

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/351346456>

Blockchain Technology: Applications and Challenges

Book in Intelligent Systems Reference Library · May 2021

DOI: 10.1007/978-3-030-69395-4

CITATIONS

62

READS

18,809

4 authors, including:



Sandeep Kumar Panda

The ICFAI University, Hyderabad

75 PUBLICATIONS 1,367 CITATIONS

[SEE PROFILE](#)



Ajay Kumar Jena

KIIT University

57 PUBLICATIONS 689 CITATIONS

[SEE PROFILE](#)



Suresh Satapathy

Institute of Electrical and Electronics Engineers

334 PUBLICATIONS 8,352 CITATIONS

[SEE PROFILE](#)

Sandeep Kumar Panda
Ajay Kumar Jena
Santosh Kumar Swain
Suresh Chandra Satapathy *Editors*

Blockchain Technology: Applications and Challenges

Intelligent Systems Reference Library

Volume 203

Series Editors

Janusz Kacprzyk, Polish Academy of Sciences, Warsaw, Poland

Lakhmi C. Jain, KES International, Shoreham-by-Sea, UK

The aim of this series is to publish a Reference Library, including novel advances and developments in all aspects of Intelligent Systems in an easily accessible and well structured form. The series includes reference works, handbooks, compendia, textbooks, well-structured monographs, dictionaries, and encyclopedias. It contains well integrated knowledge and current information in the field of Intelligent Systems. The series covers the theory, applications, and design methods of Intelligent Systems. Virtually all disciplines such as engineering, computer science, avionics, business, e-commerce, environment, healthcare, physics and life science are included. The list of topics spans all the areas of modern intelligent systems such as: Ambient intelligence, Computational intelligence, Social intelligence, Computational neuroscience, Artificial life, Virtual society, Cognitive systems, DNA and immunity-based systems, e-Learning and teaching, Human-centred computing and Machine ethics, Intelligent control, Intelligent data analysis, Knowledge-based paradigms, Knowledge management, Intelligent agents, Intelligent decision making, Intelligent network security, Interactive entertainment, Learning paradigms, Recommender systems, Robotics and Mechatronics including human-machine teaming, Self-organizing and adaptive systems, Soft computing including Neural systems, Fuzzy systems, Evolutionary computing and the Fusion of these paradigms, Perception and Vision, Web intelligence and Multimedia.

Indexed by SCOPUS, DBLP, zbMATH, SCImago.

All books published in the series are submitted for consideration in Web of Science.

More information about this series at <http://www.springer.com/series/8578>

Sandeep Kumar Panda · Ajay Kumar Jena ·
Santosh Kumar Swain · Suresh Chandra Satapathy
Editors

Blockchain Technology: Applications and Challenges



Editors

Sandeep Kumar Panda
Department of Data Science and Artificial Intelligence
IcfaiTech (Faculty of Science and Technology)
ICFAI Foundation for Higher Education
Hyderabad, Telangana, India

Santosh Kumar Swain
School of Computer Engineering
KIIT University
Bhubaneswar, Odisha, India

Ajay Kumar Jena
School of Computer Engineering
KIIT University
Bhubaneswar, Odisha, India

Suresh Chandra Satapathy
School of Computer Engineering
KIIT University
Bhubaneswar, Odisha, India

ISSN 1868-4394

ISSN 1868-4408 (electronic)

Intelligent Systems Reference Library

ISBN 978-3-030-69394-7

ISBN 978-3-030-69395-4 (eBook)

<https://doi.org/10.1007/978-3-030-69395-4>

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Switzerland AG 2021

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

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

Contents

1	Blockchain Technology: Introduction, Applications, Challenges	1
	Ajay Kumar Jena and Sujata Priyambada Dash	
1.1	Introduction	1
1.1.1	Components of Blockchain	3
1.1.2	Hashing Methods	3
1.1.3	Transactions	4
1.1.4	Public Key Cryptography	5
1.1.5	Address and Wallet	5
1.1.6	Blocks	5
1.1.7	Consensus Mechanism	6
1.1.8	Smart Contracts	6
1.2	Evolution of Blockchain	7
1.3	Applications of Blockchain	8
1.4	Challenges of Blockchain	8
1.4.1	Scalability	9
1.4.2	Loss of Privacy	9
1.4.3	Selfish Mining	9
	References	10
2	Bitcoin: A Digital Cryptocurrency	13
	Rohit Saxena, Deepak Arora, Vishal Nagar, and Satyasundara Mahapatra	
2.1	Introduction	14
2.2	Bitcoin Block's Structure	15
2.2.1	Bitcoin Transactions' Structure	16
2.3	Bitcoin's Anonymity & Privacy	19
2.4	Machine Learning Approaches to Price Prediction	21
2.5	Threats and Machine Learning Based Solution	22
2.6	Conclusion	24
	References	25

3	Blockchain 1.0 to Blockchain 4.0—The Evolutionary Transformation of Blockchain Technology	29
	Pratyusa Mukherjee and Chittaranjan Pradhan	
3.1	Introduction	29
3.2	Fundamentals of Blockchain	31
3.2.1	Historical Background	31
3.2.2	Basic Terminologies in Blockchain	32
3.2.3	Structure of a Block	33
3.2.4	Types of Blockchain	34
3.3	The Evolutionary Transformation of Blockchain 3.1	37
3.3.1	Blockchain 1.0	37
3.3.2	Blockchain 2.0	39
3.3.3	Blockchain 3.0	41
3.3.4	Blockchain 4.0	42
3.4	Comparison of Different Generations of Blockchain	43
3.5	A Blockchain Based Supply Chain Management Testcase	44
3.6	Conclusion	45
	References	46
4	Anatomy of Blockchain Implementation in Healthcare	51
	Shubhangi V. Urkude, Himanshu Sharma, Seethamsetty Uday Kumar, and Vijaykumar R. Urkude	
4.1	Introduction	52
4.1.1	Characteristics of Blockchain	52
4.1.2	Flow of Bitcoin Transaction	53
4.1.3	Types of Encryption Algorithms	54
4.1.4	Types of Encryption Algorithms	55
4.1.5	Cryptocurrency	56
4.1.6	Initial Coin Offering (ICO)	56
4.1.7	Tokens in Blockchain	57
4.2	Blockchain in Healthcare	58
4.3	Blockchain Implementations in Healthcare	59
4.3.1	Blockchain in Medical Insurance	59
4.3.2	Blockchain-Based Healthcare Infrastructure	61
4.3.3	Blockchain in Dental Industry	61
4.3.4	Personal Health Record Management	62
4.3.5	Pharmaceutical Supply Chain	63
4.3.6	Healthcare Information System Based on Blockchain	63
4.3.7	Blockchain in Genomics	64
4.4	Issues in Blockchain with Potential Elucidations	67
4.4.1	Scalability	67
4.4.2	Energy Consumption	67
4.4.3	Complication and Expenditure	67
4.4.4	Lack of Supremacy	68

Contents	vii
4.4.5 Lack of Compatibility and Standardization	68
4.4.6 Data Confidentiality	68
4.4.7 Storage Capacity	68
4.5 Issues in Healthcare that Could Be Solved Using Blockchain Technology	69
4.5.1 Blockchain-Based Insurance in Healthcare	69
4.5.2 Multimedia Blockchain System: An Immutable Connection	70
4.5.3 Blockchain-Based Electronic Health Records (EHR)	70
4.5.4 Blockchain Technology for Preventing Counterfeit Drugs from Entering in Pharmaceutical Supply Chain	71
4.5.5 Blockchain Technology in Doctor-Patient Interaction	71
4.5.6 Blockchain for Sharing Genomic Data	72
4.5.7 Enhancing Clinical Trials and Research Using Blockchain Technology	73
4.5.8 Decentralized Artificial Intelligence in Securing Health Records and Detecting Anomalies	73
4.6 Conclusions and Future Scopes	74
References	74
5 A Blockchain Framework for Healthcare Data Management Using Consensus Based Selective Mirror Test Approach	77
P. S. G. Aruna Sri and D. Lalitha Bhaskari	
5.1 Introduction	77
5.1.1 Blockchain Technology	79
5.2 Related Works	80
5.2.1 Traditional Healthcare Data Management	80
5.2.2 Blockchain-Based Healthcare Data Management	81
5.3 Proposed Methodology	83
5.3.1 Consensus Mechanism	83
5.3.2 Transaction Level Modeling	84
5.3.3 Health Data Interoperability	84
5.3.4 Fault Tolerance	87
5.4 Results and Discussions	88
5.5 Conclusion	89
References	93
6 Blockchain Technology in Healthcare: Opportunities and Challenges	97
Sachikanta Dash, Pradosh Kumar Gantayat, and Rajendra Kumar Das	
6.1 Introduction	97
6.2 Fundamentals of Blockchain Technology	99
6.2.1 Key Characteristic Features	100

6.2.2	Type of Blockchain	100
6.2.3	Consensus Mechanism	101
6.2.4	Smart Contract	102
6.2.5	Challenge and Future	102
6.3	The Blockchain Prospective in Health Sector	103
6.3.1	Management of Data in Healthcare Sector	104
6.3.2	Management in Pharmacy Sector	104
6.4	Proposed Methodology	106
6.4.1	Searching Strategy	106
6.4.2	Selection Strategy	107
6.4.3	Selection Strategy	107
6.4.4	Data Analysis Mechanism	108
6.4.5	Strategy Incorporates for Assessment of Quality	108
6.5	Findings	109
6.6	Conclusion	110
	References	110
7	Blockchain in Healthcare System: Security Issues, Attacks and Challenges	113
	Arup Sarkar, Tanmoy Maitra, and Sarmistha Neogy	
7.1	Introduction	114
7.2	Architecture of Blockchain and Existing Systems	116
7.3	Securities in Healthcare: Requirements	117
7.3.1	Data Security	119
7.3.2	Interoperability	119
7.3.3	Data Sharing	120
7.3.4	Mobility	120
7.4	Applications	120
7.4.1	Patient Data Management	120
7.4.2	Clinical Adjudication	121
7.4.3	Medicine Supply Chain Management	122
7.5	An Example Application: Medshare	122
7.6	Possible Attacks in Blockchain	126
7.7	Issues and Challenges to Design Secure Protocol	129
7.8	Conclusion and Future Direction	130
	References	131
8	Application of Blockchain as a Solution to the Real-World Issues in Health Care System	135
	Amrutanshu Panigrahi, Bibhuprasad Sahu, Satya Sobhan Panigrahi, Md Sahil Khan, and Ajay Kumar Jena	
8.1	Introduction	136
8.2	Features of Blockchain	137
8.3	Literature Survey	140
8.4	Working of Blockchain	140
8.5	Application of BlockChain	141

8.5.1	Blockchain in Health Care System Use Case	143
8.5.2	Key Benefits of Blockchain in Health Care	145
8.5.3	Challenges of Blockchain in Healthcare	146
8.6	Conclusion	146
	References	147
9	UML Conceptual Analysis of Smart Contract for Health Claim Processing	151
	Subhasis Mohapatra, Smita Parija, and Abhishek Roy	
9.1	Introduction	152
9.2	Basic Elements of Block Chain	154
9.3	Transaction in Block Chain	156
9.4	Ethereum Block Chain	157
9.5	Motivation	158
9.6	Survey of Smart Contract in Health Claim Processing	158
9.7	Analysis of UML Modelling for Block Chain Technique	159
9.8	Algorithm	162
9.9	Smart Contract Terminologies	163
9.10	Gas Terminology in Smart Contract	165
9.11	Conclusion	166
	References	167
10	Enabling Smart Education System Using Blockchain Technology	169
	A. R. Sathya, Sandeep Kumar Panda, and Sudheer Hanumanthakari	
10.1	Background	169
10.2	Introduction	170
10.3	Blockchain Application in Educational Sector	170
10.3.1	Secure Storage of Certificates	171
10.3.2	Multi-step Verification	172
10.3.3	Student's Credit Transfer	172
10.3.4	Intellectual Property Tracking	172
10.3.5	Fee Payment	173
10.4	Certification Process	173
10.4.1	Traditional Certification Process	173
10.4.2	Digital Signatures	174
10.5	Blockchain-Based Digital Certificates	175
10.6	Benefits and Challenges in Approving Blockchain in Education	175
10.7	Conclusion	177
	References	177

11	Blockchain Technology in Smart-Cities	179
P. Chinnasamy, C. Vinothini, S. Arun Kumar, A. Allwyn Sundarraj, S. V. Annlin Jeba, and V. Praveena		
11.1	Introduction	180
11.2	Groundwork of Blockchain and Its Architecture	181
11.2.1	Block Structure	181
11.2.2	Blockchain Types	182
11.2.3	Consensus Algorithm	183
11.2.4	Architecture of Blockchain	185
11.3	Smart City: Features, Stone Walls and Regulatory Standards	188
11.3.1	Features of Smart Cities	188
11.3.2	Pillars of Smart Cities	189
11.4	Smart Cities Security Requirements	190
11.4.1	Communication Security	191
11.4.2	Secure Management of Data	191
11.4.3	Authentication and Access Control	191
11.4.4	Application Security	192
11.5	Blockchain in Smart Cities	192
11.5.1	Healthcare Using Smart Devices	192
11.5.2	Smart Transportation	193
11.5.3	Vehicular Adhoc NETworks (VANETs)	194
11.5.4	Smart Grid	194
11.5.5	Supply Chain Management (SCM)	195
11.5.6	Financial Systems	195
11.6	Open Research Issues	195
11.6.1	Confidentiality and Integrity	196
11.6.2	Secure Storage	196
11.6.3	Energy Efficiency	197
11.6.4	Interoperability	197
11.7	Conclusion	197
	References	198
12	Blockchain Technology and Fashion Industry-Opportunities and Challenges	201
Gautami Tripathi, Vandana Tripathi Nautiyal, Mohd Abdul Ahad, and Noushaba Feroz		
12.1	Introduction	202
12.2	Issues in Fashion Industry	203
12.2.1	Supply Chain Issues	203
12.2.2	Intellectual Property Right Issues	204
12.2.3	Sustainability Issue	206
12.3	Related Work	208
12.4	Blockchain for Fashion Industry	209
12.4.1	Inventory Management	209
12.4.2	Distributed Management	210

12.4.3	Supply Chain Management	210
12.4.4	Security	211
12.4.5	Copyright and IPR Infringements	211
12.4.6	Tracking of Raw Materials and Finished Products	211
12.5	Blockchain for Fashion Industry-Issues and Challenges	213
12.5.1	Absence of Regulating Authority	213
12.5.2	Technology Immaturity	215
12.5.3	High Cost	215
12.5.4	Loss in Supply Chain	216
12.5.5	High Complexity of Blocks	217
12.5.6	Lack of Standardization	217
12.5.7	Need for Two-Level Security	217
12.5.8	Information Transparency	217
12.5.9	Intellectual Property Protection	217
12.5.10	Blockchain Incorporation Challenge	218
12.6	Conclusion and Future Scope	218
	References	219
13	Secure Event Ticket Booking Using Decentralized System	221
	Vihas Naman, Shanmukhi Priya Daliyet, Shagun S Lokre, and K. Varaprasad Rao	
13.1	Introduction	222
13.2	Literature Survey	222
13.3	Preliminaries	224
13.4	System Overview	225
13.4.1	Activity Diagram	226
13.4.2	Use Case Diagram	228
13.5	Smart Contracts	231
13.5.1	Algorithms	232
13.6	Security Analysis	239
13.7	Conclusions and Future Works	240
	References	240
14	Cloud Identity and Access Management Solution with Blockchain	243
	Soumya Prakash Otta and Subhrakanta Panda	
14.1	Introduction	244
14.2	Identity and Access Management (IAM)	245
14.2.1	Access Control System	245
14.2.2	Authentication Process	250
14.3	IAM Related Concerns	251
14.3.1	Overview of Identity Management	251
14.3.2	Threats for Identity and Access Management in Cloud Environment	253
14.3.3	IAM Concerns and Related Developments	254
14.4	Blockchain Technology	254

14.4.1	Blockchain Architecture and Functioning	258
14.4.2	Technical Function of Blockchain and Evolution	259
14.4.3	Workflow of Blockchain	261
14.4.4	Comparison of Blockchain	262
14.4.5	Security Techniques in Blockchain	263
14.5	Open Research Issues	266
14.5.1	Mandatory Access Control (MAC)	266
14.5.2	Discretionary Access Control (DAC)	267
14.5.3	Attribute Based Access Control (ABAC)	267
14.5.4	Role Based Access Control (RBAC)	267
14.5.5	Identity Access Management (IAM)	268
14.5.6	Additional Issues	268
14.6	Conclusion	268
	References	269
15	Blockchain: A New Safeguard to Cybersecurity	271
	Ishtiaque Ahmed, Manan Darda, and Siddhanth Nath	
15.1	Introduction	271
15.2	Methodology	272
15.3	Ethereum	273
15.3.1	Smart Contracts	273
15.3.2	Ethereum Virtual Machine (EVM)	274
15.3.3	Gas	275
15.3.4	DApps (Decentralized Applications)	275
15.4	Private Versus Public Blockchain	275
15.4.1	Public Blockchain	275
15.4.2	Private Blockchain	276
15.5	Cyber Threats and Blockchain Transformation	276
15.5.1	New Threat Landscape	277
15.5.2	Defender's Interpretation	278
15.5.3	By What Means Can Blockchain Help?	280
15.6	Future Work	282
15.6.1	Future Impacts of Blockchain	282
15.7	Conclusions and Future Scopes	283
	References	284
16	Gun Tracking System Using Blockchain Technology	285
	Shagun S Lokre, Vihas Naman, Shanmukhi Priya, and Sandeep Kumar Panda	
16.1	Introduction	286
16.2	Prerequisites	287
16.3	System Overview	289
16.4	Working Procedure	290
16.4.1	Algorithm Design	293
16.4.2	Implementation	295
16.5	Security Analysis	298

Contents	xiii
16.6 Conclusions	299
References	299

Chapter 1

Blockchain Technology: Introduction, Applications, Challenges



Ajay Kumar Jena and Sujata Priyambada Dash

Abstract Blockchain—the technology behind the popular cryptocurrency bitcoin is revolutionizing the world and bringing significant changes in our technology and business environment. Blockchain is a tamper-proof, distributed and decentralized peer-to-peer technology that could track and verify digital transactions. It aims to bring in transparency, security and integrity of data. This most trusted, decentralized ledger finds its application in almost all the domains varying from finance, education, energy, supply chain, health care and many more. This chapter elaborates the different components that make this technology more trustable and reliable. It uncovers the various application areas of blockchain technology. While detailing the space with blockchain it also brings out the shortcomings, difficulties and threats of this technology. This chapter will act as a guide for people interested to explore blockchain and blockchain based solution for any application.

Keywords Blockchain · Cryptocurrency · Peer-to-peer · Bitcoin

1.1 Introduction

For the past few decades, there had been a rise of many applications over the internet that solves real time problems in a collaborative and decentralized manner. A numerous such applications are popular and common universally. However, the concept of digital currencies exists since 1980s, but it took more than two decades to make a decentralized solution possible. Over the past, digital currencies used a central authority to store and maintain the transaction records. B-Money [1], Bitgold [2], RPOW [3] are some of the examples of a centralized approach. Later, distributed solutions to store the transactions of currencies were developed to eliminate the need

A. K. Jena (✉)

School of Computer Engineering, KIIT Deemed to be University, Bhubaneswar, Odisha, India

S. P. Dash

Department of Management, Birla Institute of Technology, Mesra, Ranchi, India

e-mail: spdash@bitmesra.ac.in

for central authorities like bank. However, these currencies had a risk of double spending. In other words, it is possible to make two different transactions with same coins which are not possible in centralized approach. Moreover, to get an agreement on distributed information and maintaining a consistent state in distributed environment led to Byzantine Generals Problem [4]. Therefore, Quorum systems are developed where malicious users and faulty information are accepted by the system. But the concept of voting in quorum systems i.e. an information will be accepted if majority of the users have voted for it have led to Sybil attacks [5]. Quorum systems also gave rise to temporary inconsistencies.

In 2008, Satoshi Nakamoto developed a bitcoin design [6] which overcomes all the above mentioned difficulties. Bitcoin becomes widespread immediately due to its combined contributions from previous research works. Bitcoin uses a unique feature named Proof-of-Work to restrict the number of votes per entity thereby making a decentralized approach real. The nodes of a decentralized bitcoin network is called *miner*. The miner collects all transactions of the network in blocks. A collection of such blocks linked via some cryptographic mechanism is called Blockchain. Blockchain Technology is a distributed, decentralized, peer-peer network to store transactions of the network without any third party. This technology came to limelight with the introduction of Bitcoin network. It allows the bitcoin users to transmit their rights to information to another bitcoin user publicly over the network. Blockchain allows the nodes to verify and manage the network. The cryptographic hashing mechanism used in blockchain lets the data in blocks to be tamper-proof and secure. In bitcoin blockchain the users are enabled to be pseudonymous which means the transactions are available public but their identities are not. Some of the key characteristics are mentioned below.

Ledger: An open, append only ledger is used by blockchain to record the transaction history. The data in this ledger cannot be modified unlike the traditional databases.

Secure: Blocks in blockchain are cryptographically linked and does not let the data to be tampered thereby assuring the security of information over blockchain.

Shared: The public ledger can be shared among the users of the network thus assuring the transparency among the users.

Distributed: The blockchain is distributed among the users of the network which makes it strong against the attacks. By increasing the number of nodes in the network the security of the information on blockchain is high.

Based on the permissions strategy, the blockchain is categorized as permission-less and permissioned. Permission less are public blockchain where anyone who are part of the network can publish blocks whereas permissioned are private blockchain where only authorised users can publish the blocks. Permissioned blockchain are usually implemented for group of organizations and permission less does not have such restrictions. The summary of distinction between permission and permission-less blockchain is given in Table 1.1.

Table 1.1 Permissioned versus permission-less blockchain

Permissioned	Permissionless
Users has to be authorized by some authority to publish blocks	No permission required to publish blocks
May be open source or closed source platforms	Open source platforms available for anyone to download
Possible to restrict read and write access to users	Anyone in the network can read or write transactions over the blockchain
Uses consensus methods but not necessary to keep or maintain expensive resources	Users' needs to adapt consensus mechanism in order to avoid malicious users to publish blocks
No rewards	Users who publishes blocks are rewarded with cryptocurrencies
Users identity are known and authorised	Users identity are pseudonymous

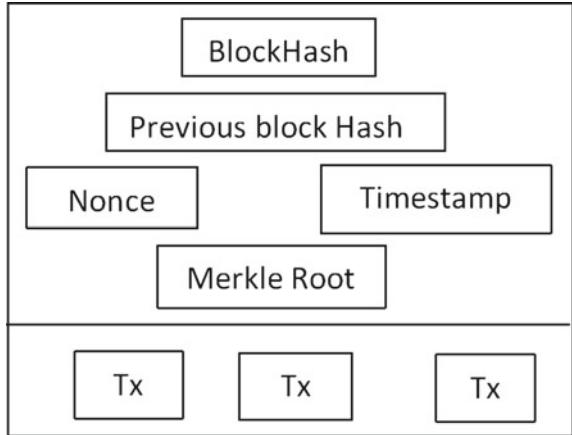
1.1.1 *Components of Blockchain*

At the top-level, widely-known cryptographic concepts like hashing, asymmetric key cryptography, digital signatures combined with principles in record keeping are used in Blockchain Technology. Some of the key components like Addresses, Blocks, transactions, hashing and digital signatures are explained below in detail.

1.1.2 *Hashing Methods*

The most important component of blockchain technology is hashing functions a cryptographic mechanism. Hashing is a cryptographic technique which simply converts a data of any size into a unique fixed size output. The input can be a text, file or image and the output is fixed size alpha-numeric string. Hashing in blockchain assures the users that the data transmitted is not changed. This can be done by comparing the hash values of the input data. That is, any minor change in the data will result in different hash value. The reason hashing technique used in blockchain is due to its security property. (i) Pre-image resistant: Hashing techniques are uni-directional. It is not possible to compute the input based on the output. (ii) Second preimage resistant: based on the input given, it is impossible to compute the second input that generates the same output. (iii) Collision resistant: It is highly infeasible to find two input generating same hash output.

Most of the blockchain implementation uses Secure Hash Algorithm (SHA) that generates an output of size 256-bits. SHA-256 hashing algorithm produces an output of 32 bytes (256-bits) usually displayed as 64 hexadecimal characters. Other than SHA-256, Keccak and RIPEMD-60 are some other hashing algorithms used in blockchain network. Hashing techniques are used for various operations in blockchain such as address creation, securing block data and block header etc.

Fig. 1.1 A block structure

Another key component used is Nonce which is used in proof-of-work consensus mechanism. A nonce is a random number that is combined with the block data to produce different hash output. The proof-of-work consensus model functions by adjusting the nonce value and provides a method for obtaining specific output values by retaining the same data. The structure of a block is given in Fig. 1.1.

Figure 1.1 shows the block structure divided into a block header and a body. The body of a block consists of all the transactions of that block whereas block header in turn has the hash of the block, hash of the previous block, the nonce value, timestamp denoting the time details of the block published and the merkle root [7] which is nothing but the consolidated hash value of the all the hashes of the transactions.

1.1.3 Transactions

A transaction in blockchain means an interaction between two entities. In case of cryptocurrencies, the transfer of bitcoin or any other cryptocurrency from one user to the other is called as transaction whereas in a business scenario transfer of ownership or activities involved in digital assets is considered as a transaction. Every block contains zero or more transactions. The data included in a transaction generally are transaction input, output, sender's address, sender's public key, and a digital signature [8]. Although mainly used for the transfer of digital objects, transactions may commonly be used for data transfer. In a basic scenario, someone might only choose to publish data public on the blockchain forever. Or it can be used to transfer and process the data and then stores the result in blockchain as in smart contracts system. More than the data and the transmission validity and authenticity of the transaction are vital. Validity of the transaction assures that the transaction adheres to the blockchain implementation protocols and authenticity implies that the sender of the transaction has access to the digital assets that are transmitted. The sender

of the transaction digitally signs it by using his private key and can be verified by anyone using the sender's public key.

1.1.4 Public Key Cryptography

Public key cryptography otherwise called as Asymmetric key cryptography is used in blockchain for various operations. Asymmetric key uses two key namely public and private key which are computationally related to each other. Out of these, the public key can be viewed by anyone whereas private key is kept secret. However, it is not possible to compute the private key using the openly available public key. At the same time, it is possible to encrypt the data using a private key and can be decrypted using the corresponding public key. This process can be vice-versa. This cryptographic mechanism assures users the authenticity and integrity of data but maintains transparency at the same time [9]. However, the process of encryption and decryption in asymmetric key cryptography is considered slow to compute. But, symmetric key encryption methodology where a single key is used for encryption and decryption is easy to compute however there's a need for trust among the users to share the keys. Therefore to simplify the process the data is encrypted using symmetric key technique and then the symmetric key in turn is encrypted using asymmetric key technique. In this way the speed of asymmetric key technique can be greatly improved.

1.1.5 Address and Wallet

Addresses are usually a short alphanumeric characters used as a sender and receiver's transaction point. A hash function is used to derive user's public key. Different blockchain implementation uses different ways to derive the addresses. And the users of blockchain network have to store their private keys in a secure place. Instead of storing them manually, software is used to store them. The software used to store the private keys is called as wallets. Apart from private keys the wallets can store the user's addresses and public keys as well. Wallets are used to calculate the number of digital assets owned by a particular trusted user.

1.1.6 Blocks

The transactions made by the blockchain users are submitted to the network via software like web services, mobile applications and so on. Once a transaction is submitted, the software sends it to a particular node or to a set of nodes. This does not mean that the transaction is added to the blockchain. The transactions would

be in queue of the publishing node and will be added in blockchain after the node publishes a block. A block includes a block header where the metadata of the block is available and a block body where all valid transactions will be included [10]. The metadata of the block varies based on the blockchain implementation. A general structure of a block can be referred in Fig. 1.1. These blocks are chained together through the hash of the previous block and form a blockchain. For instance, any data change in any of the block will result in a different hash and will be reflected in the subsequent blocks. Hence it is easy to identify whether a block has been tampered or not [11].

1.1.7 Consensus Mechanism

Key feature behind the technology of blockchain is to determine the user to publish the blocks. As the network node publishes a block they would be rewarded with cryptocurrency. Due to this, it is possible for many nodes to compete for publishing nodes. This problem can be solved using consensus mechanisms. This allows a group of users who don't trust each other to work together. There are several consensus models being used such as Proof of Work (PoW), Proof of Stake (PoS), Proof of Authority (PoA), Proof of Elapsed Time (PoET) etc.

The consensus mechanism is a process of decision making where the network users agree and support a decision for the betterment of the network. In consensus model, in order to add a block in blockchain a miner (node) has to solve a cryptographic puzzle. The process of solving the puzzle requires huge computation and is hard to solve. Once the puzzle is solved it'll be broadcasted to the network for verification. Once verification is successful, the block will be added to the blockchain [10].

1.1.8 Smart Contracts

In 1994, Nick Szabo developed an automated transaction procedure that implements the terms of an agreement or contract. Blockchain performs transactions in a pre-agreed fashion where the participating entities agree upon the contractual terms. The main objective of a smart contract is to execute the terms and conditions of a contract automatically thereby minimizing the need for intermediaries [12]. Smart contracts are cluster of data and code or programmed applications that are implemented via digitally signed transactions over the blockchain network. The execution of smart contracts is done by the nodes of the network and the results are stored on the blockchain. Regardless of the number of nodes executing the smart contract the result of the execution must always be same. Various operations can be performed using a smart contract like some computations, providing access, storing information and even reverting back the financial transactions. It is to be noted that not all

blockchain models can execute smart contracts. Bitcoin blockchain do not support smart contracts but uses some scripting languages to offer limited programmability. Whereas, Ethereum [13] and Hyperledger [14] run smart contracts built over them. The programming language used to write smart contracts are Serpent and Solidity. However, the most widespread language is solidity.

1.2 Evolution of Blockchain

Over the years, blockchain has evolved rapidly that it provides many more solutions than just the decentralization of cryptocurrency. While Bitcoin Blockchain is considered as a first generation blockchain, Ethereum and Smart contracts forms the second generation blockchain and the development of Decentralized Apps (DApps) are the third generation blockchain models. Bitcoin blockchain enables the financial transaction in a decentralized way and eliminates the need for trusted third parties. The transactions are based on public key cryptography and digital signatures. The nodes that validate the transactions uses a PoW mechanism based on Hashcash and SHA-256 hashing algorithms. Though it is claimed that the users of bitcoin blockchain can remain anonymous but, it is possible to trace back the transaction and find the identity of the users. Hence the users are pseudonymous. The users were rewarded with incentives i.e. bitcoins for publishing the blocks. However scalability played a major drawback in bitcoin blockchain. Moreover, it is not well suited for general purpose applications due to its limitations. Thus in 2013, Ethereum [15] a general purpose blockchain platform was developed. Ethereum addresses most of the scripting and transaction limitations of bitcoin blockchain. Therefore Ethereum led to the development of smart contracts a small programmed application to be stored and execute over the blockchain network. Smart contracts enable automatic execution of conditions while validating the transactions. Therefore it reduces the cost involved in verification, fraud prevention and many more and ensures transparency. Though it provides lot of advantages, Ethereum smart contracts does have some limitations like, complex programming languages to write smart contracts, difficult to modify or end the smart contracts once executed and so on. However, with the growing economic demand, Ethereum could not support huge volumes of transactions. Therefore, Blockchain is increasingly heading to decentralized web, incorporating systems for data collection, smart contracts, communication networks and open standards. This paved the way for DApps which means Decentralized Applications whose backend runs on a Blockchain network and its front end has a user interface of any programming language [16]. DApp is open source and uses decentralized consensus mechanisms. With growing popularity of DApps it is integrated with many industrial applications thereby enabling a cross chain communication [17]. This allows consumers from various systems to function together as one team, making Industry 4.0's market demands and specifications easily merged [18].

1.3 Applications of Blockchain

Due to its salient features blockchain is applied not only in decentralized cryptocurrencies but much beyond that. Blockchain can change the business transactions models and protocols of managing assets [18], E-voting [19], renting a car, watching a movie and many more. It widens its applications in major sectors like FinTech [20], Healthcare [21], Governance, Supply chain [22], Manufacturing Industries, Insurance, Education, IoT [23], Big Data systems and Machine Learning [24] etc.

FinTech: Application of Blockchain in various financial services include Financial transactions, Asset management, etc. It avoids any trusted third parties and enables faster and reliable transactional services. *Insurance:* In insurance domain, the need to detect the fraudulent claims, abandoned policies can be streamlined by using blockchain and making a risk free and transparent system. Insurers can get a hold of ownership of assets that are to be insured by the encryption properties of blockchain.

IoT: Any object connected to the Internet becomes Internet of Things. Application of Blockchain in IoT is enormous. Like Smart Home applications, smart cities, Cloud Integration [25] and so on. *Healthcare:* Healthcare is one such domain where a huge amount of data is generated. For instance, daily reports of patient monitoring, clinical research management, processing medical insurance claims and storing the medical records. Applying blockchain in healthcare includes the decentralization of the mentioned activities with patients, doctors, insurance companies being the users and managing the records. *Education:* Blockchain in education is still at the pilot level and can extend its potential in Identity management, Digital certificates, Blockchain enabled certificates etc. It enables the users to share their academic achievements with chosen users who want to verify the credentials. Similarly, *E-voting:* Enabling the users to cast their vote in a secure way. Since the data on blockchain is secure tamper-proof, it is possible to avoid any counterfeit of votes. Another major sector where blockchain has a greater potential for growth is *Supply chain:* The whole process of supply chain can be carried over the blockchain network like transmission of goods, traceability of items, customer refund in case of faulty delivery, and faster transaction at reduced cost. Blockchain can transform the way the supply chain works.

The above mentioned areas are some of the applications where blockchain is revolutionizing but not limited only to those domains. There are many more areas where researchers are trying to fit in blockchain in order to utilize its entire potential [26].

1.4 Challenges of Blockchain

Even though Blockchain Technology has numerous potential in it there are certain challenges that limit the application of blockchain on a wider range. Few major challenges can be as follows.

1.4.1 Scalability

Due to the increase in the number of transaction every now and then, the size and volume of blockchain also getting large day by day. Every node has to collect all the transactions and validate them on the blockchain. Besides this, blockchain has a restriction on block size and the amount of time taken to publish the blocks only 7 transactions per second can take place. This may not suffice the requirement of processing a large amount of data in real-time. And moreover since the size of the block is small miners tend to prefer validating transaction with higher fee due to which smaller transactions gets delayed. Some developments to resolve these issues are storage optimization and redesigning of blockchain.

1.4.2 Loss of Privacy

In blockchain a considerable amount of privacy is maintained by using public key cryptography mechanism in transactions to keep the user identity anonymous. However, the transactional anonymity cannot be assured by blockchain because the identities of all transactions and balances for each cryptographic key are publicly accessible. Thus it is possible to recognize the user by keeping track of the transactions.

1.4.3 Selfish Mining

Blockchain is more prone to attacks like this. Selfish Mining is a strategy where an over ambitious miner secretly keeps his blocks without publishing it. It would be revealed to the public only if some conditions are satisfied. This secretly mined private chains which are longer than the current openly available chain, all other miners would agree to it. As a result honest miners would have wasted their resources on a chain that is going to be abandoned. In this way selfish miners may be rewarded with higher incentives. Likewise blockchain is susceptible for many attacks like Sybil attacks, Double spending [27, 20], 51% attacks and so on.

Nevertheless, Blockchain has been transforming both the industry and the academia with its distinct properties like decentralization, anonymity, integrity and transparency. The applications of blockchain have gone beyond cryptocurrencies and transactions. The decentralization nature of blockchain over the already existing internet is very interesting in terms of data redundancy and survivability. Out of some solutions blockchain is the perfect solution for problems where trust is of key concern. Even though blockchain has not reached its maturity it still continues to suit applications of different domains globally.

References

1. Dai, W.: B-Money [Online] (1998). Available: <https://www.weidai.com/bmoney.txt>
2. Szabo, N.: Bit Gold [Online] (2005). Available: <https://unenumerated.blogspot.de/2005/12/bit-gold.html>
3. Finney, H.: Rpow [Online] (2004). Available: <https://cryptome.org/rpow.htm>
4. Lamport, L., Shostak, R., Pease, M.: The Byzantine generals problem. ACM Trans. Program. Lang. Syst. **4**(3), 382–401 (1982)
5. Douceur, J.: The Sybil attack. In: Proceedings of 1st International Workshop Peer Peer Systems, pp. 251–260, March 2002
6. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system. Tech. Rep. (2008) [Online]. Available: <https://bitcoin.org/bitcoin.pdf>
7. Merkle, R.C.: A digital signature based on a conventional encryption function. In: Pomerance, C. (ed.) Advances in Cryptology—CRYPTO '87: Conference on the Theory and Applications of Cryptographic Techniques, Santa Barbara, CA, Aug 1987, pp. 369–378
8. Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfede, S.: Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press (2016)
9. Kosba, A., Miller, A., Shi, E., Wen, Z., Papamanthou, C.: Hawk: the blockchain model of cryptography and privacy-preserving smart contracts. In: 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, May 2016, pp. 839–858
10. Tschorsch, F., Scheuermann, B.: Bitcoin and beyond: a technical survey on decentralized digital currencies. IEEE Commun. Surv. Tutor. **18**(3), 2084–2123, 3rd Quart. (2016)
11. Bitcoin Block Explorer. Accessed: 13 June 2017. [Online]. Available: <https://blockexplorer.com/blocks-date/>
12. Szabo, N.: Smart Contracts (1994). <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smарт.contracts.html>
13. Wood, G.: Ethereum: A Secure Decentralised Generalised Transaction Ledger. Accessed: 19 Nov 2016. [Online]. Available: <https://paper.gavwood.com>
14. Dhillon, V., Metcalf, D., Hooper, M.: The hyperledger project. In: Blockchain Enabled Applications, pp. 139–149 (2017)
15. Buterin, V.: Ethereum white paper: a next generation smart contract & decentralized application platform (2013). Available at: https://www.theblockchain.com/docs/Ethereum_white_papera_next_generation_smart_contract_and_decentralized_application_platfor
16. Raval, S.: Decentralized Applications : Harnessing Bitcoin's Blockchain Technology, 1st edn. O'Reilly Media (2016)
17. Bogner, A., Chanson, M., Meeuw, A.: A decentralised sharing app running a smart contract on the ethereum blockchain. In: ACM International Conference Proceeding Series, pp. 177–178 (2016)
18. Unibright—The Unified Framework For Blockchain based Business Integration (2018). <https://unibright.io>. Accessed on Nov 2018; Accenture: Banking on blockchain. A value analysis for investment banks. Report (2017)
19. Boucher, P.: What if blockchain technology revolutionised voting? Scientific Foresight Unit (STOA). European Parliamentary Research Service (2016)
20. Conti, M., Sandeep Kumar, E., Lal, C., Ruj, S.: A Survey on security and privacy issues of bitcoin. IEEE Commun. Surv. Tutor. **20**(4), 3416–3452, Fourth quarter 2018
21. Angraal, S., Krumholz, H.M., Schulz, W.L.: Blockchain technology: applications in health care. Circul. Cardiovascular Qual. Outcomes **10**(9) (2017)
22. Ahmed, S., Broek, N.T.: Food supply: blockchain could boost food security. Nature **550**(7674), 43 (2017)
23. Boudguiga, A., Bouzerna, N., Granboulan, L., Olivereau, A., Quesnel, F., Roger, A., Sirdey, R.: Towards better availability and accountability for IoT updates by means of a blockchain. In: Proceedings—2nd IEEE European Symposium on Security and Privacy Workshops, EuroS and PW 2017, pp. 50–58 (2017)

24. Abdullah, N., Håkansson, A., Moradian, E.: Blockchain based approach to enhance big data authentication in distributed environment. In: International Conference on Ubiquitous and Future Networks. ICUFN, pp. 887–892 (2017)
25. Ali, M., Miraz, M.H.: Cloud computing applications. In: Proceedings of the International Conference on Cloud Computing and eGovernance—ICCCEG 2013, Internet City, Dubai, United Arab Emirates, pp. 1–8 (2013). Available: <https://www.edlib.asdf.res.in/2013/iccceg/paper001.pdf>
26. Gartner: Top Trends in the Gartner Hype Cycle for Emerging Technologies. Gartner, Inc., Gartner Hype Cycle 2017, August 2017. Available: <https://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/>
27. Tapscott, D., Tapscott, A., Revolution, B.: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, 1st edn. Penguin Publishing Group, New York, USA (2016)

Chapter 2

Bitcoin: A Digital Cryptocurrency



Rohit Saxena, Deepak Arora, Vishal Nagar, and Satyasundara Mahapatra

Abstract Bitcoin is the largest cryptocurrency ever created and traded using a decentralized ledger known as the blockchain. Altogether, Bitcoin is a network in which every computing node is responsible to service the others and allows shared access to the data, known peer to peer (P2P) network, and provides an adaption of electronic-cash that supports e-payments. Such payments are transferred directly from transacting parties to the receiver without the requirement of any intermediary monetary body. Satoshi Nakamoto introduced bitcoin in 2009 and since then it has emerged as the most thriving cryptocurrency. Bitcoin is a globally accepted and immutable e-payment system of digital currency. All the electronic transactions performed using bitcoin are verified by the intermediate nodes called miners and then added as a block in the distributed ledger. Bitcoin blockchains are maintained by the miners running Bitcoin software. Bitcoin depends on Proof-of-Work (PoW) to confront double-spending by a distributed timestamping service. To ensure the operations and security of Bitcoin, all the transactions and their execution order must be available to all Bitcoin users. In addition to its security robustness, anonymity is the key attribute for its success. There are several factors like market-cap, the marketplace, miners-revenue, etc. which causes the rise and fall of the price of Bitcoin. This chapter focus on the factors that are responsible for the rise and fall of Bitcoin Price with a comparison with other Cryptocurrencies.

Keywords Bitcoin · Blockchain · Cryptocurrency · Consensus · Miners

R. Saxena · V. Nagar · S. Mahapatra (✉)
Pranveer Singh Institute of Technology, Kanpur, India

D. Arora
Amity University, Lucknow, India
e-mail: darora@lko.amity.edu

2.1 Introduction

Bitcoin is an interconnection of computing nodes where the source code of bitcoin is deployed and stored in its blockchain. While the collection of transactions is known as a block, blockchain is a collection of blocks. All the nodes that run the blockchain have the same collection of blocks and transactions and transparently see the new blocks being added with new blockchain transactions. To realize the wicked act, miners need to gain the hash rate 51% or more (known as the 51% attack) that makes up a bitcoin. Although, such an attack is still theoretical because bitcoin currently has more than 10,000 computing nodes which are growing consistently, making such attacks improbable [1].

Blockchain is progressing & recasting the industry of information technology with superior security, competence, and flexibility. There are various use cases of Blockchain Technology which majorly include cryptocurrencies such as Bitcoin, Ethereum, Litecoin, Ripple etc. [2]. Bitcoin is a cryptocurrency popularly used for peer-to-peer and decentralized payments where the transactions are performed without an intermediary. Transactions performed using Bitcoin are verified by intermediate nodes in the network. These transactions are then registered in the globally accessible ledger called Bitcoin Blockchain. The novel concept of Bitcoin was originally presented by the mysterious Satoshi Nakamoto in 2008 and was realised as open-source software in 2009 and since then it has surfaced as the most favourable cryptocurrency among all its competitors thereby adding billions of dollars to the economy within few years. As, Bitcoin employs P2P network that does not use any external bodies such as banks or any other electronic financial service provider for supervises and observes the validation or approval of transactions. Bitcoin has progressively drawn the attention of the public and advancing with increasingly more customers connecting with the payment system as it is now described as revolutionary, fast, tax-free, and convenient digital currency [3].

Being a cryptocurrency based on account entries, the bitcoin is described as surplus remaining in bitcoin account. Bitcoin accounts are described as Elliptical Curve Cryptographic Key Pairs. Bitcoin employs Elliptical Curve Digital Signature Algorithm (ECDSA) to make sure that electronic funds are spent by the legitimate user. ECDSA is the cryptographic algorithm that has the curve specification secp256k1 that signifies the private keys with size of 256-bit [4]. Secp256k1 is used to refer to the essential parameters of elliptic curve employed in asymmetric key cryptography for bitcoin blockchain and is described in the specifications for the competent cryptography. ECDSA conceptualizes the following [5]:

- (a) **Private key:** randomly generated secret number which is known to the entity who has generated it. In bitcoin blockchain, users that possess the private-key can spend funds using the blockchain. The private-key is a single unsigned integer of 256-bit.
- (b) **Public key:** number computed using the private key that is not kept secret. It is used to ascertain whether the signature is authentic i.e. generated with proper key while keeping the private-key secret. In bitcoin blockchain, public-keys

can be either uncompressed (i.e. 65 bytes, prefixed with 0×04 and followed by 2 keys of length 256-bits) or compressed (i.e. 33 bytes, prefixed with 0×02 or 0×03 and key-length 256-bits).

- (c) **Signature:** number, generated mathematically using a hash of something that is to be signed, plus a private-key.

Bitcoin accounts are globally recognized by their addresses and achieved through its public-key that employs simplex and unidirectional function. With the help of this knowledge, bitcoin users can transfer the bitcoins to that bitcoin address. For spending funds electronically, the sender needs the corresponding private key. The user of bitcoin can generate several addresses by applying cryptographic software or bitcoin wallets.

2.2 Bitcoin Block's Structure

A bitcoin block is a container that amasses transactions arranged linearly over a period in the globally distributed ledger, blockchain. Transaction's data is persistently stored in files known as blocks. It is data structure just like individual pages similar to the pages of the record book or bank's transaction ledger. A bitcoin block has a header and list of transactions. The transaction list takes the maximum size of the block. Various fields, their description and size of a block are depicted in Table 2.1.

Block's Header

The header of a block consists of three sets of information [4]. They are:

- (a) references to the immediately previous block connecting to the current block.
- (b) metadata set to relate the mining competition, i.e., difficulty, timestamp, and nonce
- (c) the data structure, Merkle root, to describe all the transactions in the block.

The cryptographic hash is main identifier which is also considered as digital fingerprint. The block header is hashed twice by SHA-256 hashing algorithm to compute the cryptographic hash. This results in block hash which is a 32-byte hash or more precisely block's header hash because it is calculated using the block header. For instance, the hash of the very first block header created for bitcoin blockchain is 000000000019d6689c085ae163431e934ff763ae46a2a6c172b3f1b60a8ce26f. Hash

Table 2.1 Block structure [4]

Field	Size (in bytes)	Description
Block size	4	Total bytes
Block's header	80	Comprises 6 items
Transaction's counter	1 to 9	VI = VarInt, it is positive integer
Transactions	<Transaction counter>	Non-empty transactions list

value of the header is utilized to identify the bitcoin block unambiguously and more importantly it is the unique identifier for a block. Hash of the header can be derived autonomously by any node by hashing the header of the block. Every node calculates the hash of the new block as it is received. It is then stored in a separate autonomous table as a metadata of that block. This facilitates indexing and speedy retrieval of the blocks from the disk. This hash is neither encapsulated in the data structure of the block nor transmitted in the network along with the block, nor stored as persistence storage of the block.

2.2.1 Bitcoin Transactions' Structure

The most crucial part of the bitcoin system is a transaction. These are data structures used to cipher the funds transfer from the source of the fund, known as the input, to a destination known as an output in the bitcoin system. Every transaction is needed to be created, validated, propagated, and incorporated to the public balance sheet of the transaction and then entered in the bitcoin's blockchain. There are various fields of the transaction. These are shown in Table 2.2.

One of the elementary components of the bitcoin transaction is Unspent Transaction Output (UTXO). They are inseparable blocks of bitcoin locked to a specified proprietor and reorganized as units of currency by the unified network. The bitcoin's network keeps track of the ready-to-use UTXO. The amount is saved in blockchain in the form of UTXO whenever any user receives bitcoin and might be outspread as UTXO among a large number of transactions. The concept of bitcoin balance is deduced by wallet application. The blockchain is scanned and all the UTXO belonging to the users are aggregated by the wallet to calculate the users' balance. The value of the UTXO can be arbitrarily designated as multiple of satoshis. Bitcoin is divided into 8-decimal places similar to the dollars which is divided into 2-decimal places. Once UTXO is created, it cannot be divided. Therefore, if it is larger than its required value, it must be consumed completely, and changes must be reflected in the transaction. That is if there are 30 bitcoin UTXO and only 2 UTXO are needed to be spent then the transaction must completely eat up the 30 bitcoin UTXO and produce the following two output: (a) payment of 2 bitcoin to the desired recipient

Table 2.2 Schematic structure of bitcoin transaction

Field	Description	Size (in bytes)
Version	Present the rules to be followed by transaction	4
Input counter	Total inputs included	1 to 9 (VarInt)
Inputs	Transaction input (One or more)	Varying size
Output counter	Total outputs included	1 to 9 (VarInt)
Outputs	Transaction output (One or more)	Varying size
Locktime	Block number/Unix timestamp	4

and (b) payment of 28 bitcoin as the change back to the wallet which is at hand for the transactions to come.

UTXO that are exhausted for a particular transaction are known as transaction inputs and the UTXO that are constructed through the transaction are called transaction output. In this manner, the clusters of the values of the bitcoin travel forward from one owner to the other to form a series of transactions that consume and create UTXOs. Signature of the current user is used by the transactions to unlock the UTXO and then consuming it. Transactions create UTXOs and lock them to next owner's bitcoin address.

Transaction Outputs

Transaction outputs are created and recorded on the ledger of the bitcoin. These transaction outputs create spendable clusters of bitcoins known as Unspent Transaction Output (UTXO). Entire network identifies the UTXOs and are at hand for transacting in the time to come. Transacting bitcoin is creating a UTXO registered to the address of the owner and available for spending. UTXO can be tracked by bitcoin client in a database known as the UTXO pool or UTXO set. Every transaction output comprises of following two things.

- (a) total amount of bitcoins denominated as satoshis, also the smallest bit.
- (b) locking script, also known as “encumbrance”, locks the amount by designating the state that is to be satisfied for spending the output.

Transaction Input

The pointers to the UTXO are called transaction input. These are transaction hash and sequence number of the a UTXO in the bitcoin blockchain. It includes the scripts for unlocking for spending UTXO. These scripts must meet the requirements of the spending conditions that the UTXOs has set. This is a signature that proves the possession of the bitcoin address in locking script. The wallet of the user selects from the pool of the remaining UTXOs and creates transaction. For an instance, if the payment to made is of 0.020 bitcoin, the wallet app selects 0.010 UTXO and adding them up for the payment. After UTXO selection, unlocking scripts are produced by the wallet and making the UTXO eligible for spending by satisfying the locking script conditions. The unlocking scripts contain the signatures for every UTXO. The wallet then adds unlocking scripts and UTXO references as input to the transactions³ Bitcoin Mining.

In blockchain, mining is appending a new block at the end. In bitcoin network, mining process adds a new bitcoin to the electronic fund supply. Mining nodes are the specialized nodes on the bitcoin network. Such nodes listen for the new block that is propagated on the bitcoin network.

It also helps to safeguard the bitcoin network against dishonest transactions moreover preventing transactions from paying out the same amount of bitcoin again and again which is commonly known as double-spending. In turn, the miners get rewarded for providing the processing power to the bitcoin network. They play a vital role in validating new transactions and documenting them on the distributed ledger. After

every 10 min, a newly mined block that contains the transaction that occurred since the last block is mined, i.e., the most recent transaction. These transactions are incorporated inside the block after which they are added to the blockchain as confirmed transactions allowing the possessor of the bitcoin to spend whatever they have gained in those transactions [4].

The mining nodes participate and compete for working out a difficult-to-solve cryptographic hash algorithm based mathematical puzzle. In turn, they earn two types of rewards: (a) new coin that is generated after each block has been mined and, (b) fees for all the validating and recording the transaction. The solution to such mathematical puzzles is called PoW i.e., Proof-of-Work. The battle of solving the PoW algorithm form the basis for the security model of bitcoin. The process of mining facilitates the monetary supply for Bitcoin which is similar to the banks that issues the new money by printing currency notes. The number of bitcoins that can be added by the miner drops roughly after every four years which is almost every 210,000 blocks. Initially, the number of bitcoins that can be added per block were 50 in January 2009 which declined to 6.25 bitcoin every block on May 11, 2020 [6]. In this manner, there is an exponential decrease in the reward of the miner and until 2140 approximately all the bitcoin i.e. 20.9999998 million will be issued and no new bitcoins will be issued.

Every transaction includes a transaction fee. This fee is an overabundant bitcoin between inputs and outputs of the transaction. The miner winning PoW challenge gets it as reward. As the time is increasing, the reward earned by the miner is decreasing while the total number of transactions per block are increasing and the larger proportion of miners' earning will be from the transaction fees. Mining process accredit the network-wide consensus in decentralized environment and safeguards the bitcoin network from attacks.

The traditional payment systems depend upon the trust model having centralized authority that provides the clearinghouse services by verifying and clearing the transactions. On the other hand, the bitcoin blockchain has no central authority, blocks in a blockchain are assembled separately in the network and have an entire replica of the public ledger that can be a trusted authoritative log. Decentralized consensus in bitcoin comes to the light through the interaction of four processes occurring separately on the mining nodes in the network:

- (a) Every transaction is verified independently based on an extensive criteria list. The verification is done by the full node.
- (b) The mining nodes aggregate the transactions independently into new blocks that is coupled with demonstrated computation through the PoW algorithm.
- (c) Every node independently verifies and assembles recent blocks into blockchain.
- (d) The chain with massive cumulative calculations shown by PoW are selected by every node independently.

Wallet software generates transactions by collecting Unspent Transaction Output, furnishing relevant scripts for unlocking, and creating recent outputs being allocated to new owners. Transaction is then forwarded to adjacent nodes for network-wide propagation. Every node verifies the transaction and forwards the valid transaction

to their adjacent nodes. The verification ensures that only the valid transactions are propagated across the entire network and invalid transactions are discarded at the first node that confronts them.

2.3 Bitcoin's Anonymity & Privacy

The crucial concepts which cannot be easily differentiated are anonymity and privacy. While anonymity is hiding the owner's identity, privacy means hiding of the background [7]. In a real-life scenario, the user's privacy more desirable than anonymity because the protection of personal data is required for its proper usage. For example, personal email account information may be known to many, but the restricted content can only access by the account owner using a password. Hence, privacy is necessary for almost all systems and applications [6, 8]. While anonymity is the property that the criminals look for. It becomes impossible to hold criminals accountable for the crime they have committed [9]. There are application areas other than criminal activities where anonymity is required. The best-suited example is the ballot system. Being untraceable and unidentifiable is the key objective for anonymity [10]. True anonymity cannot be ensured as many applications that claim to be anonymous have flaws due to which identity information is leaked. Mixing services [11], commonly known as mixing networks or mixnets are being employed to avert tracing acts of messages through a network. Such mixing services may be unreliable and lead to overheads in terms of computation and communication [12]. Anonymization employing onion routing [13] is extensively used to hide the personal information by unveiling the problem of tracking the IP. TOR [14], the most outstanding and prosperous anonymity network has flaws [7, 15].

Anonymity and privacy do not come for free. To maintain privacy and anonymity, extra efforts and work is needed which in turn requires more resources in terms of space, time, or computation power [16]. Moreover, users may have to pay extra to maintain privacy and anonymity. According to [17], in an incident that happened to occur in Turkey, a passenger who used local mobile applications was purportedly assaulted by a cruel cab driver who was underrated by the passenger. To avenge for the incident, the driver waited at the place of picking and dropping that passenger for two days and lastly located the passenger. All this happened because the anonymity and privacy were compromised.

Fundamentally, for achieving deanonymization and extracting the information, analysis of privacy and anonymity is performed by the spending effort that would weaken the privacy of the users.

After analysis, outcomes are the potential aims to be achieved. Outcomes of analyzing privacy and anonymity are as follows:

- (a) ***Bitcoin Addresses Discovery:*** All the possible bitcoin addresses of an entity are discovered including the name of the person or the company.
- (b) ***Identity Discovery:*** All the potential distinguishing information, for instance, the name of the company or the person is procured that starts with a bitcoin address.
- (c) ***Mapping of IP Address with Bitcoin Address:*** Mapping of possible IP Addresses where the transaction was generated is done with the Bitcoin addresses.
- (d) ***Bitcoin Address Linking:*** New bitcoin addresses are suggested for use by the bitcoin users every time they get the new payment [18]. Due to this reason, each user has multiple bitcoin addresses. In this outcome, address belonging to the users are linked.
- (e) ***Mapping of Geo-locations with Bitcoin Address:*** Using the bitcoin address geographical location of the user can be obtained.

There may be a transition among the outcomes discussed above. For example, the bitcoin address that belongs to user can be discovered which can be linked to the other bitcoin addresses of the user. In the similar manner, mapping of bitcoin address can be done so that it is easier to obtain the identity or the geographical position of the user who possesses that address.

There are various ways to serve this purpose. Research shows that there some studies that use the ways while there may be numerous studies that just mention the methods but do not use them. The following are the studies that have either mentioned or applied the methods respectively:

- (a) ***Transacting:*** The address of bitcoin can be learned by performing transaction with other users to purchase goods, etc. For such transactions, the seller's bitcoin address must be known to the buyer. Therefore, if the seller wants to receive the payment, he/she must compulsorily provide his/her bitcoin address with the buyer. Therefore, it is easier for an entity to learn the bitcoin address of any entity or a person just by acting as a buyer assuming that such parties are in sales business. Transacting methods means active participation in the network. Reid and Harrigan [19] stated that transaction methods include active participation in the network and operating in money laundry services. In [20] Meiklejohn et al. named the transacting method as re-identification attack. In re-identification attacks, accounts are opened, and purchases are made from infamous Bitcoin merchants and services providers such as Mt. Gox and Silk Road.
- (b) ***Utilizing the Off-network Knowledge:*** All the Off-network data-sources which are publicly available can be used discover bitcoin addresses belonging some user entities or conversely. The websites used for donation that brings out the IP and key information were utilized by Reid and Harrigan [19]. In this process, identification of entities related theft of 25,000 BTC was done by employing off-network information. Ortega [21] collected around 4,000 bitcoin address from a well-known wired forum where the bitcoin addresses and the real-world locations can be declared by the bitcoin users. Ortega provided scripts

to link bitcoin addresses with the identities from the information provided by users and 1,825 different users were assigned to 4,000 Bitcoin addresses while some of the users include certain different addresses in their posts. From blockchain.info, an online forum that collects address specified in the signatures of the users in bitcoin forums such as bitcointalk, Meiklejohn et al. [20] collected more than 4,500 bitcoin addresses from the address tags and declared that this method is not decisive if compared to direct transacting. Fleder et al. [22] inspected that the bitcoin addresses from the forum bitcointalk signatures and tried for identifying around 2,320 users with a 2,404 address in less than 30 h. Spagnuolo et al. [23] introduced a framework for open blockchain analysis widely known as called BitIodine that utilizes the signatures and database knowledge from forums such as bitcointalk, bitcoin-OTC market, etc. Along with this, they utilized the knowledge on the physical currency that was originated by Casascius. They also utilized the knowledge of the infamous scammers for implicit detection of bitcoin users whose feedback is considerably unfavourable on bitcoin forums. Shareholders in BitFunder, a closed stock exchange was another source of information used by them. Bitnodes, a source from which the knowledge of the users that do not use hosting services can be fetched, was utilized by Biryukov et al. [24] to produce the list of active bitcoin servers for estimating the probability of the entry nodes going offline. Lische and Fabian [24] accumulated more than 223,000 distinctive IP addresses from ipinfo.io which were allotted for almost 15.8 million transactions. They also tried various other sources for IP addresses such as torstatus.blutmagie.de, etc.

2.4 Machine Learning Approaches to Price Prediction

Bitcoin is considered as a monetary asset which is traded using various exchanges such as a stock market. Various factors have been investigated by the researchers that are affecting the price of the bitcoin and the criterion causing the fluctuations using diverse investigative and empirical approaches. Research done by the authors [25–27] are the perfect examples to support the cause. With the advances in artificial intelligence, several machine learning (ML) and deep learning (DL) based models for bitcoin prices prediction are proposed [27–33]. Chen et al. [34] developed a model for forecasting the bitcoin price. This latent source model was implemented by Shah et al. [35]. Shah's model earned a remarkable return of 89% in 50 days with Sharpe ratio which evaluate the performance of stake along with adjusting for the risk. Testing period selected for the study presented the improvement of 33% utilizing the buy and hold strategy. Several unsuccessful efforts were done to recreate the same study independently. Geourgoula et al. [36] implemented sentiment analysis using Support Vector Machine (SVM) and investigated determinants of the price of bitcoin. Matta et al. [37] inspected association among the price of Bitcoin, views for bitcoin on Google Trends and tweets, concluded that there is weak to moderate correlation among price of bitcoin and both positive tweets on Twitter and

Google Trends views and concluded that these factors can be utilized as predictors. The study came with a limitation that the same used was only 60 days and the sentiments were considered as variable. In another study, Matta et al. [38] carried out the similar technique to predict the trading volume instead of predicting the price of bitcoin and concluded that views on Google Trends' were strongly correlated with the Bitcoin price. The sample collection covered a duration of just less than one year and data source was used for implementation purpose. Some researchers have applied wavelets to find similar results [39]. Kristoufek used the wavelet coherence analysis on bitcoin price and conclude that there is a positive correlation between search engine views, network hash rate, and mining difficulty with the bitcoin price. Greaves et al. [40] examined the bitcoin for price prediction employing Artificial Neural Network (ANN) and SVM and claimed an accuracy of 55%. They found that limited forecasting in the blockchain data since the price is governed by exchanges and the behavior is placed outside of the extent of the blockchain. Similarly, Madan et al. [41] implemented ML techniques like random forest, SVM, and Binomial GLM on the blockchain data and forecasted the bitcoin price with an accuracy of more than 97% with the limitation that the results were not cross validated. Due to which, the data may be overfitted and it cannot be guaranteed that model will generalize. The two prediction models have been presented by McNally et al. [27] and compared the model built on long short-term memory (LSTM) and recurrent neural network (RNN) with an autoregressive integrated moving average (ARIMA) model [41], which is widely used time-series forecasting model. The model for classification was developed which utilized bitcoin price information that predicts that the price of the bitcoin climbs up and down based on the history of previous bitcoin price. The authors of [27] demonstrated that model based on ARIMA does not stand against the models based on RNN and LSTM. Saad and Mohaisen [28] used the price information and the information from bitcoin blockchain like mining difficulty, total count of wallets, hash rate, unique addresses, etc., and utilized the highly correlated attributes for building the forecasting models. They also considered and studied various models developed on random forests, linear regression, neural networks, and gradient boosting. In addition to the blockchain information, Jang and Lee [32] gave thought to the blockchain information and macroeconomic attributes such as the exchange rates between major flat currencies, NASDAQ, S & P 500, Euro Stoxx 50, etc. Jang et al. [29], in their follow-up researches, put forward LSTM model with rolling window and manifested that the LSTM based model overshadowed the forecasting models based on SVM, linear regression, LSTM, and neural network. Likewise, Shintate and Pichl [33] showed that deep learning-based random sampling model proposed by them has overshadowed LSTM-based models.

2.5 Threats and Machine Learning Based Solution

Network infrastructure has existed since many decades. So as the malicious users referred to as malignant [42] exist in the network system. Such malignant users carry

out mendacious transactions in the network system which carries financial transactions. The main objective is to stop such malicious users from carrying out illicit acts [42] in the network so that the financial and transactional activities run properly. It is crucial to disclose suspicious conduct in bitcoin network because of the extremely fast-growing nature of the fraud. Attempts made by the client in participating in more than two transactions over the same bitcoin or the same number of bitcoins leads to double-spending attack. This is genuine due to propagation delay in broadcasting the pending payments across the bitcoin network, which results nodes being given non-validated transactions at different times [43]. Many research solutions and studies have been presented in the recent times to overcome anomaly detection. Such attempts present a broad range of techniques that includes ML methods as well. For instance, Smith, et al. in [44] utilized clustering methods so that malicious acts are seized in the network and classify licit users from malignant users.

In past, several studies have utilized ML techniques for addressing the security threats such as [45, 46]. In their research, Pham et al. [42], investigated the Bitcoin network for detecting the such users and the transactions which seems to be disreputable and used the methods of unsupervised learning including Mahalanobis distance, Unsupervised SV Machine and k-means clustering on the graphs generated by Bitcoin Network. Again, Pham et al. [45] by using machine learning based superior method to detected anomalies in bitcoin system by analysing clients and their transactions which is most dubious where a destructive behaviour is considered as a proxy for ambiguous activities. Monamo et al. [47] used kd-trees and trimmed k-means for detection of fraud over the bitcoin blockchain network. Also, Monamo et al. [46] in another research explored the application of trimmed k-means in the identification of fraudulent activities in transactions performed using Bitcoin and claims to detect more fraudulent transactions than the researches of same type and on same dataset. While Zambre et al. [48] identified potential rogue users in the Bitcoin network on the basis real reported robberies using k-means classification. Bartoletti et al. [49] proposed an automated exploration of Ponzi schemes on bitcoin, a classic fraud masqueraded, based on supervised learning algorithms. Zhdanova et al. [50] revealed fraud-chains by developing a strategy for detecting fraud chains in Mobile Money Transfer using machine learning based micro structuring techniques. Harlev et al. [51] presented the first-ever approach to reduce the anonymous behaviour of Bitcoin by using Supervised ML for prediction of the type of undetected entities while Yin et al. [52] analysed the Bitcoin ecosystem and presented the first-ever approximation of the dimension of cybercriminal entities by applying Supervised ML on 854 observations that are classified into 12 classes and out of which 5 classes were found to be related to cybercriminal acts and around of 100,000 unclassified observations. Hirshman et al. [53] applied Unsupervised ML algorithms for exploring anonymity in bitcoin transaction by clustering the dataset. Liu et al. [54] presented an approach based on ML to capture the double-spending attacks in transaction performed using bitcoin consisting of different immune-based blockchain nodes that deals with identification component. Bogner et al. [55] adopted machine learning for graphical threat detection and presented the human operators with a perceptive way to develop an understanding of blockchain through gathering the features of the system into group

of attributes that are depicted graphically. Remy et al. [56] tracked the acts of clients in bitcoin ecosystem using the community identification on low intensity network signals employing machine learning network analysis techniques. Kurtulmus et al. [57] proposed a by-product protocol that employs the globally dispersed behaviour of smart contracts along with ML based artificially intelligent problem solving to find the crowd-sourcing funds for research and to effectively present new marketplace without the requirement of mediator. Shaukat et al. [58] presented a ML based solution for an exhaustive investigation of ransomware dataset for providing a layered defence mechanism against the cryptographic ransomwares in Bitcoin & other cryptocurrencies. Baqer et al. [59] performed empirical analysis where a stress test based on clustering is deployed for detecting spam transaction in the Bitcoin cryptocurrency network. Holub et al. [60] proposed an NLP and ML based phishing ring DNS style identification scheme where the identification strategy relies on the observations of freshly launched and/or registered domains. Ermilov et al. [61] introduced an off-chain knowledge solution along with the knowledge for bitcoin address separation and categorisation for detecting and filtering errors in users' input data and therefore avoiding an unreliable Bitcoin usage model. Dey et al. [62] provided and methodology based on the intelligent software agents which handles stakeholders' activities in Bitcoin ecosystem for detecting anomalous behaviours employing the Super Machine Learning Algorithm along with algorithmic game theory. Portnoff et al. [63] designed a machine learning based classifiers for differentiating between advertisement posted by the same author and the several other authors along with a linking technique that utilizes leakages from the Bitcoin systems and sex advertisement onto Bitcoin transactions and public wallets.

2.6 Conclusion

This chapter introduces Bitcoin and the cryptographic mechanism ECDSA used in it. It then described the structure of Bitcoin Block which has block size, block header, transaction counter, and list of the transaction as fields, followed by the structure of the Bitcoin transaction which includes the fields for the version of the transaction, total inputs, and the outputs comprised in the transactions, transaction outputs & inputs and locktime. Adding a new Bitcoin for the electronic fund supply an important task of the mining process and hence the chapter also describes the mining process in which the mining nodes participate and compete to work for the difficult-to-solve cryptographic hash algorithm based mathematical puzzle and earns the transaction fees for all the transactions they have validated as a reward. The verification of a transaction is done against the criteria defined in a checklist which includes, data structure and syntax of the transaction, list of input and output, limitation in size of the transactions, etc. Machine learning and deep learning forms the important tools and techniques for solving classification and prediction problems and can be used specifically for the forecasting the price of Bitcoin. For the prediction, LSTM outperforms the other models like Deep Neural Network, Deep Residual Network, SVM, etc. Anonymity

and Privacy are the two faces of the same coin and are very crucial for transacting over the Bitcoin network. Lastly, this chapter lists most common security menace and their abnormal behaviors in bitcoin network with their solution employing ML techniques.

In future, deanonymization of bitcoin may be taken a step forward to prevent illicit acts like robbery, ransomwares, etc. Also, ML and DL techniques can be utilized for estimating the price of bitcoin and classifying the possible threats on the bitcoin network.

References

1. Dhulavvagol, P., Bhajantri, V., Totad, S.: Blockchain ethereum clients performance analysis considering e-voting application. *Procedia Comput. Sci.* **167**. 2506–2515 (2020). <https://doi.org/10.1016/j.procs.2020.03.303>
2. Rahouti, M., Xiong, K., Ghani, N.: Bitcoin concepts, threats, and machine-learning security solutions. *IEEE Access*, 1–1 (2018). <https://doi.org/10.1109/ACCESS.2018.2874539>
3. Herrera-Joancomartí, J.: Research and Challenges on Bitcoin Anonymity. 8872. https://doi.org/10.1007/978-3-319-17016-9_1. (2014)
4. Mastering Bitcoin. Andreas M. Antonopoulos
5. Yaga, D., Mell, P., Roby, N., Scarfone, K.: Blockchain Technology Overview (2019)
6. Xiao, Z., Xiao, Y.: Security and privacy in cloud computing. *IEEE Commun. Surv. Tutor.* **15**, 843–859 (2013). <https://doi.org/10.1109/SURV.2012.060912.00182>
7. Bradbury, D.: Anonymity and privacy: a guide for the perplexed. *Network Security* (2014). [https://doi.org/10.1016/S1353-4858\(14\)70102-3](https://doi.org/10.1016/S1353-4858(14)70102-3)
8. Eckhoff, D., Wagner, I.: Privacy in the smart city—applications, technologies, challenges and solutions. *IEEE Commun. Surv. Tutor.*, 1–1 (2019). <https://doi.org/10.1109/COMST.2017.2748998>
9. Ferrag, M.A., Maglaras, L., Ahmim: A privacy-preserving schemes for ad hoc social networks: a survey. *IEEE Commun. Surv. Tutor.*, 1–1 (2017). <https://doi.org/10.1109/COMST.2017.2718178>
10. Davenport, D.: Anonymity on the internet: why the price may be too high. *Commun. ACM* **45** (2002). <https://doi.org/10.1145/505248.505267>
11. Kelly, D., Raines, R., Baldwin, R., Grimala, M., Mullins, B.: Exploring extant and emerging issues in anonymous networks: a taxonomy and survey of protocols and metrics. *IEEE Commun. Surv. Tutor.* **14**, 1–28. <https://doi.org/10.1109/SURV.2011.042011.00080>
12. Chaum, D.: Untraceable electronic mail, return addresses and digital pseudonyms. *Commun. ACM* **24**, 84–88 (1981). <https://doi.org/10.1145/358549.358563>
13. Chaum, D.: cMix: anonymization by high-performance scalable mixing. *IACR Cryptol. ePrint Archive*, Rep. 2016/008 (2016)
14. Syverson, P., Goldschlag, D., Reed, M.: Anonymous connections and onion routing. In: *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy*, pp. 44–54 (1997). <https://doi.org/10.1109/SECPRI.1997.601314>
15. Dingledine, R., Mathewson, N., Syverson, P.: Tor: the second-generation onion router. In: *Proceedings of 13th Conference on USENIX Security Symposium (SSYM)*, vol. 13, pp. 21–37, San Diego, CA, USA (2004)
16. Moser, M., Bohme, R., Breuker, D.: An inquiry into money laundering tools in the Bitcoin ecosystem, pp. 1–14 (2013). <https://doi.org/10.1109/eCRS.2013.6805780>
17. Erdin, E., Zachor, C., Gunes, M.: How to find hidden users: a survey of attacks on anonymity networks. *IEEE Commun. Surv. Tutor.* **17**, 1–1 (2015). <https://doi.org/10.1109/COMST.2015.2453434>

18. A Taxi Driver Registered in ‘Bitaksi’ Application Plans to Murder a Passenger After Very Deserved Bad Review, Reddit: The Front Page of the Internet (2017). Accessed: 23 Jan 2018. [Online]. Available: <https://redd.it/61zczy>
19. Reid, F., Harrigan, M.: An analysis of anonymity in the bitcoin system. *Secur. Privacy Soc. Netw.* **3** (2011). <https://doi.org/10.1109/PASSAT/SocialCom.2011.79>
20. Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., Mccoy, D., Voelker, G., Savage, S.: A fistful of bitcoins: characterizing payments among men with no names, pp. 127–140 (2013). <https://doi.org/10.1145/2504730.2504747>
21. Ortega, M.S.: The Bitcoin transaction graph anonymity. M.S. thesis, Security of Information and Communication Technologies, Universitat Autònoma de Barcelona, Barcelona, Spain, 2013. Accessed: 14 Sept 2016 (2016)
22. Fleder, M., Kester, M., Pillai, S.: Bitcoin Transaction Graph Analysis (2015)
23. Spagnuolo, M., Maggi, F., Zanero, S.: BitIodine: Extracting Intelligence from the Bitcoin Network, vol. 8437, pp. 457–468 (2014). https://doi.org/10.1007/978-3-662-45472-5_29
24. Lischke, M., Fabian, B.: Analyzing the Bitcoin Network: The First Four Years. Future Internet, vol. 8 (2016). <https://doi.org/10.3390/fi8010007>
25. Alessandretti, L., Elbahrawy, A., Luca, M., Baronchelli, A.: Anticipating cryptocurrency prices using machine learning. *Complexity* **2018**, 1–16 (2018). <https://doi.org/10.1155/2018/8983590>
26. Corbet, S., Lucey, B., Urquhart, A., Yarovaya, L.: Cryptocurrencies as a financial asset: a systematic analysis. *Int. Rev. Fin. Anal.* **62** (2018). <https://doi.org/10.1016/j.irfa.2018.09.003>
27. McNally, S., Roche, J., Caton, S.: Predicting the Price of Bitcoin Using Machine Learning, pp. 339–343 (2018). <https://doi.org/10.1109/PDP2018.2018.00060>
28. Saad, M., Choi, J., Nyang, D., Kim, J., Mohaisen, A.: Toward characterizing blockchain-based cryptocurrencies for highly accurate predictions. *IEEE Syst. J.*, 1–12 (2019). <https://doi.org/10.1109/JSYST.2019.2927707>
29. Jang, H., Lee, J.: An empirical study on modeling and prediction of bitcoin prices with bayesian neural networks based on blockchain information. *IEEE Access*, 1–1 (2017). <https://doi.org/10.1109/ACCESS.2017.2779181>
30. Nakano, M., Takahashi, A., Takahashi, S.: Bitcoin technical trading with artificial neural network. *Phys. A Stat. Mech. Its Appl.* **510**, 587–609 (2018). <https://doi.org/10.1016/j.physa.2018.07.017>
31. Rebane, J., Karlsson, I., Denic, S., Papapetrou, P.: Seq2Seq RNNs and ARIMA models for Cryptocurrency Prediction: A Comparative Study (2018)
32. Huisu, J., Lee, J., Ko, H., Lee, W.: Predicting bitcoin prices by using rolling window LSTM model. In: Proceedings of the KDD Data Science in Fintech Workshop, London, UK (2018)
33. Shintate, T., Pichl, L.: Trend prediction classification for high frequency bitcoin time series with deep learning. *J. Risk and Fin. Manage.* **12**, 17 (2019). <https://doi.org/10.3390/jrfm12010017>
34. Chen, G., Nikolov, S., Shah, D.: A latent source model for nonparametric time series classification. *Advances in Neural Information Processing Systems* (2013)
35. Shah, D., Zhang, K.: Bayesian regression and Bitcoin. In: 2014 52nd Annual Allerton Conference on Communication, Control, and Computing, Allerton (2014). <https://doi.org/10.1109/ALLERTON.2014.7028484>
36. Giaglis, G., Georgoula, I., Pournarakis, D., Bilanakos, C., Sotiropoulos, D.: Using time-series and sentiment analysis to detect the determinants of bitcoin prices. *SSRN Electronic Journal*. [https://doi.org/10.2139/ssrn.2607167\(2015\).](https://doi.org/10.2139/ssrn.2607167(2015))
37. Matta, M., Lunesu, Maria I., Marchesi, M.: Bitcoin Spread Prediction Using Social and Web Search Media (2015)
38. Matta, M., Lunesu, M.I., Marchesi, M.: The Predictor Impact of Web Search Media on Bitcoin Trading Volumes.<https://doi.org/10.5220/0005618606200626>
39. Kristoufek, L.: What are the main drivers of the bitcoin price? Evidence from wavelet coherence analysis. *PLoS ONE* (2014). <https://doi.org/10.1371/journal.pone.0123923>
40. Alex, G., Au, B.: Using the bitcoin transaction graph to predict the price of bitcoin (2015)

41. Madan, I., Saluja, S., Zhao, A.: Automated bitcoin trading via machine learning algorithms (2015)
42. Pham, T., Lee, S.: Anomaly Detection in the Bitcoin System—A Network Perspective (2016)
43. Xu, J.: Are blockchains immune to all malicious attacks? *Financial Innovation* **2** (2016). <https://doi.org/10.1186/s40854-016-0046-5>
44. Smith, R., Bivens, A., Embrechts, M., Palagiri, C., Szymanski, B.: Clustering approaches for anomaly-based intrusion detection. In: *Proceedings of Intelligent Engineering Systems Through Artificial Neural Networks*, pp. 579–584 (2002)
45. Pham, T., Lee, S.: Anomaly Detection in Bitcoin Network Using Unsupervised Learning Methods (2016)
46. Monamo, P., Marivate, V., Twala, B.: Unsupervised learning for robust Bitcoin fraud detection, pp. 129–134 (2016). <https://doi.org/10.1109/ISSA.2016.7802939>
47. Monamo, P., Marivate, V., Twala, B.: A Multifaceted Approach to Bitcoin Fraud Detection: Global and Local Outliers, pp. 188–194 (2016). <https://doi.org/10.1109/ICMLA.2016.0039>
48. Zambre, D., Shah, A.: Analysis of bitcoin network dataset for fraud. Unpublished Report (2013)
49. Bartoletti, M., Pes, B., Serusi, S.: Data Mining for Detecting Bitcoin Ponzi Schemes, pp. 75–84 (2018). <https://doi.org/10.1109/CVCBT.2018.00014>
50. Zhdanova, M., Repp, J., Rieke, R., Gaber, C., Hemery, B.: No Smurfs: Revealing Fraud Chains in Mobile Money Transfers (2014). <https://doi.org/10.1109/ARES.2014.10>
51. Harley, M., Yin, H., Langenheldt, K., Mukkamala, R. R., Vatrapu, R.: Breaking Bad: De-Anonymising Entity Types on the Bitcoin Blockchain Using Supervised Machine Learning (2018). <https://doi.org/10.24251/HICSS.2018.443>
52. Yin, H., Vatrapu, R.: A first estimation of the proportion of cybercriminal entities in the bitcoin ecosystem using supervised machine learning, pp. 3690–3699 (2017). <https://doi.org/10.1109/BigData.2017.8258365>
53. Hirshman, J., Huang, Y., Macke, S.: Unsupervised approaches to detecting anomalous behavior in the bitcoin transaction network, Technical report, Technical report, Stanford University (2013)
54. Liu, Z., Zhao, H., Chen, W., Cao, X., Peng, H., Yang, J., Yang, T., Lin, P.: Double-Spending Detection for Fast Bitcoin Payment Based on Artificial Immune, pp. 133–143 (2017). https://doi.org/10.1007/978-981-10-6893-5_10
55. Bogner, A.: Seeing is understanding anomaly detection in blockchains with visualized features. In: *Proceedings of the International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the International Symposium on Wearable Computers*, pp. 5–8. ACM (2017)
56. Cazabet, R., Rym, B., Latapy, M.: Tracking Bitcoin Users Activity Using Community Detection on a Network of Weak Signals, pp. 166–177 (2018). https://doi.org/10.1007/978-3-319-72150-7_14
57. Kurtulmus, A., Daniel, K.: Trustless Machine Learning Contracts; Evaluating and Exchanging Machine Learning Models on the Ethereum Blockchain (2018)
58. Shaukat, S., Ribeiro, V.: RansomWall: A layered defense system against cryptographic ransomware attacks using machine learning, pp. 356–363 (2018). <https://doi.org/10.1109/COMSNETS.2018.8328219>
59. Baqer, K., Huang, D., Mccoy, D., Weaver, N.: Stressing Out: Bitcoin “Stress Testing”, vol. 9604, pp. 3–18 (2016). https://doi.org/10.1007/978-3-662-53357-4_1
60. Holub, A., O’Connor, J.: Coinhoarder: Tracking a Ukrainian Bitcoin phishing ring DNS style. In: *APWG Symposium on Electronic Crime Research (eCrime)*, 2018, pp. 1–5. IEEE (2018)
61. Ermilov, D., Panov, M., Yanovich, Y.: Automatic Bitcoin Address Clustering, pp. 461–466 (2017). <https://doi.org/10.1109/ICMLA.2017.0-118>
62. Dey, S.: Securing Majority-Attack in Blockchain Using Machine Learning and Algorithmic Game Theory: A Proof of Work, pp. 7–10 (2018). <https://doi.org/10.1109/CEEC.2018.8674185>
63. Portnoff, R., Huang, D., Doerfler, P., Afroz, S., Mccoy, D.: Backpage and Bitcoin: Uncovering Human Traffickers, pp. 1595–1604 (2017). <https://doi.org/10.1145/3097983.3098082>

64. Biryukov, A., Khovratovich, D., Pustogarov, I.: Deanonymisation of clients in bitcoin P2P network. In: Proceedings of the ACM Conference on Computer and Communications Security (2014). <https://doi.org/10.1145/2660267.2660379>
65. Box, G., E., P., Jenkins, G., Reinsel, G., Ljung, G.: Time Series Analysis: Forecasting and Control (2016). <https://doi.org/10.2307/2284112>

Chapter 3

Blockchain 1.0 to Blockchain 4.0—The Evolutionary Transformation of Blockchain Technology



Pratyusa Mukherjee and Chittaranjan Pradhan

Abstract Blockchain is a propitious technology that has gained immense popularity and tractions. It has tremendously revolutionized the peer-to-peer information exchange by combining cryptographic principles with decentralization, immutability and transparency. The term blockchain has been coined from its fundamental feature of being a distributed ledger where each record or block is secured and bound to its successive blocks through hash functions thus resulting in this chain of blocks. This chapter first gives the historical background of this expeditious technology. It then proffers a description of the basic terminologies in blockchain, it's types, basic structure of block and different consensus models popularly known. The prime emphasis of this chapter is to bestow an extensive study of the chronological evolutions in Blockchain Technology by highlighting the nitty-gritty of each generation in detail. It also illustrates a parameter wise differences amidst the several generations in terms of their principle areas, consensus models used, utility of smart contracts, the energy and cost requirements and execution speed and scalability. In the end, a Blockchain in Supply Chain Management test case has also been elaborated in this chapter.

Keywords Blockchain · Distributed ledger · Bitcoin · Ethereum · Hyperledger fabric · Cryptographic hash · Consensus models

3.1 Introduction

The assurance of CIA triad comprising of confidentiality, integrity and availability is the prime emphasis of any cryptosystem to provide a holistic security approach to safeguard all critical and sensitive data. Data theft has been a major cybersecurity issue that threatens these primary purposes of cybersecurity. Over the years, several technologies have been proffered to eliminate this issue where Blockchain Technology [1–4] is the latest inclusion. Data while transit as well as storage is vulnerable to many plagiarism and pilferage situations that makes tracing back the criminal and

P. Mukherjee (✉) · C. Pradhan

School of Computer Engineering, KIIT Deemed to be University, Bhubaneshwar, India

original data extremely strenuous. Blockchain Technology abolishes such scenarios to great extent. A blockchain [5] can be interpreted as a distributed database that incorporates every event or transaction, executed and shared amongst the concerned parties. Each transaction is vehemently verified and once an information is entered, it can never be erased without the consent of the involved parties.

Blockchains are thus like public registers where every transaction is accumulated as a series of blocks. They are essentially based on the concept of Cryptography and Distributed Systems. Each successive block stores the hash [6, 7] of the its preceding block. Thereby, if any modification is made into the previous block, its corresponding hash is modified and hence here is a mismatch with the one stored in the successive block. This features makes blockchain tamperproof and the contaminated block can be easily identified. Also blockchains eliminate the need of any central authority for any kind of validation. Another important feature of blockchain is its distributed nature [5, 8] where its several copies are stored by different parties over different networks which makes any modification quite tedious and further enhances the security of blockchains.

