CYBER LAUNDERING:

International Policies and Practices

Edited by: **Nathalie Rébé**

World Scientific

CYBER LAUNDERING:

International Policies and Practices

This page intentionally left blank

CYBER LAUNDERING:

International Policies and Practices

Edited by: **Nathalie Rébé**

World Scientific

NEW JERSEY • LONDON • SINGAPORE • BEIJING • SHANGHAI • HONG KONG • TAIPEI • CHENNAI • TOKYO

Published by

World Scientific Publishing Europe Ltd.

57 Shelton Street, Covent Garden, London WC2H 9HE

Head office: 5 Toh Tuck Link, Singapore 596224

USA office: 27 Warren Street, Suite 401-402, Hackensack, NJ 07601

Library of Congress Cataloging-in-Publication Data
Names: Rébé, Nathalie, editor.
Title: Cyber-laundering : international policies and practices / edited by Nathalie Rébé.
Description: Hackensack, New Jersey : World Scientific, [2023] |
Includes bibliographical references and index.
Identifiers: LCCN 2022025580 | ISBN 9781800612822 (hardcover) |
ISBN 9781800612839 (ebook for institutions) | ISBN 9781800612846 (ebook for individuals)
Subjects: LCSH: Money laundering--Prevention. | Computer crimes--Prevention. |
Money laundering--Law and legislation. | Computer crimes--Law and legislation. |
Crime prevention--International cooperation.
Classification: LCC HV6768 .C87 2023 | DDC 364.16/8--dc23/eng/20220815
LC record available at https://lccn.loc.gov/2022025580

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library.

For any available supplementary material, please visit
https://www.worldscientific.com/worldscibooks/10.1142/Q0378#t=suppl

Desk Editors: Aanand Jayaraman/Adam Binnie/Shi Ying Koe

Typeset by Stallion Press
Email: enquiries@stallionpress.com

Printed in Singapore

https://doi.org/10.1142/9781800612839_fmatter

Preface

This book illustrates current cyber laundering practices and the underlying risks associated with them, such as cross-border crimes and terrorism financing. Despite the existence of regulations and strong worldwide cooperation, countermeasures and international response efforts are often hindered by enforcement and jurisdictional issues, as well as online asset recovery complexity.

This work investigates the blockages to the accomplishment of cyber laundering regulation and enforcement at the international level. It provides strong legal recommendations for fostering the construction of more efficient means of implementation.

This page intentionally left blank

https://doi.org/10.1142/9781800612839_fmatter

About the Editor

Dr. Nathalie Rébé is a Financial Crime and AML Consultant in Luxembourg. Dr. Rébé holds a Doctorate in Business Administration (DBA) from Paris School of Business and a Doctorate in Juridical Science (JSD) on Financial Crimes from Thomas Jefferson School of Law (USA). She has participated in various international conferences as an academic author and has taught both International Criminal Law and Business Administration university-level courses. With a Postgraduate Diploma in Cyber Law from the University of Montpellier, Dr. Rébé's research and publications have been focused on new technologies, security, privacy, and regulatory matters.

This page intentionally left blank

https://doi.org/10.1142/9781800612839_fmatter

About the Contributors

Dr. Mansoor Ahmed-Rengers is a visiting researcher at the University of Cambridge and the Founder of OpenOrigins Limited. His interests lie at the intersection of decentralized computing, computer security, and security economics. At OpenOrigins, he is working on systems for authenticating content to ward off deepfakes and creating a new trust layer for online content.

Benjamin Aouizerat is Head of Section for the AML/CFT Supervisory Authority — SICCFIN in Monaco. He holds a Graduate Degree in Private Law (Master 2), a University Diploma (DU) in Cybercrime: Information security and computer forensics, and a Data Protection Officer University Diploma (DU DPO). His main practice has included various experiences in the private sector and 10 years at CCIN (data protection authority in the banking and financial sector) before joining SICCFIN in 2018. http://linkedin.com/in/benjamin-a-2311a88.

Dr. Ioannis Blatsos is an experienced academic researcher in the field with significant operational background as a Senior Investigation Officer at the Financial Crime Unit of the Ministry of Finance in Greece. He holds a Ph.D. in Conflict Management from Athens University of Economics and Business and an M.Sc. (Research) degree from London School of Economics and Political Science. He is a regular speaker at the *International Symposium of Economic Crime*, University of Cambridge. Recently, the Economic Crime and Cooperation Division of the Council

of Europe awarded Dr. Blatsos a framework contract for experts on anti-money laundering.

Hon. Dr. Fausto Martin De Sanctis is a Federal Appeals Judge at the Federal Court of Appeals for the 3rd Region, in São Paulo, Brazil. Previously, he was a São Paulo State Judge (1990–1991), Public Prosecutor of the Municipality of São Paulo, and Public Prosecutor of the State of São Paulo in the area of the Public Defender's Office. He was a professor at São Judas Tadeu University for 12 years. He holds a Ph.D. in Criminal Law from São Paulo University (USP) and a Postgraduate Diploma in Civil Procedure from Brasília University (UnB). He has 39 legal works published in Brazil and abroad, in addition to articles specialized in Civil Procedure.

Eric Fulton is a cybersecurity researcher, consultant, and speaker; privacy activist; and business owner. He has spoken on topics such as cellular hacking at Defcon (USA), mobile network forensics at the Blackhat Briefings (Netherlands); guest lectured on nation state cyberattacks at the Institute of World Politics (USA); on Hacktivism at the Free Connected Minds Conference (Lebanon); on cryptocurrencies for the National Association of Insurance Commissioners (USA); and mobile privacy at European Identity & Cloud Conference (Germany). Eric has an M.Sc. in Information Security and Assurance and has published on multiple cybersecurity topics. He is currently researching DeFi attacks, fiat on-ramps, and private transaction methodologies.

Dr. Tanya Gibbs is an educator and researcher in the UAE with university teaching experience in Finance, Financial Crime, and Business Law. She has special expertise in the areas of Anti-Money Laundering and Counter-Financing of Terrorism. She holds an Undergraduate Degree from Saratov State University; an MBA from the American University of Sharjah; and a Ph.D. from the Institute of Advanced Legal Studies, University of London. Her scholarship is interdisciplinary in the areas of marketing, law, cybercrime, political science, and education.

Prof. Dr. Stavros Katsios is Professor of International Economic Relations and International Economic Crime at Ionian University, Corfu, Greece. He is the Director of the Laboratory for Geocultural Analyses (Geolab) and Holder of the UNESCO Chair on Threats to

Cultural Heritage and Cultural Heritage-related Activities. He co-headed the Greek Experts' Committee during the last FATF Mutual Evaluation Report of Greece.

Dr. Benjamin Musau is a legal practitioner in Nairobi, Kenya, and is the Managing Partner of a leading law firm, B. M. Musau & Co., Advocates LLP (https://www.bmmusau.com/), a member of the worldwide Interlaw network. He is an expert on anti-money laundering and cybersecurity and risks. He has knowledge and experience in e-commerce and the laws relating to hacking, cyber warfare, cyber terrorism, cyber defense, and blockchain technologies. He is also a part-time Lecturer at the University of Nairobi, School of Law in Kenya. B. M. Musau & Co., Advocates LLP provides legal support to global conglomerates, institutions, businesses, and governments to make the right business decisions in a fast-changing world.

Dr. Jennifer Palpacuer is Head of Section for the AML/CFT Supervisory Authority (SICCFIN) in Monaco. She holds a Ph.D. in international law. After eight years of research and lecturing at both business and law schools, she worked as a Compliance Officer before joining Monaco's Supervisory Authority in 2013.

Dr. Tal Pavel is the Head of Cybersecurity Studies in the Information Systems School at the Academic College of Tel Aviv-Yaffo and the Founder and Director of the private-owned Institute for Cyber Policy Studies. Dr. Pavel is an academic lecturer, researcher, and speaker specializing in cyber threats and cyber policy; has served as a keynote speaker at international conferences; and has been interviewed as a cyber expert by major media outlets. Dr. Pavel holds a Ph.D. in Middle Eastern Studies from Bar-Ilan University, Israel. His dissertation was titled "Changes in Governmental Restrictions over the Use of Internet in Syria, Egypt, Saudi Arabia and the United Arab Emirates between the Years 2002–2005."

Prof. Mikhail Reider-Gordon is a faculty member at the International Anti-Corruption Academy (IACA) in Austria. A lawyer, she is also Managing Director of Institutional Ethics & Integrity at Affiliated Monitors, Inc. Prof. Gordon's practice areas of expertise include anti-corruption, anti-money laundering, technology and privacy compliance, and international law. She holds leadership positions with the American

Bar Association, including Operations Officer for the International Law Section. She is the past Co-Chair of the Section's International Anti-Corruption and Anti-Money Laundering Committees; has been Co-Chair of the Working Group on Beneficial Ownership Transparency; is Chair of the greater ABA's Task Force on Gatekeeper Regulation and the Profession; and has served on the Association's Standing Committee on Technology and Information Systems. She is a noted and widely published expert on issues related to AML, corruption, and cybercrime. She currently has a podcast series, *Lies, Spies & Corporate Crime: Wirecard, the Saga*, that explores the Wirecard matter from a transnational corporate crime perspective.

Dr. Georg Thomas is a Cybersecurity and Risk Expert based in Melbourne, Australia. He has knowledge and experience in Hacking, Cyber Warfare, Cyber Terrorism, Cyber Defense, and Blockchain Technologies. He currently lectures on Cyber Warfare and Terrorism and Hacking Countermeasures at Charles Sturt University. Georg holds a number of industry certifications, including CCISO, CDPSE, CEH, CISM, and CISSP, and is on the Australian Computer Society Ethics Committee, and is also a former Board Director of the ISACA New York Metropolitan Chapter.

Dr. Ludovic Tirelli holds an LL.M. in Law, Crime and Security in Information and Communication Technology, a Master's Degree of Advanced Studies in Economic Crime Investigation, and a Ph.D. in Comparative Criminal Law from the University of Lausanne. He teaches Criminal Law, Criminal Procedure, White-Collar Crime, and Computer Crimes at the University of Applied Sciences in Neuchâtel, Switzerland, as well as specific programs for special agents in charge of cybercrime investigations. In addition to his academic activities, Dr. Tirelli is a recognized practicing attorney-at-law in the fields of Criminal Law, Criminal Procedure, and Extradition and the Founding Partner of the Swiss criminal law firm Penalex Avocats.

https://doi.org/10.1142/9781800612839_fmatter

Acknowledgments

I dedicate this work to my esteemed colleagues and dear friends who contributed to this edited volume on cyber laundering international policies and practices. I want to warmly thank the amazing experts, lawyers, and academics who believed in me and in this project and joined the team to build this collection of works. Together, their works represent the landscape of such a complex hot topic that deserves more consideration at the international level.

This page intentionally left blank

https://doi.org/10.1142/9781800612839_fmatter

Contents

https://doi.org/10.1142/9781800612839_fmatter

List of Abbreviations

3DO	Three-Dimensional Object
4AMLD	4th Anti-Money Laundering Directive (EU)
5AMLD	5th Anti-Money Laundering Directive (EU)
6AMLD	6th Anti-Money Laundering Directive (EU)
AASB	Australia Accounting Standards Board
ABA	American Bar Association
ACH	Automated Clearing House
AGRASC	Agence de Gestion et de Recouvrement des Avoirs Saisis et Confisqués (France)
AIF	Alternative Investment Fund
AIFMD	Alternative Investment Fund Managers Directive
AIFMs	Alternative Investment Fund Managers
AK-47	Kalashnikov Assault Rifle (Model 47)
AM	Ante Meridiem
AML	Anti-Money Laundering
AMM	Automated Market Maker
API	Application Programming Interface
ASIC	Application-Specific Integrated Circuit
ATM	Automated Teller Machine
AUD	Australian Dollar
AUSTRAC	Australian Transaction Reports and Analysis Centre
BBC	British Broadcasting Corporation
BCH	Bitcoin Cash
BEC	Business E-mail Compromise
BGA	Betting & Gambling Act

BIS	Bank of International Settlement
BSA	Bank Secrecy Act
BTC	Bitcoin
CAGR	Compound Annual Growth Rate
CBECI	Cambridge Bitcoin Electricity Consumption Index
CCIN	Commission de Contrôle des Informations Nominatives
CCISO	Certified Chief Information Security Officer
CDD	Customer Due Diligence
CDPSE	Certified Data Privacy Solutions Engineer
CEA	Commodity Exchange Act
CEH	Certified Ethical Hacker
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CFTC	Commodity Futures Trading Commission
CISM	Certified Information Security Manager
CISSP	Certified Information Systems Security Professional
CJEU	Court of Justice of the European Union
CL	Cyber Laundering
CLOUD	Clarifying Lawful Overseas Use of Data
CO_2	Carbon Dioxide
CPO	Commodity Pool Operator
CPV	Chip Purchase Voucher
CSD	Central Securities Depositories
CSDR	Central Securities Depositories Regulation
CSF	Cybersecurity Framework
CTA	Commodity Trading Advisor
CTF	Counter-Terrorism Financing
CTO	Chief Technology Officer
CTR	Currency Transaction Report
CVC	Convertible Virtual Currency
CVCSP	Convertible VC Service Providers
CVS	Consumer Value Store
CVSE	Convertible Virtual Security Exchange
CWP	Custodian Wallet Provider
DDoS	Distributed Denial-of-Service
DeFi	Decentralized Finance
DEX	Decentralized Exchange
DLT	Distributed Ledger Technology
DNFBPs	Designated Non-Financial Businesses and Professions

DoICS	Directive on Investor-Compensation Schemes
DOJ	Department Of Justice (US)
DOS	Denial Of Service
DPO	Data Protection Officer
EA	Electronic Arts
EBA	European Banking Authority
EC	European Commission
EC	European Council
EEA	European Economic Area
EFRAG	European Financial Reporting Advisory Group
EFTG	European Financial Transparency Gateway
eIDAS	electronic IDentification, Authentication and trust Services
EIOPA	European Insurance and Occupational Pensions Authority
ENCCLA	Brazil's National Strategy for the Fight against Corruption and Money Laundering
ENISA	European Network and Information Security Agency
ERC20	Ethereum Request for Comments 20
ESMA	European Securities and Markets Authority
ETH	Ethereum
EU	European Union
EULA	End-User License Agreements
FATF	Financial Action Task Force
FBI	Federal Bureau of Investigation
FBI	Federal Bureau of Investigation
FCA	Financial Conduct Authority
FGPA	Field-Programmable Gate Array
FIFA	Fédération Internationale de Football Association
FIFO	First-In-First-Out
FinCEN	Financial Crimes Enforcement Network
FIU	Financial Intelligence Unit
fUSDC	farm USD Coin
G20	Group of 20
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
GPML	Global Programme against Money Laundering
GPU	Graphic Processing Unit
GW	Gigawatt

HSBC	Hongkong and Shanghai Banking Corporation
HSM	Hardware Security Module
IACA	International Anti-Corruption Academy
IAS	International Accounting Standard
IASB	International Accounting Standards Board
ICO	Initial Coin Offering
ICT	Information Communications Technology
ID	Identification
IEC	International Electrotechnical Commission
IFRS	International Financial Reporting Standard
IoT	Internet of Things
IP	Internet Protocol
IPO	Initial Public Offering
IRC	Internet Relay Chat channel
IRS	Internal Revenue Service (US)
ISACA	Information Systems Audit and Control Association
ISIL	Islamic State of Iraq and the Levant
ISO	International Organization for Standardization
ISP	Internet Service Provider
KYC	Know Your Customer
LEA	Law Enforcement Agency
LAED	Lawful Access to Encrypted Data
LoK	League of Kingdoms
LoL	League of Legends
LSD	Lysergic Acid Diethylamide
LTC	Litecoin
LTDA	Legal Tender Digital Asset
LTTE	Liberation Tigers of Tamal Eelam
MAR	Market Abuse Regulation
MiFID I	Markets in Financial Instruments
MiFID II	Markets in Financial Instruments II
MiFIR	Markets in Financial Instruments Regulation
MIT	Massachusetts Institute of Technology
ML	Money Laundering
MLA	Mutual Legal Assistance
MMOG	Massively Multiplayer Online Game
MMORPG	Multiplayer Online Role-Playing Game
MOBA	Multiplayer Online Battle Arena
MSBs	Money Services Business

MUDs	Multi-User Dimensions
NATO	North Atlantic Treaty Organization
NCB	Non-Conviction-Based
NFA	National Futures Association
NFT	Non-Fungible Token
NGA	Netherlands Gaming Authority
NHS	UK National Health Service
NIST	National Institute of Standards and Technology
NPCs	Non-Player Characters
NPPS	New Payment Products and Services
NPS	New Psychoactive Substance
NTIC	Nouvelles Technologies de l'Information et de la Communication
OCC	Office of the Comptroller of the Currency
OECD	Organization for Economic Cooperation and Development
OpSec	Operational Security
OS	Operating System
OTC	Over-The-Counter
P2P	Peer-to-Peer
PD	Prospectus Directive
PEPs	Politically Exposed Persons
PII	Personally Identifiable Information
PoW	Proof-of-Work
PWC	PricewaterhouseCoopers, LLP
QR CODE	Quick Response Code
RAT	Remote Access Trojan
RBA	Risk-Based Approach
RMT	Real Money Trading
RQ	Research Questions
SAR	Suspicious Activity Report
SCC	Swiss Criminal Code
SCPC	Swiss Criminal Procedure Code
SEC	Security and Exchange Commission (US)
SFD	Settlement Finality Directive
SICCFIN	Service d'Information et de Contrôle sur les Circuits Financiers
SOE	Sony Online Entertainment
SPTA	Surveillance of Post and Telecommunications

STO	Security Token Offering
SWIFT	Society for Worldwide Interbank Financial Telecommunications
TCP	Transmission Control Protocol
T-CY	Cybercrime Convention Committee
TD	Transparency Directive
TF	Terrorism Financing
TFEU	Treaty on the Functioning of the European Union
TOLA	Telecommunications and Other Legislation Amendment
TOR	The Onion Router
DMCA	Digital Millennium Copyright Act (US)
U.S.C	United States Code
UBO	Ultimate Beneficial Owner
UIGEA	Unlawful Internet Gambling Enforcement Act
UK	United Kingdom
UN	United Nations
UNCAC	United Nations Convention Against Corruption
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNGA	UN General Assembly
UNSCR	United Nations Security Council
UNTOC	United Nations Convention against Transnational Organized Crime
US	United States
USD	US Dollar
USDC	USD Circle
USDT	USD Tether
USP	University of São Paulo
UTC	Universal Time Coordinated
UTXO	Unspent Transaction Output
VA	Virtual Asset
VASP	Virtual Asset Service Provider
VC	Virtual Currency
VCEP	Virtual Currency Exchange Platform
VCPPS	VC Payment Products and Services
VIP	Very Important Person
VPN	Virtual Private Network
WoT	World of Tanks
WoW	World of Warcraft
WWW	World Wide Web

https://doi.org/10.1142/9781800612839_fmatter

List of Tables

This page intentionally left blank

https://doi.org/10.1142/9781800612839_0001

Introduction

Nathalie Rébé

Cyber laundering raises pressing and important concerns about unlawful online financial activities. To explore this topic, this book brings together some of the most important essays in this area, written by leading scholars, lawyers, and judges, thus offering a significant contribution to how we understand and tackle cyber laundering at the international level. This introduction presents the topics of the essays included in this book, as well as some general background.

What are the different ways to launder money using technology? How can cyber laundering be connected to various international crimes? Which existing financial regulations and compliance guidelines govern cyber laundering operations and discuss international compliance and regulatory mechanisms, as well as international cooperation measures to deter cyber laundering? In this collection of essays, it is argued that there are existing jurisdictional and regulatory loopholes, which allow criminals to take advantage of technology to undertake what is illegal in the real world.

The Internet is an ideal place for commerce. It is the perfect platform for money laundering activities to be conducted, as transactions fall outside existing regulatory definitions. Quick, easy to implement, hard to track, and cheap, using the Internet with various techniques, it is possible to undertake all stages of the money laundering process, namely, the placement, layering, or integration phases. Cyber laundering, which can

be simply defined as the practice of money laundering (converting illegally obtained money) carried out online, can take place through multiple methods.

There are three main cyber payment typologies. The first is Internet payment services, such as mobile payments, micro payments, or digital precious metals; the second is store value cards and smart cards; and the third is online banking. However, there are other methods increasingly being used, such as crypto dark pools, over-the-counter purchases, crypto mining, selling artwork, non-fungible tokens (NFTs), crypto ATMs, as well as physical-to-digital-goods translation. While these methods are the best known to the general public, online gambling, gaming, and auctions, along with virtual worlds and assets, are becoming more frequently utilized to launder money. Cryptocurrencies can be created and exchanged via a decentralized network of computers, which means avoiding the involvement of financial institutions or governments in such transactions. Criminals can easily disguise their transactions, send Bitcoins anywhere, convert them into cash, and deposit them in banks.

The advancement of technology is allowing criminals to conduct their unlawful behavior online with greater levels of anonymity, with vast sums of dirty money being transferred via the Internet. The risk factors supporting money laundering activities, in addition to anonymity, include the speed of transactions, their untraceability, the cross-border nature of the Internet, and third-party funding. Cross-border activities can involve several jurisdictions, mutual legal assistance treaties issues, and the ability to transfer unlimited value. Online services, such as banking and electronic payment systems, permit the avoidance of personal "face to face" contact, thus circumventing the "know your client" principle that compliance requires from financial services providers.

Cyber launderers benefit from compliance detection and reporting inefficacy by the technology provider owing to its inability to identify and properly authenticate parties, the lack or inadequacy of audit trails, poor record keeping, and inadequate suspicious transaction reporting. The opening of online bank accounts and services can take place with the use of e-mails that can then be used solely from public terminals, such as an Internet café or in a public library, which means it is nearly impossible to follow an account's access and utilization. The use of high-level encryption can also hinder law enforcement efforts.

To understand cyber laundering, it is important to understand the concept of cybercrime, which pertains to criminal acts that are carried

out in cyberspace by using electronic communications networks and information systems. Cybercrime often involves money passed through the Internet to validate transactions, including the sale of control substances, the sale of illegal items such as firearms, tax evasion, computer crimes, human trafficking, child exploitation, scams, fraud, and extortion. There are various underlying risks associated with the current cyber laundering practices, such as financial data theft, cross-border crimes, and terrorism financing. In this book, we explain how virtual money and assets laundered through the Internet connected to criminality can be seized and recovered.

Nowadays, there are only a few statutes and regulations addressing cyber laundering and E-money at the international level. Hence, there is an increasing necessity to revise regulatory regimes, to ensure adequate and accurate records of the transactions and persons involved, and to track unusual online financial activities that could be associated with ongoing or future crimes. Regular enforcement methods are inefficient, if not obsolete, when dealing with new payment technologies, which can operate across different territories. In some jurisdictions, some new payment methods are not even subject to regulation, while in others, the degree of regulation differs depending on the type of service, with the most fertile ones being exploited by felons. This regulatory gap creates loopholes for criminal abuses, which makes it difficult to investigate and prosecute cyber laundering. While the actual law enforcement framework primarily relies on geographic borders and traditional law enforcement methods, the diminishing of international financial borders makes it essential to enhance cooperation and coordinate efforts among nations to ensure that they follow reliable policies and standards.

Structure of the Book

The following chapters explore various issues relating to cyber laundering. The first shared theme deals with current virtual laundering practices and their relationship with various international criminal activities. The second discusses the various existing cyber laundering countermeasures and international response. Insights are provided on the legal and enforcement challenges we face with technology-enabled financial crimes. The chapters are grouped and introduced according to these two themes, before explanations are provided about their selection for inclusion in this book.

Part I: Virtual laundering practices

In this part, we detail current cyber laundering practices. We discuss how cyber laundering works and can be combatted and explain the many ways in which cryptocurrency and virtual assets can turn into cash (Chapters 1 and 2). We particularly place emphasis on innovative online crimes, such as the use of artificial intelligence and money laundering through online casinos (Chapter 3), and online games (Chapter 4).

The underlying risks associated with cyber laundering include financial data theft, cross-border crimes, and the financing of criminal activities. We thus not only explain how blockchain-enabled crime, malicious financial activities in the dark web (Chapter 5), cyber terrorism, and organized crime function in relation to cyber laundering (Chapter 6) but also present theoretical and real-life worldwide examples.

Part II: Countermeasures and international response

In this part, we discuss the evolution of international regulations, as well as the inclusion of Virtual Asset Service Providers (VASPs) (Chapters 7 and 9). Worldwide cooperation, countermeasures, and international response efforts currently in place to counter cyber money laundering risks are also examined (Chapter 8). National and international regulatory efforts are often hindered by online asset recovery complexity (Chapter 10), as well as enforcement and jurisdictional issues (Chapter 11). We investigate the obstacles to the accomplishment of cyber laundering regulation and enforcement at the international level. We review the pending regulatory issues concerning cyber laundering and offer strong legal recommendations for fostering the construction of more efficient means of enforcement worldwide.

Conclusion

A final comment should be made about how these essays were selected for publication. We received submissions from all over the world, with the authors being chosen for their expertise on law, crime, money laundering, or cyber matters regarding their selected topic.

The essays can be read in the order provided by me as a single narrative to learn about cyber laundering from A to Z. Alternatively, the

chapters can also be read individually, to suit the reader's interest in particular topics. The target audience is those people wishing to learn more about financial crimes and new technologies along with the current regulatory issues related to cyber laundering.

I hope that you enjoy reading the essays in this book as much as I have. Finally, my most sincere thanks must be given to the authors for their contributions, for sharing their knowledge and expertise in a world where there is too little work being done on issues regarding cyber laundering.

This page intentionally left blank

Part I

Virtual Laundering Practices

This page intentionally left blank

https://doi.org/10.1142/9781800612839_0002

Chapter 1

Turning Cash to Cryptocurrency

Eric Fulton

Introduction

Money laundering is fundamentally a three-stage process comprising placement, layering, and integration. Placement involves introducing cash into the financial system. Layering involves somehow disguising the true origins of the proceeds of crime to mislead law enforcement and regulators. Integration is where the criminal(s) acquires wealth generated from what appears to be a legitimate source. This chapter focuses on placement, specifically converting fiat money or valuable objects into cryptocurrency.

Historically money laundering has been constrained by physical limitations; it is difficult to transmit an illicit volume of cash without it getting stolen or noticed, especially when crossing international borders. A standard pallet piled with cash "typically contains 640,000 bills" (Hellerstein and Ryan, 2011); denominated in USD 20 bills, it amounts to USD 12.8 million, certainly not the easiest cargo to conceal or transport. Cryptocurrency, in contrast, lives in the digital ether, making it hard to trace and easy to move. Money laundering via cryptocurrency is a relatively modern area of financial crime; foundationally, there is a requirement to translate value from the physical word, like diamonds or dollars, into something fungible in the digital ecosystem. This chapter is an analysis of cash-to-crypto methodologies, exploring the number of opportunities a criminal actor could use to bypass AML/KYC/CTF rules with

variable levels of effectiveness. While there are a number of individual methods of bypassing regulations, a diversified strategy using multiple methods would be the most resilient and fault-tolerant process for criminals with large volumes of cash. Thus, it is even more important for automated compliance and fraud prevention to be employed in the fight against criminal actors.

This chapter will be covering the most common methods of converting non-crypto assets into cryptocurrency, including cryptocurrency exchanges, OTC purchases, crypto mining, art and non-fungible tokens (NFTs), cybercrime, crypto ATMs, and trading markets. Of course, the easiest method is having customers or victims pay in cryptocurrency and thus bypassing fiat cash all together. With cryptocurrency entering mainstream usage, it becomes easier to skip traditional banking products (and all the compliance procedures) and work only in digital currency.

A Brief Overview of Cryptocurrency

Cryptocurrency as an ecosystem introduces a number of new terms that one must be familiar with to understand the more detailed machinations of how cryptocurrency works. Below is a brief list of terms and concepts that are necessary to understand for concepts presented later in the chapter:

(1) *Cryptocurrency protocols*: There are a number of protocols used in operating a cryptocurrency. Proof-of-stake, proof-of-work, delegated-proof-of-stake, and proof-of-space-time are all different ways of recording, sharing, and trading cryptocurrency. In some cases, exchanges have created their own blockchain, such as the newly released Binance Smart Chain.
(2) *Payment rail*: A payment rail is a gateway or provider that moves money from a payer to a payee. In cryptocurrency, payment rails are used to on-ramp fiat currencies into the cryptocurrency ecosystem.
(3) *DeFi*: "DeFi is short for 'decentralized finance,' an umbrella term for a variety of financial applications in cryptocurrency or blockchain geared toward disrupting financial intermediaries" (Hertig, 2020). Websites like https://uniswap.org allow users to exchange tokens on the Ethereum block chain without the need for a

centralized exchange. This makes it much more difficult to blacklist wallet addresses or perform taint analysis.

(4) *Taint*: "The percentage of bitcoins, that come from a known theft of bitcoins and have been blacklisted by popular exchange markets" (Moser, 2013).

(5) *Smart contracts*: A "smart contract is simply a program that runs on the Ethereum blockchain. It is a collection of code (its functions) and data (its state) that resides at a specific address on the Ethereum blockchain" (Ethereum.org, 2020).

(6) *Tethers*: Tether coins are typically assets issued on the Ethereum blockchain where there is (supposed to be) a 1-1 mapping of fiat currency to crypto asset. A great example of a tether is USDC, which is described on https://www.circle.com/ as "issued by regulated financial institutions, backed by fully reserved assets, redeemable on a 1:1 basis for US dollars, and governed by Centre, a membership-based consortium that sets technical, policy and financial standards for stablecoins."

(7) *Yield farming*: "Yield farming, also known as yield or liquidity harvesting, involves lending cryptocurrency. In return, you get interest and sometimes fees, but they're less significant than the practice of supplementing interest with handouts of units of a new cryptocurrency. The real payoff comes if that coin appreciates rapidly" (Kharif and Williams, 2021).

(8) *Vaults*: "A vault is essentially an Ethereum smart contract where users can store their cryptocurrency and get tokens that may be later used as collateral. They work like pools of funds that use particular strategies for maximizing returns on the assets therein. They were created to address the problems of yield farming and liquidity mining by implementing a more complicated approach than simply switching between various lending protocols" (*Defi Rating*, 2021).

(9) *Liquidity pools*: "A liquidity pool is a collection of funds locked in a smart contract. Liquidity pools are used to facilitate decentralized trading, lending, and many more functions" (Binance Academy, 2021).

(10) *Curve.fi*: "The easiest way to understand Curve is to see it as an exchange. Its main goal is to let users and other decentralized protocols exchange stablecoins (DAI to USDC for example) through it

with low fees and low slippage. Unlike exchanges out there that match a buyer and a seller, the behaviour of Curve is different, it uses liquidity pools like Uniswap. To achieve this, Curve needs liquidity (tokens) which is rewarded by those who provide it" (Curve Finance, 2021).

(11) *Impermanent loss*: "Simply put, impermanent loss is the difference between holding tokens in an AMM and holding them in your wallet. It occurs when the price of tokens inside an AMM diverge in any direction. The more divergence, the greater the impermanent loss. Why "impermanent"? Because as long as the relative prices of tokens in the AMM return to their original state when you entered the AMM, the loss disappears, and you earn 100% of the trading fees" (Hindman, 2021).

(12) *Slippage*: "Slippage refers to the difference between the expected price of a trade and the price at which the trade is executed. Slippage can occur at any time but is most prevalent during periods of higher volatility when market orders are used. It can also occur when a large order is executed but there isn't enough volume at the chosen price to maintain the current bid/ask spread" (Hayes, 2021).

Cryptocurrency Exchanges

Legitimate exchanges, that is, those attempting to follow laws in the jurisdiction they operate in, are the easiest method for consumers to purchase cryptocurrency. They have approved payment rails via Automated Clearing House (ACH), wire, and credit cards, allowing global citizens to purchase and trade cryptocurrency. These exchanges often require some form of identity verification for AML/KYC/CTF compliance and largely only service the jurisdiction the corporate entity exists in. It is highly unlikely for large-scale money laundering to occur at a regulated exchange as they employ advanced AML techniques and are quick to blacklist crypto wallets associated with crime.

As they deal with traditional currencies, each exchange has their own methodology to implement AML/KYC/CTF rules. It is common for exchanges to have light or non-existent KYC rules for customers trading strictly with cryptocurrency as they do not touch the traditional financial system. For customers looking to use traditional fiat money on the exchanges, they typically have to go through some sort of KYC process

as part of the exchanges AML/CTF policies. The following exchanges are the most popular exchanges that deal with fiat-cryptocurrency markets as well as cryptocurrency trading pairs:

(1) Binance
(2) Coinbase/Coinbase pro
(3) Bittrex
(4) Kraken
(5) Bitfinex
(6) Bitstamp
(7) KuCoin
(8) Huobi Global
(9) Bithumb

AML efforts by legitimate exchanges

Online exchanges often outsource identity verification, AML/KYC, and fraud prevention to third parties. Commonly used providers for cryptocurrency exchanges are as follows: https://www.acuant.com/, https://www.jumio.com/, and https://www.veriff.com/. Each provider uses slightly different methodologies for verification, but generally all providers do the following: collect photographic evidence of a government-issued photo ID (like a passport), device fingerprinting (IP address, cookies, operating system [OS] info, etc.), user video activity, and other signals helpful in combating fraud. All of these systems operate via the internet and do not require person-to-person interaction.

Exchanges also monitor transactions, wallets, and the general cryptocurrency ecosystem to combat fraud. Third parties like https://www.chainalysis.com/ provide a software platform that powers investigation, compliance, and risk management that can be integrated in an exchanges fraud prevention logic. A great example where such providers are helpful is in the identification of wallets used by cybercriminals, which allows the exchange to blacklist transactions associated with the tainted wallet. Similar tools like Unit21.ai monitor traditional financial activity in addition to blockchain transactions to give corporations insight into suspicious activity.

No tool is perfect; as much as traditional and cryptocurrency institutions try to combat bad actors, there will always be weaknesses in the

systems set up to prevent, identify, and combat fraud. Common weaknesses like the use of smurfs to distribute and obfuscate large transactions will always be a threat to financial systems; the same goes for hacked accounts and corrupted insiders. Where legitimate cryptocurrency exchanges exceed their traditional counterparts is the higher rigor required for validating customers, and the explosive growth of tools and services created to automate and enhance the art of compliance and fraud detection.

DeFi

Bitcoin, the original cryptocurrency, was created with the intent of "allowing any two willing parties to transact directly with each other without the need for a trusted third party" (Nakamoto, 2019). DeFi benefits from applications that do not require intermediaries or arbitrators to function. A decentralized exchange (DEX) is an example of a DeFi application that allows individuals to trade cryptocurrency tokens in a peer-to-peer fashion via smart contracts. This style of exchange reduces the costs associated with providing and using these products and allows for a more frictionless financial system.

While there are many great innovations in the DeFi ecosystem, there also exists an opportunity for criminal elements to take advantage of programming mistakes, unwitting users, and weak regulations. Scam contracts, exit scams, and vulnerable smart contacts are all pitfalls new users of DeFi must be on the lookout for. One example of notoriety was a contract exploitation known as the Harvest Finance flashloan attack. Yield Farming websites like https://harvest.finance/ make it easier for those with cryptocurrency holdings to leverage permissionless liquidity protocols and generate income. Harvest Finance experienced a theft of funds wherein an "attacker exploited an arbitrage and impermanent loss that influences the value of individual assets inside the Y pool of curve.fi, which is where the funds of Harvest's vaults were invested" (Harvest Finance, 2020). This attack led to the loss of USD 34 million with the burden of the loss shouldered by the individuals who held USD Circle (USDC) resources in Harvest. The attack and loss should not be read as something specific to DeFi and is simply an example of new risks associated with this new frontier of finance. Anywhere there is money, there are thieves, hackers, and fraudsters.

Crypto dark pools

Dark pools are offered by traditional exchanges as a separate order book not visible to the rest of the market (Copper Team, 2019). Each trader only knows their own orders, allowing traders to anonymously place large buy or sell orders without revealing their interest to other traders. Dark pools valuable as typically large orders, when seen by other traders, will cause the market to move unfavorably, making it more difficult to fill the order at the desired price. This unfavorable price movement may be avoided with a Dark Pool order. Simplified, the advantages of using Dark Pool orders are reduced market impact and better price for large trades. In traditional finance exchanges, "off-exchange trading was usually done between two brokers over the phone, in a legal practice called 'upstairs trading'" (Nasdaq, n.d.).

When used by criminals, dark pools simply take the form of a hidden exchange. While dark pool exchanges may operate similarly to their public counterparts, they differentiate significantly in the AML/KYC/CTF requirements and often don't have any form of compliance requirements. This allows criminals on the dark pool to trade without disclosing where the funds came from.

Over-the-counter purchases

In traditional finance, over-the-counter (OTC) trades are the buying and selling of securities via a broker–dealer network as opposed to the usage of an exchange. These trades are a means for individuals or groups to purchase large quantities of a security from an exchange. Traditional OTC deals are done because the security does not meet exchange standards or is not listed for another reason. For cryptocurrencies, OTC deals are done for a few reasons, the most common being to prevent book slippage. Slippage "refers to all situations in which a market participant receives a different trade execution price than intended" (Hayes, 2021). In the case of many crypto-traders doing large-value trades, if they were to execute a trade on a crypto market, say looking to purchase USD 500 million of Bitcoin (BTC), in the execution of their purchase, they would be driving up their purchase price as they increase their purchase. However, with an OTC deal, they can negotiate a fixed price for the entire deal and not move the markets in the process. OTC deals also allow for greater negotiation on price for the buyer and seller. Depending on market conditions and size

of trade, a discount or premium could be applied to the deal, creating greater value for the involved parties.

When used illegitimately, OTC trades offer attractive conditions for criminals looking to launder cash and cryptocurrency. Individuals and groups looking to do large OTC deals are not always equipped or even concerned with following AML/KYC rules, creating an opportunity for fraudsters to trade large amounts of cryptocurrency in a pseudo-anonymous manner. Chainalysis, a software firm which helps government agencies, cryptocurrency businesses, and financial institutions engage confidently with cryptocurrency, has said in their most recent report, "We believe the growing concentration of deposit addresses receiving illicit cryptocurrency reflects cybercriminals' increasing reliance on a small group of OTC brokers and other nested services specializing in money laundering" (Grauer and Updegrave, 2021). A byproduct of this report suggests that AML/KYC/CTF rules are effective at exchanges as criminals are seeking out specialized services bypassing regulations: "a significant share of money laundering in cryptocurrency isn't flying under the radar at big services who can sift through transactions to spot it, but is being actively facilitated by nested services for whom money laundering is a key part of the business model. Law enforcement could significantly hamper cybercriminals' ability to convert cryptocurrency into cash by identifying and prosecuting the owners of these deposit addresses" (Grauer and Updegrave, 2021).

Crypto mining (*cash-hardware-crypto*)

The cryptocurrency ecosystem is at the technical bleeding edge — diverse and constantly changing. Initially, coins were "mined" via mathematical calculations on CPUs. This then evolved into using more specialized types of hardware — GPUs (graphics cards), FGPAs (a field programmable chip), and ASICs (an application-specific chip) are all used to mine different cryptocurrencies. ASICs are the most specialized as they are chips designed with the sole purpose of mining cryptocurrency. This led to new coins designed to be "ASIC resistant" and requiring GPUs or other hardware to be used. Some coins, like the very popular Ethereum, are moving from proof-of-work to proof-of-stake. Even new coins like Chia use proof-of-space-time, which requires miners to accumulate and operate petabytes of hard drive space to obtain coins.

An indirect methodology of translating stolen money into cryptocurrency is laundering stolen money though the purchase of computer hardware. Stores retailing hardware are not equipped to undertake KYC of their customers and generally do not keep identity records for cash transactions. A criminal could use stolen funds to purchase a large amount of hardware that is then used to mine what appears to be legitimate cryptocurrency and can then be recorded as capital gains.

Mining electronics, electricity, network, and facility overhead are the raw inputs for creating cryptocurrencies. When directly purchasing cryptocurrency, an exchange requires source of funds verification; this verification is not required when directly purchasing the raw inputs of cryptocurrency. Thus, criminals with domestic currencies looking to obtain cryptocurrency can purchase mining materials and then produce clean and liquid cryptocurrencies. At scale, these laundering operations are able to purchase infrastructure like power plants and damns to further lower the overhead cost and further legitimize the funds.

In addition to skipping AML/KYC/CTF rules by mining cryptocurrencies, criminals gain the benefit of obfuscating the original source of funds. One entity can buy and resell hardware to a mining entity, which then purchases from yet another entity that provides electricity and supporting infrastructure. As each entity becomes further removed from the origin of funds, they increase their plausible deniability in their affiliation with the original source of funds. Even more obfuscated, via cryptojacking, hackers can gain access to computer systems with the intent to mine cryptocurrencies using the legitimate infrastructure owners' hardware space and power.

Art and NFTs

There are many venues to launder money, but recently it has been said, "The art market is an ideal playing ground for money laundering" (Mashberg, n.d.). This has not always been the case, but as developed countries work to clamp down on money laundering activities in traditional finance, other venues opened as "money laundering through works of art is a recent phenomenon dating to the close of the twentieth century" (De Sanctis, 2013). For large sums of money, art makes an ideal instrument to move value outside of the regulated banking system. Art makes a great rail for cryptocurrency through translating cash to art, and then art

to cryptocurrency. "It appears to be potentially even easier to commit ML offenses through art than through other commodities as the market has specific methods of trade that distinguish it from other sectors" (Hufnagel and King, 2020). As an industry, "Art is an attractive sector for the practice of money laundering because of the large monetary transactions involved, the general unfamiliarity and confidentiality surrounding the art world, and the unlawful activity endemic to it (theft, robbery and forgery)" (De Sanctis, 2013). Art deals, an already opaque market, now even allow art to be purchased directly via cryptocurrency as a "Banksy sold for USD 12.9 million in an auction that lasted 14 minutes and involved four bidders" (Martin, 2021).

An idea even more derivative, crypto is now becoming art with the advent of NFTs. To describe it better, "NFT is unique which cannot be exchanged like-for-like (equivalently, non-fungible), making it suitable for identifying something or someone in a unique way" (Wang *et al*., 2021). NFTs are then being attached to art, with crypto art seen as "limited-edition digital art, cryptographically registered with a token on a blockchain" (Franceschet *et al*., 2020).

Cybercrime

The easiest way to on-ramp cash to crypto is to have your customers do it for you. Cybercrime actors prefer payment for services in cryptocurrency as they do not have to deal with traditional payment systems, and it helps them avoid detection and tracking via traditional financial institutions and regulations. Cybercrime is a vast area, but at a high level, criminals profit via extortion, fraud, sale of illegal or stolen items and data, and supporting services. A non-exhaustive list of profitable criminal enterprises is as follows:

(1) *Botnet/DDOS*: Users purchase time/bots for cyberattacks.
(2) *SPAM*: Users purchase spam services.
(3) *Exploit toolkits*: These toolkits are often rented and operated by less sophisticated criminals.
(4) *Ransomware*: A business is held ransom in exchange for a payment to an attacker made in cryptocurrency.
(5) *Identity theft*: The sale and purchase of stolen identity data.
(6) *Financial or card payment data*: The sale and purchase of stolen payment card data.

(7) *Cyber-extortion*: A criminal uses messages, photos, or other information to extort an individual into paying a fee in cryptocurrency in exchange for silence.
(8) *Dark markets*: Illegal items like drugs, stolen identities, and more are bought and sold here.
(9) *Caller fraud*: Criminals pretending to be entities like the IRS demand payment in gift cards or cryptocurrency.

Criminal enterprises still run into the issue of legitimizing their funds. For cryptocurrency-native crimes, a useful tool in the criminal ecosystem is the use of mixers.

Mixers

For criminals moving cash to cryptocurrency, it is important to obfuscate the origination of funds, as financial crime investigators will attempt to freeze assets they have identified as proceeds from a crime. The original mixing service provider was Bitcoin Fog, which was used to launder over 1.2 million Bitcoins during its operation (Chohan, 2017). Recently, the operator of Bitcoin Fog was arrested;[1] however, mixing cryptocurrencies will not stop with his arrest. In fact, the art of mixing has improved to where it happens in a fully decentralized manner with no central point for authorities to target. The most prominent example of modern mixing is https://tornado.cash/.

Tornado Cash operates on the Ethereum blockchain using smart contracts and does not have a centralized point of control. This presents new challenges to governments and investigators looking to track and recover funds as there is no individual or group to target, and no server to appropriate or shut down.

Crypto ATM

Crypto ATMs act and operate very similarly to traditional ATMs. ATMs operate under the jurisdiction in which they are physically placed, and in the US, operators must have a money transmitter license (except for those

[1] See https://www.wired.com/story/bitcoin-fog-dark-web-cryptocurrency-arrest/. Accessed 12 August 2021.

based in Montana) to operate, which requires the operator to follow a number of rules and regulations. ATM services in the US must also sign up with the Financial Crimes Enforcement Network (FinCEN) as a money service business and are supposed to keep records of their transactions, follow KYC protocols, and report anything suspicious to the authorities. Crypto ATMs are available from a number of manufactures, with Lamassu and General Bytes manufacturing the most popular ATMs available for sale globally.

While the US has a high KYC barrier for ATM transactions, the rest of the globe does not. It is possible for criminal actors to purchase and operate Crypto ATMs that legitimize funds made from operating the ATM network.

It also gives them the ability to poorly enforce KYC rules, allowing their ATM network to be used in the depositing and withdrawal of illegitimate funds.

Physical/digital goods translation

Trade-based money laundering is not something specific to cryptocurrencies, but money launderers have embraced these markets combined with cryptocurrencies to enable translating cash to cryptocurrency while obfuscating the original source of funds. Physical goods bought with cash can then be traded on these markets for cryptocurrency. The following list identifies goods and markets which could be abused for money laundering:

(1) Premium goods (luxury items, bags, watches, and items that can be returned without receipt)
(2) Item-specific markets (https://stockx.com/)
(3) Gaming currency (V-bucks, Nintendo coins, WoW gold, etc.)
(4) Precious metals
(5) Tobacco products
(6) Real estate
(7) Prepaid cards

Prepaid cards deserve special attention as a method of translating cash to crypto as they have a number of traits valued by criminals. They are easy to transport, can be used for cashback or purchasing of physical goods, can be bought and sold, and can store a relatively high value per card.

Prepaid cards

Prepaid cards are value storage instruments usable either at specific retailers or at any retailer accepting credit cards. The cards tied to a specific retailer are called closed-loop system cards and take the form of merchant-issued gift cards, mass transit cards, long distance phone service cards, gaming credits, or value at a specific online store or in-person shop. Open-loop system cards are generally usable anywhere credit cards are accepted and take the form of Green Dot cards, or Visa/Mastercard/American Express prepaid cards.

Prepaid cards are often the criminal payment rail of choice for classic and high-tech money laundering due to their abundant availability, bearer value, ease of use, fungibility, and anonymity. Typically, they can be purchased from retail, grocery, and other physical stores with cash and no AML/KYC/CTF checks.

Open-loop cards have a maximum card value of USD 500 and two card purchases per day per person. The cash per card amount is limited by the issuing bank, and the card limit is enforced by the individual retailer. It is possible for a mule to visit a number of retailers/individual cashiers throughout a day, breaking the cards per day limit. In practice, the author was able to purchase USD 1,600 in open-loop prepaid cards, USD 400 per card, from multiple retailers in a single day; thus, the two cards per day limit should not be considered as it cannot be reasonably enforced between retailers.

Closed-loop cards have a variable maximum card value, though typically individual card values are not allowed to exceed an internally specified amount, and especially not to exceed USD 10,000 as per the Bank Secrecy Act (United States Government, 1982). Specifically, a company selling more than USD 10,000 in gift cards paid for in cash by a single individual must file a currency transaction report with the Federal Government's FinCEN (Federal Register, 2011); however, many retailers have their own internal policies to prevent illegal transactions. To give an example of a specific retailer's internal control policies, a Walmart spokesperson said, "At Walmart, you must show identification for gift card purchases of USD 5,000 or more, according to a spokesperson, and store managers have the authority to halt a transaction at any point" (Debter, 2017). Different chains dealing with fraud surrounding prepaid cards have enacted even more restrictive policies like Consumer Value Store (CVS): "CVS also requires identification any time you buy gift cards or prepaid cards of USD 300 or more" (Wilson, 2019).

Scoping stored value cards to one country, the Australian Transaction Reports and Analysis Centre (AUSTRAC) estimates over AUD 5.1 billion was loaded onto SVC's with AUD 835.5 million of that amount being loaded in cash (AUSTRAC, 2017, p. 1).

Card resale

Once the gift cards are purchased, the next step is to translate these cards into untainted fungible instruments that are easier to move cross-border. The efficient choice is to aggregate gift cards into cryptocurrencies which can then be held, transferred, and spent without limit. A number of services allow cryptocurrencies to be bought with gift cards, such as the following:

(1) Raise, Gift Card Granny, and CardCash — Services to buy and sell closed-loop gift cards.
(2) Paxful.com (Paxful, 2021) — "Paxful is a peer-to-peer Bitcoin marketplace connecting buyers with sellers just like eBay for Bitcoin. You need to select your preferred payment method and type in how many bitcoins you need."
(3) CEX.IO (CEX, 2021) — "CEX.IO is an old cryptocurrency exchange service operational since 2013, from London, UK. The list of cryptocurrencies available on the platform includes Bitcoin, Ether, Ripple, XLM, Bitcoin Cash, Dash, Zcash, and Bitcoin Gold. And the good news is that it supports VISA & Mastercard powered cards including prepaid cards."
(4) Coinmama.com (Coinmama, 2021) — "Coinmama is a digital financial service company operating in the cryptosphere ever since 2013 from Israel but is originally a venture of NBV International registered in Slovakia. It allows investors to buy popular coins such as ETH, BCH, ADA, LTC, etc., including BTC. Prepaid cards are also supported by Coinmama for buying BTC and other currencies."
(5) Localbitcoins.com (Localbitcoins, 2021) — "LocalBitcoin is a popular Bitcoin start-up that facilitates over the counter buying/selling of bitcoins for a nominal fee since 2012. The company, based out of Finland, has a network of Bitcoin buyers & sellers around the world. The good thing is, you will find many buyers and seller dealing in BTC via prepaid debit cards from across the globe."

(6) Bitpanda.com (Bitpanda, 2021) — "Bitpanda is a famous crypto exchange in Europe and is based in Vienna, Austria, where it was founded in 2014. It supports multiple payment options while buying Bitcoin, one of them being prepaid cards."
(7) Paybis.com (Paybis, 2021) — "Buy Bitcoin with Credit Card or Debit Card."

A reader may ask why there are sellers of cryptocurrency who are interested in prepaid credit cards, as prepaid credit cards have a high likelihood of risk of money laundering associated with them. The answer is a large amount of cryptocurrency also has taint as it may have been stolen as part of a cybercrime attack. Even though it is likely that a number of transactions involve trading stolen Bitcoin for stolen gift cards, there is value to both buyer and seller in obfuscating the original crime. It allows plausible deniability and moving the jurisdiction of the crime to different localities. To pose a hypothetical scenario regarding jurisdiction, if cryptocurrency is stolen in France, then used to buy a gift card in England which is then used to purchase from retailers' physical location in the EU, which is then shipped to an unsuspecting consumer in Turkey, where would an investigator start and where exactly would the jurisdiction lie for prosecution and asset recovery?

For the seller of a gift card, with cryptocurrency in hand, they are now free to further obfuscate the origination of funds or withdraw via an exchange before law enforcement has a chance to catch up.

Other gift card redemption methods

Some open-loops cards can be redeemed for cash via ATMs. It is likely that if a criminal uses the same open-loop card and ATM on a regular basis, they will trip fraud detection; however, distributing the redemption over a diverse area varying the exact methods each time using smurfs (a low-level money launderer used to break up larger transactions) is likely enough obfuscation to avoid detection. A smurf will take their ATM cards, go to an ATM, and redeem two to four cards at the ATM.

Grocery store cashback programs are another lightly regulated methodology to convert gift cards to cash. Redemption amounts vary by retailer and location but can allow for up to USD 300 in cash back per purchase.

Closed-loop cards can be redeemed for product to be resold on secondary markets like eBay, or on specialty sites like StockX.

Putting it all together, a money mule working an 80-hour day could conservatively visit 16 retail locations in a day, collecting two closed-loop and two open-loop cards at each location. Assuming a USD 400 purchase per closed-loop card and USD 500 per open-loop card, USD 28,800 in gift cards daily and USD 576,000 in gift cards per month could be purchased, assuming a 40-hour work week. Consistency of stores, cards, and purchases would likely arouse suspicion of store managers, therefore the money mule might diversify stores, times, and other variables in order to avoid detection.

Case Studies

There have been a number of recent high-profile hacks resulting in the theft of cryptocurrency — specifically in the DeFi ecosystem, where attackers can steal large quantities of funds held in automated contracts. This section aims to help understand the methods in which cryptocurrency was stolen and how the attackers elected to launder the resulting funds. The first case focuses on Harvest Finance (henceforth referred to as "Harvest") self-described as "an international cooperative of humble farmers pooling resources together in order to earn DeFi yields" (Harvest Finance, 2021). A clearer definition is Harvest Finance allows individuals to deposit cryptocurrency funds into algorithmically traded contracts which lend currencies at an interest, ultimately returning profits to the lender in a way that also reduces fees.

The second attack was against the Poly Network (henceforth referred to as "Poly"). This attack targeted cross-chain contracts to steal USD 610 million (Wagner, 2021), leveraging an issue in the code of the underlying contract. In both the Harvest and Poly attacks, the resulting funds were moved to wallets controlled by the attacking entities, allowing them full control of the captured cryptocurrencies. In the case of Harvest, the attacker elected to launder the funds and, at the time of writing, has not yet been caught. Uniquely, the Poly Network attacker ended up returning all of the stolen funds; it should be noted the attacker made millions of dollars holding onto the funds for a short period before the funds were eventually returned, and caused opportunity loss for the Poly Network and its depositors. Case studies include the crypto wallet addresses used in the

attack so readers may see what happened live on the blockchain. Tools like https://etherscan.io/ can be used to view wallets, contracts, transactions, and other data recorded on the blockchain.

Case study: Harvest Finance

The Harvest Finance attack is novel in the cryptocurrency world as it leveraged a number of new methods to exploit smart contracts — causing an ultimate loss of USD 33.8 million (Coinness, 2021). The contract vulnerability existed due to the nature of the strategies Harvest uses to invest. There was underlying pool exposure to impairment loss, arbitrage, and slippage, and contract safety thresholds not set low enough to revert the transaction algorithmically.

The primary attack was against the USDC and USD Tether (USDT) vault holdings Harvest held in the Y pool on curve.fi; this pool is vulnerable to value manipulation. The attacker manipulated the Y pool asset value and then used the manipulated asset value to deposit funds into Harvest's vaults obtaining vault shares for a beneficial price, and later exit the vault at a regular share price, generating a profit.

The attack was initiated on October 26, 2020, 02:53:31 AM UTC when an anonymous attacker began moving funds from the Harvest Finance USDC and USDT vaults. Addresses are included so readers may know the attacker's Ethereum wallet address: 0xf224ab004461540778a914ea397c589b677e27bb. It deployed contract 0xc6028a9fa486f52efd2b95b949ac630d287ce0af to initiate and carry out the attack. An amount of 10 ETH (Ethereum) was used for the attack sourced through Tornado Cash in transaction 0x4b7b9e387a79289720a0226f695913d1d11dbdc681b7218a432136cc089363c4. The attack itself initiated in transaction 0x35f8d2f572fceaac9288e5d462117850ef2694786992a8c3f6d02612277b0877.

The attacker began by sourcing a large amount of USDT and USDC from Uniswap (a DeFi protocol which exchanges cryptocurrencies) into the attacking contract. The contract converted USDT into USDC via a swap inside Y pool. The swap caused a higher value of USDC inside the Y pool as the other assets incurred impermanent loss. The attacker then deposited USDC into Harvest's USDC vault, receiving the total fUSDC at 0.97126080216 USDC per share. The price of a share before the attack was 0.980007 USDC, thus the attacker decreased the value of the share by approximately 1%. The Harvest investment strategy does account for

slippage of assets with a threshold of 3%, thus the attacker's transaction did not trigger this safety mechanism and in turn the transaction was not reverted.

Next, the attacker exchanged USDC back into USDT via the curve.fi Y pool, thus obtaining the original lower value of USDC inside the Y pool due to reverting of the impermanent loss effect. The attacker withdrew from Harvest's USDC vault, trading all fUSDC shares back for 50,596,877.367825 USDC. The price of a share was 0.98329837664 USDC as the value of USDC inside the Y pool decreased. The USDC was paid entirely by the buffer of the Harvest's USDC vault, not interacting with Y pool at all. The net profit (not accounting for the flash loan fees) was 619408.812299 USDC. The attacker repeated the process several times within the same transaction.

After executing 17 attack transactions aimed at the USDC vault within 4 minutes, the attacker repeated the process in the analogous way for the USDT vault starting with transaction 0x0fc6d2ca064fc841b c9b1c1fad1fbb97bcea5c9a1b2b66ef837f1227e06519a6. They executed 13 transactions targeting the USDT vault within another 3 minutes. At the end of the process at October 26, 2020, 03:01:48 AM UTC, the attacker transferred 13,000,000 USDC and 11,000,000 USDT from the attacking contract to address 0x3811765a53c3188c24d412daec3f60faad5f119b in transaction 0x53fae6f1d6b8a76a666a0bf7f9c724e6006465e544f89f1515 b939d8911e8c58. It took a total of eight minutes for the attacker to steal USD 24 million of value at the time of the attack.

The attacker then took steps to obfuscate and launder the stolen funds using different methods. A portion of funds was sent to Tornado Cash and, via private transaction, moved to an unknown wallet. Another portion of funds was sent to RenVM (https://renproject.io/) which is a project that enables cross-chain transactions converting the funds into BTC. The BTC then sent funds to Wasabi (https://www.wasabiwallet.io/) and to crypto exchanges. It is assumed the funds sent to the crypto exchanges were to compromised accounts or money mules.

Case study: Poly Network

The cross-chain protocol Poly Network is "built to implement interoperability between multiple chains in order to build the next generation internet infrastructure" https://web.archive.org/web/20210912170800/https://poly.network/. In this regard, Poly's greatest value proposition is the

allowance of assets on different chains to be exchanged via smart contract instead of centralized exchange. Like many other projects in the cryptocurrency ecosystem, Poly became a large target for attacks due to the large value it controlled and the relatively new code written to enable the project's goal. New code often means easier exploitation and lack of audits, which in theory would find critical bugs, which is exactly what happened to the Poly contract on August 10, 2021. The hacker discovered a flaw in the Poly contract and was able to exploit it and send funds to a wallet controlled by the attacker.

Poly has a contract called the "EthCrossChainManager." It is a privileged contract which has the ability to trigger messages from other chains. This type of contract is viewed as standard for cross-chain projects; however, the Poly contract has a function named verifyHeaderAndExecuteTx callable by anyone to execute a cross-chain transaction. This function verifies that the block header is correct by checking signatures and then checks if the transaction was included within that block with a Merkle proof. A final action the function performs is called executeCrossChainTx, which makes the call to the target contract. It is in this function that the attacker found vulnerable code.

Poly checks to verify that the target of executeCrossChainTx is a contract, but it fails to prevent users from calling the EthCrossChainData contract. This is important as it keeps track of the list of public keys that authenticate data coming from the other chain. If an attacker can modify that list, they can simply set the public keys to match their own private keys, which is what the Poly hacker did. The attacker realized cross-chain messages could be sent directly to the EthCrossChainData contract, which is valuable as the EthCrossChainManager contract owns the EthCrossChainData, allowing the attacker to trick the EthCrossChainManager into calling the EthCrossChainData contract, thus passing the onlyOwner check.

With the above information, it remains for the attacker to craft the right data to trigger the function that changes the public keys and makes the EthCrossChainManager call the right function. This depends on a nuance in how Solidity (the language Ethereum contracts are written in) picks which function to be called. The first four bytes of transaction input data is called the "signature hash" or "sighash." It is a small piece of information telling a Solidity contract what to do.

The sighash of a function is calculated by taking the first four bytes of the hash of "¡function name¿(¡function input types¿)." For example, the sighash of the ERC20 transfer function is the first four bytes of the hash

of "transfer(address,uint256)." Poly's contract was willing to call *any* contract. However, it would only call the contract function that corresponded to the following sighash: bytes4(keccak256(abi.encodePacked (method,"(bytes,bytes,uint64)"))).

Critically, the "method" in the previous sighash can be modified by any user of the contact. The attacker only had to call the right function and figure out *some* value for the "method" that, when combined with those other values and hashed, had the same leading four bytes as the sighash of our target function. Finding a collision of the first four bytes using the attacker-controlled "method" variable is something that can be trivially brute forced. In doing this, the attacker effectively got the contract to compromise itself and send funds to an attacker-controlled wallet.

Once the attacker exploited the contract and sent funds to their wallet, they attempted to move the assets. "About an hour following Poly Network's announcement of the hack, the perpetrator attempted to move stolen assets through the Ethereum address into Curve.fi, but the transaction was blocked. The hackers continued trying for about 20–30 minutes before an anonymous user sent the hackers a message on the blockchain that USD Tether had been blocked" (Wagner, 2021).

Cryptocurrency thefts, due to the public nature of the blockchain, have the side effect of being public and viewable in real time by those watching the blockchain. The CTO of Tether, Paolo Ardoino, was quick to react and freeze the Tether assets that had been stolen and share this via his Twitter account.[2] The attacker was unaware the stolen Tether had been frozen and attempted to transfer it a few times unsuccessfully, at which time an anonymous individual going by the name hanashiro.eth sent the attacker a chain message seen here https://etherscan.io/tx/0xae2442c5b57 21df8c190fd8f59b53b6dc56a875fb03035ad34276a598ddf7d31 which stated: "DON'T USE YOUR USDT TOKEN. YOU'VE GOT BLACKLISTED."

At the time of writing this case study, the issue is still ongoing as the attacker is having a conversation with Poly regarding the stolen funds, potential employment, and more. It appears the initial stolen funds will be returned (Hirtenstein, 2021), but how the situation fully resolves remains unclear.

[2]https://twitter.com/paoloardoino/status/1425090760609832978?lang=en.

Conclusion

Cryptocurrency has struggled to define its value since its inception; the first Bitcoin users mailed checks to each other in exchange for mined coins. Since then, a number of methodologies to purchase and exchange cryptocurrencies have been developed. Some of these methods are legitimate, others are used to avoid analysis and obscure the ultimate beneficial owner of a transaction. At present, the cryptocurrency ecosystem's value is siphoned from our physical reality, be it fiat currency or goods and services. Through this translation law, enforcement can use existing tools to trace and track placement of value into the cryptocurrency system. Actions such as creating regulations requiring AML/KYC for all crypto ATM operations, requiring a higher level of ID verification when purchasing prepaid cards, and having stringent reporting requirements for prepaid card purchases will curb criminal use of cryptocurrencies by defeating the effectiveness of its anonymity in placement. Greater attention should also be paid to crypto mining operations as money laundering via mining will likely increase as it is incredibly difficult to manage.

Cryptocurrencies will soon store enough value that fiat–crypto translation will not be necessary, thus making transactions crypto-native; this in turn will make it much harder for transaction analysis. New tools, methods of analysis, and regulations will need to be created to curb criminal use of cryptocurrencies in the near future.

References

AUSTRAC (2017). Stored value cards: Money laundering and terrorism financing risk assessment. Research Report.

Binance Academy (2021). What are liquidity pools in defi and how do they work? https://academy.binance.com/en/articles/what-are-liquidity-pools-in-def.i. [Accessed 22 July 2021].

Bitpanda (2021). https://bitpanda.com. [Accessed 24 July 2021].

Cex (2021). https://cex.io. [Accessed 24 July 2021].

Chohan, U. W. (2017). The cryptocurrency tumblers: Risks, legality and oversight.

Coinmama (2021). https://coinmama.com. [Accessed 24 July 2021].

Coinness (2021). https://www.coinness.com/news/805554. [Accessed 22 July 2021].

Copper Team (2019). Dark pools: Hidden exchanges where whales play with big bitcoin. https://copper.co/2019/10/03/dark-pools-hidden-exchanges-where-whales-play-with-big-bitcoin/. [Accessed 22 July 2021].

Curve Finance (2021). Understanding curve. https://resources.curve.fi/base-features/understanding-curve. [Accessed 22 July 2021].

De Sanctis, F. M. (2013). *Money Laundering Through Art: A Criminal Justice Perspective.* Springer.

Debter, L. (2017). The idiot's guide to laundering 9 million. https://www.forbes.com/sites/laurengensler/2017/01/11/gift-cardsmoney-laundering/?sh=257acc171449. [Accessed 22 July 2021].

Defi Rating (2021). https://defirating.finance/en/research-center/what-are-defi-vaults-andhow-do-we-use-them-to-farm-profits/. [Accessed 22 July 2021].

Ethereum.org (2020). Introduction to smart contracts. https://ethereum.org/en/developers/docs/smart-contracts/. [Accessed 22 July 2021].

Federal Register (2011). Bank secrecy act regulations-definitions and other regulations relating to prepaid access. https://www.federalregister.gov/d/2011-19116/p-136. [Accessed 22 July 2021].

Franceschet, M., Colavizza, G., Smith, T., Finucane, B., Ostachowski, M. L., Scalet, S., Perkins, J., Morgan, J. and Hernandez, S. (2020). Crypto art: A de-centralized view, *Leonardo* pp. 1–8.

Grauer, K. and Updegrave, H. (2021). The 2021 crypto crime report. https://go.chainalysis.com/2021-Crypto-Crime-Report.html. [Accessed 22 July 2021].

Harvest Finance (2020). Harvest flashloan economic attack post-mortem. https://medium.com/harvest-finance/harvest-flashloan-economic-attackpost-mortem-3cf900d65217. [Accessed 22 July 2021].

Harvest Finance (2021). Harvest Finance FAQ (2021). https://old.harvest.finance/faq.

Hayes, A. (2021). Slippage definition. https://www.investopedia.com/terms/s/slippage.asp. [Accessed 22 July 2021].

Hellerstein, R. and Ryan, W. A. (2011). Cash dollars abroad. *FRB of New York Staff Report* 1(400).

Hertig, A. (2020). What is defi? https://www.coindesk.com/what-is-defi. [Accessed 22 July 2021].

Hindman, N. (2021). Beginner's guide to (getting rekt by) impermanent loss. https://blog.bancor.network/beginners-guide-to-getting-rekt-byimpermanent-loss-7c9510cb2f22. [Accessed 22 July 2021].

Hirtenstein, A. (2021). https://www.wsj.com/articles/hacker-returns-stolen-cryptocurrency-inheist-reversal-11628882685. [Accessed 22 July 2021].

Hufnagel, S. and King, C. (2020). Anti-money laundering regulation and the art market. *Legal Studies*, 40(1), 131–150.

Kharif, O. and Williams, R. (July 30, 2020). What's yield farming. https://www.washingtonpost.com/business/whats-yield-farming-and-how-do-you-grow-crypto/2020/07/25/b0fc4662-ce5d-11ea-99b0-8426e26d203b_story.html. [Accessed 22 July 2021].

Localbitcoins (2021). https://localbitcoins.com. [Accessed 24 July 2021].

Martin, K. (2021). Sotheby's accepts cryptocurrency as Banksy art sells for 12.9m. https://www.foxbusiness.com/lifestyle/sothebys-accepts-cryptocurrencyas-banksy-art-sells-for-12-9m. [Accessed 22 July 2021].

Mashberg, T. (n.d.). https://www.imf.org/Publications/fandd/issues/2019/09/the-art-of-money-laundering-and-washing-illicit-cash-mashberg. [Accessed 22 July 2021].

Moser, M. (2013). Anonymity of bitcoin transactions. https://www.semanticscholar.org/paper/Anonymity-of-Bitcoin-Transactions-An-Analysis-of-M%C3%B6ser/e1aed9296c3af9139f48d15e043e2e8beab55409.

Nakamoto, S. (2019). Bitcoin: A peer-to-peer electronic cash system, Technical report, Manubot.

Nasdaq (n.d.). Upstairs market Definition. https://www.nasdaq.com/glossary/u/upstairs-market. [Accessed 22 July 2021].

Paxful (2021). https://paxful.com. [Accessed 24 July 2021].

Paybis (2021). https://paybis.com. [Accessed 24 July 2021].

United States Government (1982). Bank Secrecy Act. https://www.govinfo.gov/content/pkg/USCODE-2012-title31/pdf/USCODE-2012-title31-subtitleIV-chap53-subchapII-sec5311.pdf. [Accessed 22 July 2021].

Wagner, C. (August 10, 2021). Hackers steal over $600M; Biggest in DeFi History https://blockworks.co/hackers-steal-over-600m-biggest-in-defi-history/. [Accessed 22 July 2021].

Wang, Q., Li, R., Wang, Q. and Chen, S. (2021). Non-fungible token (NFT): Overview, evaluation, opportunities and challenges. arXiv preprint arXiv: 2105.07447.

Wilson, D. (2019). CVS taking steps to stop gift card scammers. https://abc11.com/gift-card-scam-cvs/5330206/. [Accessed 22 July 2021].

This page intentionally left blank

https://doi.org/10.1142/9781800612839_0003

Chapter 2

Combating Blockchain-Enabled Crime*

Mansoor Ahmed-Rengers

Introduction

Bitcoin attempted to create a virtual currency outside of the control of governments — and indeed, of all institutional actors — using a decentralized peer-to-peer network. This was enabled by the clever adoption of proof-of-work (PoW) in order to prevent sybil attacks as well as to provide a unified view of the network. Lastly, the use of a blockchain ensured a high level of integrity for transactions.

This ethos of decentralization as a good was driven by a desire to escape traditional banking institutions that the author(s) viewed as being corrupt and fragile. However, as Bitcoin came to gain widespread adoption, especially in criminal circles, many began to doubt the effectiveness of such a decentralized network, both in maintaining a stable value and in hindering crime. It increasingly began to be argued that Bitcoin throws the baby out with the bathwater, and that while there are issues with the traditional banking system, it performs critical functions that cannot be disregarded. These functions include recovering stolen funds, tracking the proceeds of crime, and preventing capital flight. Let us take a look at how Bitcoin fares in these regards.

*Parts of this research were previously published as a collection of three papers written in collaboration with Ross Anderson, Ilia Shumailov, and Alessandro Rietmann.

Bitcoin and Crime

The extent of cryptocurrency-enabled crime is hard to quantify due to varying definitions of what constitutes a crime and the pseudonymous identities used on the blockchain. That said, there have been several studies using different heuristics to try and gauge the scale of the problem.

According to a recent study by Chainalysis (a company that sells anti-money laundering services for cryptocurrencies), a vast majority of criminal transactions take place on the Bitcoin blockchain. Therefore, they focus on Bitcoin and report some interesting statistics: "illicit" transactions (according to their definition of illicit) made up only 1.1% of the total transaction volume in 2019. This observation is closely corroborated by another analysis firm, Elliptic, who report that this number was "less than one percent of all transactions" between 2013 and 2016.

Diving further into the numbers, Chainalysis reports that scams make up the largest share of these illicit transactions accounting for USD 4.9 billion in 2019, more than three times that in 2018. In addition, hacks of cryptocurrency exchanges accounted for USD 282.6 million in 2019 and a total of USD 1.8 billion over the last decade. Overall, Chainalysis concludes that criminal activity on the Bitcoin network is on the rise, an observation that is mirrored by BAE Systems and SWIFT (n.d.) as well, who note that cryptocurrencies are likely to be increasingly attractive to criminals.[1]

This use of cryptocurrencies by criminals as well as the investment bubble in late 2017 led the Bank for International Settlements to label Bitcoin "a combination of a bubble, a Ponzi scheme and an environmental disaster." One of the major concerns with Bitcoin is the fact that if one were to fall victim to a scam or had Bitcoins stolen, there is no recourse. The irreversibility of transactions was an explicit design goal for Nakamoto, but it turns out that when their money gets stolen, people want to get it back. Also, while the amount of cryptocurrency-enabled crime is

[1]While these numbers are indeed large, it is worth putting them in context. The FinCEN file leaks of 2020 revealed that traditional banks were involved in laundering "suspicious transactions" worth more than USD 2 trillion. Deutsche Bank alone was responsible for USD 1.3 trillion of that figure, which dwarfs all crime facilitated by all cryptocurrencies by orders of magnitude. The nature of these suspicious transactions is also very grim, as exposed by these leaks: "Terror networks, drug cartels, organized crime rings, and rapacious kleptocrats have all benefited, using the US financial system to wash clean their illicit profits." https://www.buzzfeednews.com/article/jasonleopold/fincenfiles-8-big-takeaways.

relatively low at present, the trend is clearly upward, and performing truly irreversible transactions makes dealing with crime very difficult.

In this chapter, we first discuss how the law might actually regulate Bitcoin and other cryptocurrencies so as to provide the benefits, ranging from low-cost international money transfers and decentralized resilient operation, through to competitive innovation, while mitigating the drawbacks — specifically the use of cryptocurrencies in extortion, money laundering, and other crimes and the difficulty that crime victims experience in getting redress. We show that where the relevant case law is understood, it becomes much easier to track stolen (or otherwise "tainted") Bitcoins than previously thought, and we describe a prototype system for doing so.

Second, we report our findings after talking to real-world victims who got in touch with us after the publication of our first paper on the topic. This led us to revise our initial assumptions about the cryptocurrency ecosystem.

Third, enlightened by the experiences of the victims, we look at laws passed to regulate Bitcoin in several jurisdictions and point out several issues with them. We also point out concerns with more recent technological developments in the cryptocurrency world, such as payment channels and privacy coins, and difficulties with their lawful usage. These concerns have since been borne out by surveys of cryptocurrency-enabled cybercrime. Finally, we present our recommendations for policymakers.

What the Law Says

Nemo dat quod non habet roughly translates to "no one can give what they don't own" and is an established principle of many systems of law. If Alice steals Bob's horse and sells it to Charlie, Charlie does not end up owning it. When Bob sees him riding it, he can simply demand it back. This is natural justice; the horse was not Alice's to sell. However, it does leave a shadow of doubt over ownership in general. How can you buy something without constantly living in fear that a rightful owner will turn up and ask for it back?

In medieval times, there arose a specific exception for a "market overt": if Alice steals Bob's horse and then takes it to the local public market, where she sells it openly between dawn and dusk to Charlie, then Charlie does indeed now own the horse. Bob can still seek damages from Alice, or seek to have her transported to the colonies or even hanged; but

the horse is now Charlie's. This incentivizes people to buy and sell at markets (which the king can regulate and tax), and also encourages crime victims to go to the local market to check whether their property is on sale there, which in turn may deter crime.

Britain abolished the "market overt" exception to the "*nemo dat* rule," as lawyers call it, in 1994 following abuse by thieves selling stolen antiques. However, two exceptions remain that are of possible relevance to some cryptocurrencies: for money and for bills of exchange. You can get good title to stolen money in two main cases:

(1) You got the money in good faith for value. For example, you bought a microwave oven at a high street store and got a £10 note in your change. That note is now yours even if it was stolen in a bank robbery last year.
(2) You got the money from a regulated institution, such as from an ATM. Then even if it was stolen in a robbery last year, that is now the bank's problem, not yours.

The *nemo dat* rule and its exceptions are discussed in the case of Bitcoin by Fox (2018), whose analysis we draw on and extend here. See also his book on the law of money for further details. Now, the US has designated Bitcoin as a commodity, but there is a lot of lobbying pressure to treat some of it, or at least some cryptocurrencies, as money; Japan has gone as far as designating it "virtual money," while other countries treat it as money for some purposes.[2] In the UK, the tax authorities treat it as foreign currency for the purposes of value-added tax but as a commodity for income tax. A survey of cryptocurrency status conducted by Freshfields (2018) stated that there appears to be nowhere that treats Bitcoin simply as money. This observation was corroborated by a study by the Cambridge Centre for Alternative Finance conducted in 2019 in which they compared the regulatory stances of governments across 23 jurisdictions.

In what immediately follows, we will assume that Bitcoin is a commodity. We will explore what the consequences might be if it comes to be treated as money, or as a bill of exchange. For present purposes, all we need to know is that someone who receives money or a bill of exchange

[2]Recently, the government of El Salvador announced its intention to treat Bitcoin as legal currency becoming the first country to do so. The consequences of this decision remain to be seen but it has already faced backlash from organizations such as the World Bank.

in good faith and for value can get good title to it. Unless cryptocurrencies acquire this privileged status, there is no general exception to the *nemo dat* rule. As they have not achieved this status (except, apparently, in El Salvador), a theft victim can pursue and retrieve her stolen cryptocurrency.

The second important insight from the law is Clayton's case. In English law, there is a long-standing legal precedent on tracing stolen funds. It was established in 1816, when a court had to tackle the problem of mixing after a bank went bust and its obligations relating to one customer account depended on what sums had been deposited and withdrawn in what order before the insolvency. Clayton's case sets a simple rule of first-in-first-out (FIFO): withdrawals from an account are deemed to be drawn against the deposits first made to it. The legacy of the British Empire and Commonwealth ensured that this principle has become embedded in the law of many other countries too.

Armed with this legal guidance, we can say that not only is it possible for the victim of Bitcoin theft to take back her coins (irrespective of where they ended up) but also that the right way to trace which of the Bitcoins were the victim's is by using FIFO tracing. Now, we will first see how tracing can be, and has been, done on a purely technical basis and then see how the situation changes when we apply the legal guidance.

Bitcoin Tracing

Every Bitcoin consists of its entire history since it was mined. What a wallet stores as a Bitcoin is just a pointer to the relevant unspent transaction output (UTXO) and the signing key needed to assign the value therein to someone else. However, the value derives from a series of pointers to previous transactions in the blockchain, each of which has inputs and outputs, going all the way back to where the Bitcoin's constitutive components were originally mined. So, it is fairly straightforward to trace a transaction's history, at least in principle. How might it work in practice?

There has been significant work already on tracing transactions and analyzing their patterns in the blockchain. For convenience, Bitcoin operators use multiple wallets and pass money between them using automated scripts; change wallets are used to break up large amounts and give change, while peeling chains are used to pay multiple recipients out of a single wallet, and multisource transactions are used to consolidate small

sums into larger ones.[3] Clustering analysis can link up the different wallet addresses used by a single principal; Meiklejohn *et al*. (2013) identified over half a million addresses used by Mt. Gox, then the second-largest Bitcoin exchange. Commercial blockchain analysis firms do this at scale. Their customers are typically law enforcement agencies and those exchanges that wish to do due diligence on payments to and from third parties.

