaction between facts and law. In this context, legality does not speak up of proportionality as a coherent and reasonable calculation but about adequate procedures, acknowledgment of roles, and distribution of tasks. The requirement of a *mise en scène*[112] by legality precludes systematic domination of one party on the other, and hence, the courts have to assume a pivotal role as an independent authority who can safeguard the contestability of both the setting up and the actual implementation of interventions of the government. In that sense, one can observe the role of legality not only in the test of the right to privacy but also in the 'contestability' provisions, which allows to contest the legal claims in a court of law.[113]

Legality also refers to the legal approach, which is participatory and transparent.[114] The approach includes not only human rights and human dignity but also 'procedural public law values of transparency, accountability, rational reasoning,

[110] Bankowski and MacCormick (2000), p. 46.

[111] Shklar (1986), p. 1.

[112] Goodrich (2009), p. 1.

[113] Waldron (2011), p. 6.

[114] Brownsword (2011), p. 1363.

and consistency'.[115] Similarly, a *dignitarian aspect* of the rule of law conceives of the people who can comprehend and deal with the justification of the way they are governed and can relate their own view about the actions and purpose of the sovereign as bearers of reason and intelligence. If judicial procedures do not afford the opportunity to make such arguments when the State is putting pressure in its own ways, the individuals would never accept that the society is being governed by the rule of law. But with this strand of the rule of law, 'dignitarian respect has a price: it probably brings with it a diminution in law's certainty'.[116]

All these formulations of legality have a transitional quality that has some room for rational contemplation and the exercise of autonomy, positioning in between the heteronomous social rules and anarchy. The legal and social frameworks whose guiding forces and institutions create enough space that allow for deliberations, provide an equilibrium between autonomy and duty. As a result, though an indifferent justice system is at times insensitive and tough, an intimate justice that seeks to explore and grasp the boundaries of the private world also cannot be considered to be real justice due to its lack of 'evenhandedness'.[117] The principle of legality targets to maintain the balance between these extremes, affording a certain degree of institutional guidance and certainty while at the same time upholding freedom of autonomy and opportunity.

Legality also embraces certain aspects of legalism, which is an essential component of legality, bringing in the 'predictability' aspect that is crucial to avoid the essentiality of enquiring into the specifics of every case. Such 'predictability' is also required to establish a dependable institutional order, with enough scope for deliberation, so that the individual would be in a position to determine the next course of action. The rules and heuristics are not mixed with the entirety of the law in contrast to strong legalism. This view on legality concedes a 'dignified space for the reflexive practice of reason, intelligence, and freedom',[118] unlike the proxy model of strong legalism, which allows *one-shot legitimization* at freedom and sovereignty.[119] Within this *dignified* space, the three ideas of legality, justice, expediency, and certainty jointly govern the law in all its aspects, although they may sharply contradict one another.[120] For instance, contingent upon the circumstances, legal certainty, as a goal, maybe in continual and productive tension with the aims of justice and expediency. This may call for a constant reinvigorated balance depending on the specific cases entailing new interpretations and reasonings.

Moreover, where legalism only cares to sustain the limit of the morality of duty and no more, legality spreads out to include the concept of the morality of aspiration. Here, the aspect of authenticity also comes into play, which is one of the less

[115] Brownsword (2015), p. 48.
[116] Waldron (2011), p. 18.
[117] Fuller (1964), p. 72.
[118] Waldron (2011), pp. 19–20.
[119] Wintgens (2016), p. 206.
[120] Radbruch (1950), p. 111.

strictly highlighted values. It is not enough to satisfy the minimum standards derived from a plain interpretation of the rule rather, there is a need for an 'aspirational scale', allowing measurement of the expectation of an actor, where disobeying a rule can be morally desirable more or less, which according to consequentialism if it attains a better result. It may be said that on the aspirational scale, the morality of duty is just a point that represents the minimal action needed, 'just as the rules of a morality of duty prescribes what is necessary for social living'.[121] Such an aspirational scale is also required to access the legalistic characteristics of the rule of code like fixed configuration, which follows the principles of strong legalism to the maximum, so as to locate a 'somewhat balanced' position between the 'morality of duty' and 'morality of aspiration', such that the principles of legality can be programmed into code infrastructure of the blockchain, to a certain extent.

3.3 Fuller's Design Standards for Legality

Legality focuses both on 'what the concept of the rule of law is', which refers to the set of standards that constitute the law that shapes the process of creating norms and qualities of the 'end-product' rules, the *ex-ante* factor, and how the rule of law is administered and applied, the *ex-post* factor.[122] This relationship between 'the concept of the rule of law' and 'the administration of the rule of law' can be comprehended when we appreciate the rule of law in terms of procedures and arguments rather than purely in terms of determinacy and predictability –

> the procedural aspect of the rule of law helps bring our conceptual thinking about law to life, and recognition of rules provides the basis for a much richer understanding of the values that the rule of law comprises in modern political arguments.[123]

One of the most notable and instrumental discourses about the 'normative standards' for law-making 'by which excellence in legality may be tested' is Fuller's 'The Morality of Law'. According to Fuller, 'morality' could be morality of duty or morality of aspiration–

> the morality of duty may be compared to the rules of grammar and the morality of aspiration to the rules which critics lay down for the attainment of what is sublime and elegant in composition.[124]

The eight principles of legality of Fuller, which make up 'the inner morality of law', is more or less a 'morality of aspiration and not of duty' and is primarily drawn towards 'a sense of trusteeship'.[125]

---

[121] Fuller (1964), p. 6.

[122] Waldron (2008), pp. 10–12.

[123] Fuller (1964), pp. 4–5.

[124] Fuller (1964), p. 6.

[125] Fuller (1964), p. 43.

These standards aim to achieve 'good law' rather than just 'more law'. The objective of these principles or standards can be achieved in the business of legislation via recruiting and training 'carpenters' *vis-à-vis* the lawyers to understand 'how best to design a law rather than what its political content is'.[126] These eight principles or design standards, as laid down below, are not only about making good law from the perspective of the 'conscientious legislator' but also about constraining the 'unconscientious legislator' to avert the possible disproportionate unfaithfulness.[127] Here, the phrase 'Fuller's design standards' is being used instead of 'Fuller's principles of legality' because while principles entail a theoretical framework for creating law, design standards entail actionable guidelines to formulate the legal norm. Additionally, the idea of design standards is associated with the practical implementation of Fuller's idea to create a norm.

Standard 1: Norms should be general—'There must be rules' for subjecting human conduct to the governance of rules. This is the requirement of generality. The rules must be put in place with 'reasoned generality', requiring the rules to be articulated and conveyed to the subjects properly while avoiding the 'pattern-less exercises of political power' that is arbitrary.[128]

Standard 2: Norms should be promulgated—Promulgation as a standard pays much heed to the need to educate all citizens about the full implications of laws that may affect them. It requires the law to be made 'generally' available to those who are subject to the 'laws applicable to the practice of his calling'.[129] Moreover, it also requires that the law must be adequately published such that the subjects or citizens are given an opportunity to interpret and criticize them. This includes the opportunity to question whether certain laws should be enacted if their content cannot be effectively communicated to those who are subject to them and to observe how they are applied and enforced. The premise of this principle is that if laws are not easily accessible, there is no safeguard to ensure that those responsible for enforcing them adhere to such laws.

In addition to the legal norms being readily available, the promulgated norms under Fuller's standard 2 must additionally go through the test of the principle of alternativity as set out by Wintgens, which requires that justifications are provided for imposing or enforcing any limitation in the form of legal norm as a substitute for deteriorating social interaction. It, thus, prioritizes the subject's action on the conception of freedom; however, since social interaction can fail in the end, such prioritization is not absolute.[130] Since the trade-off model requires that any limitation of freedom or the legal norm be justified, it is argumentatively required to justify why an external limitation is preferable to no limitation,[131] which, in other words, means

[126] Fuller (1964), p. 156.

[127] Fuller (1958), p. 636.

[128] Fuller (1964), pp. 46–49.

[129] Fuller (1964), p. 51.

[130] Wintgens (2006), pp. 11–12.

[131] Wintgens (2016), p. 228.

that having or creating a legislative regulation is preferable to or better than self-regulation or no regulation. The principle of alternativity operationalizes freedom undetermined, which means that the requirement to respect freedom is necessitated, and this can only be achieved if the subject is allowed to act on conceptions of freedom.[132]

As per the principle of alternativity, the sovereign can intervene only on one condition that it justifies the promulgation of the legal rule or his external limitation to the extent that it is preferable to an internal limitation of freedom or its own internal processes as a reason of act to correct the dysfunction, due to a failure of social interaction.[133] Here, the focus is not on the substantive matter of the proposed rule but on whether it is justified to have a rule to any extent.

> If an external limitation must be justified, this justification must be preceded by an adequate analysis of the facts that form the state of affairs on which the external limitation will be superimposed.[134]

Therefore, the principle of alternativity is a threshold requirement subjected under Fuller's standard 2. Once the proposed rule crosses the threshold, it is linked with the principle of normative density in respect of the behavioral impact of the design mechanism that is selected.

According to the principle of normative density, the limitation to be imposed must show that the impact or normative density of such a limitation is necessary to achieve the goal. The requirement of the principle of normative density, like the principle of alternativity, is that sanctions and external limitations imposed through the promulgation of the legal rule, respectively, are not *a priori* justified, as they are in the case of the proxy model. Under the trade-off model, while the principle of alternativity requires justification of the purpose, the principle of normative density calls for a justification of the means of realizing it.

Fuller's standard 2 also calls for a test of the principle of coherence at the time of promulgation of the legal norm where it makes a supposition that the rationality of the legislator cannot be presumed with certainty and thus, it implicitly requires the legislator to justify his external limitations so as to let the judge make compossibility or system coherence arguments. This is in contrast with strong legalism, where the rules promulgated by the legislator are law and have to be dealt with by the adjudicator irrespective of the degree of incoherence. Therefore, once the central position of the judge is restricted, the stance of the legislator becomes evident through legislative activism, which is an active justification of external limitation or legal norm promulgation, such that its effects gel with the rest of the system, including *ex-post* adjudication.[135]

---

[132] Wintgens (2016), p. 259.

[133] Wintgens (2006), p. 14.

[134] Wintgens (2016), p. 269.

[135] Wintgens (2006), p. 20.

Standard 3: Norms should be prospective and not retrospective—Fuller considers retroactive laws to be 'truly a monstrosity'.[136] This principle affects the previous two 'desiderate of legality' such that if the laws promulgated make conduct unlawful that was permitted when the event occurred, it impairs the ability of the affected citizens to know and obey the law, thus resulting in the failure of the two principles.[137] However, in certain situations, intelligently assessing retroactive laws may lead to granting retroactive effects to legal rules that are not only acceptable but also crucial for advancing the cause of legality.

Standard 4: Norms should not be unclear—According to Fuller, legality cannot be attained by obscure and inherent legislation. He views this desideratum as representing one of the most essential ingredients of legality. Should a rule lack clarity so much so that its interpretation 'twists' its primary 'kosher' meaning or the intent behind it and repeatedly runs into the legality buffer, it only indicates that the law that is 'actually applied' is not the same as the law as it was proclaimed.[138] This principle requires the legislator to do more since, according to legalism, what is perceived as law is law; that is, formal validity gives rise to law, irrespective of its content.

This desideratum on clarity is in line with the idea of coherence of the legal system, which focuses on the coherence of legal reasoning and on the coherence of the legal system since the legal system is composed of a number of complex and dynamic set of interlinked propositional rules relating to what ought to be done and how it ought to be done.[139] There are four levels of coherence,[140] underpinning the level theory of coherence, which applies to *ex-ante* legislative as well as *ex-post* judicial reasoning.

Standard 5: Norms should not be contradictory—Fuller states that contradictory laws are those that oppose each other without necessarily negating one another, as contradictory statements do in logic;[141] this renders them essentially 'repugnant'.[142] The general assumption is that it is 'simply one of logic' problems, where a 'contradiction is something that violates the law of identity in which A cannot be not-A'.[143] However, this is not true, as how much ever value this formal logic has, it is considered to be redundant in dealing with contradictory laws as it does not resolve the contradiction itself. To determine the issue of incompatibility between two laws, it

[136] Fuller (1964), p. 53.

[137] Fuller (1964), p. 54.

[138] Fuller (1964), pp. 63–65.

[139] Wintgens (2006), p. 15.

[140] These levels are the level of coherence0 (internal or synchronic coherence), the level of coherence1 (diachronic or rule coherence), the level of coherence2 (compossibility or system coherence), and the level of coherence3 (environment coherence). Wintgens (2006), p. 15.

[141] Fuller (1964), pp. 63–65.

[142] Fuller (1964), p. 69.

[143] Fuller (1964), p. 65.

is merely not enough to take into account the technological aspects, but an additional layer of extra-legal factors have to be considered.[144]

Moreover, this standard depends on intelligibility, where it must also satisfy the requirements of semantic and syntactic identity, without which a norm may be formally valid but incoherent because it makes no sense as a standard for conduct or for judgment.[145] This resonates with the legisprudential principle of coherence. For any form of discourse, internal or synchronic coherence is a necessary condition for its soundness or for making sense, which advocates for inconsistencies or contradictions to be not allowed within or in a judicial decision or legislative enactments.[146] The two elements, namely, the alignment of the understanding of individuals in respect of the intention of a concept and the absence of plausible contradiction between those understandings, can be read together at this level. According to Fuller, difficulties surface when resolving the contradictions that develop within the frame of a single statute by effecting a mutual adjustment between the two statutes and interpreting one in light of another due to the carelessness of the legislator in undermining the friction between the two statutes and thus crippling legality.[147] Internal or synchronic coherence intends to alleviate such carelessness and promote legal certainty, which operates as the index of truth in modern philosophy.

In addition to internal or synchronic coherence, coherence3 or environment coherence (as called by Wintgens) is also a necessary complement to the Fuller's standard 5. At this level, where one needs to 'make sense of the legal system as a whole',[148] an 'external rationality' is essential since, in its absence, one cannot visualize something as a whole.[149] Though it is possible for the legal system as a set of external limitations to be internally rational or coherent, it would not make sense as a whole unless a perspective that makes it possible to see it as a whole is included.[150] In addition to the general observance that law does not operate in a vacuum, we must also be sensitive to this fact and imbibe the same by justifying it according to the broader societal context. Fuller makes a similar argument in relation to the contradictory rules.[151] Further, as the whole becomes more coherent through the transformation of its elements, it is essential that the whole *qua* whole is taken into consideration.

Standard 6: Norms should not require the impossible—The essential concept for this desideratum is simple—the promulgation of laws that demand the impossible face the risk of 'doing serious injustice or… diluting respect for law'.[152] A law

[144] Fuller (1964), p. 70.
[145] Wintgens (2006), p. 16.
[146] Fuller (1964), pp. 65–70.
[147] Fuller (1964), p. 69.
[148] Luhmann (1988), p. 136.
[149] Wintgens (2016), p. 252.
[150] Wintgens (2006), p. 20.
[151] Fuller (1964), p. 70.
[152] Fuller (1964), p. 71.

commanding the impossible would not only seem absurd such that one would view the law-making business to have no sane lawmaker but also there would be no reason to enact it; 'not even the most evil dictator' would do it. For example, just as it is impossible to follow a law that requires someone to become ten feet tall, it is also impossible to obey a law that is unknown, unintelligible, or has not yet been enacted.[153] However, the tactic of demanding the impossible can be exploited in more subtle ways and sometimes even for beneficial purposes.

Standard 7: Norms should be relatively constant—Fuller notes a significant connection between the harms caused by retrospective legislation and those arising from frequent changes in the law apropos the 'birth of injustice'.[154] From the perspective of the rule of law paradigm, this requirement is beguiling. If the law is aiming for the normalization of expectations, then it can be achieved only if norms have the opportunity to settle in the society in which they are promulgated.

Fuller's standard 7 also conforms with the principle of temporality, laid down by Wintgens, which indicates a substantial departure from the 'single moment focus of strong legalism',[155] since rules or external limitations being human creations are linked to historical conditions. So much so that one can say human activity is replete with temporality. Though justification for legislative norms may change over a period of time, according to strong legalism, it is impossible to predict the future in all its detail since 'the law is the law until the legislator changes it'. The principle of temporality demands that the legislators must argue why a norm or external limitation is necessary now 'all things considered now', or as Wintgens calls it 'the ATCN clause'.[156] This clause indicates that it is 'only the right time now' to issue a norm. In this respect, according to the principle of temporality, the legislator has to argue why he acts now and consider the passage of time, as is demanded by weak legalism.[157] However, norms issued at a time and duly justified or legitimated according to the principle of temporality, the ATCN clause may lose its legitimacy over time. Justification under the principle of temporality is an ongoing justification in that legislators must be capable of continuously upholding their rulings. Even if their working field is the future, they cannot overlook it *sub specie aeternitatis*. The principle of temporality expects a thoughtful approach towards the prospective effects of the rule; continuous assessment of these effects, their subsequent rectification and re-justification are also needed to take care of untended effects.[158]

In addition to necessitating the legal norm to maintain constancy over time and be justified continuously at constant term points, Fuller's standard 7 also requires the norm to be coherent with the principle of equality or formal justice or diachronic or rule coherence (as proposed by Wintgens) and reflect the consistency needed by

[153] Fuller (1964), p. 70, footnote 29.

[154] Fuller (1964), p. 80

[155] Wintgens (2016), p. 268.

[156] Wintgens (2006), pp. 13–15.

[157] Wintgens (2016), p. 269.

[158] Wintgens (2016), pp. 301–304.

the rule of law which maintains the horizontal continuity across the system. Accordingly, a normative demand pushes for 'equal treatment for equal cases'.[159] This level of coherence takes into consideration the time dimension, recognizing that not all judicial decisions are made on the same day, by the same judge, or based on identifiable facts. Diachronic or rule coherence requires that the progression of elementary units or judicial decisions be submitted to the norm of fair treatment or of formal justice.[160] This means that similar cases should receive equal application of the general norm. Since the deviation from a general norm, precedent, or settled practice of interpretation may jeopardize coherence, the lowering of the degree of diachronic or rule coherence through legislative amendments when the legislator engages in steering legislation, creating expectational formal injustice and frustrating legitimate expectations,[161] may clash with fair treatment. Fuller defines this as 'legislative inconstancy' where the harm is caused due to too frequent changes in the law.[162]

Standard 8: The administration of the norms should be congruent with its published rules—According to Fuller, this is the 'most complex of all the desiderata that make up the internal morality of the law'. In this case, congruence may be impeded due to inaccessibility of law, deliberate or otherwise misinterpretation, corruption, bias, the pursuit of personal power, and lack of adequate information to maintain the integrity of legal infrastructure.

This, suppositionally, illustrates a 'boilerplate clause' or a 'blanket requirement' that obligates the procedural devices to be designed in a variety of forms to subside the threats towards the congruence that might manifold. These procedural mechanisms are represented in the configuration of procedural due process, judicial review, and contestation which need to operate to identify and address the exclusively mentioned problems. The desideratum also causes negative departures from other principles of legality:

> failure to articulate reasonable, clear general rules and an inconstancy in decisions manifesting itself in contradictory rulings, frequent changes of direction, and retrospective changes in the law.[163]

The problem of incongruence may also arise due to constancy and retroactive principles since there is a probability of latent incongruency to materialize due to evolving circumstances, which may cause friction with once-settled legal arrangements or law.

The 'inner morality of law' set up by the aforesaid eight standards or principles is distinct from the 'external morality of law'. However, both interact with each other, where the 'inner morality of law' is fundamentally concerned with the procedure of making law, and the 'external morality' is about the substantive rule of law

[159] Wintgens (2006), p. 16.
[160] Hart (1961), pp. 157–167.
[161] Wintgens (2016), p. 257.
[162] Fuller (1964), pp. 79–80.
[163] Fuller (1964), p. 82.

or norms which are applied in arriving at a decision. Fuller also emphasizes that internal morality should never be discretionary and non-compulsory regardless of one's political affiliation, as the internal morality of law depends on norms that are universal in the rule of law environment.

It may be noted here that Fuller's principle is an amalgamation of both *ex-ante* and *ex-post* standards. The *ex-post* standards are guided by standard 2 and standard 8, discussed earlier, where the former requires the rules to be publicized once made, and the latter obligates the executing authority to 'only' operate according to the rational interpretation of the substantive rule, subject to the 'umbrella' requirement of contestation. Concomitantly, the *ex-ante* standards are illustrated by standards 3, 4, 5, and 6, where they pilot the configuration of the proposed rule, restricting and regulating '*ex-ante*' its substantive content, provided that the rules are not or cannot be retroactive, only with exceptions there lies a possibility, the rules must be reasonably comprehensible and coherent to enable interpretation by the regulatees, there cannot be any scope for contradiction with the extant rules without altering or repealing them, and there cannot be any impossible demand by the rule.

3.4 Design Standards for 'Legitimate' Legal Rule Formulation

3.4.1 Legitimacy of Legal Norms

A legal norm is considered legitimate when its formulation is imposed within the constraints of the rule of law:

> there is a set of constraints – settings, procedures, hesitations, that form the specific legal régime d'enonciation – that must be respected in order to make law or 'to practice law'.[164]

In other words, the rule of law by restricting the arbitrary exercise of power, is a chief normative ideal that gives legitimacy to the legislations and the legal system. One of the principles of the rule of law is legality, which is based on the requirement of certainty of law, which is an inherent element of the conceptualization of the rule of law, and legality can confer legitimacy to a certain extent only when the legal system instinctively adapts to the justification requirements produced by the constructive evolution of law—more especially, in a fashion that institutionalizes legally valid decision-making processes. Legitimacy is essential to upholding and supporting the law; it does not, however, supplant or surpass legality. In the absence of legitimacy, laws, legal institutions, and procedures will, in fact, be regarded with contempt. Thus, legitimacy has two functions. It can strengthen the principles of legality and increase the authoritative power of the rules. Legitimacy, however, can be a corrective force when laws are perceived as limiting, redundant, or detrimental

[164] Gutwirth et al. (2008), p. 197.

to people; it can be invoked in the name of the rule of law, for instance, environmental security, emergency protection, human dignity, or global justice. Legitimacy has the power to concurrently bolster and oppose legality. What is legitimate ought to be legal, and what is legal ought to be legitimate. But the word 'ought to' alone implies that such unity may not constantly be present. Therefore, in addition to outlining the design standards for legal rule formulation in the context of legalism and legality, it is pertinent to discuss the design standards for 'legitimate' legal rule formulation, which will bring us further closer to understanding 'what constitutes the rule of law'.

The rule of law within the framework of democracy and legitimacy within the discourse of legal studies as well as political science studies is said to define two legitimizing mechanisms, that is, *ex-ante* and *ex-post*, which deal with certain values of the rule of law such as accountability, transparency, predictability, consistency, inclusiveness, and due process. Both types of legitimacy convey a comprehensive evaluation of the legal rule's values; however, *ex-post* legitimacy must be attained by evaluating the legal rule's efficiency, whereas *ex-ante* legitimacy concerns the design of the rule, what makes the legal rule valid, not just describing what legal rule is but describing the characteristics the legal rule ought to have.

In relation to legislation, the concept of *ex-ante* legitimacy, which resonates with the process being complied with at the law-making stage, conventionally requires participation and representation in some manner, whereas the concept of *ex-post* legitimacy, which is at the result stage, means that the legitimacy is established through an evaluation of the outcomes of a rule's functionality.[165] For a norm to realize legitimacy, there needs to be an agreement regarding the origin, embodiment, and formulation of the norm, that is, the *ex-ante* procedure, followed by any discussion and criticism regarding the appropriateness and interest of the norm's functional substance, that is the *ex-post* substantive content.[166] This difference between *ex-ante* and *ex-post* functionality resonates with the Fullerian ideas of the inner and external morality of law. Where the *ex-post* standards address the effectiveness or desirability of a particular norm, the *ex-ante* standards focus on the procedural and formal aspects of its genesis.

In the case of *ex-ante* standards, the focus is on duty & morality, while *ex-post* standards emphasize on consequences. These two perspectives interact, and their upshot is dependent upon the conditions that may lean towards both unwanted and wanted substantive rules normatively.[167] Since the principles of legality show an inclination towards less substantive iniquity, the *ex-ante* or inner morality holds back the substantive content of its *ex-post* or external morality, resulting in the form of limiting substance.[168] Likewise, whether a proposed legislative rule is legitimate or not, is subject to justification by the principles of legisprudence, which determine

[165] Waldron (2006), p. 1346.

[166] Waldron (2006), p. 1387.

[167] Waldron (2006), p. 1374.

[168] Fuller (1958), p. 636.

the minimum requirements to obtain legitimacy. Thus, while legisprudential principles are about legitimizing an invasion on freedom, such invasions are *a priori* illegitimate without adequate justification. Similar to Fuller's principles of legality, the legisprudential principles also have equal weight. These principles are aspirational in nature and not really intended to be fully embodied in a proposed norm. Rather than making futile efforts to achieve a perfection that is unattainable due to various constraints and limitations inherent in predicting the future, these principles aim to develop the best possible laws.[169]

One can understand how Fuller's design standards and the principles of legisprudence collaborate and coordinate with each other from the deliberations of *ex-ante* and *ex-post* legitimacy. While Fuller's standards are more transferable, the legisprudential principles constrain the rules more forcefully than what is feasible for the substantive content of a rule. Through this analysis, four categories constituting different standards have been identified based on their target and temporal position. Out of these, two categories are in terms of *ex-ante* standards—first, the procedural standard that controls the process of deliberation that leads to the creation of a given norm, and second, the standard that restricts the norms' formal qualities, which are assessed independently from its substantive content. The other two categories are in terms of *ex-post* standards—third, the mechanism to maintain transparency, accountability, and due process to enable the identification and rectification of operational mistakes, and fourth, evaluations of the norms' moral or political contents.

In most frameworks, theorists incorporate standards from more than one of these categories. In the case of *crypto-legalism*, there is a need to focus on the categories in terms of *ex-ante* standards. However, the *ex-ante* procedural standards are less likely to be applicable as compared to the *ex-ante* formal standards in the private sector as they lack adequate incentives and resources. If the aforementioned types of formal features are expected from a normative order that constitutes as well as regulates behavior, then it would be reasonable to expect such standards to be present in all environments, be it the blockchain environment or the rule of law environment. These standards would then be adapted to the technological design environment.

3.4.2 The Rule of Law Values for Ex-ante *and* Ex-post *Affordances*

From the analysis of the notion of legalism and legality as a strand of rule by law and the rule of law conceptualization, it can be deduced that five core values, namely transparency, accountability, predictability, consistency, and due process or contestability, are associated with the rule of law. These values promote the rule of law through technology and are generally accepted as pivotal values that are key to restraining the arbitrary exercise of power by the State and upholding political legitimacy.

[169] Wintgens (2016), pp. 282, 305–307.

One of the central features of the rule of law is that the governments or the authorities must be transparent and accountable in their decision-making. Transparency, which stands for 'the commitment to openness and candor',[170] demands that the State publicize its decisions and functions appropriately, including electoral processes, accessibility of legislations, policy decisions, and executive decisions to the citizens.[171] Such transparency can empower individuals to appreciate the reasons for the decisions that affect them and to learn about future decisions that may be made. Transparency plays an important role in safeguarding the accountability of the State. Accountability is identified as the responsibility for the exercise of power, which requires that the State should be subject to the law and be answerable for its decisions or actions.[172] As the separation of power thesis in the governance models is designed to promote the accountability of those who exercise sovereign power through appropriate checks and balances, accountability as a principle is ingrained into it.

Another crucial value of the rule of law is that it invariably obligates the law to be predictable and consistent.[173] Certainty and efficiency of the governance system which everyone desires for better public services and also to manage their private affairs effectively, gets enhanced with the principles of predictability and consistency. In this regard, Lord Bingham suggested that the predictability in the conduct of individuals, their lives and businesses[174] is the most significant thing individuals need from the law. Similarly, regularity or consistency is an essential requirement for a political state under the rule of law. Further, authorities are empowered to use State coercion but must be constrained by specific legal rules. Predictability and consistency also entail a moral significance in that *similar cases be treated similarly*.

Another value of the rule of law is 'due process rights' which requires that all individuals are subject to the same set of rules to ensure justice to all.[175] This value stems from the wider principle of 'equality before law', which stipulates that any individual or group can neither enjoy privileges nor be discriminated against due to personal bias or attributes. Though the scope and content of 'equality before law' are debatable, it can still bring about a range of significant rights. Irrespective of the status of the individuals, this value is applied to provide access to rights, *similar cases be treated similarly,* meaning equal access to rights in the law, including contestability rights.[176] This strand of the rule of law will need the testability of the technological systems as a prerequisite to critically evaluate the *ex-post* outcome.

[170] Fenster (2005), p. 885.
[171] Gowder (2016), p. 7.
[172] Kroll et al. (2017), p. 633.
[173] Fuller (1964), pp. 79–80.
[174] Bingham (2007), pp. 66–84.
[175] Dicey (1915), pp. 114–115.
[176] Hart (1961), pp. 100–110.

These values emphasize both the procedural, formal, and substantive aspects of the rule of law and its capacity to include a wider range of values comprising privacy, transparency, freedom of expression, and human rights. More specifically, the attention is on whether values connected with a traditionalist, minimalist conception of the rule of law can be designed into the blockchain architecture as an *ex-ante* technical command code rule and an *ex-post* conceptual code rule and also facilitates an obligation to build such infrastructure to develop these systems with the mechanism and purpose to protect the rule of law principles.

References

Aristotle (2009) The politics. (Ernest Barker Trans.). Oxford University Press
Bankowski Z (1989) Institutional legal positivism. Rechtstheorie 20:289
Bankowski Z, MacCormick N (2000) Legality without legalism. In: Krawietz W et al (eds) The reasonable as rational: on legal argumentation and justification. "Festschrift" for Aulis Aarnio. Duncker & Humbolt GmbH, p 46
Beetham D (1991) The legitimation of power. Humanities Press International, p 4
Bekkers V, Edwards A (2007) Legitimacy and democracy: a conceptual framework for assessing governance practices. Governance and the Democratic Deficit. Routledge, pp 44–45
Bingham T (2007) The rule of law. Cambridge Law J 66(67):66–84
Brownsword R (2011) Lost in translation: legality, regulatory margins, and techno-logical management. Berkeley Technol Law J 26:1321
Brownsword R (2015) In the year 2061: from law to technological management. Law Innov Technol 7:1–51
Brunnée J, Toope SJ (2010) Legitimacy and legality in international law: an interactional account, 1st edn. Cambridge University Press, p 54
Clark I (2005) Legitimacy in international society, 1st edn. Oxford University Press, pp 18–19
Cottier T (2009) The legitimacy of WTO. In: Yueh L (ed) The law and economics of globalisation. Edward Elgar Publishing, p 9
Dicey AV (1915) Introduction to the study of the law of the constitution: introduction to the eighth edition. (2007) Giornale Di Storia Costituzionale 13:171
Dworkin R (1986) Law's empire. Harvard University Press
Dyzenhaus D (1999) Legality and legitimacy: Carl Schmitt, Hans Kelsen and Hermann Heller in Weimar. Oxford University Press
Fakhri M (2009) Reconstructing the WTO legitimacy debates towards notions of development. CLPE Research Paper
Fenster M (2005) The opacity of transparency. Iowa Law Rev 91:885
Finnis J (2011) Natural law and natural rights. Oxford University Press, p 270
Franck TM (1988) Legitimacy in the international system. Am J Int Law 82:705
Franck TM (1990) The power of legitimacy among nations, 1st edn. Oxford University Press, p 24
Friedman LM (1977) Law and society - an introduction. Prentice Hall, p 139
Fuller LL (1958) Positivism and fidelity to law--a reply to Professor Hart. Harv Law Rev 71(630):636
Fuller LL (1964) The Morality of Law
Fuller T (1732) Gnomologia: Adagies and Proverbs; Wise Sentences and Witty Sayings, Ancient and Modern, Foreign and British, vol 1. B Barker
Goodrich P (2009) Screening law. Law Liter 21:1
Gowder P (2016) The rule of law in the real world. Cambridge University Press, p 7

Gutwirth S et al (2008) The trouble with technology regulation: why Lessig's 'Optimal Mix' will not work. In: Brownsword R, Yeung K (eds) Regulating technologies: legal futures, regulatory frames and technological fixes. Oxford University Press, p 193
Hart HLA (1961) The concept of law. Oxford University Press, pp 100–110
Hildebrandt M (2008a) A vision of ambient law. Regulat Technol 175, 178
Hildebrandt M (2008b) Legal and technological normativity: more (and less) than twin sisters. Techne: Res Philosophy Technol 12:169
Hildebrandt M (2013) Balance or trade-off? Online security technologies and Funda-mental rights. Philosophy Technol 26:357–379
Hildebrandt M (2015) Smart technologies and the end (s) of law: novel entanglements of law and technology. Edward Elgar Publishing, p 10
Holovaty S (2006) The rule of law, vol 1. Phoenix Publishing House, p 214
Hurd I (2007) After anarchy: legitimacy and power in the United Nations security council. Princeton University Press, pp 66–73
Ihde D (1990) Technology and the lifeworld: from garden to earth. Indiana University Press
Kay RS (2009) Original intention and public meaning in constitutional interpretation. Northwest Univ Law Rev 103:703
Kelsen H (1991) General theory of norms. Oxford University Press
Kelsen H (2017) General theory of law and state. Routledge, pp 110–122
Kroll JA et al (2017) Accountable algorithms. Univ Penn Law Rev 165:633
Krygier M (2008) The rule of law: legality, teleology, sociology. In: Palombella G, Walker N (eds) Re-locating the rule of law. Hart Publishers
Krygier M (2011) Four puzzles about the rule of law: why, what, where? And who cares? Getting Rule Law 64:89
Krygier M (2016) The rule of law: pasts, presents, and a possible future. Ann Rev Law Soc Sci 12:203
Latour B (2010) The making of law: an ethnography of the Conseil d'Etat. Polity, p 280
Luhmann N (1988) Law as a social system. Northwest Univ Law Rev 83:136
MacCormick N (1989) The ethics of legalism. Ratio Juris 2:184–193
MacCormick N (2005) Rhetoric and the rule of law: a theory of legal reasoning. Oxford University Press
Petersmann EU (2000) The WTO constitution and human rights. J Int Econ Law 3:19
Priel D (2011) The place of legitimacy in legal theory. McGill Law J 57(1):8
Radbruch G (1950) 'II. LEGAL PHILOSOPHY', The Legal Philosophies of Lask, Radbruch, and Dabin (Kurt Wilk Tr, Harvard University Press, p 43, 111
Raz J (1975) Practical reason and norms. Hutchinson 26:38–48
Raz J (2017) The rule of law and its virtue. In: Bellamy R (ed) The rule of law and the separation of powers. Routledge, pp 77, 210
Rousseau J (1997) Rousseau: 'The Discourses' and other early political writings, vol 1. Cambridge University Press, p 152
Scharpf F (1999) Governing in Europe: effective and democratic? Oxford University Press, p 11
Shklar JN (1986) Legalism: law, morals, and political trials. Harvard University Press, p 1
Shklar JN (1989) The liberalism of fear. In: Rosenblum NL (ed) Liberalism and the moral life. Harvard University Press
Strauss DA (2010) The living constitution. Oxford University Press
Suchman MC (1995) Managing legitimacy: strategic and institutional approaches. Acad Manag Rev 20:571
Swan M, De Filippi P (2017) Towards a philosophy of Blockchain. Metaphilosophy 48:5–619
Tamanaha BZ (2004) On the rule of law: history, politics, theory. Cambridge University Press
Thomas CA (2014) The uses and abuses of legitimacy in international law. Oxf J Leg Stud 34:729–758
Waldron J (2006) The core of the case against judicial review. Yale Law J 115:1346

Waldron J (2008) The concept and the rule of law. NYU School of Law Public Law & Legal Theory Research Paper Series, Working Paper 218
Waldron J (2011) The rule of law and the importance of procedure. In: Fleming J (ed) Getting to the rule of law. NYU Press, p 3
Waldron J (2016) The rule of law. The Stanford Encyclopedia of Philosophy. https://plato.stanford.edu/archives/fall2023/entries/rule-of-law/
Waldron J (2017) Is the rule of law an essentially contested concept (in Florida)? In: Bellamy R (ed) The rule of law and the separation of powers. Routledge, p 117
Weber M (2009) The theory of social and economic organization. Simon and Schuster
Wintgens LJ (2002a) Legisprudence: a new theoretical approach to legislation. Hart Publishing
Wintgens LJ (2002b) Legislation as an object of study of legal theory: legisprudence. In: Wintgens LJ (ed) Legisprudence - a new theoretical approach to legislation. Hart Publishing, p 20
Wintgens LJ (2006) Legisprudence as a new theory of legislation. Ratio Juris 19:1–25
Wintgens LJ (2016) Legisprudence: practical reason in legislation. Routledge, p 220
Wintgens LJ (2017) The theory and practice of legislation: essays in Legisprudence. Routledge

Chapter 4
Interaction Between Blockchain and the Rule of Law

4.1 Blockchain and Regulation

Blockchains are at once regulatable and regulatory technology.[1] There is no paradox in that statement—the blockchain code itself is self-enforcing, regulating those who engage with it. Code truly is one of the many forms of law. As such, distributed ledgers are one of many technologies that regulate those who engage with them. Code's regulatory potential made explicit by Reidenberg[2] and Lessig[3] in the 1990s, has long materialized. For example, online platforms have become regulatory agents of their own motion and are also encouraged to assume such tasks by States, including the European Union.[4]

At first sight, law and code are noticeably distinct. Law is all about intentions, which is purposefully vague, while code is about the process and, accordingly, must be specific.[5] Code embedded in the blockchain has a normative dimension, however, in that it governs the behavior of those who engage with it. While code is increasingly assuming the function of law, law is also progressively taking the form of code.[6] In recent times, we see the technical code merging with legal code, resulting in giving expression to the normative objectives of the 'figure' or its creator—whether these are public entities, such as the European Union and its member States, or private actors, such as operators of online platforms or those in charge of

[1] Dimitropoulos (2020), p. 1117.

[2] Reidenberg (1997), p. 553.

[3] Lessig (1999), p. 3.

[4] Finck (2018), p. 47.

[5] Shapiro (2002), p. 387. Fischer (2006).

[6] Schafer (2022).

A. Bisoyi, *Blockchain and Legitimacy*, Law, Governance and Technology Series 77, https://doi.org/10.1007/978-3-031-98712-0_4

blockchain regulation. This novel form of legal 'code-ification' is not a matter of surprise, as technological change has always been a source of legal change.[7]

With increasing online communications and transactions in society, regulatory functions of our online and offline lives have been taken over by digital platforms, as many transactions are governed by their terms of service, and platform-based dispute resolution mechanisms are enforced, disassociating ordinary courts.[8] These developments indicate that code has become a remarkably efficient regulatory tool, increasingly assuming the traditional function of law in shaping human behavior. Programming code has thus started a new era of legal code-ification. With the evolution of such digital jurisdictions, the famous quote, *'code is law',* coined by Lessig in the late 1990s, has a wider significance. Lessig was referring to the architecture of the Internet and its potential to impose certain regulatory effects on Internet users—by embedding a certain value principle, the architecture sets the terms on which the Internet can be used and thereby defines what is possible in that space. The blockchain technology has come to constitute an important building block of that evolution. Two main elements ground blockchains' potential as a regulatory technology. First, distributed ledgers' protocols enforce the 'figure's' normative choices. Depending on their respective set-up, this could be leveraged by both public and private actors to create a favorable environment for transactions that follow a definite set of rules, which may or may not reflect applicable laws. Second, blockchain applications, especially smart contracts, can be designed to be self-enforcing, automating compliance with a predetermined rule set.[9] However, smart contract execution cannot be stopped unless this is explicitly indented from the beginning, leading to the automated enforcement of the encoded rule set.

> As a result of these technological advances, the lines between what constitutes a legal or technological rule becomes more blurred since smart contracts can be used as both a support and as a replacement to legal contracts.[10]

Can law effectively be substituted by the blockchain? The functional similarities between code and law and that of between digital and legal jurisdictions may indeed seem increasingly striking due to the advances in blockchain technology. The real concern is that both sets of rules are by no means necessarily congruent substantively, as they may well steer to different significant results: diverging results occur whenever the technologically codified rules differ from the applicable legal rules or whenever both sets of rules, even if their substance based on the similar principle, are applied in different manners.

---

[7] De Filippi and Hassan (2016). https://firstmonday.org/ojs/index.php/fm/article/view/7113/5657

[8] Finck (2018), p. 47.

[9] Hassan and De Filippi (2017), pp. 88–89.

[10] De Filippi and Hassan (2016), p. 2.

4.2 Code in Public and Private Regulatory Frameworks

The technological architectures are the foundation and primary instrument of regulation: the notion of 'regulation' signifies a sustained and focused attempt to influence the behavior of others according to specific standards or objectives, aiming for recognized outcomes, which may involve 'mechanisms of standard-setting, information-gathering and behavior-modification'.[11] Broadly, regulation is

> encompassing any instrument (whether legal or non-legal, governmental or non-governmental in nature, direct or indirect in its operation, etc.) that is designed to channel group behavior.[12]

Such a perspective aligns with Lessig's theory—once the new architecture becomes widely available, other regulatory tools, such as law and social norms, flood in, and further constraints and limitations emerge. Users of the architecture, as well as the 'figure', adopt social norms, market policies, and legal regulations to bias the behavior of other users. From a narrower perspective, regulation may be defined as 'intentional attempts to alter the behavior of others in order to address a collective issue or problem'.[13] Therefore, it can be said that the only limit on behavior is provided by the technological architecture, the consciousness of those utilizing it, and the intention of the 'figure'.

Nevertheless, technology is able to manipulate the symbolic and fictional structure of society, which is the very structure that constitutes legitimizing the basis for law, by sculpting social habits and the normative assessment of the world, society, and self. One example to illustrate this is the emergence of *Lex Informatica*, a system of customary rules (or standards) and technical norms that developed after the advent of the internet, wherein the internet created a new architecture of social interaction.[14] Reidenberg was the first scholar to formulate the idea of information policy rules through technology and advocated the need for a *lex informatica* since rulemaking in cyberspace occurs partly through a technical architecture. *Lex Informatica* institutes a specific set of technical norms, standards, and rules that reflect the vision as well as the explicit and implied expression of the 'figure' responsible for developing the platform rather than the intentions of the legislator.

> The architectural implementation on online platforms ultimately depends on the specific choices of the platform designers, seeking to promote or prevent a certain type of actions.[15]

The information revolution has changed the way States carry out their information policies. It requires the legislator to, at least, be aware of the technological circumstances before they adopt new laws since this form of 'regulation by code' is currently employed to regulate various relationships on the Internet. Since interactions

[11] Brownsword (2015), pp. 42–45.

[12] Brownsword and Goodwin (2012), p. 12.

[13] Yeung (2019a).

[14] Reidenberg (1997), p. 553.

[15] Hassan and De Filippi (2017), p. 89.

between the code and architecture of technology must be considered in the policy-making process, it is essential that such interactions are understood to make regulations that have the intended effect.[16]

In the context of technology 'politics', it has been hypothesized that design choices in technology contribute to the broader framework of public order.[17] This hypothesis has turned out to be right in many respects, as software is used for public and private regulation, expressing the normative objectives of the 'figure'. With technological developments, many aspects of our online and offline lives are being determined by the normative choices embedded in code, which is a regulatory tool that articulates the objectives and preferences of the 'figure'. More often than not, however, this 'figure' is a private actor. Further, digital platforms are increasingly taking on regulatory and policing roles, traditionally viewed as matters of public law.[18] The functions of digital platforms include the use of injunctions against third parties, as in the case of *L'Oréal vs. e-Bay,* compelling private actors to implement the GDPR and policing online hate speech, a matter delegated to platforms by the European Commission.[19] The Commission's encouragement that platforms assume such functions is instructive, as public authorities have increasingly delegated enforcement tasks to private entities, while the latter is also self-appropriating such functions. This has turned online platform intermediaries into 'private cyber-regulators and cyber-police'.[20]

Private sovereignty, exercised through coded terms of service, is replacing public sovereignty expressed through law. Digital platforms have started to replace state power by 'adjudicating' speech rights according to their own community guidelines instead of the law.[21] To illustrate, code regulates the humans who are using digital platforms. Uber uses code to control its drivers. Its internal code of conduct is enforced through code, as non-observance thereof results in the automated delisting of the driver or rider.[22] The transportation platform, moreover, uses behavioral science to manipulate drivers through code-based psychological inducements.[23]

Code has thus doubtlessly become an important source of private regulation, an evolution that is not without problems. When code assumes this function, the principal source of rulemaking is the 'figure', that is, the technology developer.[24] Private regulation is not exposed to the same checks and balances of law-making as public authorities are. The code that so often regulates us lacks transparency and escapes

[16] Lessig (2003), p. 2.

[17] Winner (2010).

[18] Belli et al. (2017), p. 41.

[19] European Court of Justice, Loreal SA and Others v eBay International AG and Others (2011), C-324/09.

[20] Eecke and Truyens (2011), p. 129.

[21] Keller (2017).

[22] Legal | Uber (2024). https://www.uber.com/legal/en/.

[23] Scheiber (2022).

[24] Reidenberg (1997), pp. 552, 571.

scrutiny, even more so when it benefits from trade secret protection. This has led to algorithms and code being referred to as black boxes.[25] It is important to remember, however, that when code acts as law, it is not acting in total isolation. Online policies programmed by code, rather, are 'both shaped by and reshape existing laws, regulations, and social mores'.[26] In recent years, though, increasing criticism has been voiced that the law has not been able to stop the development of 'platform power' and the breach of fundamental human rights through code.[27] Standard content guidelines may not respect the principle of legality, as online codes of conduct prohibit content that is lawful under EU law.[28] While there are convincing arguments as to why entities such as platforms should be able to leverage the regulatory power of code, we must rethink the involvement of public authorities and the broader community in these processes to safeguard legitimacy. Indeed, important concerns arise when code is used as law in the absence of procedures that safeguard ideas of democracy, legitimacy, transparency, and accountability.

Public authorities progressively rely on code in their rulemaking and enforcement responsibilities. Predictive technologies are increasingly informing the State about legislative functions, and influencing its decisions that aim to shape both individual and collective behavior, while the automated law enforcement is also on the horizon. This code-ification of law has been portrayed as the source of a 'new system of social ordering known as algorithmic regulation'.[29] Yeung has defined algorithm regulation as

> decision-making systems that regulate a domain of activity in order to manage risk or alter behavior through the continual computational generation of knowledge by systematically collecting data, in real-time on a continuous basis, emitted directly from numerous dynamic components pertaining to the regulated environment in order to identify and, if necessary, automatically refine or prompt refinement of, the system's operations to attain a prespecified goal.[30]

By exerting public regulatory influence, compliance of the technical rule of code with the law can be ensured. Code has an extraordinary capacity to secure compliance as software enforces its own rules. For example, it has been used to assess people's eligibility for welfare benefits and public aid, to identify parents who might be required to provide child support, to determine who is allowed to board a flight, or, generally, to quantify security risks.[31] Several States in the United States also rely on codes to calculate whether low-income citizens qualify for the Supplemental Nutrition Assistance Program and to calculate their entitlement to food stamps.[32]

---

[25] Pasquale (2015).

[26] Brown and Marsden (2013), section xii.

[27] Cohen (2016), p. 369.

[28] McNamee and Pérez (2017), p. 99.

[29] Yeung (2018), p. 505.

[30] Yeung (2018), p. 505.

[31] Citron (2007), p. 1252. Pasquale and Cashwell (2015), p. 37.

[32] Wiseman (2019), p. 93.

By translating law into technical rules, legal provisions are automatically enforced by the underlying technological framework. Instead of hunting down wrongdoers after a legal infraction, code-based systems can ensure greater compliance with the law by preventing violations before they occur. Delegating the task of applying these rules into a technical system lessens the risk of anyone failing to implement such rules—whether inadvertently or willingly—ultimately decreasing the need for oversight and ongoing enforcement. In acting as a form of public regulatory tool, code can be used to increase State control. It would indeed be a mistake to believe that technological change is necessarily the source of deregulation, as cheaper sensors and cameras enable more surveillance, and connected devices will 'render ever more aspects of daily experience as pressure points for regulatory intervention'.[33] Such tools have the ability to enable a regulatory regime that identifies and addresses risk in real-time while promoting more efficient compliance.[34]

These assertions resonate well in the context of blockchain, where the technology has been enthusiastically embraced as an 'important tool for protecting and preserving humanity' and is said to be at the same level as the internet in terms of importance.[35] With blockchain usage increasing at an exponential rate, DAOs may replace the State by enforcing their own rules for governance which they perceive to be fair. These DAOs can be established and enforced through a set of algorithmic rules (codes) and are not bound by geographical markers. This may lead to the formation of a self-governing State aided by the development of techno-democratic systems.

Blockchain also has the potential to enhance public control over individuals. For instance, the simple process of appointing the board of directors in a company presently relies on traditional methods such as paper mailing or insecure electronic proxy services. In this process, shareholders encounter numerous obstacles when attempting to propose corporate changes or reforms. There exists an opportunity to streamline this entire system, making it more efficient and responsive by utilizing blockchain technology where the votes could be instantly recorded, simplifying the process of electing the directors significantly. Physical annual meetings could be replaced by virtual gatherings streamed online, eliminating the need for in-person attendance. Through remote participation and the secure storage capabilities of blockchain, votes could be securely submitted and tallied in real-time, ensuring trust and transparency.

Unlike other technologies, blockchain is not merely a neutral tool but is crafted with specific features that enable alegality. These features include decentralization, immutability, and cryptographic verification, which collectively create a system that operates outside the traditional bounds of the legal domain. In contrast to centralized systems where legal authority is vested in a central entity, blockchain's decentralized architecture challenges the spatial boundaries of legal orders by existing

[33] Pasquale and Cashwell (2015), p. 36.

[34] Arner et al. (2017), p. 371. Finck (2018a), p. 665.

[35] Makridakis and Christodoulou (2019), p. 258.

across multiple jurisdictions simultaneously, raising questions about jurisdictional authority and enforcement. Since data stored on the blockchain cannot be easily altered or deleted, its immutability attribute questions the temporal boundaries of legality by challenging the conventional understanding of retroactive legal application. Materially, blockchain's decentralized nature challenges traditional configurations of rights and obligations, potentially reshaping the landscape of legal interactions. Subjectively, blockchain's anonymity and pseudonymity blur the distinction between legally protected and sanctioned acts, complicating the attribution of responsibility within legal frameworks. This notion of technological systems introduces alegal challenges, highlighting the inherent strangeness or 'inhumanity' of such technologies, where the decentralized and immutable nature of blockchain disrupts traditional conceptions of legality, presenting novel challenges to legal orders worldwide. As a powerful normative tool for the people who operate it, blockchain can be used as an instrument of public and private ordering, where the dynamics between them are often fluid.

4.3 Intersection Between the Rule of Code and the Rule of Law

In order to scrutinize the extent to which 'governance by blockchain'[36] may circumvent the spread of traditional law, the intersection and interactions between two distinct governance modes need to be cross-examined (which have been the point of discussion since the start of this chapter) covering the 'rule of law' that is the conventional law, and the 'rule of code' which broadly covers the internal rules of blockchain systems in the form of executable software code and technical protocols. This conceptual analysis will provide us with a representative picture of the different kinds of interactions, including those anticipated in the future, between 'the code of law' and 'the code is law' as technology develops and matures.

Within cyberspace, 'code is law', in so far as the software code and technical infrastructure of the internet checks, controls, and enables human behavior and interactions that take place online.[37] There are remarkable parallels between the resistance to regulation adversity by parts of the blockchain community and initial conceptions of internet regulation. In the early 1990s, it was envisaged that internet users would create distributed socio-technological systems that self-regulate like biological systems,[38] that users would themselves define the rules that apply to

[36] De Filippi and Loveluck (2016).

[37] Lessig (1999). Lessig (2006).

[38] Kelly (1994).

them,[39] and that a 'New Magna Carta for the Knowledge Age', repealing existing legal systems, was needed.[40]

In the context of blockchain-based systems, it's crucial to distinguish between the rule of law and the rule of code, the latter being defined and enforced by technology. While governments wield enormous authority within their borders, exerting control over a blockchain-based system poses challenges. This is primarily due to the unique attributes of public blockchain networks—such as their distributed and decentralized nature, inherent pseudonymity (or anonymity in cases like Zcash or Monero),[41] and their (purported) immutability and incorruptibility, which makes enforcing national laws on these systems complex, though feasible. Blockchain-based systems operate under an alternative framework of code-based rules and procedures, that is, the *lex cryptographica*, dictated by the underlying blockchain protocol, where the power of *lex cryptographica* is intuitively appreciable. When specific conditions that could be represented computationally within the technological artifact are fulfilled, the code auto-executes as per the preset logic, without going into its logic. The outcomes of such auto-execution are enforced without any consideration of external factors or their relevancy for reflections of the real-world. Yet, once the codes are scripted (similar to traditional framing of legal rules), and executed, storing both the self-executing codes and their outcomes in the blockchain means both the logic and the product thereof are immutable.

The smart contracts enable this feature of '*ex-ante* enforcement of technical rules, thereby reinforcing the opportunities of regulation by code and the corresponding legal implications it might entail'.[42] In an 'order' regulated by self-executing smart contracts and similar technical arrangements, the necessity for judicial enforcement diminishes because the fashion in which the rules have been defined—the code—is the same 'formula' by which they are executed. Thus, in a legal philosophical as well as practical sense, the rule of code tends to become 'law' substantially through combining the formation and enforcement of the contract into a single instrument.

> The only way for people to infringe the law is to effectively break the code, and this raises the question over what is legally versus technically binding.[43]

While it is theoretically possible to implement basic contractual safeguards and consumer protection provisions in smart contracts, doing so in practice may prove challenging due to the formalized and deterministic nature of the code.

Regardless of the obscurity or subjective appreciation of human minds, when a smart contract is executed, the correlation between the form and substance of the outcome indicates its material effects to be governed only by the precepts and prescriptions of pure code. Being characterized by 'turing-completeness, value

[39] Rheingold (1993).

[40] Dyson (1996), p. 256.

[41] Lee (2019), p. 20.

[42] Hassan and De Filippi (2017), p. 89.

[43] Wright and De Filippi (2015), p. 26.

awareness, blockchain-awareness, and state',[44] smart contracts possess the competence to define complex conditions written in a computer code, display non-arbitrary behaviors when certain conditions are satisfied; it can also sustain and supervise the enforcement of preset rules over time, and register the results in the immutable blockchain. This feature of *lex cryptographica* can even be drawn from the definition of blockchain provided by Buterin, the inventor of Ethereum:

> a magical computer that anyone can upload programs to and leave the programs to self-execute, where the current and all previous states of every program are always publicly visible, and which carries a very strong crypto economically secured guarantee that programs running on the chain will continue to execute in exactly the way that the blockchain protocol specifies.[45]

Through *lex cryptographica*, the mainstream deployment and adoption of blockchains require a change in our perception of the law's role in society. Blockchains are perceived to offer an opportunity to 'construct a new legal structure which will give rise to new substantive legal issues and cause shifts in legal culture and legal structures'.[46] In the world of *lex cryptographica*, the law is created through regulative or legislative measures and then effected through cryptographic smart-contracting computer code, leveraging the ability of code to achieve compliance. *Lex cryptographica* also offers the benefits of flexibility and rapid adaptability so that the 'method and locus of creating crypto-legal structures' can be quickly adapted to the policy problem.[47] Through the combination of flexible adaptation and guaranteed execution, *lex cryptographica* is anticipated to fundamentally disrupt national legal systems and alter how we explore, reflect, and converse about the law.

A deep dive into the dynamics between the *lex cryptographica* and law and its reciprocal effect reveals that the application potential of blockchain has increased with the development of 'upgraded' blockchain codes. As such, blockchain technologies make it possible to incorporate instructions into the code, thereby permitting any person to enter into (contractual) relations with other persons or machines, where the contractual agreements and clauses are embedded into the rule of code. This leads to the recognition of blockchain technology as an authentic *regulatory technology*[48] in the sense that it orients and modifies the behavior of the individuals who use it. Therefore, this technology could be increasingly employed to monitor and regulate individual's behavior and conduct, ensuring their consistent compliance with legal requirements or with the contractual obligations that they have agreed upon.

> The blockchain could be used, for instance, to manage identity, making it easier to monitor, surveil, or simply keep track of various online activities. Every transfer, vote, and purchase

[44] Buterin (2014), p. 37.

[45] Ethereum Foundation Blog (2015). https://blog.ethereum.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology.

[46] Reyes (2017), p. 387.

[47] Reyes (2017), p. 400, 414.

[48] Wiener (2004), p. 483.

> can be recorded on the blockchain, creating a permanent record that will potentially push the boundaries of privacy law.[49]

With code performing as a means of delivering regulation that might diverge from State-sanctioned law, the interconnection between code and law is expected to increase in the future. It is worth stressing that regulators are also beginning to think along the same lines. The Australian Standards Organization, which is spearheading the blockchain work of the International Standards Organization, has proposed cultivating a regulatory framework that combines both legal and technical rules.[50] In fact, it may be possible to speed up information sharing between market participants and regulators by using blockchain. Blockchain technology, which enables instant global transactions, can also register customer records and digital signatures to reduce tax evasion, and, thereby, enhance digital security and identify potentially suspicious transactions in nearly real-time.[51]

4.3.1 Normative Influence

In the *crypto space*, the relationship between code and the law has a factual, legal, and political dimension.[52] Practically, however, it is difficult for the law, due to the absence of a regulatory intervention interface, to directly alter the code of a smart contract, stop its execution, or reverse its effects if they were contrary to the law. This inflexibility not only impedes 'legal overruling'[53] but also causes significant costs to the parties or the users of the blockchain application for filling gaps in incomplete smart contracts. In some smart contracts, it may be difficult for parties to enforce their legal rights if their counterparty is unknown, due to pseudonymity, or based in a country with a weak judicial system. To understand this issue, Hacker et al. provide an example where a person in the European Union buys a mobile phone directly from an Asian merchant by means of a smart contract. The payment is executed after GPS-verified delivery, but if the phone is not in conformity with the contract, then the buyer may—depending on the applicable legal regime—have remedies against the merchant. However, if the buyer fails to undertake due diligence before contract formation by seeking unambiguous identifying information, it may be difficult, in practice, to recover the payment or to enforce remedies. To this extent, code, which is specified *ex-ante*, may trump the law that only offers remedies *ex-post*. This merely shifts contractual risk between parties and does not affect the general relationship between the code and the law. It is worth noting,

[49] Wright and De Filippi (2015), p. 53. See Hassan and De Filippi (2017), pp. 89–90.

[50] Delimatsis (2019).

[51] IMF Blog (2018). https://www.imf.org/en/Blogs/Articles/2018/03/13/addressing-the-dark-side-of-the-crypto-world.

[52] Hacker et al. (2019), p. 13.

[53] Rodrigues (2019), p. 679.

however, that such risk, as well as the need to import off-chain data, for example, GPS localization or information on the contractual confirmation, which depends on the behavior of the users, does infuse a necessary and significant element of 'trust' into blockchain transaction, initially thought to dispense of it, since blockchain promises to operate in a trustless manner.

It may be asked to what extent users of a blockchain-based application may opt out of the legal system or at least out of specific legal protections. While different legal regimes offer different degrees of legal protection to which blockchain users can contract around substantive legal provisions, a more subtle but potentially even more far-reaching question arises with respect to the interpretation of blockchain-based legal arrangements.[54] This notion of a 'far-reaching' question aligns with what Brownsword asked:

> can the parties opt out of the traditional way of interpreting contracts, and more specifically, for example, restrict interpretation to the equivalent of a literal approach to the meaning of the code, devoid of a good faith-based or purposive mode of interpretation?[55]

These are some crucial 'food for thought' issues, especially whenever the specific features of a smart contract are unilaterally exploited by one party or an attacker in ways that may violate the spirit but not the actual code of the application.

On the political level, this reflects the divergence between views, stressing the 'self-sufficiency and autonomy of the blockchain space' as declared by Arvicco in Crypto-decentralist Manifesto[56] and approaches situating blockchain as set out by Eich,[57] Ortolani,[58] and Lianos[59] within the bounds of the broad realm of socio-technological instruments that necessarily communicate with, and are nested inside, the broader political and legal context and claims just as any other technology. These different normative predispositions and conflicts can also be found in the variety of approaches inherent in the contributions that range from a focus on private ordering[60] to reclaiming the political dimensions of blockchain and money[61] and even to the discussion of potential fundamental rights violations by smart contract enforcement.[62]

Code, especially when tamper-proof, may thus come to trump over other sources of normative influence that guide human behavior. The two elements of blockchain that stand out when assessing its potentially transformative impact on law are (1) the self-executing nature of the rule of code and (2) the possibility of customizing law. Seen from this perspective, blockchain enabled smart contracts are new regulatory

---

[54] Grundmann and Hacker (2017), p. 280.

[55] Brownsword (2019), p. 311.

[56] Arvicco (2016). http://etherplan.com/A-Crypto-Decentralist-Manifesto-en.pdf.

[57] Eich (2019), p. 85.

[58] Ortolani (2019), p. 289.

[59] Lianos (2019), pp. 329–410.

[60] Rohr and Wright (2019), p. 43.

[61] Dimitropoulos (2019), p. 112.

[62] Ortolani (2019), p. 289.

agents. In traditional contractual agreements, parties bear the risk of the counterparty not adhering to the agreement, and the law provides remedies when this is the case. In contrast, smart contracts remove such risks by ensuring that the agreement is self-executing. For example, when a red light at a signal is violated or a car is wrongly parked, smart contracts can automatically levy fines.

