

RECENT ADVANCES IN IoT AND BLOCKCHAIN TECHNOLOGY

Editors:
Koyel Datta Gupta
Deepak Kumar Sharma
Rinky Dwivedi
Fadi Al-Turjman

Bentham Books

Advances in Computing Communications and Informatics

(Volume 4)

Recent Advances in IoT and Blockchain Technology

Edited by

Koyel Datta Gupta

*Department of Computer Science & Engineering
Maharaja Surajmal Institute of Technology
New Delhi
India*

Deepak Kumar Sharma

*Department of Information Technology
Indira Gandhi Delhi Technical University for Women
Delhi, India*

Rinky Dwivedi

*Department of Computer Science & Engineering
Maharaja Surajmal Institute of Technology
C-4 Janakpuri, New Delhi 100058
India*

&

Fadi Al-Turjman

*Department of Artificial Intelligence Engineering
Near East University
North Cyprus*

Advances in Computing Communications and Informatics

Volume # 4

Recent Advances in IoT and Blockchain Technology

Series Editors: Pradeep Kumar Singh, Bharat Bhargava and Wei-Chiang Hong

Volume Editors: M. J. Griffin, I. W. C. F. G. M. C. U. J. C. T. P. F. y. k. g. k. H. C. V. W. L. o. C. P.

ISSN (Online): 2737-5730

ISSN (Print): 2737-5722

ISBN (Online): 978-981-5051-60-5

ISBN (Print): 978-981-5051-61-2

ISBN (Paperback): 978-981-5051-62-9

© 2022, Bentham Books imprint.

Published by Bentham Science Publishers Pte. Ltd. Singapore. All Rights Reserved.

First published in 2022.

BENTHAM SCIENCE PUBLISHERS LTD.

End User License Agreement (for non-institutional, personal use)

This is an agreement between you and Bentham Science Publishers Ltd. Please read this License Agreement carefully before using the ebook/echapter/ejournal (“**Work**”). Your use of the Work constitutes your agreement to the terms and conditions set forth in this License Agreement. If you do not agree to these terms and conditions then you should not use the Work.

Bentham Science Publishers agrees to grant you a non-exclusive, non-transferable limited license to use the Work subject to and in accordance with the following terms and conditions. This License Agreement is for non-library, personal use only. For a library / institutional / multi user license in respect of the Work, please contact: permission@benthamscience.net.

Usage Rules:

1. All rights reserved: The Work is the subject of copyright and Bentham Science Publishers either owns the Work (and the copyright in it) or is licensed to distribute the Work. You shall not copy, reproduce, modify, remove, delete, augment, add to, publish, transmit, sell, resell, create derivative works from, or in any way exploit the Work or make the Work available for others to do any of the same, in any form or by any means, in whole or in part, in each case without the prior written permission of Bentham Science Publishers, unless stated otherwise in this License Agreement.
2. You may download a copy of the Work on one occasion to one personal computer (including tablet, laptop, desktop, or other such devices). You may make one back-up copy of the Work to avoid losing it.
3. The unauthorised use or distribution of copyrighted or other proprietary content is illegal and could subject you to liability for substantial money damages. You will be liable for any damage resulting from your misuse of the Work or any violation of this License Agreement, including any infringement by you of copyrights or proprietary rights.

Disclaimer:

Bentham Science Publishers does not guarantee that the information in the Work is error-free, or warrant that it will meet your requirements or that access to the Work will be uninterrupted or error-free. The Work is provided "as is" without warranty of any kind, either express or implied or statutory, including, without limitation, implied warranties of merchantability and fitness for a particular purpose. The entire risk as to the results and performance of the Work is assumed by you. No responsibility is assumed by Bentham Science Publishers, its staff, editors and/or authors for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products instruction, advertisements or ideas contained in the Work.

Limitation of Liability:

In no event will Bentham Science Publishers, its staff, editors and/or authors, be liable for any damages, including, without limitation, special, incidental and/or consequential damages and/or damages for lost data and/or profits arising out of (whether directly or indirectly) the use or inability to use the Work. The entire liability of Bentham Science Publishers shall be limited to the amount actually paid by you for the Work.

General:

1. Any dispute or claim arising out of or in connection with this License Agreement or the Work (including non-contractual disputes or claims) will be governed by and construed in accordance with the laws of Singapore. Each party agrees that the courts of the state of Singapore shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this License Agreement or the Work (including non-contractual disputes or claims).
2. Your rights under this License Agreement will automatically terminate without notice and without the

need for a court order if at any point you breach any terms of this License Agreement. In no event will any delay or failure by Bentham Science Publishers in enforcing your compliance with this License Agreement constitute a waiver of any of its rights.

3. You acknowledge that you have read this License Agreement, and agree to be bound by its terms and conditions. To the extent that any other terms and conditions presented on any website of Bentham Science Publishers conflict with, or are inconsistent with, the terms and conditions set out in this License Agreement, you acknowledge that the terms and conditions set out in this License Agreement shall prevail.

Bentham Science Publishers Pte. Ltd.

80 Robinson Road #02-00

Singapore 068898

Singapore

Email: subscriptions@benthamscience.net



CONTENTS

PREFACE	i
ACKNOWLEDGEMENTS	i
LIST OF CONTRIBUTORS	iii
CHAPTER 1 BLOCKCHAIN FRAMEWORK FOR DATA STORAGE AND SECURITY	1
<i>Salman Azeez Syed, Vivaswat Sinha, Sachin Singh and Aarti Goel</i>	
INTRODUCTION	2
Centralized Database System	3
<i>Advantages</i>	3
<i>Disadvantages</i>	3
Decentralized Database System	4
<i>Advantages</i>	4
<i>Disadvantages</i>	5
BLOCKCHAIN TECHNOLOGY	5
Bitcoin	5
What is Blockchain?	6
Blockchain Architecture	6
Block	7
Characteristics of Blockchain	8
<i>Decentralized</i>	9
<i>Immutability</i>	9
<i>Security</i>	9
<i>Anonymity</i>	9
<i>Auditability</i>	9
VERSION CONTROL SYSTEM	10
Types of Version Control Systems	11
<i>Local Version Control System (LVCS)</i>	11
<i>Centralized Version Control System (CVCS)</i>	11
<i>Distributed Version Control System (DVCS)</i>	11
DATA STORAGE	11
Data Storage Frameworks Implementing Blockchain	12
Sharding	13
<i>Drawbacks of Sharding In Blockchain</i>	15
<i>Alternatives to Sharding</i>	15
<i>Blockchains Using Sharding</i>	15
P2P NETWORK	16
Types of P2P Network	17
<i>Unstructured Network</i>	17
<i>Structured Network</i>	17
<i>Hybrid P2P Network</i>	18
Disadvantages of P2P Network	20
Layered Structure	20
<i>Identity Layer</i>	20
<i>Data Layer</i>	20
<i>Data-swap Layer</i>	20
<i>Network Layer</i>	20
<i>Routing Layer</i>	21
<i>Consensus Layer</i>	21
<i>Incentive layer</i>	21
Libp2p	21
INTERPLANETARY FILE SYSTEM (IPFS)	21

IPFS Functionality	22
<i>Content Addressing</i>	22
<i>Content Linking</i>	23
<i>Content Accessibility</i>	23
Deeper analysis of IPFS: Networking	25
Implementation of blockchain on IPFS: Filecoin	26
<i>Structure of the Filecoin Network</i>	27
<i>Data Storage and Retrieval Protocols</i>	27
<i>Fault Tolerance</i>	28
<i>Why the Hype Around Filecoin?</i>	29
Swarm	31
BLOCKCHAIN - PRIVACY	31
Sybil Attack	32
51% Attack	32
How Blockchain Implements Data Privacy	33
<i>Blockchain Privacy Protection</i>	33
BLOCKCHAIN - SECURITY	34
A Deeper Dive into Blockchain Security	35
<i>Hash Chained Storage</i>	35
<i>Digital Signature</i>	35
Consensus	36
<i>Types of Algorithm</i>	36
<i>Proof of Work (POW)</i>	36
Some Problems with Blockchain	38
DISCUSSION	39
CONCLUSION	40
CONSENT FOR PUBLICATION	40
CONFLICT OF INTEREST	41
ACKNOWLEDGEMENT	41
REFERENCES	41

CHAPTER 2 BLOCKCHAIN BASED HYBRID FRAMEWORK FOR IDENTITY

MANAGEMENT IN HEALTHCARE	44
<i>Deepak Kumar Sharma, Arjun Khara, Koyel Datta Gupta and Rinky Dwivedi</i>	
INTRODUCTION	44
BACKGROUND AND RELATED WORK	48
MOTIVATION	49
IDENTITY MANAGEMENT: HEALTHCARE SYSTEM	49
PROPOSED SOLUTION	51
Architecture	52
Creation of Records	53
<i>Master Record</i>	54
<i>Device Record</i>	54
<i>Begin</i>	54
<i>Creation of Identifiers</i>	56
<i>Claim Chain</i>	57
CONCLUSION	57
CONSENT FOR PUBLICATION	57
CONFLICT OF INTEREST	58
ACKNOWLEDGEMENT	58
REFERENCES	58

CHAPTER 3 BLOCKCHAIN IN SMART HEALTHCARE FACILITY	61
<i>Ayush Kumar Singh, Nipunika and Deepak Kumar Sharma</i>	
INTRODUCTION	61
Technical Aspects of Blockchain	62
Applications of Blockchain	63
<i>Voting</i>	63
<i>Identity Management</i>	64
<i>Real Estate Records Management</i>	65
Traditional Technology in Healthcare	65
<i>Electronic Health Records</i>	65
<i>Patient-Generated Data</i>	66
<i>Technological Requirements in the Industry</i>	67
<i>Other Challenges</i>	67
USE CASES	68
Health Records	68
<i>Application in EHR</i>	68
<i>Personal Health Records(PHR)</i>	69
<i>Successful Implementations</i>	69
Internet of Medical Things	70
<i>Challenges Faced in IoMT</i>	70
<i>Blockchain in IoMT</i>	70
Clinical Trials	71
Health Insurance	72
<i>Smart Contracts to ease insurance claims</i>	72
Invoicing	74
<i>E-Invoicing and Blockchain</i>	74
<i>Large Scale Implementations</i>	74
Supply Chain Management	75
<i>Blockchain-based Supply Chain Management</i>	76
<i>Sustainability</i>	76
<i>Limitations in Implementation</i>	76
CHALLENGES	77
Security	77
<i>51% Attack</i>	77
<i>Criminal Smart Contracts</i>	78
Scalability	78
<i>Why is Blockchain so Slow?</i>	79
<i>Managing Storage Capacity</i>	79
CASE STUDIES	79
Gem Health Network	80
MedRec	81
<i>Technicalities</i>	81
<i>MedRec 2.0</i>	82
Guardtime	82
<i>New Ventures</i>	83
Medicalchain	83
<i>Medicalchain Solutions</i>	84
OmniPHR	85
<i>Overview</i>	85
<i>Design</i>	85

MediBchain	87
<i>Protocol for Sending Data to the System</i>	88
FURTHER DISCUSSION	89
SUMMARY	90
CONSENT FOR PUBLICATION	90
CONFLICT OF INTEREST	90
ACKNOWLEDGEMENT	90
REFERENCES	91
CHAPTER 4 APPLICATION OF IOT IN PATIENT HEALTH MONITORING SYSTEM	96
<i>Rinky Dwivedi, Harshit Mittal, Manik Agarwal and Sahil Dwivedi</i>	
INTRODUCTION	96
RELATED WORK	97
SYSTEM ARCHITECTURE	98
A. System Structure	98
<i>Algorithm 1.</i>	101
<i>Algorithm 2.</i>	102
<i>Algorithm 3.</i>	103
EQUIPMENT DETAILS	103
PERFORMANCE AND MEASUREMENT	104
EMERGENCY ALERT	109
CONCLUSION AND FUTURE SCOPE	110
CONSENT FOR PUBLICATION	110
CONFLICT OF INTEREST	111
ACKNOWLEDGEMENT	111
REFERENCES	111
CHAPTER 5 IOT BASED VERIFIED AND PUBLIC VEHICLE REGISTRATION THROUGH BLOCKCHAIN: FUTURE SMART CITIES BASED APPLICATIONS WITH SUSTAINABLE APPROACH	113
<i>Rohit Rastogi, Bhuvneshwar Sharma, Pardeep Kumar and Muskan Gupta</i>	
INTRODUCTION	114
Concept of Smart Cities	114
Problem of Car Registration and Motivation	115
Research Objectives	115
Scope of the Research Work	115
5-G Technology and Its Implications	116
IoT and Its Applications in Transportation	116
<i>Application in Automobile</i>	116
<i>Usage of AI, ML in IoT and Blockchain</i>	117
RELATED WORK	117
Carchain	117
Fabcar IBM Blockchain	118
Blockchain and Future of Automobiles	118
Significance of 5-G Technology	119
PRESENTED METHODOLOGY	120
SOFTWARE REQUIREMENT SPECIFICATION	120
Product Perspective	120
Similarities between Carchain and our application	121
Differences Between Carchain and Our Application	121
System Interfaces	121
Interfaces (Hardware and Software and communication)	121

<i>Login/Signup</i>	121
<i>Main Page</i>	121
<i>Contact us</i>	122
<i>Manufacturer</i>	122
<i>Dealer</i>	122
<i>Registration Authority</i>	122
<i>Police</i>	122
<i>Customer</i>	122
Hardware Interfaces	122
Software Interfaces	122
<i>Ubuntu 20.04</i>	122
<i>Hyper ledger Fabric v0.20</i>	123
<i>Node.Jsv12.16.0-x64</i>	123
<i>Docker 19.03.8</i>	123
<i>Postman 7.24.0</i>	123
Communications Interfaces	123
Memory Constraints	123
Operations (Product Functions, User Characteristics)	123
Product-Functions	123
User Characteristics	124
Use Case, Sequence Diagram	124
<i>Use case</i>	124
Sequence Diagrams	126
System Design	127
Architecture Diagrams	127
Data Flow Diagram	128
Activity Diagram	129
ER Diagram	130
Database Schema Diagrams	130
Customer	134
<i>Software Requirements</i>	134
<i>Hardware Requirements</i>	135
IMPLEMENTATION DETAILS	136
Snapshots of Interfaces	136
Test Cases	139
RESULTS AND DISCUSSION	140
NOVELTY AND RECOMMENDATIONS	141
FUTURE RESEARCH DIRECTION	142
LIMITATIONS	143
CONCLUSION	143
CONSENT FOR PUBLICATION	143
CONFLICT OF INTEREST	144
ACKNOWLEDGEMENT	144
REFERENCES	144
CHAPTER 6 IDENTIFICATION OF COUNTERFEIT DRUGS USING DECENTRALIZED	
SUPPLY CHAIN	146
<i>Koyel Datta Gupta, Aditya Gupta, Tanmay Sharma and Aayush Bhatnagar</i>	
INTRODUCTION	146
Blockchain	147
Smart Contract	148

Supply Chain	149
Ethereum	150
RELATED WORK	150
METHODOLOGY	152
CONCLUSION	155
CONSENT FOR PUBLICATION	155
CONFLICT OF INTEREST	155
ACKNOWLEDGEMENT	155
REFERENCES	156
CHAPTER 7 MAKING GREAT STRIDES TOWARDS ROAD DETECTION	158
<i>Vimal Gaur</i>	
INTRODUCTION	158
RELATED WORK	159
DATASET	160
Data Selection	160
Preprocessing	160
Method	161
Architecture of the Model	162
Model Summary	162
Splitting and Training	165
RESULTS	166
LIMITATIONS & FUTURE WORK	167
CONCLUSION	168
CONSENT FOR PUBLICATION	168
CONFLICT OF INTEREST	168
ACKNOWLEDGEMENT	168
REFERENCES	168
SUBJECT INDEX	170

PREFACE

It is of immense pleasure to launch our book entitled Recent Advancements In Iot And Block chain that explores the idea of the Internet of Things and Blockchain Technology.

Recent advancements in the fields of block chaining for enterprises, block chaining in financial services, block chaining in supply chain, IoT in healthcare, and other industries and technologies have resulted in the integration of block chaining and the Internet of Things (IoT). Blockchain, whether public or private, is capable enough to maintain the integrity of transactions by decentralizing the records among involved users. Many IoT companies are using blockchain technology to make the world a better-connected place. Many companies are exploring how to make this technology more and more efficient service provider for IoT. Blockchain and IoT are certainly revolutionary technologies that are changing the world around us. Therefore, the major focus of this book is to present the recent advancements in these two technologies and how these technologies, when merged together, provide a transparent, reliable, and secure model for data processing by intelligent devices in various domains.

The book chapters have been contributed by scholars, researchers, academicians, and engineering practitioners. The book received plenteous abstract-articles that were subjected to rigorous review procedures to ensure that the selected articles met the required quality standards.

We would extend our gratitude to everyone who has contributed directly or indirectly to the book. We express our sincere gratitude to all the authors and reviewers who ve been committed to shaping this book even after facing hardships due to the current pandemic situation. Our earnest thanks to the publisher Bentham Science for accepting our book proposal.

ACKNOWLEDGEMENTS

Our gratitude belongs to all the co-authors without whom these pages would be blank. We would also like to thank all the referees for their useful suggestions.

Koyel Datta Gupta

Department of Computer Science and Engineering
Maharaja Surajmal Institute of Technology
New Delhi
India

Deepak Kumar Sharma

Department of Information Technology
Indira Gandhi Delhi Technical University for Women
Delhi
India

Rinky Dwivedi
Department of Computer Science and Engineering
Maharaja Surajmal Institute of Technology
C-4 Janakpuri, New Delhi 100058
India

&

Fadi Al-Turjman
Department of Artificial Intelligence Engineering
Near East University
North Cyprus

List of Contributors

Aarti Goel	Department of Information Technology, Netaji Subhas University of Technology, New Delhi, India
Aayush Bhatnagar	Department of Computer Science & Engineering, Maharaja Surajmal Institute of Technology, New Delhi 110058, India
Aditya Gupta	Department of Computer Science & Engineering, Maharaja Surajmal Institute of Technology, New Delhi 110058, India
Arjun Khera	Department of Information Technology, Netaji Subhas University of Technology, New Delhi 110078, India
Ayush Kumar Singh	Department of Information Technology, Netaji Subhas University of Technology (Formerly known as Netaji Subhas Institute of Technology), New Delhi, India
Bhuvneshwar Sharma	Department of CSE, ABES Engineering College, Ghaziabad, U.P. 201009, India
Deepak Kumar Sharma	Department of Information Technology, Indira Gandhi Delhi Technical University for Women, Delhi, India
Harshit Mittal	Department of Computer Science and Engineering, Maharaja Surajmal Institute of Technology, C-4 Janakpuri, New Delhi 100058, India
Koyel Datta Gupta	Department of Computer Science & Engineering, Maharaja Surajmal Institute of Technology, New Delhi 110058, India
Manik Agarwal	Department of Computer Science and Engineering, Maharaja Surajmal Institute of Technology, C-4 Janakpuri, New Delhi 100058, India
Muskan Gupta	Department of CSE, ABES Engineering College, Ghaziabad, U.P. 201009, India
Nipunika	Department of Information Technology, Netaji Subhas University of Technology (Formerly known as Netaji Subhas Institute of Technology), New Delhi, India
Pardeep Kumar	Department of Computer Systems and Engineering, QUEST University, Nawabshah, Pakistan
Rinky Dwivedi	Department of Computer Science and Engineering, Maharaja Surajmal Institute of Technology, C-4 Janakpuri, New Delhi 100058, India
Rohit Rastogi	Department of CSE, ABES Engineering College, Ghaziabad, U.P. 201009, India
Sachin Singh	Department of Information Technology, Netaji Subhas University of Technology, New Delhi, India
Sahil Dwivedi	Department of Computer Science and Engineering, Maharaja Surajmal Institute of Technology, C-4 Janakpuri, New Delhi 100058, India
Salman Azeez Syed	Department of Information Technology, Netaji Subhas University of Technology, New Delhi, India
Tanmay Sharma	Department of Computer Science & Engineering, Maharaja Surajmal Institute of Technology, New Delhi 110058, India

iv

Vimal Gaur

Department of Computer Science & Engineering, Maharaja Surajmal Institute of Technology, New Delhi 110058, India

Vivaswat Sinha

Department of Information Technology, Netaji Subhas University of Technology, New Delhi, India

CHAPTER 1

Blockchain Framework for Data Storage and Security**Salman Azeez Syed^{1,*}, Vivaswat Sinha¹, Sachin Singh¹ and Aarti Goel¹**¹ *Department of Information Technology, Netaji Subhas University of Technology, New Delhi, India*

Abstract: In this age of sensitive information where knowledge is power, our data has become an invaluable resource. Easy and public access to information makes it vulnerable to adulteration. The ever-increasing cases of cyber-attacks are causing organizations to spend an exorbitant amount on security. General cloud storage systems are considered efficient for data storage and sharing, but it has multiple limitations such as data centralization, data leakage, and high maintenance cost. Data centralization makes it a hotspot for cyber-attacks, making it prone to data outflows and tampering. An effective alternative is a decentralized system. With advancements in information technology and cyber security, the need for authenticity and verification is highly sought after, making blockchain technology an extremely indispensable tool in the hands of many organizations and enterprises. It solves the problem of security by encrypting its data storing it as a “Hash” or encoded data so that only the user with the key can access the data. The finance sector is being overwhelmed by the ever-increasing reliability of blockchain and the implementation of its framework and architecture. Blockchain is a distributed ledger system across a network of users. The blockchain technology, being decentralized, is proposed as a disseminated and diffused or distributed approach which is testified to decipher and decode the security requirements of the new digital era as well as serve as a platform and a jump pad for advancements in various other fields such as Internet of Things (IoT), data storage, biometric security, healthcare facilities, smart grids, and many more.

This chapter begins with a basic outline of all you need to know about blockchain, an upcoming evolutionary technology that ameliorates the world of data decentralization and security. It further explains its use, features, areas of implementation, architecture, as well as its limitations that are detrimental to be cognizant of how the blockchain system works/is implemented. It then explores P2P networks and interplanetary file systems (IPFS) followed by its current use cases in the form of Filecoin. Next, the chapter explores the privacy and security aspects of the blockchain. It showcases some of the faults of blockchain ledgers like Sybil and discusses some techniques that are implemented to fix them. It discusses bitcoin, one of the most secure blockchain architecture to date, and describes private and public keys, peer to peer network, hash.

* **Correspondence author Salman Azeez Syed:** Department of Information Technology, Netaji Subhas University of Technology, New Delhi, India; Tel: 7428030776; E-mail: azeezsalman1@gmail.com

chained storage, digital signature, and consensus algorithms implemented by bitcoin to prevent any fraudulent transactions from taking place.

Keywords: Attribute Based Encryption (ABE), Blockchain, Consensus, Digital signature, Filecoin, IPFS, P2P network, Sharding.

INTRODUCTION

Nowadays, computers have found their way into many fields. This process of digitalization or more appropriately computerization, has now been adopted by all the departments ranging from hospitals, schools, railways, and many more areas. Why? This is because computers have huge advantages over paper-based systems, which has led to the proliferation of computers in almost all organizations and enterprises. Some of these advantages include:.

- **Compact**

In contrast to recording data on paper, storage as a digital copy massively reduces space, which is generally a constraint for small organisations.

- **Ease of Accessibility**

All the data stored on the cloud can be accessed easily and remotely by any person around the world, making it a good means of sharing data. Otherwise, the person would have to look at the papers himself in person.

- **Readability**

Papers can easily be lost or damaged. Even if it is kept safely, over time, the ink fades away and this requires the need for constant updating and refreshing of the data. With digitalization, the need for such is eliminated, saving money, time, resources, and most importantly, the environment.

- **Speed and Efficiency**

Accessing and organizing data on computers is much easier, resulting in faster and easier access to data from anywhere around the world.

• Cost-effectiveness

When a single computer can be used instead of a room full of papers for the current and the future data, which requires much more maintenance, and doesn't provide as much accessibility, the computer is a cost-effective and modern alternative in the long run.

Having corroborated the supremacy of computerization, we then come to the problems faced by it. Some of the major problems include security of data, storage space, and other miscellaneous problems such as cost of maintenance and health issues. For the first two problems, many solutions have been devised, which include a database or a data archive where all the information is stored. This database can be centralized or decentralized. We shall now discuss each of them in the next section.

Centralized Database System

A centralized database is a type of database where storage, management, and manipulation of data are done at a single central location. This center may be a server or even a mainframe computer, depending on the requirements of the network. All the data from each computer is stored at this single location which often runs around the clock and must be properly maintained. For example, a company implements a centralized database system, then all data processed or produced from its various branches and from each workstation is stored at this sole location.

In a centralized system, users rely on a central authority that can alter or change the system by altering the database. These do not distribute authority and the legitimacy of the system depends solely on the accountability of this central authority.

Advantages

- Data is easily portable and accessible since it is kept in a single location.
- Maximum data integrity as data can be easily coordinated consistently and accurately.
- Storing data in a single location reduces data redundancy and saves space.
- Cost effective, suitable for small organizations and businesses.
- Effortless debugging, simulation, and deployment for application development.

Disadvantages

- Major disadvantage is the breakdown of the central location, which affects all the associated workstations.

- All workstations accessing the data simultaneously increase network traffic and reduce efficiency.
- If central data is corrupted or lost, the entire database will be no longer useful.
- Having all data stored in one place makes it prone and also easier for hackers to target the database.
- If any software upgradation is required to the server, then all the operations occurring on the database must be halted.
- After a certain threshold, the performance will not increase significantly even if the hardware and software capabilities of the server node are enhanced.

Decentralized Database System

As the name itself suggests, the database is not centralized means all the data is not stored at one particular place. Here, the data is distributed and stored at multiple nodes, eliminating the need for a central server. This also means that the system does not depend on a singular and central point of control and hence does not have sole authority. Decentralization means no node has any authority over any other node. A node here refers to any workstation accessing the database. Every node makes its own decision, and the end behavior of the system is an agglomeration of the decisions of the individual nodes. This is an interconnected information system that is consolidated using a peer-to-peer network. Blockchain technologies such as Bitcoin and Ethereum are examples of decentralized systems.

Advantages

- Having multiple storage locations, it does not have a single point of failure. As the information is shared among multiple nodes, breakdown of any one node doesn't impede work as data can be retrieved from any other node. Higher fault tolerance and zero downtime due to redundancy.
- Does not have a sole authority, reducing the trust we put into a single third party. More autonomy of resources.
- No or less censorship as the data is openly available to all the nodes and is not manipulated by a central power.
- All operations and data have transparency.
- All the load is balanced among multiple nodes, reducing traffic and avoiding bottlenecks.
- Some nodes will always be present, increasing availability of data as compared to a single server which must be operating around the clock.
- Difficult to corrupt the data as it has multiple copies.
- Access time of data is faster as different nodes can be created in areas of high usage.

Disadvantages

- In case of malfunction of any node, it is difficult to find it.
- Difficult to coordinate big tasks as no chain of command exists to control or direct workflow of any node.
- Maintaining a decentralized system is quite expensive for small organizations.
- Requires timely optimization, the absence of which results in inconsistent performance.
- Distribution of data increases the risk of data security and privacy as some of the nodes may have lesser security compared to a central server which increases its chances of data hacks.
- Distributed authority can also cause misuse.

From this, we can see that a decentralized system is far better than a centralized system when it comes down to the basic aspect of data access. However, the above text also explains how it may be disadvantageous in the areas of security and autonomy of power. These downsides can easily be overcome with the help of additional mechanism implementations which will establish the supremacy of the decentralized system over a general centralized one. The first can be solved using encryption and the second by putting the consensus mechanism into place, both of which will be discussed in detail later on. One major technology is the blockchain technology which is making rapid strides in the modern era [1].

BLOCKCHAIN TECHNOLOGY**Bitcoin**

Often associated with bitcoin, blockchain was first implemented by Satoshi Nakamoto in 2008 who created the first Crypto currency, the blockchain based project called bitcoin. So, what exactly is a bitcoin? It is basically a Crypto currency that allows anonymous payment transactions of the bitcoin owners over an open and decentralized network using encryption.

Using consensus and cryptographic techniques, it builds a trust paradigm between untrusted users around the globe. It offers lower transaction fees than conventional online payment mechanisms and is operated by a decentralized authority antithetical to government issued currency. However, bitcoin is not a legal tender having no physical form but manages balances on a public ledger and uses peer-to-peer technology to facilitate payments. Moreover, crypto currencies do have their own flaws and forte. Flaws being their volatility of exchange rate making their prices unpredictable and investing in them a huge gamble. They are highly dependent on the blockchain technology making them share vulnerabilities

with its very own architecture. They are also known for their use in illegal activities. Their forte is primarily in transparency, resistance to inflation and elimination of third parties in transactions. Bitcoin is not the only Crypto currency out there, but rather its success has spawned many others including Ethereum, Litecoin, Ripple, Dash, zCash, *etc* [2].

What is Blockchain?

The concept was first introduced when a group of researchers wanted digital documents to be time stamped, so that they cannot be backdated or changed, in order to maintain legitimacy. Broadly, blockchain is a decentralized and distributed digital ledger of transactions that may be public or private/permissioned. Each transaction is stored as a block. Each block contains details regarding the transaction such as date, time, amount spent, product as well as information about who is participating in the transaction. After this block is created, it must be verified by the nodes present on the decentralized peer-to-peer network where the nodes either agree or disagree with each transaction which forms the basis for the consensus mechanism. Once, a majority of nodes have validated the transaction, it is time stamped and given a unique hash storing it onto the database as an immutable record. Then the ledger is updated and the block is added to the database which is the “chain” of blocks. There is no need for any administrator as the blockchain users are the administrators themselves. Each block or entry is linked to a specific user along with their previous entries to maintain a legitimacy record of each user on the network. Over the peer-to-peer network, along with all the users on it, a blockchain system can be controlled autonomously to manage information openly.

As complex as it may sound, blockchain is actually a very simple concept. It consists of a number of blocks connected or linked together with their unique hash values assigned to them. Many transactions can be housed under a single block. This huge “chain” of blocks is the database containing information that is present on each and every node of the peer-to-peer network. The identity of the users is anonymous or pseudonymous [1, 3].

Blockchain Architecture

Basically, as described before blockchain is a chain of blocks containing information forming a database. A copy of the chain is stored in each node of the peer-to-peer network making blockchain secure and original or authentic. All these nodes are linked together instead of a centralized server system making the network decentralized. The first block of the blockchain has no parent block and

is called the genesis block. This does not reference or point to any previous block and is hence a special case. It is often labeled as block 0 in modern versions of bitcoin. Its previous hash is set to 0. This genesis block has its own hash, which is added to every new block added to the blockchain creating a unique combination. The genesis block tells about the origin of that particular blockchain and forms a trust among the miners. Apart from instilling a trust for the authenticity of the blockchain the genesis block is not really necessary. Height of the blockchain refers to the total number of blocks present in the blockchain. The various components of a blockchain include [4]:

Block

Any valid block in a blockchain consists of a block header and block body. The block header contains the following essential components:

- **Block Version:** describes the structure of any block interior as well as the validation rules to follow to enable appropriate reading of the block contents by any node on the network.
- **Merkle tree root hash:** a hash tree or Merkle tree has a cryptographic hash of the block on each of its leaf nodes. The first node's hash is the root hash. Subsequent non-leaf nodes have hashes of their child nodes. It allows secure and efficient verification of the data in these blocks to check for unadulterated blocks sent from other nodes. It is also used to counter degradation and maintain the integrity of data. This is primitively the transaction data that is converted in the form of an alphanumeric fingerprint.
- **Previous hash:** any block contains the hash of its previous block or parent block forming a link.
- **Timestamp:** stores date and time of transaction completion which is immutable.
- **Nonce:** hashing is done using the block header along with an extra number called "number once". It is basically an arbitrary number used for cryptographic purposes. It is used only in proof-of-work systems.
- **Target:** a value based on the difficulty of the blockchain network, which tells miners how difficult it is to add a block to the blockchain. Block difficulty is a number value that tells us the time interval between adding two successive blocks to the blockchain. Higher the difficulty, harder it is to find a hash that works and hence lower the target.

The components of the block header have been summarized in Fig. (1). Additionally, the block body consists of the transactions as well as a counter, which keeps a track of the number of transactions that are stored under the same block. The number of these transactions depends on their size as well as the size of the block [4].

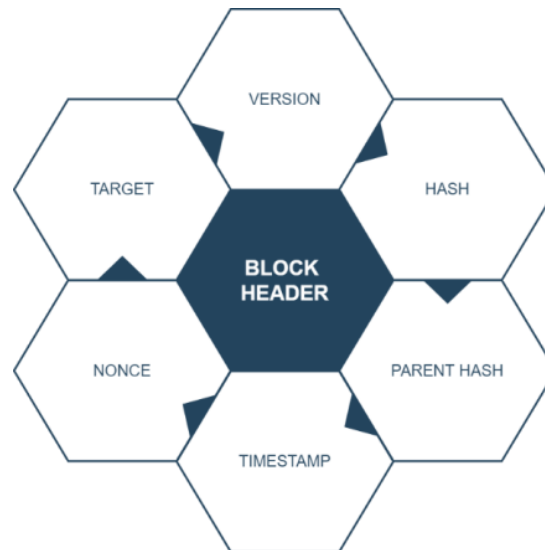


Fig. (1). Components of block header.

2. Nodes: These are the users of the blockchain. Each node is a separate computer system that stores a copy of the ledger containing the complete transaction history of the blockchain. In other words, each node stores a copy of the entire blockchain which is the very essence of a decentralized system. Sharing multiple copies ensures that the main copy complies with the copies present with each node so that there is no illegal altering of the blockchain.

3. Transaction: This is the smallest component of any block which is the backbone of the entire blockchain network. When any of the nodes makes a purchase, the details of it are stored in this transaction.

4. Miners: specific nodes which validate any transaction, verify the authenticity and solve a mathematical algorithm to add a block to the current chain.

5. Consensus: set of directives that regulate the validation of any block to carry out any blockchain operation. The consensus mechanism will be discussed in the next section.

Characteristics of Blockchain

Having talked a lot about blockchain and its rapidly increasing implementation in various fields, we need to know how blockchain is different from the conventional techniques. How the newer technology overcomes the downfalls of its ancestors is what we must focus on. This can be best explained with the help of its key

defining characteristics that makes it stand out from others and makes it an interesting prospective for organizations looking to organize their database making them secure. Blockchain has the following defining characteristics:.

Decentralized

The most defining and key characteristic which forms the foundation of blockchain is its decentralized nature discarding any reliance on a central server/authority or any external untrusted third party which is in contrast to any traditional storage network. This makes it transparent, fault-tolerant and corruption-free by distributing control, eliminating third parties and reducing breakdown probability.

Immutability

Any data once stored on the network is absolute and cannot be changed in any case. It is almost impossible to delete transactions or even undo them once they are added onto the chain. Each node containing the copy also makes sure that the data hasn't been tampered with making blockchain persistent and auditable.

Security

As mentioned earlier, blockchains have no central authority but all the nodes work together to maintain authenticity of the blockchain network. Moreover, each block is encrypted, having its own as well as its parent's hash value making blockchain tamper-proof. More about blockchain security will be discussed later in this chapter.

Anonymity

All users' identities are kept strictly confidential and hence a system of anonymity is maintained. However, absolute privacy is not warranted. Each user can have multiple identities to influence the blockchain which is also considered one of the drawbacks.

Auditability

Each transaction is time stamped and is also linked to its users and record is maintained for that particular user. This ensures authenticity of the block added and legitimacy of the chain. Linking transactions to users also makes the transaction traceable and improves its chances of verification. Public blockchains do not have any authority governing them and hence have the highest auditability compared to private blockchains making them truly decentralized [3, 5].

VERSION CONTROL SYSTEM

Version control systems are software tools that record files onto directories and help track any changes or modifications done to them. They are generally used by software professionals to oversee alterations done to the code base. A separate database is maintained by this version control software to keep track of every modification providing a backup for the data stored. Advantages of using a version control system include:

- It maintains copies of different versions of the code which can later be used to compare the differences and look for further enhancements while also correcting previous mistakes.
- All the developers can work on the code from different locations minimizing disruption to individual members.
- Responsible for the security and privacy of the source code which forms the backbone of every project the team works on. It protects the code from human degradation intentionally or unintentionally.
- Since version control tracks every change, it helps to keep record of individual contributions as well the current work of each individual ensuring that the work done by different developers does not overlap or conflict and thus all changes are compatible with one another enhancing the experience of working simultaneously.
- Even if a person is working alone, he can access the project from multiple devices.

In any version control system, the central database which contains the code, the versions and all related data is called a central repository. This central repository can be cloned by different users onto their systems to work individually on the project. Cloning a part of the repository to work on a particular feature is known as branching while cloning the entire repository to use the entire code as a base is known as forking. These individual copies of the data may not be same, as different developers keep working on and making changes to the code. This personal copy is also called as checkout. When all work is done, the changes made can be committed onto the local repository of that developer. These changes can be merged with the original repository by pushing the commits. It is the responsibility of all members of the team to maintain and work on the latest versions of the code. Getting updated to the latest version can be done simply by a pull request from the centralised repository.

Types of Version Control Systems

A version control system may also be of various types:

Local Version Control System (LVCS)

Does not have any generalized repository but all the files are maintained by the user on his own separate repository or database. It contains all versions or varieties of files known as patch sets in a special format.

Centralized Version Control System (CVCS)

These contain a single central repository and each user works on their own copy of this repository. All changes are committed onto this repository and can be updated by other users on the network. These are easier to understand and work with. Examples of CVCS include Perforce, CVS and Subversion.

Distributed Version Control System (DVCS)

These contain multiple repositories with each user having their own repository called the local repository. Committing changes will only update the local repository and must be pushed to be visible on the central one. All changes must be pulled onto the local repository. DVCS enables offline working as changes are only made locally. Examples of DVCS include Git, Mercurial, Veracity and Bazaar.

One thing we can understand here is that along with blockchain the version control system used will obviously be a distributed one. Having similar characteristics allows blockchain to be implemented along with it. Most DVCS employ cryptographic hashing to secure data. Git uses the SHA-1 hashing algorithm producing digests 160 bits in length and uses hashes for the contents of the file when a commit is made to the repository to ensure integrity of data at any point of time. It also uses hashes as database keys to find data as well as helps in DE duplication of data by comparing hashes of different files. So, files having same hashes are redundant and not stored again, thereby saving space. Therefore, it is essential to choose a good hashing function, one that does not generate the same hash for different data known as collision and the SHA-1 function has never generated a collision.

DATA STORAGE

With growing computerization, information is being digitalized increasing the demand for a place to store this data. With the requirement of large amounts of

storage, massive data centers come into picture storing data on huge computers in various formats. Next comes the demand for the accessibility of this data, further transforming the field of data storage with the arrival of cloud storages storing data on cloud servers. With innovative ways to store data also come innovative ways to steal or tamper it, arising the need for enhanced data security to avoid data breaches and hacks. Mix blockchain in and you have another great alternative with enhanced access, security, support, trust and reliability. As blockchain encrypts data for its security and has numerous nodes looking over it for any malicious activity, data breaches become far scarcer and requires very high skill, funding and computational prowess.

Data Storage Frameworks Implementing Blockchain

Blockchain is a relatively newer concept still in its budding phase. It is still being experimented in various fields and hence is constantly developing. The predicament in the field of data storage is the biggest hurdle impeding further development and requires technological solutions to further its advancement which may help blockchain be more widely accepted. Blockchain with its “revolutionary” technology can be inculcated in almost every industry but it also needs a data archive to work on which is dynamic enough to utilize its quiescent potential. Unless the obstacle for data storage isn’t solved blockchain can’t make any massive impacts on the real-world industry. There exists no ideal or universal solution but rather depends on the magnitude of the database or of the users accessing it. Databases maybe decentralized or centralized and cheap or expensive, and choosing one depends on the requirements and affordability. The most significant problems faced by data storages implementing blockchain is the high cost and limited accessibility. Storing only small amounts of data like that incurred by transactions alone is feasible while storing large files is out of question as it causes a problem called bloating. This small amount of data is the metadata which consists of only the basic essential information like location and hash. These storage costs are levied by the existing blockchains like Ethereum, Ripple or Hyperledger Fabric. Anyone cannot create his own blockchain since there are a number of drawbacks in doing so. Any blockchain’s trust factor lies in its length, number of active nodes as well as the authority given to each node. The creator of the blockchain tends to retain control over it making it hard for new nodes to join thus making the creation of a new blockchain an arduous and time-consuming task. So, the only feasible solution is to adopt a more versatile method of data storage. The true sense of blockchain lies in a decentralized storage bringing P2P networks into the limelight.

Blockchain promises decentralization and the immutability of its records, making it well-liked not only by FinTech companies but also travel industry, healthcare provider, and computer giants such as Amazon, Microsoft and IBM for cloud storage. In the FinTech industry, an average of 30,000 transactions is processed per second. Bitcoin blockchain is only able to handle 3-7 transactions per second, whereas Ethereum blockchain can store up to 12-30 transactions per second. Even though it may be more secured in the present day, these blockchains cannot be a substitute for day-to-day transactions as they are comparatively slower than conventional transaction processes. This is because blockchain is based on P2P networks [6].

Sharding is a concept which has already been implemented to improve the efficiency of databases and to improve the scalability and reliability of blockchain.

Sharding

Sharding is breaking down the database into smaller manageable chunks called logical Shards or simply shards. These shards are stored onto different nodes of a P2P network. Each shard is completely distinct and independent of other shards, though in some cases replication of data maybe required (referenced tables) [7, 8]. Sharding improves the scalability of an application. It makes the database capable of holding more data and can handle more queries resulted due to traffic surge. We are storing data on a database that is on one server. But when the maximum limit of the server is reached, there is no way to expand the database as it is not possible to combine the computational powers of multiple computers for a single operation. Sharding would increase the capacity of the database, as there would be room for more datasets by storing the data on multiple nodes. For an application having larger database, running a query would be quite costly because searching every row would be time-consuming. However, by sharding a database into multiple databases, the query only goes through only fewer rows hence speeding up the query responses. Moreover, maintaining a network of smaller servers would be more cost-efficient than a larger server, at least in the longer run [7]. Suppose if there is a power outage, an unsharded database will not be functional and the entire application will be unavailable. With a sharded database, only some parts of the application won't be available to users as other sharded databases continue to operate with no issue.

Sharding mainly divides the database horizontally. For example, one shard might be responsible for storing only transactions on a particular day. In horizontal sharding (horizontal scaling), we do not have to pre-plan on how to cut databases. We can scale dynamically and efficiently by adding more machines. Sharding

partitions the blockchain network into independent shards such that duplication of data storage can be avoided for each participating node, therefore distributing the workload among the nodes such that each node is only concerned about its shard data. Every node thereby has only part of the data and not the entire information. Since, blockchain now exists in smaller segments, transactions happen in a parallel manner rather than linear [9]. TPS (transaction per second) thus increases. It also removes the need for all the nodes on the network, making it faster and reducing latency. Information of each shard is allowed to be shared among the shards, making the blockchain decentralized and accessible by all users. Hence helping with the issue of scalability and improving the quality of service provided by blockchain.

In Fig. (2), the blockchain is partitioned into three shards. Each Shard maintains its ledger, storing the records of transactions. A Cross-shard communication protocol is essential for synchronous communication among shards, like in the case of validating a cross-shard transaction.

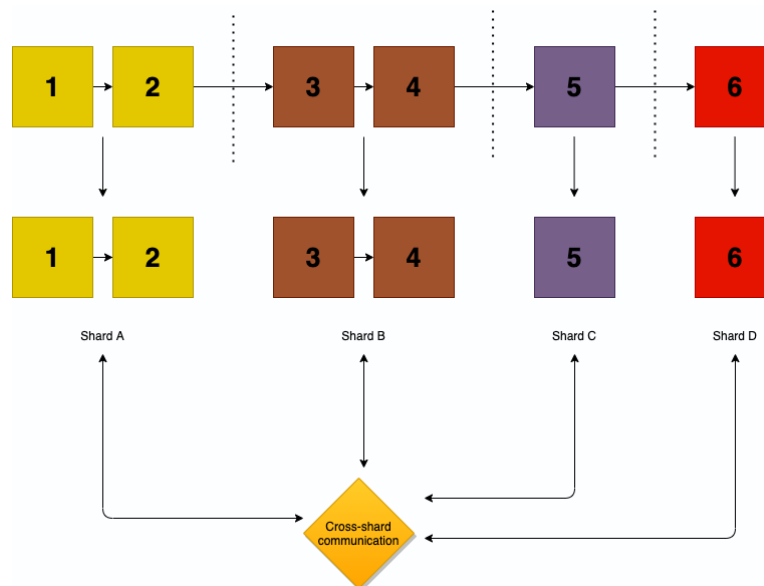


Fig. (2). cross-shard communication.

The **POW** mechanism* is the most widely used consensus mechanism. However, it is not used with sharding because each participating node has the information of one shard. **Proof of stake (POS)*** is the consensus algorithm for sharded blockchain. For each shard, a miner is chosen to execute the transaction validation [6]. The blockchain is secure as the miner selected is loyal. The time taken to valid transactions is a lot lesser and also economically viable to the miners.

Drawbacks of Sharding In Blockchain

1. Sharding would result in separate blockchain networks. Users on a particular subdomain cannot access an application on another subdomain and vice-versa without a communication mechanism among the shards. It would make the system more complex [7].
2. Hackers can take over control of shards. They can easily corrupt them. Also, they might store invalid or false data. This is known as a **single-shard takeover attack or a 1% attack**. Ethereum has proposed random sampling, meaning reassigning nodes to particular shards at random intervals of time. Corrupting the shard now becomes a lot harder.
3. Sharding is commonly used in a privately owned network. Implementing it in a public blockchain is still a challenge.

Alternatives to Sharding

1. ***Increasing the block size*** could be thought of as one alternative to sharding. But this is only a short-term solution. By increasing the size of the block, we can store more transactions hence number of TPS would be higher. As the size of the block increases, more computation power would be required by the node to verify the block. Computer equipment for such a requirement does not make it economically viable for nodes. Thereby the number of nodes on the network decreases and the network becomes more centralized and vulnerable to 51% attack.
2. ***Off-Chain Blockchain***: Blockchain does not store the contents. The miners provide their hard disk to save someone else data. They are rewarded with crypto tokens to motivate users to lay off their spare disk space.

Blockchains Using Sharding

As we know, the biggest downfall of implementing sharding in a blockchain is no communication among individual shards. Also, there is no logic to split them in a random approach if the nodes have a general distribution and are geographically widely spread. Random sharding would require smooth communication among nodes for the successful implementation of sharding. As of now, there exists no definite protocol so the individual shards can communicate with each other. Ethereum blockchain developers are having complications resolving it.