There is also research by academics trying to understand and map out the ecosystem. Seminal studies by Ron and Shamir (2013) traced a significant number of Silk Road Bitcoins that the FBI had missed, and two papers by Möser, Rainer and Breuker. In 2013, they used test transactions to analyze the operations of Bitcoin Fog, BitLaundry, and other anonymization services; in the second, they present a detailed analysis of how taint tracking might work through multiple transactions. Their focus was on two algorithms for dealing with multisource transactions of which one input was tainted: these were "poison" (whereby the whole output is tainted) and "haircut" (where the output is tainted by the percentage of input value tainted).

Commercial blockchain analysis firms are cagey about their methods — their terms of service typically require customers not to reverse engineer their algorithms. They seem to employ staff to make multiple small payments into and out of both exchanges and the underground merchants using Bitcoin; use clustering analysis to link together the wallets each actor uses; and then track the flows between them — the focus is at the application layer of payer and payee intent rather than at the level of the blockchain. Whatever the details, coin checking appears to be accepted good practice.

Bitcoin mixing

One might wonder that if tracing algorithms such as haircut and poison exist, why do we need another one? The answer lies in how Bitcoin transactions are structured and the use of Bitcoin *mixes*.

First, it is impossible to subdivide a UTXO, so if Bob wants to pay Alice 0.5 Bitcoins but his savings are in the form of a single UTXO worth

[3]If this is unfamiliar, the book by Narayanan *et al*. (2016) describes Bitcoin mechanics in detail.

50 Bitcoins, then he has to make a transaction with two outputs: one to Alice (for 0.5 Bitcoins), and one to a change address owned by himself (for 49.5 Bitcoins). This indivisibility leads us to classify Bitcoin transactions into the following types:

1-to-1 transactions

Transactions where a single UTXO is sent to a single output. These are quite rare although we have seen them used as building blocks in more complex payment schemes (perhaps as a naïve attempt to anonymize transactions).

Many-to-2 transactions

The workhorse of Bitcoin transactions; as discussed, these are a natural consequence of the indivisibility of UTXOs, and most legitimate transactions belong in this category.

1-to-many transaction

These are quite rare since normal payments to multiple entities are executed by most wallets as a chain of many-to-2 transactions. 1-to-many transactions are sometimes used in technically simplistic mixes to split crime proceeds into many wallets in order to make tracing difficult.

Many-to-many transactions

These are like 1-to-many transactions except that they have multiple input UTXOs. They are the second kind of mixing strategy; they shuffle cryptocurrency between different keys, mostly controlled by the same people.

The default transaction type being a many-to-2 transaction rather than a simple account-to-account transfer as in traditional banking complicates things. It means that even if no one was trying to cover their tracks, tracing becomes convoluted. To illustrate, suppose Alice had 29.5 Bitcoins before Bob sent her the 0.5 Bitcoins; now, suppose it turns out that Bob is a cryptocurrency exchange hacker and therefore the 0.5 Bitcoins are tainted. If we used poison, then all of Alice's 30 Bitcoins are also marked as tainted,

whereas if we used haircut, all the 30 Bitcoins would be marked as $\frac{1}{60}$ tainted. In either case, the initial taint from Bob would spread rapidly through the network, putting more and more Bitcoins in a grey area.

Things get further complicated when we bring mixes, and consequently the latter two types of transactions, into the picture. Cryptographers have long worked on remailers or mixes. Mixes were proposed in 1981 by Chaum to enable email and other message traffic to be sent and received anonymously. If Alice wants to send an anonymous email to Bob, she can send it first to Charlie and ask him to forward it to Bob. Chaum (1981) proposed that, to frustrate naïve traffic analysis, Charlie would accumulate a number of encrypted messages and mix them up before relaying them. If Alice does not want Charlie to read her message, she can first encrypt it with Bob's public key. If she does not want to let her ISP (or a police wiretap) know she is communicating with Bob, she can take the message that is already encrypted with Bob's public key, and now encrypt it also with Charlie's public key, so that all the police see is a message to Charlie. If she wants Bob to be able to reply to her, she can include a cryptographic reply coupon. As we think of more and more possible threats, such systems become ever more complex. The most common anonymity system, Tor, sends worldwide web traffic through three nodes between your Tor browser and the server you wish to visit, so that your anonymity is protected against one or two of them being compromised. There is now a very substantial literature on anonymity systems, with several sophisticated attacks on them and complex trade-offs between performance and security.

However, the perspectives of cryptographers and lawyers are sharply divergent. As noted above, even if cryptocurrency becomes money, you have to get coins in good faith in order to acquire good title; this is discussed extensively by Fox (2018). As all Bitcoin transactions ever made are in plain sight on the blockchain, the act of passing a Bitcoin through a laundry should put all its subsequent owners on notice that something may very well be wrong. Coin checking has been discussed since at least 2013; such services exist, and Bitcoin exchanges claim to perform it. If coin checking is now a reasonable expectation, the likely outcome of feeding 1 black coin and 9 white coins into a Bitcoin laundry is not 10 white coins, but 10 black ones. When matters come to court, any laundries that are clearly identifiable as such are likely to have exactly the opposite effect from that asserted by their designers and operators. In short, people designing money laundering mechanisms have been using the wrong metrics of quality from a legal point of view.

TaintChain: Practical FIFO tracing

To see what a system that takes the legal perspective into account would look like, we implemented FIFO tracing and built it into a system we call the *TaintChain*. This starts off from a set of reported thefts or other crimes and propagates the taint backward or forward throughout the entire blockchain. If working forward, it starts from all tainted transaction outputs and marks all the affected Satoshis[4] as tainted until it reaches the end of the blockchain. If working backward, it traces each UTXO of interest backward and if at any point it encounters a taint, it returns taint for the affected Satoshis. We have made the system publicly available.

To test the system, we performed a FIFO taint trace starting from a few well-publicized coin thefts[5] and ran it from the genesis block to 2016. We found that it concentrated the taint more than haircut or poison tainting strategies.

For example, the 2012 theft of 46,653 Bitcoins from Linode now taints 16,855,619 addresses, or just over 93% of the total, if we use the haircut (or poison) algorithm; with FIFO, it is 245,120 or just over 1.35%. More recent hacks spread the taint even less; for example, the 2014 Flexcoin hack (where "the world's first Bitcoin bank" closed after all their coins were stolen) now taints only 15,265 accounts if we use FIFO, but 10,421,112 (or over 57% of all addresses) if we use haircut.

The reasons for this higher concentration with FIFO should be clear from the graphics below. Imagine that the red Bitcoin inputs to the transaction are stolen Satoshis, the green ones are blacklisted as they are from Iran, the blue ones have been marked by an anti-money laundering screening program as the output of a Bitcoin laundry, and the yellow ones are the proceeds of drug sales on an underground forum. The question for someone interested in enforcing the law is as follows: which of the outputs of each transaction is tainted, and to what extent?

In poison, if you have inputs with four different kinds of taint, then all the outputs are tainted with everything. This leads to rapid taint contagion. If we were to use poison tainting for asset recovery, then we would soon end up having to confiscate almost all of the coins in the network.

Haircut is only slightly different. Here, taint is not binary but fractional. So, instead of saying that all the outputs are tainted with the four kinds of taint, we associate a fractional value to the taint. If half of the

[4]A Satoshi is the lowest denomination of Bitcoin possible. 1 Bitcoin = 10^8 Satoshis.

[5]Data from https://bitcointalk.org/index.php?topic=576337.msg6289796#msg6289796.

input was tainted red, then all the outputs are half red-tainted. Taint diffuses quickly through the network as in poison, but the result is rapid taint diffusion and dilution, rather than contagion. The taint diffuses so widely that the effect of aggressive asset recovery might be more akin to a tax on all users.

With the FIFO algorithm, the taint does not go across in percentages, but to individual components (indeed, individual Satoshis) of each output. As the taint does not spread or diffuse, the transaction processes it in a lossless way. This means that we can trace a Bitcoin's heritage backward as well as tracing taint forward, and we can do tracing efficiently once the appropriate index tables have been built.

Understanding the Theft Reporting Ecosystem

While our FIFO tracking system gave us interesting insights, we wanted to have real-world impact and help victims of cybercrime to the greatest extent possible. To that end, we first looked into the practices of commercial cryptocurrency due-diligence companies. We found a set of companies to look at via recommendations from industry insiders (many of whom were attendees at Financial Cryptography 2019) and by looking at which firms were being used by popular exchanges (if any). Then, from this set, we filtered down to those that allowed individuals to purchase due-diligence reports and used our personal funds to get reports on well-known tainted addresses.

Incentives of the taint tracking ecosystem

Existing taint tracking services appear to have two principal types of customers: the first consists of law enforcement and intelligence agencies, who typically focus on serious crimes such as underground drug markets and multimillion-dollar hacks of exchanges.[6] The second consists of exchanges and financial institutions who want to demonstrate that they exercised due diligence when acquiring cryptocurrency assets.

The second set of customers are purchasing due diligence, which is well known to suffer from perverse incentives. Lobbying pressure from

[6]The leading service, Chainalysis, was set up in an attempt to recover Bitcoins stolen from Mt. Gox in the first major heist in 2013.

financial institutions leads to risk management morphing into standardized due diligence procedures that can be applied mechanically — of which the standard requirement that new bank customers show a passport and two utility bills is a good example.

We therefore made a number of test purchases of AML reports on specific UTXOs which we identified as suspect. In one case, a "Standard AML/KYC Risk Report" assessed a tainted coin as "medium risk," noting "illicit activity risk" (but giving two risk levels of 64% and 11% with no explanation), and unquantified "danger detected" for "transactions impeding track of funds" and "transactions with distinctive patterns." Other reported categories for which danger was detected included cybercrime risk, industry risk, and connected parties. Yet this coin contained a significant component that had been publicly reported as stolen, and the report was oblivious to the fact. In a second case, a checking firm returned "scam alert: none" to one of the main Cryptolocker ransomware addresses and also to the main Sheep Marketplace theft laundry address. In a third case, a checking service gave the all-clear to an address being used by cryptomining malware distributors on an underground forum scraped by colleagues at the Cambridge Cybercrime Centre.

When we asked one firm why they stopped publishing negative recommendations and removed old ones from their websites, they said they "wouldn't match risk appetite of every user thus we can only provide risk assessment and leave the decision to the user." In short, the due-diligence market is not just a market for lemons, but one in which many customers show symptoms of information avoidance.

The incentives facing firms who supply blockchain intelligence to law enforcement are better. If hundreds of online test purchases of drugs provide evidence of drug dealers laundering their proceeds through an unregulated exchange such as BTC-e, this may provide probable cause for a warrant. And indeed the sales pitches of such firms (e.g., Bitfury) target major crimes.

However, there are still shortcomings. The leading police and intelligence agencies tend to focus more on big busts, rather than on protecting ordinary consumers. This is already a problem in frauds using normal banking and payment systems; despite most property crimes in developed countries now being frauds rather than burglary or car theft, the resources devoted by most police forces to "cybercrime" are tiny and they push crime victims to complain to their bank when they can, or even blame the victim for the crime. Given the common police view that Bitcoin users

tend to acquire cryptocurrency with a view to buying drugs online, it is even less likely that they will bestir themselves to help ordinary Bitcoin crime victims, and we have come across no sign of such enforcement action. If ordinary people are going to use cryptocurrencies at all, how can they protect themselves?

This is why we decided to make TaintChain public. We hoped to facilitate the emergence of an open crime-tracking community, first, as a resource for innocent Bitcoin users to check out coins they are offered in payment; second, as a resource for small law enforcement agencies who do not have the budget to buy in specialist services; third, as a platform for academics studying cybercrime; and fourth, as a means of mitigating the lemons market in due diligence. After we wrote the first technical paper with some early results, we publicized it with a Computerphile video and waited for some theft reports to roll in with the hopes of getting more on-the-ground data points.

Theft reporting in practice

We did not have to wait for long. We were contacted by several victims of theft as well as by companies interested in refining their tracing systems. Talking to real victims and looking at real theft cases led us to radically amend our view of the cryptocurrency world. With one exception, the victims we talked to were all using hosted wallets. So rather than downloading wallet software and running it on their own machine, they had gone to an online service — typically a firm that was also an exchange — and exchanged their dollars, euros, or pounds for Bitcoin. When they logged on, a balance was displayed to them, and they could spend it by entering a payee and an amount, just like at a conventional bank website.

In one case (one of the thefts from Mt. Gox), the theft was apparently by an insider. Our complainant reported a Bitcoin balance that amounted to thousands of dollars at the time had simply gone to zero, with an attacker presumably having intercepted the password or bypassed the password-checking mechanism. The outgoing transactions for that day include a set of four equal transactions, closely spaced in time, equal to the missing amount. That is the extent of the traceability we can offer by looking at the blockchain. The liquidators of Mt. Gox have shown little interest in such small cases.

Other cases are similar, although it is generally less clear whether the compromise resulted from a customer's credentials being guessed,

or stolen by malware, or whether there was inside collusion. In no case could we find any clear documentation of the actual ownership of the missing cryptocurrency. On inspection, this observation opens up a number of cans of worms starting with the nature of ownership of Bitcoins in the current ecosystem.

How the market really works now

In the traditional self-hosted model, each user would hold a *wallet*. This is a software program that stores and utilizes private keys that correspond to addresses with unspent UTXOs. Thus, a Bitcoin user "bank account" is her wallet which gives her access to all of her Bitcoins in the form of unspent UTXOs.

One would assume that the hosted wallet of an exchange customer behaves in a similar fashion. However, even in early exchanges, a well-known security measure was used which made hosted wallets behave differently: namely, the use of "cold" and "hot" wallets. Exchanges would keep most of their customers' Bitcoins in offline machines (cold wallets) and transfer to and from them periodically to online machines (hot wallets) used for actual trading. This meant that the hot wallets would have enough coins to transact but not so much as to pose a catastrophic theft risk.

If that were the only optimization introduced by the exchanges, then it would matter little for coin tracing. If the Bitcoin I bought from, or deposited at, an exchange was kept faithfully for me and made available for me to spend when I wished, then a stolen coin I received would still be traceable through my hands when I spent it later. This may have been the case at the time of Mt. Gox, but it does not appear to be generally the case now.

Who owns the Bitcoin stock anyway?

There are two basic models for an institution to hold value on behalf of a customer. The first is the gold merchant. If I pay £44,000 for a 1-kg bar of gold and paid the merchant to store it for me in their vault, the merchant would place a sticker on that bar in his vault with my name on it.[7] If the

[7]Nowadays, the bars have QR codes.

merchant went bust, I could turn up at the vault with my paperwork and collect the gold from the administrators; it was my gold after all, and the company was merely keeping it for me.

The second model is the bank. If I had placed my £44,000 at HSBC, then the bank does not stick my name on 2,200 £20 notes; it merely owes me the sum of £44,000. If it goes bust, I have to stand in line with all the other creditors to get my share.

Similarly, there are basically three ways you can buy and hold cryptocurrency:

(1) You buy it from an exchange and get them to transfer it to your own wallet which is resident on your computing device (or dedicated hardware wallets) and that contains your private key(s). This is the equivalent of collecting your gold from the bullion dealer.
(2) You buy it from an exchange and keep it there in a hosted wallet where the exchange holds the private key(s) on your behalf but the cryptocurrency actually resides in that wallet, in the sense that the keys are available to no other customer. Here, the exchange actually has control over your keys and executes transactions on your behalf. This is the equivalent of the gold merchant who keeps identifiable and marked gold bars on behalf of customers. You can buy, hold, and sell gold without physically taking possession of it, and you can even order it to be transferred to the account of a different customer of that merchant, but it is identifiably and legally yours. We will call this **the gold merchant model**.
(3) You buy it from the exchange and keep it in an account where you have a claim against a certain amount of cryptocurrency that the exchange is holding in its own wallet on behalf of all its customers. In other words, your balance is off-blockchain and intermediated by the exchange. The exchange simply runs an account for customers, which is backed by the exchange's assets. The exchange might not actually possess assets that correspond exactly to its liabilities to its customers; it might lend cryptocurrency to other exchanges, trade in futures and options, and so on. The exchange may also offer transaction services whereby they will remit various cryptocurrency amounts, at your mandate, to the internal or external accounts of other parties. In other words, the exchange is operating as a bank. We call this **the bank model**.

In order to understand which model of ownership is being used in popular exchanges, we looked at the accounts filed by the leading UK exchange, Coinbase. It consists of two companies, CB Payments Ltd., which holds customers' fiat money balances and is now regulated under the E-Money Regulations, and Coinbase UK Ltd., which handles digital currency and is not regulated. According to accounts filed at Companies House, the first of these companies shows a net profit of £481,000 in the year to December 2018 (the latest, at the time of writing) and net current assets of £6,935,000. The second company is more substantial, with a net profit of £6,568,000 and net current assets of £8,156,000. Such accounts have been filed for several years and contain no record of the exact amount of cryptocurrencies held by either company.

Of course, the UK Coinbase companies are part of a larger group, so perhaps all the digital currency assets are kept by the US parent. A recent press profile of Coinbase emphasizes its commitment to compliance and notes that it has USD 20 billion in assets under management. Nonetheless, such a small balance sheet would be considered odd in a UK bank with an overseas parent. If the total market cap of Bitcoin is £300 billion, and the UK's share of that is in line with its 5% share of world GDP, and Coinbase has a third of the UK market, then we would expect to see a balance sheet of £5 billion, not £15 million. Alternatively if the UK is 20% of the size of the US market and Coinbase has the same share in both, we would expect to see USD 4 billion. In short, we are out by two orders of magnitude. Looking for a hint, we note that Coinbase claims that all customer funds are kept in its cold wallet, with only 1% of the total being in its hot wallets for trading at any one time, and that this 1% consists of its own reserves.

It is curious that we see no trace of customers' pooled assets on the Coinbase balance sheet, which does not look anything like that of a bank. Perhaps the assets appear on the balance sheet of a different group company, or perhaps Coinbase has transitioned from being like a gold merchant to being like a bank in the months since the last accounts were filed. Certainly, Coinbase goes out of its way to present itself as the good guy in the Wild West of cryptocurrency and we are not imputing any impropriety whatsoever. However, if even the best actors fall short of the standard of transparency normal in legacy banking, this raises further questions, to which we will return.

Off-chain transactions

So, in practice, the transfer of Bitcoin from person to person appears to be more like this: Alice goes to a Bitcoin exchange and pays it (say) £2000. The exchange gives her BTC 0.07 and displays this balance as being available to her to spend. If Alice now orders a payment of BTC 0.05 to Bob, then the exchange looks to see whether Bob is also a customer. If so, then the transfer is just a ledger entry; the balance seen by Alice reduces to BTC 0.02 while Bob's increases by BTC 0.05. This is known in the trade as an "off-blockchain" or "off-chain" transaction. These appear to have become the default over the period 2016–2020.

The idea that off-chain transactions might become the norm was in fact first mooted by Bitcoin pioneer Hal Finney: "Bitcoin itself cannot scale to have every single financial transaction in the world be broadcast to everyone and included in the block chain… Most Bitcoin transactions will occur between banks, to settle net transfers. Bitcoin transactions by private individuals will be as rare as… well, as Bitcoin based purchases are today."

Getting hard data on the scale of off-chain transactions is hard. Demeester (n.d.) reports that Western exchanges do USD 80 million in off-chain transactions per day, while charts by Cryptovoices (2018) show trading volumes per on-chain transaction taking off from early 2017 and showing peaks in the range of 6 to 14 times. There have been various attempts to create off-chain payment mechanisms between exchanges but it appears, talking to industry insiders, that the great bulk of off-chain payments (at least for Bitcoin) is between customers at the same exchange. One of the drivers appears to have been the massive congestion in the blockchain in late 2016, when transactions could be pending for a day before being mined into the blockchain and transaction fees hit USD 50; now many blocks are partly empty and mining fees are near zero. All such figures need to be treated with caution: Ribes (2018) investigated various Bitcoin exchanges via test transactions and concluded that the largest exchange at the time was faking 93% of its trading volume.

In effect, cryptocurrencies have morphed into an unregulated shadow banking system. While this may have initially been driven by congestion, it has a secondary effect of consolidation: network effects appear to be pushing particular communities to consolidate around specific exchanges. Many Bitcoin users in the US and UK use Coinbase, while Chinese speakers are more likely to use Binance, Japanese use bitFlyer, and

South Africans use Luno. It is convenient to use the same exchange as your counterparties: transactions are instant and fees are much lower.

Another recent development that is bound to make blockchain analysis opaquer is the development of off-chain *payment channels*. Payment channels allow Bitcoin users to only commit a very small subset (usually two: the first transaction is to put a "stake" or collateral into the payment channel and the second is to cash out the collateral plus/minus any transfers to/from the channel) of their total transactions to the blockchain. These do not rely on trusted third parties like exchanges but on collateral put in by all parties as an economic incentive for good behavior, with the blockchain only used in case of disputes among the parties. The actual "Alice to Bob" transfers within a payment channel happen completely off-chain, and payment channel systems can contain many entities. We refer interested readers to the systematization-of-knowledge paper by Gudgeon *et al*. (2020) for an introduction to the field.

The benefits of these off-chain mechanisms are clear: they reduce congestion on the network and have lower latency and transaction fees. The concern is that they further exacerbate the opacity of the Bitcoin network. If payment channels become the norm, one can expect to see even fewer transactions appearing on the blockchain at all. This is even worse (from a transparency standpoint) than the off-chain transactions mediated by cryptocurrency exchanges because, in this case, there is no exchange to serve a warrant on when the need for investigation arises. The lack of any such regulated entity also makes it difficult (if not impossible) for researchers to get a grasp on the popularity of payment channels as well as their usage in cybercrime. We will return to this issue of payment channels when we discuss privacy-preserving cryptocurrencies.

The E-Money Directive

The fact that substantial transaction volumes are now handled off-blockchain raises the issue of whether financial regulators in Europe should require exchanges to comply with the E-Money Directive of 2009. According to this, "electronic money" means "electronically stored monetary value as represented by a claim on the electronic money issuer which is issued on receipt of funds for the purpose of making payment transactions; is accepted by a person other than the electronic money issuer; and is not excluded by regulation."

This regulation seeks to ensure, inter alia, that an issuer of prepaid debit cards has and maintains enough assets to back the credit balances on the cards that it currently has on issue. Exactly the same problem arises with Bitcoin exchanges: what is to stop an exchange taking my money and displaying to me a credit of Bitcoin (or other cryptocurrency assets) that it does not actually have? What is to stop an exchange selling USD 200 million worth of Bitcoin but buying only USD 100 million in actual Bitcoin, taking out the other USD 100 million as dividends for its shareholders, and hoping to get away with it for a while? The rate at which exchanges have gone bust should warn regulators that this is a real risk.

The text of the E-Money Directive appears to describe an exchange's transaction processing business well. So, do financial regulators make exchanges comply with this Directive, via the regulations that implement it in each Member State? The answer appears to be no. In the UK, it is up to the Financial Conduct Authority (FCA) to instruct the Payment Services Regulator to apply the E-Money Regulations (2011) to particular payment systems; the Regulator told us in 2017 that as the FCA has not instructed her to regulate cryptocurrencies, she only applies the Regulations to the conventional currency balances kept at UK Bitcoin exchanges. We will return to the FCA's position. Meanwhile, their reluctance to regulate anything other than the fiat money component of a transaction is exploited by the exchanges. Coinbase's terms and conditions, for example, make a clear distinction between "E-money services," which relate to customer sterling balances, are regulated, and are provided by CB Payments Ltd., and "digital money services," which are provided by the separate company Coinbase UK, Ltd. We are warned, "You should be aware that the risk of loss in trading or holding Digital Currencies can be substantial … Digital Currency Services and Additional Services are not currently regulated by the Financial Conduct Authority, the Central Bank of Ireland, or any other regulator in the UK or in Ireland."

The situation in Germany is similar, but with different details. The regulator, BaFin, has held back from imposing E-Money Regulation on virtual currencies (the term used in the EU) with the argument that they do not represent any claims on an issuer; as there is no issuer, it is not E-money within the meaning of the German Payment Services Supervision Act (*Zahlungsdiensteaufsichtsgesetz*). Bitcoins are, however, financial instruments, units of account like foreign exchange with the difference

that they do not refer to a legal tender.[8] BaFin does note that "Those buying and selling VCs commercially in their own name for the account of others carry out principal broking services which are subject to authorisation" and remarks in passing that "In practice, VC undertakings often did not offer detailed explanations as to how they work at all, or did so in a vague manner. In many cases, no general terms and conditions were provided." And there has been enforcement action: BaFin has issued cease-and-desist notices to ban the promotion of the OneCoin trading system in Germany and an unlicensed broker, Crypto.exchange GmbH.

The OneCoin case is particularly interesting because of the cease-and-desist order related to the company's not having an E-money license in respect of euro remittances made within Germany to acquire OneCoins. In that case, players in the system were "merely adjusting balances" to transfer funds. In any case, an institution providing off-blockchain transactions at scale would appear to fall under §1.1.5 of the German Payment Services Supervision Act as they are "enterprises that provide payment services either commercially or on a scale that requires a commercially equipped business operation."

In short, in both the UK and Germany, the law empowers the regulator to require that digital currency operators who settle payments by means of off-blockchain transactions to register under the E-Money Directive, yet they have so far neglected to do so. Perhaps the cryptocurrency scene is simply moving too fast for them or perhaps the scale of the cryptocurrency-enabled crime is not large enough yet. Once they catch up — perhaps being forced to act by some scandal — the tools already exist. The UK E-Money Regulations, for example, provide two years in prison for operating an E-money service without a license.[9]

Once we realized that regulators were failing to apply the applicable law to tackle the risks around off-blockchain transactions, we made a submission to the UK Parliament's Treasury Committee describing these risks and recommending that the E-Money Regulations be applied to exchanges' digital currency services as well as to their customer balances

[8]This could change if some states were to declare a virtual currency to be legal tender, as El Salvador has recently done.

[9]There are a few surveys of the regulatory status of cryptocurrencies in various countries that interested readers would find useful. The latest is from the Cambridge Centre for Alternative Finance, which compares the regulatory attitudes of 23 jurisdictions.

in fiat currency. We amplify that recommendation below, along with others on which our thinking has developed since our submission to the Parliament.

Directive PE CONS 72/17

On May 12, 2018, the European Union published Directive PE CONS 72/17, with the snappy title of *Directive of the European Parliament and the Council amending Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU* (European Union, 2018). This was agreed quietly between the European Parliament and the Council (the Member States) in April 2018, and it somewhat changes the regulatory landscape. Although it is justified as an anti-terrorism measure, it will have implications for consumer protection.

In December 2017, the Commission had signaled that regulation would be extended from exchanges to wallet-hosting services. The new Directive does this but in a way that leaves a significant loophole. The new Directive has, in Article 2(d), a definition of a "custodian wallet provider," which is just about services that hold cryptographic keys. Recall that we described two models of exchange wallet operation: the gold merchant case, where the wallet provided by the exchange to its customer contains merely the cryptographic keys needed to sign transactions with the customer's own cryptocurrency assets, and the bank case, where the customer merely has a claim on the exchange's asset pool. This definition covers the gold merchant case but fails on the bank case.

The Directive says at recital 10 that virtual currencies (as the EU calls cryptocurrencies) should not be confused with electronic money, since although they can be used for payment, they can be used for other things too. This text does not exclude the application of the E-Money Directive to off-blockchain transactions but may be used to confuse matters and argue that exchanges should continue to have a regulated business for fiat E-money balances and an unregulated one for digital currencies.

The Directive clarifies that the definition of electronic money is that given in Directive 2009/110/EC: "electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is

issued on receipt of funds for the purpose of making payment transactions as defined in point 5 of Article 4 of Directive 2007/64/EC, and which is accepted by a natural or legal person other than the electronic money issuer." That seems to cover off-blockchain payments fair and square and, in our mind, on-chain payments too. There is also a definition of "virtual currency" as "a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically."

However most of the substance of the new Directive consists of detailed amendments to the 4th Anti-Money Laundering Directive, which can only be understood by painstaking cross-reference to the original. Some of the intentions are clear enough, such that there should be centralized systems recording the relationship between addresses and identified holders, which can be queried automatically by investigators on the trail of money laundering or terrorist financing (recital 21). Of real importance may be Section 6: "Member States shall prohibit their credit institutions and financial institutions from keeping anonymous accounts, anonymous passbooks or anonymous safe-deposit boxes." The Directive also requires better public disclosure of the ultimate owners or beneficiaries of companies and trusts.

The lawgiver has, in this case, been contemplating only the money-laundering aspects of Bitcoin exchanges and not the fact that one can open an exchange and sell more Bitcoin than they have. In addition to this consumer-protection risk, there may also be a prudential risk: as some Member States (notably Malta but also Estonia and the UK) try to market themselves as natural homes for cryptocurrency innovation, there will be a temptation to race to the bottom at the cost of decreased transparency.

Positions of UK stakeholders

The UK Parliament's Treasury Select Committee called an inquiry into digital currencies to which many interested parties made submissions in April 2018. Following oral hearings and written submissions, the formal report was published in September 2018. The submissions make for interesting reading.

We already noted that although off-chain transactions appear to fall squarely under the EU E-Money Directive and the UK E-Money Regulations, the Payment Services Regulator cannot apply them as the FCA has not asked her to. The FCA explains its position in its Treasury submission. It follows the definition in EU Directive PE CONS 72/17 in that it sees wallets as storing keys; there is no recognition or mention of off-chain transactions in the set of operations around cryptocurrencies that may or may not be regulated and, like the European Commission, it sees wallets as simply storing the customer's cryptographic key. It does not use the word "currency," or even the EU term "virtual currency," preferring its own term "crypto-assets" — which further helps ignore off-chain transactions. It claims, "Where crypto-assets form part of regulated services, regulated firms can take steps to mitigate the money laundering risks." This may be somewhat optimistic given that Coinbase has separate firms for fiat money and crypto and carefully states in its terms and conditions that only the former is regulated, but the FCA is not too worried: unlike the EU, it sees the money laundering risk as mostly in "non-crypto-asset typologies." This position brings to mind the literature on information avoidance. The FCA appears to be shying away from a problem it should fix but which would complicate its mission. If it wants "crypto-assets" to be treated exactly the same way as shares in Tesco, then it should forbid regulated exchanges from providing any service that allows one customer to transfer them to another directly as a means of payment, but it does not.

The FCA is not the only institution that just does not want to know. The UK Financial Reporting Council, in its submission, discusses the difficulty of valuing crypto-assets. They should be valued at market if they are financial assets, but they do not meet the definition; so they have to be valued at cost as commodities, unless we change the rules to treat them like gold. However, this is not on the agenda of the International Accounting Standards Board.

Policy Recommendations

Thus, regulators are just not managing to keep up, and policy perspectives have changed hugely in a few years. The 2015 survey of Bitcoin economics, technology, and governance by Boehme *et al*. now seems to come from a different century. The number and scale of the scams, together with

the environmental harm caused by mining, have led to an increase in concern among governments with central bankers pushing them in favor of regulation, but so long as this is based on an outdated view of the problem, it is not likely to be optimal. In this section, I discuss the recommendations we made in 2018 which we were invited to present at a number of law and economics venues, and note how the ecosystem has changed in the intervening months.

Regulated exchanges

The main recommendation we made in our 2018 analysis was that governments should regulate exchanges based in the EU, or do business with EU citizens, and which offer off-blockchain payments or consolidate cryptocurrency assets rather than merely holding crypto keys on behalf of customers, in respect of all these cryptocurrency assets under the E-Money Directive. Off-chain transactions, at the very least, fall within the definition of E-money and are vulnerable to exactly the kinds of scams and payment service failures that the E-Money Directive was established to prevent.

If regulators continue to believe that cryptocurrency exchanges fall outside the definition of E-money as per the E-Money Directive, then we will need a similar directive to tackle the same problems. However, that seems like a waste of time and resources. The EU has a workable piece of legislation; it and its Member States just need to enforce it.

Consumer protection

A crime victim who asks an exchange for a refund of stolen Bitcoins that were taken from an account there can expect to be told that as digital currency is unregulated, they are out of luck.

However, this is nothing new. In fiat banking, a customer who complains of phantom withdrawals from her account used to get into an argument with her bank who would stonewall her with something like, "Our systems are secure so you must have been negligent or collusive." Yet the law eventually caught up in most countries. In the US, early court cases paved the way for Regulation E and Regulation Z, which provide much of the consumer protection on which bank customers rely in card transactions. In the EU, the Payment Services Directive requires that the contract

terms governing the use of the payment instrument must be "objective, non-discriminatory and proportionate" (Article 69), and where a transaction is disputed, "it is for the payment service provider to prove that the payment transaction was authenticated, accurately recorded, entered in the accounts and not affected by a technical breakdown or some other deficiency" (Article 71). Crucially, "the use of a payment instrument recorded by the payment service provider, including the payment initiation service provider as appropriate, shall in itself not necessarily be sufficient to prove either that the payment transaction was authorised by the payer or that the payer acted fraudulently or failed with intent or gross negligence to fulfil one or more of the obligations" (Article 72). European law not only agrees that payment records are not constitutive of title to money; it also imposes reasonable constraints on what may be expected of users. Simply saying "you should have chosen a better password" won't do; neither will "the blockchain now says that your money belongs to Fred."

At this point, the provider's terms of service may say "you can't sue us" while consumer protection law holds such contracts to be unfair. Again, the Payment Services Directive comes into play, and there are other laws too around unfair contract and product liability. These can give some clarity if policy degenerates into a tussle over the burden of proof.

So, our **second recommendation** was that the relationship between an exchange and its customer should be covered by the second Payment Services Directive.

Unregistered exchanges

Unregistered and downright criminal exchanges are an issue. Suppose that you were hit by the WannaCry ransomware, had paid a ransom, and wanted to get your money back. According to the US government, WannaCry was the work of North Korean government agents, but this information is not of much help. You note from the Bitfury report that almost all of the Bitcoin collected by WannaCry was laundered through the HitBTC exchange, so you want to serve a court order on them (whether for compensation, or merely to see the passport presented by whoever cashed those coins). You then find that their website does not contain a physical address for service, contrary to the E-Commerce Directive, Article 5.1(b) of which requires "the geographic address at which the service provider is established" to be provided. A simple search

reveals that others, including disappointed customers, have sought this information repeatedly. HitBTC does claim to abide by FATF rules, so where is it registered as a money service business? The Directive requires at 5.1(e) that it publishes "where the activity is subject to an authorisation scheme, the particulars of the relevant supervisory authority" yet there is no sign. It should perhaps surprise no one that HitBTC is on Ribes' (2018) list of exchanges that appear to significantly overstate their trading volume; he uses the word "fraud."

HitBTC is believed by some in the industry to be run by criminals in Russia. If it turns out that HitBTC is in a non-compliant jurisdiction, so it cannot be raided and shut down, then conversations need to turn to sanctions, and whether regulated exchanges should be permitted to transact with such operators at all.

The concern around exchanges based in non-compliant jurisdictions has taken an increased importance in the 18 months since we initially published our recommendations. The recent Chainalysis study of crypto crime suggests that 52.2% of all illicit Bitcoins in 2020 went through just two exchanges: Huobi and Binance, taking the place of HitBTC as the primary crime havens. Binance moved to Malta, which is infamous in cryptocurrency circles for its lack of enforcement, after being banned in China. Huobi seems to have subsidiaries in many jurisdictions, with the Hong Kong office serving as headquarters, although the exact structure of the Huobi group is quite difficult to decipher from their released documents.

The guidance for dealing with such exchanges exists in the aforementioned Directive 2015/849 discussed earlier, which imposes a duty in respect of transactions involving high-risk third countries, which must be presumed to apply to HitBTC and the like. Article 11 requires EU institutions to implement a number of enhanced due-diligence measures on such transactions, including getting more information on the customer, the beneficial owner, the nature of the business relationship, the source of funds, and the reasons for the intended transactions. Moreover, the EU institution doing such a transaction must have it approved by senior management. It is hard to see how a UK exchange could discharge these duties in respect of a transaction to or from HitBTC.

Again, this is nothing new. Cryptocurrencies do not solve the underlying problems that made bank regulation necessary, and we can expect that many of the familiar second-order problems will also reappear in due course.

Our **third recommendation** was that regulators should prohibit the cryptocurrency exchanges they regulate from clearing and settling transactions with unregulated exchanges.

Innovation and the role of central bank cryptocurrency

Debate continues on whether Bitcoin and cryptocurrencies have actually achieved anything other than emitting carbon dioxide and facilitating crime. Stinchcombe (2017) argues that ten years into its development, nobody has found a legal killer app for Bitcoin yet: "Each purported use case … amounts to a set of contortions to add a distributed, encrypted, anonymous ledger where none was needed. What if there isn't actually a use case for the blockchain at all?"

However, the markets still believe otherwise, with Bitcoin's valuation reaching new heights at the time of writing. This surge in valuation can also be seen for Ethereum, a system similar to Bitcoin but with a more expressive scripting language that allows the creation of smart contracts. Whether these can be legally valid contracts has been an issue of some debate.

Once again, we look toward precedent. As Raskin (2016) notes, "innovative technology does not necessitate innovative jurisprudence." In fact, a decent starting point is the existing law on vending machines and on the starter interrupters used to enforce some motor vehicle credit agreements. However, although smart contracts are nothing especially new, regulatory intervention may be needed in egregious cases. Attempts to hide contracts behind machines have failed in the past: an early vending machine was invented by a 17th century book publisher, Richard Carlile, who did not want to be jailed for selling books considered blasphemous. He argued that the purchaser's contract was with the machine, not with him; however, the court did not buy this argument and sent him to jail. The fact that he flaunted his attempts to evade prosecution made the case an easy one for the court. We can expect courts to be similarly unimpressed by contracts that are unfair, unconscionable, or illegal; that are made using the visible proceeds of crime; or that are clearly contrary to public policy.

Both regulators and entrepreneurs should consider common-mode failure risks. People have noted for some time that Bitcoin is not as decentralized as some of its promoters claim. Gervais *et al*. (2014) raised this issue, and Narayanan *et al*. (2016) expanded on it in their book, noting

that a number of players — from the Bitcoin Core developers through the mining cartels to the exchanges — have outsized power in the system. Vorick (2018) gave a fascinating account of an attempt to set up a mining equipment vendor, which revealed that Bitmain has a near monopoly in the mining equipment market; it apparently earned USD 4 billion in 2018.

Indeed, as Narayanan and his coauthors noted, the amazing and noteworthy thing about Bitcoin is that it continues to operate as a (sort-of) global trusted computer despite having various parts of its kill chain controlled by vendors, miners, developers, and exchanges. However, many people expect a denouement sooner or later, and this is one of the reasons that central banks might consider a properly engineered cryptocurrency to be worthwhile.

A quite different approach to Bitcoin is that being pursued by the Enterprise Ethereum Alliance, who have adapted blockchain technology to work in closed groups. These *permissioned blockchains* seem to be gaining traction in enterprise settings and offer tangible benefits to companies (as we shall see in Chapter 3). Nawaz, for example, describes a project at JP Morgan to use enterprise Ethereum to automate the clearing and settlement of financial assets, which would enable the financial institutions who are members of an exchange to manage the asset register collectively. This enables the common-mode failure risks, the risks of transacting with criminal counterparties, and the more traditional solvency and liquidity risks, to be managed transparently.[10]

So, how might central bankers help? Bitcoin promoters have hoped for some years that Bitcoin would become fungible, in the way that coins are — one coin is as good as any other. One way of promoting fungibility was by providing mixes and other money laundering facilities, but, as we have discussed, such facilities do not work very well and are counterproductive as they simply taint the laundered coins as being crime proceeds.

Another approach has been to argue that Bitcoin should be money. If it is, then there are two exceptions to the *nemo dat quod non habet* rule: money and bills of exchange. The simplest way for a cryptocurrency to become money would be for a central bank to issue it. If the Bank of England were to provide cryptocoins saying, as banknotes do, "I promise

[10]The proposal would also make the assets programmable, so that participants could offer futures, options, and other derivatives of arbitrary complexity — which may raise other regulatory issues, but they are not our concern here.

to pay the bearer on demand the sum of £20," then anyone who holds such a coin would be able to rely on it.[11]

A "LegitCoin," for want of a working name, would thus have powerful advantages over competitors[12]: certainty of title, trust in it as a platform, and predictable value. The E-Money Directive would apply immediately and directly, as such a coin would have a defined value.

So, why should a central bank issue cryptocurrency? The best reason, as we see it, is to support innovation by providing a platform for smart contracts whose tokens can be converted into real money at par. Firms promoting businesses based on smart contracts should not have to contend with a wildly fluctuating exchange rate between ether and sterling or with the uncertainty that comes from dealing with coins that may previously have been crime proceeds. Another reason for central banks to consider cryptocurrencies is to enable micro transactions by issuing coins directly to users: the potential for these to disrupt existing economic models is not diminished by having the coins issued by a bank versus having them issued by a mining farm.

One of the pieces of existing infrastructure that central banks might consider for smart contract functionality can be found in the Hyperledger project, a Linux Foundation hosted project that aims to provide a multitude of permissioned blockchain systems depending on the application. Other popular permissioned blockchain frameworks include Corda by R3, MultiChain by Coin Sciences, and Quorum (created by JP Morgan and recently taken over by Consensys).

Our **fourth recommendation** was that central banks consider issuing a cryptocurrency that supports smart contracts, has the legal status of a bill of exchange, and is redeemable at par for fiat money. The use of permissioned blockchains could provide for a convenient mechanism for the dissemination of this cryptocurrency to institutions in a transparent manner.

[11]The general exemption from the *nemo dat* rule is bills of exchange, which include cheques, bills of lading, and indeed banknotes. We have kept the discussion to banknotes for simplicity. However, if we end up with central banks issuing cryptocurrencies that support smart contracts for supply chain management, other bills of exchange will surely be constructed using them.

[12]Such as Facebook's Diem (previously known as Libra).

Nature of ownership

As we have seen, a serious issue with existing exchanges is that it is unclear whether the Bitcoins in the exchange's cold wallet are owned by the customer (as with a gold merchant) or by the exchange (as with a bank). The regulator should force exchanges to make that clear in their terms and conditions. As we noted, exchanges used to act sort of like gold merchants (in the days of Mt. Gox) and appear to act sort of like banks now. The lack of clarity goes back at least to Mt. Gox. According to their 2012 terms and conditions, "it (Mt. Gox) will hold all monetary sums and all Bitcoins deposited by each Member in its Account, in that Member's name as registered in their Account details, and on such Member's behalf." The comment of one of the victims to us was, "It does not state that customers were signing up to a fractionally reserved exchange, and so customers had the understanding that Mt. Gox (albeit in separate cold storage) actually possessed the Bitcoins which customers saw in their balances when they logged in."

Indeed, at present the fungibility of Bitcoin seems to flow from the lack of clarity around ownership; although theft victims can trace stolen assets, they cannot establish whether they actually owned these assets, and so cannot sue to get them back. Clarity will enable the victims to sue either the exchange of which they were a customer when the theft occurred, or the exchange in whose custody the Bitcoins now rest.

A separate policy issue is the nature of ownership of a digital asset. Some assets exist by virtue of registration, patents being an example. With most assets, the *nemo dat* rule makes the situation more complicated. Cryptographers assumed that owning the private key associated with a Bitcoin's address was constitutive of ownership, but the law does not accept this at all. If registration is to constitute ownership (as with patents) there had better be a law to say so; but, as we noted above, the EU Payment Services Directive says no such thing.

Legislation that made cryptography constitutive of ownership would violate a number of established rights and principles, as we discussed. It would complicate legal reasoning about intent, agency, liability, and other issues that have already been discussed in the context of the law on digital signatures. Probably the most that might reasonably be done is to treat the signature as a rebuttable presumption of ownership, following the Electronic Signature Directive. However, that had such adverse effects on liability that qualified electronic signatures found only very limited use.

Here, we merely flag up such issues as needing clarification, perhaps in the course of implementing the central bank study project we recommend above.

In any case, our **fifth recommendation** was that regulators compel exchanges to make clear in their contracts with their customers whether they are custodians of cryptocurrency assets that the customers own, or whether the assets are owned by the exchange with the customers simply having a claim on the asset pool.

It is natural for exchanges to try to avoid stating publicly whether they are trustees, banks, or both, as either choice brings responsibilities. It is time for regulators to force them to choose.

Dark market currencies

A further policy issue is how to deal with cryptocurrencies that are explicitly designed to provide more substantial transaction anonymity or even unlinkability, such as Zcash and Monero, and also to identifiable persons promoting anonymity services on Bitcoin and other public and address-identifiable blockchains. In the case of Zcash, the system works like Bitcoin except that coin-holders can have their coins re-mined, so that they become indistinguishable from other recently mined coins. The analysis in this chapter would suggest that when a tainted coin is treated in this way, all the coins then mined become tainted, and the victim would have a cause for action against any of their holders.

Similar concerns hold for payment channels although there exists an out: one could simply apply the FIFO tracing to the collateral and cash-out transactions used to establish the payment channel. This might result in some unfair repossessions since it may be possible that the victim's proceeds end up with someone who never even directly interacted with the thief. Still, a strict reading of Clayton's case would lead us down that path.

Perhaps the victim, in both the Zcash and payment channel cases, could also sue the operators or promoters of such a system for negligence — in that they knew that some wallets would be stolen and yet designed a system that would make it impossible to get the money back. It is not obvious that the liability stemming from this negligence in fulfilling their duty of care would be extinguished by a legal precedent that declared ordinary, traceable, Bitcoins to be money.

There is also the criminal matter of obstruction of justice, which might be used by prosecutors along with more specific offences relating

to money laundering and (in the case of organizations such as the Izz ad-Din al-Qassam Brigades) terrorist financing. This might perhaps be used against the promoters of systems such as Monero that provide unlinkability by default and that are widely used by mining malware. At the very least, the developers and promoters of such systems must expect to be held to a higher degree of accountability, and it would be beneficial for all if policy could be clarified.

A related policy issue is what the law should consider to constitute behavior "in good faith." We have argued here that Bitcoin mixes are certainly bad faith, and the use of systems like Monero might be held to count as such. This could also hold for payment channels, though arguments could be made that the primary incentive for someone to use a payment channel is not in hiding their transaction history but in the reduction of transaction processing time and cost; without a clear legal precedent, this is a gray area.

However, the new anti-money laundering regulations may settle the matter. As noted above, Article 6 requires that "Member States shall prohibit their credit institutions and financial institutions from keeping anonymous accounts, anonymous passbooks or anonymous safe-deposit boxes." A sensible transposition of the directive would discountenance anonymous instruments such as Zcash and Monero at least, if not payment channels as well.

Our **sixth recommendation** was therefore that regulators should prohibit exchanges from buying and selling cryptocurrencies that are explicitly designed to evade money laundering and terrorist financing controls. Perhaps anonymity should be restricted to cryptocoins issued by central banks, so that controls can be ramped up later if the need arises or be made contingent on transaction amounts. We note that Coinbase will not touch Monero (though bizarrely, it still supports Zcash). Coincheck seems to have seen the danger in supporting these currencies and discontinued its support for Zcash in 2018. So, although the market might abandon these anonymous coins eventually, it might take too much time without regulatory nudges.

Capital requirements

If the only thing that could go wrong with a Bitcoin was that it had been stolen, and all thefts were promptly and dependably reported, then a technically competent exchange can write scripts to fragment all incoming

coins into clean layers and stolen layers. The payer could get value for the clean money, while the victims of theft get their money back and the drug money can go into the local asset-forfeiture pot. We call this *Satoshi sorting*.

Satoshi sorting is not really a practical solution, though, for at least three reasons. First, there are issues other than theft, such as whether drug money or flight capital is to be considered tainted — and some of these questions vary by jurisdiction. Second, crimes are not always discovered and reported immediately; a big drug bust may result in the tainting of coins in transactions from months or even years ago. Third is the complexity of evidence. A victim of Bitcoin theft may take time to establish that fact and a theft report might only get to the TaintChain after years of litigation.

Thus, valid claims against an exchange's cryptocurrency assets can arise for months to years after these assets are received. This risk cannot be managed by a clearing period and it follows that, if exchanges are responsible under the E-Money Directive, or equivalently under securities law, for ensuring that the Bitcoin balances they sell to their customers are backed by cryptocurrency assets that are sufficient in quantity and quality, then they will have to keep a significant level of reserves.

In order to set appropriate standards for reserves, proper accounting standards are also needed. We noted that Coinbase — a leading exchange, which claims to be one of the good guys — has published accounts that do not reflect the assets under its control. In an ideal world, if Coinbase operates like a bank, we would like to see its balance sheet look like a bank's balance sheet, and we would like to have international standards for capitalization and reserves.

Our **seventh recommendation** was therefore that regulators should require regulated exchanges to be adequately capitalized — and develop proper accounting standards to support this.

Mitigating environmental harm

Our final policy issue is serious and controversial: the "environmental disaster," as the Bank for International Settlements describes Bitcoin mining. A detailed analysis by de Vries (2018) put cryptocurrency mining energy use at between 3 and 8 GW, that is, between the energy use by Ireland and by Austria; he noted that the current economics would drive usage toward the latter figure. He was right: the Cambridge Bitcoin

Electricity Consumption Index (CBECI) reported in late 2020 that Bitcoin's annual energy consumption now exceeds that of Austria.

Given the role of CO_2 in anthropogenic climate change and the relevant international agreements including the Paris Agreement, regulators should seek to mitigate the environmental damage done by miners — for example, by moving from PoW systems to Byzantine fault tolerance or to proof of something else. Asking bank regulators to make technology choices might not be ideal, so perhaps the appropriate policy instrument here would be a carbon tax on mined coins.

Various policy mechanisms might be used to get from here to there, including issuing central-bank cryptocurrencies or monetizing existing cryptocurrencies, but only where regulated entities such as exchanges, miners, and wallet-hosting firms pay their carbon taxes. The market could then decide whether to go for moving to proof-of-stake coins, or even (if they are properly capitalized) letting the exchanges run a ledger directly.

Our **eighth recommendation** was therefore that regulators decide how to levy a carbon tax on cryptocurrency mined using PoW methods, and that the very minimum acceptable should be the €33 per ton floor of the Emissions Trading Scheme. From a technological point of view, this would mean transitioning to more efficient consensus algorithms, such as the one I present in Chapter 5.

Conclusion

In this chapter, we analyzed the treatment of tainted Bitcoins from legal, economic, and engineering perspectives, focusing on stolen Bitcoins. Technologists claimed that taint tracking was hard, as they assumed that taint would mix and dilute when coins are joined; yet the relevant case law specifies first-in-first-out tracking, which turns out to be technically easy. Technologists also assumed that Bitcoin mixing made coins derived from innocent and stolen inputs innocuous, whereas the legal effect of attempts to conceal the source of funds is to taint the output.

We first described how to make it practical to trace stolen coins on the blockchain, at least in the theoretical world described in academic research. The same applies to other kinds of tainted coins such as those acquired via other crimes from ransomware to drug trafficking.

We then built a visualization tool to study the spread of taint on the blockchain. This led us to discover some interesting patterns that could serve as useful heuristics for picking out suspicious Bitcoins.

We published these tools and received communication from many victims of Bitcoin theft.

This led us to explore the limitations around the use of taint tracking in practice, at least by individual crime victims, and went on to describe how many Bitcoin exchanges have started working since early 2017, with off-blockchain transactions and the ownership of the underlying Bitcoins often being obscure.

We then took a close look at the measures taken by many governments to tackle the most urgent serious crime threats, including large-scale money laundering and underground drug markets, notably by forcing exchanges to register and perform basic due diligence on their customers. These have culminated in the EU's amending the 4th Anti-Money Laundering Directive to bring wallet-hosting service providers as well, with effect from November 2018. However, this still only tackles the problems of four years ago: we described how regulation has failed to keep up. While regulators have tackled the access and egress points where real money is transferred into digital currency and vice versa, they have failed to notice that the growing volume of off-blockchain transactions has created an unlicensed shadow banking system. This will have to be regulated, just as the real banking system is, and for precisely the same reasons.

Finally, when we did performed the analysis in 2018, we made eight recommendations as a guide for regulatory efforts which I gather here for convenience.

(1) The E-Money Directive should apply to exchanges doing business with EU citizens which offer off-blockchain payments or consolidate cryptocurrency assets rather than merely holding cryptographic keys on behalf of customers, in respect of all these payments and assets.
(2) The relationship between an exchange and its customer should be covered by the Second Payment Services Directive.
(3) Governments should prohibit the cryptocurrency exchanges they regulate from clearing and settling transactions with unregulated exchanges.
(4) Central banks should consider issuing a cryptocurrency using a permissioned system that supports smart contracts and micro transactions, has the legal status of a bill of exchange, and is redeemable at par for fiat money.

(5) Regulators should compel exchanges to make clear in their terms and conditions whether they are custodians of cryptocurrency assets that the customers own, or whether the assets are owned by the exchange with the customers simply having a claim on the asset pool.
(6) Regulators should prohibit exchanges from buying and selling cryptocurrencies that are explicitly designed to evade money laundering and terrorist financing controls. Regulators also need to carefully consider the issue of off-chain payment mechanisms such as payment channels and what restrictions should be placed on their usage.
(7) Regulators should require regulated exchanges to be adequately capitalized and develop proper accounting standards to support this.
(8) Regulators should decide how to levy a carbon tax on cryptocurrency mined using PoW methods; the minimum acceptable should be €33/ton floor of the Emissions Trading Scheme.

We believe that existing laws can be used to tame the cryptocurrency jungle and make it safer both for private users and for innovation. An important step is to enforce the EU's E-Money Directive in respect of digital currency assets held by EU exchanges on their customers' behalf, as well as for balances of euros and other fiat money.

Settling the legal status of digital currencies should be used as an opportunity to move operators from the PoW systems that now emit more CO_2 than Austria, to alternative systems that do not do as much environmental damage, by means of a carbon tax.

An interesting question is whether this would need new legislation, or even a trade treaty (as might be needed, for example, to impose a tax on the embedded carbon content of imported machines). If existing regulations can perhaps be used to implement our other seven recommendations, perhaps they can be used to enforce a carbon tax as well, by making it a condition of cryptocurrencies being traded on regulated exchanges.

At the time of writing, unfortunately, this carbon tax still has not been implemented and regulators have generally continued with their hands-off policy when it comes to PoW emissions. I hope that this changes in the near future since the popularity of cryptocurrencies is on the rise again, most probably due to the pandemic and consequent quantitative easing measures worldwide. Cryptocurrencies seem to be here to stay, we ought to hurry and make them less harmful to the environment.

A bright point to end this chapter on is the apparent utility of a central-bank–issued cryptocurrency as well as of smart contracts to facilitate

interactions between institutions. Here, our optimism seems to have been validated, with many companies now adopting *permissioned blockchains* in a variety of contexts as well as several central banks making strides toward issuing their own cryptocurrencies.

References

Ahmed, M., Shumailov, I. and Anderson, R. (2018). Tendrils of crime: Visualizing the diffusion of stolen bitcoins. *Proceedings of The Fifth International Workshop on Graphical Models for Security*. https://link.springer.com/chapter/10.1007/978-3-030-15465-3_1.

Anderson, R. (2016). GCHQ helps banks dump fraud losses on customers. https://www.lightbluetouchpaper.org/2016/05/27/gchq-helps-banks-dump-fraud-losses-on-customers/. [Accessed 28 October 2020]

—— (2018). Stolen bitcoin tracing. https://www.youtube.com/watch?v=UlLN0QERWBs. [Accessed 28 October 2020]

Anderson, R., Shumailov, I. and Ahmed, M. (2018). Making bitcoin legal. *Proceedings of the Twenty-sixth International Workshop on Security Protocols*. https://link.springer.com/chapter/10.1007/978-3-030-03251-7_29.

Anderson, R., Shumailov, I., Ahmed, M., Bezuidenhoudt, J. *et al*. (April 30, 2018). Failures of trust and regulation in cryptocurrency. http://data.parliament.uk/WrittenEvidence/CommitteeEvidence/EvidenceDocument/Treasury/Digital\%20currencies/written/82188.html. [Accessed 6 December 2020].

Anderson, R., Shumailov, I., Ahmed, M. and Rietmann, A. (2018). Bitcoin redux. *Proceedings of the 17th Annual Workshop on the Economics of Information Security*. https://www.repository.cam.ac.uk/handle/1810/287807.

Araujo, R. (January 2008). Assessing the efficiency of the anti-money laundering regulation: An incentive-based approach. *Journal of Money Laundering Control*, 11: 67–75. doi: 10.1108/ 13685200810844505.

Authority, BaFin — Federal Financial Supervisory (2018). Virtual currencies (VC). https://www.bafin.de/EN/Aufsicht/FinTech/VirtualCurrency/virtual_currency_node_en.html. [Accessed 28 October 2020].

—— (February 5, 2018). Crypto exchange GmbH: BaFin orders cessation of unauthorized principal broking services. https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Verbrauchermitteilung/unerlaubte/2018/meldung_180129_Crypto_exchange_en.html. [Accessed 28 October 2020].

—— (April 18, 2017). Onecoin Ltd, Dubai: Prohibition of involvement in unauthorised money remittance business. https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Verbrauchermitteilung/unerlaubte/2017/vm_170418_Onecoin_Ltd_en.html. [Accessed 28 October 2020].

—— (April 20, 2017). Onecoin Ltd (Dubai), OneLife Network Ltd (Belize) and One Network Services Ltd (Sofia/Bulgaria): BaFin issues cease and desist orders holding the companies to stop own funds trading in "OneCoins" in Germany. https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Verbrauchermitteilung/unerlaubte/2017/vm_170427_Onecoin_Ltd_en.html. [Accessed 28 October 2020].

BAE Systems and SWIFT (n.d.). Follow the money: Understanding the money laundering techniques that support large-scale cyber-heists. https://www.swift.com/sites/default/files/files/swift_bae_report_Follow-The\%20Money.pdf. [Accessed 28 October 2020].

Bambrough, B. (September 2020). Coronavirus is shaping up to be very bad for banks — but not for bitcoin. *Forbes*. https://www.forbes.com/sites/billybambrough/2020/09/19/coronavirus-is-shaping-up-to-be-very-bad-for-banks-but-great-for-bitcoin/?sh=3d437c6f3184. [Accessed 6 December 2020].

BBC News (2021). Bitcoin: El Salvador makes cryptocurrency legal tender. https://www.bbc.com/news/world-latin-america-57398274. [Accessed 20 June 2021].

Bitfury (2018). Use case — Crystal tracking ransomware payments. https://crystalblockchain.com/files/Crystal-Use-Cases-Ransomware.pdf. [Accessed 20 August 2018].

Blandin, A. *et al*. (2019). Global cryptoasset regulatory landscape study. Cambridge Centre for Alternative Finance. https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/cryptoasset-regulation/.

Boehme, R. *et al*. (July 2015). Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives*, 29(2): 213–238.

Cambridge Centre for Alternative Finance (n.d.). Cambridge Bitcoin Electricity Consumption Index. https://cbeci.org/cbeci/comparisons. [Accessed 28 October 2020].

Carstens, A. (February 6, 2018). Money in the digital age: What role for central banks? Bank for International Settlements. https://www.bis.org/speeches/sp180206.htm.

Chainalysis (2020). The 2020 state of crypto crime. https://go.chainalysis.com/2020-Crypto-Crime-Report.html. [Accessed 28 October 2020].

Chaum, D. L. (February 1981). Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of ACM*, 24(2): 84–90.

Citibank, Judd v. (1980). 107 Misc.2d 526.

Coinbase (2020). Coinbase User Agreement. https://www.coinbase.com/legal/user_agreement. [Accessed 6 December 2020].

Companies House (2019a). CB Payments Ltd, Report and Financial Statements. shorturl.at/vHMU4. [Accessed 6 December 2020].

—— (2019b). Coinbase UK Ltd, Report and Financial Statements. shorturl.at/ouEY7. [Accessed 6 December 2020].

Cryptovoices (2018). 24h trading volume per on-chain payment.

Demeester, T. (n.d.). Bitcoin: Digital gold or digital cash? Both. https://medium.com/@tuurdemeester/bitcoin-digital-gold-or-digital-cash-both-382a346e6c79. [Accessed 28 October 2020].

de Vries, A. (May 16, 2018). Bitcoin's growing energy problem. *Joule*, 2(5): 801–805.

Devaynes v Noble (Clayton's Case) (1816). http://www.commonlii.org/uk/cases/EngR/1815/77.pdf.

Directive 1999/13/EC of the European Parliament and the Council (December 13, 1999).

Directive 2000/31/EC of the European Parliament and the Council (June 8, 2000).

Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (September 16, 2009).

Douceur, J. R. (2002). The sybil attack. *Revised Papers from the First International Workshop on Peer-to-Peer Systems. IPTPS '01*. London, UK, UK: Springer-Verlag, pp. 251–260. http://dl.acm.org/citation.cfm?id=646334.687813.

European Union (May 12, 2018). PE CONS 72/17: Directive of the European Parliament and the Council amending Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.

Fanusie, Y. J. and Robinson, T. (2018). Bitcoin laundering: An analysis of illicit flows into digital currency services. Elliptic.

FCA (April 2018). Financial Conduct Authority's Written Submission on Digital Currencies. Online: Accessed on 06-12-2020. http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/treasury-committee/digital-currencies/written/81677.pdf.

Fox, D. (2008). *Property Rights in Money*. Oxford University Press.

—— (2018). Cryptocurrencies in the common law of property. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3232501.

Freshfields (January 2018). Virtual currencies: How regulators treat it.

Fung, B. (May 17, 2018). Move deliberately, fix things: How Coinbase is building a cryptocurrency empire. *Washington Post*. https://www.washingtonpost.com/business/economy/move-deliberately-fix-things-how-coinbase-is-building-a-cryptocurrency-empire/2018/05/17/623d950c-587c-11e8-858f-12becb4d6067_story.html.

George, P. (April 13, 2018). FRC submission to the Treasury Select Committee Digital Currencies.

Gervais, A. *et al*. (2014). Is Bitcoin a decentralized currency? *IEEE Security and Privacy Magazine*, 12(3): 54–60.

Glazer, P. (January 21, 2018). State of global cryptocurrency regulation. https://www.bitcoininsider.org/article/16609/state-global-cryptocurrency-regulation-february-2018. [Accessed 28 October 2020].

Golman, R., Hagmann, D. and Loewenstein, G. (2017). Information avoidance. *Journal of Economic Literature*, 55(1): 96–135.

Gox, Mt. (January 20, 2012). Terms of Use. https://web.archive.org/web/20130906174719/; https://www.mtgox.com/terms_of_service?Locale=en_US.

Gudgeon, L. *et al*. (2020). "SoK: Layer-Two Blockchain Protocols." In: *Financial Cryptography and Data Security*, J. Bonneau and N. Heninger (eds.), Cham: Springer International Publishing, pp. 201–226.

Held, M. (2015). Internet payments: Minimum requirements for security. *BaFin*. https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2015/fa_bj_1505_zahlungen_im_internet_en.html.

Her Majesty the Queen v Wannan (2003). Ottawa, 2003 FCA 423.

JP Morgan (February, 2019). J.P. Morgan creates digital coin for payments. https://www.jpmorgan.com/solutions/cib/news/digital-coin-payments. [Accessed 28 October 2020].

Leopold, J. *et al*. (2020). 8 things you need to know about the dark side of the world's biggest banks, as revealed in the FinCEN files. *BuzzFeed News*. https://www.buzzfeednews.com/article/jasonleopold/fincen-files-8-big-takeaways. [Accessed 28 October 2020].

Malta Today (2019). Why world leader crypto exchange Binance moved to Malta. https://www.maltatoday.com.mt/business/business_news/93170/why_world_leader_crypto_exchange_binance_moved_to_malta. [Accessed 28 October 2020].

Meiklejohn, S. *et al*. (2013). A fistful of bitcoins: Characterising payments among men with no names. *IMC*.

Moeser, M., Rainer B. and Breuker, D. (2013). An inquiry into money laundering tools in the bitcoin ecosystem. *IEEE eCrime*.

—— (2014). "Towards Risk Scoring of Bitcoin Transactions." In: *Financial Cryptography*.

Nakamoto, S. (2009). Bitcoin: A peer-to-peer electronic cash system. http://www.bitcoin.org/bitcoin.pdf. [Accessed 30 October 2020].

Narayanan, A. *et al*. (2016). *Bitcoin and Cryptocurrency Technologies*. Princeton University Press.

Partz, H. (May 20, 2018). Hacked crypto exchange Coincheck confirms removal of four anonymity-focused altcoins. *Cointelegraph*. https://bitlyfool.com/?p=15976. [Accessed 28 October 2020].

Raskin, M. (2016). The law and legality of smart contracts. *Georgetown Law Technology Review*. https://ssrn.com/abstract=2959166.

Ribes, S. (January 15, 2018). Chasing fake volume: A crypto-plague. https://medium.com/@sylvainartplayribes/chasing-fake-volume-a-crypto-plague-ea1a3c1e0b5e. [Accessed 28 October 2020].

Ron, D. and Shamir, A. (Financial Cryptography 2013). "How did Dread Pirate Roberts acquire and protect his bitcoin wealth?" *IACR* preprint 2013/782.

Sale of Goods (Amendment) Act (1994). 29-10-2020. https://www.legislation.gov.uk/ukpga/1994/32/pdfs/ukpga_19940032_en.pdf. [Accessed 29 October 2020].

Sale of Goods Act [RSBC 1996], Section 27 (n.d.). https://www.bclaws.ca/civix/document/id/complete/statreg/96410_01\#section27. [Accessed 29 October 2020].

Singer-Vine, J. *et al*. (2020). We got our hands on thousands of secret documents. Let's break them down. *BuzzFeed News*. https://www.buzzfeednews.com/article/jsvine/fincen-files-explainer-data-money-transactions. [Accessed 28 October 2020].

Stinchcombe, K. (December 22, 2017). Ten years in, nobody has come up with a use for blockchain. https://hackernoon.com/ten-years-in-nobody-has-come-up-with-a-use-case-for-blockchain-ee98c180100. [Accessed 28 October 2020]

TaintChain — GitHub (n.d.). https://github.com/Mansoor-AR. [Accessed 28 October 2020].

The Economist (May 19, 2018). How a few companies are bitcoining it.

UK Parliament Inquiry. http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/treasury-committee/digital-currencies/written/81677.html.

Vorick, D. (May 13, 2018). The state of cryptocurrency mining. https://blog.sia.tech/the-state-of-cryptocurrency-mining-538004a37f9b. [Accessed 28 October 2020].

Yahoo News (2021). World Bank rejects El Salvador request for help in adopting bitcoin. https://news.yahoo.com/world-bank-rejects-el-salvador-174415765.html. [Accessed 20 June 2021].

https://doi.org/10.1142/9781800612839_0004

Chapter 3

Online Casinos: Artificial Intelligence and Money Laundering

Fausto Martin De Sanctis

Introduction

Repeated tolerance of illegal activity in the gambling sector, which is known to be widespread, undermines its credibility to the extent that authorities have been unable to properly enforce the good practices required by both the law and the will of society. Inasmuch as gambling is a subject of universal interest, it must not be exempted from criminological scrutiny because of its great social, educational, and cultural importance. Its relevance constantly reflects on how authorities are defied on a daily basis in their efforts to prevent money laundering and the financing of terrorism and organized crime.

This analysis seeks to provide a basis for a number of important public decisions and to expound on the situational vulnerabilities confronting the circumstances that are not clearly understood by authorities or society-at-large.

The current work can provide a bird's eye view of novel ways in which money is laundered through illegal activities involving gambling. It adds the efforts to curb money laundering and the financing of terrorism, revealing how new techniques used by criminals have been neglected by law enforcement in most countries.

Richet (2013), a research associate at the ESSEC Business School just outside Paris, on surveying the new techniques that criminals are using in a report written for the United Nations Office on Drugs and Crime, reveals "just how creative and opportunistic money launderers have become."

Artificial Intelligence (AI) systems can bring benefits for crime containment in the gaming sector, providing agility and precision. Its applications in the gaming sector is progressing and deserves an adequate analysis. It is relevant to study the impact of the development of a deep learning system and the result of the automation of textual analyzes of online casino activities. That is deemed more than necessary, given the issues that can arise and are usually permeated in the day-to-day transactions. The debate requires reflection on the sector and its neutrality, in view of the need for institutional and normative improvement with wide debate, and not just the mere regulation of AI.

Casinos and Money Laundering

Recognizing the opportunity for huge profits, money gradually infiltrated the world of sport and began to control it. On the one hand, the increase in cash flow has allowed large numbers of people to access the world of gambling through various investments. On the other hand, it has led to fraud, tax evasion, corruption, doping, human trafficking, illegal gambling, match fixing, and money laundering. There is no doubt, therefore, about sport's vulnerability to a number of global threats.

It was not by accident the sports industry took such an unusual turn. Controls enacted pursuant to recommendations by the Financial Action Task Force (FATF), aimed at cracking down on money laundering, made it necessary for criminals to seek out new mechanisms for the laundering of ill-gotten gains. Furthermore, the globalization of financial markets and the rapid development of information technology have gradually steered the underworld economy toward new possibilities for committing financial crimes.

Like so many other businesses, sport and gambling have been used by criminals to launder money and derive illegal income. As in the art world (De Sanctis, 2013), criminals in the sport world are not always motivated by monetary gain. Social prestige, rubbing elbows with celebrities, and the prospect of dealing with authority figures may also attract private investors bent on skirting the law. Its high degree of specialization — inasmuch

as few are really familiar with this market — could also contribute toward attracting illegal activity.

The absence of adequate and well-designed legislation gives power and mobility to organized crime, allowing its continuity and illegal acquisition of unprecedented amounts of wealth. Unreasonable, unjustified, and repeated tolerance by authorities toward criminal activities "practiced in the name of sport" has undermined the credibility of the sport industry. The inertia and inefficiency that plague enforcement in this industry must be dealt with through an assessment of sport regulation. Taking isolated and uncoordinated positions is irrational and runs serious risks. It is now more than ever necessary to use legal tools to bring an end to organized crime.

The high volume of resources crossing boundaries and the lack of transparency in the transactions should demand more incisive control by authorities, whose absence or ineffectiveness provides a unique opportunity for criminals to launder money. Yet there is a true and apparent conflict. Besides football, lotteries, casinos, and gambling houses should also receive special attention of the authorities. The economic impact of the gambling sector is evident because large investments are channeled through it.

There are also societal impacts, including business development and an extensive transmission of cultural values. Yet the growth of this industry has encountered illegal practices, especially corruption, tax evasion, and money laundering. In addition, betting on games has developed a sort of sophistication, with numerous operators working in several countries and using the Internet. This has increased the risk of illegal money laundering. Therefore, countries must regulate the gaming market so as to make it transparent because profiteers use countries that do not regulate or supervise games. It is not easy to control speculators who use online services and work from abroad. This, combined with the lack of transparency in the market, makes it an ever more attractive vehicle for criminals.

One of the essential criminological features inherent in money laundering, as Caeiro (2005), citing Jorge Fernandes Godinho and Luís Goes Pinheiro, reminds us, is its necessary links to organized crime, which in turn add considerable diversity to the types of conduct that its prosecution and enforcement may prevent.

The sport and gambling industries are attractive sectors for the practice of money laundering due to the large monetary transactions involved

and the growing number of people participating in them. Isolated, uncoordinated, and purely economic solutions are not enough to tackle the problem. It is relevant work to uncover any legislative gaps that provide mobility, strength, and continuity to organized crime and enable unprecedented illicit wealth. The complexity of the sport and gambling sectors, along with the emotional involvement of the participants in these sectors, makes it easier to succumb to the authorities in these fields, who deserve particular attention. Left unchecked, the problems caused by these illegal activities can lead to conflicts and instability with serious risk to the involved industries.

It is not possible to enable persistent tolerance of criminal practices. Instead, enforcing property law and best practices will preserve their credibility. Created in December 1989 by the seven richest countries in the world (G-7[1]), FATF (or *Groupe d'Action Financière sur le blanchiment des capitaux* [GAFI][2]), organized under the aegis of the Organization for Economic Cooperation and Development (OECD), has a mandate to examine, develop, and promote policies for the war on money laundering. It initially included 12 European countries, along with the United States, Canada, Australia, and Japan. Other countries joined afterward (including China in 2007) as well as international organizations (including the European Commission and the Gulf Cooperation Council).[3]

[1]United States, Japan, Germany, France, United Kingdom, Italy, and Canada, which has since been joined by Russia (G8).

[2]The FATF is an intergovernmental agency organized to promote measures for the fight against money laundering. Its list of Forty Recommendations, drafted in 1990, was revised in 1996. Another eight recommendations were drawn up in 2003 (on financing of terrorism) and a ninth in 2004 (also about financing of terrorism). On February 16, 2012, all 49 recommendations were revised, improved, and condensed into 40. These recommendations are not binding, but they do exert strong international influence on many countries (including non-members) to avoid losing credibility, because they are recognized by the International Monetary Fund and the World Bank as international standards for combating money laundering and the financing of terrorism. In the 1996 version, they were adopted by 130 countries. In the 2003–2004 version, they were adopted by over 180 countries. It is important to mention that the idea of improving and condensing the Recommendations to avoid distortion and duplication, and to also incorporate the nine Special Recommendations on the financing of terrorism into the basic text (Forty Recommendations), originated in Brazil when it presided over the FATF between 2008 and 2009.

[3]Brazil joined, initially as an observer and later as a full member, at the XI Plenary Meeting, held in September 1999.

The following Recommendations from FATF are relevant provisions contained in the 2012 version:

- Countries should identify, assess, and understand the money laundering and terrorism financing risks for the country and take action to mitigate them *Risk-Based Approach* (*RBA*), Recommendation No. 1).
- Countries should ensure cooperation among policy-makers, the Financial Intelligence Units (FIUs), and law enforcement authorities and coordinate prevention and enforcement policies domestically (Recommendation No. 2). The current text of Recommendation No. 2 (previously contained in Recommendation No. 31) adds, for instance, legitimacy to Brazil's National Strategy for the Fight against Corruption and Money Laundering (ENCCLA).[4]

[4]According to a study conducted by the Brazilian Federal Justice Council's Judiciary Studies Center on the effectiveness of Law No. 9613/1998, through September of 2001, the Brazilian Federal Police had conducted only 260 police investigations, and most (87%) of the federal judges polled in that study answered that there were no active proceedings in their courts relating to money laundering through 12/31/2000, the date on the survey form (FEDERAL JUSTICE COUNCIL, *A critical analysis of the money laundering law*). In 2002 and 2003, with Minister Gilson Dipp of the Appellate Court presiding, and participation from representatives of the Federal Courts, the Office of the Federal Prosecutor, the Federal Police and the Brazilian Federation of Bank Associations (FEBRABAN), the Council drew up substantive recommendations to improve investigation and prosecution of criminal money laundering by engaging the cooperation of various government departments responsible for implementing the law. It was embryonic to the National Strategy for the Fight against Money Laundering and Recovery of Assets (ENCLA), later renamed the National Strategy for the Fight against Corruption and Money Laundering (ENCCLA). The ENCCLA is made up of the primary agencies involved in the matter, which are the Office of the Attorney General, the Council for Financial Activities Control (COAF), the Justice Ministry's Asset Recovery and International Legal Cooperation Council Department (DRCI), the Federal Justice Council (CJF), the Office of the Federal Prosecutor (MPF), the Office of the Comptroller-General (CGU), and the Brazilian Intelligence Agency (ABin), annually setting policy for all actions to be carried out in the execution of Law No. 9613/1998, on account of private and uncoordinated — if not conflicting — agendas having been observed among government agencies responsible for said enforcement. A meeting was held on December 5–7, 2003, in Pirenópolis in the State of Goiás, to develop a joint strategy for the fight against money laundering. To monitor progress toward the goals set forth in the objectives of access to data, asset recovery, institutional coordination, qualification and training, and international efforts and cooperation, an Integrated Management Office for the Prevention of and Fight against Money

- The crime of money laundering should apply to predicate offenses, which may include any of a long list of serious offenses or any offenses punishable by a maximum penalty of more than one year, and criminal liability should apply to all legal persons, irrespective of any civil or administrative liabilities (Recommendation No. 3).
- No criminal convictions should be necessary for asset forfeiture. Furthermore, with reference to the Vienna Convention (1988), the Terrorist Financing Convention (1999), and the Palermo Convention (transnational organized crime, 2000), the burden of proof on confiscated goods should be reversed (Recommendation No. 4).
- Countries should criminalize the financing of terrorism (Recommendation No. 5).
- Countries should implement financial sanction regimes to comply with UN Security Council resolutions regarding terrorism and its financing (Recommendation No. 6).
- Countries should implement financial sanction regimes to comply with UN Security Council resolutions regarding the proliferation of weapons of mass destruction and its financing (Recommendation No. 7).
- Countries should establish policies to supervise and monitor non-profit organizations in order to obtain real-time information on their size, activities, and other important features such as transparency, integrity, and best practices (Recommendation No. 8).
- Financial institution secrecy laws, or professional privilege, should not inhibit the implementation of the FATF Recommendations (Recommendation No. 9).
- Financial institutions should undertake customer due diligence (CDD) and verify the identity of the beneficial owner, and they should be prohibited from keeping anonymous accounts or those bearing fictitious names (Recommendation No. 10).
- Financial institutions should maintain records for at least five years (Recommendation No. 11).

Laundering (GGI-LD) was created in compliance with Target 01 of ENCLA/2004. This Office is composed of the primary government agencies, as well as the Judicial Branch and Attorney General's Office, conducting both workshops and plenary meetings on various occasions. Every year, they define new Actions (formerly Targets), in hopes that the conclusions arrived at during their work sessions will be transformed into substantive outcomes.

- Financial institutions should closely monitor politically exposed persons (PEPs),[5] i.e., persons who have greater facility to launder money, such as politicians in high posts and their relatives (Recommendation No. 12).

Other provisions worth mentioning include the following:

- Financial institutions should monitor wire transfers, ensuring that detailed information is obtained about the sender and the beneficiary, and prohibit transactions by certain people pursuant to UN Security Council resolutions, such as Resolution 1267 of 1999 and Resolution 1373 of 2001, for the prevention and suppression of terrorism and its financing (Recommendation No. 16).
- Designated non-financial businesses and professions (DNFBPs), such as casinos, real estate offices, dealers in precious metals or stones, attorneys, notaries, and accountants, should be able to report suspicious activity, while being protected from civil and criminal liability (Recommendation Nos. 18 through 22).
- Countries should take measures to ensure transparency and obtain reliable and timely information about the beneficial ownership and control of legal entities (Recommendation No. 24), including information regarding trusts — namely, information about the settlors, trustees, and beneficiaries of trusts (Recommendation No. 25).
- FIUs should have timely access to financial and administrative information, either directly or indirectly, as well as information from law enforcement authorities, in order to fully perform their functions, which include analyzing suspicious statements about operations (Recommendations Nos. 26, 27, 29, and 31).
- Casinos should be subject to effective supervision and rules to prevent money laundering (Recommendation No. 28).
- Countries should establish the means for conducting freezing and seizure operations, even when the commission of the predicate crime may have occurred in another jurisdiction (such as another country), and they should implement specialized multidisciplinary groups or task forces (Recommendation No. 30).