When distributed ledgers are used as a means of public regulation, constraining regulatory and governance mechanisms are needed, as otherwise, these systems can easily become mechanisms of control. By regulating code, blockchain may become a tool of freedom as well as of oppression. States could use the technology to expand their own power, as the 'universal visibility of transaction on a distributed ledger is an authoritarian regime's dream'.[63] It is feared that distributed ledgers may ultimately be used for personal surveillance of individuals to act 'as a powerful deterrent for those who might be tempted to commit violent interferences with the personal security and bodily integrity of others'.[64]

4.3.2 Impact of Technology on Legal Norms

As we increasingly rely on technology to enforce legal norms, there's a risk of law progressively assuming the characteristics of code, with rules becoming more rigid to fit the technology that is meant to enforce them. The emergence of blockchain technology has accentuated this risk, particularly in contract law. Over time, contractual terms have been directly embedded into code, as seen in traditional DRM systems, simplifying enforcement. As technology evolves as a preferred means to enforce contracts, the reliance on traditional legal contracts may diminish. Moreover, with smart contracts, code can be used not only for the purpose of enforcing existing legal provisions but also to define them in the first place.

Unlike other technological innovations, such as DRM systems, which impact legal enforcement by rendering the relevant rules self-executing, the blockchain affects the creation of the law that stems from the contract more effectively since it has a propensity to rely on the rule of code, to control individual behavior and transactions.[65] Blockchain, coupled with smart contracts, introduces a novel form of regulation by code, reshaping our understanding of the law.

Blockchains' core value proposition of automated execution can be used as a mechanism of private or public regulation. When it is relied upon, it forces us to reflect on the assumptions enshrined in contemporary legal orders. In addition to triggering efficiency gains, blockchain applications may cause changes to the nature of law. As more legal rules and contractual terms are encoded into smart contracts, the conventional notion of law, as a flexible and inherently ambiguous set of rules,

[63] Werbach (2018), p. 14.

[64] Yeung (2017), p. 3.

[65] Dimitropoulos (2020), p. 1117.

may need to adapt for better alignment with code. The law is not automatically self-enforcing; rather, it sets out behavioral specifications that parties are incentivized to comply with but have the freedom to disregard and assume consequences, which are, in turn, administered by the legal system.[66] When code is used, compliance is the only option, with the exception of those who are able to circumvent code. There is a need to adapt the law, its ambiguity and flexibility, into a newer law that is more compatible with code,[67] as the rule of code embedded in the blockchain is used to express legal obligations, such as in terms of smart contract rules. This would change legislative drafting, as language that can be translated into code has to be used, and conversely, also change the process of legislative negotiation, which can include the intentional use of unclear language.

Law is impersonal, as it is not tailored to an individual's specific preferences. However, due to technological innovations, more personalized rules are on the horizon. Digital footprints can be combined with machine-learning algorithms to offer personalized advertising and personalized pricing.[68] As a result, 'we should expect to see a significant increase in personalization as greater information becomes available about the informed choices of diverse people'.[69]

One anticipated effect of blockchains' *lex cryptographica* is that smart contracts could simplify the process for individuals to establish personalized legal systems. This would allow them to choose and enforce their own regulations within a technologically driven legal framework. The customization of applicable norms at the individual level would enable individuals to ascertain the rules applicable to them in accordance with their corresponding preferences and to switch between rule sets contingent upon circumstances and time. The generally established view is that the rule of code is 'distinct from legal regulation because its mechanism may implement customizations with minimal effort'.[70] This means that anyone can be a regulator and can engage in 'forum shopping',[71] possibly weakening the territorial sovereignty of the State and the rule of law.

By programming the rule of code and placing trust in it, the parties to the smart contract are, in fact, making a private law, therefore removing the need for recognition or legitimization by conventional law, which is an artificial culturally established symbolic referent. It associatively implies that coding, as in smart contracts, is fundamental for auto execution and responsible for the legal basis, the law, and its enforcement. As the symbolic referents are replaced with code, a profound displacement of the traditional imagery and symbolic basis of law takes place. 'New codified relationships that are defined and automatically enforced by code but are not linked to any underlying contractual rights or obligations' are introduced into smart

[66] De Filippi and Hassan (2016). https://firstmonday.org/ojs/index.php/fm/article/view/7113/5657.

[67] Finck (2018a), p. 665.

[68] Calo (2014), pp. 1016–1018.

[69] Sunstein (2013), p. 23.

[70] Reidenberg (1997), p. 569, 580.

[71] Wright (2016), p. 13.

contracts.[72] By enabling self-executing transactions, a blockchain allows parties to transact freely, eliminating the need for standard contractual agreements. Regardless of the technical need,

> there may be a legal need to memorialize a smart contract in writing in order to make such arrangements enforceable in a traditional court or other judicial tribunal.[73]

When governments resort to personalized law, blockchain provides the ideal database for them to store related data in light of its tamper resistance and resilience, achieved through replication. In the context of personalized law, distributed ledgers

> can be leveraged to create a decentralized, pseudonymous and dynamic government database which stores the relevant parameters for personalized law, such as the degrees of bounded rationality or specific personality traits of different persons.[74]

In addition to efficient law enforcement through smart contracts, blockchains can be used to manage individual parameters such as individualized rights and obligations, not just in contractual settings but also by the State.

When code is used to personalize law, procedures must ensure that fundamental constitutional principles or the rule of law is upheld. The ability of code to personalize law is not limited to smart contracts but constitutes a broader phenomenon. Cynics might say that these evolutions are nothing new, as, in ordinary legislative processes as well, legislation can be sold for campaign donations, votes, unspoken commitments, and occasionally direct bribes. Seen from this perspective, smart contracts simply lower entry costs to an already existing phenomenon. Yet just because the real world doesn't always live up to its ideals, it doesn't mean that these ideals, including the rule of law, should be abandoned outright. While legislative processes, including the European Union's ordinary legislative procedure, are far from perfect, they nonetheless postulate important guiding principles.[75]

Conventional legal systems, thus, have a justifiable responsibility to defend and protect certain core interests, particularly the rule of law and the safety and security of its citizens, which extends well beyond the provisions of transactional security that are endangered by blockchain applications. The magnitude of the potential threats by blockchain being faced by these core interests seems too contingent upon at least two variables. The first and foremost variable is the purpose and intention of participants of the blockchain network about conventional law in pursuing to engage in various blockchain network activities. The second variable is about the nature, scope, and magnitude of potential harm resulting from specific blockchain applications applicable to both users or network participants and to third parties.[76] Where code assumes the function of law, that is the phenomenon of 'code is law', it must be bridged with legal systems and their overarching ideals.

---

[72] Wright and De Filippi (2015), p. 11.

[73] Wright and De Filippi (2015), p. 11, see footnote 50.

[74] Hacker (2017).

[75] Deirdre and Päivi (2017), p. 1673.

[76] Yeung (2019), p. 207.

4.4 Classification of Blockchain Applications

Different blockchain applications can be broadly classified under different groups, based primarily on the purposes and intentions of blockchain participants in relation to the conventional legal system and the potential harms that these might generate—blockchain as law avoidance, blockchain as supplementary to law, and blockchain as alleviating transaction frictions.

4.4.1 Blockchain Code as Law Avoidance

Due to the decentralized, distributed nature of the computational network dispersed around the globe, it is believed that effective sovereign State control of public blockchains is not feasible. However, though the technology itself is decentralized at macro level, it is largely centralized and controlled at the software governance level or micro level. The blockchain development and evolution processes are being decided (and effectively controlled) by limited developers having the requisite knowledge, skill, and expertise.

As such, certain regulatory interventions must be made possible by focusing on the macro level and micro level, respectively, which can identify the key intermediaries and the 'figure' responsible for programming the rule of code embedded in the blockchain since the blockchain operates within an ecosystem of a broad range of applications, exchanges, and practices in which the technology interfaces with the real world.

If it is observed that blockchain networks are being used deliberately to circumvent the significant legal obligations that are meant to protect individuals and the public interest, it is quite likely that sovereign enforcement agencies will not be mere spectators if such avoidance actions are considered non-trivial in size and scale and would seek to protect the public and the State through appropriate interventions. This, expectedly, can lead to an active *battle of supremacy* wherein the 'code of law' endeavors to exercise its sovereign power over 'code is law' to stop misuse of the anonymity feature of public blockchains. However, this battle will not be a 'once-for-all fight for survival'[77] with a single winner, but in all, it probably will be akin to a series of ongoing interactions in which State regulators and authorities pursue to dodge the loopholes of blockchain, which are used to exploit to stonewall the substantive demands of the law. Although State regulatory and enforcement bodies would prefer to nail the primary culprits, that is, those individuals and groups who actively pursue to avoid substantive legal obligations by engaging in blockchain-based activity, authorities find it more effective and convenient to go after those who act as intermediaries between blockchain networks and the real-world.[78] However,

[77] De Filippi and Loveluck (2016), p. 15.

[78] Brownsword et al. (2017), p. 3.

as the role of intermediaries gets diluted with time and more services are placed on unpermissioned blockchains, sovereign authorities might pursue to enforce legal responsibilities on the 'figure' who are the code developers and miners directly, albeit the success of imposing responsibilities on the 'figure' is not yet known.

Regulatory constraints, in most cases, decide the choices of the 'figure'. In order to make software projects compliant with the regulatory environment, the design of code ought to be shaped by the law. To illustrate, legal frameworks have outlawed the reverse engineering of encryption in DRM to enforce copyright law.[79] The European Union's Directive on Copyrights and Related Rights in the Information Society has prohibited the import, sale, rental, and possession of all tools that can be exploited to bypass encryption systems.[80] Another example of how law influences network architecture can be found in the GDPR, which is essentially a code-constraining scheme that subjects the modalities of personal data processing to plentiful qualifications.

Court decisions can also have a similar effect. How the law affects software is famously illustrated in the Microsoft Corporation vs. the US Court of Justice.[81] The European Commission had accused Microsoft of having abused its dominant position in the market for the supply of client PC operating systems.[82] The European Court of Justice held that Microsoft had weakened competition by refusing to supply competitors with the option of interoperability and by bundling the Windows Media Player with Windows PC. It not only fined Microsoft almost €500 million but also ordered it to offer a newer version of the operating system only without its media player.[83] Future versions of Microsoft's software code were thus shaped by the judicial decision.

The fate of Napster demonstrates that law not only forms the design of code but also can bring its demise. Although the company encountered legal challenges regarding copyright infringement and was swiftly compelled to cease its operations, it was able to function as a method of law avoidance for some time. To evade similar legal consequences, decentralized peer-to-peer file-sharing protocols like BitTorrent were subsequently developed to eliminate the vulnerability of a central point of control, which could be legally prosecuted.[84] Notably, despite legal efforts, BitTorrent has remained operational, highlighting how software code can effectively circumvent law-originated rules and constraints.

Sometimes, code is intended to evade regulatory compliances so as to minimize legal costs. Code is a powerful tool to avoid regulations that are coupled with social

[79] Articles 11 and 12, WIPO Copyright Treaty 1996.

[80] Articles 6(2), WIPO Copyright Treaty 1996.

[81] Judgment of the Court of First Instance (Grand Chamber) of 17 September 2007, Microsoft Corp. v Commission of the European Communities.

[82] Article 102, Consolidated version of the Treaty on the Functioning of the European Union 1957 (OJ C).

[83] Judgment of the Court of First Instance (Grand Chamber) of 17 September 2007, Microsoft Corp. v Commission of the European Communities.

[84] Pouwelse et al. (2005). Wu (2003), p. 103, 105.

norms, which has, for example, allowed for the large-scale avoidance of obscenity laws with respect to online pornography. While many jurisdictions have noted obscenity laws that could be applied to online pornography, they are usually not enforced. Since such materials are widely available, which has become possible through code, States have the choice to

> either invest large sums to attempt to enforce the law in the digital environment, or they could de facto deregulate adult obscenity and focus their attentions on more pressing problems such as child-abuse images.[85]

Most provinces, however, have chosen the second option in light of changed social norms regarding sexuality.

What remains questionable is whether code is a realistic law avoidance mechanism at scale, considering that most citizens are not motivated to evade the law but, rather, prefer the defaults of legality and convenience. Only a minority of users rely on this option, while most adhere to the legal default.[86] States may indeed tolerate law avoidance only because it does not scale to cause systematic problems. While code doubtlessly can be used as a law avoidance technique, probably also at scale, it has, however, never disrupted regulatory systems. The question to ask, then, is whether this will be different with regard to blockchains. Whereas the technology's constitutive features can be operated to facilitate law evasion, it is not clear that most citizens would want to rely on systems outside the default of legality. As a matter of fact, while the rule of code embedded in the blockchain can be used as a means of law avoidance, it can certainly be used as a more efficient means of law enforcement.

If blockchain technologies are utilized by participants deliberately to evade the reach of substantive legal duties and obligations, the rule of law and sovereignty of law are directly threatened. In that case, we can expect national law enforcement agencies to assert their legal powers to stop and prevent the deliberate use of blockchain systems to avoid the reach of obligations imposed by conventional laws. If national legal authorities do not take appropriate action against flagrant attempts to evade the extent of the law, which may include criminal activity, not only the potential victims of crime are exposed to grave injury, but also the reputation of the regulator is dented, and confidence in the integrity of the national legal system is diluted.[87] In other words, if there is intentional use of blockchain networks, particularly by those dealing in cryptocurrencies, to evade the principal obligations imposed by tax authorities and financial market regulators, national legal systems can be invoked to enforce legal action against them. This can be illustrated by the case of the Ad listing site Backpage, which allowed its users to pay in Bitcoins, that lists everything, even ads relating to human trafficking, where the US enforcement

[85] Finck (2018b), p. 37. See Murray (2013).

[86] Sunstein (2013), p. 5, 6, 10.

[87] EBA/Op/2014/08(2014).https://www.eba.europa.eu/sites/default/files/2025-01/51768d88-053d-4ac2-9f99-e1ff89bf5315/EBA%20Opinion%20on%20%20virtual%20currency%20entities%20%28EBA-Op-2016-14%29.pdf.

authorities took stringent steps to stop the services of such a website and curb the crime.

Among many challenges that conventional systems are grappling with, one significant issue is about permitting the use of blockchain systems for lawful functions whilst seeking to clamp down on blockchain activities that are engaged in for the express purpose of avoiding substantive legal obligations that would otherwise apply. For example, the concept of Bitcoin was originally devised by Nakamoto as an alternative to conventional legal currencies issued by sovereign States that would facilitate payments so as to bypass the States.[88] Of course, instituting such an alternative system of payment is akin to a barter system within local communities and does not threaten the rule of law. However, with an increasing degree of anonymity associated with Bitcoin compared to that of conventional currencies, it has become a widespread tool to engage in illegal activities. Regardless, in exceptional cases, we can see that when bitcoins are used as the preferred mode of payment for the traffickers to make payment for online classified ads, such groups of ads can be linked to the common author on Backpage by analyzing the Bitcoin information available in the public domain.[89] By comparing the timestamp of making a payment with the appearance of the ads on the Backpage, the payment of ads with a common author can be traced to the unique wallet maintained by the Bitcoin user. This tool enables law enforcement agencies to establish a linkage among ads by scrutinizing payment methods and the semantics of the ads and to find answers about human traffickers and their *modus operandi*. Indeed, the architectural design of blockchain offers a potential solution to identify the people involved in human trafficking.[90]

There have been circumstances where blockchain technology has been intentionally used to evade substantive legal requirements, particularly to avoid tax liability or other regulatory obligations,[91] such as those aimed at identifying and reducing the risk of money laundering.[92] The national legal authorities have selectively wielded their sovereign authority over those activities as well as the participants when particular sites of criminal activity have developed, thereby threatening to undermine the sovereignty of conventional law. Since the blockchain network is 'distributed in nature' and is characterized by the absence of a single legal entity, conventional legal authorities have focused their enforcement activity at specific public interfaces within the larger digital canvas in which the technology has been used for illegal activities, in order to clamp down the use of the blockchain to

[88] Guadamuz and Marsden (2015). https://firstmonday.org/ojs/index.php/fm/article/view/6198/5163.

[89] Follow the Bitcoin to Find Victims of Human Trafficking (NYU Tandon School of Engineering Press Release, 16 August 2017). https://engineering.nyu.edu/news/follow-bitcoin-find-victims-human-trafficking.

[90] Israel (2017) In a Step toward Fighting Human Trafficking, Sex Ads Are Linked to Bitcoin Data. Berkeley News. https://news.berkeley.edu/2017/08/16/in-a-step-toward-fighting-human-trafficking-sex-ads-are-linked-to-bitcoin-data/.

[91] Mazur (2022), p. 115.

[92] Akinrotimi (2020), p. 217.

circumvent substantial legal obligations. For example, an online blockchain-powered marketplace, 'Silk Road', over which various illegal merchandise could be sold and purchased by using Bitcoin as a mode of payment, was shut down by the regulators instead of restricting the use of Bitcoin.[93] The enforcement agencies have also not paid close attention to identifying the individuals who are using cryptocurrencies deliberately to circumvent the substantive obligations arising under conventional law and take action against them. It seems authorities are following a more preventative and defensive strategy. Instead of focusing on apprehending and punishing the primary offenders, the authorities, it appears, are more concerned with blocking the possible use of cryptocurrencies for avoiding legal duties.

4.4.2 Blockchain Code as Complementary to the Law

Since blockchain is a general utilitarian-based technology, the programs based on this technology can be configured to operate in partnership with conventional legal systems, including attempts to harness the power of blockchain systems as a vehicle for securing compliance with substantive legal norms.

For instance, by transposing law into a smart contract and requiring that parties either interact with these smart contracts or incorporate them directly into their information systems, States can automate the enforcement of specific rules or regulations without the need to affirmatively monitor each and every transaction. Laws implemented using blockchain technology provide certain advantages over traditional code in terms of both autonomy and transparency because smart contract is executed by the underlying blockchain-based network. It cannot be unilaterally manipulated by any single party; transposing legal rules into smart contract code—rather than on a piece of software running on a centralized server—means that no centralized operator can modify these rules or prevent their execution. A blockchain-based platform thus comes with the additional guarantee that the rules it incorporates have been followed by all parties interacting with the said platform.

Code can be used as a substitute for law when technology is better suited to resolve policy issues.[94] It can assist in achieving regulatory objectives efficiently while implementing the law. For example, geolocation technology has enabled courts to impose penalties on activities related to citizens in their jurisdiction, while DRM helps to enforce copyright law in cyberspace.

We can see that technology provides potent tools for the enforcement of policies and decisions. Technology is now being employed to enhance regulatory processes to ease regulatory monitoring, reporting and compliance in replacing manual by digital processes. This illustrates the functionality of the technological artifact to enforce regulation more easily, and thus, it may facilitate a more detailed regulation,

[93] Van Hout and Bingham (2014), p. 183.

[94] Reidenberg (1997), pp. 552, 583.

with compliance being monitored through code. Thus, it is essential to understand the 'efficient alignment' between blockchain technology and law, which takes place in three ways, namely, supplement, complement, or substitute.

In the case of a functional trust architecture, a blockchain can function as an additional layer, provided the law permits the same. The chief value proposition of having a blockchain in a supplementary role is the gain in speed and efficiency of sharing a data record. In this role, the blockchain substitutes the error-prone messaging structures between participants without disturbing the general industry structure. To illustrate, the United States has a well-developed legal system for dealing with real estate transactions.[95] The presence of strong norms and formal rules has created a formidable environment of trust. However, there are significant inefficiencies in the system. Title insurance, a tool used to protect buyers against defects in land titles, is largely based on paper records and must be traded among multiple parties.[96] While the trust burden involved in the transaction is taken care of by the existing legal obligations and overarching business regulatory framework, introducing blockchain could, with a superior record-keeping mechanism, improve efficiency and mitigate risk. Moreover, by using smart contracts, States could ensure compliance with regulatory requirements embodied in these code-based systems. This makes it possible to achieve a new form of technical accountability—one that is dictated by technology, and that is less dependent on traditional *ex-post* enforcement.

Any rule implemented via a smart contract or incorporated in a blockchain-based protocol can be documented on a cryptographically secure and distributed data system, providing an auditable trail of activities performed from or tied to a particular account or smart contract. Therefore, in a blockchain ledger, the trust in the integrity of the data remains intact and the trust relationships between buyer and seller are unchanged. From a regulatory perspective, blockchains could prove more reliable than traditional reporting tools in that they are not only declarative but also performative; one cannot claim to have executed a transaction without having actually executed it. To the extent that information recorded on a blockchain cannot be unilaterally modified or deleted by any single party, a blockchain can be relied on as proof that a particular transaction has occurred. By incorporating legal requirements into a blockchain-based protocol or smart contract, States thus can determine when and how the law is applied and with whom—without incurring the risk of tampering with the logs.[97] To illustrate, States around the globe implement anti-money laundering regulations, which require that financial institutions track flows of money, including virtual currencies, and report suspicious activity to stamp out money laundering, tax evasion, and terrorist financing.[98] By relying on a blockchain, laws could require that regulated intermediaries such as virtual currency exchanges implement

[95] Malloy (2005), p. 81.

[96] Burman (2019), p. 109.

[97] Sklaroff (2017), p. 263.

[98] Radziwill (2018), p. 64.

or interact with specific smart contracts that control the flow of transactions for these regulated intermediaries, enabling transactions to occur only if they satisfy the strict logic of the underlying code. A blockchain could be used, for instance, to verify whether an individual is permitted to transfer virtual currency. According to the information retrieved from the blockchain, a smart contract could limit the amount of virtual currency a person is legitimately entitled to transfer at any given time.

Tax collection could also conceivably be streamlined with blockchain technology. The use of automated smart contracts could help ensure that people, organizations, and potentially even machines rely on blockchain-based systems to pay taxes. For instance, instead of waiting for periodic tax returns, tax authorities could require that taxes be automatically calculated and remitted as soon as a transaction is complete by using specifically designed smart contracts that would be executed every time a party receives or disperses funds with a particular smart contract. Such a system would not only eliminate the need for periodic tax reporting but would also reduce the opportunities for people or companies to engage in tax evasion or other types of fraud. In much the same way, in the context of the Internet of Things, smart contracts could be deployed to ensure that blockchain-enabled devices automatically pay taxes whenever they engage in some form of profitable economic transaction, even where these transactions do not involve any human intervention but rely on machine-to-machine interactions.

In a supplementary role, where existing legal obligations bear the burden of 'trust', the blockchain is used exclusively to protect the integrity of data on the shared ledger. Though such an arrangement is the least ambitious mode of the blockchain application without any serious transformation attempt, the same is likely to be most comfortable for regulators and other government actors because it does not ask them to change their roles or rules substantially. Overall, the blockchain, as a supplement to the law, can promote efficiency and reduce transaction costs but is unlikely to herald large-scale transformations in the industry structures or drive lasting innovations.[99]

In situations where the legal system is not sufficient to establish trust, distributed ledgers can complement and increase the coverage of the existing trust architecture. Under traditional methods, scaling up centralized arrangements is often difficult and does not produce the necessary solutions. However, when the blockchain empowers new markets and products, it performs so in such a manner that they are complementary to the existing legal regime.

Let us reflect on the challenges of dealing with *orphan works under copyright law*.[100] Since the right holders of 'orphan works' are not known, anyone who may desire to utilize them cannot do so; for example, if a documentary filmmaker wants to incorporate certain archival footage, he or she is not in a position to negotiate a license even if he or she desires. Thus, orphan works are in a legally indeterminate

[99] Alexopoulos et al. (2021), p. 1.

[100] Brito and Dooling (2005), p. 75.

state. Therefore, even if, in some cases, such orphan works are in the public domain, the risk of statutory damages for copyright infringement is too high and intimidates away potential users of the material. In this scenario, a blockchain-based distributed registry could provide the right opportunity to craft a new market.[101] Such an arrangement would ensure that the stored information is available to all, and no intermediary would have excessive gatekeeping power. Moreover, such a complementary role could also trace the efforts to engage in the persistent search for rights-holders required under copyright law. As a complement to law, smart contracts could also be used to ensure that the users of orphan works pay requisite licensing fees to legitimate rights-holders. Though the distributed ledger would not entirely replace the need to have a standard copyright law, it would certainly assist in that direction.

Blockchain also finds application as a substitute for the law in situations where there is no or weak traditional legal enforcement. If the feasible rule of law does not exist, then the rule of code of blockchain, to begin with, maybe a substantial enhancement. For example, blockchain technology in the form of Bitcoin and other cryptocurrencies can offer practical solutions to mitigate the lack of access to bank accounts being faced by several billion people in the developing world and to provide the required opportunities for easy credits and payments.[102] The United Nations World Food Program has also demonstrated that the Ethereum blockchain can be successfully used to track food aid distribution to Syrian refugees in Jordan.[103] The program ensured accountability in an environment where it is difficult to enforce traditional legal obligations.

Such approaches could enable blockchain technology to achieve specific regulatory objectives in ways that are more efficient and less costly than those of existing laws and regulations. Building on Lessig's analysis of how computer code can be used on the Internet both as a compliment and a supplement to the law, the use of blockchain technology could play an increasingly important role in regulating the behavior of individuals and machines. Depending on the initiatives of the governments and public institutions to adopt this technology, the focus of regulation can be shifted from 'code is law', that is, 'using code to implement specific rules into technology', to 'code as law', that is 'relying on technology to define and implement State mandated laws'.

[101] Goldenfein and Hunter (2017), p. 1.

[102] World Economic Forum (2015). https://www.weforum.org/agenda/2015/01/5-ways-digital-currencies-will-change-the-world/.

[103] Kohl (2021).

4.4.3 Blockchain Code as Transaction Friction Alleviator

Most blockchain participants or users have demonstrated two diametrically opposite approaches to dealing with conventional law. At one end of the pole, some work on blockchain to utilize the technology to circumvent the substantive duties that are made obligatory by conventional law, while others at the other end intend to utilize the technology to fulfill these duties. But there is also a third set of blockchain developers who are positioned somewhere between these two poles, those who are determined to use blockchain primarily to engage in novel forms of cooperation and innovation in ways that avoid the procedural burdens and associated costs and formalities associated with conventional legally supported forms of coordination.

One significant motivation to develop innovative blockchain applications is not just to escape the substantive obligations of conventional law but to escape from the economic and procedural limitations of conventional law, which is considered a legitimate objective.[104] The law-makers and enforcement agencies dealing with conventional law respond to these applications variously depending upon their judgment on whether or not any intervention into blockchain systems is practically feasible, required, or appropriate.

As distributed ledgers promise to emerge as a significant technological and economic development, institutions are adopting an innovation-friendly approach. However, innovation friendliness must also be combined with respect for public policy objectives. While openness to new technologies is of paramount importance, policymakers must look beyond innovation narratives and engage critically with actual developments. This is easier said than done, especially in light of the possible multiple uses of blockchain. The decisions to be made are much more complex than the dichotomy between 'banning' or 'allowing' use cases of the technology.[105] Rather, sensible regulatory frameworks must be designed so that a balance between innovation and public policy is maintained.

While numerous applications of blockchain technology that strive to introduce newer forms of social and economic activities are in their infancy, their prospects are largely unknown in spite of all the hype around them. As against this, conventional lawmakers are just keenly watching the game and, for the time being, just content to allow the ongoing blockchain innovation movement without attempting to exercise their sovereign authority, ensuing a relationship of 'uneasy coexistence' between the rule of code and law. At the same time, the 'figure' engaged in building innovative blockchain applications has also adorned an attitude of suspicion towards conventional law, given that one of their central objectives is to nurture and develop novel innovative forms of social cooperation to get rid of the procedural burden, delays, and costs which are typically related to the conventional legal mechanism

[104] Yeung (2019), p. 207.

[105] Deloitte (2022). https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Tax/dttl-tax-global-blockchain-wp-sept-2022.pdf.

for facilitating transactions between strangers, resulting both systems displaying an attitude of 'mutual suspicion' towards the other.

By categorizing blockchain applications based on their motivations and potential impacts on legal interests, the analysis reveals varying degrees of interaction, from adversarial to cooperative dynamics, between blockchain and conventional law. This analysis facilitates to focus on the State's decisions regarding the adoption of blockchain technology, considering its advantages, trade-offs with the rule of law values, and impacts on governance.[106] It emphasizes the importance of examining both macro-level intentions and micro-level design in order to ensure that blockchain applications align with the rule of law standards, highlighting the need for comprehensive analysis from both *ex-post* and *ex-ante* perspectives to legitimize blockchain employment.

4.5 Battle for Supremacy Between Code and Law

Technology and regulation are often 'posed as adversaries': technology represents 'markets, enterprise and growth' while regulation symbolizes 'government, bureaucracy, and limits to growth'.[107] The less-emphasized story is that there are many blockchain projects that actually strive to build legally compliant products. The history of internet regulation confirms that industry might eventually welcome regulation as it facilitates its operation. For example, internet service providers did not set up corporations in Sealand but in jurisdictions with solid legal and institutional structures and the required human capital. Ultimately, internet companies sought regulations to get the consumer confidence that comes with it and to have predictability on the actions of their competitors. There are thus abundant benefits to consumers due to cooperation between regulators and technology companies.

Since blockchains are not detached from the real world, rather, the applications based on this technology owe their success largely to the society they serve, it is but natural for code to seek societal recognition not only through politics and popularity but also through law. When tokens act as avatars of real-world goods, related actions must be enforceable in the real world.[108] When the issue of net neutrality being abandoned in the United States came up, observers expressed concerns that internet service providers may automatically decide to block traffic coming from blockchains or undermine users' ability to run a node.[109] As such, law is essentially required for stability and legal acceptability of code necessary to translate code into facts.

[106] See Chap. 9.

[107] Wiener (2004), p. 483.

[108] Bradley and Froomkin (2004), p. 103.

[109] Vogelsang (2018), p. 225.

Regulations can support the development of code by providing certainty to the 'figure' wishing to pursue a certain option or create incentives for development. When code is 'slow to evolve, law can assist by removing bottlenecks to innovations'.[110] Regulatory uncertainty nowadays affects many aspects of blockchain's operation. In fact, innovation paralysis due to fear of legal consequences can be prevented by proper and unambiguous legal frameworks, which can act as a stepping-stone towards the design of more sophisticated software. The relationship between law and code is multifaceted. This emphasizes that the code does not exist in a vacuum but constantly interacts with other normative postulates. The manifest interdependence of the world underlines the fact that the blockchain cannot be a 'alegal' construct immune to regulation.

There is no formal 'battle for supremacy' between code and law since the technology is deliberately embedded within the conventional law in a network to build upon and actively support conventional law's authority over the relationships and activities of the users or network participants.[111] Nevertheless, tensions may arise between these systems, particularly in circumstances where either conventional legal rights and obligations do not translate easily into code or where the interactions between the parties on the platform do not reflect those arising under the legal instruments that establish and define their respective rights and duties. So, although the interaction between the two regulatory systems is intended to be complementary and supportive, tensions and conflict are likely to arise from time to time. In other words, the character of their dynamic interaction might be described as equivalent to the 'joys of marriage'[112]—with a continuous, dynamic relationship that occasionally causes disagreements and discords but eventually pursues to provide long-term mutual support and collaboration so that both partners can profit. In this system, stability is almost assured by the willingness of one partner to accept the superiority of the other rather than agreeing to the partnership of equals. In fact, the 'joys of patriarchal marriage'[113] are more apt for such systems since legal philosophers believe that linguistic texts, including those used in legal contracts, will inevitably have an element of ambiguity and uncertainty associated with them.

It is possible to cause adverse effects, albeit unintentionally, on third parties who are not party to the agreement while implementing a contractual agreement between the parties through blockchain-enabled smart contracts. The smart contracts are not 'smart' in the sense that they are just computer-programmed code that verifies, executes, and enforces the terms and conditions of an arrangement automatically and require external input to determine real-world events.[114] And to that extent, they are not, strictly speaking, legal contracts. Since smart contracts can adversely impact third parties, it is feasible to use smart contracts to cause intentional harm or produce

[110] Brown and Marsden (2013), p. 31.

[111] Yeung (2019), p. 210.

[112] Yeung (2019), p. 211

[113] Yeung (2019), p. 215.

[114] Yeung (2019), p. 208.

some other adverse third-party effects. Naturally, the question then follows: how to redress the grievances of those third parties. When the contracting parties are fully committed to the rights and obligations in their dealing with both on and off the blockchain,[115] they would be sympathetic to the concerns of the third party and would look for arrangements that would reflect the allocation of rights and duties that could be due under conventional law. However, if the blockchain community does not support providing a feasible solution, affected third parties may have to seek the assistance of the conventional law for justice. If this is the case, then such blockchain applications cannot be said to be 'mutually aligned' with conventional law and do not represent those classes of cases that are motivated by a desire to 'alleviate transactional friction'.[116] Just as many blockchain developers have proactively invited interactions with legal authorities and embraced conventional law, the lawmakers have also taken positive actions to appreciate technological developments and provide legal recognition to the blockchain, although with the conviction that the 'code of law' outweighs 'code is law'.

In summary, when blockchain systems are developed unequivocally with an intent to support and partner with conventional legal systems by providing a feasible solution to execute and implement legally enforceable rights and obligations with speed, efficiency, and reliability, the outcome of dynamic interactions between such systems can be appreciated as a manifestation of the so-called 'joys of patriarchal marriage'. In this regard, some conventional law-making bodies within liberal legal regimes, which advocate that *anything not prohibited is permitted*, have taken initiatives to validate the transactions via blockchain systems and to confer legal recognition. These steps are intended to keep away from any overt 'battle for supremacy' between the 'code of law' and 'code is law', the assumption, without any doubt, is that the sovereign is supreme and its authority through the conventional law will always prevail over 'code is law'.

Since the State at the macro-level has to make decisions regarding the choice of blockchain artifacts depending on the purpose of using such technology, the advantage the technology provides, the accepted trade-offs with certain rule of law values, and the impact of such choices on the rule of law, it is important to analyze these decisions. This analysis would then facilitate an understanding of what the State intends for the blockchain to afford for a particular usage, which must result in an *ex-post* legitimacy such that the affordance follows the rule of law. Once the State's intention and affirmation towards the usage of blockchain application is absolute, the effectuation of the purpose behind the technology, that is, the *ex-post* outcome, is delegated to the 'figure', at the micro level, who designs, programs, and develops the technology with the necessary *ex-ante* configurations and affordances. Because technology is a potent tool to enforce norms, it matters what the 'figure' has created, to what end, and what are the affordances provided by the technology. The synergetic relation between law and code also manifests where law helps code. It is

[115] Yeung (2019), p. 207.

[116] Akinrotimi (2020), p. 217. Casey and Vigna (2018), p. 23.

important that not only the *ex-post* conceptual code rules (outcome) echo the values of the rule of law (at the macro-level) but also that the *ex-ante* command code rules are valid and legitimate (at the micro-level), affording the rule of law standards. *Ex-ante* analysis needs to go hand-in-hand with the *ex-post* analysis since the relationship between code and law is that of 'Tom and Jerry'; just focusing on one level, either macro or micro level, would not be sufficient to legitimize the technology. Not only the purpose behind the conceptual rules for using the technology should be justified, but also the command code rules, which make this (justified) purpose possible, should also be legitimized.

References

Akinrotimi AO (2020) Legal ramifications of Blockchain technology. In: Khan MA and others (eds) Decentralised Internet of things: a Blockchain perspective. Springer, p 217

Alexopoulos C et al (2021) How Blockchain technology changes government: a systematic analysis of applications. Int J Public Adm Digital Age 8:1

Arner DW et al (2017) FinTech, RegTech, and the re-conceptualization of financial regulation. Northwest J Int Law Bus 37:371

Arvicco (2016). A crypto-decentralist manifesto. http://etherplan.com/A-Crypto-Decentralist-Manifesto-en.pdf

Athey S (2015) 5 Ways Digital Currencies Will Change the World. World Economic Forum, 22 January 2015. https://www.weforum.org/agenda/2015/01/5-ways-digital-currencies-will-change-the-world/

Belli L et al. (2017) Law of the land or law of the platform? Beware of the privatisation of regulation and Police. Platform regulations: how platforms are regulated and how they regulate us. FGV DIREITO RIO, p 41

'Blockchain - Legal Implications, Questions, Opportunities & Risks' (Deloitte, September 2022) https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Tax/dttl-tax-global-blockchain-wp-sept-2022.pdf

Bradley C, Froomkin AM (2004) Virtual worlds, real rules. New York Law School Law Rev 49:103

Brito J, Dooling B (2005) An orphan works affirmative Defense to copy-right infringement actions. Mich Telecommun Technol Law Rev 12:75

Brown I, Marsden CT (2013) Regulating code: good governance and better regulation in the information age. MIT Press, p xii

Brownsword R (2015) In the year 2061: from law to technological management. Law Innov Technol 7:1

Brownsword R (2019) Smart contracts: coding the transaction, decoding the legal de-bates. In: Hacker P et al (eds) Regulating Blockchain: techno-social and legal challenges. Oxford University Press, p 311

Brownsword R, Goodwin M (2012) Law and the technologies of the twenty-first century: text and materials. Cambridge University Press

Brownsword R et al (2017) Law, regulation, and technology: the field, frame and focal questions. In: Brownsword R et al. (eds, The Oxford handbook of law, regulation and technology. Oxford University Press, p 3

Burman A (2019) Making land titles in India marketable: using title insurance as a viable alternative to conclusive titling. Washington Int Law J 28:109

Buterin V (2014) A next-generation smart contract and decentralized application platform. Ethereum White Paper 3:37

Calo R (2014) Digital market manipulation. George Wash Law Rev 82(995):1016–1018

Casey MJ, Vigna P (2018) In Blockchain we trust. MIT Technol Rev 121:10
Citron DK (2007) Technological due process. Wash Univ Law Rev 85(1249):1252
Cohen JE (2016) The regulatory state in the information age. Theor Inq Law 17:369
De Filippi P, Hassan S (2016) Blockchain technology as a regulatory technology: from code is law to law is code. First Monday, 21 https://doi.org/10.5210/fm.v21i12.7113
De Filippi P, Loveluck B (2016) The invisible politics of bitcoin: governance crisis of a decentralized infrastructure. Internet Policy Rev 5
Deirdre C, Päivi L (2017) In search of transparency for EU law-making: trilogues on the cusp of Dawn. Common Mark Law Rev 54:1673
Delimatsis P (2019) When disruptive meets streamline: international standardization in Blockchain. In: Kraus D et al (eds) Blockchains, smart contracts, decentralised autonomous organisations and the law. Edward Elgar Publishing
Dimitropoulos G (2019) Global currencies and domestic regulation. In: Hacker P et al. (eds) Regulating Blockchain: techno-social and legal challenges. Oxford University Press, p 112
Dimitropoulos G (2020) The law of Blockchain. Wash Law Rev 95:1117
Dyson E (1996) Cyberspace and the American dream: a magna carta for the knowledge age (Release 1.2, August 22, 1994). Inf Soc 12:295
Eecke PV, Truyens M (2011) 'L'Oréal v. eBay: the court of justice clarifies the position of online auction providers. Comput Law Rev Int 12:129
Eich S (2019) Old Utopias, new tax havens: the politics of Bitcoin in historical perspective. In: Hacker P et al. (eds) Regulating Blockchain: techno-social and legal challenges. Oxford University Press, p 85
Finck M (2018) Digital co-regulation: designing a supranational legal framework for the platform economy. Eur Law Rev 43:1
Finck M (2018a) Blockchains: regulating the unknown. Germ Law J 19:665
Finck M (2018b) Blockchains as a Regulatable technology. Blockchain regulation and governance in Europe. Cambridge University Press
Fischer H (2006) Technology perspectives on code. In: Dommering E, Asscher L (eds) . TMC Asser Press, Coding regulation: essays on the normative role of information technology
Follow the Bitcoin to Find Victims of Human Trafficking (NYU Tandon School of Engineering Press Release, 16 August 2017). https://engineering.nyu.edu/news/follow-bitcoin-find-victims-human-trafficking
Goldenfein J, Hunter D (2017) Blockchains, orphan works, and the public domain. Columbia J Law Arts 41:1
Grundmann S, Hacker P (2017) Digital technology as a challenge to European contract law: from the existing to the future architecture. Eur Rev Contr Law 13:255
Guadamuz A, Marsden C (2015) Blockchains and bitcoin: regulatory responses to cryptocurrencies. First Monday 20 https://firstmonday.org/ojs/index.php/fm/article/view/6198/5163
Hacker P (2017) Personalizing EU private law: from disclosures to nudges and mandates. European Review of Private Law, p 25
Hacker P et al (2019) Regulating Blockchain: techno-social and legal challenges- an introduction. In: Hacker P et al (eds) Regulating Blockchain: techno-social and legal challenges. Oxford University Press, Oxford, p 13
Hassan S, De Filippi P (2017) The expansion of algorithmic governance: from code is law to law is code. Field actions science reports. J Field Actions 88
Israel B (2017) In a Step toward Fighting Human Trafficking, Sex Ads Are Linked to Bitcoin Data. (Berkeley News, 16 August 2017). https://news.berkeley.edu/2017/08/16/in-a-step-toward-fighting-human-trafficking-sex-ads-are-linked-to-bitcoin-data/
Keller D (2017) Law, borders, and speech conference: proceedings and materials. Stanford Law School, Stanford Center for Internet and Society. https://cyberlaw.stanford.edu/publications/proceedings-volume/
Kelly K (1994) Out of control: the rise of neo-biological civilization. Addison-Wesley Longman Publishing

Kohl U (2021) Blockchain utopia and its governance shortfalls. Blockchain and public law, Edward Elgar Publishing
Lee JH (2019) Rise of anonymous cryptocurrencies: brief introduction. IEEE Consum Electr Magazine 8(5):20
Lessig L (1999) Code and other laws of cyberspace. Basic Books, p 3 https://lessig.org/images/resources/1999-Code.pdf
Lessig L (2003) Law regulating code regulating law. Loyola Univ Chicago Law J 35:1
Lessig L (2006) Code Version 2.0. Basic Books. <https://tigerprints.clemson.edu/cgi/viewcontent.cgi?article=1183&context=cheer>
Lianos I (2019) Blockchain competition–gaining competitive advantage in the digital economy: competition law implications. In: Hacker P et al (eds) Regulating Blockchain: techno-social and legal challenges. Oxford University Press, Oxford, pp 329–410
Makridakis S, Christodoulou K (2019) Blockchain: current challenges and future prospects/applications. Fut Inter 11:258
Malloy RP (2005) Real estate transactions: policy considerations for law. Technol Glob Law Policy 27:81
Mazur O (2022) Can Blockchain revolutionize tax administration? Penn State Law Rev 127:115
McNamee J, Pérez MF (2017) Fundamental rights and digital plat-forms in the European Union: a suggested way Forward' how platforms are regulated and how they regulate us. FGV DIREITO RIO, p 99
Murray A (2013) Information technology law: the law and society. Oxford University Press
Ortolani P (2019) The Judicialisation of the Blockchain. In: Hacker P et al (eds) Regulating Blockchain: techno-social and legal challenges. Oxford University Press, p 289
Pasquale F (2015) The black box society: the secret algorithms that control money and information. Harvard University Press
Pasquale F, Cashwell G (2015) Four futures of legal automation. UCLA Law Rev Disc 63:26
Pouwelse J et al (2005) The BitTorrent P2p file-sharing system: measurements and analysis. In: Castro M et al (eds) Peer-to-peer systems IV. Springer
Radziwill N (2018) Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world. Qual Manag J 25:64
Reidenberg JR (1997) Lex Informatica: the formulation of information policy rules through technology. Tex Law Rev 76:553
Reyes CL (2017) Conceptualizing cryptolaw. Nebraska Law Rev 96:384
Rheingold H (1993) The virtual community: finding connection in a computerized world. Addison-Wesley Longman Publishing
Rodrigues U (2019) Law and the Blockchain. Iowa Law Rev 104:679
Rohr J, Wright A (2019) Blockchains, private ordering, and the future of governance. In: Hacker P et al (eds) Regulating Blockchain: techno-social and legal challenges. Oxford University Press, p 43
Schafer B (2022) Legal tech and computational legal theory. In: Borges G, Sorge C (eds) Law and technology in a global digital society: autonomous systems, big data, IT security and legal tech. Springer
Scheiber N (2022) How uber uses psychological tricks to push its drivers' Buttons,' ethics of data and analytics. Auerbach Publications
Shapiro SJ (2002) Law, plans, and practical reason. Legal Theory 8:387
Sklaroff JM (2017) Smart contracts and the cost of inflexibility. Univ Penn Law Rev 166:263
Sunstein CR (2013) Impersonal default rules vs. active choices vs. personalized De-fault rules: a triptych. NYU Law & Economics Research Paper Series
Van Hout MC, Bingham T (2014) Responsible vendors, intelligent consumers: silk road, the online revolution in drug trading. Int J Drug Policy 25:183
Vogelsang I (2018) Net neutrality regulation: much ado about nothing? Rev Netw Econ 17:225
Werbach K (2018) The Blockchain and the new architecture of trust. MIT Press

Wiener JB (2004) The regulation of technology, and the technology of regulation. Technol Soc 26:483
Winner L (2010) The whale and the reactor: a search for limits in an age of high technology. University of Chicago Press
Wiseman M (2019) The supplemental nutrition assistance program. In: O'Leary CJ et al (eds) Strengths of the social safety net in the great recession: supplemental nutrition assistance and unemployment insurance. Upjohn Institute for Employment Research, p 93
Wright A, De Filippi P (2015) Decentralized Blockchain technology and the rise of Lex Cryptographia
Wright D (2016) Enforcing privacy. In: Wright D, De Hart P (eds) Enforcing privacy: regulatory, legal and technological approaches. Springer, p 13
Wu T (2003) When code isn't law. Va Law Rev 89:679
Yeung K (2017) Blockchain, Transactional Security and the Promise of Automated Law Enforcement: The Withering of Freedom under Law? TLI Think! Paper 58/2017
Yeung K (2018) Algorithmic regulation: a critical interrogation. Regul Gov 12:505
Yeung K (2019) Regulation by Blockchain: the emerging Battle for supremacy between the code of law and code as law. Mod Law Rev 82:207
Yeung K (2019a) "Hypernudge": big data as a mode of regulation by design. The Social Power of Algorithms. Routledge

Part II
The Design of the Rule of Code

Chapter 5
Normative Foundations of Design in Blockchain Artifact

5.1 Design Perspectives on Blockchain

In a blockchain artifact, the governance of the decentralized network is performed by following the rule-sets as determined for the performance of the technology. These rule-sets are recognized as working rules within the blockchain protocol,[1] which convey a constitutionalizing sense amongst the 'figure' and users. The blockchain protocols are essentially a set of foundational code rules establishing the structure of technological artifact that governs the functioning of the blockchain network.[2]

The main utility of the rule of code, which is identified with this technology, is to dictate what individual nodes can or cannot perform, causing a profound impact on the user. From this perspective, the rule of code can be considered as a rulebook for computing, which determines the user actions. The 'figure' aims to execute the intentions of the users who engage with the blockchain through the code programmed in the artifact. It seems that the rule of code has the power to constrain or affect individual users. For instance, a blockchain-based system designed to secure and verify evidence of human rights violations may impact users through its technical transparency and accountability features. If the rule of code is programmed in the artifact in such a manner that it fails to adequately protect user anonymity or lacks robust security measures, individuals providing crucial evidence might face risks of retaliation, potentially leading to self-censorship and hindering the reporting of human rights abuses. Additionally, poorly designed code embedded within the blockchain artifact might marginalize certain user groups, limiting their ability to contribute to decision-making processes. The transparency and fairness of the

[1] Berg et al. (2020), pp. 193–194.

[2] Rajagopalan (2018), p. 365.

A. Bisoyi, *Blockchain and Legitimacy*, Law, Governance and Technology Series 77, https://doi.org/10.1007/978-3-031-98712-0_5

blockchain system, as shaped by its rule of code, are pivotal in ensuring trust among users by safeguarding the rights of those involved.

The key attributes of blockchain are built on the values of decentralization, immutability *vis-à-vis* tamper-resistant, data integrity, and transparency, but it is not known how these attributes are perceived and how they trigger action by the users or what they afford to the users. Although one of the main fortes of blockchain technology may be its capability to ensure trust, it is not very clear how trust is programmed, generated, and developed, and how it impacts the interactions of users, bringing in a certain element of uncertainty. This uncertainty is the most important challenge for the long-term advancement of blockchain technology. Mostly, designing is treated in abstraction without engaging in what things actually do and how they do. However, if the engagement does not include the perspective of design theory and philosophy of technology, then the legal view of technology becomes very truncated.

5.2 Affordance—Concepts and Major Groupings

As technology advances, it becomes more capable of influencing a user's trust in it. Understanding affordances enabled by blockchain helps us to analyze user behavior through a heuristic framework by elucidating the relationships between their abilities to perceive and take action. The technological affordances of blockchains, shaped through the rule of code embedded in the artifact, convey the heuristic prompts, which can actuate positive or negative heuristics, contingent upon the way the affordances manifest. These affordances can manipulate the 'confirmation of trust' of a user and produce a new normativity.[3] Users' perceptions of the affordances and disaffordances provided by the artifact can affect how they feel, what they expect, and how they conform and satisfy their needs. Therefore, it is important to explore the theory of affordance coupled with the concept of technological normativity. Here, the 'technological normativity' is referred to in a manner that juxtaposes the code's normativity and, more familiarly, the legal normativity—as explained by Hildebrandt.[4] In fact, technological normativity is about how a particular technological device or infrastructure limits human actions or behavior, where the 'figure' has the power to impose these effects in code deliberately or otherwise and can create the rule of code with an emerging characteristic.

The possible actions arising from the relation between the technological features, including those of blockchain and goal-oriented actors who determine how the technology can be used to create value, are termed affordances. It is the enablement of a specific action or behavior for a particular user by the artifact's design. The concept was originated by Gibson, who defined affordances as opportunities

[3] Metzger and Flanagin (2013), p. 210.

[4] Hildebrandt (2008b), p. 173.

for actions that are offered to an actor by an object.[5] Affordance refers to how organisms perceive their environment, prompting questions about what an animal is capable of performing in a specific environment at a given moment. There exists a dynamic relationship that continuously evolves between the organism and its surroundings. Norman appropriated the theory of affordance and imported it into the design sphere, and used the term 'affordance' to denote certain design aspects of an artifact. Affordances are about those properties that determine 'how the object could possibly be used within the capability bound of the agent'.[6] The implicit moral imperative of affordance allows the 'figure' of blockchain-based systems to endorse ethical goals in society by joining the 'mining' with the ecological and social benefits.[7]

The affordances can be both beneficial and injurious to the individual, although the extent of the benefit or the injury may vary, meaning affordances can have both negative and positive values at the same time. However, instead of using value judgemental terms such as 'positive' and 'negative' in the affordance discourse, the use of the terms 'inscriptions' and 'descriptions' that are based on 'biological and behavioral facts'[8] is preferred. For example, water can afford to quench thirst and is essential to sustain life; at the same time, it can also afford drowning and floods, which can mean injury and possible death. As the degree of the benefit or injury is dependent upon the organism in question, the affordances result from the relationship between the artifact and a particular individual, as governed by its properties, and are not from the physical properties of the artifact alone. Gibson explained this relationship by listing down the physical properties of a hypothetical walking surface, which are usually measured in standard physical units.[9] However, its affordance has to be determined with respect to the user. If the surface is to provide support to a specific animal, then the affordance has to be measured with respect to the animal, which would obviously differ depending on the animal under consideration.[10] Thus, affordances are not just abstract physical properties, they are unique and cannot be quantified in physical science.[11]

The concept of affordance highlights the inherent and simultaneous objectivity and subjectivity of an artifact's potential effects on the world. The existence of an affordance is determined by both the attributes of the object and the capabilities of the interacting agent.[12] Needless to say, affordance is not a property but a relationship whose existence owes to the properties of both the artifact and the user. Thus, affordance can be defined as the potential for behavior associated with achieving an

[5] Gibson (2014), p. 217.

[6] Norman (1988), pp. 9–10.

[7] Kewell et al. (2017), p. 429.

[8] Gibson (2014), p. 129.

[9] Gibson (2014), pp. 128–129.

[10] Gibson (2014), p. 119. Baldoni et al. (2006), p. 46.

[11] Gibson (2014), p. 120.

[12] Norman (2013), p. 11.

immediate concrete outcome that arises from the relationship between an object (e.g., a technological artifact) and a goal-oriented actor(s), that is, the user.

5.2.1 Blockchain Affordances

Blockchain systems produce confidence in the user by hardcoding rules into the system both at the micro and macro levels. In fact, the non-requirement of a trusted third party is the most significant affordance of blockchain technology, which is why it is considered to be an enabler of trust.

Traditionally, the State has the authority to determine an individual's identity. However, in the online world, authorities specify how to identify an individual, for which purpose an 'identifier' is assigned to that individual, and the identity is protected through credentials like passwords that have been granted to private entities or trusted third parties. This authority is manifested in the form of prompts asking users to log in using their social media identity or email address.[13] However, reliance on 'trusted third parties' is particularly problematic since it makes users dependent on multinational enterprises that control accounts and always have the capability to arbitrarily decide not to permit the users to access. Furthermore, users are required to divulge a great deal of private information without always knowing how their data will be used. Enterprises track users, gather user data in a methodical manner, and run targeted advertisements using their identity management business. In this kind of environment, a variety of private organizations hold the data of individuals. These organizations have access to information that users have been compelled to provide in order to carry out online transactions. Given the continued frequency of identity theft and data leaks in the virtual world, the security of this data is not always assured. In this scenario, blockchain technology may be able to liberate people from the controlling activities of these big tech corporations by enabling a new form of digital identity management, such as 'self-sovereign identity', that affords users sole authority over their online persona—only they can manage their personal information, and only they have the power to decide with whom to share their information and what to share and for what purpose. The self-sovereign identity might potentially compete with the current monopoly on the State-assigned identities and, as such, can compensate for the absence of the State-issued identity documents, whether due to loss or destruction or simply because the State in question failed to furnish them. It could also be useful in circumstances where the identity document is not recognized by a State, such as in diplomatic crises. Such an affordance enhances confidence levels in data and information management systems.

[13] Such identity services are frequently provided by large technological corporations such as Apple, Meta etc.

Apart from a trustless system, blockchain technology also affords tamper-resistance, disintermediation and distributed architecture, and redundancy.[14] It is a decentralized ledger designed to register assets, and one of its affordances is traceability. Traceability can be leveraged to bring in transparency to record-keeping and tracking in the supply chain. When 'alegality' is embedded into a blockchain-based technological architecture through which people interact, then it can be said that the technological design of a blockchain-based system is providing the affordance for an alegal act.[15] Therefore, one can appreciate that the 'design constituency'[16] or the 'figure'—that is, the designer or a group of designers who create the artifact, must incorporate necessary features in the artifact to achieve the preferred relationship between it and the user. This is invariably a subjective exercise since it is not feasible for the 'figure' to foresee and predict features that every user desires. Envisioning the specific types of users to whom the process will be directed and interpreting their requirements and idiosyncrasy into desirable features as surrogates for the characteristics that the code must incorporate to create the affordance relationships the 'figure' seeks is an essential component of the design procedure. Product interfaces are, thus, constructed on this fundamental idea, interpreting and decoding the state of the underlying code into a format that the 'figure' intends the user is capable of comprehending.

5.2.1.1 Perceived and Actual Affordance

It is not necessary for an affordance to be perceived; rather, affordance is about the relationships between the true characteristics of the artifact and the organism.[17] These relationships exist eternally and are open to action for as long as the prerequisite factors are present and fulfilled in both the blockchain architecture and the organism, that is, the individual or the user, even though the individual may not be aware of the latent correlation. Such affordances have been referred to as 'actual' affordance, as opposed to 'perceived' affordance.[18]

Whilst asked to describe the primary purpose of a chair, for instance, we will mention sitting, perching, etc., yet, in a different circumstance, we may think of other applications for the chair, like steps or standing on it to reach higher ground. Comparatively, graphical items and interactive features are significantly less versatile; although we can often make use of the keyboard, double-click, hold down a button and drag, and left/right click, the actual outcomes of these activities are limited by the interface. This means that the decisions made by users are predicated on assumptions, which are verified only after the activity is completed. Therefore,

[14] Kshetri (2017), p. 1027.

[15] De Filippi et al. (2022), pp. 364–366.

[16] Pfaffenberger (1992), p. 282.

[17] Norman (2013), p. 13.

[18] Norman (1999), p. 38.

unless an individual predicts or acknowledges the presence of affordance, they may not act upon the relationship between themselves and the artifact despite the manifestation of such possibility.

Perceived affordances are actions that individuals believe are feasible based on design, as opposed to actions that are truly possible and which may or may not embody the entire gamut of relationships that exist between the individual and the artifact. This indicates that the user perceives they can take an action that is not among those that are offered to them. Such distinction between actual and perceived affordances is very significant in technological systems since the affordances in such systems exist independently of what is visible on the screen.

In the case of computers, built-in physical affordances are of little interest[19] since the design and incorporation of the perceived affordances can only be controlled by the 'figure', which is of more use in providing an interface showcasing the purpose of the application intended by the 'figure'. In the coded artifacts, the perceived affordance determines what the 'figure' can accomplish with the code. It may serve as a metric for evaluating how well an application programming interface[20] is being developed and the code that the 'figure' is creating. Even in the rule of code architecture, it is essential to understand the concept of affordances and its offerings to the 'figure' and the user.

5.2.1.2 Technological and Affective Affordance

In a blockchain architecture, there are two broad categories of affordances, namely, technological affordance and affective affordance,[21] which resonate with actual affordance and perceived affordance, respectively. While technological affordance is about users' appreciation of blockchain based on their technical features and qualities, affective affordance refers to users' interpretations of the use of blockchain service in relation to users' experience and subsequent contemplations about technological affordances.[22] Record-keeping and cryptographic hash functions, which are the vital attributes of a blockchain system, can be counted towards technological affordances in blockchains. In this regard, autonomous automation, decentralization, tamper-resistant, and immutability are specific technological affordances in a blockchain. By enabling users to verify the technological attributes and functions of blockchains, technological affordances are in a position to shape the 'trust' factor. As regards affective affordances in blockchains, transparency and

[19] Norman (1999), p. 39.

[20] An application programming interface with a clear perceived affordance enables the 'figure' to gain an understanding of its purpose and apply it easily inside the Cybernetic Environment for which it was built. If the 'figure' does not comprehend the core purpose of the environment and the application programming interface they are using, it is difficult to make good use of the tools afforded to them to create a well-designed, sustainable system. Korenhof et al. (2021), p. 1751.

[21] Scarlett and Zeilinger (2019), pp. 7, 13–14.

[22] Shin and Hwang (2020), p. 917.

reliability can be considered towards the same since these are interpreted by the users in the use of blockchain services. Codification of trust[23] and transparentizing[24] in blockchain are examples of affective affordance.[25] In blockchains, affective affordance can be a perceived object that stimulates emotions such as assurance or privacy in users. Emotional affordance is an extension of affective affordance that can be described as the ability to enable, prompt, and restrict the representation of specific emotional experiences developing between the technologies and the users. These affordances provide users with initial suggestions or emotional signals about the possibilities of user behavior.

The 'figure' can potentially manipulate the perceptions and emotional experiences of the users through choices while designing the interface. Actual (underlying) affordances can be concealed by molding the perceptions of the user about the possible functionalities of the artifact. For example, the ability to view and alter the source code of a web page is an actual (underlying) affordance of modern web browsers, which is kept hidden from users. Likewise, the 'unwaveringness' of the default configuration of an artifact might overwhelm the tendency of the individual to explore better configurations that support the users' interests or inclinations. This relates closely to the issue of 'dark patterns' in design or default configurations. It goes on to show that the relationship between the actual affordances of an artifact and the way they are communicated to the user is really important. Such communications might be clear, unequivocal, and isomorphic with the true state of the system at one end and misleading, abstract, and suppressing of the actual affordance at the other end. And most importantly, it is the 'figure' who defines the extent and quality of that communication in most cases.

5.2.2 Identifiers

The identifier, also referred to as 'signifier' in the study of UX design, communicates to the user about the affordances that are present. It is a key component of the artifact's normativity and is connected to technological intentionality.[26] The 'figure' incorporates these identifiers into the design of the artifact, defining the way the artifact 'should' be used. The use of underlining to identify and reference certain elements, such as hyperlinks on the web, distinct from the plain surrounding text, is a straightforward example of an identifier. Obviously, the user must perceive that element of the artifact to act as an identifier. It can, however, be ambiguous—for

[23] Codification of trust is the process of incorporating a certain level of trust into systems that enable agreements between agents without the need for a third party.

[24] Transperantizing is the process of opening up organizational processes and the data associated with them by depending on the persistence and immutability properties of blockchain technologies, respectively.

[25] Lichti and Tumasjan (2023), p. 9.

[26] Norman (2013), p. 13.

example, a painted zebra stripe on the side of a road is an identifier, which is a signal about where to walk. But this affordance cannot stop an individual from crossing the road anywhere unless there is a physical barricade, such as a fence by the side of the road. While identifiers are important elements that communicate to the user about how the artifact functions, the utility of an identifier is conditional to its accuracy, honesty, and entirety, which is associated with the functionality of the identifiers being able to be determined at the appropriate time by the user.

It is very important for the 'figure' to be certain about the affordances to be signified and at what instant to be signified. Such a procedure will assist the user in shaping a precise mental image of the system.[27] Moreso, the 'figure' draws up the technological artifacts with certain affordances that are not signified, either to put a veil around complex utilities from users or to comply with the regulatory or ethical norms without publicizing it, since the application of the said technology might be inconsistent with the business interests and outlook of the supplier. For example, although the complex cookie preference notices provide an interface for the user to choose which cookies to set on the computer, in reality, often a textual link is provided as the mechanism of accessing this interface, which is usually less signified than the option to accept all cookies, supposedly a more profitable option as it facilitates targeted behavioral advertising.[28]

5.3 Normative Dimensions of Affordance in Blockchain

Typically, the relationships between specific properties and features of an individual and an artifact give rise to affordances. While in many cases, affordances simply exist because of the attributes of the technology, the situations where the affordance arises through the conscious decision-making of the 'figure' is of interest in the context of code. In the case of code-based artifacts such as blockchain, affordances can be designed to make them user-friendly and craft new behavioral possibilities, for technology is not the design of physical things.[29] It is the design of practices and possibilities to be realized through artifacts. From the perspective of regulating users' actions, the choices about rendering an artifact useful can cultivate mechanisms that proactively suggest particular courses of action. These conscious choices lead to designs being instilled with usefulness as well as with normative effect. However, such decision choices invariably manifest the assumptions of the 'figure' with respect to the function and purpose of the artifact and its user.[30] Of course, problematic assumptions can be challenged by the user in the case of legitimately designed artifacts.