Blockchain Technology first came into limelight with the inception of Bitcoin by Satoshi Nakamoto [9] back in 2008 and has been transfigured to greater extents since then. The first generation of Blockchain, Bitcoin [1, 10, 11] was a decentralized peer-to-peer digital currency which eliminated the presence of any central authority such as banks or intermediaries. To address the trust issues amidst the participants, Bitcoin implements consensus models [12] to ensure the authenticity and integrity of the users. Due to the limited functionality of the first generation in only financial sector, further advancements were made to adopt Blockchain for other domains as well. Ethereum [13], the second generation technology has immense application for crowdsourcing through its trustworthy smart contact clauses. A smart contract [14] is a an autogenously assertive contract where the compliance between buyers and sellers are directly converted into lines of codes across a distributed, decentralized blockchain network. Hyperledger [15] is another advancement which provides higher modularity and versatility than Ethereum due to its permissioned architecture. The third generation Blockchain has inbuilt verification mechanism and more efficient faster and cheaper than previous versions. Combining Artificial Intelligence with Blockchain Technology has already paved way for the fourth generation of blockchain as well.

This chapter first gives the historical background of this expeditious technology. It then proffers a description of the basic terminologies in blockchain, it's types, basic structure of block and different consensus models popularly known. The prime emphasis of this chapter is to illustrate a thorough study of the chronological evolutions in Blockchain Technology by highlighting the nitty-gritty of each generation in detail. It also illustrates a parameter wise differences amidst the several generations in terms of their principle areas, consensus models used, utility of smart contracts, the energy and cost requirements and execution speed and scalability. In the end, a Blockchain in Supply Chain Management test case has also been elaborated in this chapter.

3.2 Fundamentals of Blockchain

The related work section first delves into the historical background of Blockchain Technology. It then puts forward the important terminologies related to it. The structure of a block is described in detail. Next the types of Blockchain are elaborated. The nitty-gritty of successive generations of Blockchain Technology are discussed in separate sections along with the works of several researchers in brief.

3.2.1 *Historical Background*

In 1980s, advent of crypto bound signatures revolutionized exchange of data amidst the sender and receiver. In 1989, DigiCash [16, 17] exchange via email became pretty popular. In the successive years, the usage of digital documents became common and major emphasis is laid on assuring their authentication, efficiency and reliability. In 1991, Haber and Stornetta [18–20] first suggested the concept of time stamping a digital document to ensure they cannot be backdated and are tamperproof. In successive years, incorporation of Merkle Trees allowed collection of several digital documents into a block which enhanced their security. In the late 90s, usage of digital currencies [21] became quite predominant.

Digital currencies are intangible and only available electronically, unlike physical currencies. Transactions using digital currency cannot be undone in future and they do not need any central authority, as a result of which chances of fraudulent transactions are eliminated. They are also faster and cheaper than physical cash transfers. Szabo [22] introduced the concept of “bit gold”, a decentralized digital currency in 2005 based on different cryptographic elements. In Szabo’s system [23], Bit gold begins by generating a public challenge string while using a benchmark function. The user then generates a “proof of work [24]” string from the same function, and every details associated to the transaction are stored in a title registry which is an immutable record. The last bit of string is responsible for creating the next set of strings and thus Bit gold is non-fungible.

Finney [25] proffered a system called “RPoW, Reusable Proof Of Work”, which operated by obtaining a non-exchangeable Hashcash [26] based proof of work token. In reciprocation, a RSA-signed token is created which is exchangeable amongst the users.. This abolished the probability of denial of service. RPoW also got rid of double spending problem. It tracks the possessionhip of tokens on an authentic and credible server that enables every user to verify the truthfulness and integrity in real time.

Drawing ideologies from the existing digital currency concept and fundamentals of cryptography, in 2008 Satoshi Nakamoto brought the concept of Blockchain Technology into limelight by implementing the first blockchain as the public ledger for transactions made using “Bitcoin [9]”. Since its inception, Blockchain has been garnering the attention of several researchers for its immensely secure features.

3.2.2 Basic Terminologies in Blockchain

Blockchain is basically a public distributed database which holds the encrypted ledger. Ledger [27] means a file that keeps on growing constantly. Blockchain principally contrasts from a database because of its decentralization feature. Each and every record in a database stored in a central server. On the contrary, in a blockchain every participant retains a copy of each record. A block [28] is a data structure consisting of most recent and previously never occurred or included records. The aboriginal block of a blockchain is termed as the genesis [29]. Each of the successive blocks incorporate the hash [30] of its preceding block. A hash is non-invertible which means a hash can be calculated from a particular input but not the vice versa. Also, hash is collision resistant. It is tedious to retrieve two different inputs resulting in the same hash value. Hash incorporation into Blockchain Technology makes it highly secure because even a negligible change in a block hugely differs its hash which is then reflected in all the successive blocks. As a result of this, any kind of intrusion is strongly noticed. Figure 3.1 demonstrates the block diagram of a blockchain.

Blockchain is thus keeps a time-stamped, protected, chronometric and immutable. Transactions are the basic building blocks of a blockchain system. This feature of blockchain finds adequate application in several financial as well as non-financial organizations.

Any user or device within the Blockchain is termed as a node. Specific nodes that perform block verification process are coined as Miners [31]. Each Blockchain has certain set of rules to carry out different operations and these rules are termed as Consensus [32, 33]. Every block in a blockchain is visible to each participant in the network, but they cannot replace, modify or add new blocks unless verified and validated by at least 51% of the peers. This is termed as Proof of Consensus [12]. Proof of Work [34] additionally mandates that for a new node to become a participant or for any existing node to add or modify a block, they also need to find the solution to specific laborious mathematical puzzles to prove their eligibility. Proof of Stake [35] states that every participating node has to put something at stake. For example, each have to prove their identity and validate themselves. Since an adversary will never

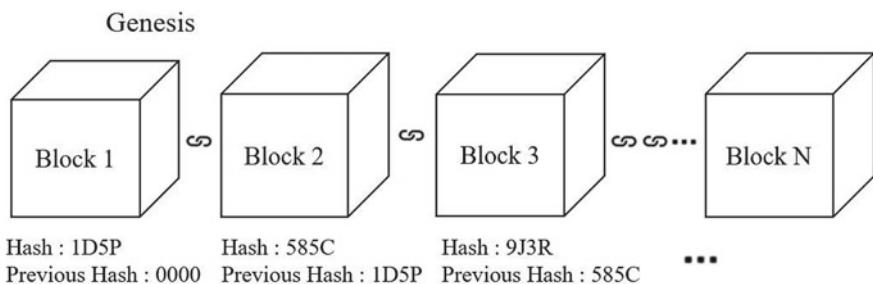


Fig. 3.1 Block diagram of blockchain

successfully pass these clauses he cannot interfere into a blockchain thus, making it safe and private.

3.2.3 Structure of a Block

The structure of a block can be assumed to be divided into two sections, one comprising of the header with all metadata and the other consisting of all the transaction details. Figure 3.2 illustrates the structure of block.

First of all, the metadata consists of Previous Hash which is used to chain the current block with its preceding block in the blockchain.

The second set of meta data comprises of the information pertaining to mining competitions such as Timestamp, Difficulty and Nonce. Mining [36] in Blockchain is performed by high end computers that solve complex mathematical problems to receive rewards in return, thus completing the verification procedures. Timestamp gives the creation time details for a particular block thus eliminating the denial of

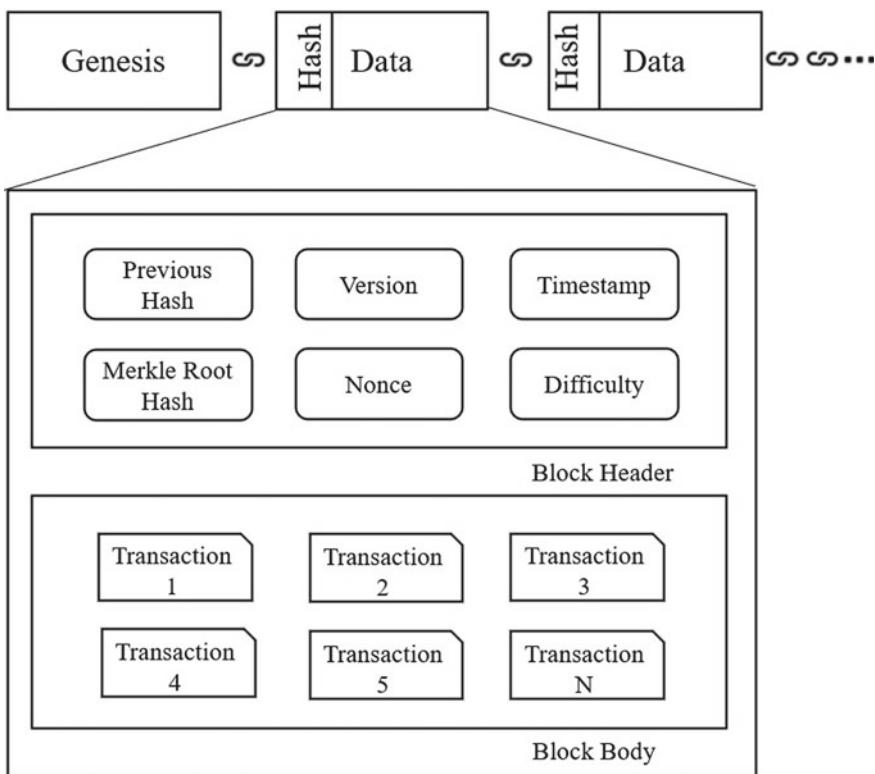


Fig. 3.2 Structure of a block

service scenarios. Difficulty gives the complexity that was used to create this block. In cryptography, nonce [37] is an arbitrary number that can be used only once in the entire communication. In Blockchain, nonce is the number that miners are competing for. Successfully mining means that the winning miner was the first to guess the nonce, which is a string of random numbers affixed to the hashed contents of the block, which is again rehashed.

The final metadata includes the Merkle Tree root which a data structure to summarize all the transaction details in the corresponding block in an efficient manner.

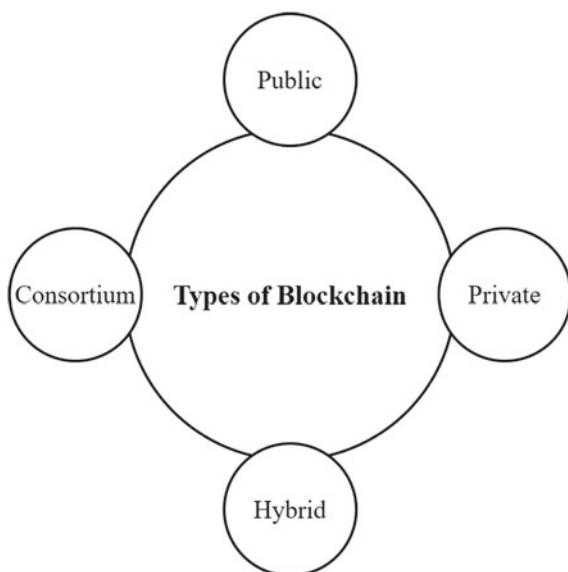
In order to identify a block, users can either use the block hash or the block height [38]. Block height is described as the number of blocks before it. Thus it can be calculated as the length of the block minus one. The block height of the entire blockchain is obtained from the height of the most recent block or the highest block in the chain.

Every first and unique transaction carried out by a miner is termed as the “Coinbase Transaction”. The miners utilize it to collect their rewards for every correct solutions. Other transaction fees collected by them are also added to this Coinbase Transaction.

3.2.4 Types of Blockchain

The different types of Blockchain are categorized on the basis of their applications. Primarily the two broad types of Blockchain are Public and Private Blockchain. Two variation also exist like the Consortium and Hybrid Blockchain. Figure 3.3 illustrates

Fig. 3.3 Types of blockchain



the types of Blockchain in a nutshell.

Public Blockchain [39–41] is are the most simple and publicly accessible blockchains. They are open source, non-restrictive, fully distributed, decentralized and permission less. Any entity with internet access can sign into a Public Blockchain to become an authorized participant and become a user, miner or developer. The contents of the blockchain are readily available to every node with complete transparency. The major benefit of Public Blockchain is its uncontrollability or not granting full authority to any particular node. All the nodes adhere to the consensus mechanisms to ensure the security of the public blockchain. The most common use of Public Blockchains are for mining activities and cryptocurrency interchange. Thus, the most common public blockchains are Bitcoin, Ethereum and Litecoin blockchains. Figure 3.4 represents a fully distributed Public Blockchain where every device has full access to the blockchain and can easily interact with each other.

Private Blockchain [42, 43] is restrictive, centralized, permissioned and operate only in closed networks such as any organization where only selected members are allowed to participate. They have a central authority who fully controls the authorization, participation and accessibility. Participants of that same organization mandatorily require the consent of the central authority to join the Private Blockchain. The contents of the blockchain are only available to the permitted participants and any Updation or modification into the blockchain also necessitates the permission of the authority. They are thus more secured and controlled than Public Blockchains and find commonly deployed in e-voting, supply chain management etc. Hyperledger and R3 Corda are popular examples of a Private Blockchain. Figure 3.5 gives the Block Diagram of a Private Blockchain.

Fig. 3.4 Fully distributed and decentralized public blockchain

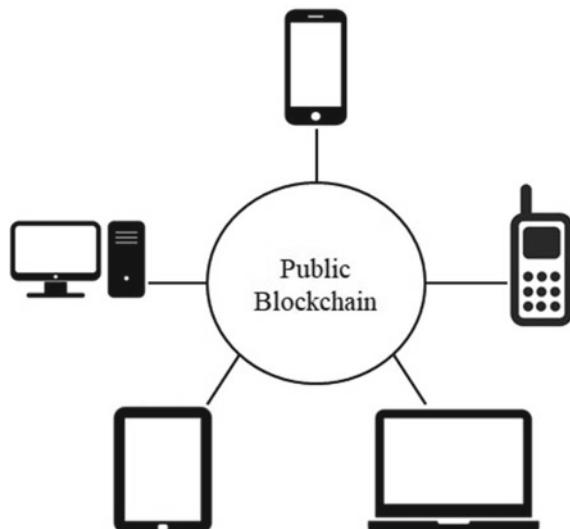
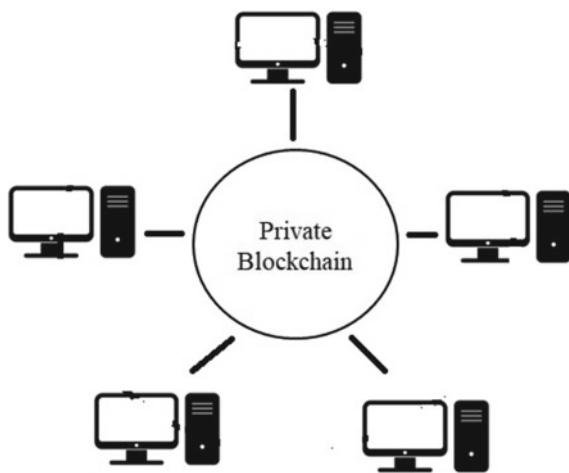


Fig. 3.5 Centralized private blockchain



Consortium Blockchain [44–46] is a specialized category of Private Blockchain where multiple organizations control and manage the blockchain instead of only one. Thus it has the similar benefits as that of a Private Blockchain. Since it is a collaborative network, it is more productive and efficient both collectively as well as individually. Consortium blockchains are typically used by banks, government organizations, etc. Figure 3.6 illustrates a Consortium Blockchain. Examples of consortium blockchain are; Energy Web Foundation, R3, etc.

Fig. 3.6 Consortium blockchain

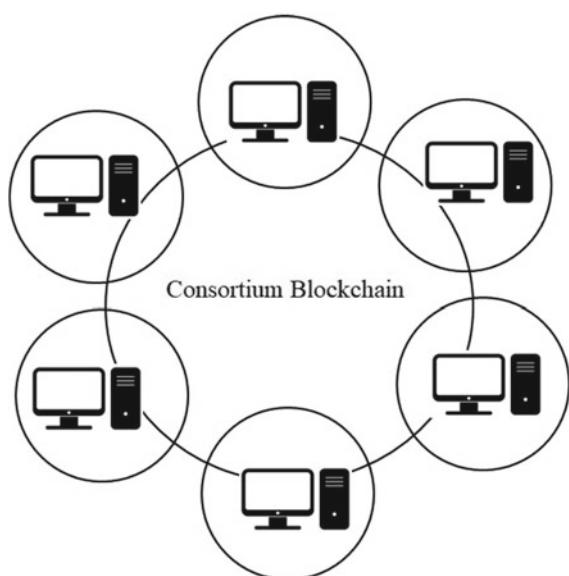


Table 3.1 Comparison between the most prominent types of blockchain

Parameter	Public	Private	Consortium
Permission	Permission less	Permissioned	Permissioned
Decentralization	Fully decentralized	Centralized	Less centralized
Participants	Anybody	Permissioned and known entities	Permissioned and known entities
Authority	Anyone	Single central authority	Multiple central authority
Reading Rights	Anyone	Invited users	Depends on scenario
Writing Rights	Anyone	Approved users	Approved users
Consensus	PoS/PoW	Multiparty consensus	Multiparty consensus
Speed	Slow	Fast	Fast

Table 3.1 highlights the comparison amidst these three prominent types of Blockchain.

Hybrid Blockchains [47–49] are combination of Public and Private Blockchains. It incorporates the privacy and permissioned facilities of Private Blockchain and the simplicity, flexibility and transparency of Public Blockchains. Participants of a Hybrid Blockchain can control the authority and accessibility of the data stored in it. Dragonchain is the most common example of a Hybrid Blockchain.

3.3 The Evolutionary Transformation of Blockchain 3.1

Till date Blockchain Technology has undergone four major evolutions and each of these has been discussed in the following sections.

3.3.1 *Blockchain 1.0*

The first generation of Blockchain, Blockchain 1.0, originated from the concept of Distributed Ledger Technology (DLT) [50–52]. Distributed ledger is a database that is consensually shared amongst several participants thus enabling public witnesses to eliminate double spending scenarios. The most prominent application of DLT was cryptocurrency where Bitcoin [53] played a pivotal role. Bitcoin thus became the “cash for the internet” and paved way for “Internet of Money [54]”. After its launch in 2009, Bitcoin proved its stability, reliability, efficiency, simplicity, independency and security to keep a track of transaction records and transfer authority of these records from one user to another directly. It essentially utilizes consensus and mining mechanisms to exchange cryptocurrencies. Figure 3.7 gives the overall working with Bitcoins. A real life scenario where Alice wants to send 1 Bitcoin (BTC) to Bob is portrayed in Fig. 3.8.

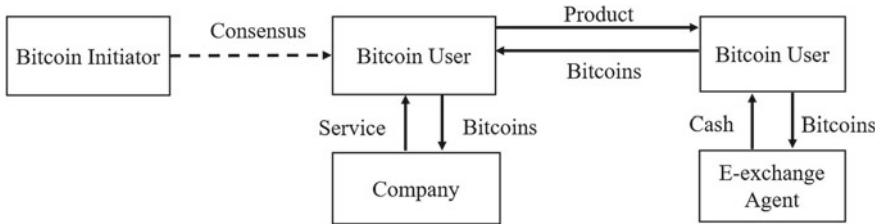


Fig. 3.7 Working model using bitcoins

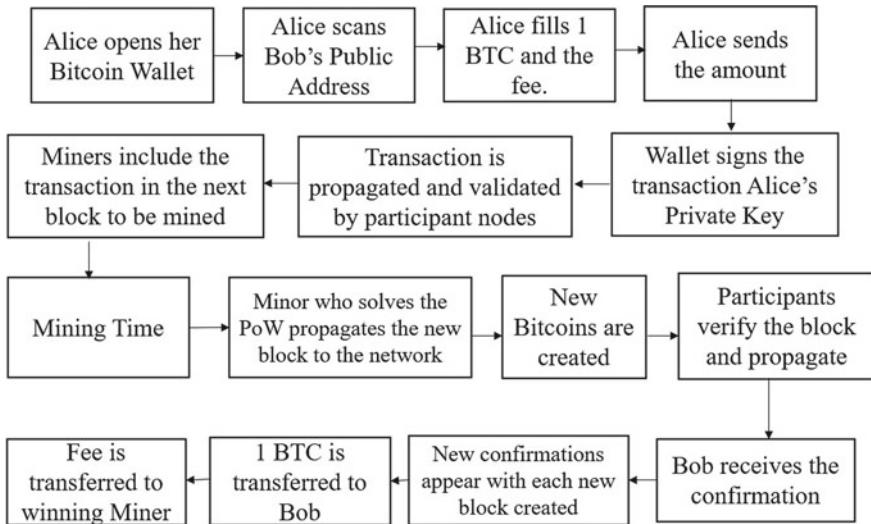


Fig. 3.8 Bitcoin transaction lifecycle

Swan [55] highlighted the utility of Bitcoin being deployed as a cryptocurrency in applications pertaining to cash transfer, remittance and digital payments whose generation and transfer is solely based on encryption mechanisms and works independent of any central bank. Thus Bitcoin has the potential to prove to be a blueprint of a new economic policy. Böhme et al. [56] thoroughly studied the Bitcoin design principles, its underlying technologies and processes, the various uses of Bitcoin for consumer payments as well as the probable risks associated with it. Narayanan et al. [57] elaborated the mechanics of Bitcoin, their mining and regulations in their work.

Decker and Wattenhofer [58] analyzed the information propagation in Bitcoin network by using multi-hop broadcasting to update the ledger. They also claimed that this mode of propagation led to delays thus resulting in inconsistencies and blockchain forks [59]. Bitcoin is largely based on mining mechanisms which involves solving algo-puzzles to verify monetary transactions in order to receive cryptocurrencies as rewards. O' Dwyer and Malone [60] studied energy consumption in Bitcoin mining in details. They carefully inspected when Bitcoins prove to be profitable in

comparison to the energy consumed while mining and suggested special hardware modifications to achieve maximum profits.

Antonopoulos [61] explained in detail how Bitcoin works and its detailed implementation along with the mining and consensus mechanisms. Velde [62] backed the technical and conceptual accomplishments of Bitcoin to be inculcated in existing financial sectors because of its freedom from any central authority intervention. The fact that anonymity and decentralization of Bitcoin makes it a potential game changer in micropayments and virtual worlds e-commerce was suggested by Grinberg [63].

Blockchain 1.0 thus has myriads of advantages over the traditional payment mechanisms such as low transactional costs and relative anonymity in transactions. Bitcoins will never be out of market as there have an adequate supply. Bitcoins apart from eliminating double spending, also remove counterfeiting by enabling secure trackable and transparent transactions.

Amidst all its achievements, Bitcoins also have some major setbacks. The first generation of Blockchain essentially utilizes the Proof of Work (PoW) consensus mechanism that necessitates the computation of complex mathematical puzzles. Due to the complexity involved, PoW is time-consuming and uses colossal amounts of energy comparable to the overall profits earned. In this, the approval of transaction is also pretty slow than electronic channels. Research shows that Blockchain 1.0 can handle at most seven transactions per second thus having a substantially slow throughput. Conti et al. [64] studied the security and privacy issues of Bitcoin in details. Eyal and Sirer [65] highlighted that Bitcoin is extensively vulnerable to Selfish Mining that is practiced by colluding miners to earn more revenues than their mining capabilities. Thus ultimately Bitcoin proceeds towards a centralized scheme fully under the control of these selfish miners. Androulaki et al. [66] claimed that behavior-based clustering techniques can unravel the real identities of the otherwise anonymous Bitcoin users up to 40%. Another vital drawback of Satoshi's idea of Blockchain 1.0 is that it utilizes only 1 megabyte (MB) blocks of information on bitcoin transactions. The last and most notable shortcomings of Blockchain 1.0 are their inability to support Smart Contracts and other application sectors instead of financial utilities.

3.3.2 *Blockchain 2.0*

The wasteful mining and poor scalability of the first generation Blockchain prompted Buterin [67] to extend the concept of Blockchain beyond currency. This led to the advent of second generation of Blockchain i.e. Ethereum which is based on new concepts of smart contracts along with Proof of Work consensus mechanisms.

Smart Contracts [68] are autonomous self-managing computer programs that execute automatically on the basis of predefined clauses between two parties. These contracts are impossible to be hacked or tampered with. So Smart Contracts [69] largely reduce the cost of verification, execution, and fraud prevention and enable transparent contract definition.

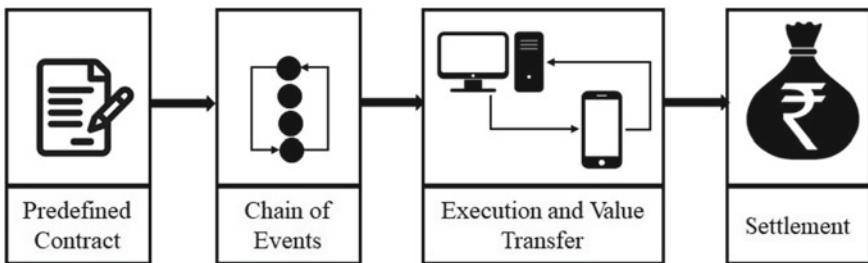


Fig. 3.9 Working of smart contract

Figure 3.9 shows how smart contracts work. The first step is formulation of the contract between two parties. It involves the terms, rules and conditions of the agreement has to be accepted by the two counterparts and translated into a code. No changes can be made into the contract without the consent of the involved parties. The smart contract is then deployed into the blockchain. As soon as the events mentioned in the contract occur, the code automatically executes. Practical example of such events can be expiration of an insurance policy or delivery of goods. Once the code execution is over, the contract will automatically transfer the value to the pertinent receiver. The settlement is thus completed instantly, securely and efficiently. This transfer is also recorded into the blockchain.

Ethereum [67, 70] utilizes the implementation of smart contracts into Blockchain. It's a community-built technology behind another cryptocurrency Ether (ETH) [71] having an array of applications in almost every field such as electronic voting, real estate and trading. In the Ethereum, instead of contesting for bitcoins, miners compete for Ether [72]. There is another type of token involved in Ethereum which is utilized to reward miners for including transactions in their block, termed as gas. Every smart contract execution necessitates a particular amount of gas to be sent along for alluring miners to incorporate it into the blockchain.

Good [73] discussed the protocol of Ethereum and fundamentals of smart contract to autonomously enforces regulation for such interactions. Dannen [13] gave a thorough insight into Solidity which is the high level programming language to implement smart contracts. Antonopoulos and Wood [74] gave the step by step guide to build a smart contract using Solidity. They explained how to chose the appropriate Solidity version, downloading and installing it, writing the simplest smart contract, compiling it with the Solidity Compiler and finally deploying it into the Blockchain.

Extensive research is being carried out to utilize Ethereum in several non-financial sectors. Yavuz et al. [75] suggested a secure e-voting system by using the Ethereum Blockchain. Ethereum wallet or simple android mobile phones are used by users to cast their votes. After the election is held, Blockchain 2.0 is used to store the ballots and votes. Their proposal proved to be more efficient, reliable, cheap and transparent to conduct e-voting. Rooksby and Dimitrov [76] proposed a Blockchain system based on Ethereum that can be used by a university to evaluate the performance of students, store and manage their grades and reward them cryptocurrencies if performance is

up to the mark. Internet of things (IoT) has tremendous utility in designing Smart Homes which are fully automated to provide highest comfort to the residents. Aung and Tantidham [77] implemented an Ethereum based Smart Home Scheme to control access policies, data storage and flow to eliminate imposters impersonating actual residents and stealing secretive information. Adhikari [78] proffered a Smart Healthcare system that incorporates the concepts of Ethereum to provide a secure, flexible and more reliable schemes than traditional ones. Shih et al. [79] proposed production and marketing of organic vegetables by using Ethereum. This methodology ensures the authenticity of the production quality as well as the sales record.

Since Ethereum is largely based on smart contracts, they have an array of advantages. Smart contacts are quite accurate and store each clauses explicitly thus Ethereum is very minutely defined. The contract is fully transparent to all involved parties. The execution speed of smart contracts is very fast up to 15 transactions per second and eliminates several middle men in any kind of application.

However, smart contracts also pose several difficulty on the users because they are extremely tricky to write [80]. Any mistakes while writing the contract can lead to unintended adverse effects [81]. Once a mistake in the code begins to be exploited, there is no efficient way to stop it other than obtaining a consensus and rewriting the entire underlying code [82]. Thus to achieve maximum benefits of Ethereum, it is essential to formulate and deploy the smart contract correctly.

3.3.3 *Blockchain 3.0*

The major setback of Blockchains 1.0 and 2.0 are that they are not scalable at all, mostly based on Proof of Work and take hours to confirm transactions. All this led to the birth of the current generation of Blockchain called Blockchain 3.0 that aims to make cryptocurrencies globally viable. Apart from smart contracts, the third generation of Blockchain mainly involves Decentralized Apps (dApps) [83]. They are digital programs that run on a Blockchain network of computers instead of a single computer and thus are beyond the purview of any central authority. This generation is hence capable of promoting inter chain transactions with aid of techniques such as sharding [84]. Sharding implies each node of Blockchain contains only a part of the data on it and not the complete information. This spreads the load and makes the system for efficient and intrusion proof. Blockchain 3.0 also utilizes Proof of Stake and Proof of Authority [85] consensus mechanisms to enable enhanced speed and computing power for smart contracts with no separate transaction fees. Although Blockchain 3.0 is in its inception but aims to improve the scalability, interoperability, privacy and sustainability of previous generations because they are designed on the “FFM” concept which is the acronym for Fast, Feeless and Minerless. Blockchain 3.0 hence eliminates the dependency on Miners to verify and authenticate transactions and instead use inbuilt mechanisms for the same. They are thus extremely fast to allow thousands of transactions per second unlike their preceding generations.

Blockchain 3.0 paved way for several platforms each with their unique advantage to encourage Blockchain usage in every-day life. ICON projects [86] aims to connect separate Blockchains together such that every transaction between these blockchains is verified by a ledger itself. Thus it tries to provide a high usability, scalability and reliability by eliminating any central authority or need of any transaction fees. Another third generation Blockchain was established using DAG (Directed Acyclic Graph) protocols [87, 88] to design no block, no chain and no miner yet public distributed ledger platform such as IOTA [89]. Another popular Blockchain 3.0 platforms are Cardano [90] which has its own cryptocurrency ADA and aims to improve all problems with Ethereum. Aion [91] is another third generation Blockchain network that aims to support basic blockchain architectures along with cross chain interoperability.

The merits of Blockchain 3.0 include no single controlling authority thereby no single point of failure. dApps don't reside on a particular IP address hence adversaries cannot tamper with the data and security is enhanced. The have extremely high transaction speed.

However, the thirds generation of Blockchain also has several disadvantages like bug fixing or updating due to their decentralized nature. The consensus mechanisms applied are comparatively complicated.

3.3.4 *Blockchain 4.0*

Another upcoming propitious progression in the evolution of Blockchain is the Blockchain 4.0. It aims to deliver Blockchain Technology as a business-usable platform to create and run applications thus converting the technology to fully mainstream. It has the possibility of inculcating other prosperous technologies such as Artificial Intelligence with Blockchain. Blockchain 4.0 enables proliferation of a seamless integration of different platforms to work under a single umbrella in coherence to fulfill business and industry demands.

The introductory platform to put forward Blockchain 4.0 utilities is Unibright [92] which enables an amalgamation of several blockchain business models. Another example is SEELE Platform [93] which allows integration in blockchain space by permitting cross communication between different protocols across various services harmonically. The fourth generation has the potential to allow the transactional speed up to 1 M transactions per second which currently impossible in the existing generations.

3.4 Comparison of Different Generations of Blockchain

After understanding the nitty-gritty of the evolutionary generations of blockchain, this section compares basin principle, consensus mechanisms, transaction speed, merits and demerits and examples of all of them chronologically in Table 3.2.

The usage of a particular generation thus depends on the application domain it has to sustain with their corresponding consensus models and respective parameter specifications. For Peer to Peer cryptocurrency exchange, Blockchain 1.0 stills proves to be an simpler alternative. Other non-financial sectors like Education, Healthcare, Agriculture, Smart Homes etc. utilize the Ethereum platform along with smart contracts to formulate the terms and regulations between the service provider and customers. The third and fourth generation of Blockchain is more predominate where Blockchains works into backend for several business models and cross communication is required amidst several Blockchain networks. The last two generations of Blockchain is still in its infancy and still undergoing several modifications to become potential enough to serve mankind.

Table 3.2 Comparison between different generations of blockchain

Parameter	Blockchain 1.0	Blockchain 2.0	Blockchain 3.0	Blockchain 4.0
Underlying principle	Distributed Ledger Technology (DLT)	Smart contracts	Decentralized Apps (dApps)	Blockchain with AI
Consensus mechanism	Proof of work	Delegated proof of work	Proof of stake, Proof of authority	Proof of integrity
Verification	By miners	Through smart contracts and miners	In-built verification mechanism via dApps	Automated verification via Sharding
Scalability	Not scalable	Poorly scalable	Scalable	Highly scalable
Interoperability	Not interoperable	Not interoperable	Interoperable	Highly interoperable
Intercommunication	Not allowed	Not allowed	Allowed	Allowed
Speed	7 TBS	15 TBS	1000 s of TBS	1 M TBS
Cost	Expensive	Cheaper	More Cheaper	Cost effective
Energy consumption	Highest	Moderate	Energy efficient	Highly efficient
Example	Bitcoin	Ethereum	IOTA, Cardano, Anion	SEELE, Unibright
Application	Financial sector	Non-financial sector	Business platforms	Industry 4.0

3.5 A Blockchain Based Supply Chain Management Testcase

Supply Chain Management demands integration of planning and execution of different processes such as the flow of materials, information as well as capital income. This in detail involves procurement of raw materials from supplier, building the finished product by manufacturer and then transferring them from producer to consumer. The interconnectivity the different participants in the supply chain gradually becomes more inefficient and unreliable when the business flourishes. To eliminate such discrepancies Blockchain Technology has the potential to revolutionize the Supply Chain Management. The advantages provided by Blockchain in this scenario are enlisted below.

- Blockchain enables more transparent and authentic end-to-end tracking in the supply chain. Each organization can create a decentralized immutable record of all its dealings, thus allowing tracking of assets from provenance to delivery.
- Blockchain enhances the trust and visibility amidst the service provider and consumers.
- Blockchain eliminates fraud and intrusion of valuable goods such as diamonds and pharmaceutical drugs.
- Blockchain abolishes all intermediary entities and curbs losses from counterfeit and gray market trading.
- Blockchain provides all participants within a particular supply chain full authority to access the same information, thus diminishing any communication or data transfer errors..
- Blockchain streamlines administrative procedures and diminishes costs by enabling an effective audit of supply chain data by getting rid of manual checks for compliance or credit which are time-consuming and error prone.

Figure 3.10 illustrates a general Blockchain based Supply Chain Management diagrammatically with all its participatory elements.

- The main entities of a Supply Chain are the raw material supplier, the product manufacturer, the finished goods distributor, the retailer and finally the consumer.
- The supplier and manufacturer formulate a smart contract amongst them and the settlement occurs between them accordingly.
- Details regarding the raw material and manufacturing such as supply date, quantity, manufacturing date, units etc. are uploaded into the Blockchain.
- Once the Manufacturing is over, the manufacturer and distributor finalize the terms of their smart contract.
- Details like number of units distributable, the address of the retailer, distribution date etc. are fed into the blockchain.
- After the retailer receives the finished products, they are updated into the inventory along with their manufacturing dates, costs expiry dates etc.
- The customer can purchase from the retailer either physically or online and back track the entire supply chain via the Blockchain to ensure the quality of the product.

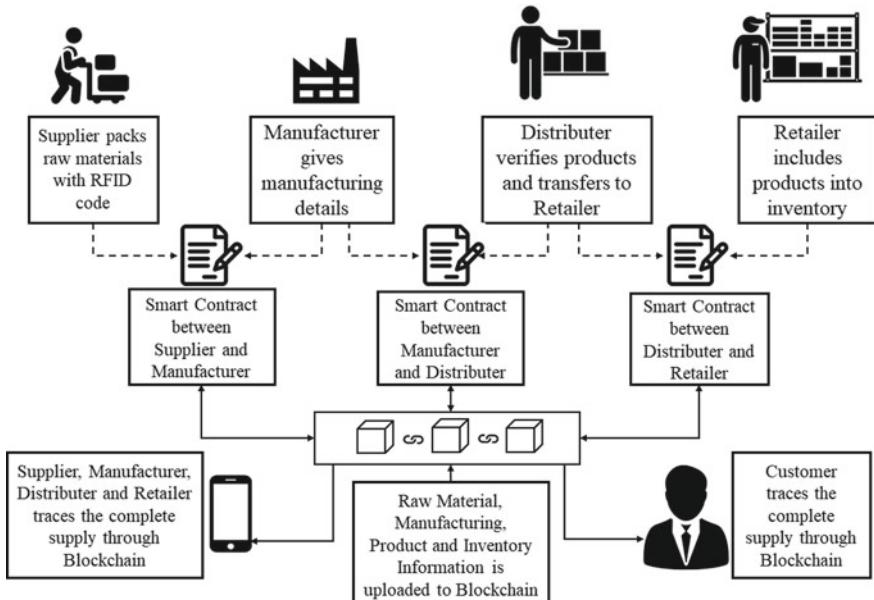


Fig. 3.10 Blockchain based supply chain management system

- The Supplier, Manufacturer and Distributer also track their relevant information and selling of goods to manage their services accordingly.

Incorporation of Blockchain introduces more transparency into the supply chain. Every entity can back track the information once uploaded into the Blockchain. Also the data becomes immutable therefore nobody can upload it without the consent of other entities. Any kinds of fraud or counterfeiting is also eliminated by the usage of Blockchain. Thus Blockchain has the potential to transform any other business domain like Supply Chain Management to greater extents.

3.6 Conclusion

Blockchain is a promising technology that has garnered immense interest of researchers. It largely impacted the peer-to-peer information exchange by combining cryptographic principles with decentralization, immutability and transparency. Since its inception by Satoshi Nakamoto back in 2008, Blockchain technology hugely transfigured to greater extents since then. The first generation of Blockchain, Bitcoin was a decentralized peer-to-peer digital currency which eliminated the presence of any central authority such as banks or intermediaries. To address the trust issues amidst the participants, Bitcoin implements consensus models to ensure the authenticity and integrity of the users. Due to the limited functionality of the first generation

in only financial sector, further advancements were made to adopt Blockchain for other domains as well. Ethereum, the second generation technology has immense application for crowdsourcing through its trustworthy smart contact clauses. A smart contract is a self-asserting contract where the decision between buyer and seller are directly written as lines of codes across a distributed, decentralized blockchain network. The third generation Blockchain has inbuilt verification mechanism and more efficient faster and cheaper than previous versions. Combining Artificial Intelligence with Blockchain Technology has already paved way for the fourth generation of blockchain as well.

This chapter begins by describing the historical background of this expeditious technology. It then proffers a description of the basic terminologies in blockchain, it's types, basic structure of block and different consensus models popularly known. The fundamental aim of this chapter was to provide a comprehensive study of the successive evolutions in Blockchain Technology by highlighting the nitty-gritty of each generation in detail. It also illustrates a parameter wise differences amidst the several generations in terms of their principle areas, consensus models used, utility of smart contracts, the energy and cost requirements and execution speed and scalability. In the end, a Blockchain in Supply Chain Management test case has also been elaborated in this chapter.

The future scope of this book chapter involves designing a two party secure message exchange protocol by utilizing the fundamental offerings of the relevant version of Blockchain. Which generation will be most suitable, the formulation of smart contract if applicable followed by its deployment and other essentials has been left for our future endeavors.

References

1. Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V.: Blockchain technology: beyond bitcoin. *Appl. Innov.* **2**(6–10), 71 (2016)
2. Pilkington, M.: Blockchain technology: principles and applications. In: *Research Handbook on Digital Transformations*. Edward Elgar Publishing (2016)
3. Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H.: An overview of blockchain technology: architecture, consensus, and future trends. In: *2017 IEEE International Congress on Big Data (BigData Congress)*, pp. 557–564. IEEE (2017)
4. Yaga, D., Mell, P., Roby, N., Scarfone, K.: Blockchain technology overview. arXiv preprint [arXiv:1906.11078](https://arxiv.org/abs/1906.11078) (2019)
5. Nofer, M., Gomber, P., Hinz, O., Schiereck, D.: Blockchain. *Bus. Inf. Syst. Eng.* **59**(3), 183–187 (2017)
6. Preneel, B.: Cryptographic hash functions. *Eur. Trans. Telecommun.* **5**(4), 431–448 (1994)
7. Bakhtiari, S., Safavi-Naini, R., Pieprzyk, J.: Cryptographic hash functions: a survey, vol. 4. Technical Report 95-09, Department of Computer Science, University of Wollongong (1995)
8. Carlozo, L.: What is blockchain? *J. Account.* **224**(1), 29 (2017)
9. Nakamoto, S.: Bitcoin: peer-to-peer electronic cash system (2008)
10. Underwood, S.: Blockchain beyond bitcoin (2016)
11. Urquhart, A.: The inefficiency of Bitcoin. *Econ. Lett.* **148**, 80–82 (2016)
12. Baliga, A.: Understanding blockchain consensus models. *Persistent* **2017**(4), 1–14 (2017)

13. Dannen, C.: Introducing Ethereum and Solidity, vol. 1. Apress, Berkeley (2017)
14. Mohanta, B.K., Panda, S.S., Jena, D.: An overview of smart contract and use cases in blockchain technology. In: 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), pp. 1–4. IEEE (2018)
15. Cachin, C.: Architecture of the hyperledger blockchain fabric. In: Workshop on Distributed Cryptocurrencies and Consensus Ledgers, vol. 310, no. 4 (2016)
16. Abrar, W.: Untraceable electronic cash with Dicash (1900)
17. Friis, J.B.: Dicash Implementation. University of Aarhus (2003)
18. Haber, S., Stornetta, W.S.: How to time-stamp a digital document. In: Conference on the Theory and Application of Cryptography, pp. 437–455. Springer, Berlin, Heidelberg (1990)
19. Bayer, D., Haber, S., Stornetta, W.S.: Improving the efficiency and reliability of digital timestamping. In: Sequences II, pp. 329–334. Springer, New York, NY (1993)
20. Haber, S.A., Stornetta Jr, W.S.: U.S. Patent No. 5,781,629. U.S. Patent and Trademark Office, Washington, DC (1998)
21. https://en.wikipedia.org/wiki/Digital_currency
22. Szabo, N.: Bit gold, unenumerated.blogspot.com (Mar. 29, 2006) Internet Archive
23. Szabo, N.: Bit gold. Website/Blog (2008)
24. Jakobsson, M., Juels, A.: Proofs of work and bread pudding protocols. In: Secure Information Networks, pp. 258–272. Springer, Boston, MA (1999)
25. Finney, H.: Rpow-reusable proofs of work (2004). Internet: <https://cryptome.org/rpow.htm>
26. Back, A.: Hashcash-a denial of service counter-measure (2002)
27. <https://en.wikipedia.org/wiki/Ledger>
28. <https://en.bitcoin.it/wiki/Block>
29. https://en.bitcoin.it/wiki/Genesis_block
30. https://en.wikipedia.org/wiki/Hash_function
31. <https://en.bitcoin.it/wiki/Mining>
32. Watanabe, H., Fujimura, S., Nakadaira, A., Miyazaki, Y., Akutsu, A., Kishigami, J.J.: Blockchain contract: a complete consensus using blockchain. In: 2015 IEEE 4th global conference on consumer electronics (GCCE), pp. 577–578. IEEE (2015)
33. Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., Qijun, C.: A review on consensus algorithm of blockchain. In 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), pp. 2567–2572. IEEE (2017)
34. Lin, I.C., Liao, T.C.: A survey of blockchain security issues and challenges. *IJ Netw. Secur.* **19**(5), 653–659 (2017)
35. Kiayias, A., Russell, A., David, B., Oliynykov, R.: Ouroboros: A provably secure proof-of-stake blockchain protocol. In: Annual International Cryptology Conference, pp. 357–388. Springer, Cham (2017)
36. Kiayias, A., Koutsoupias, E., Kyropoulou, M., Tselekounis, Y.: Blockchain mining games. In: Proceedings of the 2016 ACM Conference on Economics and Computation, pp. 365–382 (2016)
37. <https://en.bitcoin.it/wiki/Nonce>
38. <https://www.investopedia.com/terms/b/block-height.asp>
39. Zheng, Z., Xie, S., Dai, H.N., Chen, X., Wang, H.: Blockchain challenges and opportunities: a survey. *Int. J. Web Grid Serv.* **14**(4), 352–375 (2018)
40. Norman, M.D., Karavas, Y.G., Reed, H.: The emergence of trust and value in public blockchain networks. In: IX International Conference on Complex Systems, p. 22 (2018)
41. <https://www.blockchain-council.org/blockchain/public-vs-private-blockchain-a-comprehensive-comparison/>
42. Pongnumkul, S., Siripanpornchana, C., Thajchayapong, S.: Performance analysis of private blockchain platforms in varying workloads. In: 2017 26th International Conference on Computer Communication and Networks (ICCCN), pp. 1–6. IEEE (2017)
43. <https://www.euromoney.com/learning/blockchain-explained/the-rise-of-private-blockchains>
44. <https://openledger.info/insights/consortium-blockchains/>
45. <https://blockchain.intellectsoft.net/blog/how-the-consortium-blockchain-works/>

46. https://www.oreilly.com/library/view/building-blockchain-projects/9781787122147/d04_4fa02-29f4-4e24-88b2-a41641efdcf8.xhtml
47. Manian, Z.N., Krishnan, R., Sriram, S.: U.S. Patent Application No. 15/212,018 (2017)
48. Wu, L., Meng, K., Xu, S., Li, S., Ding, M., Suo, Y.: Democratic centralism: a hybrid blockchain architecture and its applications in energy internet. In: 2017 IEEE International Conference on Energy Internet (ICEI), pp. 176–181. IEEE (2017)
49. Ateniese, G., Chiaramonte, M.T., Treat, D., Magri, B., Venturi, D.: U.S. Patent No. 9,959,065. U.S. Patent and Trademark Office, Washington, DC (2018)
50. Mills, D.C., Wang, K., Malone, B., Ravi, A., Marquardt, J., Badev, A.I., Brezinski, T., Fahy, L., Liao, K., Kargenian, V., Ellithorpe, M.: Distributed ledger technology in payments, clearing, and settlement (2016)
51. Maull, R., Godsiff, P., Mulligan, C., Brown, A., Kewell, B.: Distributed ledger technology: applications and implications. *Strateg. Chang.* **26**(5), 481–489 (2017)
52. Ølnes, S., Ubacht, J., Janssen, M.: Blockchain in government: benefits and implications of distributed ledger technology for information sharing (2017)
53. Antonopoulos, A.M.: *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. O'Reilly Media, Inc. (2014)
54. Antonopoulos, A.M.: *The Internet of Money*, vol. 1. Merkle Bloom LLC, Columbia, MD (2016)
55. Swan, M.: *Blockchain: Blueprint for a New Economy*. O'Reilly Media, Inc. (2015)
56. Böhme, R., Christin, N., Edelman, B., Moore, T.: Bitcoin: economics, technology, and governance. *J. Econ. Perspect.* **29**(2), 213–238 (2015)
57. Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S.: *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press (2016)
58. Decker, C., Wattenhofer, R.: Information propagation in the bitcoin network. In: IEEE P2P 2013 Proceedings, pp. 1–10. IEEE (2013)
59. [https://en.wikipedia.org/wiki/Fork_\(blockchain\)](https://en.wikipedia.org/wiki/Fork_(blockchain))
60. O'Dwyer, K.J., Malone, D.: Bitcoin mining and its energy footprint (2014)
61. Antonopoulos, A.M.: *Mastering Bitcoin: Programming the Open Blockchain*. O'Reilly Media, Inc. (2017)
62. Velde, F.: *Bitcoin: A Primer* (2013)
63. Grinberg, R.: Bitcoin: an innovative alternative digital currency. *Hastings Sci. Tech. LJ* **4**, 159 (2012)
64. Conti, M., Kumar, E.S., Lal, C., Ruj, S.: A survey on security and privacy issues of bitcoin. *IEEE Commun. Surv. Tutor.* **20**(4), 3416–3452 (2018)
65. Eyal, I., Sirer, E.G.: Majority is not enough: bitcoin mining is vulnerable. In: International Conference on Financial Cryptography and Data Security, pp. 436–454. Springer, Berlin, Heidelberg (2014)
66. Androulaki, E., Karame, G.O., Roeschlin, M., Scherer, T., Capkun, S.: Evaluating user privacy in bitcoin. In: International Conference on Financial Cryptography and Data Security, pp. 34–51. Springer, Berlin, Heidelberg (2013)
67. Buterin, V.: A next-generation smart contract and decentralized application platform. White Paper **3**(37) (2014)
68. https://en.wikipedia.org/wiki/Smart_contract
69. Macrinici, D., Cartofeanu, C., Gao, S.: Smart contract applications within blockchain technology: a systematic mapping study. *Telematics Inform.* **35**(8), 2337–2354 (2018)
70. Buterin, V.: Ethereum: Platform Review. Opportunities and Challenges for Private and Consortium Blockchains (2016)
71. Katsiampa, P.: Volatility co-movement between Bitcoin and Ether. *Fin. Res. Lett.* **30**, 221–227 (2019)
72. Bouoiyour, J., Selmi, R.: Ether: Bitcoin's competitor or ally? arXiv preprint [arXiv:1707.07977](https://arxiv.org/abs/1707.07977) (2017)
73. Wood, G.: Ethereum: a secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper* **151**(2014), 1–32 (2014)

74. Antonopoulos, A.M., Wood, G.: Mastering Ethereum: Building Smart Contracts and dapps. O'reilly Media (2018)
75. Yavuz, E., Koç, A.K., Çabuk, U.C., Dalkılıç, G.: Towards secure e-voting using ethereum blockchain. In: 2018 6th International Symposium on Digital Forensic and Security (ISDFS), pp. 1–7. IEEE (2018)
76. Rooksby, J., Dimitrov, K.: Trustless education? A blockchain system for university grades1. *Ubiquity J. Pervasive Media* **6**(1), 83–88 (2019)
77. Aung, Y.N., Tantidham, T.: Review of Ethereum: smart home case study. In: 2017 2nd International Conference on Information Technology (INCIT) (pp. 1–4). IEEE (2017)
78. Adhikari, C.: Secure framework for healthcare data management using ethereum-based blockchain technology (2017)
79. Shih, D.H., Lu, K.C., Shih, Y.T., Shih, P.Y.: A simulated organic vegetable production and marketing environment by using ethereum. *Electronics* **8**(11), 1341 (2019)
80. Delmolino, K., Arnett, M., Kosba, A., Miller, A., Shi, E.: Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab. In: International Conference on Financial Cryptography and Data Security, pp. 79–94. Springer, Berlin, Heidelberg (2016)
81. Chen, T., Li, X., Luo, X., Zhang, X.: Under-optimized smart contracts devour your money. In: 2017 IEEE 24th International Conference on Software Analysis, Evolution and Reengineering (SANER), pp. 442–446. IEEE (2017)
82. Marino, B., Juels, A.: Setting standards for altering and undoing smart contracts. In: International Symposium on Rules and Rule Markup Languages for the Semantic Web, pp. 151–166. Springer (2016)
83. <https://www.investopedia.com/terms/d/decentralized-applications-dapps.asp>
84. <https://medium.com/edchain/what-is-sharding-in-blockchain-8afdf9ed4cff0#>
85. De Angelis, S., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., Sassone, V.: Pbft vs proof-of-authority: applying the cap theorem to permissioned blockchain (2018)
86. <https://icon.foundation/contents/icon/introduce?lang=en>
87. Agarwal, N., Vasseur, J.P., Achar, V.N.: U.S. Patent Application No. 12/790,028 (2011)
88. Vasseur, J.P., Agarwal, N., Thubert, P., Wetterwald, P.: U.S. Patent No. 8,489,765. U.S. Patent and Trademark Office, Washington, DC (2013)
89. Divya, M., Biradar, N.B.: IOTA-next generation block chain. *Int. J. Eng. Comput. Sci.* **7**(04), 23823–23826 (2018)
90. <https://tradingstrategyguides.com/cardano-cryptocurrency-strategy/>
91. Spoke, M.: Aion: The third-generation blockchain network. Whitepaper (2017)
92. Schmidt, S., Jung, M., Schmidt, T., Sterzinger, I., Schmidt, G., Gomm, M., Tschirsck, K., Reisinger, T., Schlarb, F., Benkenstein, D., Emig, B.: Unibright-the unified framework for blockchain based business integration. White paper, April (2018)
93. <https://icodrops.com/seele/>

Chapter 4

Anatomy of Blockchain Implementation in Healthcare



**Shubhangi V. Urkude, Himanshu Sharma, Seethamsetty Uday Kumar,
and Vijaykumar R. Urkude**

Abstract Blockchain is one of the leading technologies that have a huge number of implications in solving real time problems, especially in sectors like Healthcare, Banking, Aviation, Telecommunication, and so forth. Blockchain is known for its features like interoperability, improved information security, Data integrity, immutability, distributed database, Peer to Peer transaction Network, traceability, and transparency along with a trustworthy environment that makes it more secure and reliable. It is enormously known for decentralizing data, easy accessibility, and management of operations, which makes blockchain a better technology to work on. Currently, the big sectors like healthcare that have a huge number of implications in comparison to others, need to make their activities effective and efficient on a real time basis. Unlike other technologies that are presently available in the healthcare industry, Blockchain technology facilitates many things such as drug supply chain management by making it counterfeit-free, providing interoperability in patient health records, allowing data operations to be safe and precise, enhancing medical insurance security, assistance in disease predictions, etc. Ensuring absolute encryption security by way of cryptographic algorithms with healthcare taking pleasure in the stack of benefits. Blockchain can solve numerous problems in healthcare and adapting it, will not only boost the working productivity but also enhances the quality of outcomes with a progressive approach. This chapter focuses on blockchain introduction followed by its implementations in the healthcare industry and issues that could be solved using blockchain technology.

S. V. Urkude (✉)

Faculty of Science and Technology, ICFAI Foundation for Higher Education, Hyderabad, India
e-mail: ushubhu@ifheindia.org

H. Sharma

Department of Computer Science and Engineering, IcfaiTech (Faculty of Science and Technology), ICFAI Foundation for Higher Education, Hyderabad, India

S. U. Kumar

Adsana Corp USA (Canine Cancer Centre), San Francisco, USA

V. R. Urkude

Vignan's Institute of Management and Technology for Women, Ghatkesar, Hyderabad, India
e-mail: vijay@vmtw.in

Keywords Blockchain · Telecommunication · Distributed database · Cryptographic algorithm · Immutability

4.1 Introduction

Blockchain technology was initially developed to eradicate the intermediaries in digital currency transfers [1, 2]. Blockchain is a decentralized or distributed system, cryptographically secured, provides immutable links while transferring assets, and having a huge computational network. Blockchain acts as a sheltered atmosphere to store and perform data operations using node validation and a Trustworthy environment in a peer to peer transaction network.

The recognized design of Blockchain was first announced in 2008, which was implemented and deployed in 2009 [1]. It was the first decentralized digital currency system that pioneered Bitcoin as its integral constituent. It ensures a transaction is added to the block and the block has been lucratively created and dedicated to the Blockchain. The creation of new blocks and adding them to the Global Blockchain is done by a decentralized consensus system. The blocks maintain a cryptographic hash value with a link to the previous block in the Blockchain so that the data integrity inside the blockchain is preserved and remains tamper-proof. Blockchain systems are growing rapidly with an increase in investments and interests from various industrial sectors. Bitcoin Systems ensures that the transaction is recorded and structured in a cryptographically secured chain of blocks are immune to many problems resembling security, privacy, trust issues, and double spending, etc. [3–5].

4.1.1 *Characteristics of Blockchain*

Immutability Each block in the blockchain is connected to other blocks with cryptographic hash functions. Transactions are recorded in a chronological order that makes blockchain tamper-proof [6].

Transparency Changes in the network are publicly available. Transactions are validated by authorized nodes on the network, so that any change could be detected at any instance of time, making Blockchain a compatible platform to work with.

Traceability Timestamp feature in Blockchain helps in recording transactions at each point of time by tracking every movement with hash functions adding up more functionality to their succession, and making the process efficient and secure.

Decentralization A distributed database that allows multiple platforms to have authoritative access on the database. It helps in reducing mediatory expenses and make sure that the data is stored inside a secure environment [3].

Trust factor Trust is the principal factor that plays a major role while performing a transaction. Blockchain allows unknown entities to have secure transactions without any externalities and interruptions, offers a trustworthy environment for transferring assets to build trust [7].

4.1.2 Flow of Bitcoin Transaction

In the first step, a Transaction is encrypted and broadcasted on the Blockchain network. Every transaction was verified by participating nodes present on the Network that will eliminate the need for intermediaries. The verified transactions are stored in a new block; each block having a unique cryptographic hash value, subsequently block is added to the Blockchain [4, 8].

In the second step, the process of adding the block to the blockchain is done via a method called mining. Mining is done through a consensus protocol called Proof-of-Work (PoW). The entities that are involved in mining are called miners. Figure 4.1 shows the Bitcoin Transaction Process.

The third step discussed the process of the Consensus algorithm that involves a group of nodes achieving agreement on a single data assessment between decentralized systems. It is designed to accomplish consistency in a network that involves numerous untrustworthy nodes [4, 9].

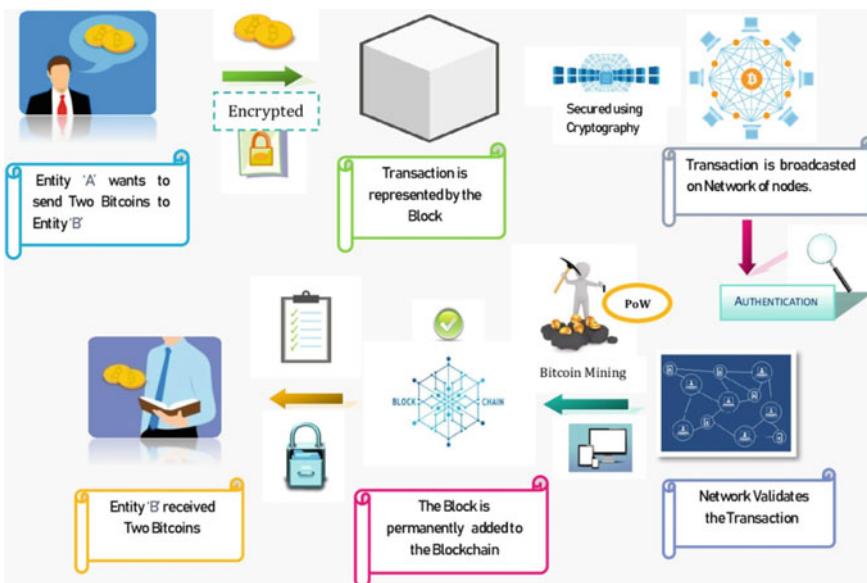


Fig. 4.1 Bitcoin transaction process

The fourth step discussed the process of Consensus protocol in Bitcoin Blockchain. It is named as Proof-of-Work (PoW) that uses Secure hash Algorithm 256 (SHA-256) to generate a unique cryptographic hash value for each transaction performed on the blockchain. PoW includes set of nodes working to crack high-computationally intensive puzzles to get an embattled hash value and the miner who cracks it first will get a chance to add the block to the blockchain and is rewarded with Bitcoin.

Intricacy in generating nonce value i.e., the complexity of the computational puzzle will depend on blocks added per hour and the infrastructure used by the miner.

The fifth step discussed transactions in the Network,

- The transaction is broadcasted to all the nodes and each node gathers new transactions into a block.
- Available nodes perform Proof-of-Work consensus and broadcast the transaction to get verified by all the nodes available.
- Since nodes allow only valid blocks to participate and are committed to the Blockchain, the double-spending problem is resolved.
- In this way, a transaction takes place by eliminating mediatory costs and third party dependence [1, 3].

Potentials of Blockchain implementation in Bitcoin are the Hash pointer and Merkle tree, which acts as the key feature in the whole network infrastructure that makes the transactions on Blockchain secure and user-friendly. Hash pointers are used to address the location of the data on the network and work on linking of data blocks using complex encryption algorithms. So that any sort of misconduct in the atmosphere can be detected by addressing the data locations. Merkle tree can be represented as a structured hierarchy of nodes, connected internally to a hash pointer, and alteration in any node will be reflected on all. This prevents data tampering and provides transparency. Digital signature plays an important role in the identification of network participants by allowing only authorized entities to take part in transactions. It consists of core components that are required to perform a digital signature, includes key generation, signing, and verification algorithms [3].

4.1.3 Types of Encryption Algorithms

Symmetric Algorithms that use the same cryptographic keys to encrypt as well as decrypt the transactions, both the parties have access to the same key that gives rise to distress in maintaining user's privacy and security [3, 4].

Asymmetric Public-key cryptography is the system that employs a pair of keys in encrypting and decrypting of data. In which public key is open to the network and the private key is known only to the owner. In this system, the sender encrypts the

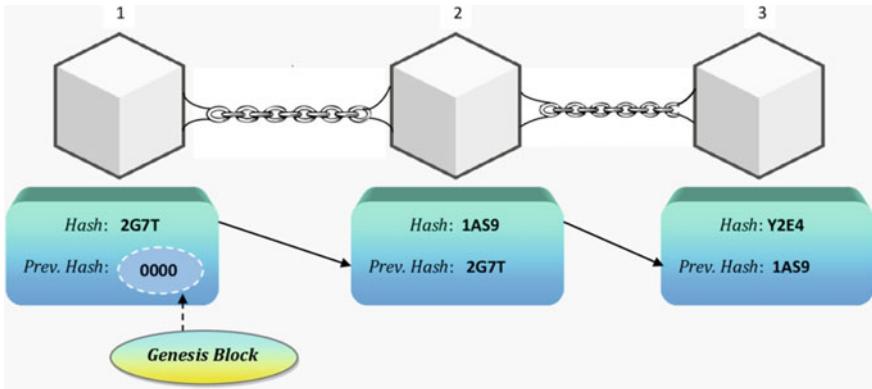


Fig. 4.2 Data blocks forming blockchain

transaction with the receiver's public key, which can be only decrypted using the receiver's private key. Bitcoin transaction utilizes public-key cryptography [3, 4].

Figure 4.2 shows the arrangement of data blocks in the blockchain. As mentioned in the figure every block is associated with the block's hash value and a hash value for the previous block. It forms a chain like structure. The first block in Blockchain is called Genesis Block, which doesn't have any previous hash value.

4.1.4 Types of Encryption Algorithms

Permissionless Blockchain Public Blockchain is a permissionless blockchain. In this network, all transactions are completely decentralized with having no individual entity controlling the whole network [6, 10]. It is a distributed network. A public blockchain is completely transparent and nodes can only examine transaction details. So anyone can view the transactions happening without knowing from whom it's been transacted and asset transfers are highly encrypted using complex algorithms. e.g. Bitcoin, Ethereum uses public blockchain to perform exchanges on their platform.

Permissioned Blockchain Private Blockchain is called permission blockchain that involves authorized access to enter the Blockchain network [11, 12]. Most of the enterprise uses private blockchain. Private Blockchain transactions are privately held with known entities making transactions more centralized than public blockchain. Enterprises use a private blockchain to perform the transfer of sensitive information among known entities. e. g. Ethereum and Hyperledger etc.

Hybrid Blockchain A combination of public and private blockchain can be called as hybrid blockchain. It gives privacy benefits of private blockchain and interoperability and transparency of public blockchain by providing adaptability to pick what

information sender needs to make open/public, transparent, and what information they need to keep private [7]. e.g. Ripple network and Dragonchain, etc.

Consortium Blockchain They are often considered as a subpart of the private blockchain. In private blockchain a single entity controls the network. A consortium blockchain is controlled by an endorsed group of entities, which makes.

4.1.5 Cryptocurrency

Cryptocurrency is the digital currency that works on the technology called Blockchain. The Cryptocurrency is used to depict encoded, decentralized digital cash moved among peers and affirmed in a permissionless open record throughout the computation intensive process of mining [11, 12]. Most dominating networks in the Cryptocurrency market are Bitcoin and Ethereum. Ethereum demonstrated Blockchain as a computational network by performance, which is above the exchanging of assets.

Smart contracts are the digital contracts that work on a technology called Blockchain, introduced by Ethereum in 2014, making it the first platform to do so. They are programmable, immutable, and robust for encouraging, executing, and upholding the arrangement or execution of an understanding. Ethereum is a well known Blockchain for smart contracts [13].

4.1.6 Initial Coin Offering (ICO)

ICOs are looked at as a way to host finances, a company looking for funds to create applications, coins, or services, etc. It can use Initial coin offering, so to enhance resources as well as give long term benefits to consumers, who are fascinated in buying them. ICOs are a popular fundraiser method, which is a preferable option for startups that are looking to provide their products and services. To participate in ICOs an entity or investor should have a proper understanding of the working of cryptocurrency wallets and transactions. When a cryptocurrency startup wants to raise capital through ICOs they typically create a whitepaper to showcase their project outlines and benefits, to convince the investors. These coins are assigned as tokens that can act as shares of the company, similar to the company selling shares in Initial public offerings (IPO) and investors buying those shares [14].

4.1.7 Tokens in Blockchain

Digital tokens are the virtual tokens that have the features of ‘security’ under financial services and markets (FSMR) 2015. They may be referred to as ‘Digital securities’ that displays characteristics of a Debenture, share, or units in finance. Crypto asset is digital representations of values that are virtually traded as a medium of exchange, part of the account, and expand of worth, but it does not have any lawful tender standing in a jurisdiction [15].

The Operating a Crypto Asset Business (OCAB) framework introduced two types of digital assets.

Utility tokens The tokens, which can be exchanged for access to specific merchandise or service, usually supplied via a digital ledger technology (DLT) platform, these tokens, do not demonstrate any traits and personality of a synchronized venture [15]. For example, to store data online they are different framework like Amazon web services, Dropbox, etc. in which a consumer have to reserve the server and is charged for the same. Unlike previous frameworks, the Filecoin network allows the client to store data in an encrypted/ decentralized form that will automatically track utilized storage and charge accordingly [16].

Security tokens They are often called ‘tokenized security’ symbolizing possession in a fundamental real-world asset with decentralized network tracking. Security tokens make it easy for the customer to access investments on multiple platforms [17].

They are many more frameworks, which have classified tokens based on their utilization by distinct authorities and multiple platforms in the world. Table 4.1a, b shows the different frameworks used in blockchain.

Table 4.1 Different blockchain frameworks

(a)				
Platforms	Type of blockchain	Consensus protocol	Transfer status	Scalability
Bitcoin	Public	PoW (Proof of work)	Public	Low transfer throughput
Ethereum	Public, Private	PoW, PoS (Proof of Stake)	Public, Private	Low transfer Throughput
Hyperledger Fabric	Private, Consortium, etc	Numerous Access protocols	Private	High transfer Throughput

(b)			
	Transaction speed	Transactional cost	Smart contracts
Bitcoin	7 Transactions/s	High	No
Ethereum	15 Transactions/s	High	Yes
Hyperledger Fabric	3000 Transactions/s	Low	Yes

The rest of the chapter is organized as follow. In Sect. 4.2, we presented a brief overview of application of blockchain in healthcare. The implementations of blockchain in different sectors are discussed in Sect. 4.3, which includes medical insurance, healthcare infrastructure, and dental industry so on. In Sect. 4.4, we explained about issues in blockchain with potential elucidations, followed by issues in healthcare that could be solved using blockchain technology is described in Sect. 4.5. Finally, we concluded the chapter with future scope in Sect. 4.6.

4.2 Blockchain in Healthcare

Blockchain has a wider scope in the healthcare industry, from storing and managing patient's health data to supply chain management & drug security, disease predictions, drug traceability, and insurance claims, etc. Blockchain technology has completely changed the way how things used to be implemented by automating all the processes, which were previously done manually with unfortunate configuration and time-draining functions. Blockchain provides efficient outcomes that create trust among entities via a reliable environment and user-friendly network. The patient's data management is playing a dominant role in building trust among entities resembling doctors, patients, and institutions, etc. Lack of standards and awareness among the entities is hampering the enlargement of blockchain technology [10]. According to Global Blockchain Survey, 40% of executives' sight blockchain as a 'top-5' intentional priority, BIS Research estimates that blockchain will grow over \$5.6 billion by the end of 2025 and healthcare industry can save up to \$150 billion per year by 2025 [18].

The Healthcare industry suffers from a lot of security breaches and blockchain promises to fill all the loopholes. Blockchain is receiving immense attention in healthcare in resolving data challenges that in turn give pharma industries enormous benefits sustaining sanity among individuals and their priorities. Pharmaceutical companies approximately losses over \$200 billion per year due to the counterfeiting of drugs. Blockchain can replace the current system with a transparent drug supply chain. This includes end to end traceability features that will be the exceptional resolution for enhancing data provenance, reliability, and security of the pharma supply chain [5].

Peer-to-Peer transactions in Blockchain will help the healthcare industry to preserve network infrastructure security. Whereas a smart contract plays a crucial role in giving permissioned access to patient data that allows third parties to have agreements on data access. The decentralized structure of the network maintains data integrity and provides interoperability to facilitate data transfers in the atmosphere, where cryptography makes patient access encrypted and confined. Secure health data creates a trust factor among participating nodes that makes health information exchange effective with eradicating mediator transactional costs [13].

Blockchain framework works for mounting healthcare applications that must execute robust validation attributes and a well-suited access control mechanism to manage how participants can interrelate with the network and the correlated data.

Transaction throughput is scaled based on speed and efficiency like in other use cases. e.g. Remote monitoring systems, Blockchain framework transactions throughput depends on the scalability factor of the participating nodes and kind of infrastructure used by the system [12].

4.3 Blockchain Implementations in Healthcare

Many organizations implemented the blockchain in the healthcare domain by taking into account there need and the kind of problems they are facing. Medicinal services are one of the most urgent segments that are contributing a tremendous part over the timeframe regardless of the foundations changed. Perhaps the greatest test looked by the social insurance industry is in the supervision of understanding Patient Health Records (PHR). It is a significant issue in everywhere throughout the world. Healthcare service is likewise a lucrative industry and clinics frequently are not all that excited about losing their patients. Subsequently, they take part in data blocking exercises which frustrate the advancement progress. Information isn't the main thing that can be taken but, medical drugs are also elevated. The pharmaceutical business can make a profit by propelling its supply chain and observing how the medications are being conveyed to forestall taking and illicit courses [9].

Medication errors are one the loophole which causes surplus deaths every year. They can be due to improper medication intakes or may be ingestion of counterfeit drugs that can have dangerous side effects. Without having proper knowledge about the background of medical products or patients' history it becomes quite complex for the health experts to initiate any treatment option. Diagnostic mistakes represent 60% of every single clinical blunder and an expected 40,000 to 80,000 deaths every year [19]. Current healthcare systems lag in the process of shipping medical products, prevent counterfeiting of drugs, data sharing, and so forth. Blockchain can help in resolving all the issues from the anti-counterfeiting of clinical medications to compatible electronic health records, data interoperability, and proper healthcare infrastructure with a cryptographically secured environment. This technology can enormously change the manner of executing things. Table 4.2 represents the implementation of different companies based on certain parameters such as blockchain network, consensus mechanism, interoperability, security, and so on. Some of the problems face by implementing the blockchain in healthcare by different companies in various sectors is discussed below.

4.3.1 *Blockchain in Medical Insurance*

Presently, the security framework requires many back-office procedures to explain whether the safety net provider or the patient pays for assistance with a lack of communication. It can cause delays, poor assistance, and redundant cost cuts. As per

Table 4.2 Blockchain implementations in healthcare by different companies

Company	MedRec [16]	Farma Trust [17]	MediBloc [18]	Nebula Genomics [23]	IYRO [30]
Consensus Protocol	Proof-of-Work (PoW)	Proof-of-Authority (PoA)	Tendermint Consensus Based on (DPoS &PBFT)	No	Delegated Proof of Stake (DPoS) + asynchronous byzantine fault tolerant (aBFT)
Blockchain Network	Ethereum	Ethereum	Ethereum	Blockstack & Ethereum	EOSIO Network
Interoperability	Slow (Yes)	Yes	Yes	Yes	Yes
Scalability	Issues	Yes	Yes	Yes	Yes
Privacy	Security concerns	Yes	Yes	Yes	Yes
System	Customer-centric	Consumer-Centric	Customer-Centric	Client-centric	User-friendly
TOKENS	No	Yes (ERC20)	Yes (Medi Tokens)	Yes (Nebula Tokens)	Yes

McKinsey publication, lavish work processes add over \$400 billion every year in surplus spending in the healthcare services industry. Smart contracts can add value to the work which was done manually by automating the workflow and allowing the transactions to be self-executed based on various parameters. When it comes to assistance, occupying a blockchain-based network throughout billing documents and associating catalogs, employees can search for trusted information in seconds. It is greatly valuable in health insurance policies which are securing the data and for the compensations also [6]. Blockchain technology also presents potential use cases for insurers that include innovating insurance products and services for growth, increasing effectiveness in scam detection and pricing, and reducing administrative costs [13, 20].

4.3.2 Blockchain-Based Healthcare Infrastructure

Guardtime reinstate Trust with Truth and is well known for providing Healthcare Data Infrastructure, Blockchain-as-a-Service [25]. Guardtime health bridges the gap between various entities across numerous platforms to sustain data integrity. Patient—report outcomes—Guardtime HSX guarantees that patient detailed results are conveyed progressively based on their clinical trials. It can distinguish and resolve cases where patient results and hazard is documented imprecisely. The Platform keeps updating the clients regarding their personalized treatment plans ensuring continuous valuation process and all of this is done via a Smartphone application programming interface (APIs). Guardtime HSX can be utilized to enroll patients for clinical preliminaries about interfacing openly to the patients ingesting explicit medications [26].

4.3.3 Blockchain in Dental Industry

Dental System at the moment from Diagnosis and X-Rays to patient receipts and prescriptions, everything is completely manual. It indicates the patient's data is open for any manipulations. The movement of the current medical data is silent inadequate, with patients having less knowledge about their data. In a Blockchain dental embed framework, the applicable information of the block or dental implant can't be discretionarily altered, so that keeping the culmination and security of the clinical records. It includes two ends a doctor end and patient end, the specialist end stores dental embed patient's clinical records in the blockchain. It also offers inventive assistance, and improves the commitment to clinical characteristics. Patient's end has the responsibility for own clinical records, fit for acquiring their clinical record information explicitly through system connection, and being better for self-health management [27].

4.3.4 Personal Health Record Management

As per an overview led by Klynveld Peat Marwick Goerdeler (KPMG), 38% of top healthcare services chief information officers (CIOs) state better administration of electronic health records (EHR) is head of their plan and planning needs [5]. MedRec provides a Distributed access and validation structure that prioritizes patient activity, giving apparent and accessible surveillance of medical records [8]. MedRec is built on the Ethereum blockchain, which uses smart contracts that allows diverse transactions to be executed on the blockchain. It includes work adjoining on agreements to execute some set of conditions. It doesn't store EHR legitimately, however, encodes metadata that permits records to be gotten to immovably by patients on Ethereum Blockchain. By employing savvy agreements to encode pointers, it may be utilized to find and validate the record areas. MedRec allows patient-provider relationships using a summary contract that gives full control to patients for acceptance, rejection and cutting off relationships. In MedRec whenever a patient wants to access a particular medical record, permission is needed from the provider. He will check the legitimacy of the identity and allows the client to have access to the requested parameter. When it comes to privacy, MedRec proposes the addition of encryption in the off-blockchain synchronization steps, safeguarding against accidental or malicious content access.

Mining in Medrec blockchain is a computationally exhaustive hashing exercise that is performed by medical researchers. In this process, when a block is mined, the block's miner is appended as the author of inquiry, allowing them to collect the data as part of the transaction. Then the block's minor will get access to anonymised data that could help them in their researches. This proposal raises a concern on data security and privacy as nodes with common interests can group up and perform unprofessional conduct. It may also affect the dignity of the blockchain as well as the integrity of clients' data.

Personal health record management uses a different approach to this by storing patients' encrypted data copies on three nodes. One at IYRO cloud node, second at their clinic storage and third on consumer's device, making data storage process more transparent and reliable and all of this is done through API's [24]. IYRO uses the EOSIO network—the most authoritative infrastructure for decentralized applications that offer shards (Blockchain apps). EOSIO consensus protocol includes Delegated proof of stake (DPoS) + asynchronous byzantine fault tolerant (aBFT), which makes it more secure than others. This platform incorporates working on patient's data using artificial intelligence (AI) and Blockchain for making predictions using EOSIO blockchain implementation and algorithm called Umbral algorithm. This algorithm allows the patient to issue re-encryption keys. An end-user can issue signed permissions like sharing EHR with the personal doctor, cancellation of access to EHR, sharing limited PHR with a time limit, and permissions to read/write.

4.3.5 Pharmaceutical Supply Chain

Casado-Vara, Prieto proposed a model that uses digital agreement contracts with multi operator frameworks planned for expanding productivity in logistics configuration management, which can be applied in the pharmaceutical supply chain [13, 28]. FarmaTrust uses Blockchain technology for preventing the counterfeiting of pharmaceuticals and ensure drug safety by the end-to-end tracking of medical products [21]. FarmaTrust Zoi System, a blockchain-based Zoi supply chain information exchange stage to safely confirm and permits the supply of authentic items over an assorted system of pharmaceutical brands. It provides a secure, interoperable, and immutable source of data, which allows tracking of successive products across an uninterrupted chain of supervision throughout the supply chain. By integrating blockchain technology, big data and machine learning with smart dealing logic help Zoi systems to prevent falsified medicines effortlessly entering the consumer market. The system does it, through a digital token referencing each consecutive product key from manufacture to end-user ensuring transparency at every point.

Scalability is one of the major disquiets in Blockchain which is solved by the Zoi system that is designed to handle millions of transactions using various techniques such as caching, data allocation, multi-processing, parallel scaling, high aptitude servers, etc. without negotiating performance and data safety. It uses a permissioned blockchain network—Ethereum and Proof-of-authority as consensus protocol, which makes it highly secured and compatible than other systems. Zoi system issues tokens called FTT tokens i.e., ERC20 standard tokens that allow the clients to take part in the Zoi ecosystem in means of transferring assets, which can be used by pharmaceutical companies, government, consumers, and FTT token holders, etc.

4.3.6 Healthcare Information System Based on Blockchain

The Healthcare sector is moving towards a decentralized database from storing data to performing operations on them and utilizing it to grant personal benefits. MediBloc is an open-source healthcare data platform built on blockchain that can secure and integrate diffused data from numerous organizations. It can track a person's daily movement via smartphones, fit bands, smartwatches, and so forth [22]. Characteristics like high security, reliability, compatibility, and transparency make this platform a well-known preference for unknown entities. Interoperability is the feature that allows all third party entities to play a part in the exchanging of data. MediBloc issues Medi tokens (MED), used on this platform for appreciating their participation by getting tokens in the reward that is not only for participants but also for healthcare professionals too. Tokens can also be used while transferring assets, for example, a third party institution need to take permission from the user to have access to their data so that users can generate revenues in terms of token transfers.

This platform contains 3 layers, first is core layer known as MediBloc core that allows encryption using user's private key on a blockchain network assuring data security. Second layer grant services passing through Ethereum smart contracts that permits the exchange of data between two layers—MediBloc core and Application. The third layer as Application Programming Interfaces (API's) to connect the platform through supervision of protocols. Consensus protocol used by MediBloc is tendermint consensus (Developer friendly and low-level protocol, a combination of Consensus protocol and Application Blockchain interface [29]) that is based on Delegated Proof of Stake (DPoS) and Practical Byzantine Fault Tolerance (PBFT). MediBloc uses blockchain technology to make its platform customer-centric, which provides data switch over services and creates a reliable personal health record (PHR) by allowing the patient to have total control over their data that can enhance data convenience with absolute transparency.

4.3.7 *Blockchain in Genomics*

Genomic refers to Deoxyribose Nucleic Acid (DNA), which helps in uniquely identify entities all over the world. In genomics data sets requires huge computation exhaustive and high sequencing processes. There is a need for a secure data platform that could assist during data allocation and provide high-level information supremacy [13, 30]. Genomic data is used by the researchers for Drug discovery, preventing viruses, disease prediction improved diagnosis, etc., but poor genomic data quality and inefficient data acquirement is becoming a major concern presently. Nebula Genomics provides a platform that enhances the data sharing, storing, enabling buyers to have easy access while surfing through the arrangement, this will not only improve the efficiency but will also make information secure and precise [23].

The Nebula network is built on the Blockstack platform (an open-source and developer pleasant network for building decentralized apps and smart contracts) and Ethereum blockchain. It reduces effective sequencing costs and enhances the protection of personal genomic data. By eradicating stress on third parties, data owners can obtain their genomic data from Nebula sequencing facilities that connect them to data buyers in a peer-peer cryptographically encrypted network. Nebula smart contract-based appraisal tool will facilitate data buyers to plan surveys that consist of mutually supporting inquiries and bring out accurate responses. Nebula token is the currency used in this network that can be used in paying for services and data purchases. Decentralized sequencing will help individuals to purchase DNA sequencing machines and perform sequence on their samples so that privacy risks can be detected.

The blockchain implementation proposed by different researchers such as Peilong, Asaph Azaria, and so on is shown in Table 4.3.

Peilong Li et al. proposed a software-defined infrastructure, ChainSDI to address the issue of sharing and computing the data of sensitive patients [31]. They addressed data interoperability issues by deploying in the cloud environment of heterogeneous

Table 4.3 Blockchain implementations in healthcare by different companies

Research work	Data interoperability	Blockchain type	Data security	Smart contract	Consensus mechanism	Data storage
Li et al. [44]	Yes	Consortium	Yes	Yes	No	On-chain
Azaria et al. [45]	Yes	Ethereum	Yes	Yes	Proof of Work	Off-chain
Nakamoto [1]	No	No	No	No	Proof of Work	–
Daraghmi et al. [46]	Yes	Permission blockchain	Yes	Yes	Proof of Authority	–
Liu et al.[47]	No	Private blockchain	Yes	No	Proof of stake	–
Ben-Sasson et. al [48]	No	Bitcoin blockchain	No	No	Proof of Work	–

nature. This ChainSDI is developed by modifying the traditional infrastructure like; to capture the data related to patient's record efficient sensors are deployed in patient's premises, use of heterogeneous cloud computing resources at a different level, and use of secure transaction protocol for data transmission between different nodes. A new data structure is proposed to add a new block addressing data interoperability. The patient's data is stored on the blockchain directly using smart contract and security with patient ID. So the patient's information is directly accessible to the authorized people and reduced the hardware requirement for other nodes in the chain. Data security is provided using a smart contract so that when the user wants to get the information it is validated by a smart contract. This will stop tampering with data. Private Key cryptography technique is used for the security purpose. They also proposed an algorithm for smart contracts to ensure data integrity and access control.

Asaph Azaria et al. proposed MedRec, a framework to handle Electric Health Records. It provides security, authenticity, interoperability, and easy access to information at different sites [32]. MedRec provides a single point access using ID (e.g. patient's name or social security number) and this ID is mapped to Ethereum address. The database server authenticates an exchange of data between a patient and provider database using a syncing algorithm. An off-chain data storage policy is used to store data in Ethereum blockchain. MedRec was implemented using Proof of Work consensus mechanism and peer-to-peer state transition to transfer data to all nodes. In MedRec three types contracts are implemented (i) Registrar contract (RC) (ii) Patient-Provider relationship Contract (PPR) and (iii) Summary contract (SC). RC maps participant ID to the address on Ethereum blockchain and it is connected to the summary contract. The PPR enables to share records among the connecting nodes. Storing and managing data between a pair of nodes PPR is issued among them. The smart contract enables to record the medical history of participants and store status variable for each relationship. After getting the acknowledgment patient can perform various actions such as accept, reject, and delete relationships and the

provider will update the status variable. System node in MedRec consists of Backend library, Ethereum client, Database gatekeeper, and EMR manager.

Satoshi Nakamoto proposed Bitcoin, direct money transform from one node to another without a third party interface [1]. He used proof-of-work to follow the majority decision and represented by the longest chain. To modify the block in the chain attacker has to modify all the previous blocks and proof-of-work. With the entire valid transaction, the block is accepted by the node. To process every transaction, some charges are taken as an incentive that will help nodes to stay connected with the chain. The attacker having more CPU power than a new coin is generated. In Bitcoin privacy is achieved by releasing anonymous public keys without telling whom it is addressing.