[5]The 2012 version expanded the definition of PEPs to include both nationals and foreigners, and even international organizations.

- Authorities should adopt investigative techniques, such as undercover operations, electronic surveillance, access to computer systems, and controlled delivery (Recommendation No. 31).
- The physical transportation of currency should be restricted or banned (Recommendation No. 32).
- Proportionate and deterrent sanctions should be available for natural and legal persons (Recommendation No. 35).
- There should be international legal cooperation, pursuant to the Vienna Convention (International Traffic, 1988), Palermo Convention (Transnational Organized Crime, 2000), and Mérida (Corruption, 2003) (Recommendation No. 36).
- Countries should provide mutual assistance toward a quick, constructive, and effective solution (Recommendation No. 37), including the freezing and seizure of accounts, even with no prior conviction (Recommendation No. 38), extradition (Recommendation No. 39), and spontaneously taking action to combat predicate crimes, money laundering, and terrorism financing (Recommendation No. 40).

In the 2012 revision, the Recommendations set forth general guidelines, with details given in Interpretative Notes. The Interpretative Notes fit within the context of common law and civil law, providing a common ground for countries with either legal system. In addition, the glossary makes it easy to place the adopted standards in proper perspective and provides important clarifications. One important innovation of the revised Recommendations, albeit not the purpose of the February 2012 review, was its emphasis on the need for countries to adopt the RBA. Under RBA, countries must establish standards to guide public policies that address money laundering, terrorism financing, and the proliferation of weapons of mass destruction, before applying measures that prevent and combat these problems.

Some Recommendations could have a special role for combating illegal gambling and money laundering. The FATF gave particular attention was given to designated nonfinancial businesses and professions (DNFBPs), such as casinos and real estate offices, which must report suspicious operations (Recommendation Nos. 18 through 21). In addition, the FATF established a specific Recommendation directed toward casinos that subjects them to effective supervision and rules to prevent money laundering (Recommendation No. 28).

Thus, the FATF has shown great concern in the prevention of money laundering, including in sport and gambling. Since 2009, a special report was launched about casinos (FATF, 2009a).

Large investments in casinos can create a real, positive economic impact when they are channeled with great social membership, business development, and extensive transmission of cultural values. However, the growth of this industry has been hindered by criminal practices, notably corruption, tax evasion, and money laundering. While certain controls to stop money laundering have been put in place through the FATF guidelines, this has led to the search for new mechanisms to launder assets in order to delink them to the predicate or underlying crime. There are obvious risks that arise when people use legitimate sectors for illicit gain, often leading to the contamination of these sectors with illicit money. Moreover, the global financial market and the development of information technologies have gradually strengthened the underworld economy, extending the possibilities of the practice of economic crimes.

Forms of gambling, such as casinos and lotteries, are occasionally the subject of discussion with respect to illicit financial crime. The study of gambling activities, such as casinos and lotteries, is a paramount issue due to their vulnerability to criminal exploitation. For instance, Brazil received special attention due to the prevalence of the game "Bingo" in the country, which was created in order to stimulate playing of sport before its alleged link with known clubs or federations. Even certain Court decisions, whether or not in favor of gambling, have demanded specific analysis regarding the remarkable possibility for money laundering that accompanies gambling.

Glenny (2008), in an important reflection, reveals the following:

> "But given that the shadow economy has become such an important economic force in our world, it is surprising that we devote so little effort to a systematic understanding of how it works and how it connects with the licit economy. This shadow world is by no means distinct from its partner in the light, which is itself often far less transparent that one might suspect or desire."

This quote illustrates the importance of enforcement authorities paying special attention to dubious payments and constant movements of large sums of money. For example, without such attention, gambling

houses can transfer or deposit funds through money changers or extra banking activities, thus preventing them from being adequately controlled. Unfortunately, many countries have little experience with controlling this business practice, which may pose a high risk of money laundering. There would be no effective exchange of information between relevant authorities responsible for overseeing this business practice or a clear definition of who would be responsible for sharing information.

This could, certainly, lead to suspicious transaction reporting of only one or a few isolated acts to the local FIU,[6] which would only have limited effectiveness. Thus, the set of illicit practices, diluted with various chain of casinos, would not lead to knowledge of the entire illegal transaction, because it could only be verified by knowing about all of the illicit activity.

To combat the practice of economic and financial crimes, it is important to scale the problem and study the methods used to launder dirty money. Given the controls that are increasingly established and the ease in laundering money, gambling houses are constantly subject to exploitation by criminals through illegal control of operations or the purchase of their own establishments, often leading to larceny, fraud, and money laundering. In order for gambling houses to continue, it is essential to have customer confidence in the institution. That is why authorities must allow the honest play of games through an adoption of specific rules and required management to ensure a high standard of safety and supervision.

A great deal of attention has been focused on money laundering due to the highly sophisticated nature of its criminal practices. These practices have been internationally organized and professionally executed for a considerable amount of time. Organized crime has had a relatively free hand in its efforts to make criminal assets legal. This is made possible by the relative ineffectiveness of current national and international laws, which have not kept pace with the changing situation.

Dipp (2004) points out that organized crime takes advantage of the "inertia of States, and their closely regulated executive, legislative and judicial branches, which are bound by the principle of territoriality — the idea that the law holds only within its boundaries. This is a hopelessly dated notion. Each State must, without giving up its sovereignty, achieve

[6]In the United States, the Financial Crimes Enforcement Network, or FinCEN; in Brazil, the Council for Financial Activities Control, or COAF.

broad international cooperation. To insist on a 19th century conception of sovereignty is to allow organized crime to exercise its will to the detriment of formal sovereignty."

Betti (2000, p. 20) views financial crimes as crimes that are generally "marked by the absence of social scrutiny, due to several factors including an excessive attachment to material things such as profit and egotistical zeal among the owners of capital, who are scornful of the lower classes and confident in their own impunity. Most of these crimes are covered up by collusive public officials. When the crimes do come to light, evidence is poorly produced and the facts are difficult to ascertain, given the specialized assessment required, culminating almost always in impunity." Betti adds that it is not always "easy for a criminal to use the proceeds of crime. Profligate spending and the eccentricities that always accompany the easy acquisition of money, and immediate purchases way above one's standard of living, are outward signs of wealth which give rise to suspicion and are conducive to investigations by either police or internal revenue authorities. Experienced criminals therefore try to come up with arrangements for investing their criminal proceeds and work with others inclined to conceal these assets and obliterate the money trails in order to avoid enforcement efforts" (Betti, 2000, p. 39).

To the extent that society has realized that serious crime can encompass more than just violent crime, an increasing number of States have ratified international regulatory instruments without restrictions, demonstrating that they are no longer willing to tolerate open-ended criminality within their borders. It should be noted that money laundering is in essence a derivative crime, because the offense is contingent upon an antecedent crime. This link between money laundering and organized crime necessitates immediate and aggressive intervention by governments to ensure the very survival of their countries.

One could indeed define money laundering as a simple procedure whereby one transforms goods acquired through unlawful acts into apparently legal goods. However, overriding considerations of legality and legal security do not permit us to make use of such a simple definition. Another difficulty with money laundering is that it is neither simple to accomplish nor does it follow any preset rule. The commission of the crime involves processes that are often complex and sophisticated. Classically speaking, the crime of money laundering involves three stages of conduct: (1) concealment or placement, in which goods acquired by unlawful means are made less visible; (2) monitoring, dissimulation,

or layering, in which the money is severed from its origins, removing all clues as to how it was obtained; and (3) integration, in which the illegal money is reincorporated into the economy after acquiring a semblance of legality. Added to this is the recycling stage, which consists of wiping out all records of the previously completed steps.

Faced with the complexity of the various forms of conduct and processes comprising money laundering, one is struck by the almost complete impossibility of imposing legal restraints, other than through combined means (i.e., proscribing more than one form of conduct) or open-ended means (i.e., targeting a large number of activities described in the UN Conventions about drugs and organized crimes and adopted by most countries). Additionally, money laundering is always a derivative crime that is necessarily connected to its antecedent or underlying crime. All these issues add innumerable peculiarities to the crime of money laundering, peculiarities which must be gradually sorted out by jurisprudence or case law.

In Brazil's case, money laundering was not typified in the main body of the Criminal Code, as was done, for instance, in the United States (see 18 U.S.C. § 1956). This poses an undeniable difficulty. If the crime in question was codified, it would be promptly adapted to the principles and rules of the Criminal Code. Because the money laundering system is integrated and hierarchical, there would be no margin for unjustifiable exceptions. This is the case in France, Italy, Switzerland, and Colombia.

The United Nations Convention against Transnational Organized Crime convened in Palermo on November 15, 2000,[7] following the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of December 20, 1988[8] (Article 5). Both global regulatory guidelines require the State Parties to make the laundering of the proceeds of crime a crime itself (Article 6), and they provide for the confiscation of "proceeds of crime derived from offences covered by this Convention or property the value of which corresponds to that of such proceeds" (Article 12(1)(a)). Parallel to that is the United Nations Convention Against Corruption held at Mérida in 2003 (Article 31,

[7]The Convention against Transnational Organized Crime was promulgated in Brazil by Decree No. 5015 dated March 12, 2004, and passed by Legislative Decree No. 231 dated September 29, 2003.

[8]The Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances was ratified in Brazil by Decree No. 154 dated June 26, 1991.

item 5 — confiscation and seizure of money in an amount equivalent to the proceeds of crime).[9]

Items 2, 3, and 4 of Article 12 of the United Nations Convention against Transnational Organized Crime held at Palermo correspondingly assert the following: "State Parties shall adopt such measures as may be necessary to enable the identification, tracing, freezing or seizure of any item referred to in paragraph 1 of this article for the purpose of eventual confiscation; if the proceeds of crime have been transformed or converted, in part or in full, into other property, such property shall be liable to the measures referred to in this article instead of the proceeds; if proceeds of crime have been intermingled with property acquired from legitimate sources, such property shall, without prejudice to any powers relating to freezing or seizure, be liable to confiscation up to the assessed value of the intermingled proceeds." Such provisions accurately depict the new world order with respect to combating organized crime, including narcotics trafficking and corruption.

It is sometimes alleged by defendants that the property seized has no links to the crime. The judge must then properly estimate the amount that flowed from the proceeds of the unlawful conduct imputed, being mindful of the need to enforce the requirements set forth in the foregoing Conventions, as well as Article 387, Section IV, of the Brazilian Code of Criminal Procedure. This Article requires that the decision be fixed at the "minimum amount required for reparation of damages caused by the crime, taking into account all losses suffered by the aggrieved party," in order to secure definitive forfeiture of that amount to the injured party or to the State as indemnification for damages caused by unlawful conduct.

Under Article K.3 of the Treaty of Maastricht (1992), European Union (EU) Member States agreed to adopt a common policy in their domestic efforts, and the 1998 joint action (98/773/JHA) sought to include money laundering as a type of organized crime. This was revoked in part by the Framework Decision[10] of the European Union Council, dated June 26,

[9]The Convention Against Corruption was ratified in Brazil by Decree No. 5687 dated January 31, 2006.

[10]Decisions and framework decisions were new instruments under Title VI of the European Union Treaty ("Provisions on Police and Judicial Cooperation in Criminal Matters") replaced joint action. Framework decisions are used to bring together the legislative and regulatory provisions of Member States. They are proposed on a motion by the Commission or by a Member State and must be unanimously adopted. They are binding

2001. Under this decision, Member States agreed to not make reservations on Articles 2 and 6 of the European Convention of 1990 (including the rule which provides for money laundering resulting from general criminal conduct), since only *serious infractions* can be at issue. The Member States also provided measures for the confiscation of proceeds from crimes that either have a maximum penalty of greater than one year or are considered to be serious crimes (Article 1).

The Framework Decision of February 24, 2005 (2005/212/JHA), regarding the forfeiture of products, instruments, and property related to crime, allows "extended powers of confiscation" aimed not only at the forfeiture of the assets of those found guilty but also the assets acquired by their spouses, companions, or those whose property transferred to some company under the influence or control of the guilty parties. These extended practices apply to organized criminal practices, such as counterfeiting, trafficking of persons, or assisting illegal immigration, sexual exploitation of children and child pornography, narcotics trafficking, terrorism, and terrorist organizations, and money laundering, as long as these crimes are punishable by a sentence of at least five years of imprisonment (or, in the case of laundering, a maximum penalty of at least four years of imprisonment) and generate financial income (Article 3, Sections 1–3).

Note that the Palermo UN Convention provides for international cooperation on matters of confiscation (Article 13(1)) and expressly provides that the proceeds of crime be allocated to finance a United Nations Organizations Fund to assist Member States in obtaining the wherewithal needed to enforce the Convention (Articles 14(3)(a) and 30(2)(c)). Any illegal proceeds can be included within the scope of this Convention if it can be shown by convincing evidence that they may be related to the commission of antecedent crimes and to money laundering. Thus, if gambling was indeed being used for purposes of money laundering, those circumstances would justify judicial search and seizure, and possibly confiscation, of gambling proceeds.

Leaving illegally obtained money in the hands of criminals — especially members of organized criminal gangs — encourages the

on Member States as to results to achieve, and leave it to national courts to decide on the manner and the means of achieving them. Decisions address all other goals besides the conference committee work on legislative and regulatory provisions of the Member States. Decisions are binding and all measures necessary to carry out the decisions within the scope of the EU are adopted by the Council through qualified majority vote.

reentry of these monies into the underworld or back into the original illegal business practices, creating the potential for serious harm to society. To prevent the use of the sports and gambling sectors for organized crime, it is important to have an adequate understanding of the methods used to launder illicit funds, the vulnerabilities of these methods, and the capacity to exchange vital information from foreign authorities. However, even assuming a high degree of sophistication, supervision, and safety, gambling houses can still be seen as attractive settings for crime to criminals who do not fear the consequences of their personal illegal actions.

Online Casinos

The operation of casinos is very similar to the operation of other financial institutions because of the extensive payments with cash, the exchange of chips for cash or checks, and the frequent participation by foreign tourists, who are the constant beneficiaries of certain amenities like room and board.

This undeniable movement of people and resources requires strict transparency to prevent the use of casinos for organized crime. Casinos on cruise ships raises important questions regarding jurisdiction to prosecute any illicit activity: whether jurisdiction is based on where the ship is registered or where it travels or operates. Many countries do not have specific regulations regarding this issue, which may result in a lack of jurisdictional action that limits the ability to prosecute criminal activity.

In addition, there is the possibility of online gambling, which gives rise to a study of how to regulate this subset of gambling effectively and how to enforce official controls to prevent money laundering in this area.

The importance of the gambling sector can be measured by numbers. The global online gambling market is expected to grow from USD 64.13 billion in 2020 to USD 72.02 billion in 2021 at a compound annual growth rate (CAGR) of 12.3% (PR Newswire, 2021). According to Kindt and Joy (2002–2003), "[P]olicy-makers worldwide generally failed to identify the large socio-economic costs associated with Internet gambling, as well as the ability of Internet gambling and other forms of cyberspace gambling to destabilize local national, and even international economies by disrupting financial institutions." Even in countries that properly regulate the gambling industry, large-scale money laundering activities still exist.

The aforementioned report from the International Financial Action Task Force (FATF, 2009a) revealed that there are many suspicious activities reports related to the gambling sector. It is very easy to convert illicit cash through electronic or cash transactions in the gambling context. For example, it is possible to exchange illicit monies through "buy ins" and "cash outs." In the first case, there is a conversion of money into tokens, tickets, or credits in order to start the game. In the second case, the reverse occurs, and tokens, tickets, or credits are replaced with casino checks, claims on accounts, or fund transfers to other casinos.

Likewise, it is possible to convert the ticket called TITO (Ticket In/Ticket Out), which allows a gaming machine to accept bills or tickets with credits printed on it (i.e., a Ticket In) or print tickets containing credits once the player wishes to settle the game (i.e., a Ticket Out). In this case, the customer can exchange the ticket for cash at the establishment or reuse it on another TITO machine to restart the game.

Brazil, despite being one of the most populous countries in the world with more than 210 million people, had a small industry of casinos. There were about 130,000 machines, including slot machines in about 1,500 "Bingos" that operated across the country, reaching its peak in 2006. However, in 2007, many casinos were forced to a standstill, and many machines were confiscated by the authorities, when the practice of corruption in the industry was revealed by the federal police's Hurricane Operation. Their findings indicated alleged involvement of politicians and organized crime within the gambling industry in order to keep the casinos open.

A bill to legalize casinos could create a serious precedent for the practice of money laundering if it is not accompanied by a strong structure for the supervision of gambling. Without strict regulation and sufficient mechanisms for oversight, it is not possible to keep organized crime away from this sector. Even if the gambling sector leads to more jobs and investments that benefit the country, legalizing gambling is not justified unless there is also an effective mechanism for preventing organized crime. However, the methods used to launder and use illicit assets are constantly evolving. For the standards to remain relevant and effective, researchers must keep up to date with the latest money laundering and terrorist financing methods, techniques, and trends. It is important to constantly monitor and identify new threats and risks to the financial system and to publish the findings in typologies studies. These studies are aimed at raising global awareness and facilitating early detection of the use and

abuse of the systems. They are also instrumental in ensuring the development of the most appropriate standards to respond globally to these new and emerging money laundering and terrorist financing risks and threats. The conclusions generated by the typologies studies played an important role in the revision of the FATF Recommendations. The FATF Recommendations, which were adopted in February 2012, provide countries with the tools to build stronger safeguards to face today's threats and challenges to the financial system.

There are records indicating the practice of "jobbery," where moneylenders' exploitation is financed by organized crime. Through this practice, moneylenders convince customers in financial difficulty to not submit to legal loans and to instead obtain resources that support gambling. For example, the purchase of winning lottery tickets easily covers up "dirty" money by making it seem clean. Winning lottery tickets can also be obtained from bets in amounts that cover all the possibilities of success, allowing the conversion of illicit money to having a known and documented origin.

It is also worth mentioning the possibility of purchasing tokens or tickets through the use of credit cards, where the leftover tokens are exchanged for cash or casino vouchers. The casino tokens are considered valid instruments, most commonly issued for their use in slot machines. However, sometimes credit cards are used to purchase narcotics, and the traffickers negotiate these deals in gambling houses. The company that manages the cards is paid with money received from the gambling houses. This mechanism allows for the illicit accumulation of wealth. Money launderers usually acquire chips or credits with cash or by depositing money in accounts with the gambling houses or casinos. In these cases, it is possible to use the credits or the gift certificates, known as Chip Purchase Vouchers (CPVs), in casino networks in different countries. It greatly complicates the control over the casino system, as the possibly existing credit can be converted into a check-in setting among various casinos that are different from the first one that provided the chips or CPV.

Other hypotheses regarding illegal gains or the illegal use of gambling houses are also worth mentioning. Criminals launder counterfeit money by making use of agents who exchange money through multiple transactions made by anonymous people, using false documents created to disguise their illicit origin. For example, this exchange can occur by using chips as currency to conduct illegal transactions. Criminals can retain the chips for a period of time and use them to buy drugs or other illegal

substances. These chips can be transported to other countries, serve as payments for clandestine activities, and eventually be exchanged in casinos by third parties in diluted amounts, which do not lead to any suspicious communication. These acts usually do not call attention to a particular gambling house unless it has a specific type of chip and does not allow the exchange of other types of chips, even though they come from the same network.

Criminals also launder illegal money by inserting bills of various denominations, such as USD 1, USD 5, and USD 10 bills, it into video poker machines and then pressing the "cash out" button after playing briefly or not even playing at all, which generates a receipt that can serve as a document for a refund to present to the cashier. Another possibility lies in converting illicit money into legal money by buying chips for high prices, i.e., an inflated purchase price. The winner can aggregate cash and then exchange the total amount for casino checks. The purchase of award certificates that can be redeemed by or passed to others keeps some distance between the winnings and their illicit origins.

In Australia and Belgium, the purchase of accumulated money in chips is done not to play with them but to exchange their value through third persons linked to the buyer. In South Korea, the acquisition of chips using checks between 2003 and 2005 totaled USD 20 million. Such chips were exchanged for cash and checks issued by casinos. The money was used for corruption by government officials.

In the United States, a lawyer in the state of New Jersey was convicted of accumulating over USD 500,000 through fraud and laundering USD 250,000 in a casino in Atlantic City. He transferred this amount to the casino and bought chips, playing for about an hour on roulette and lost USD 10,000. He traded the rest for currency in cash and left the casino. A similar case occurred in Spain, where different people entered separately into a casino and obtained chips. After playing a few sums, they exchanged the chips for checks that were paid to a third person.

The Report of the International Financial Task Force on laundering in football that took place in 2009 (FATF, 2009b) highlights the following indicators of money laundering: (1) inserting values in gaming machines and requesting their immediate exchange for credits; (2) seeking credits and not playing at all or playing very little; (3) trying to be friends with employees of gambling houses or casinos; (4) buying chips with little or no gambling; (5) people using third parties to buy chips; (6) inconsistency between the amount of the bets and the customer's financial situation;

(7) dramatic or rapid rise in size and frequency of transactions in a particular client account; (8) exchange of coins or paper currency notes for cash in the establishment; and (9) gaming machines, video lottery terminals (VLTs), and TITO machines are used to refine the currency through large sums, little gambling, and later-exchanged credits.

An interesting case involved the importation and distribution of heroin in Australia. The drug came from Vietnam. The person used large amounts of money and third parties to purchase chips in his name. On the same day, there was intensive exchange of these chips for cash that was careful to avoid exceeding USD 10,000 per transaction, the amount that triggers suspicious activity reports (SARs). Authorities discovered that there were some referrals by a remittance company to various entities in Vietnam, without the negotiator of the consignment connected to the "player."

There is also the possibility of minimizing suspicion by distributing large amounts of cash through small transactions in order to evade the legal limits that require communication with authorities in order to prevent laundering. This type of strategy is known as "structuring," which includes the following:

(1) Deposits or regular transactions below limits that require reporting to the authorities;
(2) Use of third parties to carry out transactions with single or multiple accounts;
(3) Use of regular checks from financial institutions to acquire tokens or chips, with each transaction being less than the limit that suggests a suspicious transaction and requires reporting;
(4) Requests to split awards in amounts below the legal limit and exchange them for cash at ATMs;
(5) Several people sending funds to a sole beneficiary;
(6) Checks issued to a player's relative;
(7) Inconsistent activities for the customer profile;
(8) Casino account transactions conducted by persons other than the account owner;
(9) Third parties who request structuring deposits and wire transfers;
(10) Large volumes of transactions in a small period of time;
(11) High frequency of betting amounts that are always below the limit requiring reporting;
(12) Mismatch between the purchases and exchanges of chip currencies;

(13) Refusals of compliance with the use of third-party documents, whether they are false documents or those from tourists; and
(14) Suddenly straying from typical betting patterns for a particular account.

Moreover, gambling house accounts, which are made available to customers for deposit and for converting credit lines, have fewer reporting requirements for suspicious transactions and thus allow an easy path to money laundering. For example, deposits made through electronic transfers can be used for cash or transferred to other accounts with little or no gaming activity. In such cases, the illegal money exchanger usually does not submit to obligations of reporting suspicious transactions and continues to have accounts that can supply money to casinos. Another suspicious signal of money laundering occurs when several people transfer funds to a single beneficial owner, followed by accountants or lawyers becoming in charge of these transactions. Some casinos offer safes for special customers. These safes present a serious risk because they lack transparency regarding the use by the customers or by third parties holding their passwords.

An interesting case occurred in which sums of money stemming from illicit drug trafficking, deceit, and credit card fraud traveled from England to Dubai after being laundered in a casino. Money played and exchanged provided the defendants an explanation as to the apparent lawful source of funds. In this case, the given explanation alleviated any raised suspicions almost instantly. These circumstances require more appropriate regulations to prevent suspicious transactions.

Laundering methods consist of offering award winners a premium on their earning in exchange for transferring the prize to criminals. It also raises suspicion when two people in apparent opposition, but who are in fact engaged in collusion, place identical bets on the same game, when the chance to win double (e.g., in roulette: 1,000 red and 1,000 in black). This invariably allows one party to gain winnings, and that party issues a check to the other party without generating suspicion or notifying the authorities.

There is also the possibility of converting large amounts of currency into the currency of another country, which does not raise suspicion when there are a large number of foreign players, thus altering the original form of the currency. This method was used in one case in Spain, where a group of foreigners who separately bought chips in a casino using

different currencies later converted their chips into Euros. In this case, the casino not only detected the suspicious operation in advance but also ordered the operation's cancellation and reported it to the Spanish FIU.

Unusual cases that involved employees of gambling houses or casinos were noticed. For example, complicity among employees has led to a lack of reporting suspicious transactions, the destruction of documents related to such communication, and the falsification of players' data to justify the accumulation of credits. An important case illustrating this method came from the United States, where a group of drug-trafficking money launderers bribed employees of a particular casino to access machines controlled by software that allowed the money launderers to take over certain features, thus enabling their illicit gains. Often, these types of illegal activities are made possible by contact between customers and employees outside the gambling houses.

Besides, it is possible to engage in money laundering activity through the use of stolen credit cards. However, it is easier for authorities to follow the trail of money with this method. In Belgium, for example, a person visited a casino on the country's coast on two occasions and acquired chips worth €400,000 paid by cash and credit card. The casino reported the situation to the local FIU. The FIU verified that the account of that player was supplied by several transfers from companies and cash deposits and that the player's wife had business in Belgium, maintaining contacts with organized crime in Central and Eastern Europe. The defendant-player also maintained frequent contact with a person investigated for money laundering stemming from this organized crime.

Similarly, the use of debit cards is a valuable tool to commit fraud and money laundering. In England, it was possible to verify that a person acquired the maximum chips with a debit card without playing them, later exchanging them for cash. The limitation of transactions made with debit cards do not avoid the exchange of chips for cash. In addition to credit and debit cards, the use of false documents is another common method in gambling houses for opening accounts to conduct games and obtain winnings.

Several vulnerabilities have been identified by the FATF, but it is worth mentioning tourism activities related to casinos and gaming houses in particular, called "junkets." This is a marketing program that creates a tour organized specifically for gambling, which may include transportation, accommodation, incentives to play, and movement of funds to other casinos. It can be promoted by the casino itself or through outsourcing

game houses. Participants in this type of tourism usually trust their operators to allow the movement of money across borders. This relationship between operators and customers has the potential of leading to complicity between them, thus enabling money laundering. The authorities should be notified of any suspicious transactions that occur in this setting as well. However, regional offices or outsourced casinos usually accept the previous deposits on tourists' behalf before the trip. These deposits sometimes occur by wire transfer, which do not call the attention of the local authorities that oversee money laundering.

To prevent misuse of junkets, their registration should be required before operation, with detailed qualification of authorized operators, including the requirement of filing fingerprints, so that they have the obligation to report suspicious transactions undertaken by customer-players. Moreover, the junkets should be subject to cancellation of their registration in cases of unlawful activity.

Gambling houses should also be required to report illegal junkets to the authorities. Often, junket activity is vital to the gambling houses, especially in sparsely populated countries, such that there is a very close relationship between the gambling house owners and junket operators. This may lead to the misuse of the junkets. Some junket operators may be able to gather a pool of customers, which can be used to mask individual spending. Plus, junkets in foreign countries that are not properly regulated enable connections to organized crime, even if they or companies related to them are not allowed to work in places where they have established gambling houses.

One cannot fail to mention that junkets may also be an alternative mechanism, formal or informal, for transfers of funds. The very nature of this activity has suggested that they are an informal mechanism. Some casinos also offer "junket-agents" a non-negotiable amount called "dead chips," which cannot be exchanged for cash or normal chips. These chips can be used as currency to facilitate criminal transactions. These aspects of junkets make it especially imperative to have regulatory requirements and an obligation to report suspicious activities.

There was an interesting case in which a casino's agent received large sums of money in China from a customer who wanted to play in Macao. This agent received the amount in a trade near Macao and divided the amount into parts that were physically transported to the island. All the money was deposited into an account of the casino's agent and then passed on to the gambling house. The gambling house converted the

money to non-negotiable chips. When the client had gained a certain amount of money, it was given to the agent who sent it back to China by unofficial routes.

A new issue has become the subject of concern: the growth of travel offers through casino ships with the system "junket" operated by independent operators. Normally, players deposit a significant amount of money with the junket operator. However, regulation of this kind of service is still lacking. One category of customers, the high-rolling players (or "high rollers"), occupies special VIP rooms in the complex and gets special treatment. This clientele is linked to junkets' business, and as such, they are vulnerable to potential identification and to the discovery of the origin and destination of their resources. Thus, the authorities have been hesitant to ease cash transactions, especially for high rollers. At the same time, the gambling houses have offered similar facilities to any financial institution, while the regulation and supervision of these entities are also not consistent.

Two examples illustrate the risk of money laundering that accompanies high rollers. First, in Australia, an Asian person linked to organized crime was considered a high roller and engaged in heroin trafficking through a casino-hotel, using gambling to mask illicit gains. He received incentives from the casino totaling AUD 2.5 million and spent two years as a non-paying guest. Second, in the United States, a foreigner traveled to Las Vegas to gamble and lost approximately USD 150 million. The casino offered a credit of USD 10 million, plus other benefits such as hotel suites, cars, and aircraft services. The casino held wire transfers and bank accounts linked to the bettor on a corporation. There was no suspicious transaction report made by the casino to verify the source of funds.

To avoid such problems, it is essential to provide proper training for employees of gambling houses in order to prevent and detect money laundering. These employees must be certified and undergo training to report suspicious transactions. The untrained employee is prone to misconduct even when regulations are imposed. It is also essential to penalize violations of administrative rules (i.e., not implementing adequate internal controls to prevent money laundering) to create consensus and enforce these legal provisions.

In the United States, there are an estimated 567 Native American tribes recognized by the federal government (half of them in Alaska), and 223 of them operate gambling activities in about 28 states. In one case, the Financial Crimes Enforcement Network (FinCEN) decided to institute an

administrative punishment to address the lack of implementation of preventive regulations by the Tonkawa Bingo and Casino and Edward E. Street, who operated it. The casino was located in Tonkawa Tribe territory and self-governed by Native American tribes located in Oklahoma. The casino operated under the approval of the Tonkawa Tribal Gaming Commission. The casino's violations were based on a lack of maintenance of relevant information, lack of records, lack of staff training, and, consequently, lack of internal controls to prevent and to report suspicious transactions. For example, there was nondisclosure of transactions amounting to over USD 10,000 made in one day by customers, albeit in different operations. Tonkawa Tribe was punished with a fine of USD 1 million and Edward E. Street received a fine of USD 1.5 million, in accordance with an agreement with FinCEN dated March 24, 2006. Tonkawa Tribe closed the Tonkawa Bingo and Casino as a result of this case.

In Brazil, casinos and bingos are considered illegal.[11] Abovitz (2008) reveals that "[i]n the United States, courts have traditionally recognized gambling as an area reserved for state regulation pursuant to the Tenth Amendment of the US Constitution. Currently, all fifty states and the District of Columbia conduct some form of gambling regulation, ranging from full legalization in Nevada to blanket prohibition in Hawaii and Utah."

Gambling conducted via the Internet has drawn extensive attention. Usually the regulations are designed to generate tax revenue while also providing for the safety of players and operators by limiting the social concerns associated with gambling. Kindt and Joy (2002–2003) state that "[a] majority of the money generated by Internet casinos went untaxed, created more untaxable money flow, and reduced taxable economic activities." Although the traditional methods of regulating gambling have been effective, application to the Internet has proven difficult as the boundless nature and wide accessibility of the medium are widely believed to intensify social concerns.

[11] Law n.º 8,672 of 06 July 1993, called Zico Act, wished to allow optionally clubs the chance to become companies. In turn, the Law 9615 of 24.03.1998, called Pele Act, revoked Zico Act and was later amended by Law n.º 9,981 of 14 July 2000, called Maguito Vilela Act, which revoked, in art. 2nd, the chapter devoted to bingo. Law n.º 10,671 of 15 May 2003 took care of the financial transparency of management, established offenses and considered sport as a cultural expression of the country.

On October 13, 2006, President George W. Bush signed into law the Unlawful Internet Gambling Enforcement Act of 2006 (UIGEA),[12] which prohibits the acceptance of payment of wagers by financial institutions. The UIGEA bans Internet gambling by forcing financial institutions to prevent financial payments of wagers from bank accounts and other financial instruments (Blankenship, 2008). In the United States, for instance, if the wager tries to deposit its winnings got from online gamble in a bank account, the transaction must be rejected and he or she will be brand by the federal government as "Internet gamble." Therefore, the government can go after the wager.

Online gambling has generated an overwhelming interest worldwide. Bana (2011) states that it "is being seen as a potential trading sector that could assist countries with a 'booster shot' in reducing their accumulated fiscal deficits in an effort to encourage domestic and world economies." These developments pose regulatory and technical challenges, and they also give rise to societal and public order issues, such as the protection of consumers from fraud and the prevention of gambling addiction.

As online gambling is a global phenomenon, an effective international regulator should be formed to monitor the management, accountability, efficiency, and sector proportionality of the stakeholders involved in order to sustain market confidence in trading by promoting public understanding in addition to maintaining an appropriate degree of protection for consumers. According to Mills (2000), "while facilitating commerce and communication, the Internet also facilitates the ability of criminals to elude the laws of any, and every, nation."

The Internet provides individuals worldwide with the ability to communicate and exchange information across national boundaries and continents. The project to connect scientists and defense agencies has united the globe with access to information, available anywhere, at any time. And it has also connected criminals and people with criminal purposes. There is a daily concern to reflect the current times, challenging and requiring authorities to take actions against money laundering, organized crime, and tax evasion, especially the need of a different perception of a changing world, which has allowed the perpetuation of a number of serious crimes and illicit enrichment of official agents. In other words, it is important to get an answer that allows for effective prosecution. For this reason, an incisive criminal intervention by the State is required, at the

[12]31 U.S.C. §§ 5361–5367 (Supp. 2007).

outset, including the forfeiture of goods and values of criminals once confirmed to be unlawful possession or property. Thus, it is possible to annul the idea that crime is worthwhile, and instill the fear of eventual conviction and imprisonment in future offenders.

There are obvious risks in contaminating legitimate sectors, determining and managing them with illicit money or even using them by people seeking their exclusive benefit. Various forms of gambling (e.g., casinos), which are sporadically the subject of discussion regarding their permissions or even rulings by Court decisions, in or not favorable to their practices, have demanded specific analysis regarding their remarkable possibility for money laundering. The same can be said about lotteries that are being used for the same purpose. However, the use of money of dubious origin when playing lotteries and the existence of constant movements of large sums of money require special attention of enforcement authorities and it has been prohibited. Bank accounts of gambling houses cannot be adequately controlled if those houses allow the transfer or deposit of funds through money changers, extra banking activities, or online untraceable means.

There is still, in many countries, little experience of the authorities to control this line of business, which may pose a high risk factor of money laundering. There is no effective exchange of information between relevant authorities responsible for overseeing this business practice or a clear definition of who would be responsible for sharing information. This could, certainly, lead to suspicious transaction reports of only one or a few isolated acts to the local FIU, which would lead to limited effectiveness. Thus, the set of illicit practices, diluted with various casino chains, would not lead to knowledge of the entire illegal transaction, because it would only be verifiable by taking into account all the selected activities involved.

To combat the practice of economic and financial crimes, it is necessary to measure the problem and study the methods used to launder dirty money. Consequently, customer confidence in this activity is essential, the reason why authorities must allow an honest conduct of games through an adoption of specific rules and require management to ensure a high standard of safety and supervision. The confidentiality of SARs is protected in the United States. There was some question as to whether this protection was restricted to the Report itself or extended to supporting documentation. At first, only the Report was confidential, but afterward, the Office of the Comptroller of the Currency (OCC) at the Treasury Department

decided that supporting documentation was also confidential. This secrecy is so indispensable that, even when subpoenas are issued ordering disclosure of reports or supporting documentation in several cases, the OCC held that it must be notified by the banking institution so that it might take part in the proceedings and that the disclosure must comply with the Federal Rules of Civil Procedure. There was a suggestion that information be shared among financial institutions to better detect new fraudulent schemes. Through FinCEN and other agencies, the Treasury Department decided to provide information so that they might keep abreast of the trends in that class of crimes, issued statements and hold meetings and seminars (FinCEN, 2008, 2012). Note that there is a deadline for SARs: 30 days from the time the facts are known, but if the suspect cannot be identified, this timeframe extends for another 30 days. No more than 60 days may elapse, however, once the facts become known.

Observing proper vigilance and SARs are deemed essential to ensure that the financial institution has an effective compliance program. Appropriate policies and procedures must be put in place to monitor and identify unusual occurrences by time and place. Reporting systems must include unusual event identifications or alerts (identifying the employee and giving all necessary search information), management alerts (awareness of all methods of identification and evaluation in all business areas), the Report itself and its generation, regardless of size. Monitoring system sophistication must be understood as part of banking risk, with emphasis on what goes into high-risk products, services, account holders, and entities. Financial institutions must therefore have adequate personnel to identify, research, and report on suspicious activities, with due account taken of the general risk level and volume of transactions. FinCEN is watching casinos that offer sports betting and cryptocurrency payment options for potential money laundering problems. Casinos need to identify "red flags" for illicit financing.

Kenneth A. Blanco spoke at the *12th Annual Las Vegas Anti-Money Laundering Conference* on August 13, 2019. His remarks indicated that FinCEN is monitoring casinos — both brick-and-mortar establishments and online gaming ventures — to ensure that they live up to their reporting obligations under the Bank Secrecy Act (BSA) and is also focusing more broadly on the money laundering risks associated with cryptocurrency and sports betting. Blanco's remarks affirmed FinCEN's commitment to enforcing the BSA on casinos that deal in cryptocurrency — regardless of the scale of the operation, and regardless of whether the

casino accepts cryptocurrency "from customers either on location or though mobile applications."

Indeed, all casinos that deal in cryptocurrency must design anti-money laundering (AML) programs unique to the risks posed by such transactions. For instance, he remarked on the specific compliance concerns posed by cryptocurrency, including processes for conducting due diligence on digital currency; blockchain analytics to determine the source of the cryptocurrency; and mechanisms for identifying "red flags" for "money laundering, sanctions evasion, and other illicit financing purposes" (Blanco, 2019). Blanco also underscored that, as financial institutions, casinos must conduct risk-based CDD and submit SARs on suspicious transactions to FinCEN. On this note, Blanco described how FinCEN is increasingly using AI to evaluate the data that casinos input into the BSA reporting system for indicia of criminal activity. Blanco gave the example of how a drug suspect would be more likely to give a casino his correct cell phone number to ensure his winnings were properly wired out, and a DEA agent searching FinCEN's SAR database would then be able to cross-reference that number with other leads. Also, the growth of mobile gaming ties into the rise of cryptocurrency, particularly in Internet casinos that allow pay-ins and cash-outs in cryptocurrency, or allow patrons to exchange cryptocurrency for government-issued currency.

In 2011, FinCEN issued a final rule amending definitions and other BSA regulations relating to money services businesses (MSBs), a type of financial institution under the BSA, to provide that money transmission covers the acceptance and transmission of value that substitutes for currency. Cryptocurrency is such a substitute and is covered by that regulation. In March 2013, FinCEN issued guidance further clarifying this point and providing that the BSA's AML provisions apply to all transactions involving money transmission — including virtual currency. In May 2019, FinCEN issued guidance setting forth examples of how the BSA regulations apply to business models involving the transmission of cryptocurrency, including Internet casinos (FinCEN, 2019). That guidance provides that even operations engaged in the business of gambling that are not otherwise covered by the BSA regulatory definitions of casino or card club, but that accept and transmit cryptocurrency, might qualify as money transmitters under the BSA. Casinos that accept and transmit cryptocurrency must register as MSBs with FinCEN, and, like other casinos, must develop and maintain written AML programs, implement know your

customer (KYC) programs to ensure that patrons who cash-in or out with cryptocurrency have a legitimate source of funds, identify and report suspicious transactions, and file currency transaction reports (CTRs) on transactions over USD 10,000. In particular, casinos that fall under the definition of an MSB must file SARs on suspicious cryptocurrency transactions over USD 2,000, while casinos dealing in government-issued currency must file SARs on suspicious transactions over USD 5,000.

Focusing on the rise of online sports gaming, casinos are responsible for managing the money laundering risks associated with online sports betting and other forms of mobile gambling. In discussing mobile betting, Blanco said FinCEN recently updated its form for SARs to have fields allowing financial institutions covered by the BSA (including casinos) to report cyber-indicators — that is, unique electronic footprints — ranging from source and destination information to file information, subject user names, system modifications, and account information. It is expected that all covered institutions establish AML compliance programs to correspond with expanding technologies that implicate money-laundering risks. The links between money laundering and organized crime necessitated immediate and aggressive intervention by governments, as, by the way, is happening in the United States, not least to ensure their very survival. Observe that money laundering is in essence a derivative crime because the offense is contingent upon an antecedent or underlying crime.

Another difficulty with money laundering is that it is not simple ascertain it since its practice does not follow common patterns. That was the situation until the emergence of the Internet, which made things easier for criminals. The possibility of online gambling must give rise to a study of how best to regulate this issue and how to submit to official controls to prevent money laundering. There is also no control over foreign money flows obtained through the game, requiring a more detailed supervision of the financial activity involved in this activity.

According to the *Online Gambling in the Internal Market Report* from the European Commission, online gambling services are widely available and used in the EU. The economic significance of the sector is seeing rapid growth. The advent of the Internet and the growth of online gambling opportunities are posing regulatory challenges as these forms of gambling services are subject to national regulatory frameworks that vary rather significantly between Member States. These frameworks can be broadly categorized into either licensed operators operating within a

strictly regulated framework or strictly controlled monopolies (State-owned or otherwise).

EU countries are autonomous in the way they organize their gambling services, as long as they comply with the fundamental freedoms established under the Treaty on the Functioning of the European Union (TFEU), as interpreted by the Court of Justice of the EU. The freedom to provide services or to open a business in another EU country is particularly relevant here. Most EU countries allow at least some games of chance to be offered on the Internet. Some countries allow all games, while others only allow certain types such as betting, poker, or casino games. In some European jurisdictions, monopolistic regimes offering online gambling services have been established. These are run by a state-controlled public operator or by a private operator on the basis of an exclusive right. However, a growing number of EU countries have established licensing systems that allow more than one operator to offer services on the market. Under EU law, no particular system is favored over the others.

Online gambling regulation in EU countries is characterized by diverse regulatory frameworks. In a number of judgements, the Court of Justice of the European Union (CJEU) has ruled on the compliance of national regulatory frameworks with EU law. The Commission supports EU countries' efforts to modernize their national online gambling legal frameworks, in particular in the framework of administrative cooperation between gambling regulatory authorities. It also provides support to ensure a high level of protection for consumers and vulnerable people, including minors. In the area of standardization, we requested the European Committee for Standardization to develop a European voluntary standard on reporting in support of the supervision of online gambling services by national regulatory authorities (European Commission, n.d.).

A number of Member States have also embarked on a review of their gambling legislation to account for these new forms of service delivery. Furthermore, the growth of online gambling opportunities has given rise to the growth of an unauthorized market, which consists of unlicensed illegal gambling and betting activity, including from third countries and operators licensed in one or more Member States offering gambling services in other Member States without having obtained the specific authorization in those countries.

The Use of AI to Curb Money Laundering

It is important to reflect, constantly and daily, the current times, which challenge the authorities and encourage them to take action against acting automatons, a different perception of a new world situation, which may allow the perpetuation of a series of injustices. In other words, trying to get an answer that allows, of course, an effective AML system based on a fair intervention from the State. For this reason, it is required to annihilate with the idea that technology compensates for the harm it can produce if used indiscriminately.

AI, if well conceived, must be deemed as a tool currently available for a connected world and eager for quick and less costly solutions. When applied to the prevention of crime, several benefits can be obtained in view of the high number of transactions by monitoring them and screening PEPs. The benefits can also be obtained by applying to similar transactions, with a willingness to expand their skills today. AI and machine learning can assist the reporting of suspicious activity by generating reports and by automatically filling them with accurate information. There is no precedent that can be compared to the level of development that is achieved with immense possibilities given the deep technological knowledge, generating expectations of all kinds, including scientific details.

The dynamism of the online gaming has been possible with the use of technology, allowing the quick and accurate resolution of disputes thanks to the search for information from digital platforms in the face of the easier use of software and hardware. So, AI enables CDD and Know Your Customer (KYC) systems to operate at a faster rate and with greater depth and reach. The application of technology in the sport industry has this important reason for being. The necessity for these would need to be at adequate levels in view of the current expectation of quick solutions that the development of information technology has gradually driven and, with that, the dynamization of the world economy.

AI is evolving to such an extent that it was able to predict the emergence of COVID-19, nine days before the World Health Organization issued an alert about its occurrence in China. An AI start-up detected the disease and to which locations it would travel. Canada-based start-up BlueDot's technology correctly predicted that the disease would reach Bangkok, Seoul, Taipei, and Tokyo. The technology predicted the COVID-19 spread based on another risk factor — the issue of airline tickets — because the Chinese government had not provided much

information to the global health authorities. BlueDot was founded by Kamran Khan, an infectious disease physician who worked in hospitals in 2003 during the outbreak of the disease that became known as SARS, similar to COVID-19. With 40 employees, BlueDot was created in 2013 and investments totaling USD 9.4 million (Agrela, 2020).

As in other areas, AI has been widely used, even for obtaining judicial decisions, given the notorious and persistent delay in resolving conflicts. AI should be encouraged in activities involving large monetary transactions, marked by confidentiality and prodigious criminal activity, such as gambling. Thus, it is important to enable online platforms to efficiently identify and collect data from a great range of external sources (watchlists, sanction lists), and create a factual profile of wagers and bettors. It seems prudent to recognize valuable owners of bettor entities by using external data faster and more efficiently. The incorporation of AI within an AML system helps in adding speed and efficiency, avoiding false positives, which is the result of incomplete or inadequate data or oversensitivity of AML steps. Accumulating and reconciling customer data across internal systems can remove replication and errors and intensify the density of AML measures among wagers and bettors. In fact, AI automatically enhances dubious activity reports with appropriate data from customer risk profiles or data from external sources, generating a significant transformative effect to the level of noise generated during the AML processes.

AI assists online entities to provide greater insight into the transaction patterns of wagers and bettors and enables them to remove incorrect and invalid alerts, which makes the process costly for online providers and inconvenient for customers. In many instances, repeated tolerance of unreasonable practice, already known for some time (applying the use of machine learning), can undermine the belief in online transactions based only on the "good practices" of the market. Due to the extraterritorial nature of online games, the intense and rapid international legal cooperation for the detection, prevention, and prosecution of crime assumes relevance. AI systems provide several benefits, especially in relation to the automation of repetitive or common online transactions, providing greater agility and precision. However, the impacts that new technologies have had on society also raise a series of questions in the regulatory field.

However, the online gaming sector should be regulated aiming to stimulate the formation of a favorable environment for the development of technologies in AI, creating, even with public consultation, a true

national policy for the theme. Strongly driven by rapid technological development, AI is increasingly present in people's lives, corporations, and governments, and is considered a new technological frontier with the potential to leverage new growth fronts. Research by the consulting firm Accenture, which studied the impact of AI in 12 developed economies, reveals that AI could double annual economic growth rates in 2035 by changing the nature of work and creating a new relationship between man and machine. The impact of AI technologies on business is projected to increase labor productivity by up to 40% and enable people to make more efficient use of their time (Accenture, 2016).

The prediction is that AI will increase productivity by up to 40% and allow people to optimize their time. However, the amount and the complexity of online transactions still have to be considered, especially in the gaming sector. Due to its strategic importance for economic and social development, it is necessary to have articulate ideas and efforts to facilitate the formation of an environment favorable to the implantation of a technological ecosystem that incorporates this new growth factor in several jurisdictions, through establishing ethical standards for the use of AI; promoting inclusive and sustainable growth; improving the quality and efficiency of services offered to the population; stimulating public and private investments in research and development of AI; promoting cooperation and interaction between public entities, the public and private sectors, and among companies; developing strategies to increase the exchange of information and collaboration between specialists and national and foreign institutions; stimulating research and innovation activities by science, technology, and innovation institutions; developing of mechanisms to foster innovation and digital entrepreneurship, with tax incentives aimed at companies that invest in research and innovation; training of professionals in the field of technology in AI; and promoting a fair digital transition with the mitigation of the adverse consequences of AI for the online market.

Conclusion

It is not acceptable to possess a seemingly robust and aggressive system against money laundering when a sector that is completely vulnerable to all sorts of criminal practices still exists. Hence, a justified reflection must be taken from the moment the illicit funds migrate to "untouchable" sectors. To avoid the use of gambling as a means for money laundering, tools

must be established to allow proper regulation of gambling houses, including the imposition of sanctions when they are negligent in preventing money laundering. It is important to monitor their activities through the implementation of an accurate CDD, which monitors the performance of customers following international standards (i.e., a USD 10,000 limit) as a framework for a more detailed evaluation. This limitation should be considered regardless of the type of transaction made.

International cooperation between regulators is extremely important because it allows for the exchange of relevant information regarding online gambling activities. The exchange of information about experiences involving money laundering has proven to be a valuable way to detect, prevent, or counteract money laundering. Thus, it is important to use certain mechanisms to exchange such information, including the following:

(1) The adoption of an internal and permanent monitoring of customer activities, regardless of who they are, PEP or not PEP, using AI;
(2) Constant internal and external training of employees;
(3) Designation of an employee or a group of employees to be in charge of monitoring the day-to-day operations of these gambling houses;
(4) Providing detailed information when demanded (such as name, address, identity, and activity), even when systems are used for automatic data; and
(5) Submission to civil punishment, irrespective of the criminal, through an administrative procedure managed by the FIU in the event of a breach of the duty to monitor as established by law and regulatory norms.

Thus, it is important to enable online platforms to efficiently identify and collect data from a great range of external sources (watch lists, sanction lists) and create a factual profile of wagers and bettors. It seems prudent to recognize valuable owners of bettor entities by using external data faster and more efficiently.

Lastly, it is worth mentioning that the use of algorithms must be unassailable in their ethics and solidity. The principles of neutrality and transparency must be guaranteed, but the question arises as to how and by whom this guarantee should be provided. It is necessary to know whether the State, a third-party certifier, or the invisible hand of the market would be in charge of this task. For Roquilly (2019), AI is attractive because of its usefulness if certain conditions are met, as long as there is repulsion

from its falsely divinatory character. By clarifying the present with a better understanding of the past, justice and its actors can build a future less fraught with anxiety.

The General Data Protection Regulation (GDPR 2016/679) was adopted on April 14, 2016, by the EU and, after a two-year transition period, became applicable on May 25, 2018, in addition to Norway, Iceland, and Liechtenstein (European Economic Area [EEA]). As GDPR is a regulation, not a directive, it does not require national governments to pass any legislation that admits it and that is directly binding and applicable to all members of the EU. It is, therefore, a regulation on data protection and privacy for all individuals in the EU and the EEA. It also addresses the export of personal data outside the EU and the EEA. The GDPR's main objective is to control personal data of citizens and residents and to simplify the regulatory environment for international business, unifying the regulation in the EU. In addition, it has served as a reference for the protection of private data.

Replacing the Data Protection Directive (Directive 95/46/EC) (Filho, n.d.), the regulation contains provisions and requirements regarding the processing of personally identifiable information from data subjects in the EU. Business processes dealing with personal data must be built with data protection by design and by default, which means that personal data must be stored using pseudonymization or complete anonymization and use the highest possible privacy settings by default so that the data are not publicly available without explicit consent. It also cannot be used to identify a subject without additional information stored separately. No personal data can be processed unless it is done on a legal basis specified by the regulation or if the controller or data processor has received explicit and optional consent from the data owner. The data owner has the right to revoke this permission at any time.

Despite dealing with cultural heritage focused on works of art, Denis Williams' thinking (quoted in Cummins, 2006) is pertinent here in stipulating that "the destruction and removal of our cultural heritage will not cease until everyone sees it as a personal affront. It would not be enough, for an analysis of the theme, the adoption of isolated measures, without a global concern."

The importance of a decision cannot be measured by a numerical question alone. In fact, it transcends the institutions themselves and reflects, at its core, how people conduct their lives. Therefore, as a first conclusion, in discussions about the need to reform the relevant

legislation, disagreements as to the direction to be taken should be avoided. Trends in embracing an extreme form of regulatory freedom do not necessarily mean adequate protection of vital assets. Existing laws alone do not meet the evident aspirations and challenges of our time if, in their context, the practice leads to a ethically gray and dangerous field. That is why it is necessary to fill gaps since the common law, to a large extent, has not been sufficient to face the issue in the face of the exponential increase in technology in our lives and worldwide. Online casino games, like lotteries and sport, are global activities prone to criminal activity and money laundering because of the large sums of money channeled into them. If vulnerabilities and anonymity persist in these areas, the risk of exploitation by organized criminals will continue to grow.

Several different international and national initiatives are being put forth in the war against money laundering and the financing of terrorism. International treaties, supplemented by recommendations from foreign multilateral organizations, along with recurring discussion meetings, have all sought to improve the global system of enforcement to curb these serious crimes. Now it is time to turn to effective enforcement in the sector under study: online gambling. It is time for an aggressive policy to allow its discovery and its eradication. A domestic prohibition of Internet gambling would not likely have an effect on Internet betting as a money laundering platform because many jurisdictions have legalized Internet gambling. Thus, international cooperation on this issue must be encouraged although it is a difficult task. The legalization and regulation of Internet gambling would be a better solution to avoid money laundering, with the use of AI. Demanding and analyzing secure records from online gambling providers with profound and specific evaluations of individuals (name, address, identity, activity, fingerprint, gains or losses arising, games played, photo ID) would be already relevant, better if that information can be provided to government enforcement agencies.

Thus, well-regulated online casino activity would no longer become an effective vehicle for money launderers because all gambling transactions could be recorded and readily traceable.

References

Abovitz, I. (2008). Why the United States should rethink its legal approach to Internet gambling: A comparative analysis of regulatory models that

have been successfully implemented in foreign jurisdictions. 22 *Temple International & Comparative Law Journal*, 22, 437–438.

Accenture (2016). Artificial intelligence is the future of growth. https://newsroom.accenture.com/news/artificial-intelligence-poised-to-double-annual-economic-growth-rate-in-12-developed-economies-and-boost-labor-productivity-by-up-to-40-percent-by-2035-according-to-new-research-by-accenture.htm. [Accessed 20 July 2021].

Agrela, L. (2020). EXAME. *Inteligência artificial previu epidemia do coronavírus da China*. https://exame.abril.com.br/tecnologia/inteligencia-artificial-previu-epidemia-do-coronavirus-da-china/. [Accessed 20 July 2021].

Bana, A. (2011). Online gambling: An appreciation of legal issues. *Business Law International*, 12, 335.

Betti, F. A. (2000). *Aspectos dos crimes contra o sistema financeiro no Brasil* — comentários às Leis 7.492/86 e 9.613/98. Belo Horizonte: Del Rey.

Blanco, K. A. (2019). Insight: FinCen has eye on sports betting, crypto money laundering risks. https://news.bloomberglaw.com/us-law-week/insight-fincen-has-eye-on-sports-betting-crypto-money-laundering-risks. [Accessed 18 July 2021].

Blankenship, M. (2008). The Unlawful Internet Gambling Enforcement Act: A bad gambling act? You betcha! *Rutgers Law Review*, 60, 485.

Caeiro, P. (2005). *Branqueamento de capitais*. Manual distributed in a course sponsored by the OAS and the Brazilian Ministry of Justice and presented to Brazilian judges and prosecutors on October 17–21, p. 4.

Cummins, A. (2006). In B.T. Hoffman (ed.), *The Role of the Museum in Developing Heritage Policy. Art and Cultural Heritage. Law, Policy, and Practice*. New York: Cambridge University Press, p. 47.

De Sanctis, F. M. (2014). *Football, Gambling, and Money Laundering. A Global Criminal Justice Perspective*. Cham, Heidelberg, Nova Iorque, Dordrecht, Londres: Springer.

——— (2013). *Money Laundering through Art: A Criminal Justice Perspective.* Cham, Heidelberg, Nova Iorque, Dordrecht, Londres: Springer.

Dipp, G. (2004). Interview. https://www.conjur.com.br/2004-nov-03/legislacao_atrapalha_combate_lavagem_dinheiro. [Accessed 18 June 2021].

European Commission (n.d.). Online gambling in the EU. https://ec.europa.eu/growth/sectors/gambling_en. [Accessed 20 July 2021].

FATF (2009a). Vulnerabilities of casinos and gaming sector. https://www.fatf-gafi.org/media/fatf/documents/reports/Vulnerabilities%20of%20Casinos%20and%20Gaming%20Sector.pdf. [Accessed 15 July 2021].

FATF (2009b). Money laundering through the football sector. Report. http://www.fatf-gafi.org/publications/methodsandtrends/documents/moneylaunderingthroughthefootballsector.html. [Accessed 20 July 2021].

Filho, R. (n.d.) *A Diretiva Europeia sobre Proteção de Dados Pessoais — uma Análise de seus Aspectos Gerais*. http://www.lex.com.br/doutrina_24316822_A_DIRETIVA_EUROPEIA_SOBRE_PROTECAO_DE_DADOS_PESSOAIS__UMA_ANALISE_DE_SEUS_ASPECTOS_GERAIS.aspx. [Accessed 20 July 2021].

FinCEN (2008). Recognizing suspicious activity — Red flags for casinos and card clubs. https://www.fincen.gov/resources/statutes-regulations/guidance/recognizing-suspicious-activity-red-flags-casinos-and-card. [Accessed 22 July 2021].

FinCEN (2012). Suspicious activity report in the gaming industry. https://www.fincen.gov/sites/default/files/shared/GamingIndustry508March2012.pdf. [Accessed 22 July 2021].

FinCEN (2019). Guidance for convertible virtual currencies. https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf. [Accessed 18 July 2021].

Fox, A. (2012). On-line Gambling in the Internal Market Report. https://www.europarl.europa.eu/doceo/document/A-7-2013-0218_EN.pdf. [Accessed 23 May 2022].

Gleny, M. (2008). *McMafia: Crime sem fronteiras*. Lucia Boldrini Translation. São Paulo: Companhia das Letras, p.17.

Kindt, J. W. and Joy, S. W. (2002–2003). Internet gambling and the destabilization of national and international economies: Time for a comprehensive ban on gambling over the world wide web. *Denver University Law Review,* 80, 111.

Mills, J. (2000). Internet casinos: A sure bet for money laundering. *Dickinson Journal of International Law*, 77, 83.

PR Newswire (2021). Global Online Gambling Market Report (2021 to 2030) — COVID-19 and change. https://www.prnewswire.com/news-releases/global-online-gambling-market-report-2021-to-2030---covid-19-growth-and-change-301300847.html. [Accessed 18 July 2021].

Richet, J-L. (2013). The secrets of online money laundering. https://www.technologyreview.com/s/520501/the-secrets-of-online-money-laundering/. [Accessed 21 July 2021].

Roquilly, C. (2019). The conversation. *Justice prédictive, entre séduction et répulsion*. https://theconversation.com/justice-predictive-entre-seduction-et-repulsion-122805. [Accessed 20 July 2021].

https://doi.org/10.1142/9781800612839_0005

Chapter 4

Not a Game: The Need to Harmonize a Global Regulatory Approach to Combat Money Laundering via Virtual Assets in Massively Multiplayer Online Games

Mikhail Reider-Gordon

Introduction

Commensurate with the growth of massively multiplayer online games (MMOs), the conversion of game-related virtual assets (VAs) to real money has provided an environment ripe for money laundering. With the development of much more sophisticated game assets tokenized and backed by cryptocurrencies, and virtual exchange platforms that work across thousands of games, the time has come to designate the MMOs and their related exchange platforms virtual asset service providers (VASPs) and treat them correspondingly within national anti-money laundering regimes, consistent with the FATF guidance.

Massively Multiplayer Online Games Exploited by Launderers

In 2007, a quick query on eBay using the search term "World of Warcraft" (WoW), an online game, resulted in 5,000 items, all digital, found. On the first page of the available items was a "Dread Warrior" with a variety of

magic devices associated with the game's character and skill sets consistent with a fairly mature player. The price to purchase this conjured character someone had spent time creating was USD 1,600. To the winner of the auction come instructions for the transfer of the character to the purchaser's server. Fourteen years on, in 2021, the most expensive in-game "skin" — customization of an online game's characters or items — sold for USD 150,000 cash (Kotwani, 2021).

The Financial Action Task Force (FATF), the inter-governmental body that establishes standards to combat global money laundering and terrorist financing (AML/TF) defines a virtual asset (VA) as a "*digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes*" (FATF, 2019a, p. 13). For the past two decades, the risk of money laundering has developed commensurate with the growth of VAs within online gaming environments. In this article, examination is conducted specifically of money laundering risks via VAs in massively multiplayer online games (MMOs), arguing that with the evolution of forms VAs are taking within such settings, MMO's must now be classified as VASPs and treated correspondingly within national anti-money laundering regimes, consistent with FATF guidance (FATF, 2019a). With the current lack of harmonization of AML/TF regulations across jurisdictions with respect to online gaming, VAs and VASPs have created an environment that is actively being exploited by criminals, including transnational organized criminal enterprises, and state actors with malintent. Lack of understanding of online gaming has contributed to slowness by regulators to classify MMOs as VASPs, giving rise to unregulated platforms dedicated to brokering high-volume, high-dollar sales and trades of VAs, serving as vehicles for laundering, within the borderless Internet.

In October 2018, FATF adopted two new Glossary definitions, "virtual asset" (VA) and "virtual asset service provider" (VASP) (FATF, 2018), updating its Recommendation 15 (FATF, 2019b). It established that a VASP "*means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: (i) exchange between virtual assets and fiat currencies; (ii) exchange between one or more forms of virtual assets; (iii) transfer of virtual assets; (iv) safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and (v) participation in and provision of financial services related to an issuer's offer and/or*

sale of a virtual asset." Despite the updated recommendations, lack of understanding as to the persistent threat of money laundering in online games; lack of transparency; lack of cohesive and harmonized laws to define and include MMOs, the VAs generated for and within these games, and the exchange platforms within AML regulations has hampered progress in combating laundering in this unique sector. A 2021 draft report by FATF found that challenges remain with respect to the failure of some jurisdictions to establish or operationalize AML/FT regimes for VASPs (FATF, 2021). Technology has provided these virtual game currencies and assets a life and market of their own, but regulations designed to address ML/TF in them are minimal to non-existent.

The term "MMO" typically describes an Internet-based game that allows an unlimited or a high number of players in the game all at once. It is not unusual to find thousands of players in an MMO at any one time. The nature of VAs accumulated, traded, and transferred within MMOs, by default under the FATF's definition, means MMOs should be treated as VASPs by national AML/TF regulatory regimes. So too, third-party external platforms mediating access to MMOs and offering online marketplaces providing players opportunities to buy, sell, and trade VAs intended for these MMOs, should be regulated as VASPs as defined by FAFT.

There are genres within MMOs. For instance, two of the currently most popular games, World of Tanks (WoT) and League of Legends (LoL) have thousands of players from around the world, but an individual player can only play with a handful of other players at any one time. MMOs encompass Massively Multiplayer Online Role-Playing Game (MMORPGs), those games with a role-playing element to them, and Multiplayer Online Battle Arena (MOBAs) games, of which LoL is one. Arguably, one of the most popular MMOs, WoW (launched in 2004), was also one of the first of these online games to struggle with illicit activity arising from its in-game currency, "Warcraft Gold" (itself a VA), and as such provided early warning that VAs as in-game currencies, virtual skills, paraphernalia, characters, and appearances, also provide a near-anonymous and difficult-to-detect vehicle through which money laundering can occur. As players progress through levels of play within WoW, the game is designed to 'test' them with 'challenges' (feats for their virtual characters to accomplish), for which, if they meet the challenge, they are rewarded with additional skills and properties useful to continue advancement in the game. Within only a few years of the WoW's introduction to the marketplace, players recognized that characters who had acquired

rarer skills at higher levels (typically attained through greater hours played) could be traded or sold for real-world money (real money trading or "RMT"). In the fall of 2007, a player sold for RMT their WoW character equipped with rare skills for nearly USD 10,000. While the company behind WoW, Blizzard Entertainment, would go on to ban that particular player's account, it was clear evidence the real world had identified not only a new way to generate RMT from virtual settings but also that players would begin to test the limits of asserted ownership under End-User License Agreements (EULAs) or intellectual property over VAs generated or enhanced by them within these MMOs.

Virtual Asset Platforms Raise ML Risks

VAs within MMOs have continued to develop in sophistication, giving rise to platforms dedicated wholly to brokering sales and trades within and across MMOs for an ever wider range of these digital assets. Of the more popular forms of VAs to emerge within MMOs, "skins," "loot boxes," and non-fungible tokens (NFTs) pose higher risks for exploitation by money launders given the heights to which their values often rise, the anonymity behind their creation and transfer, their convergence with blockchain, and the inherent transnational nature of online games. Regulators, law enforcement, and legislators unfamiliar with the digital milieus of MMOs may struggle to understand how value is attached to items that are largely ephemeral and chiefly are valued in the context of a game or uniquely to the culture of gamers. Because of this, despite FATF having cautioned that even though VAs have been widely adopted or used by "the public," the use of VAs has been taken up by criminals for money laundering purposes and is increasingly becoming widely embraced by those engaged in criminal activity (FATF, 2020a), adoption of regulations governing MMOs had been slow. The failure to recognize just how broadly the public has embraced VAs within the online gaming space is in part owed to a lack of understanding of how central VAs have become to MMOs, and perhaps the erroneous dismissal of gaming as something reserved for children or teenagers. One of the largest platforms catering to the greater video gaming industry maintains rolling statistics forecasting the online gaming market alone may reach a value of USD 79 billion by 2025 (WePC, 2021) which belies the idea it is the reserve of children. Some three billion people are understood to be active gamers, or nearly 40% of the global population (Faber, 2021). The sheer scale of the phenomena of MMOs is

evidenced in the increase of Internet gaming traffic which reached over 127 Exabytes in 2020 (WePC).

Skins and NFTs

"Skins" in online gaming refers to digital aesthetic looks. This can be the game's overall environment, specific objects, or the appearance of a player's character or avatar. A skin can be as basic as a change to the color scheme of the game (a "palette swap"), or as complex as a new avatar with different lighting effects and animations. Typically, skins do not change the actual gameplay. Value in skins is identified in their rarity, e.g., other players cannot easily obtain a specific skin. Given their digital nature, tradability, and, often, desirability, they are a form of VA actively sold and purchased. Of concern to combating AML/TF, skins are now being created, traded, and sold as NFTs. For instance, the MMO League of Kingdoms (LoK) advertises on its site for the skins it sells, "scarcity assured by NFT" (LeagueofKingdoms.com, 2021). Skins can be found in MMOs such as Minecraft, Pokemon MMO 3D, and LoK and also in MMOs catering to e-sports leagues and teams, and are now also used as VAs for the purposes of in-game wagering, transforming MMOs into platforms for illegal betting.

An NFT is a unit of data (a cryptographic token) recorded on a blockchain, Ethereum cryptocurrency being the most popular, which provides certification that the said VA is unique. Central to the idea of the NFT is a means by which to assert and prove ownership separate and apart from copyright. Many types of digital files can be designated an NFT, and while copies of said file may be available and visible to many, only one person or entity can claim true "ownership" of the asset. This is analogous to plenty of people having a poster of Klimt's *The Kiss* on their wall, but only one individual/entity owning the original Klimt painting. They are speculative assets, but unlike real-world assets, NFTs include a feature that allows the creator (not owner) of the work to receive a percentage of the sale or transfer value each time the NFT is sold or changes hands. Despite recordation of the ultimate owner of this form of VA on a blockchain, and setting aside the obstacles to easily trace blockchain ledger activity, NFTs are easily exploited by money launders. There is nothing to prevent someone calling themselves an artist from creating and selling an NFT for a high dollar amount, and once sold, selling the exact same image again and again as new NFTs. Once an NFT is bought, it can be sold again

with traceability obscured. There is nothing to prevent would-be launders from conjuring up an NFT skin and appearing to sell it, while the exchange really takes place purely between co-conspirators allowing the sale of the skin to legitimize the proceeds of crime. These forms of VAs have realized extraordinary prices. In 2021 alone, the artist "Beeple" sold an NFT for over USD 69 million he had created via auction house Christie's; a digital *character* known as CryptoPun3100 sold for in excess of USD 7 million; and within the Ethereum-based MMO *Axie Infinity*, portions of virtual land known as "Genesis land" (and deemed rare within the game) sold for USD 1.5 million (Iredale, 2021).

Skins as NFTs and other forms of NFTs now appearing in MMOs evidence a convergence of cryptocurrencies and gaming, elevating ML/TF risks in games higher yet. While regulators have focused on Bitcoin and other blockchain virtual currencies, the IP and economic angles of in-game digital currencies and VAs have not received the same level of scrutiny. Skins at their lowest level are VAs purchased with micro-transactions, but on some platforms, even individual micro-transactions are rising to USD 100 or more. Skins within games can be used to gamble or bet. The skins become tokens by which to stake a wager, with often the skins won or earned in a game placed in a digital wallet and moved to another game that accepts wagering. Skins won can be converted to RMT via the game's marketplace or on a third-party platform dedicated to converting VAs to RMT. Anyone doubting the commercial lucre of skins need only look at one MMO alone — *Counter-Strike*, where gamers spent an equivalent of over USD 5 billion on *Counter-Strike: Global Offensive* (CS:GO) skin gambling during 2016 (Barlowe, 2017).

Skins are believed to have first appeared in games in 2012 and enterprising companies soon built market platforms to allow players to trade and collect skins. One company, Valve, identified players' tendency to seek out colorful skins for their trophy value, with rarer skins providing a means by which players could demonstrate their proficiency in the game. By making some skins rarer than others, Valve engineered a value for these skins with the rarest being highly sought after and commanding prices that rose to over USD 3,000. Skin trading as VAs became a *de facto* virtual currency, and with every trade on their platform, Valve earned a 15% transaction fee. Valve went on to develop a digital distribution platform focused primarily on online video gaming known as Steam. Steam's software provides an application programming interface (API)

"Steamworks" that developers can use to integrate some of Steam's more popular features into their games, including Steam's widely used in-game VA marketplace (Github.io, n.d.). As popularity increases, other websites have begun to use Steam's API which allows players to trade their skins on websites completely outside of the game. These websites also allow players to deposit and withdraw RMT which is convertible to skins. Many of these same sites subsequently added gambling features, recognizing the growing popularity of using this particular form of VA for onsite wagering. With the rise of e-sports (competitive gaming), these websites offered the opportunity for players to bet with skins on their favorite e-sports teams. Critically, in many jurisdictions, skin wagering is not governed by gambling laws. For instance, in Australia, skins are not considered "real money" (Institute of Games, 2018).

As with other MMO VAs, cross-platform capabilities mean that utilization of game-based VAs is not site-limited, allowing players to move their skins into digital wallets. Players can take their wallets with their skins to other sites to gamble, trade, or sell their skins. It may be difficult to imagine fraudsters' interest in items like computerized swords for a fantasy game. But these goods are often easier to obtain than physical goods, and criminals have learned that there are ways to convert them into cash. Overlapping with transactions designed to launder via VAs is a concomitant cybercrime. A common way criminals profit from digital-goods fraud is to buy the VA with a stolen credit card and then sell it for real money on a third party's site, often at a discount. The formal convertibility of a game-specific virtual currency or VA has been used as a litmus test for qualifying exchange platforms as money-service businesses (MSBs) or otherwise subjecting them to AML/TF regulations. This is an approach destined to create gaps harmful to countering laundering and threat finance as even those VAs whose developers or publishers intend for the in-game asset to have RMT convertibility are not recognized as *legal* tender. In 2010, MMO *Ultima Online's* Britannian gold was convertible to US dollars at a rate comparable to the Romanian Lei, but UO Britannian gold is not guaranteed at all by law. Many MMO publishers may state that their intention is for their game's virtual currency or assets to be closed or non-convertible, even issuing rules to this effect, but unofficially, secondary black markets have arisen in tandem with MMOs, transforming game VAs into convertible currencies. As FATF (2015) stressed, *a non-convertible characterization* (of MMO virtual currencies) *is thus not necessarily static*.

Code Has Value

In online games, every texture, model, sound, and line of code has value and can be sold separately. Nearly every element of an MMO thus contains a basis for its convertibility, limited only by someone willing to pay real money for it. Most people don't want to buy disparate parts, but the value is in those parts because they provide functionality, aesthetics, performance, social interaction, and represent time and use. One of the key characteristics of MMOs over the past decades has been the ease with which virtual economies begun within a game's environment have been able to bleed their boundaries and comingle with RMT. New earning opportunities, that is, the development of digital scarcities that can be exploited without advanced skills, have fostered methods for money laundering. In virtual worlds, scarcity is artificially created and maintained by the publishers of the MMOs, the gamers themselves, and the third-party marketplace platforms — all for the purpose of making the goods desirable. Game laborers and those savvy in these worlds can work to harvest these goods and sell them on to others who are willing to pay real money for them.

In the fall of 2019, gaming firm Valve felt compelled to halt the trading of some in-game items in its MMO CS:GO after discovering that "nearly all" (Valve Software Corp., 2019) of the trading was part of a money laundering scheme run by "worldwide fraud networks". Players in CS:GO earned loot boxes. A "loot box" is an umbrella term for virtual boxes in which one or more game elements (VAs) with various effects for use in-game, such as skins, characters, objects, even emotions, or other player enhancements, are embedded and awarded randomly to a player (for a commonly agreed definition, see UK House of Lords, 2020b). They themselves are not VAs in the pure sense as the boxes do not serve any other purpose than to be opened. It is the contents of the said loot boxes that are of potential value. Loot boxes got their start within MMOs, being an outgrowth of an early feature of MMOs randomized "loot drop" systems. They have been embedded in MMOs since at least 2004. The contents of a loot box must be "unlocked" by the player either by paying for the keys with RMT, in-game currency, or playing the game. As MMOs have grown considerably more sophisticated and the market more competitive, loot boxes have become a way to keep players more engaged and "invested" in a game. Valve became one of the first to experience widespread exploitation of the boxes. In CS:GO, players could earn or

purchase loot boxes for RMT from other players. On its site, Valve posted its reasons for halting the trade in loot boxes, stating: *In the past, most key trades we observed were between legitimate customers. However, worldwide fraud networks have recently shifted to using CS:GO keys to liquidate their gains. At this point, nearly all key purchases that end up being traded or sold on the marketplace are believed to be fraud-sourced. As a result we have decided that newly purchased keys will not be tradeable or marketable* (Valve Software Corp., 2019). Valve didn't disclose the volume of laundering occurring on Steam, but the BBC reported that hundreds of thousands of boxes and keys had been traded via Steam, with keys and boxes selling for "a few dollars each" (BBC, 2019).

Loot Boxes and Gambling

This was not Valve's first encounter with the exploitation of its games by launderers, having already several times prior been forced to limit use and abuse of the CS:GO trading system due to laundering. Valve limited trading in the past when it emerged that some traders were, in effect, using items as gambling chips. It has also stopped players in the Netherlands and Belgium from opening loot boxes following rulings that the mechanism violated local gambling laws. In 2018, the Netherlands Gaming Authority (NGA or *Kansspelautoiteit*) imposed an administrative order upon and fined game publisher Electronic Arts Inc. (EA) and EA Swiss SARL for violating the Betting & Gambling Act [*Wet op de kansspelen* (BGA) Geldend van 28-07-2018 t/m 31-03-2021]. Specifically, the NGA ruled that certain iterations of loot boxes EA offered in its FIFA-themed MMO contravened national gambling legislation. The District Court of the Hague upheld the NGA's decision after EA challenged it, ruling the NGA had grounds for its decision predicated on having correctly identified EA's loot boxes in this particular MMO as "games of chance" (NGA, 2018). The Court specifically cited that when loot boxes can be played as a stand-alone game, then they were not manifestations of a player's skills, as players have no control over the contents of the boxes, transforming them into games of chance. Players in EA's game could purchase and win items of not insignificant value and, once won by chance, could then trade the VAs from the boxes within the game's internal transfer market as well as selling on the black market. The Court explicitly called out that the VAs awarded in the loot boxes represented real-world economic value as they

could be converted into RMT. Under existing Dutch law, there already existed precedent for subjecting VAs to real-world tests. If the VA has a demonstrable real-world value, property laws and regulations can and should be applied (see decision in *Runescape* ECLI:NL:HR:2012:BQ9251, wherein the Supreme Court of the Netherlands applied criminal robbery laws to the theft of VAs in the MMO *Runescape* owing to the VAs holding "demonstrable real-world value").

The NGA identified standards to differentiate loot boxes that rise to a violation under Dutch gambling laws (contents transferable) (NGA, 2018), but restricted its analysis only to the manner in which VAs were made available to players, using betting laws to reign in the format of delivery, but not to address the larger question of VAs facilitating money laundering. If illegal gambling is the predicate crime, money laundering follows. Yet the Dutch court did not seek to address this element despite having identified these VAs within an MMO as possessing real-world transferable value. Lastowka (2010) has argued that VAs are property subject to property laws, but identified the inherent challenge of criminalizing virtual world exploits of these properties.

Some other countries have adopted approaches similar to the Netherlands, currently criminalizing VAs only within narrow contexts. In 2018, the Belgian Gaming Commission reviewed loot boxes in four MMOs to assess whether the boxes were subject to the Belgian Gaming and Betting Act of 7 May 1999 (Gaming Commission, 2019). Despite their subsequent report observing that within the MMOs reviewed, "*it seems that unlimited amounts of money can easily be deposited into a player's account, the easy anonymous payment method is done using codes*" (Gaming Commission, 2018, p. 7). Having come to the conclusion that paid loot boxes were illegal, even recommending criminal prosecution (Gaming Commission, 2018, p. 17), they banned paid loot boxes under the Gaming and Betting Act but did not address the inherent crime of money laundering that flowed from the identified gambling. Ultimately, Valve removed its loot boxes while other publishers have altered their games to comply with specific jurisdictions. But Juniper Research in 2018, after the NGA decision, forecast loot boxes and skins gambling in online games to be growth sectors, anticipating spending on these two uses of in-game VAs to rise to USD 50 billion by 2022 (Juniper, 2018).