[27] Stutzman and Hartzog (2012), p. 769. Hartzog (2018).

[28] Ogut (2023), pp. 529–538.

[29] Verbeek (2005), pp. 47–95.

[30] Agre (1994), pp. 184–185.

In blockchains, actual affordances play a key role not only in enabling trust in an interface but also in users' understanding and experience of services. Once actual affordances in relation to trust are in place, the search begins for the perceived affordance dimensions (such as transparency and reliability) of the interaction process. Thus, users' cognitive processing of technical features is central to a transparent and reliable blockchain service. In the case of blockchain services, when artifacts are validated to have the desired security and traceability, users feel assured about their privacy, and functions as emotional affordances. The user's affective process of evaluating transparency and reliability is afforded by these emotional prompts. As transparency and reliability are drawn from the degree of user trust, instilling a sense of these aspects into blockchain service is achieved by cognitive processing of blockchain services through user perceptions of security and safety. Thus, the trust acting as a heuristic cue—a cognitive shortcut for users to prompt assurance, may activate transparency and reliability in the blockchain.[31]

Most of the affordances and user interactions in blockchains hinge on the user trust heuristics. Because blockchain systems are complex in nature, users generally choose the heuristic of trust to make decisions, considering the swift and consistent efficiency of assessments that heuristics can provide with limited information about material features.[32] Since the average users are not acquainted with the details of blockchain operation and structure and have to use their own trust heuristics, they often have to trust a plausible judgment or related incident concerning security and safety that comes to mind while passing judgments and making decisions about blockchain service. In other words, the users' perceptions about the security and safety of blockchains that are drawn from the outside world affect user heuristics of trust. In a sense, trust remains within the user's cognition and is neither premade nor a product of external stimulants.

5.3.1 Design Affordance, Disaffordance, and Dark Patterns

The outcome of affordance can have a positive or negative effect.[33] These actions ought to be differentiated from the fact that interaction is not allowed and there is no affordance relationship.[34] Actions can also be distinguished from the subjective misapprehension of the user, where the user believes to have a particular relationship between itself and the artifact when, in reality, there is no such relationship. When there is no affordance relationship between the user and the artifact, the notion of

[31] Shin and Park (2019), p. 283.

[32] Shin and Hwang (2020), p. 926.

[33] For example, water sustaining the life of an organism versus drowning or flooding it.

[34] Norman (2013), p. 11.

disaffordance indicates that there does not exist any affordance, whether or not the user is aware of this; these are actions that are blocked or constrained.[35]

In order to understand the 'figure's' choice of affordances and disaffordances, it is vital to analyze the intention or the reasoning behind such a selection. Depending on the choice of the 'figure', the technology can be anything—

> they can be like a chameleon, changing shape and appearance to match the situation.[36]

The intention or the reasoning can be assessed by scrutinizing the 'architecture of control',[37] which broadly refers to the features, structures, or methods that can be used to enforce or limit user behavior.[38] This proposition of understanding the purpose behind the affordances and disaffordances denotes the identification of intended positive affording by the 'figure' and the 'deliberate, intentional, and strategic' negative affording.[39] The 'negative affordance' is about the concept of 'engineered obedience'[40] and is not a result of the unintentional or incompetent design. The concept of disaffordance is essential and must be appreciated in capturing the hypothesis of how a blockchain technological architecture can camouflage, restrain, or prohibit the likelihood of particular behaviors as an outcome of intentional and deliberate design decisions. This helps us to determine the role of the disaffordances in restricting the users' interaction with the technological artifact.[41]

The misuse of power by the 'figure' to exploit the user is reflected in 'abusive design' and 'dark patterns'. While 'abusive design' refers to designing deliberate disaffordances that are antagonistic to the user's interests, 'dark patterns' are about misusing commonly employed design conventions against the user.[42] Here the intention of the 'figure' is to forego the user experience deliberately. Such evil designs can be deployed for coercion, confusion, distraction, interruption, obfuscation, and trickery. For example, confusion can be created by designing questions where double or triple negatives are used, users can be distracted through advertising, and popups can be introduced to interrupt the process. Even a free version of an application can be hidden by manipulating navigation; the closure of adverts can be obfuscated by reducing the contrast of the 'closure button'; users can also be tricked by designing adverts that appear to be new content.[43] Such design practices, though increase the level of frustration in a user, are employed to increase the income of

[35] Gibson (2014), pp. 133–134. Norman (2013), pp. 11–12.

[36] Norman (1988), p. 183.

[37] Lessig (2006), chp. 4.

[38] Lockton (2006a), p. 30.

[39] Lockton (2006b). https://architectures.danlockton.co.uk/2006/10/22/disaffordances-and-engineering-obedience/.

[40] Lockton (2006b). https://architectures.danlockton.co.uk/2006/10/22/disaffordances-and-engineering-obedience/.

[41] Longford (2005), p. 77.

[42] Narayanan et al. (2020), p. 67.

[43] Conti and Sobiesk (2010), p. 273.

website operators[44] since 'designers must please their clients, who are often not the actual users'.[45]

Automation offers significant benefits to the end-users; it is also dangerous when too much control is bestowed upon it. Blockchain technology automatically identifies violations of the rules embedded in the smart contract without considering the personal contexts affected by the technology's configurations. This exemplifies a disaffordance of the blockchain system, as it potentially enables abusive design by disregarding nuanced social considerations.

5.3.2 Mapping Technological Mediation and Affordance

'Mapping' is a technical term defining the relationship between two or more things, in this case, between technology and its movements and the results in the world,[46] which focuses on the role of technological mediation. This principle, particularly, assists in exploring the interactions between individuals and artifacts, with a focus on the substantive features of certain artifacts.[47] The aim is to understand how the technologies shape user experience since no technology is neutral in nature. It is, in actuality, a more complex and enigmatic artifact and thus is also not merely deterministic in nature.[48] Therefore, the examination of the function that particular technologies serve in particular situations is the basis of the 'postphenomenological theory'[49] of mapping.

Drawing a parallel with perceived and actual affordances, the relationships between humans and artifacts may also be categorized into those of perception and those of action. The former is about what the individual thinks it can do with the artifact, while the latter tells about what the individual can actually perform. There is a gulf between the intentions of the users and the allowable actions by the 'figure'.[50] This relationship between the individual and the artifact undergoes manipulation through technology mediation, resulting in the constitution of a new reality comprising specific characteristics of both the user and the artifact. One can say that the ensemble of affordances or the capability matrix constitutes of technological mediation as a whole between a specific artifact and its user.[51] Since the affordances of the artifacts are decided and incorporated by the 'figure', the choices made by the 'figure' contribute significantly to the artifact's mediation of perception

[44] Conti and Sobiesk (2010), pp. 278–279.

[45] Norman (1988), p. 228.

[46] Norman (1988), pp. 23, 197.

[47] Verbeek (2005), p. 3.

[48] Ihde (1990).

[49] Kiran and Verbeek (2010), p. 416.

[50] Norman (1988), p. 51.

[51] Kiran and Verbeek (2010), p. 409.

and action.[52] A linkage is thus established with the notion of constitutive normativity ingrained in the infrastructure of the blockchain artifact.

5.4 Shaping Actions and Intentionality

Technology, in the form of an identifier, guides the perception of the users by amplifying or reducing certain features of the artifact.[53] Through technological intervention, a design can induce the user towards a specific use or distract the user from perceiving it. While identifiers do not have any direct coercive effect on the user, they guide and manipulate the perception of the user to shape the understanding of an artifact. These identifiers also mediate the ability of the user to form a precise mental picture of how the artifact functions and what the user should do with it.[54] With the power of design mediated by code, the user can go beyond the perception of the actual affordances of the technology to append their actions and inactions within the artifact's spatial domain.[55] Technological intervention in the reality of constructs, in terms of perception and behavior, illustrates 'an important aspect of the non-neutrality of technology'[56] and indicates the substantial authority that the 'figure' enjoys who decides the interventions.

When the conception of perception is extended to security and privacy, in the case of blockchains, 'perceived privacy' assumes a crucial role because of the anonymous nature of the self-sovereign identity-based blockchain applications. While the concept of privacy can be described as the ability of the user to govern the provisions by which their personal information is collected and consumed, 'perceived privacy' is explained as the power of the users to regulate information and divulge selective information about themselves.[57] The degree to which blockchain users feel that the applications mediated by code protect their privacy may have a significant impact on their trust in the providers. Designing the technology in such a manner that it discloses information collection procedures will increase users' feelings of assurance and trust. As Norman said, it is necessary to 'make things visible'.[58] Having clear privacy terms, which state how a firm uses user data and information, predicts attitudes and trust in an application. The point is if blockchain users perceive that a blockchain application will safeguard their information, their trust in the blockchain systems and applications will be positively influenced.

---

[52] Robertson (2002), p. 311.

[53] Ihde (1990), p. 72.

[54] Norman (2013), pp. 26, 31.

[55] Cohen (2012), pp. 21, 23.

[56] Verbeek (2005), p. 131.

[57] De Filippi (2016), pp. 4–6, 10–11.

[58] Norman (1988), p. 188.

In contrast to the technological intervention for shaping perception, which amplifies or diminishes the comprehensibility of real affordances, the technological mediation for shaping action induces or restrains certain human behaviors by creating a new environment whose rules are mediated by code.[59]

Rather than just requesting a specific type of action, this kind of intermediation uses logical or physically persuasive force on the users in the form of 'logical constraints'.[60] Actually, the regulative nature of code becomes very apparent in this case since code can facilitate in favor of the coercion of action as compared to the just identifiers provided by the written legal norm. In the case of blockchains, mediation in action by code is observable in 'traceability', which refers to the ability to locate where a product comes from and its entire track throughout the distribution chain. The 'code intermediating action' in a blockchain acts as a persuasive force on the users by ensuring that the information on the blockchain is 'fixed' and immutable and cannot be changed by any malign party, thereby providing transparency and accountability of any misuse.

Code personifies a specific idea of the intention of the 'figure' about the usage of the artifacts. The rule of code can be referred to as 'procedural scripts for choreography of behavior activity',[61] which illustrates how the 'figure' envisages using the artifact. While the artifact's affordances or disaffordances are designed, usually three elements of the 'script', namely, the framework for behavior, the actors involved,[62] and the space for action,[63] based on the anticipated use of the artifact and the strategic business plan the 'figure' strives to adopt, are considered by the 'figure'.[64] When code is a manifestation of political interests, its technological design might have important implications for individuals.[65]

The aforesaid concepts of inscription, or procedural scripts, are related to the 'technological intentionality' of the 'figure', where technologies encourage the use of certain aspects of the artifact that are distinctive from all the contingent possibilities. This concept can be explained with the example of a pen and a word processor.[66] While neither the pen nor the word processor can predetermine the mode of writing with certainty, both the designs nevertheless 'promote or evoke a distinct way of writing'.[67]

Artifacts develop 'intentionalities and inclinations within which use-patterns take dominant shape' through the provision of 'procedural scripts' for the purposes

[59] De Filippi and Hassan (2016). https://firstmonday.org/ojs/index.php/fm/article/view/7113/5657. Winner (1980), pp. 121–136.

[60] Norman (1988), p. 86.

[61] Akrich (1992), p. 205. Latour (1992), p. 225.

[62] Latour (1992), pp. 160–168.

[63] Akrich (1992), p. 208.

[64] Van den Berg and Leenes (2013), p. 67.

[65] Winner (1980), p. 127.

[66] Ihde (1990), pp. 141–142.

[67] Verbeek (2005), pp. 114–115.

of orchestration of behavioral activity.[68] Here, intention generally refers to the inclinations or directions that influence the usage of artifacts.[69] While technological artifacts can be designed and used to promote or block certain user behavior, these may not deliver the expected results. In fact, their implications can be appreciated fully when the historical and social contexts of their use are known.[70] The way technology is used by 'the user group' is also important. Hence, intentionality also refers to the intent of the user and the mechanism through which the artifact intermediates the user's interactions with society by influencing the user's ability to function.[71] Since the artifact mediates the sense of agency of the user and the possible interactions of the agency, the line between subjectivity and objectivity has been blurred.[72] When the user attempts to achieve something, his or her perception of what can be done or cannot be done is mediated by the artifact, and thus, the understanding of the self and the co-constituted world is also influenced by that mediation.[73] Thus, the artifact's technological mediation comprising of affordances and disaffordances determines the way the user and its world move—the operation is mutual and bi-directional.

Different configurations of mediation can make possible different actions depending upon the configuration of the artifact, the user, and the context of use. Though artifacts are designed for a purpose, that purpose also depends on their contextual use by the user. In our everyday lives, there exists a wide range of technology-mediated 'regimens' of influencing behavior. However, there are still numerous uncertainties surrounding the characteristics and extent of technological-mediated regulation. From this point of departure, Leenes inquires

> if intention is an essential element of behavioral modification, or do unintended consequences of design, for example, a CD player not being able to play DVDs even though the discs appear identical, also qualify as behavioral modification? Can a wall socket be considered a form of technological-mediated regulation, and if so, what does it regulate? While wall sockets and plugs do restrict the user's ability to use appliances abroad, is this a form of regulation in the context the users are concerned with or discussing?[74]

This illustration indicates that the 'figure' does not have ex-ante control over the mediating effect of an artifact entirely. Nevertheless, the 'figure' would 'inscribe scripts and delegate responsibilities' in and to the artifacts and create one particular configuration of normativity through deductive reasoning, which excludes others to some extent.

Therefore, in a way, before defining the area of activity of an artifact and making design choices, the 'figure' has to determine the threshold between what can or

---

[68] Ihde (1990), p. 141.

[69] Verbeek (2005), p. 114.

[70] Winner (1980), pp. 123–127.

[71] Ihde (1990), p. 25.

[72] Ihde (2009), p. 9. Verbeek (2005), p. 161.

[73] Cohen (2012), pp. 13–26. Verbeek (2005), p. 116.

[74] Leenes (2019), p. 1.

cannot be interpreted by the user. This threshold is 'the gulf of evaluation', which reflects

> the amount of effort that the user must exert to interpret the physical state of the system and to determine how well the expectations and intentions have been met. The gulf is small when the system provides information about its state in a form that is easy to get, is easy to interpret, and matches the way the users think of the system.[75]

Thus, affordance is a crucial notion to analyze and assess the inscriptions of code that mediate the user's fundamental connections with the world, serving as the foundational element of inscription and technological mediation. Since the actual disaffordances are fundamentally ingrained in the technological intentionality of the 'figure', the design of the artifact must afford to inscribe specific 'procedural scripts' for the choreography of behavioral acts for a particular user. Conversely, if certain actions are to be excluded, the 'figure' must either omit the affordances needed for such actions or disafford them for a particular class of user.

The similarities between the perceived and actual affordances of the artifact that demonstrate technological intentionality provide an opportunity for the user to adapt its response to the pre-set script of the artifact.[76] However, if the 'actual' affordances of the artifact are beyond the intended 'procedural script' of the 'figure', the user will not be able to execute anything with the artifact that the 'figure' did not presuppose. The user will be able to enjoy freedom through the provisions of actual affordances and their identifiers, of course within the wider constraints of the artifact's mediation, on the 'space' left by the 'figure', intentionally or otherwise, for creative interpretation and action. This constraint is different from a 'condition' in the sense that 'neither is it an external limit or imperative' and does not rationalize or legitimize the action of the user. In fact, constraints do not suggest the way the users should act but leave no option than to act.[77]

The affordances that arise due to constraints refer to the context-dependent relationships between an artifact and a particular user and are not just fixed attributes of the artifact. The 'figure' anticipates these affordances while considering the 'procedural script for choreography of behavioral activity', 'film-script', or 'use-pattern' for the user. For instance, the 'figure' implements the smart contract with the 'procedural scripts' affording interaction among multiple parties, humans or machines. Such interactions are mediated by a blockchain application, controlled exclusively by a set of immutable and incorruptible rules embedded in its source code. It is only through the affordances provided by the 'figure' in the preset script that users are able to act upon, even though within the constraints; without such affordances, there will be no scope for interactions within the user interface.

---

[75] Norman (1988), pp. 50–51.

[76] Kiran and Verbeek (2010), p. 415.

[77] Prigogine and Stengers (1996), p. 74.

5.5 Normativity in Technological Mediation

The technological normativity spectrum presents to be 'harder' at one end that offers no choice and 'softer' at the other end, that is, more recommendatory in nature than coercive.[78] In 'harder' normativity, the artifact's scripts are said to be wired-in or rigid, meaning the user does not have any option but to go along with the rule of code norms offered in the artifact.[79] For example, digital interfaces, as in social media platforms such as Facebook or Instagram, evaluate and decide whether the users shall be provided with access to all the features of the database or not. Earlier, Facebook had only the 'like' button with a thumbs-up. With the introduction of 'emojis', users can now express different emotions on this platform. By disaffording a 'dislike' button and restricting emotional expressions through 'emojis', Facebook compelled its users to behave in a manner it preferred. The user interface of Instagram also controls the activities of its users by not permitting the use of hyperlinks in picture descriptions. Such design choices are consciously adopted by social media platforms to compel their users to abide by their rules so as to influence and regulate user behavior. Rules are unambiguously defined in code and are applied instantaneously at runtime without giving any further opportunity to ponder over the rules.

Blockchain relies on code and smart contracts to devise a new normative order to regulate individual actions and transactions. The code-based rules, which provide affordances to users to formalize contractual agreements, are enforced through these smart contracts that are self-executing and self-enforcing.[80] These blockchain-based smart contracts cannot be stopped arbitrarily unless they are codified to do so. Further, because of its 'rule-fetishness' behavior, it may not be possible for a single party to upgrade these code-based rules even for smooth execution. This 'rule-fetishness' is a crucial aspect of technological normativity. In fact, rule-fetishness, representationalism, instantaneity, and obscurantism are central elements of the *crypto-legalism* feature of blockchain.

The above scenario illustrates that technological design choices regulate the actions and behaviors of users by imposing certain rules through codes. In many ways, code has become synonymous with the law; it permits specific actions, prohibits some actions, and imposes certain actions.[81] The structure of blockchain technology reflects a higher level of regulation that Lessig envisages. Extending beyond Lessig's arguments, the design choices considered in blockchain technology are, in fact, design choices for the rule of code norms of regulation. As many scholars have argued, the original blockchain is not value-neutral; it is the manifestation and

[78] Van den Berg and Leenes (2013), pp. 74–75.

[79] Kesan and Shah (2006), p. 583.

[80] Hassan and De Filippi (2017), p. 90.

[81] Lessig (1999), pp. 35–45.

reinforcement of particular norms and values over others.[82] Besides, applications of this technology may further transform social relations in a way that follows the systems' rigid and non-negotiable features. The shared capacity between institutions and blockchains for being normative entities indicates the possibility of understanding blockchain trust in terms of the features of institutional trust.

At the 'softer' end of the spectrum, the artifact's code nudges the user towards a specific modus operandi while allowing the user to indicate choices beyond the default configuration.[83] However, the 'figure' deliberately puts in codes to restrict this notional scope for exercising autonomy and to discourage the users from exercising their choices by making default settings very 'unwavering'. Making a forced decision during installation or setup without suggesting a preferred alternative is one way to reduce this impact.

To give an illustration, there can be a spectrum of technological control over motor vehicles, ranging from 'soft' to 'hard'. In the 'soft' end, warning devices alert drivers when they exceed speed limits or encounter changed traffic conditions. As the technology becomes more aggressive, data—such as excess speed calculations and distance covered during speeding—can be transmitted to a central registry. The hard end of the spectrum consequently allows for perfect prevention by remotely disabling the vehicle or imposing speed limits through braking system modulation.[84]

Enterprises will frequently interpret even stringent laws that demand the safeguarding of user autonomy in ways that covertly—or overtly—serve their own interests over those of the user.[85] This relates to how design practices are evolving in the modern era. One example of this is the interface subtly embedded with dark patterns, which look like they offer notional choice but are really meant to grab end users' attention. Such an act is often referred to as affordance of 'operant conditioning',[86] which is quite the opposite of the notion of 'libertarian paternalism' of nudging.[87]

The 'softer' edge of the normativity spectrum facilitates the procedural script to support not only interpretation and reinvention by the user but also 'resistance', which is limited to the inherent boundaries of its spatial domain.[88] If the user does not know an affordance, then the user cannot avail the affordance, making the role of identifiers particularly relevant. The inbuilt business model of the artifact will decide the degree to which it is multistable. To illustrate, the inscription of *500px* can be formulated to upload photos to be viewed and commented on by other

[82] De Filippi and Loveluck (2016), p. 16. De Filippi and Hassan (2016). https://firstmonday.org/ojs/index.php/fm/article/view/7113/5657.

[83] Kesan and Shah (2006), pp. 591, 596.

[84] Brownsword (2019), p. 10. O'Malley (2013), p. 280.

[85] The GDPR privacy notices are one example of this. See Wachter (2018), p. 436.

[86] Van den Berg and Leenes (2013), pp. 71–72.

[87] Van den Berg and Leenes (2013), pp. 72–73.

[88] Van den Berg and Leenes (2013), p. 77.

participants[89] through a set of affordances for selecting an image, editing it, assigning a title and tags, and publishing it on an application platform. Even if there is a great amount of impedance, the user cannot rewrite the inscription for that application. Nevertheless, inscriptions offer some scope for reinterpretation, resulting in new possibilities unintended by the 'figure' of the application.

The 'density' of the constraints on the user behavior diminishes progressively as one shifts from the harder end of the technological normativity, that is, the most 'rule-fetish' of the code norms, to the softer edge of the spectrum.[90] A particular threshold point chosen on this scale denotes a vital design choice in the development of an artifact, indicating the distinctive affordances based on their normative effect. Moreover, affordances existing on the spectrum can be characterized under 'request, demand, refuse, allow, encourage, or discourage'.[91] These characteristics provide useful insights into the notion of affordance and facilitate an instinctive and unlearned appreciation of the relationship between the technological artifact and the user. It is apparent that the 'harder' affordances of 'request, demand, allow, and refuse' resonate with the wired-in functions of the technology. Conversely, where the artifact's affordances are designed around nudging, it is likely to find mechanisms of encouragement and discouragement. The design of an artifact represents a blend of these features since once the code is programmed in and choices are inscribed, a soft, hard, rule-fetish, or multistable form of normativity comes into existence.

5.6 Normativity in Technological Design

Constitutive rules are those rules that specify the process by which a construct or 'thought object'[92] might come into being. This means that if the essentialities are not fulfilled, then the construct will not be able to come into existence. Contrastingly, regulative rules only seek action or inaction by an individual or a cohort. However, a regulative rule has no competence to impose that requirement directly; in this case, the individual must accept the request and act accordingly. The spectrum of technological normativity is concerned with the theoretical distinction between the aforesaid constitutive and regulative rules. In the case of the design of artifacts, code can initiate both constitutive and regulative normativities. Here, the 'figure' plays a role in deciding the threshold between the two. Interestingly, Hildebrandt observes that it is better to differentiate between constitutive and regulative techno-social arrangements

[89] 500px is an application similar to Instagram for posting photos and is used among the photographers community to showcase their art.

[90] Hildebrandt (2015), pp. 41–60.

[91] Davis and Chouinard (2016), p. 241.

[92] Weinberger (1986).

> if only to make clear that technology does not necessarily rule out choice in comparison to law.[93]

Buchanan's constitutional approach establishes a system of normativity, combining constitutive and regulative elements, to guide engagement in the blockchain. This normativity, communicated through computer programming code in the format of smart contracts, mandates compliance from all users. Transactions failing to adhere to the rules encoded in the blockchain will face non-execution, while those conforming to these norms will successfully proceed. The (implicit) constitutional framework afforded by blockchain not only ensures self-execution and self-monitoring but also underscores the pivotal role of normative principles in shaping and regulating interactions within decentralized systems.[94] The fusion of constitutive and regulative normativity exemplifies the intricate balance between structural foundations and behavioral guidelines in technological design.

In the context of constitutive and regulative rules, the 'plastic' characteristics of the rule of code attain relevance, especially within the blockchain realm, since this plasticity creates numerous rules that allow and restrict certain user behaviors through technological normativity. Thus, the inscriptions, affordances, and disaffordances embodied in the design of an artifact can be constitutive or regulative in nature.[95] A set of constitutive affordances determines the existence of the artifact, its nature, form of interface, platform, or physical dimensions. Therefore, when the user desires a specific functionality, it will not be available to the user if the same feature is not allowed by the constitutive norms of the code. Thus, specific disaffordances and procedural scripts may function above the constitutive affordances of the artifact.[96] A corollary of this is that design invariably entails the prioritization of a single technical constitution or a specific configuration of normativity,[97] favoring it over the multitude of possibilities that code is inherently capable of accommodating.[98] Of course, when considered from the perspective of regulative normativity, the user has a certain degree of choice within the spatial domain set up by the code. However, such 'regulative latitude'[99] always functions within the parameters of constitutive rules beyond which no choice is allowed.

Due to their inherent attributes, such as autonomous operations, tamper-proofness, incorruptibility, and resilience, blockchain-based systems are being described as 'alegal', a term that stands for something that is neither legal nor illegal. These systems operate beyond the bounds of legality, challenging the conventional legal orders within which they operate. Such 'alegal' acts can be executed by

---

[93] Hildebrandt (2008b), p. 175.

[94] Rajagopalan (2018), pp. 365–372.

[95] Hildebrandt (2008a), pp. 177–178.

[96] Akrich (1992), pp. 208–209. Lockton (2006b). https://architectures.danlockton.co.uk/2006/10/22/disaffordances-and-engineering-obedience/.

[97] Weizenbaum (1976), pp. 37–38, 113.

[98] Grimmelmann (2005), p. 1723.

[99] Yeung (2008), p. 88.

the technological design of blockchain-based systems through appropriate affordances. However, such a capability does not render these blockchain systems 'alegal' by virtue of being unregulatable 'forces of nature', as articulated by Wood.[100] As a matter of fact, all these blockchain systems are inherently administered and regulated by humans, who function within the law, social norms, and certain economic priorities. In this context, the 'figure' possesses the ability to shape behavior by opting for affordances that are primarily regulative, employing less 'rule-fetish' mechanisms that allow users to modify default configurations mediated by code or redefine the space beyond the 'figure's' predictions. This emphasizes that the behavioral disaffordances, which may include features being incorporated, disabled, or hidden within the artifact, are contingent upon the 'figure's' choices. The discretionary powers exercised by the 'figure' play a crucial role in constituting the behaviors of users.

5.7 Technological Governance and Constitutional Dynamics

While the behavior of the user is shaped, that is, enabled and constrained, by the normativity embedded and expressed in the design of the artifact, the 'figure' is also subjected to normativities expressed in more fundamental, infrastructural elements of the design process.[101] This means that the 'figure' is susceptible to the consequences of disaffordance, procedural scripts, and mediation within the design environments, which they themselves use to create artifacts meant for users—

> designers often think of themselves as typical users; after all, they are people too, and they are often users of their own designs.[102]

The 'figure' positioning itself as a type of user[103] wields ultimate power by crafting tools and coding methods. As the creator of the programming language, the 'figure' decides what can be done by the 'figure' as a user. However, considering the 'figure' as a user can be misleading and specious. The 'figure' tends to project its 'own rationalizations and beliefs onto the actions and beliefs of others'. But the 'figure' as a professional

> should realize that human belief and behavior are complex and there is no substitute for actual users.[104]

The expertise required to be the 'figure' is different from the expertise needed to be a user; the 'figure' is often an expert with the artifact which they are designing,

[100] POW Media (2015). https://www.youtube.com/watch?v=Zh9BxYTSrGU.

[101] Karavas (2009), p. 463.

[102] Norman (1988), p. 155.

[103] Vismann and Krajewski (2007), p. 90.

[104] Norman (1988), p. 155.

while the 'user' is an expert at the job they are trying to execute with the artifact.[105] The 'figure', particularly engineers and managers, believe that since they are humans, they can also design something for other humans as good as the trained interface experts.[106] The fact is that designers require vocal advocates for the end users of the interface.[107] Thus, the 'figure' starts developing an artifact within a design environment that abounds with procedural scripts and disaffordances, which mediates the product development process.

In blockchain, the 'figure' has to distinguish between 'choice of rules', and 'choice within rules'. Constitutional politics that concerns choice within rules enforces boundaries around the sphere of ordinary politics, such as the type of blockchain, mode of verification, etc. For the purposes of this book, the 'choice of rules' is essential since it is about consensus at the level of code or protocol. As the technology is put to use, and many bugs are observed, the 'figure' would like to remove these issues by modifying or upgrading the code. However, consensus is needed among the group of network users and the 'figure' to effect the changes. The 'choice of rules' concept is deeply ingrained in the code infrastructure of blockchain right from the beginning. Though the pioneer 'Bitcoin' constitution was coded by an individual and was not decided collectively by the network users, its author had embraced an open-source system, permitting other 'figure' to propose changes to the code or upgrades to the core software, acceptance of which would depend upon consensus by all the network users. Thus, any proposal for a new set of rules or changes to the existing set of rules or protocols in Bitcoin requires to be agreed upon by the nodes within the network in order to take effect. In fact, since the development of Bitcoin, the choice of rules has been an evolving process within an open-source network.

The descriptions and inscriptions within blockchain technology define the structure within which the 'figure' executes the regular 'parliamentary' functions and behaves as the *de facto* constitution. The power of the 'figure' is subservient to the normative power of design that encompasses the technological 'constitution'. Much like a legal constitution, the technical foundation impacts the entire design process, creating a technological 'constitution' that extends to the artifacts built upon it. This gives legitimacy to the design works of the 'figure' and imposes boundaries on the 'figure', which can be leveraged for normatively sought-after purposes. Similar to the way the activities of the legislative body are bound by the constitution *ex-ante*, the formulation of the legitimate rule of code is determined by its design environment.

The preceding discourse explores how 'the rule of code' establishes and governs the conduct of users, by elucidating concepts of affordance, disaffordance, inscription, description, and technological mediation. In instances where a design significantly dictates behavior, it bestows a greater share of power upon the 'figure', elevating the influence of code over legal frameworks. A potential reorientation of

[105] Gould and Lewis (1985), p. 300.

[106] Riley and McConkie (1989), pp. 225–228.

[107] Norman (1988), p. 156.

power towards the user becomes achievable by embracing regulative normativity over constitutive norms. As Norman said,

> technology is still young, still exploring its potential. Most programmers, though fluently, write programs that do wonderful things but that are unusable by the user. They are surprised to discover that their creations tyrannize the user. There is no longer any excuse for this. It is not that difficult to develop programs that make visible their actions, allow the user to see what is going on, that make the set of possible actions visible, and display the current state of the system in a meaningful and clear way.[108]

Therefore, a pivotal consideration in this transformation lies in discerning the modus operandi by which the creation of user-centric affordances is legitimized through the inherent rule of law values embedded in the 'figure'-facing affordances, resembling a technologically oriented interpretation of the principles of legitimacy and the rule of law.

References

Agre PE (1994) From high tech to human tech: empowerment, measurement, and social studies of computing. Comput Support Coop Work 3:167

Akrich M (1992) The description of technical objects. In: Bijker WE, Law J (eds) Shaping technology/building society: studies in sociotechnical change. MIT Press, p 205

Baldoni M et al (2006) Modeling the interaction between objects: roles as affordances. In: Lang J et al (eds) Knowledge science, engineering and management. Springer

Berg A et al (2020) Blockchains and constitutional catallaxy. Const Polit Econ 31:188

Brownsword R (2019) Law disrupted, law re-imagined, law re-invented. Technol Regul 10

Cohen JE (2012) Configuring the networked self: law, code, and the play of everyday practice. Yale University Press

Conti G, Sobiesk E (2010) Malicious interface design: exploiting the user. In: International World Wide Web Conference Committee (IW3C2), p 273

Davis JL, Chouinard JB (2016) Theorizing affordances: from request to re-fuse. Bull Sci Technol Soc 36:241

De Filippi P (2016) The interplay between decentralization and privacy: the case of blockchain technologies. J Peer Prod, Issue no. 7: Alternative Internets

De Filippi P, Hassan S (2016) Blockchain technology as a regulatory technology: from code is law to law is code. 21 First Monday. https://doi.org/10.5210/fm.v21i12.7113

De Filippi P, Loveluck B (2016) The invisible politics of bitcoin: governance crisis of a decentralized infrastructure. Internet Policy Rev 5

De Filippi P et al (2022) The alegality of blockchain technology. Policy Soc 41:358

Gibson JJ (2014) The theory of affordances. The ecological approach to visual perception. Psychology Press, p 127

Gould JD, Lewis C (1985) Designing for usability: key principles and what designers think. Commun ACM 28(3):300

Grimmelmann J (2005) Regulation by software. Yale Law J 114:1719

Hartzog W (2018) Privacy's Blueprint: the battle to control the design of new technologies. Harvard University Press

[108] Norman (2013), p. 180.

Hassan S, De Filippi P (2017) The expansion of algorithmic governance: from code is law to law is code. Field Actions Science Reports. J Field Actions 88
Hildebrandt M (2008a) A vision of ambient law. Regul Technol 175, 178
Hildebrandt M (2008b) Legal and technological normativity: more (and less) than twin sisters. Techne: Res Philos Technol 12:169
Hildebrandt M (2015) Smart technologies and the end (s) of law: novel entanglements of law and technology. Edward Elgar Publishing
Ihde D (1990) Technology and the lifeworld: from garden to earth. Indiana University Press
Ihde D (2009) Postphenomenology and technoscience: the Peking University Lectures. Suny Press, p 9
Karavas V (2009) The force of code: law's transformation under information-technological conditions. German Law J 10:463
Kesan JP, Shah RC (2006) Setting software defaults: perspectives from law, computer science and behavioral economics. Notre Dame Law Rev 82:583
Kewell B, Adams R, Parry G (2017) Blockchain for good? Strategic Change 26:429
Kiran AH, Verbeek PP (2010) Trusting our selves to technology. Knowledge Technol Policy 23:409
Korenhof P et al (2021) Steering representations—towards a critical understanding of digital twins. Philos Technol 34:1751
Kshetri N (2017) Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommun Policy 41:1027
Latour B (1992) Where are the missing masses? The sociology of a few mundane artifacts. In: Bijker WE, Law J (eds) Shaping technology/building society: studies in sociotechnical change. MIT Press, p 225
Leenes R (2019) Of horses and other animals of cyberspace. Technol Regul 2019:1
Lessig L (1999) The law of the horse: what cyber law might teach. Harv Law Rev 113:501
Lessig L (2006) Code Version 2.0. Basic Books. <https://tigerprints.clemson.edu/cgi/viewcontent.cgi?article=1183&context=cheer>
Lichti CW, Tumasjan A (2023) 'My Precious!': A values-affordances perspective on the adoption of bitcoin. J Assoc Inf Syst 24:9
Lockton D (2006a) Architectures of control in product design
Lockton D (2006b) Disaffordances and engineering obedience. Architectures by Dan Lockton. https://architectures.danlockton.co.uk/2006/10/22/disaffordances-and-engineering-obedience/
Longford G (2005) Pedagogies of digital citizenship and the politics of code. Techné: Res Philos Technol 9:68
Metzger MJ, Flanagin AJ (2013) Credibility and trust of information in online environments: the use of cognitive heuristics. J Pragmat 59:210
Narayanan A et al (2020) Dark patterns: past, present, and future: the evolution of tricky user interfaces. Queue 18:67
Norman DA (1988) The psychology of everyday things. Basic Books
Norman DA (1999) Affordance, conventions, and design. Interactions 6:38
Norman DA (2013) The design of everyday things: revised and expanded edition. Basic Books, p 11
O'Malley P (2013) The politics of mass preventive justice. In: Ashworth A et al (eds) Prevention and the limits of the criminal law. Oxford University Press, pp 273, 280
Ogut A (2023) "Stay Out of My Way!": the impact of cookie consent notice design on young users' decision. In: Moallem A (ed) HCI for cybersecurity, privacy and trust. Springer
Pfaffenberger B (1992) Technological dramas. Sci Technol Hum Values 17:282
Prigogine I, Stengers I (1996) La Fin Des Certitudes: Temps, Chaos et Les Lois de La Nature, vol 77. Odile Jacob, p 74
Rajagopalan S (2018) Blockchain and Buchanan: code as constitution. In: Wagner RE (ed) Buchanan J. M: A theorist of political economy and social philosophy. Palgrave Macmillan
Riley CA, McConkie AB (1989) Designing for usability: human factors in a large software development organization. In: IEEE International Conference on Systems, Man and Cybernetics, vol 1, pp 225–228

Robertson T (2002) The public availability of actions and artefacts. Comput Support Coop Work (CSCW): J Collab Comput Work Pract 11:299
Scarlett A, Zeilinger M (2019) Rethinking affordance. Media Theory 3:1
Shin D, Hwang Y (2020) The effects of security and traceability of blockchain on digital affordance. Online Inf Rev 44(4):913–932
Shin D, Park YJ (2019) Role of fairness, accountability, and transparency in algorithmic affordance. Comput Hum Behav 98:277
Stutzman F, Hartzog W (2012) Boundary regulation in social media. In: ACM Conference on Computer Supported Cooperative Work (CSCW '12), p 769
Van den Berg B, Leenes RE (2013) Abort, retry, fail: scoping techno-regulation and other techno-effects. In: Hildebrandt M, Gaakeer J (eds) Human law and computer law: comparative perspectives. Springer, p 67
Verbeek PP (2005) What things do: philosophical reflections on technology, agency, and design. Penn State Press
Vismann C, Krajewski M (2007) Computer juridisms. Grey Room 29:90
Wachter S (2018) Normative challenges of identification in the internet of things: privacy, profiling, discrimination, and the GDPR. Comput Law Secur Rev 34:436
Weinberger O (1986) The norm as thought and as reality. In: MacCormick N, Weinberger O (eds) An institutional theory of law. Springer
Weizenbaum W (1976) Computer power and human reason: from judgment to calculation. W. H. Freeman & Co., pp 37–38, 113
Winner L (1980) Do artifacts have politics? Daedalus 109(1):121
Wood G (2015) Allegality. POW Media. https://www.youtube.com/watch?v=Zh9BxYTSrGU
Yeung K (2008) Towards an understanding of regulation by design. In: Brownsword R, Yeung K (eds) Regulating technologies: legal futures, regulatory frames and technological fixes. Hart Publishing, pp 79, 88

Chapter 6
Crypto-Legalism in 'the Rule of Code' Architecture

6.1 Concept of *Crypto-Legalism*

Legalism can be of two types: strong and weak; the rule of code's characteristics epitomizes the features of strong legalism and brings about the issue of unlegitimized regulations based on code and the assertion that code is inferior to law. Regardless of the intent of the 'figure', how vicious or virtuous that may be, this does not insinuate that the 'figure' harbors a legalistic ideology when making choices for designing the blockchain infrastructure. The 'choice architecture' plays a role not only in the space of legislation where the precept needs to be legitimized for it to fit within the democratic realm of the regulating process,[1] but such inclination towards choice architecture can also be seen in the production stage of the code in some cases. In the rule of law adhered State, where legislations are subject to transparent discussions, uninhibited dialogs, and negotiations, the terms and conditions of citizenship need to be legitimized. In the case of the rule of code governed State, the codes that govern the citizens are characteristically obscure and invisible. This is attributable to specific technological aspects and also to the fact that many of the codes arbitrating the lives of the citizens are proprietary in nature. A rule of code environment persuades, provokes, adapts, and, if required, coerces the users to agree to the norms of commercialized cyberspace,[2] which takes place in the absence of the democratic debate and legislative process of interpretation, contestation, and remediation. This process of drawing parallelism demonstrates the reproduction of the ideology of legalism in the ontological architecture of the code—in fact, the technological 'is' of code is merely the replication of the ideological 'ought' of legalism. The premise of the present discussion is rooted in the credo that legalism is undesirable for the holistic aspect of the rule of law, which is being increasingly

[1] Wintgens (2002a, b), p. 2.

[2] Berman (2017).

A. Bisoyi, *Blockchain and Legitimacy*, Law, Governance and Technology Series 77, https://doi.org/10.1007/978-3-031-98712-0_6

considered as the primary threshold for the democratic State. It follows that mechanisms aimed at alleviating legalism- through the conventional legal discipline- might also enrich and supplement the cognate sphere of code-based 'legislation'.

The notion of *crypto-legalism* has been developed from the fact that blockchain-based self-executing smart contracts and decentralized (autonomous) organizations enforce their own rules on the parties through code norms programmed into their respective architecture and are detached from the traditional legitimacy process. The idea of *crypto-legalism* shows that the code's *rule-fetishness*—dependence on austere, binary logic instead of interpretable requirements—and legalism are closely related subjects. The *crypto-legalism* mandates citizens to follow the rules as they are imparted to them without providing the citizens with the opportunity to contest or enquire about its effectiveness or legitimacy without seeking answers to questions about the origin or source of the questions; it does not take into consideration the holistic interpretation of the rule of law norms.

This new coded-legal constitution shapes the creation of the technology and its deployment, resulting in regulating the functionalities of the final product as well as the behavior of the user; the software regulates the online behavior of users, similar to regulating real-world behavior through physical architecture. It is what Lessig referred to as 'architecture'—the code, hardware, communication protocols, and structures that regulate human behavior—where rules are imposed, not through sanctions and not by States, but by the architecture of the particular technology space.[3] In other words, a rule is defined through the code that governs the space.

The principal reason for developing the idea of *crypto-legalism* is to deal with how the characteristics of legalism apply in the context of *lex cryptographica,* even though it may seem incongruous to the regulative capacity of the rule of code from the analytical perspective of legalism. However, the analogy between legalism and *crypto-legalism* is far more profound than it may first seem. Firstly, legalism is *apropos* of the written rules to be followed. Code, due to its rule-fetishness, is rigid and leaves no room for interpretation and elucidation. Secondly, written rules are considered to be the representation of reality as per the ideology of legalism. The *lex cryptographica* not only represents but also comprises of the empirical and legal realities that are confronted by the users or even cannot be comprehended. Thirdly, rules under the domain of legalism reveal the 'background truth' and are envisaged as something unaffected by time. Analogously, the rule of code endowed with characteristics such as normative ubiquity, instantaneity, and immutability at the point of execution dissolves time. Fourthly, in legalism, the provenance of the power of the sovereign is camouflaged so that individuals who are affected by the laws remain unaware or gloss over the political reasons behind its promulgation. These norms are considered as 'just existing', and individuals are expected to adhere to these rules without questioning. Likewise, in the computing topology, a concealment curtain has been established due to non-transparency of the code and the promulgation of laws pertaining to trade secrets and confidentiality of commercial practices—the

[3] Lessig (2006), pp. 123–130. Lessig (2003), p. 4.

technical and legal-economy obscurantism acts as a veil to conceal the 'sovereignty' of those programming.

Lex cryptographica in the configuration of code institutes and controls assorted forms of users, and in doing so, it not only exemplifies the ideology of strong legalism but also solidifies and augments it far beyond what the conventional legal domain can accomplish. Such a view implies not the freedom of the user but that of the 'figure' and promotes the attitude of instinctive following of rules enforced by the rule of code. *Lex cryptographica*, expects the citizens or user participants not to bother about its nuances and rather to abide by the rules offered to them. This is different from how it is in the legal sphere, which, due to the presence of the interpretative aperture, creates a gap between the pronouncement of legal norms and adherence to its requirements where such an ideology of strong legalism can be notionally challenged by the citizens or rejected by societal values. In contrast, the rule of code does not even provide a prospective crevice for resistance; some standards of technological normativity are intrinsically present 'by default'. As the ground rules and the boundaries of the playground are predetermined at the inception stage, the user can hardly do anything to amend them, even though they are cognizant of what they are. Not only are they made to 'not think about it', but they are also not allowed to fathom what it is that they are not thinking about.

Having said that, it must be acknowledged that code is universal—its presence can be realized everywhere, and its manifestation in infrastructural and artifactual levels is experiencing growth inexorably. This can be seen with various blockchain adoptions where there are experiments of integrating the same with daily mundane jobs by developing sophisticated low-power infrastructure and diversifying into the domain of connected applications. In reality, the technological revolution is increasing our dependency on code and data infrastructure more and more, and it seems that the hype around the development and deployment of code and the consequential increasing reliance on it will not subside anytime soon. It is said that 'technologies invent us as we invent them'.[4] As the distinction between offline and online content gets blurred, it has become imperative to safeguard their rights and the competence of the citizens to probe the innovative normativities that the rule of code enforces. As universalization of code would lead to realizing the next generation of virtuality, more concrete steps are required to not surrender the offline capacity of the individuals to influence and have some say in the process of code-making as it reinvents human behavior.

[4] Nørskov (2015), p. 189.

6.1.1 Blockchain Code Rules Represent 'Reality'

Legal positivism and jusnaturalism, though they offer different philosophical perspectives on law, share a common view to the extent that legal norms represent reality. In the case of jusnaturalism, the law of the sovereign is valid if it reflects the universal knowledge and substantial underlying norms of nature. As for positivism, enactment of law is a prerogative of the sovereign, and representationalism is not very evident. Both Hobbes and Rousseau claim that sovereign actions based on the social contract are valid, and therefore, the laws derived from it are also valid. This is the result of their epistemological form of philosophy. Representationalism, therefore, is connoted as the elementary abstract hypothesis of these theories and conjectured as a critical aspect that identifies legalism.[5]

The manner in which the rule of code-driven blockchain applications establishes normativity based on rules is certainly distinct from the approach taken by the legal system. The blockchain establishes 'an ontological status of novelty' as compared to the so-called 'reality'.[6] In a 'generative and systemic sense', many aspects of our actions and thoughts, as well as the 'reality', are interwoven in blockchain technology.[7]

This decentralized technology connotes the potential for enhanced possibilities in our lives and our capacity to influence and construct reality. Taken to the extreme, blockchain normativity constitutes a 'new and foundational mode of configuring reality'.[8] This technological normativity presented by the blockchain can have an immediate impact in a way unlike the legal normativity since the latter is necessarily constrained by its textual embodiment, while the instantiation of the rule of code is not so limited. The regulatory strength of the legal norms is restricted by its manifestation in the written script, which creates a hermeneutic interpretative gap between the requests made for the script and the interpretation of the rules of the script by the receiver and how it chooses to reflect on them in their behavior.[9]

The standards embedded into the rule of code of the regulating architecture are different from the standards manifested in textual legal rules. One of the differences is that the

> binary logic of technical standards is not subject to the uncertainties arising from the inherent indeterminacy of language that plagues the use of rules.[10]

Another difference is its rule-fetishness.[11] The code can be considered to occupy a position subordinate to law, as it lacks the capacity to promulgate rules in a

---

[5] Wintgens (2006), p. 4.

[6] Swan and De Filippi (2017), p. 17.

[7] Swan and De Filippi (2017), p. 17.

[8] Swan and De Filippi (2017), p. 17.

[9] Hildebrandt (2008b), p. 172.

[10] Yeung (2008), p. 92.

[11] See this chapter, Sect. 6.2.1 for more details.

fundamental manner by offering users explicit precepts for interpretation and behavioral adaptation. Further, taking cognizance of the rule of code's representationalism does not provide for any dogmatic exegetic space for connecting its rules with any debated concept of 'truth' or empirical reality. The codes and their rules work very differently. They serve as influential tools that transpire behavioral possibilities as well as limitations from the commencement stage, exhibiting diversified degrees of normative force. The 'figure' may only inscribe the rule of code into the artifacts *ex-ante* to have a default response to avoid failure in unforeseen events.[12] The artifacts do not constitute the Austinian commands that mandate adherence or the *ex-post* representative normative benchmark of the society, which serve as a criterion for evaluating the standards of conduct. This results in the hermeneutic interpretative gap between the written script of the legal rule and its tangible effects on the behavior in the material world, experiencing diminishment. Further, there is 'the halting problem' being faced by the 'figure'—whether the algorithm will run infinitely or halt is not known to the 'figure' *a priori*. Any simulation of possibilities with regard to the performance of the artifact will always remain incomplete as contrasted to the conventional law, which is probabilistic, not deterministic in unforeseen circumstances.

The magnitude of the dissolution of the hermeneutic gap is profound, yet its obliteration in the virtual world is normal and easy, and not through malignity or intentional obscurantism but plainly by the very nature of the mechanism of the apparatus. Since the rule of code is a direct constituent of the artifact, this seeming gap can be easily dissolved as they are not simply isomorphic but, in fact, at least the same at the micro level. Code enables the conception of the programming language or script, which marries both words and actions at once,[13] so what was 'ought' to simply become 'is' or, at least, will be, which results in the collision of rules and reality. These code-based technical rules embedded in the blockchain determine what people can or cannot do in a specific setting more effectively than the applicable laws. It, thus, does not merely denote reality but vigorously establishes it, which means that the behavioral possibilities are the constituents and are not simply controlled by the rule of code. If it is possible to break down legal rules into an 'if … then' instantiation, then the code exemplifies and amplifies this reality, provided that this is how they have been expressed from the inception.[14] The translation of the legal norms, which were once normative, upon translation into code becomes rules that are descriptive and not regulative; that is how the system, its components, and the users will predictably function. Thus, normativity evolves into descriptiveness. This provides an illustration of rule-following that possesses machine-like heteronomy characteristics that do not draw much attention. In a sense, the rules and their promulgation do not have any difference between them; the rule of code simply establishes reality, which is unlike the case for law, where the complaisant

[12] Yeung (2008), p. 92.

[13] Latour (1992), p. 225.

[14] MacCormick (2007), p. 24.

nature of its mode allows for a latitude of interpretation between norm and reality. In a blockchain environment, the smart contract is an example of a codified representation of a real-world legal document. Here, the code is equivalent to the actual contract agreed by two parties, and beyond this rule of code no additional contract exists.[15] It is a fictional real-world contract that becomes the basis for enforcing contractual terms in a court of law. For easy comprehension, a natural language code of contract may be prepared, but as far as legal enforcement is concerned, only code is acceptable.

The rule of code requires to be analyzed at more than one level of ideation—the rules on the conceptual level or the macro level (referred to as conceptual code rules) and rules representing the technical commands within a certain programming language at the micro level (referred to command code rules) to understand which level is important for manifesting the norms into actual programming code. The former level is specifically essential to ponder metaphysically at the macro level, which focuses on *ex-post* outcomes while comparing the instantiation of rules inscribed in code with the legal norms from which such rules have been developed, which may also be referred to as a techno-regulation level[16] at times and is ultimately what matters. This could include design patterns, architectural decisions, and overall system behavior, and understanding these conceptual code rules is crucial for aligning the code with the intended goals and functionality. However, the specific material aspects of the technical commands at the micro level which are the elementary units of the normativity, ultimately implementing the code,[17] must not be intentionally disregarded. This involves understanding the syntax, semantics, and best practices of the chosen programming language. Analyzing rules at this level is essential to ensure that the code is correct, efficient, and maintainable. While it could be burdensome to concentrate on the finer points of the individual commands in source code, it is at this level where the operations take place, and therefore, to some extent, it merits a closer look. Analyzing the rule of code at both the macro and micro levels is essential because a failure at either level can lead to issues. If the focus is only on the macro level where the conceptual code rules are considered, the code may lack correctness or efficiency. If the emphasis is only on the micro level where the command code rules are considered, the code may adhere to the syntax but fail to meet the intended design goals. Since it is the actual programming code that executes the conversion of normativities, which is designed without the knowledge of all its effects, there is a need to find an apposite ideation balance between the individual directives and the technological normativities and their limits that cause the action or the effect in the physical world.

The individual code commands that are executed regardless of the nature of the after-effects (positive or negative) can be interpreted as a rule in terms of the affordance or disaffordance of a given value embedded into the system, in a manner that

[15] Bodó et al. (2018), p. 311.

[16] Leenes (2011), p. 143.

[17] Asscher (2006), p. 61.

the way the code functions, guides the behavior of the user, influencing how they interact with the system based on the inherent capabilities or limitations encoded within the commands. Let us examine the command code of a simple login system:

```
def authenticate_user(username, password):
    # Check if username and password match in the data-
base
    if is_valid_user(username, password):
        # Grant access
        return "Access Granted"
    else:
        # Deny access
        log_invalid_access_attempt(username)
        return "Access Denied"
```

The command code rule providing affordance dictates that if the provided username and password match a valid user in the database, access is granted. However, if there is no match, access is denied, and an invalid access attempt is logged, thus providing disaffordance to an individual to access. The added logging of invalid access attempts represents a rule that signifies the importance of monitoring and recording unauthorized login attempts. This reflects the idea that the command code rules are not just about granting or denying access but also encompassing the importance of security measures, considering values of legitimacy, which denotes that command code rules also follow the conceptual code rules. The act of logging invalid attempts can be viewed as a rule in response to values related to system security.

When the command or conceptual code rules fall short of representing the values of legitimacy, more often, the 'figure' is of the view that the rules representing those values need not be taken into account as they are not considered important. This abstract aspect can be observed when technologies are designed in such a manner that privacy issues are not addressed during the development and application of the code, which can be viewed as tantamount to embedding a rule into the system, conceding that in the scheme of things, privacy is not the prime concern and in fact is inferior to other values. Since infringement of privacy is considered an acceptable outcome of the use of code, such technologies actually influence the perceptions about proper and acceptable behavior.[18] Adapting this formulation, it may be said that the code can and ought to be made harmonious with those values by offering specific affordances, such that the probability of normativity of code artifacts being illegitimate is diminished correspondingly. It is not necessary to look directly at the source code to understand the normativity that the code imposes.

It can be beneficial to link the traditional conception of various ingredients of 'legal' rule with the normative structure that command code rules institute and put

[18] Leenes and Koops (2006), p. 191.

into practice. This approach of sustaining a comprehensive sensitivity to the code's effects can help avoid narrowing the focus down to what the 'figure' purports the code's functionality is. More so, it is imperative to ponder not merely about the anticipated normative effects of an artifact but about all possible unanticipated outcomes. It becomes a substantial cause of concern if and when those effects weaken the legitimacy of the code's normativity. Instead of limiting our thoughts to what the 'figure' intends to do with the code, a relational emphasis on the theory of affordance and postphenomenology compels us to consider the actual operations and effects produced by the code itself.

6.1.2 Constitutive and Regulative Rules

Analyzing the rule of code across different ideation levels requires acknowledging if such rules are constitutive or regulative in nature when understanding the legalism within the code environment. This aspect of understanding the rule of code as constitutive or regulative rules flows from the legal jurisdictions where the rules are either constitutive of recognized institutional actions, establishing the conditions under which these actions can take place, or rules that intend to influence or control behaviors that could occur independently of any rule, seeking to manage pre-existing practices.[19]

In most cases, code rules are more constitutive. However, in cases where the user is encouraged to behave in a particular way and many digital systems are available that permit an array of behaviors for the interaction of users, it is possible for the rules to be regulative. One such example is social networks, which *ceteris paribus* provide users with an expansive scope on content and size of text, audio, video, and image elements that the users can upload. Yet, this supposedly unrestricted liberty to upload also has constitutive limits, such as 'only a certain quantity of data can be uploaded', or the code will recognize and be operative only if text, images, or video files are in specified formats. For everyday usages, these limitations will not be noticeable or approachable, and so the user would remain oblivious of their existence, even though such boundaries are always present. Also, if the digital system is embodied with constitutive normativity to a greater extent compared to regulative rules, the 'figure' exercises more control in defining the nature of that behavior. Seemingly, this approach facilitates being more profitable since limiting the regulative space granted to the users enables them to concentrate on behavior that is favorable commercially. Augmenting the scope of the contingent regulative framework in lieu of the constitutive framework entails the expectation of further probable conditions, which results in increased coding and, hence, incurs increased expenditure in its creation, support, and maintenance. This would push commercial enterprises to

[19] Hildebrandt (2008b), pp. 172–173.

adopt a constitutive rather than a regulative approach while designing code-based systems.

Regulative rules are aimed at regulating activities that are independent of the rules, such as the possibility to drive at a certain high speed, even though there exist regulative rules that forbid over-speeding, while constitutive rules create a possibility to execute specific actions. For example, marriage as an institution cannot exist autonomously without the existence of the constitutive rule that is responsible for its establishment.[20] Constitutive rules can be said to be inventive and multiplicative, while regulative rules are restrictive. For example, the rules of a game (be it soccer, basketball, or chess) do not regulate what is already happening; rather, they constitute the game. Outside of the realm of its constitutive rules, a game does not exist. If the rules of a game are ignored, even if people play something, it cannot be said that they are playing the intended game. It would not only be outside the domain of the general institution of the game but also be beyond the provisions of any given game.

The notion of the 'institutional fact' is derived from the differentiation between socially constructed 'specifics' and 'brute facts' that are present in empirical reality. Let us say A attends a soccer match between her favorite home team and a foreign team. A brings her dog with her. When the ball crosses the line into the cage, both A and her dog observe that fact. But it is only A and not her dog, who is able to observe the fact that A's home team has scored the goal, and subsequently when the spectators all cheer, A's dog only becomes frustrated and uneasy. So, the first fact, that a ball crosses a line into a cage, is called a brute fact, and the second fact, that A's home team has scored a goal, is called an institutional fact. These two facts represent the 'same' fact from two different perspectives. In other words, while brute facts are 'observer-independent', institutional facts are 'observer-dependent'. An institution, therefore, reflects an organization or composition acknowledged within the appropriate community or organisms; for example, a university empowered to confer doctoral degrees is an institution as its character is borne of certain attributes that are inculcated, monitored and maintained over a timeline by those who have the relevant authority to do so and can act as an institution-agency.[21] Institutional facts do not exist independently as they are observer-dependent and owe their origin to the shared institutional world. They can only be instituted by adhering to the conditions consented to by the members of the appropriate community. Such institutional facts are the result of the creative process of the constitutive rules. While legalism holds that the constitutive rules of law that bring into existence the system of institutional facts are 'out there', the other aspect is seeking answers to designing those constitutive rules. Consequently, there is tension between the two elements, which makes it necessary to delve into these conceptual notions to understand the means to design the rules.

[20] MacCormick (2007), pp. 36–37.

[21] MacCormick (2007), pp. 35–37.

It is possible to organize constitutive rules in a hierarchy to establish an essential or fundamental framework (sometimes referred to as a constitution), within which other rules can be made. The legitimacy of the legal rule is derived from some basic acts that operate in the backdrop to validate norms that are endorsed at a later stage. In law as well, just like any game, the constitutive rules are necessary to introduce institutions, which include arrangements—contracts or marriage, and agencies—university or local bodies, and abstract institutional things—patents.[22] In the case of marriage, the requirements stipulated in specific constitutive rules define the legal institution of marriage, and by following these rules, the arrangement of marriage as an institutional fact becomes a reality. Marriages that take place beyond this institutional legal structure are not considered a legally recognized institutional fact.

While these institutional facts crafted through constitutive rules exist in reality within the law's institutional order, the rules of *lex cryptographica* in blockchain are 'brute' in the sense that they are just basic and instinctively present and are part of the architectural framework of the system. It can be said that the immutable and predetermined nature of code-based rules embedded in a blockchain, akin to the laws of nature, establishes a predefined framework that can either empower or constrain users and therefore, when the notion of rules attributes to the discrete instructions given to a system, then such instructions are 'brute facts' manipulating the empirical reality at the level of the system's hardware. The code-based rules become less 'brute', when viewed from the notion of ideation, opening up the possibility to have multiple courses of action to the user. The scope and magnitude of this prerogative, which is conceded to the user, depends on the intentional and unintentional affordances expressed in the design; however, whatever level of flexibility the design accords, it needs to be incorporated from its origination. This means that code-based rules are constitutive of our behavior[23] and represent the inventive aspect of the constitutive structure of normativity-generation. Ultimately, in a rule of code domain, constitutive rules do not empower the users to create the appropriate normative constructs, such as a contract or will, but the 'figure' responsible for programming and developing the code is vested with the authority to creatively institute a pertinent form of normativity, technical and non-legal, constituting the terms of the user behavior, seemingly that the users were subject to the sovereign power of the 'figure'. The rule of code limits the user autonomy materially by demarcating the boundaries of the behavior within the realm of the system. The architecture of the code organizes the rules on an *ex-ante* basis and, by default, does not permit any modification at the discretion of the user.[24]

In contrast to traditional legal rules that are interpreted by the judiciary and applied on the merit of the case, code-based rules are written in the rigid and formalized language of code and do not offer any benefit of flexibility and ambiguity of

[22] MacCormick (2007), pp. 35–36.

[23] Hildebrandt (2008b), p. 174.

[24] Brownsword (2005), p. 1. Lessig (1996), p. 1403.

natural language.[25] In the context of blockchain applications for human rights, while the rule of code's unambiguous and deterministic nature ensures transparency and trust because of the smart contracts and facilitates fair distribution of resources in a tamper-resistant manner, the immutability of code in a blockchain can become a challenge in cases where amendments are required to adapt to evolving human rights standards or address unforeseen ethical concerns. Similar to the world order we observe, the limitations and enablement of code are like laws of nature.[26] In the case of smart contracts, blockchain ensures the integrity of code and its secure execution in a decentralized network. Though smart contracts can achieve and exhibit immutability to the extent of host blockchains, such immutability is not always desirable. One major drawback of immutability is that it prevents any alteration of the code of the smart contract, even for the rectification of errors and introduction of new functionalities.[27] The lack of flexibility in the rule of code may hinder the system's ability to respond promptly to changing circumstances or to incorporate nuanced interpretations of rights, potentially limiting its effectiveness in complex, dynamic situations. Thus, the code of the smart contract may deviate from the intended objective by not being able to correctly convert natural language into code. Such divergence may also occur due to the incompetence of the 'figure' or due to the inherent difficulty of translating legal obligations into a series of 'if … then' statements. In the real world, it becomes essential for the parties to agree to a version in the event of any divergence.

