

# 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: Mq{grIF cwc'I wr vc, F ggr cniMwo ct"Uj cto c."Tlpm{ 'F y kxgf k( 'Hcf k'Cr/Vwtlo cp

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](mailto: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](mailto:subscriptions@benthamscience.net)



# CONTENTS

PREFACE .....	i
ACKNOWLEDGEMENTS .....	i
LIST OF CONTRIBUTORS .....	iii
<b>CHAPTER 1 BLOCKCHAIN FRAMEWORK FOR DATA STORAGE AND SECURITY</b> .....	1
<i>Salman Azeez Syed, Vivaswat Sinha, Sachin Singh and Aarti Goel</i>	
<b>INTRODUCTION</b> .....	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
<b>BLOCKCHAIN TECHNOLOGY</b> .....	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
<b>VERSION CONTROL SYSTEM</b> .....	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
<b>DATA STORAGE</b> .....	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
<b>P2P NETWORK</b> .....	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
<b>INTERPLANETARY FILE SYSTEM (IPFS)</b> .....	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
<b>BLOCKCHAIN - PRIVACY</b> .....	31
Sybil Attack .....	32
51% Attack .....	32
How Blockchain Implements Data Privacy .....	33
<i>Blockchain Privacy Protection</i> .....	33
<b>BLOCKCHAIN - SECURITY</b> .....	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
<b>DISCUSSION</b> .....	39
<b>CONCLUSION</b> .....	40
<b>CONSENT FOR PUBLICATION</b> .....	40
<b>CONFLICT OF INTEREST</b> .....	41
<b>ACKNOWLEDGEMENT</b> .....	41
<b>REFERENCES</b> .....	41

## **CHAPTER 2 BLOCKCHAIN BASED HYBRID FRAMEWORK FOR IDENTITY**

<b>MANAGEMENT IN HEALTHCARE</b> .....	44
<i>Deepak Kumar Sharma, Arjun Khara, Koyel Datta Gupta and Rinky Dwivedi</i>	
<b>INTRODUCTION</b> .....	44
<b>BACKGROUND AND RELATED WORK</b> .....	48
<b>MOTIVATION</b> .....	49
<b>IDENTITY MANAGEMENT: HEALTHCARE SYSTEM</b> .....	49
<b>PROPOSED SOLUTION</b> .....	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
<b>CONCLUSION</b> .....	57
<b>CONSENT FOR PUBLICATION</b> .....	57
<b>CONFLICT OF INTEREST</b> .....	58
<b>ACKNOWLEDGEMENT</b> .....	58
<b>REFERENCES</b> .....	58