However, Zilliqa is the first public blockchain to implement sharding, ensuring no difficulty to be encountered while sharing information among shards. It has achieved 2828 TPS, which is higher than Ethereum and Bitcoin blockchains. Zilliqa doesn't shard the nodes completely. It implements two types of data. One stores the state of blockchain. It is small on storage and integrates with all nodes on the network easily. The other is the history of the blockchain which is bulkier and sharded. This history can be queried by inter-node communication to obtain the necessary information from the relevant shards allowing Zilliqa to be scalable and decentralized at the same time. Near is a blockchain ecosystem allowing developers to make and deploy decentralized applications also called Dapps. It calls itself a "sharded, developer-friendly, proof of stake blockchain". Sharding makes nodes remain small enough to run on cloud-hosted instances and maybe mobile phones in the future. Facebook has proposed a blockchain-based payment system, Libra, which might use some form of blockchain partitioning. The development team from Chainspace, recently acquired by Facebook, is mainly focused on blockchain sharding [10].

P2P NETWORK

Peer-to-peer network (P2P) is a network of computer systems that can exchange files and data directly with each other without storing it in a separate server (client-server model). P2P enables any two computer systems or more to interconnect with each other without any intervention of a third party. In such a network, each computer system is called a node or "peer" [11]. It can take the role of a client and a server as well. Privileges and the distribution of tasks among the nodes are equal. InterPlanetary File System (IPFS) is an example of P2P network used in blockchain.

Let us understand file sharing on a P2P network with the help of BitTorrent. The BitTorrent platform is built on the P2P network. On BitTorrent, sharing and downloading files can be done efficiently. The computer that stores the data to be shared or downloaded is called **seed**. It then splits the file into a lot of pieces. Any node on the network who wants the file uses the BitTorrent client platform. This node would receive one part of the file. Over some time, it would receive the remaining chunks from other nodes. At a particular time, a peer would be downloading parts of the file that it does not have and simultaneously uploading other parts to some other peer on the same network. There is no sequential way for it. It is random in the process. Hence at any time, cooperation is required among the peers. Such a group of nodes is called a swarm. An enormous swarm means a popular file. The cooperation among peers makes the overall process faster. Eventually, every client on the network receives a complete copy of the

file. Seeding is the process of uploading files to other nodes on the network once your copy of the file has finished downloading. However, quitting the swarm after your download is complete is called leeching. If every node leeches, BitTorrent would not work at all [12].

Types of P2P Network

Unstructured Network

An unstructured network does not follow any specific structure. As shown in Fig. (3), nodes which are depicted by circles, are connected randomly to each other. A new peer who wants to join the network can copy existing links of another node and forms its links over time. It is easy to build an unstructured peer-to-peer network. However, not having a definite structure is its limitation. A peer floods the network with queries to find desired data. At times it becomes difficult for peers to find out the desired data. Flooding of queries does not always give desirable results and hence becomes a bottleneck for network traffic.

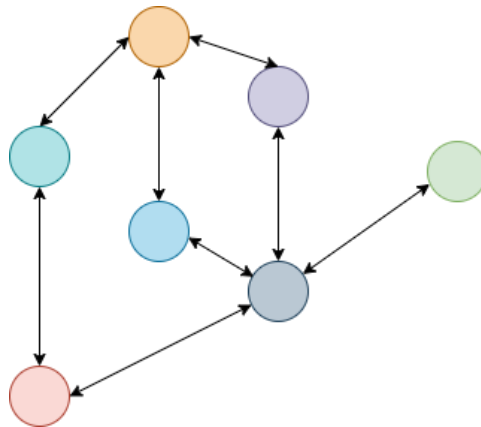


Fig. (3). Unstructured peer-2-peer network layout.

Structured Network

Structured peer-to-peer network overcomes the issue of unstructured networks by maintaining proper structure. The most common type of P2P network implements a distributed Hash table (DHT) [11]. It maintains the information in the network. A hash function is used by this network to assign values to all the content residing in a peer. Thus, hash table (Key, Value) determines which Peer is responsible for which content. Whenever a Peer wants to search for some data it uses the Hash table (Global Protocol) to determine the Peers responsible for the data and then directs the search towards the responsible Peers. Hence, we get good network traffic in this scenario [13].

As we can see in Fig. (4), hash value is assigned to the content inside every node (circle) in a structured peer-2-peer network and stored in the Distributed Hash Table (DHT), used to locate the node and its resources.

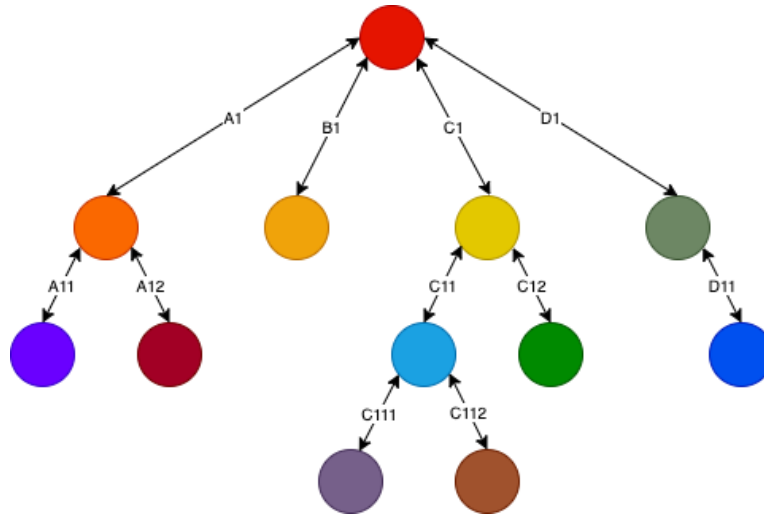


Fig. (4). Structured peer-2-peer network layout.

Hybrid P2P Network

The hybrid model is a combination of pure P2P network and client-server model. The central server in this model keeps the information of peers helping peers to find each other. Currently, hybrid networks are better than both pure structured and unstructured P2P network in terms of performance [11].

In the client-server model, the client would request data retrieval from the server *via* the internet. If the server accepts the request, then it sends data packets back to the concerned client. The client does not have to share any of its resources. For example, a user wants to download some files from a website. The computer of the user is the client. The server provides it with the required resources.

Now consider a scenario where many users want to download the same file from the same website. The server would have to provide each client with a copy of the file so the working of the server becomes costly. Since all downloading is taking place at the same time, the server divides its power so that each client receives the file slowing the downloading speed. But in a P2P network, each node is a server and client when a client needs a lot of data than several other nodes collectively provide it. Therefore, the client can download data at a faster pace. A loss of connection between server and client in a centralized network would cause failure.

However, in a decentralized P2P architecture, all connections among the nodes must be broken to prevent complete data sharing.

The participation of peers in the network should be encouraged. Cooperation among them is vital for storage performance. The selfish behavior of any node would hamper the performance of the entire P2P network. It might be limited resources like storage and bandwidth that provoke such a self-centered attitude in peers. Data retrieval at any time is the prime goal for a P2P storage network [14]. Since there is no centralized server, all data should be available to peers present on the network even though some peers might be inactive. Availability of data can be made sure by various data redundancy processes.

Even a P2P storage system is vulnerable to various attacks. Let us look into a few of them and try to understand different possible defense mechanisms:

Denial-of-Service (DoS) Attacks

DoS attacks can interfere with the storage application on the network leading to loss of services. It may use security measures such as verifications to carry out its attack. The attackers flood the target node with verification requests preventing sincere traffic on the network. Such is the most common form of DoS attack on a P2P network. DoS attacks are unquestionably hard to block as the number of computers the attacker involves is enormous, making it burdensome to trace back the attacker's origin. "Pricing" is commonly used to curb DoS attacks. It requires its clients to solve a complex puzzle that usually requires expensive computation. If the system senses to be under attack, the difficulty of the puzzle should be increased. It would reduce the magnitude of the attack [15]. However, this is only useful for smaller attacks but would fail against a massive distributed attack. Also, honest clients would require more computation power to solve puzzles that are not economically feasible and will waste a lot of power.

Man-in-the-Middle Attacks

In this attack, the attacker inserts himself in a network node and does not reveal itself. It spies and influences the communication among these nodes. It may be responsible for spoofing and transmit false data in the network. It can also farm some private data and leave the network unsuspected. In a P2P network, it is impossible to identify a man-in-the-middle attack as there is no central authority for the network. Fortunately, this attack is useless in a P2P network. Nodes have same logic for authentication and data is shared to every node on the network. Ultimately spoofing becomes useless. However, if the authentication logic varies in the network, the implication of this attack would depend on the logic itself [15].

Disadvantages of P2P Network

- Security in P2P architecture is very minimal. Viruses, spyware, and other malware can easily intrude into the network. They can move from one peer to another during file sharing.
- Data recovery is demanding in such a network. The backup of the node has to be on separate devices. If something unfortunate happens to the workstation, all the files on it are lost. There is no retrieval of these files unless a backup is available on some other device.
- It is difficult to retrieve an unpopular file from a P2P storage network. Such files may have been deleted or are not shared among peers.

Layered Structure

Any distributed system such as a P2P network has a layered structure with each layer performing different roles. The layers of any distributed system must include:

Identity Layer

Content must have a unique identifier for its recognition and distribution which is enabled by hashing the public key. A unique id is generated for each node on the network which forms its identity.

Data Layer

Organizes the data in the network most commonly using Merkle DAG which stores and links data.

Data-swap Layer

Nodes maintain communication by swapping data among each other. Promotes nodes to contribute by sharing instead of only receives data. IPFS uses Bitswap which is based on BitTorrent protocol.

Network Layer

Promotes connectivity among different nodes and enables file sharing/transport, most commonly using Libp2p.

Routing Layer

Sharded data is distributed and maintained using DHT. This layer helps in location and accessibility of each piece of data in response to queries made by communicating with these DHTs.

Consensus Layer

Ensures legitimacy of ledger and maintains consistency by providing a layer of security where all nodes in the network must consent to changes made.

Incentive layer

Any decentralised network needs active participation for its survival. This layer encourages genuine nodes to participate by providing rewards for their work and punishment for faults *via* currency system [16].

Libp2p

Libp2p is a network framework that has a modular system of protocols and libraries allowing us to write and develop peer-to-peer network applications. P2P certainly has more advantages than the client-server model although there exist certain challenges that need to be overcome by adopting apt practices. The transport layer of the network is responsible for receiving and sending data from one peer to another. It uses more than one type of transport protocol for the execution of applications at varying runtime and network environments. It promises a secure transport channel that supports numerous methods of encryption communication. Libp2p uses public-key cryptography for the identification of peers giving it a globally unique name called peerID [17]. Retrieval of public key is possible from peerID enabling secure communication among peers. Since it is needed to work on multiple networks, there should be an appropriate addressing scheme. Multi address is an encoded address for multiple networks. It is known as a “future proof” path structure.

INTERPLANETARY FILE SYSTEM (IPFS)

To put it simply, IPFS is a distributed and decentralized P2P storage network for storing and accessing data. IPFS enables data storage at peer computers using sharding instead of being present only at one single location. So, when one user on the network asks for that particular data, instead of requesting the server to deliver it, the data can be retrieved from the nearest computer on the network which has a copy of that data. This enables load distribution on the central server preventing bottlenecks and also serves the request faster. For example, if there are

multiple requests from India to a server based in California, then the standard procedure will be to make all these requests and generate equal number of responses making the whole process time-consuming and wasteful. IPFS instead shares copies of already received response to each of these requests which makes the process much faster and the server does not have to work as much. For this very purpose big companies maintain CDNs or content distribution networks but IPFS enables it for everybody removing this financial constraint. This also makes sure that the data is not managed and manipulated by a single organization. It also shares all the benefits of any decentralized network discussed so far including fault-tolerance, tamper-proof, accessibility, data persistence and censor-proof [5, 18].

IPFS Functionality

Being a P2P network, data is accessed through the peer network depending on user participation. Any peer located anywhere in the world can store and relay data forming well-connected network. Storage and access depends on the storage procedure of data, data linking and data discovery for its access. All of this wrapped together forms the IPFS ecosystem [19].

Content Addressing

Normally while accessing data, searching for it is location-based and is called location addressing done using URLs following the Hypertext Transfer Protocol or HTTP. It finds the location based on IP address. If we do not know its location, the data is lost. However, the IPFS network identifies data based on its content rather than its address which is known as content addressing. Every fragment of data following IPFS protocol has a CID or a content identifier which contains its unique cryptographic hash obtained by passing data through SHA256 hash function and a codec which tells us how to interpret that data helping in its encoding and decoding. This hash is made by converting the content itself into alphanumeric hash making it unique. Identification and verification of this data is done by comparing CIDs of the sender and the receiver using multihash. This is a type of multiform, which ensures that the data is accessible even if the hashing algorithm is compromised by allowing multiple versions of the CID generated by different hash functions to coexist, thus retaining security. Here, each CID is unique for its hashing function. This hash also facilitates data linkage. If any user has multiple copies of the same data, then all the copies have the same hash, helping avoid redundancy and conserving huge amounts of space. This is one of the special properties of IPFS called de-duplication [19, 20].

Content Linking

Data on the IPFS system is stored in an object which can store up to 256kb of data. For bigger files, they are simply broken down into multiple objects and all of them are linked together using IPLD or interplanetary linked data. IPLD is a standard based on the Merkle DAG which is a decentralized data structure and links all the objects to the base CID. IPLD is a set of tools for creating links between content-addressed data including IPFS files, commits made in VCS or blocks on any Blockchain. It also permits data access irrespective of the protocol, so internet protocols don't act as barriers for IPLD to function allowing cross-protocol operation of data. Each object consists of:

- Data – unorganized binary data having max capacity of 256kb.
- Links – structures linking all similar objects together. This further consists of:
 - Name of link.
 - Hash of the linked object.
 - Total size of all linked objects.

IPLD is protocol-independent, cross-format, easily upgradable and links all data together which brings out the true meaning of decentralization. As each object contains its own hash, it makes the data immutable similar to blockchain. The data can also be changed by versioning same as in the case of blockchain. However, changing data means a change in CID disabling users from accessing data using that CID. This means that the users will need a new CID each time some update or improvement is made making the link immutable. To overcome this problem, IPFS implements Interplanetary Naming System (IPNS), a universal namespace, which simply causes the old CID point to the new one by linking the new CID to the fixed IPNS link. Now, even if the users only know the old CID, they can still access it. Another problem solved by IPNS is making the link understandable by humans and easy to remember the same way DNS does in location-addressing by mapping IP addresses to a domain name. So you can search for the data either with its IP address or with its domain name. Main difference between the two is IPNS uses public hash key while DNS uses domain names although both have the same structure [19, 21].

Content Accessibility

The data, being stored in organized objects, is structured making it capable of being interpreted by machines. Each object is encoded in triples and these entities are unified through relationships expressed *via* these triples using semantic web technologies like Linked Data. These basic units called triples are simply

information written or more appropriately codified in a specific predicate known as the subject-predicate-object expression in the semantic web which is a standard, promoting inclusion of semantic content on the web converting all unstructured or semi-structured data into structured data so that it can be interpreted independently by machines without human intervention. This semantic web stack uses the existing W3C RDF as a base and builds upon it. This structured data after schema markup and unification can be published across different locations on the internet using the method of Linked Data. All data on the semantic web is linked together so that the “web of data” can be explored because when we have a small portion of data, it is always linked to some other related portion of data.

Coalescence of several triples forms a knowledge graph published in a format called linked data which is a way to interlink all the unstructured data on the web into structured format allowing to query them in a logical manner. This knowledge graph containing a cluster of triples is a massive structured dataset stored in RDF format and is accessible through querying using the semantic query language named SPARQL. Without the knowledge graph, huge amounts of data cannot be managed suitably and efficiently. They are crucial in retrieving data stored in distributed and decentralized networks and are an inexpensive solution to enhance performance. Colossal corporations like Google, Facebook and Microsoft have adopted knowledge graphs as part of their architecture. Semantic Web is truly powering up the web providing open and fast access to information.

Data discovery on IPFS gives special focus to distributed hash tables (DHTs) which are used to coordinate and manage metadata in most p2p systems. It is an archive containing key-value pairs, and this archive is divided into nodes and spread across all the peers in the distributed network, interlinked *via* an overlay network. In a DHT, each node has a key, a unique hashed identifier, which can access and retrieve its associated value. Being distributed, it is highly compatible with similar decentralized systems like IPFS and sharing similar advantages like fault-tolerance and scalability. It was first brought into action by early p2p file-sharing systems such as BitTorrent, Freenet, Gnutella and Napster where some are more decentralised than others. DHT implementation in IPFS is based on the Kademlia DHT.

Accessibility of this stored data can be significantly improved by documenting the data which helps in its easy access. This method is known as schema markup which is basically a semantic vocabulary for data, helping convey meaning behind the content. So, search engines return results based on the meaning rather than the keywords. Consider the example, where someone hosts a website. Then he/she will want more viewers to visit that website. To serve this purpose, the content

undergoes schema markup which helps search engines deliver more accurate results when someone searches for a particular keyword. This also helps the website climb up the SERP rankings allowing it to be displayed at the top when searched thus increasing its popularity. The most extensively used schema markup is schema.org developed collaboratively by Google, Yahoo!, Bing and Yandex who rely on this markup to return search results.

Semantic web is now playing a significant role in artificial intelligence and machine learning as well as in the pharmaceutical department, telecommunications by companies like BBC to make their content more visible through data linkage. It is also used extensively by social media platforms to allow meeting more people. This can be experienced on 'Facebook' in the form of mutual friends, whom the user doesn't actually know but is brought in contact through content linking. Or even on Instagram, looking at one post fills up your recommendations section with similar content made possible through data linking not on the basis of titles but rather on the content itself. Another field of use is by the government to make official data open and transparent [19 - 21].

Deeper analysis of IPFS: Networking

Nodes in the IPFS network need to constantly communicate with each other. IPFS can utilize any transport protocol and implements ICE NAT traversal techniques for node connectivity. As we have seen, Libp2p is an important foundation in the development of peer-to-peer network applications. It is basically a collection protocols or a modular and extensible networking stack to solve many challenges of peer-to-peer applications like content discovery and movement. Being a modular system, the whole IPFS is made of Libp2p modules. It is a key to connect the network by helping in content routing, discovery and transport as well as peer routing. It is an example of process addressing that has developed a horizontal OSI model changing guidelines for communication. The conventional vertical model as described in ISO/IEC 7498 is implemented in multiple layers making data difficult to access due to lack of its visibility being tightly packed together. This makes network up gradation even harder and discourages its improvement. Libp2p changes this framework describing the networking system operability to be spread out where all protocols co-exist. Libp2p is a crucial component of IPFS making its debut as part of the IPFS project which uses it as its networking layer. Its implementation can be done using JavaScript, NodeJS, Golang, rust and will also support Haskell, java and python in the coming days making it even more versatile. Growing out of IPFS, Libp2p can also be used in other projects as their networking layer and is not limited to IPFS [19, 20].

To summarize, data is stored on a p2p network on peer computers instead of a centralized server. The IPFS stack uses or applies the stored data. The data is named and defined for access and security by standards like IPLD and IPNS. Data discovery mainly relies on distributed hash tables (DHT). Finally, Libp2p handles data movement helping in content and peer routing and forms the networking layer.

Implementation of blockchain on IPFS: Filecoin

After all is said and done, IPFS is only a framework and requires some sort of an incentive to truly implement it. Similar decentralized networks can be layered and function hand in hand. One example is the implementation of blockchain using an IPFS system. IPFS depends largely on participation which means more active users generate a better network. Therefore, implementation of IPFS on a large scale is necessary for it to revolutionize the internet as it is today.

One trending example of blockchain over IPFS is Filecoin founded by the same group of people that founded IPFS, protocol labs. Filecoin is built on top of projects like IPFS, IPLD, Libp2p and multiformats. It is a p2p file storage and distribution network with built-in economic incentives to guarantee efficient and reliable storage of files on its own blockchain. Being a peer-to-peer network it lays down a decentralized protocol to store files on space provided by storage miners. Basically, any peer participating on the Filecoin network can provide storage space on their computer and get paid for renting out disk space provided sufficient proof that the files haven't changed. Similarly, peers can also buy storage space from other peers. Payment is made in the form a native Cryptocurrency introduced by Filecoin also known as Filecoin (FIL). One major elimination is the requirement for users to solve complex mathematical algorithms as part of proof-of-work. The Filecoin protocol handles requirements for storage providers so that they don't need to design API for their own storage or advertise themselves to invite potential customers. Filecoin holds a certain promise being the largest fundraising ICO to date where around \$257 million were raised in both presale and ICO combined. It is very likely to make history as the fastest, newly live blockchain to reach a market capitalization of over \$1 billion according to coin desk. Having its mainnet launched just recently on October 15, 2020, it is one of the fastest growing areas in decentralization.

Structure of the Filecoin Network

The basic structure contains 4 essential components:

1. Network

It consists of p2p system using IPFS and implements blockchain where all transactions are stored. Peers on this network can audit storage offered by miners who can also create new blocks to get rewards.

2. Storage Nodes

These are storage miners which provide the spare storage space called sector on their computers and are rewarded in FIL. These sectors have unique ids for recognition and must be pledged to the Filecoin Blockchain before they can store any data. Storage miners are required to constantly provide proofs for storage of client outsourced data for a period of time which can be reviewed by everyone to build trust on the miner's legitimacy. This is done by abiding to proof-of-spacetime (PoSt) mechanism which is submitted to the network before mining a block. Miners must also adhere to proof-of-replication (PoRep) to prove that they are storing the data mentioned and it is encoded in a unique way where no other miner can replicate it.

3. Retrieval nodes

These are off-chain miners responsible for data retrieval or fetching from the client or the storage miner. Client data can be divided into small pieces and stored by different storage miners. Retrieval miners receive payments from the client in the form of micropayments for each piece of data.

4. Native token

This is the native token system or Crypto currency developed by Filecoin also known as Filecoin (FIL). All transactions made between clients and miners are done using this [22, 23].

Data Storage and Retrieval Protocols

Storage miners can pledge their sector on the blockchain by specifying their sector size and depositing a collateral for that particular pledge. This collateral is used when any storage proof is missing. These storage miners can then supply an ask order which specifies the cost of service. A client can encrypt his data before storage to maintain security and can choose any storage provider by submitting a

bid order specifying how much he/she intends to pay. All these orders are recorded on a separate Order book maintained by Filecoin to prevent bottlenecks on the blockchain. When both the orders match, a deal can be made between the client and the storage miner. This transaction is then recorded onto the blockchain. As the data pieces are stored, an allocation table keeps track of these pieces and its associated sectors. This allocation table is updated at every block and its hash is maintained on the newest block on the blockchain network. Data is then transferred from the client to the miner, the completion of which it is verified to make sure it matches the deal parameters. Once the data is recorded on-chain, the miner must generate a proof-of-replication and seal the sector to maintain security. Sealing is a set of operations to transform that sector into a unique replica of the original data which is associated with the Filecoin miner's public key [24]. This sealing process is necessary for miners to submit continuous proofs. Clients can achieve fault-tolerance for their data by replicating the data they have stored causing redundancy. Data can then be retrieved by retrieval miners, before which the sector must be unsealed. Some Filecoin clients like lotus maintain unsealed copies along with the sealed ones for faster retrieval of data. However, this is not a verifiable part of the protocol although it is a useful feature. The data is then transferred back to the client. The payments for service are made off-chain through the order book and using the blockchain only when disputes arise [23].

Fault Tolerance

Filecoin implements byzantine fault tolerance where faults can either be management or storage byzantine faults. Storage providers on the network need to provide constant proofs for the storage of the outsourced data which validated by a byzantine agreement (BA) used to audit these providers. This BA can tolerate up to $f < n/2$ faulty nodes where f is the number of faults and n is the total number of nodes. These management faults are byzantine faults in the manage protocol and are (f,n) -tolerant. We can see that it has better fault tolerance than conventional byzantine agreement which can tolerate up to $f < (n-1)/2$. The violation of this agreement can get the miners slashed and the content redistributed.

On the other hand, storage faults are byzantine faults in Put and Get protocols which prevent clients from retrieving data. If the BA can tolerate f faults and has m independent storage miners, then the put protocol is (f,m) -tolerant [23].

Why the Hype Around Filecoin?

We already know the advantages of decentralized system over a centralized one. Filecoin being decentralized shares all of those in addition to its specific advantages that set it apart from its competitors. These include:

1. Scalable and Economic

Filecoin doesn't need new protocols and standards but rather builds on existing ones allowing them to be easily integrated into modern systems. It also doesn't require a different API for each provider. It also doesn't require extra storage systems but makes use of existing ones.

2. Low Cost

Solves the biggest problem of current blockchain networks, expensive storage. Having millions of computers interconnected, pricing is not corporate but depends on demand and supply. More the number storage miners competing, cheaper is the storage.

3. Security

Overcomes uncertainty over storing files on an unknown computer by sharding. These pieces can later be accumulated by the retrieval miners. Clients can also encrypt their data for added security.

4. Dynamic network

Ensures proper storage of files. Constantly searches for faulty miners, on discovery of which slashes them and redistributes data to reliable miners at the same cost through process claimed as self-healing.

5. No computation

Miners don't need to perform heavy computations as in the case of other blockchains implementing proof-of-work. Anyone with a computer and storage of any specification can participate without the requirement of expensive computational power.

6. Expansion of existing blockchains

Can provide storage to other blockchains as well which face storage issues. Blockchain will function as usual but data will be stored on the Filecoin network. May also support interoperability with other blockchain transactions in the future.

7. Easy migration

Since it doesn't use specific features unique to it, users aren't locked in by have the freedom to migrate to a different provider as they all use the same protocol and API. Also made possible with an active retrieval market.

8. Open-source code

Any development can be contributed by anyone.

Any disadvantage associated with Filecoin is shared with all decentralized networks which includes sharding. As data is broken up it needs to gather each piece from multiple servers. Any of the servers being down affects the latency and reduces the speed of data retrieval. Other drawbacks include extra overhead generated by the system of micropayments where payments are made for each piece which may impede the retrieval protocol reducing speed of retrieval. Also resistance to censorship will lead the data unchecked which may bring illegal content to the surface. However, speed of retrieval depends majorly on the physical device used by the storage miner, the solution for which could be in the concomitance along with IPFS as a caching layer giving rise to hybrid systems.

However, today's market is highly competitive with someone always ready to overthrow existing technology. Filecoin is not unique but has many competitors including Storj, symbiont and Sia among many others, the variations among which have been laid out in Table 1. While Filecoin and Sia maintain their own blockchain, Storj uses the Ethereum blockchain. However the competition as existing norms stays over a long period only if they are constantly evolving. Eventually, the success or popularity depends on how versatile, adaptive and user-friendly the network is [3, 20, 22].

Table 1. Variations between different decentralised storage networks.

-	Blockchain	Native Token	Max Token Supply	Token Limit	Consensus	Content Distribution
Filecoin	Personal	Filecoin (FIL)	\$2 billion	Capped	Proof-of-replication Proof-of-spacetime	Storage and retrieval Markets
Storj	Ethereum	STORJ	\$425 million	Uncapped	Proof-of-retrievability Proof-of-redundancy	Public Buckets (Satellite caching)
Sia	personal	Siacoin (SC)	\$425 million	Uncapped	Proof-of-work	Skyenet

(Table 1) cont....

-	Blockchain	Native Token	Max Token Supply	Token Limit	Consensus	Content Distribution
Swarm	Ethereum	Honey	\$100 million	Uncapped	Proof-of-work	Autoscaling elastic cloud (Node synchronization)

Swarm

Swarm comes in the same category being a “decentralized storage and communication infrastructure” similar to Filecoin and implements very similar architecture. It operates on the Ethereum blockchain similar to Storj forming a native base layer service for web3. Since, Ethereum allows decentralized applications or Dapps to run on their blockchain, swarm also supports Dapps by providing a local HTTP proxy API which can be used by these Dapps to interact with swarm. Similar to instances seen so far, swarm also implements content hashing, with a 32-byte hash using Keccak 256 SHA3 used all over Ethereum, which is made mutable through Ethereum name service or ENS contrary to Filecoin which implements IPNS being based on IPFS. However, both ENS and IPNS have the same objective, which is to provide domain name resolution. Swarm inherits all its protocols from Ethereum implementing same incentive, networking and consensus layer. Swarm is an extensible and configurable infrastructure allowing clients to implement their own protocols and has its storage servers on the Linux OS making swarm highly scalable. It also uses devp2p rlp suite by Ethereum as its transport layer instead of TCP, but may transition entirely to Libp2p in future updates. Content discovery is done using kadmlia DHT similar to Filecoin for peer routing and discovery. Routing layer being the Distributed Preimage Archive (DPA).

Like any other p2p network, swarm also provides economic incentives for its network participants by the contrivance of crypto economics to define its rules and protocols and reward its users accordingly. Its incentive system consists of accounting protocol (SWAP), file management and litigation. It has its native token called honey, and being implemented on Ethereum is ERC20 compatible. Users are rewarded based on their active participation on the network also called proof-of-participation which forms its incentive layer (Table 1) [25].

BLOCKCHAIN - PRIVACY

Data, be it our social media details or a company’s stock details, is an incredibly important asset which needs to be kept private and secured. If this data is leaked,

it could lead to security issues and can also lead to capital loss to the individual or business. The amount of data in our world is rapidly increasing which leads to a greater concern in user privacy. In 2013, a data breach had taken place at Adobe where a hacker had stolen encrypted customer credit card records of millions of users. In 2015, it was reported that Facebook allowed an app which collected millions of user's personal data without their consent which was supposed to be used for political advertising. The app collected the psychological profiles on the users. In first 6 months of 2019, there were more than 3800 publicly disclosed breaches exposing a total of 4.1 billion compromised records. These are some of the millions of cases of data leaks because proper security measures were not implemented.

Sybil Attack

A Sybil Attack is when a node uses multiple nodes to take control over the entire network; generally the number of nodes is greater than 51% of the total nodes in the network. Once the hacker has control over the network, they can compromise the data stored in the network by adding fraudulent blocks to the ledger, and gain access to all the private data in the network. Over time, the hacker can also vote out the honest nodes by creating enough fake nodes [26].

51% Attack

Similar to Sybil Attack, the hacker gains complete access to the blockchain by controlling more than 51% of the nodes in a network. In case of Bitcoin, they can reverse the previously completed transactions which can lead to 'double spending'. To prevent these kinds of attack on the network, blockchain implements multiple techniques to its framework that leads to better security and privacy [27, 28].

Data privacy refers to how a piece of information is handled to protect it from unauthorized access. In the past, this was achieved by storing the data in large filing cabinets and safety deposit boxes in banks. Businesses paid a very large amount every year to protect their sensitive data. Nowadays, the data is stored and monitored by large companies in centralized locations. This causes many problems:.

1. There should be a regular upgrade to the framework and privacy policies due to the rapidly growing cyber security risks.
2. The data is stored in a centralized location, which creates a single point where a small fault can lead to millions of lost or compromised data.

3. There is no transparency regarding the data collection and storing process so the users what personal data is collected and how it is used. The users have no control over their own data.
4. Communication between user and the companies should be secure so that the data remains secure.
5. The security frameworks need to be upgraded to combat the rapidly growing penetration techniques due to technological advancements [29].

How Blockchain Implements Data Privacy

Blockchain is a decentralized network of small nodes called block. Each and every user has access to the entire blockchain but each block is only accessible by a particular key only available to the owner of that data. Once the data has been added to the blockchain, it is very hard to update or change it. In addition, blockchain are stored in a P2P network where the complete Blockchain is stored on each user's computer to remove the need of a middleman [28].

Blockchain Privacy Protection

Private and Public Keys

Blockchain uses asymmetric cryptography to secure transactions between users using private and public keys. These keys contain a random string which is unique to the particular block of data. Only the users with these keys can access the data [28]. A private key consists of a series of 32 bytes. It can store a 256-length string in form of binary string, Base64 string, WIF Key, mnemonic phrase, hex string, *etc.* these 32 bytes are used to create a public key is then converted to a Hash address which is used to access the data by other users. Blockchain uses a very complex algorithm used to convert the private key to public key. These algorithms prevent the conversion of a public key back to its original form, the private key [27].

Blockchain also maintains user anonymity by representing each user by their blockchain address, this address does not reveal personal information. These addresses are calculated by a user's past interaction with the blockchain.

Attribute Based Encryption

It is a key encryption algorithm which generates a key based upon all the attributes of user such as address, type of data, *etc.* ABE has a very big disadvantage, whenever we want to add or remove a user from a particular block;

we have to re-encrypt the public keys since they are based on the attributes of all users [30].

An example of ABE is Cipher text-policy attribute-based encryption (CP-ABE). It is superior to traditional ABE because it allows the user to encrypt the data without exactly knowing the individual accessing the block. This results in the data being accessible publicly but only being decrypted by legitimate users.

Another proposed technique is the blockchain-based distributed attribute-based encryption (BDABE) [31]. In this technique, an access authority decides which of the attributes are to be assigned to a particular user, the users can then combine multiple attributes from multiple access authorities for decryption of cipher-texts.

A BDABE model has 5 different entities:

1. Distributed Blockchain: A blockchain is used to store the data which can be accessed by the keys.
2. Attribute authority: An AU is responsible of assigning attributes to users based on their particular domain.
3. Root Authority: A RA is responsible for creating the secret keys using attributes of Attribute authorities.
4. Data Reader: it is a user who intends to access the encrypted data in the blockchain.
5. Data Owner: It is a user who owns data to be uploaded and shared.

The AU plays the most important role because they get to decide all the attributes of each node, each AU is responsible for a group of nodes called a domain. An AU can assign an attribute to a node outside its domain also. The RA's are responsible for creating the secret keys of AU and RA's need to be fully trusted by the system.

BLOCKCHAIN - SECURITY

To describe the overview of security in blockchain, we describe the basic blockchain architecture. A block of a blockchain contains three important parts, first, it contains the information or data to be stored, second, the hash value of the entire block, and third, the hash value of the previous block [28]. So, to tamper a block we have to tamper all the blocks that come before. This process requires very high computational power and a lot of time. Blockchain also implements a consensus procedure to ensure the legitimacy of the data being added to the network. This guarantees the integrity of the data. Blockchain is also based on a peer-to-peer network, so no third party is involved while storing your data, which

prevents data from being exposed or sold. Thus, a blockchain is a secure ledger which can store data on an open network and protect data effectively [32].

A Deeper Dive into Blockchain Security

One of the most developed blockchain implementation is bitcoin, which is a Crypto currency transaction management framework. Bitcoin Blockchain implements three different techniques to protect the network from security breaches. These three techniques are Hash Chained Storage, Digital Signature and commitment consensus.

Hash Chained Storage

In this technique, the blockchain employs hash pointers which is the hash value of the data generated by cryptographic methods and it point to the address where the data is stored [28]. We can check if the data has been tampered as it will change the hash value of the pointer. This pointer can be publicly verified by any user. If there is an attempt to tamper with the data, the person has to change the values of all the previous blocks, but will have to stop at the first block as it is generated by the computer when the blockchain was created with some default data.

This method is further optimized by using a Merkle Tree, which is a binary search tree that stores the hash value of a parent-children pair, if the data is tampered, then the hash value also changes for its parent node, which can be verified effectively.

Digital Signature

It is a technique used to verify the validity of the data using cryptographic methods. The process of creating and validating a digital signature has three different parts:.

1. Key Generation: It is an algorithm used to create a private and public key.
2. Signing Algorithm: It creates a signature using the private key for verification later.
3. Verification Algorithm: It takes a signature, a public key and a message as input and verifies the message's signature with the given block signature using the public key [28].

This allows a user to share their data with others in a secure manner. Bitcoin implements Elliptical Curve Digital Signature Algorithm (ECDSA) which provides 128 bits security. Whenever there is a transaction between two people,

the sender sends a message to the receiver using their private key; the recipient verifies the message using the public key of the sender. This prevents false or forged transactions from taking place.

Another example is the Rivest-Shamir-Adleman (RSA) algorithm. In this algorithm [33], the public key is generated using two very large prime numbers and finding the modulus of a combination of these numbers. The algorithm is discussed below:

1. Take 2 distinct prime number x and y and find $n = xy$.
2. Using Carmichael's totient function, find value of $\lambda(n) = \text{lcm}(p-1, q-1)$.
3. Choose a value e between 1 and $\lambda(n)$ which is coprime to $\lambda(n)$.
4. Compute the modular multiplicative inverse of $d = e(\text{mod } \lambda(n))$.
5. The public key is (n, e) , the encryption equation for message M is $M^e \text{ mod}(n)$.
6. The private key is (n, d) , the decryption equation for value C is $C^d \text{ mod}(n)$.

Consensus

When a block is broadcasted to all the nodes, each node has the option to add the block to their copy of Ledger or to ignore it; this can create discrepancies as some of the blocks could be missing for some nodes. To prevent this, Blockchain implements a consensus algorithm which check what the majority of the nodes want to do with the block. The algorithm should guarantee that either the block is accepted or denied, even if it takes some considerable time [34].

Types of Algorithm

Proof of Work (POW)

Algorithm is based on the concept of validating information or a block by performing a high computational work. This process is known as mining and the nodes that participate in this process are called miners. The miners compete against each other to complete the work and the miner who completes the work the fastest earns some blockchain currency [28, 29].

A Framework which implements the Proof of Work algorithm is Bitcoin. Bitcoin uses SHA-256 cryptographic hash functions to calculate a hash value from the transaction value. This hash has a fixed length and is unique to the block. To make the computation harder, Bitcoin chooses a difficulty level or a target for each hash calculation and the miners have to add numbers to the string to get the hash value lower than the target. The lower the target, the more difficult the computation process.

For example, let us take a string “Bitcoin for storage”, it generates a hash value a5498d7cbf82e9b88e382107a96a9cb10a4fc258ecd5f0d931d2a3b287063e34 which has a value $2^{461.712}$. Now let us take the target as 2^{460} . Then the final string becomes “Bitcoin for storage0” which has a value $2^{458.46241887}$. This calculation was very easy and only took a few tries, in reality, bitcoin assigns a lower target to increase the computation cost for smaller data. This ensures that the work done is uniform for all data sizes.

Proof of work has some disadvantages.

1. The algorithm requires very high computational power and time. It also has a very low probability of generating a successful proof of work. For a framework where very large amounts of data are to be added at a particular time, the nodes will take a long time to add the block to the chain.
2. The proof of work scheme works on the basis of rewarding the miners. This incentive should be alluring enough to attract a lot of miners for proof of work to be viable.

Proof of Stake (POS)

Works on the principle that a node can mine blocks proportional to the amount of currency it holds. Only those miners who have contributed some capital as stakes can participate in the validation process. The network keeps a track of all these miners and their deposits. To validate a block, the entire miners place a bet, the chances of winning the bet are proportional to their deposits. The miner who wins the bet gets to verify the block. If the block is verified and appended to the ledger, then all the validators that placed the bet get a reward proportional to their deposit, if the validation process fails and the transaction is found to be false, the validators are penalized and they lose some of their deposit. This compels the validators to make genuine transactions [28, 29].

This algorithm has some advantages over POW algorithm. POS requires lower computation power as the miners don't have to solve a mathematical puzzle. This in turn reduces the amount of resources required. To control the ledger, a miner has to hold more than 51% of the total deposits whereas in POW, the miner has to hold more than 51% of the computational power which is easier. It has some disadvantages as well. Rich miners can dominate the chain very easily by depositing more than 51% of all deposits.

Byzantine Fault Tolerance (BFT)

Is a condition where, due to some system failure, the consensus decision is not broadcasted to all the nodes properly so that they cannot take their decision properly [34]. These nodes, instead of providing a valid decision, provide a random value that makes these nodes look like they are functioning correctly. To solve this problem, all the nodes should be allowed to discuss if the value provided by a particular node X is true. If X is true, all the other nodes must agree on the value provided by X. otherwise, all the nodes must agree on a different value. This rules out all the nodes which do not provide a value, provide a false value by mistake or provide a false value deliberately to change the final decision on the block. For this protocol to be implemented there should be at most $(n-1)/3$ number of malicious nodes in a network out of a total number of n nodes. An implementation of BFT is Redundant Byzantine Fault Tolerance.

Redundant Byzantine Fault Tolerance (RBFT) [35] is an asynchronous model where multiple instances of BFT protocol run in parallel and each instance has a primary instance. All these instances order the execution of BFT protocol, but only a selected few known as master instance execute the request, the rest of the instances known as backup instances are used to find if the master instance is malicious or not. If a master instance fails to deliver a result or does not deliver the result in time compared to the backup instance, the primary instance of the master is considered malicious and a new primary instance is chosen. This ensures that the masters executing the requests are harmless. The backup nodes check for the correct output of master nodes by checking all the different instances and deciding if there is a need to change the protocol.

Some Problems with Blockchain

1. Since most of the frameworks for security work on some form of computation or influence, a person with majority influence can easily control the data in the ledger. The 51% attack and Sybil attack are some of the most common attacks on a blockchain network [36].
2. With the increase in the computational power of computers, it is becoming easier to solve the puzzles for consensus. We need to keep upgrading the algorithms to keep up with these upgrades.
3. Most of the mining power in blockchain is concentrated with companies in China, this power needs to be distributed to attain full decentralization [29].

DISCUSSION

Blockchain, although is a relatively newer technology, it is no doubt revolutionary working towards changing the very foundation on the internet as we know it today. By the introduction of widespread use of decentralization of networks using P2P, blockchain makes the distributed data reliable depending on how regulations are standardized. The internet as we know it today has become an integral part of our lives and the absence of it cannot even be imagined. Changing the backbone of today's network is definitely not going to be easy taking substantial amount of time and money along the way. One crucial aspect of this transition is the relocation of data onto these decentralized networks which makes data storage the most important field which may make or break the vision of how the internet will be visualized in the future. With many major blockchains like Ethereum struggling in this category, many solutions are being put forward. One ingenious idea was the proposal of storing data on borrowed spaces on the computer of each peer in the network as is implemented by Filecoin. This has massively reduced costs of storage, the Filecoin network being very compatible and adaptive with other blockchains as well. Having dealt with storage, data must also be easily retrieved. To tackle speed and latency problems, sharding was adopted. In any P2P network, apart from the use of storing data on each other, communication between nodes is also necessary in case an attack breaks out on the network so that others can be warned. But, no such inter-node communication protocol exists for industrial or practical purposes, whose existence will need further research and development to improve its security and scalability. However, technology is constantly evolving and will see further improvements in this field, which will be the target of future works [37].

Blockchain technology initially gave more power to the ones having more computational power (POW) or financial backing (POS) allowing monopoly of the network by a selected few who can afford it. Also, the processing power of the general computer is increasing as technology advances and some of the consensus algorithms, considered very hard to solve, are getting solved faster and faster over time affecting the security of the ledger. However, with the inculcation of newer and more dynamic consensus algorithms, these irregularities are also being looked at allowing the network to be more autonomous and realizing the full meaning of decentralization. These algorithms must be robust and allow for upgrades because of the continuous technical advancement. In contrast to centralized systems where security must be ensured only at the central server, decentralized systems must maintain security at every node making its implementation very difficult. All the techniques are being researched and with due time, will definitely bring forth a framework that the users can trust their data with [38].

The pinnacle of blockchain lies in its implementation by individual organizations to revamp their entire database, by the government to ensure information transparency and its extensive implementation in AI which may possibly change the structure of all industrial machines as to how they are today or even how robots may think. An intelligent AI is always an enhanced armament in the arsenal of any country. The possibilities are endless and curiosity is the mother of invention. Constant updates to improve this technology may even bring about a new era of information technology that emphasizes how capable the entire technology is. All of which has emerged from something as simple as distributing data to many people, the outcomes could not even have been imagined. However, the current problem lies in how quickly blockchain evolves. Being in its infant stages, any change made is huge and existing technology gets outdated in a matter of mere months making organizations reluctant to spend on something that is changing so frequently and may not even be compatible after a few months. This highlights the need for standardization of frameworks and implementation of new regulations which are yet to take a few more years [39].

CONCLUSION

The pinnacle of blockchain lies in its implementation by individual organizations to revamp their entire database, by government to ensure information transparency and its extensive implementation in AI which may possibly change the structure of all industrial machines as to how they are today or even how robots may think. An intelligent AI is always an enhanced armament in the arsenal of any country. The possibilities are endless and curiosity is the mother of invention. Constant updates to improve this technology may even bring about a new era of information technology that emphasizes how capable the entire technology is. All of which has emerged from something as simple as distributing data to many people, the outcomes could not even have been imagined. However, the current problem lies in how quickly blockchain evolves. Being in its infant stages, any change made is huge and existing technology gets outdated in a matter of mere months making organizations reluctant to spend substantially on something that is changing so frequently and may not even be compatible after a few months. This highlights the need for standardization of frameworks and implementation of new regulations which may yet take a few more years.

CONSENT FOR PUBLICATION

Not applicable.

CONFLICT OF INTEREST

The author declares no conflict of interest, financial or otherwise.

ACKNOWLEDGEMENT

Declared none.