Lack of harmony in the treatment of MMOs and third-party game VA platforms as VASPs across jurisdictions creates loopholes easily exploited by criminals. Britain's Gambling Commission has stated that its policy is

to acknowledge "*where in-game items can be traded or exchanged for money or money's worth outside a video game, they acquire a monetary value and are themselves considered money or money's worth*," but only to prohibit or require a gaming license under Britain's Gambling Act 2005 "where facilities for gambling with tradable in-game items are offered to British consumers" (UK Gambling Commission, 2017). This policy was established despite acknowledging in the same report that it understood VAs range in form and are well-integrated into online games. The Commission accepted the publisher's explanation that in-game VAs are provided within the games which they *intend* to be "closed-loop" systems; that is, the VAs aren't supposed to be exchanged for RMT either with other players or via third-party platforms (UK Gambling Commission, 2017). However, even the Commission itself expressed incredulity at publisher's claims that their systems are not intentionally designed to be open and that players only "occasionally" exploit game networks to buy and sell VAs (Gaming Commission, 2017, p. 6). Publishers have told the Commission that they rely upon their EULAs Terms & Conditions to forbid converting in-game VAs to RMT as a form of policing, but the Commission found the "*volume, variety and sophistication of websites advertising opportunities to exchange in-game items for cash, indicates that to term such circumvention of regulation as 'occasional' risks understating the extent of this issue*" (Gaming Commission, 2017, p. 6). Nonetheless, the Commission concluded that only in circumstances where "facilities for gambling are offering using such items (as VAs) is a license required," likening the items in that context to that of casino chips. The Commission stated it had not concluded a "persuasive case" for any further regulation, continuing to allow players to purchase loot boxes with RMT, including those with skins, and for loot boxes to remain outside of the country's gambling regulations (earning it the opprobrium of the House of Lords in its report on the harms of gambling) (UK House of Lords, 2020a).

New Zealand, in its analysis of loot boxes in online games, also concluded that the boxes, VAs themselves, and their VA contents did not meet the standard of gambling as defined under their Gambling Act 2003. As observed above, not all regulators may fully appreciate how these VAs can serve as criminal devices. As the regulator responsible, the (NZ) Department of Internal Affairs licensing compliance manager wrote in a published email "Gamers do not purchase loot boxes seeking to win money or something that can be converted into money" (Millward, 2017).

China imposes restrictions on the sale of loot boxes and is one of the few countries to do so. But while it has banned using virtual currencies to purchase real-world items, it has not outlawed the reverse. Once a VAs is purchased, sale or trade for RMT on a VASP outside of the borders of China and not regulated by Chinese authorities becomes possible. Japan and South Korea ask game publishers/developers to self-regulate but admit (Hood, 2017) that plenty of RMT is continuing to be generated and moved outside of the MMO environments. South Korea taxes any VAs exchanged for RMT, deeming it income and effectively legitimizing RMT in online gaming. Singapore has legislated against loot boxes under its Remote Gambling Act, but despite defining "money's worth" to mean "any thing recognised as equivalent to money…includ(ing) virtual objects" (Remote Gambling Act, 4(1)), specifically excludes from the regulation third-party platforms that develop, offer, and accept "virtual currencies of their own which can be used to buy or redeem other entertainment products such as games of other developers," e.g., platform's like Valve's Steam (Singapore Parliament, Remote Gambling Act Second Reading, 2014). France, Germany, Poland, Sweden, and the greater EU have opted not to legislate this form of VA found in MMOs under their respective gambling regulations. Not one of the jurisdictions that have considered regulating loot boxes mentions the threat of money laundering via VAs in any of their analysis of the phenomena. This, despite the EU's 5th Money Laundering Directive (5MLD) specifically defining "property" with respect to money laundering as "*assets of any kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible…*" (5MLD, Article 3(3)). Criminals of all sorts use loot box keys because they have a consistent price across platforms like Steam. The consistent pricing transforms this VA into a base currency ideal for money laundering.

History of Laundering in MMOs

To adequately address the current scale of laundering risks within MMOs, it is useful to briefly review the history of fraud and laundering that has occurred within these specific online game environments. To understand what has gone before is instructive in formulating responses to a phenomenon that, while constantly growing, remains underappreciated by legislators who have failed to incorporate FATF's guidance on VAs and VASPs into national AML/TF frameworks. As Lehdonvirta (2005) observed,

"A key feature of virtual worlds is that they are persistent: they continue to evolve even as the user logs off."

The precursor to the MMOs of the present was LucasArts' *Habitat* created in the late 1980s. This was the first virtual "world" that allowed users to view an artificial world in near real time (Morningstar and Farmer, 1990). The game was laid on top of a standard commercial online service, so it was subject to delays due to the constraints of upload/download speeds at the time. Despite the time delays, *Habitat* did allow its users to interact with one another in a simulated world — communicating, playing, mingling, and forming groups for self-governance, business, and even founding religions. As personal computing was in its infancy, what evolved from the universities and research labs with the most sophisticated computing systems were multi-user dimensions (MUDs). A MUD was a multiplayer computer game that combined elements of role-playing (MUDs were inspired by the real-world game Dungeons & Dragons with a social chat room or Internet Relay Chat channel (IRC)) where discussions between participants occurred in near-real time (unlike bulletin boards or blogs where information was posted and others responded to postings over time). Early MUDs were text-driven and users had to rely on reading descriptions of the actions, atmospheres, and events around them. MUDs also included non-player characters (NPCs) which might be programmed by the host to be computer-controlled to act or react to certain actions the players took. This was again the precursor to the modern video game where a player might have to battle a creature in order to gain extended play or ascend to the next level of the game. By 1996, the company 3DO had released the first three-dimensional MUD: *Meridian 59* (Reynolds, 2003).

Parallel to these early MMOs, as far back as the 1980s, was the practice of trading in-game currencies, characters, and items for RMT. Eye-on-MOGS was the first site to tackle the comparison of virtual currency sellers, offering a list of rates they paid for in-game currencies (Eyeonmogs.com, 2005). They offered the opportunity to convert real-life earnings into virtual-gold and platinum, MMO *Eve Online* currency, or credits depending on one's inhabited virtual world. MMO currency exchanges emulated foreign exchange sites. A notable entry was GamerPrice, which deployed bots offering real-time price results. The largest and most successful of the MMO exchanges, IGE, at one time served as the official currency exchange house for 19 different virtual world currencies and offered RMT wire transfer services. In later years,

prior to closing its doors, IGE transferred its operations to the Philippines due to increasing legal pressure from game operators in the U.S., but the move did not deter savvy users from converting their VAs, including in-game currencies, into RMT (Reider-Gordon, 2012, p. 12). Some MMO VA exchange houses offered gift certificates in addition to the standard currencies. Most offered credit card transactions, and some accepted eChecks. In 2007, Newsweek reported that there were over 200 companies in South Korea alone working in RMT-virtual currency exchange, with total yearly turnover somewhere between USD 83 and USD 415 million (Bennett, 2007). Chen *et al*. (2004) calculated US Dollar to MMO game currencies and, in certain instances, identified them to be more stable than the national currencies of some countries.

Ownership of Value

By 2001, when Castranova identified the economics and value of virtual IP in MMOs and virtual worlds, auctions and sales of VAs were flourishing on less compliant, less traceable websites (Lastowka and Hunter, 2004), generating somewhere between USD 200 and USD 400 million a year in sales (Dibbell, 2003; Leupold, 2005). In order to participate effectively and "succeed" in these games, players must gain substantial experience. In 2005, a gamer in Shanghai killed a fellow *Legends of Mir* MMO player in the real world. The killer stabbed to death a fellow online gamer who sold a virtual weapon (a "dragon sabre") they had jointly won for 7,200 yuan to another player. However, the killer alleged that the weapon was not the victim's to sell as it had only been lent to him temporarily. Authorities in China said at the time, they felt the incident moved into the real world partly because China had no laws (at that time) that covered the theft of virtual goods as when the victim had reported the theft, police told him the weapon was not real property (Li, 2005).

Under many MMO publishers' EULAs, players are not considered the property owners of VAs, as the companies who produce the games assert IP rights. The tension between asserting VAs to be intellectual property and ultimately owned by the publishers and VAs recognized as convertible *assets* by FATF and some jurisdictions that have included these VAs under their AML/TF and/or tax laws (Library of Congress, 2021) has allowed this inconsistent agreement on the nature of ownership to evade oversight under AML/TF regulations. If publishers assert their IP rights down to the individual skin level of an MMO character (a convertible asset), then it is

the publisher who must perform the full duties akin to the banker or broker of said assets, and implement AML detection programs including Know Your Customer (KYC) due diligence and the filing of suspicious transaction reports (STRs). This approach would be consistent with FATF's recent draft updated guidance on VAs and VASPs in which FATF agreed that "all of the funds- or value-based terms in the FATF Recommendations (e.g., 'property,' 'proceeds,' 'funds,' 'funds or other assets,' and other 'corresponding value') include VAs and that countries should apply all of the relevant measures under the FATF Recommendations to VAs, VA activities, and VASPs" (FATF, 2021).

MacInnes (2004) concluded that publishers who knowingly offered VAs for RMT or in other ways allowed RMT to be used for acquiring VAs in their MMOs were exposing themselves to a litany of potential legal risks, including the need to comply with banking, AML/TF, gambling, and tax laws in the jurisdictions in which their games were played. However, regulatory oversight did not rise alongside the growth in the popularity of these virtual worlds. There is surprisingly little case law in most jurisdictions that directly settles the matter of ownership, "thing of value," and the asset question.[1] In the absence of such national-level legislation or case

[1]Lastowka and Hunter (2004, p. 50) identify *Blacksnow Interactive* vs. *Mythic Interactive (2002)* as the "first dispute over virtual property" adjudicated in court although the case was ultimately dismissed. Blacksnow Interactive, a company, had set up a VA "farm" or sweatshop in Mexico paying workers to earn in the MMO *Dark Age of Camelot (DAoC)* rare game assets that could be sold to other players. Mythic Interactive, the publisher of DAoC, asserted IP rights and claimed Blacksnow as infringers. Blacksnow countersued under the doctrine of unfair business practices specifically claiming what players do with their time in-game belongs to them and asserting rights to sell VAs from the game outside of its environment; *Li Hongchen v. Beijing Arctic Ice Technology Development Co*. (2003) is believed to be the first case in China that recognized a player's virtual property rights. Li played MMO Hongyue (Red Moon) but had his VA stolen when his account was hacked. After being refused police assistance (who failed to recognize the VA as property), Li took BAITD Co to court. Beijing's Second Intermediate Court ordered Li's virtual assets restored. https://www.newscientist.com/article/dn4510-gamer-wins-back-virtual-booty-in-court-battle/; also see Nicholas Suzor (2012) for a general discussion of early legal challenges in MMO; for discussion of early US case law involving VAs, see Blazer (2006); *Bragg v. Linden Research, Inc*. (U.S.) — 487 F. Supp. 2d 593 (E.D. Pa. 2007) was one of the first tests of enforceability of a specific provision of a EULA relating to an MMO. Bragg alleged that Linden Labas violated his property rights by suspending him from the SL community without reimbursing him for the real-world value of his holdings.

law regarding the treatment of game-associated VAs as property, the application and enforcement of confiscation and related asset-forfeiture laws relating to these properties and instrumentalities of money laundering becomes problematic or impossible, and remains inconsistent with FATF Recommendation 137 (FATF, 2019a). In some jurisdictions, players could conceivably claim to not be liable for contributory or vicarious copyright infringement because they don't infringe upon the publisher's copyright by selling or trading a customized VA for RMT, as that VA will return to the game environment, just controlled by a different player. Players may violate the T&Cs of publishers' EULAs as discussed in greater detail below, but they would then stand accused of breach of contract, not for infringement of copyright, and the question of ownership would remain unsettled. US courts have tended to view players' claims that their game-associated VAs hold independent value either in and of themselves or in secondary markets — as a question only of abiding by EULAs.[2] If a EULA forbids selling on exchanges or third-party marketplaces, then *ergo* the player has breached the T&Cs of the EULA. But this is a failure to fundamentally grasp what is recognized in global AML enforcement: the emergence of these currencies and assets linked to virtual worlds *does* represent independent value given the billions of people playing MMOs around the world and the staying power the games, currencies, and other VAs have held over the past two-plus decades. The concept of control of the VA is critical to enforcement of anti-money laundering provisions, as the conversion of the asset to RMT and extraction of value from said VA via this exchange is the actual underlying act of money laundering.

Lastowka (2004) first introduced the concept of laws in virtual worlds as cases of theft, extortion, and money laundering in MMOs began to evidence how ineffective publisher's EULAs were for policing crimes

Bragg supposedly fell afoul of Linden Lab's terms of service agreement when during a land auction Bragg discovered a loophole in Linden's auction system and exploited it to acquire land without competition. Bragg already owned significant tracks of virtual land when he availed himself of the loophole in the auction to obtain more. However, rather than just disallow the newly auctioned land to be retained by Bragg, Linden Labs froze approximately USD 8,000 worth of Bragg's previously acquired SL assets and refused to restore or recompense him for them.

[2]E.g., see *Mason v. Mach. Zone, Inc*. 140 F. Supp. 3d 457, 468–469 (D. Md. 2015) and *Soto v Sky Union, LLC*, 159 F. Supp. 3d 871, 879 (N.D. Ill. 2016).

involving VAs. By 2006, an MMO had minted its first VA-based millionaire, Anshe Chung, who amassed VA holdings in Linden Lab's MMO *Second Life* (SL) that at the time were legally convertible into genuine US currency worth more than USD 1 million (Parloff, 2006). SL experienced a sudden drop in the value of the Linden, its in-game currency, with values dropping precipitously (by 9% in a single day) when a Copybot was introduced into SL raising concerns that widespread and illicit copying and selling of virtual clothing, designs, textures, skins, etc., would begin undervaluing the items (Reider-Gordon, 2010). Criminal organizations in China and Mexico had already opened "sweatshops" of sorts hiring hundreds of works to "mine" or earn and sell MMO VAs to wealthier players typically in the West (Grimes, 2006).

As Taylor (2002) described in 2000, Sony Online Entertainment (SOE) secured the cooperation of popular online auction sites including eBay and Yahoo! in order to prevent MMO *EverQuest* players from selling game characters and other in-game items for real-world profit. Up until that time, a sort of "cottage industry" had sprung up in which users were turning their online labor into offline cash. The online auction market for *EverQuest* goods, such as virtual armor, weapons, magic wands, and even entire characters, had developed into a USD 5 million industry. Although SOE succeeded more or less in putting an end to *EverQuest* commerce on eBay and Yahoo!, the prohibition was and remains largely ineffective. In fact, in 2006, the inadequacy of these prohibitions was demonstrated when a player known by the online name "Methical" discovered a coding error in the game that could be exploited for RMT. Methical rapidly learned that MMOs could be tedious in the early levels as much time and energy were needed to build up to a stage that made the game interesting. Methical began buying and selling furniture for RMT in a showroom within *EverQuest* and almost immediately began to turn a profit. In the course of doing business, Methical identified a piece of furniture from the game, a "gnomish thinking chair," that was considered exceptionally rare. Methical identified that SOE's programmers had made an error in the chair's program that allowed for it, after performing certain actions in the game, to be replicated. Methical could sell the chair, at a substantial price to a user, and then still retain the original chair ready to be sold again. Methical began to make hundreds of dollars a day exploiting the glitch in the chair code. Methical went on to unearth similar glitches in other EverQuest prized items. It was complaints from other players that drew SOE's attention to Methical's exploits. They would

ultimately shut Methical's account down predicated on violating its EULA, but not before he had made sufficient profits to afford to take his whole family on a trip to Paris.

Evolved Methods of Laundering via Virtual Goods

By mid-decade, stories piled up of frauds, money laundering, and other crimes, nearly always around their value of game VAs and their convertibility to RMT. Dibbell (2007) wrote of earning the equivalent of a full-time salary just trading MMO VAs. Other gamers identified exploits in the vein of Methical, some "mining" or extracting RMT in the hundreds of thousands before publishers closed their accounts. A Chinese court sentenced a former executive at Chinese online gaming company Shanda Interactive Entertainment Ltd. to five years in prison for virtual embezzlement as while creating the assets for Shanda's MMO *Legend of Mir II*, he and his accomplices also created USD 260,000 worth of virtual goods for themselves to sell (Fowler, 2007). As far back as 2007, the US Department of Justice had issued an unclassified report (DOJ, 2007) on Mexican drug cartels that specifically referenced how virtual worlds were being utilized by narco-traffickers to launder proceeds: "*Online role-playing games… afford traffickers a number of unique money laundering opportunities. Drug traffickers can legitimize their income through accounts established with online game companies through the following methods: Selling virtual game items to other players for a credit to their account; the game company periodically settles the account by issuing a legitimate check to the account owner/launderer for the virtual items sold in the game; Accepting virtual money in exchange for illicit drugs, thereafter receiving a legitimate check from the game company; Maintaining multiple game accounts through which they can buy items from and sell items to themselves, in a cyber version of a trade-based money laundering scheme; and selling virtual currency in exchange for real money to other players*." A few years later, SOE identified a player moving substantial volumes of money through one of its MMOs. When lawyers for the company identified the player, assuming he was attempting to acquire rare VAs, they discovered by the player's own account that he was laundering money having identified that transferring through the MMO was less expensive than his bank, converting RMT from his US account to that of his one in Russia (Reider-Gordon, 2011). So pervasive was crime in

MMO virtual worlds, in 2008, that the South Koreans established a unit in their police force to investigate in-game crimes. The Korean Cyber Crime Investigation Team fielded over 40,000 complaints — 22,000 of which involved activity that occurred in virtual worlds (Korean Institute of Criminology, 2014).

Gold Farming

Heeks (2008) traced the activity, known as "gold farming," or producing virtual goods and services for sale to players in MMOs estimating that even over a decade ago it employed "tens of thousands" of people across the developing world. Heeks tracked back commercialized gold farming endeavors to Korea at the turn of the 21st century where cybercafes were converted into "mines" to produce VAs to be sold to players across the greater market in Asia. Arguably, the concept and terminology of "mining" VAs would later translate to the mining of another form of VAs, cryptocurrencies. Gold farming was initially focused on playing to develop or harvest in-game currencies, not to enhance player skills or ranks. However, with the growth in the value of in-game VAs, mining activities expanded.

In October 2008, Seoul Metropolitan Police Agency arrested a group responsible for laundering money generated by Chinese gold farming from Korea back to the mainland. In a little over 18 months, the group wired USD 38 million from Korea to a Hong Kong paper company as payments for purchases. In return, the group took a commission of 3–5% for purchasing the virtual currency in China, reportedly produced by traditional farming, and then cashing out in the Korean market (US State, 2009, p. 16). In the US State Department report that recounted this particular laundering case, as well as others, it was prognosticated that "*players buy and sell virtual property, goods and services. Some games also allow players to convert genuine currency deposits to virtual currency and then back to real currency at fixed exchange rates. Such capabilities in virtual world games have potential implications for money laundering and other financial crimes*" (State INL). The report observed that even in those jurisdictions where AML regulations do treat some of these exchange platforms as payment providers and, therefore, subject them to AML rules and regulations, said regulations are difficult to enforce, noting due diligence and KYC requirements often do not exist for online gaming and online payment providers.

In 2017, Venezuelans desperate for money took up gold farming in the now somewhat outré MMO *Runescape*. How-to manuals were posted and Venezuelan players started harvesting some of the game's green dragons, selling the virtual hides and bones to earn *Runescape* 2007 'gold.' The game gold was traded on VA exchange platforms alongside Bitcoin and other virtual currencies (Good, 2017). Gold farming is now being replaced by automated bot farms and increasing competition to gold farming companies is coming from criminal hacker groups that break into players' and gold farmers' game accounts stealing the virtual currency to sell for real money. Gold farming and trading for RMT of in-game currencies and virtual goods aren't just continuing, they have grown increasingly complex with the introduction of NFTs in MMOs and more sophisticated.

These games' synthetic economies collide with real-world financial markets when players want to buy or sell the VAs from them. AML/TF regulations and practices, oriented still as they are to financial institutions, mean the evolution of methods of tracking money laundering in these borderless and virtual worlds has not kept pace by any measure. VAs can be absurdly priced, with artificially inflated and astronomical values placed upon them, offered on an exchange, and function as a perfect laundering method. Transactions between players, themselves often anonymous, can be faked to allow the proceeds of crime to be cleaned. This form of cyber laundering has been allowed to expand as states have failed to classify MMOs as VASPs.

Tokenizing Game Assets

With the introduction of NFTs and thus the convergence of blockchain-backed game-related VAs, another obstacle to the traceability of the origin of the VAs and the RMT for which they are sold or traded is layered on. After the MMO environments, secondary markets oriented toward NFTs specifically for gaming will increase the difficulty in detecting and tracking illicit monies moving back and forth through them. Additionally, NFTs become artwork in their own right. So, while there exist money laundering obligations for formal bricks and mortar art markets engaging in transactions over certain value thresholds (see 5MLD, Article 2(1)(c)(i), AML requirements for real-world art markets do not readily translate online to NFTs in MMOs. For example, the US Financial Intelligence Unit, the Financial Crimes Enforcement Network (FinCEN) has, as of this

writing, not yet indicated whether certain NFT market participants (e.g., creators, sellers, dealers, and marketplace operators) are or may become subject that country's AML regulations.

Companies such as Wax.io, Hoard.Exchange, and Gamekit.com help game developers integrate blockchain technology into their games, "tokenizing" and/or providing centralized platforms where users can receive full versions of games, multiple game currencies, create game NFTs, including skins for wagering, and then exchange them for skins, full games, and gaming currencies. Gamekit boasts on its home page in excess of 21 million users and of having distributed more than USD 8 million in rewards, working across multiple platforms like Steam (see https://gamekit.com). Under one of its FAQs, the site states that it requires users to provide a telephone number and an address "for regulatory purposes." However, verification does not preclude drop boxes and burner phones. Among the prizes it awards users are prepaid Mastercards, loot boxes, and cryptocurrency vouchers good for Bitcoin (BTC), Ethereum (ETH), and others. The Company's Privacy Policy states that it gathers a list of apps on users' mobile devices and statistical information about the usage of the apps. It pulls in user profiles from Google or Facebook, but a Google profile only requires a Google ID and an email address, hardly KYC. Similar large game aggregator platforms such as Steam (which calls itself a digital *content distributor*) offer users access to "30,000 games" and the opportunity to interact with "over 100 million potential friends" (https://store.steampowered.com/about/). OpenSea.io, calling itself the "world's first and largest" NFT marketplace, claims it has in excess of one million NFTs and maintains a special section devoted just to NFTs for virtual worlds (https://opensea.io/collection/virtual-worlds). Payments are made in cryptocurrencies taken from buyer's cryptowallets. This is an example of convertibility, as a game-specific NFT made for and sold for an MMO on the OpenSea marketplace is now a VA outside of the MMO itself.

But what if the claim by the player purchasing the item is that it is destined to be used *within* the game? Here is where the gap in treatment of MMO VAs and VASPs catering to MMOs for the purposes of money laundering regulation becomes starkly evident. As Cloward and Abarbanel (2020) questioned, using New York State financial services law [§ 200.2(p)(1)(i)] as their example, *regulation governing virtual money businesses excludes specifically* "*digital units that…are used solely within online gaming platforms*". But does that mean a VA that can be used

externally to the MMO then constitutes a virtual currency under the financial services law? This is one example at a regional level no less, but one that underscores, in the absence of categorizing all MMOs as VASPs, and thus the in-game-associated VAs as *potentially* virtual currencies convertible to RMT, regulation and oversight go wanting, opening up opportunities to launder money. FATF recognized that P2P transfers are often conducted among users (of MMOs) and that these game currencies linked to virtual worlds "*are not confined to a particular online game, as they can be traded in the real world and be converted into real currencies*" (FATF, 2010). FATF case studies (FATF, 2010) have found prepaid cards being used by gamers around the world in order to fund their MMO accounts and subsequently withdraw their virtual currencies via conversion to RMT.

With tens of thousands of games being loaded and removed from MMO exchange and game platforms such as Steam on a near-daily basis, tracking the legitimacy of publishers becomes another challenge when seeking to combat laundering via these online settings. Low-complexity games are relatively easy to program and place on game distribution sites. It is not uncommon for one distributor to initially host the game on their "asset store"[3] priced at a modest sum only to then sell it to a larger platform like Steam where the price can be quadrupled by the programmer. Once uploaded, programmers/publishers can set the price for each game, allowing would-be launderers to set immoderate pricing. Examples of ersatz electronic whack-a-mole games being sold on Steam for USD 200 per use have been identified. The ultimate beneficial owners (UBOs) of the programming companies are anonymous, and because the game has been moved from platform to platform, the recipients of money paid out for these seemingly overpriced games or their VAs remain obscured.

MMO marketplaces such as Steam allow people to trade in-game items for real money of which both Valve and the developer take a cut. However, the overpriced games will have few customers if any, or the game will not be supported, and the developer will have vanished with cash in hand. Games initially launched on one platform may be in one

[3] See, e.g., Denmark-based online "Asset Store" Unity Store advertises that game designers and programmers can "just submit your awesome creations to the Asset Store and we'll take care of the rest. You can actually make enough money to fund your life…!" https://unity3d.com/asset-store/sell-assets.

jurisdiction, but as they move across platforms, so too do they move across borders, complicating enforcement. In one instance, users were able to upload over 5,000 items on Steam's marketplace for sale — all supposedly intended for use in a single game — before the platform was alerted and removed it. But, not before a fair bit of money cycled through for never-before seen items for a game no one had heard of hitherto. Items offered for any one game can sell in a package of VAs for USD 100–200. In a recent investigative report, the British newspaper *The Independent* and a cybersecurity firm posed as players of customers on MMO *Fortnite* (a game that is free to play and readily found on all major gaming platforms played by an estimated 200 million players globally), looking to purchase the games' in-game virtual currency "V-bucks" in order to purchase VAs for their characters. The journalists identified criminal operations being conducted around the globe in Chinese, Russian, Spanish, Arabic, and English, whereby threat actors were using stolen credit cards to purchase V-bucks and then selling them in bulk on the dark web at a discounted rate to players. The money launders also advertised the discounted virtual currency on social media platforms such as Instagram and Twitter. Publisher Epic Games, according to the undercover report, appeared to have minimal security measures in place to thwart such criminal activities (Cuthbertson, 2019). A VASP's risk assessment should take into account all of the risk factors that the VASP "including the types of services, products, or transactions involved…VA products or services that facilitate pseudonymous or anonymity-enhanced transactions also pose higher ML/TF risks, particularly if they inhibit a VASP's ability to identify the beneficiary" (FATF, 2019a, at 27–28).

The additional option of in-game assets generated or purchased being now embedded with blockchain-based technology (NFTs) will move the ownership of specific VAs to players. NFTs are the equivalent of certificates of authenticity. It is the formalization of the commodification of game-related VAs. This fundamental change further removes power from publishers of MMOs in that by virtue of the decentralized nature of blockchain, authority and enforcement of EULAs will be reduced or non-existent with respect to VAs being converted to RMT. Specifically, non-public ledgers for these NFTs allow for total obfuscation of the UBOs. For example, Vulcan Verse, a start-up aimed at offering gamers the ownership of the VAs they create or customize for online games, moved to an NFT-compatible platform, saying it has "*managed to increase its trading volume from approximately USD 10,000 to more than USD 6,000,000 …*

(and that) … Such an increase stems from the platform migration as well as the continued increase in popularity of NFTs" (Crypto.news, 2021). A rival platform, Wax, has written that its "target market for digital goods is a superset comprised of virtual items from video games and potentially tokenized products from consumer e-commerce" (Quigley *et al*., 2019, p. 2). Wax claims total sales of USD 140 billion with another USD 50 billion generated from the secondary games' VA market saying "*In our calculation, we add the primary sales of video games and video game items and secondary virtual item sales because the WAX Platform supports both* (emphasis added)…*the subset of products we see tokenizable is USD 1.8 trillion*" (Quigley *et al*., 2019).

Games with a play-to-earn mechanism allow users to create value through in-game activity. But, as the rewards shift to cryptocurrencies or NFTs, the new reward system enhances the previously scarce play-to-earn economy and allows direct value generation to occur in the game, and the value of each VA increases, and opportunity for money laundering via these channels also rises. Because these digital assets and the game platforms use cryptoassets such as Ethereum and the Wax Protocol to back their in-game skins and NFTs, increasing their value, user numbers are going up and additional avenues for laundering are being built faster than regulators can keep up. The markets have recognized that these game VAs are commodities in and of themselves, even if courts and regulators have been slow to recognize them as such. Gamers can now even obtain loans using their gaming VAs as collateral (For examples, see https://www.planetcalypso.com/guides/business-tradebanking/_2022; and https://farsite.online).

Levine's Boredom Markets Hypothesis (Levine, 2020) is seen clearly here. The "investments" and financial trading activities in game skins, in-game NFTs, and game-specific currencies are driven in many ways by the "lulz" and the fun to be had within the online social tribes they create. This means countering the laundering risks within these VAs is complicated by a culture that is less concerned with genuine metrics to support the valuation ascribed to these assets. These in-game VAs are fun, and thus watching and even encouraging the ratcheting up of their value is gratifying. Spurring the buying and selling of VAs at high RMT dollar amounts is as much about entertainment for many of the gamers: buy more of it and the value goes up. Unfortunately, the excitement generated within the game environment by this form of entertainment is then easily exploited by criminals seeking to launder illicit funds.

Borderless Games

As the UN Secretary-General (2019) has pointed out — and what has long been recognized by those combating cybercrime — there are no borders around the Internet, "its point of connection with the physical world happens in an existing and delimited territory of a State." In order to successfully investigate and prosecute crimes occurring online — including virtual worlds — what is needed is a cohesive international distribution of jurisdiction. But before an international law of cyberspace can be effected, a uniform agreement on defining what constitutes a VA and a VASP must be settled, and that definition must include MMOs and the platforms that support MMOs. FATF's definitions only goes so far, with too much unwritten and left to individual countries to determine. It is through this interpretative gap that less conscientious VASPs will incorporate and money launders will venue shop. Brazil's recent domestic legislation to target cybercrime is a useful guide, in that the county has anticipated future harmonization of domestic legislations by using the legal mechanism of the targeting test, which disregards the location of the servers and the nationality of the custodian company for the purposes of prosecuting cybercrimes (UN Secretary-General, p. 16).

The greatest risk with game-related VAs floating freely in cyberspace is that it is impossible to wall them off from convertibility to RMT, bestowing upon every virtual object the prospective of real-world value limited only by an individual player's intention and want of a buyer. FATF's money travel rule (Recommendation 16 — Wire Transfers) (FATF, 2012–2020) does apply to VAs, but until the agreed definition covers all VAs that have the *potential* for convertibility, the rule is ineffective. As FATF itself has observed, the private sector is currently developing various travel rule technology solutions, but there exists no common agreed-upon standard because of the "*decentralisation ethos that underpins virtual assets, there appears to be a general desire for multiple potential solutions, rather than one centralised travel rule solution*" (FATF, 2020c). FATF has also identified that of the current 195 countries in the world, only 32 jurisdictions have implemented AML/CFT regulatory requirements for VASPs and only 15 of those have included requirements consistent with Recommendation 16.

The slow progress toward adoption of the Recommendations consistent with the VA/VASP Guidance is concerning for the future success of combating money laundering in the cyber milieu that are MMOs. It can

also be viewed as an opportunity. Now is the time for countries to broaden their definition of VAs to include virtual game-related items and impose AML obligations upon both publishers of MMOs and third-party marketplaces by classifying them as MSBs and treating them accordingly. The importance of this was stressed in FATF's March 2021 Draft updated Guidance on VAs and VASPs (FATF, 2021). The Guidance makes clear that VASPs and other entities involved in VA activities need to apply *all* (emphasis added) the preventive measures described in FATF Recommendations 10 to 21. The Guidance explains how these obligations should be fulfilled in a VA context. But it does not go far enough in that, under the travel rule, the requirement to obtain, hold, and transmit required originator and beneficiary information, immediately and securely, when conducting VA transfers, the USD/EUR 1,000 threshold would miss aggregations of in-game VAs and mixing of the means by which transfers to money launderers are made, e.g., prepaid cards, cryptocurrencies, credit cards, money transfers, and digital wallets. As has been observed by Maras (2016), organized cybercriminal organizations often utilize micro-laundering, breaking up sizeable illicit proceeds into small transactions, distributed across online platforms. MMOs with their thousands upon thousands of virtual goods are settings conducive to this form of laundering. FATF has called the threat of criminal and terrorist misuse of VAs "serious and urgent" (FATF, 2019c).

According to Statista (Bucholz, 2020), Vietnam has the highest number of adult gamers per capita, with fully 94% saying they gamed at least occasionally. Countries in the developing world — aided by their younger demographics — produced more gamers with Vietnam, Nigeria, the Philippines, Thailand, Indonesia, Colombia, and Peru reporting the highest number of adults saying they played video games in a survey of 55 countries. Around 25% of Saudi Arabia's adults reported frequent online gaming. These same markets also represent countries with low or lower AML/TF enforcement, or whose efforts to combat cybercrime and money laundering are hindered by restricted resources. FIUs and national-level law enforcement need both to establish special units dedicated to understanding laundering in MMOs, including the use of NFTs in order to build expertise, afford a holistic view of this digital landscape, train not only their own people but also their financial institutions, and work across enforcement units targeting transnational organized crime and vice, as well as with counterparts in other countries.

Money laundering in the virtual space of online video games is a cross-border problem but there is no requirement of VA platforms and marketplaces to transaction monitor or report to FIUs. FATF has recently clarified its Recommendation 15 stating that "*for the purposes of applying the FATF Recommendations, countries should consider virtual assets as 'property,' 'proceeds,' 'funds,' 'funds or other assets,' or other 'corresponding value.' Countries should apply relevant measures under the FATF Recommendations to VAs and VASPs*" (FATF, 2021). However, in its review of the implementation of its VA/VASP Guidance within the private sector, it found only nascent efforts toward compliance. It observed that many of these publishers and platform companies do not have a history of regulatory oversight, and are unfamiliar with their risks and requirements (FATF, 2020b).

A decade ago, Australian gaming company My Media Gaming Network (MMGN) launched an online marketplace where gamers could sell virtual goods across multiple video games. It attracted 500,000 unique users a month, rising to a million during peak times. MMO Gaia Online enjoys 7 million unique visitors each month. Gaians create customizable avatars and virtual homes using Gaia Cash and Gaia Gold and allow users to shop at their Gold Shops, Cash Shops, and marketplaces for trading on the Gaia Exchange (Gaiaonline.com). MMOs *WoW*, *Runescape*, and *Final Fantasy* all enjoy audiences of over 2 million players. hi5, an MMO, had at one time over 50 million monthly visitors (Reider-Gordon, 2010). Sites such as China-based 5173.com, an online game trading site, were so successful in serving the sale of VAs that the local government invested in it. If these MMOs were retail banks, they'd be in the top tier for institutions by customer volume.

FATAF has called the private sector the first line of defense against ML/TF threats (FATF, 2020b), yet most of these virtual worlds offer users anonymity and are outside most government oversight. Organized criminal rings in Asia have been using them to defraud players and launder money for at least a decade now. Many may host servers in multiple countries to accommodate volumes of simultaneous global users, and many will rely upon financial intermediaries to help process electronic payments from outside the country in which they are organized, and yet few AML/TF regulations have been imposed upon them. FATF has stated that it doesn't seek to regulate the technology behind VAs and VASPs but rather those "*natural or legal persons behind such technology or software*

applications that may use technology or software applications to facilitate financial activity or conduct as a business the aforementioned VA activities on behalf of another natural or legal person" (FATF, 2019a). It is understood that not every software developer or programmer who codes or provides an application for a new VA platform is necessarily transformed into a VASP. But such publishers or programmers, if engaged as "a business in exchanging or transferring funds or conducting any of the other financial activity" using said technology for VA transactions, should be considered a VASP.

Hitherto, the manner in which publishers/programmers of MMOs and their attendant third-party marketplace platforms have dealt with their VAs being converted to RMT no longer works with the advent of the tokenization of VAs. With no standardization between virtual worlds and platforms, there is no way of knowing whether one source is making and cashing out *WoW* Gold, *Runescape* Gold, or any other in-game asset. This makes tracking transactions for evidence of money laundering extremely difficult. Playerauctions.com still converts to RMT for any number of MMOs, and while its EULA does prohibit "fraudulent" activities,[4] as Playerauctions allows its users to pay with credit cards and cryptocurrencies, for all intents and purposes, the detection of patterns of money laundering appears to be offloaded onto the banks and cryptocurrency platforms. While the company does have people identified as "risk analysts," again, it is a self-regulating environment with only contractual enforcement via its EULA. Many game developers, such as Blizzard (creator of *WoW*), prohibit converting game VAs into RMT, and for the past 20 years, these EULA-driven terms have been largely ignored by gamers. For a number of years, Blizzard filed a litany of complaints with

[4]Playerauctions, Inc. User Agreement, *Prohibited behavior: Each User hereby represents, warrants and agrees that information submitted to PlayerAuctions for display on the Site shall not: a. Contain fraudulent information or make fraudulent offers of items or involve the sale or attempted sale of counterfeit or stolen items or items whose sales and/or marketing is prohibited by applicable law, or otherwise promote other illegal activities; b. Be part of a scheme to defraud other Users of the Site or for any other unlawful purpose; c. Relate to the sale of products or services that infringe or otherwise abet or encourage the infringement or violation of any Third Party Rights; d. Violate any applicable law, statute, ordinance or regulation (including without limitation those governing export control, consumer protection)...* https://www.playerauctions.com/about/agreement/, last accessed April 9, 2021.

PayPal for individuals and companies offering RMT conversion and accepting payments for *WoW* virtual goods via PayPal. But their complaints weren't concerned with laundering; they were filed under the US DMCA[5] for IP infringement.

Verbiage in EULAs prohibiting selling virtual goods that come from the associated game is common, yet grey market RMT sites like PlayerAuctions abound. Companies can file suit for violations of their Terms of Service or for infringement, but it is an unwinnable game, another version of the "whack-a-mole" game that is played by IP owners for other types of digital content. Many MMOs such as *RuneScape*, *World of Warcraft*, *Guild Wars*, *Warhammer Online*, *Lord of the Rings Online*, and *Final Fantasy XI* strictly prohibit the use of real-world cash to buy virtual currencies, items or any other product linked with the game. *Final Fantasy XI* and *Warhammer Online* claim to have task forces dedicated to the removal of real-money trading from their games. But one of the persistent features of all of these MMOs is that they are designed to capture user's attention and get them to spend considerable sums within the game. The more VAs sold within the game's confines, the greater the revenue stream to the publisher. MMOs are often free to access; the business model relies upon players spending real money within the game — every aspect of these games is commodified.

Since the first MMO appeared nearly 30 years ago, savvy players recognized opportunities for financial gain, whether through identifying coding errors or other exploits, or through selling or trading VAs, there is money to be made. Unregulated financial transactions flourishes in these virtual worlds. Publishers and platform owners cannot have it both ways. They can't attempt to shift responsibility to the players to adhere to the EULAs and wash their hands of money laundering and other financial crimes that then ensue from the commodities they promote in their games. As McInness (pp. 47–48) rightly observes, MMO publishers need to "abandon the mindset they are providing 'just a game.'" Rather, countries and their regulators must treat all VASPs equally, meaning any publishers or hosting company that allows the trade or transfer of game-related VAs must be designated a VASP, and from a regulatory and supervisory perspective, be treated uniformly by all jurisdictions to circumvent territorial arbitrage. MMO hosts and VA exchange platforms for gamers must be

[5]Digital Millennium Copyright Act (DMCA) Pub. L. No. 105–304, 112 Stat. 2860 (October 28, 1998).

required to establish AML programs, including SAR reporting, to their home FIUs.

Detecting RMT Transactions in MMOs

Multiple researchers (Lee *et al*., 2018; Fujita *et al*., 2011; Keegan *et al*., 2010) have demonstrated that it is possible to detect the characteristics of VAs for RMT transactions in MMOs. Lee (2018) analyzed approximately 6 million transactions in a single MMO and identified unique structural nodes in user groups engaged in illicit VA conversion activities. They were able to separate out-of-game RMT transactions, including gold farming, from in-game trades between players (friends sharing VAs with one another) with specificity. This ability to monitor transactions and identify those consistent with illicit activity is akin to the AML monitoring financial institutions carry out on customer accounts. That this form of monitoring is possible is critical for regulators to understand as it negates any claims by MMO VASPs that it is too difficult or impossible to monitor for laundering in these complex virtual settings. Utilizing social network analysis, Lee (2018) identified the equivalent of 16 typologies in detecting RMT groups within MMOs and further parsed the types of RMT trades within these virtual worlds: direct and indirect. It was found that a typical illicit laundering structure consisted of a few in-game bankers and many gold farmers organized in a hierarchical manner. Bankers and brokers are divided between those in-game and those outside, based in RMT platforms, who actively advertise high volumes of VAs to potential customers and provide trusted and reliable escrow accounts or payment systems.

Additionally, researchers have recently demonstrated that tracking illicit transactions with blockchain is possible (Bellingcat, 2019) using search engines, specific BTC, and data formats on blockchain.com suggesting algorithms or bots could be used for the purposes of tracking NFT VAs by VASPs. Crypto-forensic companies have begun to offer blockchain analysis services and identification of UBOs of cryptowallets. These are private services but tell us that the capabilities exist to track and trace, meaning MMO publishers and the VA platforms that feed off game VA sales could employ similar methods for the purposes of identifying and combating laundering, if regulators required it. One of these crypto-forensic companies, Chainanalysis, has publicly stated that by its estimation over-the-counter brokers are responsible for "*facilitating some of the largest illicit transactions, with some operators set up for that purpose*

alone." Thousands of cryptoATMs have also begun to appear online allowing those with VAs to cash out without scrutiny of regulators (*Financial Times*, 2021). Blockchain was meant to facilitate transparency and traceability. Instead, it has become a key means of cybercrime.

It is instructive to look toward how underresourced countries have effectively implemented AML controls on emerging technologies. Anonymity is a unique feature of mobile phones and a clear risk factor. Most countries' KYC legislative requirements already demand that mobile operators take copies of identity documents on mobile service accounts. In doing so, these operators increase transparency and generate useful data on transactions and customers that can be shared with enforcement agencies. Back in 2015, Zambia introduced the National Payment Systems Directives on Electronic Money Issuance 2015 which covered licensing procedures, minimum capital, use of agents, consumer protection, and KYC requirements. Under the Directives, mobile money operators effectively become a reporting entity for the purposes of AML and financial intelligence. It is possible to adjust regulatory requirements to different stages of technological development and tailor them according to the risk profile of the individual services. WoW virtual gold is not unlike other tradeable virtual commodities. For instance, like EU carbon credits, WoW gold is an element in an abstract system of rules implemented as a computer program. Neither the credits nor the gold has any shape or function outside their respective systems. Both systems have a certain group of participants, and each participant has a "user account". Both credits and gold can be transferred between accounts, but creating new ones is not possible; only the operators of the system can do that. Both are thus artificially scarce. Both credits and gold can be exchanged to a national currency by selling them to another participant who finds them so useful as to be willing to pay money for them. And both are targeted by cybercriminals.

In 2018, G20 Leaders called for VAs to be clearly regulated for AML/TF purposes. In June 2019, the FATF set the first-ever global standards in this area. Since then, the G20 has focused its attention on so-called stable coins (FATF, 2020b). The effort expended on cryptocurrencies is laudable, but the lack of focus on encouraging regulatory regimes over MMOs and platforms has ignored decades of evidence of this form of VA serving as instrumentalities of money laundering, putting the AML enforcement community grossly behind. Some countries were early to adopt positions of taxing income generated from MMOs and other online gaming (OECD, 2020; Zhang *et al*., 2008), tacitly recognizing real-world value can and is

being extracted from VAs. When the V20 met in 2020, there was a fair degree of skepticism about the FATF, the new global standards, and the impact they would have on the VA sector (FATF, 2020b). There have been embryonic efforts toward implementing the FATF guidance on VAs and VASPs. For instance, Korea in 2020 amended its AML Act to include AML/TF requirements for VASPs consistent with FATF's Recommendations with a 2021 law. Italy too has taken initial steps to implement regulations on VASPs. But, *game-specific* VAs are not clearly articulated in either country's revised legislation.

Conclusion and Recommendations

Back in 2010, the FBI cautioned of the exploitation of virtual world media and applications — in-game currencies and goods — by violent extremists and criminals (DOJ, 2010). The indicators are all present — laundering is occurring regularly in MMO environments and via related third-party VA platforms. Missing are harmonized regulations to adequately address the threat this poses. Without specific efforts to address laundering, threat finance, and sanctions evasion risks posed by these evolving technologies, as more users turn to their virtual economy with its own "banking" system, AML/TF efforts will suffer a serious setback. Some of the intermediate efforts to address these laundering vehicles should include the following:

- Universal agreement among countries must be achieved in defining game VAs as commodities with real-world value predicated on their inherent potential for convertibility to RMT. The rise of tokenization via blockchain of game assets and the existing volume of trade in skins and other VAs in MMOs require acknowledgment that these belong under the greater definition of VAs.
- MMOs need to be classified as VASPs. Through the collection of over 100 cases from countries around the world, FATF has observed the use of VAs for a range of crimes. This includes money laundering from and the facilitation of a wide range of crimes including the sale of drugs and illicit firearms, fraud, tax evasion, computer crimes including cyberattacks, child exploitation, human trafficking, terrorism financing, and sanctions evasion (FATF, 2020b).
- Platforms for game-related NFT-backed items for sale/trade/transfer in video games should be required to register as MSBs/money transmitters in the jurisdictions in which they operate. This requirement must

be embraced by all countries. Countries where virtual currencies and online game playing are most popular are also frequently those that are hubs for corrupt practices and transnational crime syndicates. They also are reported to have weak law enforcement against financial crimes. At the moment, MMO VAs sit outside national financial reporting systems making it almost impossible for authorities to monitor transactions.

- MMOs and game-oriented VA exchange platforms that allow any form of VA transfer must be required to establish AML programs, including STR reporting to their home FIUs.
- With the addition of MMOs added to VASP designation, the volume of STRs can be expected to increase. However, this may yield little in the way of results in combating laundering in these fora unless multilateral policing beyond Interpol is embraced. The digital economy needs a transnational enforcement body that can move through and across jurisdictions in order to truly combat this form of laundering.

References

Barlowe, K. (2017). $5 Billion in Skins Wagered in 2016 Despite Valve Shutdown. Casino.org, https://www.casino.org/news/5-billion-skins-wagered-2016-despite-valve-shutdown/. [Accessed 28 April, 2021].

BBC News (November 1, 2019). Valve shuts down money laundering via CS: GO game. https://www.bbc.co.uk/news/technology-50262447. [Accessed 30 March 2021].

Belgian Gaming Commission (April, 2018). Research Report on Loot Boxes. https://www.gamingcommission.be/opencms/export/sites/default/jhksweb_nl/documents/onderzoeksrapport-loot-boxen-Engels-publicatie.pdf.

Belgian Gaming Commission (2021). Belgian Gaming Commission rules after analysis: "Paying loot boxes are games of chance". https://www.gamingcommission.be/opencms/opencms/jhksweb_en/gamingcommission/news/news_0061.html. [Accessed 16 April, 2021].

Bellingcat (February 1, 2019). Tracking illicit transactions with blockchain: A guide, featuring Mueller. https://www.bellingcat.com/resources/how-tos/2019/02/01/tracking-illicit-transactions-with-blockchain. [Accessed April 13, 2021].

Bennett, J. (July 29, 2007). Why miillions are living virtual lives online, *Newsweek*. https://www.newsweek.com/uhy.millions.are-living-virtual-lives-online-104537.

Blazer, C. (2006). *The Five Indicia of Virtual Property*, 5 *Pierce L. Rev*. 137. http://scholars.unh.edu/unh_lr/vol5/iss1/8.

Buchholz, K. (November 12, 2020). Where video games are popular among adults. *Statista.* https://www.statista.com/chart/18914/adults-video-game-playing-behavior-selected-countries/. [Accessed 2 April, 2021].

Castronova, E. (2001). Virtual worlds: A first-hand account of market and society on the Cyberian Frontier, Center for Economic Studies & Ifo Institute for Economic Research, CESifo Working Paper No. 618, December 2001.

Choo, K-.K.R., Smith, R. G. and McCusker, R. (2007). Future directions in technology-enabled crime: 2007–09. Australian Institute of Criminology, Research & Public Policy Series No. 78.

Cloward, J. G. and Abarbanel, B. L. (2020). In-game currencies, skin gambling, and the persistent threat of money laundering in video games. *UNLV Gaming Law Journal*, 10: 105.

Crypto.news (March 21, 2021). Gaming embraces NFTs: How long will the trend last? https://btcmanager.com/gaming-embraces-nft-how-long-will-the-trend-last/. [Accessed 28 April, 2021].

Cuthbertson, A. (January 13, 2019). How children playing Fortnite are helping to fuel organised crime. *The Independent.* https://www.independent.co.uk/news/fortnite-v-bucks-discount-price-money-dark-web-money-laundering-crime-a8717941.html. [Accessed 2 April, 2021].

Dibbell, J. (January, 2003). The unreal estate boom or the 79th richest nation on Earth doesn't exist. *Wired*. Issue 11.1.

EU Directive 2018/843, of the European Parliament and of the Council of 30 May 2018 amending Directive 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, and Amending Directives 2009/138/EC, 2018 O.J. (L 156).

Eyeonmogs.com (September 12, 2005). https://web.archive.org/web/20051218180730/.

Faber, T. (May 10, 2021). Pop stars mark out new territory in gaming. *Financial Times,* p. 14.

Farah, D. (2010). Money laundering and bulk cash smuggling: Challenges for the Merida Initiative. The Wilson Center. http://www.wilsoncenter.org/sites/default/files/Chapter%205-Money%20Laundering%20and%20Bulk%20Cash%20Smuggling%20Challenges%20for%20the%20Merida%20Initiative.pdf.

FATF (2010). Money laundering using new payment methods, FATF, Paris, France.

FATF (2012–2020). International standards on combating money laundering and the financing of terrorism & proliferation, FATF, Paris, France. www.fatf-gafi.org/recommendations.htm.

FATF (2015). Virtual currencies: Guidance for a risk-base approach, FATF, Paris, France.

FATF (2018). Outcomes FATF Plenary, 17–19 October 2018, FATF, Paris, France. https://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-plenary-october-2018.html. [Accessed 14 April, 2021].

FATF (2019a). Guidance for a risk-based approach to virtual assets and virtual asset service providers, FATF, Paris, France. https://www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html.

FATF (2019b) (February 22). Public statement – mitigating risks from virtual assets, FATF, Paris, France. https://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets-interpretive-note.html. [Accessed 2 April, 2021].

FATF (2019c) (June 21). Public statement on virtual assets and related providers, FATF, Paris, France. https://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-statement-virtual-assets.html.

FATF (2020a). Money laundering and terrorist financing red flag indicators associated with virtual assets, FATF, Paris, France. https://www.fatf-gafi.org/publications/fatfrecommendations/documents/Virtual-Assets-Red-Flag-Indicators.html.

FATF (2020b) (November 16). Opening remarks by FATF Executive Secretary at V20 Summit, FATF, Paris, France.

FATF (2020c). 12-month review virtual assets and VASPs, FATF, Paris, France. www.fatf-gafi.org/publications/fatfrecommendations/documents/12-month-review-virtual-assets-vasps.html.

FATF (March, 2021). Draft updated Guidance for a risk-based approach to virtual assets and VASPS, FATF/PDG(2020)19/REV1, Sixth draft: Public Consultation. FATF, Paris, France.

Fowler, G. A. and Qin, J. (March 30, 2007). QQ: China's new coin of the realm? Officials try to crack down as fake online currency is traded for real money. *The Wall Street Journal*, pp. B1 & B4.

Fujita, A., Itsuiki, H. and Matsuhara, H. (2011). Detecting real money traders in MMPRPG by using trading network. In *Proceedings of the Seventh AAAI Conference on Artificial Intelligence and Interactive Digital Entertainment*.

Gamekit.com (November 1, 2019). Information on personal data processing for gamekit.com users. https://gamekit.com/terms/privacy/. [Accessed April 28, 2021].

GitHub.io (n.d.). (Steam)web API how-to guide. https://danbeyer.github.io/steamapi/index.html. [Accessed 21 April, 2021].

Good, O. S. (September 10, 2017). Gold farming gets Venezuelans targeted in old-school runescape. *Polygon*. https://www.polygon.com/2017/9/10/16283926/venezuelan-gold-farming. [Accessed 2 April, 2021].

Grimes, S. M. (2006). Online multiplayer games: A virtual space for intellectual property debates? *New Media & Society,* 8(6).

Heeks, R. (2008). Current analysis and future research agenda on "gold farming": Real-world production in developing countries for the virtual economies of online games. University of Manchester, Development Informatics Group, Working Paper No. 32.

Hoge Raad 31 januari 2012 (*Runescape*), ECLI:NL:HR:2012:BQ9251, https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:HR:2012:BQ9251. (Netherlands).

Hood, V. (October 20, 2017). What the UK can learn from the far East's battle with loot boxes. *Eurogamer*. http://www.eurogamer.net/articles/2017-10-19-what-the-uk-can-learn-from-the-far-easts-battle-with-loot-boxes. [Accessed 23 April, 2021].

Institute of Games (2018). The convergence of gambling and video games: Social Casino games, gambling with virtual goods and lootboxes. https://instituteofgames.com/wp-content/uploads/2020/03/The-Convergence-of-Gambling-and-Video-Games-Social-Casino-Games-Gambling-with-Virtual-Goods-and-Lootboxes.pdf. [Accessed 28 April, 2021].

Iredale, G. (April 27, 2021). List of 10 most expensive NFTs ever sold. *101 Blockchains.* https://101blockchains.com/most-expensive-nfts/. [Accessed 28 April, 2021].

Iswaran, S. (October 7, 2014). Remote gambling bill: Second reading, (Singapore) parliamentary debates, official report, 12th Parliament, Session 2, V. 92, Sit. No. 14. https://sprs.parl.gov.sg/search/fullreport?sittingdate=7-10-2014.

Juniper Research (April 17, 2018). Loot boxes & skins gambling to generate a $50 billion industry by 2022. Press release. https://www.juniperresearch.com/press/loot-boxes-and-skin-gambling. [Accessed 10 April, 2021].

Keegan, B. and Ahmed, M. A. *et al*. (2010). Dark gold: Statistical properties of Clandestine networks in massively multiplayer online games. In *Proceedings of the 2nd International Conference on Social Computing*, IEEE, 201–208.

Knight, W. (December 23, 2003). Gamer wins back virtual booty in court battle. *New Scientist.* https://www.newscientist.com/article/dn4510-gamer-wins-back-virtual-booty-in-court-battle/.

Korean Institute of Criminology (2014). Cybercrime in the Republic of Korea II: Criminal Justice and International Cooperation for Cybercrime Prevention, Cybercrime Research Institute, Research Report Series 13-B-06.

Kotwani, B. (2021). Most expensive CSGO skin sold for a record $150K USD. https://www.talkesport.com/news/csgo/most-expensive-csgo-skin-sold-for-a-record-150k-usd/. [Accessed 10 April, 2021].

Lastowka, G. (2010). *Virtual Justice: The New Laws of Online Worlds*. London: Yale University Press.

Lastowka, G. and Hunter, D. (2004). The laws of virtual worlds. 92 *California Law Review,* 1.

LeagueofKingdoms.com (2021). Skins. https://www.leagueofkingdoms.com/skin. [Accessed 17 May, 2021].

Lee, E., Woo, J., Kim, H. and Kim. H. (January 19, 2018). No Silk Road for online gamers!: Using social network analysis to unveil black markets in online games, arXiv: 1801.06368v1 (cs.CY).

Lehdonvirta, V. (2005). Real-money trade of virtual assets: Ten different user perceptions. Helsinki Institute for Information Technology (HIIT).

Leupold, T. (May 6, 2005). Spot on: Virtual economies break out of cyberspace. GameSpot. http://uk.gamespot.com/news/2005/05/06/news_6123701.html. [Accessed 30 March, 2021].

Levine, M. (June 9, 2020). The bad stocks are the most fun. *Bloomberg.* https://www.bloomberg.com/opinion/articles/2020-06-09/the-bad-stocks-are-the-most-fun.

Li, C. (June 8, 2005). Death sentence for online gamer. *China Daily.* http://www.chinadaily.com.cn/english/doc/2005-06/08/content_449494.htm.

MacInnes, I. (2004) The implications of property rights in virtual world business models. Presented at the Americas Conference of Information Systems (AMCIS 2004), NewYork. http://web.si.umich.edu/tprc/archivesearch abstract.cfm?PaperID=382.

Maras, M. (2016). *Cybercriminology*. Oxford: Oxford University Press.

Millward, T., Manager, Licensing Compliance, Regulatory Services (N.D.), New Zealand Department of Internal Affairs, Email to Katherine Cross, reproduced in Cross, K. (December 11, 2017). New Zealand says lootboxes 'do not meet the legal definition of gambling'. *Gamasutra*. https://www.gamasutra.com/view/news/311463/New_Zealand_says_lootboxes_do_not_meet_the_legal_definition_for_gambling.php. [Accessed April 15, 2021].

Morningstar, C. and Farmer, F.R. (1990). The Lessons of Lucasfilm's Habitat, paper presented The First International Conference on Cyberspace, May 1990, the University of Texas at Austin.

Murphy, H. (May 28, 2021). Crypto laundries answer call from criminal gangs. *Financial Times*, p. 8.

Netherlands Gaming Authority (NGA) (April 19, 2018). Loot boxes & Netherlands Gaming Authority's findings. https://dutchgamesassociation.nl/2018/04/26/loot-boxes-netherlands-gaming-authority-findings/. [Accessed 17 May, 2021].

OECD (2020). Taxing virtual currencies: An overview of tax treatments and emerging tax policy issues, OECD, Paris. www.oecd.org/tax/tax-policy/taxing-virtual-currencies-an-overview-of-tax-treatments-and-emerging-tax-policy issues.htm.

Parloff, R. (November 27, 2006). Anshe Chung: First virtual millionaire. *Fortune*. https://fortune.com/2006/11/27/anshe-chung-first-virtual-millionaire/.

Quigley, W., Yantis, J., Sliwka, L. and CasSelle, M. (2019). WAX protocol white paper.Github. https://github.com/worldwide-asset-exchange/whitepaper. [Accessed 10 April, 2021].

Reider-Gordon, M. (October 6, 2010). The technology of laundry: How virtual currencies are changing the laundering landscape. *Association of Certified Anti-Money Laundering Specialists*. Presentation to Northern California chapter, Santa Clara, CA.

Reider-Gordon, M. (May, 2011). The technology of laundering: Virtual worlds, cell phones, an e-currencies — the world's new banks & AML's new frontier. Presentation to the 19th Annual West Coast Anti-Money Laundering Forum, San Francisco.

Reider-Gordon, M. (2012). Real world risk in virtual world gaming: Virtual currencies, money laundering, and the hidden risks to game companies. *M/E Insights.* Association of Media & Entertainment Counsel, Fall.

Remote Gambling Act 2014. https://sso.agc.gov.sg/Act/RGA2014. (Singapore).

Reuters (November 16, 2006). CopyBot furor roils second life currency. *Reuters Second Life*.

Reynolds, R. (2003). Commodification of identity in online communities. https://www.renreynolds.com. (Accessed 2 April, 2021).

Suzor, N. (2012). Order supported by law: The enforcement of rules in online communities. *Mercer L. Rev*. 63(2), 523–595.

UK Gambling Commission (March, 2017). Virtual currencies, eSports and social casino gaming — position paper.

UK House of Lords (July 2, 2020a). Gambling harm-time for action, Select Committee on the Social and Economic Impact of the Gambling Industry, Report of Session 2019–21, HL Paper 79.

UK House of Lords, (March 3, 2020b). Select Committee on the Social and Economic Impact of the Gambling Industry, Corrected oral evidence of Dr David Zendle, lecturer in Computer Science at the University of York, defined loot boxes as *Things in Video Games Where You Are Handing Over Money and You Are Getting Something Uncertain That is Determined Randomly in Some Way*.

UN Secretary General (July 30, 2019). Countering the use of information and communications technologies for criminal purposes, U.N. Doc A/74/130.

US Department of Justice (2007). National Drug Threat Assessment Summary. *Drug Enforcement Administration*. https://www.dea.gov/sites/default/files/2021-04/2003-2008_p_118-153.pdf.

US Department of Justice (August 23, 2010). Potential for exploitation of virtual world media and applications by violent extremists and criminals. Federal

Bureau of Investigation, (U//FOUO) Intelligence Bulletin, Los Angeles Division and Directorate of Intelligence — Cyber Intelligence Section.

US Department of State (March 2009). International Narcotics Control Strategy Report: Money laundering and financial crimes, Bureau for International Narcotics and Law Enforcement Affairs, Vol. II. https://www.hsdl.org/?view&did=38621.

US Library of Congress, Map: Regulatory framework for cryptocurrencies: Application of tax laws, anti-money laundering/anti-terrorism financing laws, or both. https://www.loc.gov/law/help/cryptocurrency/map2.pdf. [Accessed 2 April, 2021].

Valve Software Corp. (October 28, 2019). *Key Change*, Counter-Strike game blog, https://blog.counter-strike.net/index.php/2019/10/26113/. [Accessed 2 April, 2021].

WePC (2021). Online gaming statistics 2021. Available at: https://www.wepc.com/statistics/online-gaming/. [Accessed 28 April, 2021].

Zhang, B. *et al*. (November 17, 2008). China taxes real profits from virtual world transactions. Pillsbury, Client Advisory. https://www.pillsburylaw.com/images/content/2/1/v2/2130/0099534E2089DE6CFBC7E12469B4FFB8.pdf.

This page intentionally left blank

https://doi.org/10.1142/9781800612839_0006

Chapter 5

Malicious Financial Activities in the Dark Web — Prevailing Information and Knowledge

Tal Pavel

If you're looking for a step-by-step guide on how to open a fake business account and then commit tax fraud, the dark web can help you with that.

Emily Wilson, Vice-President of Research at Terbium Labs

Introduction

This study examines the scope of the dark web as well as the criminal activity that takes place there, with an emphasis on activities involving money laundering. The modern age is characterized by abundant and available information, through the Internet and various digital means. There is also the steady increase in the use of the dark web, both for positive and negative purposes. The dark web, as its name implies, is a wide space of information and actions, including malicious and criminal activities which should better be kept out of reach of the average Internet user.

The study will analyze the scope of the dark web and the volume of information existing there, with emphasis on criminal activities. Therefore, it will explore four research questions:

(RQ1) How deep is the web? With regard to the Internet, deep web, and dark web, what are their volume and extent?

(RQ2) To what extent has the information about these webs existed and been consistent, reliable, and variable over the years?

(RQ3) To what extent are criminal and malicious activities used for money laundering and criminal activities in the dark web?

(RQ4) Which measure should be taken to cope with criminal and money laundering activities on the dark web?

This will be carried out in the form of a funnel, analyzing the scope of information available on the Internet, the deep web, and the dark web, in addition to the ratio of the volumes of information between these three layers. It will then examine the scope of existing information on online criminal and malicious financial activities on the dark web.

The study has found that the dark web is indeed dark and constitutes a kind of a "black hole" in terms of the ability to estimate the volume of information contained in it, with an emphasis on criminal and malicious financial activities. Thus, the study claims that, based on a wide range of available data, it is somehow hard to form a coherent and reliable quantitative image that enables us to determine how deep the web and deep web are. Also, there is inconsistency in the data published over the years on the Internet, deep web, and dark web, to the point where there is a limited ability to estimate the volume and use of these three.

The Internet

The Internet is a vast ocean of information and an intangible digital domain that is more expansive than what we can perceive in our senses. We can hardly understand the meaning of numbers such as 2.5 quintillion bytes of data generated by users each day (Marr, 2018).

Thus, different publications have tried, over the years, to simplify and make accessible, in an understandable numerical way and even by visual

means, the scope of information available on the Internet. However, sometimes the information they present is inconsistent, contradictory, or illogical.

A minute on the Internet

Various publications have examined, over the years, the amount of information generated on the Internet every minute, with some citing data that appear in other sources, while others bring different and complementary information. For example, one source indicates, among other things, the number of photos uploaded to Facebook, video hours uploaded to YouTube, and the number of new Twitter accounts (DOMO, 2020), while another indicates the number of instances of logging in to Facebook, the number of video files viewed on YouTube, and the number of users who tweeted (Lewis, 2020). In this way, various sources complement each other to provide a broader picture of the scope of information generated on the Internet every minute.

Thus, it is also possible to follow the development of online activity of humankind and the increase in the use of social networks, email, and various applications over the years. For example, the increase in the use of Facebook can be measured by examining the number of entries into the social network within one minute: 701,000 (2016), 854,000 (2017), 973,000 (2018), 1 million (2019), and 1.3 million (2020). Apart from that, the confirmation of known trends, such as the rise in Netflix's popularity: 266,000 hours of viewing per minute in 2018, 694,000 a year later, and 764,000 in 2020 (Loomly, n.d.; Desjardins, 2019; DOMO, 2020; Lewis, 2020).

However, there is a phenomenon whereby some publications indicate different data regarding the same period of time and on the other hand, publications show there has been no change in a certain figure over the years. For example, when examining the number of hours of Netflix viewing per minute in 2017, one source indicates the number 70,017 (Desjardins, 2017) and another, the number 80,860 (Loomly, n.d.).

On the other hand, we can indicate cases in which, in some publications, there has been no change in some data over the years, or a significant change in a short time, on the other hand. For example, when comparing data from two different sources for the same period, a publication from the beginning of February 2016 indicates 1.04 million Vine users (Smith, 2016), while the same number appeared for the year 2016

(Loomly, n.d.). On the other hand, there has been an increase from 694 Uber rides in one to 1,389 in the other, as well as a jump from 590,000 Tinder Swipes to 972,000 — while both refer to the same time, or at least to a close timeframe.

Another example is the number of emails sent per minute. A tweet from the end of December 2015 shows an infographic according to which 204 million emails were sent per minute (Twitter, 2015). On the other hand, various sources indicate a consistent trend of increase in the number of emails sent per minute from 150 million in 2016 to 190 and even 200 million in 2020 (Loomly, n.d.; Fox, 2018; Lewis, 2020; NodeGraph, 2020). If so, how does the 2015 infographic indicate the number of 204 million emails per minute?

The volume of information on the Internet

Another method that can explain the scope of the Internet and the information available is an examination of the data covering the volume of information on the Internet and its development over the years. An IBM publication from May 2012 indicates the number 2.7 Zettabytes (ZB)[1] of data in the digital universe (Karr, 2012); an October 2018 publication refers to the same number (Wassén, 2018), whereas a month later, an IDC publication suggests 33ZB as the global datasphere (Reinsel *et al*., 2018). At the same time, another publication by IDC from April 2014 stated that the size of the Digital Universe in 2013 had been 4.4ZB, and another site estimates the size of the Internet as 19.25 ZB as at March 2021 (Live Counter, n.d.).

Thus, when trying to define the volume of information on the Internet, we see the following: (1) reference to the same number in different years, and conversely (2) reference to different numbers in short periods.

The extent of information creation on the Internet

Other arguments are regarding the creation of information on the Internet. The claim that "90% of all the data in the world has been generated over

[1]A gigabyte is 1,024 megabytes; a terabyte is 1,024 gigabytes; a petabyte is 1,024 terabytes; an exabyte is 1,024 petabytes; and a zettabyte is 1,024 exabytes.

the last two years" was mentioned in May 2013 (Dragland, 2013), December 2016 (Loechner, 2016), May 2018 (Marr, 2018), June 2018 (Irfan, 2018), March 2019 (Petrov, 2021), and June 2019 ("90% of the data on the Internet has been created since 2016") (Schultz, 2019).

This inevitably raises the question of whether during the years 2013–2019 nothing changed in the pace of information creation on the Internet. That further underscores the question of whether it is possible to rely on that and similar data when trying to quantify the size of the Internet and the volume of information and activity on it.

The Deep Web

What is the relation between the amount of information available on the Internet and the deep web?

When trying to estimate the volume of information available on the Internet, known as the surface web, the deep web, and dark web, one can see completely different data in a short time difference, while other data have been established over the years without any change. In March 2014, it was claimed that the surface web constituted less than one percent of the entire world wide web (Pagliery, 2014). About a year later, it was claimed that "Google indexes no more than 16 percent of the surface web and misses the entire deep web. Any given search turns up just 0.03 percent of the information that exists online" (Popular Science, 2015). Another numerical figure states that the size of the Internet is only 1% of all online information, a figure mentioned in Carapola (2017), and in various sources over the years, including on August 2018 (Creative 3200, 2018), January 2019 (Pratham, 2019), November 2019 (Adamek, 2019), June 2020 (Bisson, 2020), and even on the Kaspersky website (Kaspersky, n.d.).

Besides the above, data from November 2015 indicate that 90% of the Internet is hidden from our browser and exists on the deep web (Taiwo, 2015), while creating an internal contradiction by referring in the article to an infographic according to which the visible web makes up 4% of the entire world wide web, while the deep web contains another 96%. This claim also appeared exactly five years later (GeeksforGeeks, 2020).

This division has been recognized over the years, according to which, of the other 96%, 90% is the deep web, while the remaining 6% is the dark web. These numbers can be found unchanged over several years: May 2014

(NPR, 2014), December 2015 (McGauley, 2015), February 2016 (Chikada, 2016), November 2019 (CISO Platform, 2019), July 2020 (LegalVision, 2020), and January 2021 (Karr, 2021).

On the other hand, some sources simply state that the size of the deep web is between 96% and 99% of the entire Internet and that only a small part of it is accessible via a standard browser (Guccione, 2020).

In light of all this, the following question arises: what is the size of the Internet? What is the deep web's share of total online information? Is the ratio 99% versus 1%? Or is it 96% versus 4%? And above all, over many years in terms of the Internet, sometimes even seven years, has there been no change in the data to the extent that different sources indicate the same data over and over again over such a long period?

What is the size of the Internet relative to the deep web?

Another claim is that the deep web is 500 times larger than the regular Internet we use. According to a study conducted in March 2000, "public information on the deep web is currently 400 to 550 times larger than the commonly defined World Wide Web" (Bergman, 2001). However, the statement and the number remain the same over the years: November 2009 (Beckett, 2009), December 2015 (Thompson, 2015), February 2016 (Chikada, 2016), December 2017 (TEDxWarwick, 2017), May 2018 (Pratham, 2019), September 2018 (Roy Choudhury and Kharpal, 2018), and September 2020 (LegalVision, 2020).

That is, for two decades, different sources have treated the same numerical data as if no change has taken place in them. Has there been no change in the size of the Internet, that of the deep web, in two decades? Can we rely on such numerical data in light of this fact? To what extent do we know the size and volume of activity of the Surface Web and the deep web?

The Dark Web

In light of all the examples given regarding diverse data on the Internet and the deep web, we will examine the data that exist regarding the dark web, the number of sites, and the scope of activity on it, along with the examination of the criminal activity and crime committed there, with an emphasis on money laundering.

The dark web, as implied by its name, is a platform for dark and criminal activities, along with completely legal activities that aim to protect the user's privacy and anonymity. Thus, this space is used for positive purposes, such as protecting opposition and human rights activists, journalists, businessmen, and intelligence agents but also for negative and criminal purposes such as drug trafficking, weapons smuggling, counterfeit credit cards, exchanging information, drugs, and even people, and of course a platform for anonymous money laundering. Indeed, a December 2020 study indicates that, despite the negative reputation of the dark web, only 6.7% of all dark web users worldwide use it for malicious purposes, and most users do not actually look for malicious sites. It can be determined that the rate was higher in free countries (7.8%) and lower (4.8%) in countries where there are restrictions on Internet access, that is, "not free" regimes (Jardine *et al*., 2020).

The size of the dark web

Along with the ability to use existing websites on the Internet, there are websites with unique addresses that allow the use only on the dark web and using a Tor browser (Dingledine *et al*., 2004), i.e., the use of such a URL on the Surface Web will not yield any result and we cannot access any website. Sites that are available only on the dark web and using a Tor browser are defined as hidden service addresses and consist of 16-character domain names that the system automatically generates when creating the address (Gallagher, 2016) and have a typical .onion extension (Victors *et al*., 2017). It should be noted that even if websites with this .onion extension exist only on the dark web, this does not indicate that these websites are necessarily involved in crime. As noted in the Tor blog as early as 2015, only 3.4% of all Tor traffic is defined as hidden services (asn, 2015).

An analysis of the number of .onion addresses, as has been published regularly since December 2014 by the Tor Project, which currently manages Tor, reveals a trend of a significant increase over the years in the annual average of .onion addresses (Tor Project, 2021) (Table 1).

This means that in about six and a half years, there has been a 510% increase in the number of .onion addresses on the dark web. Various publications over the years have revealed varied data on the number of these addresses: Indeed, the Tor Project blog stated in February 2015 that

Table 1. Average number of unique .onion addresses — 2014–2021.

Year	Average number of unique .onion addresses	Change (%)
2014 (from December)	28,296	—
2015	29,235	3.35
2016	55,513	89.88
2017	54,791	–1.30
2018	92,405	68.65
2019	82,129	–11.12
2020	150,729	83.53
2021 (until mid-May)	172,609	14.52

approximately 30,000 hidden services are registered on the Tor network daily (asn, 2015), similar to the figure above. However, four months later, a study stated that there are about 7,000 sites with .onion extension (Brewster, 2015). Another study that examined the size of the dark web in 2019 in terms of the number of .onion addresses found that there are 55,828 such different addresses, but only 8,416 of them are active (Stone, 2019). The finding is reinforced by a study that examined such addresses in the dark web and found that about 90% of them are unavailable and attempts to connect to those sites had failed (Mani *et al*., 2018).

When analyzing the size of the dark web and the level of activity in it, it appears that the average daily number of users since the beginning of 2021 has been about 2–2.5 million, in contradiction to a study from September 2018 (Mani *et al*., 2018), which aims to understand who uses Tor and in which way, that estimated the daily number of users is four times greater than previous estimates and stands at about 8 million.

Over the years, there has been a change in the rate of use as per distinct countries, as well as in the names of the 10 countries with the most use of the dark web daily (*Users – Tor Metrics*, 2021) (Table 2).

The data indicate several trends:

(1) US dominance in terms of its share in the number of Tor users over the years.

Table 2. Mean daily users of Tor by country — 2014–2021.

	Mean daily users (%)							
Country	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**2021**
United States	13.93	17.62	20.16	18.08	16.53	17.57	25.90	20.49
Germany	8.78	9.72	10.27	12.24	17.70	7.77	8.02	8.51
France	6.24	6.42	5.99	4.68	4.10	4.29	3.76	3.26
Brazil	5.54	3.29	2.57	—	—	—	—	—
Russia	5.08	8.92	11.64	9.78	10.41	17.12	14.55	14.87
Spain	4.37	3.37	2.57	—	—	—	—	—
Italy	3.95	3.22	2.68	1.55	—	—	—	—
United Kingdom	3.89	4.40	4.42	3.23	2.62	3.12	2.89	2.83
Poland	3.02	2.15	—	—	—	—	—	—
Argentina	2.38	—	—	—	—	—	—	—
Japan	—	2.43	2.49	—	—	—	—	—
Canada	—	—	2.19	1.78	—	—	1.96	—
United Arab Emirates	—	—	—	11.97	10.52	—	—	—
Ukraine	—	—	—	5.68	3.96	3.06	2.19	2.37
Netherlands	—	—	—	3.14	2.21	2.36	4.87	4.62
Indonesia	—	—	—	—	3.64	4.48	3.20	3.28
India	—	—	—	—	1.87	2.53	2.08	—
Iran	—	—	—	—	—	7.81	—	—
Lithuania	—	—	—	—	—	—	—	3.26
Turkey	—	—	—	—	—	—	—	3.22

(2) The change that occurred during this period in this top 10 list in terms of countries where the rate of Tor use is highest.
(3) The dominance of European countries and Russia is in line with this study's findings that will be detailed later, according to which "the main drug suppliers among European countries in the dark web were Germany, the Netherlands and the United Kingdom".
(4) The short appearance of countries such as Iran, the United Arab Emirates, Poland, Argentina, and Japan, which throughout the period, and without continuity, have briefly joined this top 10 list, for reasons worth examining in a separate study.

When reviewing the criminal activity in the dark web, it is worth noting that the research literature indicates a knowledge gap concerning the role of traditional organized crime in the dark web markets, in the manufacture, trade, and distribution of drugs in the dark web trading sites (European Monitoring Centre for Drugs and Drug Addiction, 2017). This trade is carried out worldwide (*Online African Organized Crime from Surface to Darkweb*, 2020) through sites that constitute marketplaces and other sites that constitute stores operated by individual sellers (vendor shops).

Marketplaces and shop vendors in the dark web

Various studies attempt to estimate the volume of malicious trade in the dark web in light of its areas of activity, including issues of money laundering (Weber and Kruisbergen, 2019), which is used by both criminal and terrorist elements (Rubasundram, 2019). However, as with the data for the Surface Web and the deep web, we can see a lack of uniformity and consistency in data.

Marketplaces have existed in the dark web since 2010, but a significant milestone occurred in late January 2011 with the opening of the Silk Road marketplace, which was closed by the US authorities in October 2013. Shortly afterward, the Silk Road 2.0 site opened, which started an era of proliferation in the dark web markets. As of 2017, the number of those markets was estimated at more than 100, along with the fact that this sector is very dynamic: trading sites rise and fall relatively quickly (UNODC, 2018).

Attempting to follow the number of markets on the dark web represents another challenge due to a variety of different data over the years. An article from May 2019 refers to 100 sites in the dark web dedicated to criminal activity, including criminal forums as well as markets (Stone, 2019). In 2021, another source indicated 44 active markets as well as 25 stores, most of which are engaged in drug trafficking (Darknet Stats, 2021b). Another source from 2021 indicates 16 markets as well as six scam markets (Darknet Stats, 2021a). However, following the closure of such trading sites in 2017, as well as the shutdown of the largest Bitcoin exchange site that year (Brandom and Jeong, 2017), it is claimed that the number of trading sites in the dark web doubled in 2018, with buyers and sellers switching to instant messaging technologies and encrypted applications such as Telegram and WhatsApp

(Chainalysis, 2019). As a result, in mid-June 2018, the US Department of Justice reported a large-scale operation against merchants in the dark web during which 35 of them were arrested and illegal goods seized (Department of Justice, 2018).

In addition to marketplaces and vendor shops, one can establish forums that serve for coordination of sales with community-led discussion to share wisdom, tactics, techniques, and procedures, but with no e-commerce function (HHS Cybersecurity Program, 2020).