<b>CHAPTER 3 BLOCKCHAIN IN SMART HEALTHCARE FACILITY</b> .....	61
<i>Ayush Kumar Singh, Nipunika and Deepak Kumar Sharma</i>	
<b>INTRODUCTION</b> .....	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
<b>USE CASES</b> .....	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
<b>CHALLENGES</b> .....	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
<b>CASE STUDIES</b> .....	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
<b>FURTHER DISCUSSION</b> .....	89
<b>SUMMARY</b> .....	90
<b>CONSENT FOR PUBLICATION</b> .....	90
<b>CONFLICT OF INTEREST</b> .....	90
<b>ACKNOWLEDGEMENT</b> .....	90
<b>REFERENCES</b> .....	91
<b>CHAPTER 4 APPLICATION OF IOT IN PATIENT HEALTH MONITORING SYSTEM</b> .....	96
<i>Rinky Dwivedi, Harshit Mittal, Manik Agarwal and Sahil Dwivedi</i>	
<b>INTRODUCTION</b> .....	96
<b>RELATED WORK</b> .....	97
<b>SYSTEM ARCHITECTURE</b> .....	98
A. System Structure .....	98
<i>Algorithm 1.</i> .....	101
<i>Algorithm 2.</i> .....	102
<i>Algorithm 3.</i> .....	103
EQUIPMENT DETAILS .....	103
<b>PERFORMANCE AND MEASUREMENT</b> .....	104
<b>EMERGENCY ALERT</b> .....	109
<b>CONCLUSION AND FUTURE SCOPE</b> .....	110
<b>CONSENT FOR PUBLICATION</b> .....	110
<b>CONFLICT OF INTEREST</b> .....	111
<b>ACKNOWLEDGEMENT</b> .....	111
<b>REFERENCES</b> .....	111
<b>CHAPTER 5 IOT BASED VERIFIED AND PUBLIC VEHICLE REGISTRATION THROUGH BLOCKCHAIN: FUTURE SMART CITIES BASED APPLICATIONS WITH SUSTAINABLE APPROACH</b> .....	113
<i>Rohit Rastogi, Bhuvneshwar Sharma, Pardeep Kumar and Muskan Gupta</i>	
<b>INTRODUCTION</b> .....	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
<b>RELATED WORK</b> .....	117
Carchain .....	117
Fabcar IBM Blockchain .....	118
Blockchain and Future of Automobiles .....	118
Significance of 5-G Technology .....	119
<b>PRESENTED METHODOLOGY</b> .....	120
<b>SOFTWARE REQUIREMENT SPECIFICATION</b> .....	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
<b>IMPLEMENTATION DETAILS</b> .....	136
Snapshots of Interfaces .....	136
Test Cases .....	139
<b>RESULTS AND DISCUSSION</b> .....	140
<b>NOVELTY AND RECOMMENDATIONS</b> .....	141
<b>FUTURE RESEARCH DIRECTION</b> .....	142
<b>LIMITATIONS</b> .....	143
<b>CONCLUSION</b> .....	143
<b>CONSENT FOR PUBLICATION</b> .....	143
<b>CONFLICT OF INTEREST</b> .....	144
<b>ACKNOWLEDGEMENT</b> .....	144
<b>REFERENCES</b> .....	144
<b>CHAPTER 6 IDENTIFICATION OF COUNTERFEIT DRUGS USING DECENTRALIZED</b>	
<b>SUPPLY CHAIN</b> .....	146
<i>Koyel Datta Gupta, Aditya Gupta, Tanmay Sharma and Aayush Bhatnagar</i>	
<b>INTRODUCTION</b> .....	146
Blockchain .....	147
Smart Contract .....	148

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

<b>Aarti Goel</b>	Department of Information Technology, Netaji Subhas University of Technology, New Delhi, India
<b>Aayush Bhatnagar</b>	Department of Computer Science & Engineering, Maharaja Surajmal Institute of Technology, New Delhi 110058, India
<b>Aditya Gupta</b>	Department of Computer Science & Engineering, Maharaja Surajmal Institute of Technology, New Delhi 110058, India
<b>Arjun Khera</b>	Department of Information Technology, Netaji Subhas University of Technology, New Delhi 110078, India
<b>Ayush Kumar Singh</b>	Department of Information Technology, Netaji Subhas University of Technology (Formerly known as Netaji Subhas Institute of Technology), New Delhi, India
<b>Bhuvneshwar Sharma</b>	Department of CSE, ABES Engineering College, Ghaziabad, U.P. 201009, India
<b>Deepak Kumar Sharma</b>	Department of Information Technology, Indira Gandhi Delhi Technical University for Women, Delhi, India
<b>Harshit Mittal</b>	Department of Computer Science and Engineering, Maharaja Surajmal Institute of Technology, C-4 Janakpuri, New Delhi 100058, India
<b>Koyel Datta Gupta</b>	Department of Computer Science & Engineering, Maharaja Surajmal Institute of Technology, New Delhi 110058, India
<b>Manik Agarwal</b>	Department of Computer Science and Engineering, Maharaja Surajmal Institute of Technology, C-4 Janakpuri, New Delhi 100058, India
<b>Muskan Gupta</b>	Department of CSE, ABES Engineering College, Ghaziabad, U.P. 201009, India
<b>Nipunika</b>	Department of Information Technology, Netaji Subhas University of Technology (Formerly known as Netaji Subhas Institute of Technology), New Delhi, India
<b>Pardeep Kumar</b>	Department of Computer Systems and Engineering, QUEST University, Nawabshah, Pakistan
<b>Rinky Dwivedi</b>	Department of Computer Science and Engineering, Maharaja Surajmal Institute of Technology, C-4 Janakpuri, New Delhi 100058, India
<b>Rohit Rastogi</b>	Department of CSE, ABES Engineering College, Ghaziabad, U.P. 201009, India
<b>Sachin Singh</b>	Department of Information Technology, Netaji Subhas University of Technology, New Delhi, India
<b>Sahil Dwivedi</b>	Department of Computer Science and Engineering, Maharaja Surajmal Institute of Technology, C-4 Janakpuri, New Delhi 100058, India
<b>Salman Azeez Syed</b>	Department of Information Technology, Netaji Subhas University of Technology, New Delhi, India
<b>Tanmay Sharma</b>	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<sup>1,\*</sup>, Vivaswat Sinha<sup>1</sup>, Sachin Singh<sup>1</sup> and Aarti Goel<sup>1</sup>**<sup>1</sup> *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.

