

Blockchain Technologies

Rashmi Agrawal  
Neha Gupta *Editors*

# Transforming Cybersecurity Solutions Using Blockchain


 Springer

# Blockchain Technologies

## Series Editors

Dhananjay Singh , Department of Electronics Engineering, Hankuk University of Foreign Studies, Yongin-si, Korea (Republic of)

Jong-Hoon Kim, Kent State University, Kent, OH, USA

Madhusudan Singh , Endicott College of International Studies, Woosong University, Daejeon, Korea (Republic of)

This book series aims to provide details of blockchain implementation in technology and interdisciplinary fields such as Medical Science, Applied Mathematics, Environmental Science, Business Management, and Computer Science. It covers an in-depth knowledge of blockchain technology for advance and emerging future technologies. It focuses on the Magnitude: scope, scale & frequency, Risk: security, reliability trust, and accuracy, Time: latency & timelines, utilization and implementation details of blockchain technologies. While Bitcoin and cryptocurrency might have been the first widely known uses of blockchain technology, but today, it has far many applications. In fact, blockchain is revolutionizing almost every industry. Blockchain has emerged as a disruptive technology, which has not only laid the foundation for all crypto-currencies, but also provides beneficial solutions in other fields of technologies. The features of blockchain technology include decentralized and distributed secure ledgers, recording transactions across a peer-to-peer network, creating the potential to remove unintended errors by providing transparency as well as accountability. This could affect not only the finance technology (crypto-currencies) sector, but also other fields such as:

- Crypto-economics Blockchain
- Enterprise Blockchain
- Blockchain Travel Industry
- Embedded Privacy Blockchain
- Blockchain Industry 4.0
- Blockchain Smart Cities,
- Blockchain Future technologies,
- Blockchain Fake news Detection,
- Blockchain Technology and It's Future Applications
- Implications of Blockchain technology
- Blockchain Privacy
- Blockchain Mining and Use cases
- Blockchain Network Applications
- Blockchain Smart Contract
- Blockchain Architecture
- Blockchain Business Models
- Blockchain Consensus
- Bitcoin and Crypto currencies, and related fields

The initiatives in which the technology is used to distribute and trace the communication start point, provide and manage privacy, and create trustworthy environment, are just a few examples of the utility of blockchain technology, which also highlight the risks, such as privacy protection. Opinion on the utility of blockchain technology has a mixed conception. Some are enthusiastic; others believe that it is merely hyped. Blockchain has also entered the sphere of humanitarian and development aids e.g. supply chain management, digital identity, smart contracts and many more. This book series provides clear concepts and applications of Blockchain technology and invites experts from research centers, academia, industry and government to contribute to it.

If you are interested in contributing to this series, please contact [msingh@endicott.ac.kr](mailto:msingh@endicott.ac.kr) OR [loyola.dsilva@springer.com](mailto:loyola.dsilva@springer.com)

More information about this series at <http://www.springer.com/series/16276>

Rashmi Agrawal · Neha Gupta  
Editors

# Transforming Cybersecurity Solutions Using Blockchain

 Springer

*Editors*

Rashmi Agrawal  
Faculty of Computer Applications  
Manav Rachna International Institute  
of Research and Studies  
Faridabad, Haryana, India

Neha Gupta  
Faculty of Computer Applications  
Manav Rachna International Institute  
of Research and Studies  
Faridabad, Haryana, India

ISSN 2661-8338

ISSN 2661-8346 (electronic)

Blockchain Technologies

ISBN 978-981-33-6857-6

ISBN 978-981-33-6858-3 (eBook)

<https://doi.org/10.1007/978-981-33-6858-3>

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 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 Singapore Pte Ltd. The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

# Contents

<b>Introduction to Blockchain Technology</b> .....	1
Gurinder Singh, Vikas Garg, and Pooja Tiwari	
<b>Cloud Computing Security Using Blockchain Technology</b> .....	19
Santosh Kumar Singh, P. K. Manjhi, and R. K. Tiwari	
<b>An Introduction to Blockchain Technology and Their Applications in the Actuality with a View of Its Security Aspects</b> .....	31
Reinaldo Padilha França, Ana Carolina Borges Monteiro, Rangel Arthur, and Yuzo Iano	
<b>Blockchain-Based Cyber Security</b> .....	55
Snehlata Barde	
<b>Secured Storage and Verification of Documents Using Blockchain Technology</b> .....	71
Soma Prathibha, T. R. Sona, and J. Krishna Priya	
<b>Blockchain-Based Access Control System</b> .....	91
P. Leela Rani, A. R. Guru Gokul, and N. Devi	
<b>A Comparative Investigation of Consensus Algorithms in Collaboration with IoT and Blockchain</b> .....	115
Alankrita Aggarwal, Shivani Gaba, and Mamta Mittal	
<b>Smart Contract Deployment in Ethereum Learning Made Easy</b> .....	141
Mayank Aggarwal, Vishal Goar, and Nagendra Singh Yadav	
<b>Blockchain-Based Smart and Secure Healthcare System</b> .....	165
Sheikh Mohammad Idrees, Iffah Aijaz, Parul Agarwal, and Roshan Jameel	
<b>Blockchain for Automotive Security and Privacy with Related Use Cases</b> .....	185
M. Karthiga, S. S. Nandhini, R. M. Tharsanee, M. Nivaashini, and R. S. Soundariya	