The design of a system's code defines and constitutes the user's interactions with the system, enabling certain acts while blocking others. When considered from the context of the legal realm, the users are the target of these conceptual code rules, where how they behave is constituted. This is said to be the level to be focused on, where the rules for the macro level are constituted by a greater level of rule adherence, that is the individual code commands, where the instructions contained in the code target the system and intend to produce user technological normativity at the macro level. Without the micro-level unconditional rule-fetishness of the source code that regulates and guides the system, the macro-level metaphysical rule-fetishness of the artifact that dictates the user will never come into existence. Even though the ideation level allows for some latitude for contingent behavior, it is not possible for the interactional possibilities to exist due to the delimiting nature of the rule of code courtesy of its rule-fetishness. The system has no choice or space for arbitrating whether to follow the instructions given to it or not as compared to the technological normativity that might be impeded by the user. In other words, the pattern of technological normativity that the user is subjected to is essentially a construct due to the authoritarian rule adherence system. Code in its multiple avatars, such as a script describing what will execute, a protocol for systems to follow,

[25] Hassan and De Filippi (2017), p. 89.

[26] Bamberger (2009), p. 669.

[27] Low and Mik (2020), p. 170.

or a framework for navigating the user's behavior, indicates the crucial points at which empirical *modus operandi* can be introduced to ensure legitimacy.

6.2 Characteristics of *Crypto-Legalism*

For *ex-ante* mitigation of blockchain code(d) space, *lex cryptographica*, through design, it is essential to introduce checks and balances that can assist individual autonomy in the positive as well as the negative outcomes. Since characteristics such as rule-fetishness, instantaneity, and obscurantism are significant features in the designing of checks and balances, it would be appropriate to discuss these characteristics of legalism, demonstrating how the cryptographical form of legalism goes far beyond the imagination of the dogmatic notion of strong legalism.

6.2.1 Rule-Fetishness

The strong legalism notion embedded in the code execution of a blockchain application ensures a dualistic treatment of rules *qua* rules, suggesting categorical and straightforward enforcement of rules, possibly indicating a dichotomous, yes-or-no application without much room for comprehension and interpretation or complexity. This characteristic contributes to increased transparency and trust in human rights processes within the blockchain, fostering a secure environment where predefined rules are applied consistently, predictably, and executed without any hindrance. However, the strict dualistic treatment of rules may limit its adaptability to evolving scenarios. For example, if a blockchain-based human rights application employs smart contracts with fixed, predefined criteria for granting asylum, the lack of flexibility in the code could impede the system from accommodating exceptional cases or evolving geopolitical situations that necessitate a more nuanced evaluation of individuals seeking refuge. The rule-fetishness nature of the rule of code, which mindlessly executes the code, might hinder the system's responsiveness, potentially leading to a lack of flexibility in addressing complex human rights issues and impeding the pursuit of a more context-sensitive purpose behind the employment of the blockchain.

Strict rule-fetishness makes the process incompatible with the principle of legal certainty, which is the central requirement for the rule of law, that insinuates that rules should be clear, predictable, and understandable. This aspect of legal certainty flows in from the provision of continuity and flexibility in the application of the written law, which is dynamic and autonomous such that the law results in providing justice and effectiveness despite heterogeneous changes either in the social or

technological infrastructure of the society *à la mode.*[28] In the legal sphere, the norms of the written law have their own space beyond that of the author: the author is never in a position to know how the transcript will be perceived; at the same time, the intention of the author can also not be presupposed. The legislator is given preordained *carte blanche* to use the text and turn the process of legal code enactment into an ingenious one rather than just a monotonous process.[29] This creative customary *modus operandi* of embodying law into written text reflects the postulation of legal certainty, implying a clear and unambiguous understanding of the law when interacting with the text. The legislation process also acknowledges that when citizens interact with an apparatus, they normatively have the affordance to choose either to approach the text from a legalistic viewpoint or opt for an alternative perspective.[30]

In contrast, the execution of code represents the monotonous application of the rules. The enactment of code does not, normally, provide any scope for interpretation that is available in the legal sphere. The rules laid by the 'figure' are the rules that are to be followed by the user as well as by the machine. This rule-fetishness is drawing the bridge between *crypto-legalism* and legality, where orthodoxly, one end is fixed, has absolute rules with no means of interpretation, and the other end is partly or wholly unhinged, has comparatively flexible rules that allow for wider engagements but without detailing the structure to achieve the objectives. In this bridge, the code is positioned on the fixed rule end side. While written laws are constructed with the intention that with the passage of time and the ambiguity of language, it would provide the space where contemplation of evolving social norms or exceptional circumstances are permitted, whereas code demands strong and rigid precision and rigor, which is not native in analogue law.[31] In the absence of such precision, the code will be incapable of execution.

'Rule-fetishness' is a term used to explain the codes' nature to impose an unambiguous, demarcated, and pre-decided set of inflexible rules at the juncture of execution. Upon execution, the program follows these hard-edged rules such that nothing outside the pre-determined and limited ontology of the code will respond to changes, and everything that meets the internal conditions will be mindlessly executed. This is true even in cases where a pragmatic approach would demand consideration of other conditions so that the nature of the execution of code or the facts associated with it could be altered.

The mindless execution, the hard-edged inflexible rules, and the limited ontology that a given artifact can represent may be conceived and structured to admit different likelihoods. But the primary locus is the rule-based design choice, which is the rule-fetish structure of the code, that is pertinently binary in nature.

---

[28] Hildebrandt (2008b), pp. 171–172.

[29] Hildebrandt (2008b), p. 172.

[30] Hildebrandt (2016), p. 1.

[31] Howell and Potgieter (2021), p. 545. Kennedy (2024), p. 170. Zsolt (2022), p. 67.

> In blockchain, the final smart contract source code needs to be compiled into machine-readable bitcode and uploaded on the blockchain. From then onwards, the binary computer code is the only definitive source of truth for the smart contract.[32]

This indicates the difference between the code(d) rules that the machines follow and what it constructs and operates in the representative world *qua* technological normativity, to which the users are subjected, where they know nothing about anything that lies beyond the border they have created.

The programmed and proximate nature of the code is the origin of the mindless execution of the code. As soon as the code is released in the required operating environment, the program will be executed as many times as possible as long as the *ex-ante* conditions of the rules are satisfied, with insignificant marginal costs. Except for resources for operation and periodical maintenance of the computing and network systems, no human intervention is required.[33] The execution of the code is without consideration of the *ex-post* consequences or any reasons that imply that the code should not be executed. This shows that the ontology of the code is limited, and it is true to say that code 'produces only what it assumes'; the mechanical outcome of the *ex-ante* postulations of the 'figure' is realized whatever may be their intention[34]—the challenge is not the expected misuse of the power of the code, but the inadvertent exercise of that power by the coder.

Regardless of that, such mindlessness of the code is a significant benefit that facilitates rapid innovation where it can be envisaged to execute the complex set of rules in a programmed manner under specific conditions. This aspect of validity hints at catastrophic effects depending on the behavior and ubiquity of the code in question. Although the 'figure' iteratively tests the codes they write to ascertain if their scripts perform as intended and fix the obvious bugs manifested, the possibility of having such bugs or malcontents in a code that ostensibly performs as intended during testing cannot be entirely ruled out since in either case, the system will function though the outcome may not be as intended. In the legal domain, this is obviously undesirable and requires space for interpretation. The laws and regulations, which are well conceived and fabricated, endeavor to take care of a variety of contingencies that are not always predicted by the lawmakers.[35] The ideal condition would be to draft laws and regulations in such a way that the same can be applied in different contexts and situations that are not envisaged by legislators without amending or changing the law.[36]

Even in the case of orthodox legalism, where the legislation might produce a statutory rule that infringes the right of the citizens or creates a loophole for the malady, this rule can then be ignored by those subjected to, and if required, can also be quashed by the judiciary once the malady has been identified. Even in situations

---

[32] Drummer and Neumann (2020), p. 344.

[33] Grimmelmann (2005), p. 1723.

[34] Van den Berg and Leenes (2013), p. 67.

[35] De Filippi and Wright (2018), p. 199.

[36] Dworkin (1982), p. 179.

where strict liability rules are enforced, for example, traffic violations, enforcement still mandates an active process of investigation to provide an opportunity for the driver to justify their actions and plead for leniency, citing the conditions necessitated such action, which modulates a strongly legalistic application of the original rule.[37] However, as the blockchain is self-executing, an automatic response is generated the moment the embedded code is triggered. On the contrary, traditional law requires that unless legal compliance is monitored and ascertained, no rule violation can be sanctioned and enforced. This is because in the rule of law society, human interaction and their ability to apply rules to the actual situations where such violation has taken place, plays a definitive role in the interpretation and enforcement of rules.[38]

The flip side of the mindless execution is that if the precise circumstances for the pre-determined rules in the code are not satisfied, then, notwithstanding any external condition that arises due to the operation that may harmonize with the code-based rule, the rule will never be executed. The rules embedded into a technological artifact would be interpreted in an identical fashion irrespective of the complexity of the set of rules that are being applied, in contrast to human's ability to apply the simultaneous rules with precision. Metaphorically speaking, the 'inflexible hard edges' of technological rules are not vulnerable to blurring.[39] The rule of code domain lacks the 'penumbra of doubt', where the rule of code echoes the subjective interpretations of the 'figure', and not necessarily its established understanding that is appreciated, recognized, and agreed upon by the legislature, courts, or society. There is no possibility of alternative interpretations in the domain of mechanical jurisprudence, which means that the code is incapable of accommodating ambiguity. Any ostensible ambiguity is considered imaginary since it has been intentionally designed so, and the ambiguity exists only at the level of human interpretation rather than within the internal logic of the system. This speaks of the feature that code's ontology is limited and is in line with Hart's conceptualization of the open texture of language and his critiques against unambiguous regulation. In the real world, it is not feasible to conceive all possibilities, and therefore, a mechanical jurisprudence for all the possibilities can be thought of beforehand.[40] Code fits this vision but not as imagined by Hart. In contrast, all human understandings are built on the interpretation of ambiguous 'limited' information, which is filled out by the existing prism of tacit knowledge. While code is only responsive to the rules and representations designed into its ontology or is sensitive to 'intra-systemic meaning',[41] in the case of humans, it refers to the interactions that cross the boundaries between systems.[42]

[37] De Vries and Dijk (2013), p. 89.

[38] Yeung (2008), p. 93.

[39] Grimmelmann (2005), p. 1723.

[40] Hart (1961), pp. 100–110.

[41] Michaels and Paulwelyn (2011), p. 349. Valentinov (2017), p. 386.

[42] Hildebrandt (2021), p. 1.

When the 'figure' writes a code and creates a program, every possible response to a complete array of inputs is anticipated and predetermined for every possible case it may adjudicate. Since 'the algorithm is the rule',[43] the 'figure' relies on the predetermined conditions and responses of the code's execution, and although this concretization will not reflect the empirical world reality, or the essentiality of substantive law, or the legitimacy of normative values. This aspect of code tenders no barrier to its execution on the basis of the ontology that the 'figure' designs their artifact around. Given that it is virtually impossible to foresee all possible situations and to have rules and regulations to deal with all these circumstances, in practice, the laws banking on blockchain systems would have a limited scope than conventional laws. As all the possibilities are not taken care of in a smart contract, it is possible to find loopholes in the system to bypass the rules. Individuals can assess the code of the smart contract and decide whether to trigger the embedded conditions or not so that they would not come under the purview of any given law that has been translated into code.[44]

The traditional contract is subject to interpretation, traditional understanding of agreements, and legal contractual codes, which are dependent on statutes, legal precedents, and principles. In contrast, smart contracts are marked by a lack of context. Therefore, smart contracts need to be self-sufficient by explicitly formulating and embedding code. It may also be said that code reduces the complexity of the contingent world to a set of rules that the 'figure' can embed, irrespective of whether these rules are adequate or appropriate or not, in terms of the number of necessary representations of whatever contexts that the code will eventually operate in. The code responds only to the conditions and rules that are a kind of platonic simulacrum signified by the 'figure', who is only interested in finding answers to an obvious problem through specific technical measures which are contingent upon the inherent business models and the norms and values of the computing discourse of the 'figure'. While doing so, the 'figure' may not evaluate other relevant possibilities, thus limiting to unwarranted specific circumstances and responses. To elaborate, if the 'figure' expects only responses X, Y, or Z to which the system will respond with X1, Y1, Z1 conditions or their combinations, then that is all the code will ever recognize. These conditions engulf the impenetrable sphere that is understood by the ontology of 'inflexible' code, meaning it is rigid and cannot be made sensitive to other conditions or responses without the code being altered. Once the commands are compiled to be executable by the system, the code becomes rigid and 'closed' for good, and no information that has not been represented can be incorporated to alter the nature of the execution.[45] Similarly, if a user desires to add a 'date of birth' record to a blockchain-based ledger, the platform will accept the input data so long as it meets the conditions embedded into the code—even if the said 'date of birth' is not correct. Even if the text of the code is open to scrutiny, there is no scope

[43] Grimmelmann (2005), p. 1723.

[44] De Filippi and Wright (2018), p. 200.

[45] Krajewski (2019), p. 119.

for further interpretation by the users, and to that extent code is legalistic. Even when the user has access to and can understand the source code, there is no other option but to accept the rules as designed and embedded into the code during the course of the code's performance.[46] However, law demands that code must be able to accommodate and interact with systems outside its realms.

The connection between legalism and code-based regulation can be explained through a hypothetical blockchain-based smart-contract-enabled e-bank for lending money (micro-financing). The rules are (i) the borrowers shall make an application with requisite information for each loan, (ii) the loans must be repaid within the due date, (iii) a number of loans availed by a borrower shall be within the specified limit, and (iv) no new loan will be sanctioned to those loan-seekers that have overdue amounts. These rules are translated into code, regulating the e-bank's 'borrowing' system, which is programmed to self-destruct after the predetermined borrowing period has expired. Compared to an 'offline' bank where human facilitators are available for interpretation, the rules in the digital system are 'bright line' that accept no interpretation—once the number of loans or quantum of loan limit is reached, the system self-destructs allowing the user to not loan any further monetary amount, regardless of any external factor such as the user falling sick obstructing him to repay the loan, which could have made the human facilitator make an exception if no due process system is built into the coding framework. Therefore, including the affordance of accountability in the form of 'human in the loop' is a design choice made by the 'figure' and not an obligation.

In the absence of any conditional versions, these characteristics highlight a 'legalism' that is outside the horizon of the strongest of the orthodox legalism, which provides for elide(ification) of the interpretative space in code architecture. Because of the architecture's abrasiveness, rigidity, and lack of critical reasoning, 'the software lies at the rule-bound end'[47] where there is little scope for 'ambiguity, discretion or subversion'[48] as the computer rather than a human makes a program's decision, and there is only a little liberty to reason separately from either interpretation or even identifying the rule.[49] This is indeed why focusing on the production of the code is so important. At this stage, interpretation in a primary precautionary role can identify what critical aspects of the world must be represented and how the representations are limited. It also identifies the implications of code in reality and consequently, provides vital support in the process of designing the code.

[46] Hildebrandt (2020), p. 67.

[47] Schafer (2022).

[48] Bankowski and Del Mar (2016).

[49] MacCormick (2005), chp. 2.

6.2.2 Instantaneity

Due to the *ex-ante* 'rule-fetish' nature of code, exemplified by smart contracts with predefined criteria, where 'the tamper-resistant and automated nature of blockchain-based applications works as a double-edged sword',[50] the technological system cannot, like law, reconstruct its responses considering *ex-post* information or determination that such information is germane. This characteristic is referred to as code's instantaneity which relates to the temporality of code rules execution. For example, in a blockchain system for determining asylum eligibility, if fixed parameters within the rule of code, such as 'rigid adherence to a predetermined list of qualifying persecution categories', strictly define eligibility criteria without flexibility, overlooking geopolitical developments or individual circumstances such as threats or emergencies, the immediacy of code execution of the blockchain system may fail to adapt to evolving human rights situations, potentially denying asylum to those who need protection. Similar can be the case when the blockchain application is used for humanitarian aid services. If the initial criteria are based solely on fixed parameters such as 'rigid income thresholds' without room for reconsideration, such as without the ability to dynamically reassess eligibility based on factors like sudden economic downturns or changes in living conditions, the instantaneity of code execution may hinder the system from adjusting aid allocations in response to emerging crises or evolving needs, potentially leaving vulnerable populations without timely assistance in dynamic human rights situations.

Where the law, being a potential regulator, is unfunctional in situations that lack of presumptions to manifest its stipulations in real-world behavior, the enablement and delimitation of code constructed by the 'figure' manifest their potency before the system is operational. Because, as already discussed, there is no hermeneutic gap between the code script and behavior, which means that the script constitutes both rule and reality, and the conditions of its imposition are priorly arranged and enforced instantaneously, without procrastination and without factoring other possibilities that might have been relevant, at the point of execution. At the moment of freeze, the corpus of specifications, features, and rules (configuration of normativity) can no longer be amended and are contained in the code, and the system compliantly executes it as quickly as it can. The code's exponential execution speed is severe and indecipherable to external triggers or mitigating factors. The code's rule-fetish character, as such, moves away from the legal realm where the law's calculated approach emulates the stabilization of societal expectations.[51] While a code-based approach ensures that no rule is violated unless the underlying technological framework is tampered with, on the flip side, this can also impede the prospect of lawful pursuits. As permissible actions are restricted to predefined conditions,

[50] De Filippi and Wright (2018), p. 201.

[51] Hildebrandt (2008a), pp. 186–187.

there is a possibility that legitimate functions of the user would be hampered due to a code-based rigid framework.[52]

When the instantaneity characteristics and the rigid framework of the rule of code are combined in a smart contract, it may give rise to a situation that is detrimental to the parties involved. If a smart contract that is engaged for tax-related application has a flaw in the code, then its output will be erroneous, and the user may end up paying more tax. Under such circumstances, only judicial intervention appears to be a viable option.[53]

The characteristic of instantaneity, reflected in the code embedded in the blockchain, requires the design of any modifications and amendments to its constitution to be incorporated at the stage when they are supplied to the artifact. Moreover, unlike any regular software, smart contracts cannot simply be patched. Smart contracts are, by their nature, irreversible after contract code terms have been agreed on. However, if all parties agree, one should be in a position to amend contract terms. In this regard, Wright and De Filippi point out that

> People are […] free to decide the particular set of rules to which they want to abide, but after the choice has been made, they can no longer deviate from these rules to the extent that smart contracts are automatically enforced.[54]

These rigid configurations are largely welcomed by the users as a 'natural and immutable fact',[55] as they consider the configuration and responses of the system to be more accurate than a human equivalent, which means that there is some sort of automation bias.[56]

The default configurations may appear natural because of the familiarity of the system or because they are accepted as legitimate since people have become habituated to such arrangements offered by the system.[57] It can be deduced that the 'figure' has significant power over choosing the configuration from the inception to the end while being responsible and accountable.[58] This could potentially lead to the emergence of the modernized version of a totalitarian regime—a society based upon

---

[52] De Filippi and Wright (2018), p. 201.

[53] De Filippi and Wright (2018), pp. 201–202.

[54] Wright and De Filippi (2015), p. 40.

[55] Kesan and Shah (2006), p. 591.

[56] Citron (2007), pp. 1271–1272.

[57] Tien (2003), p. 1.

[58] See Chaps. 8, 9, 10 for further discussion on responsibility and accountability of the 'figure'. In designing and implementing the technology, it is the responsibility of the 'figure' to ensure that the application aligns with the preconditions of human existence and adheres to the fundamental values of the community. Furthermore, the 'figure' must take steps to balance the global commons with community values through deliberative and participatory mechanisms. The book primarily focuses on understanding the intentionality of the 'figure' and presenting them with some normative reference points, where it is the duty of the 'figure' to design with configurations such as legacy switch, sunsetting mechanisms, room for agonism, autonomy, choice, and desirable inefficiency. In this context, questions of accountability arise in relation to the legacy switch and the notion of desirable inefficiency.

a restrictive technical framework that is almost exclusively controlled by self-enforcing contracts, owned and managed by a sophisticated network of decentralized organizations that dictate what people can or cannot do, without any kind of constitutional safeguards or constraints. As such, the default configurations militate against any inquiry regarding more or less suitability of other configurations for the user. Instead, the defaults are admitted as fixed or immutable parameters, making other possibilities impossible or unreasonable.[59] The users, most of the time infer that the 'figure' knows best and thus legitimizes the effect produced by the configurations.[60] More so, many times, it is the case that the users either lack the technical knowledge to scrutinize all the possible tailored options or time to investigate,[61] much less to explore what inducements inspired the 'figure' to choose a particular configuration of defaults or why there is a periodical change in the functional units which do not always have the support of the users.[62]

The 'figure' must also exercise its choice to achieve an equilibrium between the number of defaults, i.e., options that can be changed by the user, and the quantum of pre-set processes since multiple options or a complex interface can add to distractions, eroding the utility of providing a choice.[63] This can result in commercial enterprises allowing for configurable options within the interface, which, upon exercising the option, is an adversary to the user, where the enterprise argues respect for the users' autonomy while at the same time undermining their interest in the face of commercial opportunism. For example, the change introduced into the Google Chrome browser interface at the design level obscures the circumstance under which the user is logged into the Google services, even though the 'block third-party cookies' setting that would normally block such behavior has been activated.[64] Such a setting is also not a default configuration in the mainstream browser, and this privacy-enhancing 'extension' setting needs to be manually enabled by the user; this means that the user must first be aware of the availability of such an option or 'extension', what it does and how can it be enabled.

It is conceivable to determine and augment the subjective value judgments of the 'figure' and the consequential effects of the rules demonstrated in the code when the systems are distributive in nature and are accepted extensively. The 'figure' has an ample amount of latitude in determining how the code ought to function while it is in production, but promptly, as it runs its course, that latitude is frozen,[65] facilitating its exponential augmentation as its outcome amalgamates with simultaneous and successive execution. Drawing a parallel with the legal realm, it is termed as 'inner

[59] Kerr (2017), p. 91.

[60] Kesan and Shah (2006), pp. 611–612.

[61] Kesan and Shah (2006), p. 598.

[62] Tien (2003), p. 16.

[63] Brownsword (2011), p. 1345.

[64] Acquisti et al. (2023), pp. 257–269.

[65] Bamberger (2009), pp. 710–711.

commitments' where technological innovations are akin to the framework for public order.[66]

As technology is like a ticking clock that is unlikely to reverse, it is quite challenging to change or delete the technology from society once it is developed, introduced, and accepted in society.[67] When normativity is at stake, the process that develops 'code is law' becomes a key concern. Due to the lack of a mechanism to make amendments to the code after the closure of the design stage, the normative value of those 'initial commitments' is more significant. These observations incentivize focusing on *ex-ante* programming of code along with its *ex-post* effects.

Even in cases where it is possible to update the code, its instantaneity would mean that its normative effects are in place before the code effectuates. It is imperative that the design is generated in a legitimate manner from its conception. Though code may undergo revisions over time, the fact remains that it is immutable at the point of its compilation, pending certain changes in the future—and that is the reality. Users are compelled to embrace the exact same technological normativity that is defined and encoded in the most recent update. This remains unaltered until the subsequent update, which results in the normativity configurations remaining fixed for a variable period of time. Its updation ability is, hence, dependent on the design possibilities envisioned by the 'figure'.

6.2.3 Obscurantism

The rule of code operates in ways that are 'only' sometimes comprehensible by the 'figure' and not the user. This obscurantism gives way to the postulation that code entails users to 'not to think'. If the users cannot appreciate the rules that influence their behavior, they cannot, in all probability, contemplate whether and how to react to such rules. For instance, in a blockchain system determining asylum eligibility, if the source code governing the decision-making process is intentionally obscured, asylum seekers may find it challenging to understand the specific criteria influencing their application outcomes. The obscurity in the code could lead to a lack of transparency, hindering individuals from comprehending how their asylum claims are evaluated and potentially eroding trust in the fairness and accountability of the system for human rights purposes.

The obscurantism characteristic of the rule of code, as observable in the source code for any application, camouflages the users' experience; examples also include HTML, IP addresses, and web browser software serve as a desirable model of code's self-concealing character. In the case of HTML, it hides the textual data that is eventually responsible for developing the graphical websites that the netizens

[66] Winner (1980), p. 121.

[67] Koops (2008), p. 166.

see.[68] Users can view source HTML code in most browsers, making it somewhat accessible. However, in blockchain artifacts, the compiled code that affects specific rules is not only inaccessible but also inexplicable due to it being in a machine-readable format. Irrespective of the programming language of the code, the system remains obscure; users cannot appreciate the codes and are compelled to just have faith in the system.[69] The user interface of the artifact i.e., the frontend, is far off and kept obsolete because of the multitude of operations taking place at the backend. The simplest operations, such as clicking an image on the webpage, require a host of invisible backend coding. More so, trying to comprehend all the details of every rule followed in the algorithmic process can be very burdensome.

The opaque algorithmic rules do not provide any insight into the decision-making process undertaken by the 'figure' to display information. Since the artifact offers a range of 'optimal' choices, the users are under the illusion of having complete freedom of choice, which, in reality, is controlled by a network of algorithms as per the predefined metrics. It may be noted that the users' behavior within the system's architecture is *a fait accompli* where the users have accepted the default configurations in their original condition such that immutable features of these configurations govern the behavior of those subjected to it within a medley of behavior-delimiting rules that might allow for minimal interpretation, if any. It is a sort of 'blind rule-following'.[70] Such behaviour facilitates achieving compliance by default instead of by enforcing proactively. Thus, the normativity of the code is not dependent on the users and is also perspicuous to those whose behavior is governed by it or even those who have developed it. Moreover, there is no obligation to make it public and understandable to humans. As the complexity of code increases, the rule of code become unintelligible even to those who have programmed them, making it difficult for the user to investigate the rules to which the behavior of the user is subjected.

Traditional laws are interpreted by the judiciary to determine the applicability of a legal rule in a particular situation. Even the law may be reinterpreted if, in the opinion of judges, the standard interpretation of the law is violative of the original intent.[71] In contrast, the core concepts of law, such as 'corporeality, finitude, and authentication', that are fundamental to sovereignty, are challenged by the virtuality of code.[72] Obscurantism poses challenges to the conventional democratic legislative process. The rule of code diminishes the individual's capacity for reflection, giving rise to some degree of instrumentalism that deprives their ability to participate meaningfully in society. This occurs even in situations where the individuals do not accord to what is forced on them by the code rule. Users have no other option but to follow the rules without having any say or authority regarding their formulation. One of the effects of this might be the de-moralisation of the users *qua* citizens,

[68] Longford (2005), p. 77.

[69] Williams and Edge (1996), p. 865. Winner (1978), p. 284.

[70] Bankowski and Schafer (2007), p. 31.

[71] De Filippi and Wright (2018), p. 200.

[72] Vismann and Krajewski (2007), p. 92.

numbing their feelings towards social norms and adversely impacting their ability to be altruistic.[73] The latter point echoes with Fuller's discussion on the morality of aspirations and how it is in conflict with the legalistic morality of duty, in which case the rule comprises of a detailed map of requirements in respect of what is necessitated from the users who would be regulated.[74] By doing away with the necessity to mull over an appropriate course of action, the frequency of broaching such inquiries declines. A community that is entirely dependent on such regulatory frameworks, thereby precluding the opportunity for moral deliberations, ceases to operate as a 'true' moral community anymore.[75] There should always be an opportunity to do good if one is to continue to exercise their reason as a moral actor. In many cases, the opacity of architectural regulation directly impacts the user's awareness and behavior. Such obscurantism keeps the law in a bind as legal norms are unable to obviate any disobedience or contestation of the technological factory default that may arise since the configurations regulating the user behavior are most of the times invisible and also due to non-presence of jurisdiction and court.[76] However, a smokescreen of actual behavior can sometimes be good and not just otherwise; for example, hiding the complex technical behavior can be for the benefit of the user when such a technical behavior is adverse to the interests of the user.

It can be espoused that *crypto-legalism* does illustrate the absolute certainties, concomitantly hiding the same from the user's cognizance under the shroud of obscurantism. It has been suggested time and again that the origin of technology is concealed 'in the state-sponsored program or market-structured order, and its effects are abstruse because it is hard to envision the alternative'.[77] This mystifying function can be drawn parallel to the doctrine of the 'veil of sovereignty' in the legal realm, where it envelops the legislator's work, shielding the sovereign power from the scrutiny of the legal scholars and the citizens,[78] that results in creating a black box within the realm. Not only the supreme source of sovereignty but also the process by which it achieves a result is not to be held in question by the jurists.

In the blockchain realm, the autonomy and authority of the 'figure' are protected by technical as well as legal shrouds. The technical shroud relates to code-based obscurantism, where the shroud is technically encoded and is incapable of being deciphered or lifted by the user *qua* citizens. The legal shroud shields the corporations through trade secrecy and anti-circumvention laws, which puts a constraint on scrutinizing their code development and production practices and thus strengthening their quasi-sovereignty.[79] This enables the exclusive autonomy of the profit-seeking enterprise to be secure, saving itself from the occurrence of real-world

[73] Brownsword (2005), p. 19.

[74] Fuller (1964), chp. 1.

[75] Brownsword (2005), p. 19.

[76] Hildebrandt (2015), p. 12.

[77] Boyle (1997), p. 177.

[78] Wintgens (2002a, b), p. 2.

[79] Schwartz (1999), p. 815.

harm, which might be covered by a technical shroud. The current neoliberal economic stance supports the idea of reallocating the sovereignty from the State to market mechanisms, at the same time concurrently prioritizing such unrestricted technological innovation as a public good.[80] Herein lies the paradox—the tenets of legalism are appealing to a certain extent because they assist in establishing a reference, that is, a line of legal certainty that is profitable to the business enterprise.[81] However, as these enterprises have somewhat mutated into *de facto* legislators of code-driven frameworks, the requirement for certainty has put a restriction on the liberty of the citizens. The reasons in support of such behavior of enterprises are not only the emergence of disparity of regulative power between the State and code but also the absence of stimuli to guarantee that their design processes and products incorporate the standards of the rule of law, especially legal protection and legitimacy aspects, which are inherent to their liberty. In the absence of stimuli, the rule of code that aligns with and promotes business interests but is unfavorable to users is expected to win where the attributes of *crypto-legalism* are easier to put into effect.

Regarding the aim of legality in the rule of law environment, the market fundamentalist cannot be appealed to prevent the 'figure' from exploiting the *crypto-legalism* to advance their own benefits, and therefore, necessary safeguards need to be incorporated at the design stage. Also, since the 'strong' version of legalism not only epitomizes the characteristics of code but also intensifies their features much beyond what has been envisioned in legal literature, such legalism is eminently pertinent in the descriptive analysis of blockchain code. In fact, while these *crypto-legalistic* characteristics generally apply to all types of code in a blockchain-based infrastructure, their severity increases due to the resilient, tamper-resistant, and autonomous attributes of code.[82] It is very important to embed the rule correctly into a smart contract because if it is not, it can be reversed only after judicial intervention.

References

Acquisti A et al (2023) Nudges (and deceptive patterns) for privacy: six years later. In: Trepte S, Masur P (eds) The Routledge handbook of privacy and social media. Routledge, pp 257–269

Asscher L (2006) Code'as law. Using Fuller to assess code rules (2006). In: Dommering E, Asscher L (eds) Coding regulation, essays on the normative role of the information society. TMC Asser, p 61

Bamberger KA (2009) Technologies of compliance: risk and regulation in a digital age. Tex Law Rev 88:669

Bankowski Z, Del Mar M (2016) Images of borders and the politics and legality of identity. In: Nobles R, Schiff D (eds) Law, society and community. Routledge

Bankowski Z, Schafer B (2007) Double-click justice: legalism in the computer age. Legisprudence 1:31

[80] Cohen (2016), pp. 387–388.

[81] Wintgens (2013), p. 4.

[82] De Filippi and Wright (2018), p. 201.

Berman PS (2017) Law and society approaches to cyberspace. Routledge
Bodó B et al (2018) Blockchain and smart contracts: the missing link in copyright licensing? Int J Law Inf Technol 26:311
Boyle J (1997) Foucault in cyberspace: surveillance, sovereignty, and hardwired censors. Univ Cincinnati Law Rev 177
Brownsword R (2005) Code, control, and choice: why east is east and west is west. Leg Stud 25:1
Brownsword R (2011) Lost in translation: legality, regulatory margins, and technological management. Berkeley Technol Law J 26:1321
Citron DK (2007) Technological due process. Wash Univ Law Rev 85:1249, 1252
Cohen JE (2016) The regulatory state in the information age. Theor Inq Law 17:369
De Filippi P, Wright A (2018) Blockchain and the law: the rule of code. Harvard University Press
De Vries K, Dijk NV (2013) A bump in the road. Ruling out law from technology. In: Hilderbrandt M, Gaakeer J (eds) Human law and computer law: comparative perspectives. Springer, p 89
Drummer D, Neumann D (2020) Is code law? Current legal and technical adoption issues and remedies for blockchain-enabled smart contracts. J Inf Technol 35:337
Dworkin R (1982) Law as interpretation. Crit Inq 9:179
Fuller LL (1964) The morality of law
Grimmelmann J (2005) Regulation by software. Yale Law J 114:1719
Hart HLA (1961) The concept of law. Oxford University Press, pp 100–110
Hassan S, De Filippi P (2017) The expansion of algorithmic governance: from code is law to law is code. Field Actions Science Reports. J Field Actions 88, 89
Hildebrandt M (2008a) A vision of ambient law. Regul Technol 175, 178
Hildebrandt M (2008b) Legal and technological normativity: more (and less) than twin sisters. Techne: Res Philos Technol 12:169
Hildebrandt M (2015) Smart technologies and the end (s) of law: novel entanglements of law and technology. Edward Elgar Publishing, p 10
Hildebrandt M (2016) Law as information in the era of data-driven agency. Mod Law Rev 79:1
Hildebrandt M (2020) Code-driven law: freezing the future and scaling the past. In: Markou C, Deakin S (eds) Is law computable?: Critical perspectives on law and artificial intelligence. Hart Publishing, p 67
Hildebrandt M (2021) The adaptive nature of text-driven law. J Cross-discip Res Comput Law 1:1
Howell BE, Potgieter PH (2021) Uncertainty and dispute resolution for blockchain and smart contract institutions. J Inst Econ 17:545
Kennedy R (2024) Rules as code and the rule of law: ensuring effective judicial review of administration by software. Law Innov Technol 16:170
Kerr I (2017) The devil is in the default. Crit Anal Law 4:91
Kesan JP, Shah RC (2006) Setting software defaults: perspectives from law, computer science and behavioral economics. Notre Dame Law Rev 82:583
Koops BJ (2008) Criteria for normative technology. In: Brownsword R, Yeung K (eds) Regulating technologies. Legal futures, regulatory frames and technological fixes. Hart Publishing, pp 157, 166
Krajewski M (2019) Against the power of algorithms closing, literate programming, and source code critique. Law Text Cult 23:119
Latour B (1992) Where are the missing masses? The sociology of a few mundane artifacts. In: Bijker WE, Law J (eds) Shaping technology/building society: studies in sociotechnical change. MIT Press, p 225
Leenes R (2011) Framing techno-regulation: an exploration of state and non-state regulation by technology. Legisprudence 5:143
Leenes RE, Koops BJ (2006) 'Code' and privacy or how technology is slowly eroding privacy. In: Dommering E, Asscher L (eds) Essays on the normative role of information technology. TMC Asser Press, p 191
Lessig L (1996) The zones of cyberspace. Stanford Law Rev 48:1403
Lessig L (2003) Law regulating code regulating law. Loyola Univ Chic Law J 35:1

Lessig L (2006) Code Version 2.0. Basic Books. <https://tigerprints.clemson.edu/cgi/viewcontent.cgi?article=1183&context=cheer>
Longford G (2005) Pedagogies of digital citizenship and the politics of code. Techné: Res Philos Technol 9:68, 77
Low KF, Mik E (2020) Pause the blockchain legal revolution. Int Comp Law Q 69:135, 139
MacCormick N (2005) Rhetoric and the rule of law: a theory of legal reasoning. Oxford University Press
MacCormick N (2007) Institutions of law: an essay in legal theory. Oxford University Press, p 24
Michaels R, Paulwelyn J (2011) Conflict of norms or conflict of laws?: Different techniques in the fragmentation of public international law. Duke J Comp Int Law 22:349
Nørskov M (2015) Revisiting Ihde's fourfold "technological relationships": application and modification. Philos Technol 28:189
Schafer B (2022) Legal tech and computational legal theory. In: Borges G, Sorge C(eds) Law and technology in a global digital society: autonomous systems, big data, IT security and legal tech. Springer
Schwartz PM (1999) Internet privacy and the state. Connecticut Law Rev 32:815
Swan M, De Filippi P (2017) Towards a philosophy of blockchain. Metaphilosophy 48:5
Tien L (2003) Architectural regulation and the evolution of social norms. Yale J Law Technol 7:1
Valentinov V (2017) Wiener and Luhmann on feedback: from complexity to sustainability. Kybernetes 46:386
Van den Berg B, Leenes RE (2013) Abort, retry, fail: scoping techno-regulation and other techno-effects. In: Hildebrandt M, Gaakeer J (eds) Human law and computer law: comparative perspectives. Springer, p 67
Vismann C, Krajewski M (2007) Computer juridisms. Grey Room 29:90
Williams R, Edge D (1996) The social shaping of technology. Res Policy 25:865
Winner L (1978) Autonomous technology: technics-out-of-control as a theme in political thought. MIT Press, p 284
Winner L (1980) Do artifacts have politics? Daedalus 109(1):121
Wintgens LJ (2002a) Legisprudence: a new theoretical approach to legislation. Hart Publishing
Wintgens LJ (2002b) Legislation as an object of study of legal theory: legisprudence. In: Wintgens LJ (ed) Legisprudence - a new theoretical approach to legislation. Hart Publishing, p 20
Wintgens LJ (2006) Legisprudence as a new theory of legislation. Ratio Juris 19(1):5
Wintgens LJ (2013) The rational legislator revisited. Bounded rationality and legisprudence. In: Wintgens LJ, Oliver-Lalana A (eds) The rationality and justification of legislation: essays in legisprudence. Springer
Wright A, De Filippi P (2015) Decentralized blockchain technology and the rise of Lex Cryptographia
Yeung K (2008) Towards an understanding of regulation by design. In: Brownsword R, Yeung K (eds) Regulating technologies: legal futures, regulatory frames and technological fixes. Hart Publishing, p 79
Zodi Z (2022) Algorithmic explainability and legal reasoning. Theory Pract Legisl 10:67

Chapter 7
Decoding the 'Legitimacy' Standards for Blockchain

7.1 Legitimizing Blockchain Design

Existing literature predominantly revolves around shaping the technology by assessing the regulation of and by technology; however, only a few analyze the standards that can legitimize its design.[1] It echoes the skepticism towards viewing the code as law per se and instinctively pushes forward the notion that the code should not be equated with law, emphasizing that legal scholars should regard it primarily as a subject of legal regulation rather than the code being at par with the law. The developmental trajectory of code has been seldom scrutinized, and even less recognized is the exercise of reflection on how regulators could use this process. A study of the production of the blockchain code in parallel to the rule of law jurisprudence makes one realize that the code exhibits *crypto-legalism*—a form of strong legalism, which brings out the 'alegal' *ex-post* normative effect that necessitates the code to be less legalistic.

The commercial purpose of the immutable and decentralized nature of blockchain is to provide a secure and transparent platform, for example, for managing and verifying identities and distribution of resources. While blockchain offers a potential solution to challenges faced by displaced populations or citizens of any State, the rule of code embedded in the technological artifact plays a crucial role in shaping the norms and standards governing the behavior of the users. However, there are potential risks and challenges associated with the *crypto-legalistic* characteristics of the rule of code, especially when blockchain-enabled applications are used for protecting the fundamental rights of individuals, particularly the vulnerable section of society such as refugees. Because of the inherent immutable and tamper-resistant feature of the technology, the rule-fetishness attribute of the code encoded in the blockchain takes the form of the 'extreme' strong legalism where the rule of

[1] Goldoni (2015), p. 123.

A. Bisoyi, *Blockchain and Legitimacy*, Law, Governance and Technology Series 77, https://doi.org/10.1007/978-3-031-98712-0_7

code becomes absolute and rigid, potentially limiting the flexibility needed to adapt to evolving human rights circumstances, such that it becomes nearly impossible to correct the error and address the poor code design at the macro level as once code is programmed and data is recorded, it cannot be easily altered. Of course, the instantaneity of execution of the rules within the blockchain, built-in through an automated smart contract, can expedite processes such as identity verification, which is crucial for refugees seeking assistance and protection. This calls for the sensitisation of the domain of the rule of law jurisprudence to alegal normativity, recognizing its significance alongside traditional legal norms in governing people's lives.[2]

The issue is how to legitimize this alegal aspect of the blockchain code from the perspective of the rule of law. To address this, it is essential to consider both *ex-ante* and *ex-post* perspectives in evaluating the legitimacy of blockchain technology. It is also crucial to highlight the significance of addressing normativity during the design phase of technology, emphasizing the challenges of rectifying issues post-deployment.

7.2 *Ex-post* and *Ex-ante* Legitimacy in Blockchain Code

Since the *ex-ante* characteristics of *crypto-legalism* and legalism per se demonstrate that *ex-post* consequentialism is not adequate to relieve the negative effects in the blockchain environment, the deontology of *ex-ante* legitimacy is imperative,[3] especially in the context of blockchain and its implications on human rights opportunities to guarantee the rule of law. When blockchain is employed for digital identification purposes in vulnerable populations, the need for *ex-ante* legitimacy is underscored by several key factors, one of them being the irreversible nature of the rule of code embedded in the blockchain in the form of smart contracts where its implementation necessitates a thorough examination of normativity during the design and development phase. Once deployed, altering or rectifying the impact of the smart contract becomes challenging *ex-post*, especially when dealing with sensitive external circumstances. The gap between the two levels (*ex-ante* and *ex-post*) is sharp and distinct. While input legitimacy refers to achieving legitimacy through rules and procedures, output legitimacy means determining legitimacy based on the result.[4]

From a normative technology perspective, the primary concern is *ex-ante* legitimacy, which should be accentuated in the development and deployment of blockchain technology. In fact, the activity of cultivating technology is the central emphasis when normativity is at stake. Quite often, it would be too late to probe whether it is acceptable to use such technology in society because, by that time, a

[2] Brownsword (2015), pp. 10–14, 30.

[3] Hassan and De Filippi (2017), p. 89.

[4] Scharpf (1997), p. 18. Scharpf (1999), p. 11.

lot of things have already passed. It is akin to—'the genie may be taken out of the bottle, but never to be put back in'.[5] In fact, one of the important components of acceptability criteria should be the 'rules of the game' criteria in the technology development process.[6]

When evaluating the blockchain system based on its operation and real-world impact, such as in the context of providing humanitarian aid to refugees, the assessment focuses on the *ex-post* outcome. This includes delivering digital identities to refugees and migrants, enabling them to easily access their basic human rights like housing and education, as well as ensuring efficient distribution of aid resources. However, by the time these outcomes are observed, the opportunity to modify the system to address any shortcomings, such as lack of accountability, transparency, or lack of personal autonomy of individuals, may have passed or become limited.

It has been propounded that two fundamental principles namely transparentizing and 'publicness', should govern the code programming;[7] this resonates with the rule of law values. According to the first principle, the rules embodied in code must be able to be understood and ascertained such that they are observable and the architects of such rules can be held responsible, while the later principle suggests that users who are bound by laws must have an opportunity to have a voice in these creations.

Focussing the analysis only on the macro level limits our vision to only the assessments of *ex-post* results, assuming that it can conspicuously detect all adverse effects, which is far from being accurate, primarily due to the code's inherent characteristics of obscurantism. The challenge with such an approach is that it does not directly address the issues of those who program the code. It creates a blockade between the jurisprudential scrutiny and the object of analysis, where lawyers are considered as *ex-post* evaluators of code while failing to recognize the role of the 'figure' as its *ex-ante* creators. The focal shift towards the *ex-ante* level is not only on participation but also in cases where the participatory angle would be minimal, courtesy of the private domains within which the code artifacts are incubated and created. The input aspect hinges more on the mundane ecosystem, where the granular design decisions with respect to the functionalities of the code are emphasized for legitimization. The 'private' programming of code results in the product not constituting the participatory democratic rule of law process per se, but they may be considered as 'inputs' since they are critical integrants of the product, which is the output of the design process and is finally liable for the consequences of the code in the real world. Treating the *ex-ante* standard as the 'nucleus' facilitates examining the design process to make sure that specific design features *in situ* allow for effective *ex-post* judgments and simultaneously abridge the need for judicial interventions, as the *ex-ante* standard configuration is considered more legitimate since its inception.

---

[5] Borges and Weinberger (1984), p. 564.

[6] Koops (2008), p. 166.

[7] Goldoni (2011), pp. 128–129.

The privacy by design scholars have also made a note that when these concerns are addressed at the end of the design cycle, there is no or little scope for maneuvering the completed design. In most cases, such problems are addressed with inelegant and imperfect solutions.[8] Moreso, focusing on the functionalist standards facilitates recognizing that some risky designs may be acceptable as long as necessary measures are put in place to reduce potential harm and the justification for the questionable design choices are verifiable. Such an instructive process can assist in mitigating the risks during the design process to a certain extent, complying with a desideratum that the proposed code must embody the standards of the legitimate normative order. This approach reduces not only the expenses but also the delays when a design is reconfigured *ex-post*.[9]

Such *ex-post* reinforcements are many times ineffectual since the *ex-ante* standards and the features of *crypto-legalism* hinder the potency of such *ex-post* evaluations. Rectification of an issue needs to be assessed from its conception since software development is integrated in nature. Due to the typical character and rationale of architectural regulations, concentrating merely on output legitimacy is often misguided. Further, as it is difficult to reverse the embedded code, the focus ought to be on the processes and stakeholders engaged in developing the technology. In many cases, it is also difficult to know how technology directly or indirectly impacts agents' behaviors, given the opacity of architectural regulation. Lastly, default technology is also important in the sense that defaults are often considered to be a 'natural and immutable fact'.[10]

When choosing normative criteria, 'input-based legitimacy' is a key consideration. It is necessary to take into consideration the *ex-ante* legitimacy, in addition to the outcome that occurs *ex-post,* when the exercise is to import the traditional rule-making or the orthodox rule of law principles into the blockchain environment. It emphasizes that *ex-ante* analysis must be performed alongside *ex-post* analysis, where the *ex-post* measures would continue to be crucial to sustaining a bond with institutional legal processes. This reflects the advocacy for the shift from a 'descriptive to a normative approach'[11] for the rule of code, in opposition to the effects of legalism in a coded world where the normative becomes the descriptive.

[8] Luger and Golembewski (2017), p. 295.

[9] The delays occur ex-post because, after the technology evaluations takes place, it unveils that the code does not address one or more requirements, and as such, it takes time to mitigate the issue.

[10] Goldoni (2011), p. 128.

[11] Bankowski (2001), p. 199.

7.3 Assessing and Managing Legitimacy Standards

The theories propounded by Koops, Leenes, Brownsword, and Hildebrandt set out different narratives on the review and analysis of legitimacy in a technology. While Koops mostly discusses procedural and substantive standards for normative technology, Brownsword's and Leene's work hovers around techno-regulation and technological management, with Hildebrandt advancing the notion of legal protection by design, focusing on exercising user rights *ex-post*.

7.3.1 Standardization Theory

The theoretical foundation of procedural and substantive standards for normative technology has been laid down by Koops, which assesses how the standards that are conventionally applied to law can also be related to norms that are embedded in the technology.[12] Such an approach facilitates moving forward and understanding the standards for normative technology. The process of translating and inscribing a legal norm should be evaluated separately because 'law in technology' cannot be precisely similar to 'law in the books'.[13] The choices available and applied during the translation process are not necessarily made by public authorities who operate within defined checks and balances but by the 'figure' who is responsible for technology development and who is, at best, answerable to technology audit. The rules embedded in technology cannot be equivalent to the rules enacted by the legislation-making institutions. In situations where norm-establishing technologies are employed by public institutions, it is necessary to prioritize the rule of law values, that is, the democratic and constitutional values. Prioritizing rule of law values deserves attention because the conventional checks and balances of the legislative processes are at risk of being undervalued through the utilization of such normative technology.

Instead of following the 'labyrinths' of discussions about 'what is good law' and imposing 'acceptability criteria' based on the theoretical interpretation of the law, a pragmatic-bottom-up approach has been adopted by Koops.[14] His approach toward finding the standards for the acceptability of normative technology focuses on outcome justice or *ex-post* justice. In this method, standards are considered valid because the user accepts the outcome as rational. Although he does acknowledge the importance of procedural justice, in which the standards are valid because appropriate procedures have been followed to find such standards, pointing towards

[12] Koops (2008), p. 166.

[13] Hildebrandt and Koops (2010), p. 428.

[14] Koops (2008), p. 162.

the fact that in normative technology, '*ex-ante* legitimacy' is the primary concern, he does not delve into it.[15]

Koops classifies 'due process, legality, legal certainty, and checks and balances' under the rule of law criteria and considers these to be substantive and not just procedural standards. While the rule of law is the primary standard, 'transparency of rulemaking, transparency of rules, checking alternatives, choice mechanism, flexibility, and accountability' are the secondary standards.[16] This implies that as per Koops, primary standards should be met first before fulfilling the secondary standards.[17] It can be argued that fulfilling the secondary level of standards will result in meeting the primary level. From a computational perspective, it should be feasible to target or embed secondary standards or values rather than targeting the essentially contested umbrella concept of the rule of law in its entirety. Koops pushes towards definitive practices, specifically in his class of secondary standards, which includes justifying choices and possibility of choice, audit, review, subsidiarity, proportionality, optimal-default setting, and context adaptability.[18] Further, Koops prioritizes testing of the standards against concrete technologies. He advocates that such evaluation of standards shall never 'be a straightforward or uncontested exercise'.[19] Indeed, a number of criteria may vary depending on the culture, either in how they are interpreted, e.g., moral norms and democracy, or how important they are, e.g., human rights and autonomy.

Since the emphasis is more on substantive legitimacy in contrast to procedural form and recognizing that procedural standards must survive the temporal landscape as a benchmark, it is crucial to reevaluate the criteria that underpin legitimacy. The formal principles that confer legitimization should strengthen the formulation of all code-based norms, independent of its material characteristics. As a matter of fact, in the context of the rule of law framework, it is a prerequisite for those rules embedded in the technology to be legitimate.[20] An added advantage of focusing on procedure is that it simplifies the standard required since the number of standards at this level becomes limited.

Koops' standardization theory tentatively refers to *ex-post* legitimacy, which corresponds to the thick version of the rule of law. Consequently, the substantive aspects of the rule of law, upon becoming a component of the evaluation, contribute to both the difficulties and the complexity of standards that Koops refers to.[21]

---

[15] Koops (2008), p. 170.

[16] Koops (2008), p. 168.

[17] Koops (2008), p. 169.

[18] Koops (2008), p. 168.

[19] Koops (2008), p. 171.

[20] Hildebrandt and Koops (2010), p. 454.

[21] Koops (2008), pp. 169–170.

7.3.2 *Theory of 'Techno-regulation'*

The dogmatic expression 'techno-regulation' insists on understanding whether 'techno-regulation' is to be considered as regulation or not. In this context, Black's definition of 'regulation', which includes intention and cybernetic control model, has broad acceptance among scholars.[22] According to Black, regulation is a targeted attempt to change or modify the behavior, standards, or goals that aim to produce more or less identified outcomes. In other words, regulation is an attempt to modify the outcomes by deploying various mechanisms to set standards, gather information, and modify behavior.[23] Taking a cue from this definition, techno-regulation can be defined as the 'deliberate employment of technology to regulate human behavior' or 'the technology with intentionally built-in mechanisms to influence people's behavior'.[24]

According to Brownsword, techno-regulation is observed when regulators, after recognizing the desired pattern of behavior without evaluating its morality compliances, secure that behavioral pattern and obliterate options for non-conforming behavior by design.[25] These actions might require the involvement of regulatees themselves, their designs, their products, and the environment in which they work or use these products. Where techno-regulation is observed to be in force, further correction or enforcement is not required. In fact, techno-regulation not only improves the likelihood of detection, prevention, or compliance, but it also ensures compliance by eliminating all options for non-compliance. This definition, which Brownsword reported prior to laying down the concept of technological management, includes only what Hildebrandt has termed 'constitutive' technological features where people are 'forced' to demonstrate certain behaviors and does not include 'regulative' technological features by which technology allows the users to exercise their choice to disobey.[26] Techno-regulation could also be considered as a design modality that blocks any detrimental behavior by superseding human decisions and actions.[27]

Leenes expanded the concept of techno-regulation to include private sectors and States as the producers of code, who are intentionally embedding norms within the technology, affecting human behavior and regulating behavior.[28] The normative intention of the 'figure' is to command and manipulate the behavior of users in a certain way, and for this purpose, technological regulations as instruments must be enacted either by law, as a social norm, or as a market or architecture. Regulation, being a deliberate and strategic action by the regulatory 'figure', aligns with Black's

[22] Yeung (2008), p. 88.

[23] Black (2002), p. 1.

[24] Van den Berg and Leenes (2012), p. 74.

[25] Brownsword (2015), p. 18.

[26] Hildebrandt (2008b), p. 169.

[27] Hildebrandt (2011), p. 223.

[28] Leenes (2011), p. 143.

definition, which emphasizes the importance of a sustained and purposeful effort aimed at modifying the behavior to produce a 'broadly identified outcome'.[29] The distinction between 'is' and 'ought' gets totally blurred when the norms can only be discovered using the artifacts. Thus, in order to have legal status for techno-regulation, it is essential to have the intention of the 'figure' as well as the transparency of embedded norms. Since, quite often, the norms appear to be opaque, the validity of such norms is also debatable. As such, a reasonable view would be that transparency of norms and the processes to which they are subjected to are vital to appreciate the legalities of techno-norms.

Techno-regulation is borne out of both State (regulating norms enacted by legislature) and non-State regulators—the 'figure'—(norms enacted by private contracts or programming code). As a transition of power from legitimate States to the 'figure' in terms of regulation is ongoing, it must be ensured that the actions of the 'figure' are considered legitimate by the users. This can be realized by actively participating in the community discourse, which advocates for open communication and dissipation of essential information.[30] Such legitimacy is required because there is no ambiguity about the legal status of the norms programmed into the artifact while implementing contractual terms in the case of technological norms. While in other cases, such norms may not be legally binding upon individuals, but in this case, they are.[31] This intersects with Brownsword's conceptualization of 'regulatory margin'[32] and Goldon's proclamation that transparentizing and 'publicness' are necessary requirements.[33]

7.3.3 Theory of 'Technological Management'

The theory of 'technological management' was propounded as a means for 'techno-regulation'[34] since technological infrastructures determine the social order.[35] By 'technological management', one means 'the use of technologies—typically involving the design of products or places, or the automation of processes with a view to managing certain kinds of risk'[36] by excluding (i) the actions that might be susceptible to 'coercive' rules and (ii) elements that can be accused of ignoring rules in the area of regulated activities. In technological management, the regulator conjectures a desire for perfect control and elimination of non-compliance by employing a

[29] Black (2005).

[30] Leenes (2011), p. 167.

[31] Leenes (2011), p. 168.

[32] Brownsword (2011), p. 1326.

[33] Goldoni (2011).

[34] Brownsword et al. (2017), p. 3.

[35] Brownsword (2019a).

[36] Brownsword (2015), p. 18.

particular technology, whereas those who are regulated may have only a limited ability to damage, disrupt, and circumvent the technology put in place.[37] Such techno-regulation is acceptable when it adheres to the principles of the rule of law and human dignity, essentially constituting three segments:

> (1) that one's capacity for making one's choices should be recognized; (2) that the choices one freely makes should be respected; and (3) that the need for a supportive context for autonomous decision-making should be appreciated and acted upon.[38]

When transferred to the blockchain environment, this conception proposes that individuals retain and reserve the freedom of choice not to go along with the rule as programmed into the technological infrastructure. Here, the litmus test for appraisal of techno-regulation is 'justification'—'whether we are over-regulating or underregulating'.[39]

When technologies are used to govern behavior in a way that assures a certain outcome, the regulatory environment gradually shifts towards a 'mechanized' community, which is moving away from the possibility of it being within the framework of the rule of law, whereby the members of the community are incapacitated of their moral judgment to make a choice or are being 'demoralized', through the removal of options to exercise their right to freedom of choice.[40] Though the regulation by technological management significantly differs from a normative legal environment, the rule of law principles ought to be applied to it. The power of technological management needs to be exercised with due care. Since it actually forces regulatory compliance, the users should also respect the constraints imposed by it.[41] Moreover, to retain the rule of law ecosystem, the individual should be empowered with the capacity to choose moral signals, that is, respecting the legitimate interests of all, or prudential signals, that is, about one's interest to do it, rather than non-normative signals. An example would be trying to open the door without the required biometric confirmation (enabling the mechanism to open), which is impossible without fulfilling the requirement.[42] Technology management seems challenging not only because it intuitively favors a specific form of alegal and amoral reasoning but also it can circumvent practical reasons absolutely,[43] effacing opportunities for either moral or prudential signals.[44] This results in desensitizing the social norms and, ultimately, the collapse of the rule of law community.[45]

---

[37] Brownsword (2015), p. 28.

[38] Brownsword (2004), p. 204.

[39] Brownsword (2004), p. 205.

[40] Brownsword (2005), p. 4.

[41] Brownsword (2019b), p. 112.

[42] Brownsword (2011), pp. 1323–1324.

[43] Brownsword (2005), p. 13.

[44] Brownsword (2015), pp. 34–35.

[45] Brownsword (2005), p. 19.

A 'regulatory margin' is entailed between the transition from normative regulations[46] towards non-normative regulations[47] to deliberate on the complex regulatory environment.[48] Initially, the main purpose of the 'margin' was to provide an opportunity to amplify the prudential signals at the cost of the moral signals. With time, the margin's function turned down such prudential signals and transitioned to non-normative signals. Now, for the purposes of ratifying the use of technological management before the product is integrated into society, deliberations must take place *ex-ante*. Otherwise, it will lead to the illegitimate use of code which, due to its rule-fetish characteristics of instantaneity (efficient rule enforcement), would compress the 'regulatory margin' that was permitted earlier in enforcement where the friction and conflict due to larger 'regulatory margin' was the driver for affirmative social changes.[49]

For example, when technologies are developed to serve techno-regulatory solutions, there could be two strands—one, a less effective regulation that allows non-compliance to some extent that impacts legitimate choices and rights of the users, and two, an effective regulation that forces us to abandon the dignity of choice. Brownsword's work shows that for the diligent application of techno-regulation, three standards, namely, (1) respect for individual dignity by preserving choices (more the choice, better it is), (2) the trade-off between the regulator and the regulatee while configuring norms, and (3) the necessity to delay 'regulatory margin' that can enable this reciprocity, need to be considered. These standards though laid down as *ex-post* assessment criteria, are very essential in the context of *ex-ante* legitimacy.

While at the policy level, such an approach is appreciated, it does not get along well with the exercises of coding that implement techno-regulations at the micro level. There must be awareness of the decisions taken such that it does not result in unrestrained use of code for regulation; the main purpose of considering *ex-ante* decisions is to appreciate the value of human dignity, which is personified in sustaining the ability of the user to think and exercise choice. The idea of human dignity can also be expanded to consider the prominent rule of law ideals such as Fuller's principles of legality. Since the rule of law emphasizes on public disclosure of rules and their adherence by the government and legal authorities in a reasonably predictable manner, citizens would be able to plan and live in a more dignified manner.

The Fullerian ideas are open to many interpretations, which enables us to understand the mutual relationship between the user and the State. In the blockchain environment (the non-normative regulatory environment) also, these ideas facilitate in laying down the antidote for the 'regulatory margin' that can assist in embedding the rule of law values of 'participation, transparency, due process', which will legitimize such regulation.[50]

---

[46] Normative regulation includes measures that invite compliance such as social and moral norms.

[47] Non-normative regulation includes measures that do not permit the scope of choice.

[48] Brownsword (2011), p. 1351.

[49] Brownsword (2015), pp. 36–37.

[50] Brownsword (2011), pp. 1363–1364.

7.3.4 *'Legal Protection by Design'*

The 'legal protection by design' concept has evolved from the standpoint of understanding and defining 'ambient law',[51] opening up the facet of research for studying the incorporation of democratic and constitutional values into technological architecture. This concept, which is a successor to the notion of 'ambient law', was developed by Hildebrandt. In this regard, Hildebrandt argues that

> the normative impact of the ambient technologies or smart technologies will change the mélange of positive and negative freedom that forms the backbone of constitutional democracy unless ways and means are found to enunciate the legal framework of democracy and the rule of law, the so-called 'ambient law', which intends to regulate the technological architecture.[52]

In this frequently changing evolutionary world, command code rules, in some sense, inherit the characteristic of strong legalism and depend on a written and unwritten law, extending its scope and competence to afford effectual protection against manipulation.[53] However, the rule of code not only depends but also goes beyond the scope of written law. Neither any introduction of administrative rules will protect the users of the technology nor the self-regulation of the industry will achieve adequate protection unless citizens actively participate in the infrastructure assessment to enable computation. This requires 'ambient law' to be developed in such a manner that enables 'legal protection by design'.[54]

Here, the issue of concern is the question regarding the design of the artifact and what and how it empowers the user to exercise their choices? Is it possible for users to contest the design choice and pursue judicial action?

> The requirement of 'resistability' precludes deterministic environments, and the 'contestability' requirement eliminates invisible regulation.[55]

Such an exercise should not be hindered by the effects of the proactive blockchain infrastructure, whether intended or unintended. According to Hildebrandt, there are two criteria for the non-doctrinal *ex-ante* elements of 'legal protection by design', that is, choice and transparency.[56] She believes that it is a formidable challenge for traditional doctrinal research methods to develop a methodology for 'legal protection by design'. Such exercise calls for developing an approach that involves 'testing how the configurations or design of the affordances can best serve the goals of the rule of law'[57] such as '*Gerechtigkeit* (distributive and reciprocal justice, fairness,

---

[51] Hildebrandt and Koops (2010), p. 428.

[52] Hildebrandt (2008a), p. 178.

[53] Cohen (1999), p. 385.