Daraghm et al. proposed MedChain, to manage medical health records [33]. Security and access control are achieved by encryption and authentication mechanism. Privacy is achieved by implementing a time-based smart contract for all the transactions. Separate logs are maintained to achieve data interoperability and accessibility. To transfer digital currency between a pair of nodes and recreating a new block new incentive mechanism is proposed. Medchain is implemented by various software components such as records evaluation Manager (REM). it will extract, manage, and classify heterogeneous data. The degree of health provider node is computed for each node and stored in Nodes Consensus Contract (NCC) to create a new block. DB manager creates a hash value for the link, the patient's medical record, and logs that are stored in the blockchain. For the client access permission blockchain is used. It had a web interface to view and retrieve information from patients. It uses NCC for registering new user, mining, and identifying the role of each participant in the blockchain.

Liu et al. proposed a mechanism to store medical and historical data [34]. They implemented a symptoms-matching mechanism by creating mutual communication between patients with similar symptoms communication in the future. It is consists of three components system manager, patients, and hospital. The system manager (SM) is a trusted authority. It is responsible for all communication between the patient, hospital, and stored data in blockchain for further reference. They used a delegated proof-of-stake (DPOS) consensus mechanism. In DPOS supernode will get the coin to generate a new block. In case of failure new supernode is selected to generate the block. They used private blockchain for medical data sharing and protection. This mechanism is having low computation and communication costs.

Eli Ben-Sasson et.al proposed Zerocash, a decentralized anonymous payment scheme (DAP) [35]. DAP is an unnamed payment application designed from Bitcoin. DAP is very efficient for the small transaction of less than 1 KB. DAP implemented a special base currency called base coin having parameters such as coin value, serial number, and address. They also defined other transactions as Mint transaction and Pour transaction. All transaction in zerocash is verified by proof-of-work and it will take time to spread on the network. They developed two algorithms, the Mint algorithm to generate a coin and the Pour algorithm to consume the generated coin and performing transaction.

4.4 Issues in Blockchain with Potential Elucidations

In this section, we discussed the general implementation issues in blockchain. All these issues should be addressed to get maximum benefit of blockchain technology in various sector such as medical, aviation, education etc.

4.4.1 Scalability

One of the major concerns in public blockchain is scalability. It arises when the network participants become more due to public blockchain openness. It increases the number of transactions and participant nodes making the whole network not much scalable [7]. Blockchain transfer also includes a node validation process in which the transaction is been shared among different nodes for verification. Once the authentication is completed a ledger entry takes place at each node that makes it tamper-proof, but on the other side, data becomes prone to potential and security risks [36]. To recover blockchain scalability divides the nodes into sub-groups called shards. A shard helps a compartment of transactions to process at a time, making the whole process faster and scalable. After that these transactions are added to the new block i.e., dedicated to the Blockchain [37].

4.4.2 Energy Consumption

Consensus protocol in bitcoin blockchain is called Poof of Work. In which bitcoin miners use about 54 TWh of electricity to perform mining processes, that is enough to power entire New Zealand / Hungary, and in case a miner is not able to hit the target then the whole energy gets wasted. Intel Corporation claims that it has proposed hardware that can reduce mining power by 35% [7, 38]. Various researchers proposed the solution to this problem is using the other available consensus protocols, which could be a better option. Each blockchain is having a different architecture and a specific consensus protocol can be chosen explicitly suitable to their structural design.

4.4.3 Complication and Expenditure

The significant deterrents to the selection of the innovation are intricacy of building and deploying a private blockchain network and the connected cost. Amazon and IBM are providing Cloud-based Blockchain models that can help in making the

process of developing and deploying blockchain networks automated. They have also included offline blockchain development platforms [7].

4.4.4 Lack of Supremacy

In a public blockchain, there is a lack of authorities that can govern the whole process with appropriate protocols and policies, as any sought negligence happening cannot be detected. In a solution to this, institutes and corporations are moving towards private blockchain wherein merely authorized nodes are permitted, which means only certified entities can join the Blockchain Network to engage in any kind of actions inside the network [7].

4.4.5 Lack of Compatibility and Standardization

Standardization is a major concern in implementing blockchain in healthcare. Every firm has its ways of running blockchain that causes delusion and can result in cyber attacks that will not only affect the dignity of the blockchain but will also make the clients suffer. So getting certified from International Standardization authorities would help blockchain to develop fast and secure [36]. Every organization, corporation has its blockchain architecture, programming languages, consensus protocols, etc. Applications built on different platforms can exchange information that makes them less compatible [39]. It provides a flexible design that allows a side chain to make data transfers across multiple platforms acting as the main blockchain.

4.4.6 Data Confidentiality

Public blockchain has data privacy as one of the major concerns when it comes to network security. The nodes can view the transactions that are happening inside the blockchain. Therefore, organizations are going for private or consortium blockchain that allows only certified entities to participate in the Blockchain network [7].

4.4.7 Storage Capacity

Healthcare deals with a huge amount of data that is generated through clinical trials, research data, diagnosis reports, and patient records, etc. It is demanding a secure platform to store data and perform operations with features like interoperability. Unlike the central database, blockchain provides a distributed database that allows

secure data operations and interoperability. Enormous data can increase the size of the database that could result in low processing speed and poor functioning, consequently, the blockchain system needs to be contingent and scalable [36].

4.5 Issues in Healthcare that Could Be Solved Using Blockchain Technology

There are many loopholes in healthcare which can be solved by blockchain technology. In healthcare sector the most promising issue is to maintain the health record of the patient, to track drug delivery etc. is discussed in this section.

4.5.1 *Blockchain-Based Insurance in Healthcare*

Blockchain in healthcare is one that makes the transactions faster and securer. The features like interoperability make blockchain an easily accessible platform to store data and provide a sheltered atmosphere when working with distinct operations. Smart contracts are programmable contracts, which syntactically deal with a set of conditions to be verified before having a transaction executed. This structure can fulfill the requirements of insurance policies given by the companies including some agreements to be signed by the end-user to accept their guidelines i.e., terms and conditions, and it is only possible using blockchain like from gathering of data to interpretation and then storing it safely in a decentralized platform have completely renovated the authenticity of transferring assets. It can detect false claims made by the entities and can easily confirm them with an unassailable registry which is extremely transparent so that no mediator could interfere and argue about data security concerns. The main purpose of blockchain in healthcare insurance is to uphold accuracy and lucidity in surroundings to withstand on client requirements that is possible using digital ledger technology (DLT) to make it a customer-centric system [40].

IBM Blockchain uses smart contracts to allow automatic payment execution for insurance claims and reimbursement processes to resolve the major harms faced by the insurance industry like an imprecise directory data. Distributed ledger technology can make the insurance claims time-stamped and automate collection with modernizing of data by significantly eradicating stress on the third party and manual paperwork. It would automatically make the whole scenario lucrative. The Healthcare industry lost over \$6 Billion in security breaches concerning data privacy, so security should be the main concern when introducing Blockchain-Based systems. The interoperability should not result in data allocation without patient acquiescence. It should be exclusively shared on patient assent and obtainable privacy regulations [41].

4.5.2 *Multimedia Blockchain System: An Immutable Connection*

The current multimedia system does not include the time-stamping of performed transactions and the history of alteration details. Multimedia deals with documentation, images, and videos so on. They are often manipulated when showcased in public like exhibitions, galleries, etc. preparing creative content by tampering with the original document to spread off beam misinformation on social media. Blockchain can play a major role in developing the watermark based Multimedia Blockchain framework which is built on the testnet of the Ethereum that fundamentally focuses on a unique hash of every transaction executed. It could be time-stamped anytime from anywhere when it is required. Since blockchain follows a node systems validation process and a signature feature, which was introduced to detect the originality of the media content. The process goes like a self-embedded watermark is hidden inside original media using Discrete Wavelet Transform (DWT). The watermarking string consists of 8-bit values, which illustrates media's authenticity. It is done using a watermarking algorithm that can sense any wrong means happening, so it can retrieve the original content of the specific media that can defend its inventiveness. This way the multimedia could be encrypted using blockchain technology healthcare marketing should always be precise and secure, so that negligence happening inside the system can be easily detected and resolved [42]. The main purpose of blockchain in healthcare is to resolve concerns on data security and platform reliability. It is severely needed in the current healthcare system, where employing Distributed ledger technology (DLT) is coming out as a better solution.

4.5.3 *Blockchain-Based Electronic Health Records (EHR)*

Personal health records in the current scenario are bounded within a specific organization as any organization will not be ready to share their Electronic Health Records in fear of competency in the market that can pull them down. The data is stored in the hospital's database i.e., a centralized database and they can even generate revenues by selling your data to third parties like institutions, researchers, etc. Due to such issues, people are getting affected because every time a person goes to a medical center with no access to his past medical history. It will take a long for the doctor to process it again and make patient ready for the treatment which is completely waste of time and money. Instead of that they can use a database which is accessible to all i.e., blockchain. Blockchain provides a distributed database which can be easily accessed among multiple organizations using a permission-based blockchain network. It can allow the patient to own their data and can make sure that without their authorization nobody could access the data. This makes the whole process transparent and trustworthy. Timicoin uses the concept of interoperability that can secure health information within Health Information Exchange (HIE). It can be defined

as a reliable platform for data sharing that embraces sharing the information of patients, physicians, pharmacists, etc. between unknown entities. When combined with blockchain the Blockchain-based HIE could eradicate avoidable services and checks, enhancing data integrity. It makes data sharing efficient, secure, and tamper-proof thereby cutting transfer costs. Nowadays, mobile applications are developed to store data, includes authorized access to others on their data for a time-stamp to generate revenues and other possessions like getting tokens in reward by keeping track of their health activities, which could keep them fit and healthy [43].

4.5.4 Blockchain Technology for Preventing Counterfeit Drugs from Entering in Pharmaceutical Supply Chain

Counterfeiting is a universal dilemma in the supply chain of pharmaceutical drugs; falsified drugs can be dangerously impacted on the person's health. The containment could cause allergic reactions which may have adverse effects on health conditions especially when a person is undergoing a treatment. Whereas, immoral dosage can cause a lot to the patient and can result in treatment failures, at times even deadly. Blockchain can fill the loopholes by features like traceability, the transparency that could stop counterfeiting of Drugs by keeping a track on drug movements from manufacturing to warehousing, shipping, and logistics to the consumer. A Pharmacosurveillance Blockchain System is developed and designed using smart contracts consisting of a Distributed File System (DFS) to ensure drug safety. It keeps a track on Drug products as they move along the chain and constructs a timeline for every supply chain. This Decentralized application (DApp) can identify irregularities, unapproved information add-ons with each progression labeled with a timestamp for evaluating. The system will allow only FDA approved manufactures and brokers to participate in the entire process. Like a node system in blockchain can verify either it is a certified manufacturer or Wholesaler or Retailer's account. The DApp consists of a log-in Interface followed by transaction history, timeline Dashboard, and contact registry [44].

4.5.5 Blockchain Technology in Doctor-Patient Interaction

The electronic Health record is playing a crucial role in the healthcare industry, which can make patient-Doctor Interaction completely online like medical prescriptions, diets, etc. This process has to be followed by the patient, and is done using a simple mobile/web Application which uses blockchain technology. It provides security, anonymity and a distributed system of records. It will also help doctors to get immediate access to overall patient history with keeping a track on their everyday activities.

Medical chain focuses on blockchain technology for creating a client-based environment which includes double encryption mechanism in permission-based blockchain network. Wherein transactions are viewable to only those who are performing it or giving customer satisfaction in the form of medications, accessibility, and healthcare benefits, etc. It built on Hyper ledger fabric and Ethereum that gives encrypted admittance on heath data when providing services like viewing and controlling convenience for a timestamp-based health record. It was secured using smart contracts to reduce manual assistance and helps in data sharing with third parties such as researches, institutions, hospitals, and so on.

The Doctor-Patient interactions blockchain allows the patient to share their medical records with the doctor securely to ensure the data safety. No need to transfer any records, you just give authorize access to the documents. Medical chain uses gadgets like fit bands to track health activities and emergencies. Telemedicine provides interaction with health experts via application and getting online medical prescriptions, diagnosis, and so on. This platform provides a feature that incorporates cross border interaction with doctors, making Medicalchain a better platform to work on. In this process, the patient has to reward the consulting doctor with med tokens as a charge for evaluating their medical records, providing them advice and assistance. Patients can get health insurance by giving access to their health record using fit bands to supervise their step by step progress with getting tokens in rewards. Patients are rewarded for sharing their data to third party institutions with a time limit access on their data for the medical testing purpose [45].

4.5.6 Blockchain for Sharing Genomic Data

Genomic data refers to the DNA of the person representing the most confidential information of an individual's present, past, and future. Currently, the big DNA testing corporations are generating revenues by selling consumer's data to the third party without even asking the authorized person or providing any compensation to them. This way the most sensitive data of the consumer is open for exploitation. EncrypGen -World's first blockchain-based genomic data market uses a consumer-based system in which consumers can have control over their personal DNA data using blockchain security. It has an option of sharing with the authorized/ registered third parties on the EncrypGen platform resembling researchers, institutions, etc. For a time limit to generate revenues that in turn will help them in adding value to their work and also the person who is sharing the information [46].

4.5.7 Enhancing Clinical Trials and Research Using Blockchain Technology

Patient data sharing is the prior concern when it comes to challenges faced by gigantic healthcare firms for clinical research and trial management. Blockchain can mechanize clinical trials using smart contracts that permit the data to be self-executed when the set of constraints are verified. The manual assistance is completely eradicated and the working flow will get well-organized by changing priorities. Ensuring data privacy is the major distress that blockchain can solve effortlessly. The features like lucidity in-process and tracking data entries to managing tasks. This technology has solved many indiscretions ever since from its evolution eradicating subjects in the vein of falsification of data, muddled etiquette classification, unavailability of records. These issues are the foremost cause of why clinical trial management is sheathing behind. They can be resolved by introducing Blockchain in the system. Research always needs to be accurate, so that the results could be the reflex of the work. But when talking about data utilization from a centralized database there is no guarantee that the data is entirely authentic. There can be any sort of malpractices that can run the whole research. In another way, Blockchain permits data sharing between unknown entities by creating a peer-peer immutable link in which data is encrypted and decrypted by authorized users in a trustworthy environment [47].

4.5.8 Decentralized Artificial Intelligence in Securing Health Records and Detecting Anomalies

Integration of Artificial intelligence (AI) and Blockchain Technology can be called as Decentralized AI. It combines immutability, transparency, and trustworthiness with a human-based artificial network that has the capability of doing wonders. Here, blockchain is secured using AI for providing decision making assistance without any third party supervision that helps in preventing malicious nodes entering into the blockchain by synchronizing and purging threats using machine learning algorithm. Decentralized AI has a lot of implications in healthcare including another sector like aviation, banking, Agriculture, etc. that makes it the best combination in solving real-time tribulations. By this assimilation, blockchain can perform smart transactions which will take a lesser amount of computational power while adding blocks to the blockchain, leasing the process of block creation faster and secure. AI helps in resolving scalability issues by utilizing the data stored in blockchain to make accurate predictions from defined constraints [2]. This way Decentralized AI will enhance the security of blockchain with artificial intelligence. It is acting as a mediator but will be artificial i.e., a machine between entities, securing medical health records and giving efficient and reliable outcomes in a trustworthy atmosphere.

4.6 Conclusions and Future Scopes

Blockchain technology was initially developed for cross-border payments as an alternative to fiat currency, which is known as bitcoin. Over the period after the introduction of Ethereum, it became a computational network. That includes decentralized applications, smart contracts, and many more, with cryptocurrency and the token system as a basic unit for each platform. Blockchain promises to create trust among unknown entities through its cryptographic secured atmosphere. Healthcare is one of the most crucial sectors, which have many implications for Blockchain as mentioned in the above survey.

Regardless, a couple of blockchain advances are energetic and sketchy, yet at the incredible degree this development holds the affirmation to change undertakings. It has many applications in government, human services, content circulation, flexible chain and that's only the tip of the iceberg. Artificial Intelligence is one of the main advances, which when joined with Blockchain have a colossal amount of implications in solving real time circumstances. It also facilitates automation of data operations in healthcare and has capabilities akin to predictions about future activities. Artificial Intelligence is one of the innovations. Blockchain with IoT can contribute its features of decentralization and allow smart contracts to play a major role. Furthermore, Big Data Analytics that focuses on forecasting from a lot of information, adapting blockchain will focus much on quality of data that will have immense compensations. These were only some of them, they are a lot more to explore.

References

1. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2008). Available online at <https://www.ildgroup.si/uploads/product/20/bitcoin.pdf>
2. Dhir, S.S., Hooda, M.: Possibilities at the intersection of AI and blockchain technology. Int. J. Innov. Technol. Explor. Eng. (IJITEE) **9**(1S), 2278–3075 (2019)
3. Zhang, R., Xue, R., Liu, L.: Security and Privacy on Blockchain. ACM Comput. Surv. **1**, Article 1 (2019)
4. What is blockchain is available online at: <https://dragonchain.com/blog/what-is-blockchain>
5. Blockchain in healthcare guide is available online at: <https://healthcareweekly.com/blockchain-in-healthcare-guide/>
6. Different types of blockchain is available online at: <https://dragonchain.com/blog/differences-between-public-private-blockchains>
7. Ismail, L., Materwala, H.: A review of blockchain architecture and consensus protocols: use cases, challenges, and solutions. Symmetry **11**(10), 1198 (2019)
8. MedRec Technical Documentation is available online at: https://medrec.media.mit.edu/images/medrec_technical_documentation.pdf
9. Healthcare projects are available online at: <https://blog.lumiwallet.com/the-most-promising-blockchain-healthcare-projects-2020/>
10. Overview of blockchain technology in the healthcare industry is available online at: <https://www.medgadget.com/2019/12/blockchain-technology-in-healthcare-industry-overview-2020-global-size-estimation-regional-analysis-technology-trends-business-challenges-opportunities-company-profile-market-growth-at-71-8-cag.html>

11. Dubovitskaya A., et al.: Secure and trustable electronic medical records sharing using blockchain. In: AMIA Annual Symposium Proceedings, pp. 650–659 (2017)
12. Agbo, C.C., Mahmoud, Q.H.: Comparison of Blockchain Frameworks for Healthcare Applications. Online Library Wiley Publication (2019)
13. Justinia, T.: Blockchain technologies: opportunities for solving real-world problems in healthcare and biomedical sciences. *Acta Inf. Med.* **27**(4), 284–291 (2019)
14. Initial coin offering is available online at: [https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp#:~:text=An%20Initial%20Coin%20Offering%20\(ICO\)%20is%20the%20cryptocurrency%20industry's%20equivalent,or%20service%20launches%20an%20ICO.](https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp#:~:text=An%20Initial%20Coin%20Offering%20(ICO)%20is%20the%20cryptocurrency%20industry's%20equivalent,or%20service%20launches%20an%20ICO.)
15. Comparative Analysis of Crypto Assets Frameworks is available online at: <https://www.unlOCK-bc.com/sites/default/files/attachments/Comparative%20Crypto%20Assets%20Regulatory%20Framework%20Report%20Final.pdf>
16. About filecoin is available online at: <https://filecoin.io/>
17. What is blockchain token is available online at: <https://theconversation.com/what-is-a-blockchain-token-98916#:~:text=A%20security%20token%2C%20sometimes%20called,an%20underlying%20real%2Dworld%20asset,&text=Security%20tokens%20use%20a%20blockchain,of%20who%20owns%20which%20assets.>
18. Digital disruption of blockchain in healthcare is available online at: <https://healthcareweekly.com/digital-disruption-blockchain-in-healthcare/>
19. Artificial intelligence in healthcare is available online at: Website: <https://healthcareweekly.com/artificial-intelligence-in-healthcare/>
20. Lorenz, J.T.: Blockchain in Insurance—Opportunity or Threat? McKinsey & Company (2016)
21. FarmaTrust Whitepaper is available online at: https://neironix.io/documents/whitepaper/949_f441102b21eaf2b5a0244e8f06a5d.pdf
22. MediBloc Whitepaper is available online at: <https://whitepaper.io/document/176/medibloc-whitepaper>
23. Grishin, D., Obbad, K., Estep, P., Cifric, M., Zhao, Y., Church, C.: Nebula genomics. Blockchain-Enabled Genomic Data Sharing and Analysis Platform, Vol 4, Issue 52, 2018. https://arep.med.harvard.edu/pdf/Grishin_Church_v4.52_2018.pdf
24. IYRO network is available online at: https://iryo.network/iryo_whitepaper.pdf
25. Website: <https://guardtime.com/technology>
26. Website: <https://guardtime.com/health/patient-engagement-for-clinical-trials-and-follow-up>
27. Lin, C.-M.: Blockchain dental implant system. US 2020/0021570 A1, 16 Jan 2020
28. Casado-Vara, R., Prieto, J., De la Prieta, F., Corchado, J.M.: How blockchain improves the supply chain: case study alimentary supply chain. *Procedia Comput. Sci.* **134**, 393–398 (2018)
29. What is tendermint is available online at: <https://docs.tendermint.com/master/introduction/what-is-tendermint.html>
30. Ozercan, H.I., Ileri, A.M., Ayday, E., Genome, A.C.: Realizing the potential of blockchain technologies in genomics. *Genome Res.* **28**(9), 1255–1263 (2018)
31. Li, P., Xu, C., Jin, H., Hu, C., Luo, Y., Cao, Y., Mathew, J., Ma, Y.: ChainSDI: a software-defined infrastructure for regulation-compliant home-based healthcare services secured by blockchains. *IEEE Syst. J.* (2019)
32. Azaria, A., Ekblaw, A., Vieira, T., Lippman, A.: MedRec: using blockchain for medical data access and permission management. In: IEEE 2nd International Conference on Open and Big Data, pp. 25–30 (2016)
33. Daraghmi, E.-Y., Daraghmi, Y.-A., Yuan, S.-M.: MedChain: a design of blockchain-based system for medical records access and permissions management. *IEEE Access* **7**, 164595–164613 (2019)
34. Liu, X., Wang, Z., Jin, C., Li, F., Li, G.: A blockchain-based medical data sharing and protection scheme. *IEEE Access* **4** (2016)
35. Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., Virza, M.: Zero-cash: Decentralized Anonymous Payments from Bitcoin. In: Proceedings of the 2014 IEEE Symposium on Security and Privacy, pp. 459–474 (2014)

36. Siyal, A.A., Junejo, A.Z., Zawish, M., Ahmed, K., Khalil, A., Soursou, G.: Applications of blockchain technology in medicine and healthcare: challenges and future perspectives. *Cryptography* **3**(1) (2019)
37. Zilliqa. Available online: <https://docs.zilliqa.com/positionpaper.pdf> 31 Dec 2018
38. INTEL corporation Available online at: <https://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahml%2FPTO%2Fsearch-adv.html&r=1&p=1&f=G&l=50&d=PG01&S1=20180089642.PGNR.&OS=dn/20180089642&RS=DN/20180089642>
39. Blockstream is Available online at: <https://elementsproject.org/>
40. Website: https://www.reddit.com/r/BlockchainStartups/comments/hqx2qw/how_does_blockchain_technology_help_in_health/?utm_source=share&utm_me%2520dium=web2x
41. Website: <https://cointelegraph.com/news/blockchain-in-health-insurance-more-accuracy-more-transparency-and-more-efficiency>
42. Bhowmik, D., Feng, T.: The multimedia blockchain: a distributed and tamper-proof media transaction framework. In: 22nd International Conference on Digital Signal Processing (DSP) (2017)
43. Timicoin Whitepaper: <https://timihealth.com/timicoinalwhitePaper.pdf>
44. Sylim, P., Liu, F., Marcelo, A., Fontelo, P.: Blockchain technology for detecting falsified and substandard drugs in distribution: pharmaceutical supply chain intervention. *JMIR Res. Protocol* **7**(9) (2018)
45. Medicalchain whitepaper is available online at: <https://medicalchain.com/en/whitepaper/>
46. EncrypGen Whitepaper is available online at: <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4woQm>
47. Benchoufi, M., Ravaud, P.: Blockchain technology for improving clinical research quality. *Natl. Center Biotechnol. Inf.* **18**, 335 (2017)
48. Himss blockchain healthcare is available online at: <https://www.ledgerinsights.com/himss-blockchain-healthcare/>

Chapter 5

A Blockchain Framework for Healthcare Data Management Using Consensus Based Selective Mirror Test Approach



P. S. G. Aruna Sri and D. Lalitha Bhaskari

Abstract Blockchain technology is promptly gaining traction in the healthcare industry as one of the most exciting technological developments. Blockchain technology in the healthcare domain has primarily focused on the complex medical process like clinical trials and surgeries that suffers from drawbacks of permission attainment. Thus, there is a requirement for fault-tolerance and secure blockchain to suit the necessities of the healthcare domain. We recommend a consensus mechanism for healthcare data management that diminishes fault tolerance and yields better data management. In addition to fault tolerance, we propose a solution for managing and accessing a huge amount of medical-based data. The outcome of this work anticipates numerous stack-holders who have engaged themselves in the medical system to provide superior services for data management. From the results, it demonstrates that the proposed approach can provide better trade-off by analyzing different parameters like transaction rate, data encryption, and fault tolerance. This study illustrates the undertakings of utilizing blockchain technology in the health domain are expanding exponentially. There are areas inside the health domain that might be profoundly affected by blockchain technology.

Keywords Blockchain · Complex data management · Consensus · Fault tolerance · Healthcare

5.1 Introduction

Recently, Electronic medical records (EMR) are crucial and extremely sensitive to some private data for prediction and treatment in healthcare industries. This may require constant distribution and sharing of data among various sectors like healthcare providers, pharmacies, insurance companies, patients' families, and researchers and so on [1]. This leads to the foremost confront in maintaining patients' medical history to be more updated [2]. Sharing and storing data among multiple entities may preserve

P. S. G. Aruna Sri (✉) · D. Lalitha Bhaskari

Department of CS&SE, AUCE (A), Andhra University, Visakhapatnam, AP, India

access control towards enormous content that may complicate patients' treatment processes [3]. However, when a patient suffers from a diverse medical condition like HIV, cancer has to hold its history of treatment and post-treatment monitoring and rehabilitation [4]. With constant access to entire medical history may consider being more crucial for patients treatment. For instance, understanding delivered laboratory doses, and the radiation-based outcome is essential for ongoing treatment [5].

Some patients have the habit of visiting various medical institutions for consultation purposes and may be moved from one hospital locality to another one [6]. Based on this legislation, patients are provided with rights over health information and may set specific rules and limitations towards health information retrieval [7]. If patients have to share their clinical data for an investigational purpose or to transform it from one hospital to another is most needed for consent signature, which may represent what kind of data to be shared, recipient information, and period of data that has to be accessed by recipients [8]. This leads to too complicated factors for coordinating specifically when patients move data to another country, region, or city and may not know information regarding hospitals or caregivers where the patients are provided with better care.

Although, if some consent is offered, the data transferring process may be time-consuming, specifically, it is transferred via post [9]. Transferring patients' information via electronic mail through the internet is not considered by most hospitals as it may encounter security risks where patients' healthcare information is in transit. Health Information Exchange (HIE) for ecosystems like common good health alliance attempts to fulfill data from patient's electronic health records more effectually, securely, and appropriately shared between worldwide [9]. This may occur when providers receive a patient's health information based on access. It is complex to fulfill patients' who receive independent opinions from diverse healthcare providers. However, these ecosystems may not resolve basic requirements while transferring data from one place to another.

For the investigational purpose, data aggregation may also need consent until data is anonymized. Moreover, it is measured as an independent release over locally anonymized medical data that is related to similar patients and derived from various sources [10]. For instance, numerous healthcare institutions are visited by patients may lead to patient de-identification, and henceforth privacy violation is considered. Based on a centralized entity that may manage and store patients' data and access control-based strategies shows a single failure point and bottleneck towards the entire system. It also needs to perform either complete operation over data encryption (anonymization or search) or selecting a complete trust entity that may access sensitivity information regarding patients [11]. Therefore, the former function needs data management towards memory, and that may not be appropriate in the hospital environment. Then, the latter function may consider it to be more complex to identify general practice [12]. As an example, a Google-based health wallet may provide patients information that is concerned regarding awareness and privacy of potential risk where sensitive data may be misused.

With access to the shared ledger, transparent history and immutable actions of all functions are considered as network participants (like patients with modified permissions, uploading or accessing newer data, doctor or sharing information for research) who may overcome issues related to the above factors. By offering a tool for achieving consensus between distributed entities devoid of relying upon a single trusted party, blockchain technology may fulfill data security, facilitate healthcare data management, and control over sensitive information for various actors or patients in the medical field [13]. In healthcare set up, transactions are defined as the process of uploading, creating, or transferring EMR data that may perform connections among peers. Some transaction set is clustered at a specific time which is accumulated in a ledger that may record every transaction and henceforth specifies network state. The primary objective of implementing blockchain technology towards healthcare applications is as follows: tampering resistance, immutable and verifiable transactions, integrity, and transparency towards sensitive medical data distribution [14]. This is significantly attained by using a consensus approach based on fault tolerance and data management.

5.1.1 *Blockchain Technology*

An overview of blockchain technology represents in Fig. 5.1. The architecture of blockchain is classified into three layers, i.e., infrastructure layer, platform layer, and distributed computing layer. The infrastructure layer comprises all the components of hardware in order to execute blockchain. Nodes in this layer perform the initiation of transactions, transaction validation, and block generation and retain the ledger's copy. It also contains a storage component that provides the ledger of transaction records in the network. Another component in this layer is network facilities required for communication in the blockchain or among different blockchains. The second layer of the blockchain is the platform layer, consists of (RPC) Remote Procedure Calls, Web Application Programming Interface, and REST (Representational State Transfer) APIs for the Communication purpose.

The distributed computing layer is the third layer in the blockchain architecture that confirms local access to data, immutability, fault tolerance, security, and authenticity. In a peer-to-peer network, nodes consist of the same replica of ledger transactions to provide the immutability feature and uses a consensus algorithm to reach an agreement of decision. This layer is also responsible for user authentication using the encryption technique and data privacy using a hashing technique. Decentralization, Immutability, Transparency, and traceability are the following features of blockchain.

The probability of blockchain utilization towards healthcare-based data management is raised presently with substantial academic and industrial attention. Moreover, only for certain prototype functionality of the system may utilize blockchain towards medical data management anticipated. In this work, the practical execution of a system with a consensus approach is concentrated with fault tolerance along

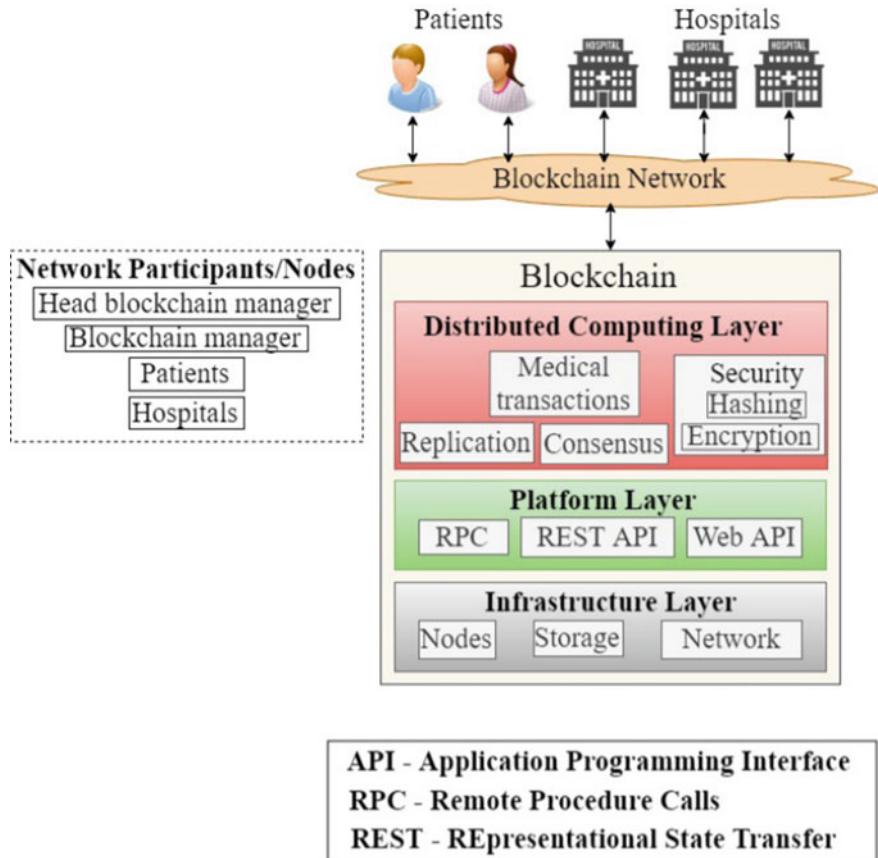


Fig. 5.1 Overview of blockchain technology [15]

with blockchain technology to preserve Metadata and accessing control policies. Data may be stored in the cloud with encryption form and by fault tolerance mechanism. By merging all these technologies that may facilitate data security fulfillment and privacy towards availability of access control policies depicted by patients.

5.2 Related Works

5.2.1 Traditional Healthcare Data Management

Healthcare data management is based on the storage of patient's medical information and manages to give enriched care, disease tracking, and its causes. Today, EHRs are generally utilized by hospitals and health providers to manage patients' medical

data using a client-server architecture [16, 17]. But in this type of healthcare data management system, the hospitals are the primary custodians of the data. A few cloud-based medical services information the executives' frameworks have been set up by the scholarly community and industry so as to permit a patient to follow his/her clinical information from various associations [18, 19]. However, cloud-based centralized database system stores patients health information suffers from a single point of failure system disclosed to errors, cyber-attacks, and information loss.

5.2.2 *Blockchain-Based Healthcare Data Management*

This section discusses Personally Controlled health care records that may initiate a patient-centric healthcare data sharing model dependent on role-based and discretionary based access control approaches. In this model, patients may construct the ultimate objective-based authority in demonstrating data access. Enigma is considered a decentralized computational platform that may determine privacy, along with data and computation storage, to acquire scalability and privacy [20]. Data is partitioned into unknown chunks, and every node must evaluate one data chunk, indeed of blockchain data that are not computed and replicated by each node. Moreover, to control the system, an external blockchain is used, handling access control and event database with tamper-proof. This model utilizes blockchain to remove third-party access to personal data. As an outcome, users may be competent to control accessing to own data [21]. The system has been executed based on the merging of off-chain storage and pointer for storing encrypted data on the bit-coin-based blockchain. This system serving of blockchain may deal with querying and sharing of data.

The author in Fehrenbacher, Helfert [22] considers Medrec as an essential execution of an access control system that may utilize blockchain technology. It is executed with Ethereum technology with specific modification of the mining procedure. It offers reward-based mining techniques to attempt medical stakeholders to participate in the system and validate transactions as miners. The author in Knieke et al. [23] anticipated a blockchain framework for accessing electronic medical data preserved in cloud repositories. Some system is dependent on the permission-based blockchain; henceforth authorized users only access system by validating cryptographic keys. This testing performance is dependent on comparison with blockchain, and bitcoin-based blockchain illustrates scalable and light-based design. In Zheng et al. [4], the author offers an execution towards role-based access control with smart contracts and confronts response protocol dependent on the Ethereum platform. The challenge-response protocol is modeled to authenticate ownership roles and for user verification. Some authors may concentrate on trans-organization for accessing control, user service access for organizations dependent on a role in another organization.

In Zyskind and Nathan [24], the author uses the blockchain model for EHR record validation using an attribute-based signature model through several authorities. Report evaluation demonstrates that this system may be strong against collusion attacks along with privacy preservation. Even though there is enormous work

associated with blockchain-based access control. MediChain is primarily executed with real-world functionalities of applications dependent on Hyperledger fabric and composer to user permission blockchain to resolve efficiency and privacy issues in health care systems.

A simple blockchain definition is provided as an open, distributed ledger that may record effectual transactions among two parties and a permanent method for verification. Conventional currencies have to trust the third party, generally, banks and governments, to fulfill transactions underwritten funds and validate identification to eliminate fraud [25]. This is a confronting approach over the internet where identity is complex to fulfill, and therefore transactions may not be trusted completely. Bitcoin is measured as the underlying technology for peer-to-peer electronic currency (cryptocurrency), offering an improved solution to the Byzantine General Problem. This is the way to attain consensus between peer groups where individual group members are transmitting inappropriate information deliberately. For instance, double count payment toward bank account may provide false identity. Bitcoin paper-based solution is provided to offer a mechanism for interchanging electronic coins, that is, fungible specification of stored values) devoid of requirements to rely upon centralized third-party trust to fulfill the security and integrity of the underlying currency.

Bitcoin reliability degree and trust may stem from public network host, and clear history towards every transaction may be considered here. Ethereum is measured as a public network; however, it is probable to develop a private solution as the hyper ledger. This may be beneficial when data has to be private. However, organizations need to show benefits over identity, and intrinsically that may build blockchain and offer usage justification for trusting technology intrinsically over complex environments [26]. Generally, blockchain may attain some advantages over various facts at a potential degree in the provided network's mistrust peer. Private blockchain may offer 'Proof of Work' for another, lesser computation expensively; block creation methods as 'proof of authority.' Here, distributed system nods maybe vote to accept complete transactions, which is more sensible in some systems that may eliminate any single node form the entire network control factor.

With enormous transaction over digital technology that is brought in every year is measured as blockchain as 'disruptive' technology poised for rapid transformation over business sectors and the economy. Indeed of this hype, in the last few decades of blockchain development has shown tremendous internal growth; however, it fails to deliver transformational impact [27]. Now, there is an acceptance that blockchain is lesser disruptive than a foundational one, indeed of providing methods for substituting prevailing working models directly, as the internet may perform with banking. It may offer background knowledge over future technology for disruption and innovation [28]. This is compared with the network protocol that underpins the internet. Unique development in the latter 1970s, it may be a decade before WWW creation and before internet emergence of internet facilitated companies like Google.

5.3 Proposed Methodology

Although there are numerous healthcare institutions, the volume of data produced in this era is continuously growing. However, privacy and security are avoided intentionally. As an outcome, numerous organizations may experience huge reputation loss and capital. Various users of healthcare may play diverse roles, and data access has to be allocated. This access mode can be fulfilled by blockchain technologies. MedRec is considered as a decentralized management system where data operation and permission are recorded in a blockchain, and implementation is performed. It has collaborated with medical information for data confidentiality, authentication, auditing, and sharing. It may provide immutable data services. In some work, the author may achieve controllable data management in the cloud environment to resolve the user's concerns regarding control lack. Here, it may be designed for trust authority to facilitate users to prevent mal functioning during significant attacks. With the data management system, the user may control entire health records using blockchain. Moreover, there is no authorization design and access control during implementation. Based on this decentralized management system, a consensus mechanism has been designed.

5.3.1 *Consensus Mechanism*

With context to the decentralized blockchain, when a block is identified to enter network broadcasting, every node may hold an option to include a block to copy of global ledger or may eliminate it. It is used to seek primary network functions to handle a single state to secure global ledger expansion and eliminate various maliciousness-based attempts.

When a block is higher, a shared global ledger may be updated. Adverse effects may be identified when the node determines the tampering of a copy state when several collusively try tampering. To facilitate blockchain functionality with correctness and security, a shared ledger must provide security and efficiency for this consensus algorithm. This can cause fault tolerance and fulfills simultaneous maintenance if blockchain, and it may not rely upon the central authority to maintain malicious adversaries for co-ordination disturbing the process.

To be specific, message transmission among nodes must be approved by the network's significant participation through consensus management. As well, the network may be resilient to partial failures, and nodes are malicious or when the message is corrupted. The most acceptable consensus mechanism that is utilized by blockchain implementation has to fulfill efficient transaction ledger with essential properties: liveliness and persistence. It may fulfill nominal responses from the system based on state transactions. For instance, if the network node state is considered to be stable, then other nodes have to report stability. State node liveliness may eventually agree with decision values. By merging liveliness and persistence, it may

fulfill transaction ledger to be positive as authentic transactions are approved and considered to be permanent.

Finally, it is known that the blockchain role is to replace a centralized database with precise access control. Some data may record global ledger blockchain; it has invalid blockchain variation. It may enforce a significant agreement for validating consensus. It fulfills the consistency state and eliminates the spending problem. Therefore, this work analyses' Proof of Word' from the consensus mechanism to analyze data management in the healthcare sector. Before analyzing the Proof of Word, the transaction model must be designed.

5.3.2 Transaction Level Modeling

Generally, BC is generated and retained as a distributed ledger for any online transaction. Here two diverse blockchains transactional modeling: unspent transactions and account-based transaction models.

Privacy degree 1. It is considered as a data structure that may hold several instances devoid of combining them into one account. By handling these sorts of instances, the holder needs to disclose to pay. This specifies that the payer may perform multiple payments at the same time.

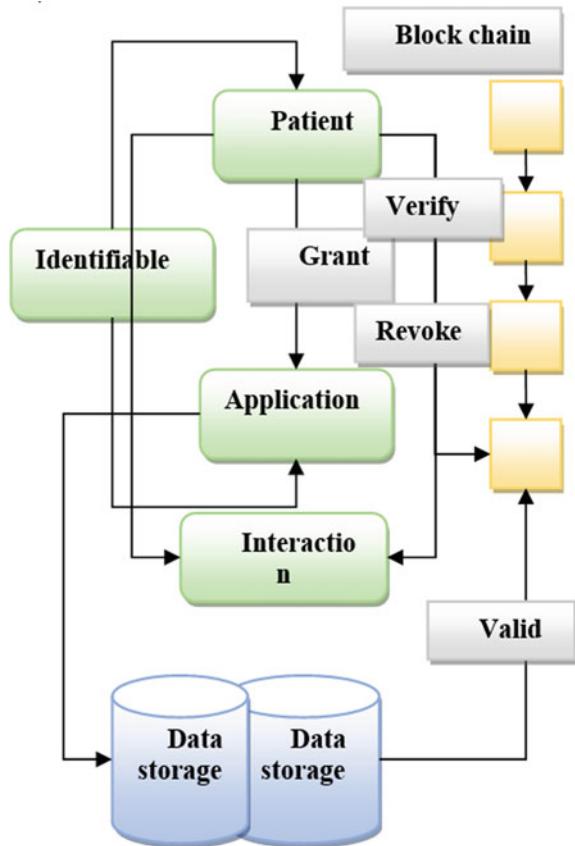
Scalability degree 2. This may eliminate certain constraints over the account-based transactional model. Here, parallel transactions may be performed independently, devoid of considering the order of transactions. This is because; it trusts on hash functions to recognize its initial state. Therefore, it is difficult for mis-ordered transactions. The transaction sequence number must be tracked in the case of distributed systems.

Security degree 3. It maintains proof of ownership for all instances. Conflicts are reduced to a double-spending problem; currency-based transactions may be duplicated easily. It may resolve the spending problem by enforcing consensus mechanisms for newer blocks to blockchain and maintains it as a universal ledger.

5.3.3 Health Data Interoperability

Interoperability resources are measured as an evolving functionality that determines data format and elements with widely accessible interfaces for health record transactions, as in Fig. 5.2. Standard was managed and created by standard organizations. It is established with a license without restriction that may serve various facilities for broader adoption. It gives probability to expanded use of cloud applications, device integration, and modified healthcare workflows. It facilitates data element separation into pre-defined structured data types as resources. Segmented resources

Fig. 5.2 Shows the data management flow



are constructed with data transfer more desirably. This resource may follow state transfer principles and validates structural standard, and conformance statements termed profiles. Transactions include the following characteristics,

Hashing: SHA algorithm can be used for resource payload. Resources may not enter blockchain until hash provides verification to transactions.

Signature: node must hold the originator signature.

URL: refers to actual resource location.

Profiles: it is held for resource conformation.

Index: encrypted index may facilitate data discovery without information leakage.

Hashes of every transaction must contribute block header. It comprises of metadata, which can be used to validate new data. Hash—a hashing algorithm is provided to every block. Assume the root has two children C_0 and C_1 with previous blocks, b_{n-1} . let hash is equal to the concatenation of b_{n-1} , C_0 , C_1 hashes. Block hashing—hash of blocks are considered for validation. Signature—nodes are contributed to blocking; a signature is needed based on the requirement. This may

fulfill blocks for validation after the miner assumption. Election—nodes have to contribute a random number encrypted with the private key. This is utilized to choose the next miner.

Algorithm 1: Adding data block with SHA

Input: registration request; nodes in network

Output: registered users of block

Step.1 $K_{pub,pri} = Keyconstruct()$

Step.2 $ID \rightarrow generateuserID$

Step.3 $location \rightarrow generateblockchainlocation() + (k_{pub,pri})$;

Step.4 $(ID, K_{pri}) \rightarrow store(ID, K_{pri})$;

Step.5 $puzzle \rightarrow checkblock() + (K_{pub,pri})$;

Step.6 $forall'n'$ blocks do

Step.7 $checkvalidation$;

Step.8 $endfor$

Step.9 $u \rightarrow userverification()$

The data stored in this model is secured through the SHA hashing function, and it will be protected against malicious attempts to unauthorized access, while users are assigned private keys for signing and validation of every transaction. Signature and encryptions are used in the network to fulfill stored healthcare records. Moreover, a consensus algorithm may be controlled by at least 50% in the network for changing healthcare data. For changing data, every copy of the global ledger has to be modified. Here, every user block are hashed, and hashes of all transactions are maintained in the blockchain. For example, SHA-512. The message blocks are processed one at a time: Beginning with a fixed initial hash value $H(0)$, sequentially compute $H(i) = H(i1) + CM(i)(H(i1))$; where C is the SHA-512 compression function and + means word-wise mod 2^{64} addition. $H(N)$ is the hash of M.

Algorithm 2: Block for data management

Input: set of nodes in network; consensus time for PoW

Output: create new block

Step.1 Initialize preliminary data transaction {};

Step.2 $\beta \rightarrow$ fitness computation (N);

Step.3 $while block_{time} < T_c$ do

Step.4 $forall n \in \{N - \beta\}$ do

Step.5 $n \rightarrow n + gettransactionfromnode(n)$;

Step.6 endfor

Step.7 End while

Step.8 Generate transaction block;

Step.9 $b_{n+1} \rightarrow generateblock(R)$;

Step.10 $forall n \in \{N - \beta\}$ do

Step.11 verifyblock{};

Step.12 endfor;

Step.13 $forall n \in N$ do;

Step.14 managedatablockwithhealthrecord;

Step.15 endfor

This may also fulfill system availability by eliminating any single point failure. With this, it is complicated for all adversaries to launch DoS attacks over the registration system. Every transaction has to be validated from the network node by making it complicated for fraudulent to initiate malicious connections. In the case of computational efficiency, users may run the lightweight client to store transactions indeed of a complete copy of blockchains, which are storage expensive. This may be computationally powerful with efficiency storage capacity, and users may manage records more effectually.

5.3.4 Fault Tolerance

The basic idea behind fault tolerance is for implementing large scale data applications. The input is data mapping from various tasks from sub-blocks to processors to determine to schedule, and fault-tolerant output is attained. The objective is to determine sub-tasks based on applications and schedules. The task key is determined in healthcare applications. To have a better understanding of this function, slack time and key sub-tasks has to be expanded. For a block is provided with a schedule, every sub-task has been completed based on scheduled time. Specifically, some may fail during the execution process. Then, the key block has to supply checkpoint files to perform further operations.

Algorithm 3: Fault tolerance in blocks

Input: sub-task key

Output: block fault tolerance

Step.1 Initialize key

Step.2 Apply it to block over chain

Step.3 If there is non-overlapping of tasks based of schedule then

Step.4 Deploy τ_i^P

Step.5 End if

Step.6 If τ_i^P is not deployed over input block

Step.7 Apply to available block

Step.8 Deploy new block with sub-tasks

Step.9 Put tasks to new block

Step.10 End if

Step.11 Deploy check point interval

Step.12 Save delay value

Step.13 Return fault computed value

However, delays encountered during this process may lead to sub-task failures and may affect the blocks. If the failed sub-task has slack, it may be influenced in the initial phase of computation. For performing block computation, the threshold has to be fixed; this should be related to the makespan of healthcare applications. This means that a higher threshold value may show more sub-tasks; when this value is smaller, it causes longer makespan. The sub-task is adopted with a mirror task to enhance fault tolerance performance. Finally, this mirrored task has to be deployed over a copy of the sub-task key over another processor. Sub-task is specified as τ_i^P , and its copy is provided as τ_i^C both these may commence at an earlier stage and generate a checkpoint interval $2\varphi_{opt}$.

$$\text{Delayrate} = \frac{\text{Practical makeapan}}{\text{ideal makespan}} \quad (5.1)$$

The distance between both the tasks is measured for providing checkpoint intervals. When failure occurs in one block, checkpoint interval if two sub-task may leads to delay by dealing with failure. To determine optimal fault tolerance of blockchain application, the delay has to be computed until the completion of the application, i.e., makespan has to be evaluated.

5.4 Results and Discussions

The proposed method shows better performance in healthcare data management in contrast to other models as blockchain technology remains to be evolved based on blockchain construction, validation, and assessment. It is classified into three fields:

- (1) The public, consortium, and private blockchain. In public, it is open to read, receive, and send transactions and facilitates participants to join consensus procedure for making decisions over blocks for appropriate transactions and added to the blockchain. Then, the consortium is based on constraints like permissions that are pre-selected for some participants in the network, which may be influenced and managed by a consensus process. Finally, private is based on getting permission for strictly prohibiting single participants, although read is accessible to openly for constraint set of participants. However, performance and security may be different for consensus speed. This is also monitored by a trusted authority. Therefore, it fulfills three characteristics: usage of decentralized peer to peer network,
- (2) Every transaction is digitally signed.
- (3) Consensus is synchronized for network replication. Even though there is a vast growth in the blockchain mechanism, it is exceptionally complex to fulfill data management, security, and privacy.

Figure 5.3 depicts node creation, node connectivity, and node establishment in the network. Initially, the node connection is established for having effectual data broadcast and retrieval.

Table 5.1 determines the block data format with the number of bytes it holds during every transaction.

Figure 5.4 shows the hash (SHA) functionality among nodes to ensure security and avoid fraudulently.

Figure 5.5 illustrates the block size and transaction of healthcare data among those blocks.

Figure 5.6 shows accuracy when data transmission is higher among nodes. This method shows better accuracy and security by adopting SHA algorithm for hashing and to generate puzzle solution. Therefore, “Proof of Word” works effectually in blockchain management for accessing health care data with consensus mechanism.

Figure 5.7 depicts the fault tolerance value of the proposed model, where it is based on the threshold value provided to every block to identify the delay during overlap. When the value is smaller, it leads to a longer make span; when it is higher, it leads to a smaller make span. Thereby, fault tolerance is measured.

5.5 Conclusion

The blockchain depicts solution for information sharing while handling security issues and facilitating transparency over every transactional record. These advantages are provided by constructing applications that facilitate data sharing and trust while gaining more values. This may offer unique opportunities to model trusted and secured data sharing and management system based on a consensus approach. This blockchain technology may provide way for modular design merged with medical providers of prevailing systems, local data storage-based solutions and facilitates

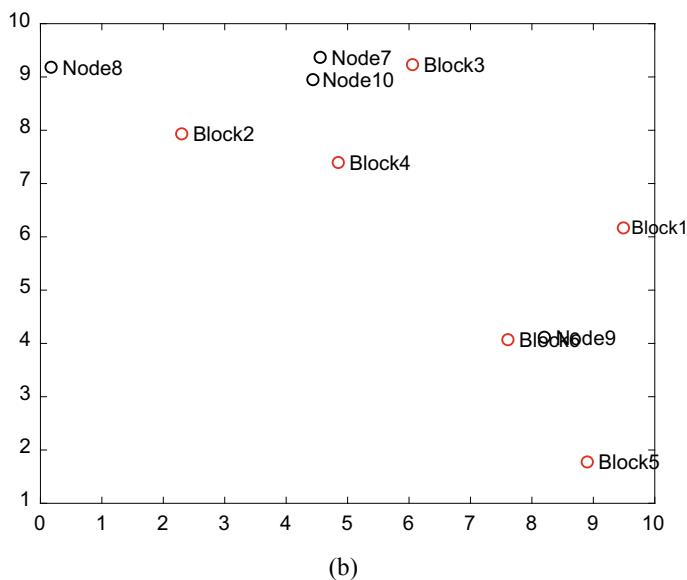
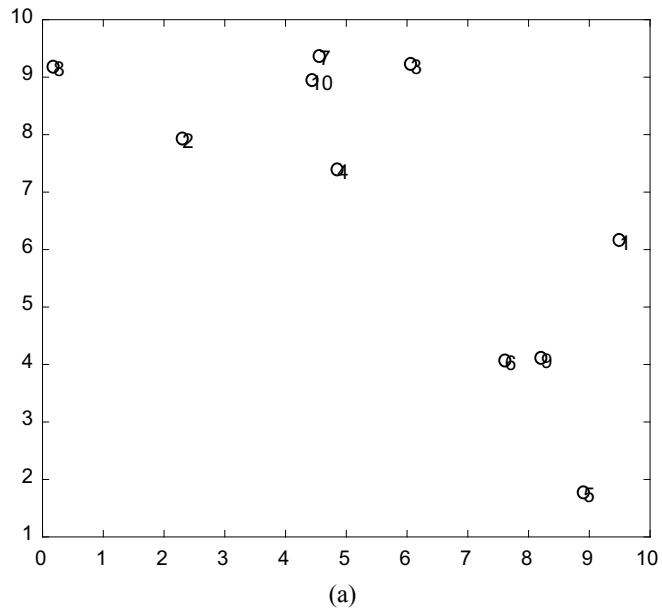
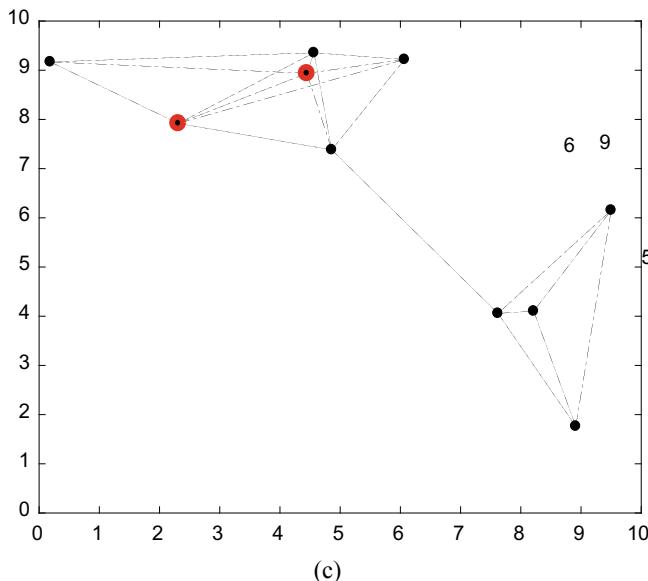


Fig. 5.3 **a** Node creation in-network, **b** block creation and **c** block connectivity

**Fig. 5.3** (continued)**Table 5.1** Various formats, their fields, and sizes

Format	Field	Size
Block data	Block size	4 bytes
	Number	4 bytes
Header	Version	4 bytes
	Block hash	32 bytes
	Merkle	32 bytes
	Timestamp	4 bytes
	Target	4 bytes
Transaction	Transaction counter	1 to 9 bytes
	Transaction list	Up to 1 MB

developing and interoperability with ‘Proof of Word’ for the adaptable and convenient system. This work is concluded by establishing interaction among the healthcare domain and blockchain-based technology, which may be inevitable with fault tolerance mechanism, as technology may offer real solutions for sharing data while measuring security properties. Nonetheless, the resources needed for implementation have been projected to sustain developments towards long term solutions. Several benefits of using the selective mirrored task method we can apply to other blockchain application scenarios to improve the fault tolerance of multiple applications in the future.

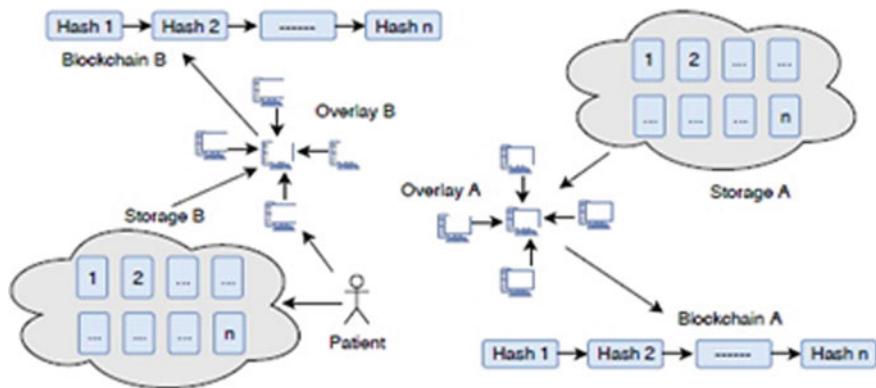


Fig. 5.4 Functionality of a Hash function

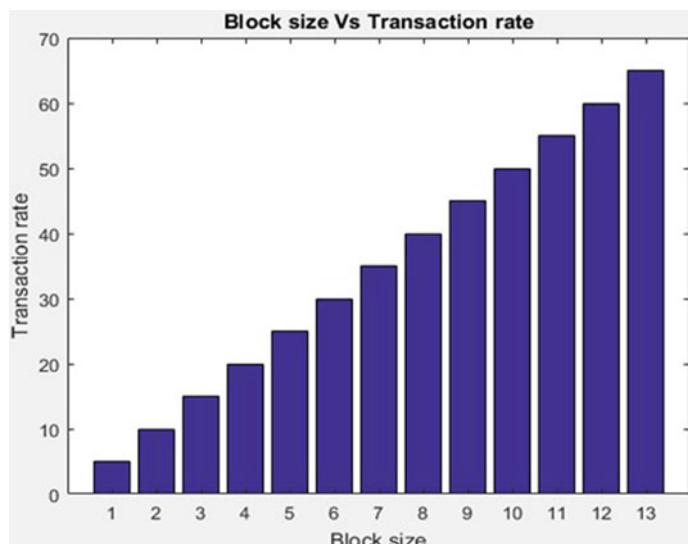


Fig. 5.5 Clock size versus transaction rate

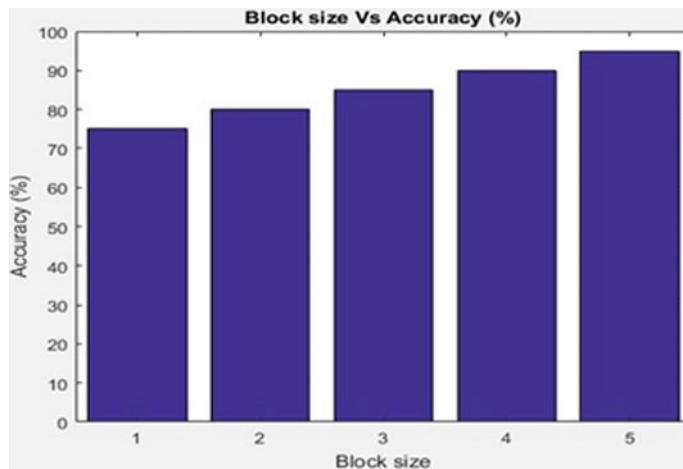


Fig. 5.6 Accuracy in data encryption

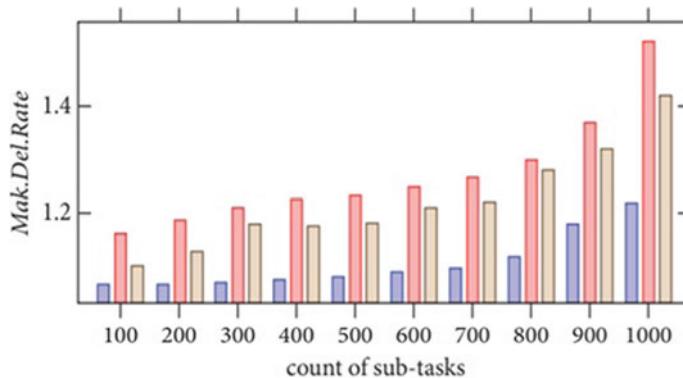


Fig. 5.7 Makespan computation for fault tolerance

References

1. Bell, E.A., Ohno-Machado, L., Grando, M.A.: Sharing my health data: a survey of data sharing preferences of healthy individuals. In: AMIA Annual Symposium Proceedings, p. 1699. American Medical Informatics Association (2014)
2. Engelhardt, M.A.: Hitching healthcare to the chain: an introduction to blockchain technology in the healthcare sector. Technol. Innov. Manage. Rev. **7**(10)
3. Randall, D., Goel, P., Abujamra, R.: Blockchain applications and use cases in health information technology. J. Health Med. Inf. **8**(3), 8–11 (2017)
4. Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H.: An overview of blockchain technology: architecture, consensus, and future trends. In: 2017 IEEE international congress on big data (BigData congress): IEEE; 2017. p. 557–564.
5. Tarasiewicz, M., Newman, A.: Cryptocurrencies as distributed community experiments. In: Handbook of Digital Currency, pp. 201–222. Elsevier (2015)

6. McCarthy, J.: MedStar Attack Found to Be Ransomware. Hackers Demand Bitcoin, Health IT News (2016)
7. Mainelli, M., Smith, M.: Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology). *J. Fin. Perspect.* **3**(3) (2015)
8. Mettler, M.: Applications and Services (Healthcom) (IEEE) Blockchain technology in healthcare: the revolution starts here. In: IEEE 18th International Conference on e-Health Networking, pp. 1–3 (2016)
9. Yue, X., Wang, H., Jin, D., Li, M., Jiang, W.: Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. *J. Med. Syst.* **40**(10), 218 (2016)
10. McKernan, K.J.: The chloroplast genome hidden in plain sight, open access publishing and anti-fragile distributed data sources. *Mitochondrial DNA Part A* **27**(6), 4518–4519 (2016)
11. Linn, L.A., Koo, M.B.: Blockchain for health data and its potential use in health it and health care related research. ONC/NIST Use of Blockchain for Healthcare and Research Workshop Gaithersburg, Maryland, United States: ONC/NIST2016, pp. 1–10.
12. Ge, Y., Ahn, D.K., Unde, B., Gage, H.D., Carr, J.J.: Patient-controlled sharing of medical imaging data across unaffiliated healthcare organizations. *J. Am. Med. Inform. Assoc.* **20**(1), 157–163 (2013)
13. Vest, J.R., Gamm, L.D.: Health information exchange: persistent challenges and new strategies. *J. Am. Med. Inform. Assoc.* **17**(3), 288–294 (2010)
14. Cheng, R., Zhang, F., Kos, J., He, W., Hynes, N., Johnson, N., et al.: Ekiden: a platform for confidentiality-preserving, trustworthy, and performant smart contracts. In: 2019 IEEE European Symposium on Security and Privacy (EuroS&P), pp. 185–200. IEEE (2019)
15. Ismail, L., Materwala, H., Zeadally, S.: Lightweight blockchain for healthcare. *IEEE Access* **7**, 149935–149951 (2019)
16. Rind, D.M., Kohane, I.S., Szolovits, P., Safran, C., Chueh, H.C., Barnett, G.O.: Maintaining the confidentiality of medical records shared over the Internet and the World Wide Web. *Ann. Intern. Med.* **127**(2), 138–141 (1997)
17. Gritzalis, D., Lambrinoudakis, C.: A security architecture for interconnecting health information systems. *Int. J. Med. Informatics* **73**(3), 305–309 (2004)
18. Bahga, A., Madisetti, V.K.: A cloud-based approach for interoperable electronic health records (EHRs). *IEEE J. Biomed. Health Inf.* **17**(5), 894–906 (2013)
19. Zangara, G., Corso, P.P., Cangemi, F., Millonzi, F., Collova, F., Scarlatella, A.: A Cloud Based Architecture to Support Electronic Health Record, vol. 207, pp. 380–389. IOS Press (2014)
20. Peters, G.W., Panayi, E.: Understanding modern banking ledgers through blockchain technologies: future of transaction processing and smart contracts on the internet of money. In: Banking Beyond Banks and Money, pp. 239–278. Springer (2016)
21. Ramachandran, G.S., Radhakrishnan, R., Krishnamachari, B.: Towards a decentralized data marketplace for smart cities. In: 2018 IEEE International Smart Cities Conference (ISC2), pp. 1–8. IEEE (2018)
22. Fehrenbacher, D.D., Helfert, M.: Contextual factors influencing perceived importance and trade-offs of information quality. *Commun. Assoc. Inf. Syst.* **30**, 111–126 (2012)
23. Knieke, C., Lawrenz, S., Fröhling, M., Goldmann, D., Rausch, A.: Predictive and flexible Circular Economy approaches for highly integrated products and their materials as given in E-Mobility and ICT, pp. 22–31. Trans Tech Publ, Materials Science Forum (2019)
24. Zyskind, G., Nathan, O.: Decentralizing privacy: using blockchain to protect personal data. In: 2015 IEEE Security and Privacy Workshops, pp. 180–184. IEEE (2015)
25. Xia, Q., Sifah, E.B., Smahi, A., Amofa, S., Zhang, X.: BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. *Information* **8**(2), 44 (2017)
26. Azaria, A., Ekblaw, A., Vieira, T., Lippman, A.: Medrec: using blockchain for medical data access and permission management. In: 2016 2nd International Conference on Open and Big Data (OBD), pp. 25–30. IEEE (2016)
27. Wachter, R.: Making IT work: harnessing the power of health information technology to improve care in England. Department of Health, London, UK (2016)

28. Michie, S., Yardley, L., West, R., Patrick, K., Greaves, F.: Developing and evaluating digital interventions to promote behavior change in health and health care: recommendations resulting from an international workshop. *J. Med. Internet Res.* **19**(6), e232 (2017)

Chapter 6

Blockchain Technology in Healthcare: Opportunities and Challenges



Sachikanta Dash, Pradosh Kumar Gantayat, and Rajendra Kumar Das

Abstract There are a few issues found because of the absence of traceability of transactions in healthcare services. Healthcare information split across numerous silos adversely influences research activities and administrations. There were no reported cases of about half of the clinical preliminaries. The expense of medication disclosure is ever-expanding, and unsatisfactory and fake medicines are as yet an enormous issue. Blockchain has the potential to address such substantial problems. Blockchain technology is a distributed and secure database organized by various groups to store and offers a permanent online transaction record. Blockchain has numerous medicinal services applications and can improve mobile health applications, preliminary clinical information, and insurance information storage. Each of the blocks has an independent unit holding its report and a dependent link that makes regulated by participants who store and share the data without third-party intervention. The blockchain technology permits members to transfer information progressively without presenting the channels to theft, malice, and forgery. In this work, we review major blockchain healthcare applications in some areas of patient information management, supply chain management of clinical goods, pharmaceutical investigation, and telemedicine related to healthcare activities.

Keywords Blockchain technology · Telemedicine · Supply chain · Disease outbreaks

6.1 Introduction

The technology of blockchain (BC), with acquired attributes, for example anonymization, transparency and decentralization was presented in the year 2008 in Bitcoin cryptocurrency. By March 19, 2019, the Bitcoins with near about 400 million finished

S. Dash (✉) · P. K. Gantayat

Department of CSE, DRIEMS (Autonomous), Cuttack 754022, India

R. K. Das

Department of ENTC, DRIEMS (Autonomous), Cuttack 754022, India

transactions which speaks to strong use case of BC technology. This has prompted conversations with recommendations that BC technology may be valuable in a scope of different information domain [1].

As indicated by IBM, more than 70% of human services leaders have the prediction that the best effect of BC inside the healthcare area will be an enhancement of medical preliminary supervision, administrative consistence and giving a decentralized system to contribute electronic health restrings (EHR) [2]. Also, the worldwide BC technology promote in medicinal services trade is relied upon to cross USD 500 million by 2022 [3]. In spite of the fact that BC technology is consider to have prospective for genuine development of healthcare information frameworks [4], the ongoing publicity of this technique likewise involves ridiculous proposition and thoughts and current writing gives little outline of utilizations that have been created, tried and additionally conveyed.

This is significant to examine if the present exploration meet the desires to BC technique inside medicinal services, healthcare sciences and healthcare education (from after this, alluded to as “the wellbeing do-fundamental”). This investigation aims to deliberately survey, evaluate and synthesize distributed companion inspected examines where BC has been used to get better process and service inside the healthcare domain. It is an exceptionally energizing time domain for healthcare sector and IT sector. Because of enhancements in genetic research area and the advancement of exactness medication, health care is seeing an imaginative way to deal with disease prevention and treatment that joins an individual patient’s genetic cosmetics, way of life and condition. At the same time, IT advancement has delivered enormous information bases of health information, given devices to follow health information in their health care. Joining this advancement in health care and information technology would promote transitive changes in the IT sector of health.

The American Recovery and Reinvestment Act required all open and private health care suppliers to adopt electronic clinical records (EMR) by January 1, 2014, to keep up their current Medicaid and Medicare repayment levels. This EMR command prodded huge development in the accessibility and use of EMRs. Be that as it may, by far most of these frameworks can’t share their health information. BC technology can address the challenges in present health IT frameworks and act as a specialized standard that empowers people, health care suppliers, health care elements and clinical researchers to share electronic health information securely. This paper portray a BC-based admittance control administrator to health records that would advance the business interoperability challenges communicated through the Office of the National Coordinator for Health Information Technology’s. Interoperability is additionally a basic segment of any framework supporting Patient Centered Outcomes Research (PCOR) and the Precision Medicine Initiative (PMI). A public health IT foundation dependent on BC has sweeping potential to advance the improvement of exactness medication, advance clinical research and welcome patients to be more responsible for their health. BC is considered as a record framework that helps with overseeing and putting away information in various blocks which will work essentially decentralized way above any processing systems and connecting utilizing cryptography. The BC capacities have a capability of more extensive acknowledge [5].

Nonetheless, application scenes and viable arrangement configuration are as yet immature. BC guarantees crucial changes across various enterprises, including fintech, government, health and supply chain. Its potential advantages remember decrease for expenses and unpredictability of transactions within various party, upgraded security, enhanced simplicity and guideline. The healthcare is portrayed as a conventional industry that is significantly inflexible to quantify because of the realities of progress and impervious to creative practice. Problem in health sector have been attracting consideration in late years around the world. BC technologies have been progressively perceived as an instrument to deal with available information circulation issue. It might progress quick healthcare rehearses, for instance, in civilizing health service conveyance and nature of care uphold [6].

6.2 Fundamentals of Blockchain Technology

The Blockchain can be depicted as a changeless record that logs information passages in a decentralized way. It empowers substances to connect without the nearness of a focal confided in an outsider. The BC keeps up a constantly developing arrangement of information passages, bundle mutually into block of information. Such types of blocks are connected to the past and future blocks with the cryptographic conventions [7] after the acceptance to BC. In blockchain's unique structure, these information blocks are lucid, writable and sealed by all. For example, permits de-unified transactions and information management. Because of these properties, BC has increased a lot of consideration for different applications.

BC is a shared (P2P) dispersed record technology for another generation of transactional applications that build up transparency and trust. BC is the basic texture for Bitcoin and is a plan design comprising of three principal parts: a distributed network, a shared ledger and digital transactions [8].

This technological arrangement works chiefly in a decentralized way to permanently store computerized information. This plan makes a change of the information incomprehensible [9], when record in block, the information can't be adjusted without modification of every subsequent block, requiring a consensus of the network greater part. In contrast to conventional approaches to store information on one essential issue, the BC utilizes a distributed (P2) network include many duplicate of analogous information that are put together in a range of areas and different gadgets [10]. A friend permits a bit of figuring assets (for example, processing powers, circle stock-piling, network bandwidth etc.), that to utilized for different participant, exclusive of their prerequisite for inner management through workers. Similar type of hubs may take various jobs during guaranteeing conservation of business information exchanges within the network system [11].

6.2.1 Key Characteristic Features

The key characteristic of BC is a decentralization process where no focal authority controls the substance included to the BC. Rather, the en-attempts gave to the BC are settled ahead in a distributed network utilizing different consensus conventions. An additional key trait of BC is consistency. It is difficult to erase passages in the wake of being accepted onto the BC because of the appropriated record, put away over different hubs [12]. Besides, the chance of obscurity (or pseudonymity) is an engaging trademark used in numerous BCs.

The qualities of the BC, with its decentralized nature, permissionless and transparency, may offer an exceptional answer in healthcare system. More extensive technological pertinence clears its process into various parts of medical care system, including development and wearable of investigation in medical science. Healthcare segment has developing requests for BC improvements, and an ongoing overview by Deloitte demonstrates that conventional business is effectively investigated new roads for the utilization of the BC for addressing its basic need.

The BC permanence is the indispensable alternative way in healthcare information system. It can protect medical healthcare report, the aftereffects of clinical preliminaries and guarantee administrative fulfillment. Work of smart contract illustrates the utilization of BC to help constant patient observing and clinical intercessions [13]. Further use of BC identifies with the supply chain in pharmaceutical and creating measures against fake medications. Whereas the advancement of new medications brings about generous costs identified with preliminaries to assess wellbeing and adequacy of the medication, the smart contract utilization permits to encourage the method of the knowledgeable consent as improving recognize management and information quality [14]. Giving admittance to patients to dealing with their own distinguish additionally permits joining of the informed consent method while guaranteeing the security of individual health information.

6.2.2 Type of Blockchain

As delineated in Table 6.1, there are, for the most part, three sorts of blockchains: open (permissionless) or public, consortium or grouping and private or confidential [15]. They have various attributes concerning who can get to, compose and read the information on the BC. All can see the information in an open chain, and anybody may join and add to both consensus (in principle) and change to the centre programming feature. The open BC is broadly utilized in cryptocurrencies. There are two major cryptocurrencies which include Ethereum and Bitcoin, are sorted as open, permission less chains. A consortium BC can be considered partially concentrated, with just a predetermined number of selected gatherings of substances approaching perspective and participate in the consensus convention. In a private BC, the network is dispersed at this point frequently unified. Blockchain can be Public or Private relying upon the

Table 6.1 Different types of blockchain

Features	Open BC	Grouping BC	Confidential BC
Determining consent	Every participants	Specific node set	Single node
Read authorization	Public	Restricted or public	Restricted or public
Immutability	Quite impossible	Might tampered	Might tampered
effectiveness	Minimum	Maximum	Maximum
Centralized	Never	Partially agreed	Agreed
Processing consensus	Permission less	With permission	With permission

consent level [16], however here we comprehensively group it to three distinct degrees of granularity.

Open or public BC is permissionless, and anybody can undoubtedly participate and approve the transactions. Transactions are open and unknown/pseudonymous. The open network keeps up the blockchain, so there is the most significant level of decentralized trust. Bitcoin is the pioneer open blockchain. Bitcoin, Ethereum.

Unified or Grouping BC, A united BC, is a permission BC working under the leadership of a gathering regularly called the consortium. Predefined consortium hubs control the consensus. The transactions could be open.

Private or confidential BC, A private BC, is a permission BC concentrated to one administering organization. Transactions are approved inside and might be open coherent. Private BCs generally have quicker block times and can process higher transaction throughput. Nonetheless, these are defenceless against security breaks. The estimation of private BC can be viewed as a trust transformer where trust depends on a calculation instead of power.

6.2.3 Consensus Mechanism

The mechanism of consensus prevents the double spending of a formerly spend transaction causes disagreement with the present state; in this manner, the transaction is dismissed and that will by no means be included to blockchain. The consensus convention incorporates the principles for the transaction approval, accepting the freshly prepared block into the chain, and collection of fork/partition in the event of network partition. Depends upon the unique situation, and the utilization case, the requirement and necessity for the consensus could vary. The mechanism for consensus may be broadly classified as local or global.

1. In the worldwide consensus model, the primary block called genesis block of the chain is basic for all hubs in the network, and each hub concurs on similar condition of the network and stores the total chain to approve any transaction. Most of the normal instances are Bitcoin and Ethereum from the worldwide BC consensus.

Table 6.2 The comparison mechanism for consensus

Property	PoW	PoS	PBFT
Node management	Open	Open	Permissioned
Energy consumption	High	Medium	Low
Tolerated power of	<25%	<51%	<33.3% faulty
Adversary	Computing power	Stake	Replicas
Example	Bitcoin [1]	Peercoin	Hyperledger fabric

2. From the recent consensus model, each participant claims an individual genesis block and the consensus is just reached among the parties engaged with the transactions. This nearby consensus minimizes the capacity necessities on singular hubs and is generally more adaptable than worldwide consensus. The various BCs models are Nano and TrustChain.

The majority of the current blockchains employ some form of the consensus gathering of the Bitcoins called Nakamoto consensus [17]. The Nakamoto consensus is a worldwide consensus model; it utilizes proof of work (PoW) for accepting the new block and direct to choose the greatest chain if there ought to be an occurrence of network partitions. The Proof of Stake (PoS), is a process to select an favorable node that is determined in the BC. As per crypto-currency, the stake is the balances of a given currency. Due to its advancement, several hybrid PoS models have been proposed to select the approving node in BC. Nowadays, the ethereum is also setting up to shift from PoW to PoS. Hyper-ledger Fabric currently uses the PBFT process. The comparison of the above-said process is explained in the table (Table 6.2).

6.2.4 Smart Contract

The smart contract possesses a self-verifying, tamper-resistant and self-executing program code piece that executes on the BC. Bitcoin supports a fundamental scripting programming language which allows citizens to mark their tradition logic for spending transactions. The scripting programming language gives the suppleness to propose primal contracts.

6.2.5 Challenge and Future

Regardless of the gigantic potential, there are restrictions as of the current condition of the BC. The scaling issues that BCs need are to defeat for more extensive adoption of overall businesses. Also, with the development in utilization, the size of BC is expanding colossally, making it hard for ordinary clients to keep its full duplicate

copies. In addition to that, with the tremendous venture and research endeavors put into BC [18], a superior, versatile BC may develop later on.

6.3 The Blockchain Prospective in Health Sector

Healthcare sector is an issue-driven, data and faculty intensive domain where the capability to get to, alter and trust the information rising. While working together with educational institutions, the healthcare division must give admittance to patients and give a field to preparing so understudies can create and refine the essential abilities. Consequently, the educational foundations furnish the segment with a qualified workforce. While working together with foundations and organizations with a research and designing plan, health establishment ought to help with giving admittance to experts, informants, tests and test people. Consequently, the investigation and designing foundations furnish the healthcare with refreshed information, instruments and strategies. Figure 6.1 depicts the different data mapping strategies in healthcare sector.

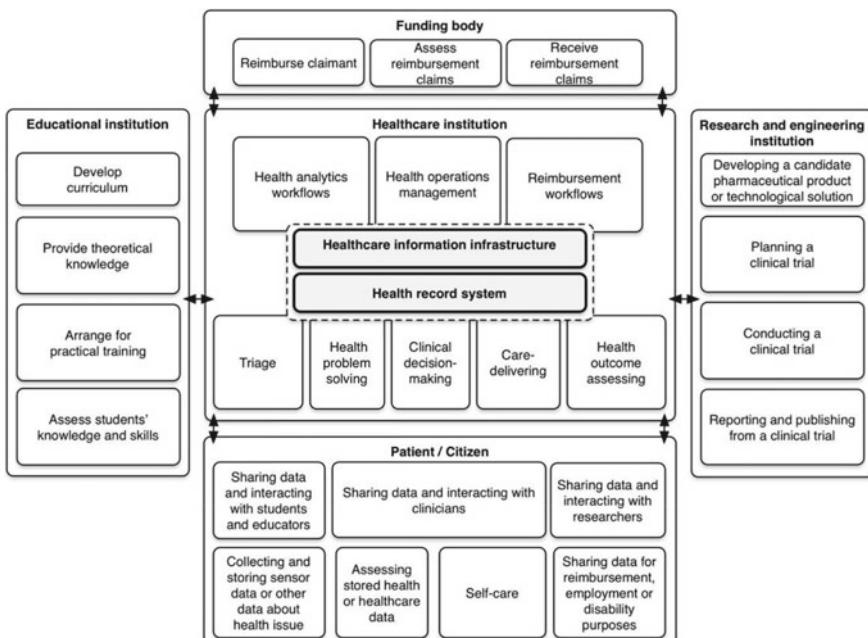


Fig. 6.1 Data mapping in health sector

6.3.1 Management of Data in Healthcare Sector

The administration of healthcare information which incorporates capacity and sharing control of the information is a significant part in healthcare business. Legitimate managing of healthcare information enhances healthcare results by permitting all-encompassing perspectives on patients, customized medicines, and productive correspondence. It is additionally basic for working healthcare industry cost-adequately and proficiently. BC may empower the proficient sharing of healthcare information while guaranteeing information respectability and securing the privacy of the patient. Secure, proficient, practical, and interoperable HIEs may work along with its correct use along with different other technologies. Also, the approval of BC may push forward the development of patient-driven model of healthcare where patients can control healthcare information of their own. Since patients have full responsibility for healthcare information in numerous nations, BC empowered patient-driven healthcare information model is one of the approaches that can bypass these administrative challenges.

A few undertakings are concentrating on building up some BC-based HIE and giving information and services commercial centre on the head of it. Out of them, some are focusing on general electronic health records (EHR) information while some are gaining practical experience in particular information modalities. For instance, Medrec is an open-source BC stage for EHR management. It has a joint effort with Beth Israel Deaconess Center. It is building up an HIE controlled by its BC. Mindshare gives a BC-based information sharing of electronic clinical records among untrusted parties by presenting information provenance, inspecting, and following on clinical information. Using smart contracts and an entrance control framework, they claim that their framework can viably follow the conduct of the information and renounce admittance to disregarded standards and authorizations on the information.

6.3.2 Management in Pharmacy Sector

Pharmaceutical goods are a significant part of medical consideration and healthcare conveyance. In this segment, we survey the different imaginative applications and activities in the pharmacy sector, by wrapping the whole range directly from the medication disclosure and clinical [19] preliminaries for the promote prologue to arrangements toward the finish of the chain-like fake medications ID and patient adherence to drug. An outline of the investigated application zones and organizations inside those application territories is shown in Fig. 6.2.

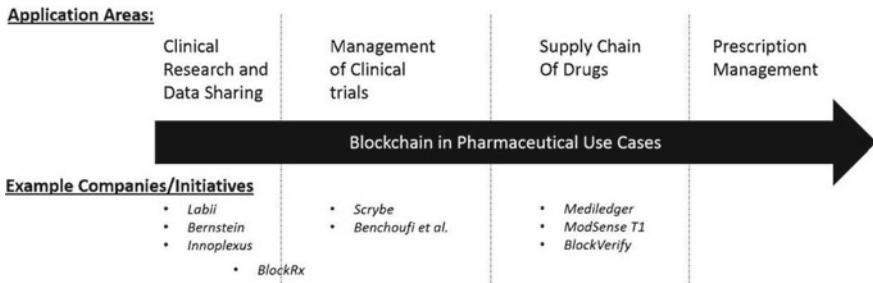


Fig. 6.2 Usecase of blockchain in pharmaceutical sector

6.3.2.1 Research in Pharmaceutical Sector

Research on discovery of drug plays a vital role in a pharmaceutical organization. With expanding expenses of healthcare, along with the need to enhance quicker on new restorative medicines, numerous pharmaceutical organizations must discover a way to deal with the team up seriously. Blockchain can empower the technological stage to encourage the transfer of confided in information and information among numerous parties. The utilization of BC empowers the Intellectual Property (IP) through permanent records for the cooperation. Considerably under a non-synergistic research and medication improvement situation, BC gives advantages to viably following and overseeing different parts of clinical preliminaries like information management, consent management, following symptoms of medications utilization, and so on.

6.3.2.2 Role of Supply Chain in Healthcare

The significance of the supply chain in the clinical business couldn't be more critical. Directly from the crude materials and creation, to various phases of capacity and appropriation, legitimate observing and following are needed to guarantee ideal and expected use. BC gives an entirely fitting answer for this requirement for following and following, where this information kept up in an open yet protected and carefully designed framework available to numerous parties.

6.3.2.3 Management of Patient's Prescription

Appropriate management of prescription is critical to guarantee the best health-care service conveyance. Abuse of the prescription has been widespread lately prompting large-scale issues like Opioid emergency. Numerous BC-based arrangements proposed to eliminate the obstacles on legitimate prescription management.

6.3.2.4 Billing Management

Monetary parts of clinical consideration are innately significant in the healthcare scene. This territory of financing angle in healthcare is overflowing with failures, generally identified with the trust and transparency, which can conceivably be enhanced by the utilization of BC. Smart contracts utilized in the premium arranging stages. Information concerning the current health status, drug use, way of life, and so forth tied through BC to developing premiums, through smart contracts. At that point, when numerous parties or mediators are associated with the claim taking care of, there may be thousands of redundant assignments and checks included which may be troublesome for the end clients.

6.3.2.5 Role of Telemedicine in Healthcare Sector

Telemedicine is an additional zone in the healthcare sector which can make a profit by the use of BC technology by presenting a trust layer among patients and healthcare experts. BC-based telemedicine strategy can approve proficient personality and information honesty, guarantee transparency and boost the participants to act reasonably by giving intensive measurements. Inside telemedicine, the distant demonstrative services might be at bleeding edge of BC adoption. It very well may be familiar that demonstrative services exclusively dependent on the quantitative and subjective translation of clinical information without a patient requires first to adopt BC technique [20] effectively. A large number of new businesses are focusing on the services where the analysis of an ailment depends on the translation of patient-generated imaging information, for example, dermatology.