**Blockchain Technology: Developers Cultivate Novel Applications  
for Societal Benefits** ..... 215  
Sheetal Zalte and Rajanish Kamat

# Introduction to Blockchain Technology



Gurinder Singh , Vikas Garg , and Pooja Tiwari 

**Abstract** In recent years, many technologies have emerged as a result of technological innovation. In the past few years, Blockchain technology or the technology of secure ledger has gained much attention. In the field of computing, Blockchain technology has been characterized as the fifth disruptive innovation. In a way, we can say that it is a distributed ledger of records which are absolute and certifiable. The technology of Blockchain is fundamentally a record of the distributed database or it is a public ledger of all the dealings or proceedings that are executed digitally and shared with other entries that are participating. Every transaction made in the public ledger is certified by mutual agreement of all the contributors in the arrangement. And after the entry of the information, it can never be erased. Each transaction made in the system can be easily verified and recorded in the case of Blockchain technology. After the advent of Blockchain technology in the year 2008, the concept of Blockchain technology has been used and applied in many different ways. The interest in this technology has increased due to its unique attributes and features of providing security, secrecy, and integrity of data without the intervention of the third party controlling the transaction, and therefore, it motivates many researchers to research to understand this technology by understanding its challenges, applications, and limitations. The most visible impact of the Blockchain technology can be witnessed as a multitude of cryptocurrencies that have emerged up. Furthermore, it is quite pertinent that the application of Blockchain technology is far ahead of cryptocurrency and much deeper than simple distributed ledger storage. This technology has been used by many sectors such as finance, manufacturing, education, and medicine to utilize the unique profits offered by this technology due to its unique technology. Blockchain technology offers unique benefits such as trust ability, collaboration, organization,

---

V. Garg (✉)  
Amity University, Noida, Uttar Pradesh, India  
e-mail: [vgarg@gn.amity.edu](mailto:vgarg@gn.amity.edu)

G. Singh · P. Tiwari  
ABES Engineering College, Ghaziabad, India  
e-mail: [gsingh@amity.edu](mailto:gsingh@amity.edu)

P. Tiwari  
e-mail: [pooja.tiwari@abes.ac.in](mailto:pooja.tiwari@abes.ac.in)



identification, credibility, and transparency. Additionally, Blockchain technology the most frequent use of Blockchain is in the area of finance and banking, and also many experiments have been done by big corporate in other domains as well. This chapter will focus on various sectors and areas where the Blockchain technology has an impact and also discusses future implementation in different sectors.

**Keywords** Blockchain technology · Challenges · Future applications · Limitations

## 1 Introduction

Blockchain is a technology that has a record of the distributed database or public ledger of all those different proceedings that are implemented and all the contributions sharing it. The transaction that occurred is authenticated by most of the participants by agreeing. When the information is entered into the system, it cannot be undone. This technology comprises records of each transaction that is ever done in the system.

The most popular technology which is well known is the bitcoin which is intrinsically tied. In the recent past, it is also one of the most discussed phenomenon as it facilitates transactions of multibillion dollars of the global market without the restriction of government, due to which there are numerous issues of regulations that involve the government at the national level and other financial institutions.

But in the past few years, the concept of Blockchain technology has been much discussed phenomena and completely non-controversial and is effectively executed in both financial and non-financial worlds. The distributed consensus model of the Blockchain has been considered as the most important invention in the era of the Internet itself according to “Marc Andreessen, the doyen of Silicon Valley’s capitalists.” This economy is driven by the digital system and relied upon by some of the authority which is trusted in nature. When the transaction is done by any individual, it requires that it should trust some system—like it can be service of email providing the information that it is delivered, or it can be Facebook providing information that post is shared with everyone or it can be any financial transaction through the bank where one can get confirmation that money is transferred to a receiver in any part of the world. We can analyze that we are living in such kind of digital world where we have to rely upon a third party for security and privacy issues. However, the fact is that this source of the third source can be operated or hacked as well. At this point where the role of Blockchain technology comes into the picture, at present, the transaction system between two individuals and two companies is mostly centralized in nature and is controlled by a third party. Whenever we make digital payment, there is always an involvement of a third party so that transactions can be completed. Additionally, some extra charges are incurred from bank or a credit card company. A similar pattern is followed in another area also, for example, games, music, software, etc. This issue has been resolved by the advent of Blockchain technology. The main emphasis of this technology is to create an environment that is decentralized in nature, and there is no involvement of the third party in case of transaction and data [1].