[54] Hildebrandt (2011), p. 223.

[55] Hildebrandt (2015b), p. 218.

[56] Hildebrandt and Koops (2010), p. 456.

[57] Hildebrandt (2015b), p. 218.

equality), *Zweckmässigkeit* (purposiveness, expediency, and instrumentality) and *Rechtssicherheit* (legal certainty and the positivity of law)'.[58]

The values of 'justice, purposiveness, and legal certainty' culminating from the idea of 'law is justice' are extracted from Radbruch's Antinomian conception of law. It implies that the emphasis is on the design phase, where the prototypes of affordances of the product are conceived and developed and where there is room for consideration to determine whether or not they satisfy both the commercial requirements of the product and the desired rule of law values. The approach of 'legal protection by design' necessitates considering the legal affordances such that it facilitates in disaffording particular behaviors of the user while designing commercial affordances (such that they become attractive and valuable to the user) of a product. The rule of code must ubiquitously allow the ideals of legality and the rule of law to be operative. In other words, the legal protection by design emphasizes on transparency and publicity of norms (that allows the users to access and observe the rules they are being subjected to) and the opportunity to differ (allowing the users to exercise choice about the applicability of the rule). It also focuses on democratic legitimation and contestability in the court of law, allowing the users to contest the norms and seek legal remedy.[59] This approach, thus, focuses on both *ex-ante* and *ex-post* legitimacy standards where the main concern is about the ability of the user to exercise their rights *ex-post*.

References

Bankowski Z (2001) Law, love and legality. Int J Semiot Law 14:199
Black J (2002) Critical reflections on regulation. Aust J Leg Philos 27:1
Black J (2005) What is regulatory innovation? In: Black J et al (eds) Regulatory innovation. Edward Elgar Publishing
Borges JL, Weinberger E (1984) The thousand and one nights. Ga Rev 38:564
Brownsword R (2004) What the world needs now: techno-regulation, human rights and human dignity. In: Brownsword R (ed) Global governance and the quest for justice vol 4: human rights. Hart Publishing
Brownsword R (2005) Code, control, and choice: why east is east and west is west. Legal Stud 25:1
Brownsword R (2011) Lost in translation: legality, regulatory margins, and technological management. Berkeley Technol Law J 26:1321, 1363
Brownsword R (2015) In the Year 2061: from law to technological management. Law Innov Technol 7:1, 18
Brownsword R (2019a) Law, technology and society: reimagining the regulatory environment. Routledge
Brownsword R (2019b) The ideal of legality and the rule of law. In: Law, technology and society: reimagining the regulatory environment. Routledge, p 132
Brownsword R et al (2017) Law, regulation, and technology: the field, frame and focal questions. In: Brownsword R et al (eds) The Oxford handbook of law, regulation and technology. Oxford University Press, p 3

[58] Hildebrandt (2015a), p. 42.

[59] Hildebrandt (2017), p. 122.

Cohen J (1999) Reflections on habermas on democracy. Ratio Juris 12:385
Goldoni M (2011) The normativity of code as law: toward input legitimacy. In: 25th IVR Congress Law Science and Technology, Frankfurt am Main
Goldoni M (2015) The politics of code as law: towards input reasons. In: Reichel J, Lind AS (eds) Freedom of expression, the internet and democracy. Brill, pp 115, 123
Hassan S, De Filippi P (2017) The expansion of algorithmic governance: from code is law to law is code. Field Actions Science Reports. J Field Actions 88
Hildebrandt M (2008a) A vision of ambient law. Regul Technol 175, 178
Hildebrandt M (2008b) Legal and technological normativity: more (and less) than twin sisters. Techne: Res Philos Technol 12:169
Hildebrandt M (2011) Legal protection by design: objections and refutations. Legisprudence 5:223
Hildebrandt M (2015a) Radbruch's Rechtsstaat and Schmitt's legal order: legalism, legality, and the institution of law. Crit Anal Law 2:42
Hildebrandt M (2015b) Smart technologies and the end (s) of law: novel entanglements of law and technology. Edward Elgar Publishing, p 10
Hildebrandt M (2017) Law as an affordance: the devil is in the vanishing point (s). Crit Anal Law 4:116, 122
Hildebrandt M, Koops BJ (2010) The challenges of ambient law and legal protection in the profiling era. Mod Law Rev 73:428
Koops BJ (2008) Criteria for normative technology. In: Brownsword R, Yeung K (eds) Regulating technologies. Legal futures, regulatory frames and technological fixes. Hart Publishing, pp 157, 166
Leenes R (2011) Framing techno-regulation: an exploration of state and non-state regulation by technology. Legisprudence 5:143
Luger E, Golembewski M (2017) Towards fostering compliance by design; drawing designers into the regulatory frame. In: Taddeo M, Floridi L (eds) The responsibilities of online service providers. Springer, p 295
Scharpf F (1997) Economic integration, democracy and the welfare state. J Eur Public Policy 4:18
Scharpf FW (1999) Governing in Europe: effective and democratic? Oxford University Press, p 11
Van den Berg B, Leenes R (2012) Abort, retry, fail: scoping techno-regulation and other techno-effects. In: Hildebrandt M, Gakeer J (eds) Human law and computer law: comparative perspectives. Springer
Yeung K (2008) Towards an understanding of regulation by design. In: Brownsword R, Yeung K (eds) Regulating technologies: legal futures, regulatory frames and technological fixes. Hart Publishing, p 79

Part III
The Rule of Law Translation: Design and Implementation

Chapter 8
The Rule of Law by Design

8.1 Shaping the Architecture

'The rule of law by design' approach encourages determining the code's function in a blockchain artifact and assessing the purpose of the technology being employed. It allows legal professionals to deal with the technology, its code, its regulations, its effects, and its verisimilitude. This means the methods and instruments that compose the 'constitution' upon which the technology and its code are enforced must be considered. The integrated development environments and software development methodologies where the text of code is written are also critical factors for an inclusive approach. At this point, constitutional protections are likely to be ingrained and purposed into the blockchain infrastructure such that an opportunity is provided to appraise and afford a benchmark that is considered legitimate and that can be channeled into the production and employment of blockchain artifacts. This approach also steers us to take a pragmatic view of code—about its development, production, and intended function and purpose.

Due to the *crypto-legalistic* characteristics of *lex cryptographica* inherent in the blockchain, the impact of the rule of code on our lives is not only enormous but also more effective than what the law aims to achieve. That is why the rule of code that does not adhere to the rule of law values or is not legitimate should not be put into effect. Such an act occurs, especially where the technology and its code are less concerned about abuses of design power. Even though code is not law, it is prudent to be concerned about techno-regulation and technological management similar to the conventional system because the rule of code must be assessed by reflecting on the techno-regulation effects anent the freedom and individual autonomy in comparison to the balance affected by the rule of law. The nature of the rule of code is such that its outcome or *ex-post* effects are predetermined, at least its broad structure. Thus, 'the rule of law by design' approach requires us to directly communicate and engage with the 'figure' to understand the practices and critical internal

A. Bisoyi, *Blockchain and Legitimacy*, Law, Governance and Technology Series 77, https://doi.org/10.1007/978-3-031-98712-0_8

production mechanisms and, as a result, allows the legal critique of the rule of code not only for its *ex-post* effect but also for its *ex-ante* state.

Since the assertion to develop the blockchain 'less legalistic' or according to 'the rule of law by design' may be incoherent and may result in questions for the 'figure', Djeffal suggests: 'to formulate a design principle of designability'. According to him, the main objective of the principle of designability is to 'translate general democratic values into design in a general and workable manner'.[1] Though he, in his paper, has discussed designability in the context of the democratization of AI, the same arguments can also be applied to blockchain for the purpose of translating the rule of law values and standards and designing it into the architecture of the technology. A contextual moot point is how the architecture or code can be altered to achieve a desired outcome and what are the consequences of employing a design-based approach to shape the outcomes.[2]

When 'architecture' is thought of as a means of shaping behavior, it is chiefly concerned with designing of space, place, and external environment in general to encourage certain behaviors while dissuading others. This understanding of architecture has long served as a tool for behavioral regulation, reflecting social order in ancient times. The royal authorities have used it as a visual expression of sovereignty and social stratification. King Sejong of the Joseon dynasty in Korea established the 'Regulation on Houses and Buildings' to enforce social hierarchy through architectural design. This regulation limited the number of rooms and embellishments based on social class—royal families could have upto 50 rooms, while commoners were restricted to 10. Structural elements like columns and room height were also controlled, emphasizing social stratification. Such regulations persisted until the Gabo Reformation of 1894 lifted such constraints. This example demonstrates how architecture, backed by a legal authority, has long been used to encode and reproduce social order.[3]

Technologically coded architecture is a 'kind of law that determines the act of people (what they can and cannot do)',[4] where the architects of the rule of code wield disproportionate power. Since the rule of code has the ability to set behavioral rules in online space and the design choices are available to choose these rules, there is a possibility of backdoor control of such power by State agencies antagonistic to civil liberties by controlling and influencing the architects of technological artifacts.

In this regard, a key concern that arises at the production stage of the code is that the 'figure' who programs such code inevitably has the power to construct alternative normative orders. These normative frameworks can substitute conventional law as a principal means for regulating behavior. Yet, these 'figures' (private enterprises) are not bound by the formal and procedural rule of law standards while producing code regulating human behavior, whereas sovereign legislatures are bound by

[1] Djeffal (2019), p. 270.

[2] Lessig (1999), pp. 91–92.

[3] Kim (2024), p. 17.

[4] Lessig (2006), pp. 77–88.

elaborate constitutional procedures conforming with the rule of law so that democratically elected representatives cannot arbitrarily enact laws to regulate citizens' behavior. By that analogy, private enterprises engaged in the production and deployment of the blockchain should also be subjected to equal or more rigorous checks and balances since the normative force of the rule of code produced through the 'private' legislation can also be unlawful.

Code embedded into technological artifacts behaves as law and regulates human behavior normatively.[5] Since the law is dependent upon the artifact that is to be regulated and the 'sovereignty' of the 'figure', the balance of power shifts against the law, rendering it not so powerful as one might suppose. As such, legal professionals cannot bank just on pleas for 'greater regulation', especially if the latter is not equipped with the knowledge or cannot appreciate design practices, importantly where the illegitimacies of the rule of code can be mitigated by bringing in the principles of the design thinking approach into the design process. This is where the knowledge and necessity for 'the rule of law by design' comes into application.

As has been discussed, blockchain works around the rule of code that has been set forth within its architecture, where the inherent characteristics of the rule of code, such as rule-fetishness, immutability, instantaneity, and obscurantism represent the strongest version of legalism, is not neutral and is alegal. It depends on the choices and decisions made by the 'figure' and, as such, also regulates the user behavior and sets rules for their actions. Such non-neutrality of the technology and its alegality leads to unintended consequences and injustices, especially when the blockchain application is being employed for humanitarian affairs such as aid distribution or for protecting the vulnerable population. To address these concerns and mitigate the *ex-post* effects of strong legalism, which is crucial for upholding the rule of law, it is imperative to introduce mechanisms that temper the rigidity and enhance the fairness and adaptability of the system. This may entail embedding principles of due process, accountability, and transparency directly into the design and operation of the blockchain infrastructure. Introducing features that enable human oversight and discretion in decision-making, establishing clear and accessible channels for contestability, and ensuring that the underlying algorithms are transparent and auditable can help uphold the rule of law. By prioritizing the rule of law values and affordances in the design and implementation of blockchain applications, the system's adherence to the rule of law can be enhanced while maintaining the benefits of technological efficiency and automation. The goal is to 'lessen' the *ex-post* effect of the characteristics of the strong legalism as is reflected from the *ex-ante* code 'as it is now' and to make it 'less legalistic' and ensure the legitimacy of the blockchain to a certain 'acceptable' extent such that the rule of law values and standards are sustained.

[5] Goldoni (2011), pp. 127–129.

8.1.1 Evolution of 'By Design' Concept

The solution to the problems of human-machine interface lies in the relationship between engineers and sociologists, which is similar to the relationship between a blind person and a lame person. Separating the technicalities of a machine and social and cognitive aspects is an artificial construct between the technologist (the blind person) and sociologist (the lame person). Unless social aspects are added to the technicalities of engineers, the problem is unlikely to be solved. A similar argument is also applicable to the relationship between computer engineers and lawyers.[6]

The 'by design' approach can be a good intervention mechanism to bridge the gap between the knowledge of machines and the knowledge of law. Here, 'by design' refers to

> not only about engineering but also about human-machine-interfacing, highlighting that inscription of legal norms is not only a matter of technique but also an art.[7]

It denotes ensuring compliance with legal obligations by way of technical enforcement, as well as the primary goal of warranting legal protection.[8] The 'by design' approach to law can be perceived as 'user-centric', which incorporates empathy of the 'figure' towards the people, which instinctively helps to spell out the precincts of rights, rules, and policies. This process is essentially a collaborative, participatory process that starts with humans and their emotional and social needs.[9] Therefore, all designers and non-designers are encouraged to understand the potential of by-design as an instrument of change.

The design of the artifacts alters the associated conditions to persuade the user to behave in a certain way so that the behavioral response of the individual is as intended. If the user does not behave in the desired manner, then the anticipated design outcomes will not be achieved due to ineffective intervention. The design-based approach aims not only to alter the impact of harm-generating behavior but also to eliminate the harm-generating behavior. For example, by introducing a car ignition locking system that prevents the starting of the car engine unless all passengers wear seat belts, the risk of serious injuries to passengers is prevented or eliminated.[10] Installing speed breakers encourages change in the behavior of drivers to reduce speed, whereas installing airbags alters the harm-generating behavior. Further, installing a smart transport system may eliminate the harm-generating behavior in its entirety.[11] Thus, comprehension of various design approaches could facilitate the legal design formulation of aspirational changes.

---

[6] Hildebrandt (2008), p. 189.

[7] Hildebrandt (2011), p. 240.

[8] Hildebrandt and Koops (2010), p. 460.

[9] This would imply the need for transparency, accountability, predictability, and consistency in the system.

[10] Yeung (2008), p. 82.

[11] Yeung (2008), pp. 86–87.

8.1.2 Law by Design

In contemporary scholarship, the 'by design' concept is positioned at the intersection of law, philosophy, and technology. It is explained through two notions: 'value-sensitive design' and the 'compliance by design'. Hagan views the 'by-design' methodology as complementary to existing legal methods, such as empirical legal studies,[12] with Perry-Kessaris putting forward the value of design approaches to socio-legal studies.[13] These notions envisage translating 'values' or 'legal requirements' into technical specifications and, eventually, designing socio-technical systems.

The 'value sensitive design' approach acknowledges that by embedding particular values into a system, architectural design choices can create opportunities or barriers for specific social and political viewpoints. In the case of the 'compliance by design' approach, legal norms are directly embedded into the design of socio-technical systems. This approach emphasizes the importance of human interpretations and evaluations to enhance conformity while designing systems with byzantine requirements. In a way, the objective is to address the field-specific requisites of substantive law within the design of techno-artifacts such that compliance is achieved and not just guaranteed. Thus, this approach concentrates on techno-regulation by design with the thought that it would enhance the transfer of regulatory norms across various domains and, at the same time, ensure that appropriate mechanisms are established to address compliance according to the legal norms.

Extending the concept of 'compliance by design', some authors have termed the notion 'legal by design' or 'legal compliance by design',[14] which falls under the concept of techno-regulation, where the emphasis is on the fact that technologies such as blockchain have the capability to effectuate or restrict and motivate or estop the conduct and behavior of users, which results in a '*de facto* regulatory effect'.[15] These regulatory effects arise not only due to the premeditated design of the technology, that is, the default configurations that 'must' be engineered, but also because of the unintentional outcome of the design choices, which were built for other purposes and with different aspirations or because of the unforeseen usage of the technology, such as the blockchain application initially built with the purpose of protecting the rights of the vulnerable population, resulting in causing discrimination among the individuals. While there is no 'completely agreed' meaning of regulation, a functional cybernetic approach is broadly used and accepted. In this approach, a regulatory system is characterized as having the ability to set standards, gather information about the state of the system, and modify the system so as to align it with the purpose for which it has been developed. This standard-setting

[12] Hagan (2020), p. 3.

[13] Perry-Kessaris (2020), p. 1427.

[14] Van den Berg and Leenes (2013), pp. 67–87. Hildebrandt (2017), pp. 307–311. De Filippi and Hassan (2016). https://firstmonday.org/ojs/index.php/fm/article/view/7113/5657

[15] Hildebrandt (2020), p. 267.

function of the regulatory system involves designing technical standards, which can be implanted into the architecture of the regulatory apparatus. Whether the standard-setting function is effective or not is typically evaluated from 'the extent to which it ensures that the chosen policy goal is achieved in practice'.[16] In a way, the standard-setting activity simply shifts to design engineers, who have been assigned the job of embedding regulatory policy objectives into the design and operation of the regulating apparatus.[17]

'Legal by design' argumentation calls for the interpretation of the legal norm in a coherent, precise manner, which can then be translated into the binary language or the programming language. For example, a landlord and a tenant enter into a smart contract, enabled by blockchain, regarding rental payments wherein the contract stipulates that the tenant must pay the rent by the third of each month. However, what constitutes a valid payment timeframe may depend on factors like banking holidays, weekends, or unexpected technical issues with online payment platforms. Since the performance of the contract takes place off-chain and to ensure accurate interpretation of timely receipts, a DBMS is integrated into the contract to verify payment receipts and provide clear signals about whether or not the legal obligation is fulfilled. In order to determine whether the performance computes as 'reasonable', the DBMS would be inputted with a set of variables concerning the contextual factors, after having interpreted them from the contract, to determine if the payment was made within a reasonable timeframe. The term 'reasonableness' is subjective in nature under the law and depends upon the relevant case law and should be interpreted taking into account the specific circumstances and factors of the case, making the aspect of timely payment to be inherently contextual. This may require human oversight in terms of interpretation and discretion in line with the legal principles, and thus, while smart contracts do enhance efficiency, it is highly unlikely that they can be equated with or guarantee 'legal compliance by design due to the rigidity of the code',[18] without accounting for contextual nuances.

In the case of 'legal protection by design', fundamental legal values are factored into the design processes of the technological artifacts, particularly concerning transparency and contestability design features.[19] This approach does not warrant enforcement of legal norms but puts a spotlight on the issue of legal protection by addressing that the legal values are not winnowed out by the 'default' affordances of the technological artifact, which is essential for diagnosing whether democratic values have been ingrained into the architecture. The requirement is that the technology be designed in such a manner as to ensure the due process rights of the users so that they are able to contest its application. The method of embedding values in design processes begins by identifying the stakeholders, relevant values, and methods for choosing values. Thereafter, technical investigations are deployed to explore

[16] Black (2008), pp. 137–164.

[17] Yeung (2008), p. 92.

[18] Hildebrandt (2020), p. 268.

[19] Hildebrandt (2020), p. 269. Hildebrandt (2017), p. 307.

the feasibility of embedding values in design. In this approach, values may or may not be embedded into a design, but the values and implications of design choices are highlighted affirmatively in a framework.

The 'legal protection by design' and 'legal by design' can be said to incorporate the 'law by design obligation', which is defined as 'the duty to incorporate legal principles in design processes of technologies'.[20] This obligation can be signified by the security by design provision[21] under Recital 12 of the Cybersecurity Act, which mentions the non-binding requirement upon the 'figure' of the ICT products and services

> to implement measures at the earliest stages of design and development to protect the security….[22]

A few other examples of 'law by design obligation' can also be located in the GDPR which standardized a modern and proactive design approach. This is particularly evident in the obligation under Article 35, GDPR, to carry out a data protection impact assessment for particularly high-risk data processing.[23] Article 35(7)(d) states that a data protection impact assessment must contain

> the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.[24]

This article explicitly indicates the necessity for data protection by default and by design, which reflects the spirit of Article 25, wherein it requires the 'figure' to

> both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.[25]

Article 25, thus, mandates the design of technological artifacts to incorporate data minimization by default, not just at the *ex-post* level but also at the *ex-ante* level, along with other GDPR obligations by design. This means that data protection

---

[20] Djeffal (2024), p. 3.

[21] Djeffal (2024), pp. 3–4.

[22] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), L 151/15, Recital 12 (hereinafter Cybersecurity Act).

[23] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), L 119/1, Article 35 (hereinafter GDPR).

[24] Article 35(7)(d) GDPR.

[25] Article 25 GDPR.

should be taken into account when designing a system from the outset so that the implementation of the data protection principles is already built into the system and unintended or non-intended use of the system would be prevented from the outset by 'technical and organizational measures', if possible.

The implementation of data protection by design, therefore, implies that right from the beginning of the system development process, a few basic principles of data protection through the use of suitable design strategies, design patterns, and privacy-enhancing technologies, including knowledge of common errors, the legal situation, current threats, and attack method, etc., are to be implemented. Since this affects both the architecture and also many designing aspects of the system, factors like state of the art, the cost of implementation, and the nature, scope, context, and purposes of processing are considered for its implementation. Such measures must be practical in view of the commercial purpose of the technology. However, it does not allow the commercial purpose to possess disproportionate 'risks of varying likelihood and severity for rights and freedoms' of individuals, and as such, these risks have to be factored in when programming the operations, where the principle of proportionality necessitates 'higher the risk, the more protection must be implemented by design'. The need for protection must be assessed based on the underlying context of use and the associated risks. This desideratum is accentuated by paragraph 2 of Article 25, requiring the technical and organization measures to be implemented in such a manner that 'only data which is necessary for each specific purpose is processed',[26] which emphasizes the data protection principles of data minimization and purpose limitation. The underlying requirement is to have a 'cautious approach' or 'risk-based approach'[27] to the protection of personal data, echoing the established security principles like 'select before you collect',[28] which seeks to implement legally mandated precautions by the data controllers to safeguard the rights and freedom of individuals.

Where the 'data protection impact assessment' makes the risks transparent and requires the formulation of technical and organizational measures to reduce, or, at best, eliminate these risks, the data protection through technological design ensures that these measures in the event of other sanctions against the person responsible are also directly integrated into the system. This requires that the principles be made more concrete when standardizing the system. The data protection by design provision is important because it is actually a normatively anchored expression of legal protection through technological design.[29]

Another by-design obligation can be found under Article 22, GDPR which Djeffal states to have an 'uncharted potential'.[30] This Article is highly relevant for blockchain since it targets the implication of automated decision-making. It is

[26] Article 25(2) GDPR.

[27] Wachter (2018), pp. 436–449.

[28] Gaakeer (2020), pp. 57–71

[29] Hildebrandt (2020), pp. 272–277.

[30] Djeffal (2020), p. 857.

argued that Article 22 should also be interpreted as a 'by-design' obligation to ensure compliance with the law, as it mandates that in the case of automated decision-making,

> the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests.

The 'law by design obligation' does not impose any mandatory process requirements for the designing of technologies; instead, it allows the translation of legal principles into tangible technology design goals. As such, the law by design obligation 'addresses actors who can influence the design of technologies over time'.[31] The European Data Protection Board indicates that this incorporates the technical measures—

> Controllers should carry out frequent assessments on the data sets they process to check for any bias and develop ways to address any prejudicial elements, including any over-reliance on correlations. Systems that audit algorithms and regular reviews of the accuracy and relevance of automated decision-making, including profiling, are other useful measures. Controllers should introduce appropriate procedures and measures to prevent errors, inaccuracies, or discrimination on the basis of special category data. These measures should be used on a cyclical basis, not only at the design stage but also continuously, as the profiling is applied to individuals. The outcome of such testing should feed back into the system design.[32]

These measures illustrate how the 'legal protection by design' can be translated into a functional necessity shaping the design of systems for processing personal data. Such an approach helps prevent unjustified breaches of data protection regulations while offering tangible and efficient protection at the level of technical (micro) and organizational (macro) levels and precluding situations where safeguarding an individual's rights and freedoms would seem illusory.

The root of all fundamental rights guarantees is the inviolable dignity of all human beings. Legislating data protection is not an end in itself and must always be interpreted with regard to the protective purpose and the risk to those affected; the ultimate protective purpose of data protection law is ensuring human dignity when processing personal data. Human dignity as a starting point and as a justifiable concept ensures that only a comprehensive and careful examination of the concrete effects on the people affected leads to a result. This is where the added value of the concepts of 'human dignity by design' and 'data protection by design' rests. The concept of human dignity by design derives its justification not so much from a substantially changed normative requirement but rather from a change in the mental attitude when solving problems.

The 'by design' approach explores the extent to which the illegitimacies of the normative effects of the technology

[31] Djeffal (2024), p. 4.

[32] Article 29 Data Protection Working Party (2017), Guidelines on Automated Individual Decision-making and Profiling for the purposes of Regulation 2016/679, WP 251, pp. 16–17.

> can be deliberately managed to realize the legal principles in socio-technical settings; they not only manage the effects of technology by prescribing hard and fast rules but they motivate the steering of the design of technologies by operationalizing legal principles to work outside the professional legal system.[33]

These approaches suggest that law serves as an instrument to shape and guide the technological design, which encompasses laying down design objectives, balancing the trade-off and identifying opportunities to resolve issues at the technical level.[34] Various notions of design, such as legal by design, data protection by design, human dignity by design, or legal protection by design, can be forwarded to nurture the concept of 'the rule of law by design' since these conceptions are co-related to each other. These notions of 'by-design' in the legal domain are a subset of the rule of law by design concept because the rule of law by design aims not only to guarantee enforcement of any legal norm but also to ensure that legal protection is not discarded due to the affordances of the technological environment.

8.2 Applying the 'Rule of Law' Principles in Design

The purpose and intention of 'the rule of law by design' is to have some form of regulation and legal protection encapsulated in the technology since the technology has the ability to influence and shape human behavior in accordance with the objectives of the 'figure' and the regulators such as the State. This form of law by design obligation is a

> principle-based regulation with an obligation to translate a legal goal into technology without providing precise procedural or substantive requirements, where the aim is to internalize values in the context of technology development.[35]

The State primarily targets the 'figure' responsible for designing and programming the artifact with the rule of law requirements and standards and obligates them to ensure that the system meets the specified legal requirements. Once the 'figure' adheres to this obligation, the 'rule of law by design' exerts an impact on the behavior of the users interacting with the technology, for example, by restricting certain alegal uses of the application. These restriction or constraints yield their signification as they emerge during the process of their coming into existence. This approach does not reduce the constraints to mere compliance because that would close the door for any transformation of norms to comply with. Hence, the figure has to think twice before programming a code in a blockchain, given that there are certain rule of law standards that they have to keep in mind.

[33] Djeffal (2024), p. 26.

[34] Djeffal (2019), p. 269.

[35] Djeffal (2024), p. 2.

> If the requirements evoke a conventional dimension of a practice, the obligations might call to mind its identity, but again not in a petrified or given form.[36]

In other words, obligations do not guarantee the fixed identity of practice, but instead, they define the 'peculiar mode of hesitation of its practitioners'[37] which may yield changes and evolutions of the practice concerned.

> Both requirements and obligations are part of what makes a good practitioner because their interplay guarantees both change and innovation of a practice against its dogmatic refuge and immobilism and consistency and continuity against its evaporation or colonialization.[38]

This calls for the need to emphasize 'the constraints of a practice, its obligations and requirements',[39] which confront every 'figure' with the question of how to change without betraying. The same assertion will also be applicable to the 'figure' who is responsible for designing and developing the blockchain, such that they take into consideration the requirements of the technology and obligations of the rule of law standards and values.

'The rule of law by design' mechanism incorporates a form of delegation wherein the State obligates the 'figure' to enforce the prescribed rule of law standards and values upon those who utilize it or are impacted by the technology. Therefore, 'the rule of law by design' aims to inspect both the *ex-ante* micro level and the *ex-post* macro level. There is no hierarchy between the two levels and should be perceived to have an equal footing that works together contemporaneously to formulate the technology such that the artifact sustains the rule of law values and standards.

It is necessary to apply the rule of law principles intentionally to the design and implementation of technologies that 'regulate' behavior and outcomes. Such regulation, which uses technologies to achieve goals instead of legal rules or normative identifiers, is called technological management.[40] In the context of blockchain, technological management can involve using smart contracts, decentralized applications, and consensus protocols to control transactions, interactions, and identities on a distributed ledger without relying on intermediaries, authorities, or legal enforcement. However, technological management in blockchain can also create problems or conflicts with the existing legal and moral order and raise issues of accountability, transparency, and legitimacy.

Some conditionalities are essential to make sure that technological management is consistent with the rule of law. First, technological management should not harm the basic conditions, 'the commons', that are necessary for human society to exist.[41] The rule of law emphasizes that the 'figure' has the main duty to protect and maintain the commons. Second, the rule of law requires that the use of technology and

[36] Gutwirth et al. (2008), p. 197. Latour (2004), pp. 73–114.

[37] Gutwirth et al. (2008), p. 198. Latour (2010), pp. 162–163.

[38] Gutwirth et al. (2008), p. 198. Latour (2010), pp. 278–279.

[39] Gutwirth et al. (2008), p. 198.

[40] Brownsword (2022), pp. 5–40.

[41] Brownsword (2021), p. 71.

its ordering matches its intrinsic constitutive characteristics, such as whether they are liberal or communitarian, rights-based or utilitarian. Third, when technological management is suggested as a way to manage risks, the rule of law demands that there is open and inclusive public discussion about the strategy that ought to be reasonable and respectful. In changing environments where decisions are made case by case, there may be a need for human intervention, as in the case of autonomous vehicles that allow human override in moral dilemmas or emergencies. Also, the right to due process against decisions enforced by technological management should be kept, especially if they limit or force certain actions or exclude some people or groups. This need for human intervention as a last resort may even be a default condition in the rule of law. Fourth, any limitations on the use of technological management that are agreed upon after public deliberation should be respected, ensuring alignment with agreed rules and the society's constitutive principles. Fifth, users should be confident that there are ways to hold the implementation of technological measures accountable for dealing with problems or failures. Sixth, the range of technological management should not go beyond that of similar traditional rules, and seventh, technological management should not try to trick or trap users but match the reasonable expectations of users and make sure they know how it works. Finally, eighth, users may want public approval and oversight of private use of technological ordering, as institutions that protect fundamental rights should balance rather than support private economic power.

The rule of law mandates that private use of technological management must follow general principles that govern its use. It can also act as a guide in different ways in the context of technology regulation in the form of political guidelines.[42] Firstly, political guidelines can be implemented directly through technology design. With regard to the *de facto* dominance of large digital corporations, the notion of *de facto* regulation by technical design is to be considered. It should be noted that technology can also have such a *de facto* regulatory effect without this being intended. Secondly, political guidelines can be implemented through legal norms that are aimed at the 'figure' responsible for designing the technology and oblige them to implement the political guidelines in the design of the technology. This is what is at the center of the concept of 'legal protection through technology design' or 'legal protection by design', which, from the perspective of the user of the technology, is a preventive regulation. Thirdly, political guidelines can be implemented through legal norms that are aimed at the users of the technology and require them to use or not to use the technology in a certain way. These are classic repressive regulations. Such a regulation is well suited to regulate numerous areas of life because it allows for a certain degree of flexibility and corresponds to our liberated, social, and legal system. What looks like a violation of the law does not always have to be so; think of the simple case of self-defense or limitations in copyright law. A constitutional procedure for enforcing repressive regulation is very well suited to taking such exceptions and nuances into account.

[42] Reidenberg (1997), pp. 553–593.

Preventive regulation or 'legal protection by design' appears to be a suitable and appropriate means of countering the arbitrary exercise of government power while at the same time enforcing the law. However, this is not simply intended to promote the spread of legal protection through technology. Examples of this can be vehicles that no longer allow exceeding the maximum speed limit; such measures usually entail significant risk, susceptibility to errors, and other weaknesses that must be taken into account when considering legal protection through technology design in a specific area of application. It should also be noted that 'law by design' usually includes technology programs and thus also the program's inherent properties of potential instability, error, and manipulation.

'The rule of law by design' concept presented here is largely a logical extension of these notions of design in the legal domain in the context of the computational society—

> what unites is the desire to delve deeper into the process of technology design to uncover potentials to steer technologies towards certain normative expectations by influencing the processes of innovation.[43]

Effective fundamental legal protection is only conceivable in an increasingly digitized State administration if the legal situation is implemented in code as precisely as possible and without loopholes. In an ideal situation, only legitimate administrative action is actually possible, at least in the completely automated storylines. Therefore, 'the rule of law by design' is an esoteric philosophical indignation about the characteristics of the rule of law and its operative functionalism in and through computational architectures and not just about the application of the rule of law doctrine within the computational context.[44]

The concept of 'the rule of law by design' endeavors to incorporate the specific values of fundamental rights and the rule of law principles into the technological infrastructures. It is an umbrella concept that is concerned not only with the compliance of technological normativity with substantive law but also with ways to ensure that such legal protection can be both resisted and contested in the conventional court of law. The fundamental purpose of this concept is to mandate that the rule of law values and standards are upheld throughout the process of conceiving, developing, designing, programming, and, finally, utilizing the system. Unlike mere regulation of technology use, which involves the application of the law externally, obligation centered around the 'by-design' seeks to influence, steer, and enhance the entire socio-technical process of technology creation and utilization from within. While it is possible to incorporate the specific rule of law features 'by design', applying the same approach to the rule of law is not forthright since it may not be feasible to automate complex socio-legal requirements fully. Linking design to values makes such choices visible and explicit. Understanding the impact of design choices on the rule of law thus requires first a definitive statement of the values associated with the rule of law that could be implemented technically (at least partially). Therefore, as said before, 'the rule of law by design' encourages one to look

[43] Djeffal (2024), p. 27.

[44] Hildebrandt (2011), pp. 238–239.

for the 'figure' to develop these systems such that it reinstates the protection that is central to the rule of law. The system ought to require the decision-making of the algorithm output to be a human-readable explanation, enhancing the transparency of such decision-making. It would also necessitate that these systems be pre-tested for their output contestability. Further, procedural checks and balances have to be introduced in default settings to offset inequalities and unfair distributions. In a democratic society, regulating citizens' behavior must achieve minimum standards of the rule of law irrespective of regulatory tools.

The duty delegated to the 'figure' goes beyond the simple enforcement of the rule of law values and standards as outlined in the legal jurisprudence. The 'figure' cannot fulfill its obligation without interpreting them: legal requirements are typically expressed in broad terms, necessitating the 'figure' to ascertain how these general formulations apply to the specific contexts in which the technology architecture is anticipated to function. Once the substance of the relevant legal requirement is established, the 'figure' must determine the technical methods that meet the demands of the rule of law. Certain requirements may compel the 'figure' to abstain from employing particular techniques, while others may necessitate the incorporation of specific rules directly into the system's code. As a result of these processes, the rule of law by design evolves into a form of co-regulation, wherein the State delegates not only the execution power but also the authority to define the actual content of the legal standards and the mechanisms employed to enforce them.

Consider the accuracy requirement introduced by the EU AI Act.[45] Within the framework of the rule of law by design mechanism, Article 15(1) establishes a crucial provision for ensuring accountability and adherence to legal standards in the development and deployment of AI systems. Under this provision, any high-risk AI system must attain a level of accuracy appropriate to its intended function. By integrating such provisions, the AI Act upholds the principles of legality and predictability, ensuring that AI technologies operate within established legal boundaries and do not undermine fundamental rights or societal values. The relationship between Article 15(1) and the rule of law underscores the importance of regulatory oversight and legal compliance in harnessing the potential of AI while safeguarding against potential harms or abuses. The requirement of such a provision significantly impacts the behavior of third parties: both public and private actors will only be permitted to procure and utilize AI systems that adhere to the accuracy standards. This assurance extends to the general population, who can trust that any AI system developed in compliance with the law will possess adequate accuracy for its intended use. However, the 'figure' retains considerable discretion in selecting techniques that meet the accuracy standard: they may opt for the most precise system they can devise, or they may design a system with sufficient accuracy to fulfill the

[45] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (hereinafter AI Act).

design requirements while also being easily comprehensible to users. Consequently, the choices and decisions made by the 'figure' have the potential to yield diverse systems, even when starting from the same requirements.

A crucial aspect of upholding the rule of law in the governance and regulation of technology is comprehending the choices made during the invention or implementation of the technology. Numerous design decisions are made during the development and programming; some of them are made with a purposeful intention, while some carry significant ramifications. From the lens of the rule of law, it is essential to recognize and emphasize specific design choices in association with the architecture, application, and other attributes of the technology in employment. If there is an alternative to choose from, there is a choice, and a decision must be made. Taking cognizance of such choices also necessitates having the rule of law mindset that remains open to various possibilities without automatically favoring particular outcomes. Particularly, computer scientists who are typically trained to prioritize specific objectives like efficiency often overlook the implications of decision choices that align and maximize their preferred value.[46]

Aiming the technology to be based on the rule of law by design may at times, be necessary to uphold the neutrality of the law concerning emerging technologies. Neutrality in the present context implies that the emergence of new technological infrastructure should not weaken the spirit and effectiveness of legal protections. This aligns with the approach developed by Nissenbaum in her decision-making heuristics regarding contextual integrity, which investigates whether and how new socio-technical practices infringe upon existing values.[47] Such an approach involves adopting a prudent stance, but not one that is overly cautious, regarding norms and values such as privacy or contextual integrity. It is a prudent approach as it concentrates on existing rights or values rather than advocating for new ones and is not overly cautious because it acknowledges that to safeguard and maintain these values or rights, their spirit and effectiveness must be assessed in light of relevant new technologies, recognizing that the design of such technologies influences the values and legal norms they uphold or supersede. To some extent, it is accepted that new technology may prompt a reconfiguration of norms and values; however, the emphasis is that this reconfiguration should not compromise the spirit and substance of existing values solely to accommodate new business models or more efficient administration. From the rule of law frame of reference, it can be added that legal norms are established or endorsed by the democratic legislature, and altering their scope should not occur without involving the affected constituency or individuals.

The rule of law by design may be perceived as an attempt to transpose the affordances of the legal script onto the technological infrastructure that may have vastly different affordances, but such an endeavor is destined to fail. Affordances cannot be transplanted; they can only be identified and, to some extent, adjusted or crafted into the technology. The objective is to identify, configure, or craft affordances that

[46] Brownsword and Yeung (2008), pp. 23–48.

[47] Benthall et al. (2017), pp. 2–60. Nissenbaum (2004), pp. 118–137.

align with specific legal norms that might otherwise lose their efficacy or to develop socio-technical systems that embody particular legal norms. This endeavor should always consider the potential for resistibility and contestability of the resulting normativity and should consistently involve assessing how the configuration or crafting of affordances can best advance the objectives of justice, legal certainty, and purposiveness. The rule of law by design mechanism calls for the need to articulate and craft the rule of law standards and values into affordances to embody them in the technological architecture through the command code rules at the micro level and the conceptual purpose code norms at the macro level.

8.2.1 Legal Standards in Technological Artifacts

Computer scientists have implemented some of the techniques that they devised for encoding legal requirements and instruments into software to enable digital systems to tackle diverse issues. These systems range from automating tax rules and social security benefits to verifying compliance with standardized trade regulations. The effectiveness of these approaches implies that, in certain situations, legal requirements can be accurately translated into code rules, which subsequently enforce the encoded requirements by situating 'specific legal principles as goals'.[48] In this case, protecting the fundamental rights of individuals can be a broad and extensive goal, whereas protection of the right to privacy or security can be considered as a specific goal. Law by design or techno-regulation proves to be a viable approach for the State in such instances.

Transposing legal rules into technical rules is a delicate process that could significantly affect the way we deal with law and technology. Though legal systems are deliberately designed to be ambiguous, leaving scope for judicial interpretation, they also give the 'figure' the power to embed their version of law into the technical artifacts.[49] Hence, while code is increasingly assuming the traditional functions of law, the law is also assuming the characteristics of code.[50] As more and more contractual rules and legal provisions are incorporated into smart contracts, the traditional conception of the law might be required to evolve into something that can better be assimilated into code.

Translating the rule of law standards and values into software requires the legal norms to follow the structure of conditional statements, such as 'if [this condition], then [that consequence]', which closely resembles the conditional logic found in programming languages.[51] If the conditions and outcomes of a norm can be translated into a code rule, like the examples mentioned earlier, it is amenable to

[48] Djeffal (2024), p. 15.

[49] De Filippi and Hassan (2016). https://firstmonday.org/ojs/index.php/fm/article/view/7113/5657

[50] Dimitropoulos (2020), p. 1142.

[51] De Filippi and Wright (2018), pp. 193–204.

programming. This translation is not always feasible, especially when the conditions of a norm pertain to human and societal elements that cannot be easily captured in binary code or technical artifacts, such as those related to the development of human personality.[52] Additionally, encoding becomes problematic when automating a norm contradicts its intended objectives, as in the principle that a defendant in a jury trial should be judged by their peers. Consequently, the substance of a legal rule may pose challenges to its expression in the technological architecture.

Additional challenges arise when the concept of the rule of law by design introduces other forms of legal requirements. In a few scenarios, the rule of law by design concept does not mandate the 'figure' to directly incorporate specific legal norms but mandates only overarching principles. The rule of law principle imposes obligations on those governed by it—in this instance, the 'figure'—without explicitly outlining the specifics of these obligations, which necessitates contextual assessment. Consequently, the 'figure' tasked with implementing the rule of law principle must anticipate potential issues that could arise in each operational context of their system and propose technical solutions beforehand. However, executing such anticipatory measures may not always be feasible in every case.

There are two instances of the rule of law by design mechanism, which sheds light on the limitation of anticipatory approaches to the rule of law principles. In the accuracy-by-design illustration provided earlier, with respect to Article 15 of the EU AI Act, there is a potential conflict of values between accuracy and transparency since certain highly accurate systems may be opaque and inscrutable to the users, posing a challenge. This conflict can be resolved during the design process. As long as the system achieves the requisite level of accuracy to meet the established standards and maintains sufficient transparency to adhere to the transparency by-design specification, the 'figure' retains the autonomy to balance these values within the system. Once the choice is decided upon that aligns with the rule of law, it stands as an acceptable solution to the value conflict until the circumstances dictate otherwise.

The 'figure' may encounter challenges when value judgments lack consistency over time. Take, for instance, a situation in which a social media platform must automatically delete posts containing hate speech. An erroneous removal decision could significantly infringe upon a user's rights, particularly freedom of expression, making accuracy a crucial factor in this context. While automated filters may identify many unlawful posts, they may also yield incorrect outcomes, particularly when dealing with parodies, for example.[53] The accuracy of a removal decision not only hinges on the context of the communication itself—such as whether it was intended as a joke or a legitimate form of protest—but also on the prevailing cultural norms within society. The 'figure' is unlikely to anticipate all relevant factors in advance, and even if they do, the standards they embed into the technology artifact may become outdated as societal attitudes toward certain types of discourse evolve.

[52] Hildebrandt (2020), pp. 69, 78.

[53] Marsoof et al. (2023), p. 64.

Adhering strictly to the rule of law principles may prove insufficient under certain circumstances, particularly when legal norms cannot be fully delineated before implementation or when relevant factors defy binary categorization. In such scenarios, compliance with the rule of law by design becomes a matter of risk management. It is perceived as a negative 'law by design obligation' where it seeks to reduce the risk or the harm generated by the artifact in question,[54] and thus, the 'figure' is obligated to select and implement measures that mitigate identifiable risks to the values at stake. If these choices diverge from the priorities of the State or result in unacceptable side effects, the actual impact of the system on users and third parties is likely to deviate from the State's initial expectations.[55] Compliance with broadly defined rule of law principles may, therefore, undermine or, at the very least, fail to advance the objectives that led the State to adopt the rule of law by design approach in the first instance. As such, for the rule of law by design approach to be employed effectively, it necessitates that the legal rules be translated coherently into specific value sets or requirements rather than overarching values.

It is important to emphasize that effectuating the rule of law by design mechanism into the technology fosters legitimacy to a certain extent, thereby mitigating any form of potential coercion towards users. The relevance and significance of legitimacy for the rule of law by design mechanism is ensured by three factors.[56] Firstly, the effectiveness of this mechanism hinges upon the adherence of 'the figure' to the norms and standards they are mandated to follow during the technology design process. Secondly, the users who are subjected to encoded rules possess the potential to influence the system's operation or the role the technology plays in society. Finally, considerations of legitimacy are pertinent from moral and political standpoints, such as upholding democratic ideals by ensuring individuals have a voice and 'choice' in shaping the 'rhythm' of their lives. Hence, even technology designed with the explicit purpose of upholding the rule of law and democratic principles with meticulous technical precision could face compromise if the legitimacy of the embedded rule of code is not established beforehand, as the *ex-post* legitimacy effects rely on the initial *(ex-ante)* production's legitimacy.

Technological artifacts can achieve *ex-post* legitimacy based on the outcome. If individuals or groups perceive the effects of the governance of technology as favorable, they are more inclined to comply with its demands, even if those demands conflict with some of their personal interests.[57] At the same time, it is essential to understand the effectiveness of the artifacts in achieving their objectives to evaluate the legitimacy of design-based instruments. For example, a smart car can be designed in two different ways to reduce motor vehicle accidents caused by driver fatigue. One, the smart car can be designed to issue a warning to the driver when the system detects driver fatigue so that the driver can stop and rest. Thus, the artifact

[54] Djeffal (2024), pp. 4–5.

[55] Brownsword (2016), pp. 129–131.

[56] Brownsword (2021), Chap. 17.

[57] Brownsword et al. (2017), pp. 3–38.

endeavors to bring in a behavioral change. Another design approach could be in which the smart car automatically directs the driver to a parking lot and prevents further journey when it detects driver fatigue. In the latter case, the artifact overrides human action to achieve the desired results, leaving no scope for human agency to thwart the desired goal. Only when the design seeks to change behavior, or to alter harm-generating behavior, or to reduce undesirable social outcomes, there may be some latitude for human agency to put impediments to achieving the goals.[58]

Technology can attain *ex-ante* legitimacy by involving relevant stakeholders in its development processes, thereby reassuring these stakeholders that the artifact considers their values and concerns. These mechanisms for building legitimacy are not mutually exclusive since sources of *ex-ante* legitimacy may either reinforce, compensate for, or undermine one another, which can impact the *ex-post* effects. Therefore, the evaluation of legitimacy in technology must consider how potential sources of legitimation manifest and interact with each other in practical contexts. Since the legitimacy of the artifact depends upon the standards and values that have been incorporated into the architecture of the technology and its operation, the rule of law by design facilitates this legitimacy by ensuring that the standards that provide affordance to the command code rules and the values which afford the conceptual code rules of the operation must comply with the rule of law and render legal protection to the users. The rule of law by design also targets *ex-ante* legitimacy in order to produce a legitimate *ex-post* result. From the perspective of the *ex-post* legitimacy, it is evident that embedding legal standards can be a double-edged sword such that, on the one hand, good design standards can result in the artifact enforcing and governing the behavior of users uniformly and fairly, but on the other hand, design standards which have been incoherently expressed and translated into the technology architecture may fail to achieve the desired outcomes. It is important to realize the formulation of a good, coherent, and specific design standard to embed the spirit of legitimacy and the rule of law within the technology artifact so as to achieve the desired output.

8.2.2 'Inner Morality' of Code Norms

Brownsword[59] and Asscher[60] both have put forward the idea of adapting or applying Fuller's principles of legality, which is nested within the rule of law, to the rules of technological instruments. Fuller has outlined eight standards or principles that are considered crucial to any legal system. Failure in any one of these eight standards does not just result in a bad system of law but actually results in a system that is

[58] Yeung (2008), p. 89.

[59] Brownsword (2019), p. 114.

[60] Asscher (2006), p. 61.

alegal. These principles are applicable to all systems, including legislative bodies as well as technology.

> Being at the top of the chain of command does not exempt the legislature from its responsibility to respect the demands of the internal morality of law; indeed, it intensifies that responsibility.[61]

Since there are proposals to regulate and utilize blockchain more by the governments to realize the policy goals in the future, it will be interesting to observe how 'the rule of code' that governs the technology satisfies the Fuller standards.

Conventional legal theories concerning code are sensitive to the development and production of codes by the 'figure' that has the potential to 'be hostile or complement or supersede Hartian legal norms'.[62] Contextually, the principles of legality, a concept interlinked to the rule of law, are binding on regulators, notwithstanding the substantive aspect of the regulations. Brownsword tends to maintain an ontological separation between the 'rule' or norm that exalts the use of a particular regulation on code and the nominal effect of the regulation itself, which introduces a gap between his analysis and the substantial elements of the code[63]—

> there is the choice between normative and non-normative ordering, between rules – signaling ought and ought not – and design – signaling can and cannot.[64]

This analogy creates a void between the design considerations, such as the limitations or disaffordances posed by an artifact, and how it practically mediates or facilitates user interaction.

Standard 1—Fuller identifies that the legislative rules should be of general application, which, when applied to the blockchain environment, the fact that the code norms in question should resonate with the conception of generality and must be germane at all times. This means that the blockchain code and smart contracts need to have general application, rather than being too specific to any individual or situation. In some cases, the articulations of the rule of code might be specific to particular individuals—for example, precision profiling, when personalized, is likely to identify and isolate dangerous individuals or a class of them,[65] adhering to the principle of generality. However, in another instance, when the 'figure' releases 'too many' updates in a short period of time, it fractures the uniformity of the code across the user database. So, such a precautionary vantage point is required to ensure fairness and consistency in the functionality of the technological artifact.

Standard 2—According to Brownsword, in the controlled, regulated space that is technologically managed, there is no rule book to adhere to, where the relationship between regulators and users is no longer arbitrated by rules, and the actions of users are no longer rule-guided. However, that is not the 'absolute' truth, since the

---

[61] Fuller (1964), pp. 39, 64.

[62] Brownsword (2015), pp. 10–14, 19.

[63] Brownsword (2016), p. 113.

[64] Brownsword (2019), p. 119.

[65] Casey and Niblett (2016), p. 1401. Casey and Niblett (2017), p. 1.

technologies are governed by the code norms determined by the rule book or the constitution of that particular technology, which is adhered to by the 'figure' while programming the system with the functionalities required for a purpose. For Brownsword,

> what matters is not the rules that result from a 'law-making' process are published, but that proposals for the use of technological management are published. What matters is not so much that regulatees know where they stand but that they have a fair warning that a particular use of technological management might be made for public purposes and, concomitantly, a fair opportunity to participate in the processes that will determine whether such use is to be authorized.[66]

In other words, Brownsword translates Fuller's second standard to the decision requirements in relation to the intended use of technological management. The focal point is not the actual technical transparency but the transparency of intent, and as such, the distinction or the gap between the two is indeed problematic.

The result is that in situations where the rule is not intended to guide the conduct of the users but to mandate the use of technological management, the proposal might take the form of an authorizing rule. The idea of notifying such rules for democratic participation would be to fortify the legality of the use of technological management. In fact, the use of technological management should be authorized in a transparent manner, and there should be a certain degree of openness about its operation.[67] For blockchain, this would involve transparency of the purpose of employing the technology, that is, the guiding values, including the transparency of the code. It will not only facilitate the diminishment of the opaque nature of the blockchain artifact but also ensure that the users can understand how the apparatus functions.

Standard 3—There are cases where retrospective acts are possible in the technologically managed environment, such as digital records being deleted and amended or in contractual relationships, retroactive adjustments of the positions of the parties are made. However, in general, where technological management is initiated to deactivate a particular act or to eliminate any earlier practice, it takes effect prospectively, which means any changes to the environment are prospective, and technological management does not advance any new hazards of 'unfair retrospective penalization of conduct'.[68] This channels the requirement for blockchain protocols or smart contracts not to be applied retroactively, as it could undermine trust and predictability in the system.

Standard 4—In the context of technological management, regulatory clarity might be somewhat less important, but it is not entirely superfluous. The 'figure' is still required to communicate with their users, and more importantly, they need to indicate the specific choices that are available. In this manner, the clarity of communication still counts in technologically managed code rules. Obviously, if the

[66] Brownsword (2016), p. 117.

[67] Brownsword (2019), p. 125.

[68] Brownsword (2019), p. 120.

regulatory environment is designed in such a way that users have no other choice than to perform a specific act, then they will conduct only in that manner, even if there is no clarity. Even so, the regulatory signal should be clearly and decisively transmitted such that the user behavior can be directed with less friction and confusion.[69] The Fullerian standard emphasizes that there should not be any uncertainty about the rules to be followed by users. The rules should be comprehensible and free from ambiguity so that the users are made conscious that the technological measures will regulate their conduct in some way.[70] When interpreted from the perspective of the blockchain environment, this design standard requires ensuring that the rule of code or smart contracts are written in a comprehensible and unambiguous fashion.

Standard 5—This Fullerian standard can be associated with the technological requirements to be consistent in allowing a certain 'act' or otherwise.[71] When the technological programs react to one another, they may cause inconsistencies that are inconvenient to the user. Due to such inconsistencies, it may so happen that users are misled, inviting penalty provisions that should have been prevented by the rule. However, since penalty inviting conduct has occurred due to the failure of the technology, it would be unjust to apply the penalty. More so, if the user performs the act with *bona fide* intention because the code permits certain actions, it implies that the said action is 'permitted', and it would be unfair to penalize the users. In the context of blockchain, this design standard emphasizes the importance of ensuring different nuggets of the rule of code or different smart contracts do not contradict with each other, which ought to lead to conflicts or system failures.

Standard 6—This standard is in relation to the user's abstract mental state and how various legal systems deal with criminalities leading to frustration of the users because of the futility of such legal systems.[72] The focus is on the subjective position of the users rather than the legitimacy of the technologically managed action. The positioning this design standard in the blockchain environment calls for the necessity to ensure that the rule of code or smart contracts only require actions that are technically feasible within the system.

Standard 7—If a technological management application permits, or otherwise, certain actions due to either technological impairment or intentional changes made to the regulatory code, then the users become uncertain about the intention of the norm. This invites confusion among the users, which is undesirable and may lead to a diminishing of the respect that users have for the system caused by too many code changes or technological modifications, resulting in users acting in violation of the terms of the system, leading to levy of unjust penalties that may arise due to the lack of consistency.

[69] Brownsword (2016), p. 122.

[70] Brownsword (2019), pp. 121–122.

[71] Brownsword (2019), pp. 122–123.

[72] Brownsword (2016), pp. 120–121.

> Just as a lack of clarity in the law breaches the fair warning principle, the same applies to a lack of constancy.[73]

Therefore, within the blockchain architecture, there is a need to maintain a level of stability over time while still allowing for necessary updates and improvements.

Standard 8—The principle of congruence demands that in case norms are administered by automated systems, technology should faithfully follow the rules as desired. This not only presents a significant challenge to the coding of regulations but also brings up the issue of legality within the Fullerian universe of norms. The moot question is, in the context of technological management, whether congruence or the spirit of congruence is the necessary condition for the legitimacy of a specific use of technological management?[74] Whether the underlying normative rule, which satisfies or would satisfy the rule of law, is sufficient for the administration of norms? Since technological management is unlike a rule that compels the users to conduct in a particular way, whether no additional conditions are to be considered? In the true spirit of congruence, the actions of the 'figure' and their enforcement agents should resonate with the expectations of users, which are reasonable, based on the regulatory signals. It is also within the spirit of congruence that the articulation of technological management should be within the limits that have been published for its particular use as well as be coherent with background limiting principles.[75] Thus, with reference to any application, the private use of technological management, such as assessing commercial risk, should be allowed only within the publicly approved parameters. And in case new uses are intended, they should be approved through a public special procedure.[76] Appreciation of the rule of law dictates that powers should be operationalized in a way that it is *intra vires*, and the rules and principles that fix the boundaries for the use of technological management are pivotal reference points to ascertain whether there has been an abuse of power.[77] Therefore, this design standard relates to ensuring that the actual operation of blockchain systems and execution of smart contracts aligns with the State purposes and rules.

Fullerian standards are all about the need for 'openness, or transparency',[78] in authorizing the use of technological management measures for specific regulatory purposes, together with the essence of fairness and due process.[79] There needs to be an empowered set-up to frame rules and processes for adopting measures of technological management through public debates for specific uses. 'Openness, transparency, and due process' are maintained where an individual's choice and

[73] Brownsword (2019), p. 122.

[74] Brownsword (2019), p. 123.

[75] Brownsword (2016), p. 125.

[76] Brownsword (2019), pp. 123–124.

[77] Brownsword (2019), p. 124.

[78] Brownsword (2016), p. 127.

[79] Kerr (2013), p. 109.

decision-making ability are preserved.[80] As mentioned before, Brownsword has maintained the fundamental differentiation between code and the 'offline' rules which stimulate the technological measure and its use by the user. In fact, except for a casual remark about transparency,[81] he resists any engagement with the 'concrete' design aspects of the code. Though it is certainly essential that the underlying rule of policy is compatible with the rule of law, it might not be a sufficient condition to accept a specific use of technological management.[82]

Unlike Brownsword's attention toward the legitimacy of the rule of code and the sheer purpose of those rules, Asscher focuses on the idea of code and the 'figure' who is responsible for the architectural development of the technology. His thrust is not only on writing the code but also on analyzing and designing the system—whether code can function as law and the 'figure' as lawmakers and what that means to the rule of law, specifically legitimacy, and democracy.[83] He applies Fuller's principles with the intention of raising questions for the assessment of code.

The first question is whether legal rules can be distinguished from code. Hart and others have situated great importance on the conceptual notion of rules. Here, the technical commands in a code are not to be confused as rules; rather, appreciation of rules at the conceptual level is a must. As technological standards are closely associated with legal rules, both substantive rules, as well as technological standards directly impact user behavior.

> As technological standards' influence on behavior increases, they will increase in similarity to legal rules.[84]

Therefore, public government institutions and political institutions should confirm the legitimacy of choices offered by technological standards by ensuring the involvement of all parties through an appropriate control structure.

The rules at the macro level are inevitably dependent on 'technical commands within a certain computer language',[85] which is at the micro level. The rule of code at the micro level is a bone of contention, which by definition, cannot be easily set aside, and thus, it is certainly essential to emphasize, at least to some extent, what the code says and does for all intents and purposes. The failure to engage and develop a connection with the normativities that code generates permits its illegitimacies to go unchecked at the micro level, and at the macro level, the code does what it professes to do or implements the conventional rule that the 'figure' has embedded.

The second question is whether the rule of code is transparent. Is it possible for the citizens to recognize and fathom the code rules they are subjected to? Whether code can be trusted? Are the conventional rules being changed arbitrarily? In the

[80] Brownsword (2016), pp. 129–131.

[81] Brownsword (2016), p. 138.

[82] Brownsword (2016), p. 139.

[83] Asscher (2006), p. 61.

[84] Asscher (2006), p. 83.

[85] Hildebrandt (2018), p. 12.

case of computational mechanism, can the users be sure of what the function of the code is and is this the result that is expected from it?[86] While the principle of human autonomy is an important facet of democratic control, it is imperative to have knowledge of the law. Therefore, the law ought to be accessible and predictable. A reliable system of rules must be designed for consistency and a certain predictability. Such rules can act as laws only when they are not subject to irrational change at any time. This means that while analyzing the morality of code law, the unpredictability of software development and deployment provides an even greater challenge. Software is a constantly updated regulatory model; if simply keeping up is a non-trivial exercise, making meaningful predictions presents an even greater challenge.

Thirdly, whether the code is consistent not only in the temporal sense, that is, in the sense of congruence with other code rules, but also with the orthodox legal rules. This question articulates the trust that users can have in the code.

Fourthly, whether the etymology of the code rules is clear, such that the user can identify the one who is responsible for the production of a certain code or part thereof—is there a distinct sovereign who can be held accountable for the software's influence?[87] Lessig speaks of the governors of code:

> the authors of code – code writers- are a kind of governor…we should be asking, who are these lawmakers, and how do they make law.[88]

Therefore, it must identify the person responsible for writing the code and implementing the same so as to designate the code as a legitimate system of regulation. It is also imperative to ask who is responsible for a certain code rule and who has the power to modify or delete a certain code rule.

Lastly, whether the rule of code enjoys 'autonomy' and if it is appreciated through the defense of the option of whether or not to obey.[89] The choice of whether or not to obey is, in fact, an inducement to make a law that is just and rational. If a sovereign State regulates the code, then it is imperative to determine whether the user has any choice as to what components of the code he has to 'obey' and what need not be. Is it still feasible to use some sort of screen or filter and make one's own decisions with regard to the observable information, or is there only a single set of code rules over which the user has no choice and must accept entirely?

According to Asscher, the first question is relatively easier to answer, and if that question is answered in a negative, then the remaining four questions can be left unanswered or unassessed; however, this is more complex than it might seem. Questions two and three are interconnected; the reliability and accessibility of a system point to some of the basic requirements that are part of even the more basic rule systems. A failure to answer these questions shall point to a lack of legitimacy. The fourth question relates to the practical aspect. With respect to the fifth question, Asscher draws a bridge between the user's right to withhold their freedom of choice

[86] Asscher (2006), p. 84.

[87] Asscher (2006), p. 84.

[88] Lessig (1999), p. 6.

[89] Asscher (2006), pp. 84–85.

'explicitly' and the issue of competition.[90] This is in contrast to Brownsword's postulation that choice is the foundation for moral reasoning and community;[91] restoration and maintenance of the balance between the code and law is the key. This question is related to one of the elements of the conventional process of legislation and application of law, that is, the practice of balancing competing interests through democratic checks and balances. For Asscher, the Fullerian analysis of code is felicitous to evaluate whether the balance of power has moved away from institutional law towards the world of code and, whether intervention of the State is required to alter and restore the balance.[92]

Thus, when legal rules are enforced by code, the code must be (1) transparent, at least comprehensible to those regulated by it or are subjected to, (2) trustworthy and reliable so that it performs as per expectations, and is not changed arbitrarily, (3) identifiable in relation to its producers, and (4) in a position to offer the users the choice of whether or not to obey its rules. These standards will be helpful in mapping out the framework for the rule of law affordances.