6.4 Proposed Methodology

6.4.1 *Searching Strategy*

An organized writing search on the point led in the accompanying bibliographic information bases. We began the survey by gathering papers from two sources that includes Google Scholar and academic information bases. Generally speaking, we play out the pursuit in 14 diary information bases identified with information frameworks and healthcare and remembered distributed papers. The inquiry system compromised looking for liberated text conditions for the idea “BC” inside the health theme information bases. Where as in different information bases, the idea “BC” joined with the idea “health” utilizing logic AND. Inside the ideas, word variations and other related conditions were secured and joined utilizing logic OR.

This total process is applied and considered when there is no availability of new extra, essential paper. Through the data set inquiry, we have looked into more than

25 top healthcare, information frameworks and business diaries. The selected diaries positioned as Q1 in the SCImago Ranked system that was our underlying premise of incorporation in this survey report. All the references to the databases traded to End Note for copy expulsion and last screening. The inquiry focused on distributed research in academic diaries, meeting procedures that asses BC ideas inside the health domain. To automate information assortment through information bases, we built up content in R programming language that got to the diaries meta-information utilizing Application Programming Interface (APIs) of the significant information bases. The PRISMA structure indicates a proof-based least arrangement of things for detailing in efficient surveys and meta-investigations. It broadly used in scholarly examinations. The advantages of utilizing PRISMA for the examination permitted to utilize rules to survey planned inquiries and utilize deliberate and unequivocal strategies to find, select, and assess essential distributions to address the research addresses recognized before.

6.4.2 Selection Strategy

Distributions are meeting the comprehensive standards, and those for which the principal analyst was in question, were surveyed a second time by three extra commentators. In instances of difference, a conversation between every one of the four commentators decided inclusion or avoidance. The downloaded meta information were examine freely by two autonomous additional researchers to investigate its importance for the experiment. The articles those were not in English format were barred. The selection technique is introduced in Fig. 6.3. The outcomes investigated to deliver the last rundown of papers which incorporated 136 different full-text manuscripts that met the inclusion criteria.

6.4.3 Selection Strategy

The analysis of the distinguished papers perform utilizing content investigation strategy is one of the research technique for investigating contented from manual collaboration procedure, composed and verbal record through motivation behind breaking down information. It is a ground-breaking technique that permits researchers to examine reports as a significant source of information. Content analysis generally utilized in IS research. We utilized both subjective and quantitative ways to deal with the content investigation. A further survey of the chosen papers finished utilizing of information prospective of input-process-output (IPO). This methodology generally utilized in earlier research. It depends on examining data sources and outcomes and understanding the hidden processes, for example, forerunners, processes and outcomes of blockchain application in healthcare.

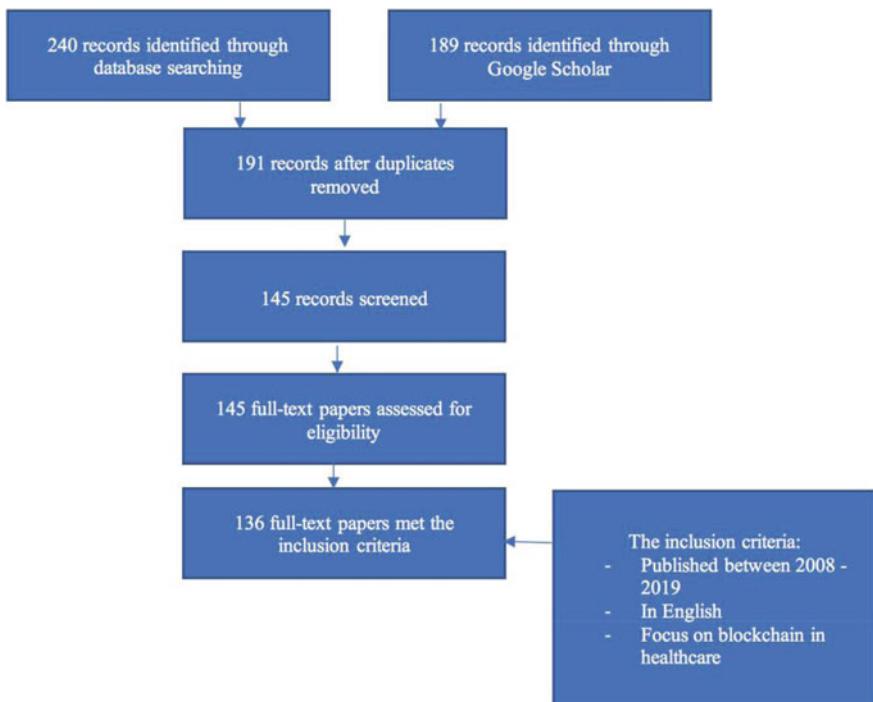


Fig. 6.3 Process flow of selection strategy

6.4.4 Data Analysis Mechanism

First of all, the related papers were included in the information matrix, and from there, the relevant data extracted. The extraction of data mainly done through 1st reviewer and later they are re-examined by other reviewers. After that, these are summarized and categorized in the information matrix. After that, these exported into tabular and graphical representation format. Google Sheet is used for a fair work process inside the research gathering and later sent out to Microsoft Excel for data storage. Figure 6.4 depicts the proposed model for the analysis of patient's health record.

6.4.5 Strategy Incorporates for Assessment of Quality

As a significant portion of the survey mechanism, a careful quality evaluation of added distributions was directed. Since created and approved tools for evaluating the various philosophies of the included distributions are deficient with regards to, the advancement of a particular device to fill, the need was fundamental to this end parts of the technique were utilized and adjusted as fitting no papers rejected in the process

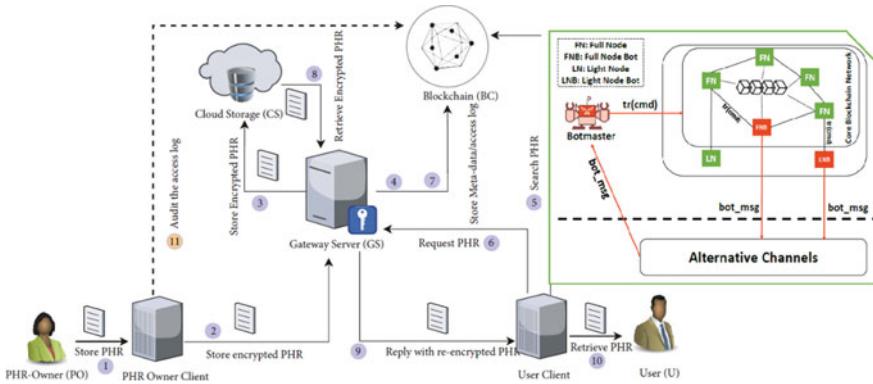


Fig. 6.4 Patient health record analysis

Table 6.3 Mechanisms for quality assessment

S. No.	Queries on quality assessment	Scaling in range of 0 to 2
1	Whether the health problem domain described?	No–Moderately–YES
2	Whether the objectives of research outlined clearly?	No–Moderately–YES
3	Whether the important contributions described well?	No–Moderately–YES
4	What is the appropriateness of the solution to problem?	Scarcely–Moderately–Adequately
5	Whether the solutions proposed are economically feasible (implementable, scalable)?	No–Moderately–YES

of quality appraisal. The papers got a score with the range of 0 to 2 dependent on the rules as per the information given in Table 6.3. The score was given as follows: ‘0’ is assigned for the NO or SCARCELY, ‘1’ is assigned for the MODERATELY and the value ‘2’ is assigned for or ADEQUATELY or YES. The process of value evaluation was finished by analyst one and later autonomously reassessed by other reviewers.

6.5 Findings

The analysis of the discoveries demonstrated that 136 manuscripts distinguished as conclusive examples are beginning from various regions of healthcare-related fields. Figure 6.4 shows the dissemination of articles over these three territories. Most of the distributions are based on the research with interdisciplinary, and the division between

the research zones generally obscured. The recognized three research zones propose three parts of BC in healthcare life cycle, from thought generation dissemination and execution. The study of the documents recognized the few significant themes that current research confronts and openings for future and current advancement. The utilization of structure of IPO permitted to arrange the discoveries to concentrate on commercial issues, as opposed to the technological arrangement.

6.6 Conclusion

In this paper, we presented a computerized technique for gathering distributed pertinent writing using a book mining calculation which gave expected result virtually to directing the audit study. The writing survey started to create a solid summary of BC in accompanying regions of healthcare sectors in the form of arrangements seen as smart contracts, information stockpiling and exchange, doctor credentialing and distributed information exchange. These features considered in different angles for healthcare arrangements plan and their developments in fulfilling logical or authoritative needs for information dispersals. Furthermore, the precision of judgments through BC-based medical reports can be improved. As well as advanced information therapy decision and numerous practical arrangements by utilizing an information base with health records as individual persistence information can be improved.

References

1. King, S., Nadal, S.: PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake (2012)
2. Sankar, L.S., Sindhu, M., Sethumadhavan, M.: Survey of consensus protocols on blockchain applications. In: 2017 4th International Conference on Advanced Computing and Communication Systems, ICACCS 2017 (2017). <https://doi.org/10.1109/ICACCS.2017.8014672>
3. Courtney, R.H.: Some informal comments about integrity and the integrity workshop. NIST Special Publication 500 (1989)
4. Coiera, E.: Introduction and Course Organization (2015)
5. Levy, Y., Ellis, T.J.: A systems approach to conduct an effective literature review in support of information systems research. *Informing Sci.* **9**, 181–211 (2006). <https://doi.org/10.28945/479>
6. Hölbl, M., Kompara, M., Kamišalić, A.K., Zlatolas, L.N.: A systematic review of the use of blockchain in healthcare. *mdpi.com* (2018). <https://doi.org/10.3390/sym10100470>
7. Zhang, P., White, J., Schmidt, D.C., Lenz, G., Rosenbloom, S.T.: FHIRChain: applying blockchain to securely and scalably share clinical data. *Comput. Struct. Biotechnol. J.* **16**, 267–278 (2018). <https://doi.org/10.1016/j.csbj.2018.07.004>
8. Zhang, A., Lin, X.: Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. *J. Med. Syst.* **42** (2018). <https://doi.org/10.1007/s10916-018-0995-5>
9. Rahman, M.A., Hassanain, E., Rashid, M.M., Barnes, S.J., Shamim Hossain, M.: Spatial blockchain-based secure mass screening framework for children with dyslexia. *IEEE Access* **6**, 61876–61885 (2018). <https://doi.org/10.1109/ACCESS.2018.2875242>
10. Guo, R., Shi, H., Zhao, Q., Zheng, D.: Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. *IEEE Access* **6**, 11676–11686 (2018). <https://doi.org/10.1109/ACCESS.2018.2801266>

11. Xia, Q., Sifah, E.B., Asamoah, K.O., Gao, J., Du, X., Guizani, M.: MeDShare: trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access* **5**, 14757–14767 (2017). <https://doi.org/10.1109/ACCESS.2017.2730843>
12. Zhou, L., Wang, L., Sun, Y.: MiStore: a blockchain-based medical insurance storage system. *J. Med. Syst.* **42** (2018). <https://doi.org/10.1007/s10916-018-0996-4>
13. Ekblaw, A., Azaria, A., Halama, J.D., Lippman, A., Vieira, T.: A Case study for blockchain in healthcare: “MedRec” prototype for electronic health records and medical research data White Paper MedRec: Using Blockchain for Medical Data Access and Permission Management. IEEE Original Author (2016)
14. Anjum, A., Sporny, M., Sill, A.: Blockchain standards for compliance and trust. *IEEE Cloud Comput.* **4**, 84–90 (2017). <https://doi.org/10.1109/MCC.2017.3791019>
15. Benchoufi, M., Ravaud, P.: Blockchain technology for improving clinical research quality. *Trials* (2017). <https://doi.org/10.1186/s13063-017-2035-z>
16. Dagher, G.G., Mohler, J., Milojkovic, M., Marella, B.: Ancile: privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustain. Cities Society* (2018). <https://doi.org/10.1016/j.scs.2018.02.014>
17. Esposito, C., De Santis, A., Tortora, G., Chang, H., Choo, K.K.R.: Blockchain: a panacea for healthcare cloud-based data security and privacy? *IEEE Cloud Comput.* **5**, 31–37 (2018). <https://doi.org/10.1109/MCC.2018.011791712>
18. Kruse, C.S., Goswamy, R., Raval, Y., Marawi, S.: Challenges and opportunities of big data in health care: a systematic review. *JMIR Med. Inf.* **4**, e38 (2016). <https://doi.org/10.2196/medinf.5359>
19. Jahan Miah, S., Gammack, J., Hasan, N.: Accepted Manuscript extending the framework for mobile health information systems research: a content analysis. *Inf. Syst.* (2017). <https://doi.org/10.1016/j.is.2017.04.001>
20. Radanović, I., Likić, R.: Opportunities for use of blockchain technology in medicine. *Appl. Health Econ. Health Policy* **16**, 583–590 (2018). <https://doi.org/10.1007/s40258-018-0412-8>

Chapter 7

Blockchain in Healthcare System: Security Issues, Attacks and Challenges



Arup Sarkar, Tanmoy Maitra, and Sarmistha Neogy

Abstract The Healthcare system as an organization has the important requirements corresponding to security and privacy, for example, protecting patients' medical information from unauthorized access, secure drug tracking, secure communication with transport like ambulance, secure and smart e-health monitoring. But due to lack of expert design of security protocols, the healthcare system is facing many security threats such as interoperability, authenticity, data sharing, the conveying of medical data, and deliberations of mobile health. In such a scenario, blockchain may help because of its unique properties. The blockchain ledger, formed by applying digital signature schemes, consensus mechanisms, and chain of hashing, offers highly reliable storage capabilities. Due to the aforementioned characteristics, blockchain provides various services like integrity, traceability, security, and non-repudiation, by storing the information in a public decentralized environment so that privacy preservation can be maintained. It is required to explore the security issues, different attacks and challenges when blockchain is applied in healthcare, which can help to design a more strong security protocol in a distributed environment. Therefore, this book chapter focuses on (a) different applications of healthcare where blockchain can be applied, (b) requirements of blockchain in such applications, (c) different possible security attacks in the blockchain-based healthcare system, (d) security issues and challenges to design protocols using blockchain, and (e) future directions to the research to be explored more.

Keywords Blockchain · Consensus · Healthcare system · Interoperability · Security

A. Sarkar (✉) · T. Maitra

School of Computer Engineering, KIIT Deemed to be University, Bhubaneswar 751024, India
e-mail: arupsarkar@ieee.org

S. Neogy

Department of Computer Science and Engineering, Jadavpur University, Kolkata 700032, India

7.1 Introduction

Within the economic system, the healthcare industry is the aggregation and integration of sectors that provide products and services for the treatment of patients, including investigative, preventive, rehabilitation, and mitigates care. It involves the generation and development of products and services that contribute to the maintenance and rehabilitation of health. The modern healthcare industry has three essential branches: (a) services, (b) products, and (c) finance. Different sectors and classes rely on trained professionals and interdisciplinary teams in groups to meet the health needs of people [1, 2]. The largest and fastest-growing industry in the world is the healthcare industry [3]. Considering more than 10% of the gross domestic product (GDP) of most developed countries, healthcare can become a big part of a country's economy.

In 2017, hospitals, physicians, nursing homes, diagnostic laboratories, pharmacies, medical device manufacturers, and other components of the healthcare system accounted for 17.9% of the total gross domestic product (GDP) in the United States. The health share of gross domestic product (GDP) is expected to reach 19.9% of GDP by 2025 [4]. In 2001, OECD countries averaged 8.4%, followed by the United States (13.9%), Switzerland (10.9%), and Germany (10.7%) [5]. The total health expenditure of U.S. healthcare in 2006 was 2.2 trillion [3]. According to the Department of Health, in 2007 in the United States, for every woman, man, and child, expenses US \$ 7,498 was spent, which was 20% of all spending. Expenditure is projected to increase to \$ 12,782 by the year 2022 [6]. Blockchain is a type of distributed ledger technology (DLT) and architecture platform launched in 2009 [7]. The concept was first developed by Satoshi Nakamoto in 2008 [8]. Blockchain stores ledger information as part of the infrastructure in a distributed and decentralized manner across all participating devices [7]. Blockchain is a peer-to-peer based infrastructure, where users participate in a network of transactions (participating in transactions) and miner (facilitating transactions in distribution) [8]. In a decentralized network of nodes, the ledger, which is created by cryptographic processes that compute all hash within the network, is stored [7]. High-reliability storage capacity was also introduced by the blockchain as it was built using a digital signature, hash chain and consensus mechanism. It stores all information in a decentralized way [7]. Applications of blockchain include banking, finance, real estate, and some areas related to government, power, and energy, and IoT [9–11]. Some researchers have also been done to the banking and finance sectors. Recently, the healthcare sector has been focusing more on blockchain-enabled applications [11]. The ability to use blockchain technology to address current challenges in healthcare has been highlighted by many researchers.

Nowadays healthcare involves lots of research in the blockchain. Google Trends graph shows a recent interest in the field (see Fig. 7.1). It appears that many researchers are interested in this field and it is growing day by day. Figure 7.2 shows regional interest in blockchain in healthcare, where India is at the top of interested countries.

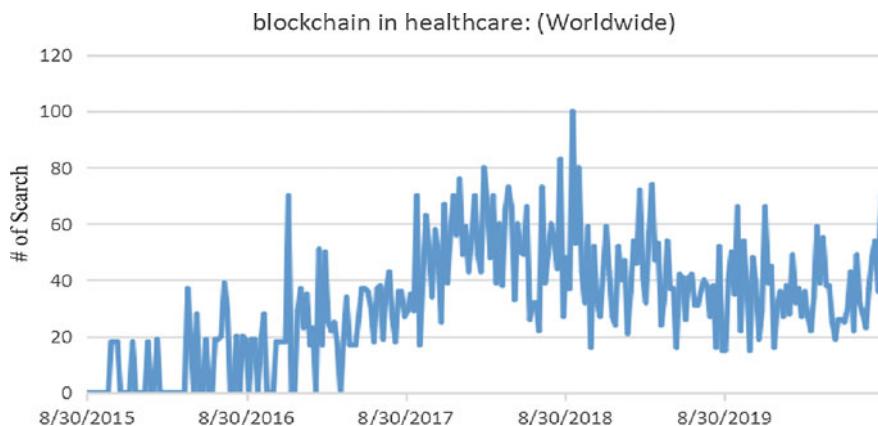


Fig. 7.1 Blockchain in healthcare trend

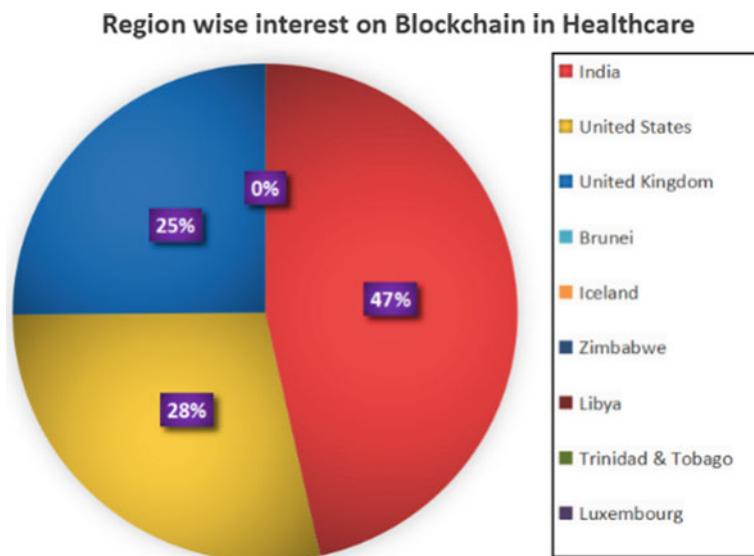


Fig. 7.2 Region wise trend

Not only academic researches on blockchain in healthcare are going on but also industries are very much interested to implement Blockchain in healthcare domain. This chapter highlights a lists of industries which are involved to deploy the healthcare system using blockchain in practical world as follows: (a) Chronicled¹ is a Startup providing secure supply chain solutions, blockchain and the IoTs to power

¹<https://www.chronicled.com/>.

smart; (b) Clinico² creates a community of patient-centered clinical experiment data sharing; (c) Coral³ provides technology oriented solutions to speed up delivery of care, computerize multidisciplinary organizational processes, and get better health outcomes; (d) Curisium⁴ tracks contract edits in concurrent and simulates possible options; (e) iSolve⁵ sets off existing systems and processes to create a distinct and high-performance environment focused on confirming data evidence and improving patient outcomes; (f) Medicalchain⁶ stores health data securely using blockchain technology; (g) Patientory⁷ is a health management software for global population by providing access to the users to their health data; (h) Pokitdok⁸ develops claims, pharmacy and identity management APIs. The platform, named Dokachin, manages both financial and clinical data in the healthcare industry by using a distributive network of transaction processors.

In this chapter, we have detailed out the studies on the architecture of blockchain system and its applications in the healthcare domain. Also we have studied different possible attacks in blockchain systems and issues and challenges to design secure applications in healthcare system. Lastly, we have identified some future research directions in this field.

The organization of this chapter is as follows: Sect. 7.2 describes the architecture of blockchain. Then it describes the existing blockchain system in the literature. Requirements of security in healthcare using blockchain are demonstrated in Sect. 7.3 followed by different applications of healthcare in blockchain discussed in Sect. 7.4. Section 7.5 briefly describes a popular healthcare application using blockchain known as MedShare followed by a comparison study of other existing healthcare applications. In Sect. 7.6, this chapter highlights the possible attacks that can be mounted in blockchain system. Section 7.7 demonstrates the issues and challenges to design the healthcare applications using blockchain. Finally this chapter concludes in Sect. 7.8 with a future direction.

7.2 Architecture of Blockchain and Existing Systems

The architecture of the blockchain is shown in Fig. 7.3 where every node is connected in peer-peer manner and distributed way. Every node has the same ledger as the network. In this network, some nodes may work as a member node and other nodes as validator or works as both. In Fig. 7.3a, b, the public blockchain and the private blockchain are shown respectively.

²<https://www.clinico.in/>.

³<https://angel.co/company/coral-health-research-discovery-1>.

⁴<https://www.curisium.com/>.

⁵<https://isolve.io/>.

⁶<https://medicalchain.com/en/>.

⁷<https://patentory.com/>.

⁸<https://pokitdok.com/>.

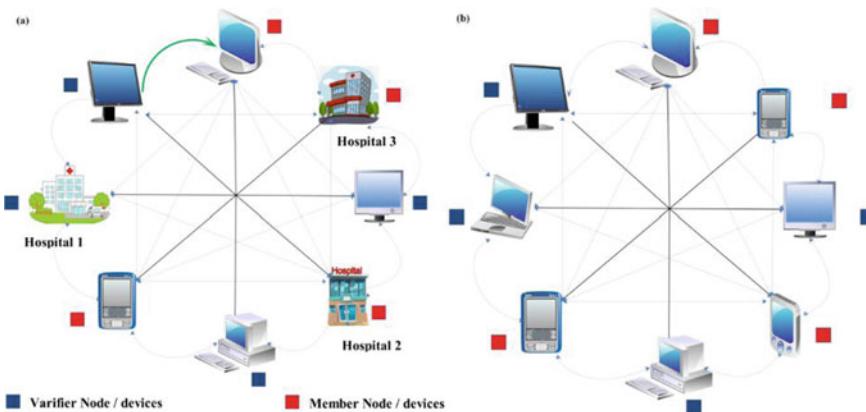


Fig. 7.3 Blockchain architecture: **a** Public blockchain, **b** private blockchain

There are four types of blockchain such as public blockchain, private blockchain, consortium blockchain, and hybrid blockchain, are available. Bitcoin and Ethereum are public blockchain, whereas Hyperledger is private blockchain. In Table 7.1, this section compares some well known Blockchain-Systems. Figure 7.4 shows the architecture of Blockchain in Healthcare System where every hospital is connected to each other. Every hospital also stores its local ledger. Authenticated data are stored in cloud storage. Certifying Authority (CA) is used for authentication. In the blockchain, cryptographic hash of the data is stored.

7.3 Securities in Healthcare: Requirements

In the healthcare industry, there are specific requirements related to protection and privacy due to additional legal requirements for the protection of patients' medical data. When medical records are shared in the Internet with the adoption of cloud storage and mobile health devices, it compromises the risk of malicious attacks and any personal information. Sharing and confidentiality of this information is a major concern, including access to health information through smart devices and patients visiting multiple physicians in many cities. Authentication, interoperability, data sharing, treatment record transfer and considerations for mobile health are unique requirements of the current healthcare industry.

Table 7.1 Comparison of some blockchain systems

Ref	Blockchain Platform	Permission Network	Consensus Protocol	Application Languages	Special Hardware Requirement	Turing Complete	Data Structure
Nakamoto [8]	Bitcoin	No	PoW	C++, Golang	No	No	Blockchain
Wood [12, 13]	Ethereum	No	PoW/PS	Serpent, Solidity, , LLVM	No	Yes	Blockchain
Androulaki et al. [14]	Hyperledger	Yes	PBFT	Golang, Java	No for Fabric, Yes for Sawtooth (Intel SGX)	Yes	Blockchain
Litecoin [15]	Litecoin	No	PoW	Golang, C++	No	No	Blockchain
Schwartz et al. [16]	Ripple	Yes	Ripple	Golang, C++	No	No	Blockchain
Goodman [17]	Tezos	No	PoS	Michelson	No	No	Blockchain
Sasson et al. [18]	ZCash	No	PoW	C++	No	No	Blockchain
SawtoothLake [19]	Sawtooth Lake	No	PoET	Python	No	Yes	Blockchain
Morgan [20]	Quorum	Yes	Quorum Chain	Golang	No	Yes	Blockchain
Monax [21]	Monax	Yes	Tendermint	Solidity	No	Yes	Blockchain
Brown [22]	Corda	Yes	BFT	Kotlin, Java	No	No	Blockchain
Martino [23, 24]	Kadena	Yes	ScalableBFT	Pact	No	No	Blockchain
Popov [25]	IOTA	No	PoW	Java	No	No	DAG
Churyumov [26]	Byteball	Yes	Main chain	Node.js	No	No	DAG

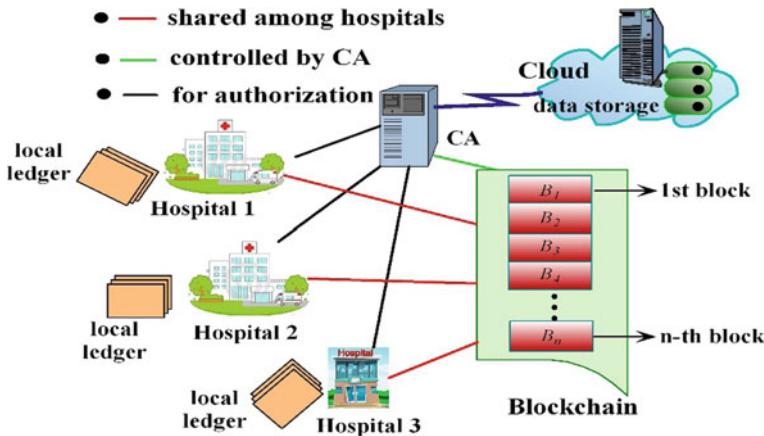


Fig. 7.4 Blockchain in healthcare architecture

7.3.1 Data Security

The main protection requirements associated with health care and treatment data, are access control, authentication, non-disclosure of records, ensuring the confidentiality, integrity and availability of medical information [27, 28]. Treatment information is treatment data such as patient files as well as treatment records that can be applied and monitored. Access to health records requires strict access control to audit the query and reduce the risk of duplication of those records (PHR- and personal health records) used [29, 30].

There are many ways to secure patient data, but they are not proven to be as accurate as they should be, and disseminating patient treatment data can lead to real world significances (such as patients' risk of confidentiality to malicious attacks) [30, 31].

7.3.2 Interoperability

Another major requirement of the healthcare industry is interoperability, which is the process of sharing data between different sources [31]. Many records are created every day and stored in a concentrated area in different hospitals [31]. Many records are fragmented due to the centralization of health record storage systems. Data authentication is centrally required to ensure a reliable database on the designated network.

7.3.3 *Data Sharing*

Data sharing and access are both safety issues and underlying health issues, including health records [32]. Sharing healthcare records is sometimes difficult because a person's extensive records can be stored in different places [32]. Patients do not have a unified view of these scattered records and are applied to healthcare providers, as they do not have access to their patient data if these records are located elsewhere [32]. Healthcare records are divided into individual hospitals, making it difficult to distinguish between record connections that cannot be divided as entity-based entities because it is a common identifier [32, 33]. The main problem with data sharing is interoperability.

7.3.4 *Mobility*

As patients become more mobile, mobility in the healthcare industry has emerged as a necessity. Therefore patient records must be met with the same level of portability. As smart devices, sensors and other Internet-enabled devices become more prevalent, the ability to transmit that data becomes important. Furthermore, sharing data from anywhere on any device raises the challenge of realistic sharing and ensuring that data is protected by law for access. The concept of mobility is divided into three different categories: mobile health, wireless and IoT.

For the above requirements, we need some solutions to protect our health information and interoperability, data sharing and data mobility. The purpose of this chapter is to discuss blockchain implementation and how it will benefit the healthcare industry, as well as the challenges and problems that the industry faces. We also discuss some research guidelines in the context of blockchain in healthcare.

7.4 Applications

Blockchain has many healthcare applications. Some applications are described below.

7.4.1 *Patient Data Management*

Healthcare industry faces challenges in the form of patient data management from unprofessional medical knowledge transmit to personalized medical care. Blockchain helps professionals better manage these circumstances. The most important problem in this case is that the patient does not have full ownership of his own data. Medical

data may be used or shared without permission. Blockchain can solve this problem by collecting patient records and by storing it in the organization's internal database. Blockchain addresses this issue via smart contracts for access to patient data regulated by patients and their respective regulations. Thus, a patient can share his medical data on his own terms. Records may be kept anonymous or completely transparent for research purposes depending on the needs of the patient. Also, by adding particular rules to these smart contacts, a patient could share health information and sensor readings (from a smart watch) with physician to personalize long-term care and achieve efficient and optimal results.

7.4.2 Clinical Adjudication

An essential part of any new treatment medicine or product is Clinical trials. At present, they present a difficult and lengthy procedure that takes lots of time to complete and generates large amount of information. This procedure is particularly subject to verification because its results can create or break a new drug or device. Doing so could also invalidate manufacturers' claims about the potency and effects of any drug/product on the individual body. The authentication capabilities of blockchain technology make sure that any data contained in shared bookkeeping is easily reached and can be accessed by all stakeholders—not only by the creator of the bookkeeping or a third party.

7.4.2.1 Claims Adjudication

Healthcare industry suffers from billing inefficiencies, 5–10% of estimated healthcare cost cheating due to overbilling, and billing not provided. For example, it may be more precise and easier for the patient to apply the entire process automatically through the blockchain. The claims are usually written in the context of a sophisticated (legal) language, perhaps subject to a separate interpretation in court. This approach is inherently wrong when it comes to healthcare, as contracts complicate matters so that they are likely justifiable from a legal point of view. As an alternative, they should spotlight on communicating the cost of healthcare to a patient in a healthy and crystal clear way. Blockchain-based smart contracts have been able to solve the problem. Contracts are written in computer programming language rather than legal language and therefore there is no chance for dual interpretation. Smart contracts standardize and make research into the claims process at the same time.

7.4.3 Medicine Supply Chain Management

Medical sector needs to be able to fully track their supply chains from suppliers and suppliers to their manufacturing facilities. A producer identifies a produced drug—creates a “hash” and uploads the information the blockchain. Then, a merchant check the product. A pharmacy worker can verify product proof at a later time before selling it. Finally, any people purchasing a medicine can trustly examine its source and production history. Short-term detection of counterfeit drugs or prescriptions not only helps medicine manufacturers/sellers financially, but can actually save a patient’s life. The scalability of this problem is astonishing, as the fake drug business itself has become a \$75 billion industry. So many initiatives has been taken to develop Ethereum-based Mediliogar project, supported by industry leaders such as Genertech and Pfizer, have launched a drug tracking solution aimed at optimizing medicine supply chains and reducing fake products.

7.5 An Example Application: Medshare

Blockchain has much potential for healthcare technology. A diversity of application exist highlighting blockchain enabled healthcare and we discuss one such application in details and a few others are mentioned in Table 7.2.

MeDshare [31], designed by Xiaod, Asamoh, Sifah, Du, Guizani, and Gao is a plan developed to address the problem of medical information sharing amongst medical service providers that stores information in a centralized database. The main goal is to store sensitive medical data in cloud, including the ability to obtain and monitor sensitive data for sharing medical data with medical community entities, for which shared records data privacy does not pose a risk to patients. Maintaining confidentiality for patient data and reducing the risk of malevolent activity in medical data is a major problem in the healthcare sector. MeDshare observes entities that access medical information and verifies for malicious access to any party attempting to access that data. In the MeDShare system all data transactions are shared from one entity to another, all functions are securely recorded to be tamper-proof. The design uses smart contracts and access control systems to track data and to revoke access to any malicious entity after detecting any rule violations within the system.

The first level is a user level that includes different categories of users who want to access information from within the system.

The second level is the data query layer, which is a set of query structures that use, process, forward, or respond to the queries used in the system. These processes are divided into two main components, namely: the query system responsible for

Table 7.2 Blockchain research in healthcare—challenges and benefits

Ref	Application	Advantages for the Healthcare	Difficulties	Shortcomings	Area of work
Mettler [34]	Gem Network	Health Data shared through Decentralized Network and legal issues addressed	Not applicable	Scalability, and key replacement capability is not addressed	Third-World Countries such as Estonia
Roehrs et al. [33]	OmniPHR	Patient Data sharing	Not Scalable	Data should be as standard as OmniPHR otherwise rejected	Laboratory
Azaria et al. [32]	MedRec	Health Data Sharing	Not addressed Mining rewards	No key replacement capability, Security, and legal issues are not addressed	Laboratory
Zhang et al. [35]	PSN	Health data on IoT Devices Sharing	Not applicable	Scalability, key management and leakage is not addressed	Laboratory
Samaniego et al. [36]	Virtual Resources	Health Data stored in a framework that is persistent data that is safe, secure, and scalable	prospective standardization	Scalability, no key replacement capability Addressed	Laboratory
Siddiqi et al. [37]	Context driven Data Logging	of Health Data Storage and put in a level of assurance to data logging	Not applicable	Security and no key replacement capability not addressed	Laboratory
Xia et al. [31]	MedShare	Security, authentication and sharing of medical information	Not applicable	no key replacement capability, latency problems and Scalability	Laboratory
Shaeet al. [38]	trial and Precision Medicine	Integrity and data access security	Not applicable	Latency problems, Scalability and no key replacement capability	Clinical Trial Databases

(continued)

Table 7.2 (continued)

Ref	Application	Advantages for the Healthcare	Difficulties	Shortcomings	Area of work
Yue et al. [39]	Healthcare Data Gateways	authentication, Security, and legal issues of data sharing	Not applicable	Scalability is not addressed, no key replacement capability	Laboratory

processing the request and the trigger responsible for translating tasks from the smart-contract environment. The third level is the data structure and the progress level, which consists of individual components that assist in the process of accessing data from existing database infrastructure through multiple entities. These units are the verification, processing and minimization nodes: smart contract, smart contract permission database and blockchain network.

Database infrastructure layer is the last layer, which includes database systems already installed by individual parties to perform precise tasks. Medicare [31] has proven that it adds a level of protection to cloud-based communications through its protection. However this increases delay as the number of requests for cloud-based services (key limitation of the system) has increased.

Though, MeDshare was capable to make a level of trust and data prowess, but there was a significant amount of delay and downside to adding or retrieving data. The issue of content management and retrieval was also not addressed.

Smart Contracts in Medshare

A smart contract performs as a finite state machine that executes instructions to activate an exploit based on examples. Smart contract is employed to report the activity is performed by a requester on the information requested from a data proprietor's system (See Algorithm 1). The data reported on the data proprietor's system is indexed, processed, and transmitted to a blockchain network. In some cases, the report is used to save and request and use the Smart Contract Permission Database where the data used by the requestor contains a set of data owner tasks. Data is indexed based on the requested and used data id where the data owner's set of tasks is applied by the applicant. The main verbs used in the smart contract are set; Read, delete, copy, write, and remove. These actions when performed on the data will trigger a smart contract to send a report based on established rules for that particular data. For Activity Monitoring, a contract is published in smart contract scripts by `getAction`. Data sensitivity is classified into two levels; High and low. These levels of sensitivity are processed by sensitivity reduction nodes based on the data set obtained from the database infrastructure. Depending on the sensitivity of the package, some of the steps taken in the data are either excluded from the infringement list or act as

infringements. The agreement requires that all actions performed in the data classified at the beginning of `getAction` should be reported for effective monitoring of the activities performed so that data breaches can be detected. The identification required to facilitate efficient identification of unique blocks is categorized into specific data by a requestor, the data owner, and the transmitted data. The advantage of mentioning these in the smart contract is to create an effective way of processing and matching the sensor quantities and process nodes and verify specific blocks. Comments are generated in the form of statements to describe the work done in the data. These typically combine the retrieval statement with an antenna statement to remove an encryption key, which will be reported to the data owner's Smartphone database to remove the encryption comments. An encrypted process is used to finalize this process. In smart contract scripts, the act of reporting and sending comments to the reporting subordinate nodes is quickly removed with a report statement. The function represents the permissions set by the access control data owner that will be executed simultaneously with the smart contract permissions database. In violation of the data agreement, data access is revoked and the data owner has a pending review, with the option to access the request or retrieve the data from the request.

Algorithm 1 : Smart Contract: Medshare

Input: Action, Sensitivity, RequestorID, OwnerID, DataID, Key, MetaIndex, comment, Genreport, accessControl;

Output: secure comment passing corresponding to an action

1. /* ----- Setup the functions ----- */
 - `Sensitivity_get();` /* function to get consensus report on a particular request i.e., low or high */
 - `Action_get();` /* function to get request from users to access data */
 - `Comment_get();` /* based on report, generates a comment corresponding to an action */
 - `AccessControl();` /* withdraw or provide access to a medical data */
- /* -----End of Setup -----*/
2. `Action ← Action_get();`
3. `{RequestorID, Potray, Data with DataID} ← Decrypt(Action);` /* Decrypt Action */
4. `retrieve (Key.OwnerID);` /* to retrieve the secret key from list of keys */
5. `comment ← Comment_get();`
6. `Encrypt(comment);` /* encrypt comment */
7. `Genreport ← {comment || RequestorID || OwnerID};`
8. `Sensitivity ← Sensitivity_get();`
9. **If** (`Sensitivity == Low`) **then**
10. `Action ← Action_get();` /* Exemptions on data */

```

11.      Exit();
12. else if (Sensitivity == Low) then
13.      Action  $\leftarrow$  Action_get(); /* Not exemptions on data (violation) */
14.      comment  $\leftarrow$  Comment_get(); /* Data violation concatenated with
   DataID */
15.      AccessControl(); /* Revokes access to data */
16.      retrieve (Key.OwnerID);
17.      comment  $\leftarrow$  Comment_get();
18.      Encrypt(comment);
19.      Genreport  $\leftarrow$  {comment || RequestorID || OwnerID};
20.      Exit();
21. else                                /* i.e., Sensitivity == High */
22.      Action  $\leftarrow$  Action_get(); /* Violation */
23.      comment  $\leftarrow$  Comment_get(); /* Data violation concatenated with
   DataID */
24.      AccessControl(); /* Revokes access to data */
25.      retrieve (Key.OwnerID);
26.      comment  $\leftarrow$  Comment_get();
27.      Encrypt(comment);
28.      Genreport  $\leftarrow$  {comment || RequestorID || OwnerID};
29.      Exit();
30. end if

```

Other researches on healthcare system are enlisted in Table 7.2. Table 7.2 also mentions the challenges and benefits of the respective applications.

7.6 Possible Attacks in Blockchain

Blockchain seems to be the ultimate security system with immutability, distribution consent, established trust, distribution identity, and perpetually verifiable claims. But new defense attacks are coming out, which can be extremely complicated and cause heavy irreversible damage. Considering these invasive vectors is very significant for the development and deployment of blockchain solutions. So it is better to prevent than cure. Figure 7.5 shows the types of possible attacks in blockchain. Following are the possible attacks in blockchain.

- (a) Peer to peer network based attacks
- (b) Smart contract based attacks
- (c) Wallet based attacks
- (d) Consensus and Ledger based attacks.

Further shown in Fig. 7.5 and some are described.

Eclipse attack—Node “x” will depend on the selected node using the peer selection technique of the node, which takes into account the distributed ledger. However, if an attacker alone can create a node to select an “x” numbered node from its malicious

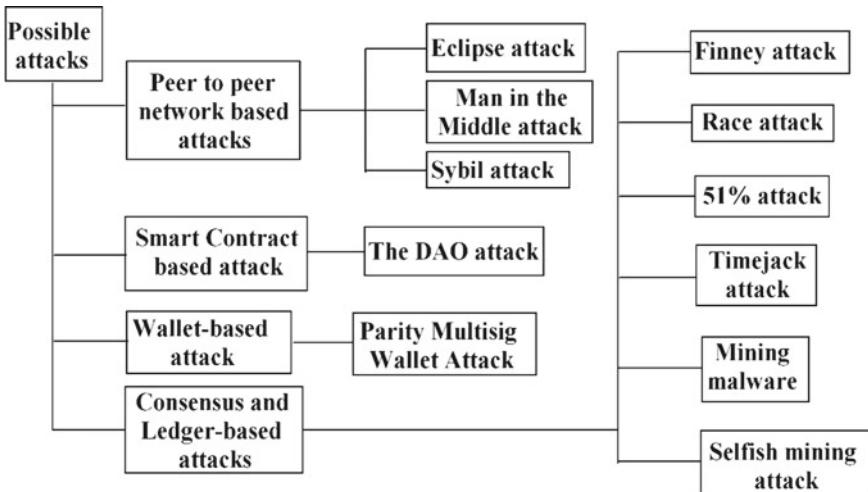


Fig. 7.5 Types of attacks in blockchain

nodes, it can capture the concept of the original malware and present its own variants for the node.

Man in the middle attack—In this attack, the attacker is secretly related and warns of possible communication between two parties who believe they are communicating directly with each other.

Sybil attack—When the Eclipse attack is directed at the actual leader of the user, the Sybil attack targets the whole network. In a Sybil attack, an attacker would try to persuade the network by flooding the network with many nodes under a pseudonym. Although these nodes are not related, the back appears to be operated by a single operator. The purpose is not to target any user, but to have multiple nodes or networks as a whole and, if possible, to allow the attacker to double the cost and carry out other attacks making a fork.

The DAO attack: The “DAO hack” is the biggest exploit in the history of cryptocurrency. The decentralized autonomous body Ethereum had aspiring features. The project called “The DAO” started gathering crowds by an organization called Slonk. This Crowdfunding, collecting 12.7 million ethers valued at \$ 150 million (then \$ 2.2 billion), received a strange response. Then an attacker identifies susceptibility in the code that allows repeated withdrawals to be performed without examining the agreement of the ongoing transaction. As a result, the attacker started the attack by giving a trivial amount and requesting a withdrawal with a repetitive task. This way he was able to draw about \$70 million dollars from crowdfunding. Then it turned to an interesting event. The attacker was pressurized by the Ethereum Foundation to stop the attack and give away the account. Then the attacker replied that he was playing by agreement and would violate the intervention agreement with a soft or

hard fork, which he could take to court (attacker's open letter). At last he called off the attack. Later money was raised by the Ethereum Foundation to restore, though the decision raised so many concerns about the sovereignty of the smart contract. This hard fork is the result of two Etherium coins—Etherium and Etherium Classic and lots of controversy.

Parity-Multisig-Wallet Attack: It was also the case of openness, including the attacker's hacked parity customer's wallet, as a result of holding 500,000 ethers (today \$ 77 million). Wallet deals are supplementary logic that can be made in the customer's purse for regular automatic payments. For reducing gas or transaction fees, Parity Multisig Wallet uses a central library agreement to operate (like a multisig wallet bank having multiple owners). He did, however, leave some important work open, which led to the attacker using vulnerabilities by adding his account as the owner to the attacker's library agreement, so that the attacker became the joint owner for all wallets applied after the due date. He then started a kill function, which was deposited in a wallet in the coin. They originally locked in \$155 million as of the day, forever on cryptographically in accessible wallets.

Finney attack: One has the opportunity to spend money if one can mine a block and steal it with any of one's transactions. If a mercantile accepts an unspecified transaction, you can transfer it to the previous trading currency. After that, you released a previously mined block that was secretly placed before your new transaction was confirmed.

Race attack: The slight variation of Finney's attack is Race attack. In this attack the attacker does not need to pre-mine the block with his transaction, which he wants to spend twice as much. During an attack, the attacker submits an unscheduled transaction to a merchant (victim) as well as another transaction he transmits through the network. If the attacker is directly connected to the merchant's node, it is easy to launch the attack. This will give the merchant the idea that his transaction is first, but the attacker never submits to the blockchain network.

51% Attack: When a miner or mining group controls the mining power of a blockchain network by 51% or more, then this type of attacks happened. While this is very difficult for large networks, it is 51% more likely to occur in smaller networks. It can foil certain transactions or even reverse old transactions if a group has majority have power over transactions on a blockchain network.

Timejack attack: In some blockchain networks, the nodes rely on internal time derived from median times, as indicated by their peer nodes such as bitcoins. For example, you depend on your friends to find the time. We say that an attacker puts lots of malevolent people on your friends list, and then he can handle your time. An eclipse attack on the target node may be the first stage of this attack. After completion of this attack on the target node, the target node will not receive the block from the actual network because the timestamp of the block will not match its timestamp. This allows the attacker to spend twice as much or transact with the target node because these transactions cannot be stored on the original blockchain network.

Mining malware: The computing power of victims' computers is used by the malware to hack crypto currencies for the hackers. The malware infected more than a million computers and assisted the attackers with 26 million tokens of a variety of cryptocurrencies.

Selfish mining attack: It is considered that the longest chain is the latest version of the ledger in many blockchain. Then a selfish miner might try to put the building block in furtiveness mode over the existing chain, and when he can lead two or more blocks in the network compared to the current chain, he reveals his personal fork which will be accepted as a new truth because it is the longest chain. He can transact on public networks before releasing his long stealth series as opposed to newly transacted. This effectively gives the attacker a small window to do double spending to make stealth chains by making enough blocks lead (Finney attack).

7.7 Issues and Challenges to Design Secure Protocol

Blockchain technology is on the rise, it is not yet fully developed and it has many potential challenges, which should be taken up for the healthcare industry.

Transparency and confidentiality: The first challenge is transparency and confidentiality. All are visible to everyone on the blockchain network. Medical data needs to be stored off-chain itself and only tag information in a blockchain.

Speed and Scalability: Speed and scalability is the second biggest challenge. Blockchain transactions are much slower than credit card transactions. The number of transactions in the healthcare industry is very high. So the blockchain revolution has to endure this momentum.

In a blockchain-based system, node is a important component It is the basis of technology that represents every entity connected to the network. Logarithmic-associative, if more nodes are added to the network, the inter-node latency increases with each additional node. In addition, the resources considered in the IoT environment increase the number of nodes. As the number of members or patients in the system increases, so does the difficulty of running blockchain-based applications. Subsequently, the perceived need for whole blockchain infrastructure has increased. Thus, it is important for research and judgment to ensure that blockchain applications are effective [19]. Light weight nodes known as partial nodes rely on complete nodes to perform tasks. Although there is no need to save the entire blockchain, the more number of light nodes can considerably increase the workload on blockchain servers. As a result, flow of blockchain applications and the scalability will be damaged. Blockchain involving a large participants or community has high reliability and gives higher reliability and higher security. However, as the number of organizations increases at each stage, this participation will decrease performance, which requires multiple computer resources. In particular, although the definition of a large population is a major problem, it has not yet been addressed or adequately tested.

In the healthcare sector, large population connections can be expected, including the use of blockchain. Thus, due to the increasing use of blockchain, high volume transactions will be generated and recorded. Blockchain-distributing ledgers will add new transactions to any transaction after the agreement on different entities in each transaction associated with the transaction. Although this process may seem complicated, it is effective due to the limited size of the blockchain. Effective pre-approval payments reduce the amount of memory used in the blockchain by some parties sharing short-term data. There is another problem with the blockchain process, which is identifying, validating or using previous transactions. Therefore, with a large number of processes occurring in real time, the effectiveness of the system deteriorates with the larger dimension of the blockchain.

The 51% Attack: Another challenge is the 51% attack threat. This is a theoretical but potential risk and should have a clear solution. Though blockchains are extremely secure, Blockchain are vulnerable to 51% attack (known as majority attack or double-spending attack). This occurs when a mining team or a miner controls more than 50% of the whole mine hash rate in the network and is able to reverse the entire transaction or intercept new transactions. A malevolent user is able to generate blocks at a faster rate than the rest of the network, and the longest chain rule, forcing the network attacker to switch series by controlling more than 50% of computing power. Although 51% of attacks are possible, the chances of a successful attack are extremely low.

Many believe that blockchain technology can change the healthcare industry and beyond, but no one has seen evidence to support their belief. The things we need are not in line with expectations, but a real case that demonstrates the potential of blockchain technology.

7.8 Conclusion and Future Direction

Finally, one of the most promising featured applications in the healthcare industry is the blockchain technology. This is due to the most powerful mastery of the blockchain technique in the area of healthcare, such as: security, integrity, decentralized nature, readiness, and truly general account of infrastructure related to the blockchain. The healthcare industry is facing of problems for a rising technology framework, focusing on IoT, Internet-enabled, devices, sensing devices and smart devices. These technologies enable the healthcare industry to serve its patients in a growing world, malicious actors can access and copy data on these technologies as well as exploit vulnerabilities (as well as process and users), leading healthcare organizations to share information harder. There may be outdated data that may result in misdiagnosis or health problems and also problems to verify patient's identity. The healthcare sector has a clear ability to use blockchain technology to solve many such current problems. Present applications focus on issues of record sharing, authentication, usability, integrity, IoT protection, patient empowerment and edge host protection. The objective is to provide ownership and patient's control of sharing their own treatment data. Though

so much progresses for smart phone applications and medical applications, there are still clear security problems, because blockchain is not without possible challenges. The industries including healthcare those who wants to use blockchain-oriented tools may need to continue to study these areas and help to create an advanced ecosystem to create better patient-oriented data empowerment. The possible future direction of the research areas as follows:

Research is to be done to focus on precise blockchain-linked attacks and issues, such as blockchain and the encouragement of blockchain mining. Research is to be done in the area of blockchain-oriented scalable healthcare. It is a major problem because healthcare industry is growing fast, especially as our society is growing. As blockchain-oriented application systems grow, it will become increasingly difficult to run when the number of members or patients grows with time. Further research with real-world datasets is needed for allowing other researchers to check results and disseminate results from open-source. Many should focus on experimental concepts and explore opportunities that will help us to use real-world healthcare records to assess proposed systems (for performance, safety, privacy-protection and scalability) to help health organizations and researchers. More research should be done on protection and key management that will able to replace easily compromised or lost keys. Also research should focus on identity verification opportunities. Many tests focus on allowing the patient to be able to access the patient's data in advance, but in emergency there should be backup plans that can be used to allow doctor to access data without permission. The blockchain has many advantages that can be applied to solve various problems in the field of healthcare data sharing and protection. But blockchain which is not a solution can be enforced under any circumstances. As an alternative, we should focus on specific blockchain issues and an evaluation of how they are affecting the healthcare industry. The mining incentives issue, which is the central part of blockchain, has not been totally considered in the healthcare industry and also there are some specific blockchain attacks that could dissuade the entire system.

References

1. Healthcare Sector. https://www.investopedia.com/terms/h/health_care_sector.asp
2. Health Care Initiatives, Employment & Training Administration (ETA)—U.S. Department of Labor. Doleta.gov. Archived from the original on 29 Jan 2012. Retrieved 17 Feb 2015
3. Snapshots: Comparing Projected Growth in Health Care Expenditures and the Economy | The Henry J. Kaiser Family Foundation. Kff.org. 14 Apr 2006. Retrieved 17 Feb 2015
4. Keehan, S.P., Stone, D.A., Poisal, J.A., Cuckler, G.A., Sisko, A.M., Smith, S.D., Madison, A.J., Wolfe, C.J., Lizonitz, J.M.: National health expenditure projections, 2016–25: Price increases, aging push sector to 20 percent of economy. Health Aff. **36**(3), 553–563 (2017). <https://doi.org/10.1377/hlthaff.2016.1627.ISSN0278-2715.PMID28202501>
5. Growth of expenditure on health. <https://www.oecd.org/dataoecd/10/20/2789777.pdf>
6. Alonso-Zalvidar, R.: Average 2016 health-care bill: \$12,782. Los Angeles Times February 21, 2000

7. Zhao, H., Zhang, Y., Peng, Y., Xu, R.: Lightweight backup and efficient recovery scheme for health blockchain keys. In: 2017 IEEE 13th International Symposium on Autonomous Decentralized System (ISADS), Bangkok, pp. 229–234 (2017). <https://doi.org/10.1109/ISADS.2017.8222>
8. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system (2008)
9. Ølnes, S., Ubacht, J., Janssen, M.: Blockchain in Government: Benefits and Implications of Distributed Ledger Technology for Information Sharing. Elsevier (2017)
10. Sullivan, C., Burger, E.: E-residency and blockchain. *Comput. Law Secur. Rep.* **33**(4), 470–481 (2017)
11. Beninger, P., Ibara, M.A.: Pharmacovigilance and biomedical informatics: a model for future development. *Clin. Ther.* **38**(12), 2514–2525 (2016)
12. “Ethereum,” Dec. 2017. [Online]. Available: <https://www.ethereum.org/>
13. Wood, G.: Ethereum: a secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper **151**, 1–32 (2014)
14. Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolic, M., Cocco, S.W., Yellick, J.: Hyperledger Fabric: a distributed operating system for permissioned blockchains. In: Proceedings of ACM EuroSys’18, Porto, Portugal, pp. 30:1–30:15 (2018)
15. “Litecoin: An open source P2P digital currency,” June 2018. [Online]. Available: <https://litecoin.org/>
16. Schwartz, D., Youngs, N., Britto, A.: The Ripple protocol consensus algorithm. Ripple Labs Inc White Paper **5** (2014)
17. Goodman, L.: Tezos: A self-amending crypto-ledger position paper, Aug
18. Sasson, E.B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., Virza, M.: Zerocash: Decentralized anonymous payments from Bitcoin. In: Proceedings of IEEE SP’14, San Jose, CA, USA, May 2014, pp. 459–474
19. “SawtoothLake”, June 2018. [Online]. Available: <https://sawtooth.hyperledger.org/docs/core/releases/1.0/introduction.html>
20. Morgan, J.: Quorum, June 2018 [Online]. Available: <https://www.jpmorgan.com/global/Quorum>
21. “Monax,” June 2018. [Online]. Available: <https://monax.io/>. 2014. [Online]. Available: <https://tezos.com/static/papers/positionpaper.pdf>
22. Brown, R.: Introducing r3 cordatm: a distributed ledger designed for financial services. R3CEV Blog (2016)
23. “kadena,” June 2018. [Online]. Available: <https://kadena.io/>
24. Martino, W.: Kadena: The first scalable, high performance private blockchain. White Paper (2016)
25. Popov, S.: The tangle, Oct 2017. [Online]. Available: <https://iotatoken.com/IOTAWhitewpaper.pdf>
26. Churyumov, A.: Byteball: a decentralized system for storage and transfer of value (2016). [Online]. Available: <https://byteball.org/Byteball.pdf>
27. Kshetri, N.: Blockchain’s roles in strengthening cybersecurity and protecting privacy. *Telecom. Pol.* **41**(10), 1027–1038 (2017)
28. Khan, S.I., Hoque, A.S.L.: Privacy and security problems of national health data warehouse: a convenient solution for developing countries. In: 2016 International Conference on Networking Systems and Security (NSysS) (2016). <https://doi.org/10.1109/NSysS.2016.7400708>
29. Suzuki, S., Murai, J.: Blockchain as an audit-able communication channel. In: 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC) (2017). <https://doi.org/10.1109/COMPSAC.2017.72>.
30. Xu, J.J.: Are blockchains immune to all malicious attacks? *Financ. Innov.* **2**(1), 25 (2016)
31. Xia, Q., Sifah, E.B., Asamoah, K.O., Gao, J., Du, X., Guizani, M.: MeDShare: trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access* **5**, 14757–14767 (2017). <https://doi.org/10.1109/ACCESS.2017.2730843>

32. Azaria, A., Ekblaw, A., Vieira, T., Lippman, A.: MedRec: using blockchain for medical data access and permission management. In: 2016 2nd International Conference on Open and Big Data (OBD), Vienna, pp. 25–30 (2016). <https://doi.org/10.1109/OBD.2016.11>
33. Roehrs, A., da Costa, C.A., da Rosa Righi, R.: OmniPHR: a distributed architecture model to integrate personal health records. *J. Biomed. Inf.* (2017). <https://doi.org/10.1016/j.jbi.2017.05.012>
34. Mettler, M.: Blockchain technology in healthcare: the revolution starts here. In: 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), Munich, pp. 1–3 (2016). <https://doi.org/10.1109/HealthCom.2016.7749510>
35. Zhang, J., Xue, N., Huang, X.: A secure system for pervasive social network-based healthcare. *IEEE Access* **4**, 9239–9250 (2016)
36. Samaniego, M., Deters, R.: Hosting virtual IoT resources on edge-hosts with blockchain. In: 2016 IEEE International Conference on Computer and Information Technology (CIT) (2016). <https://doi.org/10.1109/CIT.2016.71>
37. Siddiqi, M., All, S.T., Sivaraman, V.: Secure lightweight context-driven data logging for body-worn sensing devices. In: 2017 5th International Symposium on Digital Forensic and Security (ISDFS) (2017). <https://doi.org/10.1109/ISDFS.2017.7916500>
38. Shae, Z., Tsai, J.J.: On the design of a blockchain platform for clinical trial and precision medicine. In: 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS) (2017). <https://doi.org/10.1109/ICDCS.2017.61>
39. Yue, X., Wang, H., Jin, D., Li, M., Jiang, W.: Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. *J. Med. Syst.* **40**(10), 218 (2016). <https://doi.org/10.1007/s10916-016-0574-6.Epub>. 26 Aug 2016. PMID: 27565509

Chapter 8

Application of Blockchain as a Solution to the Real-World Issues in Health Care System



**Amrutanshu Panigrahi, Bibhuprasad Sahu, Satya Sobhan Panigrahi,
Md Sahil Khan, and Ajay Kumar Jena**

Abstract Blockchain technology now a day is becoming a more secure and effective way for information sharing in various areas such as the financial sector, SCM in different industries, and in the field of IoT as well. Along with these fields currently, blockchain technology is playing a vital role in the field of Health Care System. This technology brings the attention of the researcher toward the health care system as it aims to solve various issues such as interoperability and information security during the information sharing and data management. The interoperability and security enable the HCS application to share the information flawlessly among the patients and vendors. Lack of such characteristics finds out the difficulty for the patient in accessing its own health status. Hence, implementing blockchain technology will demolish such a disadvantage for making the HCS more effective and efficient. Because of this kind of potential benefit, it can be applied to various aspects such as patient data handling, SCM of medical equipment and pharmaceutical things, billing and telemedicine systems, etc. In this book chapter, we have tried to focus on the various issues present in the HCS along with the detailed study of potential benefits that have been achieved while integrating the blockchain with the health care system. Also, in this chapter represents the systematic review of various use case scenarios for blockchain in healthcare practice.

Keywords Blockchain · Health care system · Interoperability · Information security · Data management

A. Panigrahi (✉)
ITER, SOA University, Bhubaneswar, Odisha, India

B. Sahu · S. S. Panigrahi
Department of CSE, Gandhi Institute for Technology, Bhubaneswar, Odisha, India

M. S. Khan
Department of IT, College of Engineering and Technology, Bhubaneswar, Odisha, India

A. K. Jena
School of Computer Engineering, KIIT Deemed to be University, Bhubaneswar, Odisha, India

8.1 Introduction

Blockchain implies an advanced framework for executing and recording exchanges that can be pictured as a structure block built from keen calculations and gathered information and made sure about by cryptography. Regardless of whether in money related markets, medical care, or the military; ventures and governments are utilizing blockchain advances to overhaul key tech standards [1]. As per Gartner, blockchain is among the main 10 vital innovation patterns for the years 2018 [2]. In [3] it is clarified that utilizing a public blockchain can eliminate the requirement for trusted focal experts in record exchanges also, debate assertions. This is on the grounds that trust is incorporated with the model through unchanging records on a circulated record. Blockchain innovation is considered by a few as the most noteworthy innovation after the Web and is broadly foreseen to determine trust issues through distributed systems administration furthermore, public-key cryptography arrangements [4]. It usually concurs that the innovation needs time to develop [5, 6], yet we should be prepared for the appropriation of this uncommon archetype. The capability of blockchain innovation to drastically change communications should raise basic inquiries for governments what's more, society. Figure 8.1 gives a clear picture of the evolution of healthcare.

Blockchain 1.0 was dealing with cryptocurrency such as bitcoin where the secure transaction can be performed between different users. This also enables Distributed Ledger Technology or DLT. While in blockchain 2.0 the smart contracts are the key point. The scalable UI for the user end and the decentralized application is the main focus point in Blockchain 3.0. The DAPPS is the combination of the user-defined front end with the smart contracts. Blockchain 4.0 is fully dedicated to Industry 4.0. Blockchain is in its beginning phases however it charmed huge reactions and enthusiasm from the organization and the researcher in different fields like banking,

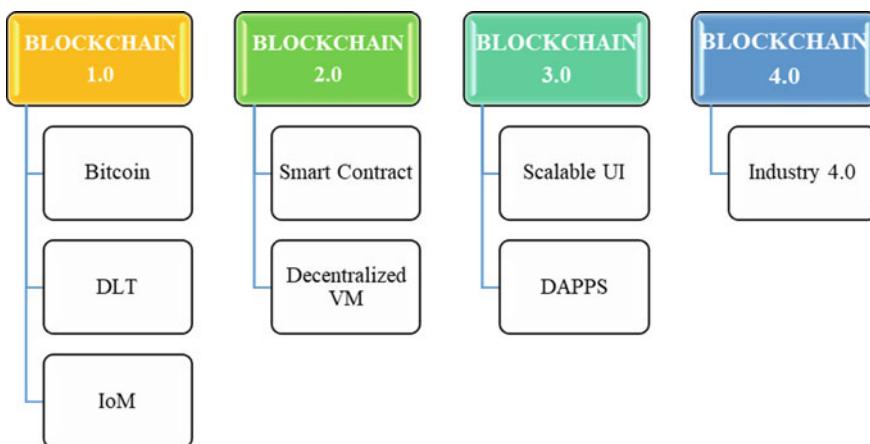


Fig. 8.1 Blockchain evolution

IoT and health care system, etc. Blockchain along with DLT can contribute various advantages to the medical industry. Blockchain innovation's different highlights like decentralization, security, protection, bitcoin, and smart contracts by means of cryptographic calculations [7] have the ability to address the current issues of the clinical and health care segment. It can ease dependence on a solitary incorporated position which is more helpless against mistake and frailty. The interoperable framework of blockchain will upgrade the information trade among different health care points to improve coordination, QoC, advancements, and market rivalries emphatically [8]. This problematic innovation could possibly resolve the issues of fake medications and billing systems as it gives chronicled data to follow the root of exchanges making all the activities straightforward [9]. This innovation can change over the current expensive frameworks to cost-saving or even cash creating frameworks [10] as the clients are remunerated with advanced money as a motivating force for their commitment. A blockchain-based foundation can be conceived for improved decentralized maintenance of different patient and other health-related records, information trade. Blockchain has a huge potential to change the current medical services foundation. Be that as it may, there are a few difficulties that have been distinguished such as security, confidentiality, and sustainability [11].

8.2 Features of Blockchain

The features of blockchain such as immutable, decentralization, security, DLT, consensus, and quick settlement make it more adaptable.

- **Immutable:** This characteristic ensures the user that the data cannot be changed which makes the peer-to-peer network more constant and unchanged network. Once the data is stored in the network then for modification purposes the permission is needed from every node present in the network for a secure transaction. Those are validating the modification request and the transaction is called the miners. By using this characteristic, the blockchain becomes more secure [12].
- **Decentralization:** If the organization is decentralized then it doesn't have a solitary individual taking care of the structure or maybe a gathering of hubs keeps up the organization making it decentralized. This is one of the key highlights of blockchain innovation that works impeccably [12]. Due to this feature, the blockchain has some significant benefits such as
 - Reduced failure
 - Transparency
 - No Scam
 - Zero Third party
 - Robust network
 - The high rate of transaction
 - Authentication.

- Security: In addition to the decentralization the cryptography plays an important role in the blockchain. Every stored data is being hashed by using some key to maintain the CIA property of information security. The process of hashing is quite tough and it is almost impossible to alter the hashed data. A simple change in the hashed data creates a different ID which will mismatch with the original ID. Since each of the present nodes in the blockchain network has the same data then the attacker needs to change the hashed value at each side which is impossible in nature. Due to this the blockchain now the day is becoming a more prominent factor in technology [13].
- DLT: It stands for distributed ledger technology which contains the transaction information and the participant information. IT opens in nature and it is not being stored privately. A blockchain is a public record that gives data of the apparent multitude of members and all computerized exchanges that have ever been executed. A square is the “overarching” part of a blockchain that should keep the record of the ongoing exchanges, and once they are finished, it goes into the blockchain. Squares are included consecutive way with the following square containing a hash of the past square. Another square is produced when the past square gets entered into the blockchain information base [13].
- Smart Agreement Algorithm: The blockchain is designed in such a way that the decision-making process will be more active and dynamic throughout the network. This can be achieved by implementing some SA algorithms such that every node has an equal chance to become a decision-maker. This means there is the trustworthiness in making a unique decision with the presence of heterogeneous type nodes [14].

Quick Settlement: Legacy banking system is quite slow in nature and it can take many days to make a transaction successful. One node is responsible for authorizing the transaction which pruned to a single-point failure. Also, there is a chance if the authority becomes malicious then the whole transaction becomes malicious. This can be avoided by using the blockchain technology where every node has the fair chance of becoming the authority to sanction the truncation. The person who will allow the transaction will choose randomly, hence the chance of malicious transaction will be very less. The person is elected on the basis of some problem-solving techniques. One puzzle will be supplied to each and every node present in the network and the node who will solve the puzzle will become the authority to sanction the transaction. The puzzle which is being given to the nodes is known as NONCE. NONCE means the Number only used ONCE is a number which is being added to the hashed data which has to be solved by the miners to authorize the transaction. In this way, the process becomes more secure and reliable in the case of blockchain [15].

Table 8.1 Literature survey

Reference	Platform	Methodology	Use case
Agbo et al. [15]	Public	PBEDA and ECDH key agreement protocol to solve the sharing problem inpatient health-related data	EMR
Azaria et al. [16]	IoT	Digital Signature Scheme and Merkle Hash function	EMR
Xia et al. [17]	Ethereum	WSN with IPV6 protocol and RPi v3	Interoperability, SCM
Zhang et al. [18]	Ethereum	Encryption, NONCE, Decryption, Hash Function	Security
Zhou et al. [19]	Ethereum	Quorochain Algorithm and Smart Contracts	Interoperability
Mytis et al. [20]	Ethereum	UIDs, Transaction History	SCM
Tandon et al. [21]	Ethereum	UID, Transaction History, Digital Signature	SCM
Afrooz et al. [22]	Permissioned Blockchain	Fault Tolerance Algorithms, Smart Contract	EMR
Agbo et al. [23]	IoT	WSN controller, Hash Function, IPV6	Biomedical Research
Ahmad et al. [24]	Ethereum	UID, Big Data	EMR
Omar et al. [25]	Public	Digital Signature, Hash	Smart Contract
Alla et al. [26]	Ripple	WSN, DAPPS, ADB, and Machine Learning	Patient-Centric Information Sharing
Angelis et al. [27]	Open Chain	Hash Function, Digital Signature, Smart Contract	Insurance
Angraal et al. [28]	Ethereum	UID, Encryption, Hash Function	EMR
Arrieta et al. [29]	Ethereum	Digital Signature	EMR
Aznoli et al. [30]	Ethereum	Transaction History, UID, Consensus Algorithm	SCM
Badr et al. [31]	Ethereum	Peer Network, Transaction History, Digital Signature	SCM
Behera et al. [32]	Ethereum	DNN, Cryptography Algorithm, UID	SCM

(continued)

Table 8.1 (continued)

Reference	Platform	Methodology	Use case
Brogan et al. [33]	IoT	Authentication, Blockchain concept	Research
Campbell et al. [34]	Public	Digital Signature	Smart Contract
Casado-Vara et al. [35]	Ripple	Android, GPS, Authentication Protocol	Patient Centric Information Sharing
Chattu et al. [36]	Ethereum	UID, Hash Function	EMR
Cios et al. [37]	Open Chain	Cryptography, Hash Function, Smart Contracts	Insurance
Dagher et al. [38]	Bitcoin	PKI, NONCE, Hash Value	Payment platform
Devadass et al. [39]	Ethereum	DAPPS, DLT, UID	EMR
Dhagarra et al. [40]	Steller	UID, Digital Signature, Hash Function, Peer Network	SCM

8.3 Literature Survey

Table 8.1 will represent the detailed study of research work that has been done in the blockchain in the health care system.

8.4 Working of Blockchain

Blockchain consists of 3 main components such as Block, Node, and Miners. Block will contain 3 things data, nonce, and hash value. Miners are responsible for creating the new blocks in the network and the process is known as mining. While creating the new block the hash value of the previous block needs to be taken care of and referenced [15]. Along with the creation of new block miners also take part in solving the NONCE to become the authority for sanctioning a transaction. Miners use dedicated software for solving the NONCE problem. For modification in any block needs remaining as all of the blocks that will come after the intended block. When a block is being mined successfully then every node present in the network will agree on the same value and the miner will be financially awarded [16]. Node is the most important factor in blockchain technology. Nodes are the electronic device that will maintain the DLT and keeps the network in functional mode. The nodes have their copies of blockchain and the network must approve any kind of mining process that is occurring inside the network. Since the blockchain is transparent so each operation on the DLT has to be checked and viewed by every participant. Figure 8.2 describes the working principle of the blockchain.

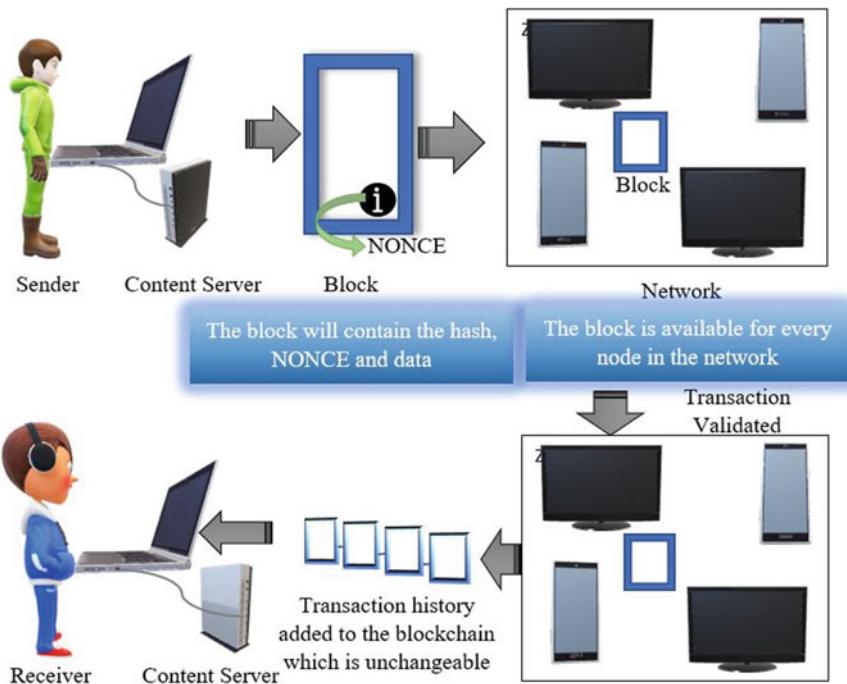


Fig. 8.2 Working procedure of blockchain

When a miner or node wants to initiate a transaction then it creates a block that contains the data, hash value along with the NONCE. After creating the block, it immediately sends the block to the network for approval. Each participant will mine the block and will try to solve the NONCE puzzle by using some dedicated software. The node which will obtain the solution for the NONCE provided in the block will have the authority for the current transaction. After approval from every participant, the node which has created the block will forward it to the destination by including the hash of the previous transaction [17, 18].

8.5 Application of BlockChain

Traditional health institutes are utilizing outdated ways to handle health-related data. The data includes patient health records, drug reports, patient insurance information, etc. This outdated data handling will put an impact on patient treatment. Most of the health care organization has its ways to deal with the health-related data which will reduce the degree of transparency in between the patient and organization. Patient health-related data are just like a puzzle that will lose its integrity and accuracy while misconfiguring the data. A small change in the data will intend in improper treatment.

With the presence of a large number of patients, it is very difficult to handle those data [19].

The use of blockchain will make a huge change in the data management system which will enable the health care system to share the patient-related data more effectively and securely. Blockchain can help to build up Blockchain clinical records. This cuts away superfluous managerial expenses and furthermore takes into account legitimate health information usage. Furthermore, the utilization of the blockchain can lessen the need to go to the third party to administer the trading of indispensable health information. Distributed Ledger Technology or DLT will be used in blockchain for storage purposes [20].

DLT which stores the information in a permanent way and updates the data progressively has been reshaping the health care area in entirety. The conventional models in this scene end up being profoundly wasteful as far as conveying quality medical services which are reasonable in nature by the people [21]. Blockchain-based medical services applications are fit to be utilized and change the health care establishments over the world. Blockchain works for improvising the transparency and effectiveness, different groups are related to the health care framework, and patients get profited. The administrative process is now a day simpler to oversee. Improvement can be found in the business tasks utilizing the inventive innovation. The customary medical service framework is moderate and costly and furthermore includes different delegates into the framework; all such issues get settled with the assistance of the blockchain technology [22]. The health care industry is generally energized for changing to blockchain method. Change to a blockchain upheld health care framework would reduce expenses and improve the security and interoperability of wellbeing reports. The blockchain medical services genuine models and cases utilize keen agreements which they could use so as to handle the medical procedure receipts effectively and productively, and development of emergency clinic bills among the medical clinic, understanding, and the protection supplier. A patient can cooperate with a blockchain-based medical services framework so as to see every one of his cases, clinical history, and past due installments effectively and in a superior way. With the assistance of smart contracts, the people can likewise utilize the blockchain to plan and book appointments and commitment with their staff, which can be begun when the enrollment sum is paid, and the specialist affirms accessibility [23].

Proper clinical information management is one of the key points of interest to Blockchain and medical care. Numerous issues influencing the medical services industry, for example, interoperability, information fruition, misrepresentation, and even information loss during a debacle, can be removed. Blockchain can do ponders regarding the recovery process. Since health information wouldn't be put away in a solitary area, there wouldn't be a primary failure point. In the event that any given clinical office crumples because of some catastrophic event—health information would be protected [24]. The capacity to guarantee that health information is right is basic for the arrangement of suitable clinical administrations. Admittance to appropriate clinical information guarantees that medical services suppliers can give legitimate

diagnostics. This is additionally reinforced by the way that, when any information hits a Blockchain, any modifications to it become almost inconceivable. It is significant that clinical information can be put away in a Blockchain from different sources like computers, wearable devices, mobile, etc. that can help in reducing the expenses of clinical organizations. Another incredible territory in the medical care part where Blockchain and medical services can see use is drug recognizability—remedy detectability, however fake medications also. All information went into a Blockchain that is unchanging and time stepped. This diminishes the opportunities for fake medications to hit the underground market, notwithstanding remedy misusing [12, 25, 26].

8.5.1 *Blockchain in Health Care System Use Case*

This section will focus on all possible health care use cases where the blockchain can be implemented (Fig. 8.3).

Electronic Medical Record (EMR) is the most important use case of the health care system. As a unique and safe record of a patient is maintainable by using the DLT. This DLT will contain all types of data such as test results, a list of medications used during the treatment, prescription details, etc. for an individual patient which is being stored in a decentralized network from where it can be accessed anywhere anytime [27].

Prescription Compliance: Medicine provided to each different patient is costly and millions of patients are being hospitalized. After treatment, the patient can visit the hospital for a follow-up process. At that time the cost can be reduced to medicine. Motivation can be accommodated any improvement in medicine through application program interfaces (APIs) which will gamify the clinical solution taking cycle. Data that can put away on the blockchain will be available to the two specialists and patients [28].

Health Insurance: The patients are spending millions on the treatment. Health insurance plays a vital role in bill settlement. By using the smart contracts, the validity, and verification of the claim from the patient. After the verification, the claim will be automatically done without including the third party. By using the smart contracts, the degree of fraud towards the insurance sector reduces severely.

Personalized Patient Care: Due to the maintenance of DLT for an individual patient which can be shared among the patient-related and the doctor for better treatment.

Supply Chain Management: The industries which are supplying medicines and medical equipment to the hospitals for the treatment of patient have to maintain a supply chain. When the same medicines are demanded again then the industry will face difficulties to supply the corresponding medicine for the intended patient. By using blockchain the industry is able to maintain the transaction history from which

easily the previous history can be found for the corresponding patient. Hence the supply of wrong medicine will be reduced [28].

Clinical Trial: In the health care system many patients are there with different diseases and their complexity. Hence the clinical trial is done on a patient with a goal to cure the person. After each trial, the results are being stored along with the test result and patient statistics which can be accessed by the researcher at any time in the future. This will reduce the time to cure another patient having the same disease.

Payment Platform: The user can set the amount in the smart contracts which can be automatically forwarded to the health care industry. The fund stored in smart contracts can be used for emergency medical purposes.

Data Security: The patient data are stored in a block that needs to be shared between the doctor and the patient. The digital ids are being used to authenticate the sender and the receiver. As per the principle of blockchain technology, it is very difficult to manipulate the data stored in the block. For modification, the NONCE has to be solved and permission from each participant present in the network is being required.

Smart Contracts: The smart contract is a computer-based protocol which is being automatically executed upon the requirement. Basically smart contracts come into account in three different health care parts such as Insurance, Telemedicine, and patient-related records. Smart contracts along with the blockchain represent the future



Fig. 8.3 Healthcare use case using blockchain

of the health care system. Smart contracts make the use of an encryption process for secure data storage [29].

Biomedical Research: The clinical trials are stored along with the prescription and medicine details which can be traced in the future for research purposes. The biomedical researcher can retrieve the patient-centric data for improving the treatment procedures which can reduce the time and the cost for the patient.

Patient-centric Information sharing: In the blockchain, the DLT is maintained for the individual patient. Whenever necessary the DLT can be shared among the doctor and the patient relatives for better treatment. While sharing the DLT five things need to be taken care of such as aggregation, information liquidity, identity, the correctness of the data, and access protocols for the secure exchange of DLT along with the transaction history.

Interoperability: It has been focused on the health care system for exchanging the data between the sender and receiver. Sender and Receiver can be the doctors, the hospital management system, and the patients. FHIR or Fast Healthcare Interoperability Resource indicates the data formats while sharing the patient-centric data in a public API [30].

Trustable Clinical Data: The use of blockchain technology in the health care system make sure about data safety during the transaction. Once the data has been stored in the block it will be hashed and one NONCE will be added in order to secure the data. Without solving the NONCE no miner can interfere with the data. For any kind of modification, the miner or node needs the permission of all available participants in the peer network. The block is publically stored at each node side [27]. So a slight change in the data will create a different hash value that will mismatch with the original hash that is being already stored at different participants. During the transaction, the hash value will be cross verified, and if mismatched the transaction will be strictly discarded. For any kind of modification, the miner needs to solve the NONCE and the solution is to be submitted to the owner. After verification and permission from every participant, the third party is allowed to change the data. In this way, the patient and clinical data are safe when the blockchain is implemented [16].

8.5.2 Key Benefits of Blockchain in Health Care

Health care system has various advantages as per the blockchain feature such as peer network, cryptography, DLT, NONCE, smart contracts, trustworthiness, permission transaction, hash function, etc., as shown in Table 8.2.

Table 8.2 Benefits of blockchain in healthcare system

Blockchain characteristic	Benefit in healthcare
Peer Network	Secure Infrastructure
Cryptography	Encrypting the stored data for preventing the unauthorized access
DLT	Cost Reduction, Reduced Operational deficiencies, Access Control
Decentralization	Removes the single point failure
NONCE	Better Authorization for a successful transaction
Smart Contracts	Increases Transparency, Increased Speed of Communication, Paperless work, High Efficiency
Trustworthiness	Secure Transaction due to random authority election per transaction
Permissioned Transaction	The reduced degree of Interference in stored data as permission from all participants is mandatory for any kind of modification in the stored data [17]
Hash Function	Increases degree of Integrity as each data is hashed with the public or private key and stored at all nodes present in the network. A small change in data will change the hash value which will mismatch at another node side whenever asked for permission for a successful Transaction [17]

8.5.3 *Challenges of Blockchain in Healthcare*

Along with the various benefits, it has several challenges such as storage capacity, dynamic data, scalability issue, privacy, lack of interest, shifting the legacy system to blockchain technology are making the scenario difficult in implementing blockchain in the healthcare system. Table 8.3 shows the parameters along with the way they are becoming the most prominent barriers in blockchain implementation.

8.6 Conclusion

Now a day the medical records such as prescription, test results, and analysis reports are stored on a paper. Hence it can be easily deleted which will create a problem. The solution is to store all data in the form of an electronic record. But the disadvantage is having a centralized admin to maintain the record which is prone to a single-point failure. In this chapter, we have described the blockchain technology, its working principle, and the key features for solving the issues of the traditional system. We then defined the BCT for the healthcare system along with the use-case, benefits, and challenges to accept the BCT as a real-world solution to the healthcare system. Despite the several key benefits like cryptography, DLT, NONCE, and decentralized nature, still, there are few drawbacks such as scalability issue, storage limit acts as a barrier.