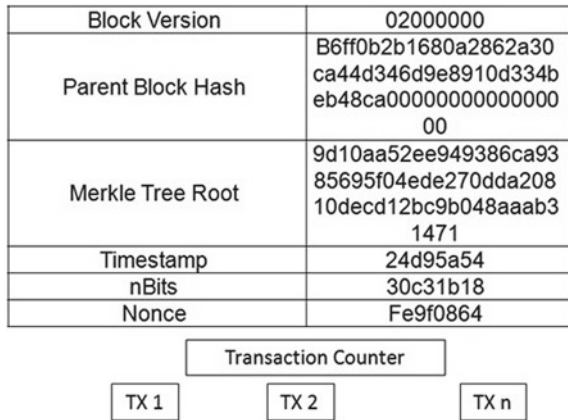
This technology has a feature where it enables us to track every transaction done in the past and present with the help of distributed consensus, which can be verified in the future. This is done even without conceding the confidentiality of third party’s intricate and digital assets. The prime features of Blockchain technology are distributed consensus and anonymity.

Blockchain enables to maintain consistently increasing the data records which are inveterate by the different nodes contributing in it with the help of distributed database solution. Each transaction that is completed is recorded in a pubic ledger. Blockchain technology provides the solution which is decentralized in nature and it does not require any mediation by a third party. Information regarding each transaction done in the Blockchain is communicated to all the nodes participating in it. This feature of Blockchain technology makes it more transparent as compared to a centralized transaction which involves the mediation of the third party. Additionally, all the nodes in the Blockchain are anonymous, which enables the transaction to be more secure for other nodes. The first application that was introduced in Blockchain technology was Bitcoin. Bitcoin is the platform where goods are purchased and exchanged with the help of digital payment by creating a decentralized environment [2].

Although this technology seems very appropriate for conducting the transaction with the help of cryptocurrencies, still it has some technical issues and restrictions that require some in-depth analysis and issues to be resolved. In the case of Blockchain, it is required that the nodes are kept private to protect them from attacks and to maintain a high level of security and transaction [3]. Additionally, computational power is also required in the Blockchain for the confirmation of the transaction.

It becomes very imperative in this scenario to understand that what are the topics which have researched by the different authors and topics and area which needs more attention which is presenting threats and challenges for future studies. To explore and understand these questions, we have used systematic mapping to understand the study process [4] to find out the different work related to the field of Blockchain. Figure 1 shows the block structure of the Blockchain.

Fig. 1 Block structure



The materials in the scientific database can be searched with the help of executing the well-designed research protocol in case of a systematic mapping study. Based on current research in the domain of Blockchain, a map is produced and other researchers will surely get benefited by understanding the future scope of research and questions. Although many researches are conducted in the domain of cryptocurrencies which is also a topic of business and management, we have focused upon the technical perspective of Blockchain. The main focus of the chapter is to understand the technical perspective of the Blockchain so our inclination is toward the different topics related to the technical perspective of the Blockchain which involves security, performance, data integrity, privacy, and scalability.

This chapter has been organized into different sections. The first section is an introduction followed by Sect. 2 which discusses the Blockchain and Bitcoin. Furthermore, authors have tried to discuss and present the challenges and few technical restrictions of Blockchain technology. Section 3 of this chapter has focused upon the methodology adopted and accordingly collecting the appropriate research papers. Based on the analysis done on the previous research papers, results are presented in Sect. 4 of the chapter. In Sect. 5, certain identified classification schemes are presented. In the next section, the results and another area of research chapter have been discussed, and in the last section, the conclusion has been presented [5].

## 2 Background

The Blockchain technology was first introduced in the form of Bitcoin, and it is one technology which is running the cryptocurrency that is Bitcoin. The integrity of the transaction of data is done with the help of a ledger system [3]. Even in the current context, the most frequently used application in Blockchain technology is bitcoin [6]. The main feature of Bitcoin is that it is a payment gateway that is decentralized in nature and it involves transaction ledger which is public [7]. The prime quality of Bitcoin is that it can maintain the value of the currency without involvement of any organization or government institution. The participants who are constantly using bitcoin are gradually increasing and also the number of transactions [8]. Additionally, it is also leading toward the conversion of the customary currencies, e.g., KRW, EUR, and USD, and it is leading to the conversion in the present currency available in the market [9, 10]. So, this cryptocurrency has gained much attention from a different set of people across the world and also successfully implemented digital currency [9].

So, a public key infrastructure mechanism is used in the case of bitcoin [11]. The use in the PKI mechanism has one public and private key. For the bitcoin wallet, a public key is employed in the discourse, and to authenticate the user, private key is used. There are three main components that are included during the transaction: receiver's multiple public keys, the public key of the sender, and the worth which is transported. Within the time zone of 10 days, this transaction will be notified in the block. The information regarding all the transaction conducted in all the respective

blocks is stored in the user’s storage disk. So, the information on whatever transaction is done in the network of bitcoin is stored, and also, it authenticates the transaction done by the previous blocks. All the transactions done are verified, and accordingly, all the nodes are rewarded. This process can be referred to as mining, and this can further be established through proof of work which is considered as one of the crucial technologies in the blockchain. A consensus is reached between all the nodes when all the transactions are completed successfully. A chain is created between all the nodes by creating the linkage between new blocks and previous blocks. This is known as a public ledger technique in the bitcoin referred to as Blockchain where there is a block of chains.