Drug Trafficking on the Dark Web

When examining the motivations for buying drugs on the dark web, various studies indicate that buyers believe that, in the dark web, the sale of drugs is more profitable online and it has a greater supply of drugs, with improved quality and convenience, while reducing the risk of direct communication with the online drug vendor. Furthermore, it reduces the possibility of fraud, police detection, robbery, or even being killed by competitors. The dark web also allows the buyer to purchase the drugs directly from the sellers located in the countries where the drugs are manufactured (European Monitoring Centre for Drugs and Drug Addiction, 2017; van Buskirk *et al*., 2016). Indeed, a study that examined the purchase of drugs on the dark web found that people buy more drugs in the dark web's marketplaces, compared to the amount purchased in physical markets (Strizek *et al*., 2019).

Thus, people use it as a platform that enables an optimal combination of high anonymity through secure communication and the use of cryptocurrencies to carry out the criminal transactions of users located around the world.

The size of the drug market in the dark web

A study by the United Nations Office on Drugs and Crime (UNODC) published in May 2017 finds that the dark web is used for various illegal activities, including drug trafficking, and adds that while drug trafficking in the dark web is small, it is growing rapidly. Indeed, in 2015, this trade accounted for less than 1% of the global drug trade, but the report indicates a 50% increase every year since 2013 (UNODC, 2017b). On the other hand, another study (Siggia, 2020) presents a sharper increase in

Table 3. Drug trade activity (million euros) — 2012–2015.

Year	Drug Trade Activity (Million Euros)	Change (%)
2012	15	—
2013	60	400
2014	120	100
2015	180	50

the rate of drug trafficking in the dark web in the years 2012–2015 (Table 3).

The UN report adds that a survey of 100,000 Internet users from 50 countries found that of those who used drugs during the past year, the proportion of those who bought drugs in the dark web during this period increased from 4.7% to 7.9% between 2014 and 2017, which reflects an increase of 70%. (UNODC, 2017a). In a 2019 study that examined, among other things, the sources from which 20,157 respondents purchased the drugs, 8% indicated that they "buy it from internet encrypted markets" (Strizek *et al*., 2019).

The UNODC study also indicates that this increase is noteworthy, especially because drug trafficking (not only in the dark web) moderately increased from 2.1 million cases in 2013 to 2.4 million cases in 2015. Another figure from the same study demonstrates the increase in online drug trafficking in the dark web over the years: according to the study, the total number of transactions in the eight main markets in the dark web in January 2016 was 2.6 times greater than the number of transactions made in September 2013 on the Silk Road marketplace, which dominated the dark web at the time. Furthermore, of the eight leading markets in that period, 71% sold drugs, including 62% that sold only drugs and related products and 9% that sold drugs along with other products. The study estimates that the minimum income from drug trafficking in the dark web was USD 14.2 million, double the estimates regarding the sale of drugs on the Silk Road marketplace in September 2013. However, an article from November 2020 estimated the volume of drugs purchased on the dark web at 4% of all its criminal activities (GeeksforGeeks, 2020). Evidence can be found from a 2019 study that states that 9 out of 10 respondents never

bought drugs from marketplaces on the dark web (cryptomarkets) (Strizek *et al*., 2019).

The volume of drug trafficking transactions and revenues

The UNODC study also reveals that, of the top eight markets in the dark web, 64% of the transactions were in amounts of less than USD 100. However, when examining the volume of income from these transactions, it turns out that 57% of the income is from transactions of USD 100–1,000, and 25% of the transactions are in amounts of over USD 1,000 per transaction. This means that at the time, drug cartels were not yet involved in the sale and purchase of drugs in the dark web. This also reinforces the claim previously raised from the same report that most dark web drug buyers do so for their personal use (UNODC, 2017a). This is reinforced by a EUROPOL report from that time, which states that the wholesale of drugs is relatively uncommon and that in most cases, these are small- or medium-volume transactions directly to the consumer (European Monitoring Centre for Drugs and Drug Addiction, 2017).

Types of drugs purchased on the dark web

There is a variety of data on the extent of crime that exists on the dark web. According to most of the data, the dark web is mainly used for illicit drug trafficking, drug-related chemicals, and pharmaceuticals. When examining the leading types of drugs in the dark web, the UNDOC report reveals that ecstasy, cannabis, LSD, and NPS were the most purchased in 2017. The report concludes that drug buyers in the dark web do so for their use and are less likely to buy drugs like heroin online on the dark web (UNODC, 2017a). Indeed, a 2019 study also lists new psychoactive substances (NPSs) as the most popular on dark web marketplaces (Strizek *et al*., 2019). According to a EUROPOL report from 2017, the best-selling drugs are cannabis and cocaine (European Monitoring Centre for Drugs and Drug Addiction, 2017).

The most active drug market countries in the dark web

Studies by various government institutions worldwide present a clear picture of the prominent place of several European countries in the dark web

Table 4. Annual drug users obtaining drug over the dark web in the past 12 months (2014–2017).

Year	Global Average	United States	United Kingdom
2014	4.7	7.7	12.4
2015	5.9	9.1	14.3
2016	7.6	15.0	18.3
2017	7.9	13.2	25.3

drug market, with most of them citing the United Kingdom, Germany, the Netherlands, and Finland as the most dominant in both the European and global arenas.

The UNDOC (2017a) report indicates that the size of the drug market in the dark web has doubled during the years 2014–2017 (Table 4).

Apart from evidence of the significant growth in the dark web drug market, Table 4 gives a glimpse of Europe's dominance in this market, as can be seen from the data on the UK's share, which is not only significantly higher than the US but also presents a consistent growth rate over the year to the point of doubling over four years (UNODC, 2017a). A 2018 EUROPOL study also highlights the importance of European vendors in the dark web. The findings indicate that in the period 2011–2015, these accounted for 46% of all drug suppliers in the dark web in terms of revenue in these markets. There are also data according to which drug suppliers from European countries accounted for 28% of all drug sales on the AlphaBay marketplace, which was the largest trading site during the years 2015–2017 in the dark web. It should be noted that the closure of this site in January 2018 did not seem to have a significant effect since 57% of the respondents stated that they considered themselves not affected by the closure. The EUROPOL study also shows that, during the years 2011–2017, the main drug suppliers among the European countries in the dark web were from Germany, the Netherlands, and the United Kingdom (European Monitoring Centre for Drugs and Drug Addiction, 2017), a finding that is also reflected in a November 2016 publication which stated that the United Kingdom leads the European countries in the sale of illegal drugs on the dark web, based on revenue and number of sellers, followed by Germany and the Netherlands (Armstrong, 2016; McCarthy, 2016). A UNODC study examining the years 2014–2019 also

reveals a steady and consistent increase over the years in the proportion of dark web users from Europe who had purchased drugs online over the past year. In the other regions, Oceania, North America, and South America, there was a significant increase in the rate of purchases in some years compared to a decrease in other years. The global list is led by European countries, with Finland, Sweden, and the United Kingdom at the top (UNODC, 2019). A study that examines the activity of Nordic countries' users in purchasing drugs on the dark web in 2018 also places Finland at the top of the countries in which respondents answered in the affirmative to the question "Have you obtained drugs from dark web markets in the last 12 months?" with a response rate of 45.2% (Statista, 2020). There is also a study published a year later, in which Finland led a list of 10 countries whose citizens purchase drugs on the dark web marketplaces, with a response rate of 23%, while in Poland, which came second on this list, the response rate was only 11% (Strizek *et al*., 2019).

Besides being a marketplace for various drugs, the dark web serves as a fertile ground for the sale of a variety of illicit products and information, including a variety of counterfeit products, hacking services, cyberattack tools, leaked information, counterfeit certificates, login credentials, financial data, and even weapons and ammunition.

Weapons and Ammunition

The dark web enables the distribution of illegal weapons that are already on the black market, as well as being a possible source for the sale of legal weapons. In addition, the dark web increases the availability of much higher quality and newer weapons at the same price, or even cheaper than at the black market on city streets. Therefore, the dark web has the potential to become the preferred platform for individuals (such as lone wolves), or small groups (such as gangs) to obtain weapons and ammunition in the anonymity that this network largely provides (Persi Paoli *et al*., 2017). In June 2018, it was estimated that the trade in weapons and explosives constituted only 1% of the trade on the dark web (Armstrong, 2018). The UNODC report for 2018 states that the proportion of weapons and explosives in the total trade in the dark web is 2% (UNODC, 2018), and so does the report by EUROPOL (European Monitoring Centre for Drugs and Drug Addiction, 2017). However, an article from November 2020 states that the sale of weapons constitutes 0.3% of the activity in the dark web (GeeksforGeeks, 2020).

When analyzing the market for the sale of weapons and ammunition on the dark web, different data can be seen, and sometimes with a significant change over the years. The analysis of marketplaces for selling weapons on the dark web, which was conducted in September 2016, found 18 such sites that sell from few weapons to several hundred on a single marketplace alongside 60 vendors in various markets. In addition, 82% of the weapons sold at the dark web trading sites were live weapons while the remaining 17% were replicas. A total of 42% were firearms, 27% were digital products, and 22% were described as other weapons. About 60% of these weapons vendors are from the US, and the weapons are supplied throughout the world and especially to Europe (Persi Paoli *et al*., 2017).

A study on the distribution of arms sales through the dark web in 2017 reveals that about 60% of them were purchased in the US (McCarthy, 2018). Regarding the cost of weapons in the dark web, a 2017 publication stated that the cost of purchasing an AK-47 was USD 2,800, an amount up to 4.6 times higher than the illegal purchase price of this weapon in various countries around the world (McCarthy, 2017). Another study from that time estimated the average cost of weapons in the dark web at USD 1,187 (Persi Paoli *et al*., 2017). It should be noted, however, that an inspection conducted by the author at the end of April 2021 on a marketplace for selling weapons on the dark web revealed that the cost of purchasing an AK-47 is only USD 500–600.

Data Trade on the Dark Web

Besides being a marketplace for drugs and weapons, the dark web is an extensive platform for the sale of various types of information, in two main areas: (1) financial data, including stolen credit cards, and bank account information that can be used for money laundering and (2) personal information, including passwords for accessing various accounts and contact lists, while making a distinction between information that can be changed by the user and lifetime data, such as date of birth, blood type, social security number, and information determined by the government (Adamek, 2019). The trade prices of stolen data are relatively low as for other criminal services on the dark web and include user access information (59%) to payment systems, online banking, and cryptocurrencies exchange sites. In most cases, the cost of such passwords is up to USD 10 and the average cost of selling online banking data is USD 11; for credit card information (24%), the cost of one credit card

information is USD 9; scanned copies of various documents (17%) amount to 64% of the cases being personal documents and 21% financial documents (Positive Technologies, 2018b). A source from October 2019 indicates the price of cards from USD 2–20 and emphasizes that these prices have not changed in the last two years (Gray, 2019). On May 2021, the price of a cloned VISA or Mastercard credit card with PIN was on average USD 25 and stolen PayPal account details with no balance were USD 14 (Ignoffo and Zoltan, 2021).

In addition, the dark web enables criminal trade in forged online and physical documents including driver license (USD 20–80), valid social security number (USD 2), fake US green card (USD 150), and even physical passports (USD 1,500–6,500), with some increase in the average price of such products between 2020 and 2021 (Ignoffo and Zoltan, 2021).

Cybercrime on the Dark Web

The dark web enables to develop the cybercrime as a business, while is serves as a platform for "Cybercrime-as-a-service" in two ways:

(1) for the experts — economy of tools and methods to commit cybercrime, including malware ("a key element in almost every cyberattack"), exploits, trojans (data-stealing trojans, Remote Access Trojan [RAT], ATM trojans, and ransomware trojans), and spam and phishing;
(2) for amateurs — "rent a hacker" services by expert hackers and information access including passwords for sites or servers (HHS Cybersecurity Program, 2020; Positive Technologies, 2018a).

Therefore, the dark web enables tools, knowledge, and human resources to carry out cybercrimes, in addition to hosting marketplaces for trade in the stolen data during such cybercrime activities as mentioned above.

As mentioned for other types of criminal activities, the price level of cybercrime services on the dark web is very low and diverse, as seen throughout this study. A study from July 2018 indicates the following prices for "cybercrime-as-a-services": hacking email from USD 40; hacking websites from USD 150, DDoS attack from USD 50 a day; infecting with ransomware Trojan from USD 750; and stealing payment data from USD 270 (Positive Technologies, 2018a).

A study from January 2019 defines a different range of prices for cybercrimes services on the dark web: Ransomware: USD 120–1,900; access to servers: USD 8–15. Another survey from October 2019 indicates the pricing of DDoS botnet from USD 1–100, depending on the bandwidth and duration. Another example for the low prices of cybercrime services on the dark web can be found in a June 2021 study which provides examples for hacked services (Uber hacked account: USD 8; hacked Gmail account: USD 80; hacked Twitter account: USD 35) and DDoS attacks from USD 15–1,000 (Ignoffo and Zoltan, 2021).

Money Laundering on the Dark Web

Cryptocurrencies and money laundering on the dark web

Due to the anonymous nature of the dark web and the possibilities for criminal transactions as described above, the dark web is widely used for money laundering by a variety of criminal entities (Elliptic, 2019), which constitutes, along with theft of information and money through phishing, malware, identity theft, and the use of stolen credit cards, one of the major types of criminal activity on the dark web (Fraud Watch International, 2018). This activity of criminal trade and money laundering is carried out through various virtual currencies (Silfversten *et al*., 2020), which provide anonymity in communications and online activity that allegedly exists in the dark web. Indeed, over the years 2011–2018, there had been an increase in the amount of Bitcoin going through the dark web from USD 5 million in 2011 to USD 603 million in 2018. However, it should be pointed out that although the average daily activity in these markets is USD 2 million in Bitcoin, this volume is only 1% of all global activity in Bitcoin (Chainalysis, 2019).

A similar figure can be found in an article from October 2020, according to which the rate of virtual currency wallets linked to the dark web markets is only 1.2%, and yet another figure wherein only 35 of crypto exchanges receive funds from dark web markets (Coinfirm, 2020).

In addition, the data show that "a small group of 270 blockchain addresses have laundered around 55% of cryptocurrency associated with criminal activity" and that "1,867 addresses received 75% of all criminally-linked cryptocurrency funds in 2020," which created a greater level of concentration in 2020 than in 2019 (Cimpanu, 2021).

So while Bitcoin is a major cryptocurrency for criminal transactions on the dark web, most of its use is not in this network. Thus, the view of virtual currencies as being used primarily for the purchase of drugs and weapons on the dark web is a misconception.

Anti-money laundry and the dark web

Feakin (2014) identified three different ways that law enforcement agencies can increase their capabilities to countermeasure the criminal activities on the dark web: invest in **technology**, build a sustainable **skills base,** and build **international partnership**. All those can be found at the Interpol activities in this regard (Feakin, 2014).

One of the main arguments in dealing with money laundering in the dark web is that there is no anti-money laundering (AML) policy regarding the dark web. For that purpose, the Interpol shaped a global cryptocurrency taxonomy, which will constitute "a set of classifications defining which categories of data from suspicious cryptocurrency transactions should be collected." To this end, the initiative will define the various entities, the types of services provided, and the types of crimes committed on the dark web (Interpol, n.d.). In 2014, it was claimed that no AML software was able to monitor and identify patterns of suspicious transactions (Financial Action Task Force, 2014). To deal with money laundering operations using cryptocurrencies, Interpol has taken several initiatives, including technological solutions, such as assisting in the development of a blockchain analytics tool called GraphSense that helps trace cryptocurrency transactions, as well as another tool called Darkweb Monitor that will collect data on criminal activity in the dark web and use it "to provide actionable intelligence to support police investigations worldwide" (Interpol, n.d.).

Another argument is that law enforcement agencies cannot target a single location or central entity to investigate and seize assets, since this activity is carried out in a network that, as its name implies, is dark. Another difficulty in dealing with money laundering in the dark web is the fact that these actions are performed by different entities, which are often in different jurisdictions, including those where there are insufficient controls on AML issues, making it even more difficult for law enforcement and regulators to get their hands on (Financial Action Task Force, 2014). To address this issue, Interpol, in collaboration with the Dutch Ministry of Foreign Affairs, has formulated the CapaCT project, which

aims to formulate a guide that will help law enforcement agencies in Southeast Asia tackle the misuse of the dark web and cryptocurrencies by terrorists and provide them with comprehensive guidelines when investigating the terrorist activities on the dark web, including those involving the use of cryptocurrencies while creating a platform for training and simulation on the subject. Another initiative in this regard is the establishment of a working group in collaboration with the Bavarian State Ministry of Justice on the matter of the dark web and cryptocurrencies to share methodologies with tools to identify how criminals exploit the anonymity of virtual currencies and the dark web. In this context, the Dark Web and Cryptocurrencies Task Force was established, which will work, among other things, to create an international database of criminal wallets of cryptocurrencies (Interpol, n.d.).

Besides shutting down online criminal commerce sites in the dark web and as part of confronting the illegal trade in the dark web and money laundering, there is an extensive activity of arresting those involved in such activities: arrest in early 2016 in the Netherlands of 10 people who have been accused of money laundering through Bitcoin trading (*The Guardian*, 2016); a US citizen was accused of laundering more than USD 19 million of drug trafficking profits he made over two years on the dark web (Wells, 2019); an Israeli citizen of Brazil, who ran on the dark web a platform that served as a marketplace for drug trafficking sites, weapons, and means of cyberattacks, was accused of laundering USD 8.4 million (Bar, 2021; Starks, 2021); a US resident was accused in 2020 of operating a website on the dark web that laundered more than USD 300 million between 2014 and 2017 (Department of Justice, 2020); in 2020, the US imposed sanctions on two Chinese citizens for their involvement in laundering money stolen during a cryptocurrency exchange intrusion linked to an attack group affiliated with North Korea (US Department of the Treasury, 2020); and, of course, the arrest of Ross Ulbricht in October 2013, who was charged with money laundering and drug distribution, after setting up and running the Silk Road drug trafficking site two years earlier and sentenced in 2015 to life in prison (Department of Justice, 2015).

Summary

This study is intended to examine the scope of criminal activity in the dark web and to emphasize the dark web being used a tool for money

laundering. To this end, the existing knowledge on the subject was examined based on a wide variety of sources to learn about the scope of the knowledge as well as the degree of ability to rely on it to examine the criminal activity in the dark web. In this regard, the existing knowledge was examined in the context of assumptions and data that have been used over the years to describe the Internet and the deep web.

Therefore, it is not only necessary to re-examine numerical assumptions relating to the Internet and the deep web that are frequently used but also to conduct research that can provide up-to-date information about their scope and volume of activity. When analyzing the criminal activity on the dark web, a picture is revealed of a domain that constitutes a platform for a wide range of criminal activities and money laundering, but even here, data were sometimes found that required reference and clarification, as mentioned above. Besides this, several facts became clear in the context of the dark web:

(RQ1): (1) The large increase over the years in the use of the surface web, the deep web, and the dark web in terms of number of users, web addresses, and content.

(RQ2): (2) The difficulty of relying on these determinations relating to the Internet and the deep web and learning from them about the true extent and the activities in those domains because in many cases one or two phenomena were found: (2.1) use of identical data over the years in a manner that raises the question of whether there has been no change in them over a long time; on the other hand, (2.2) use of different and contradictory data relating to the same field and the same period.

(RQ3): (3) The deep web is the basis for diverse criminal activities through a platform that provides anonymity at all stages of the illegal trade, both for communication and payment. (4) It provides the ability to trade in products (drugs, weapons, stolen data) and services (hacking, forge, cybercrime) at relatively low cost. (5) Even if the drug market in the dark web comprises a very small percentage of world drug trafficking share, over the years, there has been a considerable increase in the volume of the drug trade in the dark web. (6) The dominance of the US and European countries in both the use of Tor and the online drug trafficking markets, alongside the fact that in most cases this trafficking is for personal use and not for trafficking. (7) The dark web, contrary to the known

image, is not only used for criminal activity, which constitutes a small part of all the activity and information existing in it.

(RQ4): (8) In addition to the fact that in many cases these .onion addresses are inactive, which may indicate the degree of their ephemerality, possibly because law enforcement agencies disable some of these criminal sites. (9) Closing drug trafficking sites does not necessarily reduce the phenomenon but contributes to the opening and expansion of new marketplaces. (10) The inherent difficulty of dealing with this criminal trade and the money laundering associated with it, due to the anonymous and boundless nature of the dark web, which requires multidisciplinary initiatives, technological solutions, establishing procedures and methodologies for investigating crime in the dark web, and creating collaborations between organizations and countries to reduce the phenomenon, which reflects in the closure of these trading sites as well as worldwide arrests of those associated with this criminal trade and the money laundering carried out in the dark web.

This study shed light on the need both to analyze the current data and know about the surface web, the deep web, and the dark web, and the difficulty of relying on this information, and therefore, the difficulty of estimating accurately the malicious criminal and money laundering activities on the dark web. Even tougher, there is a need for combined, definite, comprehensive, and determined measures from corporates, international organizations, and governments to cope and reduce those criminal and malicious activities on the dark web, including money laundering.

References

Adamek, D. (November 20, 2019). Why finance should be terrified of the dark web. Financial Management Podcast. https://www.fm-magazine.com/podcast/dark-web-risks-for-finance-departments.html. [Accessed 16 December 2021].

Armstrong, M. (August 16, 2016). UK a hub for illicit drug sales. *Statista*. https://www.statista.com/chart/5511/uk-a-hub-for-illicit-drug-sales/. [Accessed 16 December 2021].

Armstrong, M. (2018). Drugs dominate the darknet. *Statista*. https://www.statista.com/chart/14464/drugs-dominate-the-darknet/. [Accessed 16 December 2021].

asn (February 26, 2015). Some statistics about onions. *Tor Blog*. https://blog.torproject.org/some-statistics-about-onions. [Accessed 16 December 2021].

Bar, N. (February 4, 2021). Israeli pleads guilty to money laundering on dark web, faces 20-year sentence. *Israel Hayom*. https://www.israelhayom.com/2021/04/02/israeli-pleads-guilty-to-money-laundering-faces-20-year-sentence/. [Accessed 16 December 2021].

Beckett, A. (November 26, 2009). The dark side of the internet. *The Guardian*. https://www.theguardian.com/technology/2009/nov/26/dark-side-internet-freenet. [Accessed 16 December 2021].

Bergman, M. K. (2001). The deep web: Surfacing hidden value. *Journal of Electronic Publishing*, 7(1). https://doi.org/10.3998/3336451.0007.104. [Accessed 16 December 2021].

Bisson, D. (June 29, 2020). Dark web — Scratching the surface and identifying the potential risks. *Tripwire*. https://www.tripwire.com/state-of-security/security-awareness/curiosity-dark-web-dangerous-effects/. [Accessed 16 December 2021].

Brandom, R. and Jeong, S. (July 29, 2017). Why the feds took down one of Bitcoin's largest exchanges. *The Verge*. https://www.theverge.com/2017/7/29/16060344/btce-bitcoin-exchange-takedown-mt-gox-theft-law-enforcement. [Accessed 16 December 2021].

Brewster, T. (June 1, 2015). Hackers scan all tor hidden services to find weaknesses in the "dark web." *Forbes*. https://www.forbes.com/sites/thomasbrewster/2015/06/01/dark-web-vulnerability-scan/?sh=3181a1606d23. [Accessed 16 December 2021].

Carapola, S. (April 17, 2017). Deep web: The 99% of the internet you can't see. https://www.amazon.com/Deep-Web-Internet-Cant-Everybody-ebook/dp/B06ZZXCMCX.

Chikada, A. (February 4, 2016). The Deep Web, darknets, Bitcoin and brand protection. *Law Business Research*. https://www.lexology.com/library/detail.aspx?g=effd0b0f-ddfa-400a-8a5f-6d6fb3b16dc7. [Accessed 16 December 2021].

Cimpanu, C. (February 15, 2021). 270 addresses are responsible for 55% of all cryptocurrency money laundering. *ZDNet*. https://www.zdnet.com/article/270-addresses-are-responsible-for-55-of-all-cryptocurrency-money-laundering/. [Accessed 16 December 2021].

CISO Platform (November 29, 2019). Understanding Surface Web, Dark Web, Deep Web and Darknet. https://cisoplatform.com/profiles/blogs/understanding-surface-web-dark-web-deep-web-and-darknet. [Accessed 16 December 2021].

Coinfirm (October 12, 2020). The evolution of cryptocurrency crime in the darknet. https://www.coinfirm.com/blog/cryptocurrency-crime-darknet/. [Accessed 16 December 2021].

Creative 3200 (August 21, 2018). What is the dark web and should you be worried about it? Paranet Solutions. https://www.paranet.com/2018/08/21/whats-on-the-dark-web-and-should-you-be-worried-about-it/. [Accessed 16 December 2021].

Chainalysis (2019). Crypto Crime Report: Decoding increasingly sophisticated hacks, darknet markets, and scams. https://go.chainalysis.com/2019-Crypto-Crime-Report.html. [Accessed 16 December 2021].

Darknet Stats (March 5, 2021a). Dark net markets comparison chart. https://www.darknetstats.com/dark-net-markets-comparison-chart/. [Accessed 16 December 2021].

Darknet Stats (2021b). The big list of darknet markets 2021 — Best darknet markets. https://dnstats.net/list-of-darknet-markets/. [Accessed 16 December 2021].

Department of Justice (May 29, 2015). Ross Ulbricht, A/K/A "Dread Pirate Roberts," sentenced in Manhattan Federal Court to life in prison. https://www.justice.gov/usao-sdny/pr/ross-ulbricht-aka-dread-pirate-roberts-sentenced-manhattan-federal-court-life-prison. [Accessed 16 December 2021].

Department of Justice (June 26, 2018). First nationwide undercover operation targeting darknet vendors results in arrests of more than 35 individuals selling illicit goods and the seizure of weapons, drugs and more than $23.6 million. https://www.justice.gov/opa/pr/first-nationwide-undercover-operation-targeting-darknet-vendors-results-arrests-more-35. [Accessed 16 December 2021].

Department of Justice (February 13, 2020). Ohio resident charged with operating darknet-based bitcoin "mixer," which laundered over $300 million. https://www.justice.gov/opa/pr/ohio-resident-charged-operating-darknet-based-bitcoin-mixer-which-laundered-over-300-million. [Accessed 16 December 2021].

Desjardins, J. (August 31, 2017). What happens in an internet minute in 2017? World Economic Forum. https://www.weforum.org/agenda/2017/08/what-happens-in-an-internet-minute-in-2017. [Accessed 16 December 2021].

Desjardins, J. (March 15, 2019). This is what happens in a minute on the internet. World Economic Forum. https://www.weforum.org/agenda/2019/03/what-happens-in-an-internet-minute-in-2019/. [Accessed 16 December 2021].

Dingledine, R., Mathewson, N. and Syverson, P. (2004). Tor: The Second-Generation Onion Router. [Accessed 16 December 2021].

DOMO (2020). Data never sleeps 8.0. https://www.visualcapitalist.com/every-minute-internet-2020/. [Accessed 16 December 2021].

Dragland, Å. (May 22, 2013). Big Data, for better or worse: 90% of world's data generated over last two years. *ScienceDaily*. https://www.sciencedaily.com/releases/2013/05/130522085217.htm. [Accessed 16 December 2021].

Elliptic (September 18, 2019). Bitcoin money laundering: How criminals use crypto. https://www.elliptic.co/blog/bitcoin-money-laundering. [Accessed 16 December 2021].

European Monitoring Centre for Drugs and Drug Addiction. (2017). Drugs and the darknet: Perspectives for enforcement, research and policy. https://doi.org/10.2810/834620. [Accessed 16 December 2021].

Feakin, T. (November 6, 2014). Cryptomarkets: Illicit goods on the darknet. *The Strategist*. https://www.aspistrategist.org.au/cryptomarkets-illicit-goods-on-the-darknet/. [Accessed 16 December 2021].

Financial Action Task Force (2014). Virtual currencies key definitions and potential AML. www.fatf-gafi.org. [Accessed 16 December 2021].

Fox, G. (May 23, 2018). What happens in an internet minute 2020. https://www.garyfox.co/what-happens-in-an-internet-minute-2018/. [Accessed 16 December 2021].

Fraud Watch International (November 2, 2018). The evolution of financial crime in the dark web. https://fraudwatchinternational.com/all/financial-crime-in-the-dark-web/. [Accessed 16 December 2021].

Gallagher, S. (April 3, 2016). Whole lotta onions: Number of Tor hidden sites spikes — along with paranoia. *Ars Technica.* https://arstechnica.com/information-technology/2016/03/whole-lotta-onions-number-of-tor-hidden-sites-spikes-along-with-paranoia/. [Accessed 16 December 2021].

GeeksforGeeks (November 17, 2020). Dark web analytics and interesting facts behind its anonymity. https://www.geeksforgeeks.org/dark-web-analytics-and-interesting-facts-behind-its-anonymity/. [Accessed 16 December 2021].

Gray, I. (2019). Pricing analysis of goods in cybercrime communities. https://go.flashpoint-intel.com/docs/analysis-pricing-of-goods-and-services-on-the-ddw. [Accessed 16 December 2021].

Guccione, D. (November 18, 2020). What is the dark web? How to access it and what you'll find. *CSO Online*. https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html. [Accessed 16 December 2021].

HHS Cybersecurity Program (2020). The dark web and cybercrime. https://www.hhs.gov/sites/default/files/dark-web-and-cybercrime.pdf. [Accessed 16 December 2021].

Ignoffo, Z. and Zoltan, M. (June 1, 2021). Dark Web Price Index 2021 — Dark web prices of personal data. *Privacy Affairs*. https://www.privacyaffairs.com/dark-web-price-index-2021/. [Accessed 16 December 2021].

Interpol (2020). Online African Organized Crime from Surface to Darkweb. Report. https://www.euneighbours.eu/sites/default/files/publications/2020-08/INTERPOL%20report.pdf. [Accessed 16 December 2021].

Interpol (n.d.). Darknet and cryptocurrencies. https://www.interpol.int/en/How-we-work/Innovation/Darknet-and-Cryptocurrencies. [Accessed 19 May 2021].

Irfan, A. (June 15, 2018). How much data is generated every minute? *Social Media Today*.https://www.socialmediatoday.com/news/how-much-data-is-generated-every-minute-infographic-1/525692/. [Accessed 16 December 2021].

Jardine, E., Lindner, A. M. and Owenson, G. (2020). The potential harms of the Tor anonymity network cluster disproportionately in free countries. *Proceedings of the National Academy of Sciences of the United States of America*, 117(50), 31716–31721. https://doi.org/10.1073/pnas.2011893117. [Accessed 16 December 2021].

Karr, D. (May 9, 2012). Big data brings marketing big numbers. *Martech Zone*. https://martech.zone/ibm-big-data-marketing/. [Accessed 16 December 2021].

Karr, D. (January 2, 2021). What are the types of the web (dark, deep, surface, & clear)? *Martech Zone*. https://martech.zone/types-clear-deep-dark-web/. [Accessed 16 December 2021].

Kaspersky (n.d.). Is the dark web dangerous? What you need to know. https://www.kaspersky.com/resource-center/threats/deep-web. [Accessed 27 April 2021].

LegalVision (July 19, 2020). Is it legal to access the deep web and use Tor? https://legalvision.com.au/is-it-legal-to-access-the-deep-web-and-use-tor/. [Accessed 16 December 2021].

Lewis, L. (March 10, 2020). Infographic: What happens in an Internet minute 2020. *Merge*. https://www.allaccess.com/merge/archive/31294/infographic-what-happens-in-an-internet-minute. [Accessed 16 December 2021].

Live Counter (n.d.). How big is the internet? (In petabyte). https://www.live-counter.com/how-big-is-the-internet/. [Accessed 23 March 2021].

Loechner, J. (December 22, 2016). 90% Of today's data created in two years. *MediaPost*. https://www.mediapost.com/publications/article/291358/90-of-todays-data-created-in-two-years.html. [Accessed 16 December 2021].

Loomly (n.d.). #Data — What happens in one Internet minute in 2017. https://toolkit.loomly.com/internet-minute-2017/. [Accessed 23 March 2021].

Mani, A., Wilson-Brown, T., Jansen, R., Johnson, A. and Sherr, M. (2018). *Understanding Tor Usage with Privacy-Preserving Measurement*. [Accessed 16 December 2021].

Marr, B. (2018). How much data do we create every day? The mind-blowing stats everyone should read. *Forbes*. https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/?sh=3966e50a60ba. [Accessed 16 December 2021].

McCarthy, N. (November 10, 2016). UK first in Europe for online sales of illicit drugs. *Statista*. https://www.statista.com/chart/6659/uk-first-in-europe-for-online-sales-of-illicit-drugs/. [Accessed 16 December 2021].

McCarthy, N. (May 31, 2017). The cost of an AK-47 on the black market. *Statista*. https://www.statista.com/chart/8759/the-cost-of-an-ak-47-on-the-black-market/. [Accessed 16 December 2021].

McCarthy, N. (March 23, 2018). Where guns are sold through the darknet. *Statista*. https://www.statista.com/chart/13327/where-guns-are-sold-through-the-darknet/. [Accessed 16 December 2021].

McGauley, J. (December 11, 2015). Everything you need to know about the deep web. *Thrillist*. https://www.thrillist.com/tech/nation/everything-you-need-to-know-about-the-deep-web. [Accessed 16 December 2021].

NodeGraph (March 26, 2020). How much data is on the internet? l The Big Data Facts Update 2020. https://www.nodegraph.se/how-much-data-is-on-the-internet/. [Accessed 16 December 2021].

NPR (May 25, 2014). Going Dark: The Internet Behind The Internet: All Tech Considered. https://www.npr.org/sections/alltechconsidered/2014/05/25/315821415/going-dark-the-internet-behind-the-internet. [Accessed 16 December 2021].

Pagliery, J. (March 10, 2014). The Deep Web you don't know about. *CNN*. https://money.cnn.com/2014/03/10/technology/deep-web/index.html. [Accessed 16 December 2021].

Persi Paoli, G., Aldridge, J., Ryan, N. and Warnes, R. (2017). Behind the curtain: The illicit trade of firearms, explosives and ammunition on the dark web. RAND Corporation. https://doi.org/10.7249/rr2091. [Accessed 16 December 2021].

Petrov, C. (March 18, 2021). 25+ Big data statistics — how big it actually is in 2021*? Tech Jury*. https://techjury.net/blog/big-data-statistics/. [Accessed 16 December 2021].

Popular Science (April 1, 2015). Most of the web is invisible to Google. Here's what it contains. https://www.popsci.com/dark-web-revealed/. [Accessed 16 December 2021].

Positive Technologies (2018a, July 25). Dark web markets 2018: Cyber crime statistics for darknet cyberservices and tools. https://www.ptsecurity.com/ww-en/analytics/darkweb-2018/. [Accessed 16 December 2021].

Positive Technologies (2018b, July 25). The criminal cyberservices market. https://www.ptsecurity.com/ww-en/analytics/darkweb-2018/. [Accessed 16 December 2021].

Pratham. (January 11, 2019). The deep web — 99% internet that you can't through Google. *Broggl*. https://www.broggl.com/the-deep-web-99-internet-that-you-cant-through-google/. [Accessed 16 December 2021].

Reinsel, D., Gantz, J. and Rydning, J. (2018). *The Digitization of the World From Edge to Core*.

Roy Choudhury, S. and Kharpal, A. (September 6, 2018). Beyond the valley: Understanding the mysteries of the dark web. *CNBC*. https://www.cnbc.com/2018/09/06/beyond-the-valley-understanding-the-mysteries-of-the-dark-web.html. [Accessed 16 December 2021].

Rubasundram, G. A. (2019). The dark web and digital currencies: A potent money laundering and terrorism opportunity. *International Journal of Recent Technology and Engineering*.

Schultz, J. (June 8, 2019). How much data is created on the internet each day? *Micro Focus Blog*. https://blog.microfocus.com/how-much-data-is-created-on-the-internet-each-day/. [Accessed 16 December 2021].

Siggia, S. (February 7, 2020). How do criminals launder their money using the Dark Web? *Pideeco*. https://pideeco.be/articles/dark-web-and-money-laundering/. [Accessed 16 December 2021].

Silfversten, E., Favaro, M., Slapakova, L., Ishikawa, S., Liu, J. and Salas, A. (2020). Exploring the use of Zcash cryptocurrency for illicit or criminal purposes. RAND Europe. [Accessed 16 December 2021].

Smith, C. (February 3, 2016). What happens on the Internet in one minute? *BGR*. https://bgr.com/2016/02/03/internet-activity-one-minute/. [Accessed 16 December 2021].

Starks, T. (March 21, 2021). DeepDotWeb boss pleads guilty to laundering millions. *CyberScoop*. https://www.cyberscoop.com/deepdotweb-tal-prihar-dark-web-darknet/. [Accessed 16 December 2021].

Statista (October 16, 2020). Survey on obtaining drugs from darknet in the Nordic countries 2018. https://www.statista.com/statistics/731329/survey-on-obtaining-drugs-from-darknet-in-the-nordic-countries/. [Accessed 16 December 2021].

Stone, J. (May 6, 2019). How many dark web marketplaces actually exist? About 100. *CyberScoop*. https://www.cyberscoop.com/dark-web-market places-research-recorded-future/. [Accessed 16 December 2021].

Strizek, J., Karden, A. and Horvath, I. (2019). Buying drugs on the dark net: Relevance of cryptomarkets, characteristics of purchasers and opportunities challenges for survey research. [Accessed 16 December 2021].

Taiwo, I. (2015). 90% of the internet is hidden from your browser; and it's called the Deep Web. *TechCabal*. https://techcabal.com/2015/11/18/90-of-the-internet-is-hidden-from-your-browser-and-its-called-the-deep-web/. [Accessed 16 December 2021].

TEDxWarwick. (December 4, 2017). Just How 'Dark' is the Dark Web? My fascination with the dark web all…. *TEDxWarwickBlog*. https://medium.com/tedxwarwick/just-how-dark-is-the-dark-web-1a4cfd582880. [Accessed 16 December 2021].

The Guardian (January 20, 2016). Ten arrested in Netherlands over bitcoin money-laundering allegations. https://www.theguardian.com/technology/2016/jan/20/bitcoin-netherlands-arrests-cars-cash-ecstasy. [Accessed 16 December 2021].

Thompson, C. (December 16, 2015). Difference between Dark Web and Deep Web. *Tech Insider*. https://www.businessinsider.com/difference-between-dark-web-and-deep-web-2015-11. [Accessed 16 December 2021].

Tor Project (2021). Onion Services — Tor Metrics. https://metrics.torproject.org/hidserv-dir-onions-seen.html?start=2021-01-01&end=2021-04-26. [Accessed 16 December 2021].

Twitter (December 26, 2015). Ehacking on Twitter: "What happens in an Internet minute. https://twitter.com/ehackingdotnet/status/680789959788355585?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E680789959788355585%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fbgr.com%2F2016%2F02%2F03%2Finternet-activity-one-minute%2F. [Accessed 16 December 2021].

UNODC (2017a). World Drug Report 2017 — Global Overview of Drug Demand and Supply. www.unodc.org/wdr2017. [Accessed 16 December 2021].

UNODC (2017b). World Drug Report 2017 — Executive Summary Conclusions and Policy Implications. https://www.unodc.org/wdr2017/field/Booklet_1_EXSUM.pdf. [Accessed 16 December 2021].

UNODC (2018). World Drug Report 2018 — Global Overview of Drug Demand and Supply. https://www.unodc.org/wdr2018. [Accessed 16 December 2021].

UNODC (2019). World Drug Report 2019 — Global Overview of Drug Demand and Supply. https://wdr.unodc.org/wdr2019/prelaunch/WDR19_Booklet_2_DRUG_DEMAND.pdf. [Accessed 16 December 2021].

US Department of the Treasury (March 2, 2020). Treasury sanctions individuals laundering cryptocurrency for Lazarus Group. https://home.treasury.gov/news/press-releases/sm924. [Accessed 16 December 2021].

Users — Tor Metrics (2021). Tor Project. https://metrics.torproject.org/userstats-relay-country.html?start=2021-01-01&end=2021-04-26&country=all&events=on. [Accessed 16 December 2021].

van Buskirk, J., Roxburgh, A., Bruno, R., Naicker, S., Lenton, S., Sutherland, R., Whittaker, E., Sindicich, N., Matthews, A., Butler, K. and Burns, L. (2016). Characterising dark net marketplace purchasers in a sample of regular psychostimulant users. *International Journal of Drug Policy*, 35, 32–37. https://doi.org/10.1016/j.drugpo.2016.01.010. [Accessed 16 December 2021].

Victors, J., Li, M. and Fu, X. (2017). The Onion name system. *Proceedings on Privacy Enhancing Technologies*, 2017(1), 21–41. https://doi.org/10.1515/popets-2017-0003. [Accessed 16 December 2021].

Wassén, O. (October 26, 2018). Big Data facts — How much data is out there? *NodeGraph*. https://www.nodegraph.se/big-data-facts/. [Accessed 16 December 2021].

Weber, J. and Kruisbergen, E. W. (2019). Criminal markets: The dark web, money laundering and counterstrategies — An overview of the 10th Research Conference on Organized Crime. *Trends in Organized Crime*, 22(1). https://www.researchgate.net/publication/332685663_Criminal_markets_the_dark_web_money_laundering_and_counterstrategies_-_An_overview_of_the_10th_Research_Conference_on_Organized_Crime. [Accessed 16 December 2021].

Wells, N. (November 8, 2019). Dark web drug trafficker pleads guilty to money laundering. Organized Crime and Corruption Reporting Project. https://www.occrp.org/en/daily/11076-dark-web-drug-trafficker-pleads-guilty-to-money-laundering. [Accessed 16 December 2021].

This page intentionally left blank

https://doi.org/10.1142/9781800612839_0007

Chapter 6

Cyber Terrorism and Organized Crime

Georg Thomas

Introduction

The Internet as we know it was born in the 1980s, but it was not until the 1990s that mainstream adoption of the Internet was observed. Back then, the Internet was expensive, its accessibility was limited, and it was often slow and unreliable, with dial-up modem being the primary method of connection. Fast forward to the 2000s, when technological advancements and implementation of supporting infrastructure began to address these issues and it was not long before the use of the Internet exploded. It is estimated that at the end of 2019, there were four billion Internet users worldwide, representing over half of the world's population (ITU, 2019).

Transactions that traditionally took place in the kinetic world, such as buying and selling goods and services, communicating with one other, and even establishing new relationships, have shifted or are at least in part have been augmented by the Internet. The ability to leverage the Internet is so great, and arguably the value it creates sufficiently compelling, that we have seen a multitude of innovations across all industries, including consumer, commercial, and government. Collectively referred to as the Internet of Things (IoT), this technological advancement has meant that many everyday devices now have "smart" capabilities (Williams *et al*., 2017, p. 179). The Internet has shaped the way society operates and has provided many useful applications that many of us could not imagine living without.

While the evolution of the Internet has been positive in many respects, the value of these technologies has not gone unnoticed by criminal and terrorist actors. Just as society has leveraged the Internet to transact, criminal and terrorist actors have also leveraged the Internet or "cyber" technologies to conduct activities that we previously performed in the physical or kinetic world and with greater benefits, which will be discussed later in this chapter.

Defining Organized Crime and Terrorism

Since the origin of human civilization, the notion of right and wrong and the use of laws have existed. Laws are rules created to regulate behavior and distinguish those citizens in society that behave in a manner that is considered acceptable and ethical from those that are not. Even thousands of years ago, during the Roman Empire, laws were in place to regulate society, and those that broke laws were punished through imprisonment or fighting to death in the gladiator arenas (Pike, 1873, p.13).

Such extreme forms of punishment as fighting to death may be outdated, but crime is not, and it is something that has continued to evolve with society. Crime can be defined as a violation of law (Wu and Wu, 2012) and is an issue that is experienced across the world. Any individual or group that breaks the law is considered to be a criminal, but this chapter will focus on organized crime and terrorist groups, which will be explored in detail.

Organized Crime

There is generally no widely accepted definition of organized crime (Abadinsky, 2012), but contemporary interpretations highlight that organized crime usually consists of groups that conduct illegal activities for the purpose of financial gain and have some formalized structure. When we think of organized crime groups, we often think of those portrayed in movies and television or reported in the media such as the Italian Mafia, Russian Mafia (Bratva), Mexican Cartel, or Yakuza. In reality, there are thousands of organized crime groups across the world with even the well-known groups identified consisting of multiple groups. The National Strategic Assessment of Serious and Organized Crime 2018 report published by the National Crime Agency in the United Kingdom identified

4,629 organized crime groups in the UK at the end of 2017 (National Crime Agency, 2018).

Organized crime groups operate in a similar way to any other business; they have structure, operating models, long-term strategies, and their purpose is to generate revenue, estimated in the billions, and to do so while minimizing risk (Interpol, n.d.). Common areas of crime that organized crime groups operate in include fraud, counterfeiting, drug trafficking, sex trafficking, human trafficking, murder, kidnapping, extortion, theft, financial crime and money laundering, and tax evasion (Federal Bureau of Investigation, n.d.).

Terrorist Groups

Terrorist groups are another form of organized crime, and while there is no exact definition, terrorists are described as motivated by belief rather than financial motivation, often associated with furthering political or religious goals through committing enough violence against persons or property to generate fear (Denning, 2000). Although it can be argued that traditional organized crime groups also commit violence and generate fear and therefore could also be considered terrorist groups, their primary motivations differ, and each group will be discussed separately in this chapter.

Terrorist groups are well known for committing devastating crimes perpetuating widespread fear, often through bombings and massacres, such as Black September, who were responsible for the Munich Massacre in 1972 at the Summer Olympics (Reeve, 2011); the Liberation Tigers of Tamil Eelam (LTTE), who, for over three decades, were engaged in violent terrorist activities in Sri Lanka (van de Voorde, 2005, p. 181); Al-Qaeda, which has a global terrorist network and is known to have committed the 9/11 attacks in the United States (Gunaratna, 2002, p. 50); and in more recent years, the Islamic State of Iraq and the Levant (ISIL) and the Islamic State of Iraq and Syria (ISIS), which have made headlines around the globe.

The Evolution of Cybercrime

Organized crime and terrorist groups, like the rest of the world, have evolved. While criminal activities and terrorist attacks still take place in

the physical world, these groups now also utilize cyberspace to conduct a host of activities, being able to reap the same benefits that have been observed by the rest of society.

It is important to define cyberspace in order to understand the context of this chapter. The National Institute of Standards and Technology (NIST, n.d.), a US Government agency within the US Department of Commerce, defines cyberspace as follows: "A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."

Cyberspace has provided the opportunity for many types of operations to be moved into the digital world, and we began to see the evolution of cyber terrorism and cybercrime. Like terrorism, there is no official definition of cyber terrorism. However, Denning (2000) provides a good definition of cyber terrorism, describing it as terrorism converged with cyberspace. To complicate the matter, terrorism is classified by purpose or motive (Higgins, 2002, p. 22). This means that terrorism can be carried out by any group whose purpose or motive falls within the scope of terrorism as identified. In some instances, events are considered cyber terrorism because of the impact that occurred. Although events such as bombings, shootings, stabbings, and arson, to name a few, still occur, cyber terrorism has enabled several new attack vectors, and what is considered a terrorism event has now gained a broader scope.

There are many examples of cyberattacks, and a few notable examples of significant attacks that are linked to either terrorist groups, nation states, or organized crime are as follows:

1998 — Denial of Service Attacks on Sri Lankan Embassies were conducted by the LTTE in 1998. This attack resulted in Sri Lankan embassies receiving over 800 e-mails per day for over two weeks (Houle and Pandey, 2018, p. 1). While 800 e-mails per day might not seem massive by today's standards, back in 1998 when connections were significantly slower and the capacity of ICT systems much less, this would have had a much larger impact and subsequently resulted in a denial of service (DOS) scenario.

2017 — WannaCry is a variant of ransomware that blocks access to files on the victim's system by encrypting them and requiring the payment of a ransom in order to regain access to the files (Mohurle and Patil, 2017,

p. 1938). The Lazarus Group, which is a North Korean state-sponsored group, is believed to be behind the WannaCry cyberattacks in 2017. This cyberattack inflicted widespread damage, including to the UK National Health Service (NHS), whose systems were crippled and over 19,000 appointments cancelled (Taddeo and Floridi, 2018).

2017 — NotPetya was another ransomware-based attack that occurred in 2017. This attack was attributed to Sandworm Team, who have been active for a number of years and been associated with several Ukrainian Power Authority incidents (Fireeye, 2016). Alleged to be Russian military intelligence, Sandworm Team are well known for the NotPetya attacks in 2017 (United States Department of Justice, 2020, p. 289). Similar to the WannaCry attacks, the NotPetya attacks resulted in the encryption of victim's files and the payment of a ransom to obtain the decryption keys to regain access. This attack also resulted in widespread damage, crippling organizations across the globe.

2021 — Colonial Pipeline is a pipeline system for refined oil in the US, which supplies 45% of the US East Coast's diesel, petrol, and jet fuel (Russon, 2021). In May 2021, the Colonial Pipeline was the victim of a ransomware attack, which resulted in the operator going offline. This attack was attributed to a Russian cybercriminal group called Darkside. However, the group stated that they did not intend to create problems and their stated motives were purely financial, which resulted in Colonial Pipeline paying over USD 4.4 million (Shackelford and Wade, 2021). The impact of this attack means that it can be considered an act of terrorism.

2021 — JBS are the world's largest meat suppliers and were the victim of a ransomware attack in May 2021 (Lerman, 2021). Believed to be attributed to the cybercriminal group REvil, which is believed to be based out of Russia, several of the company's operations were disrupted across the globe, and the company subsequently paid USD 11 million in order to recover their data and resume operations.

The first example, where the LTTE attacked the Sri Lankan embassy, was an example of a group classified as terrorists using cyber as an attack vector and is often classified as a terrorism event despite the attack not utilizing violence. There are other examples, such as the 1998 attack of the Institute for Global Communications (IGC) by Spanish protesters and

the 1999 attack of NATO computers during the Kosovo conflict (Denning, 2000). In addition to events that had direct impact, cyberspace has also provided a medium for recruitment of cyber terrorists and sharing of information, with groups such as Al-Qaeda and ISIS/ISIL often utilizing not only websites but also social media channels to promote their causes (Stohl, 2006, p. 223).

The other examples identify the threat actors as criminal groups and nation states. While these examples are all ransomware related, which requires a ransom to be paid and is often regarded the primary motive, this may not always be the case. Quite often within the cybersecurity field, tools can be used for multiple purposes and motives. For example, tools used for security testing can be utilized by ethical and malicious actors (Thomas *et al*., 2018, p. 122). Similarly, a cyberweapon such as NotPetya may not have been primarily used for financial gain, but to test the efficacy of the weapon at achieving another objective. With this in mind, ransomware-based cyberattacks are often used for financial gain.

Risk versus Reward

The transition to cyber often results in lower risk and higher returns. Although many activities are still undertaken in the physical world, there are several examples where cyberspace has been leveraged and is lucrative and carries less risk.

Cyberspace provides greater reach due to the borderless nature of the Internet, and organized crime and terrorist groups are no longer limited by their location and are able to operate globally and remotely. Historically, most organized crime still occurs in the physical world, and it was thought that cybercrime was more often the work of individuals (Grabosky, 2007, p. 158). However, in more recent years, there have been many instances of organized crime groups operating in cyberspace, as highlighted by some of the examples in the previous sections. Many cases of ransomware and business e-mail compromise (BEC) are often attributed to organized crime groups.

Attribution has always been one of the difficulties when investigating any cyber-related incident. Criminal groups and terrorists are able to leverage technologies that can make identification difficult, if not near impossible. This is further exacerbated by jurisdictional issues across international borders.

Virtual Private Networks

Virtual Private Networks or VPNs are services that allow subscribers to route their Internet traffic through in order to obfuscate their location and obtain some level of anonymity. These services are designed for the purpose of maintaining personal privacy but are often misused by threat actors as a cover. A threat actor located in one country would route through a VPN endpoint in a completely different country, which is what the victim will see, thus hiding their true origin.

Proxy servers

Similar to VPNs, proxy servers are designed to provide a level of anonymity and obfuscation. However, proxy servers provide less flexibility as they are often limited in the type of Internet traffic that can be passed through them, whereas VPNs often are able to pass any network traffic. One benefit of proxy servers is that there are several free services available. Most VPNs require registration and sometimes a paid subscription.

The Onion Router

The Onion Router, commonly referred to as TOR, is a free open-source network that relays traffic through different servers called "relay nodes" (Huang and Bashir, 2016, p. 1). Again, the goal of TOR is to protect the privacy of those that use the service. Not only can threat actors leverage TOR to conduct attacks, but this network is also used to access the dark web, which contains a host of illegal sites. This includes marketplaces for selling illegal goods and services to forums and sites used to spread ideas and information by terrorists (Chen *et al*., 2008, p. 1349).

Compromised systems

This list is not exhaustive and there are a multitude of methods and technologies used by criminals to conduct their operations. The use of malware and command-and-control technologies to control remote systems is still common, and in addition, the last few years have seen an increase in organizations that have either had e-mail compromised (BEC) or their servers breached due to poor security. These systems are then used to

launch further attacks either directly or in an attempt to further hide the true location of the attack.

Funding Organized Crime and Terrorism

The lower risk versus reward of using cyber has resulted in an increase in funding through cyberattacks. The risks of committing a robbery or selling contraband in person is likely to be much higher than committing those offenses remotely.

Hacking

With origins as far back as the 1960s, the term hacking was coined by programmers at MIT to describe someone who had the ability to manipulate technology (Thomas *et al*., 2018, p. 113). Since then, the definition has evolved, and hackers are most commonly recognized as individuals who break into computer systems. Although the intent of a hacker can vary (e.g., ethical, malicious, or otherwise), when applied in the context of organized crime and terrorism, these hackers are malicious in behavior and they often use their skills for financial gain. Although any type of cyberattack is often attributed to "hackers," including those that follow below, for context, hacking refers to breaking into a system by exploiting a weakness such as poor architecture, controls, or vulnerabilities in the system. There have been several different ways through which hacking techniques have been used to generate money. Often a ransomware attack begins by hacking into a system and subsequently planting the ransomware, and in other instances, exploited systems have been used to generate cryptocurrency through a process called "mining."

Business e-mail compromise (*BEC*)

Over the past few years, BEC has been a common attack vector. Through the use of phishing techniques, where the victim is sent an e-mail that requires them to provide their login details, threat actors are able to gain access to a victim's mailbox and carry out a number of operations, including wire fraud or conducting further phishing campaigns, often against the victim's contacts. In the early days of BEC, e-mails were often generic and much easier to spot, nowadays, the level of sophistication has resulted

in the identification of malicious e-mails, and the subsequent landing page becoming more difficult. There have been several instances where threat actors have intercepted transactions and requested funds to be redirected to different bank accounts, often impersonating corporate executives such as CEOs and CFOs. In 2019, the US Department of Justice, in collaboration with several other agencies globally, arrested 281 individuals, including those with ties to organized crime who were responsible for carrying out BEC attacks (United States Department of Justice, 2019).

Ransomware

The 2017 WannaCry and NotPetya cyberattacks or the 2016 Locky ransomware attacks often come to mind when we hear the term ransomware. However, ransomware dates back to 1989, when evolutionary biologist Joseph Popp created the AIDS trojan, which he distributed by sending floppy disks (O'Kane *et al*., 2017, p. 3). Ransomware blocks access to files on the victim's systems, most often by encrypting the information. In order to regain access, the victim must obtain the decryption key by paying the threat actor a ransom. In more recent examples of ransomware, ransom was paid with Bitcoin cryptocurrency, which was attractive due to the widespread belief that it had some level anonymity (Moser, 2013).

Money Laundering and the Emergence of Digital Money

Defining money laundering can be difficult, according to legal definitions, laundering can be considered something as simple as accepting proceeds of crime as well as the act of sanitizing proceeds of crime so that the funds appear to be legitimately acquired (Levi and Reuter, 2006, p. 292). Simply put, money laundering is the act of hiding proceeds of crime. Many of us are familiar with the counting rooms and pallets of money often depicted in movies and television. The transport of physical money, often across borders, is still widely practiced and utilizes a variety of methods, including baggage, couriers, freight, concealment, false declarations, vehicles, and planes (Financial Action Task Force, 2015). Moving money across borders to fund terrorism or organized crime is one of the oldest techniques to avoid government scrutiny (Zdanowicz, 2004, p. 53). The emergence of digital money has enabled new ways of transacting that often less

risky and in near-real time. As identified earlier, criminal organizations and terrorist groups often operate in the same way as businesses, and in order to continue operating and carrying on their activities, they generate revenue through various means, which is often then laundered to make the income look legitimate.

Regulation and legislation

In order to combat money laundering, regulation and legislation has been introduced in many countries. The intent of the regulation is to help identify and prevent money laundering and the subsequent financing of terrorism and organized crime.

Anti-Money Laundering and Counter-Terrorism Financing Act (2006) is an Australian legislation that requires financial institutions, and various other entities to take a number of steps such as validating a customer's identity before providing services and to report suspicious individuals/organizations and certain transactions above a threshold. In addition, there are a number of requirements around registration with specific government bodies (Australian Government, 2020, p. 6).

The ***Bank Secrecy Act (BSA)*** is a US federal law that came into effect in 1970 and requires banks to have controls in place, such as records and reports, and to notify law enforcement where appropriate. It is intended for use in criminal tax, regulatory investigations, and intelligence activities, including preventing terrorism (United States Government, 1982, p. 376).

The 5th Anti-Money Laundering Directive (5AMLD) came into force in January 2020 and is a European Union Directive for the prevention of money laundering or terrorist financing, which includes enhanced controls when dealing with countries that do not have anti-money laundering and terrorism controls, information-sharing requirements, restrictions on prepaid cards, and the inclusion of virtual currency providers (EUR-Lex, 2018).

International Convention for the Suppression of the Financing of Terrorism is a United Nations treaty that requires member countries to criminalize the funding of terrorism, including holding legal entities

liable. It requires that no act that falls within the scope of the treaty is justifiable, whether it is political, philosophical, ideological, racial, ethnic, religious, or otherwise (United Nations, 1999). In addition to specific anti-money laundering and terrorism funding regulation and legislation, some countries have cyber-related regulation and legislation that allows the government additional powers for investigation.

Clarifying Lawful Overseas Use of Data (CLOUD) Act of 2018 was introduced to allow the US government to compel US-based technology companies to provide data held offshore such as in cloud services (US Congress, 2018).

Lawful Access to Encrypted Data (LAED) Act of 2020 was a bill introduced in 2020. Similar to the TOLA Act described below, the LAED Act of 2020 is intended to compel technology companies to provide access to encrypted information to law enforcement (US Congress, 2020).

Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, otherwise known as the TOLA Act, is an Australian law that would allow law enforcement and intelligence agencies the ability to compel service providers to provide access to encrypted communications (Thomas, 2018).

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 was introduced after the September 11, 2001, terrorist attacks in the US. The Act is intended to protect the US from terrorist threats and allows enhanced surveillance procedures, anti-money laundering requirements, as well as strengthening laws against terrorism (United States Government, 2001).

More often than not, regulation and legislation is introduced in response to a significant adverse event. For example, the USA PATRIOT Act 2001 was introduced following the September 2001 terrorist attacks in the US and the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and the LAED Data Act of 2020 were introduced after the struggles of the US Federal Bureau of Investigation (FBI) in accessing encrypted data on Apple devices in the wake of the San Bernardino terrorist attack in 2015 (Thomas, 2016). Similarly, the

CLOUD Act 2018 was introduced after the Microsoft Ireland case in 2018 (Daskal, 2018).

Legal challenges

There are several identified challenges with regulation and legislation and views on the effectiveness of regulation and legislation as well as concerns. Many of the laws that allow law enforcement and government agencies to obtain access to information such as the CLOUD Act, TOLA Act, USA PATRIOT Act, and LAED Act have come under scrutiny due to privacy and security concerns.

Privacy concerns can be due to both cultural factors and conflict with laws from other jurisdictions. For example, the European Union General Data Protection Regulation (GDPR) has significant requirements to protect the privacy of EU persons, and subsequently there is potential for conflict with other laws such as the CLOUD Act. In addition, there has been discussion on whether providers could create weaknesses in their systems in order to be able to comply with law enforcement orders, such as the LAED Act and TOLA Act.

With the significant increase in ransomware — in many instances, the only way for a victim of ransomware to recover from such an attack is to pay the ransom — there are also concerns about whether paying the ransom could be in breach of any other laws. It is possible that any payment of a ransom is funding organized crime or terrorism, but this often cannot be determined because attribution is often difficult, if not impossible.

In addition to privacy concerns, cross-jurisdictional issues often impact the ability of law enforcement to investigate cyberattacks. Although this largely depends on the specifics of the attack, often when attacks originate from another jurisdiction, the investigations are limited. There are obvious exceptions, such as when it falls within international criminal law or a treaty, but once again this may not be applicable to all jurisdictions. Attacks such as ransomware attacks and BEC often go unsolved and unattributed.

Virtual currency

There are many regulations and legislations that can help thwart money laundering. As discussed earlier, banks and other financial institutions are

often required to undertake a certain level of validation as well as report any large or suspicious transactions. This is one of the benefits of a centralized and regulated model.

In 2009, that changed with the inception of Bitcoin and cryptocurrency (Ciaian *et al*., 2016, p. 1799). Known as virtual currency, as of 2021, there are hundreds of them, and due to their decentralized nature, they are borderless, resilient to bank failures, and largely unregulated. At present, ransomware attacks require payment in virtual currency, namely Bitcoin, although threat actors are starting to utilize other cryptocurrencies such as Monero due to greater focus on maintaining privacy (Wilson, 2019).

There are calls to better control virtual currency with examples such as The 5th Anti-Money Laundering Directive (5AMLD) discussed earlier already including requirements to help combat the use of virtual currency for criminal or terrorist purposes. There have also been examples of law enforcement seizing ransomware payments that have been paid using virtual currency. In June 2021, the FBI were able to recover USD 2.3 million of the Bitcoins that were paid as part of the Colonial Pipeline ransom (United States Department of Justice, 2021).

Mitigating the threat

It is clear that the use of technology is a lucrative method for organized crime and terrorist groups to carry out attacks and fund themselves and with reduced risks than traditional methods. Like society in general, it is likely that the use of technology by these types of threat actors is going to continue and evolve. Although it is likely to be impossible to mitigate such threats completely, there are a number of areas that could be improved in order to limit the possibility for successful attacks now and in the future.

Preventing Attacks

The saying "prevention is better than cure" is highly applicable with regard to cybersecurity. Arguably, organizations have improved their cybersecurity posture over the past few years, yet the ongoing media reports of organizations falling victim to ransomware and other attacks implies that there is still a significant amount of work to be done. Prevention can be divided into three areas:

Defensive strategies

Defensive strategies are focused on preventing threat actors from conducting a successful attack. While prevention is not guaranteed, every organization should implement a baseline level of defensive controls to minimize their attack surface. This includes implementation of controls such as firewalls, anti-malware, application whitelisting, endpoint threat detection and response, multi-factor authentication, vulnerability management and up-to-date patching, least privilege access, system hardening, encryption, data leakage prevention, security awareness training and education, and good overall security hygiene.

Offensive strategies

Offensive strategies are focused on identifying where weaknesses exist in an organization. Security professionals who possess the same skills often use the same tools as malicious hackers. They are often referred to as security testers, white hat hackers, penetration testers, or ethical hackers who are engaged to attempt to "break-in" to an organization. They will use a combination of hacking techniques and social engineering (where they try and manipulate people) to meet their objectives.

The security testers engaged by an organization are typically referred to as the "Red Team." They conduct their operations against the defending team, whether it be the security team of an organization or an outsourced function, who are referred to as the "Blue Team." Such engagements often occur without the "Blue Team" knowing they are being attacked. When the "Red Team" and the "Blue Team" work collaboratively, this is known as a "Purple Team" engagement. Such engagements are valuable as they feedback can be provided in real time rather than a report at the end.

Governance, standards, and frameworks

In addition to defensive and offensive strategies, there are governance, standards, and frameworks. At the very basic level, organizations should have formally developed and implemented security policies. These policies often cover areas such as access control, network security, password security, acceptable use, change management, and supplier security. As organizations mature, the implementation of standards and frameworks should be considered. Standards and frameworks provide best practices

and tried and tested approaches. Organizations should also ensure they meet the requirements of any applicable regulatory bodies. Two of the most widely adopted standards and frameworks are ISO/IEC 27001:2013 and the NIST Cyber Security Framework.

ISO/IEC 27001:2013 is an Information Security Management System (ISMS) is a standardized approach to managing information security. The current version of the standard consists of 114 controls (International Organization for Standardization, n.d.). The standard is divided into two sections, the ISO 27001 mandatory controls and the Annex A controls, which are selected based on applicability from the results of a risk assessment.

NIST Cyber Security Framework (CSF) is a framework developed by the National Institute of Standards and Technology, which is designed to help organizations improve their management of cyber security risk (National Institute of Standards and Technology, n.d.). The framework includes areas relating to identifying and protecting assets, as well as recovering and responding to cyberthreats.

Regulation

Although significant amount of regulation already exists, consideration should be given to ensuring that the regulation of emerging technologies such cryptocurrency, artificial intelligence, and quantum computing, to name a few, is sufficient. While the European Union and the United Kingdom have some regulation of virtual currency through 5AMLD, most other countries do not. It is important to also consider cultural and cross-jurisdictional issues of regulation and legislation, which significantly adds to the complexity of achieving a uniformed outcome.

The Organization for Economic Co-operation and Development (OECD) have developed a joint program designed to help policymakers get the most out of technology as well as safeguard the public. However, at the time of writing, this program titled "OECD Recommendation on Agile Regulatory Governance to Harness Innovation" was still in public consultation (OECD, 2021). It is crucial that regulation of technologies are developed both in view of the future as well as retrospectively.

Cross-jurisdictional enhancements

One area that is of significant impact is the ability for cross-jurisdictional cooperation. Although there are some jurisdictions that are unlikely to cooperate, further cooperation from those jurisdictions that are friendly and willing to would be advantageous. In order to help reduce the threats, collaboration and a collective effort is needed. While many cyberattacks are often perceived as small, there is the possibility that they originate from many of the same threat actors and subsequently the ability to investigate across borders, identify the threat actor, and prosecute will benefit citizens globally.

References

Abadinsky, H. (2012). *Organized Crime*. Cengage Learning.

Australian Government (2020). Anti-Money Laundering and Counter-Terrorism Financing Act (2006), Canberra. https://www.legislation.gov.au/Details/C2020C00362. [Accessed 4 March 2021].

Chen, H., Chung, W., Qin, J., Reid, E., Sageman, M. and Weimann, G. (2008). Uncovering the dark web: A case study of Jihad on the web. *Journal of the American Society for Information Science and Technology*, 59(8), 1347–1359.

Ciaian, P., Rajcaniova, M. and Kancs, D. A. (2016). The economics of BitCoin price formation. *Applied Economics*, 48(19), 1799–1815.

Daskal, J. (2018). Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0, *Stanford Law Review*. https://www.stanfordlawreview.org/online/microsoft-ireland-cloud-act-international-lawmaking-2-0/. [Accessed 31 May 2021].

Denning, D. E. (2000). Cyberterrorism: Testimony before the special oversight panel on terrorism committee on armed services US House of Representatives, *Focus on Terrorism*, 9.

EUR-Lex (2018). Directive (EU) 2018/843 of the European Parliament and of the Council. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843. [Accessed 1 June 2021].

Federal Bureau of Investigation (n.d.). Organized Crime. https://www.fbi.gov/investigate/organized-crime. [Accessed 1 June 2021].

Financial Action Task Force (2015). FATF Report — Money Laundering Through Physical Transportation of Cash. https://www.fatf-gafi.org/media/fatf/documents/reports/money-laundering-through-transportation-cash.pdf. [Accessed 1 June 2021].

Fireeye (2016). Sandworm Team and the Ukraine Power Authority Attacks. *Threat Research Blog*. https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html. [Accessed 1 June 2021].

Grabosky, P. (2007). The internet, technology, and organized crime. *Asian Journal of Criminology*, 2(2), 145–161.

Gunaratna, R. (2002). *Inside Al Qaeda: Global Network of Terror*, Columbia University Press.

Higgins, R. (2002). The general international law of terrorism. In *Terrorism and International Law*, Flory, M. and Higgins, R. (eds.), London: Routledge, pp. 27–43. https://doi.org/10.4324/9780203429365.

Houle, C. and Pandey, R. (2018). A layered approach to defending against list-linking email bombs. *2018 APWG Symposium on Electronic Crime Research (eCrime)*, pp. 1–9.

Huang, H. Y. and Bashir, M. (2016). The Onion router: Understanding a privacy enhancing technology community. *Proceedings of the Association for Information Science and Technology*, 53(1), 1–10.

International Organization for Standardization (n.d.). ISO/IEC 27001 — Information Security Management. https://www.iso.org/isoiec-27001-information-security.html. [Accessed 3 May 2021].

Interpol (n.d.). Organized crime. https://www.interpol.int/en/Crimes/Organized-crime.

ITU (2019). Statistics, International Telecommunications Union. https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx. [Accessed 15 March 2021].

Lerman, R. (2021). JBS paid $11 million in ransom after hackers shut down meat plants, *Washington Post*. https://www.washingtonpost.com/technology/2021/06/09/jbs-11-million-ransom/. [Accessed 11 June 2021].

Levi, M. and Reuter, P. (2006). Money laundering. *Crime and Justice*, 34(1), 289–375.

Mohurle, S. and Patil, M. (2017). A brief study of WannaCry threat: Ransomware attack 2017. *International Journal of Advanced Research in Computer Science*, 8(5), 1938–1940.

Moser, M. (2013). Anonymity of bitcoin transactions.

National Crime Agency (2018). National Strategic Assessment of Serious and Organised Crime. https://www.nationalcrimeagency.gov.uk/who-we-are/publications/173-national-strategic-assessment-of-serious-and-organised-crime-2018/file. [Accessed 1 June 2021].

National Institute of Standards and Technology (n.d.). Cyberspace — Glossary. https://csrc.nist.gov/glossary/term/cyberspace. [Accessed 23 April 2021].

O'Kane, P., Sezer, S. and Carlin, D. (2018). Evolution of ransomware, *IET Networks*, 7(5), 321–327.

Organization for Economic Co-operation and Development (2021). Better regulation and innovation. https://www.oecd.org/gov/regulatory-policy/regulation-and-emerging-technologies.htm. [Accessed 10 June 2021].

Pike, L. O. (1873). *A History of Crime in England: Illustrating the Changes of the Laws in the Progress of Civilisation* (Vol. 1), Smith, Elder & Company.

Reeve, S. (2011). *One Day in September: The Full Story of the 1972 Munich Olympics Massacre and the Israeli Revenge Operation "Wrath of God"*. Skyhorse Publishing Inc.

Russon, M. (2021). US fuel pipeline hackers 'didn't meant to create problems.' *BBC*. https://www.bbc.com/news/business-57050690. [Accessed 9 June 2021].

Shackelford, S. and Wade, M. (2021). Colonial Pipeline forked over $4.4M to end cyberattack — but is paying a ransom ever the ethical thing to do? *The Conversation*. https://theconversation.com/colonial-pipeline-forked-over-4-4m-to-end-cyberattack-but-is-paying-a-ransom-ever-the-ethical-thing-to-do-161383. [Accessed 11 June 2021].

Stohl, M. (2006). Cyber terrorism: A clear and present danger, the sum of all fears, breaking point or patriot games? *Crime, Law and Social Change*, 46(4–5), 223–238.

Taddeo, M. and Floridi, L. (2018). Regulate artificial intelligence to avert cyber arms race. *Nature*, 556, 296–298.

Thomas, G. (2016). Hacking the terror suspect's iPhone: What the FBI can do now Apple says 'no'. *The Conversation*. https://theconversation.com/hacking-the-terror-suspects-iphone-what-the-fbi-can-do-now-apple-says-no-55135. [Accessed 1 June 2021].

Thomas, G. (2018). Ethics Part 5: Could encryption legislation increase the risk of being hacked? *ACS Information Age*. https://ia.acs.org.au/article/2018/ethics-part-5--could-encryption-legislation-increase-risk-of-bei.html. [Accessed 1 June 2021].

Thomas, G., Low, G. and Burmeister, O. (2018). "Who was that masked man?": System penetrations — Friend or foe? In *Cyber Weaponry*. Prunckun, H. (ed.), Springer, Cham, pp. 113–124.

United Nations (1999). International Convention for the Suppression of the Financing of Terrorism. https://www.un.org/law/cod/finterr.htm. [Accessed 1 June 2021].

United States Department of Justice (2019). 281 arrested worldwide in coordinated international enforcement operation targeting hundreds of individuals in business email compromise schemes. https://www.justice.gov/opa/pr/281-arrested-worldwide-coordinated-international-enforcement-operation-targeting-hundreds. [Accessed 1 June 2021].

United States Department of Justice (2020). Six Russian GRU officers charged in connection with worldwide deployment of destructive malware and other disruptive actions in cyber space: Unsealed indictment. https://www.justice.gov/opa/press-release/file/1328521/download. [Accessed 1 June 2021].

United States Department of Justice (2021). Department of Justice Seizes $2.3 million in cryptocurrency paid to the ransomware extortionists Darkside.

https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside. [Accessed 12 June 2021].

United States Government (1982). Bank Secrecy Act. https://www.govinfo.gov/content/pkg/USCODE-2012-title31/pdf/USCODE-2012-title31-subtitleIV-chap53-subchapII-sec5311.pdf. [Accessed 1 June 2021].

United States Government (2001). Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001. https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf. [Accessed 1 June 2021].

US Congress (2018). H.R.4943.- CLOUD Act. https://www.congress.gov/bill/115th-congress/house-bill/4943. [Accessed 2 June 2021].

US Congress (2020). S.4051 — Lawful Access to Encrypted Data Act. https://www.congress.gov/bill/116th-congress/senate-bill/4051?r=1&s=1. [Accessed 2 June 2021].

van de Voorde, C. (2005). Sri Lankan terrorism: Assessing and responding to the threat of the Liberation Tigers of Tamil Eelam (LTTE). *Police Practice and Research*, 6(2), 181–199.

Williams, R., McMahon, E., Samtani, S., Patton, M. and Chen, H. (2017). Identifying vulnerabilities of consumer Internet of Things (IoT) devices: A scalable approach. In *2017 IEEE International Conference on Intelligence and Security Informatics (ISI)*, pp. 179–181.

Wilson, T. (2019). Explainer: 'Privacy coin' Monero offers near total anonymity. *Reuters*. https://www.reuters.com/article/us-crypto-currencies-altcoins-explainer-idUSKCN1SL0F0. [Accessed 2 June 2021].

Wu, D. and Wu, Z. (2012). Crime, inequality and unemployment in England and Wales. *Applied Economics*, 44(29), 3765–3775.

Zdanowicz, J. S. (2004). Detecting money laundering and terrorist financing via data mining. *Communications of the ACM*, 47(5), 53–55.

This page intentionally left blank

Part II

Countermeasures and International Response

This page intentionally left blank

https://doi.org/10.1142/9781800612839_0008

Chapter 7

Evolution of Legal and Regulatory Responses to Money Laundering Risks Related to Virtual Assets: The Examples of the European Union and the US

Tanya Gibbs

Introduction

From its inception in early 2000, the virtual asset (VA) industry has been evolving at an astronomical speed, endlessly producing new classes of assets, products, and services, forming a new VA economy. Terms such as virtual currency (VC), cryptocurrency, tokenization, and blockchain have entered mainstream vocabulary and transformed the conventional understanding of assets. VC, also referred to as cryptocurrency, drew broad attention from the general media and public after the price of Bitcoin skyrocketed from USD 7,200 at the start of 2020 to USD 18,353 on November 23, 2020, ultimately reaching USD 41,528 on January 8, 2021. The jump in value left individual and institutional investors stunned, considering that Bitcoin started trading at around USD 0.08 in 2010 (Edwards, 2021). According to *Forbes*, Bitcoin's performance in 2020 led some firms to start holding it "as a treasury asset" (del Castillo, 2021). Though analysts propose various explanations for this surge, the overall rapid growth and development of the VA ecosystem, propelled by advances in encryption and network technologies, has transformed the "valuation,

exchange and accounting of economic assets and commercial transactions," removing institutional intermediaries from transactions (Abboushi, 2017, p. 10).

Rowland and Kiviat (2018, p. 90) observe that "the digital asset market extends beyond the assets themselves," as new participants such as "online exchanges, payment processors and mining companies," are forming "the broader digital asset industry." Despite its many advantages, this transformation engenders new risks and unique challenges due to its susceptibility to criminal abuse (FATF, 2021, pp. 15–18). According to the Financial Crimes Enforcement Network (FinCEN), criminals have used VAs, specifically convertible virtual currencies (CVCs), "to facilitate criminal activity such as human trafficking, child exploitation, fraud, extortion, cybercrime, drug trafficking, money laundering, terrorist financing, and to support rogue regimes and facilitate sanctions evasion" (FinCEN, 2019a, p. 2). Therefore, implementation of laws and regulations aimed at preventing and mitigating these risks have gone hand-in-hand with the industry growth. Criminals have always been agile in adopting new methods and technologies to circumvent laws. This was the case with prepaid cards, online banking, internet payments, electronic wallets, smart cards, etc. Traditionally, regulators and legislators have responded to these developments by incorporating new instruments, types, and typologies to the traditional laws in a patchwork fashion. This has also been the case with addressing risks related to what are now termed VAs.[1] As a result, numerous VAs are not regulated because they fall outside of legal frameworks.

VAs' unique characteristics have a distinctive risk profile which creates a need for new legislative approaches. Poskriakov *et al*. (2018, p. 165) stress that "most VCs by definition trigger a number of ML/TF (money laundering and terrorist financing) risks due to their specific features, including anonymity (or pseudonymity), traceability and

[1] "A virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes" (FATF, 2012–2020, p. 130). VAs include VCs or cryptocurrencies, and digital tokens offered through Initial Coin Offerings (ICOs) and Security Token Offering (STO), but they "do not include digital representation of fiat currencies" (FATF, 2012–2020, p. 130). A VA is often referred to as a crypto-asset, which the European Security and Market Authority (ESMA) defines as "a type of private asset that depends primarily on cryptography and Distributed Ledger Technology (DLT)" (ESMA, 2019a, p. 4).

decentralization." These risks spread beyond VCs per se to "the surrounding ecosystem of issuers, exchangers and users" (Poskriakov *et al*., 2018, p. 165).