## Blockchain Based Hybrid Framework for Identity Management in Healthcare

Deepak Kumar Sharma<sup>1\*</sup>, Arjun Khera<sup>2</sup>, Koyel Datta Gupta<sup>3</sup> and Rinky Dwivedi<sup>3</sup>

<sup>1</sup> Department of Information Technology, Indira Gandhi Delhi Technical University for Women, Delhi, India

<sup>2</sup> Department of Information Technology, Netaji Subhas University of Technology, New Delhi 110078, India

<sup>3</sup> 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.

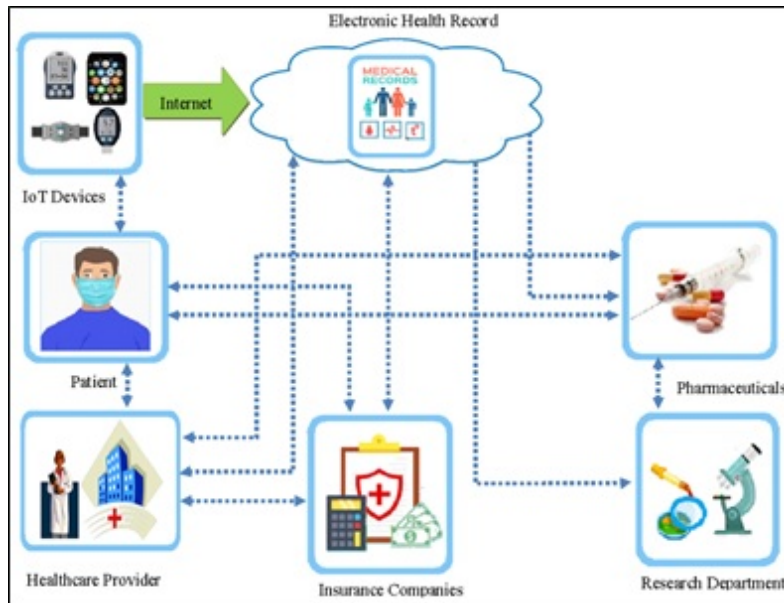


Fig. (1). IoT enabled Healthcare System.

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.