Blockchain is the technology of Bitcoin which is decentralized in nature. It is specifically designed to distribute and transmit currency for the operators of the Bitcoin. In this technology without any intervention of third party, public ledger can be supported which was previously not executed [3]. The main benefit of Blockchain technology is that once the data has been accepted by all nodes, the data stored in the public ledger cannot be altered or obliterated. This is the main reason that Blockchain technology is well known due to its feature of security and data integrity. There are so many other uses of Blockchain technology in other areas as well. For example, in the case of cloud service, an environment can be created for doing the digital transaction and sharing data on peer-to-peer basis [3]. The unique feature of Blockchain technology is the integrity of data and that is the prime factor why this technology is so successful and applied to other services and applications as well. Figure 2 shows the basic architecture of a Blockchain system.

There are certain technological limitation and challenges which have been identified in the Blockchain technology. Swan [3] has presented certain technical challenges and limitations so that in the future this technology can be adapted accordingly:

- **Throughput:** The prime issue in the Blockchain technology is potential throughput and now it extended to 7tps (transaction per second). Certain other networks are procession which is VISA (2000tps) and Twitter (5000tps). The throughput is required to be maintained when the frequency in the network rises to a similar level.

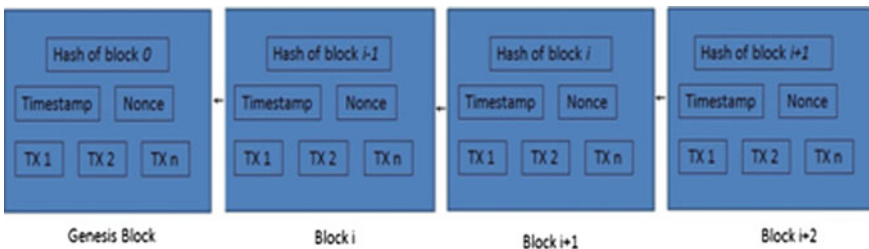


Fig. 2 Architecture of Blockchain that consists of different blocks in a sequential manner

- **Latency:** Around 10 min is consumed in completing one transaction so that sufficient security for the transaction block in the case of Bitcoin can be created. More time has to be devoted to a block so that efficiency can be achieved in security, as it has to compensate for the charge of double expenditure attacks. When the money is spent more than once, then the result generated is double-spending [12]. Bitcoin can help the user in case of double-spending by authenticating each transaction which is added to the block, ensuring that no previous inputs have been spent in the previous transactions [12]. So, in the present situation, latency has been considered a big issue. While the security is made, in seconds the transaction should be completed by making the blocks. For example, in the case of VISA, the transaction can be completed within a few seconds, which is beneficial in comparison to Blockchain.
- **Size and bandwidth:** In February 2016, the network size of the Bitcoin is over 50,000 MB (February 2016). In each year, the capability of the Blockchain to grow is 214 PB, when the throughput is increased to the level of VISA. The size of the one block is 1 MB which is assumed by the community of the Blockchain, and every 10 min the block is created [13], due to which there is a restriction in the amount of transaction that can be controlled at one point of time (on middling 500 operations in one block) [14]. The issues of the size and bandwidth have to be resolved if the technology of Blockchain needs to handle a greater number of transactions.
- **Security:** At present, the possibility of an attack on the Blockchain is around 51%. In the case of 51%, attack on the entire network of mining hash rate will be fully controlled by the single entity, and accordingly, it will be able to influence the Blockchain. So, more in-depth study and research are necessary to resolve the issue of security [15].
- **Wasted resources:** Huge amount of energy is wasted when the mining of bitcoin is done (\$15 million/day). The proof-of-work effort is creating the waste in case of Bitcoin. In the field of the industry, some alternatives are present such as proof of stake. With the help of proof of work, we can determine how much work is accomplished by the miner [16]. For example, somebody can mine around 1% of proof-of-stake Blockchain if they are holding 1% of Blockchain [16]. To make the mining more effective, the issue with the waste resources needs to be resolved.
- **Usability:** It is quite difficult in case Bitcoin API develops the services. In the case of Blockchain, it is required to cultivate additional user-friendly API. This can have a resemblance to the REST APIs.
- **Versioning, hard forks, multiple chains:** The possibility of attack is higher that is around 51% when the small chain is comprised of small nodes. One more issue that can emerge is when the administrative or versioning purpose chain is split.

So, if we look at the overall perspective, this technology has the capability to alter any transaction the way it is piloted on a day-to-day basis. Additionally, the application of Blockchain is not only confined to cryptocurrencies, but it can be applied in various other domains where the transaction can be done. So, authors are quite curious to explore the different dimensions of the Blockchain, but presently Blockchain has

many limitations and threats as well. There are three features, i.e., anonymity, data integrity, and security characteristics, which are creating a lot of challenges, and these domains need to be answered and also evaluated with high excellence exploration. In the future, one more issue that requires attention for research is scalability. Hence, it becomes quite important to explore and understand how much research is conducted in the Blockchain and for that collecting and gathering all the important literature and relevant research available in the field. So, based on the research, we can understand the challenges and limitations have been addressed and resolved and also understand the various areas that need attention in the field of Blockchain at the moment [17].