Speed, anonymity, low cost, and global reach attract criminals to VAs (EBA, 2014, pp. 32–37). FinCEN attributes their financial crime vulnerabilities "to the global nature, distributed structure, limited transparency, and speed of the most widely utilized virtual currency systems" (FinCEN, 2019a, p. 1). The VA ecosystem has been exploited for a wide spectrum of criminal activities, including money laundering (ML) offences where VA products and services are used for transferring, collecting, and layering criminal proceeds (FATF, 2020c, p. 4). The European Banking Authority (EBA) identified ML/TF risks for VCs as high (EBA, 2014, p. 22). These reasons for the criminal attraction to VA products and services have also been impediments for the successful detection, investigation, and prosecution of illegal activities using conventional law enforcement mechanism and tools. It is challenging for law enforcement to trace criminal proceeds by monitoring decentralized VC transactions conducted on blockchain due to their anonymity. In the absence of intermediaries, which can detect and report suspicious transaction to a competent authority, the VA ecosystem is an ideal environment to launder criminal proceeds. Furthermore, its borderless nature presents challenges for prosecution. Divergence in countries' responses to integrating VA services into their domestic financial markets and regulating VA service providers (VASPs)[2] produces additional global ML/TF challenges. While some countries started regulating VA products and services, others have ignored or completely prohibited them. This has led to discrepancies in the global regulatory system, creating loopholes for criminal exploitation and abuse.

This chapter surveys the evolution of legislative and regulatory efforts put forth by the European Union (EU) and the US to mitigate ML/TF risks posed by VA products and services. It also identifies issues pertained to uniformed international approach to the AML/CFT regulation of VAs and VASPs.

[2]"VASPs include VA exchanges and transfer services; some VA wallet providers, such as those that host wallets or maintain custody or control over another natural or legal person's VAs, wallet(s), and/or private key(s); providers of financial services relating to the issuance, offer, or sale of a VA (such as in an ICO); and other possible business models" (FATF, 2019a, p. 14).

VAs

Though the terms "digital," "crypto," and "virtual" have been used interchangeably in the context of assets and currencies in specific, it is important to point out that they have different meanings. Digital currency (also known as digital money, cyber cash, electronic money, electronic currency) is a broader concept which encompasses virtual (or crypto) currencies (Frankenfield and Anderson, 2021). EBA (2019, p. 4) defines VAs (or crypto-assets in the EU context) as "a type of private asset that depend primarily on cryptography and distributed ledger technology (DLT) as part of their perceived or inherent value." VAs include VCs or cryptocurrencies and digital tokens offered through Initial Coin Offerings (ICOs) or Security Token Offering (STO). FATF (2012–2020, p. 76) advises countries to consider VAs as "property," "proceeds," "funds," "funds or other assets," or other "corresponding value."

VCs

A VC is a type of digital currency. EBA (2014, p. 11) defines a VC as "digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency (FC) but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically." Though it is nominated as "currency," it does not fit the traditional definition of currency (Abboushi, 2017, p. 10). FinCEN (2013) defines a VC as "a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency." The EU's 5th Anti-Money Laundering Directive (5AMLD) specifies that VCs should not be confused with electronic money due to their broad purposes of use, which in addition to payment, also includes "exchange, investment, store-of-value products or use in online casinos" (5AMLD, 2018, p. 45). It defines it as "a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically" (5AMLD, 2018, p. 54). The fact that VCs are not issued by central banks and are not pegged to fiat currencies makes them less susceptible to government

manipulations and inflation (Tu and Meredith, 2015, p. 283). A VC is not a legal tender and is only accepted among the members of a specific virtual community (Perez, 2019). There are several categories of VCs. They can be centralized, controlled by an individual(s), or decentralized; and convertible or non-convertible to fiat currency (Abboushi, 2017, pp. 11–12). FinCEN defines a CVC "as a medium of exchange (such as cryptocurrency) that either has an equivalent value as currency, or acts as a substitute for currency, but lacks legal tender status" (FinCEN, 2020, p. 68006).

The VC market is fast-growing. EBA (2014, p. 10) reports over 200 different VC schemes in circulation. Though there are many different types of VCs, the best known is Bitcoin, which was created in 2009. Based on DLT, VC transactions are conducted on peer-to-peer basis without any intermediaries. The latter contributes to the low cost and rapidity of transactions; hence it attracts many users (Tu and Meredith, 2015). VC transactions are executed around the clock, on 24/7 basis. They are non-reversible and difficult to intercept (Nakamoto, 2008; Acheson *et al*., 2020). Today's aggregate value of all the cryptocurrencies in existence is around USD 1.5 trillion, with Bitcoin representing more than 60% of this value (Frankenfield and Sonnenshein, 2021).

Cryptocurrency

"A cryptocurrency is a digital or virtual currency that is secured by cryptography" (Frankenfield and Sonnenshein, 2021). The latter feature makes it difficult to counterfeit. Many cryptocurrencies operate as blockchain-based decentralized systems (Perez, 2019). Online cryptocurrency payments are denominated in tokens. The cryptocurrency industry is rapidly expanding. For example, one of the world's largest cryptocurrency exchanges, Binance, in 2020 listed 184 tokenized assets and had a total trading volume of close to USD 2 trillion (del Castillo, 2021).

Initial Coin Offering

"An initial coin offering (ICO) is the cryptocurrency industry's equivalent to an initial public offering (IPO)," allowing companies to raise fund

(Frankenfield, 2020). Investors receive digital tokens from the issuer in exchange for a fiat or cryptocurrency. Tokens do not only represent "a holder's right of benefit" but they can also be used "for payment to the issuing company for its services or products" (Wockener and Freudenberger, 2019). Unlike IPOs, tokens typically do not grant ownership rights to its holders (Massey *et al*., 2017, p. 5). By investing in ICOs, token holders gain a direct benefit from the company's growth. Klayman (2018, pp. 61–62) points out that there is "no single 'paradigmatic' token." Its definitions vary as "U.S. regulators may, at various times and sometimes at the same time, view a token alternatively as property (the IRS), a commodity (the CFTC), money (FinCEN) or a security (the SEC)" (Klayman, 2018, p. 62).

ICOs has been growing rapidly since its first introduction in 2014. Only three years after the introduction, USD 2.3 billion has been raised by blockchain start-ups (Leloup, 2017). In 2019, ICOs raise only for cryptocurrency industry USD 14.8 billion (Statista, 2021). Long (2018) describes the rapid growth of the ICO market in comparison to the traditional IPO as follows:

> "The initial coin offering (ICO) market — defined as capital raised on open blockchains via token sales — was 45% and 31% of the traditional IPO and venture capital markets during Q2 2018, respectively, up from 40% and 30%, during Q1 2018. ICO volume during Q2 2018 was approximately $7.2 billion, according to Coindesk, while the US IPO market raised $16.0 billion (as reported by PwC), and US venture capital markets raised $23 billion (as reported by CB Insights and PwC) during the same period."

Security Token Offering

Deloitte *et al*. (2020, p. 3) define Security Token Offerings (STOs) as "a regulated offering of securities using blockchain technology." What makes it different from regular securities is that it combines "technology of blockchain with the requirements of regulated securities markets" (Deloitte *et al*., 2020, p. 1). Contrary to ICOs, under the STO, the tokens are termed a financial instrument. The first STO was offered in 2018 in the US followed by the "flood of new tokenization platforms" (Hamilton, 2020).

Financial Action Task Force Recommendations

The development of the Financial Action Task Force (FATF) recommendations has reflected rapid technological development and expansion of VA ecosystem. To assist jurisdictions in AML/CFT efforts, FATF has systematically issued documents addressing ML/TF risks associated with new, digital financial instruments engendered by rapidly growing Internet technologies. In 2014, FATF introduced a definition for and classifications of VCs. In addition, it identified potential risks associated with various types of VCs by applying the risk factors of Section IV (A) of the 2013 Guidance for a Risk-Based Approach (RBA) to New Payment Products and Services (NPPS) (FATF, 2013). In 2015, FATF issued the Guidance for a RBA to Virtual Currencies in regard to ML/TF risks related to VC payments and services (FATF, 2015). A rapidly developing VA ecosystem, coupled with the emergence of new products, services, business models, and activities, has produced new ML/TF risks, which require continuous revising and updating of VA regulatory supervision and oversight. While the 2015 FATF Guidance addressed ML/TF risks mainly focusing on convertible virtual security exchanges (CVSEs), the points of intersection of VC with the traditional financial system, by 2018, FATF has expanded AML/CFT regulations to VAs and VASP activities, which may consist of only "virtual-to-virtual" activities, completely bypassing the fiat currency financial system (FATF, 2021, p. 6). A year later, it issued an Interpretative Note to the Recommendation 15 with further clarification on requirements concerning VA activities and VASPs (FATF, 2012–2020, pp. 76–77). Following these initiatives, a 12-month review of the FATF member countries demonstrated that while 35 out of 54 jurisdictions implemented the revised FATF Standards into their national law, 19 did not do so. The review also showed that the majority of members, 32, introduced the VASP regulations. However, three countries prohibited the operation of VASPs on their territories all together (FATF, 2020b). In 2019, the FATF issued Guidance for a RBA to VAs and Virtual Asset Service Providers (VASP), to assist jurisdictions with developing effective AML/CTF regulatory and supervisory framework for VA activities and VASPs (FATF, 2019a, 2019b). The Guidance requires VASP licensing or registration, supervision, and monitoring by a competent authority.[3] The competent authority has the power to "impose a range of

[3] It cannot be "a self-regulatory body (SRB)" (FATF, 2019a, p. 24).

disciplinary and financial sanctions, including the power to withdraw, restrict or suspend the VASP's license or registration," in case of its failure to comply with this requirement (FATF, 2019a, p. 24, 56). In 2021, FATF revised the 2019 Guidance on VAs and VASPs. The new draft refined the VA and VASP definitions, making them more inclusive of all possible financial assets. It also updated sections on licensing and registration requirements for VASPs and expanded guidance on application of the FATF Standards to "so-called stablecoins"[4] and on implementation of the "travel rule."[5] In addition, the revised Guidance highlighted potential ML/TF risks associated with peer-to-peer (P2P) transactions (FATF, 2021, pp. 14–15). It is important to stress that P2P transactions are not subject to the AML/CFT compliance. However, FATF warns these transactions "can be potential used to avoid the AML/CFT controls imposed on VASPs and obliged entities" (FATF, 2021, p. 14). Moreover, the updated Guidelines outlined "Principles of Information-Sharing and Co-operation between VASP Supervisors" (FATF, 2021, pp. 91–95).

Requirements for Regulating VA and VASPs

Absence of regulations has been one of the attractions of VA products and services for legitimate users as well as money launderers. Many VAs still operate outside of legal oversight, which makes their transactions inexpensive due to the absence of financial intermediaries and regulatory compliance costs. This lack of regulatory supervision has created risks not only for individuals but also for financial institutions and markets.

The main challenge to regulating VAs lies in their interpretation. Since VAs "can represent an asset or ownership of an asset, such as a currency, commodity, security, or a derivative on a commodity or security" they can fall under security or other financial instrument regulations (IOSCO, 2020, p. 3).

---

[4]FATF uses "so-called stablecoin" not "stablecoin," according to its own explanation, "to avoid unintentionally endorsing" stablecoin as "a marketing term used by promoters of such coins" (FATF, 2020d, p. 2). Hayes and Mansa (2020) define stablecoin as "a new class of cryptocurrencies that attempts to offer price stability and are backed by a reserve asset."

[5]"Travel rule" is "the application of the FATF wire transfer requirements in the VA context" (FATF, 2021, p. 52).

RBA

As early as 2014, FATF has addressed ML/TF risks presented by VC payment products and services (VCPPS) and proposed a guidance to help jurisdictions establish robust national legislative and regulatory frameworks for companies to identify and mitigate these risks (FATF, 2015). Application of the RBA, prescribed in Recommendation 1, requires identification, assessment, understanding, and taking actions to effectively mitigate the country's ML/TF risks, including the ones associated with VAs, VASPs, and other new technologies (FATF, 2012–2020, p. 10; FATF, 2019a, p. 19). FATF states that "jurisdictions should individually examine VAs and VASP activities in the context of their own financial sectors and regulatory and supervisory systems to arrive at an assessment of their risk" (FATF, 2021, p. 10). FATF's early Guidance (2015) mainly focuses on convertible VCs and articulated it by "its higher risks," associated with "convertible virtual currency exchangers which are points of intersection that provide gateways to the regulated financial system" (FATF, 2015, p. 4). It also makes a distinction between centralized and decentralized VC payment products and services (VCPPS), which remain a key aspect in ML/TF risk assessment and mitigation measures (FATF, 2019a, p. 19).

FATF advises "to identify, assess, and apply a RBA to mitigate the ML/TF risks associated with VCs under the relevant FATF Regulations" even to jurisdictions that do not regulate VCs outside of the ML/TF spheres (FATF, 2015, p. 9). Furthermore, it urges countries prohibiting VCPPS assess the impact of this prohibition on the overall ML/TF risks, as it might promote illegal, "underground" use of VC payments which bypasses the AML/CFT controls (FATF, 2015, p. 9).

Registration or licensing requirements

As the VC sector continued to broaden, in 2015, FATF instructed jurisdictions to develop regulations for domestic registration or licensing requirements for VCPPS and for convertible VC service providers (CVCSP) (FATF, 2015, p. 8, 10). FATF also recommended jurisdictions to apply the RBA to regulate financial institutions and designated non-financial business and profession (DNFBP) "that send, receive, and store VC" (FATF, 2015, p. 6, 12). It stressed that this regulation and supervision requirement may call for amending the national laws by including convertible VC

"nodes,"[6] and decentralized VC payment mechanisms to the AML/CTF legal framework (FATF, 2015, p. 10). In 2019, its Guidance has expanded to the establishment of "comprehensive regulatory and supervisory framework" for VA activities and VASPs "as well as other obliged entities operating in the VA space" (FATF, 2019a, p. 20).

By 2021, FATF has broadened the VA and VASP registration or licensing requirements from the jurisdiction of their creation to "the jurisdiction where their business is located in cases where they are a natural person," and to countries, they conduct business if it is required by the local authorities (FATF, 2021, p. 5). The 2021 draft Guidance also compels local authorities "to identify natural or legal persons that carry out VA activities without the requisite license or registration" (FATF, 2021, p. 5).

Recordkeeping and travel rule

Financial institutions and DNFBPs have to maintain VC transaction records. These should include "information to identify the parties; the public keys, addresses or accounts involved; the nature and date of the transaction, and the amount transferred" (FATF, 2015, p. 13). FATF argues that requirements for the customer identification, verification, and recordkeeping will help jurisdictions to apply "effective, proportionate and dissuasive," criminal, civil or administrative sanctions (FATF, 2012–2020, p. 26; FATF, 2015, pp. 10–11). Convertible VC exchanges as per FATF Recommendation 16, are required to specify "originator and beneficiary information" and to establish a threshold of USD/EUR 1,000 for cross-border wire transfers (FATF, 2012–2020, p. 17, 69, 77; FATF, 2015, p. 10; FATF, 2021, p. s5).

Customer due diligence

In 2015, FATF extended the customer due diligence (CDD) requirement to convertible VC exchanges, requiring them to conduct CDD at the customer intake and at the point of transactions "using reliable, independent source documents, data or information" (FATF, 2015, p. 12). The 2015 Guidance notes that since VC transactions are completed entirely via

[6]CVC nodes are gateways to the regulated fiat currency financial system (FATF, 2015, p. 6).

Internet, verification and corroboration of customer identity using national IDs, third-party databases, Internet Protocol (IP) address, and other reliable sources must be carried out in accordance with the country's privacy law (FATF, 2015, pp. 12–13). The same Guidance requires to apply enhanced due diligence (EDD) to convertible decentralized VCPPSs, as they encompass higher ML/TF risks due to anonymity (FATF, 2015, p. 8). FATF suggests that technology-based solutions, such as application programming interfaces (APIs), may help institutions to comply with customer identification (FATF, 2015, p. 14). In its most recent updates to the Guidance, FATF requires entities engaged in VA activities and VASPs to apply ongoing CDD processes. The institutions are responsible for setting an effective procedure to identify and verify the customer identity in the following cases:

- "when establishing business relations with that customer;
- where VASPs may have suspicions of ML/TF, regardless of any exemption of thresholds;
- where they have doubts about the veracity or adequacy of previously obtained identification data" (FATF, 2021, p. 46).

Countries may also require CDD on VA transfers or transactions performed by VASPs, including "occasional transactions," for amounts below the USD/EUR 1,000 threshold (FATF, 2021, p. 47, 73). Ongoing due diligence and monitoring obligations for VASPs includes up-to-date document keeping by undertaking periodic reviews of existing records (FATF, 2021, p. 49). Finally, FAFT recommends VASPs to avoid entering into business with or terminate an existing relationship with the customer on whom they "cannot apply the appropriate level CDD." In these cases, they should also file a suspicious transaction report (STR) (FATF, 2021, p. 74).

FATF recommends countries to "strengthen the requirements for higher-risk situations or activities involving VAs." When VAs and VASPs are regarded as higher ML/TF risks, application of monitoring and EDD is advised (FATF, 2021, p. 35, 47, 76). Companies should consider "country- or geographic-specific risk factors" of VASPs locations or VA transfers as they can potentially present higher ML/TF risks. The "nature of VA products, services, transactions, or delivery mechanisms" must also be weighed in the risk assessment (FATF, 2021, pp. 47–48).

Furthermore, if VASPs' corporate clients are engaged in trade finance, they are encouraged to collect the following information on high-risk customers and transactions:

(a) "the purpose of transaction or payment;
(b) details about the nature, end use or end user of the item;
(c) proof of funds ownership;
(d) parties to the transaction;
(e) sources of wealth and/or funds;
(f) the identity and the beneficial ownership of the counterparty; and
(g) export control information, such as copies of export-control or other licenses issued by the national export control authorities, and end-user certification" (FATF, 2021, pp. 48–49).

Suspicious transaction report

VASPs have to comply with applicable suspicious transaction report (STR) requirements "even when operating across different jurisdictions" (FATF, 2021, p. 81). FATF points that VASPs should flag, scrutinize, and report to the FIU suspicious transactions regardless of whether they are "fiat-to-fiat, virtual-to-virtual, fiat-to-virtual, or virtual-to-fiat in nature" (FATF, 2021, p. 80). Absence of required information, such as of originator or beneficiary, in transfers involving VA or VASPs should be a trigger for reporting them to the FIU (FATF, 2021, p. 81). FATF (2020a) outlines the following indicators to help VASPs detect and report suspicious transactions:

- Transaction size
- Transaction patterns
- Anonymity
- Senders or recipients profiles
- Source of funds
- Geographical risks

Coordination and cooperation

Public–private sector cooperation is crucial for developing AML/CFT effective policies for the VASP sector. Starting in 2015 FATF has urged

AML/CFT stakeholders, including financial institutions, national authorities, DNFPB, and convertible currency exchanges, to conduct risk assessment of VC products and services and to apply measures to prevent and mitigate them in accordance with the country's laws (FATF, 2015, p. 8). Development and implementation of robust policies regulating and supervising VA activities and VASPs in regard to ML/TF risks require interagency cooperation among "policymakers, regulators, supervisors, the financial intelligence unit (FIU), and law enforcement authorities" (FATF, 2019a, p. 20). Cooperation should not stop there. An international approach, or as the EBA (2014, p. 43) stresses "ideally global, coordination" is required, "otherwise it will be difficult to achieve a successful regulatory regime." Lack of cooperation and cohesiveness in the international response applies broadly to the whole AML/CFT system, that "suggests that governments need to work harder collectively to make the AML system fit for purpose" (*The Economist*, 2021).

Coordination and information sharing are crucial for investigating, mitigating, preventing, and prosecuting crime. To enable it, FATF proposes setting "national coordination mechanisms" that will facilitate cooperation and coordination between AML/CFT authorities (FATF, 2012–2020, pp. 10–11; FATF, 2015, p. 9). Due to the transnational nature of cyber laundering, international cooperation is integral for effectiveness of AML/CFT measures (FATF, 2012–2020, pp. 27–30; FATF, 2015, p.10). This cooperation can take form of either information and intelligence sharing on STRs or actual legal assistance. Countries' cooperation in the VC space should include mutual legal assistance with identification, freezing, seizure, and confiscation proceeds of crime and extradition assistance (FATF, 2015, p. 11). In 2021, FATF has proposed Principles of Information-Sharing and Cooperation (the Principles). They require an establishment of VASP supervisors who would be responsible for setting mechanisms for receiving inquiries and for maintaining a secure database of public registers or information on licensed or registered VASPs. The information between supervisors can be exchanged bilaterally, upon request, or multilaterally. The Principles include recommendations for the establishment of "supervisory colleges" for sharing less sensitive information. Parties requesting information should always specify a reason for it. The receipt of requested information should also be acknowledged. If available and legally permitted, supervisors should share "a VASP's regulatory status, details of its shareholders and directors, transaction-related data and customer information (which could have been obtained from

supervisory activities, statutory returns, and blockchain surveillance and analytical tools)" (FATF, 2021, p. 93). Supervisors cannot refuse an information request based on the following reasons:

> (a) "laws require FIs, DNFBPs or VASPs (except where the relevant information that is sought is held under circumstances where legal privilege or legal professional secrecy applies) to maintain secrecy or confidentiality;
>
> (b) there is an inquiry, investigation or proceeding underway in the country receiving the request, unless the assistance would impede that inquiry, investigation or proceeding; and/or
>
> (c) the nature or status of the requesting counterpart authority is different to its foreign Supervisor" (FATF, 2021, p. 93).

The principles emphasize proactiveness and timeliness in information sharing and effectiveness in co-operation between foreign supervisors. Supervisors "should be able to conduct queries on behalf of foreign supervisors, and exchange with these foreign supervisors all information that they would be able to obtain" (FATF, 2021, p. 94).

EU Laws and Regulations

The EU has been slow in adopting a regulatory regime for VAs and VASPs though it recognized and acknowledged their risks early. Starting in 2013, several EU authorities have issued a series of warnings to customers on risks associated with VCs. On December 12, 2013, the EBA issued a warning about numerous risks deriving from "buying, holding or trading virtual currencies such as Bitcoins," due to absence of regulations and supervision for virtual currencies (EBA, 2013, p. 1). One of these risks was the shutdown of a VC exchange platform by law enforcement agencies if it was incriminated in money laundering (EBA, 2013, p. 3). This statement was followed by a series of similar warnings issued by the EBA, the European Securities and Markets Authority (ESMA), and the European Insurance and Occupational Pensions Authority (EIOPA) highlighting multiple risks including criminal uses of VCs and ICOs for money laundering purposes (EBA, 2014; ESMA, 2017a, 2017b, 2018). In

2017, ESMA alerted investors about ICOs' regulatory risks of not complying with relevant applicable EU legislation.

The EU regulations of VAs are based on whether VAs qualify as financial instruments under Regulation on Markets in Financial Instruments (MiFID II), or they function outside of the regulated zone (MiFID II, 2014). In cases when VAs do not qualify as financial instruments, they remain unregulated, posing substantial risks to individual and institutional investors. If a VA is qualified as a financial instrument, then it will be regulated by the following legal provisions:

- The Directive on Investor-Compensation Schemes (DoICS), which requires all Member States to have "an investor-compensation scheme or schemes to which every such investment firm would belong" (DoICS, 1997, p. 22).
- The Prospectus Directive (PD), which mandates "the provision of full information concerning securities and issuers of those securities promotes, together with rules on the conduct of business, the protection of investors" (PD, 2003, p. 65).
- The Transparency Directive (TD), which requires periodic and ongoing "disclosure of accurate, comprehensive and timely information about security issuers" (TD, 2004, p. 2).
- The Settlement Finality Directive (SFD), which specifies settlement procedures in the case of insolvency (SFD, 2009).
- The Alternative Investment Fund Managers Directive (AIFMD), which lays down the rules "for the authorisation, ongoing operation and transparency of the managers of Alternative Investment Funds Managers (AIFMs) which manage and/or market Alternative Investment Funds (AIFs) in the Union" (AIFMD, 2011, p. 2).
- The EU's Second Directive on Market in Financial Instruments (MiFID II), a revised Initial Directive on Markets in Financial Instruments (MiFID I), which established a regulatory framework for investment services in financial instruments. MiFID II mandates companies providing "investment services or perform investment activities in financial instruments" to register and comply with the legal requirements stated in MiFID II. It extends the scope of regulations to data reporting service providers, "Organized Trading Facility" (OTF), high-frequency algorithmic trading, and "third country firms providing investment services or activities in the Union" (MiFID II, 2014, p. 350; Gesley, 2018).

- The EU's Regulation on Markets in Financial Instruments (MiFIR), a supplement to MiFID II, which establishes uniform requirements for investment firms authorized under MiFID II composed of the following:
  (a) "disclosure of trade data to the public;
  (b) reporting of transactions to the competent authorities;
  (c) trading of derivatives on organised venues;
  (d) non-discriminatory access to clearing and non-discriminatory access to trading in benchmarks;
  (e) product intervention powers of competent authorities, ESMA and EBA and powers of ESMA on position management controls and position limits;
  (f) provision of investment services or activities by third-country firms following an applicable equivalence decision by the Commission with or without a branch" (MiFIR, 2014, pp. 95–96).
- The Market Abuse Regulation (MAR) prohibiting "insider dealing, unlawful disclosure of information or market manipulation" in financial instruments (MAR, 2014, p. 2).
- The Central Securities Depositories Regulation (CSDR), imposing identical requirements on CSDs aimed "to reduce the regulatory complexity for market operators and CSDs [Central securities depositories] resulting from different national rules," and to allow CSDs "to provide their services on a cross-border basis without having to comply with different sets of national requirements such as those concerning the authorisation, supervision, organisation or risks of CSDs" (CSDR, 2014, p. 2).

Just as an example, the ICO is regulated by the Prospectus Directive (PD), ensuring provision of adequate information to investors; the Markets in Financial Instruments Directive (MiFID), ensuring investor protection; AIFMD provides rules for "the authorisation, ongoing operation and transparency of the managers" (ESMA, 2017a, p. 2). Despite this robust regulatory regime, EBA (2019, p. 18) acknowledges that "the vast majority of cases, activities involving crypto-assets fall outside the scope of the supervisory remits of the competent authorities" of the EU and national laws. The ESMA (2019a, pp. 39–40) concurs, pointing out that "only a fraction of them [crypto-assets] are likely to qualify as MiFID financial instruments" and are operating outside of the EU financial laws and regulations. To address this issue, the ESMA (2019a, p. 40) suggests

the EU policymakers implement "a bespoke regime for the crypto-assets that do not qualify as financial instruments." It also stressed that Anti-Money Laundering (AML) requirements "should apply to all activities involving crypto-assets" (ESMA, 2019b).

Consistency in and convergence of the national AML/CFT regimes across the EU is stipulated in and guaranteed by the EU's Money Laundering Directives. The EU's 4th Anti-Money Laundering Directive (4AMLD) set forth the CDD, record-keeping, reporting of suspicious activities rules, and cooperating requirements for authorities in ML/TF investigations, aligning the EU member-states' laws with the FATF recommendations and guidance (4AMLD, 2015). In 2016, the EU Commission proposed amending the 4AMLD by classifying "custodian wallet providers" (CWPs)[7] and "virtual currency exchange platforms" (VCEPs) as "obliged entities", consequently including them into the scope of the regulations (EU, 2016, p. 6). The proposal also included the registration and licensing requirements for these entities at national levels (EBA, 2016, p. 2). Another proposed amendment by the EU Commission concerned an establishment of "centralized bank and payment account registers or electronic data retrieval systems …, which would provide FIUs and other competent authorities with access to information on bank and payment accounts" (EC, 2016). The 2016 EU Resolution on VCs supported the Commission's proposal to include VC exchange platforms in the 4AMLD (European Parliament, 2016, p. 6). On the EU Council's request, the EU Commission conducted an assessment of the ML/TF risks in the internal market, which revealed high threat and vulnerability of VCs to ML/TF (EC, 2017a, pp. 86–87). As a result, European legislators agreed to add VC exchanges and wallet providers to the scope of the Anti-Money Laundering Directive. The EU's 5th Anti-Money Laundering Directive (5AMLD), adopted in May 2018 and signed into law in 2020, extended the scope of application of the AML/CFT requirements to VC exchange platforms and custodian wallet providers (5AMLD, 2018, p. 44). It also extended licensing or registration requirement for these institutions (5AMLD, 2018, p. 67). The 5AMLD also addressed VC risks related to the anonymity, by instructing national financial intelligence unit (FIU) to obtain information required to link virtual currency

[7]"'Custodian wallet provider' means an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies" (5AMLD, 2018, p. 54).

addresses to the identity of the VC owner. It also considered the possibility of allowing users "to self-declare to designated authorities on a voluntary basis" (5AMLD, 2018, p. 44). The 5AMLD stressed importance of efficiency and coordinated approach for FIUs' investigations related to terrorism and the misuse of VCs (5AMLD, 2018, p. 46).

Though yet to be implemented, the EU's 6th Anti-Money Laundering Directive (6AMLD), which came into effect on December 3, 2020, broadened the scope of money laundering by adding "aiding and abetting, inciting and attempting" and cybercrime to the list of predicate offences (6AMLD, 2018, pp. 27–28). Money laundering is a transnational crime; often jurisdictions where a predicate offence was committed and where the proceeds of the crime was laundered are different. This is especially relevant in the context of VAs. The new directive not only urges Member States to address new risks associated with VCs but also stresses the need to "intensify" internal cooperation among member states and external with "third countries," which should be accompanied by "effective and timely information sharing" (6AMLD, 2018, p. 23). Article 10 of the 6AMLD allows prosecution for connected crimes to take place in several jurisdictions "on the basis of the same facts." To centralize the criminal proceedings "the Member States concerned shall cooperate in order to decide which of them will prosecute the offender (6AMLD, 2018, p. 29). The new directive also extends criminal liability to legal persons (6AMLD, 2018, pp. 28–29) and toughens punishments for ML/TF offences by increasing the maximum term of imprisonment to four years (6AMLD, 2018, p. 24, 28).

US Laws and Regulations

VAs, depending on how they are classified, are regulated in the US by an array of statutes and regulations. Though some view tokens as "a new asset class" because they "were intentionally designed to have … consumptive uses, entitling the holder to purchase goods or services or granting access rights to a blockchain platform or decentralized application" (Klayman, 2018, p. 70), in 2017, the US Security and Exchange Commission (SEC) established that tokens (including other VAs, such as virtual coins) qualify as securities and hence are "subject to the federal security laws" (SEC, 2017a). The US Security Act of 1933 defines "security" very broadly as follows:

> "note, stock, treasury stock, security future, security-based swap, bond, debenture, evidence of indebtedness, certificate of interest or participation in any profit-sharing agreement, collateral-trust certificate, preorganization certificate or subscription, transferable share, investment contract, voting-trust certificate, certificate of deposit for a security, fractional undivided interest in oil, gas, or other mineral rights, any put, call, straddle, option, or privilege on any security, certificate of deposit, or group or index of securities (including any interest therein or based on the value thereof), or any put, call, straddle, option, or privilege entered into on a national securities exchange relating to foreign currency, or, in general, any interest or instrument commonly known as a 'security', or any certificate of interest or participation in, temporary or interim certificate for, receipt for, guarantee of, or warrant or right to subscribe to or purchase, any of the foregoing" (Section 2, pp. 1–2).

The US Securities Exchange Act of 1934 adds "investment contract" to its comprehensive definition (Section 3, pp. 11–12). Any security offer must register with the SEC, if not qualified for the registration exemption. Cooke *et al*. (2018, p. 35) warn about potential regulatory and legal risks to "ICO sponsors" associated with the resale of tokens, issued outside the US, to US investors, as the registration requirement "applies extraterritorially to both initial sales by an issuer and subsequent resales by holders in the secondary market." The SEC specifies that "federal and state securities laws require investment professionals and their firms who offer, transact in, or advise on investments [of virtual coins and tokens] to be licensed or registered" (SEC, 2017b). In addition to federal, most states have their own security laws, referred to as "blue sky laws," "which are not always pre-empted by federal law" (Dewey, 2018, p. 481).

FinCEN's regulatory framework is grounded in defining entities dealing with VCs as Money Service Businesses (MSBs). In 2013, FinCEN (2013) issued a guidance for "persons creating, obtaining, distributing, exchanging, accepting, or transmitting virtual currencies" as subjects to the Bank Secrecy Act (BSA). Only CVCs fall under the BSA rules. FinCEN (2013) clarifies that a CVC "either has an equivalent value in real currency, or acts as a substitute for real currency." In the 2013 Guidance, FinCEN divides all participants in the VC market into three categories: users, exchangers, and administrators. While exchangers and administrators qualify as MSBs, users are not considered MSBs, hence are not subject to FinCEN's regulations under the BSA (FinCEN, 2013).

According to the 2011 guidance, since VC administrators and exchangers qualify as MSBs they must do the following:

- "Establish written AML programs that are reasonably designed to prevent the MSB from being used to facilitate money laundering and the financing of terrorist activities";
- File Currency Transaction Reports (CTRs) and SARs;
- "Maintain certain records, including those relating to the purchase of certain monetary instruments with currency, transactions by currency dealers or exchangers … and certain transmittals of funds";
- Register with FinCEN and renew registration every two years (FinCEN, 2011, p. 43585).

Starting in 2014, FinCEN has issued several administrative rulings related to VCs. These include the following:

- *Application of FinCEN's Regulations to Virtual Currency Mining Operations*, which clarifies the application of FinCEN's registration, recordkeeping, and reporting regulations to Bitcoin miners, stating that if a Bitcoin miner uses it "solely for the user's own purposes and not for the benefit of another, the user is not an MSB under FinCEN's regulations, because these activities involve neither 'acceptance' nor 'transmission' of the convertible virtual currency and are not the transmission of funds within the meaning of the Rule" (FinCEN, 2014a, p. 3).
- *Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity*, which concludes that VC software developers are not subject to the BSA AML/CFT rules, because "the production and distribution of software, in and of itself, does not constitute acceptance and transmission of value, even if the purpose of the software is to facilitate the sale of virtual currency" (FinCEN, 2014b, p. 2). It also clarifies regulatory requirements for companies investing in VCs, stating that if the company invests in VCs "for its own account, it is not acting as a money transmitter" and hence falls outside FinCEN's regulations. It also specifies that regulatory requirements might change for the company if it provides services to others, including "accepting and transmitting of convertible virtual currency, or the exchange of convertible virtual currency for currency of legal tender or another convertible virtual currency" (FinCEN, 2014b, p. 4).

- *Application of Money Services Business Regulations to the Rental of Computer Systems for Mining Virtual Currency*, which concludes that "the rental of computer systems to third parties" falls outside of FinCEN regulations, as they "specifically exempt from money transmitter status a person that only provides the delivery, communication, or network data access services used by a money transmitter to supply money transmission services" (FinCEN, 2014c, p. 2).
- *Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Trading Platform*, which settles that CVC trading and booking platforms are subject to the AML/CFT regulations based on the definition of the "money transmitter," which includes "facilitating the transfer of value, both real and virtual, between third parties" (FinCEN, 2014d, p. 4).
- *Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Payment System*, which classifies the CVC payment system as the "money transmitter," "because it engages as a business in accepting and converting the customer's real currency into virtual currency for transmission to the merchant." This makes it a subject to FinCEN requirements to register with FinCEN, to conduct AML risk assessment, to implement an AML program, "to comply with the recordkeeping, reporting and transaction monitoring," and if the system transactions constitute a "transmittal of funds" it also have to comply with the "Funds Transfer Rule" and the "Funds Travel Rule" (FinCEN, 2014e, p. 3, 5).
- *Application of FinCEN's Regulations to Persons Issuing Physical or Digital Negotiable Certificates of Ownership of Precious Metals*, which confirms that brokers and dealers of e-currency and e-precious metal are subjects to FinCEN regulations because they fall under the definition of a "money transmitter" since their services are "going beyond the activities of a broker or dealer in commodities" and they are "acting as a convertible virtual currency administrator (with the freely transferable digital certificates being the commodity-backed virtual currency)" (FinCEN, 2015, p. 4).

In 2019, FinCEN issued a guidance on application of its regulations to entities dealing with CVCs classified as "money transmitters." FinCEN defines a "money transmitter" as a "person that provides money transmission services," or "any other person engaged in the transfer of funds" (FinCEN, 2019b, p. 3). Thus, as with all money transmitters, entities

dealing with CVCs must register with FinCEN and comply with AML/CFT requirements for recordkeeping and reporting. These rules apply to domestic as well as foreign businesses "doing business in whole or substantial part within the United States, even if the foreign-located entity has no physical presence in the United States" (FinCEN, 2019b, pp. 3–4, 12). In the 2019 guidance, FinCEN identified typologies and "red flags" related to uses of CVCs for money laundering and other criminal activities "to assist financial institutions in identifying and reporting suspicious activity" (FinCEN, 2019a, p. 1). A FinCEN advisory from 2019 specified the following crime typologies related to decentralized ledger-based currency or CVC:

- "Darknet Market Places
- Unregistered Peer-to-Peer (P2P) exchanges
- Unregistered Foreign-Located MSBs
- CVC Kiosks" (FinCEN, 2019a, p. 1)

On October 27, 2020, FinCEN proposed new requirements for recordkeeping and travel rules for international transactions, lowering the USD 3,000 threshold requirement set by the BSA to USD 250 involving CVCs and digital assets with legal tender status (LTDA). This proposal also clarifies the meaning of money by "including any digital asset that has legal tender status in any jurisdiction and CVC" (FinCEN, 2020, p. 68011). On December 23, 2020, FinCEN proposed new requirements for banks and money services businesses for reporting CVCs or LTDAs transactions greater than USD 10,000, "or aggregating to greater than USD 10,000, that involve unhosted wallets or wallets hosted in jurisdictions identified by FinCEN" (FinCEN, 2021).

As was mentioned earlier, VAs can also be classified as a property. In 2014, the US Internal Revenue Service (IRS) issued a notice qualifying a VC as a property, stating that "general tax principles that apply to property transactions apply to transactions using virtual currency," which include the following:

- "Wages paid to employees using virtual currency are taxable to the employee, must be reported by an employer on a Form W-2, and are subject to federal income tax withholding and payroll taxes.
- Payments using virtual currency made to independent contractors and other service providers are taxable and self-employment tax rules generally apply. Normally, payers must issue Form 1099.

- The character of gain or loss from the sale or exchange of virtual currency depends on whether the virtual currency is a capital asset in the hands of the taxpayer.
- A payment made using virtual currency is subject to information reporting to the same extent as any other payment made in property" (IRS, 2014).

Failure to report VC transactions in the income taxes may result in criminal charges for tax evasion under the Title 26 Tax Violation, U.S Code (IRS, 2009).

As Rowland and Kiviat (2018, p. 93) rightly acknowledge, VAs may also qualify as commodity under the Commodity Exchange Act (CEA) "due to the broad definition of the term." In 2014, the CFTC declared VCs to be a "commodity" and a subject to the CEA oversight (CFTC, 2018b). According to the CFTC's interpretation of the term "virtual currency," it "encompasses any digital representation of value (a 'digital asset') that functions as a medium of exchange, and any other digital unit of account that is used as a form of a currency (i.e., transferred from one party to another as a medium of exchange); may be manifested through units, tokens, or coins, among other things; and may be distributed by way of digital 'smart contracts,' among other structures" (CFTC, 2017). In response to comments and requests to provide a more specific interpretation of VCs, CFTC "notes that it does not intend to create a bright line definition at this time given the evolving nature of the commodity and, in some instances, its underlying public DLT" (CFTC, 2020, p. 37736). On May 21, 2018, CFTC issued an advisory for registered exchanges and clearinghouses for listing VC derivative products focusing on the following:

- Enhanced market surveillance
- Close coordination with CFTC staff
- Large trader reporting
- Outreach to member and market participants
- Derivatives Clearing Organization risk management and governance (CFTC, 2018c)

Furthermore, a 2018 ruling held that CFTC has jurisdiction over VC and futures trading in VCs, specifically Bitcoin (CFTC, 2018a). In its customer advisory, CFTC reiterates that it "maintains general anti-fraud

and manipulation enforcement authority over virtual currency cash markets as a commodity in interstate commerce" (CFTC, n.d.). The same year, the National Futures Association (NFA), a self-regulatory organization for the US derivatives industry, implemented new disclosure requirements for its members engaging in VCs or VC derivatives (NFA, 2018). Dewey (2018, p. 484) notes that "cryptocurrency fund managers that invest in cryptocurrency futures contracts, as opposed to 'spot transactions' in cryptocurrencies, are required to register as a CTA and CPO with the CFTC and with the National Futures Association (NFA)."

In 2020, CFTC issued final interpretive guidance concerning "actual delivery" for retail commodity transactions in certain types of digital assets, stating that "actual delivery has occurred when a customer achieves both possession and control of the virtual currency that is underlying the transaction" (CFTC, 2020).

Issues to Consider

The BIS observation that "recent development of digital currencies and the novelty of their design mean that they may not be specifically regulated and do not fit easily into existing regulatory definitions and structures" still applies today (BIS, 2015, p. 10). Despite the establishment of an AML/CFT regime for VAs, there are still many issues that need to be addressed by lawmakers and regulators.

Legal obligations for internet service providers

Though internet service providers are required to record and keep log files, they cannot perform CDD requirements on behalf of the regulated entity. The European Commission (EC, 2018, p. 2) stresses that though service providers "may offer FinTech-based compliance services to regulated entities," they cannot take on a responsibility to comply with AML/CFT requirements. "Regulated entities themselves remain, however, responsible for meeting their obligations" (EC, 2018, p. 2).

Asymmetry in regulations

Rapid growth of the VA ecosystem has puzzled legislators about how these assets should be regulated, leading to variations in countries' legal and regulatory responses. Criminal elements benefit from this asymmetry

in laws and regulations between jurisdictions. A United Nations study acknowledged shortcomings in the legal battle against cybercrime, pointing to "insufficient harmonization of 'core' cybercrime offences, investigative powers, and admissibility of electronic evidence" (Malby *et al*., 2013, p. xii).

Privacy laws and data sharing

The CDD and "the travel rule" requirements "to obtain, hold, and transmit required originator and beneficiary information, immediately and securely, when conducting VA transfers" raises questions regarding their interplay with data-protection laws which considerably differ in various jurisdictions (FATF, 2021, p. 5). *The Economist* (2021) points out that data-privacy laws may be "a daunting obstacle to sharing information," as "many countries prevent banks from passing information to authorities, particularly those in other countries" (*The Economist*, 2021).

The FATF addressed this issue in the 2021 revised Guidance, stating that "relevant authorities should co-ordinate to ensure this can be done in a way that is compatible with national data protection and privacy rules" (FATF, 2021, p. 5). The EU General Data Protection Regulation (GDPR) stipulates and requires compliance with safeguards for the protection of personal data from "technology enabled EU financial marketplace," which encompasses VAs (EC, 2018, p. 2).

In its 2017 Consumer Financial Service Action Plan (The Plan), the EU Commission identified the reduction of "legal and regulatory obstacles affecting business when providing financial services abroad" as one of three main foci for further integration of financial services within a Single Market (EC, 2017b, p. 4). The Plan proposed adopting digital customer identification and authentication for AML/CFT compliance and data protection standards, automating Know Your Customer (KYC) or CDD requirements via cross-border electronic identification and authentication (EC, 2017b, p. 13). The European Commission, in the 2018 FinTech Action Plans, suggested that secure cross-border electronic identification and authentication for online services provided by the eIDAS Regulation[8] (2014) will make it easier to comply with the CDD requirements under the AML/CFT framework (EU, 2014, p. 75;

[8]The EU Regulation on Electronic Identification and Trust Services for Electronic Transactions.

EC, 2018, p. 2, 4, 10). The FinTech Action Plan also acknowledged regulatory challenges associated with distributed ledger technologies and artificial intelligence (EC, 2018, p. 10).

Anonymity

BIS (2015, p. 10) remarks that "the attractiveness of pseudonymity and the avoidance of banks and authorities may be partly driven by the desire to circumvent laws and regulation." Since cyber laundering is done without human interface, identification of a perpetrator is challenging. Poskriakov *et al*. (2018, p. 167) notes that new technological solutions, such as "atomic swap," or "atomic cross-chain trading," make it harder to trace transactions as they "allow users to cross-trade different VCs without relying on centralised parties or exchanges."

FATF recommends that technology-based solutions, such as APIs, may help institutions comply with customer identification requirements (FATF, 2015, p. 14). Another possible solution for customer identity corroboration suggested by FATF is "third-party digital identity systems," which involves creating third-party "digital identity custodians," "authenticating, and maintaining digital identity solutions for specific CDD, monitoring, and reporting purposes" (FATF, 2015, p. 14). The EU solution to overcoming anonymity-related VA risks is "the European Financial Transparency Gateway (EFTG), a pilot project using DLT to facilitate access to information about all listed companies on EU securities regulated markets in the context of the Transparency Directive" (EC, 2018, p. 13).

Conclusion

Legislators around the world have been challenged to address risks created by the rapidly developing VA ecosystem. Despite the absence of uniformity in regulating the VA market, application of FATF standards has led to a convergence of laws supervising VAs. The US and EU have issued rules and recommendations making VC "exchanges" and "administrators" subjects of AML/CFT obligations. The absence of regulations for ICOs and divergences in licensing requirements for VC exchanges and wallet services still remains and poses ML/TF risks. Issues related to privacy laws and anonymity remain relevant for AML/CFT compliance. As

a final point, the divergence of international legal approaches to regulating VAs creates loopholes for criminal abuses and make it difficult to investigate and prosecute cyber laundering.

References

4AMLD (May 20, 2015). Directive (EU) 2015/849 of the European Parliament and of the Council, on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC. *Official Journal of European Union*, 141, 73–17. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L0849&rid=2. [Accessed 11 April 2015].

5AMLD (May 30, 2018). Directive (EU) 2018/843 of the European Parliament and of the Council, amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU. *Official Journal of the European Union*, 156, 43–74. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843. [Accessed 10 April 2021].

6AMLD (October 23, 2018). Directive (EU) 2018/1673 of the European Parliament and of the Council on combating money laundering by criminal law. *Official Journal of the European Union*, 22–30. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1673&from=EN. [Accessed 16 April 2021].

Abboushi, S. (2017). Global virtual currency — Brief overview. *Journal of Applied Business and Economics*, 19(6), 10–18.

Acheson, N., Biggs, J. and Nguyen, H. (December 4, 2020). "What is Bitcoin?", in Bitcoin 101, *Coindesk*. https://www.coindesk.com/learn/bitcoin-101/what-is-bitcoin. [Accessed 15 April 2021].

AIFMD (June 8, 2011). Directive 2011/61/EU of the European Parliament and of the Council on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No. 1060/2009 and (EU) No. 1095/2010, 1–99. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02011L0061-20190113&qid=1553025823876&from=EN. [Accessed 17 April 2021].

AMF (February 27, 2020). Review and analysis of the application of financial regulations to security tokens. American Monetary Fund, 1–36. https://www.amf-france.org/sites/default/files/2020-03/legal-analysis-security-tokens-amf-en_1.pdf. [Accessed 10 April 2021].

Banks. *Forbes*. https://www.forbes.com/sites/caitlinlong/2018/07/22/icos-were-45-of-ipos-in-q2-2018-as-cryptos-disrupt-investment-banks/?sh=97fc52b794c2. [Accessed 17 April 2021].

BIS (November 2015). Digital Currency, Bank of International Settlement. https://www.bis.org/cpmi/publ/d137.pdf. [Accessed 13 April 2021].

CFTC (December 20, 2017). Retail commodity transactions involving virtual currency. Proposed interpretation; request for comment, the Commodity Futures Trading Commission, *Federal Register*, 82(243), 2017–27421, 60335–60341. https://www.cftc.gov/LawRegulation/FederalRegister/proposedrules/2017-27421.html. [Accessed 20 April 2021].

CFTC (October 3, 2018a). Federal court finds that virtual currencies are commodities. The Commodity Futures Trading Commission, Release Number 7820-18. https://www.cftc.gov/PressRoom/PressReleases/7820-18. [Accessed 24 April 2021].

CFTC (January 4, 2018b). Chairman Giancarlo statement on virtual currencies, Public Statements & Remarks. The Commodity Futures Trading Commission. https://www.cftc.gov/PressRoom/SpeechesTestimony/giancarlostatement010418. [Accessed 20 April 2021].

CFTC (May 21, 2018c). CFTC staff issues advisory for virtual currency products. The Commodity Futures Trading Commission, Release Number 7731-18. https://www.cftc.gov/PressRoom/PressReleases/7731-18. [Accessed 19 April 2021].

CFTC (June 24, 2020). Retail commodity transactions involving certain digital assets, Final interpretive guidance. The Commodity Futures Trading Commission, *Federal Register*, 85(122), pp. 37734–37744. https://www.govinfo.gov/content/pkg/FR-2020-06-24/html/2020-11827.htm. [Accessed 18 April 2021].

CFTC (n.d.) Customer advisory: Understand the risks of virtual currency trading. The Commodity Futures Trading Commission. https://www.cftc.gov/sites/default/files/idc/groups/public/@customerprotection/documents/file/customeradvisory_urvct121517.pdf. [Accessed 21 April 2021].

Cooke, J., Cohen, R. and Denisenko, J. (2018). A comparative overview of securities regulatory environments in the US, UK, and Asian Pacific, in J. Dewey (ed.), *Blockchain & Cryptocurrency Regulation*, Global Legal Insights: UK, pp. 34–46.

CSDR (July 23, 2014). Regulation (EU) No. 909/2014 of the European Parliament and of the Council on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No. 236/2012, *Official Journal of the European Union*, 1–72. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0909&from=EN. [Accessed 16 April 2021].

del Castillo, M. (February 2, 2021). Blockchain 50 2021, *Forbes*. https://www.forbes.com/sites/michaeldelcastillo/2021/02/02/blockchain-50/?sh=11051c53231c. [Accessed 18 April 2021].

Deloitte, King and Wood Mallesons, HKbitEX, and University of Hong Kong — Asian Institute of International Financial Law (AIIFL) (2020). Security token offerings: The next phase of financial market evolution? pp. 1–27. https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/audit/deloitte-cn-audit-security-token-offering-en-201009.pdf. [Accessed 17 April 2021].

Dewey, J. (2018). "USA," in J. Dewey (ed.), *Blockchain & Cryptocurrency Regulation*, Global Legal Insights: UK, pp. 479–487.

DoICS (March 3, 1997). Directive 97/9/EC of the European Parliament and of the Council on investor compensation schemes. *Official Journal of the European Communities*, pp. 22–31. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31997L0009&from=EN. [Accessed 17 April 2021].

EBA (December 12, 2013). Warning to consumers on virtual currencies. The European Banking Authority, pp. 1–3. https://www.eba.europa.eu/sites/default/documents/files/documents/10180/598344/b99b0dd0-f253-47ee-82a5-c547e408948c/EBA%20Warning%20on%20Virtual%20Currencies.pdf?retry=1. [Accessed 11 April 2021].

EBA (July 4, 2014). EBA Opinion on 'virtual currencies.' The European Banking Authority, pp. 1–46. https://www.eba.europa.eu/sites/default/documents/files/documents/10180/657547/81409b94-4222-45d7-ba3b-7deb5863ab57/EBA-Op-2014-08%20Opinion%20on%20Virtual%20Currencies.pdf?retry=1. [Accessed 11 April 2021].

EBA (August 11, 2016). Opinion of the European Banking Authority on the EU Commission's proposal to bring Virtual Currencies into the scope of Directive (EU) 2015/849(4AMLD). *The European Banking Authority*, pp. 1–9. https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1547217/32b1f7f2-90ec-44a8-9aab-021b35d1f1f7/EBA%2520Opinion%2520on%2520the%2520Commission%25E2%2580%2599s%2520proposal%2520to%2520bring%2520virtual%2520currency%2520entities%2520into%2520the%2520scope%2520of%25204AMLD.pdf. [Accessed 12 April 2021].

EBA (January 9, 2019). Report with advice for the European Commission on crypto-assets. The European Banking Authority, pp. 1–30. https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2545547/67493daa-85a8-4429-aa91-e9a5ed880684/EBA%20Report%20on%20crypto%20assets.pdf?retry=1. [Accessed 13 April 2021].

EC (February 2, 2016). Communication from the commission to the European Parliament and the Council on an action plan for strengthening the fight against terrorist financing. The European Commission. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1455113825366&uri=CELEX:52016DC0050. [Accessed 13 April 2021].

EC (June 26, 2017a). Report from the Commission to the European Parliament and the Council on the assessment of the risks of money laundering and

terrorist financing affecting the internal market and relating to cross-border activities, The European Commission, pp. 1–290. https://eur-lex.europa.eu/resource.html?uri=cellar:d4d7d30e-5a5a-11e7-954d-01aa75ed71a1.0001.02/DOC_1&format=PDF. [Accessed 17 April 2021].

EC (March 23, 2017b). Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions, Consumer Financial Services Action Plan: Better products, more choice, The European Commission, pp. 1–15. https://eur-lex.europa.eu/resource.html?uri=cellar:055353bd-0fba-11e7-8a35-01aa75ed71a1.0003.02/DOC_1&format=PDF. [Accessed 15 April 2021].

EC (2018). FinTech Action plan: For a more competitive and innovative European financial sector. The European Commission, pp. 1–18. https://ec.europa.eu/info/sites/info/files/180308-action-plan-fintech_en.pdf. [Accessed 16 April 2021].

Edwards, J. (February 3, 2021). Bitcoin's price history. *Investopedia*. https://www.investopedia.com/articles/forex/121815/bitcoins-price-history.asp. [Accessed 9 April 2021].

eIDAS Regulation (July 23, 2014). Regulation (EU) No. 910/2014 of The European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. *The Official Journal of the European Union*, 73–114. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN. [Accessed 23 April 2021].

ESMA (November 13, 2017a). Statement. The European Security and Market Authority, pp. 1–2. https://www.esma.europa.eu/sites/default/files/library/esma50-157-828_ico_statement_firms.pdf. [Accessed 11 April 2021].

ESMA (November 13, 2017b). Statement, ESMA alerts investors to the high risks of Initial Coin Offerings (ICOs). The European Security and Market Authority. https://www.esma.europa.eu/sites/default/files/library/esma50-157-829_ico_statement_investors.pdf. [Accessed 12 April 2021].

ESMA (February 26, 2018). ESMA, EBA and EIOPA warn consumers on the risks of Virtual Currencies. The European Securities and Markets Authority (ESMA), the European Banking Authority (EBA) and the European Insurance and Occupational Pensions Authority (EIOPA). https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2139750/313b7318-2fec-4d5e-9628-3fb007fe8a2a/Joint%20ESAs%20Warning%20on%20Virtual%20Currencies.pdf. [Accessed 13 April 2021].

ESMA (January 9, 2019a). Advice — Initial Coin Offerings and crypto-assets. The European Security and Market Authority, pp. 1–49. https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf. [Accessed 11 April 2021].

ESMA (January 9, 2019b). Crypto-Assets need common EU-Wide approach to ensure investor protection, Press Release. The European Security and Market Authority. https://www.esma.europa.eu/press-news/esma-news/crypto-assets-need-common-eu-wide-approach-ensure-investor-protection. [Accessed 15 April 2021].

EU (September 16, 2009). Directive 2009/110/EC of the European Parliament and of the Council on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC. *Official Journal of the European Union*, pp. 7–17. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0110&from=EN. [Accessed 15 April 2021].

EU (July 23, 2014). Regulation (EU) no 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. *Official Journal of the European Union*, 257, 73–114. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN. [Accessed 16 April 2021].

EU (November 25, 2015). Directive (EU) 2015/2366 of the European Parliament and of the Council on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing directive 2007/64/EC. *Official Journal of the European Union*, pp. 35–127. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN. [Accessed 15 April 2021].

EU (April 26, 2016). Directive of the European Parliament and of the Council amending directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending directives 2009/138/EC and 2013/36/EU. https://data.consilium.europa.eu/doc/document/PE-72-2017-INIT/en/pdf. [Accessed 9 April 2021].

EU (June 20, 2019). Directive (EU) 2019/1153 of the European Parliament and of the Council. *Official Journal of the European Union*, 186, 123–137. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L1153&from=EN. [Accessed 10 April 2021].

European Parliament (May 26, 2016). European Parliament resolution of 26 May 2016 on virtual currencies (2016/2007(INI)), pp. 1–7. https://www.europarl.europa.eu/doceo/document/TA-8-2016-0228_EN.pdf. [Accessed on 10 April 2021].

FATF (2012–2020). International standards on combating money laundering and the financing of terrorism & proliferation. The Financial Action Task Force (FATF), Paris, France, pp. 1–136. http://www.fatf-gafi.org/media/

fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf. [Accessed 7 April 2021].

FATF (2013). Guidance for a risk-based approach: Prepaid cards, mobile payments, and internet-based payment services. The Financial Action Task Force (FATF), Paris, France, pp. 1–47. https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf. [Accessed 7 April 2021].

FATF (2014). Virtual Currencies: Key definitions and potential AML/CFT risks. The Financial Action Task Force (FATF), Paris, France, 1–17. https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf. [Accessed on 7 April 2021].

FATF (2015). Guidance for a risk-based approach: Virtual Currencies. The Financial Action Task Force (FATF), Paris, France, pp. 1–48. https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf. [Accessed 7 April 2021].

FATF (2019a). Guidance for a risk-based approach to Virtual Assets and Virtual Asset service providers. The Financial Action Task Force (FATF), Paris, France, pp. 1–59. www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html. [Accessed 10 April 2021].

FATF (June 21, 2019b). Public statement on Virtual Assets and related providers. The Financial Action Task Force (FATF), Paris, France. http://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-statement-virtual-assets.html. [Accessed 12 April 2021].

FATF (2020a). Money laundering and terrorist Financing Red Flag indicators associated with Virtual Assets. The Financial Action Task Force (FATF), Paris, France, pp. 1–24. www.fatf-gafi.org/publications/fatfrecommendations/documents/Virtual-Assets-Red-Flag-Indicators.html. [Accessed 7 April 2021].

FATF (2020b). 12-month Review Virtual Assets and VASPs. The Financial Action Task Force (FATF), Paris, France, pp. 1–26. http://www.fatf-gafi.org/media/fatf/documents/recommendations/12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf. [Accessed 7 April 2021].

FATF (2020c). Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets. The Financial Action Task Force (FATF), Paris, France, pp. 1–24. www.fatf-gafi.org/publications/fatfrecommendations/documents/Virtual-Assets-Red-Flag-Indicators.html. [Accessed 12 April 2021].

FATF (June 2020d), FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins. The Financial Action Task Force (FATF), Paris, France, pp. 1–32. https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-FATF-Report-G20-So-Called-Stablecoins.pdf. [Accessed 29 April 2021].

FATF (March 2021). Public consultation on FATF draft guidance on a risk-based approach to virtual assets and virtual asset service providers, Sixth draft. The

Financial Action Task Force (FATF), Paris, France, pp. 1–99. http://www.fatf-gafi.org/media/fatf/documents/recommendations/March%202021%20-%20VA%20Guidance%20update%20-%20Sixth%20draft%20-%20Public%20consultation.pdf. [Accessed 11 April 2021].

Filipkowski, W. (2008). Cyber laundering: An analysis of typology and techniques. *International Journal of Criminal Justice Sciences*, 3(1), 15–27.

FinCEN (July 21, 2011). Rules and Regulations, 43585–43597. *Federal Register*, 76(140). The Financial Crime Enforcement Network. https://www.govinfo.gov/content/pkg/FR-2011-07-21/pdf/2011-18309.pdf. [Accessed 17 April 2021].

FinCEN (March 18, 2013). Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies. The Financial Crime Enforcement Network. https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering. [Accessed 14 April 2021].

FinCEN (January 30, 2014a). Application of FinCEN's Regulations to Virtual Currency Mining Operations, FIN-2014-R001. The Financial Crime Enforcement Network, pp. 1–4. https://www.fincen.gov/sites/default/files/shared/FIN-2014-R001.pdf. [Accessed 20 April 2021].

FinCEN (January 30, 2014b). Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity, FIN-2014-R002. The Financial Crime Enforcement Network, pp. 1–5. https://www.fincen.gov/sites/default/files/shared/FIN-2014-R002.pdf. [Accessed 17 April 2021].

FinCEN (April 29, 2014c). Application of Money Services Business Regulations to the Rental of Computer Systems for Mining Virtual Currency, FIN-2014-R007. The Financial Crime Enforcement Network, pp. 1–3. https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R007.pdf. [Accessed 20 April 2021].

FinCEN (October 27, 2014d). Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Trading Platform, FIN-2014-R011. The Financial Crime Enforcement Network, pp. 1–7. https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R011.pdf. [Accessed 20 April 2021].

FinCEN (October 27, 2014e). Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Payment System, FIN-2014-R012. The Financial Crime Enforcement Network, pp. 1–6. https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R012.pdf. [Accessed 18 April 2021].

FinCEN (August 14, 2015). Application of FinCEN's Regulations to Persons Issuing Physical or Digital Negotiable Certificates of Ownership of Precious

Metals, FIN-2015-R001. The Financial Crime Enforcement Network, pp. 1–5. https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2015-R001.pdf. [Accessed 19 April 2021].

FinCEN (May 9, 2019a). Advisory on Illicit Activity Involving Convertible Virtual Currency, FIN-2019-A003. The Financial Crime Enforcement Network, pp. 1–12. https://www.fincen.gov/sites/default/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf. [Accessed 18 April 2021].

FinCEN (May 9, 2019b). Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies, FIN-2019-G001. The Financial Crime Enforcement Network, pp. 1–30. https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf. [Accessed 18 April 2021].

FinCEN (October 27, 2020). Proposed Rule, Federal Register, 85(208), 68005-68019. The Financial Crime Enforcement Network, pp. 1–15. https://www.govinfo.gov/content/pkg/FR-2020-10-27/pdf/2020-23756.pdf. [Accessed 15 April 2021].

FinCEN (January 28, 2021). Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets. The Financial Crime Enforcement Network. https://www.federalregister.gov/documents/2021/01/28/2021-01918/requirements-for-certain-transactions-involving-convertible-virtual-currency-or-digital-assets. [Accessed 14 April 2021].

Frankenfield, J. (November 3, 2020). Initial Coin Offering. *Investopedia*. https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp. [Accessed 12 April 2021].

Frankenfield, J., and Sonnenshein, M. (March 7, 2021). Cryptocurrency. *Investopedia*. https://www.investopedia.com/terms/c/cryptocurrency.asp. [Accessed 12 April 2021].

Frankenfield, J., and Anderson, S. (March 23, 2021). Digital currency. *Investopedia*. https://www.investopedia.com/terms/d/digital-currency.asp. [Accessed 10 April 2021].

Gesley, J. (February 27, 2018). European Union: New EU Legislative Framework to Regulate Financial Markets Enters into Force. Library of Congress. https://www.loc.gov/law/foreign-news/article/european-union-new-eu-legislative-framework-to-regulate-financial-markets-enters-into-force/. [Accessed 16 April 2021].

Hamilton, D. (August 16, 2020). What are "Security Token Offerings" (STOs)?" *Securities.io*. https://www.securities.io/security-token-offerings-sto. [Accessed 21 April, 2021].

Hayes, A. and Mansa, J. (June 30, 2020). Stablecoin, *Investopedia*. https://www.investopedia.com/terms/s/stablecoin.asp. [Accessed 18 April 2021].

IOSCO (February 2020). Issues, risks and regulatory considerations relating to crypto-asset trading platforms, final report. The International Organization of Securities Commissions, pp. 1–51. https://www.iosco.org/library/pubdocs/pdf/IOSCOPD649.pdf. [Accessed 28 April 2021].

IRS (2009). *Tax Crime Handbook*, Office of Chief Counsel, Criminal Tax Division, the Internal Revenue Service. https://www.irs.gov/pub/irs-utl/tax_crimes_handbook.pdf. [Accessed 20 April 2021].

IRS (March 25, 2014). IRS virtual currency guidance: Virtual currency is treated as property for U.S. federal tax purposes; General rules for property transactions apply. The Internal Revenue Service. https://www.irs.gov/newsroom/irs-virtual-currency-guidance. [Accessed 17 April 2021].

Jourova, V. (July 9, 2018). Strengthened EU rules to prevent money laundering and terrorism financing. The European Commission, file:///Users/tanyagibbs/Downloads/Factsheet_AMLD_201807_2pdf-1.pdf. [Accessed 9 April 2014].

Klayman, J. (2018). "Mutually assured disruption: The rise of the security token," in J. Dewey (ed.), *Blockchain & Cryptocurrency Regulation*, Global Legal Insights: UK, pp. 60–89.

Leloup, L. (November 8, 2017). Why ICOs will be the fastest growing form of investment in 2018. *Finance Monthly*. https://www.finance-monthly.com/2017/11/why-icos-will-be-the-fastest-growing-form-of-investment-in-2018. [Accessed 22 April 2021].

Long, C. (July 22, 2018). ICOs were 45% of IPOs in Q2 2018, as cryptos disrupt investment.

Malby, S., Mace, R., Holterhof, A., Brown, C., Kascherus, S. and Ignatuschtschenko, E. (February 2013). Comprehensive study on cybercrime, Draft. United Nations Office on Drugs and Crime, United Nations, Vienna. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf. [Accessed 20 April 2021].

MAR (April 14, 2014). Regulation (EU) No 596/2014 of the European Parliament and of the Council on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC. *Official Journal of the European Union*, pp. 1–61. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0596&from=EN. [Accessed 15 April 2021].

Massey, R., Dalal, D. and Dakshinamoorthy, A. (2017). Initial Coin Offering: A new paradigm. Deloitte, pp. 1–12. https://www2.deloitte.com/content/dam/Deloitte/ru/Documents/risk/deloitte-blockchain-initial-coin-offering.pdf. [Accessed 22 April 2021].

MiFID II (May 15, 2014). Directive 2014/65/EU of the European Parliament and of the Council on markets in financial instruments and amending Directive

2002/92/EC and Directive 2011/61/EU. *Official Journal of the European Union*, pp. 349–496. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0065&from=EN. [Accessed 26 April 2021].

MiFIR (May 15, 2014). Regulation (EU) No 600/2014 of the European Parliament and of the Council, on markets in financial instruments and amending Regulation (EU) No 648/2012. *Official Journal of the European Union*, pp. 84–148. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0600&from=EN. [Accessed 23 April 2021].

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf. [Accessed 14 April 2021].

NFA (May 17, 2018). 9073 — Disclosure requirements for NFA members engaging in virtual currency activities, interpretive notice, the National Futures Association. https://www.nfa.futures.org/rulebook/rules.aspx?Section=9&RuleID=9073. [Accessed 20 April 2021].

PD (November 4, 2003). Directive 2003/71/EE of the European Parliament and of the Council on the prospectus to be published when securities are offered to the public or admitted to trading and amending Directive 2001/34/EC. *Official Journal of the European Union*, pp. 64–89. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003L0071&from=EN. [Accessed 15 April, 2021].

Perez, Y. B. (February 19, 2019). The differences between cryptocurrencies, virtual, and digital currencies, *TNW*. https://thenextweb.com/news/the-differences-between-cryptocurrencies-virtual-and-digital-currencies. [Accessed 10 April 2021].

Poskriakov, F., Chiriaeva, M. and Cavin, C. (2018). Cryptocurrency compliance and risks: A European KYC/AML perspective. In J. Dewey (ed.), *Blockchain & Cryptocurrency Regulation*, Global Legal Insights: UK, pp. 163–174.

Rowland, G. and Kiviat, T. (2018). Cryptocurrency and other digital assets for asset management. In J. Dewey (ed.), *Blockchain & Cryptocurrency Regulation*, Global Legal Insights: UK, pp. 90–100.

SEC (July 25, 2017a). SEC Issues Investigative Report Concluding DAO Tokens, a Digital Asset, Were Securities: U.S. Securities Laws May Apply to Offers, Sales, and Trading of Interests in Virtual Organizations, Press Release. The US Security and Exchange Commission. https://www.sec.gov/news/press-release/2017-131. [Accessed 17 April 2021].

SEC (July 25, 2017b). Investor Bulletin: Initial Coin Offering, the US Security and Exchange Commission. https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-bulletins-16. [Accessed 17 April 2021].

SFD (May 6, 2009). Directive 2009/44/EC of the European Parliament and of the Council amending Directive 98/26/EC on settlement finality in payment and securities settlement systems and Directive 2002/47/EC on financial

collateral arrangements as regards linked systems and credit claims. *Official Journal of the European Union*, pp. 37–43. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0044&from=EN. [Accessed 17 April 2021].

Statista (2021). Amount of funds raised for cryptocurrency initial coin offering (ICO) projects worldwide as of November 2019, by leading industry. Financial Instruments and Investments. https://www.statista.com/statistics/802925/worldwide-amount-crytocurrency-ico-projects-by-industry. [Accessed 20 April 2021].

TD (December 15, 2004). Directive 2004/109/EC of the European Parliament and of the Council on the harmonisation of transparency requirements in relation to information about issuers whose securities are admitted to trading on a regulated market and amending Directive 2001/34/EC. *Official Journal of the European Union*, pp. 1–51. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02004L0109-20131126&qid=1553004898571&from=EN. [Accessed 15 April 2021].

The Economist (April 12, 2021). The war against money-laundering is being lost. https://www.economist.com/finance-and-economics/2021/04/12/the-war-against-money-laundering-is-being-lost. [Accessed 12 April 2021].

Tu, K. and Meredith, M. (2015). Rethinking virtual currency regulation in the Bitcoin age. *Washington Law Review*, 90(1), 271–346.

US Security Act of 1933. https://www.govinfo.gov/content/pkg/COMPS-1884/pdf/COMPS-1884.pdf. [Accessed 17 April 2021].

US Security and Exchange Act of 1934. https://www.nyse.com/publicdocs/nyse/regulation/nyse/sea34.pdf. [Accessed 15 April 2021].

Wockener, K. and Freudenberger, C. (January 30, 2019). Update of the status of Initial Coin Offerings in Europe, *White and Case*. https://www.whitecase.com/publications/alert/update-status-initial-coin-offerings-europe. [Accessed 14 April 2021].

This page intentionally left blank

https://doi.org/10.1142/9781800612839_0009

Chapter 8

Worldwide Cooperation and Enforcement Issues

Benjamin Musau

Introduction

Money laundering (ML) is not a new concept; rather, it is an ongoing issue that Governments worldwide have had to contend with for decades. However, the methods used to conduct ML are constantly changing, resulting in the need for new approaches to mitigate activities aimed at concealing the origins of money. ML is regarded as a severe economic crisis that greatly impacts levels of economic development throughout the world (Musau, 2019). ML involves processing illegitimate, illegally obtained money (commonly referred to as dirty money) and making it appear to be legitimate, legally obtained money (also known as clean money). In accordance with the Organization for Economic Cooperative Development (OECD) and the Financial Action Task Force (FATF), the process of ML is broken down into three basic steps — placement, layering, and integration (Musau, 2019).

The first step, placement, refers to putting the money in a legitimate financial system. ML activities, which include selling illegal firearms or drugs, human and child trafficking, prostitution, illegal gambling, and similar activities, generate illegal money. To transform the illegal money into legitimate or clean money, it must be placed somewhere, such as a bank or other type of financial institution. Other options include using it

to acquire assets and depositing it into the local retail economy through purchasing tangible items (Bosworth-Davies, 2007). The person engaged in ML is motivated to make the transformation quickly to avoid detection.

The second step is layering, which is commonly assumed to be the most challenging step. It consists of disguising the source of the money. Today, layering is usually accomplished through multifaceted financial transactions with the purpose of making it hard to track the origins of the funds. The more complex and convoluted the money trail, the harder audits are to conduct and, therefore, the more likely the launderer is to get away with their illegal actions (Bosworth-Davies, 2007). An example of layering might be moving drug money between two or more business accounts in distinct nations through purchasing some assets, thereby making the origin of the money hard to trace.

The third and final step is integration, during which time the money is moved into a legitimate financial system as payments. The money is, at this point, returned to the economy to look like legitimate income, and the process of laundering the money is complete (Musau, 2019).

In the 20th century, ML was mostly localized and consisted of a physical currency, such as the US dollar or British pound, being obtained through illegal means and transitioned into the economy through the three steps described previously. In the majority of cases, the money remained in one type of currency the entire time, from start to finish (Musau, 2019). However, in recent years, due to the advent of the World Wide Web and the widespread nature of globalization, ML has become more complex and digitalized. ML is no longer local, national, or even regional most of the time. It may not even take place within one or two nations, and, to further complicate matters, it might not involve a State-backed currency. Instead, it is often global and digital in nature, making it exceedingly hard to identify, track, monitor, halt, and prosecute. Once legal concerns and jurisdictions are factored into the process, it may be near impossible to stop ML activities — even if authorities know what is going on and who is responsible — due to the current limitations of governing entities (Musau, 2019).

The practice of cyber laundering (CL) adds even more challenges to monitoring and combating ML. Like more traditional forms of ML, CL involves converting illegally obtained money into money that appears to be legal and legitimate through the three-step process of placement,

layering, and integration (Integrity Asia, 2018). The difference between ML and CL is that the latter is carried out in cyberspace, often using cryptocurrencies instead of State-backed currencies. Online transactions offer many benefits for ML activities. They are quick, easy to implement, hard to track, and cheap. These activities may be carried out throughout the world at any place and at any time where there is an Internet connection, which now means nearly ubiquitously (Chambers-Jones, 2012).

Due to the prevalence of ML in general, and CL in particular, and the global nature of these illegal and harmful money-based activities, new methods of thwarting ML and CL are required. The tactics that worked in the past are outdated and no longer effective at addressing the complex and convoluted nature of these nefarious activities. Additionally, the isolationist method of monitoring and prosecuting ML and CL activities at the local level or national level are no longer appropriate. Based on these realizations, international cooperation on CL is essential to identify CL activities and hold perpetrators accountable. The purpose of this chapter, therefore, is to explore the value and usefulness of an international cooperation and to provide an overview of best regulatory and policy practices based on the research. Finally, it is important to include potential actors and agencies that may be utilized to combat CL in the international arena given that the world has advanced into a global village.

What Are Virtual Currencies?

Prior to delving into best practices for implementing an international cooperation to fight CL, it is important to briefly define various forms of virtual currencies (VCs). A VC is a digital representation of a monetary unit that possesses value. It may be traded digitally and functions in three ways — as a medium for exchange, as a unit of accounting, and as a value storage unit. It does not, however, have a legal tender value status. Moreover, it is neither guaranteed nor issued by a Government or jurisdiction, thereby making it risky. Unlike most currencies, it is not State-backed. Its only value is that which is agreed upon by the community of persons who use it. A VC is distinct from fiat currency, which is backed by some Governments as it is issued by that Government and has a face value with a legal tender (FATF, 2014). VC is different but related to digital currency. Digital currency may represent digitally either a VC or E-money (fiat money).

VCs may be convertible or non-convertible. Convertible VCs or open ones are equivalent in value to real currencies and, therefore, may be exchanged back and forth for another type of currency. An example of this is Bitcoin or WebMoney. A non-convertible or closed VC is only applicable to a specific domain and it may, therefore, not be exchanged with a real-world currency. An example of this is Warcraft Gold which is only used to buy items in World of Warcraft (FATF, 2014). There are also centralized versus decentralized VC. A centralized VC is administered by one central authority that controls the entire system of that VC. The institution administering the centralized VC establishes the rules and regulations for using the currency. A decentralized VC is sometimes referred to as a cryptocurrency, and such decentralized VCs are distributed. They are open-sourced and exchanged from one person to the next. There is no centralized authority, and no one is providing oversight and compliance. The best example of this type of currency at present is Bitcoin (FATF, 2014).

VCs require systems with participants to operate. One person in the system is called the exchanger, and this individual or entity is tasked with exchanging the VC for fiat money or some other item of value. Another stakeholder is the administrator, who may also be an individual or an entity that issues a centralized VC by placing it in circulation. The administrator establishes the rules and keeps track of the movement of currency through a ledger. The administrator may redeem the VC. The user in the system is an individual or, less often, entity that obtains the VC and uses it as a form of currency to purchase real or even virtual goods and services. The miner is the individual or entity that runs some type of software to produce the VC, relying on sophisticated algorithms. The wallet provider is the individual or entity that provides a wallet or means for storing or holding the VC. They maintain each user's balance (FATF, 2014).

There is a relationship between all components of the VC. With a convertible centralized VC, the individuals and entities involved include an administrator, exchangers, users, and third-party ledger. The VC may be exchanged for fiat. An example is WebMoney. With a convertible decentralized VC, there are exchangers and users, but no administrators and no third-party ledger. The VC may be exchanged for a fiat currency (such as US dollar or Euro), and the best example is Bitcoin. With a non-convertible centralized VC, there are administrators, exchangers, users, and a third-party ledger. However, the currency cannot be exchanged

for fiat ones. An example of this type of VC is World of Warcraft Gold. To date, there are no examples of non-convertible decentralized VCs (FATF, 2014).

VCs and CL Activities

There are numerous ways in which CL is done through online transactions, but four modes are particularly common and worth exploring. The first is e-commerce, with perpetrators using various e-commerce platforms as a means of "washing" or laundering their dirty money. For instance, in the past, members of terrorist organizations have used eBay as a platform to sell computers and move money via a PayPal account.

The second common CL strategy is digital currency which, while complex, guarantees better security and privacy than e-commerce transactions. There are two primary ways cryptocurrency is used. They both involve exchanging fiat through a digital platform for cryptocurrency, but this may be done via a bank account or via a Bitcoin ATM using either a credit or debit card (Integrity Asia, 2018). Typically, the former is preferred because some Bitcoin ATMs do offer anti-ML software. However, the anti-ML software may be circumvented using an intermediary without a history of laundering to open the digital exchange account.

The third common method of CL is through online gaming. While less common than e-commerce and cryptocurrency methods, these platforms are a means for launderers to layer more effectively and then convert illegitimate money into legitimate forms. This tactic was discovered recently by Sony Online Entertainment, with a US-based customer transferring money to a Russian account through purchasing virtual, rare items that were quite challenging for users to obtain and, therefore, of value (Integrity Asia, 2018).

The fourth CL method commonly employed is crowdfunding. Various crowdfunding sites are extremely accessible and easy to use. Most have not, to date, implemented anti-fraud detection software, thereby making them excellent platforms of changing dirty money into laundered funds (Chambers-Jones, 2012). An individual may create a fake campaign and request money. When the money is transferred from the online account to the bank, it will be recorded as a legal transaction from a legitimate crowdfunding platform.

Toward an International Cooperation for CL

There is a developing movement toward combating ML and CL activities on a global level through joint efforts rather than taking an isolationist approach. To gain an appreciation of the challenges faced and the need for an international cooperation, it is essential to explore the movement toward creating a functioning international cooperation and the obstacles that must be comprehensively recognized and addressed.

Understanding the global nature of CL

The fight to control ML activities is of special concern to local, national, regional, and international policymakers. CL is becoming a bigger and more costly concern for many countries because it directly impacts most nations, causing negative consequences for the macroeconomy and the broader financial sector of each nation that is affected. The International Monetary Fund (IMF) estimates that at least USD 800 billion is laundered each year, a sum which represents roughly 5% of the global community's gross domestic product (GDP) (Quang Tran, 2020). The cost is shared by many nations both in the developed and developing world, with some nations being disproportionately impacted by laundering activities.