REFERENCES

- [1] M. Anderson, "Exploring Decentralization: Blockchain Technology and Complex Coordination", *Journal of Design and Science*. Available from: <https://jods.mitpress.mit.edu/pub/7vxemt3/release/2>
- [2] J. Frankenfield, *Bitcoin*. <https://www.investopedia.com/terms/b/bitcoin.asp> [Accessed: 25-Oct-2020]
- [3] N. Zahed Benisi, M. Aminian, and B. Javadi, "Blockchain-based decentralized storage networks: A survey", *J. Netw. Comput. Appl.*, vol. 162, p. 102656, 2020. [<http://dx.doi.org/10.1016/j.jnca.2020.102656>]
- [4] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", *2017 IEEE International Congress on Big Data (BigData Congress)*, 2017 [<http://dx.doi.org/10.1109/BigDataCongress.2017.85>]
- [5] R. Kumar, and R. Tripathi, "Blockchain-Based Framework for Data Storage in Peer-to-Peer Scheme Using Interplanetary File System", In: *Handbook of Research on Blockchain Technology*, 2020, pp. 35-59. [<http://dx.doi.org/10.1016/B978-0-12-819816-2.00002-2>]
- [6] edChain, "What is Sharding in the Blockchain?," Medium, 05-May-2018, [Online]. Available: <https://medium.com/edchain/what-is-sharding-in-blockchain-8afd9ed4cff0#:~:text=Sharding%3A%20a%20solution%20to%20the,to%20make%20them%20more%20efficient.&text=In%20case%20of%20the%20blockchain,information%2C%20when%20sharding%20is%20implemented> [Accessed: 26-Oct-2020]
- [7] V.K. Singh, *Database Sharding*. <https://medium.com/system-design-blog/database-sharding-69f3f4bd96db> [Accessed: 26-Oct-2020]
- [8] R. Blog, *What is Sharding?*. <https://www.radixdlt.com/post/what-is-sharding> [Accessed: 26-Oct-2020]
- [9] G. Yu, X. Wang, K. Yu, W. Ni, J.A. Zhang, and R.P. Liu, "Survey: Sharding in Blockchains", *IEEE Access*, vol. 8, pp. 14155-14181, 2020. [<http://dx.doi.org/10.1109/ACCESS.2020.2965147>]
- [10] C. Pauw, *Sharding, Explained*. <https://cointelegraph.com/explained/sharding-explained> [Accessed: 27-Oct-2020]
- [11] W. Contributors, *Peer-to-peer*. <https://en.wikipedia.org/wiki/Peer-to-peer> [Accessed: 27-Oct-2020]
- [12] C. Woodford, *How does BitTorrent work?*. <https://www.explainthatstuff.com/howbittorrentworks.html> [Accessed: 27-Oct-2020]
- [13] *Peer-to-Peer Network (P2P)*. <https://networkencyclopedia.com/peer-to-peer-network-p2p/#:~:text=Back%20to%20Index-,Structured%20networks,the%20resource%20is%20extremely%20rare> [Accessed: 27-Oct-2020]
- [14] N. Oualha, M. Önen, and Y. Roudier, "Secure P2P Data Storage and Maintenance", *Int. J. Digit. Multimed. Broadcast.*, vol. 2010, pp. 1-11, 2010. [<http://dx.doi.org/10.1155/2010/720251>]
- [15] B. Prêtre, Attack on Peer-to-Peer Networks, Semester Thesis, Dept. of Computer Science: Swiss

- Federal Institute of Technology (ETH) Zurich, 2005.
- [16] H. Huang, J. Lin, B. Zheng, Z. Zheng, and J. Bian, "When Blockchain Meets Distributed File Systems: An Overview, Challenges, and Open Issues", *IEEE Access*, vol. 8, pp. 50574-50586, 2020. [http://dx.doi.org/10.1109/ACCESS.2020.2979881]
- [17] <https://medium.com/coinmonks/understanding-ipfs-in-depth-5-6-what-is-libp2p-f8bf7724d452> [Accessed: 30-Oct-2020]
- [18] K. Kwatra, *What is IPFS?*. <https://medium.com/wolverineblockchain/what-is-ipfs-b83277597da5> [Accessed: 30-Oct-2020]
- [19] *IPFS Documentation*, 2020. <https://docs.ipfs.io/> [Accessed: 02-Nov-2020]
- [20] J. Benet, "IPFS - Content Addressed", In: *Versioned. P2P File System*, 2014.
- [21] <https://hackernoon.com/understanding-ipfs-in-depth-3-6-what-is-interplanetary-naming--system-ipns-9aca71e4c13b> [Accessed: 05-Nov-2020]
- [22] Filecoin, "Filecoin Documentation", *Filecoin Docs*. [Online]. Available: <https://docs.filecoin.io/> [Accessed: 09-Nov-2020]
- [23] J. Benet, and N. Greco, *Filecoin: A Decentralized Storage Network*. Protoc. Labs, 2018.
- [24] <https://filecoin.io/blog/filecoin-features-verifiable-storage/> [Accessed: 09-Nov-2020]
- [25] Swarm, "Swarm Documentation", *Architectural Overview*, 2019. [Online]. Available: <https://swarm-guide.readthedocs.io/> [Accessed: 10-Nov-2020]
- [26] R. John, J.P. Cherian, and J.J. Kizhakkethottam, "A Survey of Techniques to Prevent Sybil Attacks", *Proceedings of the IEEE International Conference on Soft-Computing and Network Security, ICSNS 2015*, 2015 [http://dx.doi.org/10.1109/ICSNS.2015.7292385]
- [27] Hoang Giang Do and Wee Keong Ng, "Blockchain-Based System for Secure Data Storage with Private Keyword Search", *Proceedings - 2017 IEEE 13th World Congress on Services, SERVICES 2017*, 2017pp. 90-93 [http://dx.doi.org/10.1109/SERVICES.2017.23]
- [28] R. Zhang, R. Xue, and L. Liu, "Security and Privacy on Blockchain", *ArXiv*, vol. 1, p. 1, 2019.
- [29] J.B. Bernabe, "Privacy-Preserving Solutions for Blockchain: Review and Challenges", *IEEE Access*, vol. 7, no. 2019, pp. 164908-40, 2019. [http://dx.doi.org/10.1109/ACCESS.2019.2950872]
- [30] Y. Chen, S. Ding, Z. Xu, H. Zheng, and S. Yang, "Blockchain-Based Medical Records Secure Storage and Medical Service Framework", *J. Med. Syst.*, vol. 43, no. 1, p. 5, 2018. [http://dx.doi.org/10.1007/s10916-018-1121-4] [PMID: 30467604]
- [31] G. Bramm, M. Gall, and J. Schütte, "BDABE Blockchain-Based Distributed Attribute Based Encryption", *ICETE 2018 - Proceedings of the 15th International Joint Conference on e-Business and Telecommunications*, vol. 2. Icete, 2018pp. 99-110
- [32] Y. Chen, "An Improved P2P File System Scheme Based on IPFS and Blockchain", *Proceedings - 2017 IEEE International Conference on Big Data, Big Data 2017*, 2017pp. 2652-57 [http://dx.doi.org/10.1109/BigData.2017.8258226]
- [33] W. Contributors, *RSA (cryptosystem)*. [https://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](https://en.wikipedia.org/wiki/RSA_(cryptosystem)) [Accessed: 12-Nov-2020]
- [34] B.B. Technologies, *What is Consensus Algorithm in Blockchain & Different Types of Consensus Models*. <https://medium.com/@BangBitTech/what-is-consensus-algorithm-in-blockchain-different-types-of-consensus-models-12cce443fc77> [Accessed: 27-Oct-2020]
- [35] P.L. Aublin, S. Ben Mokhtar, and V. Quema, "RBFT: Redundant Byzantine Fault Tolerance",

- Proceedings - International Conference on Distributed Computing Systems*, 2013pp. 297-306
[<http://dx.doi.org/10.1109/ICDCS.2013.53>]
- [36] D.K. Sharma, S. Pant, M. Sharma, and S. Brahmachari, "Chapter 13 - Cryptocurrency Mechanisms for Blockchains: Models, Characteristics, Challenges, and Applications", In: *Handbook of Research on Blockchain Technology*, Krishnan Saravanan, E. Balas Valentina, E. Golden Julie, Y. Harold Robinson, S. Balaji, Kumar Raghvendra, Eds., Academic Press, 2020, pp. 323-348.
[<http://dx.doi.org/10.1016/B978-0-12-819816-2.00013-7>]
- [37] D.K. Sharma, A.K. Kaushik, A. Goel, and S. Bhargava, "Chapter 11 - Internet of Things and Blockchain: Integration, Need, Challenges, Applications, and Future Scope", In: *Handbook of Research on Blockchain Technology*, Krishnan Saravanan, E. Balas Valentina, E. Golden Julie, Y. Harold Robinson, S. Balaji, Kumar Raghvendra, Eds., Academic Press, 2020, pp. 271-294.
[<http://dx.doi.org/10.1016/B978-0-12-819816-2.00011-3>]
- [38] M. Sharma, S. Pant, D.K. Sharma, K.D. Gupta, V. Vashishth, and A. Chhabra, "Enabling security for the Industrial Internet of Things using deep learning, blockchain, and coalitions", *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 7, p. e4137, 2020.
[<http://dx.doi.org/10.1002/ett.4137>]
- [39] A. Riyal, Parth Sarthi Prasad, and Kumar Sharma Deepak, "Internet of Things and Blockchain Amalgamation, Requirements, Issues, and Practices", In: *Blockchain Technology for Data Privacy Management* CRC Press, 2021, p. 23.

Blockchain Based Hybrid Framework for Identity Management in Healthcare

Deepak Kumar Sharma^{1*}, Arjun Khera², Koyel Datta Gupta³ and Rinky Dwivedi³

¹ Department of Information Technology, Indira Gandhi Delhi Technical University for Women, Delhi, India

² Department of Information Technology, Netaji Subhas University of Technology, New Delhi 110078, India

³ Department of Computer Science and Engineering, Maharaja Surajmal Institute of Technology, C-4 Janakpuri, New Delhi 100058, India

Abstract: Healthcare systems face numerous impediments due to the unavailability of proper mechanisms to track the transactions related to patient's medical records. The maintenance and privacy of patient records are one of the key requirements of the healthcare system. Blockchain can be the potential solution to these problems. Blockchains have made a tremendous impact ever since their invention barely a decade ago. This paper delves into how blockchain can be used to solve the problem of patient record management by constructing scalable decentralised key systems with inbuilt sharing of credentials in a safe, secure, and digitally verifiable way. The work presents a hybrid scalable system capable of managing personal identity in a decentralized manner with no dependence on central authorities along with a rapid and simplistic way of exchanging claims among the users. The system overcomes potentially all problems associated with SOVRIN and blockchains in general by splitting itself into two symbiotic versions, one centralised and the other, decentralised.

Keywords: Blockchain, Healthcare, Identity management, Decentralized applications, IoT.

INTRODUCTION

With the rapid growth in the field of information technology, the changes in the worldwide healthcare system are eminent. IoT based medical system [1, 2] is gaining popularity because of improved coordination between healthcare personnel and patients. The patient's data recorded in the form of images, videos, text, and audio by IoT devices [3] needs to be processed and stored through

* Correspondence author Deepak Kumar Sharma: Department of Information Technology, Indira Gandhi Delhi Technical University for Women, Delhi, India; Tel: 9868861080; E-mail: dk.sharma1982@yahoo.com

multimedia techniques. The devices are connected to the internet for subsequent storage of information at the cloud level, which can be accessed by different entities like doctors, insurance companies, research wings, and pharmaceutical companies (Fig. 1). However, healthcare record contains private information that may be viable to cyber-attacks. Hence, securing such large-scale multimedia data and maintaining the privacy of the patient records is important.

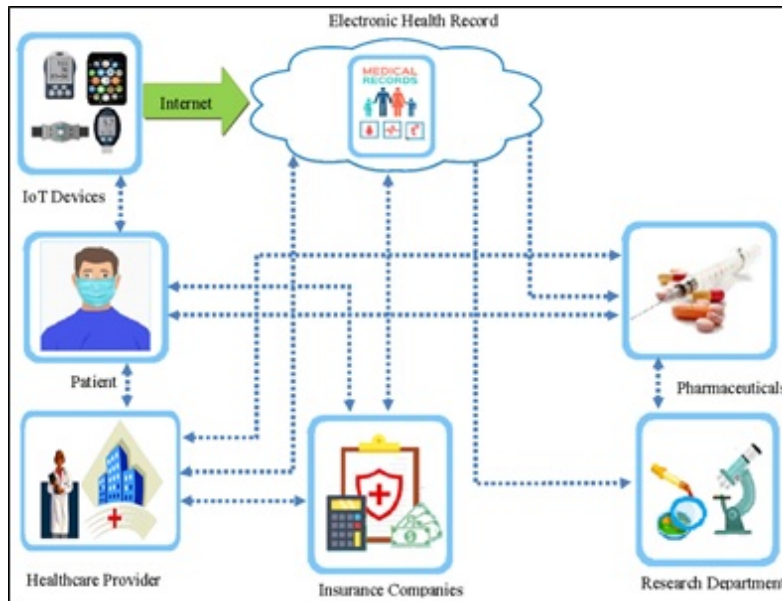


Fig. (1). IoT enabled Healthcare System.

The online transfer and storage of this sensitive record require a robust credential system. In this context, blockchain technology [4 - 7] can be used as a secure way to save and distribute information. The smallest unit of data that is linked with one another is called a block. The blockchain is a linear list of these blocks which are linked to one another using cryptographic hash functions, as depicted in Fig. (2). Evidently, the blockchain is nothing but an immutable ledger of records maintained across several computers which are linked together in peer-to-peer manner. Large number of participating entities maintain the ecosystem by storing, updating, and exchanging data among each other.

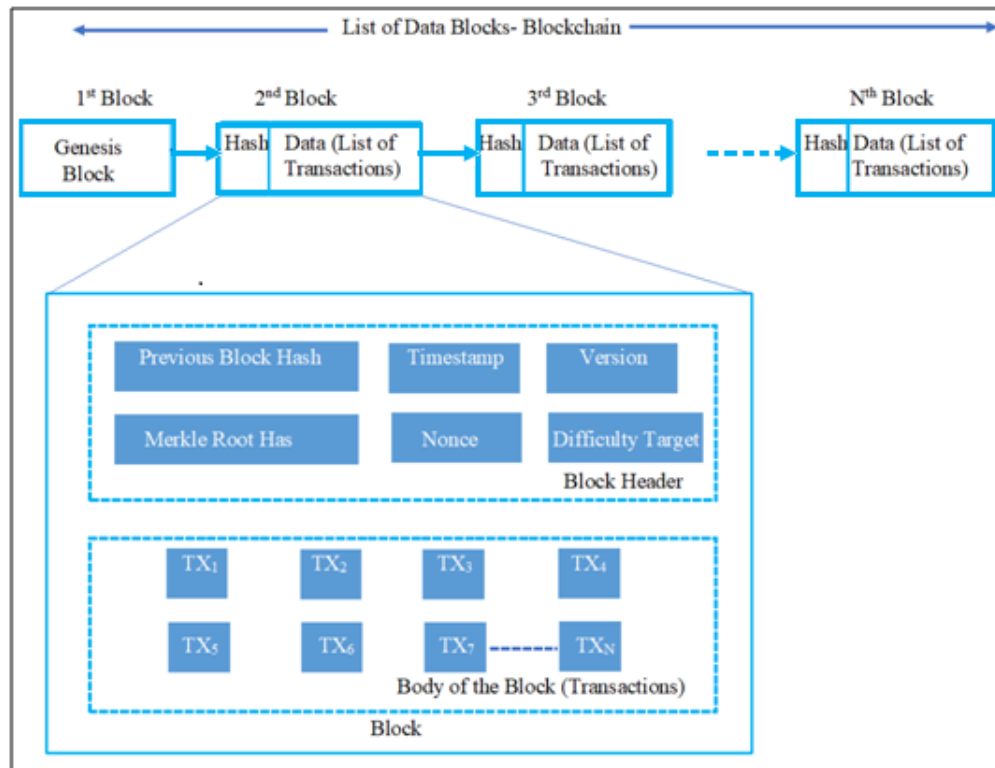


Fig. (2). List of Data Blocks.

However, like any new invention, blockchain also had its flaws, the most pervasive being scalability. Decentralization and the associated benefits come at the cost of performance and scaling. When Bitcoin experienced a surge in popularity, the associated transaction fees shot through the roof as the system was capable of processing only a single every 10 minutes, which pales in comparison to other payment processing platforms such as Visa, which processes up to 2000 transactions per second. This was not the only problem. Bitcoin also consumed a lot of energy for mining, so much so that it has come under scrutiny for wastage of resources due to consumption charting more than even what cities draw. Many variations and changes to this structure, particularly to the consensus algorithms, have been introduced since then to overcome these shortcomings. Most of the implementations of blockchain to date have been around cryptocurrencies, and there is good reasoning behind that. Blockchain or decentralisation is a novel service, and running this service without any form of commitment by a central authority means other participants need something in return for operating the chain and its operations. Monetary rewards solve this problem better than

everything else, which is the reason why even the applications not concerning digital currency still build a native currency. However, other forms of reward systems are also present. For example, decentralized storage systems like DBChain or IPFS consider reward systems in the form of storage. On the other hand, most corporations, given the Adhoc participation rules in public blockchains, find them unsuitable for their purpose. Hence, the rise of permissioned blockchains consisting of known nodes in consensus opens a lot of new avenues in solving scalability and other issues. There will always be a compromise between the level of decentralization and scalability. In simple words, blockchains are not static protocols that can be suitably repurposed for any scenario. Unlike existing distributed system protocols that remain independent of the application they are used for, blockchain design and associated consensus protocols are completely dependent on the use case. The reward system and the architecture for a currency would be completely different from one involving a database or medium publishing platform. This work contributes to the design of an Identity Management system for digital healthcare. Despite recent advances in the digitization of health services, a purely digital identity management system still remains an abstract concept. Given the lack of consensus among various stakeholders, the development of identity systems has been fractured and uneven. In the present day, a user is a bearer of multiple sets of identity documents spanning both digital and physical versions, requiring contact with multiple service providers to establish their identity. The problem is even more pervasive online, wherein a user is supposed to remember a plethora of usernames and passwords. Moreover, such a diverse spread also vastly increases the risk to privacy and security, as has been witnessed in past cases of breaches. Multiple people have taken a stab at devising a solution but to no avail. One of the reasons why a successful deployment in this field is all the more difficult is the amount of coordination that would be required to make a system successful making the process of both designing and bootstrapping such a system nearly impossible. To end this, we devised a system split into two. The proposed solution intends to plug these gaps in implementation by considering real life scenarios.

The majority of the current applications are centralized meaning the operation is in a client-server manner. The client depends on the server to provide some data, or the server may store some of the user's private data. This means that there's a large dependence on central authorities, due to which there are inherent issues at the fundamental level of this design. The emergence and major growth in the development of decentralized applications occurred after the development of Bitcoin. Decentralized applications basically remove the factor of trust on one single authority and spreads it among all the participating entities. The entire responsibility of data management is transferred over to the users themselves. The invention of Bitcoin in 2009 by Satoshi Nakamoto [8] took the world by storm.

For the first time ever, users were able to transact on a digital currency that was not controlled or managed by any central authority. The inflation as well as transfer was handled by the users themselves, giving birth to the idea of true decentralisation. The true genius in handling this extremely precarious act of decentralisation revolved around generating incentives to run the whole systems in a consistent view and without any compromises. This was achieved through the introduction of miners and subsequent rewards. However, the impact of this invention was more widespread as the underlying technology that is blockchain was seen as a promising functionality that could be shaped and repurposed for a variety of different applications involving decentralisation. The features provided by blockchain include true decentralisation, immutable ledger, cryptographic security and anonymity. Thus, the dependence and trust on central organization are not required and the entire ecosystem operates together to keep the system consistent and up to date. This ensures that compromisation of few of the entities wouldn't damage the entire system and it keeps operating normally.

The rest of this paper is arranged into several sections. The next section illustrates the related works; Section 3 describes the motivation behind this work. The subsequent section presents an overview of Identity management for the healthcare system. Section 5 details the proposed solution 'OneId' to address the problem statement using blockchain. Section 6 discusses the merits of the proposed solution. The paper is concluded in section 7 and outlines the future work.

BACKGROUND AND RELATED WORK

Efficient management of patient record is important for providing effective treatment and care, studying diseases, and inventing drugs and vaccines. However, IoT-based applications face several security challenges [9 - 12]. Most healthcare applications follow client-server architecture where the server has ownership of the records and has access to them [13, 14]. This kind of architecture causes hindrance in providing proper research and subsequent treatment of diseases. To overcome this, several researchers have been working on cloud-based healthcare systems [15]. However, the security of patient records is a challenge in cloud-based architectures. In this context, researchers are working on blockchain technology to overcome the potential problems of traditional healthcare systems. The blockchain enables the creation and simultaneous sharing of records among the other contributors of the blockchain. Several researchers have been working on blockchain enabled healthcare systems for better management of EHR (electronic healthcare record). Xia *et al.* [16] presented a cloud-based health care system coupled with blockchain technology. Few researchers-built healthcare systems did not allow the transfer of patient

medical records to the blockchain [17, 18]. In contrast, Yue *et al.* [19] presented a medical system that allowed medical care providers to access patient records to improve treatment facility. A distributed approach has been proposed [20] for improved and secured transfer of patient data among multiple organizations. A blockchain enabled medical system with improved performance is proposed by Gorenflo *et al.* [21]. Ethereum blockchain is being used [22, 23] for sharing medical records of patients. A secured pervasive social network-based healthcare system using authentication is proposed by Zhang *et al.* [24]. An on-chain and off-chain security method enabled blockchain technology is used for the exchange of patient records in [25]. Bio-sensors are being used to reduce patient record access time in the healthcare architecture proposed by Dey *et al.* [26]. Thakkar *et al.* [27] deploy belligerent caching and configuration authorization techniques to estimate the performance of the blockchain network. A secured patient data transfer mechanism using blockchain for better integrity and privacy is presented in a study [28]. A mobile-based application was developed by Ichikawa *et al.* [29] to transfer insomnia patient information to private networks in a secured tamper-proof manner using blockchain.

MOTIVATION

Despite recent advances in the digitisation of health services, a purely digital identity management system still remains an abstract concept. Given the lack of consensus among various stakeholders, the development of identity systems has been fractured and uneven. In the present day, a user is a bearer to multiple sets of identity documents spanning both digital and physical versions, requiring contact with multiple service providers to establish their identity. The problem is even more pervasive online wherein a user is supposed to remember a plethora of usernames and passwords. Moreover, such a diverse spread also vastly increases the risk to privacy and security as has been witnessed in past cases of breaches. Multiple people have tried at devising a solution but to no avail. One of the reasons why a successful deployment in this field is all the more difficult is the amount of coordination required between the process of designing and bootstrapping to make a system successful, which is nearly impossible to achieve. To this end, we devised a system split into two. The proposed solution intends to plug these gaps in implementation by considering real life scenarios.

IDENTITY MANAGEMENT: HEALTHCARE SYSTEM

In order to understand how Identity Management Systems work, we need to gain an understanding of what exactly is Identity. Identity is a term that encompasses a wide variety of definitions [30] and can never be limited to a defined set given its changing definition with its varied perception. However, more important than

defining identity is defining the purpose that the identity carries. Any form of interaction and subsequent exchange of information between a given set of parties is based upon trust. Trust in the fact that a person or an entity is in reality who they claim to be. This establishment of the trust is built on what we call as an identity. Identity is that set of basic attributes that provides an individual, entity or asset a legal representation. Identification is the prerequisite that entails access to any kind of service. A lack of identity can result in denial of access to basic services such as education, financial services, healthcare, social welfare benefits, economic development, and the right to vote. The burden of providing primary forms of identification rests on the shoulders of the government of the country to which the citizen belongs. The advancements made in the technology sector have brought a drastic change in how we create and process identity. The introduction of the EHR and subsequently increased digitization poses several threats related to unwanted disclosure of patients records. Another significant change is the introduction of a person's or organization's online identity. The widespread use of the internet has led to the creation of multiple silos of user information owned and controlled by third parties. At the most basic level of understanding, identity is a sum of attributes belonging to the entity like patient-doctor hospital, insurance companies, and medical research institutes (funded by government/pharmaceuticals). We refer to a Third Party as being a separate entity, which can either be a single individual or a legal entity, for example, a government, organization or an institute. There are three categories attributes of Identity namely 'inherent' (consist of any set of information that is drawn directly from the entity in question), 'assigned' (defined by third parties and are created with a specific purpose), and 'accumulated' which are a function of time and hence change or modify with the progression of time. A digital identity can be expressed as a sum of its attributes that does not hold any value. The value of an Identity is a direct function of the perceived trust that the accepting entity has upon the issuer of an Identity."

The massive scale of digitization has allowed a majority of legacy identity systems to transition away from the physical methods of authentication toward digital ones. Instead of registering target populations manually and storing identity information in paper registers, electronic capture and storage of data provides a number of benefits, such as:

- i. **Unique Identifiers:** Digital Identity Systems provide significantly superior accuracy in capturing data. This allows for better deduplication procedures, hence ensuring the removal of ghost enrolments and thus bringing down the associated losses due to waste and fraud.
- ii. **Increased Scalability:** Digital Identity Systems are easier to expand and

accommodate to changing requirements. Moreover, they are much easier to integrate with other services and facilitate fast data processing and collection.

- iii. **Better Monitoring and Reporting:** The data records generated by such systems provide better accountability and monitoring of the services being dispatched by creating auditable transaction records. This prevents fraud and helps in aid development planning.

In the next section, we propose a solution that revolves around the synchronous functioning of two independent systems. One of the systems is centralized and is intended for well-known identities. It is supposed to act as a central repository of identities and respective claims issued by well-known identities like hospitals, insurance, and pharmaceutical companies. The other system is decentralized and supposed to be primarily used by individuals like patients and medical practitioners. The reasoning behind this hybrid approach and how these two systems are supposed to work will be explained in the following section.

PROPOSED SOLUTION

The ultimate goal of this work is to provide Self Sovereign Identity for every user in a IoT-based healthcare system. In constructing a system that truly achieves the objective, considerable issues are raised. In order for the system to be practical while staying true to its principle required distribution of services between a centralized and a decentralized system. As explained in the previous section, SkyNet is supposed to act as a trusted repository of identities for well-known entities. The real challenge exists for the individual patients or doctors to participate and make use of these features. Unless the users are provided with the ability to onboard the network, SkyNet would not be able to gain much functionality. The factors to be kept in mind for such a hybrid network include:

1. The use of centralized service is suited for well-known entities, however, for individual users, it can present complications that come attached to any other centralized service. There will have to be a lot of trust riding on the service and the question of manipulation and self-sovereignty will be out of the equation.
2. This central service can be forced by governments for surveillance or be susceptible to offers by interested third parties to reveal information about the patients. The trust of storing invaluable data in the hands of a single entity that transcends the boundaries of countries can be hard to achieve.
3. The service needs to be free of cost, at least for some given basic set of functionalities. Identity is universal, it is the same for every rich or poor person. Placing a barrier to participation can severely hamper the adoption of the network.

In order to fulfil these requirements, we propose a decentralized network, OneId. The ideology of OneId is to allow any user to join the network and be able to create and store their identity-related in a trusted, secure and privacy-preserving manner. This is achieved through the use of a permissioned ledger.

The basic principles of OneId can be summarised as follows:

- i. Allow any entity (patient) to create and manage their identities in a decentralized manner.
- ii. Ensure the network is not subject to any form of censorship or centralization.
- iii. Stay true to the principles of Self-Sovereign Identity.
- iv. Allow any user to create and share records with any other user.
- v. Ensure security and privacy of the maximum order.

The OneId system is supposed to be a permissioned ledger in order to ensure that it scales accordingly as the number of users and the subsequent number of requests on the network increase.

In order for nodes to voluntarily participate in the permissioned ledger for others to use, the nodes will be rewarded with native currency. The mechanics of how the currency is generated, regulated, and distributed is yet to be dictated. However, there are various. A proposed method is to place a limit on the number of kids, claims, and overall storage for wallets a user will be exempted on the network. The storage services can charge users for any further added functionality or usage. The earnings from the storage services will have to be made through the native currency, and a cut will be taken from the earnings to fund the nodes running the permissioned ledger. The incentive mechanisms can work well here as the storage services cannot simply balloon their profits if the permissioned nodes are not paid their dues threatening the functioning of the network. In fact, it is highly likely that most storage services might operate a few nodes in the ledger. The overall benefits of using a Self Sovereign Identity system have already been covered in previous sections, which are expected to be received from the application of OneId.

Architecture

The OneId ecosystem is represented in Fig. (3). Every user registered on the OneId network shall make use of the Storage Services to store their health records and be able to manage them remotely from any device. This is not a necessary requirement and users will be given the option to operate medical records on their own. Most of the claims to access medical records will be issued through SkyNet given the presence of well-known identities in its trusted network. Users of OneId

will be able to transact these access as both SkyNet and OneId are constructed to be highly interoperable. Ensuring standardization will be important for the success of both networks. The Identity Ecosystem of OneId will be making use of multiple independent blockchains to run the self-sovereign identity system. The reason for keeping separate blockchains is to ensure scalability and a clear demarcation between rules. The following section will explain how Identities in OneId will function and how their information will be stored.

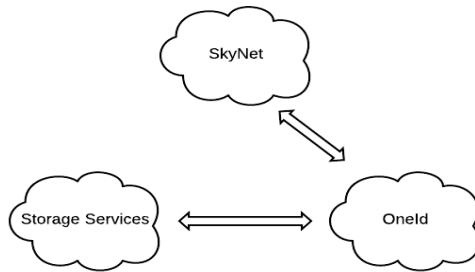


Fig. (3). SkyNet, OneId and Storage Services.

Creation of Records

The record is the core functionality of OneId. All the health data belonging to a patient will be stored in the record. The Record Chain is shown in Fig. (4). The functioning of the record has been divided into two types which are described below:

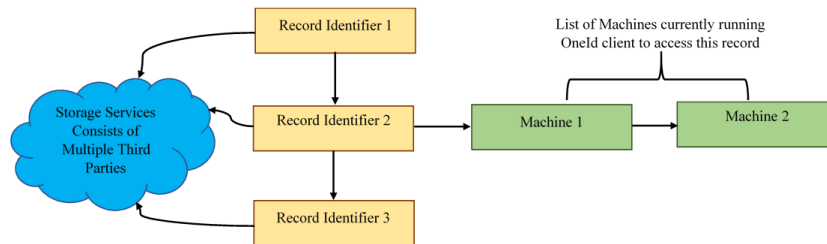


Fig. (4). Overview of the Record Chain.

Master Record

The master record is the main storage area for all related identifiers and data belonging to the controlling entity (patient). The first time a Master Wallet is created, three attributes will be generated,

1. *Master Record Identifier*: This is stored in the Record Chain and is used to identify the record. The creation of a block on the Record Chain involves the subsequent creation of secured storage area in the Storage Service. The functioning of the storage service is explained in subsequent section.

2. *Controlling Keys*: A public private key pair will be created to control the record. The private key will be destroyed after its creation. The public key will be used to encrypt the backups on the Storage Service. In case of loss of data stored in the Device Record, the only way to recover the encrypted data will be to reconstruct the private key to decrypt the data of the Master Record from the Storage Service. The public key is stored in each of the Device Record which is using this Master Record as the backup. The public key is not stored on the chain.

Device Record

The device records are used to store the identity-related data locally on the machine. Any form of data created by an entity is stored within the record. The only other place where the data is transferred is to the Master Record linked with the given Device Record to provide backup, and that too is encrypted with the decrypting private key destroyed to ensure maximum security and privacy.

Every Device Record on initiation will execute Proc_DeviceRecord

Proc_DeviceRecord

Begin

1. *Set up an Authentication Method*: The method of authentication for logging into the device record can vary, however, OneId will define some basic guidelines to ensure that device records do not prove to be the weak link their security. The most widely used and preferred medium will be a mobile phone. Using authentication methods such as fingerprint scanning along with password protection can provide extra security.

2. *Device Record Identifier*: Create a unique identifier. The method of identification creation is not yet outlined, however using characteristics unique to the properties of the machine can prove to be useful.

3. *Controlling Keys*: A public-private key pair will be created to control the record.

4. The last step will be determining either of the following options

1. Create a Master Record

In this scenario, the local client will initiate the creation of a Master Record according to the steps highlighted in the Master Record section. Once this is done, the public key along with the identifier will be registered on the Record Chain under the Master Record.

ii. Link to an existing Master Record

This is the case when a user wants to access their record from multiple machines. This requires two things, a) authorising the new device record b) copying the local data from an existing device record. These steps will require the use of an existing device record. The chain of steps are as follows:

1. The new device record creates a QR code containing its public key and identifier.

2. This is scanned using the existing device record. It then forms an encrypted communication channel with the new device record and sends the data encrypted with its public key.

3. The existing device then adds the identifier and public key of the new device on the Record Chain under their common Master Record thus authorizing the new device record.

Maintaining consistency between multiple device records without decrypting the data stored in the Cloud can present some problems. Though the consideration of storing a private key for the Master Record in every device wallet is very viable from deployment, ease of construction, and operational purposes, the security is far less than the proposed model. Methods of consistency maintenance similar to versioning software can provide some insight on how to approach this problem.

A few other important things to note here is that a single patient can create more than one record for greater security. Although managing identifiers across various records can prove to be cumbersome. Also, the user can also discard the option to store their backups in Cloud Storage and take the responsibility for backup and recovery.

Creation of Identifiers

Any entity that joins OneId can create native Identifiers. The exact nature and functioning of these identifiers are inspired from the Decentralised Identifiers Specification proposed by W3C as it shall allow users to generate identifiers in a decentralized manner. Every identifier will be added to this chain and hence will be able to refer to through a public endpoint as *OneId/identity/identifier*. Fig. (5) depicts the working of the Identifier Chain.

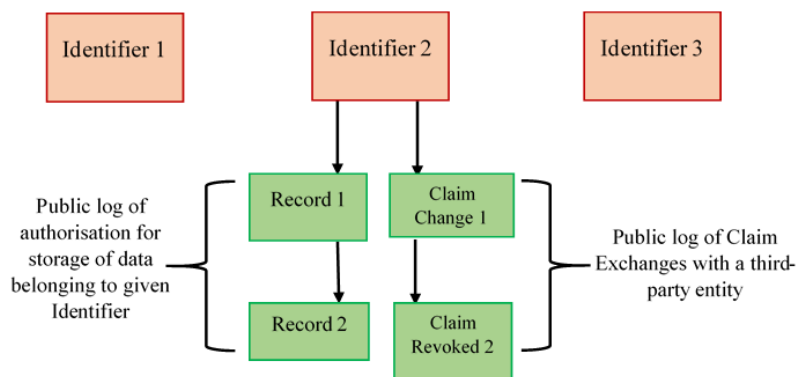


Fig. (5). Overview of the Identifier Chain.

For every identifier, we have the following set of properties:

1. A public private key pair. The private key is stored in the wallet and the public key is visible on the ledger.
2. A chain of blocks for authorisation records. The first block contains the record Id responsible for the creation of the given identifier. The same identifier can be controlled by multiple records or completely made to change ownership. The log makes sure the records are transparent.
3. Any messages relating to an entity engaged with this identifier through claims will add blocks to the claim message chain. For example, when a claim is created, claim data is modified, or the claim is revoked, the changes would not be accepted until the block expressing the changes is added to this chain. This ensures nonrepudiation and a log of claim-related activities concerning a particular identifier.

The Record and Identifier Chain is sufficient for the general purpose of functioning and fulfill most of the requirements of an EHR. The only thing to be covered yet is how will a user make and exchange claims if any. This is dealt with in the next section.

Claim Chain

The claims used in SkyNet are native to the system, and logs of changes to the claims is kept within the system. However, it might be the case that transparency regarding these changes in the claims be kept public. To solve this problem, if the issuer knows that the public records will be required, it simply uploads its claim id on the claim chain. Any changes thereof in the claim in SkyNet will have to be first uploaded as log on the claim chain in OneId before being implemented in SkyNet.

CONCLUSION

This project had started with the purpose of studying decentralized systems and finding out solutions on how they can be modified to scale like their counterpart centralized versions. Halfway through the project, the team arrived at a conclusion that decentralized systems are incentive driven, and the incentive depends on the purpose the system is designed for, unlike centralized systems where the focus is on distributed characteristics such as consistency and scalability. The project then focussed on implementing identity and credential management through these decentralized systems. Various other implementations were studied and compared. Based on their analysis, we proposed a solution consisting of a combination of centralized and decentralized services. We highlight in detail why this approach presents a favorable outcome and present the mechanics of its functioning. Workflows and data management are also presented to show real-life use cases.

However, this current version of SkyNet and OneId has left a few of the functionalities incomplete. The most important being the implementation of wallet consistency and claims exchange on OneId. The incentive mechanisms for the permissioned ledger and storage nodes are also left for further exploration to ensure that the system is practical enough to be used in real life. Overall, the combination of SkyNet and OneId presents an exciting opportunity in the field of self sovereign identity.

CONSENT FOR PUBLICATION

Not applicable.

CONFLICT OF INTEREST

The author declares no conflict of interest, financial or otherwise.

ACKNOWLEDGEMENT

Declared none.

REFERENCES

- [1] P. Verma, and S.K. Sood, "Cloud-centric IoT based disease diagnosis healthcare framework", *J. Parallel Distrib. Comput.*, vol. 116, pp. 27-38, 2018.
[<http://dx.doi.org/10.1016/j.jpdc.2017.11.018>]
- [2] D.K. Sharma, S. Bhargava, and K. Singhal, "Internet of Things applications in the pharmaceutical industry, An Industrial IoT Approach for Pharmaceutical Industry Growth", In: *In. Academic Press*, 2020, pp. 153-190.
- [3] M.F. Alhamid, "Investigation of mammograms in the cloud for smart healthcare", *Multimed Tools Appl*, pp. 1-13, 2017.
- [4] M. Sharma, S. Pant, D.K. Sharma, K. Datta Gupta, V. Vashishth, and A. Chhabra, "Enabling security for the Industrial Internet of Things using deep learning, blockchain, and coalitions", *Trans. Emerg. Telecommun. Technol.*, p. e4137, 2020.
- [5] S. Banyal, M. Saxena, and D.K. Sharma, "Blockchain-Enabled Security and Privacy Schemes in IoT Technologies", In: *Handbook of IoT and Blockchain* CRC Press, 2020.
- [6] D.K. Sharma, S. Pant, M. Sharma, and S. Brahmachari, "Cryptocurrency Mechanisms for Blockchains: Models, Characteristics, Challenges, and Applications", In: *Handbook of Research on Blockchain Technology*. Academic Press, 2020, pp. 323-348.
[<http://dx.doi.org/10.1016/B978-0-12-819816-2.00013-7>]
- [7] D.K. Sharma, T. Pardhe, Y. Kulshreshtha, and S. Singh, "Blockchain Applications and Implementation", In: *Handbook of IoT and Blockchain*. CRC Press, 2020, pp. 95-118.
[<http://dx.doi.org/10.4324/9780367854744-6>]
- [8] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", Available online: <https://bitcoin.org/bitcoin.pdf>
- [9] A. Riyal, P.S. Prasad, and D.K. Sharma, *Internet of Things and Blockchain Amalgamation, Requirements, Issues, and Practices, Blockchain Technology for Data Privacy Management*. CRC Press, 2021, p. 23.
- [10] D.K. Sharma, A.K. Kaushik, A. Goel, and S. Bhargava, "Chapter 11 - Internet of Things and Blockchain: Integration, Need, Challenges, Applications, and Future Scope", In: *Handbook of Research on Blockchain Technology*, Krishnan Saravanan, E. Balas Valentina, E. Golden Julie, Y. Harold Robinson, S. Balaji, Kumar Raghvendra, Eds., Academic Press, 2020, pp. 271-294.
[<http://dx.doi.org/10.1016/B978-0-12-819816-2.00011-3>]
- [11] S. Banyal, and D.K. Amartya, "Security Vulnerabilities, Challenges, and Schemes in IoT-Enabled Technologies", In: *Blockchain Technology for Data Privacy Management 1st Edition*. CRC Press, 2021, pp. 81-108.
- [12] R. Dwivedi, K. Datta Gupta, and D.K. Sharma, *Security and Surveillance at Smart Homes in a Smart City Through Internet of Things*. Springer, 2021.
[http://dx.doi.org/10.1007/978-3-030-52624-5_18]
- [13] R. Schoenberg, and C. Safran, "Internet based repository of medical records that retains patient confidentiality", *BMJ*, vol. 321, no. 7270, pp. 1199-1203, 2000.

- [http://dx.doi.org/10.1136/bmj.321.7270.1199] [PMID: 11073513]
- [14] D. Gritzalis, and C. Lambrinouidakis, "A security architecture for interconnecting health information systems", *Int. J. Med. Inform.*, vol. 73, no. 3, pp. 305-309, 2004.
[http://dx.doi.org/10.1016/j.ijmedinf.2003.12.011] [PMID: 15066563]
- [15] V. Stantchev, R. Colomo-Palacios, and M. Niedermayer, "Cloud computing based systems for healthcare", *ScientificWorldJournal*, vol. 2014, p. 692619, 2014.
[http://dx.doi.org/10.1155/2014/692619] [PMID: 24892070]
- [16] Q. Xia, E.B. Sifah, K.O. Asamoah, J. Gao, X. Du, and M. Guizani, "Medshare: Trust-Less Medical Data Sharing Among Cloud Service Providers Via Blockchain", *IEEE Access*, vol. 5, pp. 14757-14767, 2017.
[http://dx.doi.org/10.1109/ACCESS.2017.2730843]
- [17] C.G. Dagher, J. Mohler, M. Milojkovic, and P. Marella, "Ancile: Privacy-Preserving Framework for Access Control and Interoperability of Electronic Health Records Using Blockchain Technology", *Sustain Cities Soc.*, vol. 39, pp. 283-297, 2018.
[http://dx.doi.org/10.1016/j.scs.2018.02.014]
- [18] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, "MedBlock: Efficient and secure medical data sharing via blockchain", *J. Med. Syst.*, vol. 42, no. 8, p. 136, 2018.
[http://dx.doi.org/10.1007/s10916-018-0993-7] [PMID: 29931655]
- [19] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control", *J. Med. Syst.*, vol. 40, no. 10, p. 218, 2016.
[http://dx.doi.org/10.1007/s10916-016-0574-6] [PMID: 27565509]
- [20] G. Yang, and C. Li, "A design of blockchain-based architecture for the security of electronic health record (EHR) systems", *IEEE International conference on cloud computing technology and science (CloudCom)*, 2018pp. 261-265
[http://dx.doi.org/10.1109/CloudCom2018.2018.00058]
- [21] C. Gorenflo C, "FastFabric: Scaling Hyperledger Fabric to 20,000 Transactions per Second", *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pp. 455-463, 2019.
- [22] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management", *Proc. 2nd Int. Conf. Open Big Data (OBD)*, p. 25, 2016.
[http://dx.doi.org/10.1109/OBD.2016.11]
- [23] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology", *Sustain. Cities Soc*, vol. 39, pp. 283-297, 2018.
[http://dx.doi.org/10.1016/j.scs.2018.02.014]
- [24] J. Zhang, N. Xue, and X. Huang, "A Secure System for Pervasive Social Network-Based Healthcare", *IEEE Access*, vol. 4, pp. 9239-9250, 2016.
[http://dx.doi.org/10.1109/ACCESS.2016.2645904]
- [25] S. Jiang, J. Cao, H. Wu, Y. Yang, M. Ma, and J. He, "BlocHIE: A BLOCKchain-Based Platform for Healthcare Information Exchange", *2018 IEEE International Conference on Smart Computing (SMARTCOMP)*, 2018pp. 49-56
[http://dx.doi.org/10.1109/SMARTCOMP.2018.00073]
- [26] T. Dey, J. Shaurya, and K. Neha, "HealthSense: A medical use case of Internet of Things and blockchain", *International Conference on Intelligent Sustainable Systems (ICISS)*, pp. 86-491, 2017.
- [27] P. Thakkar, S. Nathan, and B. Viswanathan, "Performance benchmarking and optimizing hyperledger fabric blockchain platform", *IEEE 26th international symposium on modeling, analysis, and simulation of computer and telecom- munication systems (MASCOTS)*, pp. 264-76, 2018.
[http://dx.doi.org/10.1109/MASCOTS.2018.00034]
- [28] S. Ngamsuriyaroj, T. Likittheerameth, A. Kahutson, and T. Pathummasut, "Package delivery system

- based on Blockchain infrastructure", 7th *IEEE ICT International Student Project Conference*, 2018pp. 1-6
[<http://dx.doi.org/10.1109/ICT-ISPC.2018.8523944>]
- [29] D. Ichikawa, M. Kashiyama, and T. Ueno, "Tamper-Resistant Mobile Health Using Blockchain Technology", *JMIR Mhealth Uhealth*, vol. 5, no. 7, p. e111, 2017.
[<http://dx.doi.org/10.2196/mhealth.7938>] [PMID: 28747296]
- [30] J.D. Fearon, *What Is Identity (as we now use the word)?*, 1999. Accessed 2/1/2021. Retrieved from: <https://web.stanford.edu/group/fearon-research/cgi-bin/wordpress/wp-content/uploads/2013/10/W-at-is-Identity-as-we-now-use-the-word-.pdf>

Blockchain in Smart Healthcare Facility

Ayush Kumar Singh¹, Nipunika¹ and Deepak Kumar Sharma^{2,*}

¹ Department of Information Technology, Netaji Subhas University of Technology (Formerly known as Netaji Subhas Institute of Technology), New Delhi, India

² Department of Information Technology, Indira Gandhi Delhi Technical University for Women, Delhi, India

Abstract: Healthcare is an indispensable system whose efficiency and robustness are reliable indicators of a nation's prosperity. This sector has seen technological advancements not only in terms of medical equipment and drugs but also in varied fields such as Electronic Medical Records, wearable health monitoring devices, and telemedicine. In this chapter, we explore the aspects of utilising the disruptive technology of blockchain in healthcare. Ever since its initial use in cryptocurrency and finance, aiming to shift the industry from institute-centric to patient-centric, blockchain technology has found its use in healthcare. This chapter analyzes its use cases along with the limitations posed by traditional healthcare systems and how blockchain alleviates them. Furthermore, we will also walk through the roadblocks in implementing blockchain-based healthcare services and discuss a few implemented as well as proposed blockchain-based healthcare frameworks, highlighting their successes and failures.

Keywords: Applications, Blockchain, Electronic medical records, Electronic health records, Healthcare, Services, Supply chain.

INTRODUCTION

Blockchain technology came into existence in 2008 after Satoshi Nakamoto, a pseudonym for a developer or a group of developers, released a whitepaper with the title “Bitcoin: A Peer to Peer Electronic Cash System” [1]. Bitcoin became the first major cryptocurrency, with its peak market capitalization reaching 238 billion USD in the fourth quarter of 2017 [2]. Since its conception, Blockchain has been thoroughly researched for implementation in fields other than cryptocurrency and finance. The key features of blockchain include immutability, privacy, incorruptibility, and transparency, which makes it a suitable framework for implementing healthcare based applications. In this section, we will explore.

* Correspondence author Deepak Kumar Sharma: Department of Information Technology, Indira Gandhi Delhi Technical University For Women, Delhi, India; Tel: 8743075567; E-mail: dk.sharma1982@yahoo.com

the working of blockchain and its prominent use-cases. This will be followed by analyzing the traditional systems in healthcare and then we will look at an overview of how blockchain technology can reform the healthcare industry.

Technical Aspects of Blockchain

In its essence, Blockchain is a distributed public ledger. In other words, it is a decentralized database. There is no central authority in charge of its functioning and maintenance. This is the reason it enables peer-to-peer transactions, eliminating the need for a middleman. As the name suggests, a blockchain is a linear arrangement of blocks, which are its data units. These blocks can store data ranging from transaction records to medical records and even media. This linear arrangement is like an append-only data structure. New blocks can only be added to one of the ends of this chain. Every block has a hash value that uniquely identifies it. Further, the block also contains the hash value of the block previous (otherwise known as the parent block), which forms a link. The very first block of a blockchain, which has no parent block, is known as the genesis block.

Since there is no entity to verify which blocks are to be added to the ledger, blockchain makes use of various consensus algorithms to validate new blocks. All participating users agree to abide by a pre-defined consensus algorithm to decide on the concurrent state of the ledger and allow the blockchain to facilitate “trustless” transactions within the network. Every new block needs to be verified by the consensus algorithm before being introduced into the blockchain. The time it takes to verify and append a new block is known as the Block time of the network. It is about 10 minutes for the Bitcoin blockchain and about 20 seconds for the Ethereum blockchain [3]. Proof of Work (PoW) is a widely used and robust consensus algorithm that is used in the Bitcoin blockchain. It uses cryptographic hash functions, like SHA 256 to enforce security and integrity. A cryptographic hash function uniquely maps input data to a corresponding hash value. Also, it is a non-reversible function, so it is practically not possible to compute the input data from a given hash value. PoW protocol requires the users to put in some computational work to obtain a hash value for a block that satisfies some predefined condition. This condition is usually a number known as a nonce, which sets the “difficulty” for computing the hash. For example, the nonce can define the number of zeros with which the hash value must begin. Due to the “Avalanche Effect”, even a small change in the input data completely alters the corresponding hash value. Hence, the users who want to add a block have no other option but to brute-force till they find a combination that satisfies the given hash condition. Once a combination is found, other users in the network can simply run this combination with the cryptographic hash function and confirm

whether it satisfies the condition or not. This process of adding blocks to the blockchain is known as mining and the users who put in the computational effort to add the blocks are known as miners (see Fig. 1).