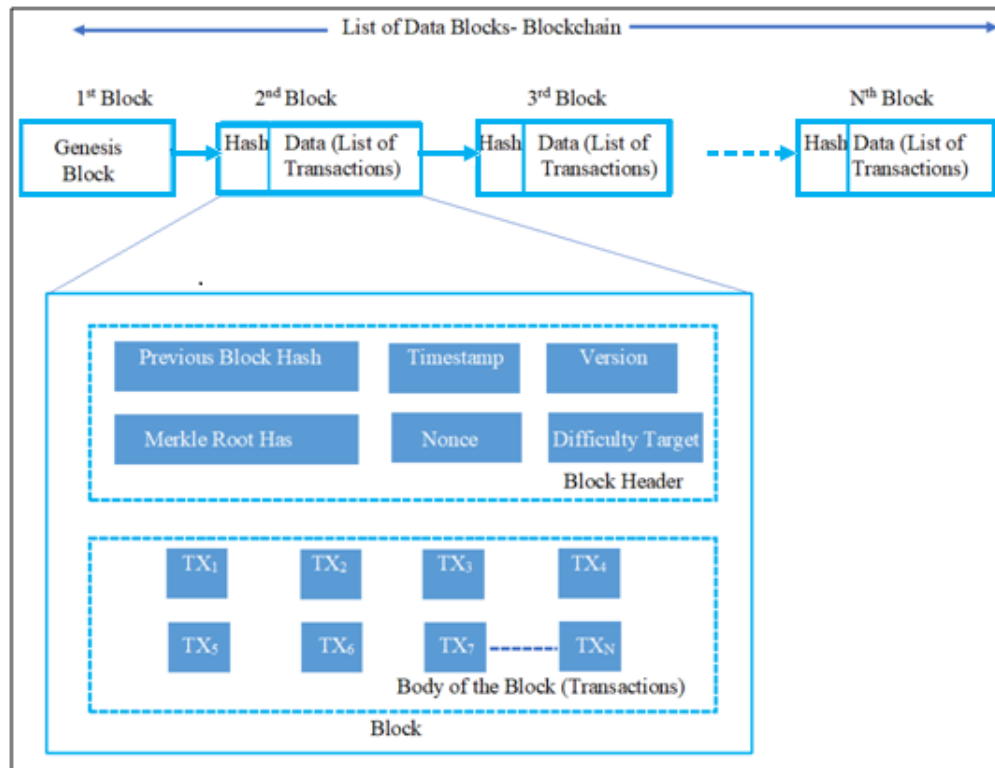


Fig. (2). List of Data Blocks.

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

## Blockchain in Smart Healthcare Facility

Ayush Kumar Singh<sup>1</sup>, Nipunika<sup>1</sup> and Deepak Kumar Sharma<sup>2,\*</sup>

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

<sup>2</sup> 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).

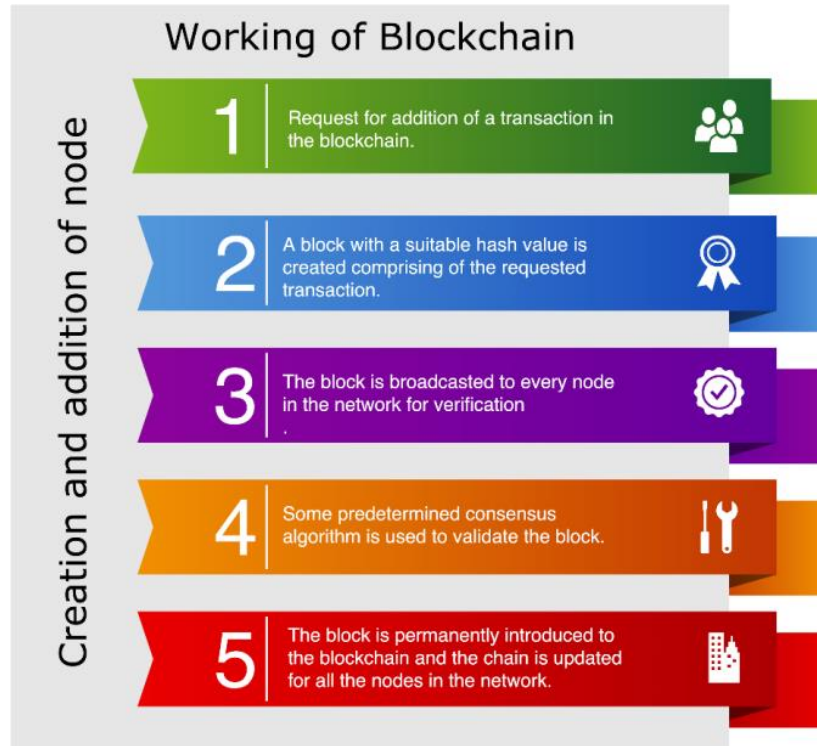


Fig. (1). Sequential working of Blockchain.

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



## Application of IoT in Patient Health Monitoring System

Rinky Dwivedi<sup>1,\*</sup>, Harshit Mittal<sup>1</sup>, Manik Agarwal<sup>1</sup> and Sahil Dwivedi<sup>1</sup>

<sup>1</sup> 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.

---

**CHAPTER 5**

---

**IoT Based Verified and Public Vehicle Registration through BlockChain: Future Smart Cities based Applications with Sustainable Approach****Rohit Rastogi<sup>1,\*</sup>, Bhuvneshwar Sharma<sup>1</sup>, Pardeep Kumar<sup>2</sup> and Muskan Gupta<sup>1</sup>**<sup>1</sup> Department of CSE, ABES Engineering College, Ghaziabad, U.P. 201009, India<sup>2</sup> 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

## **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.

## Identification of Counterfeit Drugs Using Decentralized Supply Chain

Koyel Datta Gupta<sup>1,\*</sup>, Aditya Gupta<sup>1</sup>, Tanmay Sharma<sup>1</sup> and Aayush Bhatnagar<sup>1</sup>

<sup>1</sup> 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.