Previously, most of the transactions were focusing on the third party for validation during the online transaction of digital assets but now the existing market in case of Blockchain technology can be applied in the domain of both financial and non-financial transactions. In the year 1994, there was one more application that was invented by Nick Szabo named “Smart Contracts.” It was rather a wonderful idea that the participating parties can automatically execute the contract between them. Conversely, until the idea of cryptocurrency did not come into existence, this idea was not very functional and in use. When the pre-programmed conditions of a contractual agreement are triggered, both Blockchain and smart contract applications can work simultaneously. In the world of cryptocurrencies, smart contracts are the killer of this respective application. Certain protocols are automatically enforced by computers and these are smart contracts.

With the help of Blockchain technology, the task to register, authenticate, and implement smart contracts has become much calmer. Many companies are open source in nature like Ethereum and Codius which enables smart contracts to use Blockchain technology. Many companies are currently working on technologies of bitcoin and Blockchain which are providing support to smart contracts [18].

There are many situations where assets can only be transferred when certain conditions are fulfilled and it requires lawyers for the creation of agreement and banks to deliver escrow service which can be substituted by smart contracts. Ethereum due to its capability of the programmable platform was able to generate curiosity. Ethereum cryptocurrency can be created by anyone and it can be implemented to pay in case of smart contracts. To pay for the other or additional services, ether is the own cryptocurrencies of Ethereum. There is a wide range of applications in the case of Ethereum which includes governance, autonomous banks, keyless access, crowdfunding, financial derivatives trading, and expenditure using smart contracts. Not only cryptocurrencies are available but numerous Blockchains are available so that a wide range of applications can be supported. At present, three approaches are available in the industry which can also support the other applications and can help to overcome the estimated limitation of Bitcoin Blockchain [19]. On a particular digital asset to attain the consensus at the distributed level, a system of Blockchain algorithm is used which can be referred to as an alternative Blockchain. Merged mining is the process where the miners can be shared with the parent network. Various applications are suggested to be implemented which include DNS, SSL certification authority, file storage, and voting.

On the top of bitcoin Blockchain by employing the functionalities beyond the creation of digital assets, there one open source named as a colored coin demonstrates the different methods for developers for the creation of digital assets. Side chains are alternative Blockchains that are supported by Bitcoins through bitcoin contract—as gold hacks some dollars and pounds.

There is a possibility of having thousands of side chains attached to Bitcoin each having diverse features and purposes—all of them fetching the benefit of scarcity and resilience guaranteed by Bitcoin Blockchain. Once all the alternative Blockchains are tried and tested, Bitcoin Blockchain can repeat and it can support the additional features as well.

### 3 Technological Applications

#### 3.1 Applications in Financial Domain

##### (a) Private Securities

In the case of making the company public, it is a very costly affair. Many processes have to be performed by the syndicates of the bank which includes the process of underwriting and attracting different investors. The companies which are listed under the stock exchanges are sharing with the secondary market to function properly in case of a trade setting and well in time. By using the technology of Blockchain, corporations can unswervingly distribute the shares to the people. The shares which are on the top of the Blockchain can be directly purchased and sold in the secondary market. Some of the examples regarding this are given as below:

**NASDAQ Private Equity:** In the year 2014, NASDAQ has launched its private equity. This has been launched for some pre-IPO and private companies for the provision of crucial functionalities like cap table and investor relationship management. As multiple third parties are involved in the procedure of trading stocks in the interchange process, the process is quite slow and inefficient [20]. There is a joint partnership between NASDAQ and a new start-up known as chain.com for the implementation of private equity on top of the Blockchain. To implement exchange functionality, chain.com is doing it through Blockchain-based smart contracts. The performance of this merchandise is anticipated to fast, noticeable, and efficient. By using Blockchain as counterparty in implementation, Medici is developed as a security exchange. The main focus is the creation of the stock market which is cutting edge. Through the counterparty protocol, the traditional financial instrument can be implemented as the self-executing smart contracts. The requirement of physical contract is eliminated due to these smart contracts. Various contracts can be negotiated and facilitated, and it can be enforced and also eliminated the requirement of a third party as a mediator which includes broker, exchange, or bank.

To address the various issues which are related to alternative cryptocurrencies such as fragmentation and security, an open-source project is introduced with the main emphasis on the side chain. Its uses can vary from security registration, such as stocks, bonds, and derivatives, for ensuring the security in bank balance and mortgages.

There is a new New York-based Bitcoin exchange known as CoinStarter. This Bitcoin exchange is working on a project referred to as Highline, whereby the help of Blockchain technology financial transaction is cleared and settled in  $T + 10$  min in contrast to customary  $T + 3$  or  $T + 2$  days.

There is more market that is decentralized in nature known as Augur through which users can purchase and sell shares by predicting the probability of the vents that it will occur in the future. So, based on the “Wisdom of crowds,” it can also be employed to make the financial transactions and economic forecast.