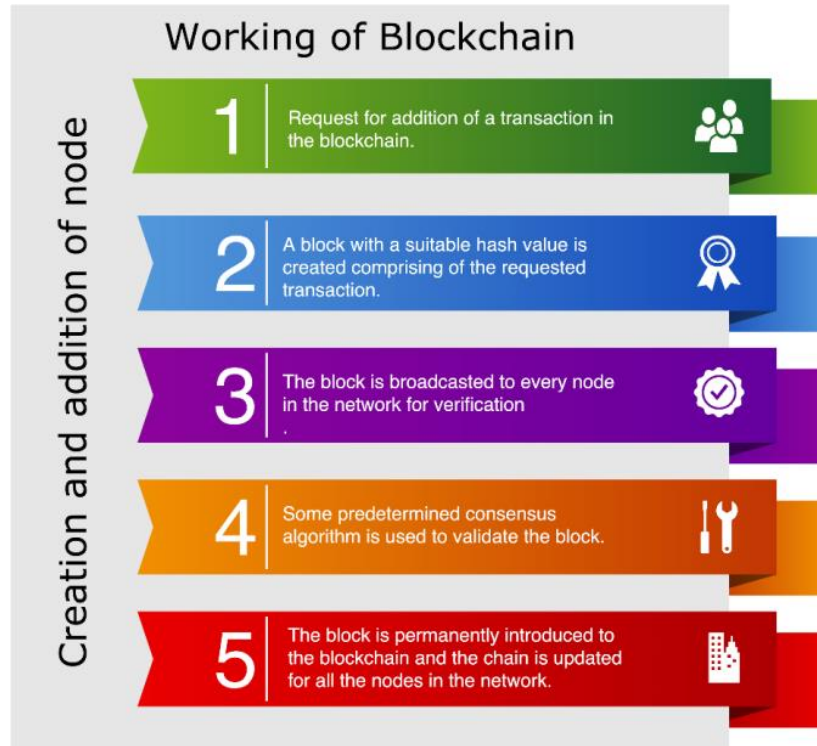


Fig. (1). Sequential working of Blockchain.

Some other consensus algorithms are Proof of Stake, Proof of Burn, and Practical Byzantine Fault Tolerance. While these algorithms differ in the way they are implemented, their functions remain the same; to validate new blocks and to make sure that only one version of the database exists in the entire network [4].

Applications of Blockchain

As of 2020, blockchain has been researched and implemented in numerous fields, proving the versatility of this technology. Following are some examples.

Voting

Blockchain has the potential to revolutionise voting. A blockchain-based voting

framework can offer security, privacy, reliability, and non-tamperability to higher standards than the traditional voting methods. The immutability of blockchain ensures that once a vote is placed, it cannot be tampered with. Tampering of votes remains a grave issue with traditional voting methods. In 2020, Malawi's constitutional court ordered re-election after investigations revealed that tallying forms had been tampered with in the general election of 2019 [5].

Blockchain allows voters to anonymously cast votes after some authentication. Further, it can maintain a real-time count of the votes cast. This saves the time spent in the collection and calculation of votes. This is exemplified by the 2019 fisheries council advisory board election in which the South Australian government contracted a blockchain-based startup Horizon State to host blockchain-enabled voting. The month-long election's result was immediately published once the voting concluded [6].

Identity Management

We often associate ourselves with different institutions or organizations that can be both public and private. To authenticate ourselves as a member of an institution or a valid benefactor of a scheme, we are given some sort of identity proof by the authorities. Moreover, to enrol ourselves in some new institutions, we may be required to present a set of previously owned identity proofs. Maintaining a separate identity proof for different purposes is a tedious task for consumers. Further, managing a centralized identity management system is effort and resource-consuming for the organization as well. The aspect of decentralization in blockchain technology can help alleviate these limitations.

A distributed ledger-based framework for identity management can help in securely maintaining personal identification information and also allowing this information to be seamlessly accessible whenever and wherever required. uPort is an example of such a framework that uses the Ethereum blockchain for identity management. It is an open-source project which aims to provide users to own and maintain digital identity and assets. Further, it facilitates secure disclosure of information to other users to organizations when required [7]. Another example of blockchain-based identity management is the Illinois Blockchain Initiative which aims to register the digital identity of citizens right at birth. Only the individual or their guardian will have permission to access the cryptographically sealed identity attributes [8].

Real Estate Records Management

Ownership of real estate is often a matter of dispute. This dispute can be between people, government, and people, or even between governments. In India, for example, land records are sometimes maintained by multiple authorities which may have conflicting information regarding the same land. Thus, these disputes are not easily resolved. Land registry is also a tedious process that requires the involvement of many stakeholders and middlemen. Blockchain technology, with the power of immutability and smart contracts, can help in tracking ownership records and ease the registration process.

In 2017, the government of Andhra Pradesh in India collaborated with Chromaway, a Swedish company, to set up a blockchain-based land registry system with the aim to reduce errors and administrative burdens [9]. Similarly, in 2019, South Burlington in the USA initiated a blockchain-based land title registry with the help of Propy, a real estate transaction management platform [10].

Traditional Technology in Healthcare

The Healthcare industry currently follows an institute-centric approach to health record collection resulting in hospitals and practitioners being solely responsible for the storage, sharing, updating, and collection of patient records. Let us look at how patient records are stored by hospitals.

Electronic Health Records

Earlier, most practises used Electronic Medical Records (EMR) before the implementation of Electronic Health Records (EHR). Despite sounding similar, EMRs and EHRs are vastly different. EMRs are essentially the digital form of a patient's chart from only a particular practice, *i.e.* different hospitals will have different EMRs for the same patient disregarding patient history. However, with the advent of medical tourism, immigration and the growing popularity of second opinions, real-time data sharing became the need of the hour making EHRs an indispensable tool to promote interoperability of medical records. EHR is now the most common form of digitally storing medical records which were specially built to share data with other healthcare providers and organizations.

Even though switching from paper to digital records aids secure and efficient data management, certain caveats need to be followed:

Security

The sensitive and personal nature of medical records demands extra precautions to ensure no tampering of data. Health Insurance Privacy and Accountability Act (HIPAA) of 1996 in the United States of America has a security rule which explicitly requires healthcare organizations to have security protocols in place to protect patient information but the level of security is left to be interpreted as per ability and means of the provider exposing a gap that can easily be exploited. EHRs achieve this by:

- A. Access control mechanisms that define who can access what data, this may avoid external attacks but is ineffective against internal attacks.
- B. Encrypting data using cryptographic principles which may impede interoperability since no universal standard of encryption has been agreed upon.

Furthermore, there needs to be a secure and reliable trail of access and change history so that it can be known who made what changes at which time to ensure maximum accountability.

Scalability

Healthcare is a heavy data generating industry, from entering patients' personal information to updating large-sized radiology images upon every test for every patient not only requires large reliable storage systems but also a robust database system to ensure role-based views and quick queries on large amounts of data. Back in 2011, the US healthcare industry stored 150 exabytes of data [11]. To deal with larger data, larger networks are required resulting in cost inflation which may not be favourable to many practices especially because these local networks are a bottleneck in system reliability. So even if a hospital spends millions of dollars on its EHR, it could only be accessed within the hospital and the EHR will only be as secure as its local network.

Patient-Generated Data

The potential of using millions of gigabytes of data from health tracking apps and wearables remains untapped in the status quo. Even though this well-labelled data could aid physicians and researchers alike, it remains fragmented, disconnected and unanalyzed.

There exists a myriad of apps, mainly aimed at tracking different indicators such as calories consumed and steps walked as well as wearable devices with built-in sensors to track more intricate stats such as blood pressure and heartbeat, which have enabled the existence of “Personal Health Records”(PHR). Unlike EHR, patients have agency over data collection and sharing of PHR making them more involved in the process of personal health monitoring. PHR however raises the question of reliability and authenticity of such data, who shall be held responsible if a faulty sensor results in a fatal misdiagnosis?.

Technological Requirements in the Industry

Data sharing in clinical trials is an extremely complicated and sensitive process not only because of the nature of data but also because of the sheer volume of stakeholders involved and their associated “views” of data. However, the requirements which make clinical trials technologically complicated and costly are the same requirements that make blockchain a perfect fit: scalability, immutability, traceability and various levels of data “views”. Blockchain will be worth USD 3 Billion to the pharmaceutical industry by the end of 2025 according to some estimates [12].

Counterfeit drugs flooding the market poses a huge problem for the pharmaceutical industry. These drugs contain either very few active ingredients or none at all causing great harm to public health. The production process of drugs is extremely delicate and carries huge liability issues so naturally blockchain can come to the rescue.

A lot of sensitive processes are carried out by the healthcare industry where accountability and extensive audit histories are a huge concern. From clinical trials, cancer registries to opioid prescription tracking, the cost of data accumulation, storage, update, and the query is incredibly high when compared to its low effectiveness for conventional database management systems. So blockchain has found a natural place in the industry.

Other Challenges

Since in the status quo, medical data is generated to aid the operational needs of healthcare providers rather than data analysis, it remains fragmented across various medical organizations. This fragmented, duplicate or incomplete data ends up increasing the average cost of patient care significantly.

Patients fail to have a unified view of their medical records which are scattered across various institutions. This institute-centric approach to data collection also takes away a patient's agency over their medical records. Everything from updating to sharing is the sole responsibility of providers. Data sharing with researchers or even other providers despite patient consent is slow and insecure. Previous providers generally need to be contacted by the new provider to send over previous patient records. This process is carried out at either end at the medical institute's speed. So if a cancer patient undergoing treatment needs urgent critical care in the nearest hospital, the previous provider would need to be contacted for medical records to ensure the new drugs do not affect the previous treatment.

USE CASES

Blockchain is one of the most popular and secure implementations of decentralized data management. It has applications well beyond financial services. As we have seen in the previous section that traditional healthcare technology has certain limitations where the common theme seems to be: a lack of accountability and trustworthy audit history and ineffective real-time data sharing. You can guess that blockchain technology has been tailor-made to tackle such issues, let us see how. In this section, we will look at some of the Use Cases of Blockchain technology in the Healthcare industry in detail.

Health Records

The Healthcare industry needs to move from an institute-centric to a patient-centric view of data. Since data is centrally controlled by several medical organizations, it has been fragmented causing a large cost overhead in its storage and retrieval. Centralized data control results in slow and ineffective data sharing especially with medical researchers. To truly achieve patient control, we must decentralized data storage through blockchain with cryptographic constraints to ensure data integrity and security. There are several barriers to the immediate implementation of blockchain, namely regulatory requirements compliance and technical barriers. As a result of which most immediate implementations focus on data validation, auditing and authorization [13].

Application in EHR

One of the most important, expensive and common pieces of software that almost all medical organizations invest in is Electronic Health Records(EHR) which is in

dire need of transformation as discussed above. Data security, interoperability and integrity remain an issue that can easily be addressed using Blockchain.

Security and Integrity

A role-based mechanism ensures that only authorized personnel can view or alter the information which is under their purview, gracefully shielding external attacks. This security is twofold as the blockchain technology in itself is secure from third-party intrusion with the added layer of role-based data access. Furthermore, the information stored on EHR should be trustworthy and tamper-proof which can easily be ensured with an extensive audit history implementation in the blockchain.

Scalability

Scalability refers to the ability of software to perform at the same speed even with large volumes of users/data being added. Scalability is a known issue in both blockchain and traditional EHR systems. Some implementations suggest storing data off-chain as the volume grows but more research is required before a definite solution can be reached.

Personal Health Records(PHR)

As discussed in the previous section, patient-generated health information is unintegrated with EHRs. PHRs can help patients control, access, and manage their data which is where blockchain comes in. Blockchain can allow patients to securely collect and manage their data with control over viewing and sharing rights while integrating this record with other mainstream records so that they can have a unified view of their data. Furthermore, blockchain can help connect this record system with other devices by ensuring data integrity with the help of consensus algorithms.

Successful Implementations

The most popular blockchain implementation of EHR is MedRec which is an Ethereum based project enabling users to have agency over access to their medical records. It offers a decentralized approach to data sharing and authorization. The permissions and audit logs are stored on the blockchain while the actual data is not. While the team is working on adding more functionality to this project, it still serves as a proof of concept in the medical community [14].

Another successful implementation that focuses on patient identity validation is Guardtime, a blockchain-based framework. It ensures data integrity and maintains an immutable audit trail by linking EHR data to a blockchain-based patient identity. Any EHR update is time-stamped and registered on the trail minimizing the risk of data manipulation [15]. Both of these implementations will be discussed in detail later in the chapter.

Internet of Medical Things

Ever since the advent of the internet and the advancements in semiconductor technologies, there have been consistent and fruitful attempts in developing and engaging in machine-to-human and machine-to-machine communication [16]. With the aim of modifying traditional devices and developing new devices to aid automation and data sharing, the Internet of Things (IoT) has depicted immense pervasiveness in varied fields. Using sensors and wireless technologies in specialised sectors has given rise to classes of IoT like the Internet of Military/Battlefield Things, Internet of Vehicles and Industrial Internet of Things. On similar lines, the Internet of Medical Things (IoMT) concerns itself with the application of IoT in smart healthcare.

Challenges Faced in IoMT

Like blockchain, IoMT has seen expansion, diversification, and the evaluation of the global IoMT market is estimated to be 72.02 Billion USD by 2021 [17]. IoMT includes wearable technology which allows for remote health monitoring and analysis. IoMT sensors can precisely monitor the vitals of the patient and make this data available to physicians and clinics in real-time. This helps in timely diagnosis and accurate prognosis of the patient's ailments. Apart from patient-centric care, IoMT also has applications in tracking the status of essential medical equipment like MRI machines to quickly locate the required equipment at the time of need. But, with the widespread adoption of IoMT devices, data collection and sharing from a great number of sensors is challenging. Further, IoMT frameworks deal with very critical and sensitive medical data, hence security and privacy are of utmost importance.

Blockchain in IoMT

In most cases, IoT services use cloud storage which makes the data vulnerable to all kinds of cyber-attacks including DDoS attacks. Using blockchain technology with IoMT greatly eliminates these issues. Being decentralised, removes the

possibility of a single point of failure which might erase or corrupt important medical data. Its immutability ensures that once uploaded, the data cannot be tampered by a malicious party. The public key cryptography preserves the privacy of the patient by only allowing concerned shareholders access to the data. There has been a considerable amount of research done and frameworks developed regarding the implementation of blockchain in IoMT. Seliem and Elgazzar proposed a hierarchical system with four primary layers which have various security algorithms and protocols to bolster privacy [18]. Their framework proved to be effective against DDoS, replay and man-in-the-middle attacks. Dilawar, Rizwan, Ahmad and Akram proposed a Proof of Work-based implementation of blockchain in IoMT [19]. Their framework aims to secure PHRs on a blockchain that can be viewed and updated by relevant participants in the IoMT network.

Although blockchain technology provides a secure and robust framework for IoMT generated data, it comes with its own set of caveats. The immense amount of generated data may overwhelm the storage capabilities of the blockchain. Presently, most of distributed ledgers are meant for small-sized data like transactions or records. One way to get around this issue would be to use a separate storage system to store the actual IoMT generated data and to only store cryptographic hashes on the distributed ledger. Even though it would help take the storage load off the blockchain, using centralized storage would make it vulnerable to some of the security risks which motivated the use of blockchain technology in the first place [19].

Clinical Trials

Data generated during clinical trials are used for research purposes or approval of new research treatments. The integrity of this data holds utmost importance for various stakeholders: researchers, journal editors, publishers, pharmaceutical companies, prospective patients and the general public. A huge amount of money is at stake, thus, security and data integrity are a priority [20].

Clinical trial data runs several risks such as intentional or unintentional data alteration. Naturally, the consequences of such data are dire for the discussed stakeholders. Hackers are greatly incentivized to manipulate clinical data to achieve expected results or selectively report the outcome of an experiment. The introduction of blockchain in healthcare for improved Clinical Trial Dataset Management would not only provide privacy to patient records but would also ensure that data shared among researchers and publishers is untampered. This would maintain confidence between various stakeholders as only authorized parties were given access to its creation and manipulation.

In the current paradigm, ensuring data integrity is not always feasible. Therefore, we need a system for data collection for trials immutable, secure and traceable which is where blockchain comes in. Wong, Bhattacharya, and Butte used data from a real clinical trial and a blockchain-based system as a proof of concept and tested its security and integrity [21]. They also assessed traceability by checking its audit trails. Their report concludes that such blockchain-based systems improve trial data management making it more secure and trustworthy while also making the process of overseeing trials easier and properly managed. Reproducibility and data sharing poses yet another challenge in clinical trial research making blockchain a well suitable solution. In such a situation, users will have higher control over their data, especially to concerning traceability of consent in clinical trials through Smart Contracts. Blockchain helps make clinical trials more trustworthy and transparent while ensuring data integrity and traceability.

Health Insurance

Health or Medical Insurance refers to the coverage provided by any insurance firm to the customer on the occasion of an accident, sickness, or some other injury that incurs medical expenses. Medical treatments are often costly procedures considering consultations, tests, medicines, and other expenses. Arranging large sums of money on short notice can be difficult. Health insurances play a very important role in the compensation for any medical treatment. In 2018, the value of the global health insurance market was estimated to be 3,153 Billion USD [22]. This value is only predicted to rise in the following years due to a general increase in medical expenses. Further, some public and private departments follow mandatory health insurance plans for their employees. Even with a deep level of pervasiveness in the healthcare department, the health insurance sector faces many inherent issues.

Smart Contracts to ease insurance claims

In most countries, the entire health insurance ecosystem is riddled with middlemen and involves a large number of stakeholders. As shown in Fig. (2), the exchange of information among the different stakeholders involved turns out to be quite a hefty and time-consuming task. These stakeholders include, but are not limited to, insurance companies, pharmacies, hospitals, testing laboratories, and other third-party administrators. Each stakeholder traditionally maintains their record of any patient's treatment that is relevant to them. Verifying insurance claims would require tedious interaction between the stakeholders, some of which still use paper-based records.

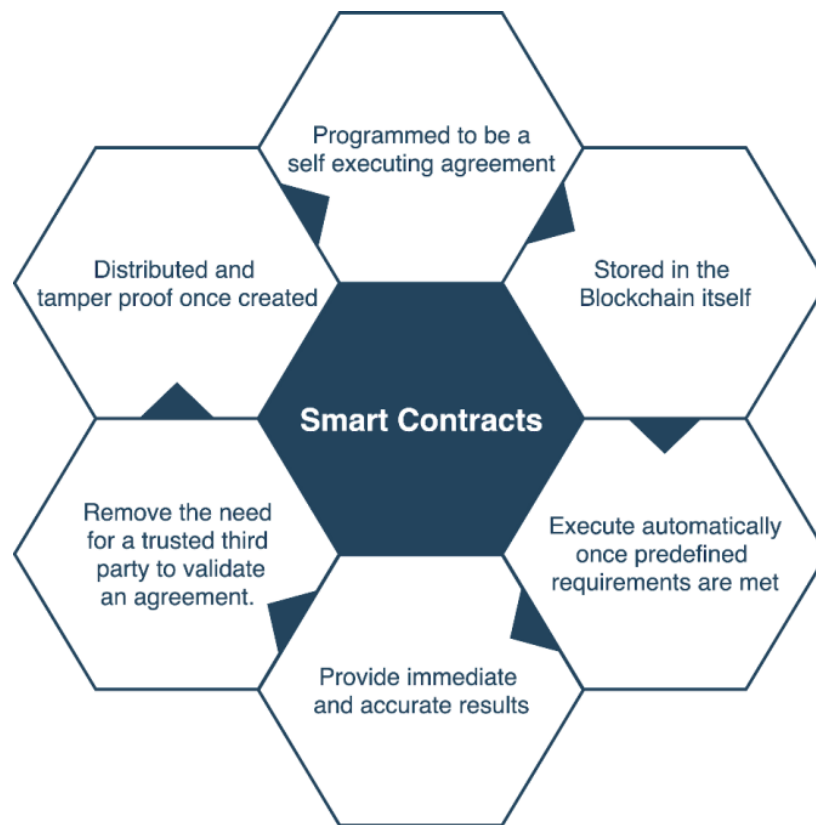


Fig. (2). Smart Contracts.

These issues can be skillfully addressed by the use of blockchain-based smart contracts. Essentially, smart contracts are functional protocols that are meant to execute once the predefined terms of the contracts are satisfied. Further, this can also alleviate the issue of maintaining several centralized records. Blockchain allows for a tamper-proof, transparent, and easily verifiable health insurance claim settling system which will greatly prevent any disputes. For example, smart contracts will directly update the blockchain once a premium has been paid by the customer. This will be easily verifiable by any other stakeholder without needing to communicate with the insurance agency for proof [23]. Zou, Wang, and Sun proposed MISore, a blockchain-based medical insurance storage system. MISore uses a Practical Byzantine Fault Tolerance as the consensus algorithm and its data is efficiently verifiable by the hospital staff, the patient, and the insurance company [24].

Health insurance fraud is a major problem that insurance companies around the world face. This can either be done by falsifying medical treatment or overstating

medical bills to get compensation. Insurance companies tend to lose millions of dollars due to these frauds and disputes. The transparency, auditability, and immutability of blockchain-based smart contracts will make these frauds virtually impossible.

Invoicing

Medical treatments often require many transactions between the patients and the hospital, pharmacies, or any other stakeholder involved. Maintaining billing details of all the transactions is not only cumbersome for the patient but also not friendly to the environment. These transactions are recorded on paper and maintained in files. Generating these bills takes a considerable amount of time as there are multiple levels of verification involved. Hence, oftentimes these bills have to be delivered via the post, adding to their cost. A large amount of human dependence on generating medical bills naturally increases the risks of errors in them. Medical records are very sensitive and crucial. Erroneous transactions or records can prove to be very problematic for the patient. Even if one of the pages of the entire invoice goes missing, it may lead to the loss of precious information.

E-Invoicing and Blockchain

Implementing blockchain technology in invoicing can help alleviate all the previously mentioned concerns of traditional billing. Although E-Invoicing has been around for quite some time now, the use of blockchain to empower the process is relatively recent. Since blockchain was initially used in recording transactions of cryptocurrencies, using the technology for invoicing is a similar use case. Being decentralized removes the risk of a single point of failure which might wipe out crucial information. Apart from being immutable and transparent, blockchain also ensures complete digitalization of the process; making it cheaper, more efficient, and environment friendly. This directly saves time and resources for the patients as well as the stakeholders. Blockchain in e-invoicing has been tried and tested. In March 2019, the Shenzhen Metro System in China began using blockchain-issued rail transit invoices, handling over 170,000 invoices daily [25].

Large Scale Implementations

China has been very successful in the execution of distributed ledger technology to aid medical billing. In 2019, Alipay and Ant Financial helped in the development of the blockchain-based Zhejiang's medical bill platform. The Zhejiang's Provincial Department of Finance declared that 41.7 Billion Yuan in

medical bills was processed on the platform. This not only prevented long billing queues but also sped up the insurance claims. Further, the average medical visits of the patient were reduced from 6 to 2. This saved hospitals' administrative time and resources [26].

In June 2020, Fuzhou Second Hospital of the Fujian province successfully launched a blockchain-based medical bills platform. The platform was developed to counter some issues like excessive paper wastage and the prevalence of counterfeit bills. Users can retrieve their invoices either directly on their phones using WeChat or visiting a self-service kiosk [27].

Supply Chain Management

With the tremendous increase in manufacturing processes around the world, we have an increasing need for transparency between suppliers and supply chains. Distributed Ledger Systems in blockchain offer end-to-end decentralized processes that make their system transparent. Blockchain offers real-time tracking of goods and services which is of particular interest to Multinational Corporations (MNCs) having multiple supply chains.

Let us recount why blockchain technology is suited for its previous use cases: transparency, traceability, and security which is exactly why supply chain management is another important application. The globalization of a supply chain has made it difficult to keep track of the management. When you buy something as small as a shirt, you cannot know where every material which was used in the shirt was sourced from, reducing the accountability of any big brand selling a product, aiding exploitation of labor and natural resources along the supply chain of a product. What could all of this mean to a pharmaceutical company? Imagine every transaction having a traceable and secure history so that when a final party receives a product, they can be sure of the source and price of every material without any intermediaries which is exactly what blockchain offers.

Various geographically distributed intermediaries serving several MNCs make modern supply chains inherently complex. Currently, companies rely on single departments to maintain their supply chains offering one single point of failure in case anything goes wrong [28]. Modern supply chains are centralized and rely on trust between parties to store sensitive information [29]. These issues suggest that the current framework for supply chain management is falling behind and unable to address the needs of the time. We shall look into blockchain as a framework for supply chain management with sustainability as an added dimension and issues in its practical implementation.

Blockchain-based Supply Chain Management

Unlike other applications of blockchain, supply chain management may require a close and private network [30]. Mainly, the following players are involved in blockchain-based supply chain management: Registrars, Standard Organizations, Certifiers, and Actors.

If an actor wants to sell a product to another actor, they need to authenticate the transaction by either signing a digital or smart contract then transactional details are updated on the ledger. From that point onward, other details are automatically updated [31]. The ledger can also store and update important information about the product such as quality, ownership, *etc.* maintaining a trustless decentralized supply chain.

Sustainability

As mentioned earlier, tracking the manufacturing process of every product is a complex task but it is incredibly important to ensure that at no point in the process does the product raise any environmental, health, or safety concerns [32].

Since blockchain-based supply chains are immutable, no one can modify any information without authorization which is then registered on the blockchain thus preventing any corrupt entities from supplying dubious products or services contributing to social supply chain sustainability. It can also aid in environmental supply chain sustainability, by tracking damaged or hazardous products and recalling them as soon as a problem is identified.

Limitations in Implementation

Supply chain management is less about a product and more about the management of relationships between suppliers and customers to create value for stakeholders [33]. Blockchain enables transparency of information that may be unacceptable to certain parties which assume their information gives them a competitive advantage. Blockchain technology isn't exactly simple or compatible with existing technological frameworks. Implementation of blockchain-based supply chains would require an overhaul of the entire existing framework which can prove to be a very expensive deal for most pharmaceutical companies. In current proof of concept implementations, transaction logs are not protected. Further work is needed to ensure the security of sensitive information which several companies are very keen on protecting [34]. So a lot of discussion and

research is required before we can think about changing the landscape of supply chain management.

CHALLENGES

Blockchain technology has some inherent technical problems and bottlenecks. In this section, we will discuss two of these problems in detail and why they need to be considered before implementing this technology in healthcare.

Security

In the previous sections, we have discussed that medical information is not only crucial but also very confidential. Securing the privacy and integrity of this information is of utmost importance. This has incentivized hackers around the world to increasingly participate in the lucrative business of hacking medical data. In the USA, over 32 million healthcare records were breached in a duration of just 6 months (January 2019 to June 2019). This number is twice the total number of breaches in all of 2018 [35]. This alarming increase is a direct result of the widespread adoption of electronic means of storing medical records by hospitals. But as previously mentioned, the electronic frameworks used by hospitals are often incompetent in safeguarding medical information from hackers. They are mostly developed to make the process easy and efficient for the medical staff and the patients. Furthermore, this data has multiple points of exposure during the process. This can be when it is transferred from one medical stakeholder to the other, like transferring prescriptions to the pharmacy. Hackers can exploit these vulnerabilities to gain access to and sell these records on the black market [36].

Hence security is a very compelling reason to incorporate blockchain in a healthcare facility. Blockchain technology indeed is much more robust than traditional frameworks as it uses cryptographic hashing, consensus algorithms, and immutability to ensure security. But like any other disruptive technology, blockchain also has some inherent security flaws. These security issues are mostly exclusive to the blockchain as they exploit its certain key aspects. The following are two security threats that can be a cause of concern in a blockchain-based healthcare framework.

51% Attack

Also known as the majority attack or the double-spend attack, this kind of attack exploits the 51% vulnerability of blockchain consensus mechanisms. If a miner,

or a pool of miners, gains control of over 50% of the computing power of the entire network, they can essentially control the entire blockchain. This will allow them to modify transaction data and reverse transactions which cause double-spending. Further, this will disrupt the normal functioning of other miners in the network. In 2018, the cryptocurrency Bitcoin Gold suffered a 51% attack for several days and the attackers double-spent at least USD 18 million [37]. In January 2014, GHash.io, the largest bitcoin mining pool at the time, gained control of 42% of the network's computing power dangerously approaching the 50% mark. It had to voluntarily reduce its computational involvement and the pool operator released a statement declaring that the pool would not initiate a 51% attack on bitcoin. In a healthcare facility blockchain framework with consensus protocols where there won't be many actors, to begin with, initiating a 51% attack would be relatively easy [38].

Criminal Smart Contracts

We have discussed how smart contracts can be used in many ways to automate otherwise resource and time-intensive works. Smart contracts can be used to verify billing and also authenticate insurance claims. Further, new Turing complete programming languages are emerging for the sole purpose of developing smart contracts. A solidity is an object-oriented programming language for developing smart contracts for many blockchain networks like Ethereum. However, there are some critical risks involved with smart contracts. Those smart contracts capable of undertaking illicit activities are known as Criminal Smart Contracts (CSC). CSCs can be programmed for private key theft and exposing other private data. An example of a CSC can be a contract that rewards after the delivery of some private information. In a healthcare facility scenario, CSC can be used for fraudulent insurance claims or leaking private medical information. Technically, there is a scope for implementation of CSC in all the units which make use of smart contracts [38, 39].

Scalability

One of the biggest concerns in the practical implementation of blockchain is scalability. Even in the case of bitcoin, a transaction speed depends on network congestion. If a network has a higher number of nodes then it will be greatly slowed down. From image-heavy and abundant health records to complex supply chains of drugs, we can easily expect a high number of nodes holding copious amounts of data making scalability a key concern for most practitioners. Scalability refers to the ability of applications, programs, networks, *etc.* to improve or at least retain their efficiency even when it serves an increasingly large

number of users. So far in most proof-of-concept implementations of blockchain in the healthcare industry, efficiency has not been much of a concern so it has not been dealt with properly and remains a key area for discussion and research. Even in bitcoin, the most popular application of blockchain, efficiency is much lower than its traditional centralized counterparts. Bitcoin handles maximum of 7 transactions per second [40] whereas VISA handles 65 thousand transactions per second.

Why is Blockchain so Slow?

As blockchain technology relies on peer-to-peer networking and a consensus algorithm, it has a much slower transaction processing time than centralized networks. A valid transaction has to satisfy proof-of-work which is a heavy time-consuming process. So when requests for multiple transactions pile up on a network, it slows down the system greatly. The security of a network is dependent on the efficiency of the consensus and proof-of-work mechanism which is directly proportional to the size of a block in the chain. However, the time taken to append a block and thus, process a request is inversely proportional to the block size. Therefore, to have a security system, you will need to compromise transaction speed and *vice versa*. This issue becomes even graver when you couple blocks size with data-heavy health records. In bitcoin, the upper limit for a block size is 1MB whereas its 2MB for Ethereum handles 7 transactions per second and 15 transactions per second respectively. The Healthcare industry has large data needs and blockchain needs to find a way around them by providing both security and speed.

Managing Storage Capacity

Blockchain is designed for systems that don't need large storage but the healthcare industry doesn't come under that scope. Health records, patient history, detailed audit trails, heavy image scanning, and test results mean that the storage capacity of each node needs to be humongous. Data heavy nodes in the chain also imply that the cost of querying and accessing data will be proportionally increased.

CASE STUDIES

In this section, we will explore some successfully implemented and proposed blockchain-based healthcare frameworks in detail.

Gem Health Network

Founded in November 2013, Gem is a California, USA-based company that provides cryptocurrency and distributed ledger-based enterprise-level enterprise-level solutions. An established startup, it raised USD 7.1 Million in its Series A funding round. It had already raised USD 4.9 Million in its seed round. Conceptualized in the initial days of blockchain technology, Gem has been pioneering the use of blockchain technology for financial solutions since its advent. But in 2016, it entered the healthcare stage and launched Gem Health Network.

The primary motivation behind the development of a healthcare framework was the glaring increase in medical data “silos”, which essentially are private databases maintained by medical institutions, professionals, and other stakeholders. Retrieval of data from one “silo” for it to be transferred to another is a resource-intensive and error-prone task. For example, consider a patient who is being treated by their local doctor. If the patient needs to travel to some other place, to continue their treatment they will either need to have an entire copy of their medical history, diagnosis, and treatment schedule or set up a way to quickly retrieve this data from their local doctor. This issue of interoperability can be life-threatening because of the lack of a data storage or transfer protocol. Further, this also involves an Information Security dilemma of the trade-off between data access and data protection which means that increasing data security compromises data availability and *vice versa*. Gem Healthcare uses blockchain to address this issue by incorporating identity schemes and decentralized data storage. It allows for a transparently shared infrastructure where each medical stakeholder has access to the same information and can trust each other reliably.

The Gem Health Network was developed using the Ethereum blockchain, which provides the initiative with highly functional tools to build a stable, continuously evolving, and multi-faceted platform. The CEO of Gem, Micah Winkelspecht, aims to create a blockchain-enabled global repository where medical data integrity is maintained. In the ideation phase of Gem Health, the company was mostly approached by active physicians who were discontented with their present technologies and wanted a platform that allowed the different medical stakeholders to collaborate. Moreover, various healthcare companies also reached out to Gem Health including Philips Blockchain Labs, the research and development department of Philips healthcare. The support and partnership from a prominent healthcare operator ensured that the research for the use of blockchain in patient-centric healthcare would be extensive [41].

In October 2016, Gem announced the development of GemOS which is a platform allowing different blockchains to connect and interact. Using the GemOS infrastructure, companies can develop their blockchains on Ethereum, Hyperledger, or any other provider, and can connect to the GemOS network for automation and sharing of information between different networks. GemOS prospects to become a core platform for different healthcare institutions and departments to interact seamlessly and securely using blockchain technology [42].

MedRec

Azaria, Ekblaw, Viera and Lippman of the Media Lab of Massachusetts Institute of Technology proposed MedRec, a blockchain-based EMR management system. The motivation behind the research and development of MedRec was the lack of a standard protocol for interoperability between different healthcare providers and stakeholders who maintain their private records. In analogy, financial systems also have different stakeholders and depositories like banks, credit and debit cards, loans, and so on. But these systems are substantially interoperable because they share a common infrastructure of currency. Medical records of different stakeholders are largely incompatible to allow for a smooth exchange of medical information.

Technicalities

In August 2016, MedRec began its operations in the Beth Israel Deaconess Medical Centre in Boston, United States. This was the first implementation of MedRec also known as MedRec 1.0. Currently, MedRec 2.0 is under development and differs significantly in the way it is developed. MedRec 1.0 uses small private blockchain and used the Proof of Work (PoW) consensus mechanism which is also used in the Bitcoin blockchain. MedRec uses PoW innovatively to incentivize its miners in two ways. The first way is to reward them with Ethers, the currency of Ethereum, and the second way is to provide them with anonymized medical data of users. Medical data is required to conduct medical research hence researchers will be incentivized to mine. MedRec does not technically store medical data on the blockchain. Instead, it contains the metadata required, like authentication and location, to retrieve the data. It employs three types of smart contracts for this.

- a. Registrar Contract (RC): MedRec caters to many medical stakeholders like patients, doctors, lab technicians, and insurance companies. They would need to have individual access to the patient's medical records. Hence, they are

given Ethereum address identities which are equivalent to public keys. The RC maps individual IDs of the stakeholders to their respective Ethereum address identities.

- b. Patient-Provider Relationship Contract (PPRC): This is an implementation of pairwise data stewardship. In the case of MedRec, this refers to the interaction when the patient queries for some data and the provider return the required data from its database. This interaction is regulated by a predetermined protocol. The queries are in the form of SQL queries which allows users to have a high level of filtering and efficiency.
- c. Summary Contract (SC): This is essentially a database that contains all the interactions made by a user. For a patient, this may be reference to all their medical providers and for providers, this may be reference to all the patients that they have encountered. Hence this allows the stakeholders to have a complete record of all of their previous and ongoing interactions. Further, this acts as a backup in case any of the network participants drop out of the network and rejoin later. SC also enables notifications for all the participants whenever a new interaction is made. Each participant can approve exactly who they want to share their information with.

MedRec 2.0

To improve security and scalability, Solidity and Go Ethereum are used to develop MedRec 2.0, unlike Pyethereum and Serpent libraries which were used in the development of MedRec 1.0. Also, the second version of MedRec does not use PoW as its consensus algorithm. Instead, it uses Proof of Authority (PoA), which saves the excess computation required in mining. This mechanism uses the healthcare providers themselves to provide consensus. This is because the healthcare providers are already trusted parties, hence it is logical to have them maintain the blockchain securely and efficiently [14, 43].

Guardtime

The government of Estonia has been a global leader in blockchain technology. It partnered with a startup called “Guardtime” mere three years after the publication of Satoshi Nakamoto’s paper on distributed ledgers. In 2011, Estonia decided to protect their public records using blockchain, and then again in 2016, they declared their intention to secure over 1 million health records using blockchain in a GovTech partnership with Guardtime.

The success of this venture will be a critical factor in deciding whether blockchain is successful in increasing the security of health records while also making them

widely available to millions of medical professionals with ease. This project has been supported by Estonia's Health Information System Act of 2007 and the Government Regulatory Act of Health Information Exchange in 2008 [15]. Standardization of such health records remains a key concern with the government as their national blockchain encrypted data will require global acceptance and more discussion on protocols for digitally storing medical information. Even though shifting the entire healthcare infrastructure to a blockchain-based infrastructure will require more research, discussions, and capital investment, this innovative step taken by the Estonian government is concrete proof that it is certainly possible.

New Ventures

We are already seeing the payoff as Guardtime has also partnered with 10 pharmaceutical companies to work on blockchain-based contracts with actual patients [44]. This project also led to the development of the MyPCR platform [45], jointly launched by Guardtime, Instant Access Medical and Healthcare Gateway. Medication non-adherence is a rampant problem in the industry that affects everyone from insurance companies to patients. This is where MyPCR comes in, electronically monitoring all patients and ensuring that they follow their own specific and specialized Personal Care Pathway(PCP). MyPCR will be available to 30 million UK NHS patients and is estimated to have potential savings of 290 billion USD in the US and 800 million GBP in the UK. This application will provide its users instant access to their medical information, PCPs, and online support through Medical Interoperability Gateway owned by Healthcare Gateway.

Medicalchain

Founded in 2016, Medicalchain was conceptualized by Dr. Abdullah Albeyatti who is currently the CEO of the company. The initial developments of Medicalchain were in terms of discharge summaries which are detailed descriptions of a patient's entire interactions with their hospital. The motivation behind Medicalchain was that these summaries have to be written by doctors with immense attention to detail. This ordeal is error-prone, and Johns Hopkins estimated medical errors to be the third leading cause of death in the USA after heart disease and cancer [46]. Medicalchain eventually expanded its horizons in the healthcare sector and has become a blockchain-based comprehensive healthcare ecosystem with diverse applications. To cater to its different use cases, it is built on a dual blockchain structure. For medical records management, Hyperledger Fabric is used and other services use the ERC-20 token of the

Ethereum blockchain for smart contracts and token application. Medicalchain has its token by the name of MedToken which participants can use to conduct payments in the system.

Medicalchain Solutions

4.4.1.1. Secure Decentralised Records

As previously discussed, the primary concern of any healthcare framework is the prevalence of mutually incompatible siloed medical records. The Hyperledger blockchain used by Medicalchain is a closed permission-based network. It uses symmetric key cryptography with 2048 bit RSA keys. It manages identity and levels of authorization. For example, the patient would be allowed to create, update and read their medical records. But medical researchers would only be allowed read access to permissioned records. Further, patients can grant access to their doctors to view limited or all of their medical records. In case of emergencies, if the patient is not in the capacity to operate the Medicalchain platform, there is a provision of an emergency bracelet worn by the patient which can be scanned after following proper protocol. This would unlock parts of the medical records which were pre-determined by the patient.

Telehealth

Globally, the digitization of medical treatments is on the rise. In 2019, the Telehealth market was valued at USD 61.4 Billion and by 2027, it is estimated to rise to USD 559.52 billion [47]. But the problem of siloed data persists even with telehealth treatments. Due to a lack of standardization in this field, many telehealth frameworks have not incorporated financial systems which makes the process inefficient. Medicalchain has provisions for remote consultations with real-time sharing of medical records securely with the consent of the patient. Further, patients can pay using MedTokens directly. This is more efficient than the traditional process of setting appointments, traveling to the healthcare facilities, and conducting transactions.

Research and Insurance Claims

Since the process is entirely patient-centric, researchers will no longer have to approach hospitals and clinics for relevant medical data. They can directly interact with the patients who, for example, can consent to reveal medical data for some study. This can also be anonymized and patients can choose the amount of

medical data they wish to reveal.

Patients can also allow their insurance agencies to access their medical records to verify claims. There can also be an integrated insurance system that makes use of MedTokens for transactions [48].

OmniPHR

As we saw earlier, interoperability is a major issue in EHR and PHR maintenance. These records are created and maintained by specific organizations for their exclusive use with restricted access. Several organizations even maintain outdated records indefinitely and do not update their records because of an unwillingness to share this data with other practitioners. One of how omniPHR divides up data for efficiency is a logical division of health records such as imaging data, lab results, *etc.* with security features for personal data. The fundamental unit of this logical division will be referred to as a “data block”.

Overview

When we talked about EHR and PHR in previous sections, we aimed to achieve a unified view of all health records scattered across different organizations and “wearables” and to do so in a scalable and efficient manner. This is the motive behind making omniPHR. The data blocks in omniPHR are distributed in a network composed of nodes, each of which belongs to a subnetwork. Each device that connects to this network can either provide medical data as a “provider” or obtain a unified view of existing data as a “consumer”.

4.5.1.1. Superpeer node

In a P2P network, a superpower or ultapeer will act as a server to clients and as a peer to other super peers [49]. OmniPHR proposes a model where such superpower nodes will serve a variety of functions in routing overlay such as maintaining system user registers, creating and updating data blocks, maintaining audit and access trails, *etc.* Such nodes are supposed to be horizontally scalable and elastic to make the network much more efficient.

Design

As you can see in the diagram, all information is collected from trusted sources such as EHRs, EMRs, and health wearables which are then passed through the

user interface to the middleware and then onto the repositories as shown in Fig. (3) [50].

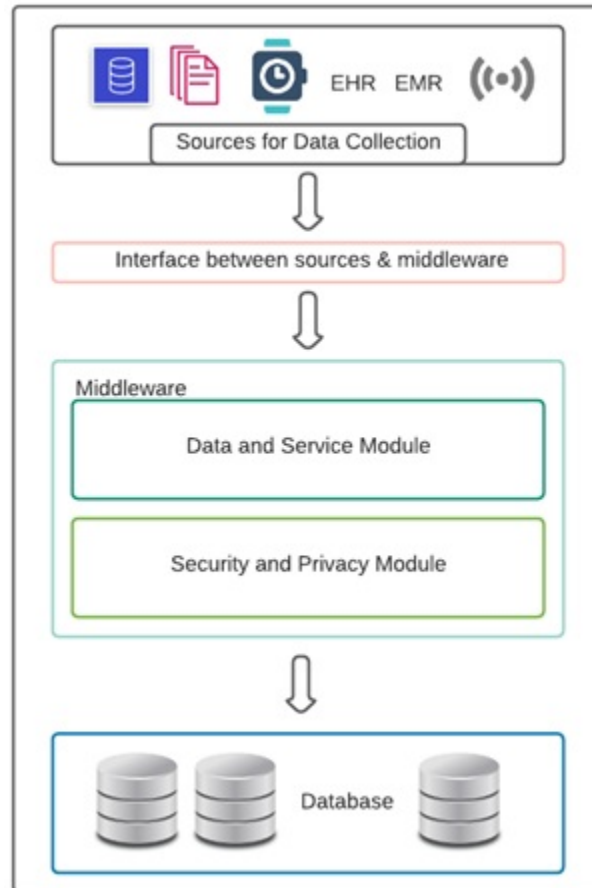


Fig. (3). Architecture of OmniPHR.

Datablock and Service Module

This comprises 5 submodules:.

- a. **Translator**: if the source data block follows a different standard than omniPHR, this module translates the data block into an equivalent omniPHR standard ensuring interoperability.
- b. **Distributor**: essentially in charge of fetching and replication desired data blocks.

- c. **Nodes Manager:** every node has to go through this component to be added to the network.
- d. **Validator:** ensure data integrity and consistency of the nodes.
- e. **Message Router:** packages and routes messages to and from nodes.

Security and Privacy Module

This module also comprises several submodules which work in tandem to maintain the privacy and security of each data block. It encrypts the data block as well as all its references, serves, or denies access requests based on access profiles, and registers and maintains access profiles.

MediBchain

This framework was proposed to mitigate the recent rampant cyber-attacks on sensitive healthcare data. In current data preservation models, data is accountable to the system, *i.e.* data first needs to be accessible to the system which will then encrypt and store it on the blockchain. The system here acts as a gateway through which we must pass to store, access, or share data. MediBchain proposes (see Fig. 4) storing the encrypted data directly in the system eliminating its role as a gateway, therefore, making the user themselves accountable for their data [51].

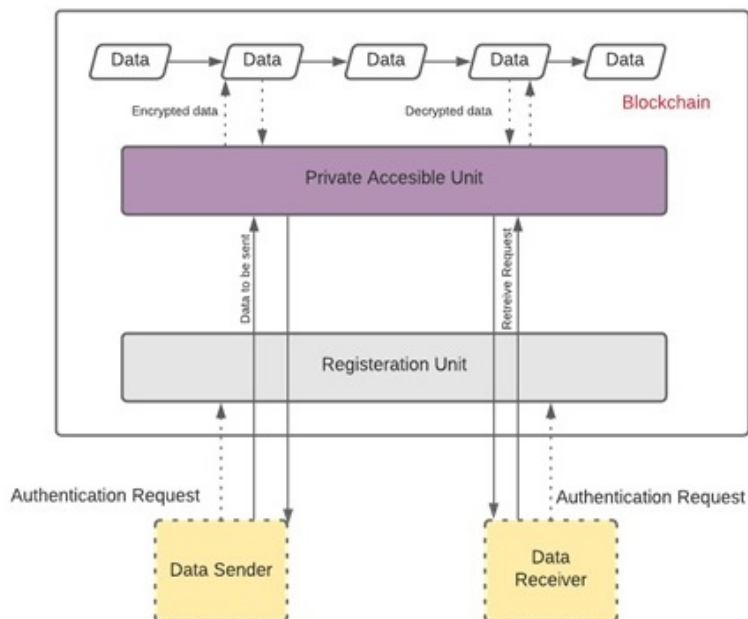


Fig. (4). Architecture of MediBChain.

MediBchain promises pseudonymity, data integrity, and security to its users. Either a data sender or a data receiver can interact with the system. Its system only consists of the blockchain storing data and outside channels consist following crucial components:.

Registration Unit: used to authenticate every user and map them to a unique ID.

Private Accessible Unit: accessible only after proper authentication, can request services from the main system.

Protocol for Sending Data to the System

The flowchart of MediBchain's protocol is shown in Fig. (5).