Table 8.3 Challenges of blockchain in healthcare system

Parameter	Effect in Implementing BCT
Storage Capacity	The number of hospitals and patients is large so numerous amount storage is needed for storing those data which is practically very difficult [19]
Dynamic Data	The health care data is dynamic in nature. The data are changing every second which needs to be stored in the blocks of blockchain regularly. The modification process is very long as it needs permission from every participant is mandatory which will increase time complexity indirectly [19]
Scalability Issue	The decentralized framework of blockchain makes difficulty in adding more health care system to the existing blockchain. Every time the node has to be elected which will add the new system to the existing one [19]
Privacy	Due to the independent, decentralized nature, a less number of regulations are there for controlling the BCT
Lack of Interest	Various systems are there who do not have any interest to share health-related data as they are maintaining the data in their own convenient way [21]
Shifting the Legacy System to Blockchain Technology	Many doctors are dependent on the paper while making the prescription to the patient and not showing their interest in EMR. It is very difficult to shift the legacy system into the BCT

References

1. Zhao, H., Bai, P., Peng, Y., Xu, R.: Efficient key management scheme for health blockchain. *CAAI Trans. Intell. Technol.* **3**, 114–118 (2018). <https://doi.org/10.1049/trit.2018.0014>
2. Zhang, P., White, J., Schmidt, D.C., Lenz, G., Rosenbloom, S.T.: FHIRChain: applying blockchain to securely and scalably share clinical data. *Comput. Struct. Biotechnol. J.* **16**, 267–278 (2018). <https://doi.org/10.1016/j.csbj.2018.07.004>
3. Boullos, M.N.K., Wilson, J.T., Clauson, K.A.: Geospatial blockchain: promises, challenges, and scenarios in health and healthcare. *Int. J. Health Geogr.* **17**, 25 (2018). <https://doi.org/10.1186/s12942-018-0144-x>
4. Tseng, J.-H., Liao, Y.-C., Chong, B., Liao, S.-W.: Governance on the drug supply chain via Gcoin blockchain. *Int. J. Environ. Res. Public Health* **15**, 1055 (2018). <https://doi.org/10.3390/ijerph15061055>
5. Griggs, K.N., Ossipova, O., Kohlios, C.P., Baccarini, A.N., Howson, E.A., Hayajneh, T.: Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *J. Med. Syst.* **42**, 130 (2018). <https://doi.org/10.1007/s10916-018-0982-x>
6. Yue, X., Wang, H., Jin, D., Li, M., Jiang, W.: Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. *J. Med Syst.* **40**, 453 (2016). <https://doi.org/10.1007/s10916-016-0574-6>

7. Cichosz, S.L., Stausholm, M.N., Kronborg, T., Vestergaard, P., Hejlesen, O.: How to use blockchain for diabetes health care data and access management: an operational concept. *J. Sci. Technol.* **13**, 248–253 (2018). <https://doi.org/10.1177/1932296818790281>
8. Nugent T., Upton, D., Cimpoesu, M.: Improving data transparency in clinical trials using blockchain smart contracts. *F1000 Res* **5**, 2541 (2016). <https://doi.org/10.12688/f1000research.9756.1>
9. Liang, X., Zhao, J., Shetty, S., Liu, J., Li, D.: Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In: Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, Canada, 8–13 Oct 2017, pp. 1–5
10. Marefat, M., Juneja, A.: Leveraging blockchain for retraining deep learning architecture in patient-specific arrhythmia classification. In: Proceedings of the 2018 IEEE EMBS International Conference on Biomedical & Health Informatics (BHI), Las Vegas, NV, USA, 4–7 March 2018
11. Zhao, H., Zhang, Y., Peng, Y., Xu, R.: Lightweight backup and efficient recovery scheme for health blockchain keys. In: Proceedings of the 2017 IEEE 13th International Symposium on Autonomous Decentralized System (ISADS), Bangkok, Thailand, 22–24 March 2017, pp. 229–234
12. Fan, K., Wang, S., Ren, Y., Li, H., Yang, Y.: MedBlock: efficient and secure medical data sharing via blockchain. *J. Med Syst.* **42**, 136 (2018). <https://doi.org/10.1007/s10916-018-0993-7>
13. Al Omar, A., Rahman, M.S., Basu, A., Kiyomoto, S.: MediBchain: a blockchain based privacy preserving platform for healthcare data. In: Human Centered Computing, vol. 10658, pp. 534–543. Springer Nature, Basingstoke, UK (2017)
14. Liu, P.T.S.: Medical record system using blockchain, big data and tokenization. In: Human Centered Computing, vol. 9977, pp. 254–261. Springer Nature, Basingstoke, UK (2016)
15. Azaria, A., Ekblaw, A., Vieira, T., Lippman, A.: MedRec: using blockchain for medical data access and permission management. In: Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), pp. 25–30, Vienna, Austria, 22–24 August 2016
16. Xia, Q., Sifah, E.B., Asamoah, K.O., Gao, J., Du, X., Guizani, M.: MeDShare: trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access* **5**, 14757–14767 (2017). <https://doi.org/10.1109/ACCESS.2017.2730843>
17. Zhang, P., Walker, M.A., White, J., Schmidt, D.C., Lenz, G.: Metrics for assessing blockchain-based healthcare decentralized apps. In: Proceedings of the 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom), pp. 1–4, Dalian, China, 12–15 October 2017
18. Zhou, L., Wang, L., Sun, Y.: MIStore: a blockchain-based medical insurance storage system. *J. Med. Syst.* **42**, 149 (2018). <https://doi.org/10.1007/s10916-018-0996-4>
19. Mytis-Gkomethe, P., Efraimidis, P.S., Kaldoudi, E., Drosatos, G.: Notarization of knowledge retrieval from biomedical repositories using blockchain technology. In: IFMBE Proceedings, vol. 66, pp. 69–73. Springer Nature, Basingstoke, UK (2017)
20. Accenture: Percentage of healthcare payers and providers that reported select types of data breaches as occurring most frequently as of 2018, 15. Statista. Statista Inc. (2020)
21. Afroz, S., Navimipour, N.J.: Memory designing using quantum-dot cellular automata: systematic literature review, classification and current trends. *J. Circuits Syst. Comput.* **26**(12), 1730004 (2017). <https://doi.org/10.1142/S0218126617300045>
22. Agbo, C.C., Mahmoud, Q.H., Eklund, J.M.: Blockchain technology in healthcare: a systematic review. *Healthcare* **7**(2), 56 (2019)
23. Ahmad, M.O., Dennehy, D., Conboy, K., Oivo, M.: Kanban in software engineering: a systematic mapping study. *J. Syst. Softw.* **137**, 96–113 (2018)
24. Al Omar, A., Bhuiyan, M.Z.A., Basu, A., Kiyomoto, S., Rahman, M.S.: Privacyfriendly platform for healthcare data in cloud based on blockchain environment. *Future Gener. Comput. Syst.* **95**, 511–521 (2019)
25. Alla, S., Soltanisehat, L., Tatar, U., Keskin, O.: Blockchain technology in electronic healthcare systems. *IISE Annual Conf. Expo* **2018**(1), 754–759 (2018)

26. Angelis, J., da Silva, E.R.: Blockchain adoption: a value driver perspective. *Bus. Horiz.* **62**(3), 307–314 (2019)
27. Angraal, S., Krumholz, H.M., Schulz, W.L.: Blockchain technology: applications in health care. *Circ. Cardiovasc. Qual. Outcomes* **10**(9), e003800 (2017)
28. Arrieta, A.B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., García, S., Gil-López, S., Molina, D., Benjamins, R., Chatila, R.: Explainable artificial intelligence (XAI): concepts, taxonomies, opportunities and challenges toward responsible AI. *Inf. Fusion* **58**, 82–115 (2020)
29. Aznoli, F., Navimipour, N.J.: Cloud services recommendation: reviewing the recent advances and suggesting the future research directions. *J. Netw. Comput. Appl.* **77**, 73–86 (2017)
30. Badr, S., Gomaa, I., Abd-Elrahman, E.: Multi-tier blockchain framework for IoT-EHRs systems. *Procedia Comput. Sci.* **141**, 159–166 (2018)
31. Behera, R.K., Bala, P.K., Dhir, A.: The emerging role of cognitive computing in healthcare: a systematic literature review. *Int. J. Med. Inform.* **129**, 154–166 (2019)
32. Brogan, J., Baskaran, I., Ramachandran, N.: Authenticating health activity data using distributed ledger technologies. *Comput. Struct. Biotechnol. J.* **16**, 257–266 (2018)
33. Campbell, S.M., Roland, M.O., Buetow, S.A.: Defining quality of care. *Soc. Sci. Med.* **51**(11), 1611–1625 (2000)
34. Casado-Vara, R., Corchado, J.: Distributed e-health wide-world accounting ledger via blockchain. *J. Intel. Fuzzy Syst.* **36**(3), 2381–2386 (2019)
35. Chattu, V.K., Nanda, A., Chattu, S.K., Kadri, S.M., Knight, A.W.: The emerging role of blockchain technology applications in routine disease surveillance systems to strengthen global health security. *Big Data Cogn. Comput.* **3**(2), 25 (2019)
36. Cios, K.J., Krawczyk, B., Cios, J., Staley, K.J.: Uniqueness of medical data mining. In: How the New Technologies and Data They Generate Are Transforming Medicine, arXiv preprint [arXiv:1905.09203](https://arxiv.org/abs/1905.09203) (2019)
37. Dagher, G.G., Mohler, J., Milojkovic, M., Marella, P.B.: Ancile: privacypreserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustain. Cities Soc.* **39**, 283–297 (2018)
38. Devadass, L., Sekaran, S.S., Thinakaran, R.: Cloud computing in healthcare. *Int. J. Stud. Res. Technol. Manag.* **5**(1), 25–31 (2017)
39. Dhagarra, D., Goswami, M., Sarma, P.R.S., Choudhury, A.: Big data and blockchain supported conceptual model for enhanced healthcare coverage: the Indian context. *Bus. Process. Manag. J.* **25**(7), 1612–1632 (2019)
40. Dimitrov, D.V.: Blockchain applications for healthcare data management. *Healthc. Inf. Res.* **25**(1), 51–56 (2019)

Chapter 9

UML Conceptual Analysis of Smart Contract for Health Claim Processing



Subhasis Mohapatra, Smita Parija, and Abhishek Roy

Abstract Block chain and current economic scenario allow decentralization of data profile over peer to peer network. In this research work authors take the help of UML (Unified modeling language) to build a framework for health insurance claim processing that is using block chain to built smart contract. Smart contract application in health insurance industry incorporate user profile, electronic medical record, health insurance profile and linked bank agencies to automate claim settlement walk out on any third-party control. Smart contract is providing a promising solution to support insurance data validation over peer to peer transaction. Health insurance industry is untangling power of smart contract. Embedding UML analysis for block chain network build intelligence that showcase a conceptual processing of insurance data transaction. Though substantial research work in this regard is going on in numerous fields but still it needs more conceptual analysis before it's real time implementation. So, in this experimentation authors pinpoint block chain basic UTXO (Unspent transaction output) and UML test bed analysis for smart contract in health insurance service. This meticulous research outcome is justified by factual analysis of block chain. Moreover, it is given with context aware sequence analysis of smart contract in health insurance.

Keywords Smart contract · UML. UTXO · Health insurance · Sequence analysis · cloud computing

Please note that the LNCS Editorial assumes that all authors have used the western naming convention, with given names preceding surnames. This determines the structure of the names in the running heads and the author index.

S. Mohapatra (✉) · A. Roy

Department of Computer Science Engineering, Adamas University, Kolkata, India

S. Parija

Department of Electronics, CV Raman Global University, Bhubaneswar, Odisha, India

9.1 Introduction

Blockchain use case provide a specific level of security to any business model. In this perspective block chain is associated with a huge context to untangle some common security misconception [1]. Bit coin is offering certain common plan of security by using proof-of-work algorithm. To add block in a transaction it must validate all transaction block that is performed by repeated calculation which is called hashing. It is combining with one famous technique i.e. commonly known as longest chain rule to mine own subversive chain. There are three kind of blockchain (1) Public, (2) Private, (3) Permission. In public block chain there is no need of approval that indicate any one can read and write data over this network. If any discrepancies will happen then no boss is allocated to solve this issue. For example, Bit con in this anybody can join and leave without any restriction [2]. It is an open source wallet application. In private block chain all the participant is known and trusted. Here access is provided to limited number of participants. It can control access to business model. Now the third-party permission block chain falls in this category it is collaborating with parties for ease of governance ex-Automobile, health service industry. Bit coin and block chain don't provide any inherent security against read access Indeed block chain is a mechanism that can copy data to all relevant participant in this way consensus is achieved in network. Block chain is providing a remedial solution against hacking espionage system. So, the fertile ground of hacking surface is ruined by block chain application up to a remarkable extent. It is emerging as the most resilient technique compared to centralized system Peer to peer transaction in block chain provide multi redundancy.

Specifically, block chain introduces a vital concept of smart contract it consents claim service of citizen from citizen to bank end. Furthermore, the aim of this UML ontology in smart contract utilizes block chain technology. It supports peer to peer policy access without any third-party access control. A number of block chain researcher already working in this claim processing domain to verify different aspect of autonomous claim governance system. But it still needs some comprehensive overview to further analyze characteristics of ownership in claim. In smart contract intelligent business logic interact with each other autonomously to process claim request. In mean time smart contract reduce market counterfeit and manual processing of claim. Here in this research finding authors deal with a business prototype of smart contract through Unified modelling language-sequence diagram. This prototype model provide solution in smart contract. It concentrates upon different mode i.e. Bank, claim company, and peer group etc. By the use of smart contract everyone would get a clear idea of claim processing path and company policy. Despite of several advantages of smart contract majority of claim processing still need external expert suggestion before being resolved. From the model point of view authors has given a suitable choice to embrace a combination of public and private block chain. The private block chain is suitable for tracking policy record and claim, and the same time public block chain deal with refund of tradable crypto

currency (e.g. Bitcoin, Ethereum). The above policy definitely holds company's reputation and trust. As we all know block chain work without intermediaries so no one could steal claim credential of a person. In this research outcome authors has given credential checking mechanism of citizen in terms of User id and pass word. This paper provides precise analysis of participating nodes i.e. (Insurance company, Bank, Person). Smart contract can exploit various business logic for technology enhancement in health insurance claim industry. In addition to this smart contract authors have sincerely tried to accomplish business logic for health insurance claim. This is the future technology which gains momentum to exploit massive business opportunities in claim. Here authors have given certain future direction to extend smart contract logic for back office transaction. It comprehends between insurers and re insurers. Typically, when a claim is initiated insurer must verify its re-insurance content and channelize the logic with re-insurers for re-insurance recovery. A smart contract logic can be embedded on a block chain plat form to initiate recovery of transaction instantly. Smart contract in health claim processing will gradually add new revenue sources for micro level transaction. It is nothing but a pay per use insurance model that reckon on public block chain.

So many organizations opt for this application because certain significance level of security make it unique in compared to other application [3]. The underlying significance i.e. cryptography and digital signature i.e. enforcing arbitrary read and write access rights. So historical record adheres to transaction can't be modified easily. If anybody want to change this content that can be easily traced in block chain as all the record hash is linked with previous block hash if one hash has changed then it exhibits a wrong matching it is the underlying fashion of immutability in block chain. In current scenario block chain is emerging as a box of technology from which different item can be put in different ways to create different solution. For a easy understanding one analogy is given block in block chain is compared with page in a book as the page contains contents and header information in a similar way block contains information and implicit hash value of previous valid block [4]. It showcases a nice way of validating data to provide internal consistency if any intruder wants to meddle with record then he has to generate all hash from the current position so it is accumulating accountability feature that make access control more imperative to centralized system. Now new paradigm shift in block chain strengthen digital backbone of block chain crypto currency is rather a proven technology in block chain is considered as type-I, in type-II currency and business logic is embedded, in type-III only business logic is embedded Ex-Hyper ledger under Linux [5]. It is adding cryptographic proof to some part of block chain it is enhancing cryptographic auditability. Crypto currency is a digital currency which is a medium of exchange nobody is authorized to change unless specific condition is fulfilled for ex-Ethereum is a Turing complete programmable currency it is used in distributed application [6]. It would not work with Bitcoin. Another example is Ripple it has not taken advantage of block chain rather it is mapped on iterative consensus process [7]. Ripple is faster than Bit coin but more vulnerable to attack. In digital world two things are vital authorization and authentication. Some innovative crypto currency is given as below for reader guidance [8].

- **IOTA (Internet of Things Architecture)**

It depicts an open source distributed ledger architecture for internet of things. Also, uses break through ledger technology i.e. named as tangle. Sender in a transaction must adhere to proof-of-work that approves two transaction [9, 10]. So, it ultimately eliminates dedicated miners from the framework [11].

- **NEO (Network of Smart Economy)**

It is a smart contract network ex-all kind of financial transaction contract is based on this application [12].

- **DASH (DASH formerly called as dark coin)**

This is a two-tier network the first tier is deal with miners which secure network and second tier is master node it is capable of relaying transaction. At the same time enable private sender to type transaction [13, 14].

- **QTUM (Pronounced as Quantum)**

It is a conglomeration of bit coin and Ethereum technology for broad business application [15].

This model enables a platform for others to access records by granting access to patient and practitioner. The remainder of this paper is organized as follows the remainder of this paper is organized as follows. In Sect. 9.2, we present some basic concepts of Block chain. Section 9.3 describes transaction in block chain. Section 9.4 explains Ethereum block chain. Section 9.5 depict motivation and contribution of the proposed work. Section 9.6 survey upon smart contract contribution in health insurance analysis. Some related study presented in Sect. 9.7. Analysis of UML modeling for block chain technique explained Sect. 9.8. Smart contract terminology is depicted in Sect. 9.9. Section 9.10 describes gas Terminologies in Smart Contract and finally conclusion is presented.

9.2 Basic Elements of Block Chain

Orchestration of three technology guide the internal framework of block chain private key, internet and protocol governing E-transaction in this perspective the basic element in block chain is given as below.

1. Block store data in block chain it is prefaced by block header and protected by proof of work. A chain of block is preceded by referencing [16].
2. Block header contains 80 bytes; it signifies size of block chain which is hashed repeatedly to create proof of work [17].
3. Block height is the number of preceding a particular block on a block chain- genesis block has height zero because it the first block in block chain [18].

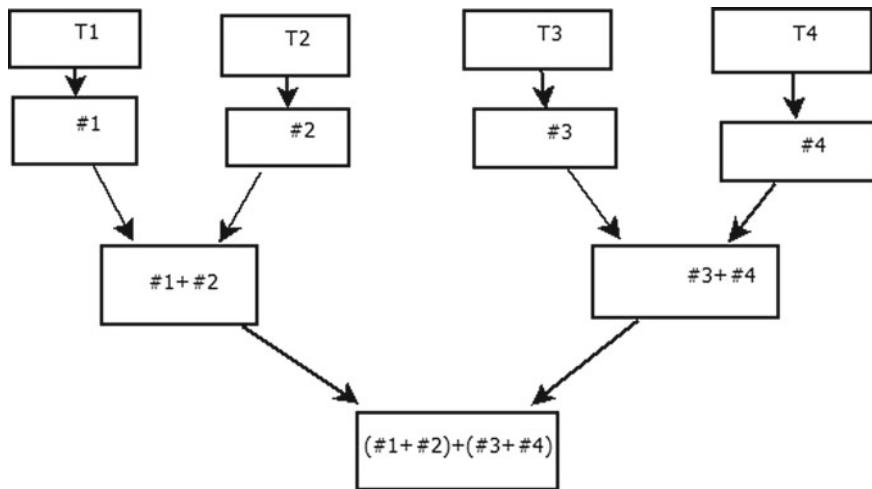


Fig. 9.1 Block diagram of Merkle tree computation

4. Block reward signifies the amount that miners claim as reward for creating a block. It is equal to sum of the block subsidy plus transaction fees paid by transaction. [19].
5. Maximum block size as per current consensus rule is four million height unit [20].
6. Merkle tree it is nothing but a binary tree where each internal node contains hash value of the children node. Hashing is paired with data in children node it goes on until a single root is generated i.e. called Merkle root. The leaves are almost always transaction from a single block [21]. The Merkle tree computation block diagram is given in Fig. 9.1 here T1 to T4 are depicted as transaction in each internal node computation is done as below Fig. 9.1.
7. Mining is the act of creating a valid bitcoin block. miners are nothing but device that mine complex cryptographic puzzle. People own these devices [22].
8. Miners fee indicate the amount remaining when the value of all output in a transaction are subtracted from all input in a transaction. It is paid to miner who includes that transaction in a block.
9. Wallet is a software that store private key and monitor block chain to allow user to spend and receive Satoshi's.
10. Satoshi's is a denomination of bit coin value one bit coin is equal to 100,000,000 Satoshi's [23].
11. Peer is a machine that is connected to bit coin network, Genesis block is first block in block chain.
12. A fork is a term defines when two or more miners find block at the same time it is a part of attack.

13. Double spend is a transaction that uses the same input as already broadcast transaction. The duplication of transaction is adjudicated by only one of the transactions [24].
14. Network difficulty signifies how hard it is to find a block relative to difficulty of finding the easiest possible block.

9.3 Transaction in Block Chain

The basic element of block chain is transaction block is added to it in a consensus process. One special power node is called miner. The fundamental element of block chain is UTXO (Unspent transaction out) which is input to a transaction it is held by participant node. so, a block is given input UTXO and in output it generates output UTXO. UTXO include Unique identifier of transaction it is created at the initial stage of transaction, Second one is index of UTXO, third is condition under which output can be spent which is optional. Transaction is termed as (Tx) it includes reference number of current transactions, reference to one or more input UTXO, reference to one or more output UTXO i.e. newly generated by the current transaction. Block chain operation is done in a decentralized network by peer to peer participation here peer is nothing but a node for example server rack, laptop etc. validation of a transaction gathers valid transaction for block creation. So, it achieved by broadcasting. There are two major participants in a block chain one that initiate transaction and second one is miner, Miner verify, broadcast, and compete to build a block. Miners are members in a network with high level of computing power that compete to validate transaction by giving a solution to complex coded problem and win a reward for this (Bit coin) Miner efforts confirmation to get bit coin. The concept of block chain transaction is given in Fig. 9.2 it propagates easy understanding to reader. Now in this block chain context authors gives a brief overview of Bit coin it is first appeared in 2008 white paper by Satoshi Nakamoto. It is a P2P (Peer to peer) E-cash system transferred directly any intermediary. It is a digital transaction based on cryptographically protected block. Miners compete for solving puzzle when the block is solved it is broad casted to network, after verifying new block it is added to chain. TX [0] has no input UTXO coin base transaction currently it is 12 BTC. Here block chain aim is to create a single consistent chain. Transaction is a broad concept in this regard every node needs to

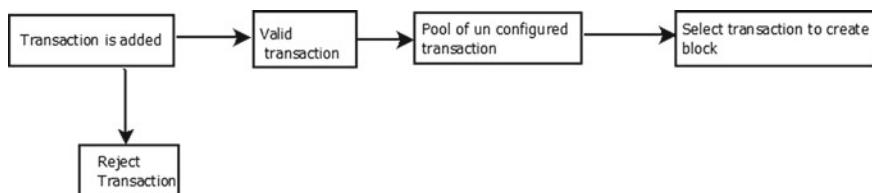


Fig. 9.2 Flow of block chain transaction

keep update different version of event. Now script is added to transaction ex-smart contract.

9.4 Ethereum Block Chain

Its main component is depicted as follows

- Block header
- Transaction hash
- Transaction root
- State hash
- State root.

The major component of Block header is given as a pictorial representation in Fig. 9.3.

It establishes trust in a block chain SHA-3 algorithm Keccak can compute block header in smart contract. Every state change in smart contract require re computation of state root hash for verification and integrity. Hashing and encryption are the two major component in smart contract. Block header is computed by SHA-256 algorithm twice. It is calculated by each node for establishing verification in a network. Once it is a variable element it is changed by miners to try numerous sets of permutation to achieve a specific difficulty level. Smart contract is changing current economy in term of trust building which is given in Fig. 9.4.

Validation process in Ethereum is not a single step process it needs to verify syntax, signature, timestamp, nonce, gas limit, sender account balance, gas point of resource and transaction signature hash. Gas value is nothing but the pricing mechanism to build a transaction in Ethereum smart contract [24].

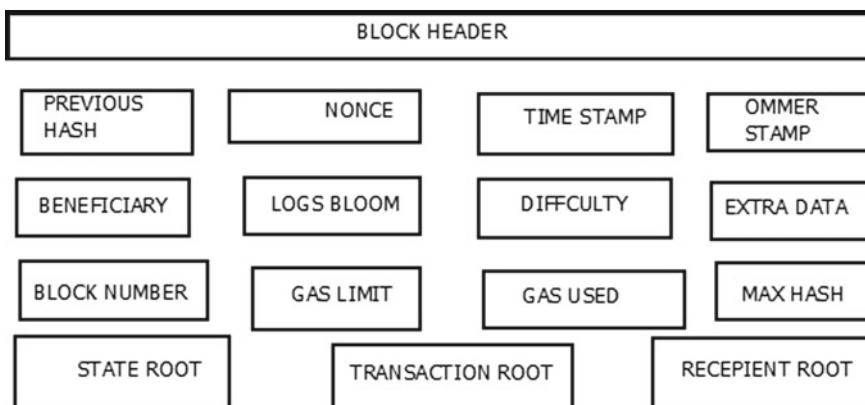


Fig. 9.3 Ethereum block header

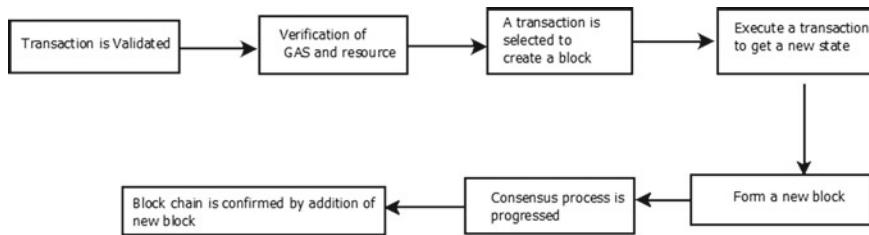


Fig. 9.4 Confirmation steps of new block addition in a block chain

9.5 Motivation

The entire gamut of block chain application in healthcare service domain show case service redistribution with peer to peer management and abolishing third party control. The feasible solution march towards resolving queries of service seeker and service provider. Block chain authenticate streamline access of service to service seeker. The block chain administration automates linking of information i.e. policy tariff in a non-disputable manner over smart contract. Now the question arise why block chain logic penetrates like wild fire to every sector, the feasible answer is immutable control. Here each data is associated with unique hash. Hence it prevents against single point failure. Though it gathers popularity in every single day but still some resilient research is needed in timestamp based immutable linking of business record.

More over in this research exploration authors collected various approximate information to build this conceptual model, so it must revamp health insurance ecosystem. The model includes vale added service design to bank, claim company, beneficiaries. The interaction among them is given in sequence diagram in Fig. 9.8. The complexity of claim processing in smart contract is shown in a piecemeal manner through various class node i.e. citizen, kiosk, smart contract, policy claim and bank. The effective key parameter of this research outcome include how it mitigates centralized control from multiple stake holders. The information flow between different class node is participative parameter to exchange data. It creates a tamper proof authentic model for a trusted domain like health insurance which needs qualitative attention in this regard. The model analysis showcases operational efficiencies to simplify complex time bound decision logic in smart contract.

9.6 Survey of Smart Contract in Health Claim Processing

This section of article propagates a comprehensive survey of health insurance data management and peer to peer self automation. Health care communities still need direct integration of citizen, claim organization, bank and block chain to achieve smooth integration. In this section authors have given reports on UML ontology

development and concept building frame work in health insurance. That helps to achieve operational resilience. In addition to this block chain overcome certain architectural short coming in health insurance. Block chain is a ubiquitous security enhancement research trend. It categorizes usage pattern of immutability. Health insurance is at the peak of hype curve as per recent market survey. So for quality enhancement in health insurance it need block chain integration As we can shift our focus from decentralized architecture to peer to peer accessibility. The potential of block chain collects useful security enhancement option i.e. smart contract, chain code etc. It provides tamper proof and highly decentralized solution for health insurance record dissemination. In block chain each peer is appropriately authenticated and authorized. Health insurance continuously face privacy leak over exchange of data over electronic media. So, block chain provide solution to this problem. The major step taken by block chain is decentralized infrastructure that concept truly help to built the security ecosystem in health insurance. As block chain creates an opportunity in health insurance domain. It has tremendous potential to track citizen insurance information over Claim Company and bank. At some point insurance record monitor patient's credential in terms of how much claim is covered, how much premium patient has paid, and personal information. These are information which need zero exploitation. Each day rise in cyber vulnerabilities aims to explore existing internet infrastructure so from consumer end health insurance industry are shifting their legacy ecosystem to block chain. So, in respective section authors propagate idea of block chain integration opportunity as a future research direction. As we know block chain is redefining health insurance sector in terms of improving quality and effectiveness of data mobility. Every country has their own law over protection of data in their code of law (privacy and owner ship of data).so consumer information under transient environment need enforceable security infrastructure like block chain to protect against cyber attack.

9.7 Analysis of UML Modelling for Block Chain Technique

UML modelling diagnoses efficiency of system in research area before its implementation. The recent research area includes support service for patient claim in personalized medical service through smart contract. The autonomous management of patient claim request is designed in this paper. Subsequently communication through class component is studied effectively by sequence diagram. Its further coordinates action constructively among method within the class by use case analysis. It processes citizen request and provide quality of service in placing claim request and processing. This is an adaptive model for real life implementation. The behavior of model is going to monitor judiciously patient response for claim. The research including online e-payment request processing through bank. It is elaborated in Fig. 9.5, in this section.

Further it consists of claim processing from citizen to bank in an interoperable efficient load distribution technique. We judiciously focus upon object-oriented

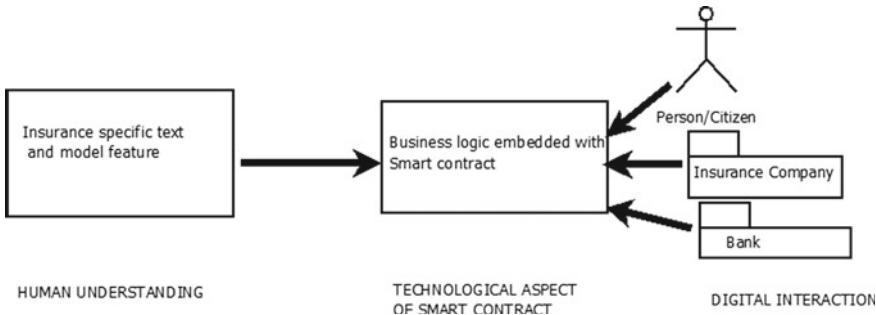


Fig. 9.5 Basic model of smart contract in insurance processing

modelling technique for a group of class cooperation leading towards effective coordination of job. Here in Fig. 9.5 rectangle component at the top indicate class (Citizen, KIOSK, Smart contract, Policy claim, Bank).

The proposed infrastructure of the model is given in Fig. 9.5. It amplifies user understanding in this perspective it focuses on three levels of abstraction (1) Human understanding, (2) Technological aspect behind smart contract, (3) Digital interaction. Smart contract provides interface logic between digital interaction and human affective understanding. In Fig. 9.4 Meta model of smart contract defines roles and responsibility of each three levels of abstraction. This intuitive block model identifies potential ontology behind smart contract for future implementation.

Recently healthcare industry giving more emphasis towards placing of patient claim request settlement in peer to peer manner. It can be extended to provide helpful information to health management and citizen. It minimizes the action of virtual health broker who misguide citizen in the name of help. Here we propose an interactive sequence analysis to carry out claim feedback from citizen, Smart contract, and bank. We also add flowchart analysis as subject of research in this paper. It concentrates study upon interactive method call. It is studying functional feature of each component to validate a model. It can be enhanced further in provision of claim guideline rule. The key aim behind this paper urges reader to harness the potential of digital claim intervention in health industry in addition to this, the fundamental class components can realistically address all vital function for real life model implementation. The UML analysis can accelerate exchange of information between components for effective web-based application. The eventual impact of this analysis can access the entire financial ecosystem in health industry at a glance. In health insurance processing eco-system, a large volume of data is generated every day. So it needs proper processing in an intelligible manner in block chain environment each data is bound to certain technique and linked hashing concept.

Automating transaction is the vital aspect achieved through smart contract. The given UML application of smart contract can specify domain specific knowledge for analysis in block chain network. The UML sequence diagram incorporates semantic method for insurance application. i.e. pacing of claim service request, key generation, and transaction confirmation. It depicts ontological encoding behavior of smart

contract. As smart contract is one of the prominence field in block chain that has been leveraged across several industries, supply chain, healthcare, finance, and insurance. This research work relies on smart contract sequencing rule and functionality for of smart contract. The detailed analysis of Figs. 9.5 and 9.6 will surely help further research work in this domain. Smart contract is governed by self executing rule and embedded program logic it is a challenging task over which way to select embedded logic so UML approach design give a precise validation. It not only enforces end to end traceability between classes but also give dynamic overview of business level application. Here in this application dynamic aspect is distributed within citizen, kiosk, smart contract, policy claim and bank class. Smart contract helps to minimize

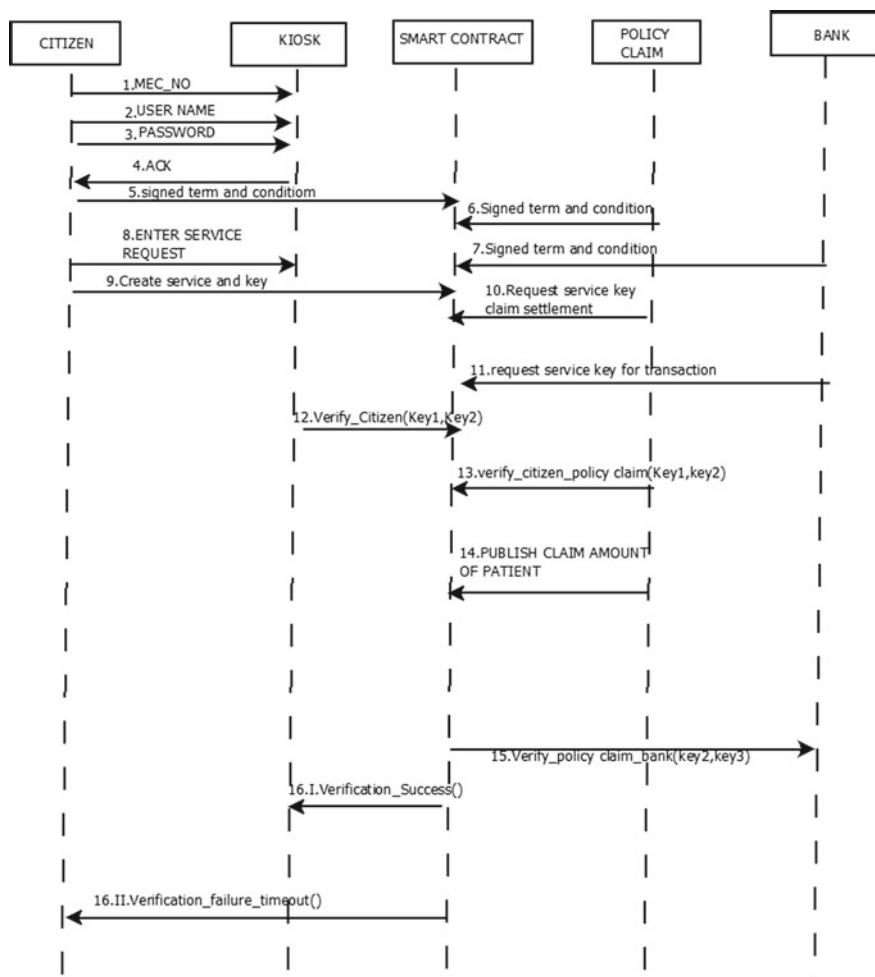


Fig. 9.6 Sequence diagram for claim service in smart contract

intermediaries as intermediaries in some cases channelize citizen specific personal information. In this finding authors has given a knowledge-based framework in Fig. 9.5, it can serve as a meta model for sequence diagram in Fig. 9.6. The vital component of UML ontology is class and relation so adhering to this concept this research work helps smart contract over Ethereum virtual machine. Knowledge representation in UML put standardization for client understandings this UML ontology stipulate functionality aspect of smart contract in block chain network. For example, when a citizen claims for insurance service her credential is checked and verified by KIOSK (GUI based application). Moreover, it makes a block of citizen information, claim service and secret key. The secret key would generate transaction over citizen, claim company and bank.

So, it will offer a robust mechanism under smart contract. Smart contract offers an innovative solution against data leakage. The latter advantage of this paper is to protect movement of personal data. Smart contract is not only providing law-full data processing but also it preserves legal obligation of insurance holder. It protects insurer data protection rights. Smart contract grant person's consent before its declaration so it accomplishes insurer data protection regulation (IDPR). UML sequence diagram given in Fig. 9.6 elaborate a vital user centric approach for the development of smart contract. It preserves transparency and un-ambiguousness. Relevant to insurance holder personal data leakage will destroy overall privacy of a company so in this research work authors propose a specific framework. It gives a overview of how data is filled in a GUI application (KIOSK) then processing over smart contract, claim processing and bank. The sensitive data has been accessed through cryptic key. It enforces a vital concept of block chain i.e. integrity and non-repudiation. So unauthorized user can't alter subject of data. Here aim of this research work is to build a citizen centric solution in health-insurance domain. State of art technology of block chain protect against malicious un-authorized attempt of intruder. Smart contract is providing an intelligence component class in this section. So, it can protect real-time user privacy in terms of policy disposal to specific policy holder. So, this UML reference model helps in future for risk assessment and supported implementation in smart contract that will surely saves time and money. UML approach potentially guide software analyst to decide technological aspect that is the basis of business model.

9.8 Algorithm

Algorithm for Sequence diagram

Step 1.

Start

Step 2.

User provide its credential to perform claim service. That include Unique MEC-NO (), USER_NAME (), PASSWORD () in KIOSK which is a GUI (Graphical user interface).

Step 3.

If patient credential is correct acknowledgement is sent ACK (), then it will go to next step otherwise time out go to END.

Step 4.

Citizen must initiate term and condition to build Smart contract, In subsequent step Claim company and bank must sign necessary credential to built smart contract.

Step 5.

Citizen create service key ENTER _SERVICE_REQUEST () AT Kiosk at the same time CREATE_SERVICE_KEY () is created for building smart contract, at the succeeding step claim company and bank request for this service and key through smart contract.

Step 6.

In smart contract class it will check on Key-1 and Key-2 value, Key-1 is held by citizen and Key-2 is held by claim company.

Step 7.

Bank class provide service by giving acknowledgement to smart contract. It check authenticity of transaction by SIGNED_TERM_CONDITION () with smart contract and at the same time it verifies CITIZEN_POLICY CLAIM () If verification is successful PUBLISH CLAIM_AMOUT_OF_PATIENT() otherwise verification failure message is given in KIOSK application to citizen.

Step 8.

Transaction End.

9.9 Smart Contract Terminologies

Before insurance transaction between insured and insurer authors have given some common terminologies and set of concepts that define data, rules, and concept in smart contract. The smart contract lays foundation of business model that facilitate interaction between transacting parties' smart contract is nothing but an executable code which help to invoke operation in block chain. It invokes operation in block chain ecosystem. It opens door for new business possibilities for any business model. Here in Fig. 9.7 execution logic of smart contract is specified in a block diagram which surely improves business logic in terms of insurance request action flow. So,

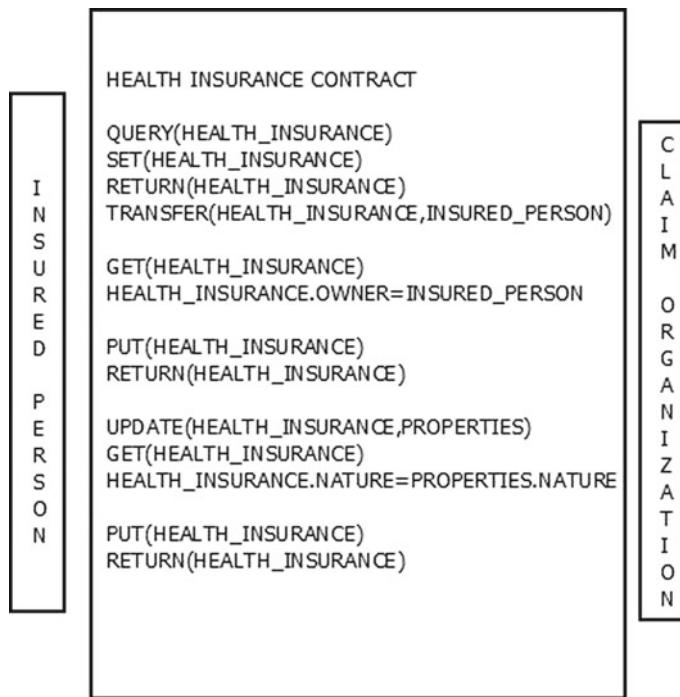


Fig. 9.7 Smart contract terminologies for health-insurance

in Fig. 9.7 business logic is interface between Insured (Person who claims insurance) and claim organization (Provider of health insurance). Hyper ledger fabric defines concept of chain code where as smart contract and chain code both refer to same thing. Chain code logic of block diagram is given in Fig. 9.8a, b. It encodes domain independent canon for system interaction. Chain code establish independent business logic in block chain network. Consequently, for reader reference authors simplify

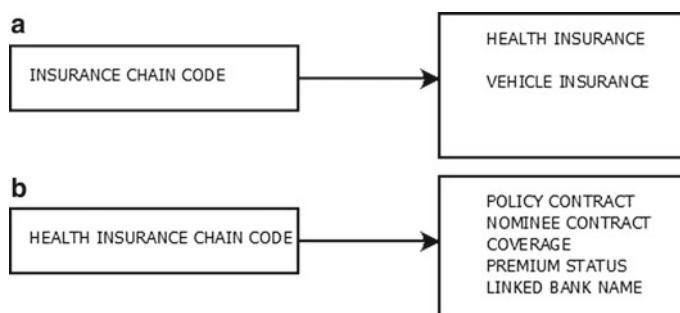


Fig. 9.8 **a** Insurance chain code logic in block chain, **b** Health insurance chain code logic in block chain

the concept as transaction logic. It controls lifecycle of a business object contained in world state. It is then packaged into a chain code followed by deployment into block chain network. Smart contract observes business transaction at the same time chain code set the principle for smart contract packaging and deployment.

9.10 Gas Terminology in Smart Contract

Gas is the vital aspect of smart contract. Ethereum block chain needs gas as it is utilized for transaction to pay off miners. Which in terms secure block chain transaction. Here the question arises how the amount of gas is decided for smooth operation. Subsequently what will be amount of gas and how maximum limit of gas will be set it is a challenging task for block chain developers. A precise amount of gas is needed to initiate a transaction as it sets transaction. If gas amount is low then transaction can't be initiated. At the same time miners lose the amount of remuneration. Block chain architect smartly decide amount of gas to set a robust platform the fundamental aspect of gas economy should be designed in such a manner that the smart contract platform pick right dynamics. Gas economy always try to minimize energy waste for long winding transaction. The gas economy judiciously set a priority by which important transaction compute cost in a priority basis to secure miner cost over the network This add legitimacy in smart contract.

Gas economy in my Ether wallet (Ethereum blockchain, Ethereum virtual machine) there is a field known as gas limit it sets maximum amount of gas, block chain designer provides different amount of gas limit for variety of transaction if we will provide little amount of gas transaction will prematurely. It makes transaction in an incomplete state. Right amount of gas boost network in a correct direction. In design time gas limit is an important guideline so gas limit reflects intelligence of network designer. As from miners' point of view miners has the ability to increase or decrease gas limit of block it sets right propagation in smart contract. Now the question arises if we set the gas limit high what will happen to block chain network?

As per general convention high fees proportional to faster operation in certain smart contract service gas price and gas limit is set automatically. The fees are calculated in gas unit. But in certain case manual setting of gas limit is also possible, faster operation need high charge too little gas amount make transaction risky. Here in this section authors have given an example of Ethereum gas refund scenario. In Solidity there are two command that guarantee gas refund mechanism, (I) **Suicide**—It describes kill operation in smart contract and get back of 24,000 gas, (II) **SSStore**—It means storage deletion and refund of 15,000 gas, here one example is taken for easy understanding of user, Example—A smart contract designer is using 13,000 gas and want to delete storage then refund gas amount will be $(15,000 - 13,000 = 2000)$ in this case miner will be in loss situation as he has done certain computation in block chain network. Hence to get rid of such scenario one condition is imposed i.e. refund which has been accumulated can't exceed half the gas used up during computation. As in example smart contract use 12,000, gas limit is 21,000. As per command

SStore Ethe creator get back $(21,000 - 12,000)$ as an unused gas, thus command theoretically refund 15,000 gas to creator but 12,000 gas is used by smart contract as per condition $[15,000 > 12,000/2]$, so, refund will be $6000 + 9000 = 15,000$. In Suicide operation suppose smart contract use 70,000 gas, as this operation delivers 24,000 gas so condition is given as follows $[24,000 < 70,000/2]$, In this scenario gas refund will be $24,000 + \text{unused gas amount}$. Gas trade of maintain balance of smart contract design complexity.

9.11 Conclusion

Now a days, block chain technology plays a vital role in all kinds of fields as it's one of the most important creative developments as well as discoveries. Smart contract will provide a unique identifier-based computing platform in claim processing. It abolishes third party intervention that play a crucial role in insurance industry. Smart contract is a major monitoring parameter in block chain application that significantly enable secured real time claim processing. Meanwhile It increases threshold of trust among service provider and service seeker. Smart contract evaluates unique delivery component of claim processing by assessing a cryptic code. Interestingly it employs better performance by adding cryptic defense layer against intruder attack. Smart contract in claim request processing add a hybrid detection mechanism such as security protection and legal binding of code. Due to massive digitization in health care and rise of claim processing has attracted many challenges like data theft, loss of privacy and integrity. It opens a new research field among investigator. Claim settlement over electronic media involves many sensitive information that include medical work flows, data of service seeker and provider for claim, etc. So, these components are taken into consideration for smart contract architecture. So, in this research outcome authors indicate conceptual solution of smart contract by reviewing on various relevant research outcome. Smart contract will surely provide a reliable healthcare solution in electronic health management system. Smart contract is next generation of high dimensional data security to decentralized claim processing. Smart contract split information between computing node by embedding business logic. Here the sole objective is to speed up the process of claim settlement by executing smart contract. It can reduce administrative burden by embedding general purpose business protocol. It can act a smart solution for automated monitoring of insurance claim. Smart contract is the current need of claim industry. It can be implemented in complex medical ecosystem to streamline claim procedure. However, in this paper authors focus upon demanding aspect of health care industry and limitation of current claim processing in health care. The ultimate goal of smart contract can ensure fine-grained and robust ecosystem in claim processing domain.

Block chain technology stirs in the direction of revolution and change. In this research work authors have proposed a framework in respect to health insurance domain. So smart contract accumulate money from citizen. (e.g. Ethers, Bitcoin) The research finding in this section give a broader aspect to reader for harnessing

potential application of smart contract. This study will further analyze scalability and potential outcome for different sector in claim i.e. micro claim, re-insurance claim and death claim etc. The model given in section—give a initiative plan for investigation of smart contract solution in healthcare claim processing. It is the future smart insurance model. It grants personal data management for comprehensive model development in smart contract. This UML ontology would provide reference model for assessment of underlying risk in their supported real time implementation. It definitely guides future insurance organization to unify understanding in terms of smart contract attribute building. Consequently, it standardizes insurance asset transaction over smart contract. The following research work focus on model accuracy and security assessment.

References

1. Griebel, L., Prokosch, H.U., Köpcke, F., Toddenroth, D., Christoph, J., Leb, I., Sedlmayr, M.: A scoping review of cloud computing in healthcare. *BMC Med. Inform. Decis. Mak.* **15**(1), 1–16 (2015)
2. Bhatti, A., Siyal, A. A., Mehdi, A., Shah, H., Kumar, H., Bohyo, M.A.: Development of cost-effective tele-monitoring system for remote area patients. In: 2018 International Conference on Engineering and Emerging Technologies (ICEET), pp. 1–7. IEEE (2018, February)
3. Foster, I., Castaneda, C., Nalley, K., Mannion, C., Bhattacharyya, P., Blake, P., Pecora, A., Suh, K.S.: Clinical decision support systems for improving diagnostic accuracy and achieving precision medicine. *J. Clin. Bioinform.* **5**(1), 4 (2015)
4. Zhang, P., White, J., Schmidt, D.C., Lenz, G., Rosenbloom, S.T.: FHIRChain: applying blockchain to securely and scalably share clinical data. *Comput. Struct. Biotechnol. J.* **16**, 267–278 (2018)
5. Downing, N.L., Adler-Milstein, J., Palma, J.P., Lane, S., Eisenberg, M., Sharp, C., Northern California HIE Collaborative and Longhurst, C.A.: Health information exchange policies of 11 diverse health systems and the associated impact on volume of exchange. *J. Am. Med. Inform. Assoc.* **24**(1), 113–122 (2017)
6. National Azaria, A., Ekblaw, A., Vieira, T., Lippman, A.: Medrec: Using blockchain for medical data access and permission management. In: 2016 2nd International Conference on Open and Big Data (OBD), pp. 25–30. IEEE (2016, August)
7. Zhang, J., Xue, N., Huang, X.: A secure system for pervasive social network-based healthcare. *Ieee Access* **4**, 9239–9250 (2016)
8. Kuo, T.T., Kim, H.E., Ohno-Machado, L.: Blockchain distributed ledger technologies for biomedical and health care applications. *J. Am. Med. Inform. Assoc.* **24**(6), 1211–1220 (2017)
9. Angraal, S., Krumholz, H.M., Schulz, W.L.: Blockchain technology: applications in health care. *Circul.: Cardiovasc. Qual. Outcomes* **10**(9), e003800 (2017)
10. Yue, X., Wang, H., Jin, D., Li, M., Jiang, W.: Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. *J. Med. Syst.* **40**(10), 218 (2016)
11. Griggs, K.N., Ossipova, O., Kohlios, C.P., Baccarini, A.N., Howson, E.A., Hayajneh, T.: Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *J. Med. Syst.* **42**(7), 130 (2018)
12. Ivan, D.: Moving toward a blockchain-based method for the secure storage of patient records. In: ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST, pp. 1–11 (2016, August)
13. Chen, Y., Ding, S., Xu, Z., Zheng, H., Yang, S.: Blockchain-based medical records secure storage and medical service framework. *J. Med. Syst.* **43**(1), 5 (2019)

14. Wang, S., Wang, J., Wang, X., Qiu, T., Yuan, Y., Ouyang, L., Guo, Y., Wang, F.Y.: Blockchain-powered parallel healthcare systems based on the ACP approach. *IEEE Trans. Comput. Soc. Syst.* **5**(4), 942–950 (2018)
15. Jiang, S., Cao, J., Wu, H., Yang, Y., Ma, M., He, J.: Blochie: a blockchain-based platform for healthcare information exchange. In: 2018 IEEE International Conference on Smart Computing (smartcomp), pp. 49–56. IEEE (2018, June)
16. Cyran, M.A.: Blockchain as a foundation for sharing healthcare data. *Blockchain Healthc. Today* **1**, 1–6 (2018)
17. Shubbar, S.: Ultrasound medical imaging systems using telemedicine and blockchain for remote monitoring of responses to neoadjuvant chemotherapy in women's breast cancer: concept and implementation. Doctoral dissertation, Kent State University (2017)
18. Ianculescu, M., Stanciu, A., Bica, O., Neagu, G.: Innovative, adapted online services that can support the active, healthy and independent living of ageing people. A case study. *Int. J. Econ. Manage. Syst.* **2** (2017)
19. Ekblaw, A., Azaria, A., Halama, J.D., Lippman, A.: A case study for blockchain in healthcare: "MedRec" prototype for electronic health records and medical research data. In: Proceedings of IEEE Open & Big Data Conference, vol. 13, p. 13 (2016, August)
20. Xia, Q.I., Sifah, E.B., Asamoah, K.O., Gao, J., Du, X., Guizani, M.: MeDShare: trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access* **5**, 14757–14767 (2017)
21. Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., Wang, F.: Secure and trustable electronic medical records sharing using blockchain. In: AMIA Annual Symposium Proceedings, vol. 2017, p. 650. American Medical Informatics Association (2017)
22. Mohapatra, S., Parija, S.: A brief overview of blockchain algorithm and its impact upon cloud-connected environment. *Bitcoin and Blockchain* 99–113 (2020)
23. Siyal, A.A., Junejo, A.Z., Zawish, M., Ahmed, K., Khalil, A., Soursou, G.: Applications of blockchain technology in medicine and healthcare: challenges and future perspectives. *Cryptography* **3**(1), 3 (2019)
24. Mohapatra, S., Parija, S.: A brief understanding of blockchain-based healthcare service model over a remotely cloud-connected environment. In: Evolutionary Computing and Mobile Sustainable Networks, pp. 949–955. Springer, Singapore

Chapter 10

Enabling Smart Education System Using Blockchain Technology



A. R. Sathya, Sandeep Kumar Panda, and Sudheer Hanumanthakari

Abstract Blockchain Technology is gaining lot of attention in recent days due to its distinct characteristics like decentralization, reliability, security and data integrity. Many companies are researching the possibility of adapting Blockchain Technology in their respective domains to utilize the potential of blockchain to the fullest. In spite of its rapid growth very little is known about the state of the art of blockchain in educational sector. The book keeping process of degrees and certificates can be one such potential area where blockchain can play a major role. This chapter presents the detailed analysis of Blockchain Technology and its application in education. Its emphases on (i) Blockchain Technology and its diversified application (ii) Digital Signatures and (iii) Blockchain based educational solutions. This chapter also highlights the challenges of blockchain in education based on an intensive research.

Keywords Blockchain applications · Blockchain in education · Decentralization · Digital signatures · Certificates · Book keeping

10.1 Background

Digital files could be as ephemeral as paper that vendors often issue to consumers in proprietary formats; the organizations can't read or validate the records without the necessary tools. In many cases the verification process can be slow and unpredictable even with access to the appropriate tools. The same applies to digital signatures: even where laws have required their adoption, digital signatures come in a broad range of formats with different security levels, most of which are not regarded as legal

A. R. Sathya (✉) · S. K. Panda · S. Hanumanthakari

IcfaiTech (Faculty of Science and Technology), ICFAI Foundation for Higher Education (Deemed to be University), Hyderabad, India

S. K. Panda

e-mail: sandeep@ifheindia.org

S. Hanumanthakari

e-mail: hsudheer@ifheindia.org

evidence. Another problem with digital documents is the way it was shared. One primary method is sharing them digitally via highly insecure email. Hence it is necessary to build proprietary transmitting infrastructures to send sensitive documents like certificates, health records, bank statements. On the other hand, other transmission methods create interoperability issues. Ultimately, as with paper documents, it is also possible to manipulate digital documents in ways that are hard to discover.

10.2 Introduction

Blockchain is a distributed ledger that allows us to record and share information across a distributed network. The information could be any digital transactions, contracts, digital assets, digital certificates and signatures or anything that are in digital form. Information in blockchain is permanent and transparent thereby allowing any nodes in the network to entirely view any transaction history. All transactions are compiled in blocks and every new update is added in a new block and is appended to the chain of blocks that already exist through cryptographic techniques. Whenever a transaction is initiated in a blockchain, the set of nodes in the network validates, distributes and records them on the public ledger. Each network node maintains a copy of this ledger. Blockchain replaces the need for intermediate third parties as every node in the network solves complex computations to maintain the integrity of the data. A typical blockchain transaction stores information like transaction number, transaction timestamp, sender and receiver information and the transaction asset.

Blockchain the technology behind Bitcoin came into limelight after the success of Bitcoin. As bitcoin becomes popular, a lot of researchers recognized the potential of the underlying technology. The distinct nature of Blockchain such as immutability, transparency and trustworthiness made it applicable to domains beyond Bitcoin. The development of blockchain is categorized as Blockchain 1.0, 2.0 and 3.0. Blockchain 1.0 focuses on cryptocurrencies and simple cash transactions and Smart Contracts were introduced in Blockchain 2.0. Whereas Blockchain 3.0 spotlights the application of Blockchain in various domains like Government, FinTech, Supply chain, Healthcare, Education and many more. Applications of Blockchain in different sectors are shown in Fig. 10.1.

10.3 Blockchain Application in Educational Sector

Education is ubiquitous. Blockchain provides solution to concerns related to privacy, security and vulnerability. A distributed blockchain based ecosystem was proposed in 2016 [1] using which the educational records can be stored. Using blockchain based solutions educationalists can store student's learning achievements, educational certificates, credit management etc. Any information related to an educational

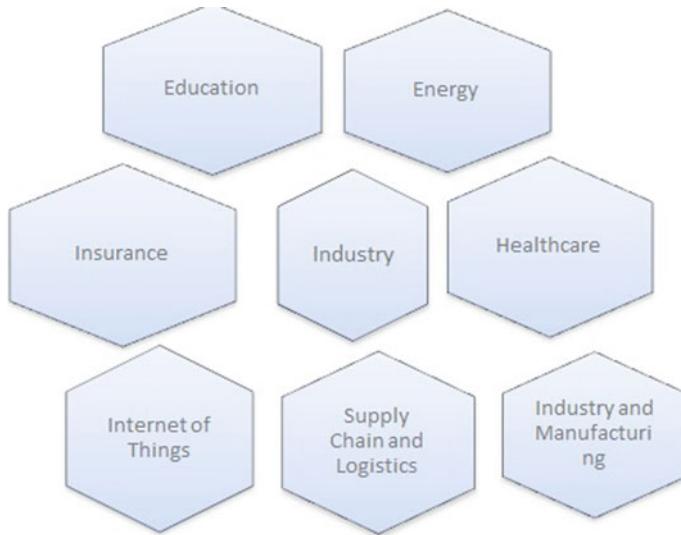


Fig. 10.1 Applications of blockchain technology

institute can be stored which can later be used for analysis and decision-making processes. To carry the research article publication in a timely manner blockchain can be adopted. Through this submission, reviewing and verification process can happen on time and even counterfeit of research articles can be avoided. The first institute to store academic certificates in blockchain is University of Nicosia [2]. Later, MIT Media Lab along with Learning Machine a software enterprise developed Blockcerts, an open source environment for creating, broadcasting and validating the blockchain based educational certificates. Smart contracts, asset transactions, digital signatures and certificates can generally be stored in blockchain with respect to education. Smart contracts are referred as a set of programs that will be executed automatically when certain conditions are met [3]. Whereas asset transactions are ownership evidence documents of any tangible or intangible assets. Certificates are proof of achievements and signatures are proofs that the certificate is issued from and to authorized persons. Some of the areas where blockchain can be adapted in educational sector is listed below [4, 5].

10.3.1 Secure Storage of Certificates

Majority of the educational institutes across the world issues certificates either in paper or digital format. Paper certificates are easy to store and recipients also find it easy to carry and show it to others for any purpose. However, the process of

issuing, verifying and maintaining these certificates are time-consuming and expensive process. However digital certificates acts as an alternative to paper certificates. Digital certificates use digital signature which requires an intermediate entity to issue and verify the certificates. In this case, the proofs of the certificates can completely be recorded in blockchain in a safe and secured way. Even if the institute that issues the certificate closes, the certificates will still be available in the blockchain. In case of digital certificates, the issuing institutes can use a public blockchain to keep the digital signature in blockchain.

10.3.2 Multi-step Verification

Regarding education, there is a lot of scope for fake degrees. Every education institute must be verified by an accreditation entity for verifying the quality of the institute that issues the certificate. In order to check whether a certificate has been issued by a genuine institute, an individual might verify with the concerned institute whether it really issued the certificate, Can check for the accreditations the organization owns, may check the quality of the accrediting body itself in private sector circumstances. This is very much time consuming and needs experts in managing the accreditation process. In this case, the accreditation body can put their digital signature in blockchain. By doing so, a multi-step verification can happen. That is, the student's certificate issued by authentic institute which is accredited by an authorized accreditation body.

10.3.3 Student's Credit Transfer

Instead of uploading the digital signature alone, if the certificate itself is uploaded in a blockchain, it will be stored permanently and immutable. There is no need for intermediate person to manage those certificates. The learners can provide the employer or higher educational institutes the access to view his/her profile, the complete educational history of the learner can be made visible and can be verified. In case of credit transfers, a smart contract can be written based on certain condition being fulfilled the credits can be automatically be transferred from one institute to the other.

10.3.4 Intellectual Property Tracking

Educators can use a blockchain to mark the publishing and documentation of free educational resources. This would require notary of the publication date for purposes of copyright and enable monitoring of the extent of re-use of any given property. The same is the case of journal articles. Tracking of journal citations is a costly process

and needs a third party to do the process. Through blockchain, we can avoid the third party and can allow anyone to publish articles and can track the citations without much access restriction the original articles. A rewarding system may also be introduced for the authors based on the amount of the resource re-used.

10.3.5 Fee Payment

A specific currency is used by students for their fee. Especially when they go outside their country many institutes accept payments digitally. Under these circumstances, the students can make payments through cryptocurrencies. In this case, both the student and the receiving organization should have a wallet to accommodate the cryptocurrency transaction.

10.4 Certification Process

Certificates are proof of statements issued from an authorized entity to another because of certain achievements made by the recipient are true. The key components of a certificate are the achievement—the fact for which the statement has been issued. For example, the student has completed a course successfully, the issuer—the authorized source who has verified and validated the achievements of the learner, the receiver—the learner who has achieved the fact mentioned by the issuer, the certificate—a document of proof that includes the achievement, the issuer, the receiver, and the evidence if there are any. Once the learner has received a certificate based on the blockchain it is possible to share it by the learner on demand.

10.4.1 Traditional Certification Process

Traditionally the certificate issuing process includes issuing, verifying and sharing of certificates. The issuing process includes the activities involved in including the certificate information like the issuer, learner, achievements, logos, signature, etc. this information usually will be stored in a central repository. The verification process involves a third party to check the authenticity of the certificate issued. This can be done in various ways like checking the in-built security features of the paper certificates or checking with the issuer itself asking about the details. Sharing means the receiver on receiving the certificates can share it with a third party via post or email or in-person in case of higher education or employment. The whole process needs a centralized system for storage or a trusted third party for verifying the certificates. It is time-consuming and needs lots of security mechanisms and regulations for issuing and verification process. However, digital certificates have certain advantages over

paper certificates like fewer resources needed for issuing, verifying, maintaining and using. But there are no proper global standards available for digital signatures. Also, it needs third-party verification for the digital signatures and digital certificates are easy to counterfeit without signatures.

10.4.2 Digital Signatures

A digital signature is not an electronic signature. Rather it is a cryptographic mechanism used to authenticate that a document is signed by a specific person. To digitally sign any document, one needs a pair of private and public keys and a timestamp and a hashing function. In blockchain SHA-256 hashing technique is being used. A public key is a publicly available id which is used to identify an entity. A private key is a secret key that is mathematically linked to the public key of the user. The framework of a digital signature is given in Fig. 10.2. The digital document is signed by combining the contents of the documents and the private key of the issuer and a timestamp. In case of blockchain it includes the sender's private key, receiver's public key, achievements of the receiver and a timestamp. A hashing function is applied on this data which produces a unique hash value which would be stored in the blockchain [6]. Any smallest change in the document also will result in a different hash and the integrity of the data can be maintained. However, since hashing used the signature cannot be reversed to identify the contents of the document or the issuer's private key.

The verification process of blockchain certificate that are digitally signed is shown in Fig. 10.3. The signatures can be verified by comparing the hash value of the digitally signed document and the hash value on blockchain matches. And the signature is cryptographically matching the public key of the issuer. Thus, the process doesn't

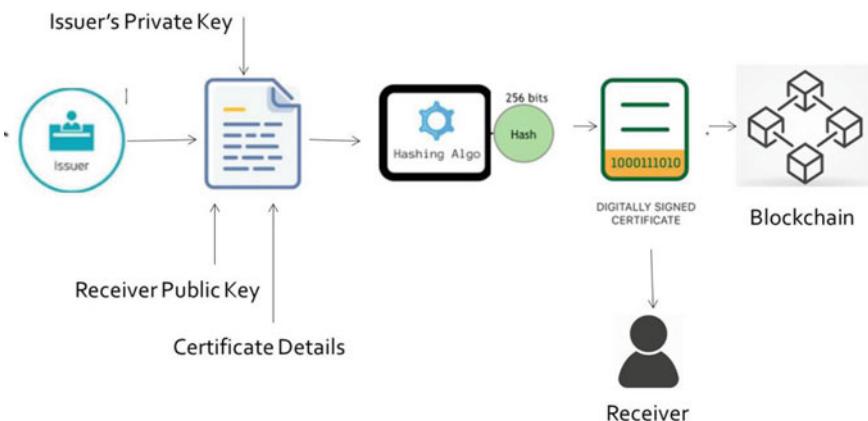


Fig. 10.2 Framework of digital signature on blockchain

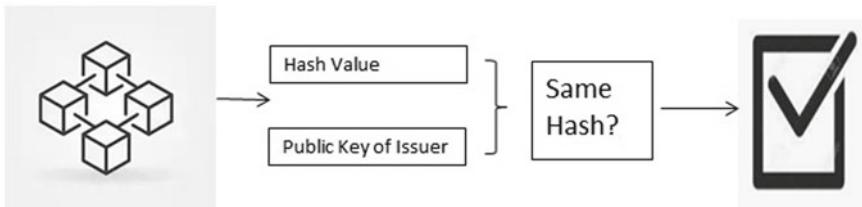


Fig. 10.3 Blockchain based digital signature verification process

need any private key to be revealed. The process of digital signature needs a public key infrastructure (PKI) which generally depends on third parties for generating public and private keys, to timestamp the documents and to verify the signature. But, in blockchain by design only all the above steps can be done and does not need a PKI for digital signatures.

10.5 Blockchain-Based Digital Certificates

Blockchain resolves the problems of paper and digital certificates and provides and infrastructure to access for verifying and sharing the certificates in a secured way. By using Hashing techniques, it keeps the document containing issuer, receiver and achievement details and whatever data need to be incorporated in the certificate in the blockchain which is spread across the network. Therefore, forging the certificates is almost impossible in the blockchain. Since the certificates are available over the network it is possible for anyone who has access to the blockchain thereby eliminating the need for third-party verification. Only the hash of the document is stored in the blockchain and not the document itself [7]. Therefore, the privacy of the user is maintained. Thus, the benefits of the receiver of this blockchain based digital certificates are data independence and ownership. Recipient has the control over the achievements and can share wherever he wants to share. At the same time the data record is permanent and cannot be destroyed. The workflow of blockchain based digital certificate is shown in Fig. 10.4. For commercialization few vendors like Learning Machine, Sony Global Education, Attore Solutions, Gradbase and Stampery are building innovative blockchain based certificated in market [8–10].

10.6 Benefits and Challenges in Approving Blockchain in Education

The significant advantages of having blockchain education can be more security, improved students' assessment, controlled data accessibility, transparency, low cost

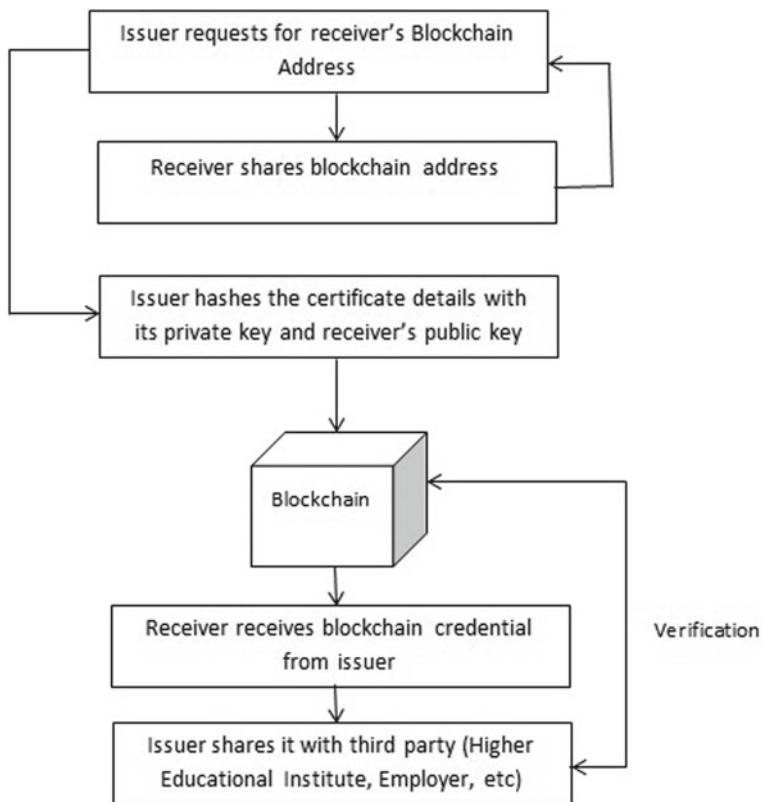


Fig. 10.4 Workflow of blockchain based digital certificates

transactions, identity authentication and many more. Reliability can be achieved by digital signatures and cryptographic hashes. Even though blockchain has great potential in education domain there are quite several challenges which cannot be ignored. Scalability the well-known issue of blockchain can be a challenge. Acceptance of any system based on sensitive records needs guidelines, standards and regulations. System interoperability is more vital in such case. Development of tools to support digital certificates is not fully shaped and needs proper meta-data standards for digital records. The need for open standards is mandatory, if we expect people to be able to carry and validate their data across the world as data transferability and operability is significant. As applications of blockchain are in its early stage without proper implementation illustrations it is difficult to make people understand the potential of blockchain technology. In cases where multiple institutes should agree to share their data, it might be difficult to make all institutes to agree to share their data. Presently, blockchain is in its evolutionary stage, so framing standards for digital certificates may not be easy and optimal. Blockchain has high storage cost and extremely high computational cost needed to process the cryptographic activities.

Even though only the hashes of the documents are stored in the blockchain it doesn't suffice the energy and storage constraints of blockchain. Adapting blockchain needs technical knowledge to use. Therefore, dependencies on third parties are unavoidable.

10.7 Conclusion

Despite having several benefits, many implementation models of blockchain are in pilot stage and an extensive research must be carried out to conclude the appropriateness of blockchain in education. Therefore, to attain the complete potential of blockchain in education a systematic and balanced approach is needed. In future, blockchain can bring the concept of digital certificates into mainstream.

References

1. Sharples, M., Domingue, J.: The blockchain and kudos: a distributed system for educational record, reputation and reward, pp. 490–496. Springer International Publishing, Cham (2016)
2. Sharples, M., et al.: Innovating pedagogy 2016: Open University innovation report 5 (2016)
3. Cheng, J.-C., Lee, N.-Y., Chi, C., Chen, Y.-H.: Blockchain and smart contract for digital certificate. In: Proceedings of the 2018 IEEE International Conference on Applied System Invention (ICASI), Chiba, Japan, 13–17 April 2018; pp. 1046–1051
4. Chen, G., Xu, B., Lu, M., Chen, N.-S.: Exploring blockchain technology and its potential applications for education. *Smart Learn. Environ.* **5**, 1 (2018)
5. Han, M., Li, Z., He, J.S., Wu, D., Xie, Y., Baba, A.: A novel blockchain-based education records verification solution. In: Proceedings of the 19th Annual SIG Conference on Information Technology Education, Fort Lauderdale, FL, USA, 3–6 Oct 2018, pp. 178–183
6. Palma, L.M., Vigil, M.A., Pereira, F.L., Martina, J.E.: Blockchain and smart contracts for higher education registry in Brazil. *Int. J. Netw. Manag.* **29**, e2061 (2019)
7. Jagers, C.: Blockchain-Based Records and Usability (2017). Available at: <https://medium.com/learning-machine-blog/Blockchain-based-records-and-usability-179a4eeaeb6e>
8. Shrier, D., Wu, W., Pentland, A.: MIT Blockchain & Infrastructure (Identity, Data Security) (2016). Available at: https://cdn.www.getsmarter.com/career-advice/wp-content/uploads/2016/12/mit_Blockchain_and_infrastructure_report.pdf
9. Credentials, Reputation, and the Blockchain. Available at: <http://er.educause.edu/articles/2017/4/credentials-reputation-and-the-Blockchain>
10. Arenas, R., Fernandez, P.: CredenceLedger: a permissioned blockchain for verifiable academic credentials. In: Proceedings of the 2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), Stuttgart, Germany, 17–20 June 2018, pp. 1–6

Chapter 11

Blockchain Technology in Smart-Cities



**P. Chinnasamy, C. Vinothini, S. Arun Kumar, A. Allwyn Sundarraj,
S. V. Annlin Jeba, and V. Praveena**

Abstract With the fast pace of population, intelligent city wants effective and sustainable smart solutions in transport, climate, energy, and government affairs. Amongst the most sensible solutions is the smart city platform which includes IoT, Big Data and the Internet of Energy. It faces many issues, including such inadequate IoT security, trouble maintaining and improving efficiency, higher operating expenses of large amounts of data center construction, good permeability to damage, difficulty building confidence in electricity internet users, quick leakage of consumer privacy and a business model which is not acceptable etc. Blockchain is one of today's most disruptive technologies. As part of the overall efforts to shape the urban future, numerous cities around the world are launching blockchain initiatives. With a range of potential advantages, digital transformation poses many key issues like data security and confidentiality. This study proposed a security architecture which utilizes the blockchain-based with smart devices and provide a secure communication system in an intelligent city.

Keywords Smart device · Blockchain · Bitcoin · Secure communication · Intelligent city · Consensus · Smart contract

P. Chinnasamy (✉)

Department of Information Technology, Sri Shakthi Institute of Engineering and Technology, Coimbatore, India

C. Vinothini · V. Praveena

Department of Computer Science and Engineering, Dr.N.G.P. Institute of Technology, Coimbatore, India

S. Arun Kumar

Department of Computer Science and Engineering, Sikkim Manipal Institute of Technology, Sikkim Manipal University, Majitar, East Sikkim, Sikkim, India

A. Allwyn Sundarraj

Department of Food Technology, Sri Shakthi Institute of Engineering and Technology, Coimbatore, India

S. V. Annlin Jeba

Sri Buddha College of Engineering, Padanilam, Kerala, India

11.1 Introduction

The last few centuries can see a stratospheric increase in the world's population residing in metropolitan areas. Upwards of 55% of the total population currently living in cities, and this proportion is estimated to hit 70% within next three decades, like an unprecedented 25 million people in the world are projected to transport to the cities in 2050 [1]. Due to destructive increasing population, the eco system and economic issue emerge both at the technological and institutional levels. The number of enterprises are also strongly involved in implementing the 'intelligent' principles for optimizing use of both physical and transitory assets. In this aspect, it is suggested that idea of "Smart City" using new information and communications technologies (ICT) in an articulate way focused at creating a healthy pedestrian areas and enhancing the QoL. In industrialized democracies, the smart city appears to have a broad range of uses including smart devices to monitor surface temperatures and lighting systems, smart electric power management, enhance healthcare use, stimulate the educational systems through advanced technology, and strengthen the digital money exchange through smart governance structure.

Unlike conventional approaches, blockchain technology (which was initially created for digital currency) enables peer-free transfer and exchange currencies. Bitcoin has seen a tremendous increase in the financial sector since Satoshi Nakamoto was founded in 2009 [2]. Blockchain is a distributed ledger, freely accessible and irreversible digital ledger that pioneered how members regulate payment, communicate, register and monitor transactions while removing the use of a central body to handle operations altogether [2]. The information gathered by the smart sensors devices was stored in traditional systems in a central database for future smart city study. These central servers are vulnerable to many threats, including the leakage of sensitive data collection due to use of unsecured server as well as the need for more than one management authority [3]. This underlines the need for a new approach to establish efficient architecture for data storage and processing in a decentralized fashion. In this situation, blockchain seems to be the only opportunity to connect with a decentralized peer-to-peer network, exchanging data and resources.

To the best of authors' knowledge, however, there have not been any recent studies discussing the issues of security and privacy in smart cities. This study presents the governor-of-the-art blockchain technology for resolving the privacy concerns of smart cities. The contributions are as follows

1. This research presents state-of-the-art blockchain technologies such as blockchain architectures, consensus processes, implementations, trade-offs and problems.
2. This study concentrates more on analysis to implement blockchain technologies to enhance smart cities' effectiveness, secure, and sustainability.
3. This study examines the usefulness of blockchain in different smart societies, including healthcare, transport, supply chain management, and accounting systems.

The substance of the article is structured as follows: Sect. 11.2 addresses the history and functionality of blockchains. In Sect. 11.3, various features of a smart city are addressed. Section 11.4 sheds light on the reasons for applying emerging technology to smart cities. Section 11.5 explores new blockchain developments in the various implementations of smart cities. Section 11.6 discusses future problems and study questions, finally concluded in Sect. 11.7.

11.2 Groundwork of Blockchain and Its Architecture

In simple terms, blockchain is a rapidly growing block chain designed to store all the accumulated activities with the aid of a shared database in which all interactions are cryptographically validated and authorized by all miners. In this section, the detailed description of blockchain structure, various types, and different consensus mechanisms.

11.2.1 Block Structure

Analogous to a distributed ledger, blockchain is a series of nodes that collect data about all transactions and are connected together through the previous block. Every block header contains a hash, authenticated proof of transactions, and hash values of preceding block. The block structure must have the following information as shown in Fig. 11.1,

1. **Hash:** A hash value is something which accepts any long messages as input and returns distinctly fixed sized text as output. Unless the input is changed, then there is a complete change in the output. Through blockchain technology hash functions are used everywhere. A person called Alice, for examples, attempts to create and modify the structure contained in a block. When changed, ensures that the changed blocks contains a completely new hash value, ensuring that each nodes or miner in the system will ensure the visibility of the change by refreshing all users' blockchain copies [4].
2. **Merkle Tree:** Growing node is expressed as a leaf in a hash tree or Merkle tree, and is highlighted with a marker. This Merkle tree permits the system to securely and efficiently manage the huge data repositories [4].
3. **Timestamp:** Using that, we could monitor any document's creation or alteration time in a secured manner [4].
4. **Nonce:** A nonce value is practically a 32 bit value looking directly at 0 and increased every time hash computation is done [4].
5. **Previous Block:** A sha-256 hash which points to the previous block header [4].

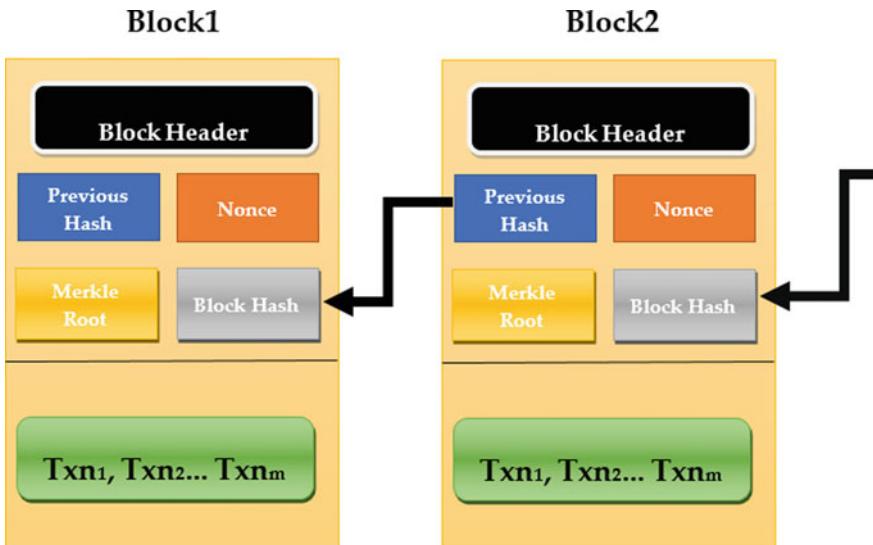


Fig. 11.1 Skelton of block header

11.2.2 Blockchain Types

Blockchain strategies have been widely divided into three groups based on influence and authorization mechanisms, which include public, private and consortium blockchain. Similar forms are listed as following as shown in Fig. 11.2 and detailed summary are listed out in Table 11.1.

1. **Public Blockchain (Permissionless):** Anyone with an internet access will engage in reading, writing or internal audit activities in this blockchain [4]. Decision-making in this form happens with the aid of various distributed consensus mechanisms such as PoW and PoS. The Bitcoin, Ethereum, and Litecoin are examples of public blockchains.

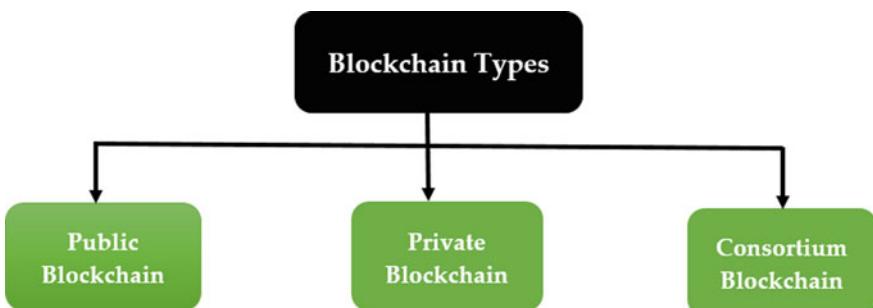


Fig. 11.2 Classification of blockchain

Table 11.1 Blockchain types

Services	Public	Private	Consortium
Nature	Federated and secure	Governed and filtered	Governed and filtered
Consensus methods	PoW, PoS, DPoS	PBFT, RAFT	PBFT
Transaction processing	Time-consuming	Moderate	Tiny
Categories of participant	Robust and unverified	Confidential and discovered	Confidential and discovered
Approvals	Permission less	Permissioned	Permissioned
Limpidity	Low-slung	Great	Great
Utilization of energy	Extraordinary	Low-slung	Low-slung
Scalability	Extraordinary	Extraordinary	Low
Illustration	Bitcoin, Litecoin, Ethereum, and Block-stream	Bankchain, R3	Hyperledger, Multichain, and Blockstack

2. **Private Blockchain (Permission):** The applicant can still participate in this form upon receiving the approval from its system administrator [4]. Bankchain, R3 would be an illustration of private blockchain.
3. **Consortium or Federated Blockchain:** It is a hybrid of private and public blockchain, through which a number of entities feel responsible for approval and cryptocurrency enforcement. Blocks in these networks are mined using a multisignature strategy and the miner objects are still only considered necessary if accepted and authorized by the regulating. Types of consortium blockchain systems include Hyperledger, Blockstack and R3CEV.

11.2.3 Consensus Algorithm

A consensus is a method for achieving a collective bargaining agreement on a multi-Objective network, hierarchical or decentralized [4]. It is really significant for the machine which passes the message. Assuming a possibility for commanders to invade the city, whom has surrounded the city with some kind of portion of a Byzantine Army. In this case, a few of the leading commanders supported the possibility of destroying the city whereas the other commanders favored the withdrawal decision as in Fig. 11.3. However, when only a portion of the commanders invade the city, the invade would really be ineffective [4]. In a propagated setting such ineffective attempt results in consensus.

1. **Proof of Work (PoW):** The consumer publishes the new block throughout this proof of work, by first solving the mathematical problem. Several mathematical procedures have to be performed to test the user or node when resolving the problem. Although it is hard to solve the puzzle in PoW to confirm that even a

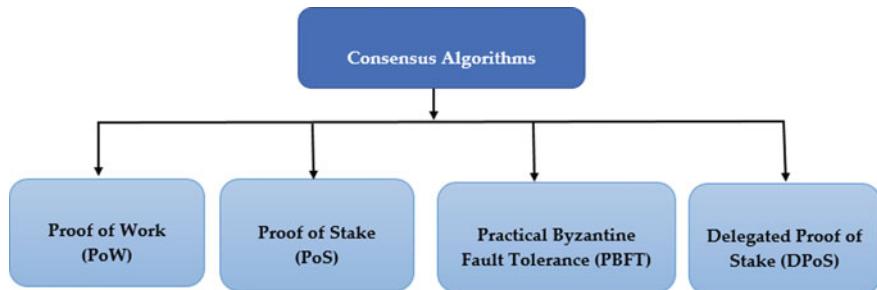


Fig. 11.3 Mechanisms for consensus

method is legitimate [4]. Following the resolution of the PoW puzzle the frame will be telecast to other endpoints as seen in Fig. 11.4. Types of PoW are the bitcoin, ethereum.

2. **Proof of Stake (PoS):** In PoS the transaction validity is verified determined by the amount of cryptocurrencies that the consumer owns. Ultimately the new terrain transactions or blockchain should be checked meaning that the sum would be granted through reward otherwise it would be confiscated. It needs low processing power similar to POW processes. Types of PoS are indeed the Ethereum, Casper, Krypton.

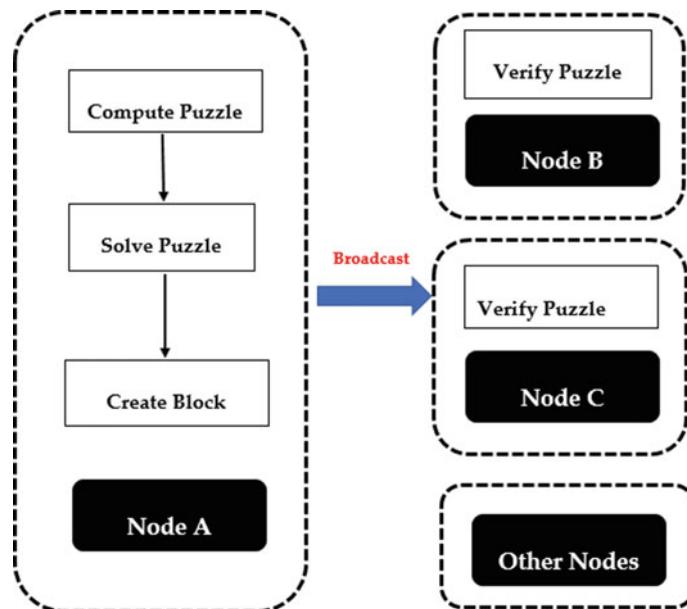


Fig. 11.4 Consensus mechanisms for PoW

3. **Practical Byzantine Fault Tolerance (PBFT):** It is just an algorithms for exaggeration generated to recognize byzantine faults. PBFT manages up to 1/3 of byzantine fraudulent reproductions. The whole process is classified into three main parts, including pre-preparation, preparation and committing. Also the node is allowed into another step after collecting 2/3 of the ballots from many of the nodes in the system. The evaluation of the transaction is conducted on the basis of 3 phases. In the first phase, distributed a predicting block. In the phase 2 a block or transaction is precommitted. Legitimizes a block or transaction in the third phase and transmits the contribute for that too [4].
4. **Delegated Proof of Stake (DPoS):** It is just like the PoS specification, which aims to achieve a global consensus in a blockchain network [4]. The biggest example of DPoS include the Bitshares, Steem, Cardano, and EOS.
5. **Proof of Authority (PoA):** Authoring nodes on cryptocurrency networks, users can demonstrate and verify their identity. Then it's only appropriate to approved strong confidence blockchain [4]. Sources for PoA include the Ethereum, Kovan testnet, POA Chain.
6. **Proof of Elapsed Time Consensus (PoET):** The key ultimate goal is to create a prototype that is somewhat analytical than PoW, with strong safety assurances. The new block that is released depended on spontaneous queue length from a stable infrastructure [4, 5]. Illustration for PoET was its Hyperledger Sawtooth.
7. **Raft:** Raft [6] is a consensus-based voting mechanism suggested to render the Paxos process more realistic situations achievable and recognizable. The initial Paxos methodology attempts to solve the problems of accuracy relevant to the generalized byzantine problem. Both Paxos and Raft gain comparable performance and are algorithms insensitive to pre-Byzantine faults. Raft depends on two main activities, such as the collection of members and the duplication of logs. The leader controls the organizing of transfers and the new candidate is chosen using periodic timeout in case the original manager loses.
8. **Ripple:** Ripple [7] is an open-source payments application that provides use through publicly authorized, large-scale network segments. Ripple seeks to regulate and control the roles of payments, currency trading and clearance. The network elements are categorized as: a client exchanging money, and a server participating in consensus protocols. The client makes transactions inside the system, and the verifying clients or monitoring clients relay them to the entire system. Such verifying domains are necessary to respond to the application for register from the recipient and also some transmitting financial data.