References

Article 29 Data Protection Working Party (2017), Guidelines on Automated Individual Decision-making and Profiling for the purposes of Regulation 2016/679, WP 251 03.10.2017

Asscher L (2006) 'Code' as law. Using fuller to assess code rules. In: Dommering E, Asscher L (eds) Coding regulation, essays on the normative role of the information society. TMC Asser, p 61

Benthall S et al (2017) Contextual integrity through the lens of computer science. Now Publishers

Black J (2008) Constructing and contesting legitimacy and accountability in polycentric regulatory regimes. Regul Gov 2(2):137–164

Brownsword R (2015) In the year 2061: from law to technological management. Law Innov Technol 7(1):18

Brownsword R (2016) Technological management and the rule of law. Law Innov Technol 8:1

Brownsword R (2019) The ideal of legality and the rule of law. In: Law, technology and society: reimagining the regulatory environment. Routledge, p 132

Brownsword R (2021) Law 3.0: rules, regulation and technology, 1st edn. Routledge

Brownsword R (2022) Law, authority, and respect: three waves of technological disruption. Law Innov Technol 14:1

Brownsword R, Yeung K (2008) So what does the world need now? Reflections on regulating technologies. In: Brownsword R, Yeung K (eds) Regulating technologies: legal futures, regulatory frames and technological fixes. Hart Publishing

Brownsword R et al (2017) Law, regulation, and technology: the field, frame and focal questions. In: Brownsword R et al (eds) The Oxford handbook of law, regulation and technology. Oxford University Press, p 3

Casey AJ, Niblett A (2016) The death of rules and standards. Indiana Law J 92:1401

Casey AJ, Niblett A (2017) Self-driving contracts. J Corp Law 43:1

[90] Asscher (2006), p. 85.

[91] Brownsword (2015), pp. 34–39.

[92] Asscher (2006), pp. 85–86.

De Filippi P, Hassan S (2016) Blockchain technology as a regulatory technology: from code is law to law is code. First Monday 21:12. https://doi.org/10.5210/fm.v21i12.7113
De Filippi P, Wright A (2018) Blockchain and the law: the rule of code. Harvard University Press
Dimitropoulos G (2020) The law of blockchain. Wash Law Rev 95:1117
Djeffal C (2019) AI, democracy and the law. In: Sudmann A (ed) The democra-tization of artificial intelligence: net politics in the era of learning algorithms. Transcript, p 255
Djeffal C (2020) The normative potential of the European rule on automated decisions: a new reading for art. 22 GDPR. Zeitschrift für ausländisches öffentliches Recht und Völkerrecht 81:847
Djeffal C (2024) Law by design obligations: the future of regulating digital technologies in Europe? SSRN Electron J SSRN 4765471:3
Fuller LL (1964) The morality of law
Gaakeer J (2020) "Select before you collect": uses and abuses of profiling and data mining in law and literature. Pólemos 14:57–71
Goldoni M (2011) The normativity of code as law: toward input legitimacy. In: 25th IVR congress law science and technology, Frankfurt am Main
Gutwirth S et al (2008) The trouble with technology regulation: why lessig's 'optimal mix' will not work. In: Brownsword R, Yeung K (eds) Regulating technologies: legal futures, regulatory frames and technological fixes. Oxford University Press, p 193
Hagan M (2020) Legal design as a thing: a theory of change and a set of methods to craft a human-centered legal system. Des Issues 36:3
Hildebrandt M (2008) A vision of ambient law. Regul Technol:175
Hildebrandt M (2011) Legal protection by design: objections and refutations. Legisprudence 5:223
Hildebrandt M (2017) Saved by design? The case of legal protection by design. NanoEthics 11:307–311
Hildebrandt M (2018) Law as computation in the era of artificial legal intelligence: speaking law to the power of statistics. Univ Toronto Law J 68:12
Hildebrandt M (2020) Law for computer scientists and other folk. Oxford University Press
Hildebrandt M, Koops BJ (2010) The challenges of ambient law and legal protection in the profiling era. Mod Law Rev 7:428
Kerr I (2013) Prediction, pre-emption, presumption: the path of law after the computational turn. In: Hildebrandt M, Vries KD (eds) Privacy, due process and the computational turn. Routledge, pp 91–109
Kim M (2024) Dignifying law in design. In: Kim M, Jackson D, Sievert JR (eds) Legal design: dignifying people in legal systems. Cambridge University Press, pp 11–31
Latour B (2004) Scientific objects and legal objectivity. In: Pottage A, Mundy M (eds) Law, anthropology, and the constitution of the social: making persons and things. Cambridge University Press, pp 73–114
Latour B (2010) The making of law: an ethnography of the Conseil d'Etat. Polity, p 280
Lessig L (1999) Code and other laws of cyberspace. Basic Books, p 3. https://lessig.org/images/resources/1999-Code.pdf
Lessig L (2006) Code Version 2.0. Basic Books. https://tigerprints.clemson.edu/cgi/viewcontent.cgi?article=1183&context=cheer
Marsoof A et al (2023) Content-filtering AI systems–limitations, challenges and regulatory approaches. Inform Commun Technol Law 32:64
Nissenbaum H (2004) Privacy as contextual integrity. Wash Law Rev 79:119
Perry-Kessaris A (2020) Making socio-legal research more social by design: Anglo-German roots, rewards, and risks. Ger Law J 21:1427
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), L 119/1
Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

Reidenberg JR (1997) Lex informatica: the formulation of information policy rules through technology. Texas Law Rev 76:553–593

Van den Berg B, Leenes RE (2013) Abort, retry, fail: scoping techno-regulation and other techno-effects. In: Hildebrandt M, Gaakeer J (eds) Human law and computer law: comparative perspectives. Springer, pp 67–87

Wachter S (2018) Normative challenges of identification in the internet of things: privacy, profiling, discrimination, and the GDPR. Comput Law Secur Rev 34:436–449

Yeung K (2008) Towards an understanding of regulation by design. In: Brownsword R, Yeung K (eds) Regulating technologies: legal futures, regulatory frames and technological fixes. Hart Publishing, p 79

Chapter 9
Blockchain Choices and State Decisions

9.1 Blockchain as the Technological Choice

The macro-level decision-making mechanism by the State is devised to further its key interests, and as such, these decision choices have an overarching influence over the general governance architecture of the State. Studies of this institutional apparatus insinuate that the State is the 'basic building block' of the political order in the modern world,[1] and the leaders who influence and exercise the power of State authority[2] are at the 'apex' of this pyramid. These leaders are concerned with a bounded set of goals[3] that result in an advancement of the material notions of the rule of law, such as human rights. The comparative importance of these goals is adjudged on the basis of leaders' perception of the situations at the time when they are considered. The relative priorities assigned to these judgments are also contingent on many 'environmental factors' such as geography, climate, demography, geopolitics, economy, and the state of technology prevalent at that time.[4] It is important to analyze the choices made at the apex level and how these choices reflect the rule of law values. Are there any trade-offs of values? Which values have been prioritized, and why? The answers to these questions would provide valuable insights on macro-level strategic decisions that shape the micro-level choices and affordances as well as the relationship between the government officials, developers, and the user, that is, the relation between the individuals within the system and those outside of it. The 'why', 'what', and 'which' of the choices that are decided for and 'designed-in' at the macro-level must be deciphered first to understand the 'design' choices and affordances at the micro level, that is, the programming stage.

[1] Jeffrey and Painter (2008), p. 20. Roberts (2020), p. 631.

[2] Allen (2018), Chap. 1.

[3] Merriam (1944), p. 21.

[4] Gaus (2006), pp. 5–9.

A. Bisoyi, *Blockchain and Legitimacy*, Law, Governance and Technology Series 77, https://doi.org/10.1007/978-3-031-98712-0_9

Since blockchain offers a high degree of confidence, transparency, and accountability, blockchain consortiums are being adopted for public services and humanitarian purposes, which can reduce, or even eliminate, the need for centralized oversight by agencies.[5] The use of blockchain technology facilitates the fostering of new relationships between multiple actors, which are traditionally addressed through government regulation and other traditional means.

The very first choice to make is whether blockchain technology is the appropriate instrument to be deployed for the purposes of public administration services and humanitarian actions by the State and international organizations, where a system must satisfy the rule of law values to a certain extent, to obliterate any arbitrary exercise of power and corruption within the traditional institution. The blockchain architecture should protect the system from manipulation to ensure predictability and consistency, allow publicity for transparency and accountability, and have provisions to rectify for due process. As public and private blockchains satisfy different elements of the rule of law,[6] the State and international organizations can opt for either private or public blockchain depending on their priorities—access to justice or anti-corruption. However, the act of fulfilling the different rule of law values as prioritized may limit the use of the blockchain.

Blockchain-based technological artifacts can reach its full potential in different fields of development if an appropriate framework is in place. This means that blockchain applications must resonate with the rule of law values for better governance and systematized employment, especially in case of a two-pronged situation, for example, where it concerns the issue of non-discrimination as well as the productivity and efficiency-based use of technology. Nevertheless, the core principles of humanity, freedom, impartiality, and neutrality are important considerations in any technological solution. Consequently, a blockchain application in a particular public administration and humanitarian operation can be considered a suitable artifact for usage if it passes all the following tests:

1. Do the gains offset the costs of deploying this new technology?
2. Do the system requirements need an immutable digital ledger?
3. Is it essential to have a technology that supports decentralization through distribution and built-in trust through transparency?
4. Does the purpose, intention, and *ex-post* value of the proposed technology comply with the rule of law values?

Blockchain is not the right technological solution if all the answers to the above question are not affirmative, suggesting that other technological choices should be explored for a feasible solution. In addition to the above-mentioned questions, there also lies a fundamental question:

[5] De Filippi (2021), pp. 3–4.

[6] See Sect. 9.1.2 for further explanation.

> Whether the technology threatens to change the cultural environment in a way that no aspirant moral community can live with.[7]

When such a threat arises due to the technology, the State and international organizations proposing to utilize the technology should desist from deploying the technology further. This is because 'when States trade technologically guaranteed compliance for legitimacy', they strike a deal with the intention to 'dispense with a public distinction between right and wrong'.[8] However, if blockchain-based solutions reduce or eliminate the harmful consequences (maybe unintentional) of socially valued activity, then such solutions may be embraced, provided they consume a reasonable amount of resources. Of course, a higher degree of scrutiny and caution would be required if the design is embedded or targeted at living organisms.[9]

Compliance of the technology with the rule of law values is the key, where issues pertaining to infringement of the 'cultural environment of the aspirant moral community',[10] which is essentially based on the rule of law principles, would require to be addressed upholding the harm principle[11] before deploying the same where the stakes are high. This means that the 'figure' must ensure that no harm is done to the generic conditions of human dignity and the fundamental rights of the user. It follows that the 'figure' should always take into consideration the 'critical infrastructural'[12] values of the rule of law, which reflects 'the antecedents and essential nature' of human dignity and human existence and thus puts the protection and upholding of the rule of law values at a higher pedestal. At the same time, it is to be appreciated that immutability, transparency, or decentralization attributes of blockchain technology, which are considered intrinsic, are not always essential for all applications since they depend on the purpose based on which the technology is being employed.

9.1.1 Intentionality of Design

The blockchain artifact works according to its own rules and principles, which are, though not law in the strictest sense, but display law-like characteristics. Similar to traditional laws, the *lex cryptographica* of blockchain can also regulate individual behavior by coding various smart contracts into it. Since individuals' direct role in international law is limited, and the States are the primary actors in international affairs, the use of blockchains serves a dual purpose—it enables the States to expand their role in global policy-making bodies and also supports the international

[7] Brownsword and Yeung (2008), p. 48.

[8] Brownsword and Yeung (2008), p. 48.

[9] Yeung (2008), p. 104.

[10] Brownsword (2011), p. 1335.

[11] According to the harm principle, people should be allowed to do what they choose as long the action does not negatively impact another individual. Baron (1995), p. 71. Ripstein (2006), p. 215.

[12] Brownsword (2020a), p. 135. Brownsword and Somsen (2021), p. 1.

organizations to withdraw from their traditional role as implementing agency of the transnational State policies.[13] While the State can use blockchain to improve the efficiency and efficacy of public administration with better legal compliance at reduced costs, international organizations can use it as an effective instrument to realize their development goals. In fact, the utility of blockchain extends beyond these transactional goals strengthening the rule of law to eradicate corruption in public services.[14]

Though blockchain technology majorly advances the causes of democratic institutions, it is distinctly user agnostic, which means as a 'living'[15] tool, it can be used for both good and bad causes, depending on the purpose for which it was designed, which is interdependent on the intention of the 'figure'. Essentially, according to the intention of the 'figure', an artifact can either be designed as a norm-setting or norm-enforcing technology,[16] regulative or constitutive technology,[17] panopticon technology for monitoring and detecting non-compliance or exclusionary technology to eliminate the option of non-compliance.[18] The 'figure' must always take into consideration that though the technology can be intentionally designed to be used as a regulatory instrument, but more often than not, the artifact may afford an 'unintentional' use of the technology. Hence, the blockchain needs to be designed with affordances that relate to the discernment of what the software can do to bolster the rule of law.[19] It is important to recognize that there exists a diverse set of design-focused strategies where each strategy has its own unique effect on the 'moral choice', and it is also crucial to consider the 'nuanced nature of regulating by design'.[20] Depending on the design of blockchain and the way it is implemented, individuals and institutions can achieve a multitude of outcomes.

In the case of the design of conventional digital technology applications, the code can be assessed and modified to rectify the design flaws even after launching the technological artifact. Once the flaw is identified and a solution is feasible, a new version of the application or the product can be released by incorporating the changes in the code. However, in the case of blockchain, modification of code is complex since the infrastructure is immutable in nature that relies on the consensus among its network nodes, and any changes in the code require approval from the majority of the nodes in the network, resulting in invalidating the block created based on the old code. Even so, all transactions and information already processed in a blockchain application are immutably stored in a distributed ledger. This

[13] Myeong and Jung (2019), pp. 3971–3950. Wilhelm (2019), pp. 9–30.

[14] World Economic Forum (2018). https://www.weforum.org/stories/2018/03/will-blockchain-curb-corruption/

[15] De Filippi (2017), pp. 51–62.

[16] Koops (2008), pp. 157–174.

[17] Hildebrandt (2008), pp. 175–192.

[18] Brownsword (2008a), Chaps. 9, 10.

[19] Kewell et al. (2017), pp. 429–437. Zwitter and Boisse-Despiaux (2018), pp. 3–4.

[20] Yeung (2008), pp. 79–108.

necessitates the *ex-ante* design considerations to identify the attributes that would require to be prioritized over others during the design process.

Prior to choosing blockchain technology for any application, it is essential to clearly identify the problems and the expected outcomes. The State should be *au fait* with the intention and design of the technology since the artifact can be designed to demonstrate trustworthiness that supports transparency and accountability but may not actually effectuate trust. Technology crafted for trustworthiness, such as for public participation, could paradoxically exacerbate the erosion of trust.[21] In the case of blockchain, the rules governing human interactions with the technology are determined from the earliest stages of design because once blockchain technology is implemented, any further change or modification cannot be achieved easily—

> Once standards have been established, there is no opportunity for adjustment within the system itself if the standards turn out to be misaligned with their intended policy goal.[22]

It is essential to employ the rule of law by design approach to craft the artifact in congruence with the legal values to bring it closer to the 'inner morality of code'. This brings the focus on 'the law-by-design obligation', which is composed of three ingredients—

> the first is an evaluation of the consequences of the planned technology in its socio-technical environment, the second is an assessment of potential modifications for mitigation of negative consequences, and the third refers to the proportionality test which is used to appraise to what extent and how the original design is to be altered.[23]

The first step in the design process is to establish the intentionality of design through a conventional design process, that is, assessing 'the subject, aims, and purposes of the technology'.[24] It includes *inter alia* defining the problem or the 'illegitimacy' to be tackled, specifying the outcome being expected, assessing the associated ecosystem, formulating the design philosophy, and finally, determining the appropriateness of choosing blockchain as the technology solution. The contextual elements of the aforementioned steps in a conventional design approach include the blockchain community, the users of the blockchain application, the existing infrastructure, and prevalent and possible technologies that may affect the outcome.

Once the intentionality of the design is established, in the second phase, the foundational issues pertaining to legal protection and the rule of law are considered to understand their effects on the outcome. Since the precise depiction of possible negative effects maps out the inconsistencies between the design goals and predicts the impact of technology, it induces

> a search for mitigation strategies, leading to a revised design proposal that must undergo scrutiny for potential societal impacts.[25]

---

[21] Sunstein (1990), pp. 407–441.

[22] Yeung (2008), pp. 93–94.

[23] Djeffal (2024), pp. 16–20.

[24] Djeffal (2024), p. 16.

[25] Djeffal (2024), p. 16.

The House of Lords Select Committee on Artificial Intelligence suggested that the development of the code for the use of AI should satisfy the proposed five overarching principles—one, it should be 'for the common good and benefit of humanity', two, it should be based on 'principles of intelligibility and fairness', three, it should protect 'rights or privacy of individuals, families or communities', four, all citizens have the right to know and enjoy the benefits of AI, and the fifth, AI should not have the power 'to hurt, destroy or deceive, human beings'.[26] While these principles may not be expressly constitutive in nature, they certainly reveal the type of relationship that can exist between smart machines and humans. These principles, though envisaged in the context of AI, can also be applied to the blockchain, such that the technology is coherent with the principles relating to the rule of law. Through iterative assessments, every design decision is evaluated with respect to its effect on the outcome or how it will be affected by other elements of the ecosystem, such as community, infrastructure, technology, and users. Design choices, such as the type of blockchain platform and consensus protocol, have a significant bearing on the users and stakeholders as well as the desired outcome. Mapping of all significant design decisions with the key components of the ecosystem helps us to relate the design decisions with the user's perspective, the community dynamics, the role of existing infrastructure and processes, and technological choices. The ambition of such an approach is to introduce a new socio-technical setting through 'not the technology… but the technology in its environment'.[27]

There are three ranges of regulatory responsibility, which, when applied in the context of blockchain, necessitates the regulators, that is, the State and the 'figure', to consider design choices as to how they should approach the technology to ensure it aligns with the responsibilities. These regulatory responsibilities are one, to maintain the essential pre-conditions necessary for human coexistence within any type of social structure; two, to respect and uphold the fundamental values integral to that community; and three, to seek out an equitable equilibrium among competing legitimate interests. Brownsword emphasizes that the first responsibility is broad-based and nontransferable, and the second and third responsibilities are deemed to be

> contingent, depending on the fundamental values and the interest recognized in each particular community.[28]

Since blockchain has the potential to impact the foundational conditions for human existence by offering secure and transparent systems for transactions and data management, the 'figure' must ensure that blockchain applications do not compromise these foundational conditions. Ensuring data privacy and security protocols should be robust enough to protect individuals and prevent harm. That is, as Koops has so clearly elucidated—'privacy has an infrastructural character' where privacy spaces are an essential requirement to have autonomy, and in their absence, 'there is no

[26] House of Lords Select Committee on Artificial Intelligence (2018), p. 100, para. 417.

[27] Djeffal (2024), p. 17.

[28] Brownsword (2019b), p. 27. Brownsword (2020b), Chap. 17.

opportunity to be oneself'.[29] Blockchain can empower individuals by giving them greater control over their data and transactions, which demands the 'figure' to foster an environment where blockchain applications facilitate meaningful self-development and an agency reflecting the right and freedom of autonomy—'to choose one's own ends, goals, purposes, and so on; and to form a sense of one's own identity',[30] while safeguarding against exploitation or manipulation. Given that different communities may have distinct values and 'self-interest' when it comes to blockchain, the 'figure' and State should respect these values while overseeing the blockchain implementations. For instance, in a community that prioritizes decentralization and transparency, the 'figure' might focus on ensuring that the blockchain systems remain decentralized and transparent in their operations, as disallowing such developments would be judged as being contrary to the self-interest of the community. This requires the State and the 'figure' to prioritize measures that protect the integrity of blockchain networks, ensuring they remain reliable and secure, which might involve enforcing standards for data encryption, authentication, and resilience against cyber threats.

The next phase requires the proportionality test for the purposes of careful consideration and assessment of the benefits and negative impacts of the choices.[31] It is necessary for the State, along with the 'figure', to navigate the balance between promoting beneficial blockchain innovation and addressing potential risks or negative impacts.[32] This phase signifies the transition of the appraisal of the technology from 'a simplistic binary framework to a more nuanced and iterative process'.[33] At this stage, regulatory frameworks encourage innovation while mitigating risks such as fraud or misuse of blockchain systems. Equilibrium among competing legitimate interests requires opting for the choice to design the technology for the ethical use of blockchain technology, ensuring it aligns with principles of fairness, accountability, and justice, which would involve establishing guidelines for transparent governance and ethical decision-making within blockchain networks.

9.1.2 Public Blockchain or Private Blockchain?

At the macro level, decision-makers put emphasis on framing rules and norms that are drawn from historical, cultural, constitutional, and legal foundations of the rule of law, which would affect the organization, accountability, and control of a

[29] Koops (2018), p. 621.

[30] Brownsword (2019a), p. 22.

[31] Koops (2008), p. 17.

[32] The balancing of interest standard was emphasized in the Google Spain case in order to draw a line to prevent over-regulation and under-regulation. CJEU, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González,* Case C-131/12, 1305.2014, ECLI:EU:C:2014:317.

[33] Djeffal (2024), p. 17.

blockchain-based system. Keeping this in view, the State will have to make a decision on the choice of the blockchain type they want to deploy to realize their policy goals, functions and aspirations. A well-articulated comprehension of the blockchain infrastructures and their associated relationship with law facilitates the development of a legal-political economic framework of blockchain that can shape the interaction between the *lex cryptographica* and those of the physical world.[34]

As has been mentioned before, blockchain-based systems can be categorized as 'public' or 'private' depending on whom the ownership of data infrastructure rests. These systems can also be grouped as 'permissionless' or 'permissioned' based on the restrictions enforced on network participants in terms of read, write, and commit functions. While in the former, the platform is accessible to all, where anyone can participate, in the case of 'permissioned' systems, only selected bodies are authorized to participate and validate in the platform. These systems demonstrate varying degrees of decentralization, transparency, accountability, trust, security, privacy, scalability, speed, and confidentiality, according to the type of blockchain. In the case of public and permissionless blockchains, dimensions concerning transparency, accountability, trust, and security for data infrastructure get a boost, while scalability, speed, and performance are likely to be deficient. In contrast, private and permissioned blockchains permit control over data privacy and the governance of the system to a certain extent.

The choice of a blockchain system in a public administration may necessitate the trade-off of privacy for public security issues pertaining to policy priorities with the impact of the decision-making among the network actors and the organization of governance at different levels. As these trade-off conditions are context-dependent, the criticality of these dimensions varies among different public sectors. For public sector organizations dealing with security and intelligence services of the State, the privacy and security of individuals and data infrastructure are the most important and sensitive factors. However, in public service delivery and distribution systems, the transparency and immutability of public blockchains are crucial. Hence, a hard choice needs to be made by the regulators on the type of blockchain to be employed for the policy goals they are pursuing.

9.2 Infusing the Rule of Law Values

While designing a response to the 'illegitimacy' or negative impact posed by the technology, the 'figure' including the State, needs to be sensitive towards the rule of law values such as transparency and accountability and should undertake any revision of design configuration only when specifically mandated to do so. Such perceptiveness is required because, first, 'the State-sponsored code-based regulation may undermine constitutional values of transparency and accountability' and second,

[34] See Chap. 2, Sect. 2.4, and Chap. 4.

'the capacity of the private sector to employ code for private gain may override the legislatively authorized balance between competing values'.[35]

It is necessary to identify and design the conditions required to ensure the rule of law values in the architecture of blockchain and smart contracts. For the purpose of designing and configuring a technology in accordance with the rule of law, ten design '*sine qua non'* have been outlined, although in the context of regulatory design in competition law, which can also be employed for general applications. These principles can be grouped into five pairs in relation to trade-offs between them:

> independence and accountability, expertise and detachment, transparency and confidentiality, efficiency and due process, and predictability and flexibility.[36]

These '*sine qua non*' address both the constitution and operation of technology, highlighting the tensions inherent in their design. For instance, the principle of transparency necessitates a careful balancing act with confidentiality, accountability must be weighed against independence, and the need for consistency or predictability has to be balanced with the demand for flexibility. However, these interrelationships get more complicated since many of the values 'interact with each other in polycentric',[37] often mutually reinforcing or conflicting with each other. While accountability may impede administrative efficiency by necessitating contestability provisions, expertise can enhance efficiency. Similarly, confidentiality and flexibility may undermine due process, which in turn might clash with expertise. Though Trebilcock and Iacobucci's desiderata do not directly address the substance of the regulatory standards, the legitimacy of the substance is integral to the design of the technology, particularly in the tension between efficiency and due process, which reflects a broader conflict amongst utilitarian ethics favoring efficiency and rights-based ethics advocating due process.[38] The obvious conclusion is that the substance of the rule of law design standards should be assessed concerning its legitimacy prior to implementation within the technology.

The technology may not reflect the common values or norms of the society to a certain extent but rather reflect the preferences or interests of the 'figure', who may have different or conflicting agendas or motivations or moral dilemmas. Within the design of the technology, the 'figure' encounters various moral dilemmas. One of the dilemmas involves uncertainty about the right course of action, such as deciding 'whether the right thing is to tell the truth or to tell a white lie',[39] for instance, between maintaining confidentiality and making the risks transparent to the users. Another dilemma pertinent to discussions on the impact of design-based techno-regulation arises when the 'figure' acknowledges the morally correct action (e.g., keeping the promise to uphold the rule of law and protect the fundamental rights of the individuals) but is tempted by self-interest to act contrary to it (e.g., breaking the

[35] Lessig (1999), pp. 98, 135. Yeung (2008), pp. 95–96.

[36] Trebilcock and Iacobucci (2009), p. 9.

[37] Trebilcock and Iacobucci (2009), p. 9. Brownsword and Yeung (2008), p. 37.

[38] Brownsword and Yeung (2008), pp. 37–38.

[39] Brownsword and Yeung (2008), p. 41.

promise for financial gain). This scenario reflects a conflict between the autonomous moral will and the heteronomous will, driven by personal inclinations and desires. Generally, conflict involves four main elements:

> (a) awareness of the morally required action, (b) inclination or desire to act contrary to it, (c) a genuine practical choice between the two actions, and (d) circumstances facilitating the contrary action.[40]

In order to design around or design out the negativity or illegitimacies posed by the technology, the State, along with the 'figure', may require addressing any of these elements. It is necessary that the technology should be subject to democratic oversight and participation while being in harmony with the fundamental rights and principles of the legal system, which are at the core of the rule of law.

Drawing from Koops's approach towards acceptability of 'code as law' considering democratic and constitutional values, code as law should respect the principles of legitimacy, transparency, accountability, accessibility, contestability, and adaptability—which imitates the rule of law principles. Blockchain can also be considered as a form of techno-regulation and technological management as it uses code to regulate the interactions on and off the system and creates a new mode of governance. If a technological artifact is developed as a form of techno-regulation and not merely to assist traditional social constructions, then there is a choice to be made:

> to settle for less effective regulation, possibly permitting a degree of non-compliance that impinges on the rights and legitimate choices of 'victims' or, for the sake of effectiveness, to adopt techno-regulation, seemingly abandoning the importance that we attach to the dignity of choice.[41]

This decision carries profound implications for how we perceive responsibility and rights within our society. By leveraging blockchain, there emerges a novel approach to regulation that transcends the dichotomy presented. Blockchain's inherent transparency and tamper-resistant attributes offer a middle ground, facilitating effective regulation while upholding individual rights to a certain extent. Through smart contracts where the rules can be encoded into the architecture, blockchain enables the creation of regulatory frameworks that are both robust and adaptable, fostering accountability without sacrificing autonomy. In the realm of techno-regulation, blockchain emerges as a synthesis of efficiency and ethical considerations, offering a path forward that reconciles the demands of regulation with the dignity of choice and responsibility. Blockchain requires critical evaluation and regulation based on the rule of law values that ensure compatibility and alignment of the system with the morals and interests of the society, either by 'fixing the environment or by fixing humans' and through designing systems that minimize the opportunity of non-compliance. This is particularly important when technology is utilized to enhance traditional methods of prevention and enforcement while continuing to respect human rights and human dignity.

---

[40] Brownsword and Yeung (2008), p. 40.

[41] Brownsword (2008b), p. 47.

In a public blockchain, the entire sequence of blocks is stored in perpetuity. The records of all the transactions taking place in a blockchain are stored permanently, thus enhancing the transparency of the system. Since blockchain rigorously follows a consensus mechanism, the 'rouge' members in the network can neither alter historical records nor transact a business unless the requirements of the code under which the blockchain operates are fulfilled. Thus, a public blockchain has the potential for public verifiability of its records by design. It can be said that blockchain, when seen in the form of techno-regulation or technological management, can increase the transparency of transactions by making them visible and traceable on the network, but at the same time, it can also reduce the transparency of transactions by obscuring or concealing the underlying logic or purpose of the code. This may create issues of accountability, responsibility, and liability, especially when the code fails, malfunctions, or produces unintended or harmful consequences. For instance, who should be held accountable for the losses or damages caused by a faulty or fraudulent smart contract? Who should be responsible for fixing or updating the code when it becomes obsolete or incompatible? Who should be liable for the breaches or violations of the code or the law? Blockchain as an instrument should be subject to audit, review, and verification and should be compliant with the applicable rules and standards of the rule of law.

Blockchain can be designed to improve the accountability dimension within the applications by enabling dispute resolution and enforcement mechanisms. It can also impair the accountability of transactions by restricting or eliminating the recourse to external or alternative remedies and circumstances, which may create issues of justice, fairness, and redress, especially for those who are harmed or dissatisfied by the outcomes of the transactions. For example, how can a user challenge or appeal a decision made by a smart contract? How can a user seek compensation or restitution for a wrong or injury caused by a blockchain transaction? How can a user enforce a right or obligation arising from a blockchain transaction? A plausible answer lies in blockchain technology providing adequate and effective means of recourse and remedy and respecting the jurisdiction and authority of the legal system.

Likewise, blockchain can be designed to facilitate the contestability aspect by enabling feedback and evaluation mechanisms, but at the same time, it can also hinder the contestability of transactions by creating rigidity and path dependence. This may create issues of innovation, diversity, and evolution, especially for those who want to change or improve the technology or the transactions. How can a user express or communicate their preferences or opinions about a blockchain service or platform? How can a user influence or participate in the development or governance of the technology or the transactions? How can a user adapt or modify the technology or the transactions to suit their needs or expectations? Therefore, blockchain technology should allow and encourage the participation and contribution of all parties in the design and operation of the technology and should enable the flexibility and diversity of the technology.

It is difficult to achieve the desired decentralization and coordination without proper monitoring or enforcement.[42] While monitoring is required to ensure that all actors remain accountable and act in accordance with the general system of rules,[43] enforcement is necessary to ensure that all actors who deviate from these rules will be sanctioned appropriately, including exclusion from the system.[44] The problem with decentralized monitoring is that it could be construed as an invasion of privacy for the users. This issue can be addressed by adopting *ex-post verifiability* concept, using blockchain technology to record data in an encrypted and tamper-resistant manner so that its content and integrity can be verified later by the relevant agencies. Enforcement can also be achieved in a decentralized setting by means of *ex-ante automation*, using a system of smart contracts for the trusted execution of specific agreements.[45] Through *ex-post verifiability*, blockchain technology could increase the trust level of public and private institutions and, at the same time, reduce the need for global scrutiny and oversight. Through *ex-ante automation,* blockchain could also facilitate new forms of cooperation amongst different institutions by providing a trusted mechanism for coordination without depending on any centralized (trusted) agency.[46] By using blockchain, the States and international organizations should be able to ensure that specific legal and societal requirements are fulfilled before providing a particular public service or disbursing humanitarian aid to refugees by deploying a proactive and agile process embedded with the rule of law values. Such a system will efficiently eliminate corruption and patronage, as there is no need to rely on an individual or institution to record or execute a transaction, thereby strengthening the predictability and consistency of the system.

9.2.1 Blockchain for Public Services

As already discussed, blockchain applications in government structures and processes can bring qualitative changes to public services and build 'trust' into the system, which has implications on the society-state relationship for social participation as well as formulation of public policies. Out of notable use cases, a few are discussed here to understand how and why the States have made design choices and utilized the technology. These use cases draw a picture of different blockchain models employed that promote different values, such as privacy, security, and transparency.

[42] Ostrom (2001), pp. 237–256.

[43] It is important to note here that in a centralized setting, this is generally referred to as surveillance.

[44] This is usually referred to as policing. De Filippi (2021), p. 8.

[45] Hassan and De Filippi (2017), p. 90.

[46] De Filippi et al. (2020), pp. 88–90. De Filippi (2021), p. 8.

The Mexican Government, in response to the suggestions of the World Economic Forum (WEF), initiated the project Blockchain HACKMX to enhance innovation in government digital services and to improve the provision of digital public services.[47] The objective was to combat corruption and the frail rule of law in Mexico to realize its full economic potential. Blockchain HACKMX, built on the open-source Ethereum platform, is a decentralized (private) blockchain that can execute smart contracts. This tool is comprised of many smart contracts corresponding to different steps of public procurement. The system does not allow bypassing of any step in the validation process, and thus, by design, it fulfills the rule of law values of predictability, consistency, and accountability in governance. Given the distinct advantages and potential, it has been suggested Blockchain HACKMX be utilized to establish an ecosystem for the digital delivery of public services.[48]

Another relevant use case is the blockchain strategy adopted by the United Arab Emirates (UAE). As a part of Dubai Blockchain Strategy, the UAE intends to provide all public services using blockchain technology.[49] Dubai has implemented a centralized payment gateway with over 40 public and private entities for government payment collection. The system enables UAE citizens, residents, visitors, and businesses to pay online for smart services. Blockchain-based applications have also been implemented in other major sectors: commerce, real estate, transportation, security, health, education, and tourism.[50] The UAE envisages running social welfare programs, collecting taxes, providing passport and visa services, and managing land records by deploying private blockchain to ensure transparency, accountability, accuracy, and integrity in government functions.

The Government of Estonia has also been a pioneer in implementing blockchain-based technologies in public administration.[51] Its flagship project, E-Estonia, based on three technological pillars, namely 'e-ID',[52] 'X-Road',[53] and 'KSI Blockchain',[54] envisages digitalizing the entire gamut of citizen-centric activities.[55] The third component of Estonian digital infrastructure, 'KSI Blockchain', a public blockchain, is used to ensure not only the integrity and security of registries and transactions but

[47] World Economic Forum (2018). https://www.weforum.org/agenda/2018/03/will-blockchain-curb-corruption/

[48] Zbinden and Kondova (2019), pp. 55–64.

[49] Bishr (2019), pp. 4–8.

[50] Alketbi et al. (2020), pp. 1170–1191.

[51] Alexopoulos et al. (2021), pp. 1–20. Semenzin et al. (2022), pp. 386–401.

[52] e-ID is a Digital identity service which includes an electronic ID-card-based system used to access digital services.

[53] X-Road is an open-source data exchange layer solution that enables interoperability between institutional organizations. It serves to exchange information between public institutions in a secure way and allows data to be automatically exchanged not only internally but also between countries.

[54] Keyless Signature Infrastructure (KSI) is a timestamp system used for preserving the integrity of digital documents within multiple public registries.

[55] Kalvet (2012), pp. 142–157.

also the data privacy of its users.[56] This component is central to an array of services such as e-voting, e-health Records, e-prescription databases, e-law and justice systems, e-banking, and e-business Register. Here, the blockchain affords authorized individuals access to data and, at the same time, secures the data of individuals, thus, by design, incorporating the rule of law values of transparency and accountability. By deploying blockchain in its digital architecture, Estonia ensures data integrity and authenticity, making government data trustworthy in any situation. The systems are designed to harness blockchain's potential in relation to transparency and data ownership at the institutional level to foster a participatory approach toward governance. Similarly, registration of land titles can be executed on a distributed ledger to ensure that the transactions are immutable, transparent, and trustworthy.[57] Since this system can store all the details of land records, such as description, geo-coordinates, site photographs, and history of previous transactions, such a land registry would be more desirable for collaterals and credit. In case of natural disasters, land records can be recovered easily if the data is stored in a distributed ledger as compared to paper-based records.

Few other countries and organizations are also using blockchains for e-voting since coercion resistance is achieved by blockchain through its transparency and accountability by design. The province of Gyeonggi-do of South Korea used a blockchain-powered platform with reasonable success to vote on community projects. At the national level, Sierra Leone has conducted general elections by using blockchain to store votes in an immutable ledger anonymously. The electoral process, particularly with respect to control of security and agility in the process, could be better managed with this technology.[58] The proposed model for e-voting is mostly private blockchain, which allows individuals due process rights while limiting transparency and accountability of the system by design. In such a system, each vote-token transaction can be easily tracked down and accounted for. On the flip side, it may pose a possible conflict between the necessity to identify and authenticate voters and the requirement to guarantee the secrecy of the ballot as a democratic principle. Hjálmarsson[59] has proposed a solution for this by advancing the use of permissioned blockchain[60] as e-voting systems strive to achieve privacy and security goals. Each voter is assigned an identity wallet to participate in the electoral process. The voter can vote after the election administrator creates a smart ballot contract for each corresponding district node. Then the data of the voter is verified at the district node and added to the blockchain. Only voting data (not the voters) is stored in the blockchain to comply with privacy requirements. Such anonymized voting data stored are also available for review in the public domain.

[56] Semenzin et al. (2022), pp. 386–401.

[57] Wilhelm (2019), p. 4.

[58] Kshetri and Jeffrey (2018), pp. 95–99.

[59] Hjálmarsson et al. (2018), pp. 983–986.

[60] What Hjálmarsson referred to as permissioned blockchain was actually a hybrid of public and private blockchain.

9.2.2 Blockchain for Humanitarian Purposes

Though blockchain technology is being employed by States to improve the efficiency and effectiveness of public administration, it is also one of the most important instruments that assist in launching advanced information and communicative applications in humanitarian operations.[61] However, most studies focus only on improving the efficiency, coordination, and transparency of humanitarian operations without considering its impact on the humanitarian principles of humanity, neutrality, impartiality, and independence, which are in congruence with the rule of law values. In line with the values of legality or the rule of law philosophy, the primary purpose of humanitarian operations is to assist, for instance, vulnerable people, reduce their suffering, preserve human dignity, and save lives. Though the composition of offline and online human endeavors is rapidly changing due to large-scale digitization,[62] the core humanitarian principles must be preserved in any technological solution. The pertinency of an information system for any humanitarian application is contingent upon its potential to integrate humanitarian values and ensure human dignity into the application since preserving human dignity must be integral to the design of technologies for humanitarian purposes.

In humanitarian operations, the blockchain design choices are guided by the desired outcomes and a philosophical approach to the rule of law. A blockchain-based aid distribution system would require the rule of law by design approach to ensure equal and equitable access to all the members of a community. The rule of law as the guiding design philosophy would prioritize the available design choices to minimize aid distribution disparities if there are substantial inequalities in power among the members of the community. Resolving these issues at the outset of the design process provides the required legal protection and intentionality that assists in achieving design trade-offs. This process ensures that the choice of technology and other associated aspects are focused on realizing the expected outcome.

Since blockchain technology affords to increase transparency and traceability in the supply chain, several blockchain-based applications are being used to improve real-time tracking and logistics and to ensure the traceability and provenance of specific goods or services. Such systems have been implemented for humanitarian purposes since they enable improving visibility and accountability, enhancing trust, collaboration, and resilience, leveraging partnerships with logistics service providers, and facilitating resource sharing. Since blockchain allows for real-time tracking capability with respect to food, medicine, and other basic goods that are in transit for any crisis zone, the technology could be used by humanitarian authorities to trace across the globe. Though the correctness, legitimacy, or accuracy of the data stored in a blockchain cannot be guaranteed, the system discourages inaccurate or negligent information as it is always possible to trace back the source of such information due to ‘the non-censorability and non-repudiability of the information

[61] As has been identified in Chap. 2.

[62] Zwitter et al. (2020), pp. 26–39.

recorded on a blockchain'.[63] Moreover, blockchain-based systems can be designed not only to record and track the virus in the event of a pandemic, but also to keep track of various tests and vaccines provided to people without impinging upon their privacy too much. Such monitoring is feasible by following the 'transparency by design' mechanism in public blockchain and is helpful to achieve the rule of law and humanitarian values optimally.

The blockchain-based supply chain system has been incorporated and deployed effectively to combat human slavery and exploitation. For example, a blockchain-based project to track tuna fish from 'bait to plate' had been launched by the WWF in Fiji.[64] The idea is to tackle the modern slavery and human rights abuses prevalent in the fishing industry. In this project, the journey of each tuna fish is recorded to ensure that they are not obtained from illegal fishing boats that are prone to slavery and exploitation. Each tuna fish, when caught, is tagged with a radio-frequency identification (RFID) tag and a quick response (QR) code. These tags are then stored on the blockchain and scanned at multiple points as they move to the market. Even after processing, by linking the QR code tags on the processed fish packages with the information stored on the blockchain, it is possible for the user to verify that the fish has been sourced from legal fishing boats that do not engage in modern slavery and human rights abuse.

Another issue that affects the humanitarian operations relating to refugees is their lack of proper identification documents. The blockchain's architecture has the potential to change the way we interact with data. Users' data can only be shared among partners and entities in the exact same way it was recorded, canceling out any chance of fraud and secretarial errors due to the immutable characteristics of blockchain. The focus is on having a public ledger that, by design, affords transparency and accountability, where everyone is the owner of their digital identity, as envisioned in a decentralized governance model. As many refugees fleeing from a conflict zone do not possess identification documents, they are often subjected to exploitation and human trafficking. In the absence of any document establishing their citizenship, it becomes impossible to legally transact with such people and to provide humanitarian aid. Since such people are not tracked by any government, they easily become victims of modern slavery with no clear citizenship. Even if the victims of modern slavery have identity documentation, the same is confiscated by the 'rouge' employers to exploit them at the workplace and control their movement. This problem can be addressed by storing unique biometric data, such as fingerprint and iris scans of the victims, and creating a virtual identity on a blockchain. As the records on the blockchain are immutable, forged identification documents cannot be created by the traffickers to illegally transport victims over borders. When the identities can be verified by using the information stored on a blockchain, the import of physical identity documents is greatly diminished. Human traffickers and rouge employers cannot control and exploit victims by confiscating physical documents,

[63] De Filippi (2021), p. 4.

[64] Cole et al. (2019), p. 469–483.

and as a result, the vulnerability of paperless refugees to trafficking will also be reduced. As blockchain by design is not bound by physical boundaries, the identification information could be accessed anywhere in the world if access to that blockchain application is available through the internet at that location.

9.3 Design Choices for Blockchain-Based Systems

As blockchain applications are designed to apply the same set of rules consistently to all transactions without any exception, their use in the public sector and humanitarian domain improves predictability and consistency. While normative use of blockchain demonstrates increased efficiency in public management and humanitarian purposes, it can potentially incorporate the rule of law values beyond such transactional goals. There are disagreements about which rule of values would be or ought to be augmented into blockchain. There needs to be, thus, more agreement on how a blockchain should be designed in relation to the concepts of transparency, accountability, and legal certainty.

While designing a blockchain application for the public sector and humanitarian sector, it is imperative to critically analyze the governance decisions at the macro level to figure out how the decisions impact each other and what design choices are feasible to fulfill the requirements of the rule of law values and how do such decisions affect the principles of transparency and accountability.

9.3.1 Infrastructure Architecture

The decisions concerning the infrastructure architecture of blockchain applications are primarily about the type of blockchain—private or public, depending upon the ownership of infrastructure. Since these classifications are not watertight, deploying a hybrid blockchain with certain permissions is also feasible. Public and permissionless blockchains are adopted in situations where trust and security in the context of transparency and accountability are the principal concerns and not scalability and performance. If it is desirable to control data privacy and security, then private and permissioned blockchains are primarily used. This choice would be contingent upon the rationale of deploying the technology or the functions that the State or the international organizations want to attain consistency with the rule of law values and commitments. While designing a blockchain-based application, a tussle between the technology and the rule of law values inevitably takes place.

'Equality before law' necessitates that all individuals are subjected to the same set of rules and due process mechanisms, including the right to access and rectify the relevant information and the right to seek remedy against a decision, which is allowed in all cases without discrimination. If blockchain technology is deployed, then the transactions would be automatically executed as per preset rules, and the

individuals will not have any access, nor can they ascertain the correctness of the input data used for a specific transaction. Only with a special built-in mechanism designed to incorporate changes at the programming stage can any change be affected in a public blockchain, which is immutable in nature. Though such a system is advantageous for being predictable and consistent, there is no way of making an appeal against a decision to undo the same. As such, the blockchain application may weaken the due process rights of individuals due to a lack of intelligibility in the decision-making process and, hence, fail to challenge the decisions that affect them. A private blockchain, conversely, can allow changes.[65] In a way, the choice to promote some rule of law values through blockchain may lead to the undermining of certain other values and characteristics.

Design features and actual execution determine the transparency, accountability, predictability, and consistency of a blockchain application. While blockchain technology invariably comprises of encryption and anonymity attributes, a public blockchain supports transparency and peer validation. In a public or permissionless blockchain, all the information is stored in blocks permanently, and every transaction is available as a public record, ensuring transparency and accountability by design. As a design solution, it offers immutability except when the majority of nodes take contrarian decisions, and it provides consistent and predictable results by eliminating the probability of appeal to negate a decision. In such blockchains, transparency clashes with the classical concept of privacy since everybody can see others' transactions. A permissioned or private blockchain, however, allows the participants with the necessary permission to control the transparency. In such applications, citizens cannot access all transactions and history of modification unless granted the requisite permission. Since subsequent changes are not possible post-implementation unless specific provisions are made while designing the blockchain application, there could be friction between blockchain and the rule of law values.

It seems that governments prefer private blockchains to deliver public services since such blockchains allow them to retain centralized control at the expense of certain rule of law values such as transparency. Priorities of the government—anti-corruption or access to justice, are the deciding factors for adopting a particular type of blockchain—private or public. Depending upon the design choices for infrastructure architecture, various trade-off conditions vary.[66] If building trust among the users is the foremost reason, then transparency is given precedence over other properties such as performance, flexibility, and usability. However, decisions regarding infrastructure architecture are invariably political and involve optimization of the trade-off conditions.

Since blockchain technology has been specifically designed to be tamper-resistant, the erasure of records is not a choice, especially in the case of public blockchains where there is an additional degree of data being fragmented among

[65] Yeung (2019), p. 28.

[66] As many as twenty-three endogenous trade-off conditions among seven blockchain properties such as usability, performance, flexibility, security, transparency, law & regulation, and community have been identified. Kannengießer et al. (2020), pp. 1–37.

multiple nodes, possibly in different jurisdictions. When such fragmented data is encrypted, it becomes virtually impossible for the data subject to know who exactly has the particular data. The controller of the node also does not know whose data they have. In comparison, permissioned blockchains or private blockchains are quite distinct to the extent that it is possible for the controller to make a copy of specific blocks for the data subject and then anonymize them, leaving only a binary trace. Such characterization of public and private blockchains is extremely important concerning the protection of data in situations where a technological tool is used to transact and record the personal data of vulnerable populations such as refugees, trafficking victims, etc. When seemingly innocuous transactions are tagged with real-time locations, even simple data points can be sensitive and life-threatening for refugees, victims of human trafficking who have escaped, or political dissidents who are on the run. A single data set can have catastrophic potential if it falls into the wrong hands. The dangers posed by a potential data breach or fault in security are real, which gets further amplified in the case of the personal datasets garnered during humanitarian action. In a normal business transaction, personal data is collected and processed as per bilateral agreement with both sides having equal say to agree or disagree to data sharing. But, in the case of humanitarian aid, the circumstances do not favor the user, who has little option but to agree to user data collection in case of emergency assistance. Seeking aid in adverse situations is not the same as applying for a club membership. Permitting someone to collect biometric data from an individual who is in distress, disorganized, scattered, and comparatively less technically literate is not comparable to that from an individual in normal or favorable situations.

This illustrates the profound importance of data collected in aid and relief efforts, making it abundantly clear that the protection of the data of users necessitates not only setting up a comprehensive legal framework but also to design systems that represent political and moral principles. Therefore, when blockchain is deployed as an instrument to record and store user data, the 'figure' ought to analyze how the technological artifact can empower individuals and groups to participate in the decision-making processes and also protect their interest with this data. But the moot question is, once a blockchain application is operational in the humanitarian sector with the informed consent of the users to process their data on the blockchain, what would happen if the users decide to withdraw their consent? For example, if a refugee who has been participating in a humanitarian program and has been receiving aid automatically for a long time by virtue of data being stored in a blockchain, one can safely assume that the welfare of the refugee is favorably bound to the system. If such a refugee decides not to receive aid in this manner anymore, then what should be the recourse? Hence, the blockchain architecture should be designed to have some reasonable tussle points in the withdrawal process while complying with the legal requirements. This issue goes beyond legal compliance and into the realm of human dignity and the rule of law. The ability of people to autonomously decide the degree of involvement with a specific system and to choose the data

collection and processing methods is the pivotal pillar of the data justice 'disengagement with technology' concept.[67]

Certain conditions, particularly the capability to access information and to consent, being part of a violently displaced population, render consent ineffective. In these circumstances, rather than relying on consent, collecting and processing data for 'the vital interests of the subjects' would be prudent until the prevention of immediate danger. As already explained, while blockchain secures data, it makes its users too technology-dependent, which is rather burdensome. This aspect of blockchain needs to be considered carefully so as to provide authentic autonomous choices representing the unique values and needs of individuals and groups.

Since the technology of the artifact allows design and built-in features that promote the rule of law, the artifact must be accepted and trusted in society. To ensure that the technical specifications of the application correspond to legal requirements, both technical and legal experts are involved in the design, development, and testing stages. Education and public awareness about the trustworthiness of blockchain applications are also important. Furthermore, as in value-based design, it would be required to track the rule of law values against the system's technical requirements and undertake expensive purpose-built open-source software. The legislative changes must also be affected wherever needed to ensure legal compliance.

As for blockchain, the limitation is that it is yet to implement disparate rule of law values simultaneously. While adequate publicity is required to foster transparency and accountability, rectification is necessary to facilitate due process. Safeguards are also essential to infuse predictability and consistency. Unless these concerns are addressed, the much-discussed advantages of the rule of law may not accrue to the general public.

9.3.2 Decision-Making Mechanism

The decision-making mechanism depends upon whether it is an on-chain or off-chain governance process.[68] In the case of on-chain governance, the proposal, participation, and decision-making process are embedded within the technology architecture through a protocol, that is, the rule of code constitution in the form of programming language. Since the decision-making procedures have been encoded in the blockchain infrastructure, the protocol executes the decision automatically once the pre-determined set of rules has been fulfilled. On-chain governance appears to be the preferred mode of governance as it ensures that no individual or group can impose their will on the blockchain community. Such a mode of governance embraces key ideas of legal positivism, notably, the type of positivism espoused by

[67] Currie et al. (2022), pp. 1–18.

[68] Reijers et al. (2018), pp. 1–20.

Kelsen,[69] which intends to exclude any notion of private human judgment within law-making and also to settle disputes by enforcing processes based on rational, factual tests only.[70] It does not matter who makes the laws or who is the sovereign as long as the automated process of law-making and enforcement is working well.

In a blockchain-based system, the validity of the transactions is not determined by their contents but by their conformity with the factual and mathematical verification process. This has an uncanny similarity with Kelsen's legal theory—

> by presupposing the basic norm (…) one ought to behave as the constitution prescribes.[71]

In an on-chain blockchain governance system, once a basic norm is presupposed, one has to behave as the protocol or the rule of code prescribes. All the decision-making rules and processes embedded in a blockchain are derived from this basic norm. On the contrary, in the case of off-chain governance, which looks like real-world politics, decision-making is based on internal and external rules and processes.[72] In this case, external interventions into the blockchain that are not prescribed by the protocol are allowed. While it portrays a democratic alternative to the rigid on-chain governance model, it intrinsically introduces the problem of personal sovereignty by allowing strong individuals to dominate the decision-making processes.

This plutocratic behavior of blockchain is not just limited to off-chain governance. Similar behaviors are also noticed in on-chain governance processes. As the on-chain governance manifests the features of a positivist legal system, it gives rise to competing private interests.[73] In a sense, on-chain blockchain governance systems are vulnerable to private participants, similar to the way the liberal democracies are but not to a greater degree like off-chain governance. Ultimately, all such systems shall lead to corporate consolidation or to plutocracy.[74] The blockchain-based systems do not offer a combination of democratic and plutocratic decision-making processes. In fact, such systems implement an exclusively plutocratic governance structure, particularly in on-chain governance.[75] What sets blockchain-based systems apart from the State is that their participants are free to leave or to implement a hard fork[76] in order to launch a new voluntary community.

---

[69] Kelson believed that laws are valid if promulgated in accordance with the 'basic norm' of the legal order and with the legislative procedure that is authorized by this basic norm. Kelsen (2017), pp. 110–122.

[70] This is most evident in Kelsen's conception of a pure legal rule.

[71] Reijers et al. (2018), p. 6. Kelsen (2005), p. 202.

[72] Reijers et al. (2018), p. 2.

[73] Schmitt (2005), pp. 48, 63.

[74] A plutocracy implies government or rule by the wealthy and consequently favors private interests over the common good.

[75] Reijers et al. (2018), pp. 16–18.

[76] A hard fork involves a significant and non-backward-compatible modification to the network's protocol, which has the potential to lead to the emergence of a distinct blockchain if a consensus is not achieved.

9.3.3 Accountability Mechanism

Accountability at the macro level is about regulating and enforcing rules in governance matters such as dispute resolution and change management. In blockchain governance, it is feasible to identify four forms of accountability mechanisms: coercion, voluntarism, targeting, and framework regulation.[77]

Coercion is typically associated with regulations and detailed procedures that are rigid and binding. The concept of *lex cryptographica* is representative of coercion in blockchain applications. In this mechanism, smart contracts are executed mechanically in a deterministic manner as per the rigid rules already encoded in the blockchain. Since codes must be written at the design stage prior to their implementation, it inherently limits the usefulness of code-based rules. This is particularly challenging in areas where it is not possible to determine the possibilities beforehand. The self-enforcing nature of blockchain instruments significantly tilts the power equations in favor of the 'figure' who establishes the regulatory code standards as compared to the users.[78] Voluntarism is about governance by legally non-binding instruments and implementing rather broad goals. In a blockchain, soft forks would represent the principle of volunteerism. In this approach, the functions are modified while the structure of the blockchain remains unaltered. In the case of targeting, detailed regulatory procedures (though non-binding) are used. Initiating improvement proposals and digital applications in a blockchain could be considered as examples of targeting. Finally, in the case of framework regulation, the mechanism favors binding rules but with a tweak that users may or may not agree to policy options. Hard forks in a blockchain are examples of framework regulation; when a rule is modified and adopted in the blockchain, then the older version is not accepted by the nodes of the latest blockchain.

9.4 Legitimacy of Using Blockchains

Since legitimacy is a prerequisite to ensure loyalty, a system must be constructed in such a way as to be perceived as legitimate. In a blockchain system, 'legitimacy is one of the most important scarce resources' and is the main social force that directly impacts its governance.[79] Legitimacy may be defined as a 'higher-order acceptance' occurring in contexts in which 'large groups of actors [...] work together for their common interest'.[80] It is a descriptive phenomenon that refers to the community acceptance of a blockchain system, which depends on whether most people find the traits of the system as 'psychologically appealing'. The traits that appeal to most

[77] Treib et al. (2007), pp. 1–20.

[78] Yeung (2008), pp. 94–95.

[79] Buterin (2021). https://vitalik.eth.limo/general/2021/03/23/legitimacy.html

[80] Buterin (2020). https://nakamoto.com/credible-neutrality/

blockchain communities are brute force, continuity, fairness, process, performance, and participation. When a blockchain-based system exhibits these traits, the community perceives it to be legitimate.[81]

As per law, States have the sole recognition as legitimate actors,[82] who can create and confer legitimacy through specific constitutional provisions that restrict the discretionary or arbitrary power of certain agencies, individuals, or groups of individuals.[83] This recognition extends to the framework of international organizations, which upholds the conventional model of legitimacy within international law. As such, these organizations, constituted by States, are accountable exclusively to them. As far as the legitimacy of international organizations is concerned, it is intrinsically linked to States on a 'transmission belt'. This transmission belt mechanism links domestic institutions to national governments, which in turn connects with international organizations and further to their governance institutions and compliance mechanisms.[84]

When the blockchain is employed by the State directly, it is considered legitimate by virtue of the State being the 'sole' will of the sovereign. The use of blockchain by international organizations also requires this orthodox model of legitimacy to justify the employment of the technology, or else there would be conflicts with the sovereign legitimate actors. For example, the issuance of identification documents falls within the competence of the State. This function of the State, in certain circumstances, may be delegated to international organizations when they are authorized to issue such documents, for instance, with the use of blockchain.[85] A dispute can very well arise between the State with a traditional document identification system and the international organization with its records in the digital ledger pertaining to the legal validity of identification documents issued by them. A sovereign State may refuse someone who is not in its records but possesses a digital identification document issued on blockchain by an international organization. Since the transmission-belt legitimacy in international law is considered weak,[86] the widespread use of blockchain in international organizations must be favored by the traditional model of legitimacy. Since international organizations have been vested with powers that impact the sovereign states and private stakeholders, particularly in the matter of human rights, alternative legitimacy frameworks that can substantiate the use of blockchain by these institutions have to be sought in 'deliberative democracy' models.[87]

---

[81] Buterin (2021). https://vitalik.eth.limo/general/2021/03/23/legitimacy.html

[82] Buchanan and Keohane (2006), pp. 412–417.

[83] De Filippi et al. (2022), p. 31.

[84] Peters (2016), p. 11. Dellmuth and Tallberg (2015), p. 457.

[85] This is a hypothetical example.

[86] Dellmuth and Tallberg (2015), p. 454.

[87] Berman (2005), pp. 485–556. International Law Association (2004) https://www.ila-hq.org/en_GB/documents/final-conference-report-berlin-2004-1

The focus on *ex-post* legitimacy emphasizes on the output of the actions of the public authorities. It is about the effectiveness of the rules or the extent to which the rule delivers the result effectively and efficiently.[88] As long as a decision or a rule produces desirable policy outcomes, the same may be considered legitimate. Efficacy, enforcement, and coverage are important standards to evaluate *ex-post* legitimacy.[89] *Ex-post* legitimacy also resonates with substantive legitimacy, which is about the actual substance of the decisions and rules with respect to principles such as justice, democracy, and human rights, which are held in high esteem in society. Using blockchain technology to serve humanitarian causes and public services is likely to be more legitimate from the lens of *ex-post* legitimacy. However, since one form of legitimacy may not compensate for other forms of legitimacy, it is also essential to increase the *ex-ante* legitimacy which canvasses the input and procedural legitimacy.[90]

9.4.1 Legitimacy Through Trust and Confidence

In blockchain systems, the actions of the network participants can be constrained by the rule of code using on-chain mechanisms. The rule of code does not mean that such rules would always be considered legitimate. There are two interrelated aspects—trust and confidence, which must be accounted for to probe legitimacy. Confidence in the system stems from 'the predictability' attribute drawn from the code-based technological certainty of a blockchain and its on-chain governance structure. Although the 'governance by the infrastructure' gives rise to confidence, the 'trust' factor needs to be considered since the off-chain governance, or the 'governance of the infrastructure', is unpredictable and uncertain. 'Trust' and 'confidence' in blockchain systems are inherently interrelated because it is essential to have trust in the underlying governance structure of a blockchain network to instill confidence in the functioning and technological certainty of a blockchain-based system.[91]

Continuity, process, and performance are key to increase confidence in a system.[92] A system ought to have confidence-building and trust-building elements in the right proportions to establish its perceived legitimacy. If confidence elements are in deficit due to a lack of process and performance certainty, then the requirement of trust will be 'more' towards perceiving the system as legitimate. However, the contribution of trust to legitimacy may not be enough to guarantee such legitimacy.

---

[88] Scharpf (1999), pp. 16–28.

[89] Mastenbroek et al. (2016), p. 1336.

[90] See Chap. 10 for further discussions.

[91] De Filippi et al. (2022), pp. 16–19.

[92] Buterin (2021). https://vitalik.eth.limo/general/2021/03/23/legitimacy.html

> Principles and values such as fairness and the ability to contribute meaningfully to governance in terms of participation are necessary additional ingredients.[93]

Since a veritable 'trustless' system with perfectly codified rules does not provide enough space for trust, participation, and freedom from decision-making, too much confidence also hinders the system's legitimacy. As the 'trustless'-ness leads to the elimination of individual agency, it may decrease the legitimacy of the system since the users and participants perceive that they do not have any constructive role in the development of the functioning of the system.[94] Similar to a legitimate government that uses its coercive authority to preserve the liberty and equality of individuals, a blockchain system must enforce the coercive authority of the rule of code to preserve individual autonomy and agency to be perceived as legitimate.

9.4.2 Legitimacy Through Transparency and Choice

The blockchain technology embraced by the States for public service delivery applications is not public blockchains per se; rather, these are private blockchains being used for public purposes. With technological developments, States increasingly use more private and permissioned blockchains as compared to public permissionless blockchains. In fact, international organizations have mostly opted for private and permissioned blockchains to achieve their policy objectives. This not only diminishes their legitimacy from the standpoint of participation and transparency as the mode of legitimation but also brings up *ex-ante* legitimacy issues. Since the private permissioned blockchains used in the operation of international organizations do not allow any voice to the individuals (outside of the system, such as the user, since the governing body of such systems usually comprises public officials), it may infringe the fundamental right of an individual to exercise freedom of expression. Ultimately, the substantive legitimacy of international organizations is harmed due to the use of private permissioned blockchain because of the contradictions between those who have access to blockchain and those who do not.

The 'privatization' of blockchain in international law may stifle the blockchain innovation,[95] that has been instrumental in providing free access to all individuals desirous of participating in the network. Being public institutions, international organizations should avoid the privatization of blockchain and deploy public permissionless blockchains to pursue their goals. However, one cannot say with certainty that there are no issues in using public permissionless blockchains under international law. As a matter of fact, some of the typical characteristics of blockchain that are supposed to protect may be harmful to individuals under certain conditions.