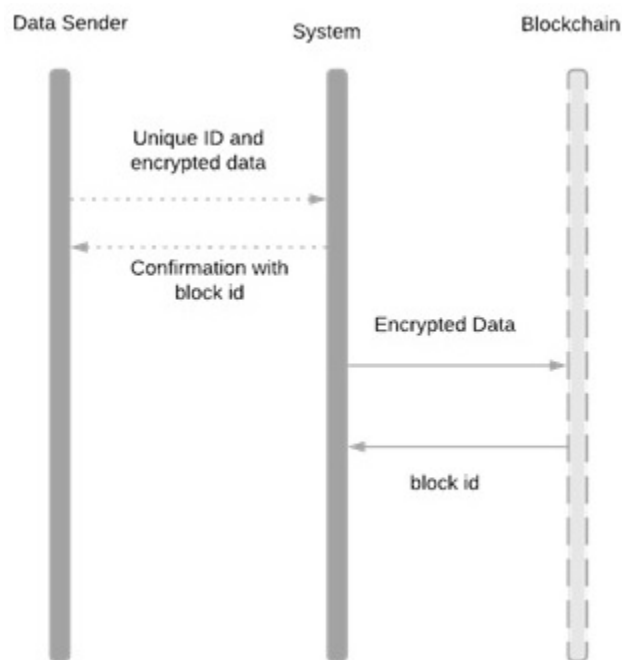


Fig. (5). Flowchart of MediBchain's protocol.

Step I. Data Sender provides its unique identifier and is authenticated to enter the system.

Step II. Data Sender sends encrypted data to the blockchain. Each authenticated user has its key which can be used to encrypt and decrypt data through an encryption function. In this step, the user is directly communicating with the blockchain and this will be managed through a smart contract.

Step III. When the data is successfully stored on the blockchain, a unique ID will be returned to the sender which can be used in conjunction with the user ID to access this information again.

FURTHER DISCUSSION

Blockchain technology has come a long way since its inception in cryptocurrency and finance. But being disruptive, there still are concerns regarding its standardization, regulation, and widespread adoption in the field of healthcare. Almost every traditional system in healthcare and other public or private sector enterprises is entirely backed by a central authority. Hence, the introduction of a decentralized framework in these fields is often inconvenient. To ease this transition and also incorporate the reliability that comes with a central authority, permissioned blockchain can be used in these fields. This partial decentralization can be achieved by making use of private blockchains where an organization will run its network. In healthcare, a more suitable type would be consortium blockchain, where multiple organizations run the network. This semi-private system would allow for different medical stakeholders to exchange information in real-time securely [52, 53].

In the case of public blockchains, which mostly rely on consensus algorithms, suitable consensus algorithms need to be developed for healthcare-specific implementations. This is because a blockchain based healthcare framework will have a relatively smaller number of participating nodes as compared to bitcoin or other cryptocurrencies. Hence, using Proof of Work like consensus algorithms might be too computationally intensive for the network. We saw that Medicalchain worked around this issue by incentivizing medical professionals and researchers to act as miners in the network and be awarded precious medical information required for research [54 - 57].

The amalgamation of IoT with blockchain has proved to be revolutionary too. In terms of medical innovation, the Internet of Medical Things is thriving on the previously done concrete research on IoT and blockchain too [58, 59].

With systematic research and development, blockchain has the potential to transform the healthcare sector by making it patient-centric and robust at the same time. With its current rate of involvement and acceptance in healthcare, blockchain is expected to find even more use cases and implementations in the coming years [60 - 63].

SUMMARY

We started this chapter with an elaborate introduction to blockchain technology digging into its technicalities followed by a discussion on its vast applicability in areas other than Healthcare. Since one of the major applications of technology in Healthcare is medical records collection we also spoke about the current methods of storing medical information and its limitations.

In the next section, we moved on to the various areas within Healthcare where blockchain technology will prove useful such as health record management and Internet of Medical Things (IoMT), a subset of IoT. Several areas of research interest and huge monetary value to pharmaceutical companies are brought up in this section such as Blockchain in Clinical Trial Management, Health Insurance, Invoicing, and Supply Chain Management.

So far we had only focused on blockchain as a positive transformative force within the healthcare industry which begs the question of why has it not been globally implemented. Therefore, in the next section, we discussed the limitations of blockchain namely in terms of security and scalability. In the penultimate section, we took a look at several successful implementations of blockchain technology within the healthcare industry. Here, we discussed everything from the motivation behind the project to its design and loopholes.

We wanted the reader to leave this chapter with an inquisitive mind and look up further information which is why in the next section we discussed upcoming areas of research that are of interest to healthcare, standardizations to transition from outdated technologies to blockchain, and how different blockchain in healthcare will be from blockchain in traditional private enterprises. In the end, we can safely conclude that blockchain is a truly disruptive technology in healthcare that still needs wider acceptance and more research to transform the industry.

CONSENT FOR PUBLICATION

Not applicable.

CONFLICT OF INTEREST

The author declares no conflict of interest, financial or otherwise.

ACKNOWLEDGEMENT

Declared none.

REFERENCES

- [1] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain", *Bus. Inf. Syst. Eng.*, vol. 59, no. 3, pp. 183-187, 2017.
[<http://dx.doi.org/10.1007/s12599-017-0467-3>]
- [2] "Statista. 2021. Bitcoin market cap 2013-2021", *Statista*, 2021. [online] Available at: <https://www.statista.com/statistics/377382/bitcoin-market-capitalization/#:~:text=The%20market%20capitalization%20of%20Bitcoin,circulation%20by%20the%20Bitcoin%20price>
- [3] Investopedia. What is block time in cryptocurrency?, [online] Available at: <https://www.investopedia.com/terms/b/block-time-cryptocurrency.asp#:~:text=Block%20time%2C%20in%20the%20context,its%20own%20defined%20block%20time>
- [4] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: a survey", *Int. J. Web Grid Serv.*, vol. 14, no. 4, p. 352, 2018.
[<http://dx.doi.org/10.1504/IJWGS.2018.095647>]
- [5] BBC News. 2021. Malawi election: Court orders new vote after May 2019 result annulled, [online] Available at: <https://www.bbc.com/news/world-africa-51324241>
- [6] SmartCompany, "SA government uses startup Horizon State's democratic blockchain in fisheries council election - SmartCompany", [online] Available at: <https://www.smartcompany.com.au/startupsmart/news/horizon-states-democratic-blockchain-fisheries-council-election/>
- [7] P. Dunphy, and F. Petitcolas, "A First Look at Identity Management Schemes on the Blockchain", *IEEE Secur. Priv.*, vol. 16, no. 4, pp. 20-29, 2018.
[<http://dx.doi.org/10.1109/MSP.2018.3111247>]
- [8] GovTech, "Illinois Announces Key Partnership in Birth Registry Blockchain Pilot", [online] Available at: <https://www.govtech.com/data/illinois-announces-key-partnership-in-birth-registry-blockchain-pilot.html>
- [9] V. Thakur, M. Doja, Y. Dwivedi, T. Ahmad, and G. Khadanga, "Land records on Blockchain for implementation of Land Titling in India", *Int. J. Inf. Manage.*, vol. 52, 2020.101940
[<http://dx.doi.org/10.1016/j.ijinfomgt.2019.04.013>]
- [10] P. Blog, "South Burlington in Vermont to Use Propy's Technology", [online] Available at: <https://propy.com/blog/south-burlington-in-vermont-to-use-propys-technology/>
- [11] A. Mazlan, S. Mohd Daud, S. Mohd Sam, H. Abas, S. Abdul Rasid, and M. Yusof, "Scalability Challenges in Healthcare Blockchain System—A Systematic Review", *IEEE Access*, vol. 8, pp. 23663-23673, 2020.
[<http://dx.doi.org/10.1109/ACCESS.2020.2969230>]
- [12] PreScouter, "Blockchain in Healthcare & Life Sciences - PreScouter", [online] Available at: <https://www.prescouter.com/press/blockchain-in-healthcare-life-sciences/>
- [13] S. Angraal, H.M. Krumholz, and W.L. Schulz, "Blockchain Technology", *Circ. Cardiovasc. Qual. Outcomes*, vol. 10, no. 9, 2017.e003800
[<http://dx.doi.org/10.1161/CIRCOUTCOMES.117.003800>] [PMID: 28912202]
- [14] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management", *2nd International Conference on Open and Big Data (OBD)*, 2016
- [15] T.F. Heston, Case Study in Blockchain Healthcare Innovation (November 24, 2017). Authorea Working Paper No AUTHOREA_213011_3643634, Available at SSRN: <https://ssrn.com/abstract=3077455>
- [16] M. Banerjee, J. Lee, and K. Choo, "A blockchain future for internet of things security: a position paper", *Digital Communications and Networks*, vol. 4, no. 3, pp. 149-160, 2018.
[<http://dx.doi.org/10.1016/j.dcan.2017.10.006>]

- [17] "Internet of Medical Things Revolutionizing Healthcare", The Alliance of Advanced BioMedical Engineering, [Online]. Available: <https://aabme.asme.org/posts/internet-of-medical-things-revolutionizing-healthcare> [Accessed: 20- Dec- 2020]
- [18] M. Seliem, and K. Elgazzar, "BIoMT: Blockchain for the Internet of Medical Things", *2019 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*, 2019 [http://dx.doi.org/10.1109/BlackSeaCom.2019.8812784]
- [19] N. Dilawar, M. Rizwan, F. Ahmad, and S. Akram, "Blockchain: Securing the Internet of Medical Things (IoMT)", *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 1, 2019. [http://dx.doi.org/10.14569/IJACSA.2019.0100110]
- [20] C. Yan Zhuang, *Applying Blockchain Technology to Enhance Clinical Trial Recruitment*, 2021. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7153067/> [Accessed: 20- Dec- 2020]
- [21] D.R. Wong, S. Bhattacharya, and A.J. Butte, "Prototype of running clinical trials in an untrustworthy environment using blockchain", *Nat. Commun.*, vol. 10, no. 1, p. 917, 2019. [http://dx.doi.org/10.1038/s41467-019-08874-y] [PMID: 30796226]
- [22] "Health Insurance Market Size, Share | Industry Trends and Analysis 2026", *Allied Market Research*, 2021. [Online]. Available: <https://www.alliedmarketresearch.com/health-insurance-market> [Accessed: 20- Dec- 2020]
- [23] Ledger Insights - enterprise blockchain, "HIMSS: How blockchain could transform health insurance - Ledger Insights - enterprise blockchain", [online] Available at: <https://www.ledgerinsights.com/himss-blockchain-healthcare/>
- [24] L. Zhou, L. Wang, and Y. Sun, "MIStore: a Blockchain-Based Medical Insurance Storage System", *J. Med. Syst.*, vol. 42, no. 8, p. 149, 2018. [http://dx.doi.org/10.1007/s10916-018-0996-4] [PMID: 29968202]
- [25] "China makes history – Blockchain e-invoicing is automating trust in the payment process | Corcentric", *Corcentric*, 2021. [Online]. Available: <https://netsend.com/blog/china-blockchain-e-invoicing-automating-trust-payment-process/> [Accessed: 20- Dec- 2020]
- [26] "China's Zhejiang processed \$5 billion medical bills using Ant blockchain, Alipay - Ledger Insights - enterprise blockchain", *Ledger Insights - enterprise blockchain*, 2021. [Online]. Available: <https://www.ledgerinsights.com/chinas-zhejiang-processed-5-billion-medical-bills-using-ant-blockchain-alipay/> [Accessed: 20- May- 2020]
- [27] "Chinese blockchain healthcare apps launched for prescriptions and medical billing - Ledger Insights - enterprise blockchain", *Ledger Insights - enterprise blockchain*, 2021. [Online]. Available: <https://www.ledgerinsights.com/chinese-blockchain-healthcare-apps-prescriptions-medical-billing/> [Accessed: 20- May- 2020]
- [28] F. Dong, P. Zhou, Z. Liu, D. Shen, Z. Xu, and J. Luo, "Towards a fast and secure design for enterprise-oriented cloud storage systems", *Concurr. Comput.*, vol. 29, no. 19, 2017.e4177 [http://dx.doi.org/10.1002/cpe.4177]
- [29] S. Abeyratne, "Blockchain ready manufacturing supply chain using distributed ledger", *Int. J. Res. Eng. Technol.*, vol. 05, no. 09, pp. 1-10, 2016. [http://dx.doi.org/10.15623/ijret.2016.0509001]
- [30] S. Saberli, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain technology and its relationships to sustainable supply chain management", *Int. J. Prod. Res.*, vol. 57, no. 7, pp. 2117-2135, 2018. [http://dx.doi.org/10.1080/00207543.2018.1533261]
- [31] "Bitcoin, Blockchain and Fintech: a systematic review and case studies in the supply chain", *Taylor & Francis*, 2021. Available: <https://www.tandfonline.com/eprint/ZS2AEKBEIAKKGHUNREMV/full?target=10.1080/09537287.2019.1631460>
- [32] R. Adams, B. Kewell, and G. Parry, "Blockchain for Good? Digital Ledger Technology and

- Sustainable Development Goals", In: *Handbook of Sustainability and Social Science Research. World Sustainability Series.*, W. Leal Filho, R. Marans, J. Callewaert, Eds., Springer: Cham, 2018. [http://dx.doi.org/10.1007/978-3-319-67122-2_7]
- [33] D. Lambert, and M.ENZ, "Issues in Supply Chain Management: Progress and potential", *Ind. Mark. Manage.*, vol. 62, pp. 1-16, 2017. [http://dx.doi.org/10.1016/j.indmarman.2016.12.002]
- [34] "The Supply Chain and Blockchain. I: Pros and Cons - Blocktac", *Blocktac*, 2021. Available: <https://www.blocktac.com/en/newness/the-supply-chain-and-blockchain-i-pros-and-cons/> [Accessed: 20- Dec- 2020]
- [35] H. Journal, "First Half of 2019 Sees 31.6 Million Healthcare Records Breached", *HIPAA Journal*, 2021. Available: <https://www.hipaajournal.com/first-half-of-2019-sees-31-million-healthcare-records-breached/> [Accessed: 20- Dec- 2020]
- [36] "Patients Beware: Hackers Are Targeting Your Medical Information", *Healthline*, 2021. Available: <https://www.healthline.com/health-news/hackers-are-targeting-your-medical-information-010715#Medical-Data-More-Valuable-Than-Credit-Card-Data> [Accessed: 20- Dec- 2020]
- [37] "What Is a 51% Attack?", *Investopedia*, 2021. Available: <https://www.investopedia.com/terms/1/51-attack.asp#:~:text=A%2051%25%20attack%20is%20an,other%20miners%20from%20completing%20blocks> [Accessed: 20- Dec- 2020]
- [38] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems", *Future Gener. Comput. Syst.*, vol. 107, pp. 841-853, 2020. [http://dx.doi.org/10.1016/j.future.2017.08.020]
- [39] A. Juels, A. Kosba, and E. Shi, "The Ring of Gyges", *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016 [http://dx.doi.org/10.1145/2976749.2978362]
- [40] Comp.nus.edu.sg, [Online]. Available: <https://www.comp.nus.edu.sg/~prateeks/papers/Bitcoin-scaling.pdf>
- [41] "The Blockchain for Healthcare: Gem Launches Gem Health Network With Philips Blockchain Lab", *Bitcoin Magazine: Bitcoin News, Articles, Charts, and Guides*, [Online]. Available: <https://bitcoinmagazine.com/business/the-blockchain-for-healthcare-gem-launches-gem-health-network-with-philips-blockchain-lab-1461674938> [Accessed: 20- Dec- 2020]
- [42] "GemOS: Automating the Healthcare Industry Using Blockchain", *Bitcoin Magazine: Bitcoin News, Articles, Charts, and Guides*, [Online]. Available: 2021 <https://bitcoinmagazine.com/business/gemos-automating-the-healthcare-industry-using-blockchain-1475614314> [Accessed: 20- Dec- 2020]
- [43] "MedRec", *media.mit.edu* [Online]. Available: <https://medrec.media.mit.edu/> [Accessed: 20- Dec- 2020]
- [44] Guardtime.com, "EY, Sensyne Health and Guardtime to use AI and blockchain to link health care reimbursement and actual patient outcomes — Guardtime", [online] Available at: <https://guardtime.com/blog/ey-sensyne-health-and-guardtime-to-use-ai-and-blockchain-to-link-health-care-reimbursement-and-actual-patient-outcomes> [Accessed 20-Dec-2020]
- [45] "World's first blockchain-supported Personal Care Record Platform launched by Guardtime and partners to up to 30 million NHS patients in the UK — Guardtime", *Guardtime.com*, <https://guardtime.com/blog/world-s-first-blockchain-supported-personal-care-record-platform-launched-by-guardtime-and-partners> [Accessed: 20- Dec- 2020]
- [46] A. Sharma, "Medical errors: The third leading cause of deaths", *Expresshealthcare.in*, Available at: <https://www.expresshealthcare.in/healthcare-it/medical-errors-the-third-leading-cause-of-deaths/420524/#:~:text=Globally%2C%20medical%20errors%20are%20one,after%20heart%20disease%20and%20cancer> [Accessed 20-Dec-2020]
- [47] "Telehealth Market Size, Growth, Share | Global Industry Analysis [2027]",

- Fortunebusinessinsights.com, [Online]. Available: <https://www.fortunebusinessinsights.com/industry-reports/telehealth-market-101065> [Accessed: 20- Dec- 2020]
- [48] Home; Medicalchain, [Online]. Available: <https://medicalchain.com/en/> [Accessed: 20- Dec- 2020]
- [49] B. Beverly Yang, and H. Garcia-Molina, "Designing a super-peer network", [<http://dx.doi.org/10.1109/ICDE.2003.1260781>]
- [50] A. Roehrs, C.A. da Costa, and R. da Rosa Righi, "OmniPHR: A distributed architecture model to integrate personal health records", *J. Biomed. Inform.*, vol. 71, pp. 70-81, 2017. [<http://dx.doi.org/10.1016/j.jbi.2017.05.012>] [PMID: 28545835]
- [51] A. Al Omar, M. Rahman, A. Basu, and S. Kiyomoto, *MediBchain: A Blockchain Based Privacy Preserving Platform for Healthcare Data*. Security, Privacy, and Anonymity in Computation, Communication, and Storage, 2017, pp. 534-543.
- [52] C.C. Agbo, Q.H. Mahmoud, and J.M. Eklund, "Blockchain Technology in Healthcare: A Systematic Review", *Healthcare (Basel)*, vol. 7, no. 2, p. 56, 2019. [<http://dx.doi.org/10.3390/healthcare7020056>] [PMID: 30987333]
- [53] T. McGhin, K. Choo, C. Liu, and D. He, "Blockchain in healthcare applications: Research challenges and opportunities", *J. Netw. Comput. Appl.*, vol. 135, pp. 62-75, 2019. [<http://dx.doi.org/10.1016/j.jnca.2019.02.027>]
- [54] D.K. Sharma, S. Pant, M. Sharma, and S. Brahmachari, "Chapter 13 - Cryptocurrency Mechanisms for Blockchains: Models, Characteristics, Challenges, and Applications", In: *Handbook of Research on Blockchain Technology*, Krishnan Saravanan, E. Balas Valentina, E. Golden Julie, Y. Harold Robinson, S. Balaji, Kumar Raghvendra, Eds., Academic Press, 2020, pp. 323-348. [<http://dx.doi.org/10.1016/B978-0-12-819816-2.00013-7>]
- [55] D.K. Sharma, A.K. Kaushik, A. Goel, and S. Bhargava, "Chapter 11 - Internet of Things and Blockchain: Integration, Need, Challenges, Applications, and Future Scope", In: "Chapter 11 - Internet of Things and Blockchain: Integration, Need, Challenges, Applications, and Future Scope", In: *Handbook of Research on Blockchain Technology*, Krishnan Saravanan, E. Balas Valentina, E. Golden Julie, Y. Harold Robinson, S. Balaji, Kumar Raghvendra, Eds., Academic Press, 2020, pp. 271-294. [<http://dx.doi.org/10.1016/B978-0-12-819816-2.00011-3>]
- [56] M. Sharma, S. Pant, D.K. Sharma, K.D. Gupta, V. Vashishth, and A. Chhabra, "Enabling security for the Industrial Internet of Things using deep learning, blockchain, and coalitions", *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 7, 2020.e4137 [<http://dx.doi.org/10.1002/ett.4137>]
- [57] A. Riyal, S.P. Parth, and S.K. Deepak, "Internet of Things and Blockchain Amalgamation, Requirements, Issues, and Practices", In: *Blockchain Technology for Data Privacy Management*. CRC Press, 2021, p. 23.
- [58] B. Siddhant, S. Mayank, and S.K. Deepak, "Blockchain-Enabled Security and Privacy Schemes in IoT Technologies, Handbook of IoT and Blockchain",
- [59] S.K. Deepak, P. Tushar, K. Yash, and S. Shivani, "Blockchain Applications and Implementation", In: *Handbook of IoT and Blockchain* CRC Press, 2020, pp. 95-118.
- [60] A. Khera, D. Singh, and D. Sharma, "Application design for privacy and security in healthcare", In: *Security and Privacy of Electronic Healthcare Records*, S. Tanwar, S. Tyagi, N. Kumar, Eds., 1st ed. The Institution of Engineering and Technology, 2019, pp. 116-153.
- [61] A. Khera, D. Singh, and D. Sharma, "Information security and privacy in healthcare records: threat analysis, classification, and solutions", In: *Security and Privacy of Electronic Healthcare Records*, S. Tanwar, S. Tyagi, N. Kumar, Eds., 1st ed. The Institution of Engineering and Technology, 2019, pp. 246-270.
- [62] S. Chugh, S. Kumaram, and D. Sharma, "Application of tools and techniques of Big data analytics for healthcare system", In: *APPLICATIONS OF BIG DATA IN HEALTHCARE*. Academic Press, 2021,

pp. 92-107.

[<http://dx.doi.org/10.1016/B978-0-12-820203-6.00010-2>]

- [63] K. Singhal, and D. Sharma, "Fuzzy Systems in Medicine and Healthcare: Need, Challenges and Applications", In: *Soft Computing Applications and Techniques in Healthcare*. CRC Press, 2020, pp. 139-162.

Application of IoT in Patient Health Monitoring System

Rinky Dwivedi^{1,*}, Harshit Mittal¹, Manik Agarwal¹ and Sahil Dwivedi¹

¹ Department of Computer Science and Engineering, Maharaja Surajmal Institute of Technology, C-4 Janakpuri, New Delhi 100058, India

Abstract: The Internet of Things (IoT) is the infrastructure that enables the process of collecting data using various devices which in turn communicate with each other and store this data over the cloud. This helps to retrieve, analyze, and communicate data to any part of the world faster with great efficiency. IoT has indeed opened the doors to endless new possibilities in different areas and industries. From smart home appliances to remotely observing and controlling different objects to self-driven cars and whatnot. The healthcare industry has still not leveraged the true power of this modern IoT revolution. Specifically, when it comes to monitoring the health of elderly people, the techniques used today are still not robust and lack conviction. This has been an area of concern for a long time, and it is an even bigger challenge to remotely monitor the health condition. In this paper, our goal is to depict the current situation of the technology of the health monitoring projects based on IoT and propose an improvement in the actual practices currently prevalent in remote monitoring of the health of elderly people. We will also try to forecast the trend of various health parameters demonstrated in the paper beforehand to make the concerned people aware with precision if any alarming situation is spotted so that instant action can be taken, thus ensuring a reduction of casualties.

Keywords: Ardiuno, Internet of Things (IoT), Remote monitoring, Forecasting, Moving Averages, Health Assistant.

INTRODUCTION

The phrase “Internet of Things” is thought to have been coined at the beginning of the century, when work on the MIT Auto-ID Center [1] was underway to develop a smart identification system that would help minimize error rates while boosting efficiency and automating the process. However, the notion of IoT has grown rapidly in many ways since then, such as with the help of a large number of small networks that can stay linked to each other and transfer data to the main network without the need for human interaction.

* Correspondence author Rinky Dwivedi: Department of Computer Science and Engineering, Maharaja Surajmal Institute of Technology, C-4 Janakpuri, New Delhi 100058, India; Tel: 9958433922; E-mail: rinkydwivedi@msit.in

Quality of service in healthcare has always been under constant criticism in the modern era, as it is a very touchy subject. Monitoring the health of elderly people specifically has been a concern for a long time. In this modern world, most people have a hectic work life with long hours of continuous work, due to which the elderly are left neglected and vulnerable. It is difficult to keep a constant check on the elderly people in the house. Also, keeping an attendant or a servant is very expensive nowadays. In this situation, remote health monitoring based on IoT can help solve the problem.

IoT provides the means by which it is possible to collect and analyze data remotely without any human interaction. So, this helps us to possibly foresee and minimize any future hazard with precision and further notify the concerning authority like the family member or the physician if there is an alarming situation. IoT is important for this project for two main reasons. Firstly, it is automated, so no human intervention is needed. And secondly, because of automation, the process is less prone to errors, *i.e.*, having a more robust system indicating a better quality of service.

In this paper, we describe how we collected data regarding three health parameters, namely temperature, heartbeat, and lung capacity, and used the time series algorithm to forecast these parameters to cope with any alarming situation looming in the future and take necessary actions beforehand to prevent it.

The paper is structured in the following way; the introduction is included in section 1. In section 2, previous works related to IoT in healthcare being discussed. The proposed system is described in section 3, which includes the methodology, block diagram, and system architecture. section 4 describes the equipment details. Section 5 contains the performance measurements and section 6 includes the conclusion. Finally, section 7 contains the future scope.

RELATED WORK

Extensive research on the topic related to the system shows a very few of the related works could build their preliminary framework and prototype of the system. Some of the works like the research conducted on **Ambient Assisted Living (AAL)** [2] did more of a literature survey of the state of its present condition of the monitoring system *via* IoT. They also tried to identify and highlight the critical issues and the quality of service as well as the user-driven experiences in their work. Some others worked on showing or highlighting the importance of IoT in the health sector and some proposals for the health monitoring architectures.

Some related findings used specific models for the health monitoring aspect. Like the abstraction of the **Model-Driven Tree Reference Model (MDTRM)** [3], where they explained the necessity of this model in the health field as well as identifying the complexities of the models. They also benched marked the models which came in handy for the initial phase of this research.

One of the other related models we found is **General Domain Model Architecture (GDMA)** [3], the health monitoring and sensing with cloud processing was also a helpful source behind the research, as it was useful for generating ideas to get raw data from wearable devices which are compatible and capable of measuring many physical values which we can be used to obtain meaningful results.

Masimo Radical-7 [4], a health monitor for the clinical environment helps to collect data and wirelessly transmit it for ongoing display. This provides high-resolution display of information with higher graphical capabilities. It also has a touch-based user interface. But as it can already be assumed how cost-effective it is, it can't send an alarm message to notify of any emergencies. **Free Scale Home Health Hub reference platform** [4] stores patient data in the cloud *via* various sensors, which the people related to the patient can have access to. This platform too can't notify about any alarming situations to the people engaged with the patient.

Some surveys of ours also lead us to projects which even discussed monitoring the health whole area through wireless network sensors [5, 6]. They also tried to share their ideas by giving a model of their frameworks like cloud-based processing [7] and big data [8 - 14]. However, these systems face several attacks, and research works are being carried out to detect such activities [15].

SYSTEM ARCHITECTURE

A. System Structure

In this paper, we used three health parameters that we will monitor using three different sensors namely body temperature, heartbeat, and lung capacity as shown in Fig. (1). Once we have collected all the sensors, the first step is to integrate these sensors into the microcontroller. A microcontroller is a cheap, small-sized computer, that can be portable and multitasking. We have used Arduino Uno as our microcontroller in the paper. Also, to keep a check on the values that are being collected by the sensors in real-time we have attached an LCD to our microcontroller for this purpose.

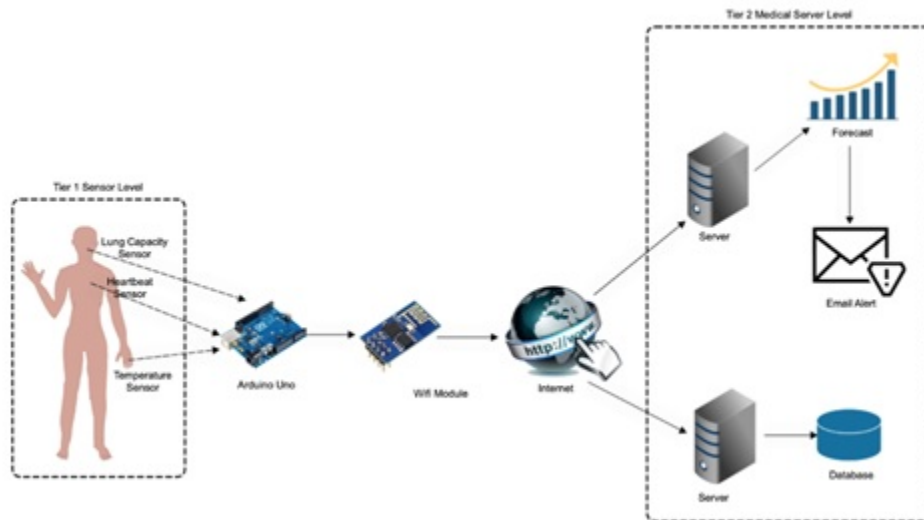


Fig. (1). Architecture of IoT-based Remote Patient Monitoring System.

Integration of sensors with the microcontroller is not enough to send our data over the internet. We need a WIFI module that will send our collected data over the internet.

For this purpose, we integrate the ESP8266 WIFI module into our microcontroller so that we could send the data over the internet and store it on our server.

After integrating and configuring all the sensors and WIFI Module with the microcontroller, we send our data collected from three sensors as a query string over the internet to the server where it is stored in the database (see Fig. 2).

Once we have enough data collected, we start forecasting the trend of the three health parameters. Forecasting is done by using the time series algorithm. In this paper, we have compared the results of three techniques under the time series algorithm namely naive moving average, simple moving average, and weighted moving average.

A moving average is a calculation used to analyze data points by creating a series of averages of different subsets of the full data set. By calculating the moving average, the impacts of random, short-term fluctuations on the values of various health parameters over a specified time frame are mitigated.

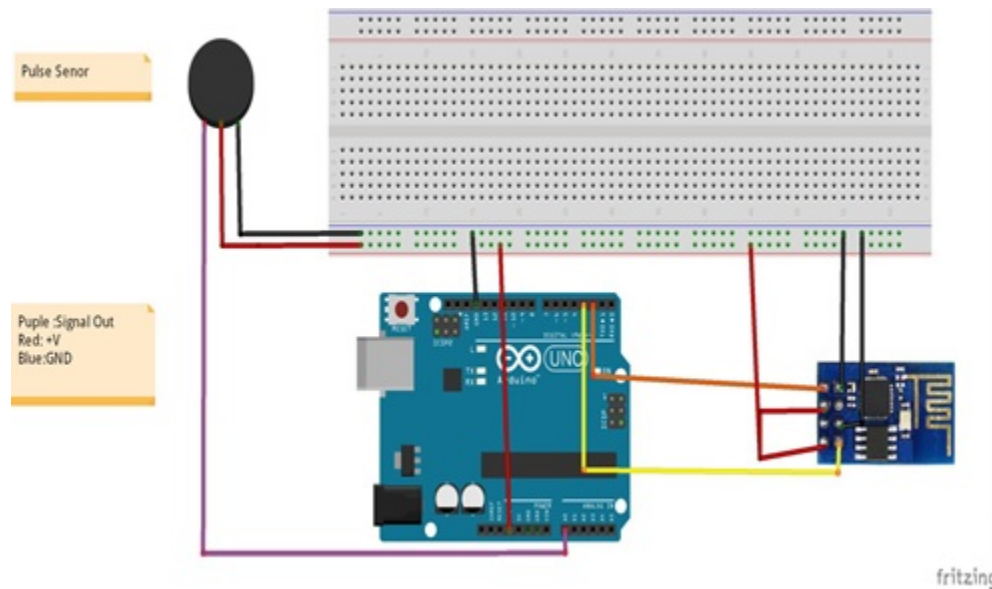


Fig. (2). Circuit Diagram of the Pulse Sensor.

The simple moving average is a forecasting method in which the estimation of future values is done by taking an average of K values in the past. This parameter K depends on the parameter we are modeling.

$$y_{T+h|T} = (y_1 + \dots + y_T) / T$$

$y_{T+h|T}$ notation is a short-hand for the forecast of y_{T+h} based on the data y_1, \dots, y_T .

Naïve moving average is a forecasting method in which we use the value of the last observation in time series to forecast the next value. This technique is beneficial when the data that has to be forecasted is very random.

$$y_{T+h|T} = y_T$$

The weighted moving average is similar to the simple moving average where we estimate the future values by taking an average of the past values but with a slight and an important change. Instead of an average, we take a weighted average where we assign more importance to the data points in the recent past. This way we can have a better and fair estimate of the future values.

$$\mathbf{M} = \frac{\sum_{t=1}^n \mathbf{W}_t * \mathbf{V}_t}{\sum_{t=1}^n \mathbf{W}_t}$$

So, we will analyze the trend of the health parameters using all of the three techniques and compare the results conveyed by each technique in the paper.

Forecasting the trend of our health parameters using moving averages gives us the advantage of taking preventive measures for an alarming situation that may loom in the future. For this, we have integrated an email alert feature on our server wherein if the value of any health parameter goes above a set threshold then we will send an emergency alert to the concerned party to notify them of their patient conditions and take preventive measures to prevent future mishappenings.

Algorithm 1.

Data Collection.

1. Initialize the Arduino module. The LED with respect to each sensor in the circuit will start glowing.
2. Press the green button in the circuit to start the 30 secs window in which the data is collected.
3. Start collecting the data corresponding to three health parameters namely temperature, heartbeat and lung capacity.
4. Send the collected data to the server in the form of a query string over the internet with the help of a WIFI module.
5. Store the collected data in the database.

Algorithm 2.

Forecasting health parameters & generating emergency alerts.

Input: Data for health parameters is taken as input.

from the database.

Step 1. Apply times series algorithmic techniques to.

forecast the health parameters.

Step 2. Set an appropriate threshold for each health.

parameter.

Step 3. If (temperature > threshold).

Step 3.1. The user is critical and an emergency alert is.

sent to the concerned person via.

email.

Step 4. If (pulse rate > threshold).

Step 4.1. The user is critical and an emergency alert is.

sent to the concerned person via.

email.

Step 5. If (lung capacity > threshold).

Step 5.1. The user is critical and an emergency alert is.

sent to the concerned person via.

email.

Step 6. Else.

Step 6.1. The user is safe no alert is generated.

Step 7. Exit.

Algorithm 3.

Time Series Forecasting Techniques.

Step 1. Forecast using Naïve Bayes Moving Average.

Step 1.1. Take the last recorded value from the

database and use this to forecast the

next value.

$$y_{T+h|T} = y_T$$

Step 2. Forecast using Simple Moving Average.

Step 2.1. Take the average of the last 5.

recorded values from the database.

and use this to forecast the next to.

value.

$$y_{T+h|T} = (y_1 + \dots + y_T) / T.$$

Step 3. Forecast using Weighted Moving Average.

Step 3.1. Take a weighted average of the last 5 recorded values from the database assigned a higher weight to the value in the recent past.

$$M = \frac{\sum_{t=1}^n w_t * v_t}{\sum_{t=1}^n w_t}$$

EQUIPMENT DETAILS

Of all the ideas and models that are surveyed for this research, we differ with the use of lung capacity sensors which is a significant part of our research. Instead of using a typical spirometer we have used a dynamo wherein we need to blow air and the motor will rotate and the rpm can be calculated. As result, one can find out the lung capacity of the host. This further can be used to determine the associated diseases corresponding to the lung capacity of the host. For example, depending on the lung capacity of the host it can be suggested whether one should go out during high levels of air pollution. Also, this lung capacity can be used to

determine and identify if there are any complications in the lungs of the host and correspondingly the host can be suggested with suitable precautions and medical help Table 1.

Table 1. Health parameters monitored using three different sensors namely body temperature, heartbeat, and lung capacity.

Parameters	Name of Sensors	Functions	Dynamic Range	Selectivity
Heartbeat	LM 324 Pulse Sensors	It can measure the pulse in real time	Operates from a single 2.3V to 3.6V supply. Temperature ranges from – 40C to 105C	It can be used by students,artists, atheletes,makers, game etc. The flow of blood volume is decided by the rate of heart pulse.
Temperature	LM35	It is a temperature sensing device that senses temperature and gives a voltage output linearly proportional to the Celsius temperature	It has arrange of -55 to 150 and its scale factor is 10mV/oC	It can be used in medical, motorsport, HVAC, agriculture, Industrial, aerospace etc. It can measure the amount of heat energy or even coldness that is generated by an object or system
Lung Capacity	Dynamo	It measures the volume of air inspired and expired by the lungs, when blown in the dynamo.	It depends upon the volume of air in the lungs upon the maximum effort of inspiration	It can be used to calculate the respiratory volume breathed in and out. It can also be used in medical practices.

PERFORMANCE AND MEASUREMENT

First of all, sensors namely heart rate, temperature, and lung capacity are being attached to the patient's body. After the setup of the sensors in the patient's body, the sensors will begin to measure the data and will send it to the microcontroller. Each sensor is having a LED attached to it which notifies the patient that the sensor has started recording the data.

The values that are measured can be seen in real-time on the LCD of the microcontroller. Finally, the microcontroller will send the final data to the server with the help of a WIFI Module.

Fig. (3) shows the sensor used on the patient's hand in real-time.



Fig. (3). Pulse Rate Sensor on Patient's Hand.

Fig. (4) shows the LCD attached with the Arduino microcontroller showing the values of temperature denoted by T, lung capacity denoted by P, and heartbeat denoted by H.

The time elapsed to collect the data is denoted by variable t. There is a 30-sec time frame in which the data needs to be collected.

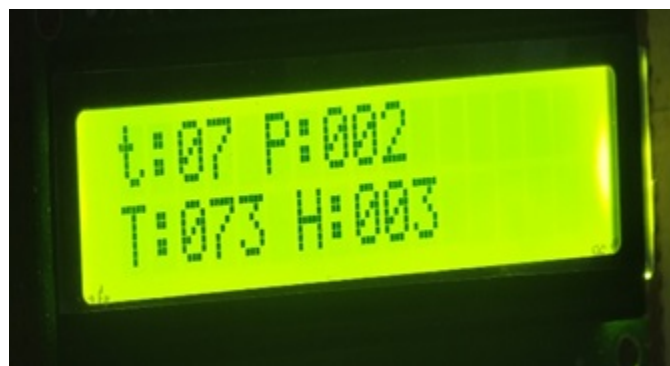


Fig. (4). LCD Display.

Fig. (5) shows the complete IoT patient monitoring system with all the sensors, Arduino microcontroller, LCD attached to the breadboard.

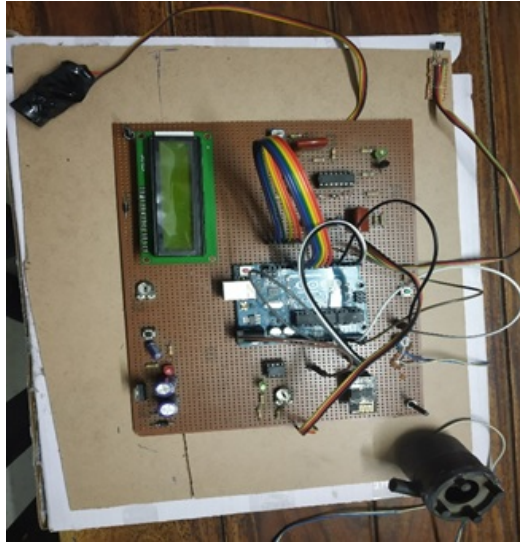


Fig. (5). Patient Monitoring System.

Fig. (6) shows the recent 25 values collected for temperature, heart rate, and lung capacity in the database on the server. We can see in the figure below that the dataset has a very high entropy/randomness due to noise.

Id	Temperature	PulseRate	Pressure	name
1	23	72	52	Test
2	23	80	62	Test
3	98	85	72	Test
4	98	85	65	Test
5	99	85	65	Test
6	2	1	1	Test
7	2	1	8	Test
8	0	0	0	Test
9	0	0	0	Test
10	0	0	0	Test
11	2	1	8	Test
12	102	20	8.5	Test
13	0	0	0	Test
14	102	20	8.5	Test
15	102	20	8.5	Test
16	0	0	0	Test
17	102	20	8.5	Test
18	0	0	0	Test
19	0	0	0	Test
20	75	0	3	Test
21	104	0	2	Test
22	84	24	2	Test
23	75	12	2	Test
24	77	0	2	Test

Fig. (6). Recorded Values.

Next, we have shown a comparison between three-time series forecasting techniques namely naïve, simple and weighted moving averages.

Fig. (7) shows the forecasting based on a naïve moving average.

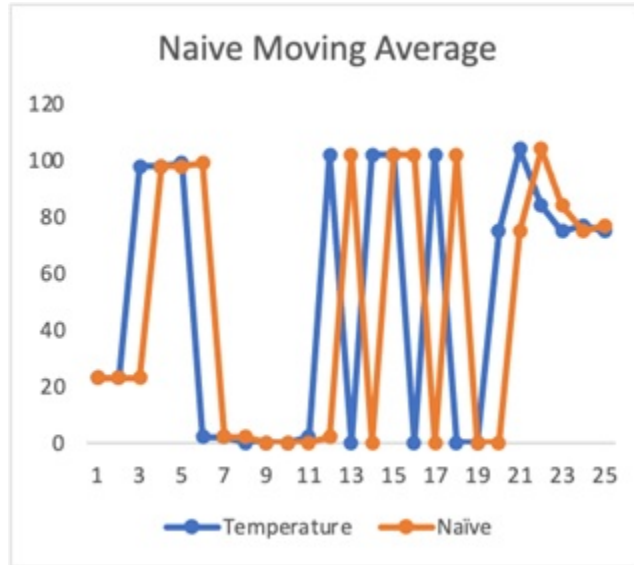


Fig. (7). Naïve Moving Average.

Fig. (8) shows the forecasting based on a simple moving average.

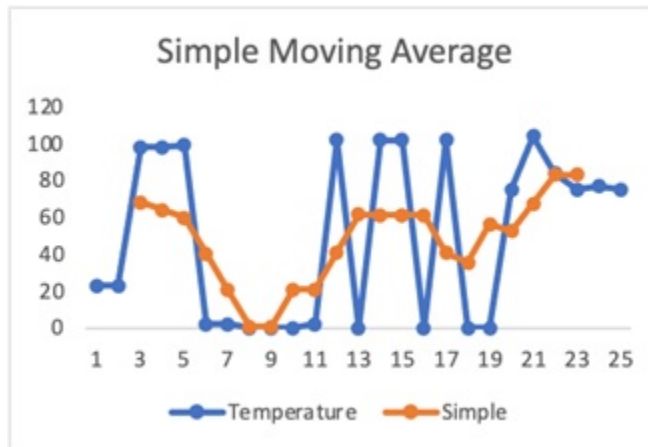


Fig. (8). Simple Moving Average.

Fig. (9) shows the forecasting based on the weighted moving average.

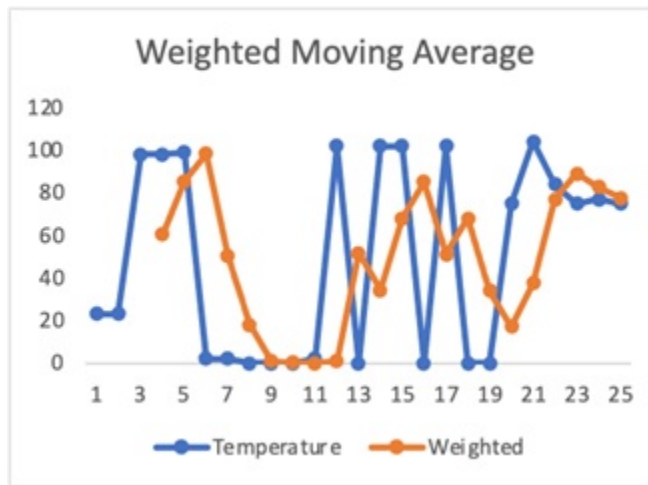


Fig. (9). Weighted Moving Average.

Forecast accuracy as shown in Fig. (10) is the difference between the actual data and the forecast value. When making a decision we want the most accurate forecasting model possible, but how we measure forecast accuracy depends on how the model will be used. We present three methods of measuring forecast accuracy, mean absolute deviation (MAD), mean squared error (MSE), and mean absolute percent error (MAPE).

Moving Averages	MAD	MSE	MAPE
Naïve	37	3361	305%
Simple	36	2212	480%
Weighted	35	2234	435%

Fig. (10). Forecast Accuracy.

For the health data at our disposal, the naïve moving average algorithm gives the best forecast of the health parameter. This is because a naïve moving average is extremely effective when modeling data that has very high entropy.

From the table also we can see that the forecast using the naïve method on average is within 305% of the actual value which is the best among all the three algorithms in consideration even though the overall error is the highest.

EMERGENCY ALERT

In this busy world, everyone is occupied with their work. No one gets sufficient time to look after their loved ones who are suffering from a disease. Hiring a full-time nurse is very costly, not everyone can afford it. For old aged people whose health is always at stake and we never know what illness they can suffer from at any hour. In order to avoid this, we have made an emergency email alert.

When the temperature sensor device is attached to the patient's body it will be taking a reading of the body temperature, and whenever the body's temperature goes above the threshold temperature it will send an emergency email to the person.

This is how immediate action can be taken at the right time.

Fig. (11) displays the alert message sent to the patient's emergency email ID to minimize the patient's health risk.

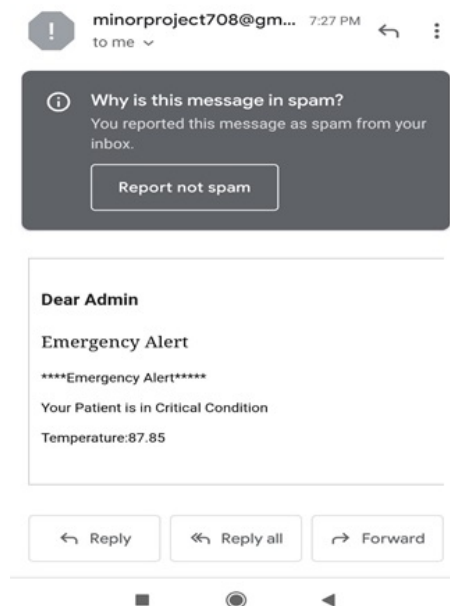


Fig. (11). Email Alert sent to the patient.

CONCLUSION AND FUTURE SCOPE

The main goal of this project was to successfully monitor the basic three health parameters namely temperature, pulse rate, lung capacity, and then respond during emergencies without any human intervention. The rise of IoT has added another dimension to this era of technology and to keep pace with these new technologies, this project has taken big strides towards advancement in general and in the health sector to be specific. We have rightfully leveraged the power of IoT in this project to increase the efficiency of the health sector. Though our model is tested and implemented, the continuation of this project without proper backing with funds will be difficult as the project requires a considerable amount of quality hardware support. The real potential of this work can only be realized when we can implement this project at scale using various big data frameworks.

There is still scope for improvement and potential for future development in this project which can take this project to new heights.