11.2.4 Architecture of Blockchain

Blockchain works in a decentralized network that is backed by many technological innovations include distributed consensus protocol, computational hash, and digital certificates. The blockchain architecture generally consists of the following

6 components as shown in Fig. 11.5. A complete explanation of all these levels and their process is performed throughout the sub-chapter below.

1. **Data Layer:** This layer handle the various information acquired from different sources [8–11]. This module is primarily responsible for encapsulating the time-scribbled information blocks. In the block body, authenticated messages are stored whereas the genesis block contains the current description of the block, time, Nonce, Merkle root and hash. The new block contains past block hash (parent block) to link to its preceding block. The time-stamp shows the block's formation date. The two crucial elements for block chain are time stamp and Merkle tree in this layer. Time stamp allows the blockchain data to be placed correctly and traceably. This could also include time-dimensioned blockchain data to allow the recurrence of previous data histories. The Merkle tree will preserve the transactions within this given period of time using a binary hash tree to authenticate the integrity and presence of such activities effectively.

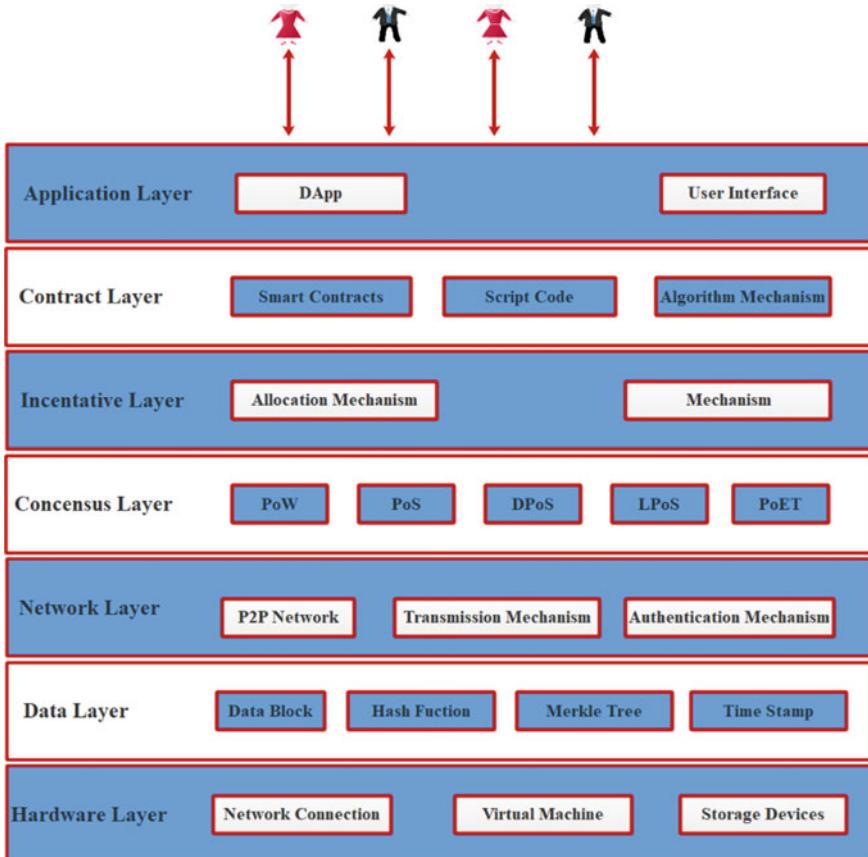


Fig. 11.5 The architecture of blockchain

2. **Network Layer:** The architecture's center stratum is recognized as the network layer. This is also occasionally defined as the Point-to-Point component (P2P). It is responsible for the interaction between the internodes. It is also responsible for discovering nodes, transactions, and block perpetuation and integrations to establish the authenticity of the current state in the system of blockchains [8–11].
3. **Consensus Layer:** It is the main body of the system of blockchains. It tackles different consensus mechanism. A consensus mechanism is cohort mechanisms that synchronize between communicating entities and force people to reach a common contract, also widely acknowledged as unanimous agreement, on the current transaction data status in a cloud environments [4, 11]. For strongest base station of many communicating entities, a conventional wisdom algorithm is used to generate the cryptographic keys. Consensus mechanism have three main components: safety/coherence, liveliness/affordability and sensitivity to faults. The different types of consensus protocol is clearly shown in Fig. 11.3.
4. **Incentive Layer:** The incentive module's fundamental purpose is to inspire modules for ability to contribute in blockchain data security validation. Every other module in the public ledger is evaluated by a mining operation using complicated mathematical processes, called consensus computations on the consensus layer. A node consumes its computational power and electricity even during authentication process. Blockchain incentivizes the expected to participate node or nodes with a digital currency based on as cryptographic techniques to encourage them to take aspect in the verification process. The component incorporates 2 methods for such a reward in a procedure called as assemble and launch mechanism [8–11].
5. **Contract Layer:** It is responsible for monitoring commercial logic-based transaction inquiries. It incurs the contract elements, such as scripting script, system of algorithms, logical contract, etc. A consensus mechanism is a conglomeration of corporate rules and procedures in the form of technology programs, wherein the system devices in the ethereum blockchain activate once predefined terms of the agreement are achieved. Smart contracts generally compiled just use a syntax of high standard like ethereum platform (EVM), solidity, etc. As well defined as the modelling interface is the contract layer [10, 11]. The contract layer could well struggle from different types of attacks, including a threat on reentrancy, access control, assault on structural rigidity growth, etc.
6. **Application Layer:** It enables the customer with a functionality via an application programme. The app and so it could can be enforced in any computer language and it can be implemented across a number of platforms. Safety of application level is among the most challenging issues of the block chain [4, 8–10]. It can suffered from security breaches to an exchange server, DDoS transfer, host protection for workers, malicious codes infection, faint password attack, selfish mining attack, etc.

11.3 Smart City: Features, Stone Walls and Regulatory Standards

Smart City relates to the notion of a synchronized application of all accessible resources and services to formulate and implement, liveable and environmentally friendly urban center. All the well-known smart city technologies in western cultures encompass smart energy to optimize energy usage; smart building equipped of independently controlling power usage, ventilation and protection across the board; smart technology to enable cutting-edge methodological choice and smart city networking capabilities; smart maneuverability to license innovation initiatives; Smarter healthcare to allow interconnected medicinal products and smart systems to enhance diagnostic testing, patient monitoring and healthy lifestyle; intelligent protection to mitigate privacy issues to prevent breaches, assets and even people; and smart governance to provide government digital services and programs; Building a smart city to save highly valued efforts and money requires a certain level of internet connectivity which could lead to security flaws to security [11, 12]. This problem has been exacerbated by connected systems that capture information from diverse sources and migrate it to a centralized backup system. It also enhance the texture of the assaults by constructing an adversary access point which facilitates their encroachment. These assailants will weaken the efficiency of smart applications by initiating a large range of threats including certain unauthorized access, embedded scripting Language, Denial of Service (DoS), snooping and hashing assault [13].

11.3.1 *Features of Smart Cities*

A smart city is built on asset condition include conservation, cleverness, industrialization and social functioning (Life Quality). Conservation is the first mode of thought in industrial growth and the introduction of smart cities is really the result of widespread conservation recognition. In [12], emphasized a need to preserve smart urban sustainable growth through the protection of energy technologies and cultural resources. A city's right to conduct its activities and maintain natural ecosystems in most all services is recognized as sustainable. The willingness to boost the city's collective social, economic and environmental metrics is called cleverness. Enhancement in QoL is an indicator of residential resident's economic and personal quality of life-being. The transportation infrastructure, cultural, technical and regulating investigation report in urbanization transition are defined as urban expansion. Figure 11.6 shows interconnectedness and interrelatedness of all these attributes.

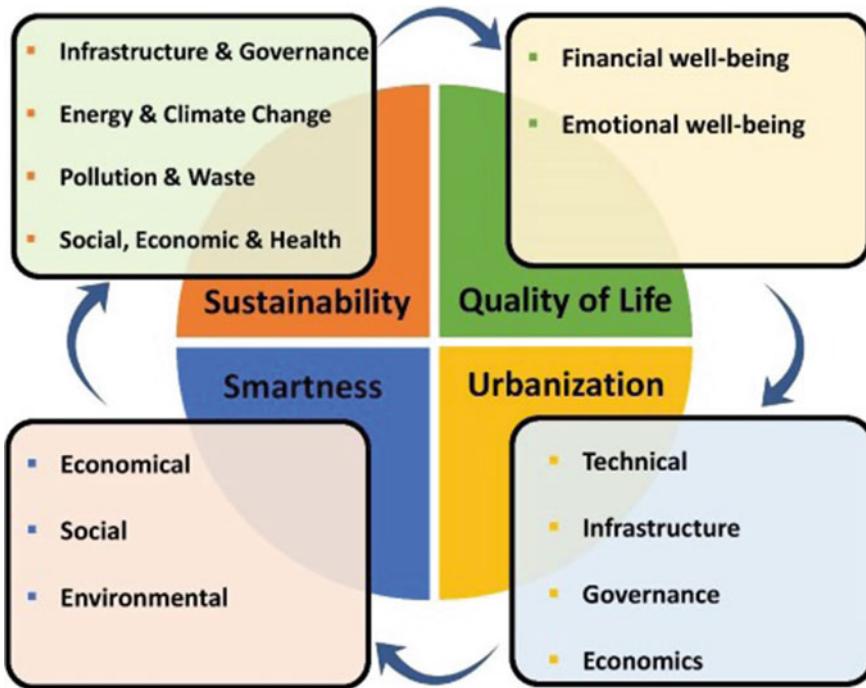


Fig. 11.6 Features of smart cities

11.3.2 Pillars of Smart Cities

It's often thought that smart city is focused on 4 philosophies/key elements, including physical, institutional, social and economic infrastructures. The principal obligation of these elements is shown in Fig. 11.7 and described as follows.

1. The physical infrastructure involves ensuring sustainable growth of the resource and perfect operational processes in the city. It consists of the fabricated transportation system and environmental assets. With the aid of an efficiency IoT device network and Infrastructure facilities, Smart City is recognized. The physical infrastructure also includes smart technology, construction upgrades, sustainable urban design and intelligent architecture [14].
2. The institutional infrastructure focuses on improving smart city democratic accountability through participation in decision-making, based rehabilitation, consistent management and social service providers. Gaining greatest benefit from the intellectual resources and working with the civilians for convenient system of government and also improving the city is crucial. The operational framework works with both the national and regional authorities to optimize the smart city's value. In addition to provide enough requisite coordination and

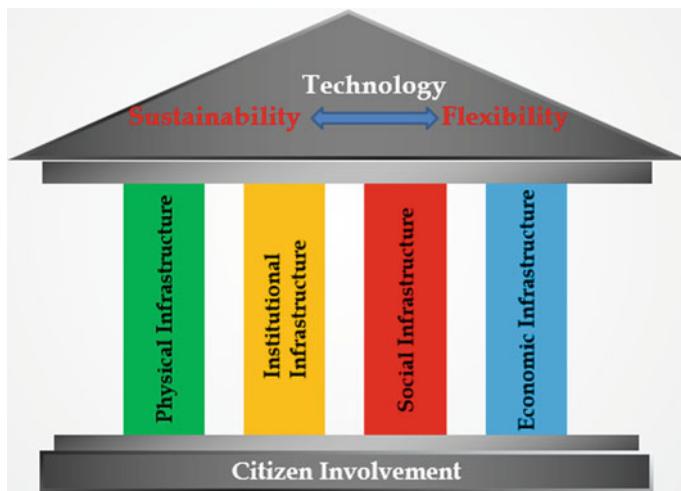


Fig. 11.7 The pillars of smart cities

- collaboration through institutions, it incorporates regional, political, public, and commercial institutions [14].
3. Social infrastructure consisted mainly of living organism, QoL and technical expertise. In a smart city, societal development tends to preserve competitiveness as citizens' awareness, visibility and dedication relate to popularizing the idea of smart city [14].
 4. The economic infrastructure pertains to the fairly consistent strength of the economy and job opportunities in order to increase the performance of the city by using e-business and e-commerce methodologies [14].

11.4 Smart Cities Security Requirements

In almost some area of our real experiences, ICT has played a crucial role, from learning, family and wellness existence to domestic security. Many federal agencies have implemented smart city initiatives to handle healthcare, water, electricity, transport, security and stability aspects. In order to facilitate our lives, the smart cities also pose many security threats due to growing interdependence, networking and sophistication between themselves. A good understanding of the determinants is of extreme significance for the successful implementation of the smart city. In this chapter, we're discussing the most influential criteria that really need to be addressed to create a safe smart city [15].

11.4.1 Communication Security

Smart city architectures depend completely on communication protocols to combine multiple elements to take advantage, share and disseminate information thru the smart city. Protecting all wired and wireless connectivity in a smart world ensures that basic safety standards including privacy, honesty, authenticity and integrity be guaranteed [3, 15]. Mahmood et al. [16] presented a modified streamlined shared trust model focused on encryption techniques directed at evaluating the costs of communications and productivity thereby suffering consequences in key enabling technologies. Alternatively, Lara et al. [17] suggested a flexible remote user authentication system ideal for Named Data Networking (NDN) projects providing IoT services through in-network persistence, state-of-the-art routing and integrated heterogeneous distributed verification.

11.4.2 Secure Management of Data

Data collection technique is an important prerequisite for any program committed to the identification and analysis of unauthorized activities. IoT devices which gather and transmit data are susceptible to malware such as intrusion of inaccurate or false data sources. To react to a dubious behavior or an assault, the framework must anticipate eradication or reaction techniques. In dissolution plan, the framework must effectively eradicate or involuntarily segregate the affected parts of the sensor node while the communication plan recognizes the resilience to be countered by a structured incident management procedure. This surveillance control system was first developed by Cisco [18] and offered security protection guidance using the principle of disaster recovery. The acceptability of the research proposal is indeed restricted to network devices from Cisco [17, 19].

11.4.3 Authentication and Access Control

It is important for IoT systems to monitor and manage the data created by the sensor nodes while at the same time detecting unauthorized access. Smart cities had to be possible to deter illegal entry by retaining secure user access, building encrypted connection and IoT systems authentication. A few other access control and authorization mechanisms including Identity Based Encryption (IBE) [19–21], Role-Based Access Control (RBAC) [19–21], and Attribute Based Encryption (ABE) [19–21] have been developed to ensure data protection in cloud-enabled smart cities. The above protocols help smart cities manage the legitimate access and withdraw their authorization privileges as well.

11.4.4 Application Security

In a traditional smart city, different approaches ought to be leveraged concurrently to recognize security vulnerabilities and ensure security toward possible attacks that could be initiated in an intelligent city. Many current systems could be used to protect apps for IoT devices. For example, it is possible to maintain the privacy of mobile apps by protecting the cellphone's IMEI, MEID, and Unique Device Identifier (UDI). Besides this, current cryptographic algorithms and data security strategies can be used to safeguard the network connectivity, thus enabling safe data transmission between various elements of smart cities.

11.5 Blockchain in Smart Cities

There are comprehensive Smart City major ingredients, like smart healthcare, supply chain management etc. This should offer the opportunity to gain insight towards how blockchains would be implemented in the smart city environment.

11.5.1 Healthcare Using Smart Devices

A traditional health-care system represents a range of hospitals purchased, operated and funded by a centralized authority. Yet, one single point of failure is susceptible to all these tightly regulated healthcare services. In fact, satisfying citizens' expectation is a daunting challenge for conventional healthcare schemes attributable to the increasing urbanization. The inconsistency between some of the constrained capacity with the ever-growing demand shows a need for reliable, informed and affordable healthcare. Blockchain is the famous approach to deliver the significant level of democratization in healthcare services and thus improve their defense.

Realizing smart healthcare dependent on a variety of subsystems, including smart patient transport systems, smart clinics, smart watches and emergency service. The exchange of resources by the physician is quite crucial for efficient medication, as it can allow researchers justify making real-time decisions about the treatment of people by assessing their situations sometimes in distant communities.

The processing steps in using blockchain to protect health care systems are shown in Fig. 11.8 and explained below

1. IoT devices gather and track medical patient information including systolic pressure, glucose level, heartbeat, blood pressure, temperature, etc.
2. The managers track the information recorded and produce reports for the patients.
3. The obtained review will be conducted by the physicians, who often prescribe the treatment needed.

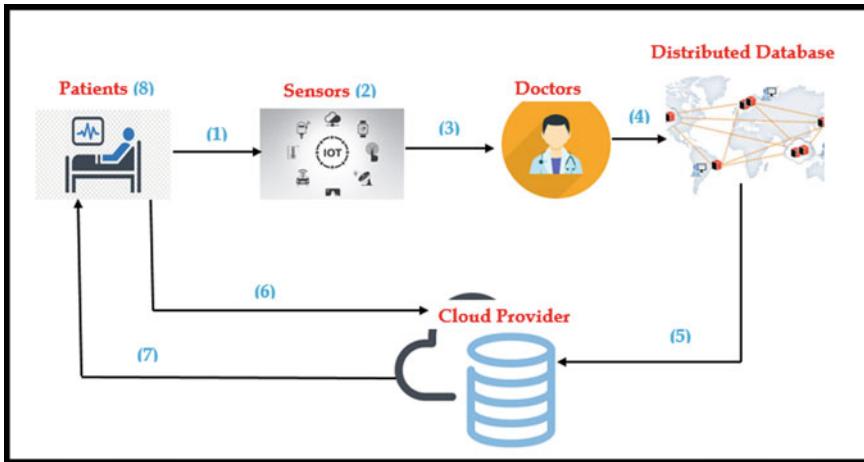


Fig. 11.8 Securing healthcare system using blockchain

4. Doctors can opt to use central database to exchange the care documents for more review.
5. It shares the authenticated documentation in encoded file.
6. Patients are demanding access to medical records history from the cloud service provider (CSP).
7. Upon positive confirmation, the patient receives the encrypted message of the medical record.
8. To access the actual care report, patients decode the downloaded encrypted message to use their own secret key.

11.5.2 Smart Transportation

In recent years, smart transportation often gained widespread popularity primarily due to the advent of ICT. It helps to strengthen pedestrian safety for cars, increase transport quality or provide comfort for both customers and drivers alike. Blockchain technologies can enhance knowledge exchange, promote vehicle performance and improve network lifetime reliability. In addition, blockchain strengthens the transportation industry by creating shorter turnaround times, quicker security checks, inspections and data management. In [22] proposed that blockchain technology could manage privacy and security concerns relating to the intelligent vehicles (ITS) appropriately. The subsequent paper summarizes research activities on intelligent transportation approaches focused on blockchain.

Electric Vehicles (EVs) over the recent decades, EVs gradually received more popularity because the need for sustainable transportation networks to be built in several nations. EVs are powered by a rechargeable, and have a communications

system that enables the exchange of knowledge between various elements. They will need reimburse the battery systems, which are conveniently hidden in metropolitan centers, a certain quantity of funds to guarantee regular fast charging of such EVs. Smart contracts and blockchain technology allow the exchange of such energy among fast chargers and EVs.

In [22], created a four-stage mechanism for Electric vehicles (excavation, selling, examination and trying to charge) that allows for automatic, privacy-conserving and efficient distribution of charging points based on cost and proximity to the EV. In [23] suggested Blockchain-based consortium to strengthen electricity vehicles distribution. The electrical transaction data is registered by a mutual ledger and an incremental multiple intervention technique is followed to maximize the electricity rates and the volume of resources exchanged. Likewise, in [23] suggested a blockchain technology and Smart Contract (LNSC) that could be commonly adopted with previous methods to secure exchange among charged stacks and EVs. In [24, 25] proposed a two-stage protection system throughout the Internet of Vehicles (IoV) to defensive towards polling competition among electors.

11.5.3 Vehicular Adhoc NETworks (VANETs)

VANET is amongst the most advanced technologies in which automobiles can interact even without any centralized authority being associated with the borderline device. Fortunately, the competitors may insert inaccurate and misleading details in an independent system in order to obtain private gain.

Yang et al. [26] suggested a trust monitoring system focused on blockchain for the VANETs. Originally each vehicles scores the neighboring vehicle and accesses the ranking to the nearby vehicles (RSUs). Then-RSU measures the develop practices of such devices and uses PoS and PoW consensus procedures to combine together it into block. Li et al. [27] introduced a blockchain based announcement of network, which confirmed the announcement. Luo et al. [28] introduced a blockchain based on mutual respect that allowed the VANETs privacy protection scheme. Markov random distribution-based trust evaluation framework is structured throughout this function in just such a way that either the founder-operator or the recipient can comply mostly with the authorized vehicle. The truthfulness of the vehicle is documented on a chain which is accessible to the public however any vehicles could obtain counterparty transaction records.

11.5.4 Smart Grid

Most of nationwide generated power is extracted through coal and oil. Given that over-use of natural gas will translate to increased levels of carbon dioxide and environmental destruction, sustainable energy needs to be used. With emergence of energy

generation technology, users appear to be wealthy by producing and supplying their extra energy from several other renewable sources. P2P based power exchanging is an important viewpoint in smart grid whereby consumers and providers share electricity. As electronic transactions are recorded throughout this phase of energy markets, various security schemes have been suggested to safeguard similar activities and to preserve the identification of the clients. Smart grid is recommended in this respect, providing a stable, efficient, effective and productive national grid system. Besides supporting the creation of a distributed electric grid that is secure, efficient and confident. The Decentralized framework also enhances the data protection and reliability of such systems [29].

11.5.5 Supply Chain Management (SCM)

A supply chain [30] is constituted by a group of objects including the firms and people instantly relating to the distribution of services, information, and ingredients between origin and suppliers. All these complicated supply chains had already permitted various types of products to be manufactured and sold around the world, however the organizations in those chain system also have constrained information about product development cycle. Fortunately, sufficient commodity knowledge is vital as customers need such ways to enhance overall trust, and companies need such data to make financial decisions or forecast industry trends. Thus, the prime element in chain management is data exchange that could be accomplished through the latest developments in blockchains [31, 32].

11.5.6 Financial Systems

A traditional banking process is driven by consumer, creditor, lender and borrower exchanging of money. Hence protecting the consumer's privacy and ensuring transaction data protection are the two most significant challenges. To this extent, blockchain is the right approach suggested to guarantee secure control of transactions inside a banking sector. In [33] suggested a payment processing Management monitoring system that would store all transaction records into the cloud. In [34] introduced a decentralized platform named Corda devoted to documenting and managing the significant contributing.

11.6 Open Research Issues

The technique of smart city is already emerging, as well as the sophistication and responsiveness characteristics of smart city systems that rely on blockchain

makes this an incredibly dynamic and fast-moving field. Consequently, several major research issues ought to be tackled mostly in coming years before its successful integration. The rest of this section addresses numerous problems and potential trends as part of the research.

11.6.1 Confidentiality and Integrity

The smart city is full of a multitude of sensor networks. For security solutions, therefore, it becomes important to concentrate on a defense mechanism instead of delivering appropriate defenses. Consequently, clear guarantees of security and complex strategies to protection becomes essential to a smart city [32, 35, 36]. The security and privacy is the huge challenge in smart city systems. In a block chain, the primary cause of security issues would be that consumers of these networks become entirely anonymous instead of fully identifiable. The transactions are generally accessible and open to those user groups, due to the greater transparency of cryptocurrency. This may result in user behaviors being tracked and members' real-world identities exposed. These records may be used to facilitate the sharing information. Thus, real privacy must be assured.

11.6.2 Secure Storage

Maintaining and processing such details is an objectives to accomplish, pertaining to the exponential rise in the quantity of data produced by recent technologies. Numerous studies have classified cloud storage as a most suitable method throughout this aspect because cloud service providers has massive data storage and computational resources [32, 37, 38]. Fortunately, in key enabling technologies, maintaining data into the cloud is insecure and unsustainable, as exporting services to the cloud storage may induce significant delays or maybe even violate integrity of the data. In addition, the cloud service providers' fraudulent actions or untrusted behavior making it important for a data owner to check the credibility of an outsourced data. Towards this extent, it introduced multiple distributed cloud storage mechanisms. Such strategies are susceptible to single point failure and malicious attacks, conversely. Blockchain highly centralized storage solutions were suggested to solve those problems.

11.6.3 Energy Efficiency

Energy efficiency plays a very important role because of the increasingly growing energy bills in smart cities. Numerous consensus techniques like PoW are computationally efficient, even as sensor nodes require computational power to mine a next block. Because of such extensive and intermittent calculations in PoW, it produces enormous power usage yet is not recognized an energy-efficient approach [32, 39, 40]. Considered to be highly encouraging, additional research is needed on this consensus algorithms as PBFT requires robustness and PoS protection has not yet been rigorously investigated.

11.6.4 Interoperability

The adoption of rules for blockchain systems is still not widely recognized. Numeric organizations like NIST and IEEE would be in the process of establishing guidelines for blockchain adoption, and protection. [32, 41]. This ambiguity is again enhanced when the self-governing blockchain networks implement different consensus frameworks. For e.g., Hyperledger requires PBFT, and Ethereum utilizes the PoW consensus algorithm but these two processes have to be coordinated to allow efficient process. Consequently, in order to promote streamlined content management framework, it is important to transfer data between one blockchain into the next. Therefore, the concept of integrated data applications for smart city technologies blockchain-based data requires more research.

11.7 Conclusion

The rapid urbanization and population growth in emerging markets, associated with the rapid development of cities, continues to challenge the economic and environmental affordability of the cities. Towards this extent, it is suggested that its idea of “Smart City” leverage conventional ICT through an effective manner to create a healthy metropolitan services and develop the lives of the people. But security breaches are spreading rapidly in smart cities. Because of its highlight the importance like interoperability, efficiency, intractability and democratization such issues could be proposed to resolve through use of blockchains. The opportunities and implications of adapting blockchains to smart cities and their trade-offs are discussed in this article via a detailed survey. The study begins with many recent comprehensive scope of the issue and context information about blockchain-based smart cities. It just addresses the inspiration behind its adoption of blockchain technology in growing technologies. In addition, the article attempts to combine the two approaches by investigating the usefulness of blockchain in several systems, like smart healthcare,

intelligent vehicle, smart grid, supply chain management, and banking sectors. Eventually, various open opportunities for the future prospects of science in important areas are highlighted. In extending block chain to emerging technologies, this study is supposed to address as a body of knowledge and comprehensive guidance for future consideration.

References

1. World urbanization prospects: The 2014 revision, highlights (ST/ESA/SER.A/352), United Nations, Department of Economic and Social Affairs, Population Division, Tech. Rep., 2014 (Online). Available: <https://esa.un.org/unpd/wup/Publications/Files/WUP2014-High-lights.pdf>
2. Nakamoto, S., et al.: Bitcoin: a peer-to-peer electronic cash system (2008)
3. Mick, T., Tourani, R., Misra, S.: LASeR: lightweight authentication and secured routing for NDN IoT in smart cities. *IEEE Internet of Things J.* **5**(2), 755–764 (2018). <https://doi.org/10.1109/jiot.2017.2725238>
4. Chinnasamy, P., Deepalakshmi, P., Praveena, V., Rajakumari, K., Hamsagayathri, P.: Blockchain technology: a step towards sustainable development. *Int. J. Innov. Technol. Explor. Eng. (IJITEE)* **9**(2S2)
5. Bhushan, B., Khamparia, A., Martin Sagayam, K., Sharma, S.K., Ahad, M.A., Debnath, N.C.: Blockchain for smart cities: a review of architectures, integration trends and future research directions. *Sustain. Cities Soc.* (2020). <https://doi.org/10.1016/j.scs.2020.102360>
6. Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., Qijun, C.: A review on consensus algorithm of blockchain. In: 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC) (2017). <https://doi.org/10.1109/smcc.2017.8123011>
7. Schwartz, D., Youngs, N., Britto, A.: The ripple protocol consensus algorithm. Ripple Labs Inc White Paper, vol. 5 (2014)
8. Saghir, A.M.: Blockchain Architecture. In: Kim, S., Deka, G. (eds.) *Advanced Applications of Blockchain Technology. Studies in Big Data*, vol. 60. Springer, Singapore (2020). https://doi.org/10.1007/978-981-13-8775-3_8
9. Mohanta, B.K., Jena, D., Panda, S.S., Sobhanayak, S.: Blockchain technology: a survey on applications and security privacy Challenges. *Internet of Things* (2019). <https://doi.org/10.1016/j.iot.2019.100107>
10. Aggarwal, S., Chaudhary, R., Aujla, G.S., Kumar, N., Choo, K.K.R., Zomaya, A.Y.: Blockchain for smart communities: applications, challenges and opportunities. *J. Netw. Comput. Appl.* **144**(June), 13–48 (2019). <https://doi.org/10.1016/j.jnca.2019.06.018>
11. Wang, H., Zheng, Z., Xie, S., Dai, H.N., Chen, X.: Blockchain challenges and opportunities: a survey. *Int. J. Web Grid Serv.* (2018). <https://doi.org/10.1504/ijwgs.2018.10016848>
12. Nicolas, C., Kim, J., Chi, S.: Quantifying the dynamic effects of smart city development enablers using structural equation modeling. *Sustain. Cities Soc.* **53**, 101916 (2020). <https://doi.org/10.1016/j.scs.2019.101916>
13. Arora, A., Kaur, A., Bhushan, B., Saini, H.: Security concerns and future trends of Internet of Things. In: 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT) (2019). <https://doi.org/10.1109/icicict46008.2019.8993222>
14. Wu, J., Ota, K., Dong, M., Li, C.: A hierarchical security framework for defending against sophisticated attacks on wireless sensor networks in smart cities. *IEEE Access* **4**, 416–424 (2016). <https://doi.org/10.1109/access.2016.2517321>
15. Dabeeodoal, Y.J., Dindoyal, V., Allam, Z., Jones, D.S.: Smart tourism as a pillar for sustainable urban development: an alternate smart city strategy from mauritius. *Smart Cities* **2**, 153–162 (2019)

16. Mahmood, K., Chaudhry, S.A., Naqvi, H., Kumari, S., Li, X., Sangiaah, A.K.: An elliptic curve cryptography based lightweight authentication scheme for smart grid communication. *Futur. Gener. Comput. Syst.* **81**, 557–565 (2018). <https://doi.org/10.1016/j.future.2017.05.002>
17. Lara-Nino, C.A., Diaz-Perez, A., Morales-Sandoval, M.: Lightweight elliptic curve cryptography accelerator for internet of things applications. *Ad Hoc Netw.* **103**, 102159 (2020). <https://doi.org/10.1016/j.adhoc.2020.102159>
18. Cisco security monitoring, analysis and response system (Online). Available: <https://www.cisco.com/c/en/us/products/security/securitymonitoring-analysis-response-system/index.html>
19. Chinnasamy, P., Deepalakshmi, P., Shankar, K.: An analysis of security access control on health-care records in the cloud. In: *Intelligent Data Security Solutions for e-Health Applications*, pp. 113–130. Academic Press-Elsevier (2020)
20. Chinnasamy, P., Deepalakshmi, P.: A scalable multilabel-based access control as a service for the cloud (SMBACaaS). *Trans. Emerg. Telecommun. Technol.* **29**(8), e3458 (2018). <https://doi.org/10.1002/ett.3458>
21. Chinnasamy, P., Deepalakshmi, P.: A survey on enhancing cloud security through access control models and technologies. *Int. J. Comput. Sci. Eng. (IJCSE)* **9**(5), 326–331
22. Kang, J., Yu, R., Huang, X., Maharjan, S., Zhang, Y., Hossain, E.: Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains. *IEEE Trans. Ind. Inf.* **13**(6), 3154–3164 (2017). <https://doi.org/10.1109/tti.2017.2709784>
23. Huang, X., Xu, C., Wang, P., Liu, H.: LNSC: a security model for electric vehicle and charging pile management based on blockchain ecosystem. *IEEE Access* **6**, 13565–13574 (2018). <https://doi.org/10.1109/access.2018.2812176>
24. Kang, J., Xiong, Z., Niyato, D., Ye, D., Kim, D.I., Zhao, J.: Toward secure blockchain-enabled internet of vehicles: optimizing consensus management using reputation and contract theory. *IEEE Trans. Veh. Technol.* **68**(3), 2906–2920 (2019). <https://doi.org/10.1109/tvt.2019.2894944>
25. Zhou, Z., Wang, B., Guo, Y., Zhang, Y.: Blockchain and computational intelligence inspired incentive-compatible demand response in internet of electric vehicles. *IEEE Trans. Emerg. Top. Comput. Intell.* **3**(3), 205–216 (2019). <https://doi.org/10.1109/tetci.2018.2880693>
26. Yang, Z., Yang, K., Lei, L., Zheng, K., Leung, V.C.M.: Blockchain-based decentralized trust management in vehicular networks. *IEEE Internet of Things J.* **6**(2), 1495–1505 (2019). <https://doi.org/10.1109/jiot.2018.2836144>
27. Li, L., Liu, J., Cheng, L., Qiu, S., Wang, W., Zhang, X., Zhang, Z.: CreditCoin: a privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles. *IEEE Trans. Intell. Transp. Syst.* **19**(7), 2204–2220 (2018). <https://doi.org/10.1109/tits.2017.2777990>
28. Luo, B., Li, X., Weng, J., Guo, J., Ma, J.: Blockchain enabled trust-based location privacy protection scheme in VANET. *IEEE Trans. Veh. Technol.* **69**(2), 2034–2048 (2020). <https://doi.org/10.1109/tvt.2019.2957744>
29. Wang, J., Wu, L., Choo, K.-K.R., He, D.: Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure. *IEEE Trans. Ind. Inf.* **16**(3), 1984–1992 (2020). <https://doi.org/10.1109/tti.2019.2936278>
30. Mentzer, J.T., Dewitt, W., Keebler, J.S., Min, S., Nix, N.W., Smith, C.D., Zacharia, Z.G.: Defining supply chain management. *J. Bus. Logist.* **22**(2), 1–25 (2001). <https://doi.org/10.1002/j.2158-1592.2001.tb00001.x>
31. Gonczol, P., Katsikouli, P., Herskind, L., Dragoni, N.: Blockchain implementations and use cases for supply chains—a survey. *IEEE Access* **8**, 11856–11871 (2020). <https://doi.org/10.1109/ac-cess.2020.2964880>
32. Bhushan, B., Khamparia, A., Martin Sagayam, K., Sharma, S.K., Ahad, M.A., Debnath, N.C.: Blockchain for smart cities: A review of architectures, integration trends and future research directions. *Sustain. Cities Soc.* **61** (2020). <https://doi.org/10.1016/j.scs.2020.102360>
33. Chen, P., Jiang, B., Wang, C.: Blockchain-based payment collection supervision system using pervasive Bitcoin digital wallet. In: *2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)* (2017). <https://doi.org/10.1109/wimob.2017.8115844>

34. Khan, C., Lewis, A., Rutland, E., Wan, C., Rutter, K., Thompson, C.: A distributed-ledger consortium model for collaborative innovation. *Computer* **50**(9), 29–37 (2017). <https://doi.org/10.1109/mc.2017.3571057>
35. Nagel, E., Kranz, J.: Smart city applications on the blockchain: development of a multi-layer taxonomy. *Progress in IS Blockchain and Distributed Ledger Technology Use Cases*, pp. 201–226 (2020). https://doi.org/10.1007/978-3-030-44337-5_10
36. Hakak, S., Khan, W.Z., Gilkar, G.A., Imran, M., Guizani, N.: Securing smart cities through blockchain technology: architecture, requirements, and challenges. *IEEE Network* **34**(1), 8–14 (2020). <https://doi.org/10.1109/mnet.001.1900178>
37. Mokhtari, G., Anvari-Moghaddam, A., Zhang, Q.: A new layered architecture for future big data-driven smart homes. *IEEE Access* **7**, 19002–19012 (2019). <https://doi.org/10.1109/access.2019.2896403>
38. Alli, A.A., Alam, M.M.: SecOFF-FCIoT: machine learning based secure offloading in Fog-Cloud of things for smart city applications. *Internet of Things* **7**, 100070 (2019). <https://doi.org/10.1016/j.iot.2019.100070>
39. Mendling, J., Weber, I., Aalst, W.V., Brocke, J.V., Cabanillas, C., Daniel, F., Zhu, L.: Blockchains for business process management—challenges and opportunities. *ACM Trans. Manage. Inf. Syst.* **9**(1), 1–16 (2018). <https://doi.org/10.1145/3183367>
40. Vukolic, M.: The quest for scalable blockchain fabric: proof-of-work vs. BFT replication. In: *Open Problems in Network Security Lecture Notes in Computer Science*, pp. 112–125 (2016). https://doi.org/10.1007/978-3-319-39028-4_9
41. Xiao, Y., Zhang, N., Lou, W., Hou, Y.T.: A survey of distributed consensus protocols for blockchain networks. *IEEE Commun. Surv. Tutor.* **1**-1 (2020). <https://doi.org/10.1109/comst.2020.2969706>

Chapter 12

Blockchain Technology and Fashion Industry-Opportunities and Challenges



Gautami Tripathi, Vandana Tripathi Nautiyal, Mohd Abdul Ahad, and Noushaba Feroz

Abstract Fashion and textile industry are one of the fastest growing sectors that involves a complex supply chain at local and global levels to procure raw materials and supply finished products to the market. The complexity of the industry demands for a system which is transparent, distributed and can protect the intellectual property rights. With key characteristics like decentralization, immutability, consensus etc., blockchain technology has the potential to enhance the exiting fashion industry by adding an extra layer of security and trust to it. One of the major challenges faced by the fashion industry is the counterfeit products flooding the market place. These fake products have a negative impact on the brand image and value. Blockchain has the ability to protect and secure the digital identities and establish authenticity in fashion industry. Despite of the exponentially growing popularity and interest in this technology, very little is known about the current state of application and use of blockchain in fashion and textile industry. This paper discusses the various aspects of the use of blockchain technology in the fashion and textile industry highlighting the benefits that blockchain could bring. The role of blockchain in providing potential solutions to the existing issues and challenges faced by the fashion industry are discussed with an insight into the current state of the blockchain technology in fashion industry. Further, the work also discusses the challenges in the integration of blockchain into the existing processes of the fashion and textile industry.

Keywords Blockchain · Fashion and textile industry · Intellectual property · Fashion supply chain · Transparency · Counterfeit products

G. Tripathi (✉) · M. A. Ahad · N. Feroz

Department of Computer Science and Engineering, School of Engineering Sciences and Technology, Jamia Hamdard, New Delhi, India

V. Tripathi Nautiyal

MIT Institute of Design, MITADT University, Pune, India

12.1 Introduction

Blockchain technology is considered as one of the most impactful technological breakthroughs in the last decade. The unique features like decentralization, transparency and immutability has gained considerable attention from researchers across the globe and has helped blockchain technology to move beyond the financial domain and register its presence in other areas. A blockchain is a transparent and dynamically growing ledger which stores a permanent record of all the current and historical transactions in a secure, chronological, and immutable way. Initially incepted as a “peer-to-peer” ledger for registering the transactions of bitcoin cryptocurrency, blockchain is now becoming popular in many other application domains that require trust-less exchanges in decentralized distributed environments. In the last decade, blockchain technology has seen exponential growth in its popularity. Blockchain technology is based on the concept of digital distributed ledger technology that enables to maintain a timestamped record of transactions and other events and store it into blocks. The concept was initially developed for financial transactions with the introduction of bitcoin in the year 2008 by Nakamoto [1]. The technology gets its popularity from the fact that each block in the blockchain has a unique identifier called the block hash that is linked to the previous block in the blockchain. These cryptographically linked blocks of information are immutable and makes it difficult to change or modify any information in the blockchain as all the blocks forms a part of a verification process which makes changing data expensive [2–4]. Another important feature of the blockchain technology that makes it popular is the removal of the intermediaries and the third parties from the whole transaction process. Despite being a decade old technology blockchain has gained rapid popularity across various domains. The key characteristics of blockchain technology as presented in Fig. 12.1 provides potential solutions to ensure the transparency, security, anonymity, privacy and robustness of various processes across industries and businesses. Today many solutions based on this technology are being used across an array of industries like healthcare, agriculture, education, banking, smart cities etc. [2, 3, 5, 6]. Fashion industry being one of the rapidly growing industries has also seen significant technological innovations in the way of its working. The unique features of the blockchain technology makes it a potential solution to overcome the difficulties faced by the fashion industry. This chapter is divided into 6 sections. Section 2 discusses some of the major challenges and issues faced by the fashion industry highlighting the prime issues of supply chain management, intellectual property rights and sustainability. The next section presents a study of some of the related researchers in the area of fashion industry and blockchain technology. Section four highlights the role of blockchain technology in the fashion industry by providing insights into some of the major benefits and potential solutions to overcome the existing issues faced by the fashion industry. Section five presents the challenges in the integration of blockchain technology into the fashion industry processes. The potential challenges that may affect the successful implementation of blockchain into the fashion industry are discussed. Section six provides the conclusion and future scope.



Fig. 12.1 Key characteristics of Blockchain

12.2 Issues in Fashion Industry

The global fashion industry is growing rapidly due to several factors and is all set to take its graph further to a higher level in the coming times. Over the period of time, various digital technological advancements have played a major role in enhancing the capabilities of fashion industry to provide value and seamless experience to its customers across the globe. Bridging the gap between fashion and digital technology and especially blockchain technology can lead to solving various crucial issues that persist in Fashion Industry today. Coupling fashion industry with blockchain technology can help business achieve better service to their customers. In view of this situation below are the main key issues existing in Fashion industry today which can probably be address with the help of block chain technology.

12.2.1 Supply Chain Issues

Supply Chain Management constitutes the sequence of key business processes from procurement of raw materials to getting the product delivered to the end user.

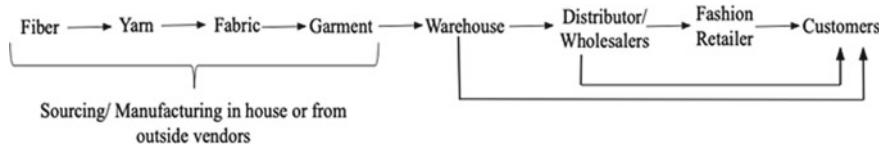


Fig. 12.2 Supply chain in fashion industry

Supply chain in fashion industry is very long, complex and demanding in nature. The ecosystem of an apparel supply chain generally comprises of sourcing of raw material (fiber, yarn, fabric) from in-house or from outside vendors, manufacturing of apparels which can be again done in-house or through outside vendors, distribution of apparels through distributors and wholesalers and finally the apparel product reaches the retailers from their it reaches the customers. There are many intermediary parties in between especially vendors, logistic and other supporting partners which are involved as a part to complete supply chain network as presented in Fig. 12.2.

Longer lead times, shorter seasons and global sourcing adds to complexity of fashion supply chain [7]. Also, high degree of uncertainty of consumer demand affects the flow of supply chain making it complicated. In order to meet the consumer demand on time the supply chains need to be quick in response without delays and to achieve this the information flow at various points should be smooth, accurate and on real time basis. In traditional system of supply chain, information sharing at each step of supply chain is very minimal and difficult to obtain. With the help of enhanced ERP systems this problem is reduced but cannot be totally resolved. Moreover, implementation of an ERP system is a complex, large scale project, which has significant strategic, operational and increased business cost implications for the organization [8]. Finding an ERP solution to fit specific need of a fashion business is another challenge [9].

Also, with the increasing demand of radical transparency from consumer's side it is pushing business to be more efficient in monitoring and disclosing their supply chain activity. Customers are proactively interested in complete transparency and traceability throughout supply chains. However, most brands are still following the legacy supply chain frameworks which lacks transparency and traceability [10].

12.2.2 Intellectual Property Right Issues

The fashion industry is much more than just clothes and apparels. It is more about creating and manufacturing novel designs with an aim to monetize with intellectual proprietary rights [11]. Fashion managers must be able to timely identify the valuable assets and their business relevance in order to safeguard the intellectual property rights [12]. The universal selling point (USP) of any fashion business is innovation and creativity. Therefore, such businesses are primarily focused on creating new and innovative design and manufacturing ideas and invests a good amount of time and

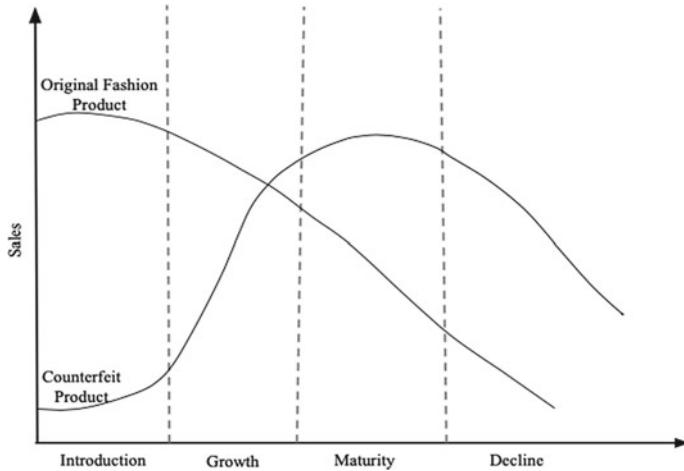


Fig. 12.3 A typical lifecycle of a counterfeit product [16]

money in such initiatives. However, it is pertinent to protect such initiatives from copyright infringements and IPR issues. Counterfeiting design ideas and products is a crucial problem for fashion business and as well as for consumers which needs to be tackled effectively. Especially luxury brands in a globalized market are the most affected segment [13]. But counterfeits are not limited to luxury products, it has an ill effect on the reputation of the brands as well [14, 15]. Counterfeit products once enter the supply chain, disrupts the supply with identically similar items of poor quality. A counterfeit product has highly devastating effect on a brand which results in loss of sale revenue and profit. Figure 12.3 presents the life cycle of a Counterfeit Fashion Product [16].

The designers for fashion brands process some unique and creative work which is simply copied and sold by others without consent from brands which is treated as infringement of intellectual property rights by a business. This act of copying severely affects the fashion business revenue and overall brand image. The protection of design copyrights is very much crucial in fashion industry. The design and appearance of the clothes and apparels are one of the most crucial determining factors in consumer choice. The designs in Fashion industry can be protected as under Patent Act, Copyright Act and Design Act. But mostly fashion designs are not registered under these protection acts due to short product life cycle which does not justify the time and cost involved in getting protected and there is no other alternate solution to this problem. In such scenario the Intellectual property rights available at the moment are not much relevant and practical to Fashion businesses.

12.2.3 Sustainability Issue

Sustainable fashion has become one of the most talked about concepts amongst the fashion community. Many big design houses and renowned brands are opting for environment friendly processes and moving towards sustainable fashion. However, the mass adoption of this concept of sustainable fashion is still far from reality. Sustainability in fashion depends of three major aspects namely the environmental aspect, the social aspect and the economic aspect.

The environmental aspect deals with the best practices to ensure that the various production processes are nature friendly. The major part of environmental impact come from the usage of various chemicals and natural resources leading to negative impact on the environment. The social aspect of sustainable fashion aims to ensure healthy working conditions for the labours. In most parts of the world the fashion industry provides harmful working environments and unfair labour practices to the artisans and labours. The economic sustainability aims at making the fashion affordable while balancing the environmental and social aspects.

To establish equilibrium between these three aspects is a major challenge for the fashion industry. The efforts to cut costs and make fashion affordable have a negative impact on the environmental and social sustainability as it results in minimizing the budget for chemical waste treatments, resource recycling, low labour etc. On the other hand, improving the environmental and social sustainability leads to increased cost of production. These increased costs create an overhead for small and medium scale industries thus making environmental and social sustainability less feasible and less desirable. Figure 12.4 provides the various environmental and sustainability aspects in fashion industry.

Sustainability issues in the fashion industry is surfacing across the globe and is gaining ground in Fashion industry. Moreover, shift in consumer behavior towards sustainable lifestyle lays emphasis on developing circular economic models which are sustainable. Fashion business are trying to push themselves towards ecological integrity and social justice while earning profits to balance the triple bottom line of sustainability [17] as shown in Fig. 12.5.

Businesses are trying to build brands that are for people, planet and profit. Sustainable Fashion business conduct themselves in an ethical and fair way. Fashion is a labor-intensive industry and the welfare of the people or human capital involved in fashion ecosystem is the responsibility of businesses. This includes the workers, laborers, artisans and other people directly or indirectly working in the industry are treated fairly, have good working conditions, and receive fair wages and appreciation for their work. Also, the businesses should be concerned about their impact on other people around them and specially their customers. Fashion industry is one of the biggest culprits for pollution on this earth. Caring about the planet by reducing the impact on environment by making clothes in a more environment friendly manner is one of the triple bottom lines of sustainability. Fashion business these days vie hard to incorporate sustainable materials, sustainable design and manufacturing process in their business to reduce the size of their ecological footprint as much as possible.

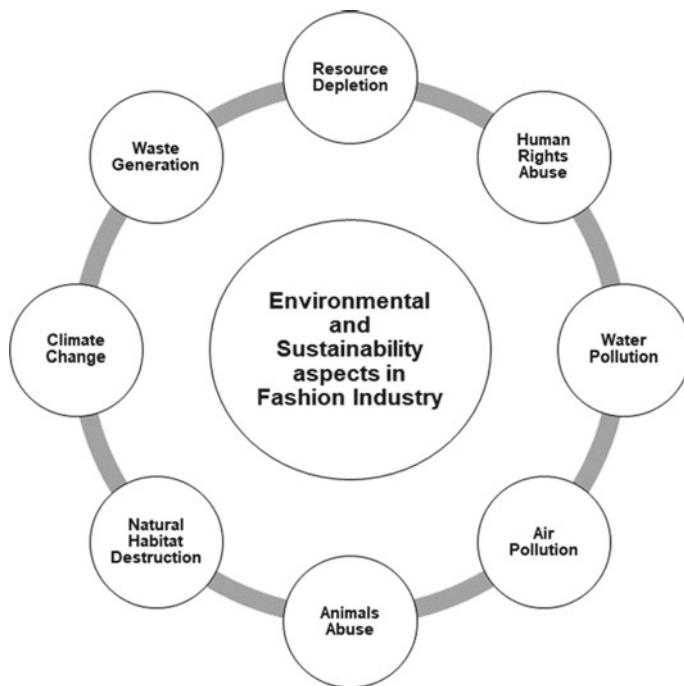


Fig. 12.4 Environmental and sustainability aspects in fashion industry

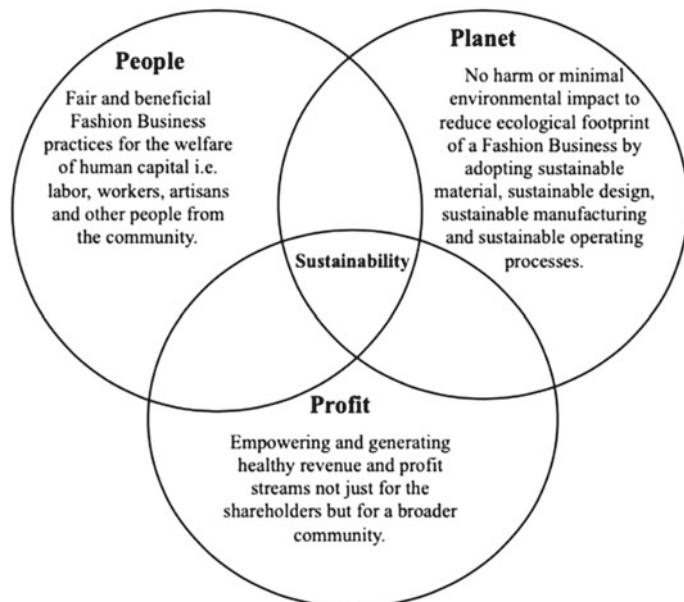


Fig. 12.5 A triple bottom line of sustainability in fashion business

Also, customers should be made aware about the initiatives that the business take to make better choices for people and planet. These thing needs to be promoted, educated and communicated to the customers in a very transparent way which can help build trust between the businesses and customers. Also, this will empower and generate healthy revenue and profit streams not just for the shareholders but for a broader community. Fashion business are trying to pioneer in sustainability aspect to leverage the commercial opportunity. Business need to start measuring their sustainability performance and develop strategies to achieve sustainability goals and also inform consumer in a transparent way to enable trust.

12.3 Related Work

The last decade has seen a significant increase in the researches, academic debates and publications in the fashion domain. The growing interests in fashion has helped to establish it as one of the major industries in today's world [18]. The authors in [19] highlights the main characteristics of the modern fashion industry in terms of the volatility, velocity, variety, complexity and dynamism of the fashion industry. The paper also focuses on the management of the supply chain in the fashion industry as characterized by the time to market, time to serve and time to react. The authors used systematic, comparative and logical research approaches for conducting their research and analysis. The authors in [20] discussed about the possibility of designing and adopting sustainable fashion designs. The various challenges associated with it are also discussed. The paper further presents a model for designing sustainable fashion that identifies the principles and best practices to be implemented for achieving sustainability in fashion designs. The authors in [21] highlights the importance of innovative sustainable business models in fashion industry. The study comprises of interviews and case studies to propose a framework that showcases the various trends and drivers of sustainable and innovative models of business in fashion industry. The work discusses the concept of circular economy, corporate social responsibility, collaborative consumption and sharing economy, consumer awareness and various technological innovations. Further the authors also discussed about the various fashion-based startups that are focused on innovation and sustainability. The work presented in [22] highlights the changes that have occurred since 1990 in the fashion industry. The study focuses on the emerging trends of fast fashion from the perspective of the suppliers as well as the consumers. In [23] the authors discussed about the technological interventions in the fashion industry by highlighting the role of Information and Technology (IT) in bringing a paradigm shift in the overall consumer experience in the online shopping environment. Further the author also discussed about the influence of online shopping experiences on the fashion consumers based on a survey conducted on 439 consumers from UK. The authors in [24] proposed an innovative and sustainable model for fashion industry that redefines the manufacturing process to reduce the carbon footprints. The authors used the blockchain technology to improve the Emission Trading

Scheme (ETS) that enables to measure and record the carbon emissions for fashion apparel manufacturing industry. The results of the study show that blockchain integration into the ETS helps to significantly improve the performance of the system and provides environmentally sustainable solutions. In [25] the authors highlighted the data quality issues in the fashion industry and its impact on the sustainable supply chain operations. The authors further advocate the use of blockchain technology for enhancing the supply chains and presents an environmental taxation waiver scheme for social welfare. The study presented in [26] shows how blockchain technology can provide a solution for Intellectual Property related issues in the fashion and other industries by enhancing the process of registration, transaction processing, enforcements, payments, licenses, distributions and agreements. The authors in [27] highlighted the potential of blockchain technology to create a transparent system in the fashion industry by filling the gaps in the efficient implementation of Intellectual property rights. The paper focuses on how blockchain can help the small and medium scale industry and new designers to defend and protect their IP. The use of smart contracts to eliminate the intermediaries and third parties in the IP law process is also discussed.

12.4 Blockchain for Fashion Industry

Blockchain technology has disrupted almost every business domain ranging from transportation, agriculture, healthcare, education, manufacturing etc. Fashion industry is no exception. The new age fashion industry is harnessing the unique characteristics of blockchain technology to improve the capital expenditure and operational expenditure. The blockchain technology not only brings transparency but also gives the ability to provide real-time tracking of the goods and services. In a typical fashion industry, copyright infringements are common. With blockchain technology a unique identity can be provided to the designs and products of the designers and brands which is immutable. Another important aspect that blockchain technology brings in fashion industry is the ability of tracking of raw materials and finished products from source to destination with a much more precision and less cost as compared with the legacy tracking mechanisms. As a result of the unprecedented features of the blockchain technology, many fashion brands and startups are already implementing the technology in their core business models. Figure 12.6 provides the domains of fashion industry where blockchain technology can be used.

12.4.1 Inventory Management

Blockchain based inventory management provides a transparent mechanism to maintain inventory and real-time updates on inventory. Since it is a linked block of immutable chains, it can easily trace and track the inventory items. We can also

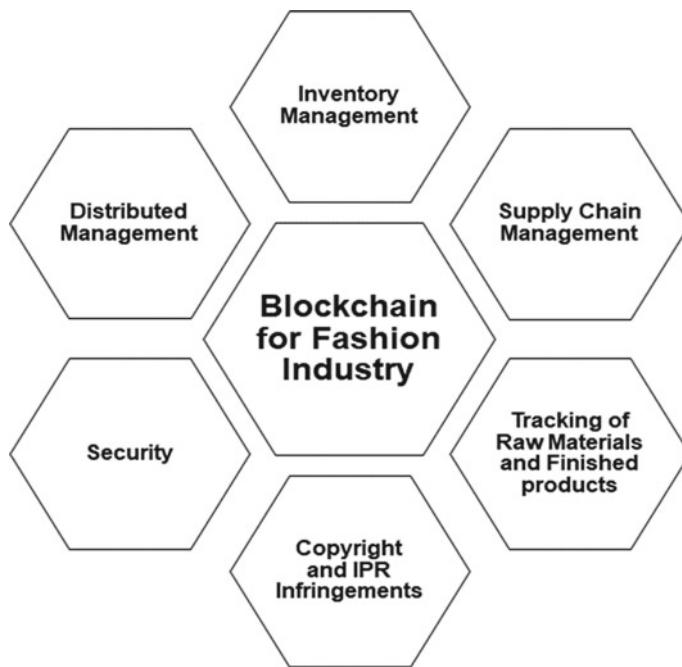


Fig. 12.6 Blockchain in fashion industry

provide better forecast of the inventory items and thus cater to dynamically changing demands.

12.4.2 Distributed Management

Blockchain provides a distributed means to organize data items. These items are linked together through an immutable chain of blocks. Therefore, instead of depending upon a single server, a peer to peer network of goods and services can be maintained using the blockchain technology. This mechanism makes it much more effective and easily manageable and highly scalable with the growing needs of the customers.

12.4.3 Supply Chain Management

With the transparency of blockchain technology, the tracing and tracking of goods and services can be managed in real-time. With the help of advanced analytics and

blockchain technology, better and informed decisions can be taken to maintain the balance between the supply and demands.

12.4.4 Security

Blockchain technology makes the system more secure and immutable. In blockchain, only the legitimate entities of the system are allowed role-based access on mutually agreed smart contracts. No other entity (external or internal) can have access to the system. Furthermore, the anonymity of the blockchain technology enable the users to interact with each other without the fear of compromising their personal and other information (which is not needed).

12.4.5 Copyright and IPR Infringements

In fashion industry, the main USP of the fashion brands is the uniqueness and quality of the designs and products. The blockchain based IR tags and chips can be used to ensure the legitimacy of the goods and services as well as track them throughout the product life cycle from raw materials to the finished products. Blockchain based digital designs are highly secure and are not prone to copyright infringements.

12.4.6 Tracking of Raw Materials and Finished Products

Blockchain technology helps in tracking and tracing the raw materials. The blockchain based IR tags can be used to track the goods and services and provide the customer with the history of the apparels in order to make them aware about things like from where the raw material is procured, what is the product life cycle, what procedure is involved in making the finished products etc. Figure 12.7 shows the life cycle of Apparels and Garments.

Raw Material Procurement

Integrating blockchain at the raw material procurement stage make it possible to track the source and origin of the raw material. The quality and authenticity of the raw materials used for the production can be ensured using the blockchain technology. The compliance with international labor and environmental laws can also be ensured through blockchain technology.

Textile Production

At this stage, the blockchain technology can be used to oversee the production steps including yarn development, textile thickness, quality etc. in a transparent manner.

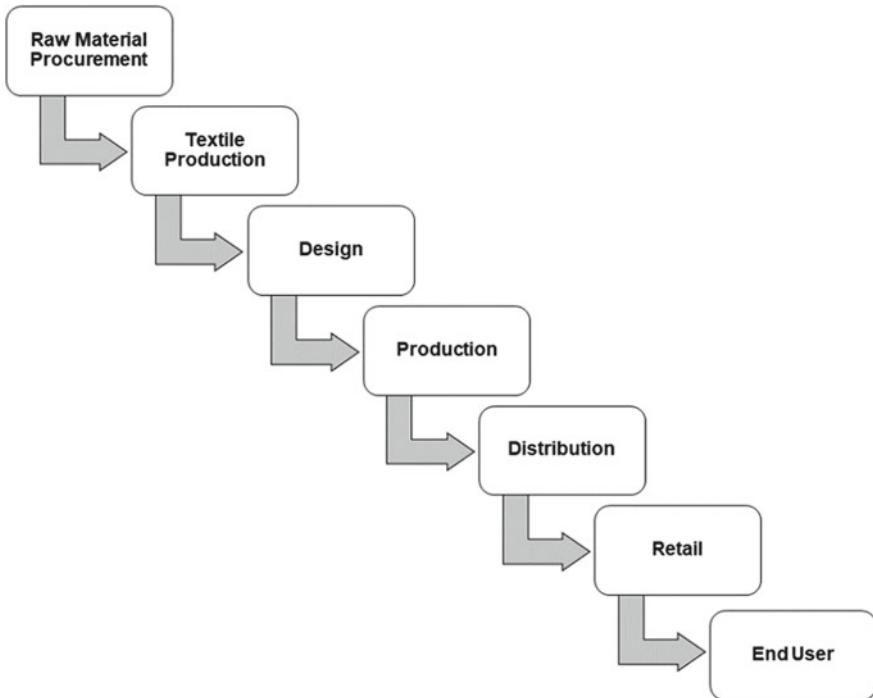


Fig. 12.7 Life cycle of apparels and garments

Design

Once the textile is developed, the next and the most important stage is the designing of the product. With blockchain technology, the unique designs of the designers can be protected against copyright infringements and IPR thefts. The blockchain based tags can be used to uniquely identify the designs in a digital format which is impossible to counterfeit.

Production (Final Goods)

After the finalization of the designs, the textiles are sent to the production warehouses for bulk productions. The complete production life cycle can be tracked using the blockchain technology.

Distribution

Blockchain technology makes it possible to track and trace the textile throughout the transportation cycle till it reaches the destination.

Retail

Once the textile and finished products reach the retailers, they can use blockchain technology to effectively manage the supply chain, inventory and thus reduce costs and save time.

End Users

The garments and apparels which are created by integrating blockchain technology makes it possible for the end user to identify the production life cycle, authenticity and source of origin of the clothes giving them complete satisfaction.

The increasing awareness amongst the masses to opt for sustainable, cruelty free and environment friendly products has led to the ideas revolving around the use of technology in fashion industry. Many fashion houses, brands and startups are experimenting with solutions to cater this demand. One of technologies that has gained considerable notice in the last few years the blockchain technology. Many new ideas have emerged on the integration of blockchain technology into the existing fashion industry processes to make it more sustainable, ethical and efficient. Table 12.1 presents some of the organizations that have used blockchain in the fashion industry.

12.5 Blockchain for Fashion Industry-Issues and Challenges

Blockchain has emerged as a revolutionary technology capable of transforming a wide spectrum of sectors, including fashion industry. It offers a mechanism that facilitates reliable, secure and immutable transactions, without the need of a centralized control. In the fashion industry, blockchain implementation enhances product regulation, brand security, supply chain handling, and combatting infringement, thus building an effective, accountable and profitable market [27]. While blockchain technology has several unprecedented advantages, the introduction of this platform in fashion industry leads to certain issues and challenges briefly described in Fig. 12.8 [16, 25, 28–32].

12.5.1 Absence of Regulating Authority

The implementation of blockchain implies an end for intermediaries, eliminating the dependency on a regulating authority. The regulating authority has conventionally generated ample profit by eliciting desirable actions from agents to address external vulnerabilities. As such, the absence of such an authority resulting from blockchain deployment could render the fashion market vulnerable [28].

Table 12.1 Organizations using blockchain in fashion industry

Startups/Brands/platforms	Key features	Significance	References
Loomia	Developed a cloth blended with circuits that collects data and sync it on Loomia data exchange based on Blockchain technology	The users own their data and can share it with researchers for digital assets called Loomia Tokens	[33]
Provenance	Developed a transparent fashion supply chain	Helps brands to keep an eye on the entire production process to restore the trust, authenticity and values	[34]
CURATE	Ehtereum based app brings together the various stakeholders of the fashion industry to create a transparent community using a reward system	The trusted comments motivate the fashion creators to set new trend and increase the brand value and sales	[35]
Fashion Coin	Developed a P2P stem where the customers can directly contact the various people involved in the process of product development like designers, logistics, fabric menders etc.	Helps to create transparency and trust amongst the stakeholders	[36]
Faizod	Setting up of global supply chain management for seamless interaction between producers, intermediaries and consumers	Provides real time tracking of products this ensuring complete transparency about how product are made, transported and paid for and Helping fashion industries by providing a ubiquitous supply chain management platform for identifying key bottlenecks as the products are developed	[37]
VeChain	Creates a digital trace of the fashion goods using unique IDs, NFC Chips and QR codes	Helps to eliminate the Counterfeit goods from the fashion industry	[38]
LVHM	Using blockchain for tracking of products and their authenticity	Put a check on counterfeit products illegally sold under the brand name	[39]

(continued)

Table 12.1 (continued)

Startups/Brands/platforms	Key features	Significance	References
Martine Jarlgard	Used blockchain platform provenance for tracking raw materials at every stage of production	Provides information to the users about the nature and type of raw material used, life cycle stages etc.	[40]
Levi Strauss & Co	Used blockchain for workers wellbeing survey for ensuring worker welfare	Provided an anonymous means to the employees to share their personal well-being information which they are hesitant to share face to face	[41]
Somish Blockchain Labs	Working for promoting CSR activities and identify cost saving mechanisms, better worker wellbeing etc.	Helps the fashion brands to implements sustainable practices using technology driven approaches that also helps to discover cost saving approaches and ensures other aspects of contracts	[42]
Arianee	It is a protocol used for certifying products for authenticity and communication between fashion brands and users	Every product has a blockchain based certificate for validating its authenticity	[43]
SourceMap	Build a network to facilitate verified communication between people involved in the supply chain process	Helps to improve the transparency in the fashion supply chain	[44]

12.5.2 Technology Immaturity

Blockchain technology continues to evolve and grow. This technology is still at its initial stage and researchers are currently testing the beta stage of blockchain seeking to overcome various issues associated with the technology [29].

12.5.3 High Cost

The expense of deploying and managing a blockchain-based infrastructure may be high because of the intricate design involving multiple transactions. The high computational complexity arising from billions of transaction verifications could result in a bottleneck, particularly for supply chain involving numerous items and related details [29].



Fig. 12.8 Issues and challenges of blockchain deployment in fashion industry

12.5.4 Loss in Supply Chain

In the context of fashion industry, when the deployment of blockchain is costly and the environmental expense related to the remaining commodity is substantially high, it will benefit the society at large but it will lead to losses in the supply chain [25].

12.5.5 High Complexity of Blocks

The scale and number of blocks grows with growing information, commodity complexity and supply chain partners, leading to higher processing and database needs. The management of such circumstances involves examining and selecting only critical product lifecycle phases and relevant details for the purpose of traceability [29].

12.5.6 Lack of Standardization

Blockchain lacks standardization and interoperability, hence the concerned parties need to compromise their data and policies considerably to generate maximum compatibility. Moreover, being a novel technology, industries such as fashion industry are reluctant to adopt blockchain [30].

12.5.7 Need for Two-Level Security

In the case of blockchain, the real product details may be retrieved by a bogus product from the database with the intent of forgery. Hence, security framework needs to be deployed at the business level (to facilitate secure information exchange among supply chain players and businesses) and product level (to safeguard product and traceability tags from forgery) [29].

12.5.8 Information Transparency

As blockchain renders the supply chain transparent, many stakeholders are hesitant to reveal critical details about their trade since their rivals might steal this information. Moreover, the collection and processing of this information is a tiresome task, thereby requiring additional incentives to encourage the involved participants [29].

12.5.9 Intellectual Property Protection

The automated nature of blockchain poses concerns for intellectual property protection for fashion vendors, such as the inability to provide legal defense to intellectual properties. The general theory is that blockchain cannot override existing

copyright legislation, and third parties cannot provide copyright defense without the unequivocal permission of the lawmaker [31].

12.5.10 Blockchain Incorporation Challenge

Incorporating blockchain into the existing fashion industry can pose a serious challenge as the overall process could be highly expensive and time consuming. An additional funding of human resources may be required for the successful cultural transition from centralized to decentralized framework.

Consequently, blockchain deployment requires strong enthusiasm and anticipation among the concerned players in the fashion market [29].

12.6 Conclusion and Future Scope

In the last few years fashion industry has greatly impacted the social and economic life of individuals. Today fashion has become a powerful medium of communication. The consumers of fashion, use it as a medium to express themselves to the external world where it has become a tool to represent the culture, personalities and social status. With the large popularity of high-end fashion brands amongst the masses has increased the demand of these products amongst all groups of people. Today the markets are flooded with counterfeit products to meet the increasing demands. The increasing demands has led to various malpractices in the fashion industry related to the labor laws, copyright, sustainability, supply chain etc. This increased popularity and demand of fashion products amongst the masses, has led to a considerable amount of attention towards the issues and challenges faced by the industry and its impact on the social, economic and environmental aspects. Today fashion industry is using various ICT tools and other technological innovations to transform their processes and meet the demands of the market and at the same time increase their profits. Blockchain technology has gained significant attention from the fashion world in the last few years. The key features of blockchain technology like transparency, immutability, decentralization, anonymity etc. are seen as potential solution to the existing issues and challenges of the fashion industry. The work presented here explores the potential of blockchain technology in transforming the fashion industry from an opaque to a transparent system along with the various challenges that might come in the way. Blockchain has the potential to address the issues of the fashion supply chain by facilitating transparency and traceability along with the elimination of intermediaries and third parties. The technology can also help to achieve sustainability by addressing the various social, economic and environmental aspects. Further the transparency and immutability of blockchain helps to protect the intellectual property rights and fight against the counterfeit products. Being a newly adopted technology the fashion industry the mass adoption of blockchain

is still far from reality. However, the study shows that integrating blockchain into fashion industry operations can bring traceability, transparency, scalability and flexibility in the system thus providing risk reduction, value creation, fault detection and elimination.

References

1. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. Manubot (2019)
2. Tripathi, G., Ahad, M.A., Paiva, S.: S2HS-A blockchain based approach for smart healthcare system. In: Healthcare, vol. 8, no. 1, p. 100391. Elsevier (2020, March)
3. Ahad, M.A., Paiva, S., Tripathi, G., Feroz, N.: Enabling Technologies and Sustainable Smart Cities. In: Sustainable Cities and Society, p. 102301 (2020)
4. Zheng, Z., Xie, S., Dai, H.N., Chen, X., Wang, H.: Blockchain challenges and opportunities: a survey. Int. J. Web Grid Serv. **14**(4), 352–375 (2018)
5. Tripathi, G., Ahad, M.A., Sathiyaranayanan, M.: The role of blockchain in internet of vehicles (IoV): issues, challenges and opportunities. In: 2019 International Conference on contemporary Computing and Informatics (IC3I), pp. 26–31. IEEE (2019, December)
6. Alam, M.A., Ahad, A., Zafar, S., Tripathi, G.: A neoteric smart and sustainable farming environment incorporating blockchain-based artificial intelligence approach. In: Cryptocurrencies and Blockchain Technology Applications, pp. 197–213 (2020)
7. K3 team: Supply Chain Challenges in Apparel Industry and How You Can Fix Them (2019, July 22). Retrieved from <https://www.k3software.com/post/2017/08/30/supply-chain-challenges-in-apparel-industry-and-how-you-can-fix-them>
8. Waters, B., Waters, I.: ERP in Fashion: Implementation Issues and Business Benefits (2013)
9. Hodge, G.L.: Enterprise resource planning in textiles. J. Tex., Apparel Technol. Manage. **2**(3) (2002)
10. Naila, K.: Traceability and Information in the Garment Supply Chain (2020, March 2). Retrieved from <https://impakter.com/traceability-and-information-in-the-garment-supply-chain/>
11. Saxena, A.: Significance of intellectual property in the fashion industry (2020, March 19). Retrieved from <https://www.lexology.com/library/detail.aspx?g=3011b365-d004-402f-8a62-1a52265787b0#:~:text=The%20lack%20of%20protection%20of,infringement%20of%20 heir%20fashion%20designs>
12. IP and Business: Intellectual Property in the Fashion Industry (n.d.). Retrieved from https://www.wipo.int/wipo_magazine/en/2005/03/article_0009.html
13. Hilton, Brian, Choi, Chong, Chen, Stephen: The ethics of counterfeiting in the fashion industry: quality, credence and profit issues. J. Bus. Ethics **55**, 343–352 (2004). <https://doi.org/10.1007/s10551-004-0989-8>
14. Counterfeit goods and piracy: a reality, Economie. Retrieved from <https://economie.fgov.be/en/themes/intellectual-property/protection-intellectual>. Accessed on 19 Aug 2020
15. Purnashri, D.: Biggest Threat to Intellectual Property: Counterfeiting with Special Focus on Fashion Industry (2019, June 20). Retrieved from <https://www.khuranaandkhurana.com/2019/06/20/biggest-threat-to-intellectual-property-counterfeiting-with-special-focus-on-fashion-industry/#:~:text=Counterfeits%20are%20not%20limited%20to%20luxury%20products.&text=So%2C%20we%20see%20that%20fashion,what%20is%20the%20original%20product>
16. <https://www.datadotdna.com/how-counterfeiting-can-destroy-your-brand-business/>
17. Sustainable fashion (2020, August 20th), In Wikipedia. Retrieved on https://en.wikipedia.org/wiki/Sustainable_fashion#:~:text=Sustainable%20fashion%20is%20a%20movement,addressing%20fashion%20textiles%20or%20products.&text=An%20adjacent%20term%20to%20sustainable%20fashion%20is%20eco%20fashion

18. Black, S.: Editorial in “fashion practice: design, creative process and the fashion industry”. *Fash. Pract.: J. Des., Creative Process Fash. Ind.* **1**(1), 5–8 (2009)
19. Ciarnienė, R., Vienazindiene, M.: Management of contemporary fashion industry: characteristics and challenges. *Procedia—Soc. Behav. Sci.* **156**, 63–68 (2014)
20. Aakko, M., Koskenurm-Sivonen, R.: Designing sustainable fashion: possibilities and challenges. *Res. J. Text. Apparel* **17**(1), 13 (2013)
21. Todeschini, B.V., Cortimiglia, M.N., Callegaro-de-Menezes, D., Ghezzi, A.: Innovative and sustainable business models in the fashion industry: entrepreneurial drivers, opportunities, and challenges. *Bus. Horiz.* **60**(6), 759–770 (2017)
22. Bhardwaj, V., Fairhurst, A.: Fast fashion: response to changes in the fashion industry. *Int. Rev. Retail, Distrib. Consum. Res.* **20**(1), 165–173 (2010)
23. Blázquez, M.: Fashion shopping in multichannel retail: the role of technology in enhancing the customer experience. *Int. J. Electron. Commer.* **18**(4), 97–116 (2014)
24. Fu, B., Shu, Z., Liu, X.: Blockchain enhanced emission trading framework in fashion apparel manufacturing industry. *Sustainability* **10**(4), 1105 (2018)
25. Choi, T.M., Luo, S.: Data quality challenges for sustainable fashion supply chain operations in emerging markets: roles of blockchain, government sponsors and environment taxes. *Transp. Res. Part E: Logist. Transp. Rev.* **131**, 139–152 (2019)
26. Burstall, R., Clark, B.: Blockchain, IP and the fashion industry. *Managing Intell. Prop.* **26**, 9 (2017)
27. Yanisky-Ravid, S., Monroy, G.: When Blockchain Meets Fashion Industry. Available at SSRN 3488071 (2019)
28. Trautman, L.J.: Virtual currencies; bitcoin & what now after Liberty Reserve, Silk Road, and Mt. Gox? *Richmond J. Law Technol.* **20**(4) (2014)
29. Agrawal, T.K., Sharma, A., Kumar, V.: Blockchain-based secured traceability system for textile and clothing supply chain. In: *Artificial intelligence for fashion industry in the big data era*, pp. 197–208. Springer, Singapore (2018)
30. Mistry, I., Tanwar, S., Tyagi, S., Kumar, N.: Blockchain for 5G-enabled IoT for industrial automation: a systematic review, solutions, and challenges. *Mech. Syst. Signal Process.* **135**, 106382 (2020)
31. Anderson, S.: The missing link between blockchain and copyright: how companies are using new technology to misinform creators and violate federal law. *North Carolina J. Law Technol.* **19**(4), 1 (2018)
32. Bhushan, B., Khamparia, A., Sagayam, K.M., Sharma, S.K., Ahad, M.A., Debnath, N.C.: Blockchain for smart cities: a review of architectures, integration trends and future research directions. *Sustain. Cities Soc.* **61**, 102360 (2020)
33. <https://www.loomia.com/tiletag>
34. <https://www.provenance.org/case-studies/martine-jarlgaaard>
35. <https://curate.style/index.html>
36. <https://coin.fashion/auth>
37. <https://www.intelligenthq.com/how-blockchain-could-support-ethical-fashion/>
38. <https://www.vechain.com>
39. <https://www.ledgerinsights.com/lvmh-luxury-blockchain-microsoft-consensys/>
40. <https://martinejarlgaaard.com/About>
41. <https://www.levistrauss.com/2019/01/24/new-way-measure-worker-well/>
42. <https://www.somish.com/lp/sustainable-fashion-survey-caif/>
43. <https://www.arianee.org>
44. <https://www.sourcemap.com>

Chapter 13

Secure Event Ticket Booking Using Decentralized System



Vihas Naman, Shanmukhi Priya Daliyet, Shagun S Lokre,
and K. Varaprasad Rao

Abstract Over the past years, it has been noticed that there is a steady increase in the number of events being conducted across the globe, and the entry to these events is monitored through a system of tickets. One of the biggest problems faced by the event organizers regarding the current system of events is the duplication and reselling of the tickets at a cost higher than the original cost. It has become easier for the commen to carry out this process as most of the tickets are purchased through various online platforms. Therefore, it is important to establish a reliable system to make sure that there won't be any tampering of the ticket. The objective behind this chapter is to introduce a new system of ticketing wherein, the issues faced in the current system can be tackled with the help of blockchain technology. In our proposed model, an online platform is engineered where the digital tickets are linked to the purchasers with the help of their mobile numbers. All the events are stored in the form of the ledger based on handling variance and tracking of the system. Due to its characteristics of decentralization, transparency, integrity, and immutability, blockchain can be effectively used to eliminate the above problems and improve the proof of ownership, making the tickets tamper-proof. This system will introduce trust between the participants involved in this chain and allows the consumers to authenticate and verify the ownership of the tickets before purchasing them. However, the usage of blockchain technology brings some constraints to our model when it comes to a large population.

Keywords Events · Ticket · Proof of ownership · Blockchain · Decentralization · Transparency

V. Naman (✉) · S. P. Daliyet · S. S. Lokre · K. Varaprasad Rao
Computer Science and Engineering Department, Icfai Tech (Faculty of Science and Technology),
ICFAI Foundation for Higher Education (Deemed to be University), Hyderabad, Telangana, India

K. Varaprasad Rao
e-mail: varaprasad.fst@ifheindia.org

13.1 Introduction

In the current time and day, there are a lot of frauds and scams in every monetary field, due to the present growth of the e-commerce market worldwide. The annual amount which is scammed by fraudsters in India is in the form of thousands of crores [1]. This majorly happens in the banking, corporate, medical sector, and also in the field of ticket selling for service or event management. With the latest facilities provided by various online platforms, people prefer buying tickets over the internet when compared to the traditional methods of waiting in the queues for a long time [2]. Over the last decade, due to the anonymity of the customers on the internet, it has become easier for the conmen to dupe customers. Even if the duped customers want to contact the sellers of the tickets it is really difficult. Since up until the last minute, the buyers do not know whether the ticket is fake or not, at which point in time, the conman disables the medium of connection which was used originally, this severs all connection methods to the conman. In this chapter, we propose a model as a solution to this problem, which will reduce fraud-practices like ticket counterfeiting and reselling tickets, by using blockchain technology [3–5]. Using this, we can make all the transactions transparent and the counterfeiting of any ticket nearly impossible. In this model, tickets are considered assets on the blockchain, similar to Ethereum and other cryptocurrencies [6, 7]. Since the content on the blockchain cannot be changed, the ticket or voucher once uploaded on it cannot be altered. The transactions are based on a token system, which will allow us to track and identify each transaction [8]. The security features of the proposed system are that data related to transactions and bookings are viewable, it is next to impossible to replicate the tickets for selling using an illegal manner, there is never a data leakage as there is a minimal human intervention which reduces most of the errors. There is no possibility for third party attacks as the blockchain is a decentralized system which consists of nodes that are mutually untrustworthy, and this property prevents the creation of malicious nodes for false transactions [9–11]. As the major problems with the ticket vending are reselling the ticket at an increased price and replication of the tickets, these problems are solved using the proposed model.

13.2 Literature Survey

As of now, blockchain technology faces core obstacles related to scalability, regulatory limits, identity registration, consumer protection, laws and regulations, and compliance requirements [12, 13]. This chapter is written based on the literature of the previous research, combined with the benefits and the drawbacks of the scheme, proposed a ticket booking system that is decentralized and supported by blockchain technology. The proposed model resolves the problems in this field using the supply chain management and it can trace the ticket and previous buyer's information available in the chain nodes [14–16]. The design presented solves the matter within the

current issues of ticket frauds and ticket traceability process with information stability among the availability chain nodes [17]. The ever-growing greed for money is also increasing along with the current progress of science and technology, leading to a rise in the number of scam and fraud cases. The current understanding of blockchain technology helps us make the world a better place by inhibiting scams in multiple fields [1]. This chapter consists of research from various papers and the main idea for this chapter comes from a lack of transparency and clarity in the transactions in the event management field [6]. This takes place mainly due to the anonymity of any user of the internet and the comforts of the internet. In light of recent events, it has been noticed that counterfeiting is increasing at an alarming rate, and to control this in the event management field, we are using blockchain for making various versions of a single ticket required for attending events [2]. The key fact here is that even the user who purchased a ticket can be accessed by him/her only before a stipulated time of the event. The non-editable property of the data on the blockchain assures that the tickets cannot be replicated by any means owing to the immutable property. The smart contracts and the properties of the blockchain assure the security of the ticket [18]. The main drawback of this model is that there can be a delay in scanning the dynamic QR code, only if there is a large crowd there is a time delay [19]. The papers we referred to and the insights we took from there are as follows: Li et al. [20] have suggested a peer-to-peer networking architecture which will help the customer understand the logistic information in real-time using a decentralized approach to ensure clarity in the distribution of data in an up-to-date and timely manner. Ye et al. [21] also took into consideration the encryption of personal data security which allowed businesses to avoid divulging sensitive data when exchanging the personal information and ensuring that the information was accessible transparently, traceable, and immutably. Lu and Xu [7] carried out a traceability procedure utilizing the blockchain technology backed shared protocol, however, they did not take into consideration the additional benefit of the blockchain through the existing structure and hence the application of clever contracts. Salah et al. [9] suggested a way to follow up and carry out transfers without the need for a trustworthy third-party entity using an Ethereum blockchain of smart contracts.

Since the research done on blockchain to be used in the event management field is still developing, there are not many platforms in the market that use the chain information management systems which are supported by blockchain technology, the theoretical research on the blockchain is yet to improve.

13.3 Preliminaries

In this section, we discuss some of the detailed key points that are relevant and important for the sake of understanding this chapter.

What is a blockchain?

Blockchain is one of the booming technologies that is gradually becoming more prominent [15]. A blockchain can be described as a combination of a distributed ledger database and a consensus algorithm that gives it certain characteristics like distributed, decentralized, immutability, integrity, tamper-proof, etc. [22]. This records all the transactions that have occurred in a network in the form of logs that are verified and authenticated by the nodes in the network, making the entire procedure transparent and irreversible.

This technology came into existence about 10 years ago when the cryptocurrency Bitcoin was first introduced [23]. Now, blockchain technology is not only being used in cryptocurrency but is also used in many applications such as the medical industry, supply chain management, the travel industry, and many more [14, 24, 25]. It can broadly be divided into permission-less and permissioned blockchain, where the permission-less or public blockchain is entirely decentralized as a node can enter and leave a network at any point in time [26]. Whereas, the permissioned blockchain which is further classified into private and consortium blockchains, has restrictions regarding certain decisions to be taken in the network.

What are the Ethereum and smart contracts?

Most people go by the misconception that Ethereum and bitcoins are the same but in reality, the only similarity they share is cryptocurrency [27]. Bitcoin is a cryptocurrency that is not Turing-complete and Ethereum, being Turing-complete generates a cryptocurrency token named Ether [28]. However, Ethereum is also a decentralized platform that runs smart contracts and can be used to replace internet third parties [12, 29]. The other major difference is that the nodes of the network store all the ether transactions along with the most recent state of each smart contract.