---

[93] Levi (2019), p. 368.

[94] De Filippi et al. (2020), p. 7.

[95] Dimitropoulos (2022), p. 337. Mandel (2009), pp. 75–92.

> In many cases, they [refugees] abandon everything, and it's a big problem when they don't have any way to prove who they are to the refugee camp. So, there's a lot of discussion about using blockchain technology to give someone a digital identity. The risk that you run into there is creating a very robust, hard-to-change record that collects everyone's data. If you were a refugee, would you really want to become part of this system? Why would you trust this party and trust that they're not going to go give it to your government? There remain many hard questions here.[96]

The grand intention of blockchain has been to entrust economic and political power to individuals or users, bypassing public and private intermediaries, including the State. In reality, however, private miners have the power to use commercial server firms to validate transactions on the blockchains and the 'figure' as a private entity works on the further development of the blockchain code. Therefore, it is necessary that the 'figure' behave with integrity and reasonableness, indicating that their decision-making procedures are transparent and inclusive. The decisions of the 'figure' should be explainable to the user in a manner that plausibly connects to these procedures. If the 'figure' struggles to meet this standard, perhaps due to reliance on 'smart' technologies that function effectively but are 'alien' to humans, a resolution must be reached, where either regulatory dependence on the technology reduces or user expectations shift—

> it is not yet possible to generate thorough explanations for the decisions that are made, this may mean delaying their deployment for particular uses until alternative solutions are found.[97]

A contrarian notion of 'public-ness' or 'transparency' that the advocates of blockchain say is that it is about having universal access to public resources, irrespective of the origin of the technology. In that sense, international organizations' operations should be at least accessible to the individuals and the States concerned. The legitimacy issues concerning international organizations may be addressed by means of public permissionless blockchains utilizing the concept of 'transparency by design'. Since the established aspects of 'public-ness' are not to be disregarded, international organizations would be required to intervene to rectify transactions that are considered erroneous in the real world or that would be treated as irregular under international and domestic laws. For example, if refugees are not provided with any dispute resolution mechanism within the blockchain application and their issues are not addressed by rectifying the transactions (account details, etc.) to render justice, they would be deprived of access to basic needs.

> Techno-regulation approaches the problem of social order in a way that does not rely on building normative consensus; it is amoral; it does by-pass the realm of values; and it does not rely on moral discipline or obedience to authority. ……it bypasses practical reason altogether … far from a normalizing crime, techno-regulation seeks to eliminate it as an option.[98]

---

[96] Walch (2018), p. 30.

[97] House of Lords Select Committee on Artificial Intelligence (2018), p. 40, para. 105.

[98] Brownsword (2005), p. 13.

When individual decisions and actions are outside the scope of the code architecture in a blockchain, the users lose their ability to seek a remedy through human reasoning and judgment. This implies that when the 'figure' restricts the individual's capacity to engage in moral deliberation and decision-making, it undermines the essential conditions for a thriving moral community. In such cases, the 'figure' wields greater influence over the users compared to the lawmakers, effectively elevating their authority. However, a moral community will grow only if the individuals are competent to choose. They must have the choice to choose both right as well as wrong.[99] Having greater accountability towards the rule of law values of the society,[100] the increased power enjoyed by the 'figure' calls for closer attention to the design failures while instituting regulatory-coded standards. There may be a need for the State to close down a blockchain system by attacking the gatekeepers within their jurisdiction, because some blockchain systems may be too widely distributed such that it may get difficult to be restricted by the States.[101]

Such conflicts can only be settled normatively by developing meta-norms that go beyond the law as well as blockchain. A reasonable equilibrium of conflicting interests within a particular community can be achieved by respecting the requirements for sustained social existence, aspirations, and fundamental values of the community. It is emphasized that technological tools should only be used for regulation if they conform to a threefold legitimacy licensing framework, which includes 'a global common license, a community license, and a social license'.[102] The foregoing discussions on the legitimacy of the use of blockchain by international bodies indicate that there is a need to move beyond the traditional legitimacy and governance models. A three-level test can be applied to the blockchain, which would require the technology, in order to be legitimate, to hinge on the design choices for being globally accessible, community-endorsed, and socially accepted, which are the ideals inscribed in the rule of law. Firstly, it accentuates that any technological measures, including blockchain, must be compatible with the 'preconditions for human social existence and the global commons'.[103] In the context of blockchain, this could mean ensuring that the technology respects principles such as privacy, security, decentralization, and sustainability. Blockchain applications should prioritize data protection, transparency, and accountability so as to align with the rule of law values. Secondly, it highlights that the design choices in the blockchain should align with the fundamental values and preferences of the particular community for which the technology is being employed. Blockchain designs should reflect the unique cultural and ethical standards that define such a community. Different types of blockchains and their specific purpose and aspirations of usage have varying priorities and principles. For instance, some communities may prioritize absolute

[99] Yeung (2008), pp. 97–98.

[100] Yeung (2008), p. 95.

[101] Wright and De Filippi (2015), p. 50. Schillig (2023), p. 44.

[102] Brownsword (2020a), pp. 71–76.

[103] Brownsword (2020a), pp. 71–72.

decentralization and censorship resistance, while others may prioritize scalability and efficiency. Thirdly, it requires the 'figure' to engage in transparent and inclusive processes to reach a reasonable accommodation of diverse views and concerns within the community, particularly on the values of innovation versus its risks.

A reasonable equilibrium should not be seen as an abandonment of the core of all legitimacy models, that is, 'public power is and should eventually be accountable to the public',[104] but should be seen as an upgraded version of the traditional legitimacy model. This is important because, in a democratic environment, international institutions, including blockchain, will prosper only if the public considers them to be legitimate entities.[105]

9.4.3 Legitimacy Through 'Human in the Loop'

Another factor in enhancing the legitimacy of the technology is the 'human in the loop' factor or 'democratic oversight'.[106] The main idea behind it is that for *ex-post* legitimacy, while blockchain can automate processes and remove the need for intermediaries, there are still decisions that may require human judgment, especially in situations with legal or ethical implications. This technology operates on predefined rules and consensus mechanisms, but certain essential tasks may still necessitate human intervention. These tasks could include governance decisions, dispute resolution, or ensuring compliance with legal frameworks. Even within decentralized systems, there may be a need for human oversight to uphold fairness, accountability, and justice. One can also find a similar emphasis on human intervention under Article 22 of the GDPR, which imposes a prohibition on 'solely automated decisions that have legal or other significant effects' in relation to an individual[107] and provides for humans to be brought back to the loop. Blockchain systems must also consider the implications of automated processing. This involves ensuring transparency, accountability, and mechanisms for human intervention where necessary to address biases, errors, or unforeseen circumstances.

Design choices in blockchain systems influence their legitimacy and acceptance within communities. These choices encompass governance models, consensus mechanisms, privacy features, and mechanisms for human oversight. Transparent and inclusive design processes that consider ethical, legal, and social implications can enhance the legitimacy of blockchain systems. There are three different aspects

[104] Brownsword (2020a), p. 76.

[105] Buchanan and Keohane (2006), p. 407.

[106] See the next chapter for a detailed discussion on this as an affordance of accounta-bility that is necessary to be incorporated within the blockchain architecture.

[107] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), L 119/1 (hereafter GDPR), Article 22.

of mental models of the technological architecture: one, 'the design model', which is the mental conceptualization of the 'figure'; two, 'the user's model', which the user will develop to elucidate the functions of the system, and three, 'the system image' which the 'figure' uses to communicate and respond. While the 'design model' and the 'user's model' are ideally equivalent, the 'system image' is critical to ensure consistency because the user and the 'figure' use the physical appearance and functions of the system to communicate through the system.[108] The 'figure' needs to make design choices, bearing in mind the system image, which is critical to ensure that everything about the blockchain application is consistent with and exemplifies the operation of the proper conceptual model in adherence with the fundamental rights of users, transparency and accountability *vis-à-vis* the rule of law, such that the artifact is legitimate.

Within the blockchain, the code assumes the role of 'law', whereby the technology permits law to transmute into code. This supports *lex cryptographica,* which has the potential to remove ambiguities present in the law and make the interpretation and administration of laws by traditional enforcement agencies progressively redundant. So much so that blockchain could even challenge the sovereignty of the State. Though blockchains are considered to be self-enforcing 'technical' machines, they are not so in reality. These are developed and crafted by humans, and so also their regulations, that is, the rule of code. As blockchains and their regulation depend on human decisions, which are subject to political or other interests for internal governance and user functions, the bias of the 'figure' also affects the code and underlying algorithms and causes prejudiced and unjust treatment of the users. This necessitates the mitigation of the *crypto-legalistic* characteristics of the rule of code to attain *ex-ante* legitimacy to a certain degree.

References

AI in the UK: ready, willing and able? House of Lords Select Committee on Artificial Intelligence (2018), 100, paragraph 417

Alexopoulos C et al (2021) How blockchain technology changes government: a systematic analysis of applications. Int J Public Adm Digit Age 8(1):1–20

Alketbi A et al (2020) Novel blockchain reference model for government services: Dubai government case study. Int J Syst Assur Eng Manag 11(6):1170–1191

Allen P (2018) The political class: why it matters who our politicians are. Oxford University Press. Chapter 1

Baron J (1995) Blind justice: fairness to groups and the do-no-harm principle. J Behav Decis Mak 8:71

Berman PS (2005) From international law to law and globalization. Colum J Transnatl Law 43:485

Bishr AB (2019) Dubai: a city powered by blockchain. Innov Technol Gov Glob 12(3–4):4–8

Brownsword R (2005) Code, control, and choice: why east is east and west is west. Leg Stud 25:1

Brownsword R (2008a) Rights, regulation, and the technological revolution. Oxford University Press

[108] Norman (1988), pp. 180–190.

Brownsword R (2008b) So what does the world need now? Reflections on regulating technologies. In: Brownsword R, Yeung K (eds) Regulating technologies: legal futures, regulatory frames and technological fixes. Hart Publishing
Brownsword R (2011) Lost in translation: legality, regulatory margins, and technological management. Berkeley Technol Law J 26:1321
Brownsword R (2019a) Law disrupted, law re-imagined, law re-invented. Technol Regul 2019:10–30
Brownsword R (2019b) Law, technology and society: reimagining the regulatory environment. Routledge
Brownsword R (2020a) Artificial intelligence and legal singularity: the thin end of the wedge, the thick end of the wedge, and the rule of law. In: Deakin S, Markou C (eds) Is law computable: critical perspectives on law and artificial intelligence. Hart Publishing, p 135
Brownsword R (2020b) Law 3.0: rules, regulation, and technology. Routledge
Brownsword R, Somsen H (2021) Law, innovation and technology: fast forward to 2021. Law Innov Technol 13:1
Brownsword R, Yeung K (2008) Regulating technologies: legal futures, regulatory frames and technological fixes. Hart Publishing, p 48
Buchanan A, Keohane RO (2006) The legitimacy of global governance institutions. Ethics Int Aff 20:405
Buterin V (2020) Credible neutrality as a guiding principle. Nakamoto. https://nakamoto.com/credible-neutrality
Buterin V (2021) The most important scarce resource is legitimacy. Vitalik Buterin's Website. vitalik.eth.limo/general/2021/03/23/legitimacy.html
Cole R et al (2019) Blockchain technology: implications for operations and supply chain management. Supply Chain Manag Int J 24:469
Currie M et al (2022) Data justice and the right to the city: an introduction. In: Data justice and the right to the city. Edinburgh University Press
De Filippi P (2017) Plantoid – the birth of a blockchain-based lifeform. In: Catlow R et al (eds) Artists Re: thinking the blockchain. Torque & Furtherfield, p 51
De Filippi P (2021) Blockchain technology as an instrument for global governance. SciencesPo Chair Digital, Governance and Sovereignty:1
De Filippi P et al (2020) Blockchain as a confidence machine: the problem of trust & challenges of governance. Technol Soc 62:101284
De Filippi P et al (2022) Blockchain technology, trust & confidence: reinterpreting trust in a trustless system? In: HIIG Discussion Paper Series, p hal-03895402
Dellmuth LM, Tallberg J (2015) The social legitimacy of international organisations: interest representation, institutional performance, and confidence extrapolation in the United Nations. Rev Int Stud 41:451
Dimitropoulos G (2022) The use of blockchain by international organizations: effectiveness and legitimacy. Polic Soc 41:328
Djeffal C (2024) Law by design obligations: the future of regulating digital technologies in Europe? SSRN Electron J SSRN 4765471:3
Gaus JM (2006) Reflections on public administration. University of Alabama Press
Hassan S, De Filippi P (2017) The expansion of algorithmic governance: from code is law to law is code. Field Actions Sci Rep J 17:88
Hildebrandt M (2008) A vision of ambient law. Regul Technol:175
Hjálmarsson F et al (2018) Blockchain-based e-voting system. In: 2018 IEEE 11th international conference on cloud computing (CLOUD). IEEE, pp 983–986
International Law Association. (2004, August 16–21), Final conference report on the accountability of international organizations (Berlin). https://www.ila-hq.org/en_GB/documents/final-conference-report-berlin-2004-1
Jeffrey A, Painter J (2008) Political geography: an introduction to space and power. Sage, p 20

Kalvet T (2012) Innovation: a factor explaining e-government success in Estonia. Electron Gov Int J 9(2):142–157
Kannengießer N et al (2020) Trade-offs between distributed ledger technology characteristics. ACM Comput Surv 53(2):1–37
Kelsen H (2005) Pure theory of law. In: The Lawbook Exchange. Clark
Kelsen H (2017) General theory of law and state. Routledge, pp 110–122
Kewell B et al (2017) Blockchain for good? Strateg Chang 26:429
Koops BJ (2008) Criteria for normative technology. In: Brownsword R, Yeung K (eds) Regulating technologies. Legal futures, regulatory frames and technological fixes. Hart Publishing, pp 157–166
Koops BJ (2018) Privacy spaces. West Va Law Rev 121:611
Kshetri N, Jeffrey V (2018) Blockchain-enabled e-voting. IEEE Softw 35(4):95–99
Lessig L (1999) Code and other laws of cyberspace. Basic Books, p 3. https://lessig.org/images/resources/1999-Code.pdf
Levi M (2019) Trustworthy government and legitimating beliefs. In: Knight J, Schwartzberg M (eds) Political legitimacy: NOMOS LXI. NYU Press, New York. (online edn, NYU Press Scholarship Online, 23 Jan. 2020)
Mandel GN (2009) Regulating emerging technologies. Law Innov Technol 1(1):75–92
Mastenbroek E et al (2016) Closing the regulatory cycle? A meta evaluation of ex-post legislative evaluations by the European Commission. J Eur Publ Policy 23:1329
Merriam CE (1944) The ends of government. Am Polit Sci Rev 38:21
Myeong S, Jung Y (2019) Administrative reforms in the fourth industrial revolution: the case of blockchain use. Sustain For 11:3971
Norman DA (1988) The psychology of everyday things. Basic Books
Ostrom E (2001) Decentralization and development: the new panacea. In: Dowding K et al (eds) Challenges to democracy: ideas, involvement and institutions. Palgrave Macmillan, p 237
Peters A (2016) International organizations: effectiveness and accountability. In: Max Planck Institute for Comparative Public Law & International Law (MPIL) Research Paper, p 11
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
Reijers W et al (2018) Now the code runs itself : on-chain and off-chain governance of blockchain technology. TOPOI Int Rev Philos 37:17
Ripstein A (2006) Beyond the harm principle. Philos Public Aff 34:215
Roberts A (2020) Bridging levels of public administration: how macro shapes meso and micro. Admin Soc 52:631
Scharpf FG (1999) Governing in Europe: effective and democratic? Oxford University Press, p 11
Schillig MA (2023) 'Lex cryptographi (c) a', 'cloud crypto land' or what?–blockchain technology on the legal hype cycle. Mod Law Rev 86:31
Schmitt C (2005) Political theology: four chapters on the concept of sovereignty. University of Chicago Press, p 13
Semenzin S et al (2022) Blockchain-based application at a governmental level: disruption or illusion? The case of Estonia. Polic Soc 41(3):386–401
Sunstein CR (1990) Paradoxes of the Regulatory State. Univ Chic Law Rev 57:407
Trebilcock MJ, Iacobucci EM (2009) Designing competition law institutions: values, structure, and mandate. Loy Univ Chic Law J 41:455
Treib O et al (2007) Modes of governance: towards a conceptual clarification. J Eur Publ Policy 14(1):1–20
Walch A (2018) Blockchain applications to international affairs: reasons for skepticism. Georget J Int Aff 19(1):27–35
Wilhelm A (2019) Rule of Law 4.0: blockchain technology and the development of legal institutions in Africa. SSRN Electron J:9

World Economic Forum (2018) Will blockchain curb corruption? World Economic Forum. https://www.weforum.org/agenda/2018/03/will-blockchain-curb-corruption/

Wright A and De Filippi P, 'Decentralized blockchain technology and the rise of lex cryptographia' (2015)

Yeung K (2008) Towards an understanding of regulation by design. In: Brownsword R, Yeung K (eds) Regulating technologies: legal futures, regulatory frames and technological fixes. Hart Publishing, pp 79–88

Yeung K (2019) Regulation by blockchain: the emerging battle for supremacy between the code of law and code as law. Mod Law Rev 82:207

Zbinden F, Kondova G (2019) Economic development in Mexico and the role of blockchain. Adv Econ Bus 7(1):55–64

Zwitter A and Boisse-Despiaux M (2018) Blockchain for humanitarian action and development aid. J Int Humanit Action 3:1

Zwitter AJ et al (2020) Digital identity and the blockchain: universal identity management and the concept of the "self-sovereign" individual. Front Blockchain 3:26

Chapter 10
Plotting the Rule of Law Affordances

10.1 Reducing *Crypto-Legal* Characteristics

In the case of technological artifacts, the affordances provide opportunities to enquire about the features provisioned in a particular design. These affordances also provide a set of aspirational objectives for the affordances themselves so as to attain legitimacy and desired efficacy. Hence, the 'figure' should not only ponder about the intended end use of the code from a commercial standpoint but also assess rationally whether the said features of the artifact are within the boundaries of the rule of law or not and, if not, how it might fall within the purview of the rule of law.

Since the rule of code performs the job of manifesting the normativity of code, which is ultimately embodied, not paying much heed to the *ex-ante* decisions regarding the use of code will introduce an Achilles heel in the analysis. Though a technological irritant, it is an unavoidable activity. We have discussed earlier how user behavior is directly influenced by the design of the artifact and how the text of the command code rule represents the design. The exercise here is not to question the rationale behind the designing of the code of a specific artifact but rather to investigate the resulting functions of the code and whether its normativity affords legitimacy, independent of their prior justifications. The distinction, though very subtle, is critical to understanding the implications of the code's behavior and its regulatory context. If the motivation behind the design is not analyzed critically, it is possible not only to fail to observe the actual performance of the artifact but also to approve the flawed belief about the robustness of the implementation of the code since the decision to use code is sound.

The logic behind crafting the rule of law affordances and embedding them into the blockchain artifact *ex-ante* is to address the Collingridge dilemma –

> the social consequences of technology cannot be predicted early in the life of the technology. By the time undesirable consequences are discovered, however, the technology is often so much part of the whole economics and social fabric that its control is extremely difficult. This is the dilemma of control. When change is easy, the need for it cannot be foreseen;

A. Bisoyi, *Blockchain and Legitimacy*, Law, Governance and Technology Series 77, https://doi.org/10.1007/978-3-031-98712-0_10

> when the need for change is apparent, change has become expensive, difficult, and time-consuming.[1]

The blockchain-based human rights application, which employs smart contracts with fixed, predefined criteria for granting asylum, illustrates some of the challenges and limitations of applying the rule of law in complex and dynamic situations. While the use of smart contracts may enhance the transparency, efficiency, and accountability of the asylum process, it may also undermine the flexibility, responsiveness, and context-sensitivity of the system due to the rule-fetish and instantaneity characteristics of the blockchain code. The smart contracts may not be equipped to accommodate exceptional cases or evolving geopolitical situations that require a more nuanced evaluation of individuals seeking refuge. These contracts may not be able to reflect the changes in the laws or the human rights principles that may occur over time. Thus, there is a need for the rule of law as affordances to counter the *crypto-legalistic* characteristics of the technological artifact and, as such, render the artifact legitimate.

The objective is to steer the development and production mechanisms of code in ways that reduce its *crypto-legalism* within the blockchain artifact. The crucial question is: does the design afford due process rights, the freedom to choose (personal autonomy), transparency, and deferment to the user? Does the design afford (human) supervision and accountability to the 'figure'? The goal of this litmus test's commitment to the *ex-ante* rule of law measures (legality, legitimacy) is to ensure that irrespective of the substantiveness of *ex-post* functionality, technological normativity includes mechanisms to restructure the *crypto-legalism's* historical trajectories that influence its current development.

10.2 Plotting the Rule of Law Affordances Against *Crypto-Legalism*

In line with the rule of law design standards of legality and legitimacy, the mapping of the Fullerian design standards against the appropriate attributes of *crypto-legalism* demonstrates the way these standards apply across different normative orders of institutional law and code. The mapping will help to understand how the affordances reflect the objectives of the standards within the boundaries of the rule of law. While many of the proposed affordances intersect with each other since the application of an affordance is not limited to enhancing a particular characteristic signified, a holistic consideration would be able to achieve and facilitate technological normativity by concurrently addressing various pertinent matters that are legitimate in the eyes of 'the rule of law'.

Figure 10.1 shows the relation between the degree of rule of law affordances in terms of the increasing difficulty of implementation and the degree of the

[1] Collingridge (1980), p. 11.

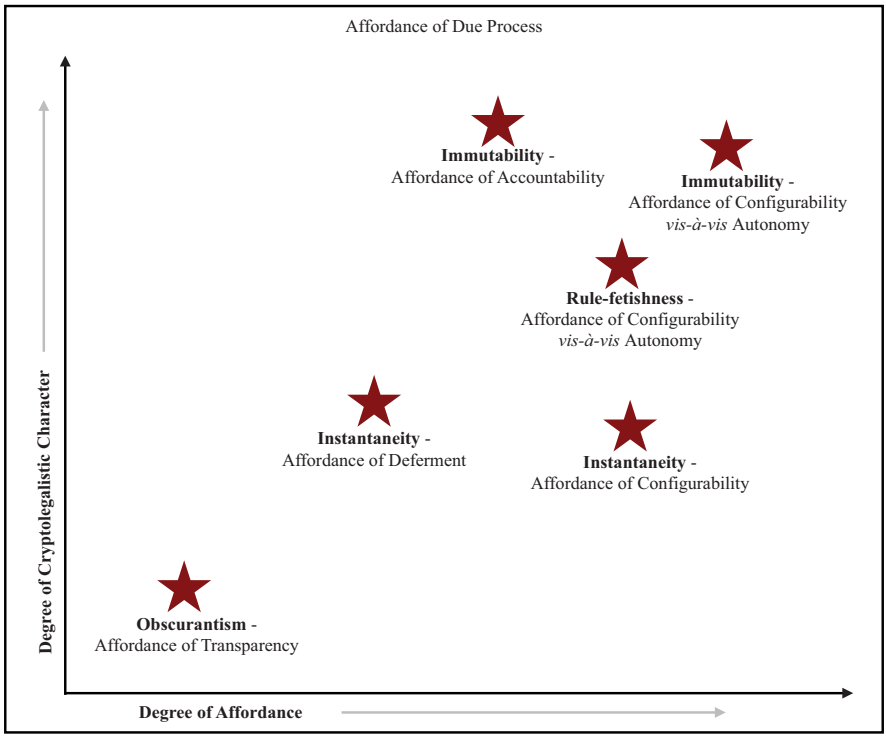

Fig. 10.1 Plotting the Rule of Law Affordances

crypto-legalistic characteristics of the blockchain code from low to high. Here, for the purposes of clarity and simplicity, four *crypto-legalistic* characteristics, namely, *immutability, rule-fetishness, instantaneity, and obscurantism,* have been considered on the *y-axis*, whereas various affordances such as *autonomy, configurability, accountability, deferment, and transparency* have been plotted on the *x-axis*. Though the affordances have been plotted here as 'points', they are to be considered as a cluster of elements that perform in unison to realize and establish the legitimacy of the 'geography' of technological normativity. The artifact is deemed to have certain affordances whose relevance varies contingent upon the function and expected end-use of the particular technological product, and as a consequence, the justification for such affordances also differs. The idea is to explore an array of normative reference points that are unequivocally concerned with the rule of law issues.

10.2.1 Immutability

As the graph illustrates, the immutability attribute of code has a higher degree of *crypto-legalism* in blockchain architecture, which makes it very hard to amend the code after it has been scripted and programmed into the architecture to balance the

affordance of configurability *vis-à-vis* autonomy and affordance of accountability with its *crypto-legalistic* nature. This is because the immutability of code in blockchain draws itself from the inherent fundamental characteristics of the technology due to the network's decentralized nature, cryptographic techniques, and consensus mechanism. The immutability of code is a desirable property for blockchain applications that require trustless transactions, such as smart contracts. It may also create some obstacles, such as the difficulty of correcting errors, updating the code, or complying with legal regulations that may require users to be given autonomy to choose among options coded in the artifact.

The issues associated with the immutability of code intersect with those exhibited by its 'rule-fetishness' and 'instantaneity' characteristics. The attribute of immutability can be said to be compatible with the Fullerian design standard 7, which describes the constancy of rules over time and its frequency of change, where the standard is appertained in a reverse fashion, implying that 'code is resistant to change',[2] a fact that must be considered while programming at the micro level. Concurrently, there has to be a delicate balance between duty and aspiration when defining the boundaries. It is necessary to acknowledge the potential emergence of path dependencies—situations where the choices made in the past and present significantly impact future possibilities—where these paths can inadvertently bind the users within the confines of a specific design. Since users are being coerced to operate within the constraints of a particular blockchain design, leaving less scope for modification in the future, there is a need to recognize and raise awareness regarding the sensitivity toward the concreteness of the imposed rule of code. This demands that the justification for imposing the rule of code that regulates user behavior should go through continuous assessment of time, calling into action the principle of temporality, an additional requirement that conforms to Fullerian design standard 7. Considering the manner in which the immutable rule of code manifests into a specific configuration of technological normativity, it is essential to endorse the affordance of configurability *vis-à-vis* autonomy and to balance it with the affordance of accountability. Immutability can be linked with Fullerian design standard 4 on clarity, specifically focusing on the notion of coherence, and also with Fullerian design standard 5 on non-contradictory and consistent norms. Only coherence 'consistent' with the 'internal justification' of the system is not enough. It should be feasible to alter the rule of code when there is a change in the external justification. The absence of such an affordance would mean that reliance on the 'illegitimate' rule of code may persist, notwithstanding the legitimacy of the rule of code at the time of initial deployment.

[2] Shay et al. (2016).

10.2.1.1 Affordance of Configurability *Vis-à-Vis* Autonomy

Since the rule of code in the blockchain continues to operate 'immutably' even if the same has been rendered illegitimate or meaningless, the *ex-ante* anticipation of future effects and a resolution thereof becomes important. Hence, the 'figure' who is responsible for designing the blockchain applications should be aware of contingencies ahead of time. However, the normative scope of the configuration of code is limited to those facts that the 'figure' can reasonably ascertain. Unless the rule of code is designed with the affordance of configurability to check for complexities and emergencies, the code will operate as pre-defined, even if the external contingency calls for a different action.[3] For instance, smart contracts can be designed to accept human judgment as input while executing the contract. Fulfillment of contractual conditions can be determined by making such conditions dependent on judgments of external parties. Also, it is important to see if it is possible to anticipate and fix all significant exigencies that might arise in the future and, if so, whether they would be supported by external parties.[4] The fundamental assumption is that the external parties will continue to provide services as designed for the initial version of the blockchain. If the said third party modifies the code and formats, or stops providing services, then the blockchain applications would be stuck and become inoperable. In terms of due process rights, if a judicial process is invoked to address such disputes, it would be difficult to identify the parties to demonstrate legal standing to contest or seek a decree, as only anonymous public keys are used for identification in a blockchain. In any case, the judicial remedy would be the *ex-post* event after the code has been executed with all its illegalities or negativities.

While deciding the incorporation of the affordance of configurability *vis-à-vis* autonomy into the code, if the 'figure' is uncertain about whether specific vital information will be available at the time of execution, then the wired-in components of the code should be restricted to avoid the inclusion of such uncertainties. Further challenges accrue when distinguishing between the functional characteristics of the blockchain application that can be automated and the non-functional characteristics that cannot or should not be automated. In the case of heavy automation, most or all of the effects of *crypto-legalism* are seen to have intensified and become more pronounced, whereas, in the case of less automation where the code's logic is oversimplified, blockchain is reduced to a 'dumb'[5] artifact and may lose its functionality. However, this could be a beneficial constraint, transforming the code into a tool[6] for implementing real-world agreements, with humans maintaining the responsibility and being accountable for handling and resolving any uncertainty. While the function of the blockchain application is limited to those specific elements that can be reliably and predictably represented and enforced through code, the social aspect of

[3] Weber (2018), p. 705.

[4] De Filippi and Wright (2018), p. 202.

[5] Lipshaw (2019), p. 1.

[6] Mik (2021), p. 478.

consensus, encompassing formal legal contracts, remains the focal point for the variable components of real-world human agreements.[7]

If the 'figure' is reluctant to sacrifice the 'smartness' of the blockchain application and opts for heavy automation, the external variables it depends on must be verifiable at the moment of execution, that is, *ex-post* assessment. This suggests the use of data points in the future[8] that are trustworthy, reliable, and precise. An accountability issue could arise as it shifts away the figure's decision-making responsibility to third-party services regarding the key aspects of the artifact's logic, thereby undermining their responsibility towards the performance of their own design and diminishing their control over their own work. A viable solution could be designing the blockchain applications with some sunsetting features so that the artifact will become inactive if the system is not able to verify a certain fact with the required level of certainty at the moment of execution.[9] When the *ex-post* alteration of code is not feasible, and in such a situation, it is confronted with the challenge of executing the code indefinitely without any modifications, then this mechanism offers a viable solution. If the intermediate and extended impacts of the system's technological normativity cannot be foreseen and predicted, then the 'figure' ought to implement a sunsetting mechanism to constrain the potential consequences of the rule of code running indiscriminately in unfamiliar or irrelevant circumstances. This calls for intentional designing of the safety measure into the rule of code through the affordance of configurability.

Related to the affordance of configurability is the concept of the 'legacy switch', which disables optional affordances, for example, network access, and limits the system to its core functions only.[10] For instance, in a smartphone, activating the legacy switch would disable features like internet browsing, leaving only core functions like calling and messaging. This contrasts with the affordance of deferment, where it gives the user more control and flexibility over the system and allows to delay an action or decision because the feature of legacy switch does not allow the user to choose when to resume the optional affordance but rather disable them permanently or until the switch is reversed. The legacy switch reduces the complexity and functionality of the system and may limit the user's options and preferences.[11] The efficacy of this approach is contingent upon the type of artifact; if the networking is the key to the application, then disabling it by activating a legacy switch might cause the application to be practically useless.

[7] Levy (2017), p. 3.

[8] One of the suggested tools is Oracle which is responsible for delivering reliable data from off-chain sources to smart contracts on the blockchain.

[9] Kouroutakis (2020), p. 16.

[10] Ohm and Kim (2023), pp. 101–107.

[11] Evans et al. (2017), p. 35.

The blockchain applications, such as decentralized identity systems, use the technology to provide users with control over their personal data, helping to protect their privacy and prevent identity theft. A legacy switch could be helpful here because it could allow the user to enhance their privacy and security by disabling some optional affordances or features that may expose their personal data to other parties. This way, they could still use the core functions of the decentralized identity system, such as verifying their identity or accessing their data, without compromising their privacy or risking identity theft. The proactive *ex-ante* flipping of the legacy switch, constraining the application's design from the outset, is essential with the understanding that it could otherwise possess excessive normative influence. However, the viability of such a theoretically legitimated blockchain application, in terms of its market appeal, remains ambiguous.

10.2.1.2 Affordance of Accountability

Although the tamper-resistant and immutable attributes of blockchain are its key value propositions,[12] from the standpoint of traditional contract law, it is tricky in the sense that it causes the blockchain to execute when the conditions satisfy the *ex-ante* interpretation formalized in the code, despite certain interventions which might have sought more adaptability and flexibility.[13] In terms of accountability, blockchains are problematic since this technology requires that a consensus must be reached to effect any change and also does not allow the breach of the contract unilaterally. While it is possible to observe the execution of the application as the output is immutably stored on the underlying chain, what is important to ensure the normativity of the code from the point of view of accountability is continuous maintainability and revocability. Answers to questions like which are the affordances that are weakened by the immutability 'feature' of a blockchain are also important.

> In the case of competencies where the administrative authority has a margin of appreciation that requires the balancing of interests or interpretive discretion, rigid rule-based smart contracts realistically seem to be deployable in the case of circumscribed competencies without discretion.[14]

As regards the accountability of the 'figure', they must not release code without putting in place the conditions required to ensure accountability and mitigation of any unanticipated negative outcomes. This notion closely aligns with revocability, whereby users retain the option to withdraw any permissions they might have

[12] De Filippi and Wright (2018), pp. 35–37.

[13] Allen (2018), p. 307. Durovic and Lech (2019), p. 493. Klass (2023), p. 69.

[14] Goossens (2021), p. 81.

conceded to the 'figure'.[15] The principle of revocability demands that the 'figure' ought to have the ability to maintain some control over the artifact.[16] In order to be considered legitimate, the 'figure' must foresee *a priori* the potential necessity for making alterations *ex-post*, which requires the design of the artifact to be reconfigurable; otherwise, such a design would become *prima facie* illegitimate at any time in the future. Anticipating and predicting the possibility of future amendments depends on many externalities, where the 'figure' must identify in advance the necessary information and details that must be known before the deployment of the technology. The trusted third parties must also provide accurate information to the 'figure'. Since the variety of factors and their complexities are key determinants, it may not be feasible to fulfill the standard of accountability 'absolutely', and thus, the question of the legitimacy of the blockchain applications *a priori* still persists. In many cases, therefore, code is sold off in the marketplace without having any provision for *ex-post* software updates or commitments to address security vulnerabilities in the future.[17]

With regards to the concept of the legacy switch, which is used as a mechanism for affordance of configurability, the 'figure' has the power to permanently disable the optional affordances without enabling the user the option to resume the disabled affordances. Such deactivation cannot be reversed by the user until the 'figure' turns off the legacy switch. This raises questions about the control and use of the legacy switch: who decides when to activate it, and under what circumstances? Should the user have the power to activate the switch on a work laptop, or should it be controlled by the computer department? Instead of relying solely on the technology's built-in rules (the rule of code), traditional regulatory roles, such as legal regulations, might be needed to address these issues.

If the identification management application provides users control over their personal data, with the legacy switch that deactivates the extra feature like giving personal information to other third-party applications, questions are raised about the affordance of accountability: who should have the control to activate this switch? Should it be the user who might want to maintain their privacy and control over their personal data? Or should it be the 'figure' responsible for the development and governance management of the identity system who might want to ensure the system's integrity and prevent misuse? Instead of focusing on the rule of code feature, traditional regulatory roles, such as those played by data protection authorities, might be needed to resolve these challenges.

The rule of code-based artifacts that prevail over human action offers significant benefits such as 'consistency' and 'immediacy' as compared to the traditional rule-based instruments while avoiding the use of critical resources required for monitoring and administering regulatory rules.[18] The pertinent point is if there is no

[15] Gürses et al. (2011), p. 25. Naor and Pinkas (2010), p. 411.

[16] Winner (1978), p. 314.

[17] Desai and Kroll (2017), p. 1. Raskin (2017), p. 305.

[18] Yeung (2008), p. 93.

commitment from the 'figure' in respect of service support, updates, and maintenance for a reasonable period or no commitment about sunsetting or phased discontinuation of the application or any specific components of its functionality, or no commitment about retaining adequate control to allow a legacy switch in case of necessity, then the design would not be legitimate and as such the artifact does not afford the required level of accountability.

The 'figure' must include affordances of accountability into the design of the artifact so that changes, if required, to the rule of code can be incorporated. It also means that if there is no commitment from the 'figure' to such standards of accountability, then one can derive that the legitimacy of the design has not been established, and its technological normativity is unwarranted. Likewise, if the technological architecture does not allow updates as a design feature due to limited connectivity, processing power, or other considerations, then the scope of the functionality of the code should be, to that extent, limited to ensure that the 'rigid' or 'immutable' code will not impact negatively in future. The 'figure' must foresee external change and either facilitate remote updation or restrict the scope of the design's normativity from the beginning. In cases where it is not easy to predict these potential contingencies, *ex-post* remedial strategies, such as engaging a trusted third party, must be put in place. In the absence of any of these measures, it can be concluded that the design is *a priori* illegitimate.

10.2.2 Rule-Fetishness

Another attribute of blockchain code that has a strong *crypto-legalistic* tendency is rule-fetishness. The position of 'rule-fetishness' in Fig. 10.1 indicates that it is not simple to re-script the code with the affordance of configurability *vis-à-vis* autonomy but is as complicated and demanding as the attribute of the immutability of code. That is because rule-fetishness refers to the adherence to the predefined 'rigid' rules of the blockchain code, which can be modified by the consensus of the network users or the 'figure'. Immutability, on the other hand, refers to the resistance to any change or deletion of the code rules and data embedded within the blockchain, which is enforced by the cryptographic and distributed nature of the technology. This means re-scripting the rule of code before setting down the code into the artifact is not too complicated as compared to updating the code rules when they are already programmed in, as the former requires less computational and coordination effort than the latter.

Since the rule of code is inflexible and extremely precise and does not allow any ambiguity, it applies to all users 'fairly' and 'equally' without any discrimination irrespective of the attribute of the person such as their gender, race, age, religion, etc. However, this 'rigid' inflexible feature is a desirable quality 'only' if the design of the code is legitimate. Characteristics such as tamper resistance, auto-execution, and resilience empower the authoritative 'figure' to incorporate its set of rules into blockchain-based applications so that all users of the applications will have to abide

by the rules set by the 'figure'. It may ultimately assist the authoritarian and rigid regime to control its subjects through a series of self-executing code-based rules.[19] If the preset desideratum is satisfied, the code executes the rules and, in the same vein, does not execute in situations where those prerequisites are not fulfilled. It does not matter how 'nearly' the desideratum is fulfilled, or what would be the possible consequences of executing or not executing the said rule of code. This aspect of rule-fetishness, which is at the core of *crypto-legalism*, is concerned with the balancing of the blockchain constitution or the 'default' behavioral constraints of the design and its regulative aspects. Since rule-fetishness is related to the threshold between what has been coded and the regulatory latitude available to the users to decide whether or not to yield to a suggested restriction, there is a need for the affordance of configurability *vis-à-vis* the affordance of autonomy to be incorporated into the design of the technology artifact.

10.2.2.1 Affordance of Configurability *Vis-à-Vis* Autonomy

The rule of code of the blockchain artifact is fixed and executed mindlessly without further reflection once it has been embedded and without any intermediaries or authorities, demonstrating its rule-fetishness attribute. This means that the architecture of blockchain is rigid, inflexible, and immutable, which can create problems when the code rules need to be changed or adapted. The rule-fetishness attribute, in addition to the 'immutability' characteristics of code, could pose significant problems. This is where the affordance of configurability comes in, which is the faculty to modify the configuration and parameters of the artifact and is diametrically opposite to the notion of immutability. Configurability allows for some degree of flexibility and customization, which can offset upshots of the instantaneity and immutability attribute of the code, core components of the rule-fetish characteristic of blockchain code. The provision for configuration may not be enough to improve the rule-fetishness, yet it challenges the rule-fetishness of code, which is based on the idea that code is superior and that the rule of code should be followed without questioning or interpretation. By allowing configurability, we acknowledge that code is not perfect or absolute and must be modified or improved.

Deciding the approach to the affordance of configurability of code in advance is important to empower the relevant audience with autonomy. The affordance of configurability calls for a provision to make a choice that depends on relevant options and appropriate timing[20] to ameliorate rule-fetishness and empower the user with autonomy. However, configurability with too many options can be baffling and daunting, particularly for users who lack expertise or are inexperienced and can turn out to be more of a hindrance than help.[21] Even when critical reflection shows that

[19] De Filippi and Wright (2018), p. 203.

[20] Kesan and Shah (2006), p. 601.

[21] Kesan and Shah (2006), p. 627.

customization could be beneficial in the form of providing options that serve their interests and/or preferences,[22] many users still consider it as time-consuming and avoid it.

If the possibility of choices and configurability has not been foreseen at the design stage, the tamper-resistance characteristic turns into a bottleneck during execution. It is crucial to decide prudently how much of the code would be rule-fetish and how much would be dependent on the input by the user and the external contingency to afford configurability *vis-à-vis* autonomy. As the issue of choice is closely related to the issue of immutability, designing the threshold between wired-in and configurable code is critical in light of the continuity of code in a blockchain. The threshold could have legal implications, given the complexities involved in the automatic execution of the rule of code in blockchain applications.[23] In the context of rule-fetishness, it is to be noted that default configurations of code do influence and guide the user's appreciation of the behavioral possibilities it affords. Even when the code allows choices, these default configurations are trusted by the users as the right choices created by the 'figure'; the user perceives the 'default' situation as normal and acceptable and even as legitimate in pervasive systems. Due to automation bias, the user tends to trust the outcome of the operation executed by the artifact.[24]

It is inevitable to have some degree of configuration in any artifact, including the things we see around in the offline world, which suggests the fundamental non-neutral character of technologies. The 'figure' cannot leave the interpretation of the design of the artifact open-ended or ambiguous on purpose, which can be deliberately misinterpreted, unlike the legislators who intentionally leave the meaning of a textual norm vague. The 'figure' has to limit the endless course of action of the *lex cryptographic tabula rasa* by making certain choices in the configuration. This makes it necessary to pursue deliberate interventions or decisions to ensure that the default configurations are legitimate in order to make the artifact itself legitimate.

The job of decision-making is *de facto* outsourced to the 'figure' through the default setting mechanism, in which the focus shifts from the user as well as the sovereign. So, it is essential to nudge the 'figure' to establish default configurations that align with recognized societal notions,[25] like the rule of law. If the concern is about the legitimacy of behavioral regulation, then the attributes of the code that comprise of the choices must resonate with the same value of legitimacy. The quality of choices referring to the substantive functionalities in the artifact that are authorized to the user to configure or allow the user to customize, and the number of choices are central design questions. The answers determine the extent to which autonomy is provided to the users and the way in which this affordance of configurability *vis-à-vis* autonomy is communicated or signified through the design of

[22] Kesan and Shah (2006), p. 598.

[23] Levy (2017), p. 3.

[24] Citron (2007), pp. 1271–1272.

[25] Shah and Sandvig (2008), p. 42.

choices to the user. If these choices do not empower the user to exercise its freedom of autonomy in a true sense,[26] just making a provision of choice for the sake of it won't make the artifact or its code legitimate.

On a scale of configurability, the affordances could range from wired-in functionality that cannot be modified at one end through default settings that offer certain choices to modify to complete customization provision at the other end.[27] It is pertinent to note that even at the level of 'complete customization', the configurability is not really completely autonomous because the design considerations, by definition, restrict the limitless possibilities that consequently define the boundaries for the user to function autonomously. However, an important concern is how much the users are aware of their power to configure.[28] Since it is entirely contingent upon the perception of the affordance of configurability *vis-à-vis* autonomy (freedom to choose), it is not sufficient if the affordance is only real but is unknown or so complex that it is not practicable to afford. There are also factors such as efficiency and the consideration of rookie users, which drive the design decisions in the real world. These goals, particularly with regard to the criteria for measurement of efficiency and determination of the 'novice-ness' of the user, are largely vague, especially because the impact of the default would often impact on blurry values that are hard to quantify.[29]

The design process is also influenced by the legal philosophies of default rules,[30] which help to ponder over both immutable configurations that are wired-in and 'just' default configurations or what is merely arranged as a default and can yet be changed and adjusted.[31] In case of immutable or wired-in configurations, it must be contestable, that is, the design must have provisions to notify the user and allow for judicial due process rights. In harmony with the affordances of due process and transparency, the user ought to be provided with an easy-to-use interface that permits them with the ability to personalize the configuration of the program or software.[32] Where the settings do not have any material impact on the basic societal concerns, for example, data security or privacy, the laying down of the initial default configurations begins with the abstraction that 'this is what the target users would have intended and wanted' while adhering to the design and usability conventions.[33] This 'would have wanted' code of behavior entails the 'figure' to anticipate the outcome had there been an opportunity to deliberate between itself and the user. If an information asymmetry exists or emerges between the 'figure' and the user, it is essential that the default settings safeguard the interests of the user by providing

[26] Owens and Cribb (2019), p. 23.
[27] Kesan and Shah (2006), p. 591.
[28] Kesan and Shah (2006), p. 597.
[29] Kesan and Shah (2006), p. 600.
[30] Schwartz and Scott (2016), p. 1523.
[31] Kesan and Shah (2006), p. 614.
[32] Kesan and Shah (2006), pp. 615–616.
[33] Norman (1999), p. 40.

them with enough appropriate information or guiding them to change the settings (to non-default) if they want.[34] It is the responsibility of the 'figure' to explain the negative consequences of the non-default settings to the users before the user chooses them. In other words, the default settings are those which the 'figure' 'would not have intended and wanted' to be part of non-default settings that would require informing the users.

The justification for this 'would not have intended and wanted' code of behavior is grounded in the theory of externalities (often employed in Economics), which refers to wide-ranging negative impacts of the parties who are not directly related.[35] By the same logic, the default settings should lessen these externalities. When high stakes are involved, no 'regulatory margin' in defaults should be allowed, and the best-considered option should be wired in.[36] The rigidity of a default setting gets strengthened by cognitive biases that influence the exercise of choice and autonomy by the user. It is all the more important for the 'figure' to initially configure the rule of code with the right list of objectives and interests.[37] The default settings and the 'stature' accorded to these settings in an interface can influence the awareness of users about its usage. As such, it is essential for the 'figure' to clearly draw the attention of users to defaults that need more attention but are not so important that they have to be fixed or wired in. These attention-seeking tools can include, among others, alerts and notifications asking the user to make a choice. This mechanism is instrumental in affording positive deferment within the technology architecture. The user may be required to make a choice when they first use the application, with no predefined option to prompt the user's decision or a choice to avoid the configured organizational request. The design of these affordances of autonomy must consider how the natural language affects and influences the understanding of the options.[38] The idea is that the design should not promote the goal of the business at the cost of legitimacy. A corollary to this logic is that it is *de facto* illegitimate to use adversarial design methods.

Analyzing 'choice' from the perspective of configurability and autonomy adds nuance to the rather straightforward idea that more choice is, per se, better, and technological normativity preserves the possibility of choice. As a principle, the spirit of legitimacy should be exhibited at each locale as the user rides through the inscriptions of the artifact by its affordances. If the choice is not appropriate, then it may not be sufficient to ensure the legitimacy of the code. Simply providing more options is not the objective of the design; rather, it must afford environments to exercise autonomy in a meaningful way.

A necessary requirement for implementing blockchain applications for humanitarian purposes is mitigating the 'rule-fetishness' characteristic of code. One

[34] Ayres and Gertner (1989), p. 87.

[35] Posner (2006), p. 563.

[36] Kesan and Shah (2006), pp. 621–622.

[37] Kesan and Shah (2006), p. 633.

[38] Sunstein and Thaler (2003), pp. 1179–1183.

approach to do that is to reconsider the rule-fetish attributes simply as stewards of the multi-interpretability and focus on what ought to be effected programmatically. For example, the objective of the Wise Contract[39] is not just automation of the purposive elements of a contract-like agreement but rather maintaining the flexibility of text-based agreements and supplementing it with limited functionalities of code that complements the text-based agreements.[40] Minimum code semantics are applied to the natural language text of the agreement to enable the rule of code characteristics through the use of hash function and public key cryptography. Since the actual text of the agreement preserves all the nuanced interpretations that a natural language can accommodate, this arrangement facilitates combining the notional immutability of the agreement with the inherent flexibility of expression. The code contributes to producing the ancillary advantages to the essential terms and conditions of the agreement, reflecting the substantive content of the contract in the format of immutability and 'radix' checking while retaining the human aspects of the execution of the agreement. In this case, choices are not included in inscriptions or codes and thus are outside this rule of code environment. Restricting the rule-fetishness of blockchain code to such ancillary benefits evidently avoids a 'strong legalism' outcome, but in practice, it may cause a dent in the perceived value of the application.

The idea of 'conflicts' in technological artifacts deals with the issue of choice and the function of design while acting in response to the interests of different stakeholders. The 'figure' ought to anticipate the conflicts that may arise due to techno-legal, social, or even economic reasons. The tension between the commercial interests of *crypto-legalism* and the spirit of legitimacy leads to the construction of a room for conflict, which is used by the 'figure' to press forward its interests such that the rule-fetishness and immutability attributes provide predictability, the characteristic of obscurantism ensures protection of commercial and trade secrets but conceals vacillating normativities, while the attribute of instantaneity yields prompt feedback and tangible outcomes that can be marketed. This demonstrates a possible conflict situation between the interests of the user and that of the 'figure' since the efforts of the 'figure' are directed towards channeling the user's behavior in predictable and profitable ways.

It is important to anticipate conflict points during the programming phase so as to avoid any challenges during execution. The affordance of configurability *vis-à-vis* autonomy can deal with these conflicts by anticipating problems and making provisions for choices for different possibilities. Designs that are rigid will fail to hold, whereas those that accommodate variability will adapt and ensure.[41] Although there are concerns associated with infrastructural designs, there are designs that afford autonomy to users and promote equal treatment to all. Of course, the extent of autonomy to be exercised depends on the main aspirations of the design of the artifact.

[39] It is commonly referred to as the Ricardian contract.

[40] Hazard and Haapio (2017), p. 425.

[41] Clark et al. (2002), p. 348.

The constitutive power of the 'figure', which is the ability to shape the behavior and preferences of the user, thus drifts away from the 'figure' when the provision of choice is allowed to occupy the conflict room.[42] Since this requirement, once articulated in code, impacts the business model of the 'figure' leading to possible existential questions about the desirability of a given application, it calls for an assessment of the design of the artifact through Fullerian design standard 2 on promulgation of norms, in relation to the principle of alternativity which requires that there should be a good reason to impose a 'rule-fetish' and 'immutable' rule instead of leaving a room for choice. This standard demands that not only should it be more desirable to implement the unconfigurable normativity in the code rather than configurable normativity or affordance of configurability, but also there must be a necessity for rigid application of the rule itself, rather than relying on less rule-fetish mechanism like a recommended default, or a modifiable setting.[43] In the present context, Fullerian design standard 2, read in line with the principle of alternativity, would evaluate first the necessity of having a particular description or inscription for the operation of the artifact and demand a justification for such an inscription or description for deteriorating social interaction. If it is not, then it can be concluded that the restriction on the user's freedom is neither necessary nor justified and, hence, should not be included *a priori* in the design.

If a particular affordance is considered necessary, the next logical question would then be about the rule-fetishness of the implementation—how does the 'figure' achieve the functionality needs of the artifact through wired-in codes? Would the user be provided with an opportunity to exercise choice or an option for complaisant configuration by the code? Or does it imply there is a necessity for nudging, or inscription, or wiring-in of one of the possible options to exclude others? While nudging is less constraining, wiring-in is the most rule-fetish form of technological normativity. Fullerian design standard 2 would require that the resolution to opt for a more rule-fetish, less choice-oriented design approach must be backed by justification since such a decision places larger restrictions on the freedom of the user.

Within the concept of 'conflicts', the anticipation of conflict of interest is associated with the concept of agonism in the rule of law,[44] meaning thereby that it can be productive to have a confrontational argument that facilitates contrasting opinions to be voiced and to reach conciliation. Since dissent is at the core of the rule of law, the design can consciously promote and permit dissent in the form of *ex-ante* participatory design processes,[45] which consider the views of all the stakeholders and targets to achieve an agreement at the design stage. Of course, such approaches are not expected to be adopted in all cases. Participatory design processes such as constructive technology assessment strive to legitimize a prototype by incorporating the views of the different parties in its substantive characteristics. Since the

[42] Clark et al. (2002), pp. 350–353.

[43] Wong (2020), p. 225.

[44] Hildebrandt (2018), pp. 7–8.

[45] Carlsen et al. (2010), p. 209.

stakeholders, in a sense, have approved the features, the design is considered legitimate. Instead of a minimalist idea of the rule of law that does not depend on or influence the substantive views of the participants on the quality of a design, these approaches follow the maximalist notion of the rule of law.

Since, alongside the 'room' for conflicts, the preservation of an agonistic room can also be treated as a constitutional principle in the programming of the rule of code, it is quite feasible to preserve the room for both choice and agonism to circumvent forcing one outcome *ex-ante* and consequently *ex-post*. This design configuration for (autonomous) choice considerations implicitly directs the 'figure' to retreat deliberately from imposing any constitutive outcome and thereby preserving room for agonism and conflict within the operating landscape of the technological artifact. While this leads to a contraction of the realm of the morality of duty, such as *crypto-legalism* and external limitation on freedom, the aspirational domain, such as legality and individual freedom, gets bigger. The decisions at the design time facilitate this change in agonism at the runtime, and at the same time, the design also affords room for agonism during its operation. Yet 'agonism' is still considered an operational feature of the artifact rather than a design feature. How far it is possible to implement this extended affordance of autonomy (to choose) depends on the artifact's intended use.

An important practical design approach for facilitating a conflict room is to modularize different functions of the artifact so that a separation of interest is maintained, which means that the function within the conflict room must become disjoined from the functions that fall outside the boundary of the room.[46] Such an idea gels well with Fullerian design standard 2, which also demands conformity to the principle of normative density. When Fullerian design standard 2, closely connected with the notion of normative density, is associated with code, it connotes that the bundling together of the rule of code norms that are not conceptually related should be avoided because the user should not be forced to accept heterogeneous normativities which are not essential in the eyes of the user. This notion can be demonstrated in the consent mechanism established by GDPR, wherein the regulation mandates separate consent for separate processing operations and does not allow bundling of consent with the performance when the latter is dependent upon the former.[47]

When these normativities display *crypto-legalism*, their agglomeration in an artifact can result in serious adverse consequences as their legalistic features amplify the ramifications on one another. Modularization of different elements of normativity according to their specific features or functions can enhance the ability of the user to understand the effects of the system. The possibility of enhancing the ability through modularization assumes importance since only the 'figure' is able to

[46] Cerf and Ryan (2014), p. 1. Clark et al. (2002), p. 348. Kalogiros et al. (2009).

[47] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter GDPR), Articles 7(2) and 7(4), Recitals 32, 42 and 43.

modularize the design along the contours of conflict, preventing the issues from escalating.[48] Segmentation of these distinct functionalities facilitates and augments user comprehension, enabling more targeted responses to each aspect. This underscores the bond and friction between the affordance of configurability *vis-à-vis* autonomy and default configurations.

Designing to afford autonomy in choice (choosing) in an artifact needs the inscriptions to be responsive to various architectural consequences of blockchains, such as the technological normativity typical to blockchain and *de facto* immutability. As the normative density or the normative impact of the logic of the code increases, the necessity to preserve autonomy over choice also becomes significant. In real life, it is achieved through featuring notifications to the user, defining appropriate choices, and including suitable logic to deal with the end result. However, anticipating all the pertinent points where choice would be required is very problematic in the case of blockchains, given its unusual characteristics. These requirements may challenge the very basis of deploying blockchain applications, particularly those that are powered to perform with minimal or no human involvement, raising a further fundamental question about the *a priori* legitimacy of such applications.

10.2.3 Instantaneity

The next attribute in line with a *crypto-legalistic* tendency is the instantaneity of code, where it is comparatively easier to balance its instinctual nature with the affordance of configurability *vis-à-vis* affordance of autonomy and affordance of deferment. Instantaneity of code does not necessarily imply a fixed or predetermined outcome, as rule-fetishness and immutability do. The instantaneity of code means that code executes as soon as possible, without waiting for human validation or intervention—it preserves the original functionality and purpose of the code without allowing external factors or actors to interfere or modify it. The code can still be configurable, autonomous, and deferrable, depending on the design and logic of the code. For example, a smart contract can execute instantly, but it can also have parameters that can be changed by the users, or conditions that can trigger different actions, or events that can delay or cancel the execution.

When the attribute of the instantaneity of code is read in conjunction with the Fullerian design standards 5 and 6—contradictory and impossible rules—it is deduced that the contradictions and lack of consistency in the language of the rule of code can confuse the user at the interface level and impossible code rules can steer the users into no logical solution scenarios, when the rule of code executes instantaneously and automatically, without the need for human intervention. Similarly, frequent modifications and alterations to the code can introduce

[48] Clark et al. (2002), p. 348.

significant complications. When users become habituated to certain processes or methods of an artifact, then if changes are affected by a software update, coping with such changes could be problematic as the scope for such changes would vary depending on the artifact's utility. In real life, modifications in respect of the design of the interfaces of online platforms have bewildered users, so much so causing backlash.[49] Apart from changes to code, changes to the functionalities of the artifact can also have significant implications. For example, the periodic changes effected to the algorithm of Facebook considerably alter the results and affect the perception of the users, having wide societal implications.[50]

From the point of view of Fuller's principle of inner morality, the instantaneity of code brings up design standard 2 in relation to the notion of normative density that requires *ex-ante* consideration of design for the immediate imposition of a given normative configuration. As instantaneity also heightens the density of the technological normativity, it involves Fullerian design standard 7 emphasizing the principle of temporality that demands sensitivity towards the application of normative standards and the continuing justifications necessary to maintain the relevance and appropriateness of the method utilized in pursuit of normative objectives.

Many of the considerations of rule-fetishness also apply to instantaneity. Since blockchain applications are code-based, they can be instantaneously enforced without relying on the interventions of institutions and human-enabled transfers. Speed and mindless execution of the rule of code are the prototypical elements of *cryptolegalism* and are linked to certain pitfalls. These characteristics of blockchain, though beneficial to the legal system and society, can lead to decreased freedom and autonomy.

10.2.3.1 Affordance of Configurability

The human-in-the-loop principle is the primary mechanism for affordance of configurability in code-mediated processes. It is possible to differentiate between the components of the technical process that can be performed mechanically by an apparatus and those that necessitate human involvement, particularly because the latter encompasses essential human actions required to validate the output of the machine. This distinction is crucial, as each of these components carries important social, legal, and ethical values that influence the overall operation and accountability of the system.

The application of this principle can be seen in autonomous weapon systems, where the ultimate decision to trigger the systems is taken by a human controller, even though such systems boast of being autonomous all the way.[51] In this regard, from a policing perspective, the conservation of inefficiency principle can be

[49] Sevignani (2016), pp. 413–446.

[50] Gillespie (2019).

[51] Winner (1978), p. 284. Beard (2014), p. 617.

suggested, according to which, by retaining some degree of human discretion within the enforcement process, a certain level of legitimacy can be ensured. The human-in-the-loop principle is a form of necessary fortification against the inflexible and rigid code that suggests a proportionate increase of the desirable inefficiency and indeterminacy when actions such as surveillance and crime detection are preset in code.[52]

In cases where the users themselves assume the role of the human-in-the-loop, the interfaces must afford users' notification, choice as well as configurability before the execution of the code. All the relevant information should be delivered in tranches at appropriate intervals through notifications as the user moves ahead through the imprints of code, rather than front-loading the entire information at the beginning along with the voluminous terms and conditions of the agreement when the user might not be able to visualize all possible implications. The objective is to granularize permissions, ensuring they are contextually applicable, and to empower users to make an informed decision based on this tailored information.

Human-in-the loop-principle is essential to maintain indeterminacy, which refers to certain aspects of an episode that are not effectively reflected in the code.[53] Whereas code can impose such interpretation, under-determinacy should be retained to allow appropriate responses considering the subjective and complex nature of the real world.[54] In such scenarios, the human has a role in closing the contextual gaps that suffer from insensitivity shown by computational representations towards them, but which are still crucial to the pursuit of user autonomy or justice.[55] The broad objective is to ensure that the design affords the human-in-the-loop principle at appropriate points in code through the affordance of configurability so that wired-in code does not erode the aspirations of freedom and autonomy.

While text as a normative vehicle is shallow, code is said to have depth, which cannot be easily observed and comprehended due to its intrinsic complexities. Therefore, the focus is on designing interfaces that afford the appropriate deferment in blockchain applications, alongside an appropriate autonomy and configuration, allowing technical feedback so as to facilitate a model for the user to visualize what is going to happen next. Unless there is some feedback mechanism by which failure in the design standards can be appropriately communicated to designers to rectify or modify, the failure will continue to repeat itself within the system. In blockchain applications, it is essential to conduct prior assessments of the consequences arising from the near instantaneous and predetermined execution of code according to its embedded preset logic. This necessitates the introduction of a mechanism that provides appropriate affordance of configurability *vis-à-vis* autonomy along with the affordance of deferment when appropriate.

[52] Hartzog et al. (2016), pp. 1763–1778.

[53] Pasquale (2019), p. 49.

[54] Hildebrandt (2008), p. 177.

[55] Hartzog et al. (2016), p. 1785.

10.2.3.2 Affordance of Deferment

The affordances of text as a mode result in the existence and character of law, which in turn allows the legal norms to facilitate understanding and consensus through democratic evolution and appropriate response to societal changes.[56] When legal norms are instantiated in code programming, they become under-determined and subject to interpretation, depending on the perspective of the interpretation. While the affordance of text as a technology facilitates understanding and consensus, it is, in principle, contingent upon the 'figure' for its implementation. Since the 'figure' responsible for developing the technology generally believes that inefficiency and friction are inherently against the interests of the user, a serious commitment on the part of the 'figure' is called for considering the inelastic nature of the code. Such a stand undermines a market-centered rationality that (supposedly) presumes both instrumental and intrinsic values of the user. The important point here is to identify the intersectional points where the instrumental concept of 'efficiency' is necessary. The potential to remove the perceived inefficiency of the processes and systems is the hallmark of blockchain applications. Unless the code is designed appropriately, this could be very problematic. When the immutability of a blockchain is combined with poor designing of code, it could be indeed serious. The smart contracts' automated and instantaneous characteristics, along with their inability to modify the rule of code embedded within it, may cause even a flawed piece of code to run continuously, causing harm to all parties concerned.[57] Though identifying the points where it is required to avoid the concept of efficiency to protect broader value is important, this method of dealing with inefficiency is not to be encouraged where the 'figure' does not optimize the code. Such a step would be arbitrary since the deferments that are introduced or maintained depend on the expertise and conscientiousness of the 'figure' in identifying and improving them. In some cases, it might even be irresponsible, where the broader objectives suffer due to the lack of optimization, which adversely impacts what should be universal goals. Identifying the values that are critical to the user and deliberately implementing deferments in the code's inscriptions is the key.