Our pulse rate sensor can be upgraded so that it can measure the heart rate when patients are in motion. Right now, the sensor is a little unstable when it comes to measuring heart rate when the patient is in motion. We can also measure other health parameters like blood pressure, EEG, *etc.* to make our system more robust. More sensors mean more data for doctors to identify diseases. Data stored in the database need protection from potential threats and that is why incorporating security measures in our system can add a level of abstraction for the patient's data and earn their trust. We can also add a video conferencing functionality to our system which helps doctors to prescribe medicines to people in rural areas efficiently without having to travel large distances.

We can use the lung capacity data combined with pollution measuring sensors to monitor whether an elderly person can be allowed to go out of the house in the current times of rising pollution. All these functionalities can make this model a household thing and can completely revolutionize the healthcare industry.

Our project can be considered as a platform to develop in the field of IoT in the health sector. In developing countries like ours, this kind of innovative and cost-effective project can improve the future of technology. So, we are looking forward to implementing the project to make an impact in the new era of technology.

CONSENT FOR PUBLICATION

Not applicable.

CONFLICT OF INTEREST

The author declares no conflict of interest, financial or otherwise.

ACKNOWLEDGEMENT

Declared none.

REFERENCES

- [1] D.L. Brock, "The electronic product code (EPC)", *Auto-ID Center White Paper MIT-AUTOID--H-002*, 2001.
- [2] Q. Ni, A.B. García Hernando, and I.P. de la Cruz, "The elderly's independent living in smart homes: A characterization of activities and sensing infrastructure survey to facilitate services development", *Sensors (Basel)*, vol. 15, no. 5, pp. 11312-11362, 2015.
[<http://dx.doi.org/10.3390/s150511312>] [PMID: 26007717]
- [3] P.P. Ray, "Home Health Hub Internet of Things (H 3 IoT): an architectural framework for monitoring health of elderly people", *Science Engineering and Management Research (ICSEMR)*, 2014 International Conference on (pp. 1-3).
- [4] S. Patel, H. Park, P. Bonato, L. Chan, and M. Rodgers, "A review of wearable sensors and systems with application in rehabilitation", *J. Neuroeng. Rehabil.*, vol. 9, no. 1, p. 21, 2012.
[<http://dx.doi.org/10.1186/1743-0003-9-21>] [PMID: 22520559]
- [5] N. de Battista, J. A. Rice, S. H. Sim, J. M. W. Brownjohn, and H. P. Tan, "Structural health monitoring of civil infrastructure using wireless sensor networks",
- [6] M. Hassanaliereagh, A. Page, T. Soyata, G. Sharma, M. Aktas, and G. Mateos, "Health monitoring and management using Internet-of-Things (IoT) sensing with cloud-based processing: Opportunities and challenges", *Services Computing (SCC)*, 2015 IEEE International Conference on (pp. 285-292).
- [7] S. Tyagi, A. Agarwal, and P. Maheshwari, "A conceptual framework for IoT-based healthcare system using cloud computing", *Cloud System and Big Data Engineering (Confluence)*, 2016 6th International Conference (pp. 503-507).
[<http://dx.doi.org/10.1109/CONFLUENCE.2016.7508172>]
- [8] M. Sathya, S. Madhan, and K. Jayanthi, "Internet of things (IoT) based health monitoring system and challenges", *International Journal of Engineering and Technology (UAE)*, vol. 7, no. 1.7, pp. 175-178, 2018.
[<http://dx.doi.org/10.14419/ijet.v7i1.7.10645>]
- [9] D.S.R. Krishnan, S.C. Gupta, and T. Choudhury, "An IoT based Patient Health Monitoring System", *2018 International Conference on Advances in Computing and Communication Engineering (ICACCE)*, 2018 Paris.
[<http://dx.doi.org/10.1109/ICACCE.2018.8441708>]
- [10] M.M. Islam, A. Rahaman, and M.R. Islam, "Development of Smart Healthcare Monitoring System in IoT Environment", *Comput. Sci.*, vol. 1, no. 3, p. 185, 2020.
[<http://dx.doi.org/10.1007/s42979-020-00195-y>] [PMID: 33063046]
- [11] A. Rahaman, M. Islam, M. Islam, M. Sadi, and S. Nooruddin, "Developing IoT based smart health monitoring systems: a review", *Rev Intell Artif.*, vol. 33, no. 6, pp. 435-440, 2019.
[<http://dx.doi.org/10.18280/ria.330605>]
- [12] S.M. Riazul Islam, Daehan Kwak, M. Humaun Kabir, M. Hossain, and Kyung-Sup Kwak, "Kwak Daehan, Humaun Kabir M, Hossain M, Kwak Kyung-Sup. The Internet of Things for health care: a comprehensive survey", *IEEE Access*, vol. 3, pp. 678-708, 2015.
[<http://dx.doi.org/10.1109/ACCESS.2015.2437951>]

- [13] G. Mois, S. Folea, and T. Sanislav, "Analysis of three IoT-based wireless sensors for environmental monitoring", *IEEE Trans. Instrum. Meas.*, vol. 66, no. 8, pp. 2056-2064, 2017.
[<http://dx.doi.org/10.1109/TIM.2017.2677619>]
- [14] J.J. Oresko, H. Duschl, A.C. Cheng, S. Huang, Y. Sun, H. Duschl, and A.C. Cheng, "A wearable smartphone-based platform for real-time cardiovascular disease detection via electrocardiogram processing", *IEEE Trans. Inf. Technol. Biomed.*, vol. 14, no. 3, pp. 734-740, 2010.
[<http://dx.doi.org/10.1109/TITB.2010.2047865>] [PMID: 20388600]
- [15] M. Hasan, M.M. Islam, M.I.I. Zarif, and M.M.A. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches", *Internet Things.*, vol. 7, p. 100059, 2019.
[<http://dx.doi.org/10.1016/j.iot.2019.100059>]

CHAPTER 5

IoT Based Verified and Public Vehicle Registration through BlockChain: Future Smart Cities based Applications with Sustainable Approach**Rohit Rastogi^{1,*}, Bhuvneshwar Sharma¹, Pardeep Kumar² and Muskan Gupta¹**¹ Department of CSE, ABES Engineering College, Ghaziabad, U.P. 201009, India² Department of Computer Systems and Engineering, QUEST University, Nawabshah, Pakistan

Abstract: Blockchain technology replaces centralized applications with distributed computing. Modern economy is estimated by the place of motor transport in the infrastructure of the national economy. An automobile registration system is a unified information system. This information system takes care of every information about automobile registration. It is administrated by a national registry entity and has access to other government and non-government services that handle automobile information. Cyber Physical System (CPS) is defined as the combination of computation and physical process. It is mainly used in the ICT section. It is also focused on resolving the problems related to authors of the data regarding transparency, media, and storage problems by technical handling.

The presented chapter uses all the above concepts in one place and integrates them to build a useful application. The presented frame allows car manufacturers, owners, repairing companies, and insurance agencies to register and add new car entries through a simple method. In addition, database technology has been leveraged to cache intermediate data. It efficiently uses the Industrial IoT and 5G technologies.

Many researchers have called for rules and applications to draw old maps based on distributed applications into the blockchain. New protocols are available in this work for the International Automated Vehicle Management System, called DriveLoop, which were proposed and developed.

Keywords: Driveloop, Blockchain, Peer to Peer (P2P), Hashing Algorithms, Car Registration, Overlay Network.

* Correspondence author **Rohit Rastogi**: Department of CSE, ABES Engineering College, Ghaziabad, U.P., 201009, India; Tel: 9818992772; E-mail: rohit.rastogi@abes.ac.in

Koyel Datta Gupta, Deepak Kumar Sharma, Rinky Dwivedi and Fadi Al-Turjman (Eds.)
All rights reserved-© 2022 Bentham Science Publishers

INTRODUCTION

Anyone who has purchased or sold a car, or who has worked in the automobile manufacturing or distribution industry at any point, is familiar with the complication that is the Vehicle Registration process. Given the fact that all vehicles in the market have been sold and resold as they passed through multiple hands, it becomes a cumbersome task to maintain a legitimate record of the history of each vehicle and make it available when needed.

But before one goes on to talk about the problems of the process of Vehicle Registration, one first needs to understand why Vehicle Registration is such an important aspect of automobile dealing. Car ownership changes as many times as you can imagine.

Whether you look at it in terms of dealing in spare parts or in assembled vehicles, dealings by the middlemen or by the retailer who makes the final sale to a consumer, or in terms of the resale of a second-hand vehicle, some stakeholders are interested in learning everything there is to know about the car they are purchasing. Not to mention the insurance agencies, the police, and other authorities, and the government too needs to keep tabs on the automobiles for various reasons.

The fact of the matter is that all these stakeholders need information about the vehicles, starting from its manufacturing story, covering its first sale, the accidents, if any, that it has been in, and any and all repairs and maintenance. This is crucial not just to maintain a track record of the vehicle in question to determine its market value but also for legal and insurance purposes.

Vehicle Registration is a way to facilitate this record keeping by maintaining a link between the vehicle and its owner. It might be or not be compulsory, depending on the law of the land. This helps the authorities with regard to taxation, insurance, or crime detection purposes. Also, it is a way for automobile dealer to keep track of their vehicles [1 - 3].

Concept of Smart Cities

The urban development has resulted in a change of archetype in the 21st century. Research activities for smarter cities became a priority task. The life was improved in the last century in terms of technologies and services. Smart City is the demanding solution to sustainability and urbanization. Smart Cities may lead to a dystopian world that is regulated by technocratic governments, which propel citizens to subaltern roles. However, the massive industrialization and the

increasing population in the big cities has been a big challenging for urban planner, architects, and administrators.

The service platforms of smart cities are the Internet of Things (IoT), big data systems, and mobility. Connected automobile with their advanced technology reduces the chances of accident and help drivers save time and gasoline within their limits. An increase in population in urban areas often leads to the problem of parking spaces. Smart parking is one of the most important parts of smart city. Sensors are placed in smart cities with good internet connectivity. More urban our planet becomes, the smarter the cities have to be. The cities of tomorrow will be more prone to transformation embellishment than the cities of yesterday [4].

Problem of Car Registration and Motivation

The process of registering a car has always been difficult. This is a lengthy process involving several parties, and there is also the risk of manipulating information, replicating data and various errors. In this case, critical information can be very vulnerable to fraud or data falsification, or even available for tracking.

By bringing the power of Distributed Ledger Technology called Blockchain into the picture and moving the entire process of registering a car on to Blockchain, a lot of these vulnerabilities can easily be resolved [5].

Research Objectives

Blockchain comes to the rescue by reducing the average response time. The Blockchain will allow parties to send data in the form of an intellectual contract or chain code, which will eventually become the single source of unchanged data for all parties. In addition, the Blockchain in the vehicle registration ecosystem will help reduce the risk of fraud and aggression, since only authorized personnel can use the data when updating the private key in the province.

In fact, any attempt to track fake data can be easily done on the Blockchain. The best part is that Blockchain provides one single idea of the lifecycle of the car in one book, which is not currently available [6].

Scope of the Research Work

This research experiment is a generalized project implemented using open source technologies developed by Linux Foundation called hyper ledger Fabric in a permission model. Anyone can use this project by taking the authorization and adding their stakeholders into the system.

5-G Technology and Its Implications

With an advanced access technology and with an increase in the demand of the users, 4G will now be easily replaced with 5G. There are several reasons to switch to 5G have higher capacity, increase data rate, lower end-to-end interruption, massive device connectivity, reduced cost and consistent quality of experience [7].

5G consists of microcells, small cells, and relays and hence heterogeneous. Device to Device communicative (D2D) and Internet of Things (IoT) are major concerns. 5G provides a good policy for future 5G standardization network MBB mobile broadband. 5G will allow wireless networks to matter data rates and use cases that are currently handled by fiber access. One of the widely used technology in today's era is IoT. IoT further consists of two technologies. These technologies are used to describe a key focus area for the ICT sector [8, 9].

- a. Cyber Physical System (CPS) - This system is used to describe a key focus area for the ICT section. It is basically defined as the unification of computation and physical processes.
- b. Machine to Machine (M2M) - It represents the way in which machines can communicate between themselves.

5G validates IoT for new use cases and economic sectors. The objective of 5G is to meet projected mobile traffic demand and to heuristically address the communications needs of most sectors of the economy. Also, the aim of the group is to promote the development of 5G technologies in China. South Korea's 5G forum is also a public private partnership program that is formed in May, 2013.

IoT and Its Applications in Transportation

Application in Automobile

If you have ever bought your own vehicle or have sold one, or have been a part of an automobile manufacturing or dealing at any stage of the cycle, you would be familiar with the complication that is Vehicle Registration.

Given the fact that all vehicles in the market have been sold and resold as they passed through multiple hands, it becomes a cumbersome task to maintain a legitimate record of the history of each vehicle and make it available when needed. By applying Blockchain and IoT technologies and the whole process of registering vehicles in Blockchain, many of these problems can be easily solved.

Usage of AI, ML in IoT and Blockchain

A good working model could be IoT generating data from a multitude of sensors and analytics, Blockchain storing data and, AI/ML drawing intelligence from the same data. An example of the above is in a supply chain where IoT can measure a lot of different metrics from the environment to trip record to motion sensing, use Blockchain to store that data and then use AI on that data to make human-like decisions. The purpose of Blockchain in this solution is to provide transparency across organization and immutability of data as well as executing smart contracts.

This is not just true for the supply chain but is possible in many sectors such as healthcare manufacturing, identity, and security applications and even finance industries. For example, a bank offering line of credit to SMEs may depend on these technologies to make a faster, accurate and error-free assessment by using IoT to measure goods, raw materials, finished products, assets, *etc.* of an SME, store these in Blockchain for audit and other decision-making purposes and employ AI to make recommendations [3], [9, 10].

Each technology in itself is capable of transformation. They don't need one another to be useful. But together, they are even more powerful catalysts to solve problems that are difficult to handle otherwise. Take an example of healthcare. Healthcare issues such as surgical infections, hygiene, negligence, *etc.*, can have a bad impact on the patient as well as the hospital in itself. The combination of IoT, Blockchain and AI can be used effectively to bring accountability, efficiency and better and faster patient recovery [11].

RELATED WORK

Blockchain is not a new technology. It is a set of existing methods, which are organized in a new specific order to solve problems related to different strengths, security and sharing. Many applications are suggested to move from a normal or normal operation to a Blockchain. In addition, many surveys were written to obtain information about applications [12]. The following are some of the previous works related to Driveloop. Two important Blockchain systems for this application are CarChain and Fabcar IBM Blockchain [13].

Carchain

The Carchain is a distributed and decentralized system that connects the car owner and tenant, securely leases and secures financial exchange based on the time spent. The system operates in the open network Blockchain - Ethereum and can be moved to a private Blockchain - Hyper ledger. It consists of an intellectual agreement that integrates systems and applications into the system (for web

application owners, for the user's mobile phone), to manage the system, send information to the Blockchain and make changes to the system. An electronic signature method that allows you to unlock the car on arrival.

Fabcar IBM Blockchain

This code demonstrates network configuration on the standard IBM blockchain platform and the implementation of the Fabcar smart contract on the network. We then configure our application to interact with the network, including identity, to send transactions in a smart contract. The application is configured with Node.js using the Fabric Node SDK to handle network requests and the Angular client to open the web interface [14].

Nowadays, career opportunities are rising rapidly. To achieve success, every field needs lots of dedication and hard work. Automobile Engineering career is one of the best careers that are very creative and fast paced. It mainly deals with construction, manufacturing and design of automobile. Due to rapid growth of auto component in automobile sector because of an advanced technology, the jobs in automobile engineering is increasing everyday and the reason behind it are automobile engineers.

Blockchain and Future of Automobiles

The Authors Pham and team explained the future Scope and limitations as below:

As future perspective, it can be said that nowadays, career opportunities are rising rapidly. Any field requires lots of dedication and hard work to learn any profession and achieve the success.

Basically, in this research, authors have presented a write-up for an automobile registration or automobile parking using Blockchain. Automobile which is designed for passenger and is run by an internal combustion engine with the help of volatile fuel. In today's world, people prefer vehicle to go anywhere whether it is miles away or it is near to the location. It is the daily need of the person as they have to go for their work or to fulfil their needs. The smoothing lubrication of an automobile helps to move vehicles fast and easy which make our life so simple.

As its known that nowadays people move to the big cities for better jobs, excellent education and of their bright future. This migration often leads to the increase in population which further leads to the problem of parking spaces. Mostly, many people cannot find safe parking spaces in a crowded area. So, this is insecure solution of centralised based car parking system. An automobile registration system is a unified information system. These information system controls of

every information related to an automobile registration. Blockchain is being used nowadays as one of the most emerging domains.

The authors' team have applied the methodology for the help of assigned unique ids and without disclosing their personal information, vehicles can communicate with deployed parking lots. Then register vehicle book parking by requesting the controller. Then the controller check for parking space around their establishment when receive a request from the ordinary. Then the complete information is sent to the ordinary node and then the ordinary node reserves the parking and pays for it.

In limitations, one can see that the study was a good learning process and was a very satisfying experience. Yet there are several factors that limited this researchers plan to study as every researcher desired limitations are as follows.

- Access to Documentation and information
 - Required data was not readily available. The process of documentation during design and development is not a regular practise. Due to confidentiality of the companies, an R&D and Design activity, the information shared was limited about the processes that are followed for a particular product category.
- Automobile Industry
 - The R&D and Design executives in the automotive industry are tied up because of many rules and policies.
 - Data sharing is very limited. It is not the general practise in the corporation culture to openly and willingly share the information.

In concluding remarks, they explained that they implemented the blockchain technology to maintain trust, security, and clarity in the system. We use many technologies and one of the technologies is IoT, Ethereum.

They tested proposed idea on the basis of latency of blockchain, the throughput of blockchain, the accuracy of transactions, latency upon TAIVs and throughput upon TAIVs [15].

Significance of 5-G Technology

One of the widely used technologies in today's era is IoT. IoT further consists two technologies. These technologies used to describe a key focus area for the ICT sector. b-) Machine to Machine (M2M) - It defines the way of communication of machine between them.

The purpose of 5G is as follows:

- a. To meet projected mobile traffic demand.
- b. To address the communications that is mostly needed by the sectors of the economy.

PRESENTED METHODOLOGY

With Blockchain, Stakeholders, such as automotive vehicle manufacturers, agents, customers and agencies, can easily participate in accessing and updating vehicle data based on their access to security. The solution also ensures that the most secure and complete information is stored and shared securely and economically [16].

To further explain, let's first look at the roles of the various stakeholders involved in the vehicle registration process. We also looked at some basic workflows and understood how they were simplified with Blockchain.

- a. **Manufacturer:** Push the vehicle towards blockchain by adding details including make, model, Version, chassis number, engine number, *etc.* And he sells vehicles.
- b. **Dealer:** Car sales are applied to end customers.
- c. **Insurance Agency:** Checks customer and car information and provides insurance.
- d. **Registration Authority:** The RTO will be responsible for approving registries and providing registration numbers, sending vehicle transfers and resetting vehicles.
- e. **Police:** It issues vehicle licenses and transfer certificates, as well as traffic invoices.
- f. **Service Center:** Parts of the service are included as work cards and replacement parts.
- g. **Customer/ Car owners:** Allow the exchange of confidential information as PII.

SOFTWARE REQUIREMENT SPECIFICATION

The Following Software Requirements have to be fulfilled.

Product Perspective

This idea is not totally implemented anywhere in this world. There exists an app named “Carchain” which provides a way to connect the car owner and tenant securely leases and secures financial exchange based on the time spent.

Similarities between Carchain and our application

- a. Both Carchain and this application are service based applications.
- b. In both the applications there are customers who want to avail the services and the professionals who want to provide those services.
- c. One can join as a service provider in both applications.
- d. Feedback can be provided for both the applications.

Differences Between Carchain and Our Application

- a. Our application provides an automated way of purchasing a car right from the first step to the last step. Carchain doesn't involve selling cars.
- b. Carchain uses the Ethereum network to implement the blockchain but our application uses Hyper ledger Fabric - a private network.

System Interfaces

- a. HTML5, JavaScript, CSS3 and Bootstrap are used for the front end portion of the application.
- b. Node JS is used to write the chain codes for the backend.
- c. Docker is used as a service product that uses OS-level virtualization to deliver software in packages called containers. The containers are isolated and group their own software, libraries and configuration files, they can communicate through clearly defined channels.
- d. Hyper ledger Fabric is used as a platform to operate the application.
- e. Two databases are used - LevelDB for storing the transaction data and CouchDB for storing the asset data.
- f. Visual studio code is used as a source code editor.
- g. Postman is used to create, share, test and document APIs.

Interfaces (Hardware and Software and communication)

We use many interfaces like

Login/Signup

This interface lets a customer enter the application and avail services and if someone is not a customer to this application, it also helps them to become a registered customer.

Main Page

This interface consists of all the services available also it is a connecting medium to all interfaces.

Contact us

This interface lets any customer with any issue to contact us.

Manufacturer

This interface lets the manufacturer push the vehicle towards blockchain by adding details including make, model, version, chassis number, engine number, *etc.* and he sells vehicles.

Dealer

Car sales are applied to end customers.

Registration Authority

The RTO will be responsible for approving registries and providing registration numbers, sending vehicle transfers and resetting vehicles.

Police

It issues the vehicle license and transfer certificate.

Customer

Allows the exchange of confidential information as PII.

Hardware Interfaces

- a. Processor: Intel i5-6200U / Intel Core or better.
- b. GPU:2.30Ghz
- c. Ram: 8GB or more.
- d. Hard Disk: 20GB or more.
- e. Operating System: Linux/Mac.
- f. Input Device: Standard Keyboard, Mouse and USB.
- g. A browser which supports HTML and Java script.
- h. Internet Connection.

Software Interfaces***Ubuntu 20.04***

Team has chosen Linux operating system for its best support and user friendliness for this project.

Hyper ledger Fabric v0.20

It is used as a modular blockchain structure, which serves as the basis for the development of blockchain-based products, solutions and applications using plug-and-play components intended for use in private companies.

NodeJs v12.16.0-x64

It is been used to write down the back end logic *i.e.* Chain code for the automation of the transactions.

Docker 19.03.8

It is used as a service product that uses OS-level virtualization to deliver software in packages called containers.

Postman 7.24.0

It is used to create, share, test and document APIs. This is achieved because users can create and save simple and complex HTTP/s requests and their responses. This results in more effective and less tiring work.

Communications Interfaces

This project supports all types of web browsers. The team is using simple forms for the registration forms, feedback, availing the services *etc.*

Memory Constraints

Primary Memory: 8GB or above.

Secondary Memory: 20GB or above.

Operations (Product Functions, User Characteristics)

Following operations will be performed by our software.

Product-Functions

- a. It allows people to register onto the application for the use its services.
- b. The manufacturer can add a new car into the blockchain for sale purpose.
- c. The dealer can sell a car and can change the ownership of the car after some validations.
- d. The registration authority can validate a car for changing its ownership from one person to another.

- e. The customer can check all the steps involved in a registration process directly from a single dashboard.
- f. Any change done anywhere is reflected everywhere in the network.

User Characteristics

- a. Only 18+ adults can register or can provide service to other needed people.
- b. Basic technical knowledge of using the computer system is required.
- c. 2-week hands-on training is enough for using the software.

Use Case, Sequence Diagram

Use case

The following are the various Use case diagrams of the various Actors involved in the project.

Manufacturer- Fig. (1) depicts the relationship between manufacturer and the various use cases.

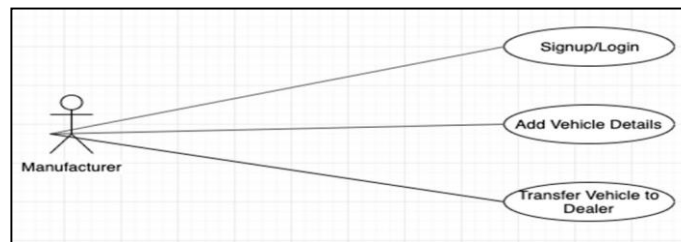


Fig. (1). Use Case of Manufacturer.

Dealer- Fig. (2) depicts the relationship between Dealer and the various use cases.

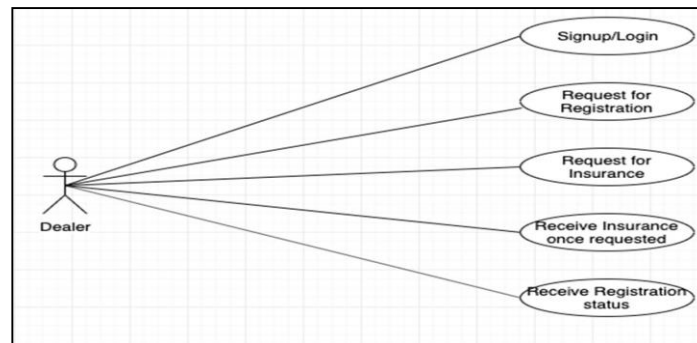


Fig. (2). Use Case of Dealer.

Registration Authority- Fig. (3) depicts the relationship between the Registration Authority and the various use cases.

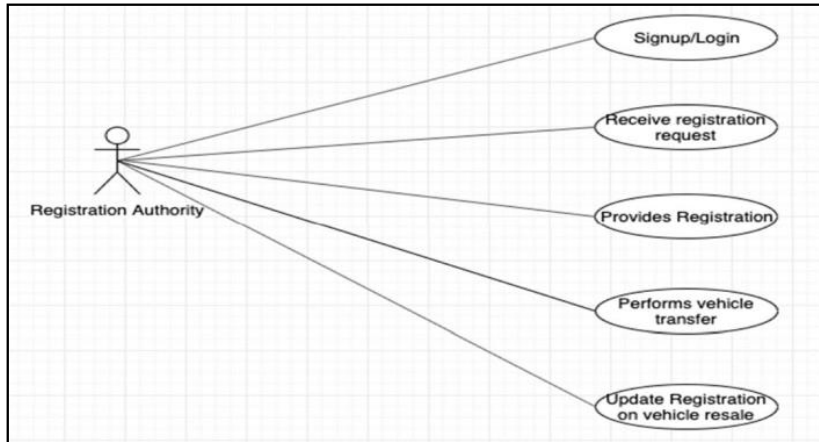


Fig. (3). Use Case of Registration Authority.

Police- Fig. (4) depicts the relationship between the Police and various use cases.

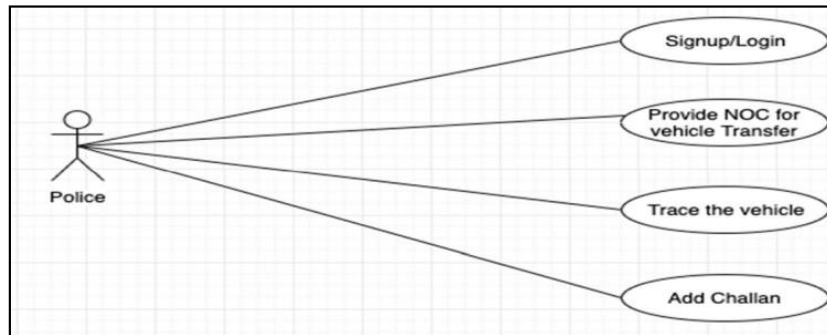


Fig.(4). Use Case of Police.

Customer- Fig. (5) depicts the relationship between Customer and the various use cases.

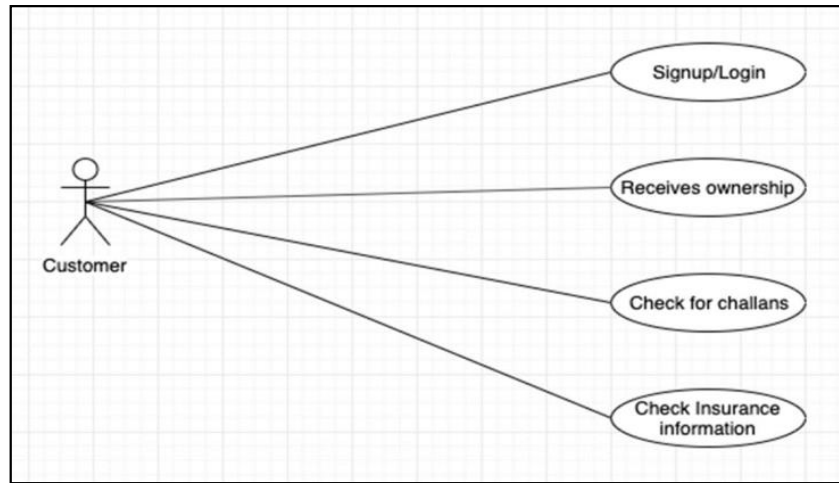


Fig. (5). Use Case of Customer.

Sequence Diagrams

A sequence diagram is shown in Fig. (6), which basically depicts collaboration between articles in a sequential order. This diagram shows how the client enters into the network and a new block of transactions is created and finally added to the block chain network.

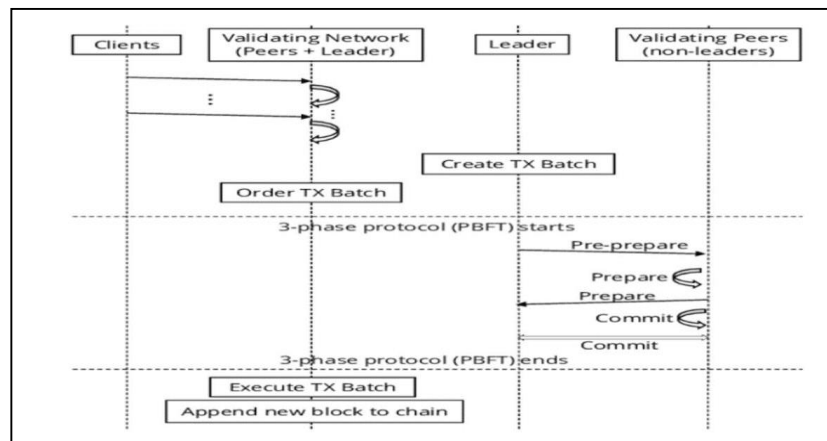


Fig. (6). Sequence Diagram.

System Design

System design is the way towards defining the engineering, modules, interfaces, and information for a system to fulfill indicated prerequisites.

Architecture Diagrams, Data Flow Diagrams, Activity Diagram, ER Diagram, Database schema Diagrams (as per Figs. 7 to 13).

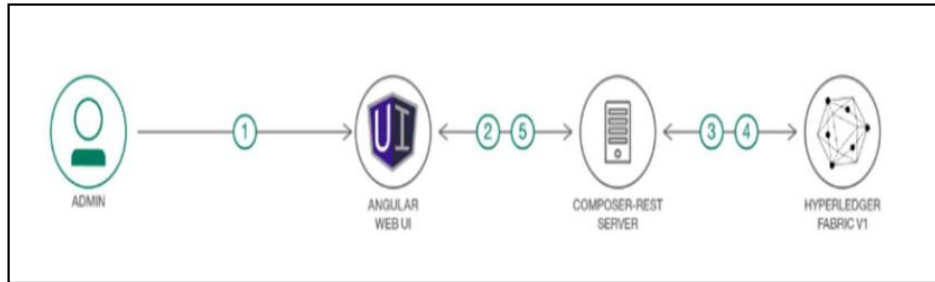


Fig. (7). High level view of Architecture.

Architecture Diagrams

The following is the system architecture design for the project.

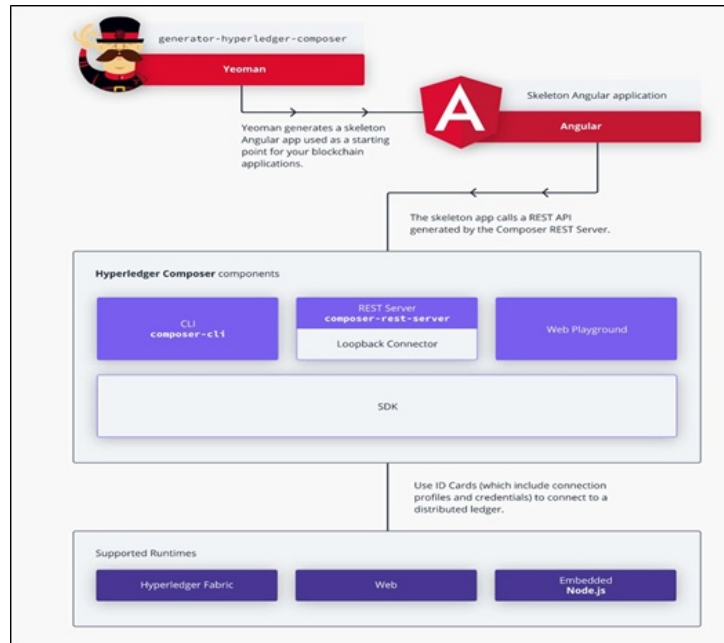


Fig. (8). Detailed view of Architecture.

Data Flow Diagram

Level 0- The following is the level-0 data flow diagram of the project.

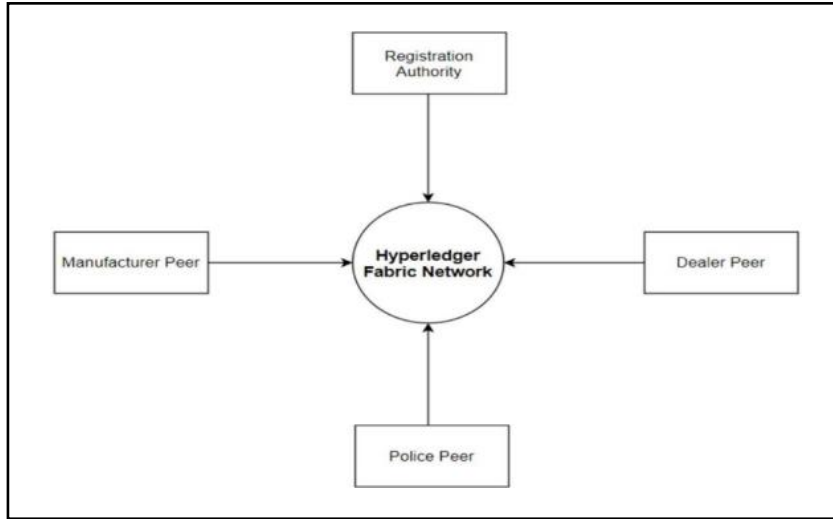


Fig. (9). Level 0 DFD.

Level 1- The following is the level-1 data flow diagram of the project.

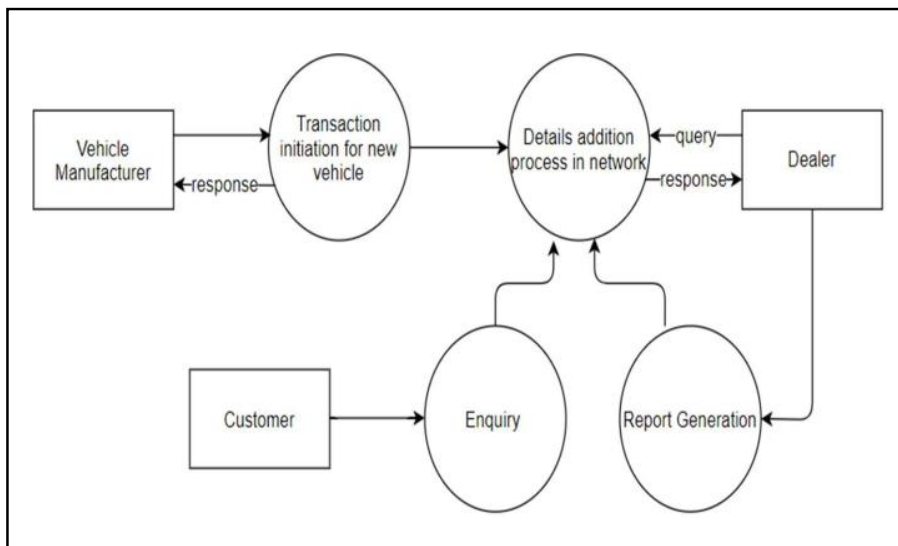


Fig. (10). Level 1 DFD.

Level 2- The following is the level-2 data flow diagram of the project.

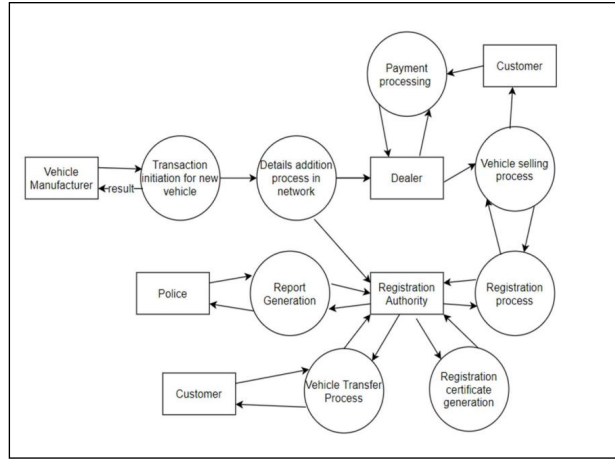


Fig. (11). Level 2 DFD.

Activity Diagram

The following is the Activity diagram showing the Login of the customer into the system.

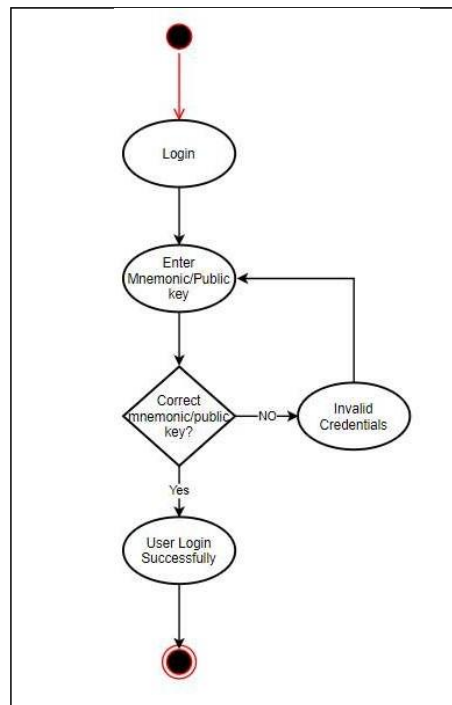


Fig. (12). Activity Diagram.

ER Diagram

The following is the Entity-Relationship Diagram for the system.

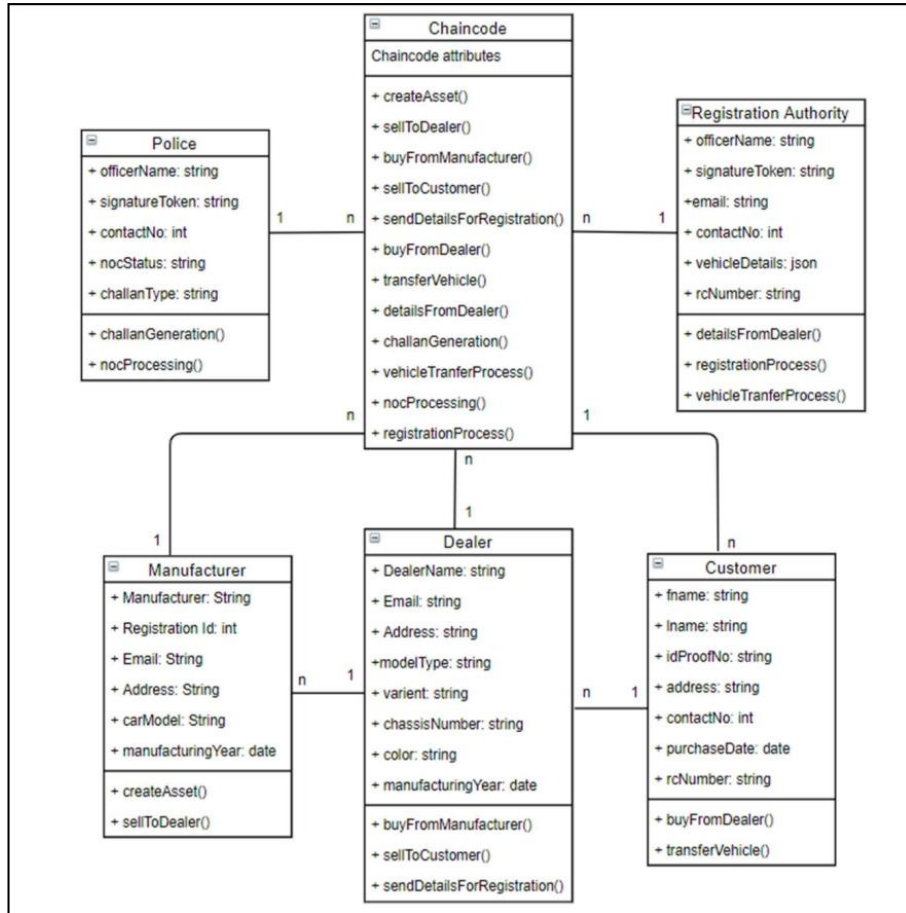


Fig. (13). Entity Relationship Diagram.

Database Schema Diagrams

Hyper ledger Fabric supports two types of peer databases: LevelDB is the default state database embedded in the peer node and stores chain code data as simple key-value pairs; and CouchDB is an alternate state database that supports advanced queries when modeling chain code data values as JSON(as per Figs. 14 to 19).

1. Assets

The following is the schema for the asset data stored in the system.

```
{
  "$class": "org.driveloop.vehicle.Vehicle",
  "vin": "4242",
  "vehicleDetails": {
    "$class": "org.driveloop.vehicle.VehicleDetails",
    "make": "fvefvsd",
    "modeType": "svsds",
    "variant": "csdcsc",
    "chassisNumber": "sdsdcscd",
    "engineNumber": "csdcscd",
    "colour": "sdcsc",
    "manufacturingYear": "csdcsc",
    "bodyWeight": "cdcsc"
  },
  "vehicleStatus": "UNDER_MANUFACTURER"
}
```

Fig. (14). Schema for Assets.

2. Manufacturer

The following is the schema for the manufacturer data stored in the system.

```
{
  "$class": "org.driveloop.participant.Manufacturer",
  "make": {
    "$class": "org.driveloop.participant.Make",
    "name": "BMW",
    "registrationId": "asj5w67dw87wgx87x8vw"
  },
  "particioantId": "9192"
}
```

Fig. (15). Schema for Manufacturer.

3. RTO

The following is the schema for the RTO data stored in the system.

```
{
  "$class":
  "officerName": "Mr. Joe",
  "signatureToken": "43546756545",
}
```

Fig. (16). Schema for RTO.

4. Dealer

The following is the schema for the dealer data stored in the system.

```
{
  "$class": "org.driveloop.participant.Dealer",
  "dealerName": "Man Sales",
  "contact" :{
    "$class": "org.driveloop.participant.Contact",
    "email": "mansales@gmail.com",
    "address": "south district"
  },
  "participantId": "3888"
}
```

Fig. (17). Schema for Dealer.

5. Police

The following is the schema for the police data stored in the system.

```
{
  "$class": "org.driveloop.participant.Police",
  "officerName": "Mr. Joe",
  "signatureToken": "43546756545",
  "participantId": "8753"
}
```

Fig. (18). Schema for Police.

Customer

The following is the schema for the customer data stored in the system.

```
{
  "$class": "org.driveloop.participant.Customer",
  "fName": "Anuranjan",
  "lname" : "Singh",
  "contact": {
    "$class": "org.driveloop.participant.Contact",
    "email": "anuranjansingh@gmail.com",
    "address": "ballia"
  },
  "participantId": "9317"
}
```

Fig. (19). Schema for Customer.

5 Software and Hardware Requirements

Software Requirements

Ubuntu 20.04

Team has chosen Linux operating system for its best support and user friendliness for this project.

Hyper ledger Fabric v0.20

It is used as a modular blockchain structure, which serves as the basis for the development of blockchain-based products, solutions and applications using plug-and-play components intended for use in private companies.

Node JS v12.16.0-x64

It is been used to write down the backend logic *i.e.* Chain code for the automation of the transactions.

Docker 19.03.8

It is used as a service product that uses OS-level virtualization to deliver software in packages called containers.

Postman 7.24.0

It is used to create, share, test and document APIs. This is achieved because users can create and save simple and complex HTTP/s requests and their responses. This results in more effective and less tiring work.

Hardware Requirements

Processor

Intel i5-6200U / Intel Core or better.

GPU

2.30Ghz

Ram

8GB or more.

Hard Disk

20GB or more.

Input Device

Standard Keyboard, Mouse and USB.

IMPLEMENTATION DETAILS

Snapshots of Interfaces (shown in Figs. 20 to 27)

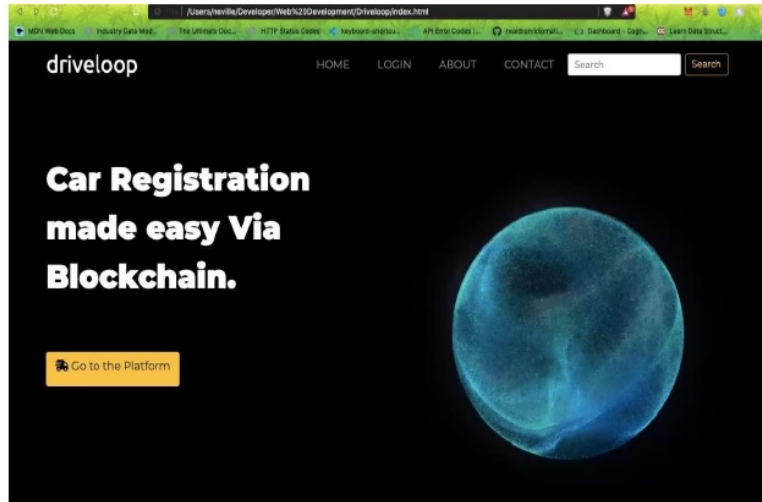


Fig. (20). Front Page.

There are few snapshots from are project.

The above Fig. (20) demonstrates the front page where the user can easily go to the platform and using the drive loop and different blockchain techniques, it felicitates the user for automobile registration using authentic and transparent manner.

Fig. (21) depicts the main page on which user can upload the documents of automobile and can see the all parties which were involved earlier in whole transaction before the registration of this particular vehicle. It will be able to show the whole history of automobile.

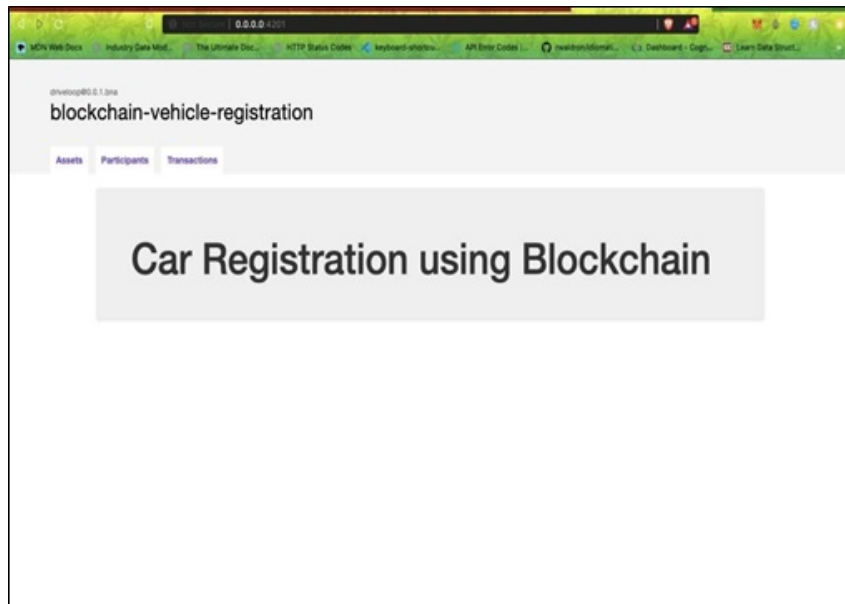


Fig. (21). Main Page.