The international community has long recognized the dire consequences of illegal money activities and the need to put into place better practices to discourage them. CL undermines and alters legitimate forms of earning money through permitting outside factors aside from appropriate business practices to impact the decisions by businesses worldwide. It serves to corrupt officials at all levels of Government or even entire Governments through lobbying and buying votes and then influencing the decisions made by powerful politicians. CL negatively impacts macroeconomic standards and estimates, alters currency markets, and, in some instances, even destabilizes entire financial entities through the creation and proliferation of illegal economic transactions (Turner, 2004).

The international community, moreover, views ML and CL as threats to the entire global economy and, consequently, is motivated to work together to identify, address, thwart, and penalize ML and CL activities. Even nations which, in the past, took a more isolationist approach to dealing with cybercrime are slowly coming around to the realization that a global effort is the only legitimate way to tackle these types of crimes.

Therefore, the fight to control CL activities is of special concern to local, national, regional, and international policymakers and all the countries in the world should be involved in cooperating for great benefits that arise from unity instead of individual or disunited approaches to the fight against CL activities. It is even more to cooperate now than ever before as the world continues to become a smaller global village than previously as the World Wide Web is growing to almost every household worldwide.

Catalysts and consequences of CL

Globalization has brought about many benefits as well as new challenges to financial institutions and economies throughout the world. There are numerous catalysts that have promoted an environment conducive to CL activities. Liberalized capital markets, coupled with advances in technology, have reduced legitimate and criminal transaction costs associated with moving money (Turner, 2004). With reduced costs, some of the barriers that prevented CL have been removed, creating a situation more conducive to CL activities. At the same time, nations, particularly in the developing world, have been pushed to relax their ML and CL regulations to attract new businesses and industries (Turner, 2004). This serves as a severe challenge for the global community to address comprehensively and a catalyst for the proliferation of CL activities.

The ramifications of ML and CL are not limited to the direct economic consequences of these activities. The most dangerous aspect, arguably, is that they promote other crimes that are socially destructive and which result in illegal money, such as drug, weapons, and human trafficking; corruption at every level of business and Government; and even terrorism. All these activities pose major human rights challenges, and, often, the most vulnerable nations and their people reap the consequences. Emerging markets are at heightened risk for ML and CL activities, and it will take a concerted, global effort to overcome the spread of these illegal money transactions (Quang Tran, 2020). Anti-ML and anti-CL policies are becoming major talking points with Governments throughout the world, leading more policymakers to push for a cooperation process to prevent and overcome ML and CL activities. The overall global consensus is that strategies that enhance cooperation on the international and national scales should be prioritized and supported (Quang Tran, 2020).

Challenges and obstacles for fighting international CL

While most experts agree that an international form of cooperation is required to effectively fight against ML and CL activities, the process of implementing such a plan requires careful attention and meticulous planning. There are numerous challenges and obstacles, some of which are highly problematic and complex, that must be taken into consideration by the international effort. The cooperation will need to find innovative means of overcoming them through collaborations and the sharing of resources.

Logistical challenges

International cooperation designed to fight against CL will have numerous logistical challenges, but it must be considered to stop the illegal activities. One of the biggest challenges is the sheer number of worldwide Internet users, and the substantial challenges associated with tracking activities of all those users to determine which ones are legitimate and which are illegal. It is nearly impossible for any nation or international organization to monitor all the Internet traffic, even if they would be able to gain access to it — a process that poses its own legal barriers (Wangui Maina, 2021).

The overwhelming abundance of Internet activity makes an effective and precise targeting of key platforms and persons responsible for CL activities essential to fight against CL. The availability of information and technological developments are further challenges that make tracking and monitoring CL an arduous task. Most people, even in developing nations, have access to several Internet-capable devices, thereby adding elements of challenges to tracking and monitoring CL practices and following the money to effectively counter or combat CL activities. The evidence, furthermore, reveals that most traditional investigation instruments fail on the global level (Wangui Maina, 2021).

Legal challenges

In addition to logistical challenges, numerous legal challenges have been identified for international cooperation to address combating CL activities. The first is identifying new offences and drafting criminal law based on the types of activities launderers are carrying out (Wangui Maina,

2021). There is a lack of technical capacity among enforcement agents, and challenges persist concerning the investigation and prosecution of cybercrimes at the international level. Currently, it is unclear which governing body is responsible for each step in the legal process and, due to the international nature of most CL crimes, there are typically more than one and sometimes many governing entities are involved. The legal procedures and protocols for investigation and digital evidence are not adequately defined and, in some instances, non-existent. Jurisdictional barriers are a major concern that is associated with the international dimensions of the practice (Wangui Maina, 2021).

Technical challenges

There are additional technical challenges that deserve mention when dealing with combating CL activities. One major shortcoming is the inadequate skills still present in the cybersecurity sector, particularly in the most vulnerable nations. For instance, Kenya is a nation known for being at risk of CL. A case study conducted on Kenya's ML and cybersecurity situation found that not only were cybersecurity skills in the nation inadequate but also there was an overwhelming lack of awareness concerning cybersecurity issues among the stakeholders responsible for monitoring and combating CL crimes (Sambuli *et al*., 2016).

Furthermore, largely due to developing nations having unconducive legal frameworks for monitoring, tracking, and prosecuting CL crimes, there is also a lack of related infrastructure at the institutional level to carry out the development and application of crime-fighting tasks, particularly those that require the use of sophisticated technology and computer programs. Some of the technical challenges are more regulatory in nature. A study found that inadequate regulatory capacity is responsible for some nations not being able to do their part to stop cybercriminals to include those participating in CL activities (Sambuli *et al*., 2016). This is particularly prevalent at the convergence of services with networks. Significant resources and knowledge are required to implement some of the basic practices required, from a technical perspective, to combat ML and CL activities. For instance, digital signatures, encryption, and security practices all take monetary resources and technological skill to implement, thereby making them challenging for developing nations to put into practice in any consistent manner (Sambuli *et al*., 2016).

Cultural challenges

Some of the most significant issues with fighting international ML and CL activities have to do with the cultural climate and worldview concerning cybercrime, in general, and ML practices in particular. There exist nations and cultures throughout the world that do not see these activities as particularly problematic and, therefore, do not want to invest significant sums of money into addressing them. For instance, a case study on Kenya revealed that there is a lack of culture to support the adoption of basic Internet security practices, particularly in certain sectors of the economy where CL activities are prevalent. This same trend is, undoubtedly, witnessed in other nations. The same case study found that there was a lack of effective and efficient legislative instruments to deal with issues of ethical and moral conduct, further creating a culture where cybersecurity in general is not prioritized and targeted (Sambuli *et al*., 2016).

Current Stance of the International Community on International Cooperation

The international community recognizes that the current frameworks for combating ML and CL are inadequate and antiquated, at least in certain aspects. Most significantly, some of the existing laws were put into place years before new technologies were adopted, such as mobile money and cryptocurrencies, thereby rendering them ineffective at addressing CL activities that are taking place today. This is significant because mobile payment channels are used regularly, and launderers are believed to carry out millions of illegal transactions with them (Wangui Maina, 2021). A common tactic of ML is to interweave illegal with legal sources of money and, later, switch them between various types of business accounts to make them harder to track. When this is done on a global scale and through banking institutions in several nations, the illegal money activities became exceedingly hard to track and identify, let alone prosecute in a court of law (Wangui Maina, 2021). Without international cooperation, it is nearly impossible to stop ML and CL, resulting in serious national security and socioeconomic consequences.

The international community and individual nations, collectively, have long recognized the immediate need for a comprehensive anti-ML committee or organization dedicated to stopping ML and CL from proliferating. Discussions on the theme of international cooperation to stop ML

have been ongoing since at least the late 1970s; however, in the past, the efforts were primarily focused on preventative regulations. Today, launderers make use of open international financial institutions and global free-flowing capital streams. Thus far, several bilateral and multinational institutions have been created to help curb ML, such as the Financial Task Action Force (FATF), which was founded in 1989 (Quang Tran, 2020). It is tasked with controlling all ML leads, identifying ML trends, and monitoring international activities. Additionally, FATF is responsible for recommending policies to overcome the ML challenges.

Ideal cooperation will include efforts in capacity-building throughout the globe. It will train Governments on how to recognize and stop ML and CL activities. It will improve general and specific techniques and tools for detecting and monitoring ML and CL actions. It should provide platforms and communication channels to effectively exchange key evidence and data regarding these illegal activities. Finally, all members of the international cooperation should commit to enforcing the same standards and regulations to prevent ML and CL activities. Based on these minimum requirements for an effective approach to dealing with ML and CL, international cooperation is mandated to deal with all three stages in each of the various types of ML and CL and, then, to hold perpetrators accountable. International cooperation, moreover, ought to work toward collecting financial intelligence, investigating known leads and suspected criminals, and prosecuting those culpable as the evidence dictates (Quang Tran, 2020).

Fortunately, there is a growing global recognition for the need to empower such an international group to deal with ML and CL activities. Most of the effort is directed toward the financial banking system, with policies geared toward preventing organizations from turning developing or emerging nations into hotbeds of ML and CL activities (Quang Tran, 2020). These nations are prime targets because they do not have a sophisticated Government and banking system capable of detecting and fighting against these types of illegal activities, and there are economic incentives, at least in the short-term, associated with relaxed laws that turn a blind eye to ML and CL activities. Overcoming these challenges is the job of an international cooperation system (Quang Tran, 2020).

Recommendations for Regulations and Practices

Individual nations and the international community collectively have worked toward establishing regulations and practices aimed at combating

various types of ML to include CL. However, identifying the regulations and practices and putting them into place with oversight is an ongoing challenge and process. More work is required to establish the best practices for creating and enforcing regulations and practices. Lessons from legal frameworks and Governments that have successfully implemented anti-ML and anti-CL legislature may be used to establish the regulations and practices for the international cooperation to adopt.

Lessons from legal frameworks for combating CL crimes

A successful approach for determining the regulations and practices for the international cooperation on CL to put into place is the exploration of legal frameworks for combating CL crimes. Several legal frameworks, such as cybercrime law, substantive law, procedural law, and preventative law, are all applicable and should be analyzed to shed light on best practices for the international cooperation to adopt.

Cybercrime law

It is worth exploring cybercrime legal standards to determine how they may be applied by an international cooperation dedicated to fighting CL activities on the global level. Cybercrime law serves to identify the standards of behavior that are acceptable for users of information and communication technology (UNODC, 2021). Cyber law also sets forth legal and social sanctions for cybercrimes. The main purpose of these laws is to protect information and communication technology users by preventing harm to individuals, groups, Governments, organizations, data, systems, and key infrastructure. Cybercrime law permits Governments and other institutions to cooperate, either at the local, state, or international level, to investigate and prosecute when appropriate people or organizations that commit crimes online. Cybercrime law is excellent for promoting cooperation between nations because it sets an online standard that the international community may agree to enforce. Laws pertaining to cybercrimes provide an agreed-upon set of rules and regulations for acceptable conduct when using the Internet and other digital technologies. These laws also establish appropriate actions for the Government to take when dealing with evidence and criminal procedure, as well as other matters pertaining to criminal justice (UNODC, 2021). For an international cooperation to be

effective, it must establish cybercrime laws and a set of practices for enforcing them and prosecuting people who break them. Cybercrime law includes aspects of substantive law, procedural law, and preventative law (UNODC, 2021).

Substantive law

Substantive law is based on the notion that, for an act to be described as illegal, it must be clearly written that it is, indeed, legally prohibited. It is based on the notion that there is no crime without a law or *nullum crimen sine lege* (UNODC, 2021). From a moral perspective, an individual cannot be held accountable for something that there is no law to prohibit. Substantive law, therefore, describes in detail the rights as well as the duties of people who are subject to the law, such as Governments, businesses, organizations, and individuals. The sources of substantive law differ from one Government to the next, but they include statutory law and case law.

In the context of an international cooperation to prevent CL activities, substantive law would be written to include prohibitions against certain types and forms of cybercrime. The codified laws should also detail the punishments associated with breaking each of the established laws. To date, many nations have established these types of laws that are applicable to their respective jurisdictions (Lenaerts *et al*., 2012). The focus of substantive law is on the essence of the crime and the mental aspect. The international community will need to determine if levels of culpability based largely on state of mind apply to CL practices. For example, there is a distinction in many courts between purposefully and willfully committing a crime.

Procedural law

Procedural law serves as an additional legal framework for the international cooperation on CL to utilize when creating appropriate regulations and practices. Simply put, procedural law defines the processes and the procedures that are to be applied to substantive law as a means of enforcement (Lenaerts *et al*., 2012). Criminal procedure falls under procedural law and entails a complete set of standards for dealing with persons, organizations, or Governments suspected, accused, or convicted of breaking

substantive law. With cybercrime law, procedural law will include the jurisdictions of each entity involved on the global level. It will also lay out the investigative powers of each stakeholder, rules and regulations concerning evidence and data collection, search and seizure standards, and standards for retaining and preserving evidence such as data. Establishing agreed-upon procedural law would be essential for any international cooperation to combat CL activities. The laws would dictate the precise framework to be used for enforcing the laws set forth by the organization.

Preventative law

As the name suggests, preventative law serves to prevent crimes through regulation and managing risks. Within the broader context of cybercrime, the goal is to prevent cybercrime. If prevention is not feasible, then the goal is to minimize the damages of these types of harmful actions. Preventative law is excellent for ensuring that the required tools, processes, and protocols are in place to allow law enforcement agents to do their jobs. These tools, processes, and protocols are required for the law enforcement agents to identify CL behavior, investigate the persons or organizations involved, and prosecute the perpetrators (UNODC, 2021).

Lessons from Other Nations' Approaches to Combating ML and CL Activities

Another way for international cooperation in establishing appropriate regulations and practices for combating ML and CL activities is to explore the tactics used by other nations with successful programs already in place. The US' anti-ML strategy is often used as a blueprint for the international community to follow. The US anti-ML strategy may be modified and updated to apply to CL activities, too.

The US anti-ML strategy, at its core, is based on the overarching notion that three specific groups of stakeholders benefit from ML activities — the launderers, the institutions who earn money through the associated transaction fees for transferring the money (i.e., doing the laundering either intentionally or unintentionally), and nations which use ML to attract capital investments through offering relaxed regulations on ML (UNODC, 2021). The US policy, therefore, aims to shift the costs of

ML to these three groups to put pressure on them to stop engaging in illegal money practices.

The first US policy for combating ML involves implementing and enforcing the Bank Secrecy Act of 1970, which serves to allocate costs to the vehicles of potential ML. The US implemented, through the Bank Secrecy Act, extremely strict and specific reporting requirements for commercial banking institutions to follow in their daily reporting practices. More specifically, any transaction over USD 10,000 requires meticulous reporting and record-keeping minimum requirements, and fines are levied on institutions that fail to do so (Turner, 2004). The goal is to force these institutions to create a paper trail that will serve investigators in their auditing process and lead them from the laundered money to the individuals responsible for conducting illegal activities. For wired transfers, financial institutions must maintain written records for at least five years so that investigators have a comprehensive look at the money being wired to a specific account. The same rules and standards apply to any entity described as a money transmitter (Turner, 2004). The US Government realized that, given the new rules, some financial institutions started to complain about the hassles and expenses associated with the regulations. The increased number of complaints were viewed as evidence that the policy is forcing these institutions to internalize the costs associated with participating in ML activities, thereby reaching one of the goals of the US-based policy (Turner, 2004).

The same type of policy as the US Bank Secrecy Act of 1970 may and should be implemented on an international scale to deal with CL activities and discourage money transmitters from participating in ML and CL activities. If financial institutions throughout the globe were required to uphold these same standards of reporting and record-keeping, they might be less likely to engage in illegal activities or turn a blind eye to questionable transactions. While it is challenging to precisely estimate the degree to which the policy reduced ML activities in the US, the available evidence suggests that it was effective, at least at reducing these types of activities (Turner, 2004).

The second US policy worth exploring and applying on a global level is the Money Laundering Control Act of 1986. This was the very first regulatory scheme designed to explicitly criminalize ML activities in the US. It criminalized the willful acceptance of money that is obtained from illegal activities or the act of structuring "transactions for the purpose of avoiding the reporting requirements" (Turner, 2004). The US Money

Laundering Control Act of 1986 stipulates that guilty parties must forfeit any money obtained through ML activities. The goal of this mandate is to force money launderers to bear the cost of their illegal activities, again, harkening back to the US' core framework for discouraging ML in the first place.

The US Money Laundering Control Act of 1986 is composed of two sections. The first focuses on money obtained through specific illegal activities. In accordance with the mandate derived from that section, an individual is culpable of ML if they make a transaction that involves dirty money with the purpose of promoting an illegal activity that is specific in nature. The second section explores ML in terms of property which is obtained through specific illegal activities. This stipulation does not leave a loophole for people engaging in willful blindness toward ML activities. Penalties are harsh and include forfeiting the illegally obtained funds as well as additional fines and, in some cases, prison time, regardless of whether the individual knew that they were engaging in illegal monetary activities (Turner, 2004).

The US Money Laundering Control Act of 1986 framework is applicable to the international arena as well. The same general rules and standards, with appropriate penalties for breaching the law, may be applied to the international community. The goal would be to have all participating nations agree to uphold these standards. Sanctions should be placed on Governments which refuse to do their part to uphold these minimum requirements, thereby shifting costs to the Governments as a means of encouraging participation to ensure a worldwide control of the CL activities.

The US utilizes a different approach abroad than it does domestically. It makes use of economic coercion to encourage foreign nations with loose anti-ML or anti-CL standards to internalize costs for activities associated with inappropriate money handling (Turner, 2004). The US is able to do so because it is an international economic leader, but the same general principles should be applied by a global cooperation since it would likely include the US and, therefore, have even more economic clout. If most nations in the world agreed to require the same high standards, other nations would be obliged to strengthen their monetary policies to better tackle issues of ML and CL. The US cuts off the ability of nations with relaxed ML standards to use the US financial system (Turner, 2004). On the international level, the same economic sanctions should be

implemented on nations that are willfully turning a blind eye to the control of ML and CL activities, thereby forcing them to internalize the costs associated with their harmful monetary policies or change their approaches to tackle these illegal money handling practices.

The USA PATRIOT Act is a highly polemic piece of legislation, but it does serve to thwart CL activities through monitoring online traffic. While the legislation might be overreaching, it has been shown effectiveness at identifying CL behavior and holding culpable parties responsible. The tools used by the US to combat CL are excellent and include sophisticated technology designed to monitor online communications and exchanges. The US spreads the cost throughout the worldwide cyberspace to make various entities internalize the fees associated with CL activities (Turner, 2004). The same policy might be applicable at the international level, but there would be legal obstacles associated with implementing it. However, a modified version that more appropriately tracks illegal ML, CL, and terrorist activities should be accepted by the international community.

Another framework to consider is the FATF Anti Money Laundering and Counter Financing of Terrorism (AML/CFT) Standards. AML/CFT has a variety of tools and technologies at its disposal that may be used to combat CL activities at the global level. Its current tools may expose the internal and external infrastructure used by criminal organizations that engage in CL activities. The tools may outline the webs and networks of corruption and uncover terrorist planning actions. The tools, moreover, provide law enforcement authorities with a variety of roadmaps to individuals who are responsible for criminal, illegal, and illicit actions. AML/CFT's technologies have been employed to recover laundered assets and force culpable parties to forfeit their holdings. Finally, evidence shows that the tools and technologies owned by AML/CFT support effective and far-reaching deterrence policies against a comprehensive list of criminal activities such as ML and CL (United States Department of State, 2021). AML/CFT makes use of national and international forums to identify, analyze, and promote international standards against ML and terrorism financing. These forums are excellent for sharing information and encouraging various stakeholders to work together to establish a comprehensive plan. Therefore, AML/CFT's framework for disseminating information as well as their tools and technologies should be incorporated into any international cooperation to fight against ML and CL activities.

Agencies and Actors

Logically, an international effort to combat CL activities will include numerous agencies and actors. Ideally, the already-established ones would join the international cooperation because they have significant resources and robust networks in place. The purpose of this section is to explore some of the best potential agencies and actors to form the international cooperation and share in the efforts to fight against CL activities in the international arena.

The United Nations

The United Nations (UN) plays a significant role in combating CL activities in part due to its extensive outreach and ability to unite many key stakeholders throughout the international community. Its Member States, which currently total 193 sovereign nations, are obligated to follow the rules and regulation set forth by the UN, so the organization has a broader outreach backed by law than most international efforts. Importantly, the UN hosts a variety of conventions that may be used to address issues aiming at the international cooperation on how to control or combat CL activities in a comprehensive manner, and these events transpire throughout the year, making them appropriate for updating stakeholders on changes in policy and procedures, as well as excellent venues for sharing time-relevant information (Rébé, 2019).

The United Nations Office on Drugs and Crime (UNOCD) tackles ML and CL issues since drugs and other criminal behaviors result in the need for ML and CL. The UNOCD is a global program which recognizes that illegal crimes result in criminals having to disguise the origin of their money, resulting oftentimes in ML and CL activities (United Nations, 2021). ML allows criminals to hide the true origins of their money to make it look legitimate. Therefore, the UNODC encourages all Member States to develop effective, enforceable policies that counter ML and CL activities and, consequently, make it more difficult for nefarious groups to fund terrorist activities and get away with their unethical and illegal actions. UNOCD monitors and analyzes a wide range of problems and concerns internationally that deal with ML and CL activities. There is also an educational component that includes raising awareness about ML and CL and how these activities are used to finance terrorism. The educational

component is particularly useful for nations that do not have sophisticated intelligence-gathering capabilities to create their own databases of criminal actions and suspicious activities (United Nations, 2021).

The Global Programme against Money Laundering, Proceeds of Crime, and the Financing of Terrorism (GPML) is another international initiative aimed at stopping ML and CL activities. GPML provides aid in helping nations, particularly developing ones, to create a framework with appropriate policies and law enforcement activities that will halt the proliferation of ML and CL. GPML was tasked, by the UN General Assembly, to:

> "…continue providing technical assistance to Member States to combat money laundering and the financing of terrorism in accordance with United Nations related instruments and internationally accepted standards, including, where applicable, recommendations of relevant intergovernmental bodies, inter alia, the Financial Action Task Force on Money Laundering, and relevant initiatives of regional, interregional and multilateral organizations against money laundering." (Rébé, 2019)

Based on its set of tasks, GPML is specifically designed to explore the link between ML and terrorism funding. The primary goal or the group is to tackle ML so that funding for terrorism becomes more arduous. Undoubtedly, any international cooperation designed to thwart ML and CL activities should network with the UN and benefit from its wealth of resources, task forces, tools, technologies, and databases.

European Union and European Commission

The European Union (EU) is another stakeholder with a vested interest in working with an international cooperation to fight CL since its Member States are negatively impacted by these types of monetary crimes and criminal behaviors. The EU provides regulations that all EU Member States are expected to uphold, and the EU may directly enforce these standards through its legal frameworks. The EU recognizes that ML is complex and widespread, therefore, an international, multifaceted approach is required to stop ML activities (Migration and Home Affairs — European Commission, 2021). The EU holds that a solid approach attacks the problem from various angles. Therefore, the EU places most

of its efforts on regulating financial institutions because the evidence shows that policies directed at monitoring these types of organizations work best for combating ML. The mandate that directs the EU's efforts to stop ML is the 3rd Anti-Money Laundering Directive, which was signed into law in 2005. According to the EU's 3rd Anti-Money Laundering Directive, financial operators as well as some non-financial ones are designated as gatekeepers. As such, they are responsible for reporting to the appropriate authorities any activities that seem suspicious or unusual in nature (Migration and Home Affairs — European Commission, 2021).

A complementary component of the EU is the European Commission (EC), which is responsible for conducting risk assessments for the purpose of identifying any issue that will negatively impact the EU market and, subsequently, creating appropriate responses. The EC provides actionable recommendations for solving the problems associated with ML and CL activities throughout the EU and lists best approaches for responding to all threats at the international level. To date, the EC has provided the research and recommendations that the EU requires to put into place strong legislation that fights against ML and CL activities (Rébé, 2019).

The EU recognizes that, to effectively fight against ML and CL activities, law enforcement agencies in each Member State must cooperate and work together to catch criminals and organizations culpable of engaging in these illegal and harmful money-based practices. The EU framework allows for more effective and quicker law enforcement cooperation to take place.

The EU Agency for Law Enforcement (Europol) is the main support for all EU member states when it comes to countering serious activities to include ML, CL, and terrorism (Migration and Home Affairs — European Commission, 2021). Europol provides support and services to Member States' law enforcement agencies, and it is designed to help mitigate serious crimes that impact more than one Member State. It also serves as the hub of criminal data collection, which it shares with each Member States' law enforcement agencies. It provides the support required to combat organized crime, ML and CL activities, and terrorism (Migration and Home Affairs — European Commission, 2021). Again, any international effort to stop ML and CL activities should partner with the EU on some level to take advantage of its complex networks and comprehensive resources.

Egmont Group and Financial Intelligence Units

Another stakeholder that may be employed to stop ML and CL on the international arena is the Egmont Group, which is composed of some 166 Financial Intelligence Units (FIUs) (The Egmont Group, 2021). The Egmont Group unifies these FIUs and provides a platform for them to share information and expertise in terms of human resources. Financial intelligence is exchanged between members of the group, which is based on the notion that, through collaboration, ML and CL activities may be halted. The Egmont Group recognizes that FIUs are in an excellent position to support and cooperate with international organizations and law enforcement agencies to counter ML and CL and, by extension, other criminal behaviors to include terrorism. FIUs are highly respected and trusted gatekeepers of key financial data that serve both domestic and international interests. The Egmont Group operates in tandem with the standards that FATF has developed on Anti Money Laundering and Counter Financing of Terrorism (AML/CFT) (Rébé, 2019).

One of the major commitments of the Egmont Group is to support the missions of its various global partners and related stakeholders. It strives to serve the initiatives of FATF in its quest to overcome illegal and unethical monetary activities. The Egmont Group provides added value to its member FIUs by providing a shared community of resources and improving knowledge through research and discovery of current ML and CL practices. It has significant operational experience and is the tactical component of the AML/CFT reforms. The Egmont Group strongly supports the sharing of financial intelligence reports among stakeholders and views these collaborations as paramount to fighting against ML and CL activities (The Egmont Group, 2021).

The Egmont Group is composed of FIUs, which play a vital role in fighting against ML and CL, particularly as the money is used for terrorist activities. FIUs are tasked with obtaining and collecting, analyzing, and reporting on information that deals with financial terrorist activities and ML, including CL. Most law enforcement agencies worldwide have a FIU component, which works directly with other money-based organizations and branches of the Government. When an organization, such as a bank or a casino, among others, suspects unethical or illegal activity to be taking place, they are legally required to report these happenings to their respective FIUs. The reports they must file are often referred to as suspicious transaction reports. The goal of these reports is to allow the FIUs to

identify potential ML and CL activities and trace the guilty individuals or organizations. FIUs then report on their findings and turn their reports over to law enforcement agencies that may act on them. If the crime is committed abroad, then the FIU in one nation will turn their reports and data over to those in the nation where the crime is taking place. Criminal investigations may be initiated based on the intelligence collected by FIUs (The Egmont Group, 2021).

Red Flags for International Cooperation to Target

The evidence shows that there are red flags to look out for in international cooperation to tackle CL activities. It is essential to understand the telltale signs of CL so that efforts may be placed appropriately without wasting resources. There are only a limited number of resources that Governments and organizations have at their disposal. If they are not careful, these limited resources will be used in an ineffective and unproductive manner. Identifying red flags and, then, focusing efforts on these activities is an essential framework for dealing with CL.

The first red flag pertains to the size and frequency of the transactions in VCs. VC transactions that are indicative of CL activities are typically small amounts, so that they do not reach record-keeping and reporting thresholds. In most nations, the threshold for reporting is around USD 10,000, so the transactions are often less than this amount. The small nature of the transaction may make them hard to detect since they are not reported as most standards do not place a reporting obligation regarding them. Therefore, other indicators are required. When small transactions are made in a staggard or regular pattern in frequent, short succession, they are signs of CL activities. Another sign is depositing a VC and, then, immediately withdrawing it without another activity exchange or converting it into multiple types of VC. Often, these transactions are done quickly and at a premium cost, another indicator that they are illegal in nature (FATF, 2020).

Another red flag involves using multiple users to launder the VC. For instance, transactions which involve many VCs and several accounts, often with no logical business ties and relationships, should be monitored. These may be hard to detect because it is not always clear who might be the likely business partners and associates. Financial organizations, however, should be alerted if more than three parties are involved in the VC

transaction (FATF, 2020). Other suspicious activities include making frequent transactions within a specific time period (like over the course of a day or week) by more than one individual or from the same IP address or using large sums of money. These actions are often an indicator that someone is trying to quickly move money so as not to get caught with it in their possession (FATF, 2020).

Other signs of CL activities involve monitoring key indicators about the senders and the recipients of the funds. Sometimes, with these types of accounts, there are irregularities identified when the virtual account is created. These might include creating various accounts under several different names or using non-trusted IP addresses such as an IP address from a sanctioned jurisdiction. The individual who holds the account might change primary information associated with it often, such as email address, name, or birthdate. These are all indicators that the account might be used for illegal CL activities (FATF, 2020). With the merchant, the Internet domain might be registered to a different area than their establishment, such as a US-based company having an Internet domain registered in the Cayman Islands (FATF, 2020). This is often done to avoid careful monitoring and procure an Internet domain that will not be subject to oversight.

International cooperation should recognize these red flags and focus most of its efforts on tracking these types of patterns and behaviors to identify problematic behaviors with VCs. The result will be a better allocation of resources and, ultimately, more effective approaches to tackling CL issues on a global scale.

Conclusion

The evidence overwhelmingly shows that CL is a major issue that negatively impacts people, organizations, Governments, and the entire international community on various levels. CL activities are widespread and often international in nature. Therefore, any effort to combat CL must take a global approach to be effective and it should involve a comprehensive plan to stop launderers from making use of the global financial systems to undertake CL activities.

Many organizations already exist that are dedicated to stopping ML and CL activities. If an international cooperation is formed, it should draw on the resources and networks of organizations such as the UN, EU, EC,

Egmont Group, and established FIUs. Moreover, many nations and international institutions have already put into place robust anti-ML and anti-CL policies, such as the US, EU, and the FATF, that may be applied to a global scale. These policies may serve as frameworks for applying the same standards to a broader audience.

Global efforts should recognize the tell-tale signs of CL and dedicate their limited resources to monitoring the red flag activities. If an international cooperation is formed and makes use of the groups/organizations, best practices, tools, and technologies already in place, then it should be highly effective at combating CL activities as well as complementary ones such as terrorism, thereby resulting in positive outcomes for the entire global population.

References

Bosworth-Davies, R. (2007). Money laundering — chapter five. *Journal of Money Laundering Control*, 10, 189–208.

Chambers-Jones, C. (2012). *Virtual Economies and Financial Crime*. Cheltenham, UK: Edward Elgar Publishing.

FATF (2014). FATF report: Virtual currencies. Key definitions and potential AML/CFT risks. Financial Action Task Force.

FATF (2020). Money laundering and terrorist financing. Red flag indicators associated with virtual assets. https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf. [Accessed 4 June 2021].

Integrity Asia (2018). Cyber-laundering. The money laundering in the digital age. https://integrity-asia.com/blog/2018/09/26/cyber-laundering-the-new-face-of-money-laundering-in-the-digital-age. [Accessed 28 May 2021].

Lenaerts, K., Arts, D., Maselis, I., Bray, R. and Gutman, K. (2012). *Procedural Law of the European Union*. London: Sweet & Maxwell.

Migration and Home Affairs — European Commission (2021). Law enforcement cooperation. https://ec.europa.eu/home-affairs/what-we-do/policies/law-enforcement-cooperation_en. [Accessed 4 June 2021].

Musau, B. M. (2019). Anti-money laundering and compliance strategies of Kenya. Unpublished Doctor of Juridical Science, Diamond International Tax and Financial Services Graduate Program.

Rébé, N. (2022). *Counter-Terrorism Financing: International Best Practices and the Law*. Brill. https://brill.com/view/title/55779?language=en. [Accessed 25 May 2022].

Sambuli, N., Maina, J. and Kamau, T. (2016). Mapping the Cyber Policy Landscape: Kenya. Global Partners Digital.

The Egmont Group (2021). The Egmont Group of Financial Intelligence Units. https://www.fincen.gov/resources/international/egmont-group-financial-intelligence-units. [Accessed 4 June 2021].

Tran, H. (2020). "International Cooperation to Combat Money Laundering in the Southeast Asia: A Narrative Perspective in Vietnam." Iiste.org. https://iiste.org/Journals/index.php/JLPG/article/view/52495/54227. [Accessed 25 May 2022].

Turner, S. (2004). U.S. anti-money laundering regulations: An economic approach to cyberlaundering to cyberlaundering. *Case Western Reserve Law Review*, 15, 1–27.

United Nations (2021). Office on Drugs and Crime. https://www.unodc.org. [Accessed 4 June 2021].

United States Department of State (2021). Anti-money laundering and countering the financing of terrorism. https://www.state.gov/anti-money-laundering-and-countering-the-financing-of-terrorism. [Accessed 4 June 2021].

UNODC (2021). Cybercrime module 3. Key issues: The role of cybercrime law. https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/the-role-of-cybercrime-law.html. [Accessed 29 May 2021].

Wangui Maina, J. (2021). Cybercrime and the legal and regulatory framework. http://www.isaca.or.ke/resources2018/Juliet%20Maina-Cybercrime-Legal-and-Regulatory-Framework-2018.pdf. [Accessed 28 May 2021].

This page intentionally left blank

https://doi.org/10.1142/9781800612839_0010

Chapter 9

Anti-Cyber Laundering: The Inclusion of Virtual Asset Service Providers

Jennifer Palpacuer and Benjamin Aouizerat

Prolegomena: Anonymization and Pseudonymization

Virtual assets (VAs) are often linked to the notion of anonymity. If this were the case, this chapter would be condemned to be the shortest in this book. Perfect anonymity in no way correlates information to a determined or determinable person. On the contrary, de-identification allows information to be linked to a person, but at the cost of some effort.

Anonymization is a technique that removes all identifying information from a dataset. According to the international standard ISO 29100 (2011), it is "the process by which personally identifiable information (PII) is irreversibly altered in such a way that the subject of the PII can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party." Anonymization is therefore marked by the irreversible nature of the loss of the identifiability of individuals.

In contrast, pseudonymization or "reversible anonymization" consists of replacing one attribute by another in a record. The natural person is therefore still likely to be identified indirectly. For example, the coding of a client's name does not prevent his or her individualization if it is possible to have access to other attributes such as gender, address, or date of birth. Pseudonymization limits the risk of direct correlation between

personal data, but it does not eliminate it. Therefore, pseudonymization is not a weakened form of anonymization, but a security measure.

Asymmetric encryption (public key, private key) guarantees the security of transactions. Without additional data, it is not possible to identify the owner of a public key, but if the link is established, then it is possible to trace all the transactions he has received and sent. As such, Bitcoin, for example, is a pseudonymous system rather than an anonymous one. And it is this pseudo-anonymity that is at the center of anti-money laundering and terrorist financing thinking.

Introduction

It is wholly accepted that cryptocurrencies and related technologies create new opportunities for criminals and terrorists to launder their proceeds or finance their illicit activities. Many characteristics of VAs and virtual asset service provides (VASPs) point to a high(er) risk activity: cross-border flows, use of anonymity-enhancing techniques, and non-face-to-face business relationships. The above-mentioned indicators were already considered high risk by the Financial Action Task Force (FATF),[1] an intergovernmental body that sets international standards to fight money laundering and terrorist financing (AML/CFT). To achieve this goal, the FATF issued a set of 40 Recommendations in 1990, which have been regularly been updated since (FATF, 1990).

The FATF defines VAs as "a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. VAs do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations" (FATF, 2021).

A VASP is designated as "any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

- exchange between VAs and fiat currencies;
- exchange between one or more forms of VAs;

[1]The FATF was established by the G-7 Summit that was held in Paris in 1989.

- transfer of VAs (in this context of VAs, transfer means to conduct a transaction on behalf of another natural or legal person that moves a VA from one VA address or account to another);
- safekeeping and/or administration of VAs or instruments enabling control over VAs;
- participation in and provision of financial services related to an issuer's offer and/or sale of a VA (FATF, 2012–2021).

The FATF has been addressing issues related to virtual currencies since 2014, by regularly updating its 40 Recommendations and through regular publications on the subject, such as the "Key Definitions and Potential AML/CFT Risks" (FATF, 2014) or the "Guidance to a Risk-Based Approach to Virtual Currencies" (FATF, 2015).

The most significant changes to the 40 recommendations, regarding VAs and VASPs has been made fairly recently. In October 2018, modifications were made to Recommendation 15 and new definitions of "virtual assets" and "virtual asset service providers" were included in the glossary. A few months later, in June 2019, an Interpretive note to Recommendation 15 was added in order to explain how AML/CFT obligations apply to VAs et VASPs.

To keep up with a rapidly changing environment, FATF follows up regularly on VAs and VASPs domestic regimes through 12-month reviews by analyzing how the revised recommendations are being implemented and the progress made. They are based on a questionnaire completed by members of the FATF and FATF-style regional bodies (FSRB), representing more than 200 countries and jurisdictions. The first review took place in June 2020, the second followed a year later.

These annual reviews are also helpful in helping the FATF update its "Guidance to a Risk-Based Approach — Virtual Assets and Virtual Assets Service Providers" (FATF, 2019) (the VA and VASPs guidance), initially adopted in June 2019. In addition to contributions by the countries themselves, a public consultation of the guidance, whose goal is namely to help VASPs, as well as other regulated entities, implement the FATF recommendations is currently underway. The revised Guidance should be adopted by the next FATF plenary, which will take place in June 2021. Two of the main goals of this revision is to define more clearly the concepts of VAs and VASPs and provide more clarity of the Travel Rule's implementation.

Other than the obligations that apply to VASPs, the VA and VASP guidance also details what obligations apply to VAs as such. For example, the definition of "funds," often used throughout the 40 recommendations, expressly and clearly include VAs.

Risks related to new technologies in general, and VAs and VASPs in particular, should be regularly assessed. Contrary to certain other regulated entities for which it is acceptable to be supervised by self-regulatory bodies, FATF recommendations requires VASPs to be monitored only by a competent authority. As for any other regulated entity, supervision is to be dependent on a risk-based approach.

To gain a better understanding of the role, VASPs can and should participate in the fight against money laundering and terrorist financing, and pinpointing the obligations they are required to perform is a first step (I). The VASP sector faces many significant challenges (II) but if they are resolved, VASPs are in a position to contribute actively and markedly to AML/CFT (III).

The applicable FATF recommendations to the VASP sector

Considered the global benchmark for AML/CFT regulations, the FATF standards have included many references to VAs and VASP and have detailed what is expected of countries in order to deal with such activities. First and foremost, licensing or registration of VASPs (A) is considered key to ensure necessary and adequate supervision of how they are complying with their AML/CFT obligations (B).

The licensing or registration of VASPs: A prerequisite

Recommendation 15 requires VASPs to be licensed or registered, an essential step in identifying such activities. In the case of legal persons, VASPs must register in the jurisdiction where they are created. Individual jurisdictions also have to option to demand a form of licensing or registering by VASPs that have a link with said jurisdiction, whether by offering their products or services to customers based locally or if they conduct operations in this jurisdiction.

Regarding natural persons acting as a VASP, Interpretive note to Recommendation 15, the place of business should determine the licensing or registering jurisdiction. Because of its cross-border nature, a VASP's

"place of business" may mean different things: it could be where the business is conducted, where the natural person resides, or even where the data are stored. If the business is linked to more than one jurisdiction, a solution could be to choose the prevailing factor to determine the licensing or registering country. Another option would be to require multiple licenses similarly, to what is potentially applicable to legal persons.

Licensing or registering is an important preventive measure, one that keeps criminals or persons associated to them from having an active role in a VASP, whether as a beneficial owner or holding a significant or controlling interest or carrying out a management function. Hence, the licensing or registering process must include controls on the individuals wishing to establish themselves in a VASP activity. These checks can be undertaken by the licensing or registering authority or may be delegated to any other competent authority. These verifications should take place not only when the activity is created but also when there are changes to shareholders or managers.

Like for other obliged entities, the FATF standards insist on preventing unlicensed or unregistered VASPS from conducting their activities. Countries are thus expected to be proactive in identifying those operating without the appropriate license or registration, and subjecting them to appropriate sanctions. The 40 recommendations do not specify what sanctions to apply but the standards require they always be "effective", "proportionate," and "dissuasive."

In light of these rigorous requirements, some jurisdictions may be tempted to prohibit VASP activities altogether, but the FATF standards encourage countries to apply the same licensing or registration procedures as for financial institutions who offer VASP activities. Thus, the implementation of an entirely new process is not necessary and may facilitate it.

Once a system to identifying and authorizing VASP activity is in place, it is essential to clarify what AML/CFT obligations should be fulfilled by this new type of obliged entity and to what extent.

Measures applicable to the VASP sector

For the most part, VASPs are upheld to the same obligations as other regulated entities, but some of them must be adapted to the activity's specific nature.

Measures common to all obliged entities

One of the main points to keep in mind is that the FATF recommends that VASPs be required to apply the same AML/CFT obligations as any other regulated entity. The requirements in question are described in Recommendations 10 through 21: they cover issues such as customer due diligence (CDD), record-keeping, politically exposed persons (PEPs), reliance on third parties, internal controls and foreign branches and subsidiaries, higher-risk countries, reporting of suspicious transactions, tipping-off, and confidentiality.

With regards to reporting of suspicious transactions, in September 2020, the FATF published a report entitled "Virtual Assets — Red Flag Indices of Money Laundering and Terrorist Financing" (FATF, 2020) to guide national authorities in detecting criminal activity related to VAs. To this end, it highlighted various indicators that could suggest criminal behavior. The key indicators in this report focus on technological features that enhance anonymity; geographic risks by use of legal failures; unusual or suspicious transaction patterns; consistency of transactions in terms of purpose, amount, and frequency; profiling of parties to the transaction; and the source of funds. This report contains a great deal of useful information for taxable persons who are required to establish and implement their risk-based approach.

It is interesting to note that VASPs are required to comply with similar obligations as other regulated entities. Even though the language used by Recommendation 15 refers to the "use of new or developing technologies," it seems that these do not necessarily require new or different obligations. In fact, AMC/CFT obligations for all regulated entities, including VASPs, have roughly remained the same even if the FATF has adjusted a certain number of requirements throughout the years, to take into account the inherent qualities of the services or products.

Measures customized to VASPs

Among some of the adjustments mentioned above, one affects occasional transactions. Through its standards, in particular the Interpretive note to Recommendation 15, the FATF has upheld a USD/€1,000 threshold for occasional transactions: above that amount, VASPs should apply preventive measures as prescribed by the FATF standards, in particular Recommendation 10, which requires conducting CDD. It is noteworthy

that the threshold applicable to financial institutions when carrying out occasional transactions for clients is far higher, and set at USD/€15,000. When considering designated non-financial businesses and professions (DNFPBs), an identical threshold is applicable to dealers in precious metals and stones whereas casinos apply a much lower threshold, set at USD/€3,000 threshold. On a risk-based approach, a fundamental principle within the FATF standards, the risks associated with VASP-linked transactions are clearly assessed as more important, which explains the difference between the chosen thresholds. Considered more at risk, VASPs are required to pull their weight in the global fight against money laundering and terrorist financing.

In fact, certain countries are considering applying even more stringent measures than the FATF recommends, such as the US. A proposal to amend the Bank Secrecy Act (BSA) plans to lower current USD 3,000 threshold down to USD 250 (FinCEN.gov, 2020), way below the recommended USD 1,000. It is common knowledge that terrorist financing can be carried out in a plurality of unit amounts. Similarly, the laundering of the proceeds of crime in the form of crypto-assets is often disseminated to a large number of wallets created for the purpose. The question of thresholds is therefore crucial in this ecosystem. Nevertheless, when establishing business relationships, which implies more or less medium-to-long-term interactions with a client, the same preventative measures apply to VASPs and financial institutions.

The other main adjustment applies to the wire transfer rules set out in Recommendation 16. Like other financial institutions, VASPs are to apply the same rules, in a modified form, under what is now commonly known as the "travel rule." The FATF defines a wire transfer as "any transaction carried out on behalf of an originator through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary person at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person."

This definition has remained the same, but the Interpretive note to Recommendation 15 mentions that countries should apply Recommendation 16 to VA transfers. The term "wire transfers" has thus evolved to include such transfers, since they operate in a similar way as traditional wire transfers. The term "transfers" has therefore evolved to include these transfers, since VA flows are largely reminiscent of traditional transfers even though they use specific technologies. The FATF

methodology, used to assess compliance to its standards, mentions all VA transfers should be treated as cross-border transfers, for the purposes of applying Recommendation 16 to VASPs.

The Recommendation, which applies to both domestic and cross-border transactions, requires both originating and beneficiary VASPs to obtain and hold originator and beneficiary information.

The interpretive note to Recommendation 16, paragraph 6, applicable to cross-border qualifying wire transfers, itemizes what is expected of originating and beneficiary VASPs.

Information accompanying all qualifying wire transfers, including VA transfers, should always contain:
Information related to the originator:

(a) the name of the originator;
(b) the originator account number where such an account is used to process the transaction;
(c) the originator's address, or national identity number, or customer identification number, or date and place of birth;

as well as information related to the beneficiary:

(d) the name of the beneficiary; and
(e) the beneficiary account number where such an account is used to process the transaction.

If there is no account, a unique transaction reference number should be included which allows traceability of the transaction (FATF, 2016–2017).

For VA transfers below the chosen threshold, the FATF standards do not encourage any exemption and consider that VASPs should collect, at a minimum, the name of the originator and the beneficiary as well as the wallet address for each or a unique transaction reference number. In any case, if any cause for concern, related to money laundering or terrorist financing, is raised, VASPs should process them and undertake any remedial action, as needed.

The requirement for VASPs to "obtain" the information indicated above, whether it is the name or the address, is achieved by applying traditional CDD measures[2] (FATF, 2012–2021), through a know your

[2]Recommendation 10 of the FATF standards.

customer (KYC) process, which requires identifying the client and verifying said identity using reliable, independent sources of documents, data, or information.

VASPs should also "hold" said information, which refers to the requirement developed in Recommendation 11 on record keeping which explains that all CDD information and transaction records should be maintained for at least five years. This obligation covers all originator and beneficiary information collected.

The FATF requirements also mention the term "accurate." An ordering VASP (or any other obliged entity, such as a financial institution) should obtain and hold required and accurate originator information and required beneficiary information and submit the information to beneficiary institutions. According to FATF terminology, "accurate" is used to describe information that has been verified for accuracy. Thus, the ordering VASP, when obtaining originator information, must make sure to verify such information. As for beneficiary information, the ordering VASP must collect the required information but need not verify it. Similarly, beneficiary VASP must also obtain and hold required originator and beneficiary information but is only required to check accuracy on beneficiary information (and not originator information).

In some instances, the above-mentioned information is not necessarily what a VASP has on hand, thus adequate equivalent information in a VA context should be collected. Although obtaining the names of the originator and beneficiary is the same process for VASPs and financial institutions alike, in practice, an account number (whether for the originator or the beneficiary VASP) may mean different things for a VASP or a financial institution. In the VA context, this could mean the "wallet address" of the VA and the "public key" of the customer who is sending the VA transfer.

The interpretative note to Recommendation 15 also states that VASPs should submit the required information immediately and securely. A footnote to the interpretative note indicates that the information can be submitted either directly or indirectly. It is not necessary for this information to be attached directly to the VA transfers. It is acceptable to submit the information through a different process, as long as the transfer is compliant with the FATF standards. VASPs are not restricted to a chosen technology but they must make sure the selected process encompasses all the requirements, developed below.

The use of the term "immediately" indicates to importance of submitting the required information within a specific timeframe. The submission should intervene either before or precisely at the same time as the transfer. If the submission of information occurs subsequently to the transfer, the FATF standard loses much of its value: many of the actions a VASP are called on to perform would be impossible to complete if the information accompanying the VA transfer is not sent simultaneously.

VASPs should submit the required information "securely" by any means which protect the security and integrity of the information and its availability. Data protection is key, and any breaches of security should be avoided. The purpose of a secure submission is twofold: it helps VASP observe their record-keeping obligations as well as facilitate the use the information.

One of the main uses of originator and beneficiary information is intended for the authorities. The Interpretive note to Recommendation 15 (paragraph 7(b)) requires VASP and other obliged entities to make such information available on request to the appropriate authorities. Competent authorities comprise financial intelligence units and law enforcement agencies (police and judicial). The strict framework is intended to take into account the cross-border nature, inherent to VA transfers, and their speed, characteristic of this type of transfer. It is not necessary for the information to be attached directly to the VA transfer itself, and the information can be submitted either directly or indirectly. The FATF expects countries to apply Recommendation 16 regardless of whether the value of the traditional wire transfer or the VA transfer is denominated in fiat currency or a VA.

The FATF standards do not specifically address the issue of VA transfers to or from unhosted wallets. The individual holder of the VAs controls the private keys associated with the addresses and can store or use them without the need of any third party. The generalization of cold wallets creates an additional difficulty on AML/CFT grounds. The holder of a cold wallet has the full availability of his assets without an intermediary. If this holding mode meets a legitimate security requirement, it makes a significant part of the VAs invisible to the regulators. Unlike standard bank accounts, cold wallets cannot be frozen or emptied by governments.

Unlike traditional fiat wire transfers, it is highly unlikely that VA transfers always involve two obliged entities, whether it be a VASP or a financial institution. If Recommendation 16 is to be applied strictly, it is safe to say that in the case a VA transfer originates from an obliged entity or is sent to one, either the originator or beneficiary entity should be

required to comply with their information-holding obligation with respect to their customer only.

Furthermore, "peer-to-peer" (P2P) transactions are transfers of VA without the need for a VASP or other reporting intermediary. Thus, P2P transactions are not expressly subject to AML/CFT obligations under the FATF Recommendations. Indeed, the FATF Recommendations impose obligations on intermediaries rather than on the customers or users themselves. P2P transactions may present an increased risk of money laundering and terrorist financing, as they can potentially be used to bypass regulated operators and thus evade AML/CFT regulations.

However, submitting originator or beneficiary information to a non-obliged entity does not appear practical and of limited value to AML/CFT. The fact that such a transaction does not include an obliged entity may be an indicator of a higher risk situation that may require the obliged entity to consider many alternatives: prohibiting, limiting, or placing such transactions under enhanced monitoring, which could lead to suspicious activity reporting, if applicable. At a domestic level, some countries are considering applying stricter regulations and/or are already enforcing existing regulations. For example, in May 2015, Ripple Labs Inc. was fined USD 450,000, on the basis of a settlement agreement, after it violated many requirements of the BSA, including failing to implement and maintain an adequate AML/CFT program designed to protect its products from use by money launderers or terrorist financiers. Ripple agreed to engage in remedial actions, which expressly cited complying with the Funds Transfer and Funds Travel rules (FinCEN.gov, 2015).

Although the usefulness of the measures prescribed by the FATF standards cannot be denied, their effective implementation is not entirely without difficulties.

The main challenges

VAs and VASPs combine two types of difficulties, both of a legal and technical nature.

Legal challenges

Following the adoption of the European Union Anti-Money Laundering Directive (5AMLD) in May 2018, Member States were required to bring into force any law, regulation, and administrative provision necessary to

comply with the Directive by January 10, 2020. Its content mostly corresponds to the FATF standards but they are not identical. 5AMLD applies to exchange services between virtual currencies and fiat currencies as well as custodian wallet providers[3] (5AMLD, 2018) but crypto-to-crypto exchanges are not included and, as such, not required to comply with the EU Directive. Not only is the EU Directive not as comprehensive in terms of the list of mandatory entities, but it is also more restrictive than the FATF regulation in terms of the due diligence requirements for VASPs.

In an ecosystem that is already very singular, the coexistence of competing terminologies adds additional complexity that is detrimental to the understanding of the greatest number. In AMLD5, virtual currencies refer to a digital representation of value that is not issued or guaranteed by a central bank or public authority, is not necessarily attached to a legally established currency, and does not have the status of money or currency but is accepted by natural or legal persons as a medium of exchange and can be transferred, stored, and exchanged electronically. According to FATF, a VA is a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes. VAs do not include digital representations of fiat currencies, securities, and other financial assets that are already covered elsewhere in the FATF Recommendations. AMLD5's definition of "virtual currencies" is much more restrictive than the FATF definition of "virtual assets." AMLD5 only covers "cryptocurrencies" in a general sense and therefore does not include all types of VAs. It is also quite remarkable that the common thread in these definitions is to say what VAs are not rather than what they are.

On the harmonization of texts, ESMA[4] and EBA[5] have advocated in various works published in 2019 for a common approach for all crypto-assets, notably through the inclusion of tokens (utility and investment) in the notion of "virtual currency" insofar as they use comparable technologies and can be stored, transferred, or even exchanged on the same platforms as cryptocurrencies. This approach can only be approved insofar as

[3]According to the EU Directive, a custodian wallet provider is an "entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies."

[4]European Securities and Markets Authority (ESMA), the EU's securities markets regulator.

[5]European Banking Authority (EBA).

all tokens are de facto vehicles for moving economic value independently of their initial purpose. Also, recent developments in the crypto-sphere call to question the need to go even further and, in particular, to erase superfluous qualifications and unnecessary borders in favor of a notion of crypto-asset that would encompass all these media and be as neutral as possible from a technological point of view. Indeed, it would not be surprising if the volatility of some tokens sparks the interest of a traditionally Bitcoin-centric crime for liquidity reasons. The craze for different classes of tokens in circulation, such as non-fungible tokens (NFT), calls for a systemic thinking that imposes a broad and independent approach to technological developments.

At a domestic level, jurisdictions have implemented, to varying degrees, VASPs AML/CFT regimes, while others have yet to adopt any type of measure. This situation is likely to impede any efforts due the cross-border nature of VAs and VASPs. Depending on its country of registration or where it is located, some VASPs may be required to implement and comply with the travel rule while others are still exempt. This is what is known as the sunrise issue. The challenge VASPs face when dealing with other VASPs, located in jurisdictions where the travel rule is not yet in force, is quite understandable. If the risk-based approach is to be applied, it is each VASP's individual decision to interact with other VASPs who submit to different regulatory regimes. Potential supervisory action may push VASPs, placed under stricter mechanism, to comply, and possibly, coax other VASPs to implement the travel rule, despite a lack of regulation, through business traditional business practices (market pressure, contracts, etc.). Nevertheless, as long as the travel rule is not standardized and applicable to all, it seems difficult to ensure compliance with robust measures and may very well dampen technological innovations.

VAs and VASP activity are based on pioneering technologies that have multiple uses but their development and their features may constitute obstacles to effective implementation of AML/CFT measures.

Technical challenges

Contrary to financial institutions who are equipped with the SWIFT network for interbank transfers, VASPs currently do not benefit from an existing system, whether at a national or an international level for reliably

transferring identification data for payment transactions on the blockchain. Even if bilateral agreements between service providers develop, this is currently not enough of a widespread practice to include all market players.

FATF engages in "technology-neutral" recommendations. Their goal is to remain sufficiently flexible and include any system that allows VASPs to meet the FATF's requirements and have left it up to industry participants to develop an appropriate solution. While it is commendable for an international body providing guidance to be impartial, it has left many VASPs uncertain on how to comply with their obligations. Many countries have followed suit and adopted the same position has the FATF — for example, Switzerland, through FINMA's[6] guidance note 02/2019 entitled "Payments on the blockchain" and published in August 2019, in which the supervisory authority "reaffirms its technological-neutral approach" (FINMA, 2019).

Even if this may come as a surprise, the industry, mainly created on principles of decentralization and deregulation, has not remained passive and have proposed many innovative solutions. Many actors realize and accept that their refusal to comply with an international/national regulatory framework may likely, in the long term, impede their ability to do business.

Regardless of what solution(s) VASPs will commit to, it is highly likely to need to bring together the following criteria:

- be common (similar to what financial institutions experience with SWIFT);
- transfer the information immediately;
- transfer the information securely; and
- minimize the risk of data breaches.

As already mentioned, it is not necessary for the information to be transmitted on the blockchain; transmission can take place via other communication channels.

As the extent of the requirements for VA transfers are not identical, depending on whether a counterparty is another VASP or an unhosted wallet, an added difficulty emerges: VASP must be in a position to determine

[6]FINMA is the Swiss Financial Market Supervisory Authority.

whether a transfer is with a counterparty VASP or not. It is also conceivable that VA transfers involve "intermediary VASP" or other intermediary entities that facilitate transfers and thus create a chain of VA transfers. It appears in line with the FATF standards to ensure that such intermediaries duly comply with the travel rule. If a comparison is to be made, such rules already apply to wire transfers between financial institutions. If the legal and technical challenges cannot be met by the VASP sector, they may impede the ability of these obliged entities to contribute usefully to AML/CFT, through remedial actions on their part.

Enforcement measures

If such challenges can be overcome, the VASP sector is in position to inform competent authorities, notably through applying their reporting obligation (A) but also by freezing and prohibiting transactions with any designated person of entity (B).

The consequences of monitoring the availability of information

The interpretive note to Recommendation 15 clearly mentions that VASPs should monitor the availability of information, as required by Recommendation 16. VASP should screen all VA transfers and detect those which lack the required originator and/or beneficiary information. When such cases are identified, "appropriate measures" have to be taken. Such measures could include not executing or rejecting, as the case may be, a VA transfer that does not include the required information.

In this case, especially if it is a recurring issue, the VASP may want to consider reporting to the competent financial intelligence unit, through a suspicious transaction report (STR). In this respect, VASPs are potentially an important contributor to financial intelligence.

A number of VA flow monitoring solution providers have developed a classification of known VASPs to highlight their sensitivity to AML regulations and the type of available data they collect on their customers.

Though essential, VASPs reporting obligations are not complete without addressing their freezing and prohibiting transactions requirement.

Freezing and prohibiting transactions

According to Interpretive note to Recommendation 15, still in Paragraph 7(b), VASPs should take "freezing action and prohibit transactions with designated persons and entities." This requirement is applicable on the same basis as set out in Recommendation 16.

It is accepted that criminals may make use of VAs to evade financial sanctions (FATF, 2020). Movement of funds outside of the traditional financial system and the possibility of avoiding sanctions explains the willingness to include VASPs in freezing obligations. In this regard, it is constant that some countries are questioning the advisability of adopting a cryptocurrency in order to free themselves from their dependence on certain currencies and related regulations.

Like financial institutions, VASPs are required to take freezing action and should prohibit conducting transactions with persons and entities, designated on the basis of the relevant United Nations Security Council (UNSCR) resolutions, such as Resolution 1267 (UN Security Council, 1999) and its successor resolutions, and Resolution 1373 (UN Security Council, 2001), relating to the prevention and suppression of terrorism and terrorist financing.

In this respect, Recommendations 6 and 7 of the FATF standards expressly include VAs within the obligation to freeze without delay funds or assets of designated persons or entities. In this context, no funds or assets are to be made available to or for the benefit of such persons or entities in relation to two types of sanctions. These include targeted financial sanctions linked to terrorism and terrorist financing and those related to proliferation.

VASPs are thus required to screen transactions to comply with relevant UNSCR resolutions and take to appropriate follow up action if needed. However, obliged entities are in the position to identify designated persons or entities only if information, such as the name of the originator of the beneficiary, is collected.

Interpretive note to Recommendation 15 refers to "freezing," which implies that a VASP must refuse to make any type of fund or asset available to a designated person or entity if present in their customer base. Prohibiting transactions requires a VASP to ban any movement of funds or assets to or for such persons or entities: outgoing and incoming transfers are not allowed.

Complying with freezing measures are crucial for obliged entities, as failure to do so is among the more severely sanctioned AML/CFT obligations. Freezing assets or prohibiting transactions are not easy tasks: obliged entities, including VASP, must be equipped with filtering solutions. Several market players offer acceptable solutions. Supervisory authorities are open-minded to different solutions but do require that features of the chosen system be capable of processing the name of all clients as well as transactions and expect that any "hit" has a blocking effect.

Customer screening, for the originator VASP and the beneficiary one, should be implemented as soon as the client is onboarded and continuously throughout the duration of the entirety of the business relationship. This requirement implies the obligation to keep all information on customers up to date to take into account any modification, such as a name change.

Screening a customer base is only part of the freezing and prohibition obligations. Both ordering and beneficiary institutions should prohibit transactions with designated persons and entities. In this respect, they are also expected to screen the names of the counterparty (the originator or the beneficiary) when a VA transfer is carried out. As mentioned earlier, since the FATF standards do not require the information regarding the originator and beneficiary to be transferred using the same system as the VA transaction, purely technical aspects may impede VASPs' efforts to comply fully with their obligations. It is the VASPs' responsibility to implement a system designed to complete a VA transfer only once the screening process is achieved and no results have come about. If a cause for concern is raised, it must be processed accordingly before the transaction is allowed to go through. False positives are a possibility and may occur regularly. Supervisory authorities expect the false positives to be analyzed and confirm that any indicator of risk is ruled out. Any action on the part of VASPs must be documented to ensure effective supervision. It is obvious that the processing of such hits, whether regarding the customer or the counterparty, can be labor intensive, and it is left up to concerned entities to find the best solution.

Furthermore, any future innovations to VA transfer systems should take this obligation into account and remember to include an appropriate framework of control.

Conclusion

Challenges linked to obfuscation are numerous

Given their intrinsic characteristics, VAs constitute a medium that can be exploited by criminals for money laundering and terrorist financing practices. In terms of money laundering, crypto-assets make it possible to cloud financial flows by loosening the link between the transaction and its authors. This opacity results from two main factors: the support and the channels. The medium is the crypto-asset itself. Some well-known VAs have been natively designed to ensure maximum anonymity. On the contrary, Bitcoin alone offers pseudo-anonymity.

Channels are also an important consideration. Without even resorting to very specific networks, many websites now offer mixing services. For example, a VA is sent to a trusted third party who is responsible for dispersing multiple fractions of it to thousands of addresses. These fractions are passed on to other wallets. Other users do the same, and after mixing all these transactions, the VA is fetched to a single address. It is then almost impossible to trace the origin of Bitcoin to the final address, knowing that additional time-stamping processes still make it possible to play on the temporal dimension of transactions.

When it comes to the financing of terrorism, anonymity is particularly sought after by criminal organizations. Networks known for their very high level of pseudonymization make it possible to anonymize the origin of transmission control protocol (TCP) connections (on the Internet TCP-IP model). Malicious individuals can, even without great computer skills, gain access to "turnkey" cyber terrorism services. Payment for these services is often made in VAs.

Technical solutions exist to monitor the flow of VAs. They are still expensive and require dedicated teams and a certain level of expertise. Pending the large-scale dissemination of these tools and knowledge, international cooperation currently remains the cornerstone of an effective fight against the use of VAs for AML/CFT purposes.

International cooperation between all competent authorities should be as extensive as possible with regard to predicate offences, money laundering, and terrorist financing linked to VAs. The FATF recommendations call on international cooperation to be swift, constructive, and effective. FIUs and law enforcement agencies should be attentive in providing financial intelligence information and mutual legal assistance regarding investigations, prosecutions, and other legal proceedings; taking into

account freezing, confiscation, and extradition requests; and, generally, offering the widest range of cooperation through any necessary means. Due to the cross-border nature of VAs and VASPs, cooperation between supervisory authorities is particularly crucial, given the importance of identifying non-licensed or authorized VASP activity and the lack of homogenous domestic regulations.

References

5AMLD (2018). Directive (EU) 2018/843 of the European Parliament and of the Council, amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU. *Official Journal of the European Union*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843. [Accessed June 24 2021].

FATF (1990). The Forty Recommendations of the Financial Action Task Force on Money Laundering. https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%201990.pdf. [Accessed June 24 2021].

FATF (2012–2021). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. www.fatf-gafi.org/recommendations.html. [Accessed June 24 2021].

FATF (2014). Key definitions and potential AML/CFT risks. https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf. [Accessed June 24 2021].

FATF (2015). Guidance to a risk-based approach to virtual currencies. https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf. [Accessed June 24 2021].

FATF (2016–2017). Consolidated FATF Standards on Information Sharing, updated November 2017. www.fatf-gafi.org/publications/fatfrecommendations/documents/consolidated-fatf-standard-informationsharing.html. [Accessed June 24 2021].

FATF (2019). Guidance to a risk-based approach — Virtual Assets and Virtual assets service providers. https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf. [Accessed June 24 2021].

FATF (2020). Virtual Assets — Red Flag Indices of Money Laundering and Terrorist Financing, https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf. [Accessed June 24 2021].

FATF (2021). Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. www.fatf-gafi.org/publications/fatf

recommendations/documents/Updated-Guidance-RBA-VA-VASP.html. [Accessed June 24 2021].

FinCEN.gov (2015). Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger. https://www.fincen.gov/news/news-releases/fincen-fines-ripple-labs-inc-first-civil-enforcement-action-against-virtual. [Accessed June 24 2021].

FinCEN.gov (2020). Agencies Invite Comment on Proposed Rule under Bank Secrecy Act. https://www.fincen.gov/news/news-releases/agencies-invite-comment-proposed-rule-under-bank-secrecy-act. [Accessed June 24 2021].

FINMA (2019). Guidance note 02/2019. Payments on the blockchain. https://www.finma.ch/en/news/2019/08/20190826-mm-kryptogwg/. [Accessed June 24 2021].

ISO 29100 (2011). https://www.iso.org/fr/standard/45123.html.

UN Security Council (1999). Security Council Resolution 1267, Afghanistan. 15 October, S/RES/1267 (1999).

UN Security Council (2001). Security Council Resolution 1373. On threats to international peace and security caused by terrorist acts. 28 September, S/RES/1373 (2001).

https://doi.org/10.1142/9781800612839_0011

Chapter 10

Cryptocurrencies' Asset Recovery: A Multi-Dimensional Approach

Stavros Katsios and Ioannis Blatsos

Interpretations of Digital Currency

As the world is steadily being divided into real and virtual worlds, old rules governing the real world seem to be no longer relevant for both the real and virtual worlds. This seems also to be the case with the cryptocurrencies. Cryptocurrencies are rapidly expanding as people tend to use them. However, as technology and the notion of cryptocurrencies are advancing, several legal challenges surface. Through our contribution, we attempt to approach the sensitive and quite complex theme of cryptocurrencies' asset recovery. Before moving further, we have to confront a complex and ambidextrous set of questions: Do cryptocurrencies fall in the category of money? Are they considered as an asset? Are they considered as property? The answer to each of these questions will signal the relevant asset recovery procedures and methods to be adopted.

According to many theoreticians and researchers, money plays three roles in every economy: (1) a store of value, (2) a medium of exchange, and (3) a unit of account. To determine whether digital currencies can be classified as money, we must examine if and to what extend they fulfil these three different functions (Gebra and Rubio, 2019). According to Ali *et al*. (2014) and Yermack (2013) for example, anyone with access to a computer or device with Internet connectivity may use digital currencies

as money. However, as Gebra and Rubio (2019) point out, in practice, this feature is only used to a limited degree and by a small number of people, and always concurrently with the users' traditional currencies. Digital currencies may be viewed as speculative investments similar to the late-1990s Internet stocks (Gebra and Rubio, 2019).

> The definition of virtual currencies under the 5th EU Anti-Money Laundering Directive (AMLD5) is the following: "a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency, and does not possess a legal status of currency or money, but is accepted by natural or legal persons, as a means of exchange, and which can be transferred, stored and traded electronically."

Further according to Houben and Snyers (2018), every cryptocurrency is (1) a digital representation of value; (2) decentralized, i.e., not issued or guaranteed by a central bank or a public authority; (3) not attached to a legally established currency; (4) not possessing the legal status of currency or money; and (5) electronically transferable, storable, and tradeable.

Digital currencies as a store of value

It seems necessary to distinguish between the long and the short run to study the use of digital currencies as a store of value. For an asset to be a store of value in the long run, it is key what people expect about its future supply and demand (Gebra and Rubio, 2019). Even though supply of digital currencies is totally assured because of the algorithmic essence of its production, demand is rather uncertain. That said, public belief that digital currencies will continue being on demand is crucial for them to function as a store of value. Thus, the worth of digital currencies as a store of value over the long run is directly linked to their demand, and this relates to the users' belief on the future success of the currency (Gebra and Rubio, 2019).

However, in the short run, it is more difficult for digital currencies to convincingly serve as a store of value as they have a large volatility in exchange rates compared with traditional currencies. Managing the risk arising from this exchange volatility is a further problem that makes

digital currencies a poor short-term of value. For instance, the daily exchange rate of Bitcoin to the US dollar has almost no correlation (yet) with the dollar's exchange rates against other major currencies such as the Euro, Yen, Swiss Franc, or British Pound, as well as gold (Yermack, 2013). Bitcoin thus cannot be considered as a good tool to manage risks (Gerba and Rubio, 2019). A number of researchers point out the usefulness of digital currencies, e.g., Bitcoin, to serve as a store of value is limited by its high volatility rates; indeed advocates of digital currencies, and more specifically of Bitcoin, argue that it can serve as a good store of value because its value is expected to increase in future. However, as Baur *et al*. (2018) pinpoint, even if the predictions are correct that Bitcoin's price will rise, this is only an argument that Bitcoin is a good investment scheme — not a useful form of money.

Nevertheless, investors do tend to use algorithms (algos) to buy and sell Bitcoin in smaller chunks that will not move prices so much, a technique which evidently allows, through smart order routing and advanced algorithms, the purchase of significant sums of Bitcoins. A single large order is broken into many small pieces that are executed across multiple trading venues, achieving an average execution price, which is less than the price at which buying starts and improving the clients execution in periods of high volatility.[1]

When considering digital currency as a store of value, security is also an issue (Gebra and Rubio, 2019). Protection against theft is of paramount importance when treating currency as a store of value. Accordingly, as digital currency is not tangible, it cannot be physically hidden (e.g., under the mattress), but rather be stored in so-called "digital wallets," which actually are computer accounts susceptible to a variety of security issues (Gebra and Rubio, 2019). Security for these wallets poses an important issue in the digital currency discourse.

Digital currencies as a medium of exchange

Some theoreticians and researchers suggest that, as long as retailers agree to accept digital currency as payment, it can be used as a medium of exchange. Worldwide, retailers are increasingly willing to accept payment

[1] https://blog.coinbase.com/coinbase-is-helping-corporate-companies-diversify-with-crypto-444e8d91ebca.

in digital currencies (Gerba and Rubio, 2019). However, this does not automatically imply that the currency is used widely. According to McKinney *et al*. (2013), a digital currency must have a broad trading base to operate in order to serve as an effective medium of exchange. One main obstacle for digital currencies to be viewed as a medium of exchange, as Yermack (2013) points out especially in the case of Bitcoin, is the difficulty to obtain new Bitcoin. Furthermore, one cannot bypass the requirement of possessing digital currencies before procuring goods and services from an intermediary. So far, there are no credit cards or consumer loans denominated in digital currency and especially in Bitcoin (Yermack, 2013).

Digital currencies as a unit of account

According to Ali *et al*. (2014), there is little evidence of any digital currency being used as a unit of account. A significant difficulty for digital currencies to serve as a useful unit of account is their extreme volatility in exchange rates. For example, the value of a Bitcoin, compared to other currencies, changes significantly on a day-to-day basis and thus retailers must recalculate prices very frequently, something that it may be costly and confusing (Gebra and Rubio, 2019). As a result, the unpredictability of the market value of digital currencies makes them difficult to use as a valid reference point for setting consumer prices. Another factor complicating the adoption of digital currencies as units of account is the fact that most merchants quote prices in four or more decimal places (Gebra and Rubio, 2019). While this should not present a problem in mathematical terms, these decimal points can be confusing for consumers (Gebra and Rubio, 2019).

Is digital currency money?

Digital currencies appear to hardly fulfill the criteria for money functions. Thus, digital currencies do not really appear to function as "money" and pose some significant risks if they are to be used extensively in the long-term (Gebra and Rubio, 2019). In the meantime, it is highly unlikely that digital currencies in their current form will be the main form of money for the economic system (Gebra and Rubio, 2019). Moreover, according to Ali *et al*. (2014), the fact that people are not familiar with the technology,

applications are still not very user-friendly, and digital currencies do not offer the same type of security as deposits and are also characterized by great volatility in their exchange rates, is linked to other issues which may occur by considering them as money in broad terms.

However, as Bolt and van Oordt (2016) point out, highly inflationary currencies are not preferred by investors to serve as a store of value, while at the same time speculative motives appear to be one of the main reasons for someone to hold a virtual currency. The usefulness of digital currencies, and more specific of Bitcoin, as a means of exchange is being undermined by its high value fluctuation and proves to be a poor store of value (Carstens, 2021). In addition, digital currencies lack other economic monetary features. For example, digital currencies cannot be kept as deposits in the bank; they typically form part of "digital wallets," exposed to many risks and costs, without the standard insurance as in the case of deposits (Gerba and Rubio, 2019). Moreover, digital currency cannot serve as a loan or mortgage account unit or be denominated for credit or credit cards (Gebra and Rubio, 2019; Yermack, 2013). Having said that, digital currencies are not a claim, and can thus be regarded as a commodity, rather than conventional money; however, they are intangible, not as gold or other similar commodities for instance (Gerba and Rubio, 2019).

As aforementioned, the usefulness of digital currencies is mainly dependent on the user acceptance. Although the absence of a Central Bank's liability does not appear as an obstacle for digital currencies to function as money, they do differ significantly from cash and notes (Gebra and Rubio, 2019; Ali *et al*., 2014). Indeed, in some ways, digital currencies show similarities to earlier forms of money; despite the recent e-Yuan project by YuanPay Group in partnership with the Central Bank of China, till now central banks do not govern their supply, and payments are made in a direct way, without any intermediary. In Australia for example, the Australian Parliament's Senate Economic References Committee suggested that digital currencies should be treated as money for the purposes of the goods and services tax, and particularly in order for a double taxation effect to be avoided (The Law Library of Congress, 2018). According to PWC (2019), if someone holds one unit of a digital currency, a contractual right or obligation to receive cash or another financial asset is neither given nor does the digital currency come into existence as a result of a contractual relationship. Consequently, as PWC (2019) points out, digital currencies fail to be defined as a financial instrument.

Can digital currencies be considered as assets?

According to EFRAG (2020), crypto-assets can be considered as assets under the IASB's revised *Conceptual Framework for Financial Reporting* broad definition of assets. The definition of assets based on this Conceptual Framework considers an asset as "a resource controlled by the entity as a result of past events and from which future economic benefits are expected." This definition is also in line with the definition of intangible assets from IFRS (IAS 38). Based on the above definitions, crypto-assets are to be considered as assets because of the following:

(1) *They are a present economic resource* (i.e., a right or access to future economic benefits): Crypto-assets represent the created, transferred, and stored digital value or contract rights of some kind on distributed ledger technology (DLT) network. They offer potential economic advantages to their owners, because some crypto-assets can have currency-like economic characteristics (e.g., they can be used as means of exchange), while others can have investment value, and others can have financial advantages linked to network configuration or network consumption goods or services (EFRAG, 2020).
(2) *Future economic benefits are expected from them*: The economic value of different tokens can reflect: their perceived value as a by-product of the dynamics of supply and demand; or their intrinsic value, which reflects current or future cash flow generation ability; or their expected economic usefulness by participating or consuming network goods or series. Crypto-assets, in other words, hold both a "value in exchange" and/or "value in use" (EFRAG, 2020).
(3) *They can be controlled by the holder entity*: Control is defined as the power to obtain the economic benefits generated by the asset and to restrict access of others to those benefits. The notion of economic control is defined in accordance with various IFRS standards (IFRS 15, IFRS 16, IFRS10 Consolidated Financial Statements), which also outline several control indicators. As a result, determining whether a reporting entity has economic control over an asset judgment is required. A similar situation arises in crypto-assets, where there are additional indicators of economic control, in addition to holding the private key (EFRAG, 2020). This approach is also in line with the definition of control under the IAS 38 definition regarding intangible assets. More specifically, when a crypto-asset is obtained, an entity

can obtain economic benefits, by selling it or using it as a payment method (where accepted) (AASB, 2018).

(4) *They arise from past transaction on the DLT network*: Holders of crypto-assets become holders by:
   (a) Buying them with fiat currency or exchanging with other crypto-assets;
   (b) From mining activities where miners earn block rewards of new crypto-asset units;
   (c) As compensation for goods or services; or
   (d) From airdrops and hard fork events (EFRAG, 2020).

Can digital currencies be considered as property?

Lack of legal certainty on the existence and enforceability of crypto-assets arrangements has continued to be exacerbated by the lack of a consistent legal description of crypto-assets (EFRAG, 2020). To address this issue, the LawTech Delivery Panel's UK Jurisdiction Taskforce published an authoritative "Legal Statement on crypto-assets and smart contracts" in November 2019. The argument concludes that crypto-assets are property and that smart contracts relating to them are legally binding. It rejects the viewpoint held by some stakeholders that crypto-assets are outside the law (LawTech, 2019). The LawTech panel statement (2019) appears to be based on common law, so it could be limited to the UK and other common law jurisdictions. Nonetheless, the statement's rationale could influence the evolution of legal positions on the subject in other jurisdictions too (EFRAG, 2020). According to EFRAG (2020) some of the key features that the LawTech panel statement (2019) indicates are the following:

(1) Crypto-assets have novel and distinctive attributes including the intangibility or digital representation of economic value; cryptographic authentication; use of distributed transaction ledger; decentralization; and rule by consensus;
(2) Unlike physical property, crypto-assets are neither "things in action" nor "things in motion";
(3) Other digital assets (e.g., software, digital photographs, databases) can have in-built economic value, which is based in the very information they contain or comprise and are typically applied as cash-generating assets in the normal course of business. In contrast, as

crypto-assets are merely a token to be used within the system, they do not convey anything and therefore have no intrinsic value (LawTech, 2019; EFRAG, 2020);

(4) Crypto-assets contain digital information that is distinct from digitized electronic data (e.g., electronics documents and other textual, visual, and structured data). Since the latter can be duplicated and exchanged by many people, it lacks digital scarcity. As a result, electronic information does not qualify as property from a legal standpoint because it is difficult to exert realistic control over, and assert ownership over, something that is easily shared. Crypto-assets, on the other hand, have the property of exclusivity, since each transaction generates specific data parameters that are only available to the holder, resulting in their digital scarcity (LawTech, 2019; EFRAG, 2020);

(5) The value of the crypto-asset is not in the information found in the private key, which is similar to a password. Its value rests upon the interplay of encrypted public data, private key information, and ecosystem system rules (LawTech, 2019; EFRAG, 2020).