There are digital tokens also named Bit shares that re-side the Blockchain and reference-specific assets such as currencies or commodities. It provides unique features to the token holders who can earn interest in commodities, such as gold and oil, as well as dollars, euros, and currency instruments.

#### (b) Insurance

Blockchain can register those assets which are unique and can be recognized by one or more identifiers and which are challenging to abolish or duplicate. This can further be utilized in authenticating the possession of a strong and also locating the history of the transaction. Any possessions (corporeal or digitally such as real estate, automobiles, physical assets, laptops, other valuables) can be validated by the insurer, and also, it can be registered and owned by the Blockchain [21].

A permanent ledger of diamond certification is done by the company known as Everledger, and also, the transaction history can be traced. The unique features of the diamond which differentiate from others such as height, width, weight, depth, and color are recorded and hashed in the Blockchain. These diamonds can be verified by insurance companies by enforcing the different laws through enforcement agencies, owners, and claimants. Web service API can be easily used in the case of Everledger for verifying the diamond, cresting, and updating its claim by the insurance companies and in the same police reports can be done.

### ***3.2 Applications in Non-financial Domain***

#### (a) Notary Public

Blockchain can verify the authenticity of the various documents and eliminates the requirement for centralized authority. The service of document certification will surely benefit in the proof of ownership (who authored it), proof of existence (at a certain time), and proof of integrity (not tampered) of the documents.



These services are legally bounded as it can be authenticated by the third party and also counterfeit-proof. Blockchain technology can be used for notarization which helps in ensuring the document's privacy. With the help of cryptographic hashes of different files in the Blockchain, time stamping of the notary can be brought to the next higher level. Blockchain technology can also help in eliminating the required notarization fees which are quite expensive and not appropriate ways of transferring the document [22].

A thorough Blockchain company named as Stampery is mailing any files. Each email is certified by emailing specifically to individual customers by creating an individual email for them. There are many law firms which are employing the technology of Stampery's for the authentication of documents in a cost-effective way.

For the notary service, one of the companies known as Viacoin is used for the clearance of protocol. By using TestNet3 or Bitcoin Network, proof of existence can be created by as iOS app referred to as Block Notary.

Documents can be notarized with the help of a trivial number of bitcoins so that it can be recorded in the public Blockchain and for this Crypto Public Notary.

There is another service known as proof of existence which is employing Blockchain to SHA256 digest of the document.

With the help of Blockchain, Ascribe is a company that is involved in authorship certification. With attribution to the original author, the ownership of the service can also be transferred.

#### (b) Applications of Blockchain in the Music Industry

In the past few decades, there is a tremendous transformation in the music industry due to digitalization; streaming services have raised to the next level and also increased awareness about Internet services. This transformation has influenced everybody in the music business starting from artists, labels, publishers, songwriters, and also other facility benefactors which are giving streaming services. Because of the emergence of the Internet, the process of determining the royalties has become more complex and has given rise to the demand for transparency in the royalty payments by both artists and songwriters [23].

This is one domain where Blockchain technology plays a crucial role. With the help of this technology, a comprehensive and accurate distributed database can be maintained which records all the rights of music ownership in a public ledger. Smart contracts can determine the rights of ownership and additionally regarding the right of ownership. The relationship between different stakeholders is defined, and interactions between them are automated with the help of smart contracts.

## 4 Decentralized Proof of the Existence of Documents

In case of any legal solution, it is very crucial to validate the existence of the post-session of the signed documents [24]. Some security challenges are present

in the traditional document validation model which put forth central authorities for storing and for the validation of documents. It became more difficult for these as the documents become older.

The technology of Blockchain is giving the alternative model for proof of existence and also regarding the ownership of legitimate forms. Online proof of the different documents can be secured anonymously with the help of the service known as proof of existence. When the user submits the document at the same time, this service of proof of existence stores the cryptographic digest of the file. It has to be taken into consideration that cryptographic digest or fingerprint is deposited and not the real document. In this domain, the user is not required to take tension regarding the privacy aspect and securing the information. At a certain point in time later on, it is allowed to certify the existence of the document. The signature and timestamp which are related to the legal document can easily be stored by leveraging the technology of the Blockchain and can be authenticated by native Blockchain mechanisms [25].

The main pros of this service are that it permits its user to maintain the security and privacy that permit the handler to maintain dispersed proof of document which cannot be a midwife by the third party. So, the document's existence is authenticated by employing the technology of Blockchain which does not rely upon the single centralized entity.

## ***4.1 Decentralized Storage***

To store the different types of files such as photos, videos, and music files, there are different types of cloud file storage such as Dropbox, Google Drive, or One Drive which are gaining the attention of many individuals. However, they are gaining the attention and interest of the people despite that cloud file storage has a limitation of security, privacy, and data control. The foremost problem is that even in the case of confidential files one has to trust the third party.

Peer-to-peer distributed cloud storage platforms can be provided by Blockchain technology known as Storj which facilitates the user to exchange and transfer the data without depending upon the third party. Users can be benefited in such scenarios where unusual bandwidth can be used and also personal space in the PC can be utilized for the purpose of micropayment based on Bitcoin [26].