Asset can be created by above Fig. (22) where the blocks will contain the records for automobile and whole details of all possible transactions will be stored for future purposes. This Asset will be base information and will be authenticated by all parties for transparency.

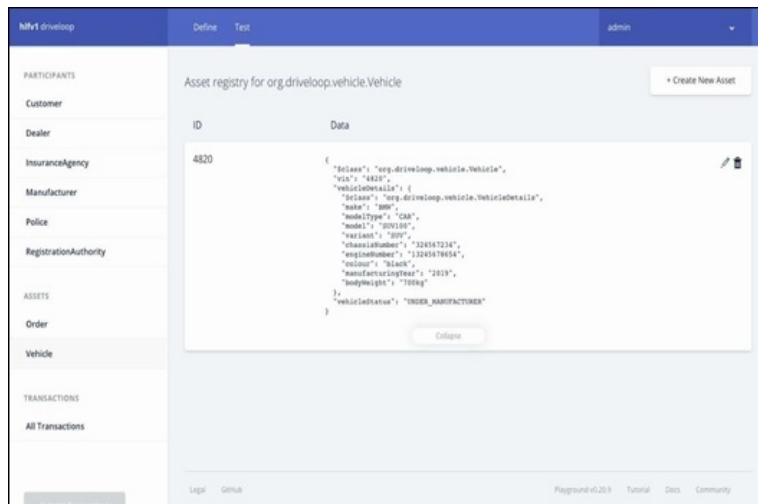


Fig. (22). Asset creation.

Above form in Fig. (23) is to show the model for manufacturer and displays the process of entering the unique and basic details of automobile by the manufacturer which will help to maintain the transparency and ease in smart contract and future transactions.

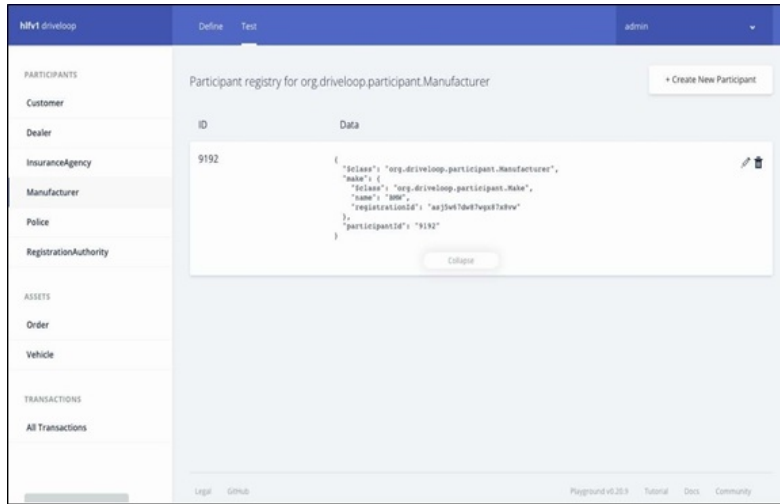


Fig. (23). Model Testing for Manufacturer.

The Fig. (24) code in Hyper ledger shows the transaction history along with all necessary details for a automobile.

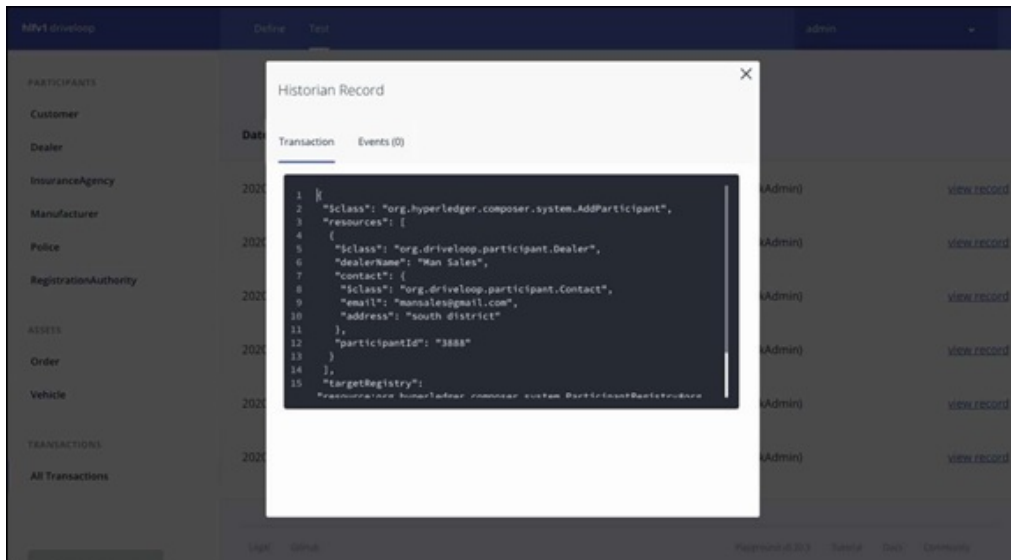


Fig. (24). Transaction History.

Fig. (25) runs the possible test cases and checks the right functioning of the software.

Category	Date, Time	Entry Type	Participant	Action
PARTICIPANTS				
ASSETS				
TRANSACTIONS				

Fig. (25). Process History.

Test Cases

To run the tests locally, we use a Docker file that builds our environment. The Docker file is shown in Fig. (26).

```

EXPLORER
  Dockerfile X
  Dockerfile > ...
  5 #
  6 # http://www.apache.org/licenses/LICENSE-2.0
  7 #
  8 # Unless required by applicable law or agreed to in writing, software
  9 # distributed under the license is distributed on an "AS IS" BASIS,
 10 # WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
 11 # See the license for the specific language governing permissions and
 12 # limitations under the license.
 13 #
 14
 15 FROM node:8-alpine AS builder
 16 ENV NPM_CONFIG_LOGLEVEL warn
 17 RUN mkdir -p /usr/src/app
 18 WORKDIR /usr/src/app
 19 COPY package.json /usr/src/app/
 20 RUN apk add --no-cache make gcc g++ python git && \
 21     npm install && \
 22     npm cache clean --force && \
 23     apk del make gcc g++ python git
 24 COPY . /usr/src/app/
 25 RUN npm run build
 26
 27 FROM node:8-alpine
 28 ENV NPM_CONFIG_LOGLEVEL warn
 29 RUN mkdir -p /usr/src/app
 30 WORKDIR /usr/src/app
 31 COPY package.json /usr/src/app/
 32 RUN apk add --no-cache make gcc g++ python git && \
 33     npm install --production -g pm2 && \
 34     npm install --production && \
  
```

Fig. (26). Docker File.

We'll get a response like this if everything went nicely in Fig. (27) after running all the test cases. The sample snippets are presented for the understanding of the readers.

```
==== RUN: Test_CreateRelatedInvalidParameterNumber
--- PASS: Test_CreateRelatedInvalidParameterNumber (0.00s)
==== RUN: Test_CreateRelatedInvalidJSON
--- PASS: Test_CreateRelatedInvalidJSON (0.00s)
==== RUN: Test_CreateRelatedValidWithName
--- PASS: Test_CreateRelatedValidWithName (0.00s)
==== RUN: Test_CreateRelatedWithInvalidDataTypeForIntegerField
--- PASS: Test_CreateRelatedWithInvalidDataTypeForIntegerField (0.00s)
==== RUN: Test_CreateRelatedWithValidDataTypeForIntegerField
--- PASS: Test_CreateRelatedWithValidDataTypeForIntegerField (0.00s)
==== RUN: Test_DeleteRefugeeInvalidID
--- PASS: Test_DeleteRefugeeInvalidID (0.00s)
==== RUN: Test_DeleteUserInvalidID
--- PASS: Test_DeleteUserInvalidID (0.00s)
==== RUN: Test_DeleteRelatedInvalidID
--- PASS: Test_DeleteRelatedInvalidID (0.00s)
==== RUN: Test_DeleteProcessInvalidID
--- PASS: Test_DeleteProcessInvalidID (0.00s)
==== RUN: Test_DeleteRefugeeValid
--- PASS: Test_DeleteRefugeeValid (0.00s)
==== RUN: Test_DeleteUserValid
--- PASS: Test_DeleteUserValid (0.00s)
==== RUN: Test_DeleteRelatedValid
--- PASS: Test_DeleteRelatedValid (0.00s)
==== RUN: Test_DeleteProcessValid
--- PASS: Test_DeleteProcessValid (0.00s)
PASS
ok      _/usr/src/app/ngo      0.061s
→ chaincode git:(master) X
```

Fig. (27). Test cases.

RESULTS AND DISCUSSION

Driveloop enables all information to be accumulated into one place so that it can be easily accessed and managed. Vehicle Registration, Citations, Insurance Details and everything else accruing to the vehicle in question is integrated on this platform. So, when you log in to find out something about one particular vehicle, what you will find is everything there is to know about it. A comprehensive, all-encompassing history. Anybody who is even remotely aware of the Blockchain technology will tell you how authentic it is.

Driveloop enables all information to be accumulated into one place so that it can be easily accessed and managed. Vehicle Registration, Citations, Insurance Details and everything else accruing to the vehicle in question is integrated on this platform. So, that when you log in to find out something about one particular vehicle, what you will find is everything there is to know about it. A comprehensive, all encompassing history. Anybody who is even remotely aware of the Blockchain technology will tell you how authentic it is. It is structured in such a way that only authorized personnel can make entries or change records. Hence, there is no need to worry about any kind of tempering with the data or falsification of information.

From our research, we implement the blockchain technology to maintain trust, security, and clarity in the system. We use many technologies and one of the technologies is IoT, Ethereum. On the basis of latency of blockchain, the throughput of blockchain, the accuracy of transactions, we test our proposed idea (Table 1).

Table 1. Comparison with existing State-of-the-Art Technologies.

Carchain	Driveloop (Our Application)
1. It is used to maintain the data for rental cars.	1. It is an automated process for buying and selling of cars.
2. It uses the Ethereum platform.	2. It uses Hyper ledger Fabric platform.
3. It is a public blockchain.	3. It is a private blockchain.

NOVELTY AND RECOMMENDATIONS

If you have ever bought your own vehicle or have sold one, or have been a part of an automobile manufacturing or dealing at any stage of the cycle, you would be familiar with the complication that is Vehicle Registration. Given the fact that all vehicles in the market have been sold and resold as they passed through multiple hands, it becomes a cumbersome task to maintain a legitimate record of the history of each vehicle and make it available when needed.

But before we go on to talk about the problems of the process of Vehicle Registration, we first need to understand why Vehicle Registration is such an important aspect of automobile dealing. Car ownership of changes as many times as you can imagine. Whether you look at it in the terms of dealing in spare parts or in assembled vehicles, dealings by the middlemen or by the retailer who makes the final sale to a consumer, or in terms of the resale of a second-hand vehicle, there are a number of stakeholders who would very much want to know about all the history of the vehicle they are buying. Not to mention the insurance agencies, the police and other authorities and well, the government too need to keep tabs on the automobiles for various reasons.

The fact of the matter is that all these stakeholders need information about the vehicles, starting from its manufacturing story, covering its first sale, the accidents, if any, that it has been in, and any and all repairs and maintenance. This is crucial not just to maintain a track record of the vehicle in question to determine its market value, but also for legal and insurance purposes [14].

Vehicle Registration is a way to facilitate this record keeping by maintaining a link between the vehicle and its owner. It might be or not be compulsory, depending on the law of the land. This helps the authorities with regard to

taxation, insurance, or crime detection purposes. Also, it is a way for automobile dealer to keep a track of their vehicles. Thanks to the inclusion of blockchain and the transition of the entire vehicle registration process to blockchain, many of these problems can be easily solved.

The word automobile is derived from the Greek word auto which means “self” and the French word mobile which means ‘moving’. The significance of automobile are as follows:

- a. The increase in the demand for automobiles such as cars and other vehicles increase the income of driver of the automobile industry.
- b. In this foster age, people need to reach destinations rapidly. So, automobiles help one over here and thus have become popular. With the help of automobile, people from all over the world can travel anywhere. Automobiles play a vital role in the country's socio-economic development.
- c. There is also a worldwide sharing in automotive industry of cars, vehicles, parts and accessories that ranges from 15% to 40% in US, South Korea, *etc.*
- d. The automotive industry provides development of the taxable base and revenues of the state budget.
- e. It also influences scientific and technical progress.

FUTURE RESEARCH DIRECTION

There is a huge transformation in urban development in the 21st century because of the advanced technologies and various services. Nowadays, research activities become common for growing smarter cities. Smart City is the demanding solution to sustainability and urbanization. Nowadays, corruption is common and mostly it is paid for by the poor. It is like cancer that eats away at a citizen's faith in the government. For example - smart cities may lead to an injustice world where citizens or people are pushed to subaltern roles and it is regulated by technocratic governments. The increase in population in urban areas often leads to the problem of parking spaces and has been a big challenge for urban planners, architects, and administrators.

There are a few future remedies that can be carried out in this project:

- a. We intend to add certain features like location detection through GPS and the addition of some more services according to user requirements afterwards.
- b. We also intend to add an Insurance party to our project.
- c. We also intend to increase the scalability of this project worldwide *i.e.* beyond our country [17, 18].

LIMITATIONS

The study was a good learning process and was a very satisfying experience. Yet there are several factors that limit these researchers' plans to study as every researcher desired limitations. Some are as follows:-

- a. Access to Documentation and information- The required data was not readily available. The process of documentation is not a continual practice.
- b. Automobile Industry- Because of strict rules and many policies, the R&D and Design executives are bound up in the automotive industry. Data sharing is very limited. To share the information openly and willingly is not considered good practice in corporations.

CONCLUSION

The interesting parts, like fabricators, conventions, clients and automobile agencies, can easily be facilitated for accrediting and updating the information of the vehicle in its security function. The solution also guarantees that the information is more precise and completely sealed and transmits a secure and economical form.

Performance Evaluation

- a. The performance of the service providers is based on ratings given to them by service users.
- b. The performance of the service users is based on ratings given to them by service providers.
- c. The performance of the overall website is based on feedback given to us by the users of the website.
- d. The reviews for the website will be taken from mentors, coordinators and peers' students.

Internet of Things (IoT), big data systems and mobility are some of the services programmers of smart cities. Smart parking is a crucial part of the smart city. Connected automobile with their advanced technology reduces the chances of accident and help drivers save time and gasoline within their limits. More urban our planet becomes, the smarter the cities have to be. In the coming days, due to the advanced technology, the smart cities would be prone to the smarter cities.

CONSENT FOR PUBLICATION

Not applicable.

CONFLICT OF INTEREST

The author declares no conflict of interest, financial or otherwise.

ACKNOWLEDGEMENT

Declared none.

REFERENCES

- [1] A. Agarwal, D. Goel, A. Tyagi, A. Aggarwal, and R. Rastogi, "A Smarter Approach for Better Lifestyle in Indian Societies", In: *Progress in Advanced Computing and Intelligent Engineering. Advances in Intelligent Systems and Computing*, K. Saeed, N. Chaki, B. Pati, S. Bakshi, D. Mohapatra, Eds., vol. 563. Springer: Singapore, 2018, pp. 355-362.
[http://dx.doi.org/10.1007/978-981-10-6872-0_33]
- [2] R. Rastogi, P. Mondal, and K. Agarwal, "An exhaustive review for infix to postfix conversion with applications and benefits", *2nd International Conference on Computing for Sustainable Global Development (INDIACom)*, 2015pp. 95-100
- [3] A. Singh, R. Gupta, and R. Rastogi, "A novel approach for vehicle tracking system for traffic jam problem", *2nd International Conference on Computing for Sustainable Global Development (INDIACom)*, 2015pp. 169-174
- [4] R. Rastogi, R. Mishra, S. Sharma, A. Nigam, and P. Arya, "Security of data transmission using logic gates and crypt analysis", *2nd International Conference on Computing for Sustainable Global Development (INDIACom)*, 2015pp. 101-105
- [5] R. Rastogi, S. Agarwal, P. Sharma, U. Kaul, and S. Jain, "Unsupervised Classification of Mixed Data Type of Attributes Using Genetic Algorithm (Numeric, Categorical, Ordinal, Binary, Ratio-Scaled)", *Proceedings of the Third International Conference on Soft Computing for Problem Solving. Advances in Intelligent Systems and Computing*, vol. 258, 2014pp. 121-131
[http://dx.doi.org/10.1007/978-81-322-1771-8_11]
- [6] B. Rajapandian, V. Harini, D. Raksha, and V. Sangeetha, "A novel approach as an AID for blind, deaf and dumb people", *2017 Third International Conference on Sensing, Signal Processing and Security (ICSSS)*, 2017pp. 403-408
[<http://dx.doi.org/10.1109/SSPS.2017.8071628>]
- [7] S. Arora, J. Maini, P. Mallick, P. Goel, and R. Rastogi, "Efficient E-learning management system through web socket", *3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, 2016pp. 509-512
- [8] D. Goel, A. Agarwal, and R. Rastogi, "A Novel Approach for Residential Society Maintenance Problem for Better Human Life", In: *Communication and Power Engineering.*, R. Rajesh, B. Mathivanan, Eds., De Gruyter: Berlin, Boston, 2017, pp. 177-185.
[<http://dx.doi.org/10.1515/9783110469608-017>]
- [9] D. Goel, A. Agarwal, and R. Rastogi, "'A Novel Approach for Residential Society Maintenance Problem for Better Human Life,'" *International Journal of Urban Design for Ubiquitous Computing, IJUDUC*. Sept. 2016, affiliated to the National Library of Australia", *Global Vision School Publication, Sandy Bay, Tasmania, Australia*, vol. 4, no. 2, pp. 1-8, 2016.
[<http://dx.doi.org/10.21742/ijuduc.2016.4.2.01>]
- [10] R. Gupta, R. Rastogi, P. Mondal, and K. Aggarwal, "GA Based Clustering of Mixed Data Type of Attributes (Numeric, Categorical, Ordinal, Binary, Ratio-Scaled)", *BIJIT*, vol. 7, no. 2, pp. 861-866, .
- [11] R. Sharma, A. Jain, and R. Rastogi, "A New Face To Photo Security Of Facebook, Proceedings", *In the Proceedings of Sixth International Conference on Contemporary Computing (IC3-2013) Jointly*

Organized by Jaypee Institute of Information Technology & University of Florida on August 8–10, 2013 pp. 415-420. <https://ieeexplore.ieee.org/document/6612231>
[<http://dx.doi.org/10.1109/IC3.2013.6612231>]

- [12] M. Pilkington, "Blockchain technology: principles and applications", *Research handbook on digital transformations*, p. 225, .
- [13] Shwet, S.K. Sharma, and R. Rastogi, "A revolutionary technology to help the differently abled person", *2nd International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 622-624, 2015.
- [14] R. Rastogi, S. Agarwal, P. Sharma, U. Kaul, and S. Jain, "Business Analysis and Decision Making Through Unsupervised Classification of Mixed Data Type of Attributes Through Genetic Algorithm", *BIJIT- 2014*, vol. 6, 2014no. 1, pp. 683-689. <http://bvicam.ac.in/bjit/issues.asp?issue=11>
- [15] T.N. Pham, M. Tsai, D.B. Nguyen, C. Dow, and D. Deng, "A Cloud-Based Smart-Parking System Based on Internet-of-Things Technologies", *IEEE Access*, vol. 3, pp. 1581-1591, 2015.
[<http://dx.doi.org/10.1109/ACCESS.2015.2477299>]
- [16] R. Rastogi, S. Agarwal, P. Sharma, and U. Kaul, "A Novel D&C Approach for Efficient Fuzzy Unsupervised Classification for Mixed Variety of Data. Advances in Intelligent Systems and Computing", *Emerging ICT for Bridging the Future - Proceedings of the 49th Annual Convention of the Computer Society of India CSI Volume 2. Advances in Intelligent Systems and Computing*, vol. 338, pp. 553-563
[http://dx.doi.org/10.1007/978-3-319-13731-5_60]
- [17] R. Rastogi, S. Mittal, and S. Shekhar, "Linear algorithm for Imbricate Cryptography using Pseudo Random Number Generator", *2nd International Conference on Computing for Sustainable Global Development (INDIACom)*, 2015pp. 89-94
- [18] S. Srivatava, R. Rastogi, S. Rungta, and U. Yadav, "A Methodology to Find the Cycle in a Directed Graph Using Linked List", *BIJIT*, vol. 6, no. 2, pp. 743-749, 2014.

Identification of Counterfeit Drugs Using Decentralized Supply Chain

Koyel Datta Gupta^{1,*}, Aditya Gupta¹, Tanmay Sharma¹ and Aayush Bhatnagar¹

¹ Department of Computer Science & Engineering, Maharaja Surajmal Institute of Technology, New Delhi 110058, India

Abstract: This research attempts to overcome the problems faced by the medical healthcare system by using the advancing technology of blockchains. Pharma companies that manufacture and sell medicines face difficulties in tracking drugs, which in turn allows the counterfeiters to exploit the system. The decentralized abilities of blockchain technology enable us to counter the problems in existing centralized systems. The blockchain helps us to make sure that the quality is maintained throughout the decentralized supply chain. The use of blockchains in the medicine supply chain solution entails tracking the validity of the medicine from the producer to the distributor to the pharmacy. It assures that the pharmacist receives the original medication and does not reach the grey market. In this paper, the decentralized application which we created works using Ethereum and is based on blockchain technology. The medicine discovered by a pharmaceutical company is to be validated by an officer in a decentralized manner using smart contracts over Ethereum transactions. The validated drugs can then be produced and sold on the platform, where the entire data and the stages of the drug/medicine are tracked and stored. Research and development of such a system are necessary to facilitate the proper supply and tracking of medicines and to avoid counterfeiting.

Keywords: Blockchain, Ethereum, Smart contracts, Decentralized application (DApp).

INTRODUCTION

According to recent findings, drug counterfeiting is one of the significant problems in second and third-world countries. Individuals and the general public are in danger due to the effects of this occurrence. They are especially common in countries where surveillance and regulation ought to be enhanced or are inadequate, as well as in nations where drugs are in great demand but remain

* Correspondence author **Koyel Datta Gupta**: Department of Computer Science & Engineering, Maharaja Surajmal Institute of Technology, New Delhi, 110058, India; Tel: 9999061790; E-mail: koyel.dg@msit.in

mostly expensive. They are also prevalent during disease outbreaks and epidemics when vital pharmaceuticals are in limited supply and counterfeiting is widespread. Unauthorized pharmaceutical companies employ their cunning minds and expertise to develop identical replicas of the real pharmaceuticals that are undetectable. Fake drugs are harmful to the consumers as they might contain false ingredients and the patients are unable to identify them. Overdosage of the ingredients is also a common issue. Toxins and pollutants have the potential to cause allergic responses as well as adverse medicinal responses. Counterfeit pharmaceuticals squander people's money and raise the government's financial burden. Additionally, it may undermine public trust in the effectiveness of genuine treatments.

The Indian government presently lacks an efficient strategy for dealing with the problem of fraudulent medications made in India. Despite some progress, there has been no major innovation in combating the country's fraudulent medicines economy. A thorough study of the world's pharmacy business indicated that many of the substandard pharmaceuticals originate in India. India is among the leading exporters of drugs worldwide. Thus, there is a scope for intermixing fraudulent medicines and original medicines. This makes it arduous for government authorities to detect fraudulent drugs. This makes India one of the biggest fraud medicine markets worldwide. It is found that this problem is the result of complexity in the medication supply chain and a lack of process integrity.

Another obstacle faced by the customer is the monitoring of medications that can only be obtained through a prescription. While the selling of medicines without a prescription is against the law, keeping track of wholesaler honesty, in addition to the challenge of counterfeit drugs, is difficult and requires a unique strategy. Blockchain medication inventory might give major benefits with barcode-tagged medications scanned and placed into secure digital blocks anytime they change hands. Every exchange of hands is deemed a transaction, and it is recorded on blockchain technology, which is unchangeable, decentralized, and global.

Blockchain

Satoshi Nakamoto first created blockchain in the form of the popular cryptocurrency 'Bitcoin' [1]. In a peer-to-peer (P2P) network, each user is referred to as a node, and the transactions that take place are categorized as blocks. The blocks are then interconnected in an order. One pair of public-private keys is associated with each node. The public key is used to recognize the node as a sender or a recipient, while the associated private key is used by a sender to sign transactions and by a recipient to validate them. In addition to enabling the appropriate key to decrypt and collect the information, a deal among the

participating nodes must be attained before adjustments can be implemented. This guarantees that all blockchain ledger replicas are synchronized across the network. Users can always get the most up-to-date or, in other words, the most recent copy of a transaction when a transaction occurs, thanks to the blockchain's build architecture (Fig. 1). Whenever a transaction occurs in the chain, the entire network is updated. This is possible as all other network participants are provided with a copy of the transaction. Blockchain has been used in several applications [2 - 4].

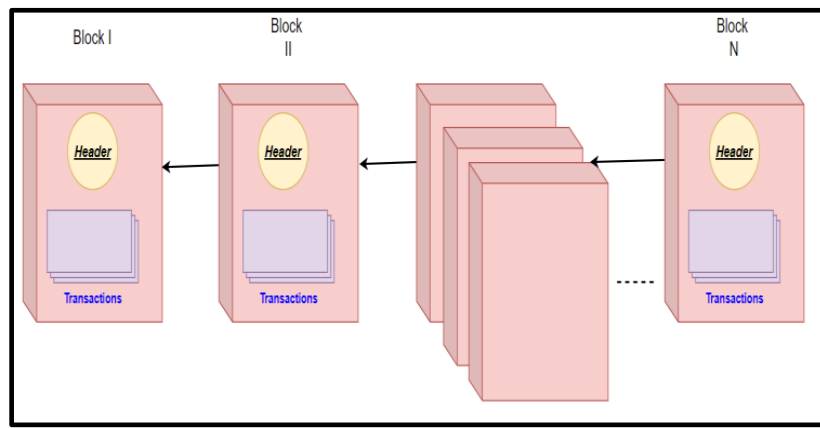


Fig. (1). Blockchain Architecture.

Public, private, and consortium are the three types of Blockchain. Each participant on the public blockchain can see and authenticate any transaction occurring on the network, as well as partake in the consensus mechanism. In the consortium blockchain, there must be an administrative node, which is initially chosen by network members based on the effective ways to accomplish their business objectives, such as in the case of a company. Except for one difference, a private blockchain is similar to the previous type where the public has no access to any of the data in such a distributed registry.

Smart Contract

A decentralized ledger can also be utilized to build a self-executing contract, also known as a smart contract. They are a type of digital service agreement stored in the blockchain as codes and execute only when a specific criterion is reached. Smart contracts can thus be implemented into a blockchain database and allow users to create computer codes based on contractual agreements. A contract hash and a contract address are present in a smart contract, which played a significant

role in the subsequent process of recovering the contract in a secure and abscond way. Smart contracts, with updates and an event-driven framework, may make it easier to manipulate supply chain processes. Commercial pilots such as IBM and Maersk, for example, recently revealed their successful deployment of blockchain technology and smart contracts for shipment tracking and trade finance.

The supply chain's efficiency can be improved using smart contracts. Drug transportation is prone to a range of factors, such as toxicity due to high temperature or delay in payment by the recipient. Various vaccines, such as insulin, and specially prepared drugs, must be stashed at a reduced temperature to avoid contamination. A thermometer can be installed inside the storage system to constantly monitor the temperature. Using smart contracts, if the temperature rises to a certain level for an extended period, an alert system will be recorded in the blockchain. As a result, the receiver is notified that the medications are not being handled appropriately and may be polluted.

Similarly, smart contracts can be used to conduct fees to the sender as quickly as the package is delivered to the recipient. Smart contracts on a blockchain-based network can be used in a variety of industries; however, past research has revealed several unsolved challenges in terms of technological and legal problems. Contract weaknesses, such as transaction-ordering and timestamp reliance, mishandled errors, re-entrance, and call stack concerns, are examples. Smart contracts, based on technical openness, may ease obligation execution and automation systems among participants; yet, their long-term growth still needs a multidisciplinary strategy that combines technical, economic, and legitimation methods.

Supply Chain

A supply chain is nothing more than a diagram that depicts how items move from one location to another by storing them or by establishing checkpoints. In terms of geographical locations, the reach of the supply chain has shifted dramatically during the last several decades. This chain's function has shifted dramatically, and errors are now extremely rare since it validates transactions at multiple stages using a variety of approaches. The primary entities in this scenario are the buyer and vendor. As a result, if any entity in this process engages in illicit conduct, the entire system suffers.

Large files, like photographs, are often saved off-chain in most blockchain-based apps, whereas text data is kept on-chain. With the use of blockchain, a specific mobile app and its movement throughout the supply chain might be tracked. Thus, the outmoded medicine supply chain may be redesigned utilizing blockchain, potentially unlocking the actual benefit of interoperability. A fake medicine enters

the supply chain when its aspect is as close to the original as feasible. With sophisticated printing processes and expertise, imitating a QR code is not a tough feat. This creates a dilemma in that more than two medicine packages with identical printed codes, one is real and the others are false, can infiltrate the supply chain, and each one is detected to be the genuine one.

Ethereum

Ethereum is a blockchain-based, open-source, software platform (decentralized) with ether as its cryptocurrency that was launched on 30th July 2015. Smart contracts and Distributed Applications are allowed to be written and operated without the risk of an outage, control, fraud, or 3rd party intervention. Ethereum is both a programming language and a platform that runs on a blockchain, using which software developers create distributed applications. Ether is used in Ethereum which is a platform-specific token of cryptography. Ethereum hosted a pre-sale for ether in 2014, which grabbed large-scale attention. Software developers wishing to create and run apps on the platform. Ether is a transportation mode for the platform of Ether. Because of its programmability, Ethereum is utilized as a platform to operate numerous decentralized apps.

RELATED WORK

The authors of the study [5] suggested an approach based on the Ethereum blockchain taking advantage of smart contracts and decentralized offline storage for effective product tracking in the medical supply chain. The proposed solution builds upon the core principles of cryptography underlying blockchain technology to produce immutable logs of supply chain events and uses smart contracts inside the Ethereum blockchain to carry out automated transcribing of events that are available to all stakeholders. The proposed solution is cost-effective in terms of how much gas is spent performing the different functions that are triggered in the smart contract. Thomas Bocek *et al.* [6] showcased the use of IoT (Internet of Things) sensors devices taking advantage of blockchain technology to affirm the immutability of data and public availability of temperature records while minimizing the operating costs of the drug supply chain. To assure quality control and adherence to regulations for the transportation of medical items, the healthcare sector employs of several complicated and stringent environmental control techniques. The sensors monitor the temperature of each package during shipping to verify compliance with GDP guidelines. All data is transmitted to the blockchain, where it is evaluated to about the product qualities *via* a smart contract.

The authors of the study [7] attempted to overcome possible barriers associated with the adoption of blockchain through rigorous application design and

execution. They used blockchain to safely and efficiently distribute privacy-preserving prediction models among healthcare organizations. They used smart contracts to automate data management procedures, encrypted sensitive data over the blockchain, preserved sensitive data off the blockchain, and only broadcasted “pointers”. The author of [8] initially tells the need for which blockchain technology was created and then speaks about the uses for which it has been adapted. One such use case is the healthcare system. The author talks about the 2 main applications - handling of data and traceability of drugs. The author suggests a system that can help trace drugs and reduce the possibility of counterfeit drugs. Discussion and application of such methods have also been suggested.

The author of the study [9] states counterfeiting is the most serious problem in pharmacology. The main problem is the side effects due to these counterfeit drugs (much higher than normal drugs). The author also tells about the distribution of such drugs on various continents. Online pharmacies and their distributed supply chain have made the job of tracking harder. A blockchain-based smart contacts solution is suggested by the author. The author of [10] states blockchain is a popular emerging technology. Healthcare is the field that could benefit the most from such secure technology. Problems and issues in the healthcare system have been stated. The author discusses blockchain’s use in this field and how it tackles and solves problems and issues. More services inside healthcare that can benefit from blockchain have been mentioned.

The authors of the study [11] claimed that the pharma companies that produce and ship the supply products face difficulties in tracking and organizing the medicine products, which allowed counterfeiters to exploit the current system. With blockchain, the records of the medicines/drugs can be accurately determined and tracked to check the authenticity of medicines. The development and proper implementation of such a system is the next important task. Neeraj Kumar *et al.* [12] proposed that the use of blockchain across the supply chain can solve a lot of queries of the manufacturers, distributors, and the verification organization. They have used an Ethereum blockchain to create a decentralized app. The main reason they have used blockchain is because of the features it provides like traceability and immutability. The users can track the medicines or products to their origin.

The authors of the study [13] explored the current status and applications of blockchain in decentralized supply chain management systems. Qualitative methods were implemented to describe and predict the evaluation of blockchain in such systems. They implemented a system to publish research papers on blockchain in a traceable and immutable fashion. Similar procedures can be introduced to other supply chain systems such as our “drug supply chain” system. The authors of [14] addressed the problem of duplicate drugs created by fake

manufacturers by using smart contracts which help to track the movement of medicines in the supply chain starting from the manufacturer to the patient. To avoid an overdose of medicines patients, they implemented a mobile application so that patients cannot buy excess drugs and that they could only purchase medication with the doctor's prescriptions that could be verified using an attached QR Code scanner.

The author of the study [15] explains the problems faced by the healthcare system. The major reasons for such problems are non-regulation and the complexity of the supply chain of drugs. Assurance of quality and transparency will strengthen the whole system. Implementing India's supply chain of drugs most of the problems are resolved. Smart Contracts are employed for building trust, security, and automation of the solution. The authors of [16] suggested a Distributed Application that will run on the Ethereum blockchain using smart contracts. They suggested modifying the proof-of-work algorithm of Ethereum into a proof-of-stake consensus algorithm as it will be more scalable and suitable to the medicine supply chain systems. They created a GUI portal for their "Drug Surveillance System" where the pharma company and the consumers can check the origin of the drug by scanning the barcode of the medicine.

METHODOLOGY

We have proposed a solution based on Ethereum using smart contracts for the Identification of Counterfeit Drugs Using a Decentralized Supply Chain. It assures that the pharmacist receives the original medication and that it does not reach the grey market.

The full flow of the supply chain of our proposed solution (Fig. 2) looks like this:

A Pharmaceutical Company discovers a drug (all the information regarding the drug will be looked at, such as the ingredients of the drug and the name of the pharmaceutical company) and generates a universal product code. The Medicine Verification Organization then approves the medicine corresponding to the Universal Product Code and creates a unique hash out of drug details.

The Pharmaceutical Company sends the drug to mass production to the manufacturers. Then, the Pharmaceutical Company sends the drug to the wholesalers.

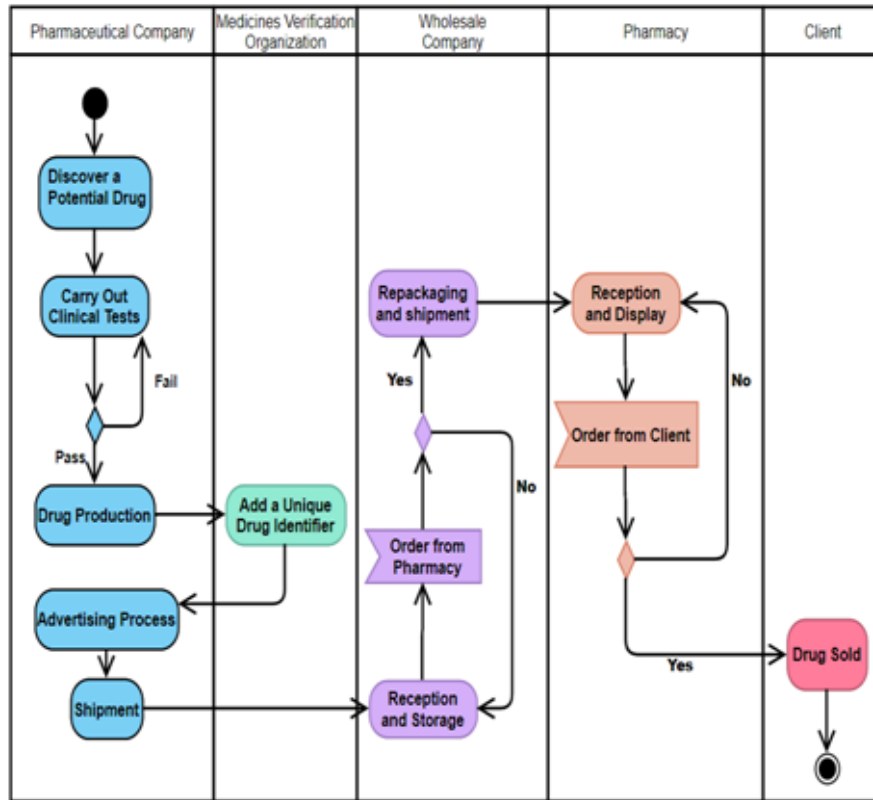


Fig. (2). Activity Diagram.

The Wholesalers then buy the drug and sell it to retail. The pharmacy buys the drug and puts it on sale. The consumer buys the drug from the pharmacy and the entire transaction process will be tracked and stored on the website, where every member of the supply chain from the pharmaceutical company to the consumer can check the website for the details of the transaction on.

This procedure will be implemented on Ethereum transactions using smart contracts. The sequence diagram of the same is shown in Fig. (3).

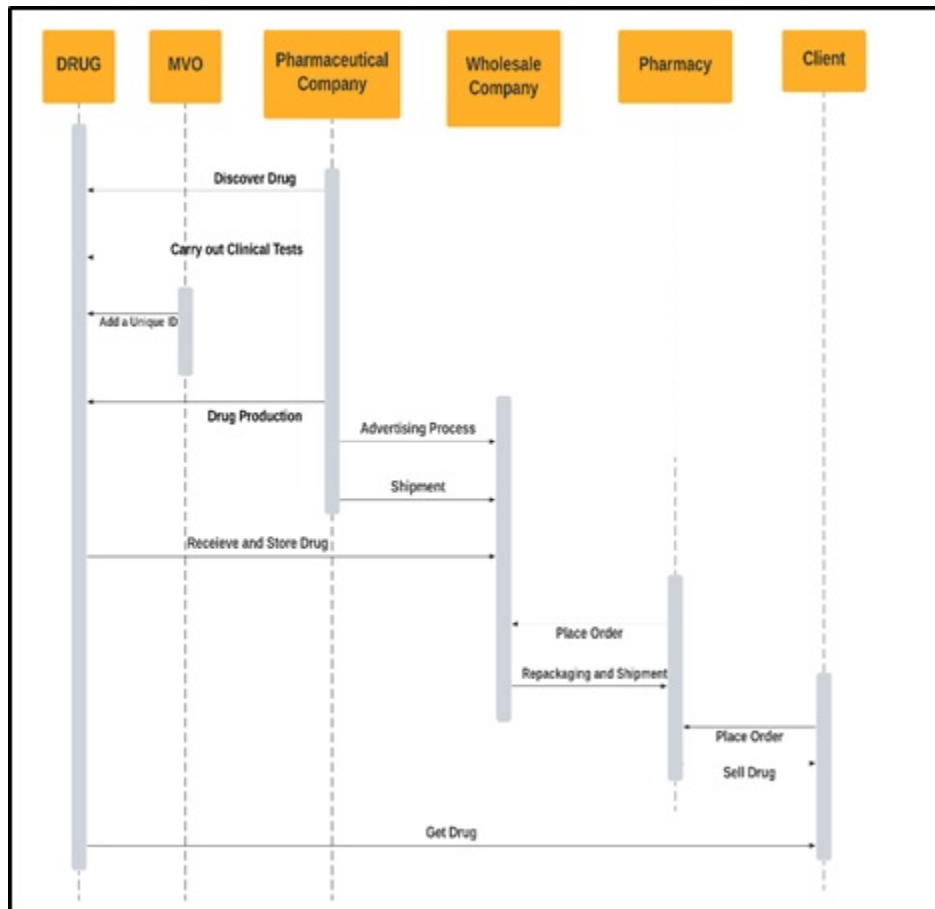


Fig. (3). Sequence Diagram.

The states of the drug/medicine in the supply chain are: Discovered- The drug to be sold is first designed by the manufacturer, Approved- The drug will then be approved (by MVO). Produced- The drug is then produced by the manufacturer, For Wholesale- The drug is allowed to be bought by the wholesalers, For Retail (owned by a wholesaler) - The drug is then sent to the retailers, For Sale (owned by a pharmacy)- the drug is put on sale by the retailer, Sold (owned by a client). The transaction (Fig. 4) will be tracked using smart contracts.

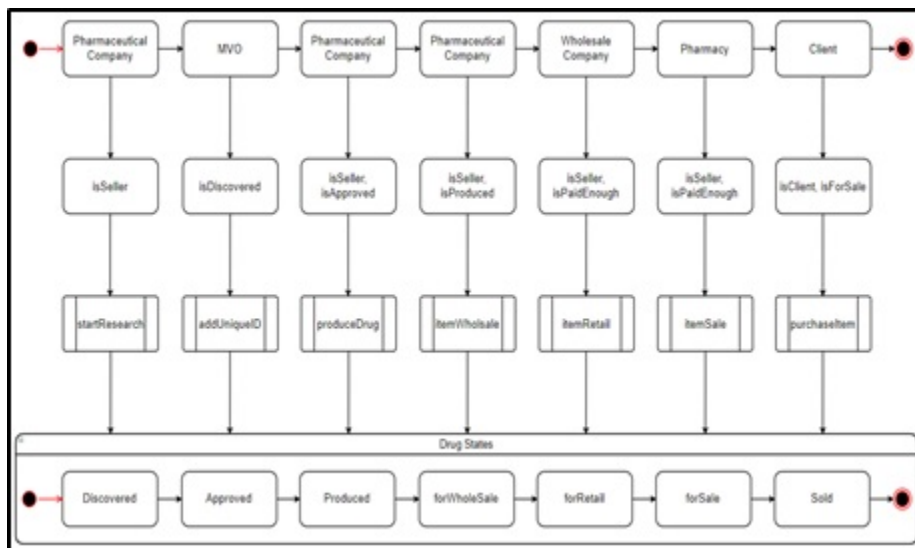


Fig. (4). State Diagram.

CONCLUSION

In this study, we explored the problem of medication tracking within supply chain networks, emphasizing its importance in combating fraudulent medicines. We created a blockchain-based system for tracking and tracing medicines in a decentralized manner for the pharma industry. The client cannot purchase excess medication since the supplier includes a maximum limit per patient. The medicine supply chain is adequately tracked thanks to smart contracts in blockchain. The suggested system is a proof-of-concept tool that enables blockchain technology to maintain track of individual medication data in a decentralized manner. Through continuous records, enables healthcare professionals, nurses, clients, and chemists to maintain, access, and exchange personal medical information as well as a complete individual medication cycle of life way safely and responsibly.

CONSENT FOR PUBLICATION

Not applicable.

CONFLICT OF INTEREST

The author declares no conflict of interest, financial or otherwise.

ACKNOWLEDGEMENT

Declared none.

REFERENCES

- [1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", Available online: <https://bitcoin.org/bitcoin.pdf>
- [2] M. Sharma, S. Pant, D.K. Sharma, K. Datta Gupta, V. Vashishth, and A. Chhabra, "Enabling security for the Industrial Internet of Things using deep learning, blockchain, and coalitions", *Trans. Emerg. Telecommun. Technol.*, p. e4137, 2020.
- [3] S. Banyal, M. Saxena, and D.K. Sharma, *Blockchain-Enabled Security and Privacy Schemes in IoT Technologies*, 2020.
- [4] D.K. Sharma, S. Pant, M. Sharma, and S. Brahmachari, Cryptocurrency Mechanisms for Blockchains: Models, Characteristics, Challenges, and Applications. *Handbook of Research on Blockchain Technology*. Academic Press, 2020, pp. 323-348.
[<http://dx.doi.org/10.1016/B978-0-12-819816-2.00013-7>]
- [5] A. Musamih, K. Salah, R. Jayaraman, J. Arshad, M. Debe, Y. Al-Hammadi, and S. Ellahham, "A Blockchain-Based Approach for Drug Traceability in Healthcare Supply Chain", *IEEE Access*, vol. 9, pp. 9728-9743, 2021.
[<http://dx.doi.org/10.1109/ACCESS.2021.3049920>]
- [6] T. Bocek, B. Rodrigues, T. Strasser, and B. Stiller, "Blockchains everywhere - a use-case of blockchains in the pharma supply-chain", *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, 2017pp. 772-777 Lisbon, Portugal.
[<http://dx.doi.org/10.23919/INM.2017.7987376>]
- [7] T.T. Kuo, H.E. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications", *J. Am. Med. Inform. Assoc.*, vol. 24, no. 6, pp. 1211-1220, 2017.
[<http://dx.doi.org/10.1093/jamia/ocx068>] [PMID: 29016974]
- [8] K. Kumari, and K. Saini, "Data Handling & Drug Traceability: Blockchain Meets Healthcare to Combat Counterfeit Drugs", *International Journal of Scientific & Technology Research*, vol. 9, no. 3, pp. 728-731, 2020.
- [9] F. Jamil, L. Hang, K. Kim, and D. Kim, "D., "A Novel Medical Blockchain Model for Drug Supply Chain Integrity Management in a Smart Hospital", *Electronics (Basel)*, vol. 8, no. 5, pp. 505-536, 2019.
[<http://dx.doi.org/10.3390/electronics8050505>]
- [10] K. Shuaib, H. Saleous, K. Shuaib, and N. Zaki, "Blockchains for Secure Digitized Medicine", *J. Pers. Med.*, vol. 9, no. 3, pp. 35-55, 2019.
[<http://dx.doi.org/10.3390/jpm9030035>] [PMID: 31337080]
- [11] S.R. Bryatov, and A. Borodinov, "Blockchain technology in the pharmaceutical supply chain: researching a business model based on Hyperledger Fabric", *Proc. International Conference on Information Technology and Nanotechnology*, vol. 2416, 2019 pp. 134-140.
[<http://dx.doi.org/10.18287/1613-0073-2019-2416-134-140>]
- [12] N.K. Yadav, and H.P. Singh, "Pharmaceutical Supply Chain Management Blockchain", In: *Proceedings of International Conference on Big Data, Machine Learning and their Applications. Lecture Notes in Networks and Systems*, S. Tiwari, E. Suryani, A.K. Ng, K.K. Mishra, N. Singh, Eds., vol. 150. Springer: Singapore, 2021, pp. 181-190.
[http://dx.doi.org/10.1007/978-981-15-8377-3_16]
- [13] S.E. Chang, and Y. Chen, "When Blockchain Meets Supply Chain: A Systematic Literature Review on Current Development and Potential Applications", *IEEE Access*, vol. 8, pp. 62478-62494, 2020.
[<http://dx.doi.org/10.1109/ACCESS.2020.2983601>]
- [14] K. Benita, "Authentic Drug Usage and Tracking with Blockchain Using Mobile Apps", *International Journal of Interactive Mobile Technologies*, vol. 14, no. 17, pp. 20-32, 2020.