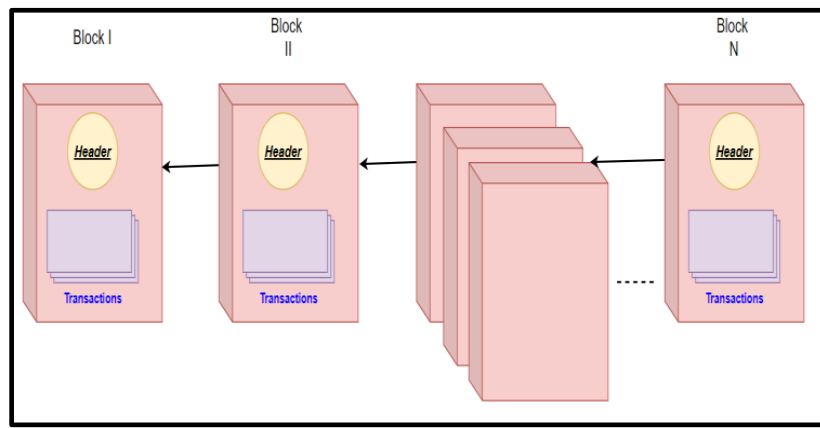
Another obstacle faced by the customer is the monitoring of medications that can only be obtained through a prescription. While the selling of medicines without a prescription is against the law, keeping track of wholesaler honesty, in addition to the challenge of counterfeit drugs, is difficult and 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

## Making Great Strides Towards Road Detection

Vimal Gaur<sup>1,\*</sup>

<sup>1</sup> *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).

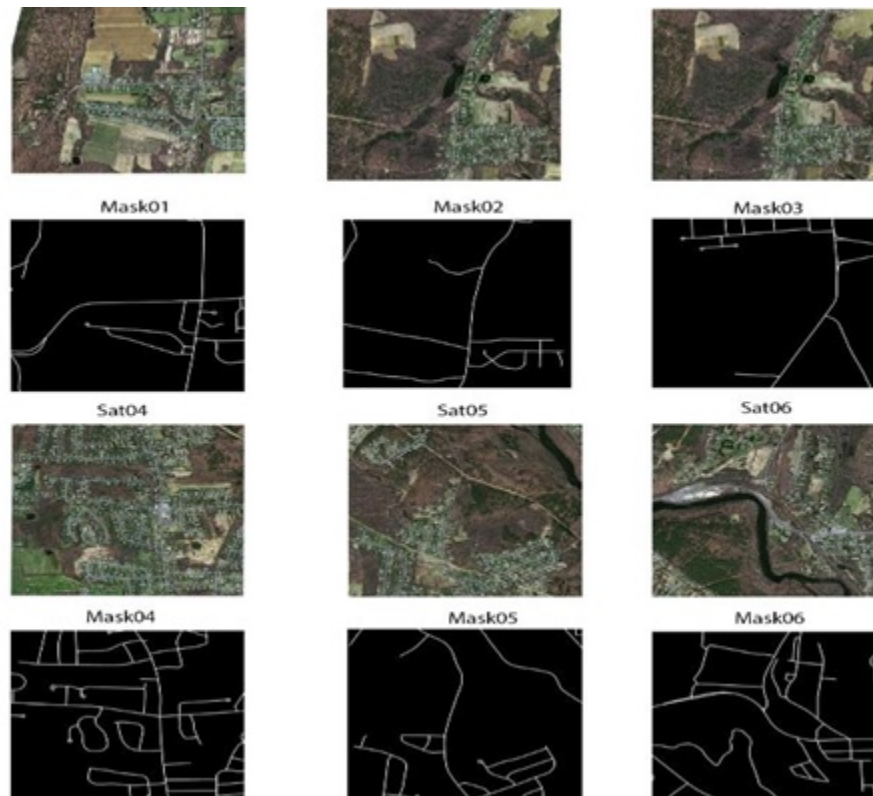


Fig. (1). Images before Pre-Processing.

### 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

## 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  
  validation 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.