Security, privacy, and data control are significantly increased if the central control is absent, and also, it eliminates the most conservative data failures and outages. For the proper participation in the network, Storj's platform is employed which relies upon a challenging algorithm to offer incentivization.

So, in this style, the integrity and availability of files can be checked cryptographically with the help of Storj and also offering the rewards in a direct way to the people maintaining the file. In a similar example, we can see that both an incentive and method of payment can be done by the bitcoin-based micropayments; on the other hand, separate Blockchain is used for the metadata file.

## **4.2 *Decentralized IoT***

The Internet of Things (IoT) is gaining attention and it is becoming quite prevalent technology in both domains such as consumer and enterprise space [27, 28]. There are many platforms of IoT which are based on the centralized model in which the control and interaction between the devices are controlled by the broker or hub. However, there are many situations in which this approach is quite impractical where the devices are required to alteration of data among themselves independently. This specific need leads to efforts toward decentralized IoT platforms. The implementation of decentralized IoT platforms can be facilitated with the help of Blockchain technology which includes record keeping and secured and trusted data exchange. In this type of architecture, the general ledger is served by the Blockchain technology, which maintains the trusted record of all the messages in a decentralized typology between smart devices.

ADEPT (Autonomous Decentralized Peer-to-Peer Telemetry) is a platform that is jointly developed by IBM and Samsung and which uses the design if the bitcoins and distributed networks of devices are built or decentralized Internet of Things (IoT). There are three protocols which are used in ADEPT: BitTorrent (file sharing), Ethereum (smart contracts), and Telehash (peer-to-peer messaging).

The filament is a startup that provides a decentralized IoT software stack that uses the bitcoin Blockchain to enable devices to hold unique identities on a public ledger.

## **4.3 *Blockchain Based on Anti-counterfeit Solutions***

In contemporary business, one of the prevalent challenges is counterfeiting. Rather, if we talk specifically, one of the biggest problems digital commerce facing in today's scenario is the problem of counterfeiting. The solution to this problem is the dependency on the third party which brings into a scenario the logical friction between merchants and consumers.

This issue of counterfeiting mechanism can be handled by the Blockchain technology by providing its decentralized implementation and security capabilities. A situation can be assumed where all merchants, different brands, and markets share a system of Blockchain with different nodes where the evidence can be stored and authenticity can be validated of the product. By employing the technology of Blockchain, the supply chain stakeholders will not depend on the centralized entity for validating the exclusive products.

Anti-counterfeit solutions can be provided with the help of Blockchain technology using block verify that has presented the transparency to the supply chain. There are various applications in different domains such as in the pharmaceutical, luxury items, and diamonds and electronics industries.

## 5 Blockchain in Internet Domain

There is one alternative Blockchain technology named as Namecoin having small variations by the help, of which decentralized version of DNS (domain name system) can be implemented which is irrepressible to suppression. At present, the DNS servers are mainly well ordered by administrations and large establishments; in case of consumer's Internet usage, the powers can be abused to censor the power, hijack, or spy. By using the technology of Blockchain, the phonebook or Internet's DNS can be sustained in a decentralized manner and respective users can save the same phonebook records on their workstation.

For digitally managing the certificates and for the centralized distribution, the technology of public key infrastructure is widely used. For the verification of the digital certificate, each device is required to have origin credential of the certification authority (CA) [29]; although the technology of PKI was very successful and widely deployed, the issue of scalability makes it dependent on CA. The features of the Blockchain can facilitate and help to resolve some of the issues of the PKI by employing the feature of Keyless Security Infrastructure (KSI).

The cryptographic hash function is used in the case of KPI, which allows the confirmation to depend on solitary on the safety of hash functions and also the Blockchain availability.

### 5.1 Risks of Adoption

This technology of Blockchain is quite promising and breakthrough. As previously also we have discussed that, some numerous applications or problems can be solved with the help of Blockchain technology, starting to form financial (remittance to investment banking) to the domain of non-financial applications like notary services.

Furthermost of the innovations are fundamental. As it happened due to the adoption of radical innovation, there is a probability of a certain risk associated with it.

### 5.2 Behavior Change

The only permanent thing in this world is change, which is permanent, and it is quite obvious to have resistance toward this change. Customers are required to have the awareness that the electronic transfer they are doing is safe, secure, and complete in the present situation of a non-tangible third party. There will be a transformation in the roles and responsibilities of the intermediaries as well like Visa or Mastercard (in case of credit cards). It can be assumed shortly that these firms will also invest in this technology and all their platforms will also be moving toward Blockchain-based

platforms. Further, to maintain customer relationships, these firms will continue to provide services.

### ***5.3 Scaling***

There is a challenge that the services are at the nascent stage and based on the technology of the Blockchain. As an individual we have to assume that we are doing blockchain transactions for the very first time. In this case, a person is required to download the entire set of Blockchain and has to authenticate it before doing the first business. This can take many hours as the number of blocks increases exponentially [30].