According to Spink *et al*. (2019), several jurisdictions with common law philosophies to UK view crypto-assets as property as well. More specifically, in the case *B2C2 v Quoine*, Simon Thorley of the Singapore International Commercial Court ruled that Bitcoins could be the subject of a trust and therefore be considered property. Cryptocurrencies were found to have the "have the fundamental characteristic of intangible property as being an identifiable thing of value" and to meet all the criteria set forth by the National Provincial Bank (Spink *et al*., 2019). Furthermore, Mrs. Justice Moulder of the Commercial Court in London issued an asset preservation order over a million pounds worth of Bitcoin acquired fraudulently from the defendant in a "spear phishing attack" in the Liam David Robertson v Persons Unknown case (Spink *et al*., 2019). Coinbase, a digital currency exchange, held the Bitcoin in a digital wallet. In the specific case, although the judge did not expressly rule that Bitcoin was property, she did state that there was a significant question to be resolved about whether a proprietary claim existed (Spink *et al*., 2019).

The LawTech panel (2019) concludes that crypto-assets should be classified as property since they possess the following indicative property characteristics:

(1) *Definability or identifiability*;
(2) *Exclusivity and control*: Putting aside situations of multi-signature private keys and intermediary holders, the holder of the private key has exclusive control of the crypto-asset;
(3) *Assignability*: Crypto-assets are capable of assumption by third parties; and
(4) *Certainty or Permanence*: Crypto-assets appear to be as permanent as financial assets, which may exist only until they are, for example, cancelled, redeemed, repaid or exercised.

Scholars have also been working on a legal-oriented perspective analyzing the characteristics of crypto-assets. Chason (2019) compares Bitcoin transactions with the transfer of real estate titles. In the context of title signatures during the transfer of US-based real estate, the author draws an analogy between the "chain of title" and the characterization by founder Nakamoto of Bitcoins as a "chain of digital signatures." Chason (2019) also notes that Bitcoin's transactions have features similar to those of real estates, and more specifically, hold notions closely related to grantor names, grantee names, legal descriptions, and signatures in real property reeds. In addition, the Bitcoin system, through proof of work, consensus-based verification, replicates important institutional aspects of the real estate transaction, in particular the recording and securities insurance.

Houben and Snyers (2018) set forth a critical question: what if a cryptocurrency is a medium of exchange but also and foremost an investment vehicle? This appears to be a crucial issue, as it is evident from cryptocurrency's high volatility and numerous alerts from financial regulators and supervisors that certain cryptocurrencies are being seen as investment instruments by users, not in the least Bitcoin, which continues to have the highest market capitalization among all cryptocurrencies (Houben and Snyers, 2018).

According to the 5th Anti-Money Laundering Directive's (AMLD5) definition, cryptocurrencies are viewed as a means of exchange; however, the definition itself does not mandate that this should be cryptocurrency's sole or primary feature (Houben and Snyers, 2018). As a consequence according to Houben and Snyers (2018), it makes no difference if the cryptocurrency is solely or primarily an investment tool.

We believe that cryptocurrencies appear to be a difficult notion for asset management and recovery mechanisms as they contain several

sub-themes that should be taken into account. Moreover, whatever the view of cryptocurrencies be, the general approach for the asset management and recovery procedures for cryptocurrencies should be similar to other types of seized assets.

General Principles of Seized Asset Management

Before continuing to observe the practical approaches regarding cryptocurrencies asset recovery, it is vital to take into account some of the basic general principles of seized asset management as proposed by the Organization for European Cooperation and Development (OECD).

Transparency and integrity

The first general principle is Transparency and Integrity. Managing seized assets transparently is essential for an asset management program to be efficient and accountable. A broad spectrum of procedures can make the system more transparent and accountable, starting with careful planning and record keeping at every stage of the process. In this direction, several OECD countries have taken such actions (OECD, 2018).

The French Agency for the Recovery and Management of Seized and Confiscated Assets (AGRASC), for example, is obliged to keep a registry of all seizure and confiscation requests for assistance as well as relevant information regarding the assets, their location, and the people who own them, regardless of the asset. AGRASC must also publish seized and confiscated real properties (OECD, 2018).

The notion of the asset management system's integrity is equally important. As a general principle, the person responsible for the seizure and management of assets should be prohibited from receiving any personal financial gain or using the assets for a private gain. The financial records and the Asset Management Body should be certified in order to prevent fraud and/or mismanagement and its activities should be reviewed by external auditors annually. The asset managers and all authorities involved in the asset management process should be subject to the same safeguard.

In conclusion, the rules concerning the funding of the asset management program should be clear and specific and aim at reducing excessive external influence. Several countries have taken measures to protect them

from political interference in order to safeguard the independence of such programs. AGRASC is ultimately financed through the Agency's selling assets and seized money returns in the Loan and Consignment Fund (OECD, 2018). According to the United Nations Office for Drugs and Corruption (UNODC), a basic principle for an asset management program should be that, in the case where a decision is made to remove tainted property from its owner's possession, the measures in place to protect those priorities must be impenetrable. Reports revealing inadequate asset management or demonstrating that confiscated property is being handled in violation of a court order can severely damage the asset recovery program's reputation (UNODC, 2017).

Protection of a bona fide third party

With regards to the seizure and management of assets, bona fide third parties are persons who, although not primarily the objective of an asset recovery procedure, are still affected by them, e.g., persons residing in a house or employees of a company that is subject to an order of conviction. Asset management programs of several OECD countries are being established with an emphasis to third party's protection (OECD, 2018). According to Article 31(9) of the OECD Convention against Corruption, States have to ensure that confiscation measures do not impair the rights of bona fide third parties.

The G8 Best Practices for the Administration of Seized Assets recommends that a court should be required to amend a seizure order allowing for the release of property, subject to adequate controls, including mechanisms to inform potential bona fide third parties on seized property. This includes mechanisms that may inform them that an asset is being confiscated or seized (UNODC, 2017).

According to OECD in Belgium, if a seized asset is unique and/or highly valuable, the owner's consent shall be necessary in order to proceed with a sale (e.g., a Picasso painting). In addition, in Italy, judicial administrators who manage seized assets may, without the consent of the delegated judge, sell, destroy, or maintain the assets under their custody but may not perform extraordinary operations (OECD, 2018). There are also cases where seized assets in custody of the asset manager were to be sold but a final judicial decision overturns the initial one. In these cases, a mechanism should be put into place to ensure that the money equal to a sold item is returned to its owner quickly (OECD, 2018).

Cost management and efficiency

Cost management is a key component of an effective asset management program. Computerized systems should be used for record-keeping purposes as they can help streamline processes, improve efficiency, reduce error risks, and ultimately reduce operating costs substantially. Indeed, in many OECD countries, the Asset Management Body is entitled to sell seized assets which can only be stored at an excessively or disproportionately price. Similarly, if the storage and/or management costs outweigh the value of the asset, low-value assets should be destroyed (OECD, 2018).

Cryptocurrencies' Asset Recovery Procedures

The legal and physical procedures that prohibit the transfer, conversion, or movement of property linked to crime are referred to as the "seizure of proceeds" or "instrumentalities." Provisional measures include the terms of seizure and restraint, referring to measures used while a case is pending, whereas confiscation is the permanent deprivation of funds or other assets by court order and the transfer of ownership to the state. Provisional measures apply to assets that can or are likely to satisfy the eventual confiscation order. Applications for provisional measures must be carefully crafted to correspond to the confiscation sanction or sanctions that may be applied to restrained or seized assets. Depending on whether the confiscation regime in place is property- or value-based, it will be determined whether the appropriate assets are subject to provisional measures or not. There would, for instance, be an aim of confiscating virtual assets (VAs) in jurisdictions where a property-based confiscation order is the only available sanction of a target, which could be described as corruption or money laundering proceeds or instruments.

Seizing VAs can be more difficult than seizing tangible property due to their distinct characteristics. As a result, VA seizure and post-seizure management necessitate a high level of technical expertise, and investigators must take appropriate steps and procedures to ensure proper seizure and storage.

Identification of assets subject to provisional measures

There could be a good reason to seize an asset (i.e., VAs), if there is strong evidence that the target has derived benefit from the alleged offense,

in jurisdictions where value-based confiscation orders or substitute asset provision are available. Certain jurisdictions use additional procedural aids, like presumptions, which effectively transfer the burden of proof-of-ownership to third parties. These provisions aid in the restraint or seizure of assets that a target has sold to a third party for less than market value or in simulated legal transactions. Other jurisdictions only allow the retention of assets held by the target, by defining "held" in broad terms to include possession and other assets in the interest of the target.

As with any other type of asset, VA tracing relies mostly on specific indicators — "red flags" — that may help the criminal nature of the proceeds in question to be determined. According to UNODC (2014), these flags include the following:

- Large number of bank accounts held by the same virtual currency administrator or virtual currency exchange company apparently being used as flow-through accounts, without a business rationale for such a structure.
- Virtual currency administrator or virtual currency exchange company located in one country but holding accounts in other countries where it does not have a significant customer base (unexplained business rationale which could be suspicious).
- Back-and-forth movement of funds between bank accounts held by different virtual currency administrators or virtual currency exchange companies located in different countries.
- The volume and frequency of cash transactions conducted by the owner of a virtual currency administrator or virtual currency exchange company do not make economic sense.
- Virtual currency systems that lack appropriate registration and/or transparency or are known to be popular with notable criminal groups.

Apart from these "red flags," FATF (2020) recently published a more detailed and updated list of red flags. These indicators are sorted by categories and include the following:

- Size and frequency of transactions.
  - Structuring VA Transactions (e.g., exchange or transfer) in small accounts, or in amounts under record-keeping or reporting thresholds.

- Making multiple high-value transactions (such as within a 24-hour period, or in a staggered and regular pattern or to a newly created or previously inactive account).
- Transferring VAs immediately to multiple VA service providers (VASPs), especially to those registered or operated in another jurisdiction (having no relation to where the customer lives or conducts business and/or jurisdictions characterized by weak AML/CFT regulations).
- Depositing VAs at an exchange and often immediately (withdraw the VAs without additional exchange activity or convert VAs to multiple types of VAs or withdraw VAs from a VASP immediately to a private wallet).
- Accepting funds suspected as stolen or fraudulent.

- Transaction patterns that are irregular, unusual, or uncommon.
  - Incoming transactions from many unrelated wallets in relatively small amounts (accumulation of funds) with subsequent transfer to another wallet or full exchange for fiat currency. Such transactions by a number of related accumulating accounts may initially use VAs instead of fiat currency.
  - Conducting VA–fiat currency exchange at a potential loss (e.g., when the value of VA is fluctuating, or regardless of abnormally high commission fees as compared to industry standards, and especially when the transactions have no logical business explanation).
  - Converting a large amount of fiat currency into VAs, or a large amount of one type of VA into other types of VAs, with no logical business explanation.
- The sender or recipient suggest criminal activity.
  - Irregularities during account creation, such as creating different accounts under different names, or transactions initiated from IP addresses from sanctioned jurisdictions.
  - Irregularities during the customer due diligence process, for example, incomplete or insufficient customer information or forged identification document during onboarding.
  - Irregularities in customer profile, such as shared credentials or presence on forums associated with illegal activity.
  - Potential mule or scam victims, who are often unfamiliar with VAs technology, or available wealth not consistent with an individual's historical financial profile.

- The source of funds or wealth, related to criminal activities, such as illicit trafficking in narcotics and psychotropic substances, darknet marketplace, online gambling or fraudulent initial coin offerings (ICOs).
  - Transacting with bank-cards that are connected to known fraud, ransomware schemes or darknet marketplaces.
  - The use of one or multiple credit and/or debit cards that are linked to a VA wallet to withdraw large amounts of fiat currency (crypto to plastic), or funds for purchasing VAs are sourced from cash deposits into credit cards.
  - Deposits into an account or VAs address are significantly higher than ordinary with an unknown source of funds, followed by conversion to fiat currency, which may indicate theft of funds.
  - Lack of transparency or insufficient information on the origin and owners of the funds, such as those involving the use of shell companies or those funds placed in an ICO where personal data of investors may not be available, or incoming transactions from online payments system through credit/prepaid cards followed by instant withdrawal.
  - Bulk of a customer's source of wealth is derived from investments in VAs, ICOs, fraudulent ICOs, etc.
  - A customer's source of wealth is disproportionately drawn from VAs originating from other VA service providers that lack anti-money laundering or counter-terrorist financing controls.
- Geographical risks — criminals may take advantage of countries that have poor or no national laws in place to detect, prevent, and punish money laundering and terrorist financing regarding VAs. To comply with FATF's criteria, several countries have put in place stringent anti-money laundering and counter-terrorism financing initiatives (FATF, 2020). However, some countries have not yet completely enforced the FATF's new safeguards to counter the money laundering and terrorist financing risks presented by VAs. Criminals will take advantage of these flaws in implementation to move their illicit funds to countries with less strict regulations (FATF, 2020). The following are some indicators of this sort of activity:
  - Customer's funds originate from, or are sent to, an exchange that is not registered in the jurisdiction where either the customer or exchange is located.

- Customer utilizes a VA exchange or foreign-located money value transfer service in a high-risk jurisdiction lacking, or known to have inadequately regulated VA entities, including inadequate customer due diligence and Know Your Customer measures.

Houben and Snyers (2018) note that some cryptocurrencies, such as Dash and Monero, are currently fully anonymous, while other cryptocurrencies, such as Bitcoin and others, are pseudo-anonymous. These essentially mean that, with a large effort and complex techniques deployed, authorities can identify the identities of their users. These entirely anonymous cryptocurrencies are intended to remain obscure and beyond the scope of authorities.

Having all these indicators in mind, another approach for asset tracing is through Artificial Intelligence. Cryptocurrency-based networks differ in various ways from traditional fiat-currency networks. However, for some cryptocurrencies such as Bitcoin, the transactions are on a public ledger. In addition, the unique identities are more difficult to be identified because every person can utilize multiple transaction wallets. Blockchain-based networks will detect anomaly with different features as regards traditional financial networks. Indeed Artificial Intelligence may prove a useful tool for Law Enforcement Agencies (LEAs) to detect anomality patterns in the transaction blockchain territory and essentially will help to "follow the money."

Another useful approach to detect anomalies and illegal transactions is from utilizing third-party companies specialized in cryptocurrencies and blockchain analysis. Recently, in 2020, US law enforcement officers used a third-party cryptocurrency attribution company to analyze Bitcoin transactions executed by Silk Road. This analysis indicated several transactions to two Bitcoin addresses totaling 70,411.46 BTC (valued at approximately USD 354,000 at the time of transfer) (US Court Decision Case: 3:-20-cv-07811-VC).

Asset management considerations

Aside from determining which assets are subject to provisional action, it is important for the team involved to consider the requirements for asset management, which may be generated by the restraint or seizure proposed. Particularly, the involvement of the asset management agency

when determining that there will be a restriction or seizure (if one exists) should be considered, as the manager is in the position to give valuable advice on how assets are to be restricted or seized, as well as on specific powers and conditions the order should foresee for the asset management facilitation. The Asset Recovery Office can also offer invaluable insight. The management's early participation will permit consideration of any logistical arrangements necessary for physical asset control.

Taken the above into account, it seems necessary for assets that require management to conduct some form of cost-benefit analysis. Asset management is a risky business that, in some cases, could cost more than the value of the managed assets itself; in other words, the availability of restraint or seizure of certain means does not necessarily prejudge the positive outcome of the procedure. It is therefore advisable that assets should in principle not be seized or restricted if their likely costs of maintenance, storage, or management exceed or significantly decrease the confiscation return. Indeed, some jurisdictions have developed several guidelines and may even refuse to retain or confiscate certain types of low-value assets such as livestock; other jurisdictions may nominate a depository holder, escrow agent, or custodian for assets too risky to manage, or may allow the seizure and sale of some items.

Often, physical ownership is the only practical means of preserving assets. Prior to physical possession by an asset manager, specific measures should be put in place in order to secure the safe confiscation, storage, and transportation of the asset to the storage facilities. Notably virtual currencies/assets that are seized in some jurisdictions, like Belgium, are stored using an external, private company, pending the court's final decision.

Timing of provisional measures

One of the most challenging components of asset confiscation is the timing of provisional measures. The target can be tipped off and illegal activities can be aborted if measures are imposed too early (making it difficult to father evidence and identify other accounts, targets, or the typologies used). However, if the measures are imposed with considerable delay making the target aware of the investigation, the assets will very likely be dissipated or hidden. Interaction on both formal and informal levels

becomes crucial when provisional measures involve a foreign jurisdiction. Bad timing may lead to loss of assets and need for additional evidence. Practitioners should commence early consultations in the framework of the investigation and before overt actions against a target are being taken. They should develop a strategy that allows criminal investigation goals to be achieved in timing with the optimal time for the restraint or seizure of the assets.

Non-Conviction-Based Confiscations (NCB) seizures can also provide an opportunity for property restraint or seizure much earlier, since the power to do so does not depend on criminal charges. In many jurisdictions, the notions of "balance of probabilities" or "preponderance of the evidence" help to establish an NCB confiscation more easily — thus the evidentiary burden on the authorities to be eased (Brun *et al*., 2021).

Procedures for Seizing VAs

To seize VAs, investigators must first identify the private key of the target and then use that key to initiate a transaction that will transfer the VAs from the target's address to an address created and controlled by the investigation authorities. If a search order is executed on site, it is good practice to obtain legal power to seize all the electronic devices at the search location in advance, where evidence of a suspect's use of VAs can be obtained, and then proceed to the imaging of the devices (US Department of Justice, 2018). The investigation authorities should have in mind to use specialized third parties to review the imaged material to uncover hidden evidence, which may indicate VAs' use.

If VAs are not appropriately and promptly seized, harmful results could arise; even if investigative authorities do seize the hot or cold wallet, anyone who knows the suspect's individual key or recovery seed may access the wallet. Thus, the immediate transfer of the suspect's VAs to wallets controlled by the investigative authorities is extremely important. It is possible that if the VAs in place are not transferred immediately, the suspect or anyone with access to the private keys to continue to dispose them. In that case, this action may not be viewed as a punishable violation of the seizure because the VAs did not actually come under the absolute control of the investigation authorities and thus a proper seizure did not occur. All these processes must be well documented to retain the chain of custody.

Pre-seizure planning

According to US Marshal Service, pre-seizure planning is being defined as a process of "anticipating and making a collaborative, informed decision about what property to seize for forfeiture, how and when it is to be seized and, most importantly, whether it should be seized or targeted for forfeiture at all" (UNESCO, 2017). The generation of LEA-controlled public and private keys, referred to as a keypair, is the first step in pre-seizure preparation. VAs may be stored in both custodial and non-custodial wallets. Some jurisdictions may allow a private party to be ordered to create an "on the fly" online wallet for temporary storage.

LEAs should ensure that the VA wallet they created is secured. For example, if an online wallet is being used, it should operate on a secure server. Also, the creation of a vault provides an additional layer of security as the transactions of the wallet are subject to approval by multiple parties.

Taking control of assets

Once the proceeds or tools of crime are identified, and the pre-seizure measures have been taken, seizure proceedings may be initiated. Seizure involves taking possession, administration, or management of the seized property by the competent authorities.

There are two main categories of VA wallets: hot storage and cold storage. Hot storage includes all types of wallets such as computer, mobile, or online wallets. Cold storage, as many experts suggest, is the more secure way to store VAs because a private key that is never exposed to the Internet is required to access the wallet. Cold storage includes hardware wallets that often have the appearance of a USB stick and allow their owners to keep their virtual currency holdings offline and paper wallets, which is literally a piece of paper in which the wallet address and the private key are written down.

Generally speaking, there are two different ways for taking control of the suspects' virtual currency wallet (UNODC, 2014). The first option is that the user be compelled to provide his/her credentials associated with the wallet to investigative authority. This option has the advantage of retaining the possibility for the investigative authorities to further follow the money (transactions, etc.), but there are more disadvantages. More specifically,

- the user can refuse to provide the credentials to the investigative authorities. In this case, the jurisdiction perspective is of great importance as the availability of legal powers to compel the user to provide the credentials is mainly dependent on the state's legal system;
- the absence of guarantee that even if wallet credentials are passed on to the authorities, the offender or crime associates have not made copies that would permit such persons to recover control of the seized assets.

The second method is to try and "crack" the code, but this method has several inconsistencies. First, such an act may be against the law in several jurisdictions and thus the suspect can make an appeal. Second, it is time consuming, as it can take up to several months and be quite expensive as it includes the use of super-computer and a successful outcome cannot be guaranteed. In a recent case in US, the Justice Department came into an agreement with the suspect to turn over the password to the digital wallet, since the cryptography protecting such wallets was deemed unbreakable (Roberts, 2021).

Therefore, at the moment, the most viable way to seizure virtual currencies is to transfer the VAs to a wallet controlled by the investigative authorities using the regular transaction mechanisms, or by making a third-party seizure in the case where a VASP manages access to the wallet. It is critical for the investigative authorities to also seize every electronic device and search for sub-wallets and recovery seeds as well as to search for different ways that the codes can be saved such as in paper, in visual link/scannable QR code, etc. Regardless of the type of the wallet used, if the wallet can be recreated using a backup or recovery seed, then the wallets seized by the investigative authorities are at risk as the funds can still be transferred out. That is why it is critical to obtain not only the credentials (private key) of the suspect but also the recovery seed.

According to UNODC (2014), there are a number of steps involved in the process of transferring the virtual currencies to the wallet of the law enforcement authority. More specifically,

- determining the amount of virtual currency items, wallets, or both to be seized;
- securing suspect's cooperation or exercising control over the wallet through other means permitted by law, so that the required sum can be

transferred to a government-controlled wallet, pending liquidation upon forfeiture;
- conformation of receipt duly recorded; or
- where cooperation or control over the wallet is not viable:
  - determine the value of virtual currency to be seized in local currency based on exchange rate;
  - apply value-based recovery procedures.

Needless to say, value-based recovery can be used from the initial steps of the process, especially where direct seizure and control of virtual currency is not viable due to either security or asset management considerations.

In a decision of the Taipei Court of District in November 2019, for example, approximately 94 Bitcoins were declared to be confiscated for ransoms extorted by the defendant by sending emails threatening websites (most of them based in Mainland China or HK) with distributed denial-of-service (DDoS). As the virtual currencies in this case were never seized, the confiscation holding included a provision, stating that "if the entire or partial confiscation is impossible or not appropriate, the value thereof shall be collected from the offender," which is a verbal reprint of the provisions of Article 38-1 (3) of the Criminal Code of Taiwan (Chang, 2020). However, the date of valuation was not clear: should the value of Bitcoins be as the date of ransom payment (mainly by the end of 2016) or the judgment date (November 27, 2019)? This appears to be a meaningful point for lawmakers as the difference in the market price between these two dates may be significant.

Chain of custody

The chain of custody for VA evidence should be quite similar to that for normal evidence regarding asset seizure. As with the assets' seizure considerations, several characteristics should be considered for creating an appropriate and sound chain of custody for VAs.

Specialized Staff: Due to the specific, unique, and complex nature of VAs, specialized staff will be required to deal with specific technical features that may arise during the investigation or seizure process. The specialized staff could be from third parties too but their inclusion in the process, and therefore in the chain of custody, should be well documented and specific measures regarding confidentiality be taken.

Accuracy and Consistency of Data: The integrity of relevant seized or case-related data should be maintained. The access to these data should be restricted only to the investigators that handle the specific case, and the access and handling of these data should be always recoded and documented.

Designated Officer: A designated officer that will supervise and witness each phase during the investigation and seizure process should be appointed. More specifically, regarding VAs seizure process, a designated office should observe for example the creation of a storage wallet for the investigation authority, observe the transfer of seized cryptocurrencies to the investigation authority's wallet, observe the storage of the investigation authority's private key, as well as the storage of any confiscated electronic devices or other materials.

Jurisdictional issues

Legal issues may arise concerning the seizure of VAs in cases where there is no physical or electronic representation of them. One of the main notions here is the location of the VA wallet, private keys, and/or recovery seeds. International or mutual legal assistance (MLA) is of primary importance. Through this approach, authorities obtaining information regarding the location of the VAs may seek assistance in the tracing, freezing, or even confiscating of VAs. The main tools that need to be considered for MLA of international asset recovery are as follows:

(i) Bilateral MLA Treaties.
(ii) Council of Europe Convention on Laundering, Search, Seizure and Confiscation of Proceed from Crime and on the Financing of Terrorism (Warsaw Convention of 2005).
(iii) Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime (1990).
(iv) United Nations Convention Against Corruption (UNCAC).
(v) United Nations Convention against Transnational Organized Crime (UNTOC).
(vi) OECD Anti-Bribery Convention.
(vii) European Investigation Orders.

Post-seizure asset management

In the post-seizure asset management phase, several considerations should be taken into account. More specifically, due to the anticipated price fluctuations, and/or the desire to preserve value, authorities should decide which approach to choose: (1) no liquidation asset management, (2) liquidation of VAs, or (3) profitable management of seized VAs. Their decision has to be based on the existing legal regime of the jurisdiction avoiding customized solutions and judging upon each case separately due to its unique characteristics.

Asset management of cryptocurrencies till a final court order judgment

The first strategic option is to put a central authority to manage the seized VAs until a final court order is taken. The management of these assets should be governed by specific rules and always maintain the principle of maximizing value. The advantage of this approach is that, if the suspect is found not guilty, there will be an easy way to return the confiscated assets in the form in which they were seized and were treated according to best practices by the designated asset manager. The disadvantages of this approach have mainly to do with security and high costs of asset management. More specifically, retaining the seized assets in a wallet, for example, bear security concerns as it is susceptible to theft or hacking. As far as the high costs of asset management is concerned, a central authority should manage this portfolio in a daily basis and demands specialized personnel. In the case where a specialized private company (e.g., VASP) will be appointed as the asset manager there will presumably result a high cost for maintaining and managing the seized assets. In each of the above cases, it should be noted that the wallet can be viewed as a collateral wallet or account, meaning that the suspect does not have any power over the seized VAs until a final court order is being made.

Converting VAs immediately to fiat currency

Competent authorities can proceed with the valuation of the VAs upon seizure and sell them at market price as soon as reasonably possible

through an auction. This approach is a conservative and safe one, eliminating the risks that high price volatility of VAs holds as well as the high cost of asset management and related security risks. The amount generated from the auction should then be retained in a collateral bank account until a final court judgment is being made. However, there are several legal considerations to be considered. More specifically, if the suspect is found not guilty, he/she may seek compensation about potential profits, claiming that if the authorities did not auction his/her VAs, their value in the day of the final court judgment would be higher. That is why before a decision on auctioning is taken, an agreement with the suspect about the sale of the VAs is essential.

An example of cryptocurrencies' auctions comes from the US Marshals Service.[2] The agency controls several digital currencies wallets from seized cryptocurrencies, representing some of the biggest wallets in the world. For several years, US Marshals Service conducts auctions regarding mainly Bitcoins. These auctions involve multiple blocks of several thousand Bitcoins, which fetch the federal government millions of dollars.

Profitable management of seized VAs

Competent authorities may choose to convert VAs to stable-coins, which are characterized by a low volatility in their stock prices as they correspond to national currencies, such as being fully backed by the Euro or Dollar or implementing so-called "smart contract"-based derivatives. VAs, including these low-volatility stable-coins, can be used to generate additional income for the authorities through non-custodial decentralized finance protocols. These protocols can automatically use seized funds to generate a return. Sometimes their use is for automated loans that return a significant interest, over 8% per annum in most cases. Other use cases will allow authorities and their seized VAs to provide liquidity to automated market makers and collect a part of the transaction fees.

With proper management and Operational Security (OpSec) standards, the value of seized assets can provide a much needed second income stream for LEAs without risking compensating the owner of these funds in case courts look in his favor.

[2]https://www.usmarshals.gov/assets/2020/febbitcoinauction.

Valuation

A designated asset management authority should take VAs into possession as soon as feasible. In some cases, it may even be advisable for these authorities to take part in executing the seizure. After taking possession of the VAs, the specialized asset manager should create a record for the valuation of the assets. Each valuation should be recorded and sourced.

Possible VA forks may occur during the asset management phase, something that an asset manager should be aware of. Hard fork coin splits are created through changes of the blockchain rules and share a transaction history with cryptocurrency up to the time of the split. The asset manager should claim and bring under control the new coins that may arise from a hard fork split. A hard fork example occurred in August 2017, when Bitcoin split into two cryptocurrencies, which led to the creation of Bitcoin Cash (BCH) (US Case: 3:20-cv-07811-VC). Through this split, a Bitcoin address, which had a Bitcoin balance, will retain the same balance both on the Bitcoin blockchain and on the Bitcoin Cash blockchain.

Inventory

The asset manager should keep inventory of the seized VAs and maintain detailed records of the assets and any transactions involving them. The records should contain any detail related to the seized VAs, as in the case of every other seized asset, including but not limited to the date of seizure, the amount and type of VAs, the seizing agency, and every other detail that seems appropriate. It is essential that every other electronic device that was related and seized to be supplemented with photographs and video recordings that show the condition of the asset at the time of seizure (Brun *et al*., 2021). Reports should be made containing all the above details as well as the valuation of the seized assets and be forwarded to the applicant for the restraining order (Brun *et al*., 2021). A reporting component may increase the transparency of the asset manager's activities and raise awareness among the public about the purpose and the achievements of the asset management authority (Brun *et al*., 2021).

Security

A designated employee should keep a list of passwords for each confiscated electronic device and recover seeds, private, and public keys.

All these can be securely stored in text files in an external storage device. Each external storage device containing passwords, private keys, and VA wallet addresses should be kept offline in a secure location. As far as the private keys are concerned, the loss of the secret key equates to the loss of the resource or asset as well. According to ENISA (2021), there are four different methodologies that can be used in order to protect the storage of such keys:

Hardware Security Module: The standard way of securing cryptographic keys in large organizations such as banks is to use a Hardware Security Module (HSM). These are special-purpose computers that are dedicated to cryptographic operations and have undergone a stringent certification process (ENISA, 2021).

Since they are relatively costly, they are best suited for large corporate use; indeed, most financial institutions already have a large HSM footprint in-house (ENISA, 2021).

Multi-Sig: A multi-sig is a technique that connects a set of public keys to each asset (ENISA, 2021). Each private key is assigned to a particular entity and a structure of access is defined. If a transaction relating to this asset is to be carried out, something similar to an intelligent contract will be performed. The asset is only operated on if sufficient digital signatures meet the access structure criteria (ENISA, 2021).

Secret Sharing: The use of secret sharing is a classic means of saving secrets, so that recovery in case of losing/damaging a computer is possible as well as for avoiding theft (ENISA, 2021). With this procedure, the keyholder divides its key in n shares by using a threshold secret sharing scheme with threshold t. The n different shares are then stored in n different places (ENISA, 2021).

Multi-Party Computation: By using MPC/Threshold Cryptography, the issue of having to carry the shares in a secret sharing-based solution into one location to generate a signature may be resolved (ENISA, 2021). This technology allows the signing process to be completed without the need to rejoin the shares. This allows a standard digital signature to be created, with the signer's preferred access structure (ENISA, 2021).

Disposal

At the disposal phase, confiscation laws frequently require that confiscated assets and, in this case, VAs, be sold directly (e.g., to an exchange platform) or liquidated through a public auction, as discussed previous, but always in such a way as their value to be maximized (Brun *et al*., 2021). The funds generated from the disposal of the seized VAs should be transferred to asset confiscation funds that numerous jurisdictions have established. The proceeds of the sale of VAs should be used, as with any other type of confiscated asset, for designated law enforcement and confiscation programs as well as for a potentially restitution to victims (Greenberg *et al*., 2009; World Bank, 2009). There are also cases where suspects enter into an agreement with the authorities to buy back their VAs and, in some other cases, they agree to the conversion of the VAs to fiat currency on behalf of them by the authorities.

Final Thoughts/Conclusions

Although cryptocurrencies are not characterized by a solid performance in terms of a constant purchasing power, they are here to stay and are expected to establish their role as a new form of money in years to come. That said, improved governance of global resources need not imply formal governmental legislation or regulation. As Blockchain technology evolves, so do the threats of using it for illicit purposes. In the salient, complex and in general lawlessness nature of blockchain technology, cryptocurrencies' asset recovery should follow the path of established and well-tested procedures for other assets but functioning in tandem with business and technology development, avoiding the neutralization effect of a prolonged questioning of the nature of cryptocurrencies. Cryptocurrencies' asset recovery procedures are complex, highly sophisticated, and do not always bear the desirable outcome. Nevertheless current asset forfeiture systems need to get adapted to developing technological change; understanding the technology we may understand also the implications of VAs. Keeping that in mind, future research should pursue issues like standardization and common accepted practices for data exchange especially regarding best practices for cryptocurrencies' asset recovery mechanisms.

References

AASB — Australia Accounting Standards Board (2018). Digital currency — A case for standard setting activity. A perspective by the Australian Accounting Standards Board (AASB). https://www.ifrs.org/content/dam/ifrs/meetings/2018/may/eeg/ap2d-digital-currencies-paper.pdf. [Accessed 1 February 2021].

Ali, R., Barrdear, J., Clews, R. and Southgate, J. (2014). The economics of digital currencies. *Bank of England Quarterly Bulletin*, 2014 Q3.

Baur, D. G., Hong, K. and Lee, A. D. (2018). Bitcoin: Medium of exchange or speculative assets? *Journal of International Financial Markets, Institutions and Money*, 54(C), 177–189.

Bolt, W. and van Oordt, M. (2016). On the value of virtual currencies. www.bankofcanada.ca › uploads › 2016/08 › swp2016-42. [Accessed 5 February 2021].

Brun, J.-P., Sotiropoulou, A., Gray, L., Scott, C. and Stephenson, K. (eds.) (2020). Asset Recovery Handbook: A Guide for Practitioners, Second Edition. Washington, DC: World Bank, StAR Initiative.

Carstens, A. (2021) Digital currencies and the future of the monetary system. https://www.bis.org/speeches/sp210127.pdf. [Accessed 3 February 2021].

Chang, T.-Y. (n.d.). Taiwan: How are virtual currencies seized, confiscated and auctioned in Taiwan? https://www.mondaq.com/fin-tech/882628/how-are-virtual-currencies-seized-confiscated-and-auctioned-in-taiwan. [Accessed 3 February 2021].

Chason, E. D. (2019). How Bitcoin functions as property law. *Seton Hall Law Review*, 49(1), Article 3.

EFRAG — European Financial Reporting Advisory Group (2020). Discussion paper accounting for crypto-assets (liabilities): Holder and issuer perspective. https://www.efrag.org/News/Project-430/EFRAGs-Discussion-Paper-on-the-accounting-for-crypto-assets-liabilities---holder-and-issuer-perspective. [Accessed 5 February 2021].

ENISA — European Union Agency for Cybersecurity (2021). Crypto assets: An introduction to digital currencies and distributed ledger technologies. https://www.enisa.europa.eu/publications/crypto-assets-introduction-to-digital-currencies-and-distributed-ledger-technologies. [Accessed 05 February 2021].

FATF — Financial Action Task Force (2020). *Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets*. Paris: FATF.

Gebra, E. and Rubio, M. (2019) *Virtual Money: How Much Do Cryptocurrencies Alter the Fundamental Functions of Money?* Luxembourg: European Parliament, Policy Department for Economic, Scientific and Quality of Life Policies.

Greenberg, T. S., Samuel, L. M., Grant, W. and Gray, L. (2009). *Stolen Asset Recovery: A Good Practices Guide for Non-Conviction Based Asset Forfeiture*. https://star.worldbank.org/sites/star/files/Non%20Conviction%20Based%20Asset%20Forfeiture.pdf. [Accessed 5 February 2021].

Houben, R. and Snyers, A. (2018). *Cryptocurrencies and Blockchain: Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion*. Brussels: European Parliament, Directorate-General for Internal Polices.

LawTech Delivery Panel (2019). Legal statement on cryptoassets and smart contracts — UK Jurisdiction Taskforce. https://technation.io/about-us/lawtech-panel. [Accessed 10 February 2021].

McKinney, R. E., Shao, L. P., Shao, D. H. and Rosenlieb, D. C. (2013). The reality of digital currency as a financial medium of exchange. *Journal of International Finance Studies*, 13(3), 45–50.

OECD — Organisation for Economic Co-operation and Development (2018). *Assessment and Review of Asset Recovery Institutional Arrangements in Greece*. https://search.oecd.org/daf/anti-bribery/OECD-Greece-Asset-Recovery-Institutional-Analysis-ENG.pdf. [Accessed 10 February 2021].

PWC — PricewaterhouseCoopers (2019). In depth — A look at current financial reporting issues — Cryptographic assets and related transactions: Accounting considerations under IFRS. https://www.pwc.com/gx/en/audit-services/ifrs/publications/ifrs-16/cryptographic-assets-related-transactions-accounting-considerations-ifrs-pwc-in-depth.pdf. [Accessed 10 February 2021].

Roberts, J. J. (January 22, 2021). Criminals drop bitcoin for other cryptocurrencies. *Forbes*. http://fortune.com/2018/01/22/bitcoin-monero-cryptocurrency-crime/. [Accessed 12 February 2021].

Spink, A. Q. C., Butler, S. and Bell, C. (2019). CryptoAssets and Smart Contracts — The UKJT Legal Statement. https://www.outertemple.com/wp-content/uploads/2019/11/Crypto-Paper-ASQC-SB-and-CBE-FINAL-VERSION.pdf. [Accessed 11 February 2021].

The Law Library of Congress (2018). Regulation of cryptocurrency in selected jurisdictions. https://www.loc.gov/law/help/cryptocurrency/regulation-of-cryptocurrency.pdf. [Accessed 11 February 2021].

UNODC — United Nations Office on Drugs and Crime (2014). Basic manual on the detection and investigation of the laundering of crime proceeds using virtual currencies. https://www.imolin.org/pdf/imolin/FULL10-UNODCVirtualCurrencies_final.pdf. [Accessed 14 February 2021].

UNODC — United Nations Office on Drugs and Crime (2017). Effective management and disposal of seized and confiscated assets. https://www.unodc.org/documents/corruption/Publications/2017/17-07000_ebook_sr.pdf. [Accessed 12 February 2021].

US Court Decision Case: 3:-20-cv-07811-VC (2020). https://www.justice.gov/usao-ndca/press-release/file/1334771/download. [Accessed 12 February 2021].

US Department of Justice (2018). Report of the Attorney General's Cyber Digital Task Force. https://justice.gov/cyberreport. [Accessed 5 February 2021].

World Bank (2009). Stolen Asset Recovery; Management of Returned Assets: Policy Considerations. https://star.worldbank.org/sites/star/files/Management ReturnedAssets.pdf. [Accessed 12 February 2021].

Yermack, D. (2013). Is Bitcoin a real currency? An economic appraisal. NBER Working Paper No. 19747.

https://doi.org/10.1142/9781800612839_0012

Chapter 11

Prosecuting Transnational Cybercrimes: From Territorial Sovereignty to New Jurisdiction — The Swiss Experience

Ludovic Tirelli

Cyber Money Laundering: An Introduction

This chapter focuses on the procedural tools available to the prosecuting authorities to investigate, prosecute, and judge cybercrimes, which of course include cyber money laundering. At the outset, it should be noted that cyber money laundering can be defined as the use of computers and information and communication technologies (ICT) to commit an act that hinders the identification of the origin, discovery, or confiscation of assets derived from a crime. Thus defined, cyber money laundering can be criminalized both by means of the usual provisions for the repression of money laundering (in Switzerland, Article 305bis of the Swiss Criminal Code (SCC)) and by means of computer-related offences which, depending on the form that the cyber money laundering takes, may alternatively fall under the heading of data theft (Article 143 SCC), unauthorized access to a computer system (Article 143bis SCC), deterioration of data (Article 144bis SCC), or the fraudulent use of a computer (Article 147 SCC). When these latter offences, typically related to cybercrime, are involved, the prosecution issues raised by cyber money laundering will be exactly the same as those raised by the prosecution of other cybercrimes. In particular, the investigation and prosecution of cyber money laundering

cases will face the same jurisdictional hurdles as those faced by prosecuting authorities for other cybercrimes. For this reason, this chapter will consider the terms cyber money laundering and cybercrimes as synonymous.

The Rise of Cybercrime: A Historical Perspective

State sovereignty is intrinsically linked to the effectiveness of criminal justice. As a result of this sovereignty, criminal justice authorities have jurisdiction, under Swiss law, when the perpetrators are present on the Swiss territory and when the evidence is at their disposal. Therefore, the State's action is not free when the accused is not in Switzerland or when evidence is located in the territory of another State due to foreign sovereignty (Zimmermann, 2019; Yar and Steinmetz, 2006). Indeed, both international and national law (Article 299 SCC) cracks down any person who violates the territorial sovereignty of a foreign State without its consent or without a treaty supporting it. To overcome those difficulties, States assist each other in criminal liability, according to the rules they define (Zimmermann, 2009).

In the early days, mutual assistance was granted only in extradition cases. During the 20th century, States started to face international criminal phenomena such as arms trafficking, money laundering, corruption, and terrorism, therefore urging the necessity of bilateral cooperation treaties. Therefore, States have first concluded bilateral treaties in the field of extradition, but then extended them to mutual assistance matters (Zimmermann, 2009).

Nonetheless, the globalization of the world economy has led to the need for strengthening relations between countries. Furthermore, intensification of financial flows, increased mobility of capital, development of extremely rapid and sophisticated means of communication, and the invention of the Internet in the 1960s led to the emergence of economic networks *across borders* and not anymore only at a national level (Zimmermann, 2009; Yar and Steinmetz, 2006). The States had no other choice but to come to the conclusion that effective criminal liability can only take place on a large scale. The high number of treaties concluded at that time indeed testifies to this collective awareness (Zimmermann, 2009).

In addition to the social, economic, and cultural consequences of the Internet, new threats and dangers arose. Cyberspace offered a vast range of new opportunities for criminals (Council of Europe, 2021a;

Luis Cordova *et al*., 2017; Yar and Steinmetz, 2006; Sviatun *et al*., 2021). In the mid-1990s, the commercialization of the Internet expanded in an exponential way. While in 1993, only 83 countries were connected to the Internet, between 1994 and 1999, 143 countries became connected, totaling 226 countries (Yar and Steinmetz, 2006). About 16 million Internet users worldwide were counted in December 1995, which rose to 580 million in May 2002 (Yar and Steinmetz, 2006). In 2019, 4.1 billion people were using the Internet, representing 53.6% of the world's population (Statista Infographies, n.d.).

Criminals, as well as criminal organizations, quickly realized that these ICTs would offer them the possibility of drastically reducing the costs of committing crimes and, above all, increasing the number of potential victims and thus obtaining greater profits. Furthermore, because of cyberspace, criminals and victims may well be physically situated in different countries and even in different continents. Cybercrime can then no longer be thought of in a national context, but has to be considered beyond the borders (Zimmermann, 2009; Majid Yar and Steinmetz, 2006; Shan-A-Khuda and Schreuders, 2019).

Moreover, the Internet allows criminals to commit crimes while remaining anonymous or by reinventing a social identity far away from their real world identities (Zimmermann, 2009; Yar and Steinmetz, 2006; Shan-A-Khuda and Schreuders, 2019). This is one of the major challenges for prosecution, as criminal justice is aimed at punishing criminal individuals that must therefore be identified. The ICTs and the new forms of criminality, cybercrimes in particular, unquestionably led the States to face new challenges for individual and collective safety, social order and stability, economic prosperity, and political liberty (Zimmermann, 2009; Yar and Steinmetz, 2006). While criminals have adapted quickly to these ICTs, the law has struggled to do the same (Müller, 2012; Yar and Steinmetz, 2006). The rapid growth of cybercrime requires the development of effective mechanisms in order to prevent such crime (Sviatun *et al*., 2021).

The Challenges of Cybercrime and Cybercrime Investigations

National sovereignty is synonymous with autonomy and self-determination. A country is therefore sovereign within its borders and not beyond.

Thus, the national sovereignty of a State is strongly protected by various mechanisms. As such, it is considered a violation of the sovereignty of Switzerland when a state unlawfully extends its jurisdiction over the Swiss territory. In this regard, international law prohibits a foreign authority from applying foreign law within Switzerland's borders (e.g., by directly ordering, in the context of foreign proceedings, the collection of evidence contained in documents located in Switzerland). The same applies for Swiss criminal justice authorities wishing to investigate abroad. Violations of national sovereignty are therefore criminalized under Swiss criminal law not only when Swiss territory is violated (Art. 271 SCC: *Unlawful activities on behalf of a foreign state*) but also when Swiss officials violate a foreign State territory (Article 299 SCC: *Violation of foreign territorial sovereignty*). Only mechanisms provided for under international law can authorize a foreign authority to proceed so.

Criminal liability is the supreme power of a State over its territory. It is in this sense that the criminal law is conceived. As mentioned in the above, traditional criminal laws focus their legal scope of action on physical objects *over a territory* (Confédération suisse, 2013). But the main problem States are now facing is that with the rise of the ICTs, cybercrimes occur beyond the borders and fully disregard them. Thus, the perpetrator can easily be, and usually is, in another State, and therefore jurisdiction, from the one where the result of the crime occurs, the evidence being often stored on servers located in foreign jurisdictions (or even worse, in the cloud). Within cyberspace, geographical borders disappear as well as the traditional principle of territoriality (Luis Cordova *et al*., 2017; Sviatun *et al*., 2021).

Legal systems as historically conceived are facing many challenges. As such, we can mention the fact that cybercrimes are different from the crimes we were used to in terms of objects. Indeed, the object of cybercrimes is not a material one but immaterial, which considerably complicates the tasks of the prosecuting bodies (Luis Cordova *et al*., 2017; Sviatun *et al*., 2021), which are not used to this kind of work. As a consequence, the collection and use of evidence has now reached a higher level of difficulty. In cyber investigations, it is necessary to have qualified, well-trained personnel with strong computer skills, which is not necessarily the case with physical evidence. Therefore, the states need to invest in this new kind of training and education because of the constant evolution in this sector (Luis Cordova *et al*., 2017). Indeed, this very specific knowledge is often unfamiliar to criminal justice.

The evidence itself in relation to cybercrime requires specific attention. In the cybercrime-related investigations, evidence is extremely volatile and easily editable, in addition to being stored on servers located in various jurisdictions. Evidence can disappear, be removed, be altered, as well as be moved to another country in a matter of seconds. Swiss authorities are used to gathering physical evidence from a physical crime scene, but in cybercrime investigations, physical evidence does not exist because it is in the so-called cyberspace (Council of Europe, 2021a; Luis Cordova *et al*., 2017).

Furthermore, 144,910,000 million new forms of malicious software (AV-Test) appeared in 2019, and in April 2020, 38,48 million new samples were detected. While our traditional legal systems require time to be effective, cybercrimes necessitates an urgent, dynamic, and integrated response (Sviatun *et al*., 2021).

The multitude of legal frameworks at the national and international levels must also be considered. Indeed, not all States criminalize the same behaviors. For example, when it comes to pornography, some States allow the production and distribution of all types of content, while others prohibit pornography when children are involved, and still others prohibit all types of pornography. Thus, behaviors that are criminalized in one country are not necessarily repressed in another (Luis Cordova *et al*., 2017).

In view of the above, cybercrime is without a doubt a global phenomenon, therefore requiring an international framework of repression. Access to data, data loss, loss of data location, problems related to various national legal frameworks, obstacles to international cooperation, and problems of public and private partnership are some of the problems that the states are facing in regard to the principles of state sovereignty. The states thus have to improve their legal mechanisms to be able to respond to cybercrimes (Luis Cordova *et al*., 2017; Sviatun *et al*., 2021). Indeed, even today, only a small proportion of cybercrimes are reported to the criminal prosecution bodies and leads to court decisions, while most of the time victims do not obtain justice (Council of Europe, 2021a). The 2001 Convention on Cybercrime was meant to solve all of the above challenges.

The Convention on Cybercrime

The 2001 Convention on Cybercrime (also known as The Budapest Convention) is one of the most efficient resources in the international

framework to fight against cybercrimes, not only because of its content and international cooperation mechanisms but also because of the number of the States that are party to it. As for June 2021, no less than 66 States were members of the Convention on Cybercrime (Council of Europe, 2021b).

Aware of the need for an international framework, the Council of Europe, as well as Canada, Japan, South Africa, and the US participated in the negotiation of this Convention on Cybercrime. Those countries wanted to ensure to the Member States of the trust on an efficient cooperation between them to contain cybercrimes authors (Council of Europe, 2021b). The Cybercrime Convention is divided into two main parts. The first part is related to the measures to be taken by the States at national level (Chapter II), be it related to substantive law (Section 1), procedural law (Section 2), or jurisdiction (Section 3). The second major part of the convention focuses on international cooperation (Chapter III) and is divided into a Section 1 related to the general principles of international mutual cooperation (Extradition and Mutual Legal Assistance) and a Section 2 focusing on specific provisions in cybercrime matters.

Section 1 of Chapter II has to be highlighted as it describes the "cybercrimes" and elements of those crimes that each Signatory State commits to criminalize under its national legal system, thus trying to reach harmonization and common language in relation to what behavior need to be criminalized on an international level. The behaviors criminalized under this section are limited to illegal access (Article 2 CCC), illegal interception (Article 3 CCC), data interference (Article 4 CCC), system interference (Article 5 CCC), misuse of devices (Article 6 CCC), computer-related forgery (Article 7 CCC), computer-related fraud (Article 8 CCC), offences related to child pornography (Article 10 CCC) and offences related to copyright or related-rights (Article 11 CCC). Cyber laundering is not criminalized *per se* under the Cybercrime Convention.

In relation to international cooperation, the Section 2 of Chapter III deserves specific attention as it provides "exotic" measures of action from the traditional mutual legal assistance perspective that enable law enforcement agencies of a Member State to act in the jurisdiction of another member without going through the whole mutual legal assistance process. As an example, we can refer to Article 32 CCC related to *trans-border access to stored computer data with consent or where publicly available*. In this regard, another major achievement of the Convention

on Cybercrime is that it establishes the basis for cooperation between private companies and States (Sviatun *et al*., 2021).

It is also important to highlight Article 18 CCC. Thus, one of the most valuable assets that prosecution bodies need to investigate cybercrimes is any type of data that might help to identify the perpetrators and break the usual anonymity shield associated with the use of ICTs. Therefore, under Article 18 CCC, each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order the following: (1) a person in its territory to submit specified computer data in that person's possession or control, which are stored in a computer system or a computer-data storage medium; and (2) a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. We will later see how the terms "possession" or "control" have been interpreted by national courts, specifically in Switzerland.

Despite this Convention, the number of cybercrimes continues to rise. In 2018, 77.2% of the surveyed companies were victims of cybercriminals, while in 2020, that number has increased to 80.7%. This growth thus easily demonstrates that the existing mechanisms are not effective enough or widely outdated as cybercrimes are being updated faster than the prevailing mechanisms aimed at fighting them (Sviatun *et al*., 2021).

Therefore, States have considered various options to provide greater effectiveness to the existing anti-cybercrime legislation. One of the most valid solutions is a draft second protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence.

The Swiss Perspective

Switzerland has always had a restrictive policy on jurisdiction. This derives from (1) material provisions of the SCC as well as (2) a recent case law in relation with ICT investigations.

Article 299 SCC: Violation of foreign territorial sovereignty

Under Swiss law, Article 299 of the SCC is particularly interesting in terms of jurisdictional issues, as its analysis reveals both the limits and possibilities of action for Swiss prosecuting authorities when investigating abroad.

Article 299 of the Criminal Code therefore criminalizes anyone who performs official acts on the territory of a foreign State without authorization. In relation to this crime, a question that regularly arises is what is meant by "without authorization." For the authors as well as the Swiss Supreme Court, official acts are done without authorization when they do not comply with international law, or intervene without the prior consent of the State concerned, or are considered by the foreign State to be of such a nature as to prejudice its sovereignty, or do not comply with the applicable domestic legislation (Bottinelli, 2017). On the other hand, the consent of the person affected by the official act does not have the effect of rendering lawful the conduct of Swiss authorities acting on foreign territory (Bottinelli, 2017). It will therefore always be necessary to ensure that Swiss investigators can rely on either a treaty, a convention, or the prior consent of the State concerned. Furthermore, investigative acts must always be in accordance with foreign national law (Bottinelli, 2017).

In particular, with regard to investigative acts related to computer evidence, it is accepted that there is no violation of foreign sovereignty when the Swiss prosecution authorities merely intercept evidence which, although not destined for Switzerland, transits its territory or through Swiss airspace or reaches Switzerland (Bottinelli, 2017). This principle thus allows Switzerland to intercept telecommunications from a monitored connection, whether abroad or in Switzerland, solely on the basis that the communication is transiting through Switzerland (Bottinelli, 2017). However, the situation is radically different when the authority proceeds to secretly tap conversations that take place in a vehicle that is certainly registered in Switzerland but that is going to drive abroad. The Swiss Supreme Court recently confirmed on two occasions that, in such a situation, the tapping could only be based on international conventions, or even on the prior agreement of the foreign State on whose territory the secret tapping is carried out (ATF 146 IV 36). Failure to do so makes the evidence inadmissible under Article 141 of the Swiss Criminal Procedure code (SCPC), as well as all derived evidence based on the well-known theory of the "fruit of the poisonous tree."

Swiss case law in ICTs and cybercrime-related investigations

In Switzerland, as elsewhere, the prosecuting authorities were soon confronted with jurisdictional problems related to cyber investigations.

It is not insignificant to point out that this has concerned both classic cybercrimes, in which the perpetrator acts from abroad, and strictly national crime, in which networks and ICT were used to commit common crimes. In both these types of cases, the needs of the investigation made it necessary to obtain addressing resources to find out who was hiding behind a user profile, a pseudonym, an e-mail address, or an IP address. But in most cases, the data relevant to the investigation were located on servers in foreign jurisdictions. Therefore, prosecution authorities have systematically encountered jurisdictional problems and tried to be creative with jurisdiction, most of the time unsuccessfully as the following cases show.

With regard to the questions raised by the access of Swiss prosecuting authorities to data on servers located abroad, the Convention on Cybercrime has often been used as an international treaty allowing States Parties to access data located on the territory of other States Parties without infringing their sovereignty. Indeed, by means of such conventions, the States concerned agree to give up some of their sovereignty in favor of a more effective fight against cybercrime.

As previously seen, this configuration is expressly provided for in Article 32 CCC. Thus, such direct access to data located in the territory of another State Party does not infringe the sovereignty of the latter if the data are either "freely accessible" or if its transmission is made with the legal and voluntary consent of the person legally authorized to disclose such data. The first category, which concerns data freely accessible on the Web in particular, does not pose any problem. The second category, on the other hand, has given rise to more discussion and is the lowest common denominator on which the States Parties to the Convention on Cybercrime have been able to agree without going too far in relation to the loss of sovereignty (Bottinelli, 2017). For a long time, Switzerland defended a restrictive interpretation of the hypothesis provided for in Article 32 lit b CCC, in the sense that the communication could only take place if the legally authorized person had, in the State conducting the criminal proceedings, given his or her consent and that in doing so, he or she did not infringe on the protected secret domain of a third party (Bottinelli, 2017). The particularly restrictive scope of this interpretation is clear, which ultimately allowed the prosecuting authority to obtain information (e-mails, social network account data, etc.) from service providers only if the owner of these services, often the defendant, had given his consent, which was rarely the case.

However, in a recent decision, the Federal Court considered that such an interpretation had no basis in the preparatory work of the Convention and even contradicted the purpose of the Convention (Bottinelli, 2017). Thus, the Federal Court considered the legal consent provided for in Article 32 lit b CCC could also be given by the person or entity which, abroad, held the data in question on the basis of the legal provisions applicable in the State where it is located. The Federal Supreme Court considered the consent requirement of Article 32 lit b CCC already placed narrow limits on the scope of cross-border access to stored data (cf. c. 5.10–5.11). In the view of the Federal Supreme Court, by adopting Article 32 CCC, the parties had reached a common minimum consensus providing for cross-border ("extraterritorial") access. If the consent of an authorized person in Switzerland were additionally required (contrary to the wording of Article 32(b) CCC), the primary objectives of the CCC (improving the fight against cross-border cybercrime, facilitating mutual legal assistance, and partially relieving the requirement for formal mutual legal assistance) would not be met. Foreign e-mail accounts or social network addresses would almost completely escape the direct access provided for in Article 32 lit b CCC, given that (for data stored abroad) one would only rarely find a person authorized in Switzerland to give consent, who would still have to consent to the collection of data (ATF 141 IV 108) (Swiss Supreme Court, 2015). For this reason, the Federal Supreme Court has considered foreign persons or companies as authorized persons within the meaning of Article 32 lit b CCC. The legal right of a person to dispose of data and to pass them on to a State administration is governed first and foremost by the legislation of the State in which the person is acting. The following are entitled to give their consent. In particular, Internet service providers or social network providers who have reserved the right to pass on their customers' data to national and foreign law enforcement authorities in their general terms and conditions of use or in their guidelines on data use. However, it is not sufficient for a cross-border collection of stored data (according to the clear wording of Article 32(b) CCC) that a foreign access provider is entitled to consent to the direct transmission of data in this sense: it must be examined whether the requesting prosecuting authority has obtained legal and voluntary consent from the foreign access provider. The Federal Supreme Court has ruled that implicit voluntary consent can be assumed if the Internet service provider (or the account holder himself) provides the data without further proceedings (ATF 141 IV 108). Voluntary consent will no longer

exist, however, if the authorized person is required to provide the data on the basis of an order to do so.

In practice, Article 32(b) CCC, with its new interpretation following ATF 141 IV 108, has become of considerable practical importance when it comes to obtaining information held by Internet service providers located in the US. Indeed, these service providers are free to disclose, if they wish, a certain amount of information about their users to anyone other than the US government. For its part, the US government admits that foreign prosecuting authorities go directly to US Internet service providers without going through the whole mutual legal assistance route to obtain the data (Bottinelli, 2017). In this case, the Internet service provider is considered to be the person legally entitled to disclose the data within the meaning of Article 32 lit b CCC.

Another of the consequences of this case law is that private entities and no longer the States are given the responsibility of verifying whether the national legal provisions entitle them to follow the requests of foreign prosecution authorities (Bottinelli, 2017).

Subsequently, the Swiss Supreme Court handed down three important decisions, which once again put the scope of direct access under Article 32 CCC into perspective and highlighted a principle that has now become essential in cyber investigations, namely the primacy of access to data over its location. Indeed, the question of the geographical location of the data systematically arises in such cases, if only to find out which jurisdiction they come under and which authorities are competent to implement any necessary investigative and related enforcement measures.

In the first two decisions, the Federal Court resolved the question of whether the Swiss subsidiary of a foreign Internet service provider — in this case Facebook — could be required to hand over user data for the purposes of criminal proceedings. In the context of an investigation focusing on online racial discrimination, the Public Prosecutor's Office had requested that Facebook Switzerland produce the identity of the account holder used to commit the discrimination, the IP addresses used to create the profile, the connection logs and the IP addresses linked to these logs, as well as the private content of the account, under threat of the penalties provided for in Article 292 SCC. After several reminders, Facebook Switzerland indicated that it did not manage the platform but only the development of the advertising market in Switzerland. Then, by e-mail, Facebook Ireland Ltd had indicated that the production order should be sent to her by way of international legal assistance. Notwithstanding this,

and probably as a matter of convenience taking advantage of the subsidiary's presence in Switzerland, the Public Prosecutor's Office sent Facebook Switzerland an order for the production of documents relating to the same information. The Federal Court had in this case the opportunity to clarify the scope of Article 18 CCC. According to the Federal Court, under Article 18 CCC, each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order a person present in its territory to disclose specified computer data in its possession or control that is stored in a computer system or computer data medium (Paragraph 1(a)), or a service provider offering services in the Party's territory to disclose data in its possession or control relating to subscribers and concerning such services (Paragraph 1(b)). The place of storage of the data is not in itself decisive, since it may be a random location, impossible to define *a priori*, and liable to change rapidly, since data centers are widely distributed geographically.

However, it follows from the provisions of both the CCC (Article 18, "in possession or control") and the Swiss Criminal procedure Code (Art. 265, "the holder") that the person against whom the production order is issued must be the possessor or holder of the data in question, or at least have "control" over it, i.e., have *de facto* and *de jure* power of disposal over it.

In this case, however, there was nothing to establish that Facebook Switzerland was actually the owner of the data requested by the public prosecutor. On the contrary, it was established that Facebook Switzerland was "not the owner of the disputed information autonomously." The result was that the Facebook service was controlled by American and Irish companies that were completely separate from the Swiss subsidiary. In this regard, an affidavit from a data protection officer of Facebook Ireland attested that the latter was the only contractual partner with Facebook users outside the US and Canada. Similarly, she was also the only one who "controlled" the personal data of these same users. This was further confirmed by the "Terms of Service", as well as by the e-mail sent to the Public Prosecutor by Facebook Ireland. Consequently, for the Swiss Supreme Court, it appeared that the Swiss company did not have direct access to or control over the data relating to the service.

The Federal Court also stated that a possible power of representation of the Swiss subsidiary could not be recognized in the context of criminal proceedings requiring access to personal data. Indeed, the Swiss and Irish companies have no links with each other and there was no reason to

believe that the Swiss company could have obtained from the foreign companies the information required by the Public Prosecutor. The Public Prosecutor therefore had no choice but to seek mutual legal assistance from the Irish authorities in order to obtain the desired information.

Admittedly, this judgment recalls the importance of jurisdiction and the principle according to which, in the case of evidence to be collected abroad, the usual method of mutual legal assistance in criminal matters must be preferred. In this sense, it is not very progressive and is ill-suited to the realities of the prosecution of cybercrimes or crimes committed using NICTs. However, it does have the merit of highlighting the principle of "control" of data and clarifies the scope of Article 18 CCC, also extending the concept of control to *de jure* control. Indeed, as explained above, in the era of the "cloudization" of computer data, the location of such data is no longer a relevant criterion, but rather a source of problems. Thus the criterion of the location of data must give way to the principle of their control. Only the controller, whether a service provider or a user, can locate the data at a given moment, compile it and decrypt it. On the contrary, the location can change regularly and without human intervention, just as it can be multiple (due to backups) and/or fragmented (due to partitioning). In addition, the data are now encrypted and only the controller has the key to read them. Finally, the territorially competent authorities are generally not able to locate, collect or use the data/evidence present on their territory.

The control criterion was recalled in a Federal Court ruling (Swiss Supreme Court, 2016), this time concerning Google. In this case, the Public Prosecutor's Office of the Canton of Vaud had opened a criminal investigation against unknown persons for copyright infringement, following a complaint by the French Society of Authors, Composers and Music Publishers. The complaint was directed against the administrator of an Internet site, operating under the identity "C" at the e-mail address C@gmail.com. The latter had allegedly distributed musical works on a large scale by offering illegal download links, causing damage estimated at several tens of thousands of euros.

As part of the investigation, the Public Prosecutor's office had requested Google Switzerland to produce the identity of the holder of the above-mentioned Gmail account, the IP addresses used to create the account, the log of connections and the IP addresses linked to these logs from 2008 onwards, as well as the private content of the account. Google Switzerland had then appealed to the Federal Court, explaining in

particular that the information requested was in the hands of the American company Google Inc. It explained in particular that the Public Prosecutor's order violated the principle of territoriality. The Gmail e-mail system is operated in California by the American company Google Inc. so that the required evidence could only be obtained through mutual legal assistance. According to the Budapest Convention on Cybercrime, unilateral access to electronic data stored in another State is only possible under exceptional conditions (consent of the owner or free access to the data, Article 32 CCC), which in this case was not met. Moreover, even if it had had access to the data, the Swiss subsidiary could not have provided it without exposing itself to prosecution under Article 299 SCC and the provisions of US law. Finally, Google Switzerland did not consider itself to be in possession of the required data and was therefore not under an obligation to provide the required information.

In this case, the Swiss Supreme Court began by recalling that the Convention on Cybercrime, which was intended to increase the effectiveness of international cooperation in this area, enshrined a broader concept of "service provider" than the one known under Swiss law. The term refers to "any public or private entity that offers users of its services the possibility of communicating by means of a computer service or any other entity processing or storing computer data for that communication service or its users." However, for the Federal Court, the Convention was based on the principle of territoriality, according to which a State is not entitled to take investigative and prosecutorial measures in the territory of another State. In order to do so, the requesting State must act through international mutual assistance (Article 23 et seq. CCC) and has at its disposal, under the Convention, various instruments intended to facilitate its execution (rapid preservation of stored computer data under Article 29 CCC) or even to circumvent it (cross-border access to stored data, with consent or when they are publicly accessible, under Article 32 CCC). The Federal Court also recalled these problems of territoriality by underlining that on the occasion of the modification of the Federal act on the Surveillance of Post and Telecommunications it had been stressed that "since many important Internet service providers have their headquarters and infrastructure abroad, the opening of certain e-mail accounts is a matter of urgency. The opening of certain e-mail accounts abroad by persons living in Switzerland, which are in themselves controllable

services, is an example of this. It would therefore be unrealistic and problematic to expect Swiss authorities to have unhindered access to the data concerned, since this would run counter to the principle of territoriality of laws." Then, as it had done in the Facebook case, it noted that in the case in point, while Google Switzerland exercised control over the compatibility with Swiss law of the content of blogs hosted "by a site of which it is the administrator," as well as other activities related to advertising, it disputed that it was involved in any way in the opening or operation of a Gmail account, since the e-mail system was the sole responsibility of the American company. As for the power of representation attributed to it by the Public Prosecutor's office, it could certainly be recognized in other legal matters or with regard to the other specific activities of the company based in Switzerland, but not in the context of criminal proceedings requiring access to Gmail e-mail data. Thus, the Swiss Supreme Court did not find that the Swiss company had any direct access or "control" over the data relating to this e-mail service. However, the Swiss Supreme Court held that it follows from both the provisions of the CCC (Article 18, "in his possession or under his control") and the Swiss Code of Criminal Procedure (Article 265, the "holder") that the person against whom the production order is issued must be the possessor or holder of the data, or at least have control over it, i.e., have *de facto* and *de jure* power of disposal over it. This is why the Swiss Supreme Court referred the case back to the lower authority to establish whether Google Switzerland did not actually have any right of access to the disputed data, and that control of these data would be the sole responsibility of the company based in the US. The Swiss Supreme Court emphasized that if it were to appear that the Swiss company cannot, in fact or in law, have access to the data requested by the Public Prosecutor's Office, the latter will have no other choice than to apply to the US authorities for mutual legal assistance in order to obtain the desired information. As in the Facebook case, the importance of "control over data" is clear here.

The criterion of data control was finally confirmed in a subsequent decision of the Swiss Supreme Court (2017), where the prosecution authorities had accessed the Facebook account and stored the related data of a detainee after having obtained his login and password which he had written on a paper he was trying to exfiltrate from jail. The detainee complained that this investigative measure was unlawful

because it violated the sovereignty of a foreign State, as it involved data on servers located abroad. However, the Swiss Supreme Court found that the investigating authority had not taken any decision to collect data or to order the production of data from Facebook USA, Facebook Ireland, or Facebook Switzerland. Nor had the Public Prosecutor's office taken any action of public authority abroad (based on the Cybercrime Convention or through mutual legal assistance). On the contrary, the investigating authority had undertaken its own investigations on the Internet — using computers, servers, and IT infrastructure located in Switzerland. This online search had been made possible because the prosecution was in possession of a secret message containing the access data to the defendant's Facebook account (which the defendant had tried to retrieve from the prison). Thus, for the Swiss Supreme Court, a person who uses a derived Internet service, via Internet access within Switzerland, which is offered by a foreign company, is not acting "abroad." The mere fact that the electronic data of the derived Internet service in question is located on servers (or clouds) that are managed abroad, does not qualify such an online search, which took place from Switzerland and in accordance with the law, as an inadmissible act of investigation on foreign territory. For this reason, the Federal Court found that the online search and the provisional collection of data that preceded it was compliant with federal law.

These few considerations, based on major rulings by the Swiss Supreme Court, are sufficient to highlight the difficulties faced by the prosecuting authorities in the area of cyber investigations, since these almost always lead to requests for information from the giants of the Web, such as Facebook and Google. However, the criterion of data control implies addressing entities located in foreign jurisdictions, which is only possible through direct access in accordance with Article 32 CCC, the conditions for which are strict, or to through the usual mechanisms of international mutual legal assistance, the responsiveness of which leaves something to be desired.

Therefore, a consensus emerged regarding the need for tools that would give the prosecution authorities more flexibility and responsiveness. States have considered various options to provide greater effectiveness to the existing anti-cybercrime legislation. One of the most valid solutions is a draft second protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence.

New Paths Toward Effective Cyber Investigations: The (Draft) Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence

The Convention on Cybercrime already includes a First Additional Protocol: The Additional Protocol on Xenophobia and Racism Committed via Computer Systems.

However, in order to respond to the various problems mentioned in the previous chapters according to cybercrimes, specifically in relation with the need for an effective criminal justice within the respect of the rule of law, the Cloud Evidence Group has recommended the enactment of a Second Additional Protocol to the Budapest Convention. Hence, since June 2017, the Cybercrime Convention Committee (T-CY) has started to draft this Second Additional Protocol (Council of Europe, 2021a). This "(Draft) Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence" (DSP-CCC) was made public on April 12, 2021, and will apply when the authorities are investigating a cybercrime or any criminal offence involving evidence in electronic form commonly referred to "electronic evidence" or "digital evidence" (Council of Europe, 2021c). It was approved by the Council of Ministers on November 17, 2021, and should be opened for signature in May 2022.

This Draft Protocol is divided into four chapters, beginning with the common provisions (Chapter I), focusing then on the specific measures for enhanced cooperation (Chapter II). Chapter III considers the conditions and safeguards related to this enhanced cooperation, and finally, Chapter IV is related to the final provisions.

In terms of measures, the main achievements of the Draft Protocol can be found in Articles 6 and 7, which enable direct cooperation between the authorities of one Party and entities (public or private) providing either domain name services (Article 6 DSP-CCC) or acting as Service providers (Article 7 DSP-CCC). Article 7 DSP-CCC, if enacted, will probably be a major step forward to an increased effectiveness of cyber investigations as it aims at collecting "subscriber information" directly from the Service provider. Hence, in national and international cybercrime investigations, the fundamental data needed for the authorities to proceed with an investigation are precisely the subscriber

information (Council of Europe, 2021c). Subscriber information is defined in Article 18 CCC as "any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: (a) the type of communication service used, the technical provisions taken thereto and the period of service; (b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; (c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement." Therefore, if Article 7 DSP-CCC is an important development, it would occur in regard to the Article 18 CCC.

As discussed earlier, Article 18 CCC provides that each Party of the Budapest Convention shall adopt legislative and other measures as may be necessary to empower its competent authorities to order a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. This facility can then only be implemented if the competent authorities empower the service provider to submit that information. Therefore, authorities in charge of the investigation of a cybercrime often have to use international cooperation procedures, such as mutual assistance. Those proceeding are not always able to provide a prompt assistance or an effective response to answer the needs of the investigation (Council of Europe, October 2021c). Experience also shows that, by the time the request of mutual assistance is notified to the service provider, the subscriber information might have been erased. As an example, under Swiss law, service providers have to store subscriber information for six months only (Article 21 of the Federal Act on the Surveillance of Post and Telecommunications (SPTA)).

Thus, Article 7 DSP-CCC will provide to Article 18 CCC mentioned earlier a much larger scope of application as it will allow a Party to issue certain orders directly to the service provider in the territory of another Party (Council of Europe, 2021c) to ensure a quick and effective response of the criminal justice system.

Nonetheless, Article 7 DSP-CCC will not enable a Party to require a Service provider to use the enforcement mechanisms available under its domestic law for enforcement of these orders. In this regard, Article 7

paragraph 7 DSP-CCC states that a service provider can refuse to disclose subscriber information. In this situation, the issuing party may only seek to enforce the order only via Article 8 DSP-CCC or other (traditional) forms of mutual assistance. Parties may request that a service provider give a reason for refusing to disclose the subscriber information sought by the order.

The draft of the Second Additional Protocol also establishes in its Article 9 an expedited disclosure of stored computer data in emergency situations, such as a terrorist attack, a ransomware attack that may cripple a hospital system, or when investigating e-mail accounts used by kidnappers to issue requests and communicate with the victim's family (Council of Europe, October 2021c). Article 9 DSP-CCC allows the Party to cooperate at any time (according to the Article 35 of the Convention on Cybercrime) by using the 24/7 channel. This 24/7 network is adapted to handle the time-sensitive and high-priority requests with the mechanisms exposed in Article 9 DSP-CCC and is staffed with points of contact who are able to communicate quickly without needing any written translations. Those points of contact can follow up on issues originating from any Party to the Convention on Cybercrime and directly ask the service provider in their territory on behalf of the requesting Party (Council of Europe, 2021c).

This mechanism avoids losses of time related to the preparation of a request for mutual assistance. Indeed, drafting a request and then having it translated and transmitted through national channels to the requesting party having jurisdiction over that request necessarily requires a certain amount of time (Council of Europe, 2021c).

Thus, under Article 9 DSP-CCC, there will be no immediate necessity to comply with these formalities, thus enabling the criminal justice authorities to act promptly against cybercriminals wherever they are.

Let us also stress that a large section of the Draft Second Protocol is dedicated to Conditions and Safeguards (Article 14 DSP-CCC) and data protection matters (Article 15 DSP-CCC) in order to balance the extensive powers given to prosecution authorities seen above. In this regard, Article 14 DSP-CCC requires that each Party shall ensure that the establishment, implementation, and application of the powers and procedures provided for in this Protocol are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties.

Conclusion

In conclusion, it should be noted that jurisdictional problems are the main obstacles to the prosecution of not only cybercrimes but also ordinary crimes committed through ICTs. Indeed, prosecution authorities will very quickly come up against their national borders and their lack of competence *ratione fori* whenever they investigate this type of crime. As criminal jurisdiction is an indispensable component of State sovereignty, international mutual legal assistance in criminal matters has long been the only way to pursue the investigations. However, international mutual legal assistance, with its slow and cumbersome procedures, is particularly ill suited to the fight against cybercrime, which is flexible, fast, and ubiquitous. Thus, recourse to mutual legal assistance mechanisms has the effect of considerably slowing down the action of the prosecuting authorities and thus leads to the loss of strategic data that could either be used as evidence or lead to the obtaining of evidence necessary to prove the commission of the offence and the identification of its perpetrator. Since State sovereignty is the problem, it will only be through international treaties, through which States will give up a few crumbs of their sovereignty, that the prosecuting authorities will have effective tools to fight cybercrime. Twenty years ago, a first step in this direction was taken under the aegis of the Council of Europe Cybercrime Convention, but it continues to be interpreted restrictively. Today, a second step is about to be taken with the adoption of the Second Protocol, through which States give up some more of their sovereignty to strengthen the fight against cybercrime. The idea of a common, uniform Internet law that would ignore borders no longer seems so far-fetched, at least as far as criminal procedure for online investigations is concerned and provided that the principles of the rule of law are respected.

References

Bottinelli, N. (2017). Commentaire de l'article 299 CP. In Commentaire romand du Code pénal II, Macaluso, A., Moreillon, L., and Queloz, N. (eds.), Bâle: Helbing & Lichtenhahn.

Confédération suisse (2013). Rapport explicatif: Concernant un avant-projet de la loi fédérale sur la collaboration avec des autorités étrangères et la protection de la souveraineté suisse et un avant-projet d'arrêté fédéral portant

approbation des conventions du Conseil de l'Europe sur la notification à l'étanger des documents et sur l'obtention à l'étranger d'informations et de preuves en matière administrative [in French].

Council of Europe (2021a). Enhanced cooperation on cybercrime and electronic evidence: Toward a Protocol to the Budapest Convention.

Council of Europe (2021b). Commentary - Acceding to the Budapest Convention on Cybercrime: Benefits - The Budapest Convention on Cybercrime. https://rm.coe.int/cyber-buda-benefits-june2021a-en/1680a2ddb0. [Accessed 19 May 2022].

Council of Europe (2021c). Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence as approved by the T-CY at its 24th Plenary (28 May 2021) with Explanatory Repost edited October 2021.

Luis Cordova, J. G., Correa Álvarez, P. F., Echerri Ferrandiz, F. and Pérez-Bravo, J. C. (2017). Law versus cybercrime. *Global Jurist*, 18(1), 1–9.

Müller, J. (2012). *La cybercriminalité économique au sens étroit: Analyse approfondie du droit suisse et aperçu de quelques droits étrangers*. Genève Etc.: Schulthess.

Shan-A-Khuda, M. and Cliffe Schreuders, Z. (2019). Understanding cybercrime victimisation: Modelling the local area variations in routinely collected cybercrime police data using latent class analysis. *International Journal of Cyber Criminology*, 13(2), 493–510.

Statista Infographies (n.d.). *Infographie: Plus de la moitié de la planète est connectée sur la toile*. https://fr.statista.com/infographie/17328/utilisateurs-internet-dans-le-monde/. [Accessed 10 November 2021].

Sviatun, O. V., Goncharuk, O. V., Roman, C., Kuzmenko, O. and Kozych, I. V. (2021). Combating cybercrime: Economic and legal aspects. *WSEAS Transactions on Business and Economics*, 18, 751–762. [Accessed 10 Novembre 2021].

Swiss Supreme Court (2015). Swiss Supreme Court decision, 14th of Januar 2015 (ATF 141 IV 108). https://www.bger.ch/ext/eurospider/live/fr/php/aza/5http/index.php?lang=en&type=show_document&page=1&from_date=&to_date=&sort=relevance&insertion_date=&top_subcollection_aza=all&query_words=&rank=0&highlight_docid=atf%3A%2F%2F141-IV-108%3Afr&number_of_ranks=0&azaclir=clir.

Swiss Supreme Court (2016). Swiss Supreme Court decision, 16th of November 2016 (1B_142/2016). https://www.bger.ch/ext/eurospider/live/fr/php/aza/http/index.php?highlight_docid=aza%3A%2F%2F16-11-2016-1B_142-2016&lang=fr&type=show_document&zoom=YES&.

Swiss Supreme Court (2017). Swiss Supreme Court decision, 24th of May 2017 (ATF 143 IV 270). https://www.bger.ch/ext/eurospider/live/fr/php/aza/http/index.php?lang=en&type=show_document&page=1&from_date=&

to_date=&sort=relevance&insertion_date=&top_subcollection_aza=all&query_words=&rank=0&highlight_docid=atf%3A%2F%2F143-IV-270%3Afr&number_of_ranks=0&azaclir=clir.

Yar, M. and Steinmetz, K. F. (2006). *Cybercrime and Society*. Los Angeles: Sage.

Zimmermann, R. (2009). *La coopération judiciaire internationale en matière pénale*. Berne: Stämpfli.

Zimmermann, R. (2019). *La coopération judiciaire internationale en matière pénale*. 5e edition. Berne: Stämpfli.

https://doi.org/10.1142/9781800612839_bmatter

Index