A smart contract is a self-executing piece of code containing the terms of the agreement between different parties [13]. These contracts can be written in specific high-level languages like solidity, which are then compiled into bytecode that can be read and executed by Ethereum Virtual Machine (EVM) [17]. In short, smart contracts are special applications that run on EVM [30]. Once these contracts are deployed on the blockchain, they will be executed according to the predefined set of rules after which, no one can make any changes to it.

What are tokens?

A token can be used as a tool for managing the rights of any existing physical or digital asset or to transfer the rights to assets owned by someone else [16]. A token can represent anything. The cryptographic tokens are issued using smart contracts that are deployed onto the blockchain.

13.4 System Overview

As you can see in Fig. 13.1, the blockchain-built traceability system explained in this chapter consists of organized entities such as users and events. Every node within the network correlates to an Ethereum account, that represents its identity within the system and it might not deploy the smart contracts. The organized entities within the chain can be reviewed as Admin, Organizer, Events, User, and Tokens. The functions of each of the following nodes are as follows:

Admin: Admin is the head of the department who plays a key role in this supply chain network. Admin provides a web platform where the user can register for an event that he has to attend and at the same time mints the tokens to the token entity. Admin forms an agreement with the organizer who wants to organize the event.

Organizer: As a middleman in the process of forming an agreement with the admin and organizing the event, the organizer is responsible for conducting events and

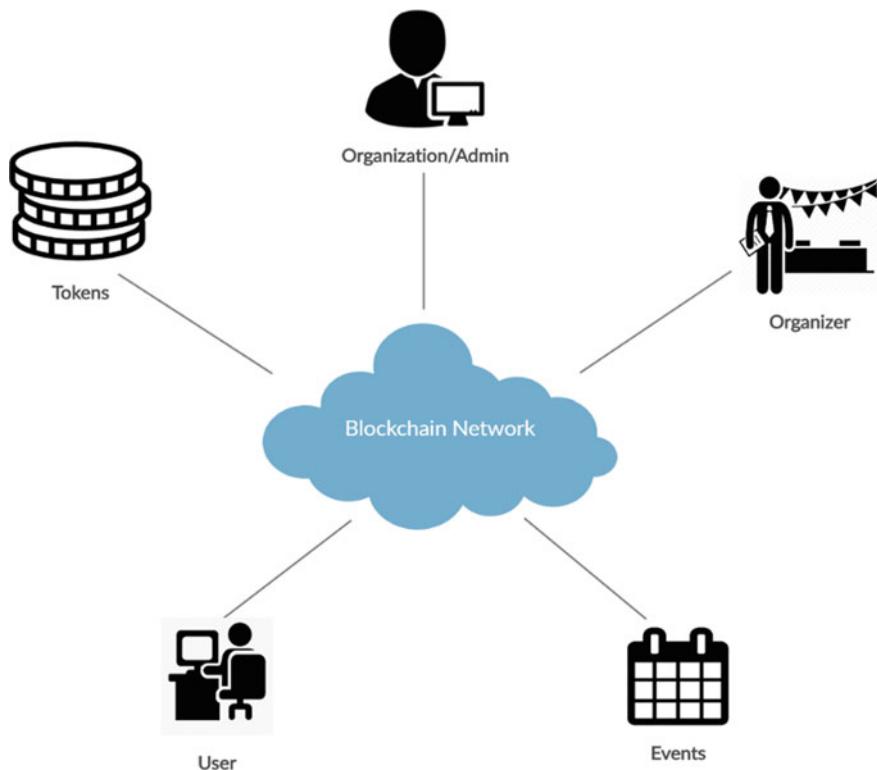


Fig. 13.1 An overview of the participants in the system of the solution proposed

managing all the process planning for the event. When an organizer forms an agreement with the admin, he will share every detail about the event with the admin so that the application can be tweaked to display the right details for the usage of customers.

Event: In the workflow, the event is the entity that provides the details of the event such as type of event, venue, date of the event, etc. to the users who want to register and book their tickets.

User: User is the individual who finally decides whether he wants to attend the event or not. The user signs up on a website provided by the admin by giving his details such as his name, phone number, email, etc. Instead of giving his card details for booking tickets, the user first pays the fiat cash using a gateway where this cash is received and in turn, the value of the token in the e-wallet is changed, this token is assigned to the user in an e-wallet provided by the admin at the time of registration.

Token: This is the entity which allows the transfer of ownership of the ticket(s) from the admin to the customer, this token is assigned to the user when he creates his account in the application. The user can change the value of the token by spending fiat currency or he can also change the value by spending the deposited amount for buying a ticket to any specific event.

Ticket: In the form of a QR Code, this is the most essential part of gaining access to any event, the code is scanned at the event and the ticket holder is allowed into the event. This is generated using the id of the customer and the details of the events. This data is converted into a QR code and this is shown to the customer only before a stipulated time of the event commencement, this is done so that there is no duplication of the code.

13.4.1 Activity Diagram

Figure 13.2 depicts the activity diagram for the event ticket booking system in which the flow between the activity of signing up, minting of tokens, organizing the event is portrayed, and finally generates a dynamic QR code.

The main activities involved in this activity diagram are as follows: Sign up activity, Choosing event activity, Payment activity.

Signup activity: The signup activity allows users to log in or create an account on a particular website. The user should provide his details (name, phone number, email id), by doing this the user account gets created. Once the user creates his account, an OTP will be sent to his registered phone number/email id. Once the user enters the password, his account gets created on the website and the user can proceed to the next forum.

Choosing event activity: After signing up successfully, the user can set the location and select the choice of the event that he wants to attend. Once he selects the event

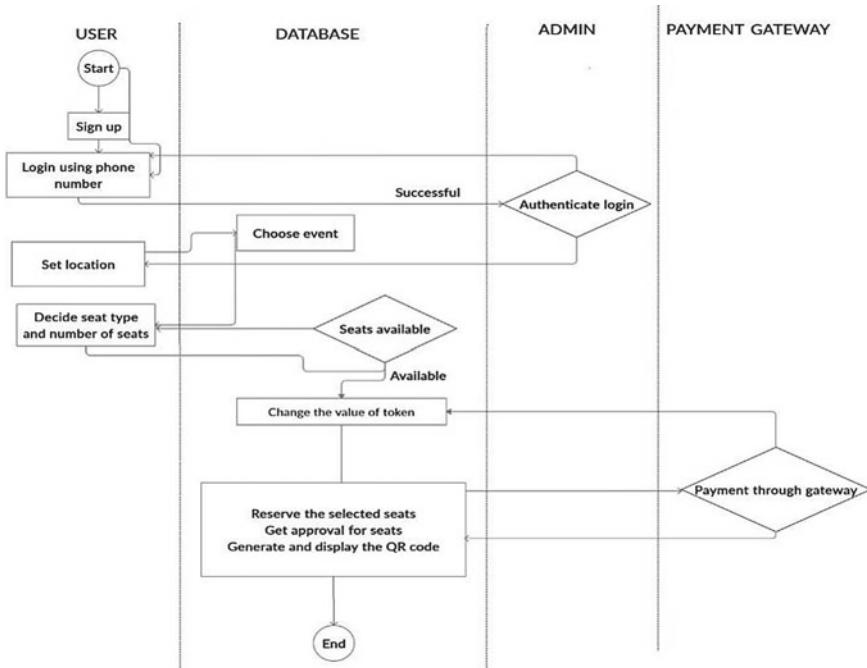


Fig. 13.2 The activity diagram showing the activities carried out as a part of this solution

of his choice, he then has to select the number of seats required and check if they are available or not.

Payment: The most important phase of this proposed model where there is no involvement of third parties in the exchange for the currency. Once the user reaches this stage instead of paying the amount through the card on an online portal, he will have to pay fiat cash to the organization department from where the tokens are minted and will be credited into the user's wallet which is assigned to each user who signs up. When the tokens are received, the user can do the payment through the gateway and if the payment is successful the user will get a message of confirmation details to his mobile number, and finally, the QR code gets generated and will be displayed on the ticket.

Features of the activity diagram for the event ticket booking system include all the objects (sign up, choosing an event, payment) that are interlinked. Users will be able to register for an event by signing up on the online portal. The value of the token changes every time there's a fiat payment. Tokens are minted and assigned only when a new user signs up, once a token is received and confirmed by the database, the user can reserve the seats, get approval for them, and finally view the dynamic QR code, which shows the full description and flow of booking a ticket, updating token value and payment for the seats.

13.4.2 Use Case Diagram

This use case diagram shown in Fig. 13.3 is a graphical depiction of the interactions among the entities of the event ticket management system. It represents the plan used in the system analysis to fetch, clarify, and organize the system requirements for the model proposed. The main 4 actors involved in this process include user, admin, database, and payment gateway.

User: The use case of a user includes signing up if he/she is new to the web platform. Log in if he/she is an existing user and authenticate whether the user is a valid person or not. Once the user is directed to the website, his/her next task is to select a location, choose the event, check if the seats are available and if they are available then select the type and number of seats required by the user. Once everything is done, the user should pay fiat cash to increment the value of their token through which the tickets can be bought.

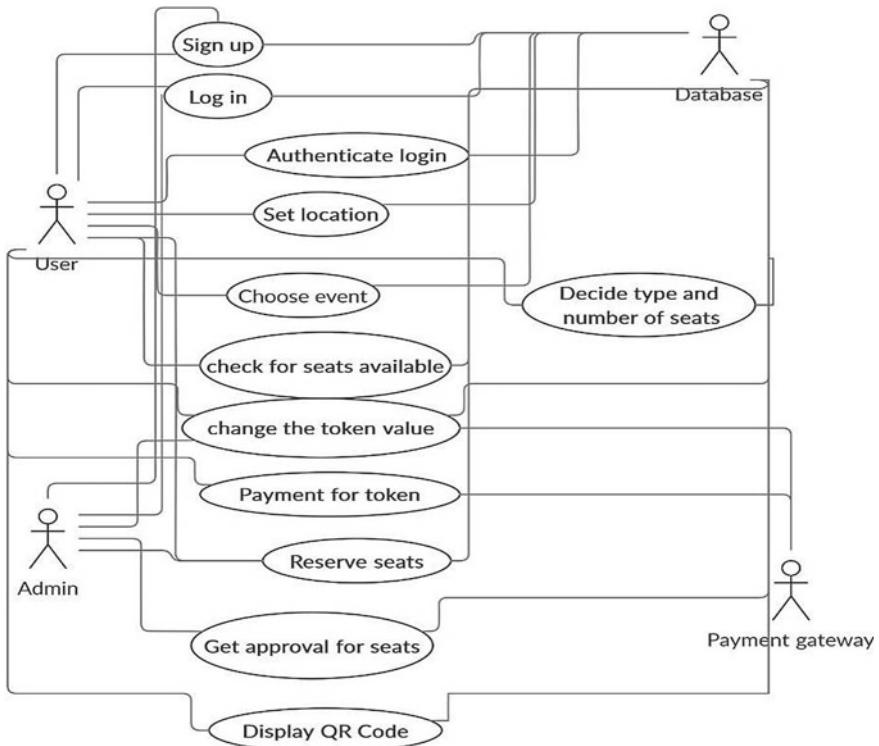


Fig. 13.3 The activity diagram showing the activities carried out as a part of this solution

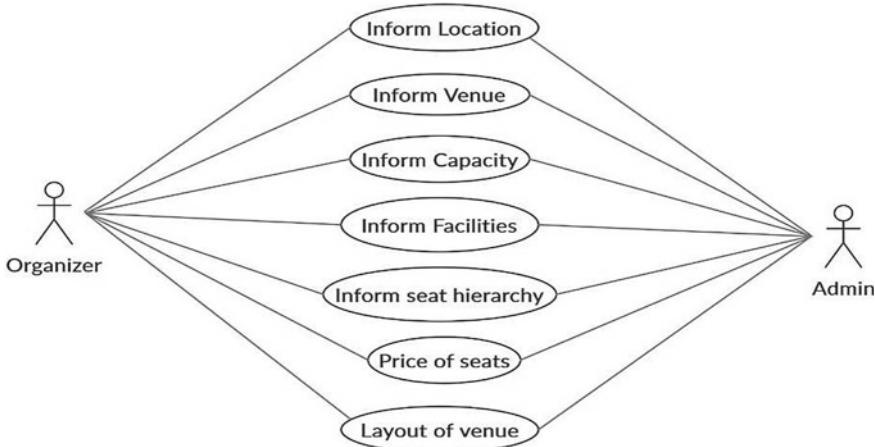


Fig. 13.4 Use case description between admin and organizer

Database: The main objective of the database is to store each information provided by the user and the admin and once the payment is successful display the QR code to the user.

Admin: The use case of an admin includes signing up, and responding to the user's actions such as reserving the seats, getting approval of seats.

Payment Gateway: The use case of a payment gateway is to verify the fiat cash payment made by the user to increment the value of their token so that they can purchase the required ticket/s.

Figure 13.4 depicts the various interactions between the admin and the organizer which are explained below in detail. The relation between the admin and the organizer must be clear and strong for the successful organization of any event without any miscommunication or difference of opinions.

For that to happen, the organizer must inform the admin about the venue and location of the event. They must also inform the capacity, facilities, seat hierarchy, and layout of the venue. Along with these details, the price of each seat/ticket must also be discussed with the organizer so that the individual profits can be decided upon with mutual agreement.

The proposed model (Fig. 13.5) described in this chapter mainly includes organized entities and users which are secured through a decentralized network. The enterprise entities include organizers, organizations, events, and tokens. The responsibility and individual roles of every network are given as follows.

Organization Department: The organization department is the head of the department where the procedure of minting tokens is decided and the procedure of forming an agreement with the event organizer takes place. In this department, the particular organization member is going to provide his name, email id, and phone number

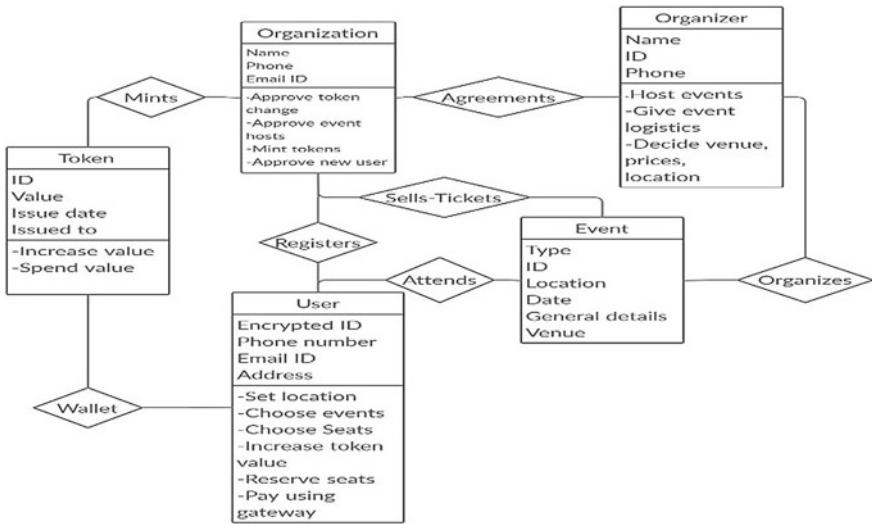


Fig. 13.5 The class diagram describing the properties of the various entities

(which is the primary key). These details are only visible to the organizer who wants to agree with the organization member.

Organizer Department: The organizer's work is to organize an event. They will handle the whole process of planning an event and carrying on post-event evaluation. This organizer shares his name, phone number, and email id with the organization department and each organizer has a unique ID (primary key) which helps the organization department to identify what type of event is being organized and it helps in forming an agreement signed between the organizer and the organization.

Event Department: This department includes the details about the event name, the event type, venue of the event, date of the event. Even this department has a unique ID (primary key) which allows the organizer to refer to the event and its details.

Token Department: This is the department in which the value of the tokens is updated when the user pays the fiat cash for purchasing an event ticket. Tokens will only be minted when there's a new user and these minted tokens will be added into the user's wallet. It keeps the record of how much value has been spent and keeps changing the value.

User Department: This department takes care of storing the details like name, phone number (primary key), email id, address provided by the user at the time of signing up, and assigns each user with a unique ID that is encrypted. This ID contains the details of the user and helps maintain their identity. After the user is registered, they are provided with a unique e-wallet that has a token and the unique ID linked to it. Whenever a user wants to book a ticket, he needs to login onto the online portal and pays the fiat currency to update the value of his token in the wallet. The user can then

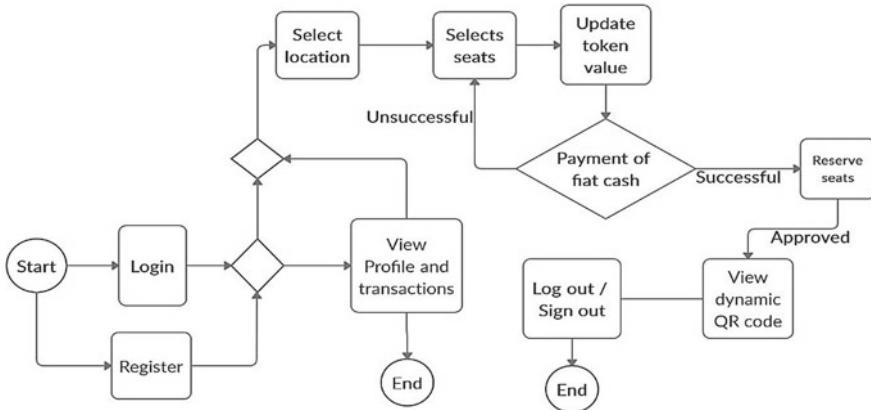


Fig. 13.6 The state-chart description

pay for the ticket using the token and the generated dynamic QR code is sent to the user's registered phone and the value of the token is changed accordingly.

The above state (Fig. 13.6) diagram represents the flow of the process a user has to follow to be able to log in, book a ticket, and exit the application. Firstly, the user would have to register by entering all the details in the designated boxes, if registration is over, then the user can directly login using the username and password designated to the user during the registration process.

The user can check his previous transactions, the user can also book tickets by setting the location which is comfortable to the user. He can then decide on which event he wants to go to and he has to select the seats in the event.

After this, he has to update the value of the token using the payment gateway. Using the updated token, he can buy the tickets for the value in the token. After paying for the seats, the seats will get reserved under your name. The user will receive a QR code that can be scanned at the venue of the event. After receiving the QR code the user can then decide to log out of the application to exit it.

13.5 Smart Contracts

We have designed three smart contracts, they are User Registration contract, Wallet contract, and Ticket Update contract for the sake of our model. The user registration contract holds the address of the wallet contract, and the wallet contract holds the address of the ticket update contract such that the contracts are linked to each other and coordinated. In the user registration contract, every user is designated with a wallet contract address when they register on the platform. In the wallet contract, the user can update the value of the token possessed by the user's wallet. In the ticket update contract, the user is given ownership over a ticket after the user meets the

required criteria. Any user can inquire about the transfer history of the acquired ticket to verify the authenticity of that ticket. The individual functions of each contract are as follows:

User Registration Contract: This contract is deployed by the admin. Furthermore, it provides a user registration function register() which stores the registration information of each user forever. The user provides information like name, phone number, email, etc. and gets registered through a unique code (OTP) sent to the user's unique phone number. As soon as the user is registered, this contract will deploy the wallet contract with the current user's address. This will assign the current user with an e-wallet that is linked to the user's address in the user registration contract.

Wallet Contract: This contract is deployed by the user after registration and it provides the function addWallet(). The wallet assigned to the user will contain a token whose initial value is zero. This contract also contains another function buyToken() through which the value of this token can be incremented after the user's payment has been verified at the payment gateway. After the buyToken() function is executed, the ticket update contract is deployed. This contract provides the function of assigning and updating the ownership of the tickets.

Ticket Update Contract: This contract is deployed after the buyToken() function is executed and it provides the functions buyTicket() which decrements the value of the token assigned to the wallet owned by the user and updateTicket() which updates the owner of the ticket. If the ticket is purchased for the first time, the QR code is also attached, otherwise, the hash of the previous transaction is referred. The acquired transaction information is added to the list of transaction records managed in this contract, including the hash of the current buyer of the ticket, the seller of the ticket, the previous transaction's hash, and timestamp.

Note: The list of transactions will only be revised if the current transaction is completed successfully and it will be linked to the blockchain if the previous transaction's hash is valid; else, an exception/error occurs. This guarantees that every transaction added to the block is credible and legit, prohibiting the selling of false tickets or multiple copies of a ticket.

13.5.1 Algorithms

Following is the explanation of the five algorithms that we have used as per the solution.

Algorithm 1 register()

Input: Message sender (msg.sender), username (username), phone number (phonenumer), Email (emailID), current timestamp (now), authorization list (authlist), user count (usercount), wallet contract address (wcaddr) (Fig. 13.7).Please check and confirm if the inserted citations of Figs. 13.7–13.11 are correct. If not, please suggest an alternate citations. Please

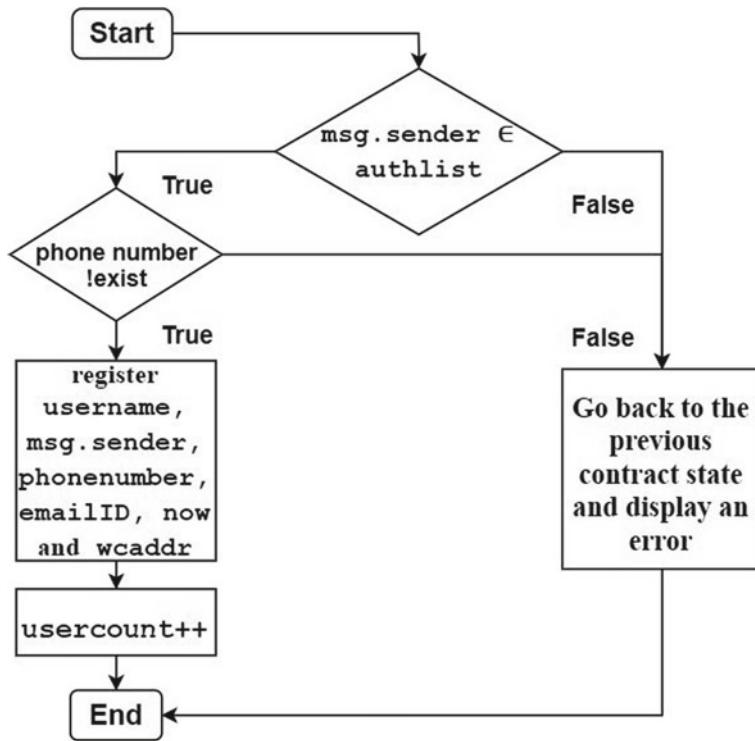


Fig. 13.7 The decision chart for Algorithm 1

note that figures should be cited sequentially in the text. All the inserted citations of figures from 13.7-13.11 are correct.

Explanation

The function `register()`, represented in Algorithm 1 allows a new user to register on the online platform. This function takes the following inputs: message sender (`msg.sender`), username (`username`), phone number (`phonenumer`), email (`emailID`), current timestamp (`now`), authorization list (`authlist`), user count (`usercount`), and wallet contract address (`wcaddr`).

Here, the authorization list includes the list of all accredited user's Ethereum addresses in this contract. If the message sender's address matches any address in the authorization list, then the algorithm will check to see that no user with this phone number has already registered. If both of these conditions are satisfied, then the algorithm will register this user on the platform and stores the details like the `username`, `msg.sender`, `phonenumer`, `emailID`, `now` and `wcaddr` to the blockchain. The algorithm will then increment the count of the users by incrementing `usercount`.

If either one of the conditions fails, then the state of the contract is reverted, an error is shown and the user is not registered. Once a user is registered, he/she can then use all the facilities provided on the platform.

Algorithm 2 addwallet()

Input: Message sender (msg.sender), username (username), phone number (phonenumbers), Email (emailID), current timestamp (now), authorization list (authlist), user count (usercount), wallet count (walletcount) (Fig. 13.8).

Explanation

The function `addWallet()` described in Algorithm 2 is used to assign every user with a unique e-wallet which contains a token whose initial value is zero. This function takes in the following inputs: message sender (`msg.sender`), username (`username`), phone number (`phonenumbers`), email (`emailID`), current

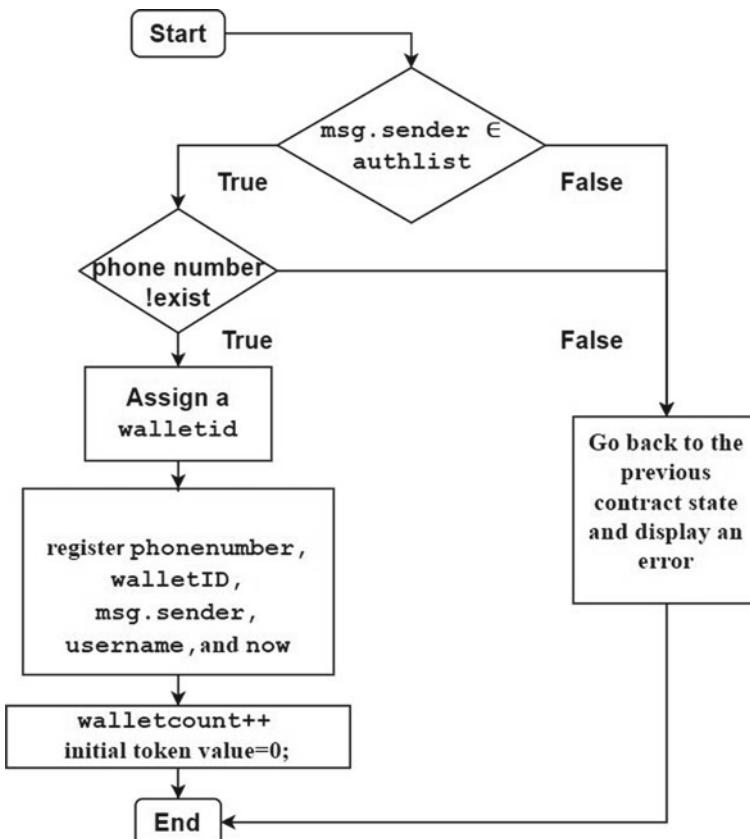


Fig. 13.8 The decision chart for Algorithm 2

timestamp (now), authorization list (authlist), user count (usercount), and wallet count (walletcount).

Here, the authorization list includes the list of all accredited user's Ethereum addresses in this contract. If the message sender's address matches any address in the authorization list, then the algorithm will check to see that no user with this phone number has already registered. If both of these conditions are satisfied, then the algorithm will assign an e-wallet and every user will have a unique wallet id. Then, the phonenumbers, walletID, msg . sender, username, and now are added to the blockchain, linking the wallet to the user. The algorithm will then increment the count of the wallets by incrementing walletcount and the initial value of the token is made equal to zero.

If either one of the conditions fails, then the state of the contract is reverted, an error is shown and the wallet is not assigned. Once a user is assigned a wallet, he/she can use the platform to purchase tickets to any event via the tokens.

Algorithm 3 buytoken()

Input: Message sender (msg . sender), phone number (phoneNumber), money paid (moneypaid), wallet ID (walletID), token value (tokenValue), authorization list (authlist), ticket update contract address (tucaddr), current timestamp (now) (Fig. 13.9).

Explanation

The function buyToken() represented in Algorithm 3 is used to increment the value of the token in the wallet of the user after the fiat currency payment has been verified by the payment gateway. This function takes the following inputs: message sender (msg . sender), phone number (phoneNumber), money paid (moneypaid), wallet ID (walletID), token value (tokenValue), authorization list (authlist), ticket update contract address (tucaddr), and current timestamp (now).

Here, the authorization list includes the list of all accredited user's Ethereum addresses in this contract. If the message sender's address matches any address in the authorization list, then the algorithm will check to see that the user with this wallet id and phone number is already registered. If both of these conditions are satisfied, then the algorithm will increment the value of the token with the amount of fiat currency paid after this payment is verified at the payment gateway. Then the walletID, phoneNumber, tokenValue, now, msg . sender, moneyPaid, and tucaddr are added to the blockchain.

If either one of the conditions fails, then the state of the contract is reverted, an error is shown and the value of the ticket is not incremented. Once the value of the token is incremented concerning the fiat currency payment made, he/she can then book the tickets for any event on the online platform.

Algorithm 4 buyticket()

Input: Message sender (msg . sender), phone number (phoneNumber), event name (eventname), wallet ID (walletID), token value

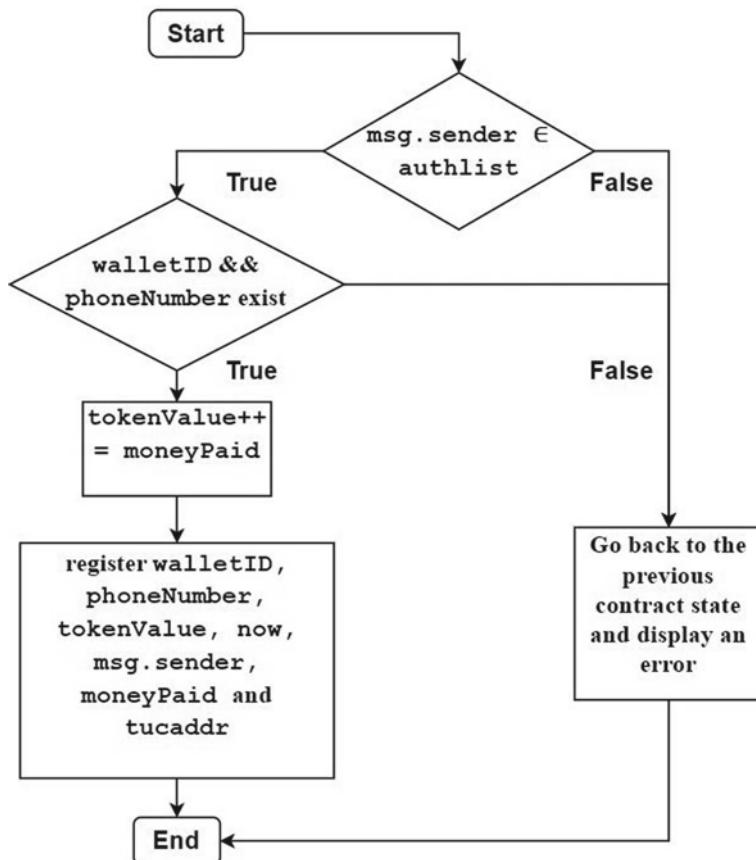


Fig. 13.9 The decision chart for Algorithm 3

(`tokenValue`), authorization list (`authlist`), current timestamp (`now`), ticket cost (`ticketcost`) (Fig. 13.10).

Explanation

The function `buyTicket()` represented in Algorithm 4 allows a user to buy tickets for any event that is available on the online platform by consuming the value of the token in the user's wallet. This function takes the following inputs: message sender (`msg.sender`), phone number (`phoneNumber`), event name (`eventname`), wallet ID (`walletID`), token value (`tokenValue`), authorization list (`authlist`), current timestamp (`now`), and ticket cost (`ticketcost`) (Fig. 13.11).

Here, the authorization list includes the list of all accredited user's Ethereum addresses in this contract. If the message sender's address matches any address in the authorization list, then the algorithm will check to see that the user with this wallet id and phone number is already registered. After this, the algorithm will verify the

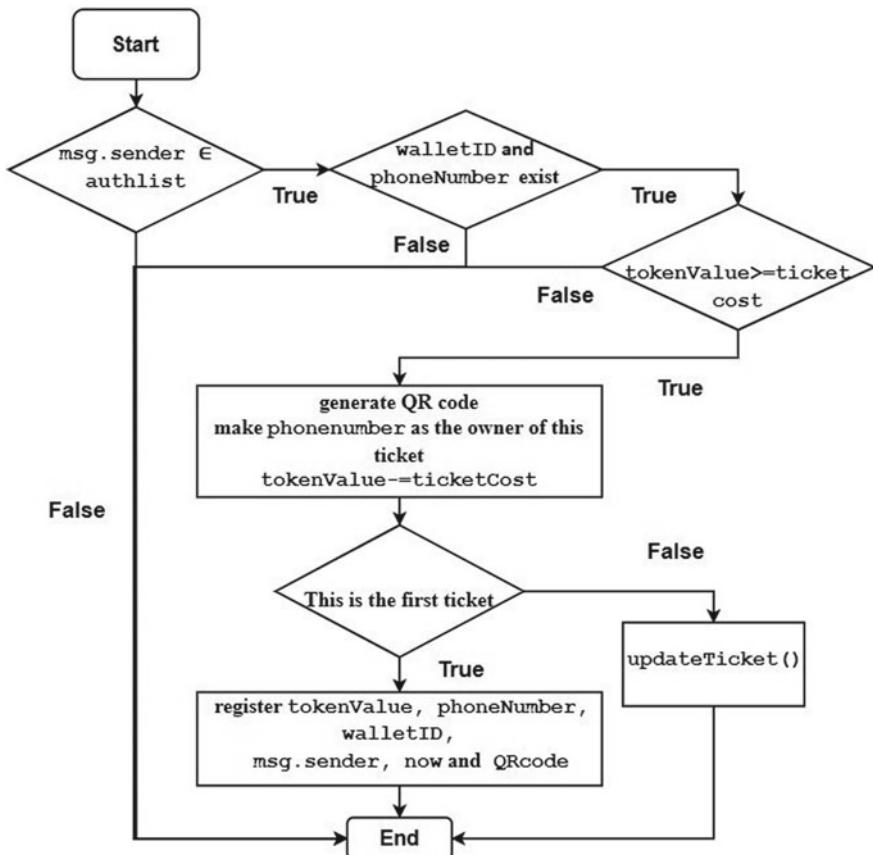


Fig. 13.10 The decision chart for Algorithm 4

value of the token to be greater than or equal to the cost of the ticket. If all the three conditions are satisfied, then the algorithm will generate a QR code and make the user the owner of the ticket, keeping the phone number as the main constraint. The value of the ticket cost is subtracted from the value of the token and the final token value is updated.

If this user is the first owner of this ticket, then the `tokenValue`, `phoneNumber`, `walletID`, `msg.sender`, `QRcode`, and `now` are added to the blockchain, otherwise, the `updateTicket()` function is called. If either one of the conditions fails, then the state of the contract is reverted, an error is shown and the user does not get the ownership of the ticket. Once the ownership of the ticket is given to the user, he/she can use this to either attend the event or sell it to another user at a cost not more than the original ticket cost.

Algorithm 5 `updateticket()`

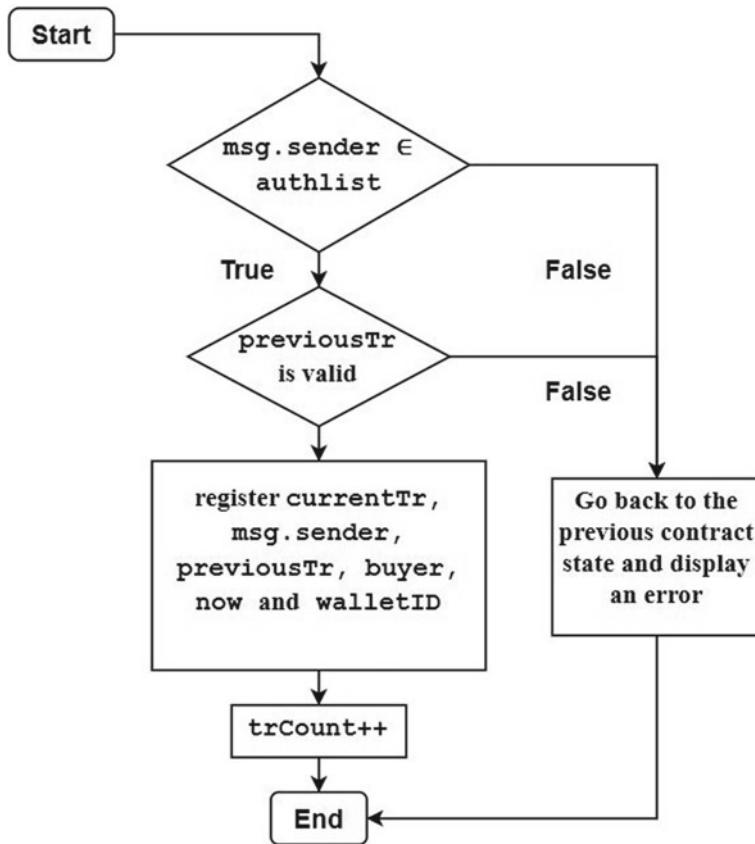


Fig. 13.11 The decision chart for Algorithm 5

Input: Message sender (`msg.sender`), buyer's address (`buyer`), current transaction (`currentTr`), previous transaction (`previousTr`), authorization list (`authList`), transaction count (`trCount`), seller's wallet id (`walletID`), current timestamp (`now`).

Explanation

The function `updateTicket()` represented in Algorithm 5 allows the transfer of ownership of the ticket between various users. This function takes the following inputs: message sender (`msg.sender`), buyer's address (`buyer`), current transaction (`currentTr`), previous transaction (`previousTr`), authorization list (`authList`), transaction count (`trCount`), seller's wallet id (`walletID`), current timestamp (`now`).

Here, the authorization list includes the list of all accredited user's Ethereum addresses in this contract. If the message sender's address matches any address in the authorization list, then the algorithm will check to see that the previous transaction is

valid in the blockchain. If both of these conditions are satisfied, then the algorithm will log `currentTr`, `msg.sender`, `previousTr`, `buyer`, `now`, and `walletID` to the blockchain. The algorithm will then increment the count of the transactions by incrementing `trCount`. If either one of the conditions fails, then the state of the contract is reverted, an error is shown and the buyer is not given the ownership of the ticket. Once the ownership of the ticket is given to the buyer, he/she can use this to either attend the event or sell it to another user at a cost not more than the original ticket cost and the seller no longer owns any right over this ticket.

13.6 Security Analysis

The blockchain traceability system proposed in the chapter meets the following security requirements [31, 32]:

Data accessibility: As the system can be viewed to anyone, users can access the system to see data related to their transactions and bookings.

Sale of non-valid or invalidated tickets: In today's world, it has become easy to produce a copy of the tickets without valid identifiers, but when it comes to blockchain based-solutions it is close to impossible to replicate the tickets. The system proposed allows only authorized tickets to be stored in the ledger. Once the ticket is identified as an invalid ticket, the re-selling of the ticket is not allowed by the chain code and the indivisibility which is vowed by the blockchain makes sure of a consistent state for each ticket [33].

Data immutability: The selling of paper tickets allows a person to make copies of the tickets and sell them to different buyers. The proposed model has a tamper-proof functionality to provide true and reliable data to the users.

System autonomy: The data that gets exchanged in the system follows a fixed algorithm, the nodes that are present in the system will exchange, record, and update data on their own without any human interference [34].

Opposition to 3rd party attack: Since blockchain is a decentralized system, the nodes within the system mutually cannot be trusted. Therefore, the system resists 3rd party attacks and prevents malicious nodes from producing false transactions [35].

From a conceptual point of view, the proposed model need not require a blockchain. For every ticket, there should be a trustworthy organizer to allow the owner of the ticket to enter the event. But when it comes to a non-theoretical point of view, however, blockchain allows the organizer to deploy the application to multiple providers, trusting them fully.

Moreover, it seems fair for the organizer to run such a system hand in hand which lets an increase in resilience by earning trust in their infrastructure and improves user's encounter by producing all valid tickets being governed in a single application.

13.7 Conclusions and Future Works

It has become easy for the scammers to make a copy of a legally-acquired ticket and replicate the same QR code which helps them in making illegal profits by selling multiple fake tickets to the users via online platforms or at the event venue. In this scenario, using blockchain provides a guarantee that the ticket the users are going to receive is indeed valid and is not a counterfeit or copied ticket. The proposed prototype shows how blockchain technology helps in recording this step-by-step procedure in a ledger which cannot be changed with the help of smart contracts and therefore the process of event registration, minting of tokens, and generating QR code is conceived through the combination of smart contracts. The proposed system has some evident decentralized characteristics, which at second hand reduces the chances of altering data within the enterprises. All the occurrences can be listed and safely stored in the blockchain via a log. The outcome of the security analysis shows how the proposed model is identified by data accessibility, sale of non-valid or invalidated tickets, system autonomy, and opposition to 3rd party attack.

For the betterment of the traceability system suggested in this chapter, future work could be dedicated to enhancing the proposed prototype by:

1. recognize formatted upload of data with the help of IoT technology to reduce the chances of manual internal inputs,
2. to make the whole prototype fully automated with no human interaction using AI or ML.

References

1. Konstantinidis, I., Siaminos, G., Timplalexis, C., Zervas, P., Peristeras, V., Decker, S.: Blockchain for business applications: a systematic literature review. In: Abramowicz, W., Paschke, A. (eds.) *Business Information Systems. BIS 2018. Lecture Notes in Business Information Processing*, vol. 320. Springer, Cham (2018)
2. Toyoda, K., Mathiopoulos, P.T., Sasase, I., Ohtsuki, T.: A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain. *IEEE Access* **5**, 17465–17477 (2017)
3. AXS: Ticket selfie equals ticket theft unless you have id-based, digital tickets. <https://www.theguardian.com/money/2016/mar/21/online-ticket-fraud-social-media-users-warned-twitter-facebook-get-safe-online>
4. Koblitz, N., Menezes, A.J.: Crypto cash, cryptocurrencies, and crypto contracts. *Des. Codes Cryptogr.* **78**, 87–102 (2016). <https://doi.org/10.1007/s10623-015-0148-5>
5. Fan, K., Wang, S., Ren, Y., Li, H., Yang, Y.: MedBlock: efficient and secure medical data sharing via blockchain. *J. Med. Syst.* **42**(8), 136 (2018)
6. Hasan, H.R., Salah, K.: Blockchain-based solution for proof of delivery of physical assets. In: Chen, S., Wang, H., Zhang, L.-J. (eds.) *ICBC 2018. LNCS*, vol. 10974, pp. 139–152. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-94478-4_10
7. Lu, Q., Xu, X.: Adaptable blockchain-based systems: a case study for product traceability. *IEEE Softw.* **34**(6), 21–27 (2017)

8. Jones, R.: Social media users warned over a rise in online ticket fraud (December 2015). <http://solutions.axs.com/ticket-selfie-equals-ticket-theft-unless-you-have-id-based-digital-tickets/>
9. Salah, K., Nizamuddin, N., Jayaraman, R., Omar, M.: Blockchain-based soybean traceability in the agricultural supply chain. *IEEE Access* **7**, 73295–73305 (2019)
10. Tackmann, B.: Secure event tickets on a blockchain. In: Garcia-Alfaro, J., Navarro-Arribas, G., Hartenstein, H., Herrera-Joancomartí, J. (eds.) *Data Privacy Management, Cryptocurrencies, and Blockchain Technology. DPM 2017, CBT 2017. Lecture Notes in Computer Science*, vol. 10436. Springer, Cham (2017)
11. Gencer, A.E., Basu, S., Eyal, I., Van Renesse, R., Sirer, E.: Decentralization in bitcoin and ethereum networks (2018)
12. Nofer, M., Gomber, P., Hinz, O., et al.: Blockchain. *Bus. Inf. Syst. Eng.* **59**, 183–187 (2017). <https://doi.org/10.1007/s12599-017-0467-3>
13. Glomann, L., Schmid, M., Kitajewa, N.: Improving the blockchain user experience—an approach to address blockchain mass adoption issues from a human-centred perspective. In: Ahram, T. (ed.) *Advances in Artificial Intelligence, Software and Systems Engineering. AHFE 2019. Advances in Intelligent Systems and Computing*, vol. 965. Springer, Cham (2020)
14. Perboli, G., Musso, S., Rosano, M.: Blockchain in logistics and supply chain: a lean approach for designing real-world use cases. *IEEE Access* **6**, 62018–66202 (2018)
15. Lin, Q., Wang, H., Pei, X., Wang, J.: Food safety traceability system based on blockchain and EPCIS. *IEEE Access* **7**, 20698–20707 (2019)
16. Wang, S., Li, D., Zhang, Y., Chen, J.: Smart contract-based product traceability system in the supply chain scenario. *IEEE Access*. pp. 1-1 (2019). <https://doi.org/10.1109/access.2019.2935873>
17. Figorilli, S., et al.: A blockchain implementation prototype for the electronic open-source traceability of wood along the whole supply chain. *Sensors* **18**, 3133–3146 (2018)
18. Zhang, J., et al.: A review on blockchain-based systems and applications. In: Hsu, C.H., Kallel, S., Lan, K.C., Zheng, Z. (eds.) *Internet of Vehicles. Technologies and Services Toward Smart Cities. IOV 2019. Lecture Notes in Computer Science*, vol. 11894. Springer, Cham (2020)
19. Yining, H., et al.: A delay-tolerant payment scheme based on the Ethereum blockchain. *IEEE Access* **7**, 33159–33172 (2019)
20. Li, Z., Wu, H., King, B., Miled, Z.B., Wassick, J., Tazelaar, J.: A hybrid blockchain ledger for supply chain visibility. In: *Proceedings of 17th International Symposium on Parallel and Distributed Computing (ISPD'C)*, Geneva, Switzerland, Aug 2018, pp. 118–125
21. Ye, X., Shao, Q., Xiao, R.: A supply chain prototype system based on blockchain, smart contract and Internet of Things. *Sci. Technol. Rev.* **35**(23), 62–69 (2017)
22. Schiller, K.: Was ist eineDApp (dezentralisierte App), Blockchainwelt. <https://blockchainwelt.de/dapp-dezentralisierte-app-dapps/> (2018). Retrieved 31 Jan 2019
23. Benatia, M.A., Remadna, A., Baudry, D., Halftermeyer, P., Delalin, H.: QR-code enabled product traceability system: a big data perspective. In: *Proceedings of 16th International Conference on Manufacture Research (ICMR)*, Skövde, Sweden: University, Skövde, Sept 2018, pp. 323–328
24. Guts, B.V.: Guts tickets (2017). <https://guts.tickets>
25. Buterin, V., Di Lorio, A., Hoskinson, C., Alisie, M.: Ethereum: a distributed cryptographic ledger (2013). <http://www.ethereum.org/>
26. Szabo, N.: Smart contracts: formalizing and securing relationships on public networks. *First Monday* **2**(9) (1997). <https://doi.org/10.5210/fm.v2i9.548ljdf>
27. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system. Bitcoin.org, White Paper, 2008
28. Barber, S., Boyen, X., Shi, E., Uzun, E.: Bitter to better—how to make bitcoin a better currency. In: *International Conference on Financial Cryptography and Data Security*. Springer, Heidelberg, pp. 399–414 (2012)
29. Croman, K., Decker, C., Eyal, I., Gencer, A.E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., Gun Sirer, E., Song, D., Wattenhofer, R.: On scaling decentralized blockchains. *3rd Workshop on Bitcoin Research (BITCOIN)*, Barbados (2016)

30. Alharby, M., van Moorsel, A.: Blockchain-based smart contracts: a systematic mapping study, 125–140 (2017). <https://doi.org/10.5121/csit.2017.71011>
31. Singh, S., Singh, N.: Blockchain: future of financial and cybersecurity. In: Proceedings of 2nd International Conference on Contemporary Computing and Informatics (IC3I), Noida, India, Dec. 2016, pp. 463–467
32. Tracking Platform Test. Accessed 18 July 2019 (Online). Available: <https://github.com/snowby-ldy/eth-traceabilityplatform>
33. Meier, A.: Blockchain. HMD55, 1133–1134 (2018). <https://doi.org/10.1365/s40702-018-00467-5>
34. Aitzhan, N.Z., Svetinovic, D.: Security and privacy in decentralized energy trading through multi-signatures, blockchain, and anonymous messaging streams. IEEE Trans. Dependable Secur. Comput. (2016)
35. Siddiqui, S.T., Ahmad, R., Shuaib, M., Alam, S.: Blockchain security threats, attacks, and countermeasures. In: Hu, Y.C., Tiwari, S., Trivedi, M., Mishra, K. (eds.) Ambient Communications and Computer Systems. Advances in Intelligent Systems and Computing, vol. 1097. Springer, Singapore (2020)

Chapter 14

Cloud Identity and Access Management Solution with Blockchain



Soumya Prakash Otta and Subhrakanta Panda

Abstract Present solutions to problems of Cloud Identity and Access Management are costly, inefficient with information duplication across service providers. It also comes with additional overhead for users requiring to keep track of associated credentials of desired services. Securing same is difficult and has resulted in worldwide huge breaches of personal data in recent times. A comparatively new approach is required for identity management with ownership of cloud user and also controlled by cloud user. Blockchain technology decentralize various services, security, and verifiability, by offering a peer to peer system. Particularly Blockchain operates by enforcing continuous storage of various transaction performed that are secured by digital signatures and affirmed through consensus. This chapter provides a detailed and systematic description of blockchain for identity and access management. The specific characteristic features of this technology that could revolutionize the management process are highlighted. Towards this end, comparative study and critical analysis of many approached and related aspects are incorporated. In the chapter, we bring out various shortcomings identified from the studied literature, limiting ourselves to the aspects of blockchain technology and their relevance. For addressing these gaps, our comprehensive study also points out some future directions and further enhancement to the blockchain technology. Depending on such findings, we pin point several research gaps and associated fields that are significant for research aspects.

Keywords Decentralized identity · Identity management · Authentication · Security · Blockchain · Distributed ledger

S. P. Otta (✉) · S. Panda
CSIS Department, BITS Pilani, Hyderabad Campus, Hyderabad, India
e-mail: p2016300@hyderabad.bits-pilani.ac.in

S. Panda
e-mail: spanda@hyderabad.bits-pilani.ac.in

14.1 Introduction

Advancements in communication technologies permit verity of devices to be interconnected over networks. This provides various ways to communicate between systems and users. This is reflected more relevantly in present data enabled society. Simultaneously it has opened areas of concern for vulnerability regarding user privacy, resources authorization, and user authentication. To prevent violations regarding privacy and fraudulent uses, Information Technology (IT) assets require safeguard and proper security mechanisms in place called *Access Control Systems (ACS)*. Such systems are designed to check any attempt for gaining access or granting the desired access for the specific target resources. The need to ensure provisioning of right resources to the legitimate users has opened research areas for *Identity and Assess Management (IAM)*. This is continuously evolving as enterprises face increasingly complex and difficult digital identity problems. With respect to new enterprise philosophies and models, IAM presently a crucial topic for industry and academia. Cloud computing is being rapidly applied to many IT environments due to its availability and efficiency. Importance of IAM in terms of cloud security as well as privacy issues have been deliberated considering vital security aspects namely confidentiality, integrity, authentication and access control.

Access management of resources is a crucial task for any enterprise cloud infrastructure. Significantly in a cloud environment, functionality of Access Control for external systems is made available “as a Service (aaS)” by a *trusted third party (TTP)*. As per Gartner Research report, worldwide cloud infrastructure as a service (IaaS) market has grown 37.3 percent in 2019. Cloud services mostly make use of open platform based *Application Program Interface (API)*, ensuring that users do not get specifically bounded to use any particular implementation. For instance, Amazon users are offered an Access Control Service for IAM towards Amazon Web Services (AWS). Hence Amazon users can manage their access for allowing or denying to corresponding AWS services. There is a possibility that a TTP Cloud Access and Control facility may intentionally trigger deny response from system, thereby denying access to genuine user although enforced policy might have been granted for the same. This could even permit without policy being effectively followed, thereby granting access to a user not having legitimate right.

In blockchain, resource owners as well as subjects are empowered to check and verify each access request that is executed for evaluating policy implementation. Every transaction saved is immutable as every node of network saves all executed transactions involving blockchain. Enciphering means like asymmetric algorithms for encryption, digital signatures as well and hashing function to ensure data integrity are employed. Value of attributes during execution and resulting access decisions generated for corresponding access requests are stored. Hence, blockchain is capable to ensure non repudiation of performed operations. Additionally, all transaction involving blockchain are also traceable to every user with inbuilt timestamp. Notable utilization of blockchain technology for IAM is adequately covered in [14], using Bitcoin methodology for signifying, storing, and retrieving user policies mentioning

rights of users for various resources. This also permit the transfer of right among users originating from any policy changes in the enterprise.

The organization of the rest of the chapter is as follows: Sect. 14.2 provides details of Identity and Access management. Section 14.3 discusses some IAM Concerns. Section 14.4 elaborates Blockchain as a technology and its application to address IAM issues. Open research issues are covered in Sects. 14.5 and 14.6 concludes the chapter.

14.2 Identity and Access Management (IAM)

Conceptually Cloud Computing has evolved from grid computing. This is used for organizing and providing internet-based information technology (IT) management functions for enterprises. Everything is delivered in enterprise computing as service, where the user is required to communicate multiple service providers to perform desired transaction. In this matter, identity federation in Enterprise Computing model, is a security model which facilitate users to log into interconnected and integrated system having single set of credentials for signing on, without considering implementation technologies as well as infrastructure involved.

14.2.1 Access Control System

In cloud environment, ACS is designed for protecting resources of the system. This is done by verification of access requests made from that system for corresponding access events. ACS takes a decision to provide or deny desired rights to perform the accesses being requested. Such rights are denoted by Access Controlling tokens that gets generated from access policies, consisting of various conditions that are verified to take access decision. In some cases, the access rights are not fixed. Hence, this verification is a continuous process for entire time of access. This results in interruption in case this access permission gets expired because of a change in access scenario. Various suggested access control models are *Mandatory Access Control model (MAC)*, *Discretionary Access Control model (DAC)*, *Role Based Access Control model (RBAC)*, *Policy Based Access Control model (PBAC)*, and *Risk-Based Access Control model*.

A detailed analysis that resulted in highlighting of various access control techniques along with their advantages and disadvantages are represented in below mentioned Table 14.1.

Table 14.1 Detailed Comparison Of Access Control Techniques

S. No.	References	Tech name	Observation	Advantages	Disadvantages
1	[2]	Attribute based Encryption	<ul style="list-style-type: none"> (i) Attribute expert creates public key and master key as per attributes (ii) The data owner encodes data with a public key and arrange attributes (iii) Client decodes encrypted data with its private key, sent from issuing authority and deciphered data is obtained 	<ul style="list-style-type: none"> (i) Collusion resistance in pivotal state and security level is highest (ii) Minimize the communication overhead 	<ul style="list-style-type: none"> (i) To Encrypt Data, data owner required to use legitimate users public key
2	[4]	Role Based Model	<ul style="list-style-type: none"> (i) The data protector mechanism encodes data of cloud with encryption strategy and conceals access to clients having specified roles (ii) Particular set of role are defined. Users are allocated with every role having set of permissions 	<ul style="list-style-type: none"> (i) This system provides additional provisioning, more efficient access control and administration with minimal representative downtime (ii) ABE are difficult to set up and complex to deal with. Access complexity is made robust by Role based encryption strategy 	(continued)

Table 14.1 (continued)

S. No.	References	Tech name	Observation	Advantages	Disadvantages
3	[23]	Identity Based Authentication	<p>(i) Identity framework creates identity functionality with many to many correspondences</p> <p>(ii) Trusted outsider creates a private key</p> <p>(iii) Public key is distributed as users' public key and user can process private key by joining public key. In this way client can decrypt data</p> <p>(iv) In this method pre appropriation of verified secret key is not feasible. Hence distribution among users is not required</p>	<p>(i) Complexity of encoding process can reduce</p> <p>(ii) Certificates are not required</p> <p>(iii) Pre enrollment is not required</p> <p>(iv) No need to revoke key because of key expiry</p>	<p>(i) Safe channel between user and private key generator is required</p> <p>(ii) Encrypted data is decoded just by one user hence this needs advance information sharing</p>

(continued)

Table 14.1 (continued)

S. No.	References	Tech name	Observation	Advantages	Disadvantages
4	[28]	Key-Policy Based Access Control	<p>(i) Encrypted data is stacked with attribute and every user having those attribute can only decode</p> <p>(ii) In Key Policy based and Attribute Based Encryption, cipher text are related with an arrangement of clear attributes while trusted in quality authority generate and issues private key to client which has a strategy that indicates which all cipher texts this particular key can decipher</p>	<p>(i) Simple to manage user revocation key</p> <p>(ii) Its intended for One to Many communications</p> <p>(iii) More adaptable than ABE</p>	<p>(i) The data owner can't choose as to who can decrypt the encrypted data</p> <p>(ii) Its vulnerable for snot for some applications since data owner needs to have confidence in the key issuer</p>
5	[29]	Fine-Grained Access Control	<p>(i) This type of access control systems dependent on CP attribute based encryption, and advances high proficient capacity conspire dependent on data secretly sharing, simultaneously storing a copy of the data</p> <p>(ii) This plan can essentially decrease the outstanding task with Data Owner and also the storage requirements of cloud service provider</p>	<p>(i) Simple to manage user revocation key</p> <p>(ii) Its intended for One to Many communications</p> <p>(iii) More adaptable than ABE</p> <p>(iv) This scheme is capable of reducing workload of Data organization so also the storage space related overhead of cloud service provider</p> <p>(v) This can balance between the system's security and associated requirements</p>	(continued)

Table 14.1 (continued)

S. No.	References	Tech name	Observation	Advantages	Disadvantages
6	[26]	Hierarchical Attribute Set Based Access Control	<ul style="list-style-type: none"> (i) Data owner has to first encrypt data before sending it to the cloud (ii) The strategy of information documents refreshes by owner by refreshing the associated expiration time (iii) Domain expert gives the benefits and data owners are controlled by domain authority 	<ul style="list-style-type: none"> (i) Less inventory capital investment (ii) Lower maintenance cost (iii) Easier disaster recovery 	<ul style="list-style-type: none"> (i) It's even more complex arrangement
7	[19]	Blockchain Based Access Control	<ul style="list-style-type: none"> (i) This is type of cipher text-policy attribute-based encryption having dynamic attributes (ii) Utilization of blockchain technology, typically using a decentralized record (iii) The system gives unchanging key generation facility. It handles request of access policy assignment or revocation dynamically 	<ul style="list-style-type: none"> (i) Without copying them, the capacity to alter the access policy for the encrypted information 	<ul style="list-style-type: none"> (i) A secured channel among user and attribute authority is required for sharing attribute secret keys

14.2.2 Authentication Process

A secured communication channel facilitates exchange data of sensitive nature with trustworthiness, confidentiality, and integrity service over the transferred data. For provisioning of such services, it is required to establish an authentication process basing upon user's registration information for identification. It is based on either the user is aware of (like a password), user holds (akin to a smart card), or anything the user has (like user profiling, fingerprint or other biometric method). Many types of authentication mechanism have been developed as described:

Password Authentication

This is the easiest method to be used. But it must have desired difficulty level to prevent it from being easily guessed. It must be regularly renewed to maintain security. This type of authentication is well established with a common weakness. Although proper user id and associated passphrase is applied, still it may be difficult to justify that such access is initiated from a legitimate user and is vulnerable to shoulder surfing attack [1]. However, password authentication continues to be most commonly followed authentication means for transactions.

Trusted Platform Module Based Authentication

It is based on a hardware security module like a hardware lock. This lock uses a secure crypto processor that is capable of storing cipher keys for information protection. A commonly known variant of this is *Mobile Trusted Module (MTM)*. This suggested standard is issued by *Trusted Computing Group (TCG)*, which is a consortium of Microsoft, AMD, IBM, Intel, and Hewlett-Packard. This method is mostly applied to authenticate telecommunication system terminals. Moreover, this is considered to be a type of authentication method using online mechanism involving *Subscriber Identity Module (SIM)* for its effective utilization in smartphones.

Trusted Third Party Authentication

Generally, a Trusted Third Party (TTP) service those are implemented in cloud services establishes desired trust mechanism and provide solutions to ensure confidentiality, integrity, and authenticity. This is also used to ensure security of transacted data. Public key infrastructure (PKI) with TTP facilitates a robust means for implementing effective authorization having desired authentication inbuilt into it. Public key cryptography authentication means are used for implementation of PKI. A known example of authentication using TTP is known as Single Sign On (SSO). Moreover, TPP performs the task of an authentication server or a certifying authority that has overcomes security bottlenecks concerning the system. This SSO method of authentication is generally a preferred means to be widely followed in federated cloud environments. However the TTP associated could be treated as a singular failure point.

Multifactor Authentication

Authentication using multiple and collective factors [20] is a process that ensure, there is a combination of two or more means of authentication for a legitimate user.

Combination of multiple factors are applied for determining identity of a person for a higher level of trust for user's authenticity. Generally, user ID with associated password, biometric means, and authentication certificates are used for single factor authentication. Towards this end a second factor authentication like One Time Password(OTP), e-mail, SMSs, and mobile enabled OATH Tokens are being used. In a cloud environment this further adds an overhead for performing administration and management.

Implicit Authentication

Authentication by implicit method uses constant observation of client behavior. This is most suitable for mobiles as they can collect many type of users' information. To name a few, user location, movement of user, communication made by user, as well as usage of various applications by the users. For providing stable and desired services to users and their profile associated saved personal credential, many techniques have been studied which are applicable to mobile cloud scenario [25].

Blockchain Authentication

Using Blockchain authentication method, a distributed ledger carries out desired verification thereby ensuring legitimacy of users messages and transactions. The need for a TTP to provide authentication is eliminated. Simultaneously costs of expenditure could be further curtailed with security and privacy are remarkably improved. The process of authentication is accessed to be more difficult in a distributed scenario. Blockchain authentication [11] is done by smart contracts which are deployed associated with blockchain. Smart contract generator is usually created using Smart Contract Authentication (SCA) layer. This is activated and executed whenever an authentication request gets generated or self-govern it from pre-defined set of desirable actions.

14.3 IAM Related Concerns

Information on users' identity is continuously becoming a vital enabling factor of present day data driven society. This also is being considered as most important aspect in the inter communications among end users, intermediaries, and various service providers for accessing resources of the system. Accordingly, identity as well as access management continues to be an important challenge for information security and also to maintain user privacy.

14.3.1 Overview of Identity Management

Identity management process is incorporated in administrative mechanism of any organization and other corresponding protocols which are used to create, maintain

and also responsible for the de-provisioning of user accounts. Effective management of identity and associated control of attributes are required for managing identities towards various services. It is essentially desired to simplify user provisioning process by proper identity management. Identity management may be analyzed considering both users as well as digital entities. Security of user identity is associated with related software systems to store identity credentials, related data, so also communication link over which identity is desired to be verified and then established. For access control and related matters, digital signature technique provides a secure mechanism for user verification. For secured identity and access management using blockchain, cryptographically secured system for managing identity can become more robust by decentralizing the access method, verification and related transactions. Several types of identity management methods are described below in this regard.

Independent IDM

In this method managing and owning of user credentials are responsibility of a single entity. It is seen as mostly centralized internet identities. However, such independent identity repository model possesses some definite shortcomings. In this the users are not regarded as the owners of their own identity record. There is a possibility that user identity credentials could be revoked or may even be misused by identity provider.

Federated IDM

This mechanism is comparatively difficult for its implementation and require desired service level agreement and proper trust relationship between offered service. Federated identity management systems [24] is expected to provide authentication as well as authorization spreading beyond one organization and its administrative system boundary. This essentially needs service level agreement (SLA), by means of that identity credentials of one service provider is respected and acknowledged by other providers. Data ownership of the systems associated with corresponding service providers are also covered in the SLA. Identity provider is responsible for managing user accounts independently. There is no requirement of enterprise user directory wise integration. This mechanism lowers the security risk because of propagation of use credentials and non-replication.

Self-sovereign IDM

In this type users and systems are capable of storing own identity related data on its devices in a decentralized manner. This system securely give out their identity related credential to those who require this for validation as and when required, without depending on a central identity data repository. Self-sovereign identity concept is emerging as a new means in which users are permitted for controlling self-digital identity [17]. This method facilitates full control for user security as well as complete portability of user's data. As described by Sovrin foundation self-sovereign identity is expressed as an Internet for identity. There is no identity owner in this huge pool. Rather every user can use it and also permitted to further improve it.

14.3.2 Threats for Identity and Access Management in Cloud Environment

In integrated system, Identity and Access Management (IAM) signify how securely identity authentication and authorization means are used to manage desired applications of the system. This is followed for authentication of users, devices and in certain cases services. For accessing the desired application, own identity repository or technique to authenticate a system or service is always not mandatory. Rather process of establishing identity may be achieved with the help of trusted third party identity provider. This mechanism reduces workload of the application substantially. This can also be used from outside an enterprise for handling business to business oriented strategic relationship. This can even be used between a private enterprise system and cloud service provider. This way this is implemented in a Multi-Cloud or Federated environment.

Many method and protocols have been proposed by various researchers for handling identity in cloud environment. Among authentication and authorization protocols already developed and available for federated identity, three protocols are generally found to be well accepted and established. They are SAML, OAuth and OpenID [16]. These protocols differ in provisioning to address security related issues of exchanging privileged data, authentication and authorization. Simultaneously all three mentioned methods adopt same procedure, which is essentially a token based solution. Below we deliberate on such methods.

Security Assertion Markup Language (SAML)

This is well established and also known for Single Sign On (SSO) assertion that is utilized to exchange digital authentication as well as resource authorization among identity provider (IdP) and service providers (SPs). It uses token based sign on method. Trust is vital aspect among IdP and SPs in which corresponding SPs agree for trusting various associated IdPs to authenticate respective users. The SSO assertions are managed by authentication method of the IdPs with essential functionality of token generation in this technique.

OAuth

This is an Open Standard protocol that is used to provide secured and authorization service in delegated manner. Without sharing users' password, only limited access may be permitted for other applications with this method. With reference to OAuth nomenclature, Service Provider is termed as Resource Server, Identity Provider is called as Authorization Server and the User is known as Resource Owner. In OAuth flow of operation, when resource owner's status is online by logging in, the client application essentially receives two tokens from the Authorization Server. One is Access Token while other is Refresh Token. Access tokens so generated are designed to be short lived considering its security and for preventing token theft. Client use refresh token without undergoing login process again and again for getting access token, afresh from respective Authorization Server on completion of active life of last

generated access token. Newly generated refresh tokens also carry relevant expiry period.

OpenID

This is operated as an additional authentication mechanism over OAuth. It is essential for having specific OpenID account associated with available OpenID identity providers. After logging on a user on such IdP is then capable of obtaining access to privileged services which directly reside on resource servers. At the same time relaying party then processes the desired OpenID authentication. There is a redirection from OpenID for the concerned user to IdP and further OpenID Provider for getting authenticated. While using services by relying party's access request and on being authenticated with login credentials for user SSO session, the IdP assign that service access having desired authorization.

14.3.3 IAM Concerns and Related Developments

Several researchers have identified problems associated with this research area and have suggested many solutions to IAM. Below mentioned Table 14.2 depicts a list of suggested approaches for solution to some of such problems. Related aspects of solutions specifically have been highlighted on the usage of Blockchain technology.

14.4 Blockchain Technology

Blockchain is represented as a time stamped data structure which is distributed in nature having append-only feature. Blockchain facilitates establishment of a peer to peer network in which members who are non-trusting could communicate without any central agency or TTP. This interaction can also be verified. In this infrastructure, digital signature enabled transaction among peers takes place. These transactions signify a mutually agreed coordination mechanism between participating users or agents, which could incorporate transaction of physical or digital resources. This could be even the completion of particular event or task. Essentially one of the participant sign this transaction. After that it is passed on to the neighboring ones. An entity that gets connected with a blockchain is known as node. All the nodes who successfully verify all defined rules of blockchain are termed full nodes. Such nodes are responsible to organize the transactions into various blocks of the blockchain. They also determine validity of transactions so that they are allowed to be kept in the blockchain, or otherwise. Blockchain technology facilitates building an always available, secured, distributed, immutable and commonly accessible repository of associated data termed as ledgers. This depends on distributed and commonly accepted set of rules to manage this repository specifically to decide about validity of new data to be stored in the database in a distributed manner.

Table 14.2 Authentication and authorization problems with suggested solutions

S. No.	Research problem	Suggested solution	References
1	It is possible for a malicious user to get information on relationships of users, access user interests and may even act to be one among them	To suggest an authentication mechanism capable to protect information on users' privacy, Blockchain algorithm was proposed. Assuming user having a close affinity, the authentication procedure to use encryption along with a hashing function for enhancing its security infrastructure	[29]
2	Presently used authentication mechanism essentially requires to remember various complex IDs with passwords. Alternatively it can depend on a trusted third party(TTP), for handling possibility of a system failure arising out of denial-of-service (DoS) attacks	A user authentication mechanism was designed, which is distributed in nature using blockchain technology. In this method, identity information is stored in a distributed manner in a blockchain. Personal credentials of users are encrypted and are stored at other than blockchain maintained storage locations. Desired access permissions are permitted by an attached and deployed smart contract	[27]
3	In the absence of a cloud server for merging requirements of storage as well as computing, management of resources akin to cloud services can be achieved by applying external methods for services. Authentication method with such external services with mobile device is not generally identified	Secure Authentication Management human centric Scheme (SAMS) was suggested for achieving mobile device authentication with the use of blockchain technology. This is an enabler for effective resource handling pertaining to information in the user devices	[8]
4	Concerns pertaining to privacy of users are not addressed	For authentication and also for managing users' privacy concerns, digital signature technique has been suggested. A gateway was suggested using Blockchain as well. This acts as a gateway between users with deployed IoT devices	[3]

(continued)

Table 14.2 (continued)

S. No.	Research problem	Suggested solution	References
5	Using Cloud based radio access network devices are connected. Accordingly, in order to increase services of 5G network covered area of IoT devices, for authentication purpose centralized access mechanism is generally followed. An additional overhead is cost of network. Hence most effective mechanism cannot be effectively used to achieve security of desired high level for given services	5G infrastructure of BTA and BAA technique using cloud radio using optical fiber network have been suggested. For evaluating the efficiency of this architecture SDN testbed was used	[28]
6	Internet or alternatively gateway are used to manage Smart Homes. This is implemented having intercommunication of IoT devices with cloud servers. Communication devices like smartphone are also used in Smart homes for various purposes. It is essential to prevent any breach of security due to attack form outside the network. Hence a secured network access is required in this situation	Key management, Secure smart home authentications along with group key have been suggested basing on a multiple solution chain to provide confidentiality of data	[22]
7	The real issue is to how to ensure privacy, security in a centralized system. However, untraditional nature of IoT like heterogeneity, mobility and scalability require identity management systems to have a decentralized and trust less environments	Blockchain enabled Identity Framework for IoT (BIIFT) was suggested. It is possible to get established in smart home scenario to manage identity issues by following self management by the users themselves. Signature of individual users are used in this method along with blockchain. However, IoT device signature with low level identities interconnected with owners identities for authentication of credentials and to bring normal and uniform behavior of connected IoT devices	[13]
8	Known drawback of usage of public key certificates, such as changing a selected message adaptively. Identity attack using random mode of operation is also required to be addressed	Identity based linear homomorphic signature mechanism has been prepared	[22]
9	Development as well as usage of IOT is affected with privacy related concerns and associated security issues	A robust authentication mechanism has been designed along with identification of its enabling technologies	[21]

(continued)

Table 14.2 (continued)

S. No.	Research problem	Suggested solution	References
10	IOT devices are required to authenticate among themselves. They are also required to maintain data integrity while communication. They are also required to prevent malicious users and tampering caused due to their usage	Bubbles of trust system has been suggested. This method empowers the devices to have more efficient identification and authentication. It enhances system availability and also protects data integrity	[7]
11	Interoperability of the cloud is desired	Using JSON Web Token (JWT) tool and blockchain mechanism, end-to-end and more efficient authentication technique has been suggested	[6]
12	Authentication of mobile user required	Blockchain technique has been applied to put forth a new IIaaS in a solution with digital identity management	[9]
13	The credit or debit card companies require more and more details, like know your customer(KYC) with details of identity before permitting any financial transaction	A CIMA framework has been proposed which use a context to represent shared secret among mobile device with enterprise. This mechanism enable establishment of one time session encrypted key as well for mutual authentication	[15]
14	Authentication mechanism meant for undirected graphs signifying authentication using graph edges which are non-existent along with identified problem that need to be addressed	A mechanism namely transitively closed undirected graph authentication (TCUGA) has been developed	[12]
15	Having a very close similarity among users, cloud Service providers commonly experience unconditional anonymity in IoT environment. Accordingly no specific means is proposed to decide about particular user who is to be made responsible regarding specific action for system functioning	Authentication mechanism depending on Wi-Fi hotspot accessing has been suggested that can provide accountability without depending on any ITTP. This solution is known to have been developed from Bitcoin techniques	[18]

14.4.1 Blockchain Architecture and Functioning

From its architecture point of view, Blockchain is a distributed ledger system. Figure 14.1 shows an example of blockchain having a number of consecutively interconnected blocks. All of the blocks, except first block of blockchain always points to corresponding immediate previously located block. This is named as parent block. This linking is executed by inverse mechanism of reference which is represented by hash function value generated from the parent block. Referring to Fig. 14.2, node i should hold the hash of block $i - 1$. The first of the blocks of a blockchain is termed as genesis block. The genesis block does not point to any parent block associated with it.

Blockchain is composed of many consecutively interconnected blocks. It can be described in detail in terms of a Merkle tree structure having multiple transactions. A blockchain continuously grows with the transactions being executed and blocks are appended. At the time of generation of a new block, all nodes of the network play their role for the block validation process. Once validated, a block then gets automatically added to end of blockchain by an inverse referencing for pointing towards parent block. Due to this technique any attempt on the previously generated block for any attempt for making any alterations are comfortably detected because hash value of the apparently manipulated block definitely varies from hash of the intact block. Since blockchain signify its distributed nature throughout the network, any attempt to tamper it can be effortlessly identified by other nodes in network.

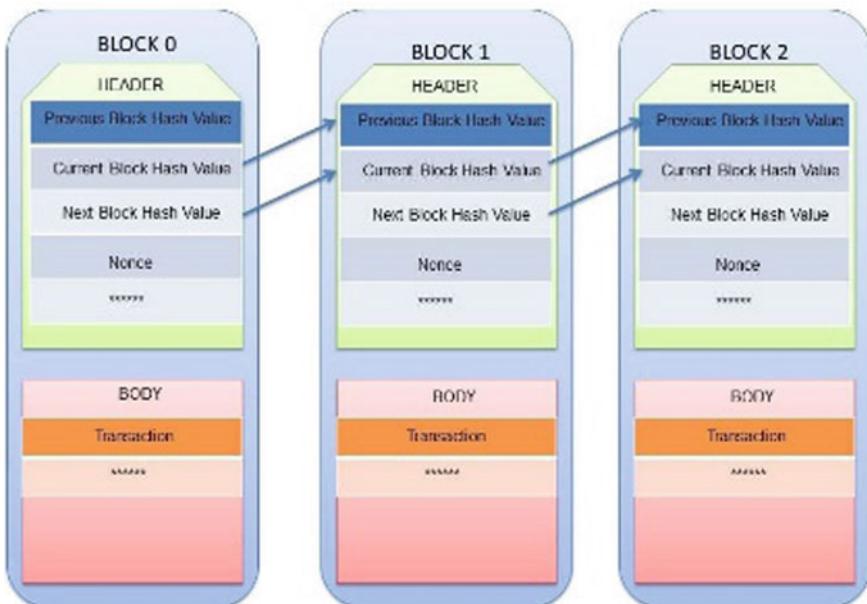


Fig. 14.1 Generic blockchain model

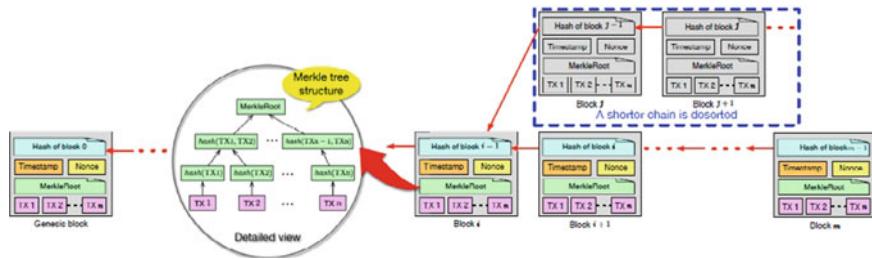


Fig. 14.2 Blockchain as distributed ledger (Inspired from [5])

The structure of a block essentially has the following information:

1. Version of the Block which indicate the rules for validation to be followed.
2. The hash of parent block functioning as a connecting information link.
3. Corresponding time stamp recording of the current time expressed up to seconds.
4. Starting from a zero count and increases for every further hashing calculation is made.
5. Number of transaction performed in Blockchain.
6. Merkle Root signify that Merkle tree's hash value corresponding to the root having concatenating hash values in block for all transactions, as depicted in Fig. 14.2.

Two types of participating nodes are there in Blockchain: Firstly, node that are capable of only reading facts are termed as passive node. Secondly, nodes which may be able to read and write data termed as active mode which are also generally known as miners. For adding new transaction to blockchain, undermentioned set of activities are performed.

1. Transactions yet to be performed are generally bunched together along with other transactions, termed as a block in the description of Blockchain.
2. Responsibility of verifying whether transactions in Blockchain are done with respect to defined rules lies with the Miners.
3. Miners perform on a mutually agreed upon consensus mechanism to perform check and validate the added block.
4. Miners those perform validation of the block are generally rewarded.
5. Those transactions performed that are verified are stored in the blockchain. For proving honesty in validation of blocks, several techniques exist.

14.4.2 Technical Function of Blockchain and Evolution

In this subsection, technologies used in blockchain is highlighted. Fundamentals of trust mechanism, also commonly known as the consensus mechanism, used

in blockchain is described. Subsequently synchronization process of the nodes is deliberated upon. Further evolution of blockchain are described.

Consensus Mechanism

Blockchain systems are independent of any third party trusted authority due to their decentralized approach. In blockchain adoption, decentralized consensus mechanism is vital for ensuring reliability, consistency of data, and also the transactions. Some four well known consensus mechanisms are in use. They are *Proof of Stake (PoS)*, *Proof of Work (PoW)*, *Practical Byzantine Fault Tolerance (PBFT)*, and *Delegated Proof of Stake (DPoS)*.

PoW mechanism use puzzle solution for establishing credibility of data. Generally used puzzle is computationally difficult but an easily verifiable problem. For creation of a block by a node it is mandatorily required to solve a PoW puzzle. On being resolved, it is broadcasted to other nodes for achieving consensus. PoW mechanism require huge amount of calculations thereby wasting of computation capabilities.

For proving credibility of user data, the PoS mechanism use proof of ownership of cryptocurrency. For block creation or any transaction, in a PoS based arrangement users are supposed to pay desired amount of cryptocurrency. On successful validation of transaction or block creation used cryptocurrency amount are sent back to original node like a type of bonus. Else it is used as a fine. PoS mechanism increases the throughput of blockchain system as it can effectively reduce load of computation.

Block Propagation and Synchronization

Every node is capable to store details of information regarding to all blocks in blockchain. This is the foundation for establishing consensus and trust for blockchain. For establishment of trust and consensus, propagation mechanisms may be divided into the following types [10]

1. *Propagation Based on Advertisement:* This method draws its origin from Bitcoin. When node X receive information pertaining to a block, X would generate *inv* message (which is a type of message in Bitcoin) to corresponding connected nodes. At the time of node Y getting *inv* message from X, it operates with further mentioned steps. For the instance of node Y having information on the block, it would ignore it. If node Y is not having this information, this would respond to node X. On receipt of message from node Y at node X, node X would send entire information of the block to node Y.
2. *Advertisement or Push Hybrid Type Propagation:* As the name suggests, it is a hybrid propagation method used in Ethereum. It is assumed that node X is connected to n number of peers. Using such mechanism, node X would be able to push the block straight to square root of n peers. For rest of n-square root of n of the connected peers, node X would be able to advertise block hash to the rest.
3. *Relay Network Propagation:* Using this method every miner shares a transaction pool. All transaction are denoted as an unique global ID, that would minimize block size of broadcast. This reduces network load and as a result improve propagation speed.

4. *Sendheaders Propagation:* In this method, node Y would initiate a sendheaders message which is a type of message in Bitcoin, addressed towards node X. On receipt of information of a block at node X, block's header information is sent to node Y. As a matter of comparison to propagation mechanism based on advertisement, it is not necessary for node X to send inv messages. This is how it aids in speeding up block propagation.
5. *Propagation by Unsolicited Push:* Using this mechanism, a miner broadcasts the block directly to other nodes, after one block is mined.

Evolution of Technology

From its inception, the blockchain as a distributed ledger technology has matured through two development stages. They are commonly termed as blockchain 1.0 and blockchain 2.0. Blockchain technology is primarily utilized for cryptocurrency transactions in stage 1.0. Like Bitcoin, there exists several other examples of cryptocurrency. To name a few Litecoin, Dogecoin and many more. With development of Blockchain 2.0, a new idea called smart contract was introduced for developing various applications. Smart contract is also signified as a specialized code for lightweight decentralized application(dAPP). A commonly known example of blockchain 2.0 implementation is Ethereum. Every node of Ethereum run specific Ethereum Virtual Machine (EVM) which enables execution of smart contracts. In comparison to classical applications, a dAPP possesses undermentioned characteristics and advantages.

1. *Autonomy:* Smart contracts are designed to be deployed and run on the blockchain systems. Smart contracts are the core mechanism behind development of dAPPs. Accordingly, dAPPs can run autonomically and independently without any other's assistance or participation.
2. *Stable:* State tree of blockchain holds generated bytecodes of smart contracts. Every full node has information of all blocks as well as stateDB. These nodes also store the generated bytecodes. Accordingly, considering probable failure of some nodes, its operation is not likely to be affected. This mechanism ensures stability of dAPPs.
3. *Secure:* Blockchain consensus mechanism along with public key cryptography ensures the security as well as desired operations of smart contracts. This in turn also maximizes security of dAPPs.
4. *Traceable:* All information related to smart contracts is stored as event logged transactions in the blockchain. Accordingly every actions and operations involving dAPPs are saved which are traceable as well.

14.4.3 Workflow of Blockchain

Working of blockchain is explained here with the help of Fig. 14.3. It depicts a money transfer example scenario, wherein Alice wishes to transfer some money to Bob.

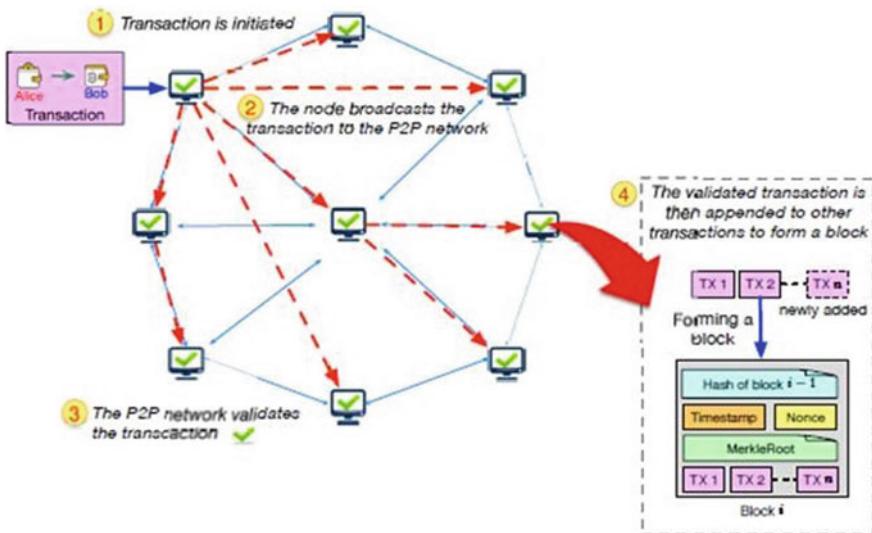


Fig. 14.3 Blockchain work flow (Inspired from [30])

1. Firstly, Alice starts initiation of this transaction with computer using her slotted Bitcoin wallet.
2. This transaction incorporates related sender information like the sender's wallet, address of the receive and to be transferred amount. Its mandatory for said transaction to be signed by private key of Alice which thereafter could be verified and made accessible to other users with public key of Alice. Further the system broadcasts this initiated transaction to everyone in the P2P network.
3. Subsequently, successfully validated transaction gets appended at the end of transactions list. This creates a new block in blockchain when the miner of blockchain solves required puzzles successfully.
4. Ultimately, all nodes save a snap sort of updated blockchain. This happens when the successful validation of transaction is said to be complete and it is appended to blockchain.

14.4.4 Comparison of Blockchain

There are definite differences noticed with blockchain technologies. These differences are prominently noticed with respect to scalability and native of cryptocurrency. Differences could also be noticed pertaining to participation of nodes in the decentralized network, consensus mechanism etc. An analytical comparison between various types of Blockchain is presented in Table 14.3.