This brings us to the conceptualization of 'desirable inefficiency',[58] wherein the efficiency of the code is tempered on purpose to preserve certain values that might be weakened otherwise. Efficiency can be defined as how well the rule of code reduces the use of resources like space, time, energy, or cost to achieve a specified acceptability requirement for a given task.[59] In the case of a desirable inefficiency approach, some goals of efficiency are sacrificed to solve certain other problems. Such an approach tries to provide a solution for the two-pronged problem. At the primary level, the technical outcome, that is, 'the mechanistic metrics of success

[56] Hildebrandt (2015), chp. 3.

[57] De Filippi and Wright (2018), p. 201.

[58] Ohm and Frankle (2018), p. 777.

[59] Stanley-Marbell et al. (2020), p. 1

and failure',[60] sought by the 'figure' is the problem, whereas at the secondary level, necessitating 'human judgment, values, or discretion in the definition of success and failure'[61] is the problem. The problem at the secondary level needs the intentional imposition of inefficiency, enabling humans to perform something that only humans are capable of. The notion of desirable inefficiency calls for the exploration of a novel interdisciplinary research plan to examine the integration and incorporation of values into code.[62] In our day-to-day interactions with technology, we come across many digital speedbumps and stop signboards—securing mobile phones with numerical or pattern passcodes, which is an example of desirable inefficiency. If a wrong passcode is entered, there is a mandatory deferment in entering the second time. This mandatory waiting time will increase, and even the phone will refuse to respond for some time if several incorrect attempts are made to unlock the phone. Phone designers use time deferments to make the unlocking process inefficient in order to prevent thieves from rapidly guessing the passcode of the device.[63] With this built-in inefficiency, the aim of the 'figure' is to maintain an equilibrium between the inconvenience imposed on the user and the security of the device.

Desired inefficiency is also consciously introduced in blockchain proof-of-work applications. The operation of storing the output of a transaction in a blockchain application database, which otherwise is almost instantaneous, can and may be designed to be inefficient so that the values of trust and clock time can be reintroduced.[64] In such applications, while the fundamental challenge is achieving 'tamper-resistant validation' of transactions, the enhanced problem is 'fair validation' of transactions,[65] which adds a layer of complexity to the validation process.

The idea of applying desirable inefficiency to the code at the interface end of the user is particularly meaningful when it facilitates other human values, such as respect for autonomy or affordance of autonomy. Sometimes, even if it is technically feasible to achieve greater efficiency, opting for a less efficient design may be preferable. This choice makes it viable to segregate the elements in the design of the artifact, which involves diverging or conflicting interests.[66] The deliberate inclusion of slowness and inefficiency in the code's design can assist in incorporating broader normative standards and values. The objective is to set up slowness and inefficiency as potentially beneficial features.

The conceptualization of desirable inefficiency, when incorporated into the user-facing code in terms of affordances and inscriptions, can throttle *lex cryptographic* instantaneity in favor of comprehension and empowerment. By purposefully reducing temporal compression, fragmentation, and densification in the

[60] Kroll (2018), p. 4.

[61] Ohm and Frankle (2018), p. 31.

[62] Ohm and Frankle (2018), p. 5.

[63] Bay (2017). https://firstmonday.org/ojs/index.php/fm/article/view/7006/5860.

[64] Ohm and Frankle (2018), pp. 19–22.

[65] Ohm and Frankle (2018), pp. 29–30.

[66] Clark (2010), pp. 36–37.

user-code interactions, the notion of slow computing pitchforks humans to the forefront of technology.[67] Such a viewpoint also connects with the philosophy of technology that considers instantaneity as a major risk to the rule of law *vis-à-vis* justice.[68] The rule of law values ought to be accorded with reasonable time and space to function in the social domain without being constrained by the notion of efficiency and strategic manipulation that is centered on technological rationality.[69] The affordance of deferment is about limiting 'technological rationality', such as certainty, efficiency, and speed, in favor of those rooms.[70] At the same time, it is linked to a counterintuitive notion that fosters ambiguity intentionally in an affordance so that the responses of the user are not limited to only those possibilities constituted by the 'figure'.

Similar to the affordance of configurability, the affordance of deferment also entails identifying and recognizing suitable circumstances where a certain amount of autonomy ought to be afforded to the user. Deferment allows them to assess the circumstances before continuing with further code execution.[71] Since every possible outcome of execution cannot be foreseen in advance, any attempt to hedge emergencies emerging due to the same will probably launch unforeseen and undesirable results.

The concept of imposing friction is strongly rebuffed in blockchain applications. The lack of friction often opposes the exercises of autonomy demonstrated through choices and consequences.[72] Automatic sharing of everyday events, such as going to the groceries or exercising in fitness studio on social media platforms without any information feeding by the user, is a simple outcome of a reduction in frictional code.[73] Due to the incorporation of the affordance of deferment into the technological system, the user has to follow a couple of steps, like manually inputting the information into the application and then confirming it to share online and also, in some cases, manually choosing the individuals to share the details with. Unlike the one-click mechanism,[74] the aforementioned 'non-automated' steps involve thoughtful and conscious decisions by the user.

If designs are not complemented with appropriate informative identifiers, then such designs, even if provisioned with efficient affordances, can have unanticipated and unfavorable outcomes. For example, the frictionless sharing feature of Instagram in connection with Facebook is problematic for many as they do not realize with whom they are sharing intimate posts. By deliberately designing friction into the relevant parts of the code of the artifact as an affordance of deferment, users are

[67] Fraser and Kitchin (2020), pp. 2, 11–16.

[68] Zimmerman (1995), p. 86.

[69] Feenberg (2010).

[70] Cohen (2012), chp. 2.

[71] Vitale et al. (2019), p. 1463.

[72] Narayanan et al. (2020), p. 82. Krisam et al. (2021).

[73] Frischmann and Benesch (2023), p. 376.

[74] Hayes et al. (2016), p. 171.

given an opportunity to review and make a considered decision before the code executes the next step.[75] The notion of friction connects with the design process, where the quantum of friction presupposes a compound design decision that instinctively benefits certain users while being burdensome for others.[76] The ability to share should not be switched on as a design principle before the execution of the act itself—'it should not be easier to share an action online as compared to doing it'.[77] Of course, analogous principles could be applied to any rule of code-based step that will have normative effects, and the code should afford the user an opportunity to consider before taking the next step.

10.2.4 Obscurantism

The attributes such as rule-fetishness, immutability, and instantaneity are necessary features of blockchain code, or at least desirable for the system to achieve its commercial goals, and changing or compromising these attributes can affect the functionality, performance, or security of the system or undermine its purpose or value.[78] However, obscurantism is an attribute whose *crypto-legalistic* nature can be balanced with the affordance of transparency relatively easily. Obscurantism of code is not inherent or essential to the system but rather contingent or optional. That is, the obscurantism of code is not a necessary feature of blockchain code but rather a design choice or a consequence of other factors. It can be reduced or eliminated by changing the design or the implementation of the code or by providing additional information or tools to the users. For example, the code can be made more readable, documented, or standardized, or the system can provide interfaces, dashboards, or audits that reveal the code, its functionality, its execution, and its outcomes.[79] Other attributes of code are more inherent to the system and, therefore, more difficult to balance with the rule of law affordances.

In the context of *crypto-legalism*, obscurantism is primarily associated with Fullerian design standards 2 and 4, which describe the promulgation of rules in relation to the principles of alternativity and normative density and clarity of rules. As per Fullerian design standard 2, ordinary rules by which the citizens are governed must be known to them so that they can press for their rights, responsibilities, and entitlements when disregarded by the administrative authorities. There ought to be agreement or harmony between the rule and the official action derived from it, in consonance with the Fullerian design standard 8. Of course, citizens are also empowered to observe the operation of the artifacts, an essential precondition to

[75] Calo (2013), p. 773.

[76] McGeveran (2013), pp. 53–54.

[77] McGeveran (2013), p. 63.

[78] Adler-Nissen and Drieschova (2019), p. 531.

[79] Tollon (2022), p. 239.

challenge the rules. Attaining the legality of rules is very difficult or impossible when the rules are obscure and incoherent. A rule should be intelligible for it to be legally validated and legitimate.

The use of the rule of code is subjected to a higher threshold of justification since the user is not able to see the rules incorporated in the code. Though the threshold of justification is lowered with the decrease in the level of rule-fetish measures the design adopts, the obscurantism of the code must be considered in the best interests of the user. Fullerian design standard 2 enunciates that it could be challenging for the users to comprehend the intensity of the technological normativity to which their behavior has been subjected, if the code becomes opaquer. Threats of penalty are positioned at the denser end of the normative density spectrum, while simple recommendations are positioned at the less dense end. With this, Fullerian design standard 2 envisages balancing the policy objectives and the means to achieve the same. At the same time, the usage of a specific designing procedure must be validated taking into account other design standards, specifically whether substitute instruments have accomplished similar results more legitimately. The user often assumes that the characteristics of the code are natural and not just some possibilities among innumerable others. The obscurantism surrounding normative impact becomes especially pronounced in situations where there is a necessity to legitimize strong configurations of disaffordances and inscriptions that guide the behavior of the user.

10.2.4.1 Affordance of Transparency

Social scientists and scholars from the humanities support ‘explainability’, which covers both descriptive accounts and critical simulations.[80] From the perspective of affordance of transparency, even though the code is accessible by all in a public blockchain, the problem of command code rule (source code) transparency potentially persists—the artifact does not automatically become comprehensible to the user by having access to the application’s code. In the case of blockchain applications, initiatives such as solidity contracts that allow special forms of comments are an effort to address this problem.[81] This special form of comments, named the Ethereum Natural Specification Format (NatSpec)[82] facilitates rich documentation for various functions and variables and segmentation thereof into developer-focused messages and user-facing messages. When the user interacts with the contract, it can access these messages. By using NatSpec, the ‘figure’ can provide descriptive code commentaries about the operation of the application from which a natural language explanation can be automatically generated. Here is an example of how NatSpec comments can be used in the code to document a blockchain application designed for digital identity management:

[80] Rennie et al. (2022), p. 837.

[81] Umucu (2021). https://doi.org/10.2139/ssrn.3916072.

[82] Solidity (2025). https://docs.soliditylang.org/en/latest/natspec-format.html.

```
/// @title Digital Identity Management Smart Contract
/// @notice This smart contract allows users to create and manage
their digital identities on the blockchain.

contract DigitalIdentityManager {
 struct Identity {
 string username;
 string email;
 address userAddress;
 bool isVerified;
 }

 // Mapping of Ethereum addresses to digital identities
 mapping(address => Identity) public identities;

 /// @notice Create a new digital identity.
 /// @dev The caller's Ethereum address will be linked to this
identity.
 /// @param _username The desired username for the identity.
 /// @param _email The email address for the identity.
 function createIdentity(string memory _username, string memory
_email) public {
 require(bytes(_username).length > 0, "Username cannot be
empty");
 require(bytes(_email).length > 0, "Email cannot be empty");
 require(identities[msg.sender].userAddress == address(0),
"Identity already exists for this address");

 identities[msg.sender] = Identity({
 username: _username,
 email: _email,
 userAddress: msg.sender,
 isVerified: false
 });
 }

 /// @notice Verify an identity.
 /// @dev Only authorized entities can verify identities.
 /// @param _userAddress The Ethereum address of the identity to
be verified.
 function verifyIdentity(address _userAddress) public {
 require(msg.sender == authorizedVerifier, "Only authorized
entities can verify identities");
 require(identities[_userAddress].userAddress != address(0),
"Identity does not exist for this address");
```

```
 identities[_userAddress].isVerified = true;
 }

 /// @notice Get information about an identity.
 /// @param _userAddress The Ethereum address of the identity.
 /// @return username The username associated with the identity.
 /// @return email The email associated with the identity.
 /// @return isVerified A boolean indicating if the identity is
verified.
 function getIdentityInfo(address _userAddress) public view
returns (string memory username, string memory email, bool
isVerified) {
 Identity memory identity = identities[_userAddress];
 return (identity.username, identity.email, identity.isVerified);
 }

 address public authorizedVerifier;


 /// @notice Set an authorized entity to verify identities.
 /// @dev Only the owner of the contract can set the verifier.
 /// @param _verifier The Ethereum address of the
authorized entity.
 function setAuthorizedVerifier(address _verifier) public {
 require(msg.sender == owner, "Only the owner can set the
verifier");
 authorizedVerifier = _verifier;
 }
}
```

In this example, /// @title Digital Identity Management Smart Contract provides a high-level description of the smart contract's purpose. This smart contract allows users to create and manage their digital identities on the blockchain, further clarifying the contract's functionality. NatSpec comments are used for explaining the purpose and usage of functions such as createIdentity, verifyIdentity, getIdentityInfo, and setAuthorizedVerifier. These comments help users understand how to interact with the digital identity management contract and emphasize the transparency and purpose of the contract.

The objective is to provide transparency in operation, that is, transparency in the imposition of normativity, so as to explain to the user the logic of the blockchain application. This mechanism is about recording the use of a code rule at any particular point on a normativity scale and communicating the documentation or information to the user. However, transparency has often been criticized as a tool by which

the 'figure' justifies their decisions that are against the interest of the user.[83] By including lengthy descriptions of functionality in voluminous documents, the legitimacy of the transparency can be achieved, but it does not have any practical value for the user to be enlightened about the functions or processes.[84] The idea behind transparency is that by providing more information it will empower the users to make informed decisions about which products will be a catalyst for greater competition and better products.

The 'figure's' comprehension and interpretation of the code, which is often subjective and personal, is a continuing hindrance to this approach. Unless the 'figure' accurately documents the logic of the application in natural language at appropriate moments, the end result would be less desirable than if there were no explanation at all, and the user will have a misdirected trust in the understanding of the system. Such explanatory notes that are not written with accuracy bring in an auxiliary interpretative layer between the code's normativity and the user, thus increasing the possibility of committing errors and misinterpretations by both the 'figure' and the user.

There are also solutions for transparency that seek to engage directly with the user. For example, in order to facilitate third-party audits, the command code rule that lies beneath the regulatory, technological systems could be needed to be open. Though such an idea has been acceptable to public sector regulators,[85] business corporations, in general, have not been very supportive of the idea of opening up their proprietary codes of products and services.[86] Another approach could be to have an escrow system, where the command code rule of the artifact would be under the custody of a trusted third party to be published only at the direction of a court in case of litigation.[87] These approaches, however, do not consider the entire context and texture of the code's corporeality.

Code is not just about technical details but also about social and cultural values that are built into it. While the study of bare code facilitates the accumulation of information about the artifact and its functions, an expansive sensitivity to design concepts, such as affordance, inscription, and description, is still essential to fully appreciate its implications on the execution since the rule of code and design choices for it enables and limits what users can do with it. Since such approaches are not based on *ex-ante* legitimacy, the programming of illegitimate code cannot be avoided just by relying on *ex-post* assessment, and therefore, the harmful code or malware would continue to operate, possibly indefinitely, if no issues are detected in the *ex-post* assessment.

The real purpose of transparency is not just limited to the openness of the command code rule but to facilitate comprehension so that the 'figure' can ensure

[83] Casey et al. (2019), p. 143. Edwards and Veale (2017), p. 18.

[84] Newberry (2013), p. 165.

[85] European Commission (2020). https://commission.europa.eu/about/departments-and-executive-agencies/digital-services/open-source-software-strategy_en.

[86] Rolandsson et al. (2011), p. 576.

[87] Denson (2002), p. 1.

reasonable correspondence between the conceptual framework of the system in the user's mind and the actual artifact.[88] Needless to say, the 'figure' has the capability to signify the particular functionalities of the artifact that have been enabled for the user.[89]

> Communicating the results of the design processes helps the public or specific stakeholders to better understand how the technology has been designed and how it has been mitigated.[90]

This template uses resources from the interface of the artifact to formulate advertisements, press releases, and instruction manuals that are largely under the control of the 'figure'. The Digital Services Act also mandates the publication of comprehensive reports, which shall include the identification and assessment of systemic risks of very large online platforms and very large search engines, and best practices to mitigate such risks.[91]

Such transparency enables user trust and compliance towards the artifact. As the conceptions of the 'figure' are likely to be distinctly different from the idea and understanding of the user who is less informed, a sense of empathy by the 'figure' with the user is also a necessity.[92]

The user should be able to grasp, to a reasonable extent, the functioning of the code within the technological artifact through the affordance of transparency in the programming of the code rules as well as in operation. This affordance of transparency is linked with the affordance of accountability, that is, the ability to hold the system accountable. Since technology is often updated with either new features or disabling features, the 'figure' has the responsibility to inform the user of these changes that alter the interaction between the user and the system. When seen from the prism of Fullerian design standard 4, which throws light on the notion of coherence, the programming language of the code ought to be consistent in terms of the Fullerian design standard 5 on non-contradictions and consistency of norms in relation to the idea of coherence. Ensuring the comprehensibility and usability of the artifact is the responsibility of the 'figure'.[93] In terms of the legisprudential principle of coherence, harmonized with Fullerian design standard 7, once the user becomes familiar with the functioning of the artifact, any arbitrary change can be confusing and misleading. Hence, the design of the artifact should not be inconsistent or conflicting to avoid any misconception on the part of the user.

'Radix' is a vital component for affording transparency that relates to the affordance of due process. This approach can be tricky since even relatively simple

---

[88] Norman (2013), p. 31.

[89] Bergman et al. (2007), p. 11.

[90] Djeffal (2024), p. 21.

[91] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (hereinafter DSA), Article 35(2).

[92] Norman (2013), p. 31.

[93] Norman (2013), p. 32.

computing systems are often an assemblage of a number of components.[94] The 'figure' must afford reasonable indications of the sources of the code so that the user can be adequately informed and able to appropriate the affordance of due process. Transparency of 'radix' requires that such information be provided to the user. Even so, the user is unlikely to realize that the back-end processing of technological artifacts relies heavily on a host of services and third-party code libraries.

In the context of legitimation, the designed purposive functionalities of the conceptual code rules are linked with the environment, falling under Fullerian design standard 5. In addition to justifying the rule on internal legal grounds, it must also be backed by externalities that justify its nature. To contextualize, the affordance of transparency in the rule of code blueprint will need the reason for having a particular functionality if the same is not manifested in the artifact. A corollary of this argument is that an unexpected functionality needs to be justified by an external theory other than internal rationality. If the affordance of transparency cannot justify the normativity of the functionalities, then the 'figure' should not include such functionalities in the design of the artifact. Introducing a geolocator into an alarm clock application is an apt example where affordance of transparency is necessary; the reason being that determining the location is not a standard affordance of an alarm clock.[95] Such affordances ought to be considered by the 'figure', keeping in view the transparency of purpose (to use the application).

A word of caution—the 'figure' must not suffer from a false sense of transparency with the idea that 'any function can be incorporated by giving due notice and choice to the user'.[96] From this perspective, a 'monitoring citizen' would be a better normative ideal than a 'well-informed citizen'.[97] Though, in theory, the idea of a fully informed user seems desirable, considering the complexity and pervasiveness of code, it is not. A 'monitoring citizen' may not be aware of all functionalities and all activities but can effectively observe and monitor them and can conduct inquiries and contest policies when necessary.[98] Rather than aiming for full transparency, which is a sort of mirage, the idea of an 'appropriate' amount of affordance of transparency is more reasonable as a guiding principle for programming technological artifacts such as blockchain.

[94] Thornton et al. (2021), pp. 64–76.

[95] West (2018). https://youtu.be/YjVW4dD88hk.

[96] Hartzog (2019), p. 459.

[97] Van den Hoven (2005), p. 51.

[98] Lessig (1999), p. 56.

10.2.5 'Umbrella' Affordance of Due Process

One of the main issues to consider is how to afford due process rights in a technological artifact, which means allowing the code to be challenged and, thus, by drawing inference, challenging the 'figure' in the judicature. This is essential for upholding the rule of law in the realm of blockchain regulation. The possibility of switching from a normative framework of code to those of the conventional law is crucial for preserving the function, authority, and integrity of the rule of law in the code's alegal domain. Affordance of due process is hindered by *crypto-legalism*, which demands that the users comprehend the normative systems they are subjected to overcome any legal challenge. Friction in the form of affordance of deferment and transparency as an affordance is related to such conception, as they involve the user's capacity to inspect and question the rule of code they are bound by. This represents the side of the coin that is for the user in terms of due process rights, where the other side of the coin represents the legal systems, especially the judicature. Regardless of the advantages or disadvantages of the design, it must always be feasible for the user to seek legal recourse to determine the illegality and illegitimacy of the code. This guarantees that the rule of law has an enduring influence in the design process, even when the code operates as a distinct alegal normative structure.

References

Adler-Nissen R, Drieschova A (2019) Track-change diplomacy: technology, affordances, and the practice of international negotiations. Int Stud Q 63:531

Allen JG (2018) Wrapped and stacked: "smart contracts" and the interaction of natural and formal language. Eur Rev Contract Law 14:307

Ayres I, Gertner R (1989) Filling gaps in incomplete contracts: an economic theory of default rules. Yale Law J 99:87

Bay M (2017) The ethics of unbreakable encryption: Rawlsian privacy and the San Bernardino iPhone. First Monday 22

Beard JM (2014) Autonomous weapons and human responsibilities. Georgetown J Int Law 45:617

Bergman M et al (2007) Boundary objects in design: an ecological view of design artifacts. J Assoc Inf Syst 8:11

Calo R (2013) Code, nudge, or notice. Iowa Law Rev 99:773

Carlsen H et al (2010) Assessing socially disruptive technological change. Technol Soc 32:209

Casey B et al (2019) Rethinking explainable machines. Berkeley Technol Law J 34:143

Cerf V, Ryan P (2014) Internet governance is our shared responsibility. I/S: J Law Policy Inf Soc 10:1

Citron DK (2007) Technological due process. Wash Univ Law Rev 85:1249, 1252

Clark DD (2010) Tools of engagement: mapping the tussles in cyberspace. MIT Political Science Department, ECIR working paper no. 2010-4

Clark DD et al (2002) Tussle in cyberspace: defining tomorrow's internet. ACM SIGCOMM'02, p 347

Cohen JE (2012) Configuring the networked self: law, code, and the play of everyday practice. Yale University Press

Collingridge D (1980) The social control of technology. St. Martin's Press, p 11

De Filippi P, Wright A (2018) Blockchain and the law: the rule of code. Harvard University Press
Denson WD (2002) The source code escrow: a worthwhile or worthless investment. Rutgers Bankruptcy Law J 1:1
Desai DR, Kroll JA (2017) Trust but verify: a guide to algorithms and the law. Harv J Law Technol 31
Djeffal C (2024) Law by design obligations: the future of regulating digital technologies in Europe? SSRN Electronic J (SSRN 4765471) 3
Durovic M, Lech F (2019) The enforceability of smart contracts. Italian Law J 5:493
Edwards L, Veale M (2017) Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for. Duke Law Technol Rev 16:18
European Commission (2020) Open-Source Software Strategy 2020-2023. https://commission.europa.eu/document/download/97e59978-42c0-4b4a-9406-8f1a86837530_en?filename=en_ec_open_source_strategy_2020-2023.pdf
Evans SK et al (2017) Explicating affordances: a conceptual framework for understanding affordances in communication research. J Comput-Mediat Commun 22:35
Feenberg A (2010) Between reason and experience: essays in technology and modernity. MIT Press
Fraser A, Kitchin R (2020) Slow computing. Bristol University Press
Frischmann B, Benesch S (2023) Friction-in-design regulation as 21st century time, place, and manner restriction. Yale J Law Technol 25:376
Gillespie T (2019) Algorithmically recognizable: Santorum's Google problem, and Google's Santorum problem. In: Beer D (ed) The social power of algorithms. Routledge
Goossens J (2021) Challenges and opportunities of blockchain and smart contracts for democracy in the distributed, algorithmic state. In: Pollicino O, De Gregorio G (eds) Blockchain and public law: global challenges in the era of decentralisation. Edward Elgar, p 76
Gürses S et al (2011) Engineering privacy by design. Comput Privacy Data Prot 14:25
Hartzog W (2019) The public information fallacy. Boston Univ Law Rev 99:459
Hartzog W et al (2016) Inefficiently automated law enforcement. Mich State Law Rev 1763
Hayes RA et al (2016) One click, many meanings: interpreting paralinguistic digital affordances in social media. J Broadcast Electron Media 60:171
Hazard J, Haapio H (2017) Wise contracts: smart contracts that work for people and machines. In: 20th international legal informatics symposium (IRIS 2017), p 425
Hildebrandt M (2008) Legal and technological normativity: more (and less) than twin sisters. Techne Res Philos Technol 12:169
Hildebrandt M (2015) Smart technologies and the end (s) of law: novel entanglements of law and technology. Edward Elgar, p 10
Hildebrandt M (2018) Algorithmic regulation and the rule of law. Philos Trans R Soc A Math Phys Eng Sci 376:20170355
Kalogiros C et al (2009) On designing for tussle: future internet in retrospect. In: Oliver M, Sallent S (eds) The internet of the future. Springer
Kesan JP, Shah RC (2006) Setting software defaults: perspectives from law, computer science and behavioral economics. Notre Dame Law Rev 82:583
Klass G (2023) How to interpret a vending machine: smart contracts and contract law. Georgetown Law Technol Rev 7:69
Kouroutakis A (2020) The virtues of sunset clauses in relation to constitutional authority. Statute Law Rev 41:16
Krisam C et al (2021) Dark patterns in the wild: review of cookie disclaimer designs on top 500 German websites. In: European symposium on usable security (EuroUSEC 2021)
Kroll JA (2018) The fallacy of inscrutability. Philos Trans R Soc A Math Phys Eng Sci 376
Lessig L (1999) The architecture of privacy: remaking privacy in cyberspace. Vanderbilt J Entertain Technol Law 1:56
Levy KEC (2017) Book-smart, not street-smart: blockchain-based smart contracts and the social workings of law. Engag Sci Technol Soc 3:1
Lipshaw JM (2019) The persistence of "Dumb" contracts. Stanf J Blockchain Law Policy 2:1

McGeveran W (2013) The law of friction. Univ Chic Leg Forum 15:53–54
Mik E (2021) Contracts in code? Law Innov Technol 13:478
Naor M, Pinkas B (2010) Efficient trace and revoke schemes. Int J Inf Secur 9:411
Narayanan A et al (2020) Dark patterns: past, present, and future: the evolution of tricky user interfaces. Queue 18:67
Newberry B (2013) Engineered artifacts. In: Michelfelder DP et al (eds) Philosophy and engineering: reflections on practice, principles and process. Springer, p 165
Norman DA (1999) Affordance, conventions, and design. Interactions 6:38
Norman DA (2013) The design of everyday things: revised and expanded edition. Basic Books, p 11
Ohm P, Frankle J (2018) Desirable inefficiency. Florida Law Rev 70:777
Ohm P, Kim N (2023) Legacy switches: a proposal to protect privacy, security, and the environment from the internet of things. Ohio State Law J 84:101
Owens J, Cribb A (2019) "My Fitbit thinks I can do better!" Do health promoting wearable technologies support personal autonomy? Philos Technol 32:23
Pasquale F (2019) A rule of persons, not machines: the limits of legal automation. George Wash Law Rev 87:1
Posner EA (2006) There are no penalty default rules in contract law. Florida State Univ Law Rev 33:563
Raskin M (2017) The law and legality of smart contracts. Georgetown Law Technol Rev 1:305
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)
Rennie E et al (2022) Toward a participatory digital ethnography of blockchain governance. Qual Inq 28:837
Rolandsson B et al (2011) Open source in the firm: opening up professional practices of software development. Res Policy 40:576
Schwartz A, Scott RE (2016) The common law of contract and the default rule project. Virginia Law Rev 102:1523
Sevignani S (2016) The problem of privacy in capitalism and alternative social media: the case of diaspora. In: Fuchs C, Mosco V (eds) Marx in the age of digital capitalism. Brill, pp 413–446
Shah RC, Sandvig C (2008) Software defaults as de facto regulation the case of the wireless internet. Inf Commun Soc 11:25
Shay LA et al (2016) Do robots dream of electric laws? An experiment in the law as algorithm. In: Calo R et al (eds) Robot law. Edward Elgar
Stanley-Marbell P et al (2020) Exploiting errors for efficiency: a survey from circuits to applications. ACM Comput Surveys (CSUR) 53:1
Sunstein CR, Thaler RH (2003) Libertarian paternalism is not an oxymoron. Univ Chic Law Rev 70:1159
Thornton L et al (2021) Fifty shades of grey: in praise of a nuanced approach towards trustworthy design. In: ACM conference on fairness, accountability, and transparency (FAccT '21), pp 64–76
Tollon F (2022) Artifacts and affordances: from designed properties to possibilities for action. AI Soc 37:239
Umucu EH (2021) Solidity: smart contract language or legal contract language
Van den Hoven J (2005) E-democracy, E-contestation and the monitorial citizen. Ethics Inf Technol 7:51
Vitale F et al (2019) Keeping and discarding personal data: exploring a design space. In: Designing interactive systems conference (DIS '19), p 1463
Weber RH (2018) "Rose is a rose is a rose is a rose"–what about code and law? Comput Law Secur Rev 34:701

West DM (2018) The future of work: robots, AI, and automation. Brookings Institution Press. https://youtu.be/YjVW4dD88hk
Winner L (1978) Autonomous technology: technics-out-of-control as a theme in political thought. MIT Press, p 284
Wong PH (2020) Democratizing algorithmic fairness. Philos Technol 33:225
Yeung K (2008) Towards an understanding of regulation by design. In: Brownsword R, Yeung K (eds) Regulating technologies: legal futures, regulatory frames and technological fixes. Hart, p 79
Zimmerman AD (1995) Toward a more democratic ethic of technological governance. Sci Technol Hum Values 20:86

Part IV
Conclusions

Chapter 11
Conclusions

The widely used classical 'law and technology' approach targets legal rules as an instrument to focus on the hiccups produced by technology.[1] However, there is a need for the action 'law+technology' to call for legal rules to nullify the negative ramifications while maintaining the technology's benefits.[2] While acknowledging the positive aspects of the technology, the effort here is to reduce the harmful effects of the blockchain by using the rule of law by design framework as a moral aspiration to bring in change in the artifact by answering the central question—*can the rule of law shape, guide, and influence the design and implementation of blockchain technology in a legitimate manner?*

> Though technological systems rival legal constitutions in their power to order and govern society, there is no systematic body of thought, comparable to centuries of legal and political theory, to articulate the principles by which technologies are empowered to rule us.[3]

Hence the discussions are not about formulating another thesis on regulating blockchain but more concerned about shaping and guiding the intentionality of the 'figure', that is, the designers, innovators, and stakeholders involved in developing, designing, and implementing the blockchain technology, which can potentially regulate human behavior 'strongly' as compared to the law,[4] through code that is commended as a powerful regulator since 'technology is not particularly suited as a

[1] Schrepel (2023), p. 2. European Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts 2021 [COM/2021/206 final]'.

[2] See Chap. 2, Sect. 2.4 to read more on the risks and opportunities of the blockchain for the rule of law.

[3] Jasanoff (2016), p. 9–10.

[4] See Chap. 5.

A. Bisoyi, *Blockchain and Legitimacy*, Law, Governance and Technology Series 77, https://doi.org/10.1007/978-3-031-98712-0_11

regulatory target'[5] because 'it is generally not the technology that is regulated, but rather a socio-technical landscape'.[6]

11.1 Reflections on the Rule of Law, Blockchain and Legitimacy

The rule of law can be and must be used as an instrument for shaping blockchain since this technology is being sought as a solution for strengthening the rule of law-based society and negating the detrimental aspect of the centralized government, such as the arbitrary exercise of power, due to the blockchain's inherent characteristics of immutability, tamper-resistant, distributed nature, and automated execution which promises transparency and accountability, by the States and international organizations. As an instrument, it allows the technology to produce normative impacts on the society where the technology is employed for the purposes of fulfilling human rights and humanitarian goals as well as democratic e-public service aspirations. Since blockchain gives rise to the notion of the rule of code or *lex cryptographica*, which operates according to pre-defined and specific rules, without any human intervention, through smart contracts programmed via code, it portrays itself as trust and confidence machine to be employed in order to curb corruption in a democratic society.

> The decisions that shape the public's everyday experience are found not in legislative codes but software codes and are made not by elected officials in parliaments, but by scientists and innovators in private settings. Their choices will resonate for generations to come.[7]

Since, in addition to positive impacts, adverse normative effects are also created due to the blockchain being employed for illegal purposes such as tax evasion or human trafficking[8] or because of lack of proper governance,[9] it becomes necessary to eliminate or minimize any such conceptual norms which generate alegal *ex-post* effect, in order to preserve the rule of law domain, by guiding the 'figure', in the form of affordance possibilities and design choices. It becomes imperative to investigate the purpose behind the employment of the technology in the form of (design) choices made and decisions taken by the State to provide for a framework such that the technology is implemented with the intention to comply with the rule of law to generate and realize the common good.

Such an inquiry not only pertains to shaping the blockchain at the implementation level, that is, *ex-post* or macro-level, but also emphasizes on the micro level, that is *ex-ante* or design level. This is because the blockchain gives rise to the notion

[5] Moses (2013), p. 1.

[6] Leenes (2019), p. 4.

[7] Brownsword (2022), p. 252.

[8] See Chap 2, Sect. 2.4.1 and Chap. 4, Sect. 4.2.

[9] See Chap. 2, Sect. 2.2.2.

of the rule of code, or *lex cryptographica*, which acts as a hegemony rule structure over the rule of law for the protection of fundamental rights of users or citizens, which results in a space where there is the coexistence of two 'so-called' divergent environments. Where the rule of law provides fundamental rights with certain limitations, such as not violating the rights of others, the *lex cryptographica* environment questions this model and facilitates fundamental rights to be guaranteed with absolutism, irrespective of whether this absolute power may violate the rights of individuals.[10] Moreover, it creates a novel normative architecture, uncoupling the traditional infrastructure on which the rule of law and legal legitimacy are based, where it has the potential to codify legal norms and define as technological code in the form of smart contracts governing the normative contractual relationship between parties, such that the line between law and code gets blurred.[11] Unlike traditional legal rules that are only enforceable after the event (*ex-post*), regulation by code can proactively restrict individual actions since the rule of code is at once rule and reality, ensuring compliance before any potential violation occurs (*ex-ante*). In other words, code-based regulation prevents people from violating technical rules even before they can act. Since the *lex cryptographica* acts as an autonomous agent, live and ready to be executed when nudged by a transaction, and has the potential to replace the responsibilities of the State[12] that works according to the rule of law as a principle of governance mechanism and penetrates the fabric of society, it is crucial to establish that the rule of code norms are programmed in a legitimate manner and is in compliance with the rule of law, in order to not risk losing the basic tenets of the democratic society. The rule of code norms calls for the development of a schema that would facilitate the design of the technology to uphold the rule of law and be permissible for the public interest.

Technology, including blockchain, is never neutral and is inherently alegal by design where 'they tend to reflect the inherent biases in whatever environment they originate from'.[13] Technologists view the artifact to be flourishing on 'scientific knowledge and objective facts',[14] intentionally separating technology and politics where politics is based on subjective values. When the technology solely bases itself on modifying behaviors, by any means possible, it forsakes and undervalues the rule of law notion of checks and balances due to 'the lack of democratic control' over the technological artifact.

> Where the law is created in the public domain, techno-regulation (even when adopted by 'the state') often is not.[15]

[10] See Chap 2, Sect. 2.4.2.

[11] See Chap 2, Sect. 2.2.

[12] See Chap 2, Sect. 2.2.2.

[13] Naarttijärvi (2019), p. 39.

[14] Feenberg (1991), p. 149.

[15] Feenberg (1991), p. 149; Leenes (2011), pp. 147–148.

This is why technological artifacts such as blockchain must be positioned within the rule of law environment—'a framework that encapsulates the mutual entanglements between culture, politics and technology'.[16]

The principle of the rule of law in modern democratic systems is a fundamental pillar of the moral dimension, which reduces the rule-fetish nature of legalism. It requires that rules are publicly declared in advance and have the qualities of generality, equality, and certainty.[17] Without these qualities, the rule of law would

> either collapse into ethics and come to depend on the ethical inclinations of those in power and authority, or collapse into arbitrary rule by law, undoing the checks and balances secured by an independent judiciary.[18]

An intelligible, reliable, and predictable order is essential for protecting rights, preventing arbitrariness, and holding the State accountable for unlawful acts. The notion of the rule of law primarily consists of universality and relatively consistent application over time in a prospective and non-contradictory manner.[19] Citizens need to know the limits and proper scope of their rights in advance for those rights to be meaningful, and as such, the rule of law allows individuals to modify their conduct in accordance with legal standards, enabling them to act autonomously and empowering them to a certain extent. The rule of law also establishes specific criteria that legislators must follow to govern legitimately, limiting power outside the legal framework. This brings in the dichotomy between the notion of 'what ought to be' and 'what is' the characteristics of the legal norm.[20]

The rule of law is a guidance tool that enables the valuation of 'the projective capacities of men and women',[21] an idea that can be realized only where the rules are clear, transparent, and notified. Since it carries the archetype of being 'good', that is, every individual accepts it and is in favor of it, even though some may have dissimilitude views about the concept,[22] the rule of law should be worth striving after as a measurement of a 'good', specifically, when developing, designing, and implementing the technology. In this context, Fuller's standards of inner morality of law are employed in relation to the legisprudential conceptualization, which lays down the rule of standards that the characteristics of the legal rules must possess that are conducive to shaping the *ex-ante* and *ex-post* evaluation of various normative rule-making processes.[23] With the Fullerian principles diagnosing values that are 'internal to the law in the sense that they form a part of the concept of law itself', reflecting 'what the law is only by reference to its purpose, and its purpose is an ideal rule of law', the analysis in this book establishes the aspect of legalism and

[16] Leenes (2011), pp. 147–148.
[17] Tamanaha (2004), p. 8.
[18] Hildebrandt (2020), p. 74.
[19] Waldron (1989), p. 84.
[20] Brownsword (2016), p. 102.
[21] Simmonds (1986), p. 120.
[22] Tamanaha (2004), p. 3.
[23] See Chap. 3.

legality and draws out the issues or notions that undermine the legitimacy of legal rules within the rule of law framework.[24] This discussion shows that without legality, the law collapses into legalism,

> which separates law from morality or into a rule by men that delivers us to the whims of whoever is in power or authority.[25]

Since the rules and norms within the coded architecture play a role in social ordering, there is an underscored conflict between the rule of code and the rule of law.[26] The relationship between the conventional rule of law environment and the blockchain environment is akin to that of 'Tom and Jerry'.[27] One of the features of the rule of code is that it entails law being approached as a language a computer can consume, which resonates with the idea that code helps to understand, create, and enforce the law better.[28] To test this aspect of 'law as code' or the rule of code, the regulatory sandbox technique or the 'boxing methods'[29] has been advocated where it requires 'placing the technology in an environment in which it cannot cause harm' to order to build a 'barrier between the diagnosis and its implementation in the real world'.[30] This technique stops technology from automatically breaking the law but also delays the decision-making process and reintroduces more human cognitive constraints. The diagnosis generated by code can be immediately put into action in real-life situations. However, there is a higher chance that the constraints of the code may result in legal violations.

The rule of law environment provides the citizen with the choice to follow the legal norm or not, the blockchain environment does not offer such a choice; it resonates with the 'take it or leave it' state of affairs, where the rule of code norms determines the individual user behavior, leaving no *carte blanche* for the user to consider the degree to which one wants to observe the code norm. It is essential to recognize the link between the normative intention of the 'figure' and the technological artifact that infuses within itself these intentions, which encourages and realizes the mapping of the rule of law against the technology.[31] In the blockchain domain, the 'figure', who might be a private enterprise, is bestowed with authority to make rules 'that are locked away in the black box'. While the rule of law ensures that the political dynamics shaped by the legal system reflect the ethical principles of reciprocity and respect for autonomy, the blockchain architecture undermines the notion of reciprocity such that the technology portrays obscurantism characteristics, disabling users from knowing what decisions they have been subject to. Such

[24] See Chap. 3, Sect. 3.2.

[25] Hildebrandt (2020), p. 74.

[26] See Chap 4, Sects. 4.1 and 4.2.

[27] See Chap. 4.

[28] See Chap. 4, Sect. 4.1.

[29] This was mentioned in Schreprel's paper on Law + Technology, but the idea was originated by Nick Bostrom on his paper on Super-intelligence. Bostrom (2014).

[30] Schrepel (2023), p. 12.

[31] Brownsword (2016), p. 102.

functioning of the technology may result in a 'downward spiral of diminished trust'[32] among the users.

Whereas the rule of law, conceived as 'a positivist system of rules',[33] directs society and governs behavior by sanctioning certain behaviors and actions as illegal, the code, on the other hand, fancies itself for being 'self-sufficient to address the problems created by technology',[34] which resonates with the observation of Lessig.[35] Here, the argument is not that the code can substitute for law but rather that code can effectively regulate users' actions in a similar way because the structure of any technological artifact shapes its usage, enabling the 'figure' to function as a regulator.[36]

Through technological mediation, the artifact refashions not only the 'implications of law through its interpretation into new contexts or new possibilities that the technology affords' but also reconfigures by way of 'normative refraction'[37] that happens when the legal standards interact with the coded values, design and decision choices, and norms of the technology used. Therefore, from the point of departure, one can explain and extrapolate how blockchain technology affords user behavior by inhibiting, constraining, and restricting their actions.[38] It recognizes that the materialization of the blockchain artifacts and the rule of code has a role to play 'in what we do, how we perceive and interpret the world, how we make our choices, and under what conditions'.[39] The ability of the rule of code to influence human behavior and determine what information is deemed accurate is endorsed as legitimate power. However, the challenge with the emerging blockchain epistemology is 'the kind of knowing',[40] which implies it may not align with our intentions or wishes if we seek to uphold the rule of law but instead with what technology enables. By employing the theory of affordance and technological mediation, it is established that 'the technology will affect what law governs, but also how the law governs'.[41]

As the law 'carries a commitment to the idea of man as a rational purposive agent, capable of regulating his conduct by rules rather than as a pliable instrument to be manipulated',[42] the values of the rule of law are expressed in terms of the Fuller's principles, which state that

> the rule of law is the enterprise of subjecting human conduct to the governance of rules.[43]

---

[32] Brownsword (2016), p. 102.

[33] Krygier (2014); Rosenfeld (2001), p. 1307.

[34] Schrepel (2023), p. 2.

[35] Lessig (2003), p. 2.

[36] See Chap 4, Sects. 4.2 and 4.3.2.

[37] Naarttijärvi (2019), p. 36.

[38] See Chap. 5.

[39] Verbeek (2005).

[40] Carayannis et al. (2021), p. 1; Finck (2018), p. 665.

[41] Naarttijärvi (2019), p. 37.

[42] Simmonds (1986), p. 122.

[43] Brownsword (2015), p. 3.

Ingeminating this view, the rule of law is applied to the blockchain environment, advancing an analogical comparison between the legal norms and the rule of code norms embedded into the technology resulting in *crypto-legalism.*[44]

Taking the rule of law as a meta-principle facilitates assuming an autonomous individual who can challenge the legal norms and offer a new interpretation. In contrast, the standards implemented by the blockchain paradigm do not allow 'effective contestation but only rationalized logical and probabilistic reasoning'.[45] This leads to an 'all-or-nothing approach that does not align with the principles of proportionality, individual autonomy, expediency, and certainty'.[46]

The binary nature of Turing computation, an inherent feature of blockchain artifact, and its logical consistency eliminate the discretionary power of the legal system to consider external knowledge when addressing complex cases. Inherently, this technology is a 'black box' stimulating its obscurantism *crypto-legalistic* characteristics due to its complexity and trade and commercial protections. The lack of transparency and the difficulty in comprehending the functioning of these systems, which are increasingly utilized by States and international organizations, pose a challenge to traditional legal principles underpinning the rule of law, such as transparency, fairness, and explainability. Even though the law may become entirely predictable with the use of the rule of code, it will still not have the required transparency and moral accountability, as it needs to be open to scrutiny and in compliance with the rule of law.

The regulatory landscape shifts when blockchain-enabled smart contracts are utilized to control behavior to ensure a predictable result.[47] As a result, the user's behavior is no longer based on moral norms because the environment is managed to prevent specific actions or to limit the available options. The signals change from being based on prudence (whether something ought or ought not to be done based on self-interest) or morality (whether something should or should not be done based on respect for one's own and others' legitimate interests) to indicating what is reasonably achievable or feasible (or what is not reasonably attainable or impossible).[48] In the translation from a conventional legal order to the blockchain environment, there appears to be a loss of the orthodox concept of normativity - 'ought' and 'ought not' are replaced by 'can' and 'cannot'. In this type of system, thus, individuals are unable to act based on their own judgments of what should be done, whether for self-interest or for moral reasons. The 'rigid' interpretation of code or its rule-fetishness decides what is legal or executable and what is not, which is very different from how law takes into effect –

[44] See Chap. 6.

[45] Hildebrandt et al. (2012).

[46] McIntyre and Scott (2008), p. 109.

[47] See Chap 6, Sect. 6.1.1.

[48] Brownsword (2011), pp. 1323–1324.

> legal effect is not a matter of brute force or mechanical application, but a matter of ensuring what use of language counts as having what effect. The effect is not causal but performative.[49]

The well-known DAO breach exemplifies the details of this functioning of code. The inadequately constructed code of a smart contract enabled a perpetrator to withdraw more than 3.6 million Ether (approximately 50 million dollars at that time and about 13.2 billion dollars today)[50] without the consent of its creator. The rule of code advocates contended that the action did not constitute theft because the attacker did not hack into the code but took advantage of or exploited it. It portrays the notion of 'code is law' into working, which shows that the rule of code can be considered a normative enterprise.

As legal scholars hinge on the abstraction of law as a normative enterprise, the question arises regarding the methodology of interpreting technological changes to the systems of social order and the implications of regulating technology through design.[51] To achieve the transition from 'code is law' to 'code as law', it is necessary to utilize the regulatory force of code to fully implement legal regulations in three different ways. One, legal obligations can be embedded directly into code. For instance, if a smart contract must include a withdrawal provision, then the platform can reject the contract if the provision is missing. Two, code can be designed to ensure that users adhere to specific legal obligations. Even though it doesn't directly translate legal duties into code, it demonstrates its capability to communicate legal information.[52] Third, while code is not explicitly created to maximize the enforcement of legal rules, it nonetheless assists users in complying with those rules. The emergence of public blockchains with non-coercive and horizontally structured governance substantially diminishes various malicious and arbitrary exercises of power techniques.[53] These techniques entail utilizing technical control of an infrastructure, that is, the rule of code, to impact compatible products and to reduce any infringement.

These mechanisms of transitioning to 'code as law' are also demonstrated through the works of Koops, Leenes, Brownsword, and Hildebrandt.[54] Since the reconfiguration of the technology is grounded on a behaviorist, cybernetic comprehension of human society continuously intertwining standard setting with monitoring and behavior modification,[55] examining the contemporary works on normative *ex-post* and *ex-ante* standards facilitates drawing a landscape of affordances and values that can be employed and intended for the implementation of the technology and production of the code embedded in the blockchain. Such an investigation

[49] Hildebrandt (2020), p. 74.

[50] The amount estimated as on 24 May 2024.

[51] Yeung (2008), p. 88.

[52] See Chap. 4, Sect. 4.3.2.

[53] See Chap. 4.

[54] See Chap. 7.

[55] Hildebrandt (2020), p. 74; Leiser and Murray (2016).

developed an understanding of the application of the ideals of the rule of law, specifically legality and legitimacy, onto the technology and its rule of code in order to channel and steer the conduct of the user and the intention of the 'figure'.[56]

The basis of the rule of law is that it is 'the fulcrum of normative legal orders',[57] which provides constraints on both institutions and citizens. It does not allow unjust governance and arbitrary exercise of the power of the law by its institutions, officials, and representatives. When governance meets the necessary criteria, the rule of law imposes restrictions on the citizens who are required to adhere to adequately established laws and demands accountable citizenship.[58] The ideals of the rule of law, such as legality and legitimacy, stand at disempowering the alegal technological normativity; the question is how to articulate and employ these ideals.

11.2 Relevance of the Rule of Law by Design

'The rule of law + blockchain' fosters a coalescence of 'social and technical constraints that leverage their strengths'[59] while acknowledging that various attributes and features of the rule of law and blockchain create synergies. In fact, since the rule of law and blockchain are complementary, one should use the other. It reinforces the question, 'How well does our existing conceptual apparatus serve us?'[60] The fundamental ideas of human rights and human dignity, which resonate with the virtue of legality and the rule of law, serve as the intellectual foundation we must safeguard to maintain a critical separation between emerging technologies and their perceived positive and negative uses and practices. Schrepel observes that 'the '+' approach is a positive contribution to the legal systems, not a concession to technology'.[61] This approach is also taken by the legislators when formulating the EU AI Act, which aims to 'ensure legal certainty to facilitate investment and innovation in AI'.

The rule of law by design emphasizes on the '+' perspective rather than '&', which helps to understand what Darwin calls 'complexity science'. According to Darwin, complexity science explores how the interplay between systems shapes and is reshaped by the evolving environment they collectively influence.[62] The by-design methodology provides a critical insight for States operating in the digital sphere. It is essential to avoid eliminating the unique attribute of technology through legal regulations, such as mandating a single point of access in blockchain governance. Doing so may cause the technology to lose relevance in favor of others. Technologies

[56] Brownsword (2011); Brownsword (2020), p. 100.

[57] Brownword (2016), p. 107.

[58] Brownsword (2016), p. 138.

[59] Schrepel (2023), p. 3.

[60] Brownsword (2011), p. 1322.

[61] Schrepel (2023), p. 3.

[62] Darwin (1859), p. 69.

exist and endure alongside others precisely because they offer unique value. Stripping away the elements that set a technology apart from others diminishes its value and can lead to its obsolescence. Regulators must ensure they do not hinder a technology's ability to adapt, thrive, and coexist with other technologies. A blockchain smart contract is unchangeable. It cannot be erased, halted, or modified. This immutability poses constraints for both the 'figure' who is the creator of the smart contract and the regulator, mainly when the smart contract facilitates an illegal transaction. In relation to this, one may read Article 30 of the EU Data Act, which has provided the implementation of a 'mechanism to terminate the ongoing execution of transactions'.[63] The proposed mechanism would challenge the survival of blockchain's inherent attribute of immutability, specifically immutable smart contract code. For instance, opting to introduce a 'kill-switch' within the smart contract can be interpreted in two ways under the said Data Act—firstly, smart contracts that include a kill-switch function will be considered legally compliant, whereas those without one will not receive the same presumption; secondly, only smart contracts featuring a kill switch function are deemed legal, while those without are not.

The immutability attribute distinguishes smart contracts from other forms of contracts. It generates value, fosters trust between parties by preventing one-sided non-execution, reduces transaction costs associated with monitoring and enforcement,[64] and helps combat corruption by preventing malicious alterations once the smart contract is on the network. It is crucial to maintain the integrity of the information on the blockchain. For instance, if an AI system running on a blockchain malfunctions, the company cannot erase entries from the database to conceal the reasons behind the malfunction. Immutability in blockchain can also be problematic when courts declare past transactions as illegal or when a user mistakenly sends a token to the wrong address. Since this attribute has both negative and positive implications, it must be regulated while being preserved.

The rule of law by design assists in understanding both the technology and the relevant rule of law principles better and thereby prevents disconnection between the two so that the strengths of both are not sacrificed.[65] The disconnection becomes an issue when legal regulations require compliance with technically challenging or potentially harmful obligations for technology. For instance, requiring the addition of kill-switch functions to existing smart contracts on the blockchain effectively puts these contracts to no use. There is also a risk that the 'figure' may poorly implement these ideas due to a lack of technical and legal expertise. Through the rule of law by design, the legal norms can be translated to different affordances and standards that should not be abandoned. Hence, an obligation is imposed on the 'figure' to embed moral and technical constraints, both *ex-ante* and *ex-post*. These by-design obligations safeguard the survival of technology because if the blockchain enforces

[63] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on Harmonised Rules on Fair Access to and Use of Data and Amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (EU Data Act)'.

[64] Schrepel and Buterin (2021), p. 12.

[65] See Chap. 8.

a rule that is in line with the rule of law, then it can be deduced that the technological artifact is also living up to the rule of law values.[66] Such a process encourages a relook at the normativity of law with respect to legality and the rule of law, where the technological artifact and its normativity exert pressure on the basic premise that law is a normative enterprise.[67]

The approach of the rule of law by design has been conceived to fulfill three main functions: firstly, establishing the 'die-hard' rule or standard; secondly, overseeing compliance, not only through warranting the incorporation of legal rules into the artifact but also ensuring that the notion of legal protection is not winnowed out of the system; and thirdly, rectifying non-compliance.[68]

11.2.1 State Decisions and the Rule of Law Affordances

The rule of law by design approach is apt because it focuses on upholding the existing standards and values instead of prescribing new ones. However, it is not overly conservative since it recognizes the need to assess the substance and effectiveness of these values and standards in light of new technologies, considering the fact that the design of such technologies can impact the values and legal norms they support or override. It is essential to acknowledge that new technology may reform our norms and values; the key is to ensure that any new configuration does not diminish the significance of existing values to align with new business models or more efficient administration.[69]

In respect of Fuller's standards of inner morality of law, adherence to the rule of law requires the State to provide explicit authorization for using technological artifacts, whether through general or specific provisions. This means that if authorization is lacking or an appropriate procedure for adopting a technological artifact has not been followed, then such an artifact would be deemed illegitimate.[70] The State decisions and their intentionality of design choices[71] in the employment and implementation of a blockchain for public services and humanitarian purposes,[72] reflect the influence of technology on society and the behavior of individuals. The State's legitimacy in employing the blockchain can be registered through different mechanisms –first, trust and confidence, that is, on-chain governance or off-chain governance; second, transparency, that is, public or private blockchains; and third, human

[66] Brownsword (2016), p. 102.

[67] Brownsword (2011), p. 1323.

[68] Morgan and Yeung (2007), pp. 74–75.

[69] Hildebrandt (2015), p. 216.

[70] Brownsword (2016), p. 111.

[71] See Chap. 9 with emphasis on Sect. 9.1.1.

[72] See Chap. 9 with emphasis on Sect. 9.2.

in the loop, that is democratic oversight.[73] The rule of law requires that the proposals for the implementation of blockchain artifacts to be promulgated be infused with the intentionality to incorporate the values of transparency, accountability, predictability, and due process as well as legal protection, while at the same time, ascertaining both the fundamental regulatory intent and the specific technological solution to be used. Regardless of whether the regulation method is a legal rule or a technological solution, the rule of law denounces regulatory processes that are inclined to deceive or ensnare those being regulated.[74]

> Although the Fullerian principles of legality are focused on the use of rules as the regulatory instrument, the spirit of promulgation, of transparency and of fair dealing that underlies Fuller's specification of his principles can be copied across to the use of technological management.[75]

The attempt is not to apply these legal standards and values as affordances 'directly' to the blockchain, which demonstrates different technological and affective affordances since such an attempt will result in failure. The rule of law affordances are identified, configured and designed to be compatible with Fuller's inner morality of law to create blockchain artifacts that reflect and embed these legal standards and values. These affordances should always focus on the 'resistibility' and contestability of the ensuing normativity. This requires that the design of affordances must be tested to achieve the broader goal of purposiveness, legal certainty, and justice.[76]

The entire premise of plotting the rule of law affordances against the *crypto-legalistic* characteristics of code[77] lies in the argument that –

> should we wish to preserve the legal protection of the rule of law in the context of a democratic society, we cannot take for granted that the upcoming technology will afford such legal protection. We will have to take a stand for the substance of the norms and the values we wish to retain, and this will involve active participation in the design of the onlife world.[78]

The concept of Fuller's inner morality of law has been employed to act as a 'virtuous' instrument to translate legal norms to plot the rule of law affordances for the reconfigured formulation of the rule of code, allowing the retention, articulation, and 'interpretation of the moral commitments'[79] into the blockchain architecture. Moreover, plotting the rule of law affordances with the mindset that the 'figure' can comprehend the legal norm results in misleading and flawed translations of legal norms to the rule of code. This causes predestined discordance between legal expectations and actual code functionality. It is acknowledged that introducing new laws may assist in bridging a few of the discordances; however, it is not sufficient to address the issue at the substratum layer, particularly as increasingly complex and

---

[73] See Chap 9, Sect. 9.4.

[74] Brownsword (2016), p. 139.

[75] Brownsword (2016), p. 139.

[76] Hildebrandt (2015), p. 218.

[77] See Chap. 10.

[78] Hildebrandt (2015), p. 219.

[79] Brownsword (2011), p. 1325.

'strict' textual legal rules can hinder rather than promote compliance. Due to the absence of legislation that is more compatible with blockchain technology, the rule of law by design provides an 'action-guiding test' framework for the 'figure' in programming the rule of code that may not be strictly legal but is formulated and configured to embody the rule of law standards, values including the notion of legality and legitimacy. The plotting exercise can minimize the risk of substantive illegitimacy—for instance, by affording a kill switch to disable the application—and can support due process procedures if such illegitimacy is discovered—'in the transition from legal normativity to technological normativity, we do not have to lose the spirit of the rule of law'.[80] Once the legal standards and values of the rule of law are construed and mapped into command code rules and conceptual code rules, compliance with these affordances and design requirements is guaranteed to a minimalist extent—the spirit of legitimacy and the rule of law are inherited.

References

Bostrom N (2014) Superintelligence: Paths, Dangers, Strategies. Oxford University Press, Oxford
Brownsword R (2011) Lost in translation: legality, regulatory margins, and technological management. Berkeley Technol Law J 26:1321
Brownsword R (2015) In the year 2061: from law to technological management. Law Innov Technol 7:1
Brownsword R (2016) Technological management and the rule of law. Law Innov Technol 8:1, 100
Brownsword R (2020) Law 3.0: rules, regulation, and technology. Routledge, London
Brownsword R (2022) Rethinking law, regulation, and technology. Edward Elgar Publishing, Cheltenham, p 252
Carayannis EG et al (2021) Known unknowns in an era of technological and viral disruptions - implications for theory, policy, and practice. J Knowl Econ:1
Darwin C (1859) On the Origin of Species: Facsimile of the First Edition. p 69
European Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts 2021 [COM/2021/206 final]'
Feenberg A (1991) Critical theory of technology, vol 5. Oxford University Press, Oxford, p 149
Finck M (2018) Blockchains: regulating the unknown. German Law J 19:665
Hildebrandt M (2015) Smart technologies and the end (s) of law: novel entanglements of law and technology. Edward Elgar Publishing, Cheltenham, p 10
Hildebrandt M (2020) The artificial intelligence of European Union law. German Law J 21:74
Hildebrandt M et al. (2012) Digital enlightenment yearbook 2012. IOS Press, Amsterdam, p 332
Jasanoff S (2016) The ethics of invention: technology and the human future. WW Nor-ton & Company, New York, pp 9–10
Krygier M (2014) Rule of law (and Rechtsstaat). In: Silkenat JR et al (eds) The legal doctrines of the rule of law and the legal state (Rechtsstaat). Springer, Cham
Leenes R (2011) Framing techno-regulation: an exploration of state and non-state regulation by technology. Legisprudence 5:143
Leenes R (2019) Of horses and other animals of cyberspace. Technol Regulation 2019:1

[80] Brownsword (2011), p. 1364.

Leiser M, Murray A (2016) The role of non-state actors and institutions in the governance of new and emerging digital technologies. In: Brownsword R (ed) Oxford handbook of law, regulation and technology. Oxford University Press, Oxford
Lessig L (2003) Law regulating code regulating law. Loyola Univ Chicago Law J 35:1, 2
McIntyre TJ, Scott C (2008) Internet filtering: rhetoric, legitimacy, accountability. In: Brownsword R, Yeung K (eds) Regulating technologies: legal futures, regulatory frames and technological fixes. Hart Publishing, London, p 109
Morgan B, Yeung K (2007) An introduction to law and regulation: text and materials. Cambridge University Press, Cambridge, pp 74–75
Moses LB (2013) How to think about law, regulation and technology: problems with 'technology' as a regulatory target. Law Innov Technol 5:1
Naarttijärvi M (2019, 2019) Legality and democratic deliberation in black box policing. Technol Regulation:35, 39
Rosenfeld M (2001) The rule of law and the legitimacy of constitutional democracy. South Calif Law Rev 74:1307
Schrepel T (2023) Law + technology. J Law Technol @ Texas 1:2
Schrepel T, Buterin V (2021) Blockchain code as antitrust. Berkeley Technol Law J 1:12
Simmonds NE (1986) Central issues in jurisprudence: justice, Laws, and rights. Sweet & Maxwell, London, p 120
Tamanaha BZ (2004) On the rule of law: history, politics, theory. Cambridge University Press, Cambridge, p 8
Verbeek PP (2005) What things do: philosophical reflections on technology, agency, and design. Penn State Press, University Park
Waldron J (1989) The rule of law in contemporary Liberal theory. Ratio Juris 2:79, 84
Yeung K (2008) Towards an understanding of regulation by design. In: Brownsword R, Yeung K (eds) Regulating technologies: legal futures, regulatory frames and technological fixes. Hart Publishing, London, p 79

Index

A. Bisoyi, *Blockchain and Legitimacy*, Law, Governance and Technology Series 77, https://doi.org/10.1007/978-3-031-98712-0