[<http://dx.doi.org/10.3991/ijim.v14i17.16561>]

- [15] A. Kumar, D. Choudhary, M.S. Raju, D.K. Chaudhary, and R.K. Sagar, "Combating Counterfeit Drugs: A quantitative analysis on cracking down the fake drug industry by using Blockchain technology", *9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, 2019pp. 174-178.
[<http://dx.doi.org/10.1109/CONFLUENCE.2019.8776891>]
- [16] P. Sylim, F. Liu, A. Marcelo, and P. Fontelo, "Blockchain Technology for Detecting Falsified and Substandard Drugs in Distribution: Pharmaceutical Supply Chain Intervention", *JMIR Res. Protoc.*, vol. 7, no. 9, p. e10163, 2018.
[<http://dx.doi.org/10.2196/10163>] [PMID: 30213780]

Making Great Strides Towards Road Detection

Vimal Gaur^{1,*}

¹ *Maharaja Surajmal Institute of Technology, Computer Science and Engineering Department, Janakpuri, New Delhi 110058, India*

Abstract: A significant amount of research has been carried out in extracting land surface objects, but intelligent digital surface models for monitoring land surface objects are still an active research topic due to emerging technologies such as IoT and Blockchain. These technologies play an important role in quantifying the ecological and geographical properties of the land surface. About such technology of detecting buildings, roads, and terrain from satellite images offer a lot of potential for tracking the migration of large chunks of the population and helps in geographical analysis of the city. In this paper, we explore a Convolutional Neural Network method for extracting land surface objects from satellite imaging with the help of U-Net. As a known fact, the number of disasters occurring every year affects thousands of the population, so suitable mechanisms must be provided for rescue operations. To provide these rescue operations, predictions about the geographical location are of primary importance. Our model produces reasonable accuracy of 60.62% at a very minimal loss rate.

Keywords: U-Net, Spatial Processing, Image Segmentation, Deep Learning, Computer Vision, Down and Up Sampling, Skip Connection.

INTRODUCTION

The extensive process of mapping out the populated regions of a metropolitan city or even a remote town can be laborious and painstaking when done according to outdated methods. Population hotspots in metropolitan areas are rapidly changing the cause of bodily movement but also because of environmental alterations both induced naturally, like fluctuation in living conditions such as a change in weather, or human-induced like contamination of groundwater through drilling for oil. This indicates that mapping is difficult, especially in remote divisions where the attention of the authorities is minimum. Our paper focuses on addressing the wider aspect of image segmentation of satellite images by directing our classification at pixel level and checking whether pixels belong to road/path-

* **Correspondence author Vimal Gaur:** Maharaja Surajmal Institute of Technology, Computer Science and Engineering Department, Janakpuri, New Delhi, Delhi 110058, India; Tel: 9999620069; E-mail: vimalgaur@msit.in

way or not. We have developed a model for dealing with affected areas that are under stress and finding the most efficient routes to provide aid in those areas as early as possible. As seen in the year 2020 and its harrowing outbreak all around us, the outbreak of COVID-19 tested the readiness of governments of many nations. The impact of the virus could have been made minimal in many countries just by simple mapping out hotspots and by also calculating the appropriate way of distributing the test kits. All this could have been a straightforward task by using a deep learning algorithm altogether like ours. The impact on third-world countries like India, where masses have to depend on a government instantly in a situation of a pandemic like this, needed to be calculated beforehand amidst the lockdown [1 - 3]. We have tried to extend this concept to the physical world rather than in the medical field. This paper addresses the issue of segmentation of images obtained by satellite imaging. It dissects the image pixel by pixel and classifies each pixel as part of the road. We have trained our model on a set of high-resolution images obtained from [4]. As we learned from another study [5] downsampling could help us in simplifying the problem we face with high-resolution and small-size lesion regions. Our images were correspondingly labeled with binary masks, *i.e.* given a satellite image as input, our program was then able to output a corresponding predicted binary mask, which was then further processed into more labeled and accurate data to aid us in our mission of mapping route enhancement using image segmentation [6].

RELATED WORK

A few authors [5] extracted maximum accuracy when U-Nets are used in global and local modes.

Extracting objects namely buildings, lakes, ships etcetera from satellite images is not a recent field of examination. SVM algorithm has been used to extract buildings from high-resolution images [6]. A different approach called a full convolution network, which is very prevalent in today's image segmentation projects has been applied.

By extrapolation of and building more on FCN network, we get a specific type of neural network which is called U-Net, which has proven its worth in bio-medical research and works even on a small number of datasets. Moreover, similar work has been done on loss function and accuracy metrics [7]. In this paper, the author discusses pixel accuracy and the importance of right accuracy metrics and loss metrics [8, 9].

Some other works in the field of medical science include the implementation of a convolutional neural network in the segmentation of blood vessels in retina

fundus images. The neural network classifies each pixel in the fundus images as either a vessel or not using binary classification tasks.

DATASET

Data Selection

The dataset required for our model consists of 1113 satellite images and their masks [4]. Images in this dataset are very high resolution and their masks are black and white. The white pixel in the mask represents the road and the remaining area is represented by the black pixel. These are clearly shown in Fig. (1).



Fig. (1). Images before Pre-Processing.

Preprocessing

After completely analyzing the dataset, it has been noticed that all the images are not complete. To avoid vague data, all these images are removed and the dataset

is reduced to 979 images. Another big issue in training our model was the size of images, size has been reduced from (1500x1500) to (256x256). The main benefit of reducing the size of the image is the increase in the size of the training dataset. Pre- Processing training dataset includes 35244 images and a few samples of images have been shown in Fig. (2).

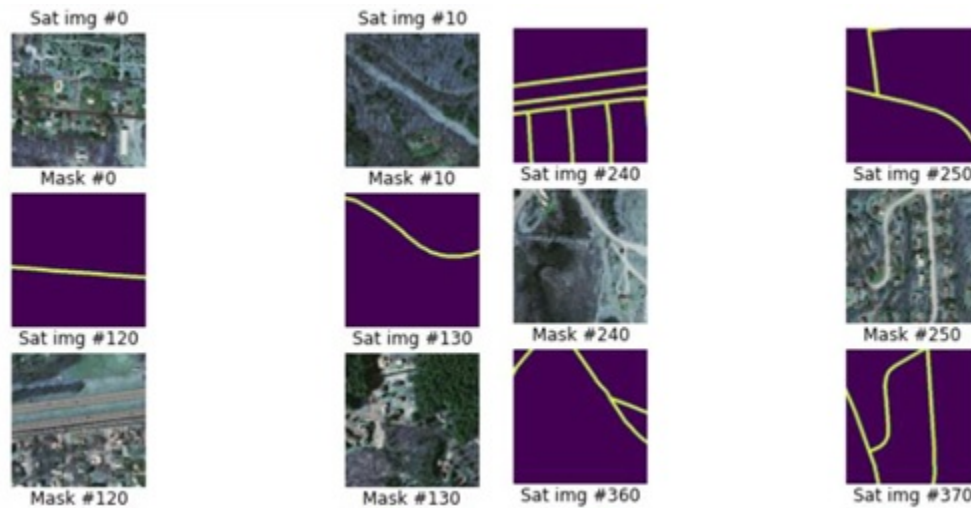


Fig. (2). Images after Pre-Processing.

Method

In our paper, we have developed a model using Convolution Neural Network and U-Net and it has been implemented in Tensor-Flow.

CNN (Convolution Neural Network) automatically extracts useful features from an image by performing several pooling and convolution operations on the image, which is fed to the model as input. U-NET is a special case for CNN in which convolution and deconvolution are used simultaneously. It is a very powerful and precise model for image segmentation tasks and works on even a limited number of inputs [10 - 12].

TensorFlow is open-source software as it interacts with GPU to maintain data flow and differential programming for a range of tasks. Keras is also an open-source software that is written in python. It works over TensorFlow. It comes in handy in experimentation with a deep neural network which can be a tedious task on TensorFlow as it contains different libraries and functions which work as building blocks for the neural network.

Architecture of the Model

In our model, we have inculcated the basic principles of U-Net [13]. U-Net is a pair of down-sampling and up-sampling. During contraction path, features of down-sampling activation function and max-pooling extracts and features from images and symmetric expanding path up-sample the result from the previous step and increase the resolution of the extracted feature. Along with expanding and contracting path skip connections are used, which provides context and localization. This architecture can be more clearly depicted in Fig. (3) below:

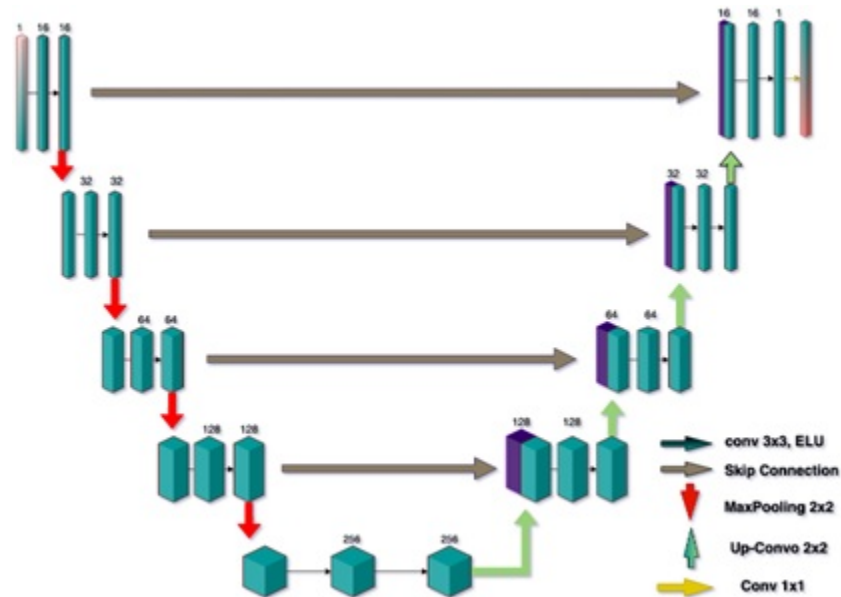


Fig. (3). U-Net Architecture.

Model Summary

The above architecture has been implemented using Keras and is depicted below using the snapshot of the involved portion of the script. Our model starts with taking input of dimension (256, 256, 3) after passing through various parts of U-Net it is reduced to (128,128,32) after batch normalizer 2.

The similar layers perform the same function to new image input and successively reduce it to (64, 64, 64), (32, 32, 128), (16, 16, 256) after batch normalizer 4, batch normalizer 6, and batch normalizer 8, respectively. This process is called contraction in which downsampling of features takes place and has been shown in Figs. (4 and 5) below.

Layer (type)	Output Shape	Param #	Connected to
input_1 (InputLayer)	(None, 256, 256, 3)	0	
conv2d_1 (Conv2D)	(None, 256, 256, 16)	448	input_1[0][0]
batch_normalization_1 (BatchNor	(None, 256, 256, 16)	64	conv2d_1[0][0]
dropout_1 (Dropout)	(None, 256, 256, 16)	0	batch_normalization_1[0]
conv2d_2 (Conv2D)	(None, 256, 256, 16)	2320	dropout_1[0][0]
batch_normalization_2 (BatchNor	(None, 256, 256, 16)	64	conv2d_2[0][0]
max_pooling2d_1 (MaxPooling2D)	(None, 128, 128, 16)	0	batch_normalization_2[0]
conv2d_3 (Conv2D)	(None, 128, 128, 32)	4640	max_pooling2d_1[0][0]
batch_normalization_3 (BatchNor	(None, 128, 128, 32)	128	conv2d_3[0][0]
dropout_2 (Dropout)	(None, 128, 128, 32)	0	batch_normalization_3[0]
conv2d_4 (Conv2D)	(None, 128, 128, 32)	9248	dropout_2[0][0]
batch_normalization_4 (BatchNor	(None, 128, 128, 32)	128	conv2d_4[0][0]
max_pooling2d_2 (MaxPooling2D)	(None, 64, 64, 32)	0	batch_normalization_4[0]
conv2d_5 (Conv2D)	(None, 64, 64, 64)	18496	max_pooling2d_2[0][0]
batch_normalization_5 (BatchNor	(None, 64, 64, 64)	256	conv2d_5[0][0]
dropout_3 (Dropout)	(None, 64, 64, 64)	0	batch_normalization_5[0]
conv2d_6 (Conv2D)	(None, 64, 64, 64)	36928	dropout_3[0][0]
batch_normalization_6 (BatchNor	(None, 64, 64, 64)	256	conv2d_6[0][0]
max_pooling2d_3 (MaxPooling2D)	(None, 32, 32, 64)	0	batch_normalization_6[0]
conv2d_7 (Conv2D)	(None, 32, 32, 128)	73856	max_pooling2d_3[0][0]
batch_normalization_7 (BatchNor	(None, 32, 32, 128)	512	conv2d_7[0][0]
dropout_4 (Dropout)	(None, 32, 32, 128)	0	batch_normalization_7[0]
conv2d_8 (Conv2D)	(None, 32, 32, 128)	147584	dropout_4[0][0]
batch_normalization_8 (BatchNor	(None, 32, 32, 128)	512	conv2d_8[0][0]
max_pooling2d_4 (MaxPooling2D)	(None, 16, 16, 128)	0	batch_normalization_8[0]
conv2d_9 (Conv2D)	(None, 16, 16, 256)	295168	max_pooling2d_4[0][0]
batch_normalization_9 (BatchNor	(None, 16, 16, 256)	1024	conv2d_9[0][0]

Fig. (4). Summary of the Keras model implemented in the system.

dropout_5 (Dropout)	(None, 16, 16, 256)	0	batch_normalization_9[0][0]
conv2d_10 (Conv2D)	(None, 16, 16, 256)	590080	dropout_5[0][0]
batch_normalization_10 (BatchNo	(None, 16, 16, 256)	1024	conv2d_10[0][0]
conv2d_transpose_1 (Conv2DTrans	(None, 32, 32, 128)	131200	batch_normalization_10[0][0]
concatenate_1 (Concatenate)	(None, 32, 32, 256)	0	conv2d_transpose_1[0][0] batch_normalization_8[0][0]
conv2d_11 (Conv2D)	(None, 32, 32, 128)	295040	concatenate_1[0][0]
batch_normalization_11 (BatchNo	(None, 32, 32, 128)	512	conv2d_11[0][0]
dropout_6 (Dropout)	(None, 32, 32, 128)	0	batch_normalization_11[0][0]
conv2d_12 (Conv2D)	(None, 32, 32, 128)	147584	dropout_6[0][0]
batch_normalization_12 (BatchNo	(None, 32, 32, 128)	512	conv2d_12[0][0]
conv2d_transpose_2 (Conv2DTrans	(None, 64, 64, 64)	32832	batch_normalization_12[0][0]
concatenate_2 (Concatenate)	(None, 64, 64, 128)	0	conv2d_transpose_2[0][0] batch_normalization_6[0][0]
conv2d_13 (Conv2D)	(None, 64, 64, 64)	73792	concatenate_2[0][0]
batch_normalization_13 (BatchNo	(None, 64, 64, 64)	256	conv2d_13[0][0]
dropout_7 (Dropout)	(None, 64, 64, 64)	0	batch_normalization_13[0][0]
conv2d_14 (Conv2D)	(None, 64, 64, 64)	36928	dropout_7[0][0]
batch_normalization_14 (BatchNo	(None, 64, 64, 64)	256	conv2d_14[0][0]
conv2d_transpose_3 (Conv2DTrans	(None, 128, 128, 32)	8224	batch_normalization_14[0][0]
concatenate_3 (Concatenate)	(None, 128, 128, 64)	0	conv2d_transpose_3[0][0] batch_normalization_4[0][0]
conv2d_15 (Conv2D)	(None, 128, 128, 32)	18464	concatenate_3[0][0]
batch_normalization_15 (BatchNo	(None, 128, 128, 32)	128	conv2d_15[0][0]
dropout_8 (Dropout)	(None, 128, 128, 32)	0	batch_normalization_15[0][0]
conv2d_16 (Conv2D)	(None, 128, 128, 32)	9248	dropout_8[0][0]
batch_normalization_16 (BatchNo	(None, 128, 128, 32)	128	conv2d_16[0][0]
conv2d_transpose_4 (Conv2DTrans	(None, 256, 256, 16)	2064	batch_normalization_16[0][0]
concatenate_4 (Concatenate)	(None, 256, 256, 32)	0	conv2d_transpose_4[0][0] batch_normalization_2[0][0]

Fig. (5). Summary of the Keras model implemented in the system.

In between down sampling and up sampling dropout, maxpooling2d, convolution layers are being used whose functions are as followed:

- Dropout: The dropout layer is simply used to avoid overfitting. It subsamples the output layer randomly thus avoiding reducing capacity or thinning of the network.
- Maxpooling2d: It proved the feature map after scanning input by a fixed size filter containing the most prominent features. Its filter selects maximum elements from the region of the feature map.
- Convolution: The convolution layer is the soul of any neural network. Its simple application of filter over input results in the activation of features. Moreover,

repeated activation results in a feature map which in turn is used by the maxpoolig2d layer. Pseudocodes for Accuracy metric and loss function has been shown in Figs. (6 and 7), respectively:

```
#accuracy Metric
from keras import backend as K
def iou_coef(y_true, y_pred, smooth=1):
    intersection = K.sum(K.abs(y_true * y_pred), axis=[1,2,3])
    union = K.sum(y_true,[1,2,3])+K.sum(y_pred,[1,2,3])-intersection
    iou = K.mean((intersection + smooth) / (union + smooth), axis=0)

    return iou
```

Fig. (6). Accuracy Metric determined using accuracy and loss metrics.

```
#loss function
def dice_coef(y_true, y_pred, smooth = 1):
    y_true_f = K.flatten(y_true)
    y_pred_f = K.flatten(y_pred)
    intersection = K.sum(y_true_f * y_pred_f)
    return (2. * intersection + smooth) / (K.sum(y_true_f) + K.sum(y_pred_f) + smooth)

def soft_dice_loss(y_true, y_pred):
    return 1-dice_coef(y_true, y_pred)
```

Fig. (7). Loss Function.

After the sample is downsampled and features are extracted, the model starts upsampling. Also, an important point to note is that selectively downsampling connections made to the mirror side of U-Net known as skip connection, which helps in encoder and decoder type of architecture to retrieve fine details in prediction might have been lost during processing through various layers.

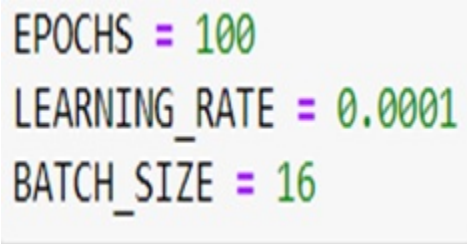
Splitting and Training

After pre-processing the dataset and defining our model we need to split our data into the train and test samples. Training data consists of 80% images and the rest 20% of images correspond to testing data from the sample. This splitting has been shown in Fig. (8).

```
TRAIN SET
(22070, 256, 256, 3)
(22070, 256, 256, 1)
TEST SET
(5518, 256, 256, 3)
(5518, 256, 256, 1)
```

Fig. (8). Train and Test set.

The training of our model stopped after the 48th epoch as the loss value was not improving leading to early stopping, which was fine and appropriate according to the conditions. Hyper-parameter optimization has been done and parameters have been listed in Fig. (9) below.



```
EPOCHS = 100
LEARNING_RATE = 0.0001
BATCH_SIZE = 16
```

Fig. (9). Hyper Parameters.

RESULTS

The training and early stopping of our model yielded a loss of 24.462% and an accuracy of 60.62%.

Following is the prediction obtained on a separate set of images that are not the part of train and test split. From predicted images, it can be seen that results are fairly good. It is visible in Figs. (10 and 11), that accuracy of prediction is greatly dependent on the input resolution of images.

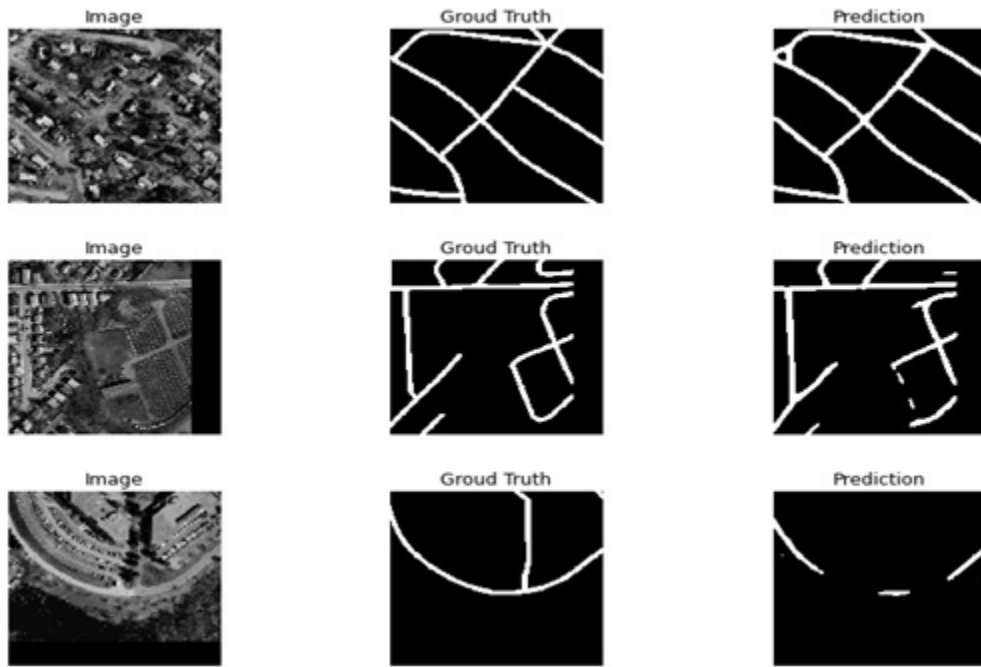


Fig. (10). Predictions.

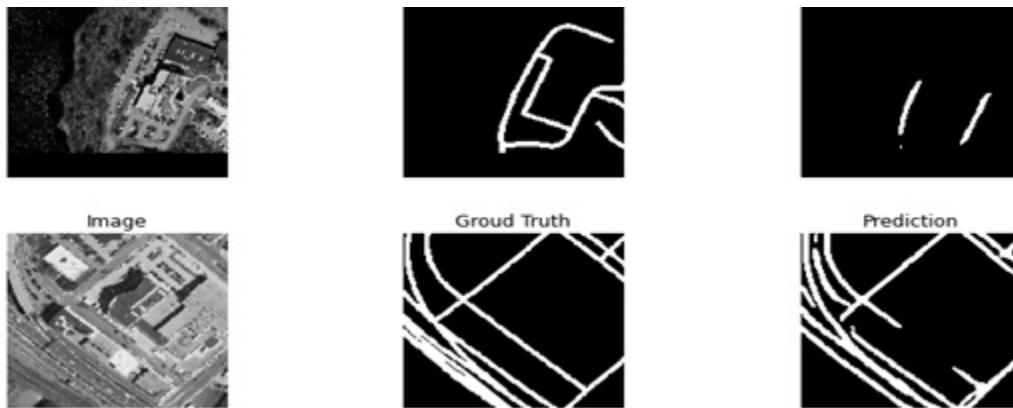


Fig. (11). Predictions.

Moreover, accuracy can further be improved when the above network is paired with other pre-trained models like the VGG16 encoder, SegNet etcetera [14].

LIMITATIONS & FUTURE WORK

Very large computational power is required for training the model since the images captured are not of high resolution. Also, image segmentation depends on

the type of images sent as input. The accuracy of prediction using the model is directly proportional to the resolution of the image. This implies resolution can be further increased.

Secondly, we can focus on detecting roads step by step, as some roads are wide and some roads are narrow. This classification has the potential to turn image segmentation for road detection upside-down as in the case of the wide road we will have freedom or flexibility to detect its boundary first, and detecting boundary is a fairly easy task as compared to the whole road.

CONCLUSION

In this paper, we trained our model after masking images we received from the dataset. Dataset consists of 2-d images captured through satellite imaging and we developed our model using CNN architecture in association with U-NET. In addition, Keras libraries help to approach the problem of semantic segmentation of images or motion for that matter with efficiency. Keras working on top of TensorFlow created a robust environment, maybe not a new-fangled model but with reasonable accuracy.

The lapses in scalability and accuracy still exist but they open new doors to future development in resolving the problem by greater understanding.

CONSENT FOR PUBLICATION

Not applicable.

CONFLICT OF INTEREST

The author declares no conflict of interest, financial or otherwise.

ACKNOWLEDGEMENT

Declared none.

REFERENCES

- [1] Z. Li, X. Chen, W. Zhou, Y. Zhang, and J. Yu, "Pose2Body: Pose-Guided Human Parts Segmentation", *2019 IEEE International Conference on Multimedia and Expo (ICME)*, pp. 640-645, 2019. [<http://dx.doi.org/10.1109/ICME.2019.00116>]
- [2] L. Shen, and R.M. Rangayyan, "A segmentation-based lossless image coding method for high-resolution medical image compression", *IEEE Trans. Med. Imaging*, vol. 16, no. 3, pp. 301-307, 1997. [<http://dx.doi.org/10.1109/42.585764>] [PMID: 9184892]
- [3] E. Drelie Gelasca, J. Byun, B. Obara, and B.S. Manjunath, "Evaluation and benchmark for image biological-image segmentation", *15th IEEE International Conference on Image Processing*, pp. 1816-

- 1819, 2008.
[<http://dx.doi.org/10.1109/ICIP.2008.4712130>]
- [4] Y. Hua, S. Lobry, L. Mou, D. Tuia, and X.X. Zhu, "Learning Multi-Label Aerial Image Classification Under Label Noise: A Regularization Approach Using Word Embeddings", *IGARSS 2020 - 2020 IEEE International Geoscience and Remote Sensing Symposium*, pp. 525-528, 2020.
[<http://dx.doi.org/10.1109/IGARSS39084.2020.9324069>]
- [5] Z. Yan, X. Han, C. Wang, Y. Qiu, Z. Xiong, and S. Cui, "Learning Mutually Local-Global U-Nets For High-Resolution Retinal Lesion Segmentation In Fundus Images", *IEEE 16th International Symposium on Biomedical Imaging (ISBI 2019)*, pp. 597-600, 2019.
[<http://dx.doi.org/10.1109/ISBI.2019.8759579>]
- [6] O Benarchid, and N Raissouni, "Support vector machines for based object-based building extraction in the suburban area using very resolution high-resolution satellite images, a case study: Tetuan, Morocco", *IAES International Journal of Artificial Intelligence*, vol. 1;2, no. 1, 2013.
- [7] E. Fernandez-Moral, R. Martins, D. Wolf, and P. Rives, "A New Metric for Evaluating Semantic Segmentation: Leveraging Global and Contour Accuracy", *2018 IEEE Intelligent Vehicles Symposium (IV)*, 2018pp. 1051-1056
[<http://dx.doi.org/10.1109/IVS.2018.8500497>]
- [8] S. Ji, S. Wei, and M. Lu, "Fully Convolutional Networks for Multisource Building Extraction From an Open Aerial and Satellite Imagery Data Set", *IEEE Trans. Geosci. Remote Sens.*, vol. 57, no. 1, pp. 574-586, 2019.
[<http://dx.doi.org/10.1109/TGRS.2018.2858817>]
- [9] Y. Chen, L. Cheng, M. Li, J. Wang, L. Tong, and K. Yang, "Multiscale Grid Method for Detection and Reconstruction of Building Roofs from Airborne LiDAR Data", *IEEE J. Sel. Top. Appl. Earth Obs. Remote Sens.*, vol. 7, no. 10, pp. 4081-4094, 2014.
[<http://dx.doi.org/10.1109/JSTARS.2014.2306003>]
- [10] Y. Song, and H. Yan, "Image Segmentation Techniques Overview", *2017 Asia Modelling Symposium (AMS)*, 2017pp. 103-107
[<http://dx.doi.org/10.1109/AMS.2017.24>]
- [11] J. Long, E. Shelhamer, and T. Darrell, "Fully convolutional networks for semantic segmentation", *2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2015pp. 3431-3440
[<http://dx.doi.org/10.1109/CVPR.2015.7298965>]
- [12] H. Monajemi, D.L. Donoho, and V. Stodden, "Making massive computational experiments painless", *2016 IEEE International Conference on Big Data (Big Data)*, 2016pp. 2368-2373
[<http://dx.doi.org/10.1109/BigData.2016.7840870>]
- [13] W. Weng, and X. Zhu, "INet: Convolutional Networks for Biomedical Image Segmentation", *IEEE Access*, vol. 9, pp. 16591-16603, 2021.
[<http://dx.doi.org/10.1109/ACCESS.2021.3053408>]
- [14] B. Bischke, P. Helber, J. Folz, D. Borth, and A. Dengel, "Multi-Task Learning for Segmentation of Building Footprints with Deep Neural Networks", *2019 IEEE International Conference on Image Processing (ICIP)*, 2019pp. 1480-1484
[<http://dx.doi.org/10.1109/ICIP.2019.8803050>]

SUBJECT INDEX

A

Access control mechanisms 66
 Adhoc participation rules 47
 Agglomeration 4
 Aid 51, 67, 70, 74, 76, 159
 automation 70
 development planning 51
 Air pollution 103
 Algorithmic techniques 102
 Algorithms 8, 33, 35, 36, 37, 38, 39, 63, 97,
 99, 101, 102, 103, 108, 109, 159
 key encryption 33
 learning 159
 mathematical 8
 naïve moving average 108
 time series 97, 99
 Amalgamation 89
 Ambient assisted living (AAL) 97
 Ameliorates 1
 Applications 13, 15, 47, 48, 49, 68, 70, 75, 78,
 83, 113, 116, 117, 118, 121, 123
 mobile-based 49
 Apps 32, 66, 67, 120, 149, 150
 blockchain-based 149
 health tracking 66
 Architecture 1, 34, 48
 basic blockchain 34
 client-server 48
 secure blockchain 1
 Attribute based encryption (ABE) 2, 33, 34
 blockchain-based distributed 34
 Auditability 9, 74
 Authenticity 1, 7, 8, 9, 67, 151
 Automate data management procedures 151
 Automation systems 149
 Automobile 114, 116, 118, 119, 141, 142, 143
 agencies 143
 engineering 118
 industry 119, 142
 manufacturing 114, 116, 141

B

Based distributed attribute-based encryption
 (BDABE) 34
 BFT protocol 38
 Billing 74, 78
 traditional 74
 Binary classification tasks 160
 Bitcoin blockchains 13, 16, 35, 62, 81
 BitTorrent 16
 client platform 16
 platform 16
 Blockchain 6, 7, 8, 9, 12, 14, 15, 16, 28, 29,
 33, 38, 49, 77, 78, 89, 90, 136, 148
 architecture 6, 148
 consensus mechanisms 77
 consortium 89, 148
 database 148
 ecosystem 16
 encrypts data 12
 in clinical trial management 90
 ledger replicas 148
 network 7, 8, 9, 14, 15, 28, 38, 49, 78
 operation 8
 privacy protection 33
 techniques 136
 transactions 29
 Blockchain-based 16, 65, 72, 81, 155
 EMR management system 81
 land registry system 65
 payment system 16
 systems 72, 155
 Blocks, genesis 7, 62
 Blood 67, 110, 159
 pressure 67, 110
 vessels 159
 Boosting efficiency 96
 Breakdown 3, 4, 9
 probability, reducing 9
 Businesses 3, 32, 77, 147
 lucrative 77
 world's pharmacy 147

Subject Index

Byzantine 28, 38, 63, 73
 agreement (BA) 28
 fault tolerance (BFT) 28, 38, 63, 73

C

Cancer 83, 142
Carmichael's totient function 36
Celsius temperature 104
Cloud 2, 31, 55, 96, 98
 elastic 31
Cloud-based 48
 architectures 48
 health care system 48
Cloud storage(s) 1, 12
 storing data 12
 systems 1
CNN architecture 168
Communication 14, 15, 19, 20, 21, 25, 33, 39,
 70, 116, 119, 120, 121
 cross-shard 14
 encryption 21
 machine-to-machine 70
 smooth 15
 synchronous 14
Computation(s) 15, 19, 29, 36, 38, 82, 113,
 116
 excess 82
 heavy 29
 power 15, 19
 process 36
Computational 13, 37, 38, 39, 62
 power 13, 37, 38, 39
 work 62
Computer vision 158
Computing power 78
Configuration authorization techniques 49
Connectivity 20, 116
 massive device 116
Consensus algorithms 36, 39, 46, 62, 63, 69,
 73, 77, 79, 82, 89
 dynamic 39
 robust 62
Consistency 21, 57, 87

Recent Advances in IoT and Blockchain Technology 171

 wallet 57
Contract 73, 78, 83, 149
 blockchain-based 83
Convolutional neural network 158
Criminal smart contracts (CSC) 78
Cryptocurrencies 46, 61, 74, 80, 89, 150
Cryptographic 5, 66
 principles 66
 techniques 5
Cryptography 33, 150
 asymmetric 33
Crypto 15, 31
 economics 31
 tokens 15
Cyber 1, 113, 116
 physical system (CPS) 113, 116
 security 1
Cycle 116, 141
 complete individual medication 155

D

Database 3, 4, 6, 9, 10, 11, 12, 13, 40, 66, 67,
 82, 99, 101, 102, 103, 106, 113
 management systems 67
 system, robust 66
 technology 113
Data 5, 12, 19, 20, 68, 69, 80
 integrity, medical 80
 redundancy processes 19
 security 5, 69
 storage frameworks implementing
 blockchain 12
 swap Layer 20
 alidation 68
Dataset 13, 106, 159, 160, 165, 168
Decentralised storage networks 30
Decentralized 1, 4, 5, 8, 9, 22, 24, 26, 29, 30,
 33, 39, 47, 51, 52, 57, 117, 151
Database System 4
 nature 9
 networks 5, 22, 24, 26, 30, 33, 39, 52
 storage systems 47
 supply chain management systems 151

systems 1, 4, 5, 8, 24, 29, 39, 51, 57, 117
 Decryption equation 36
 Deep Learning 158
 Defense mechanisms 19
 Design 47, 85, 90, 118, 119, 127
 system architecture 127
 Devices 10, 20, 44, 52, 61, 69, 85, 96, 104, 109, 116
 sensing 104
 temperature sensor 109
 wearable health monitoring 61
 Digital healthcare 47
 Diseases, heart 83
 Distributed 11
 version control system (DVCS) 11
 Drugs 48, 61, 67, 78, 146, 147, 149, 151, 152, 153, 151, 152, 154
 duplicate 151
 fraudulent 147
 normal 151
 surveillance system 152
 transportation 149
 validated 146
 Drug supply chain 150, 151, 152
 system 151
 Dynamic network 29

E

Economy 113, 116, 120
 national 113
 Ecosystem 45, 48, 72, 83, 115
 blockchain-based comprehensive healthcare 83
 health insurance 72
 vehicle registration 115
 Efficient management of patient record 48
 EHR systems, traditional 69
 Election 64
 advisory board 64
 Election's result, month-long 64
 Electronic 48, 50, 57, 61, 65, 66, 67, 68, 69, 85

health records (EHR) 48, 50, 57, 61, 65, 66, 67, 68, 69, 85
 medical records (EMRs) 61, 65, 85
 Elliptical curve digital signature algorithm (ECDSA) 35
 Encrypted 55, 151
 communication channel 55
 sensitive data 151
 Encrypting 36, 66
 data 66
 equation 36
 Energy 46, 104
 heat 104
 Estonia's Health Information System Act 83
 Ethereum 13, 16, 30, 31, 49, 62, 80, 146, 150, 151, 152, 153

 and bitcoin blockchains 16
 blockchain 13, 30, 31, 49, 62, 80, 150, 151, 152
 transactions 146, 153
 Exchange 49, 72, 81, 117, 120, 122, 147, 155
 financial 117, 120
 smooth 81

F

Faults 1, 21, 28, 32
 Filecoin 26, 27, 29, 39
 blockchain 27
 network 26, 27, 29, 39
 Files 11, 16, 17, 18, 20, 23, 24, 26, 29, 74, 121
 configuration 121
 sharing systems 24
 storage 26, 29
 Finance 1, 117
 industries 117
 sector 1
 Financial systems 81
 FinTech 13
 companies 13
 industry 13
 Flaws 5, 46, 77
 inherent security 77

Subject Index

Forecast accuracy 108
 measuring 108
Forecasting 96, 99, 100, 101, 107
 method 100
Framework 70, 71, 77, 78, 84
 blockchain-based 70
 electronic 77
 healthcare facility blockchain 78
 robust 71
 telehealth 84
Fraud(s) 50, 51, 73, 74, 115, 147, 150
 health insurance 73
 medicine markets 147
Fraudulent medicines 155
Functionalities, video conferencing 110
Functions 23, 29, 50, 53, 62, 63, 85, 88, 104,
 150, 161, 162, 164
 down-sampling activation 162
 encryption 88
 non-reversible 62

G

GemOS network for automation 81
General domain model architecture (GDMA)
 98

H

Hash functions 17, 22, 45, 62
 cryptographic 45, 62
Hashing 7, 11, 20, 22, 77, 113
 algorithms 22, 113
 cryptographic 11, 77
 function 22
Healthcare 49, 80, 83, 84, 117
 architecture 49
 framework 80, 84
 gateway 83
 infrastructure 83
 issues 117
 manufacturing 117
Healthcare records 45, 48, 77
 electronic 48

Recent Advances in IoT and Blockchain Technology 173

Healthcare system 44, 48, 49, 151, 152
 cloud-based 48
 secured pervasive social network-based 49
Health 66, 98
 insurance privacy and accountability Act
 (HIPAA) 66
 monitoring 98
Hybrid 18, 30, 51
 networks 18, 51
 scalable system 44
 systems 30
Hyperledger blockchain 84
Hyper-parameter optimization 166

I

Identity management, blockchain-based 64
Images 44, 158, 159, 160, 161, 162, 165, 166,
 167, 168
 high-resolution 159
 large-sized radiology 66
 segmentation 158, 159, 167, 168
Immutable record 6
Indispensable 1, 61, 65
 system 61
 tool 1, 65
Industry 12, 13, 61, 67, 83, 90, 96, 119, 142,
 143, 149
 automotive 119, 142, 143
 real-world 12
Information 1, 3, 4, 6, 11, 12, 14, 16, 24, 40,
 50, 64, 69, 74, 75, 76, 113, 119, 140,
 143
 automobile 113
 crucial 74
 sensitive 1, 75, 76
 system 113
 transparency 40
Infrastructure 83, 113
 blockchain-based 83
Inherent technical problems 77
Insurance 45, 50, 51, 72, 73, 74, 75, 81, 83,
 84, 85, 114, 120, 141, 142
 agencies 73, 85, 113, 114, 120, 141

claims 72, 75, 84
 companies 45, 50, 72, 73, 74, 81, 83
 Integration of sensors 99
 Internet of medical things (IoMT) 70, 71, 89,
 90
 Interplanetary 1, 16, 21, 23, 26, 31
 file systems 1, 16, 21
 naming system (IPNS) 23, 26, 31
 IoT 44, 70, 116
 devices 44
 services use cloud storage 70
 technologies 116
 IoT-based 48, 51, 99
 applications 48
 healthcare system 51
 remote patient monitoring system 99
 IP address 22, 23
 IPFS project 25

L

Linux foundation 115
 Local version control system (LVCS) 11
 Lung capacity sensors 103

M

Machine learning 25
 Malicious activity 12
 Mandatory health insurance plans 72
 Manufacturer 113, 120, 122, 123, 124, 132,
 138, 151, 152, 154
 automotive vehicle 120
 Market 70, 72, 152
 global health insurance 72
 global IoMT 70
 Mass production 152
 Mean 108
 absolute deviation (MAD) 108
 squared error (MSE) 108
 Mechanism implementations 5
 MediBchain promises pseudonymity 88
 Medical 44, 49, 52, 62, 65, 67, 68, 71, 72, 74,
 75, 77, 80, 81, 83, 84, 85

bills 74, 75
 data 67, 71, 77, 80, 81, 84, 85
 equipment 61, 70
 Insurance 72
 interoperability gateway 83
 records 44, 49, 52, 62, 65, 68, 69, 74, 77,
 81, 84, 85
 researchers 68, 84
 Medicine supply chain 146, 152
 solution 146
 systems 152
 Medicine verification organization 152
 Methods 12, 35, 49, 64, 109, 118, 149
 cryptographic 35
 electronic signature 118
 legitimation 149
 naïve 109
 off-chain security 49
 traditional voting 64
 versatile 12
 Model-driven tree reference model (MDTRM)
 98
 Modern economy 113
 Multinational corporations (MNCs) 75

N

Nations 146, 159
 Native cryptocurrency 26
 Network 22, 78, 118, 149, 159, 160, 161, 164
 blockchain-based 149
 configuration 118
 congestion 78
 neural 159, 160, 161, 164
 well-connected 22
 Networking 25, 31
 system operability 25

O

Off-chain blockchain 15

Subject Index

P

Pair 55, 147, 162
 public-private key 55, 147
Paper-based 2, 72
 records 72
 systems 2
Payment processing platforms 46
Personal 67, 69, 83, 85
 care pathway (PCPs) 83
 health records (PHR) 67, 69, 85
Processing, cloud-based 98
Product 6, 75, 76, 123, 134, 151
 blockchain-based 123, 134
 hazardous 76
Production process 67
Psychological profiles 32
Public blockchains 9, 15, 47, 89, 141, 148
Public key 1, 20, 21, 28, 33, 34, 35, 36, 54,
 55, 56, 71
 cryptography 71
Puzzles, mathematical 37

Q

QR code 55, 150

R

Redundant byzantine fault tolerance (RBFT)
 38
Registrar contract (RC) 81
Repository 10, 11, 80, 86
 blockchain-enabled global 80
RTO data 132

S

Safety deposit boxes 32
Scalable decentralised key systems,
 constructing 44
Secure decentralised records 84
Security 32, 33, 48, 71, 77

Recent Advances in IoT and Blockchain Technology 175

 algorithms 71
 cryptographic 48
 frameworks 33
 risks, growing cyber 32
 threats 77
Segmentation 159, 168
 semantic 168
Sensors 67, 70, 98, 99, 101, 104, 105, 110,
 115, 117, 150
 devices 150
 measuring 110
 wireless network 98
SERP rankings 25
Snapshots of Interfaces 136
Social media platforms 25
Software 10, 68, 69, 121, 122, 123, 124, 135,
 139, 150
 developers 150
 interfaces 122
 professionals 10
 version control 10
Spatial processing 158
Stakeholders, medical 77, 80, 81, 89
Storage network 19, 20
Structure 83, 123, 134
 dual blockchain 83
 modular blockchain 123, 134
Supply chain 75, 76, 77, 90, 147, 149, 151,
 155
 blockchain-based 76
 management 75, 76, 77, 90
 medication 147
 networks 155
 processes 149
 systems 151
Surgical infections 117

T

Technologies 68, 70, 151, 158
 emerging 158
 popular emerging 151
 traditional healthcare 68
 wireless 70

Telehealth market 84
Telemedicine 61
Three-time series forecasting techniques 107
Time series forecasting techniques 103
Token application 84
Tracking 65, 67, 70, 75, 76, 115, 146, 150,
151, 155, 158
 effective product 150
 ownership records 65
 real-time 75
Transaction(s) 6, 7, 8, 9, 12, 13, 14, 15, 27,
28, 36, 37, 62, 74, 78, 79, 121, 147, 148,
153
 completion 7
 data 7, 78, 121
 forged 36
 processes 13, 153
 reverse 78
 records 14, 62
Transaction validation 14
Transfer data 96
Transformation 69, 117
Transparency 4, 6, 57, 61, 74, 75, 76, 113,
117, 137, 138
Transport 25, 113
 motor 113
Transportation 116, 150
Treatment 68, 80, 84, 147
 telehealth 84

V

Validation process 37
Vehicle registration process 114, 120, 141,
142



Koyel Datta Gupta

Dr. Koyel Datta Gupta is a professional with an experience of 17+ years in academics. She completed her B. Tech in Computer Science and Engineering from the University of Kalyani, West Bengal in 2003 and is a gold medalist in M.Tech (Computer Technology) from Jadavpur University, Kolkata (2007). She received her doctorate in 2015 from Jamia Milia Islamia, New Delhi. Her areas of research include network security, digital signal processing, pattern recognition and machine learning. Dr. Koyel Datta Gupta is currently working as an associate professor at the Maharaja Surajmal Institute of Technology (MSIT) (under the IP University), New Delhi. She is currently the head of the department of the Department of Computer Science and Engineering. She has held various other positions in MSIT for the past 12+ years. She has published more than 25 research papers in reputed journals and conference proceedings and has also authored books.



Rinky Dwivedi

Dr. Rinky Dwivedi completed her B.Tech in Computer Science and Engineering from Guru Gobind Singh Indraprastha University, Delhi in 2004 and M.E. in Computer Technology and Application from Delhi College of Engineering, Delhi in 2008. She has received her doctorate in 2016 from the Delhi Technological University, New Delhi. Dr. Rinky has over 17 years of experience in Academics, currently working as an associate professor at the Maharaja Surajmal Institute of Technology, Delhi. She has published more than 20 research papers in reputed journals and conference proceedings and has also authored books.



Deepak Kumar Sharma

Deepak Kumar Sharma is working as an associate professor at the Department of Information Technology, Indira Gandhi Delhi Technical University for Women (IGDTUW), Kashmere Gate, Delhi, India. Earlier, he worked as an assistant professor at the Netaji Subhas University of Technology (Formerly N.S.I.T.), Dwarka, Delhi. He obtained his Ph.D. in Computer Engineering from the University of Delhi, India in 2016. His research interests include opportunistic networks, wireless ad hoc and sensor networks, software defined networks and IoT networks. He has over 17 years of experience in academics. He has published various research papers in reputed international journals like ETT Wiley, IEEE Systems Journal, IEEE IoT Journal, Computer Communication Elsevier, IJCS Wiley, etc. and conferences of repute like IEEE AINA, GLOBECOM, etc. He has also authored various book chapters in edited books of IET, Wiley, Springer, Elsevier, etc. He has served as session chair in many conferences and is also a reviewer of various reputed journals like ETT Wiley, AIHC Springer, IJCS Wiley, etc.



Fadi Al-Turjman

Prof. Dr. Fadi Al-Turjman received his Ph.D. in computer science from Queen's University, Canada, in 2011. He is the associate dean for research and the founding director of the International Research Center for AI and IoT at Near East University, Nicosia. Prof. Al-Turjman is the head of the Department of Artificial Intelligence Engineering and a leading authority in the areas of smart/intelligent IoT systems, wireless, and mobile networks' architectures, protocols, deployments, and performance evaluation in Artificial Intelligence of Things (AIoT). His publication history spans over 400 SCI/E publications, in addition to numerous keynotes and plenary talks at flagship venues. He has authored and edited more than 40 books about cognition, security, and wireless sensor networks' deployments in smart IoT environments, which have been published by well-reputed publishers such as Taylor and Francis, Elsevier, IET, and Springer.