Table 14.3 Comparison of types of blockchain

Parameter	Public blockchain	Private blockchain	Consortium blockchain
Decentralization	Decentralized	Centralized	Partially centralized
Immutability	Nearly impossible	Immutable	Partially immutable
Non repudiation	Non refusible	Refusible	Partially refusible
Level of Transparency	Transparent	Opaque	Partially opaque
Traceability	Traceable	Traceable	Partially traceable
Scalability	Poor	Better	Good
Flexibility	Poor	Better	Good
Efficiency	Low	High	High
Permission type	Permissionless	Permissioned	Permissioned
Employed Consensus algorithm	PoW, PoS	Ripple	PBFT, PoA, PoET
Example	Bitcoin,	GemOS, Multichain	Ethereum, Hyperledger

14.4.5 Security Techniques in Blockchain

Various Basic Security Techniques and principle that specify as to how Blockchain technology can ensure security are mentioned below:

1. *Confidentiality*: It is ensured by this means that only permitted users are allowed to access the desired information. Blockchain uses a notional-anonymization technique namely a hash function for hiding user identities and thereby ensuring confidentiality.
2. *Integrity*: This property ensure that the information is changed or updated, only by users permitted to do so. Blockchain incorporates cryptographic technique for ensuring that transactions are immutable with an aim to verify data integrity.
3. *Availability*: This property ensures availability of data as desired. It also facilitates that the services are always activated upon the request of genuine users. To achieve this aim Blockchain allow to get blocks stored in decentralized manner having multiple copy stored in the blockchain.
4. *Authentication*: By this means, computer system tries establishing identity of user or computer to permit that user or computer to gain access to certain allowed and secured resources. This ensure restricted or controlled access permissions for the said resources. Blockchain technology enables this functionality in terms of provisioning of private keys for users those are permitted for performing transactions.
5. *Non repudiation*: It signify impossible nature for a user or some entity associated to communication, to not agreeing to have received or to have sent a message. Such functionality is employed with blockchain due to time stamped event logging property.

Security Requirements for Blockchain based Authentication

Considering available literature, a mutual authentication system, blockchain based and fine grained access control system is required to fulfill following essential requirement on security:

1. *Single registration:* The system is required to follow a single registration process. This means user is required to register only once for performing corresponding transactions.
2. *Mutual authentication:* System is essentially required to follow mutual authentication technique among terminals and corresponding gateway. This would enable for resisting commonly known attack like impersonation as well as man in the middle attack.
3. *User anonymity:* For preserving system's privacy, it must ensure anonymity with respect to associated terminals. Considering blockchain system point of view, an attacker would not be able to determine the actual identity of terminal by performing an analysis of transaction performed.
4. *Fine grained access control:* Dynamically granting or revoking of permission by authority or manager could be performed associated with terminals for the policy at a fine grained standard. This action is performed in a near real time manner.
5. *Session key agreement:* For secure communication for participants, there should have established mechanism helps for establishing session keys. Most likely one can establish secured connection with others for negotiating session key to support further communication establishment.
6. *Perfect forward secrecy:* For ensuring secrecy of previously transmitted message, a mechanism of forward secrecy is required to be provided in which an attacker who manages to get both of the communicating partners private or public keys would not be allowed for recovering previously generated session key.
7. *No verifier table:* System is not required to maintain any verifier table. This can reduce communication related overhead. It should also actively control stolen verifier as well as denial of service (DoS) attack. Without any reference to any verifier table, mutual authentication mechanism must be established in the system.
8. *No online registration center:* For reduction of cost related to communication, it is suggested that the system not to have any online registration center. This arrangement facilitates each communication entities to authenticate directly not depending on any central establishment for registration.
9. *Relay current timestamp:* For maintaining trust, the corresponding blockchain is to be stored in a chronological order. The system must make use of trust nodes to convey presently used timestamp in the blocks. There should not be any potential means to enable any modification of the timestamp.
10. *Birthday collision resilience:* There is a rare chance that two same blocks being created at the same time. The system should be in a position to control birthday collision and eliminate any types of dispute among the sub blockchain.

11. *Interception and modification resilience:* It is essential to maintain integrity of transmitted message. It is required to be protected from interception and modification, and not being detected.
12. *Hijacking resilience:* To have a smoother transaction, it must minimize scope for an attacker for hijacking any transaction, and not being detected.
13. *Resilience to known attack:* System is required to facilitate to ensure resilience to commonly known types of attacks, like impersonation attack, DDoS attack, modification attack, man in the middle attack as well as replay attack.

Addressing IAM Concerns with Blockchain

The Blockchain by design is decentralized, thus, it provides a decentralized approach to Identity Management. In most state of the art systems, users store their identity in their personal decentralized wallets thus eliminating the problems of centralization. This decentralization also provides a large degree of mobility and user control to such identities. A blockchain Identity also automatically provides a clear separation between the roles of Authentication agents and Authorization agents, hence degrading the probability of collusion of these agents against a subject. In most cases Authentication and Authorization agents may be completely decoupled, thus removing the incentive to misappropriate subject data. Lastly, trust scales very well in the Blockchain environment as compared to traditional central server solutions. This is simply because, new entrants into the Blockchain Identity only need to trust the consensus algorithm as compared to trusting a server or even a group of servers.

Here we bring out a broad view as to knowing the best way blockchain could be utilized for IAM functioning. Figure 14.4 describes a generic model for possible interactions of the various IAM functions corresponding to blockchain. It mentions at what position of a classical IAM processing cycle following blockchain technique could be applied effectively and facilitate for IAM operations. Figure 14.4 describe that blockchain technology which may be effectively applicable to all basic IAM operations, particularly authentication, management of identity, access control, and also monitoring or auditing.

Blockchain as a technology is found to be useful for ensuring privacy, Access control, Data Integrity and also for protecting personal information associated. Fine examples regarding employment of PoW enabled, blockchain for IoT application to put in place integrity and confidentiality are available. For access control functionality Blockchain could be used effectively. Using blockchain technology, a Fair Access procedure has been proposed which allow clients for controlling own data. Access control functionality on blockchain with data storage and distributed hash table having with multiple nodes is a known phenomenon. This technique may effective used for data location management following a distributed database system. Such a system essentially has a control mechanism which implements name registration protocol with corresponding link associated with data storage.

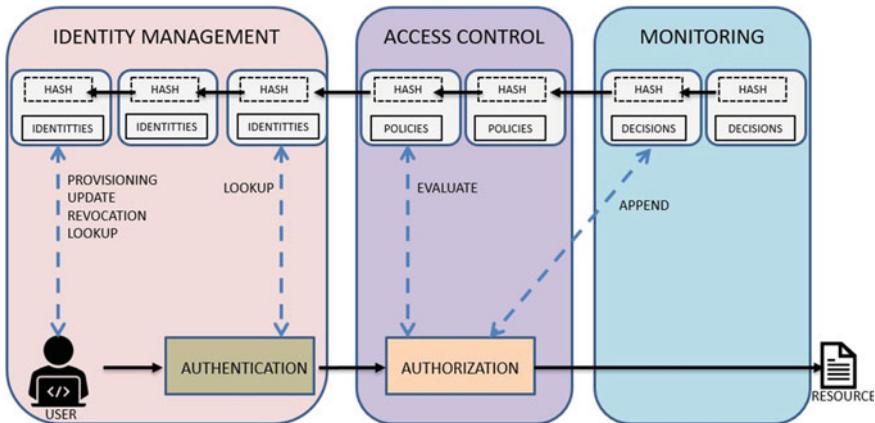


Fig. 14.4 Blockchain for IAM function

14.5 Open Research Issues

It is concluded from above discussion that the methods involving MAC and DAC may not be suitable enough for present day techniques of security advancement. ABAC and RBAC could be able to keep them abreast with current requirements. IAM is the most challenging field for research work having huge scope and can be further explored for its enhancements. Since applications are vulnerable to attacks in numerous means, this can only be handled with new security techniques for the situation. Based upon the type of access control means adopted, some issues that needs attention of researchers are mentioned below.

14.5.1 Mandatory Access Control (MAC)

1. MAC intends to use dispatch functionality for the related tools, utility and system for the access control infrastructure.
2. MAC model restricts user access. Depending on the protection policy it does not allow any attempt for alteration by user themselves.
3. A determined setup is essentially required to implement MAC in efficient manner. It is required to have a heavily loaded organization management to periodically refresh object and account labels for collecting new data when a MAC system is implemented.

14.5.2 Discretionary Access Control (DAC)

1. It may be an easier task to compromise a Trusted Third Party(TTP) and then it is possible to have a copy of unique message without consent of owner.
2. Lack of assurance on the flow of information is there.
3. Threads of Trojan horse pose as vulnerabilities.

14.5.3 Attribute Based Access Control (ABAC)

1. For a Multi-tenant or multi cloud or federated cloud environment, extension of currently followed technique for heterogeneous cloud platforms along with its policy integration matters for heterogeneous multi cloud IaaS requires further attention.
2. There is a possibility to explore Multi-tenant ABAC covering context and other associated attributes. Administrative schema is a challenging development towards of Multi-tenant ABAC.
3. To extend the scope towards authorization for Multi-tenant situation, particularly as a Service. Open Stack API support is desired for attribute based Multi-tenant access control models.
4. Since tenant are not allowed to arrange own policy matters, cloud's policy and role of users are the alternative which can be explored.
5. It's not capable to arrange tenant level administrator.
6. User role assignment management is not offered in ABAC.

14.5.4 Role Based Access Control (RBAC)

1. Sometimes it produces extra and may even contradicting roles than those of users.
2. RBAC method of allocation of roles is a static process for the users, which are not chosen in dynamic situation. It is very troublesome to implement when the system function dynamically and its environment further distributed.
3. It is troublesome to change access rights of the user without making a change to the role of that particular user.
4. Dynamic attributes are not recommended for usage with RBAC.
5. Access rights are not likely get modified without changing the user roles. For implementing RBAC model roles it is recommended to be assigned well prior to its implementation.
6. A role change may be of advantage for permissions associated role which could be deleted or distorted.

14.5.5 Identity Access Management (IAM)

1. Multilevel security may result in fine grained and on demand access control methods.
2. Lack of prominent Personal Identifiable Information (PII).
3. It may lack desired architecture to support clients in data distribution during information exchanging.
4. Lack of assurance on performance parameters of users by Service Provider.

14.5.6 Additional Issues

In this discussion it is pointed out regarding audit and privacy concerns are comparable to each sides of a coin. Both of above mentioned concerns follows the principle of blockchain technology's nature of storing information in a tamper proof and openly accessible mechanism of storage. While trying to handle the privacy related matters it is not advisable to neglect required transparency of the system. Such a facility can be achieved by limiting access to stored information following a need to know basis approach and also only to intended parties. The simplest way for its implementation could be to adopt a private blockchain implementation. For operating the block, trusted parties only are permitted to add new blocks to the chain and also to access information already saved in the blocks. In order to efficiently process encrypted data in clear mode enough miners would need to decipher such information in the event data be encrypted in a private chain to further limit information access by others. A private blockchain is not able to solve this issue of processing of deciphered data and storage as well as of retrieval of data in encrypted mode in general. This may even limit itself to replace such matter with the need a TTP. This may lead to a situation where the private blockchain miners are required to be trusted.

14.6 Conclusion

Blockchain technology came to existence due to requirements for cryptocurrency transactions. Essence of such transaction is to exchange cash in electronic form where the transacting parties don't trust each other, not even they trust intermediate party. Since the technology is continuously evolving and getting matured, it has been able to address many more modern day requirements. Blockchain is accessed as a potent means for improving the efficiency of IAM by infusing the associated technical advantages like immutability, decentralized nature and fault tolerance. Further owning and verifiability aspect of user credentials have been coined to above, enhancing its way toward achieving Self-sovereignty in the field of IAM. Without depending on any centralized third party, having a secure platform to authenticate user to avail sensitive online services has become a reality. Hence a cost effective,

reliable and technically robust IAM solution for government agencies as well as corporates can be made available with the help of Blockchain.

References

1. Awang, M.I., Mohamed, M.A., Mohamed, R.R., Ahmad, A., Rawi, N.A.: A pattern-based password authentication scheme for minimizing shoulder surfing attack. *Int. J. Adv. Sci., Eng. Inf. Technol.* **7**(3), 1049–1055 (2017)
2. Belguith, S., Kaaniche, N., Russello, G., et al.: Lightweight attribute-based encryption supporting access policy update for cloud assisted IoT. In: Proceedings of the 15th International Joint Conference on E-Business and Telecommunications-Volume 1: SECRIPT, pp. 135–146. SciTePress (2018)
3. Cha, S.-C., Chen, J.-F., Su, C., Yeh, K.-H.: A blockchain connected gateway for Ble-based devices in the Internet of Things. *IEEE Access* **6**, 24639–24649 (2018)
4. Cruz, J.P., Kaji, Y., Yanai, N.: RBAC-Sc: role-based access control using smart contract. *IEEE Access* **6**, 12240–12251 (2018)
5. Dai, H.-N., Zheng, Z., Zhang, Y.: Blockchain for Internet of Things: a survey. *IEEE Internet of Things J.* **6**(5), 8076–8094 (2019)
6. Faisca, J.G., Rogado, J.Q.: Personal Cloud Interoperability. In: 2016 IEEE 17th International Symposium on a World of Wireless, Mobile and Multimedia Networks (Wowmom), pp. 1–3. IEEE (2016)
7. Hammi, M.T., Hammi, B., Bellot, P., Serhrouchni, A.: Bubbles of trust: a decentralized blockchain-based authentication system for IoT. *Comput. Secur.* **78**, 126–142 (2018)
8. Kim, H.-W., Jeong, Y.-S.: Secure authentication management human centric scheme for trusting personal resource information on mobile cloud computing with blockchain. *Hum. Centric Comput. Inf. Sci.* **8**(1), 11 (2018)
9. Lee, J.-H.: BIDaaS: blockchain based id as a service. *IEEE Access* **6**, 2274–2278 (2017)
10. Li, X., Jiang, P., Chen, T., Luo, X., Wen, Q.: A survey on the security of blockchain systems. *Futur. Gener. Comput. Syst.* **107**, 841–853 (2020)
11. Lim, S.Y., Fotsing, P.T., Almasri, A., Musa, O., Kiah, M.L.M., Ang, T.F., Ismail, R.: Blockchain technology the identity management and authentication service disruptor: a survey. *Int. J. Adv. Sci., Eng. Inf. Technol.* **8**(4-2), 1735–1745 Insight Society (2018)
12. Lin, C., He, D., Huang, X., Khan, M.K., Choo, K.-K.R.: A new transitively closed undirected graph authentication scheme for blockchain-based identity management systems. *IEEE Access* **6**, 28203–28212 (2018)
13. Lin, Q., Yan, H., Huang, Z., Chen, W., Shen, J., Tang, Y.: An Id-based linearly homomorphic signature scheme and its application in blockchain. *IEEE Access* **6**, 20632–20640 (2018)
14. Maesa, D.D.F., Mori, P., Ricci, L.: Blockchain based access control. In: IFIP International Conference on Distributed Applications and Interoperable Systems, pp. 206–220. Springer (2017)
15. Morrison, J.: Context integrity measurement architecture: a privacy-preserving strategy for the era of ubiquitous computing. In: 2016 Ieee 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (Uemcon), pp. 1–10. IEEE (2016)
16. Naik, N., Jenkins, P.: Securing digital identities in the cloud by selecting an apposite federated identity management from Saml, Oauth and Openid Connect. In: 2017 11th International Conference on Research Challenges in Information Science (Rcis), pp. 163–174. IEEE (2017)
17. Naik, N., Jenkins, P.: Self-sovereign identity specifications: govern your identity through your digital wallet using blockchain technology. In: 2020 8th Ieee International Conference on Mobile Cloud Computing, Services, and Engineering (Mobilecloud), pp. 90–95. IEEE (2020)
18. Niu, Y., Wei, L., Zhang, C., Liu, J., Fang, Y.: An anonymous and accountable authentication scheme for Wi-Fi hotspot access with the bitcoin blockchain. In: 2017 Ieee/Cic International Conference on Communications in China (Iccc), pp. 1–6. IEEE (2017)

19. Ouaddah, A., Abou Elkalam, A., Ait Ouahman, A.: FairAccess: a new blockchain-based access control framework for the Internet of Things. *Secur. Commun. Networks* **9**(18), 5943–5964 (2016)
20. Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., Koucheryavy, Y.: Multi-factor authentication: a survey. *Cryptography* **2**(1), 1 (2018)
21. Polyzos, G.C., Fotiou, N.: Blockchain-assisted information distribution for the Internet of Things. In: 2017 IEEE International Conference on Information Reuse and Integration (Iri), pp. 75–78. IEEE (2017)
22. Ra, G.-J., Lee, I.-Y.: A study on KSI-based authentication management and communication for secure smart home environments. *KSII Trans. Internet Inf. Syst.* **12**, 2–3 (2018)
23. Salman, O., Abdallah, S., Elhajj, I.H., Chehab, A., Kayssi, A.: Identity-based authentication scheme for the Internet of Things. In: 2016 IEEE Symposium on Computers and Communication (Iscc), pp. 1109–1111. IEEE (2016)
24. Selvanathan, N., Jayakody, D., Damjanovic-Behrendt, V.: Federated identity management and interoperability for heterogeneous cloud platform ecosystems. In: Proceedings of the 14th International Conference on Availability, Reliability and Security, pp. 1–7 (2019)
25. Vhaduri, S., Poellabauer, C.: Multi-modal biometric-based implicit authentication of wearable device users. *IEEE Trans. Inf. Forensics Secur.* **14**(12), 3116–3125 (2019)
26. Wan, Z., Deng, R.H., et al.: HASBE: a hierarchical attribute-based solution for flexible and scalable access control in cloud computing. *IEEE Trans. Inf. Forensics Secur.* **7**(2), 743–754 (2011)
27. Yang, H., Zheng, H., Zhang, J., Wu, Y., Lee, Y., Ji, Y.: Blockchain-based trusted authentication in cloud radio over fiber network for 5G. In: 2017 16th International Conference on Optical Communications and Networks (Icogn), pp. 1–3. IEEE (2017)
28. Yin, H., Xiong, Y., Zhang, J., Ou, L., Liao, S., Qin, Z.: A key-policy searchable attribute-based encryption scheme for efficient keyword search and fine-grained access control over encrypted data. *Electronics* **8**(3), 265 (2019)
29. Yu, R., Wang, J., Xu, T., Gao, J., An, Y., Zhang, Gong, Yu, M.: Authentication with block-chain algorithm and text encryption protocol in calculation of social network. *IEEE Access* **5**, 24944–24951 (2017)
30. Zheng, Z., Xie, S., Dai, H.-N., Chen, W., Chen, X., Weng, J., Imran, M.: An overview on smart contracts: challenges, advances and platforms. *Futur. Gener. Comput. Syst.* **105**, 475–491 (2020)

Chapter 15

Blockchain: A New Safeguard to Cybersecurity



Ishtiaque Ahmed, Manan Darda, and Siddhanth Nath

Abstract Blockchain and Cybersecurity are two vivid technologies that have developed tremendous consideration in recent years. This chapter presents a structure of existing and possible utilization of blockchain-based cybersecurity solutions for attackers and defenders to evaluate whether the convergence will steer the results for one of these groups. It focuses on the blockchain architecture and clarifies the ideas and different features such as decentralization, trustworthiness, smart contracts, and immutability. It attempts to feature the role of Blockchain in molding the eventual fate of Cyber Security. It also deals with trending cryptocurrencies like bitcoin and Ethereum which are gaining prominence in the recent times and will revolutionize the way people trade.

Keywords Blockchain · Cybersecurity · Cyberattacks · Threats · Defense

15.1 Introduction

Blockchain technology was presented in 2008 as a foundation of bitcoin that has increased across the board consideration as the first cryptocurrency. Besides, beginning from mid-2010s clients started to understand that Blockchain as the central innovation can have a lot more extensive use than the bitcoin itself, and the two terms began to follow separate ways [1]. In simpler terms, a period ventured course of action of immutable records of data, which is supervised by a group of PCs not influenced by any single element. These blocks of information (for example, block) are made sure about and assured to one another utilizing cryptographic standards. The information is put away in various areas; in this manner, being by definition public and broadly unquestionable along these lines progressively hard to control given that a similar duplicate exists at the same time in numerous spots.

When you have a decentralized ledger and encryption, the security potential is unbound. Today, if a hacker performs a breach, most information is stored in one

I. Ahmed (✉) · M. Darda · S. Nath
SVKM NMIMS, Vile Parle, Maharashtra 400056, India

place, such as a file or database server [2]. But what if a company's data was encrypted and then distributed on a digital ledger. There's already a company working on this solution. Companies would be able to archive off their data, have it encrypted, then distributed. The advantage in this is that even if a hacker could somehow penetrate the Blockchain, they would only be able to retrieve a small piece of the puzzle.

But blockchain technology could change all this. For instance, because of Blockchain's decentralized nature, a group of devices would be able to form a consensus regarding the regular occurrences within a given network and shut down any node that has an anomaly. It is the significance of a democratized structure as the blockchain network has no central power. Since it is an immutable record, the info in it is public for everyone to see [3, 4]. Therefore, anything that hinge on the Blockchain is for its very nature direct, and everyone included is liable for their trainings.

This chapter is organized into seven major sections. First section describes the basic introduction of Blockchain. Next section deals with the methodology and working of Blockchain. Third section summarizes one of the major applications of Blockchain i.e. Ethereum. Fourth section compares and contrast the differences between different types of Blockchain. Fifth section presents brief summary of different Cyber Threats and how Blockchain can prevent Cyber Security from these cyber threats. Sixth section compiles the future aspects and impacts of blockchain technology. In the last section we conclude that how Blockchain is a great innovation for eradicating Cyber Threats.

15.2 Methodology

Blockchain innovation works by making a safe and upfront condition for the monetary exchanges of digital assets, i.e., Bitcoin. Each block's Hash codes protect records in the Blockchain. This is mostly in light of the fact that independent of the size of the data or record, the numerical hash work gives a hash code of a similar length [5]. Along these lines, endeavoring to change a square of information would produce a totally new hash value.

When an exchange has been approved and settled upon by all the nodes, it, at that point, gets added to the digital ledger and secured utilizing cryptography that utilizes a public key available to the various nodes and a private key that must be left well enough alone.

A system that is available to everybody and simultaneously keeps up the client's secrecy without a doubt raises trust issues in regards to the members. Along these lines, to manufacture the trust, the members need to experience a few agreement consensuses protocols, for example, Proof of Work and Proof of Stake [6].

The Blockchain is upfront and shrewd technique too of passing data from X to Y in a completely computerized and safe way. The procedure of making a block starts when a group participates in an exchange. Thousands check this block, maybe a huge number of PCs disseminated around the net. The confirmed block is added to a chain

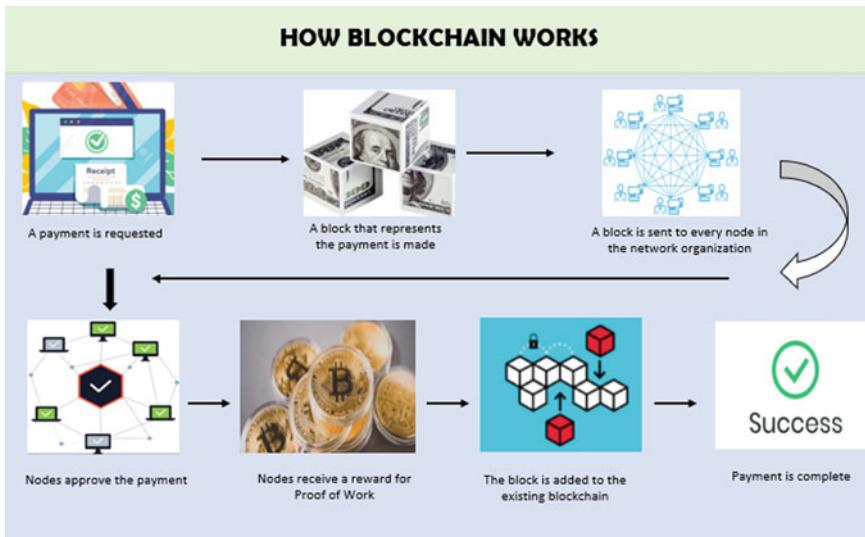


Fig. 15.1 How blockchain works [8]

set aside over the net, making an uncommon record, yet an exceptional business with a unique history [7]. Corrupting a singular report would mean delivering the whole chain in limitless models. Bitcoin uses this model for cash related trades, yet it might be passed on from various viewpoints (Fig. 15.1).

15.3 Ethereum

Ethereum is an open-source processing platform and operating system. It additionally has its related cryptocurrency, ether. It has features like Smart Contracts and Distributed Applications to be assembled and run with not a single fraud, misrepresentation, or interference from a third party. It isn't only a platform yet, besides a programming language running on a blockchain [9]. Ethereum is a decentralized network that has the capacity of running applications in a distributed domain.

15.3.1 Smart Contracts

A smart contract is a PC program or a self-executing deal managed by a P2P network of computers. In simpler terms, it is an agreement between buyer and seller written

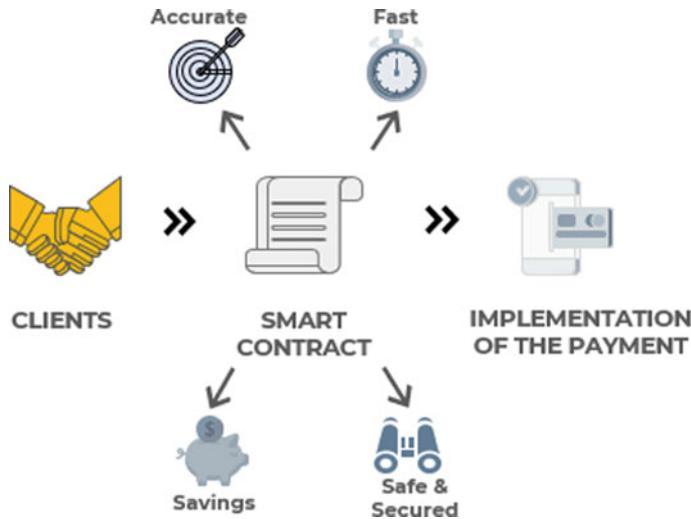


Fig. 15.2 From the book “**Token Economy**” by Voshmgir [10]

into lines of code. It helps exchange money, property, offers, or anything of noteworthy worth in a straightforward, conflict-free way while staying away from the organizations of a third party (Fig. 15.2).

Example

Assume we rent a flat from person X. We can do this with the help of blockchain technology by paying in digital currency. We get a certificate which will hold in our virtual agreement; Person X gives us the computerized passage key, delivered to us by a predefined time and date. On the off chance that the key doesn't come on schedule, the Blockchain discharges a refund. If Person X sends the key before the specified date, the system holds it, which was previously releasing both the expense and critical to us and person X separately when the time shows up. The framework works on the If-Then reason and is observed by several individuals to anticipate a flawless performance. If Person X gives us the key, Person X makes sure to be paid. If we send a certain sum in bitcoins, we get the key. The archive is consequently dropped after the time, and the code cannot be hindered with both of us without the other knowing since all members are at the same time alerted.

15.3.2 Ethereum Virtual Machine (EVM)

If we try developing a smart contract on the Ethereum Blockchain, then coming across the term EVM, short for Ethereum Virtual Machine is sure. EVM can primarily be understood as a framework intended to work as a runtime domain for Ethereum based smart contracts. In Ethereum, with each program, a system of thousands of PCs

forms it. Smart Contracts are aggregated into bytecode, which a component called EVM can read and execute. EVM works in a sand-boxed domain as it is completely disengaged from the principle Blockchain system, and works perfectly as a testing situation. Along with these, anyone who might need to make a smart contract utilizing EVM can do so without interfering with other Blockchain operations.

15.3.3 *Gas*

Gas refers to the expense or estimating value, required to effectively direct exchange or execute an agreement on the Ethereum blockchain platform. It is valued in sub-units of the cryptocurrency ether, known as gwei. Gas quantifies the measure of work miners need to do to remember transactions in a block. The market determines the estimation of gas as the bitcoin market. If a higher gas cost is paid, the node will organize the transactions for benefit.

15.3.4 *DApps (Decentralized Applications)*

dApp utilizes incentives, for example, crypto-tokens and inbuilt consensus mechanisms. A distributed application doesn't have to store its states; in any case, Ethereum-based dispersed application stores confided in states, and these outcomes in a prudent answer for end-users.

The dApp client is required to program the frontend, aside from the user interfaces with the Ethereum blockchain. The clients are regularly written in JavaScript because they can be run in an internet browser, which many of us have.

15.4 Private Versus Public Blockchain

Blockchain is a distributed ledger that records exchanges between every client in the chain. Although it's usually viewed as a single technology, there are various sorts of Blockchain: public and private. From its inception, Blockchain has been permissionless, open to the general public no matter what.

15.4.1 *Public Blockchain*

It's a type of Blockchain network in which anyone can join, i.e., a permissionless blockchain. In a public blockchain, anyone can read, write, or take an interest. This type of Blockchain is decentralized, no one has ordered over the framework, and

they are protected in that the information can't be altered once approved. Data on a public blockchain are secure as it is not possible to expect some modification or change data once they have been passed on the Blockchain.

Public blockchains do carry some necessary inconveniences concerning the business. Organizations are generally increasingly keen on private blockchains to make blockchain solutions with better protection and security.

15.4.2 Private Blockchain

While Private Blockchain is a permissioned blockchain, it puts a few limitations on who is permitted to take an interest in the system and in what exchanges. It is built to give better security over transactions and is appropriate for banking and other budgetary institutions [11]. Private blockchains permit associations to utilize distributed ledger technology without making information public. There is at least one entity that controls the network, and this prompts dependence on third parties to transact. But in private Blockchain, it's different as only the entities participating in a transaction will know about it, while the others won't have the choice to get to it.

Private blockchains can likewise be called consortium blockchains dependent on their limitations and control levels. One of the most mainstream executions of this is Hyperledger Fabric, a permissioned blockchain structure facilitated by the Linux Foundation.

15.5 Cyber Threats and Blockchain Transformation

Cyber Security Challenges have expanded complex, and there is a change in perspective in Threat Landscape. Not regarding significant spending on heritage security items, advanced cyber-criminals are bypassing these protections effectively, making the life of security Professional hopeless. How about we take a look at this present reality. The Chinese government and their military, the People's Liberation Army (PLA), have been blamed for accessing technology and trade secrets unknowingly, regularly from private organizations worldwide. We always imagine that China wants to obliterate the US. However, that is not true. China essentially needs to be the superpower and needs to be a technology chief. In the long run, it requires every American, and even the remainder of the world, to be an innovation subject to the Chinese market. Due to this, the outcome is that the Chinese cybercriminals always spy activities focusing on worldwide organizations and government organizations to assemble free trade secrets. Sometimes political parties gather essential information using advanced analytics of their citizens to foresee future election results.

15.5.1 New Threat Landscape

Cybercriminals have changed in form, capacity, and refinement. The principle distinction is the new dangers are conclusively determined by people, rather than past age assaults, which were malware-based assaults like viruses, trojans, worms, etc. When a cybercriminal finds a defenselessness system and decides how to access an application, they have all that they have to manufacture an infection for the form; thus, it is essential to creating solid helplessness the network management.

15.5.1.1 Ransomware

Ransomware is malware in which data on a casualty's PC is encoded, and payment is requested before giving them getting it [12]. Ransomware is one of the most inclining and exceptional yield kinds of crimeware. It has pulled in a tremendous measure of media included in the previous two years. The ransomware creator has the administration over the dark web, which permits any purchaser to make and adjust the malware.

15.5.1.2 Distributed Denial-of-Service (DDoS) Attack

A distributed denial of service (DDoS) attack is a malignant endeavor to make an online help inaccessible to clients, mostly by incidentally hindering or suspending the services of its facilitating server [13]. But in distributed denial-of-service (DDoS) attacks happen when numerous machines work together to assault one network or system. DDoS attacks might be joined with an extortion danger of all the more disastrous attacks except if the organization pays a cryptocurrency ransom. DDoS attacks have become a regular risk, as they are usually used to render retribution, lead blackmail, activism, and in any event, for cyberwar.

15.5.1.3 Insider Threat

An insider threat is a security risk that begins inside the focused-on association, at the point when an insider deliberately or inadvertently abuses access to adversely influence the classification, respectability, or accessibility of the organization's primary data or frameworks. They could be an expert, previous worker, colleague, or panel member. Traditional safety efforts will result in the global spotlight on outer or third-parties' dangers and are not generally fit for recognizing an interior danger radiating from inside the association.

15.5.1.4 Data Breach

A typical case of a cyber threat is a Data Breach, which is a security incident wherein data is gotten to without approval. It may incorporate the mishap or burglary of your Aadhar Card Number, bank details, personal healthcare data, passwords, or email. Data Breaches are achievable because of weak passwords, missing anti-virus patches that are abused, or lost or taken PCs cell phones, laptops. Cybercriminals regularly hamper information breaks, and there are likewise episodes where ventures or government offices accidentally uncover delicate or private information on the web.

15.5.2 Defender's Interpretation

In the wake of understanding the developing cyber threats and the absolute best cyber-attacks, it is imperative to figure out our self-defense. These cyber-threats groups have all that they have to find an association's benefits and afterward discover the vulnerabilities to assemble their weapons appropriately. Cyber threats prompt a vast worry for organizations that have been non-versatile, here and there for more than decades, yet how about we acknowledge the way that there are a decent number of bodies who have been splendid in accomplishing cyber cleanliness and better resistant cyber systems. We should concentrate on a portion of these bodies, including governments and organizations.

15.5.2.1 Governments

As government services go computerized, cybercriminals are spotting new open doors for false claims and theft. The government consistently attempts to concentrate on actualizing these innovative systems to safeguard against and moderate cyber-attacks. Significantly, government authorities become better at securing their primary resources.

15.5.2.2 India

Taking into account the developing occurrences of financial cybercrimes, including cheats utilizing cards and e-wallets, Home Minister Rajnath Singh has requested the fortifying of the surveillance and legal systems to check the hazard [14]. That is why in February 2017, the Indian government's Computer Emergency Response Team (CERTIn) propelled Cyber Swachhta Kendra, a Botnet Cleaning and Malware Analysis Centre to make secure Indian the Internet through distinguishing and cleaning bots in client endpoints.

15.5.2.3 The United States (US)

As a significantly developed economy, the United States is exceptionally reliant on the Internet and along these lines extraordinarily exposed to cyber-attacks. The United States Department of Defense notices the utilization of PCs and the Internet to lead fighting on the Internet as a threat to national security yet besides as a platform for assault [15]. Because of which US President Donald Trump marked an official request on May 11, 2017, that spreads reinforcing the cybersecurity of the government network, underscoring responsibility, an adjustment of the structure to improve its basic framework, and modernizing existing cybersecurity structures.

15.5.2.4 Europe

The European Union is reinforcing its cybersecurity rules to handle the expanding danger acted by cyber-attacks like well as to make the most of the chances of the new advanced age. The European Union Agency for Network and Information Security (ENISA) fills in as a focal point of skill and greatness for both part-state and EU establishments identified with system and data security [16]. On April 9, 2019, the Council received a guideline called the Cybersecurity Act which presents:

- An arrangement of EU-wide affirmation plans
- An EU cybersecurity organization to update and take control from the current European Union Agency for Network and Information Security (ENISA).

15.5.2.5 Endpoint Detection and Response (EDR)

Endpoint security is the foundation of IT security, so it put significant time and thought into this rundown of top endpoint detection and response (EDR) sellers. It gives security groups a concentrated stage for ceaselessly observing endpoints and reacting to occurrences as they emerge, frequently utilizing automated response.

Main aspects of EDR:

1. Exhaustive Unified Data
2. Broad Visibility
3. Real-Time Response
4. Incorporation with Other Security Tools.

15.5.2.6 Cyber Threat Intelligence (CTI)

Like every other intelligence, cyber threat intelligence gives a value add to digital threat data, which decreases vulnerability for the shopper while supporting the purchaser in recognizing dangers and openings. The system is a cycle since it identifies understanding gaps, unresolved requests, which guidelines new grouping

essentials, this way restarting the information cycle. Intelligence experts recognize knowledge holes during the investigation stage.

15.5.3 By What Means Can Blockchain Help?

Blockchain-based arrangements are among the generally thought about alternatives. And it's not just common among business pioneers. As of late, NASA chose to execute blockchain innovation to help cybersecurity, and forestall denial of service and different attacks on air traffic administrations. Blockchain is rising as an entirely reasonable innovation with regards to safeguarding organizations and various entities from cyber-attacks.

15.5.3.1 PKI-Based Identity with Blockchain

Public Key Infrastructure (PKI) can be followed back to the 1970s when significant encryption forward leaps from a couple of British intelligence office designers molded the eventual fate of key distribution [17]. A certificate authority (CA) fills in as a mediator for these transactions. It ensures the genuineness of the public key, making it workable for a beneficiary of information to approve the transaction's content. But with the help of Blockchain, an innovative concept is achieved, which is a Decentralized Public Key Infrastructure (DPKI) that accomplishes verification over public systems without relying upon a solitary third-party that can bargain the trustworthiness and security of the system. Blockchain works with a trustless methodology that permits both trusted and untrusted gatherings to speak with one another. With DPKI, any content will be a type of mystery property.

A conventional blockchain can replicate the signature functionality of a PKI for approving exchanges. What's more, it gives the advantage that, with the help of a consensus mechanism, no central CA is required, which significantly diminishes the danger of an attack on that vector.

15.5.3.2 2FA Authentication with Blockchain

Two-factor authentication (2FA) gives an additional layer to the current credential-based system protection as an answer for this radically developing issue. It includes another significant segment of security you can set up to keep your wallet secure. 2FA is a critical, easy-to-understand, friendly tool that should be consistently utilized, at whatever point.

Although despite everything, experiences the downside of having the centralized database store a rundown of secret client data. The central database can be altered or tainted by focused dangers, and this can prompt massive information breaches. With the assistance of Blockchain can genuinely change the 2FA framework to accomplish

an improved security strategy. By structure, Blockchain is a decentralized innovation that permits exchanges of any sort of significant worth among numerous members without the contribution of a third-party. By utilizing Blockchain, we can guarantee that this sensitive data never stays on one database; rather, it very well may be inside blockchain hubs that have immutability and can't be altered or erased. With blockchain-based 2FA in this framework, client devices will be validated by a third-party 2FA supplier through the blockchain network. Each party in the blockchain system will safely hold the endpoint data and enact the 2FA framework to create a second-level password.

15.5.3.3 Blockchain-Based DNS Design

An enormous number of studies have endeavored to take care of common DNS issues utilizing blockchain-based decentralization plans, such as Namecoin, BNS (Blockstack Naming service), ENS (Ethereum Name Service), and Handshake [18].

Namecoin is the primary task of joining an area name administration with a blockchain. Blockstack based Namecoin, relocates area name administrations to the Bitcoin blockchain, and isolates the control and info layers to advance network security. ENS is a distributed, public, and extensible naming framework dependent on the Ethereum, which is midway kept up by a select arrangement of signers. BNS straightforwardly forsake similarity, receiving another new domain namespace and another domain name allocation system. The ENS group is endeavoring to be good with DNS on high-level domains. Handshake proposed a root zone the executive's system dependent on a blockchain, which takes care of the centralization of existing root zones by blockchain innovation.

15.5.3.4 DDoS Mitigation Using Blockchain

As examined above, Distributed Denial of Service (DDoS) attacks are the same old thing. However, ongoing assaults are expanding in seriousness, intricacy, and recurrence and have like this become a standard worry for organizations and private clients the same. Organizations are starting to investigate Blockchain to forestall and alleviate DDoS attacks. Working the DNS on a blockchain would guarantee that attacks are not focused on a brought together to source, devastating it.

Then again, organizations are likewise utilizing blockchain technology to make a decentralized system of servers that can rapidly send bandwidth capacity to different servers confronting attacks. The attacked server would then be able to withstand the DDoS attacks by engrossing the overabundance traffic utilizing the extra bandwidth. Organizations can be distributed between different server nodes that give high strength and evacuate the single purpose of failure to prevent systems from DDoS attacks.

15.6 Future Work

Cybersecurity is one of the most flexible ventures in which organizations see another variety of danger every other day. That is why it is essential to set up an appraisal of potential hazards and potential security advancements to keep predicting client and partner trust. The mix of block-building algorithms and hashing makes Blockchain an incredible arrangement in the cybersecurity portfolio, as Blockchain is changing the cybersecurity solution in a few different ways.

15.6.1 Future Impacts of Blockchain

For example, Akasha, Steem.io, or Synergo are distributed social organizations that work like Facebook, however, without a focal platform. Rather than depending on a centralized association to deal with the system and specify which content ought to be shown to whom, these stages are run in a decentralized way, accumulating crafted by different gatherings of peers, which facilitate themselves, just and only, through a lot of code-based standards revered in a blockchain. By empowering peer-to-peer transactions, the blockchain technology makes way for direct collaboration between groups—a decentralized sharing economy outcome.

Supply chains contain complex systems of providers, makers, wholesalers, retailers, examiners, and customers [19]. A blockchain's IT foundation would smooth out work processes for all gatherings, regardless of the size of the business system. Moreover, a common foundation would give inspectors more exceptional visibility into members' exercises along the worth chain. Blockchain can drive cost-sparing efficiencies and to upgrade the customer experience through recognizability, straightforwardness, and detectability.

Consolidating Blockchain and IoT permits organizations and even shoppers to legitimately adopt the “multiple times more data” that is produced by the roughly 30 sensors in your vehicle, motor sensors in planes estimating 5000 components for each second, and billions of different sensors in all aspects of our day by day lives figuring things like climate impacts, contaminations, area, fuel, temperature, moistness, sound, vibration, wind opposition, pressure, weight, power, and over 300 different kinds of components.

Blockchain could go about as an incomprehensibly secure and precise approach to store singular data, which is utilized for KYC and AML consistency. On the off chance that Blockchain is used for KYC and AML consistency, a customer could make a solitary “block” by taking care of their information, which understandings for KYC and AML consistence [20]. The underlying one is that a customary KYC and AML Blockchain library can be made, and different banks and money related establishments can utilize it. Another critical edge is that a KYC and AML vault is additionally made for intra-bank use. Blockchain can significantly enliven and bring down expenses for KYC.

With the stock market over the globe, increasingly holding onto Blockchain's local capacities as the reason for advertising exchanges, numerous foundations investigate how blockchain technology can be utilized in the securities exchange. Blockchain offers enormous potential for following protections loaning, repo and edge financing, and checking significant hazards.

Blockchain can be the answer to compatibility, belief, and truthfulness issues in divided market structures. The innovation can have suitable use in clearing and settlement, while safely robotizing the post-exchange process, enabling desk work of exchange and legitimate possession move of the security. It can kill the need for third-party participation to a considerable degree. The standards and guidelines would be in-worked inside smart contracts and official with each exchange request to enrol exchanges with the Blockchain arrange to go about as a controller for all trades.

15.7 Conclusions and Future Scopes

Overseeing cybersecurity over an undertaking is a unique challenge. The stakes have never been higher, with the pace of cyber-attacks expanding each year. Notwithstanding Blockchain being a moderately youthful innovation with just a long time since initiation, it has increased critical consideration and is alluring because of a portion of its extraordinary properties. As depicted in the paper, various attacks focus on the Blockchain itself. Until this point, the vast majority of these were intended to take cryptocurrency or coerce cash in ransomware plans.

Blockchain has different applications, such as public records, private records, money related exchanges, ID, and so on. Mainly it adds to key flexibly chain destinations, including speeding up, confirming manageability, lessening dangers, and so forth. Mainly it adds to core flexibly chain destinations, including speeding up, confirming manageability, lessening dangers, and so forth. Insurance, e-casting a ballot, closeout, lawful issues, and so forth are genuine models where smart contracts function admirably. This examination uncovered that this innovation is suspected to improve everything from improving information integrity and digital identities to forestall DDoS assaults and data breaches.

We expect that the first applications that require unwavering quality and information security will soon change to this innovation since the blockchain core is protected and reliable. We accept to presume that approval and computational expenses in mining blocks. Blockchain upgrades cybersecurity and data affirmation; particularly, it has the potential to improve massive information security and healthcare services cybersecurity.

References

1. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System. Cryptography Mailing list at <https://metzdowd.com> (2009)
2. Kury, T.: Russians Hacked into America's Electric Grid. Here's Why Securing It Is Hard. Government Technology, July 2018
3. Mission Support Center, "Cyber Threat and Vulnerability Analysis of The U.S. Electric Sector," Idaho National Laboratory, 2016
4. Huang, Z., Su, X., Zhang, Y.: A decentralized solution for IoT data trusted exchange based-on blockchain. In: International Conference on Computing and Communication Technologies, 2016
5. How Blockchain Technology Works. Guide for Beginners, Coin telegraph. (Online). Available: <https://cointelegraph.com/bitcoin-for-beginners/how-blockchain-technology-works-guide-for-beginners>
6. Amaba, D.B., Leed, P.C., Ahram, D.T., Sargolzaei, D.A., Daniels, D.J., Sargolzaei, D.S.: Blockchain Technology Innovations, p. 5, 2017
7. Bahalul, A.K.M., Haque, Rahman, M.: Blockchain technology: methodology, application and security issues (Feb 2020)
8. How blockchain architecture works? <https://www.zignuts.com/blogs/how-blockchain-architecture-works-basic-understanding-of-blockchain-and-its-architecture/>
9. Marr, B.: A very brief history of blockchain technology everyone should read, Forbes, 16 Feb 2018. Available: <https://www.forbes.com/sites/bernardmarr/2018/02/16/a-very-brief-history-of-blockchain-technology-everyone-should-read/#19c60b067bc4>. Accessed 15 Feb 2019
10. Voshmgir, S.: Token economy: how blockchain and smart contracts will revolutionize the economy, pp. 105–107, 2019
11. Kim, J.-T., Jin, J., Kim, K.: A study on an energy effective and secure consensus algorithm for private blockchain systems (PoM: Proof of Majority). In: 2018 International Conference on Information and Communication Technology Convergence (ICTC)
12. Paquet-Clouston, M., Haslhofer, B., Dupont, B.: Ransomware payments in the bitcoin ecosystem, 2018
13. Flashpoint. Mirai Botnet Linked to Dyn DNS DDoS Attacks. Accessed: 18 Dec 2018. (Online). Available: <https://www.flashpointintel.com/blog/cybercrime/mirai-botnet-linked-dyn-dns-ddos-attacks/>
14. Botnet Cleaning and Malware Analysis Centre (Cyber Swachhta Kendra) <https://www.cyberswachhtakendra.gov.in/about.html>
15. National Cyber Strategy of the United States of America, <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>
16. Training for Cybersecurity Specialists, <https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/blockchainw>
17. Shbair, Y., Wallborn, A.: A blockchain-based PKI management framework. In: IEEE NOMS Conference, 2018
18. Lepoint, T., Ciocarlie, G., Eldefrawy, K.: BlockCIS—a blockchain-based cyber insurance system. In: 2018 IEEE International Conference on Cloud Engineering (IC2E), IEEE, pp. 378–384, Apr 2018
19. Kshetri, N.: 1 Blockchain's roles in meeting key supply chain management objectives. Int. J. Inf. Manage. **39**, 80–89 (2018)
20. Bhaskaran, K., Ilfrich, P., Liffman, D., Vecchiola, C., Jayachandran, P., Kumar, A., Lim, F., Nandakumar, K., Qin, Z., Ramakrishna, V., Teo, E.G.: Double-blind consent-driven data sharing on blockchain. In: 2018 IEEE International Conference on Cloud Engineering (IC2E), IEEE, pp. 385–391, Apr 2018

Chapter 16

Gun Tracking System Using Blockchain Technology



Shagun S Lokre, Vihas Naman, Shanmukhi Priya,
and Sandeep Kumar Panda

Abstract One of the major concerns for the government in terms of security is the safety of the citizens. We have come across many cases in which the individuals have access to the ammunition without having the required license. Inadequacy in the management of weapons, especially those which remain reserved is the major contributing factor. Individuals submit counterfeit documents to some third party dealers who help them in getting a fake arms license. That's not all, no one knows whether the individuals who use the ammunition with the fake license have any criminal background at that time. The production of such reserved deteriorating weapons is creating a huge problem leading to an unsafe environment among the citizenry. In this chapter, we lay forward a model that helps to overcome these challenges with the help of blockchain technology. In our model, we provided a simple solution on how the transfer of guns can take place between the dealer and the seller using digital signatures and a digital gun safe just like a bitcoin (BTC) wallet which stores each and every information about an individual securely and it helps us in identifying whether the person who has a weapon holds an original arms license or has a fake one and also checks whether the person has a previous criminal record on his name. Since blockchain is immutable and hackproof, this technology can be used to eliminate the above claims and improve the ownership, traceability of the weapon and keeps the records securely inside the digital safe. Although the use of blockchain technology has some constraints when a large number of records are to be stored inside the safe, its properties can be used to improve the current scenario.

Keywords Government · Ammunition · Blockchain · Bitcoin wallet ·
Immutable · Gun safe

S. S. Lokre (✉) · V. Naman · S. Priya · S. K. Panda

Computer Science and Engineering Department, IcfaiTech (Faculty of Science and Technology),
ICFAI Foundation for Higher Education (Deemed to be University), Hyderabad, Telangana, India

S. K. Panda

e-mail: sandeepanda@ifheindia.org

16.1 Introduction

In today's world, the supply of illegal weapons has increased drastically and most of these weapons are being sold in the black market and on online sites such as the dark web [1]. Though the arms business is small in the capacity as compared to other products smuggled online, its consequences on security are quite significant. Despite efforts being made for regulating firearms, there has been news about people carrying ammunition wherever they go with them for their safety concerns. But, most of these people do not have a valid arms license for carrying any kind of weapon with them [2]. It has become easy for conmen to get a fake arms license from a third party dealer by providing fake documents [3]. Due to this, tension is prevailing among the people about their safety of roaming freely in the environment. It has become necessary to track these people and find out if they hold a valid arms license or not. Therefore, we intend to use blockchain technology to eliminate the above-listed problems. In this model, we provided two solutions. One for forming an agreement between the dealer and the seller without any involvement of third party and two, to have a digital gun safe, which is similar to a bitcoin (BTC) wallet which securely stores each and every information about the person owning a gun or wanting to purchase a gun [4]. Forming an agreement between any two parties requires a signature. Normally these signatures can be tampered and the document is accepted without knowing that the signatures are not valid and that the document is not legal. So to avoid this kind of problem we make use of digital signatures. Digital signature is one of the way to ensure that the message is not tampered and that it maintains the integrity of data. Once the agreement is formed between the dealer and the seller, the transfer of weapons take place. At the time buying the weapon the customer will be provided with a Digital Gun Safe same like Bitcoin Wallet (BTC). This digital safe can be opened only through biometric data such as a retina scan or with the help of a fingerprint [5]. Ahead of purchasing the gun, the receiver should make the required background checks and if the information provided by the receiver is proven to be correct, then the transfer of ownership takes place where the buyer has the right to purchase a weapon. If the individual fails to provide the correct information then the transfer of ownership gets contradicted and will be recorded in the individual's digital gun safe. This helps in reducing the involvement of any third party dealer. In this way, all the legal/illegal information about an individual will be recorded in the gun-safe and it becomes easy for the authorities to track them. Since blockchain is immutable, the details regarding the transactions made from one gun safe to the other, that are recorded on the blockchain cannot be tampered with. The transactions recorded in the gun safe can only be accessed by the individual's biometric and private key and hacking these transactions is impossible [6]. With the help of this model, it will be easy for us to track these people and reduce the crime rates in countries where such practices are common [7].

16.2 Prerequisites

Blockchain

We all know that technology continues to constantly advance in a field that aims to beat itself, coming up with remarkable developments one after the other of some paradigm-shifting innovation [8]. Blockchain Technology is one such technology that became a hot topic in today's world. Blockchain can be characterized as a decentralized public distributed ledger. On the off chance that we go through the definition we will recognize the 4 fundamental terminologies (i.e. decentralized, public, distributed, ledger) to understand. Let us see what these terminologies mean:

- Decentralized: Unlike a centralized system where all the information is being held by a central authority, where hacking the system becomes pretty simple, blockchain technology follows a decentralized system in which the information is dispersed among all the nodes that participate in the system, this lowers the risk of systematic failure [9].
- Public: A public blockchain is a permissionless blockchain [10]. It can be viewed publicly which means that anybody can take part in the network, read and write in the blocks. Public blockchains are decentralized and are secure such that the data cannot be changed once validated on the blockchain.
- Distributed: The data is stored on multiple systems or multiple nodes on the blockchain. This will ensure smooth retrieval of data even when one of the nodes is malfunctioning.
- Ledger: In simple terms, a ledger is a list of records [11]. These records can be of any type such as transactions or items etc. A blockchain-based ledger has properties such as immutability which prevents tampering of data and integrity through hash functions and is secured through cryptography [12].

With its intuitive applications being powered by its network architecture, blockchain technology has become a front and center of technology with discussions [13]. Being the technology acting at the core of bitcoin and other cryptocurrencies, blockchain is an open, distributed ledger that can record transactions between two or more individuals in a more efficient, verifiable, and permanent way [14].

Cryptography

Cryptography is the hone of creating conventions that avoid third parties from seeing the information. The name itself says “crypt” means hidden or vault and “graphy” means writing. In cryptography, the approach which is used to secure the information is obtained from algorithms by converting messages in such a way that it is very hard to decode it [15]. These algorithms are used to generate cryptographic keys, in digital signing, verification to protect data privacy, and many more. In the present era of computers, cryptography is usually related to the technique where an ordinary plain text is processed to the ciphertext in which the text is intended such that the receiver who receives the text can decode it. This process of converting a plain into ciphertext is known as encryption and the process of converting the ciphertext back

to the original message is known as decryption. Cryptography is taken after by the organizations to go with the goals of:

- Confidentiality: The given information can only be accessed by the person to whom the message is intended to and no other person can.
- Immutable: The given information cannot be altered in storage or transition between the sender and the receiver.
- Authentication: The identities of the sender and the receiver are confirmed. As well as the origin/destination of the message is confirmed.

There are three types of cryptography (Hashing, Symmetric Key cryptography, and Asymmetric key cryptography) but in this model, we will be utilizing Asymmetric Key Cryptography.

Asymmetric Key Cryptography

Asymmetric Key Cryptography, also known as Public-Key Cryptography uses two different keys to encrypt the plain text [16] (Fig. 16.1).

Secret keys are traded over the web or large network. It ensures that malicious people do not take any advantage of using these keys. Note that anyone who has the secret key can decrypt the information that is why asymmetric encryption uses two keys that boots the security system [17]. A public key is made available to anyone who wants to send the message to you. A private key, unlike a public key, is kept secret so that only you can know. A plain text/message can be encrypted using a public key and can be decrypted using only the private key and if the message is encrypted using a private key can be decrypted using the public key. Asymmetric Encryption is far safer and highly secure in terms of sharing any documents over the internet or large network.

Digital Signature

Digital signatures are used to carry out electronic signatures [18]. It is an arithmetic scheme showing the authenticity of the digital messages/documents. A valid

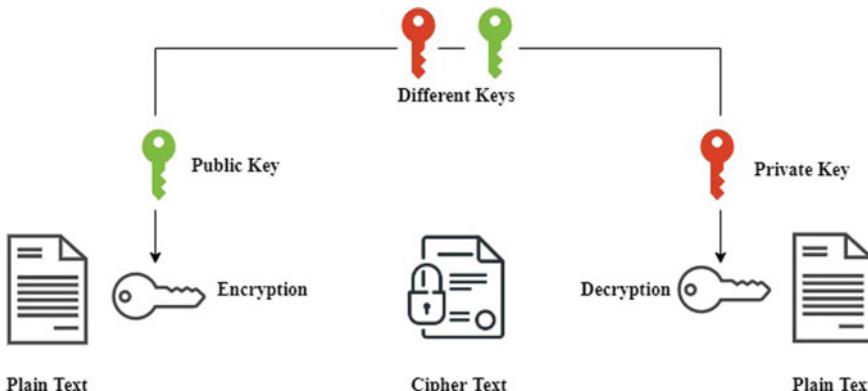


Fig. 16.1 Asymmetric key cryptography

signature gives the receiver reason to believe that the message is generated by an authenticated sender, that the sender cannot repudiate having sent the message and that the message is not altered in transit.

These signatures are identical to the standard handwritten signatures but the one with properly implemented digital signatures is next to impossible to forge. Digital signatures are implemented using asymmetric cryptography as discussed in the above paragraph. One of the advantages of a digital signature is that if a hacker tries to access the information and alter it, then the hash of the modified information and the output presented by the authenticated algorithm will not match and the receiver can deny information by assuming that data integrity was violated [19, 20].

16.3 System Overview

The above Fig. 16.2 represents the nodes that are taking part in this blockchain-based traceability system and how each node in a blockchain network is going to act and that each node in the network is connected to an Ethereum account which shows its identity within the system [21, 22]. Since blockchain is a decentralized system, all the

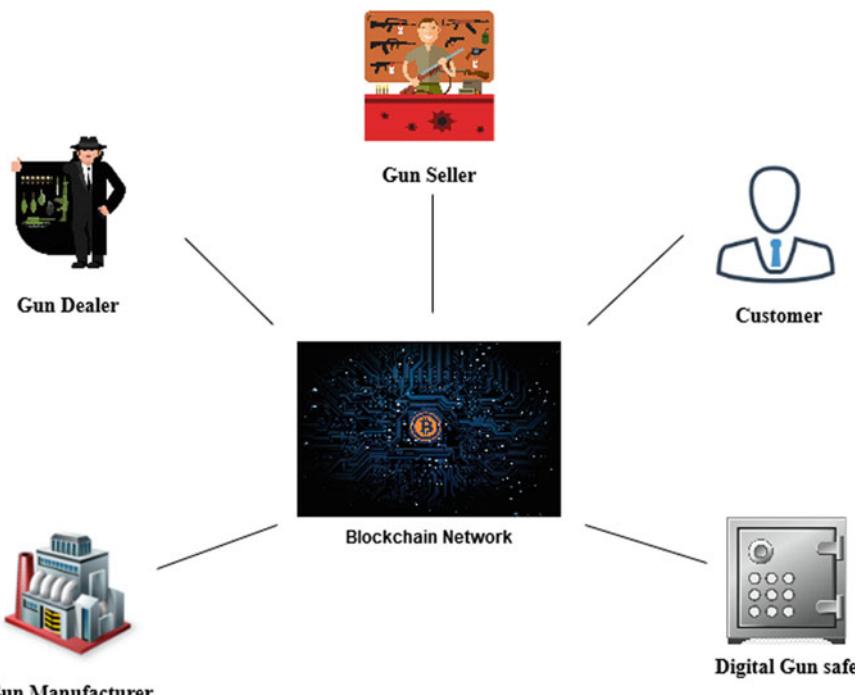


Fig. 16.2 System overview

transactions that happen inside the system will be present with each node that takes part in this traceability system. Let's look at each of the nodes before proceeding ahead:

Gun Manufacturer: The gun manufacturer processes the raw materials provided by the supplier into the desired weapon. At the same time, the manufacturer sells these weapons to the licensed dealer and will be distributed among the licensed shops for sale [23]. The manufacturer is responsible for wrapping the information of the weapon and recording it in the blockchain system.

Gun Dealer: The main role of the dealer is to form an agreement with the licensed seller so that all the transactions that happen between both of them are recorded as a ledger in the system [23]. For making the agreement successful, the seller shop should be a licensed shop with all the necessary documents being recorded in the system.

Gun Seller: Prior to the sale, the seller as well as the dealer should sign an agreement so that the transaction details will be recorded in the system and can be approved for sale [24]. Just like a digital signature, both the parties need to sign the transfer.

Customer: The customer is the final end receiver of the weapon. But before purchasing a weapon, the customer should pass a few background checks for authentication purposes [25]. Once the individual clears the test the transfer of ownership takes place. Once the transfer of ownership and weapon is successful, the individual will be given a digital gun safe where all his personal information such as name, mobile number, arms license, and the weapon information that he is using will be stored inside this safe.

Digital Gun Safe: Like an e-wallet, a digital gun safe is a safe where the individual's information such as name, mobile number, arms license and the weapon information that he is using will be stored. When an individual purchases a weapon, he/she will be given a gun safe which is digital just like a bitcoin (BTC) wallet. This safe is tamper-proof and can only be accessed with the help of biometric data (i.e. fingerprint, retina scan) of the individual [26].

16.4 Working Procedure

Handling the complexities and difficulties in implementing the blockchain in this scenario is of the utmost importance in securing gun safety. How much ever productive blockchain can be, the effort cannot pay off if the data that goes into the ledger is not secured and meticulous. So the solution for the system proposed in the chapter works according to the current cryptocurrency of blockchain technology. When a gun gets manufactured from a licensed manufacturing shop, the manufacturer supplies these weapons to a licensed gun dealer who then supplies them to the licensed gun shops. At the time of supplying the weapon, the manufacturer maintains a record of

the details of the weapons such as how much quantity is to be supplied, the date of supply, etc. This record will be stored securely inside the blockchain.

Once the weapons are supplied to the dealer, the dealer contacts the gun seller and forms a dealership agreement between him and the seller. This is where digital signatures come into the picture. At the time of agreement formation, unlike handwritten signatures, the deal takes place inside the blockchain network. First, the dealer creates a document (Fig. 16.3) that includes the information that is required to sign and form an agreement which proves the transfer of ownership.

Next, he hashes the document and encrypts it with the help of his private key. The encrypted hash is known as a digital signature as shown in Fig. 16.4.

Once this is done, the dealer sends the document and the digital signature to the seller where the seller verifies if the received document matches the digital signature or not. As shown in Fig. 16.5, the seller uses the dealers public key to decrypt the digital signature which results in the hash value of the document.

Next, In Fig. 16.6, the seller applies the same hashing algorithm to the document he received and checks if both the hashes match with each other or not.

If it matches then the seller approves from his side and forms a deal with the dealer and if it doesn't then the seller assumes that the document has been altered during the transit which results in the cancellation of the deal.

The above diagram (Fig. 16.7) depicts the overview diagram of the contract deal between the dealer and the seller. With the help of digital signatures, there won't be any third party involvement, and any kind of deals can take place in a fair and transparent manner.

Once the agreement is confirmed in a fair and transparent manner, the assets can now be transferred between the dealer and the seller as per the directives mentioned

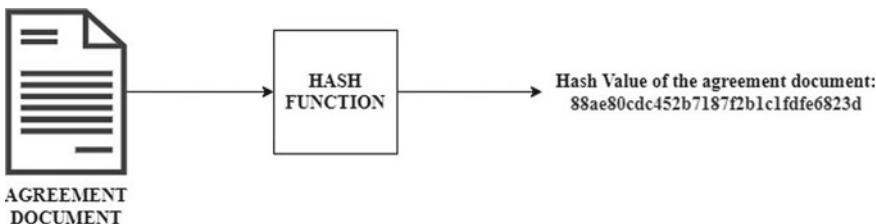


Fig. 16.3 Hashing the document

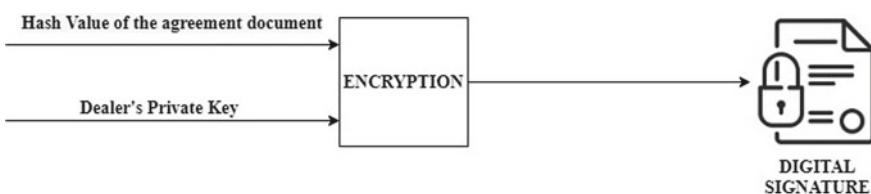


Fig. 16.4 Encrypting the document



Fig. 16.5 Decrypting the document

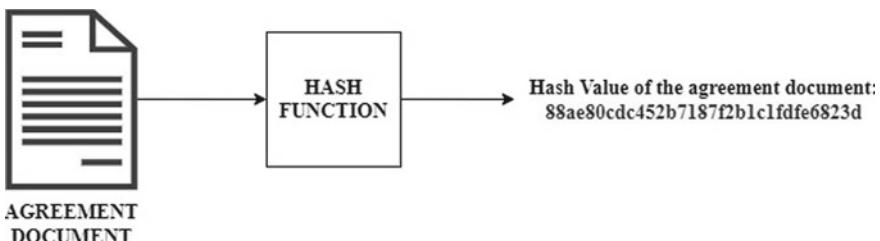


Fig. 16.6 Checking the hash value of the document

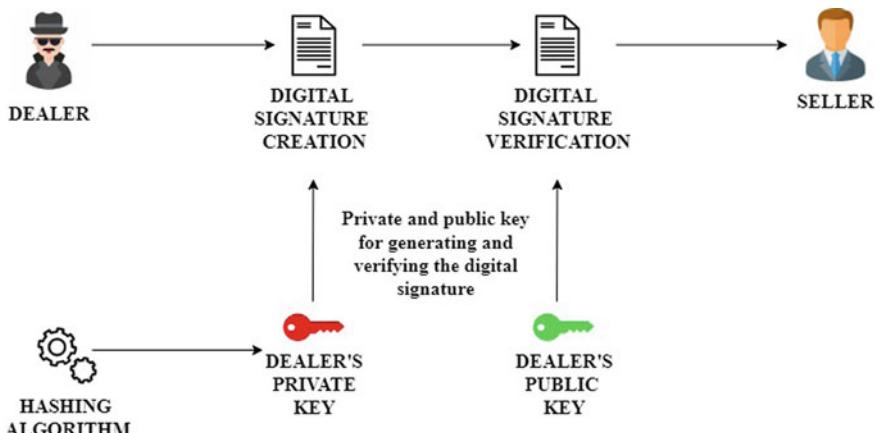


Fig. 16.7 Overview diagram of contract deal

in the agreement document. The gun transaction between the buyer and the seller can take place in a similar way to sending and receiving bitcoins. Before that, the buyer should pass a background check as shown in Fig. 16.8 which includes age verification, valid arms license, crime records, citizenship proof.

Blockchain technology supports peer-to-peer transactions where there is no involvement of any third party who makes the transaction successful. So for transferring and receiving the coins, the buyer and seller use a very safe and secure platform known as “Omni-layer”. Omni is a protocol modeled as a layer over the bitcoin which allows us to send and receive the transactions. The main advantage of Omni is that it can transform into any currency using the smart contracts on the layer. So when a

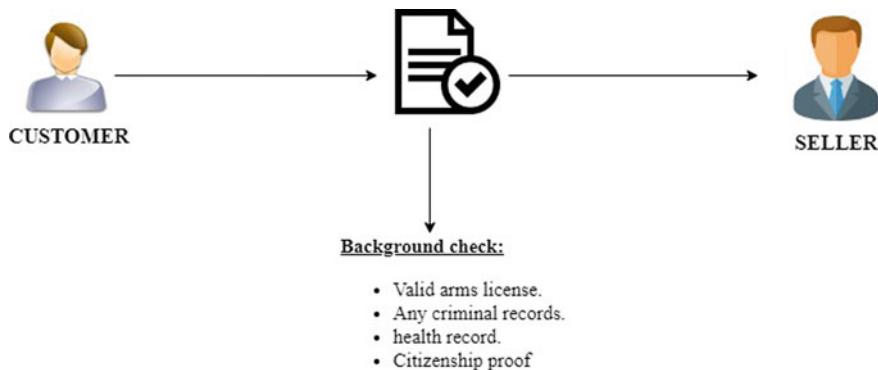


Fig. 16.8 Overview diagram of background check

buyer wants to make any transaction, he can transfer the money irrespective of the currency as the Omni protocol converts any currency into omnis with the help of a smart contract. For the transaction to take place just like a bitcoin wallet, we can use the Omni wallet which is safe, secured, easy to use and multi-currency support. Once the safe transfer of gun and ownership takes place, the buyer will be provided with a gun safe, known as “electronic digital gun safe” as proposed by Heaston. Unlike a physical gun safe, this gun-safe is digitally secured which contains information about the owner.

This gun safe can be accessed with a fingerprint scan, or with a retina scan of the owner. The main purpose of providing this gun safe is to track each and every information about the owner and the gun that he is using (Fig. 16.9). If a crime is committed and if people had to trace a particular weapon, then the safe provides each and every information regarding the person as well as the weapon that he used to commit the crime.

Tracking guns with advanced blockchain protocols will help regulate overall gun significance upon society, so reasonable gun control measures can be implemented.

16.4.1 Algorithm Design

Explanation of Algorithm 1: msg_digest()

The function `msg_digest()` allows the dealer to sign an agreement to deal with the seller. For signing a message the dealer creates a document and then hashes the document with the help of `crypto.SHA256` which gives the hash value of the document. This hash value is the fixed numeric representation of the message that gets assigned to the `msg_digest` function. The function `sign_message` takes two values `pvt_key` and the numeric value of `message`. Once the document gets

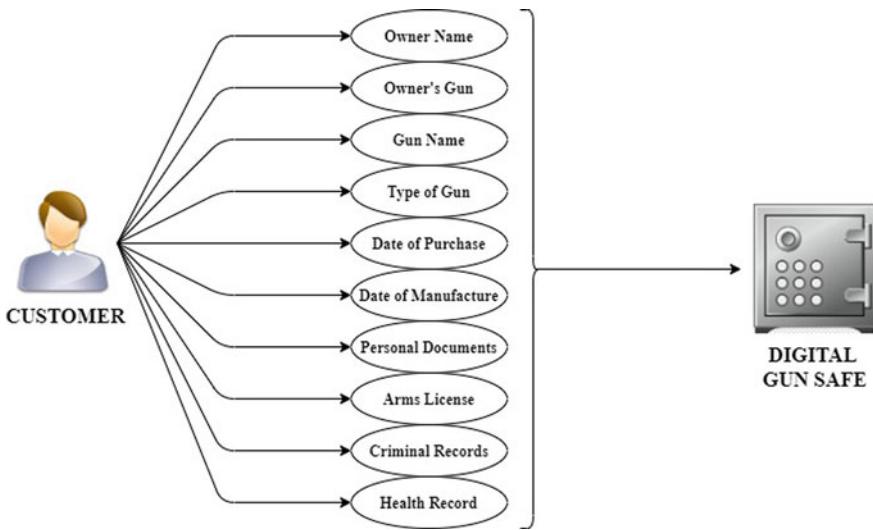


Fig. 16.9 Pictorial representation of the digital gun-safe and what it contains

converted into its equivalent hash value, the dealer uses his private key (`pvtkey`) to encrypt the document.

```
function msg_digest(message)
{
    var m=msg_bytes("Signed message\n").concat(msg_bytes(message));
    return crypto.SHA256(crypto.SHA256(m, {asbytes:true}), {asbytes:true});
}

function sign_message(pvtkey, message)
{
    if (! pvtkey)
        return false;
    var signature=pvtkey.sign(msg_digest(message));
    var address=message.gethash();
}
```

Explanation of Algorithm 2: document_verify()

The function `document_verify()` allows the seller to verify whether the document that he received and the document that has been hashed is the same or not. For verification of the document, the seller uses the dealer's public key (`pub_key`)

to decrypt the hash value to its equivalent message using `base64Tobytes`. If the hashed value and the message turns out to be different then the program throws an error with which the seller gets to know that the document has been tampered with and that the deal cannot be signed.

```
function document_verify()
{
    if (!pubkey) {
        return false;
    }
    var signature=pubkey.sign(msg_digest(message));
    var address=message.gethash();
}
try {
    var sig=message.base64Tobytes(signature);
}
catch(err)
{
    return false;
}
```

16.4.2 Implementation

As we can see that the model that is proposed in this chapter requires execution of multiple steps. The agreement deal has to be signed with the seller, the seller sells the product to the buyer and the buyer gets an electronic gun-safe which stores the information of the buyer securely. Therefore, for the purpose of clarity we will be looking into the first implementation i.e. the implementation of digital signature between the dealer and the seller.

The execution requires creation of two files:

- **Signing_message.js:** This file includes the code that is required for signing the document and encrypting the file with the help of private key.
- **verify_message.js:** This file includes the code that is required for verifying the document and decrypting the file with the help of public key.

After completing the code, the next step is to execute these codes at a time. For that we can create a HTML file in which we can link the above two codes so that we can execute it simultaneously.

As you can see in Fig. 16.10, when we open the HTML file the browser opens up a new window where the digital signature takes place. This page includes 2 links. One is for signing the message and another is for verifying. Upon clicking the sign link, the webpage gets directed to the sign page as shown in Fig. 16.11.

This page consists of entries like private key, address, message and signed message. The dealer now enters his private which has an option of show and hide. According to the dealer's choice he can select the option. Once he enters his private key, an address hash value gets generated as seen in Fig. 16.11. This address value is nothing but the address of the document that is signed by the dealer. In the message box, the dealer writes the message i.e. the document that is to be signed. Once these details are entered and when the dealer clicks on the sign message button, a hash value of the document that is to be signed is generated as shown in Fig. 16.12. The signed message generated for the document and the public key of the dealer is now shared with the seller for the verification purpose.

For the verification purpose, the seller now clicks on the verify link (Fig. 16.10) which is directed to the verify message page. On this page the seller enters the



Fig. 16.10 Homepage

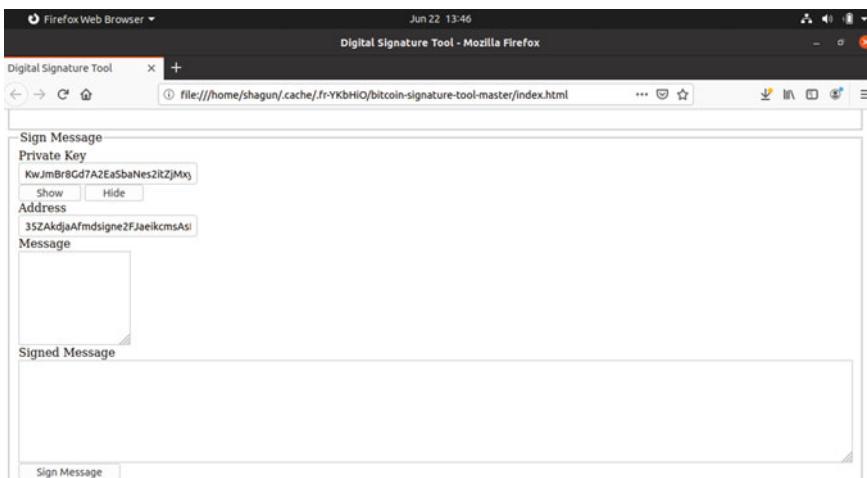


Fig. 16.11 Signing message

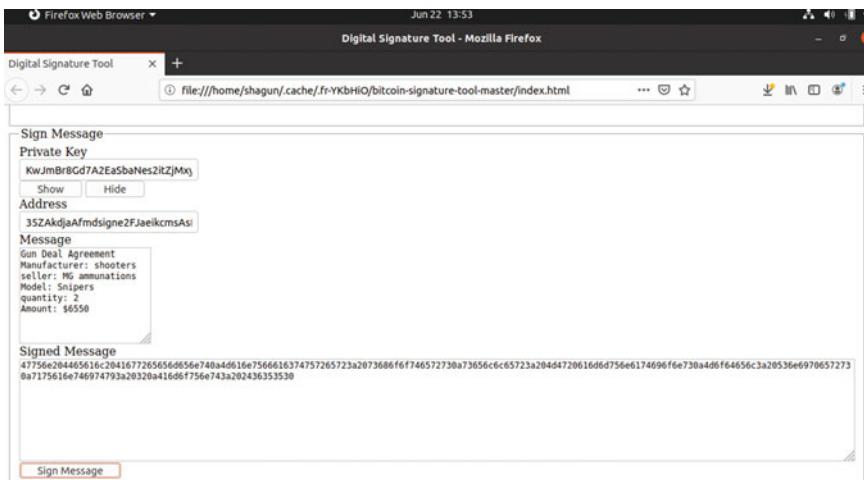


Fig. 16.12 Signed message (hash value)

public key and the signed message hash value for verification purposes as viewed in Fig. 16.13.

Once the seller enters the public key and the signed hash value of the message, he then clicks on the verify button, which decrypts the signed hash value into its equivalent message (Fig. 16.14) which helps the seller to verify whether the decrypted message matches with the original message.

With this, the seller can confirm that the message has not been tampered and that the original message matches with the decrypted message. You can see that in the

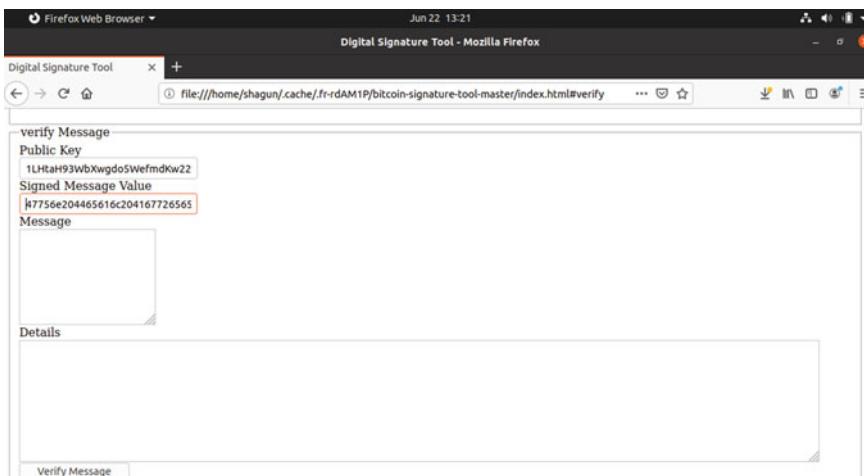


Fig. 16.13 Verify message

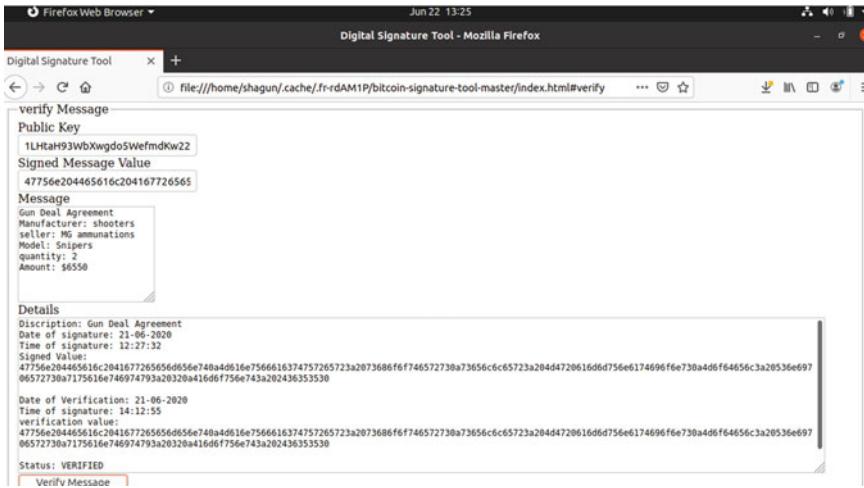


Fig. 16.14 Verification

details section which shows the date and time of the signing document and date and time of verification of the document.

16.5 Security Analysis

The blockchain tracking system described in this chapter meets the following security requirements:

Durability and Reliability: Since blockchain is a decentralized network, it does not have a central point of failure and is good at resisting the malicious attack [27].

Non-repudiation: Any signature that is affected using a private key, is known/owned by the owner and that he cannot contradict his/her signature attached to the document i.e. the signator cannot affirm effectively that they did not sign a letter, and that their private key remains hidden as well. [28].

Data Integrity: Once the document is signed and received by the recipient it guarantees that the contract is authentic, reliable and defends against unwanted manipulation of the recipient during transmission. If any tampering of a document takes place, then it produces a whole new digital signature.

Authentication: As long as the owner's private key is safe and secure with him, the recipient can use the public key to confirm that the signature was created by the owner and no one else.

Timestamping: Timestamping is the most important security feature when it comes to digital signature of such legal documents [29]. It Provides the details of time and date of the document existed at a point in time and are unchanged.

As you can see that the above mentioned security features are enough to make our system immutable, transparent, tamper proof and most important trustless exchange which does not involve any third party strongly eliminating the risk of counterparty.

16.6 Conclusions

The main motive of this chapter is to find a viable solution for reducing the violence and crime rate especially the crimes committed using illegal firearms. With blockchain coming into the picture this can be reduced to quite an extent. The blockchain protocol is the most precise system to track a gun flow from the manufacturer to the end-user who receives it. Its salient features such as transparency, immutability, and decentralization helps the network to be highly secure against any kind of tampering information or anything that looks malicious. With this technology, the agreement deal between the dealer and the seller happens smoothly compared to the existing system in which there is an involvement of the third party. With each and every information being stored in the blockchain platform, makes the transaction process in a very transparent manner without any altering of the data. Undergoing a background check before the transfer of the ownership helps to identify whether the eligibility of the buyer regarding the correct licences. An “electronic digital gun safe”, just like a BTC wallet which is given at the time of purchasing the gun helps to track the person and the kind of weapon that he is using. Blockchain technology, when applied in improving tracking systems, automatically creates a climate where the crime rates decrease and the society need not be scared of ammunition anymore.

References

1. Fincham, D.: Assessing the viability of blockchain to impact the antiquities trade. *Cardozo Arts & Ent. LJ*, 2019—HeinOnline
2. Caplan, D.I.: The Right of the Individual to Bear Arms: A Recent Judicial Trend—*Det. CL Rev.*, 1982—HeinOnline
3. Baza, M., Lasla, N., Mahmoud, M., et al.: B-ride: Ride sharing with privacy-preservation, trust and fair payment atop public blockchain ... on Network Science 2019—ieeexplore.ieee.org
4. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system—2019—git.dhimmel.com
5. repository.library.georgetown.edu/handle/10822/1056615
6. Qu, H., Yan, Z., Lin, X.J., Zhang, Q., Sun, L.: Certificateless public key encryption with equality test. *Information Sciences*. Elsevier (2018)
7. Keane, K.: Does bitcoin use affect crime rates? 2020—kb.gcsu.edu
8. Allen, D.W.E.: Blockchain innovation commons. *SSRN Electron. J.* 2017—academia.edu
9. Subramanian, H.: Decentralized blockchain-based electronic marketplaces. *Communications of the ACM*, 2017—dl.acm.org

10. Neudecker, T., Hartenstein, H.: Network layer aspects of permissionless blockchains. *IEEE Communications Surveys & ...*, 2018—ieeexplore.ieee.org
11. Hughes, A., Park, A., Kietzmann, J., Archer-Brown, C.: Beyond Bitcoin: What blockchain and distributed ledger technologies mean for firms. *Business Horizons*, 2019—Elsevier
12. Raikwar, M., Gligoroski, D., Kralevska, K.: SoK of used cryptography in blockchain. *IEEE Access*, 2019—ieeexplore.ieee.org
13. Zheng, Z., Xie, S., Dai, H., Chen, X., et al.: An overview of blockchain technology: architecture, consensus, and future trends. In: *2017 IEEE International ...*, 2017—ieeexplore.ieee.org
14. Gupta, S., Sadoughi, M.: *Blockchain Transaction Processing*. 2019—researchgate.net
15. Al-Shabi, M.A.: A survey on symmetric and asymmetric cryptography algorithms in information security. *Int. J. Sci. Res.* 2019—researchgate.net
16. Zhang, Y., Xu, C., Ni, J., Li, H.: Blockchain-assisted public-key encryption with keyword search against keyword guessing attacks for cloud storage. *IEEE Transactions on ...*, 2019—ieeexplore.ieee.org
17. Li, H., Zhang, F., He, J., Tian, H.: A searchable symmetric encryption scheme using blockchain. *arXiv preprint arXiv:1711.01030*, 2017—arxiv.org
18. Watanabe, H., Fujimura, S., Nakadaira, A., et al.: Blockchain contract: a complete consensus using blockchain. In: *2015 IEEE 4th global ...*, 2015—ieeexplore.ieee.org
19. Liu, M., Wu, K., Xu, J.J.: How will blockchain technology impact auditing and accounting: permissionless versus permissioned blockchain. *Current Issues in Auditing*, 2019—meridian.allenpress.com
20. Zikratov, I., Kuzmin, A., Akimenko, V., et al.: Ensuring data integrity using blockchain technology. In: *20th Conference of ...*, 2017—ieeexplore.ieee.org
21. Ethereum white paper: a next generation smart contract & decentralized application platform
22. Ferdous, M.S., Chowdhury, F., Alassafi, M.O.: In search of self-sovereign identity leveraging blockchain technology. *IEEE Access*, 2019—ieeexplore.ieee.org
23. Yeoh, P.: Regulatory issues in blockchain technology. *J. Financ. Regul. Complian.* 2017—emerald.com
24. Min, H.: Blockchain technology for enhancing supply chain resilience. *Business Horizons*, 2019—Elsevier
25. Hammı, M.T., Bellot, P., et al.: BCTrust: a decentralized authentication blockchain-based mechanism. *2018 IEEE Wireless ...*, 2018—ieeexplore.ieee.org
26. Garcia, P.: Biometrics on the blockchain. *Biometric Technology Today*, 2018—Elsevier
27. Karafiloski, E., Mishev, A.: Blockchain solutions for big data challenges: a literature review. *IEEE EUROCON 2017-17th ...*, 2017—ieeexplore.ieee.org
28. Savelyev, A.: Copyright in the blockchain era: promises and challenges. *Comput. Law Secur. Rev.* Elsevier (2018)
29. Zhang, Y., Xu, C., Li, H., Yang, H., et al.: Chronos: secure and accurate time-stamping scheme for digital files via blockchain. In: *ICC 2019-2019 IEEE ...*, 2019—ieeexplore.ieee.org