### ***5.4 Bootstrapping***

If we have to move the existing document or business document framework to the new methodology of the Blockchain, it put forth the significant set of tasks related to the migration which needs to be executed. If we take an example of the ownership in real estate, existing documents that are still lying in the country or escrow companies required to be transferred to the Blockchain which is in the equivalent form. This process may involve a huge amount of time and costs [31].

### ***5.5 Government Regulations***

In the advent of technology and a new era of transaction which are based on Blockchain technology, FTC and SEC are some government agencies which may reduce the pace of the adoption process by introducing new laws and monitoring and regulating the different organizations for compliances [27]. So accordingly, the facility of the adoption in the USA can be adopted as most of the agencies have gained the trust of their customer. Although the economies are more controlled like China, the process of adoption will have some significant challenges.

### ***5.6 Fraudulent Activities***

If we look at the pseudonymous feature of this technology named as Blockchain, which is considered as easy going with valuables, the same features can be misused by some individuals for fraudulent activities like money trafficking. So, we have to understand that to protect these activities and to minimize fraudulent activities,

strong laws, regulations, and technology support laws are required and some law enforcement agencies will be required to monitor and supervise [32].

## ***5.7 Quantum Computing***

It has been observed that it is quite impossible if we calculate mathematically and then, it is quite difficult for a single party as the more computer power is required in case of Blockchain technology. With the help of the sheer brute force approach, the keys in the domain of cryptographic keys can be easily cracked due to the future advancement in the quantum of computers. Due to this, the entire system will come on the knees. On the contrary, there is an agreement that these cryptographic keys will become stronger and it becomes difficult for them to crack [28].

## ***5.8 Corporate Funding and Interest***

In the year 2015, the currency of bitcoin has reached the highest level over September–October in both the domains which include price and volume. This new era of digital currency is gaining momentum in both the places which include customer marketplace and tradable security and also with the different regulators. People are very enthusiastic as more and more capitals are injected into the digital infrastructure. The level of excitement is growing gradually for the Bitcoin and Blockchain as organizations have acknowledged around US\$1 billion of record investment in the year 2015 came to an end. There are numerous companies such as American Express, Bain Capital, Deloitte, Goldman Sachs, MasterCard, and the New York Life Insurance Company who have invested millions of dollars into bitcoin recently [33].

It has been analyzed that many corporate houses and industries have started showing interest in the technology Blockchain and bitcoin infrastructure in different segments. For the creation of a more secure and efficient system for stock trading, NASDAQ has come up with tapping technology in the domain of Blockchain. A company known as DocuSign, specialized in the electronic markets, has just revealed the joint idea to utilize the Blockchain to track the rental of the car and also to minimize the paperwork [24]. Microsoft has also revealed the idea of its venture with smart contracts that are using the technology of Blockchain. At the same time, the curiosity level for the Blockchain technology has gone to such a height that many companies are even conducting a different experiment by creating the different smaller “private Blockchain” inside their office premises. For example, many firms are hiring different companies such as Block Cypher, which is a start-up of Redwood City, California, and working in the domain of creation of the Blockchain technology within their own office and business premises [34].

## 6 Conclusion

Bitcoin cryptocurrency is handled by Blockchain technology. This is a platform and the environment is decentralized in nature, whereas in the public ledger system all the transactions are recorded and can be seen by all the participants. The main focus of Blockchain technology is to provide anonymity, security, privacy, and transparency to all the people using it. But, despite these features, there are many challenges and limitations which need to be resolved. To explore and understand the latest position of Blockchain technology, authors have used the process of systematic mapping in which all the recent research conducted in the domain of Blockchain technology has been explored [4]. The main aim of this systematic mapping was to explore the existing status of Blockchain technology and various areas where future researches can be conducted. We have only involved in the technical perspective in this study; rather, economic, law, business, and regulation perspectives have not been taken into consideration. Many papers are extracted from the scientific database and through which authors have tried to analyze the data. Based on the study conducted through different papers, authors have recommended the scope for future research in the domain of Blockchain technology based on understanding the current status done in the domain of Blockchain technology.

- Identifying issues and challenges in Blockchain technology and suggestion solutions to address these issues. Since 2013, it has been analyzed that Blockchain technology has gained momentum and it drastically increased in every sphere. There are many types of research which were conducted in this domain and every year the number of papers and researches conducted in this area increased. Out of the researches done in the concerned area, majority of the paper was stressing upon the challenges and limitations in the area, but still, there are so many issues that are still not addressed.
- More research is required to address the issue of scalability in Blockchain. After analyzing and extracting the information from different research papers, it has been identified that majority of the current research is dedicated to security and privacy issues. If the Blockchain technology is implemented in a pervasive manner, the issue of scalability which includes performance and latency needs to be addressed.
- More Blockchain application beyond Bitcoin and Cryptocurrency needs to be developed.

This study has mainly focused on one application of Blockchain which is Bitcoin. Additionally, the study has also addressed the other applications of Blockchain technology such as smart contracts, property licensing, and voting. To address the different challenges and limitations in the domain of Blockchain technology, many researchers have recommended just a brief solution but these solutions have a deficit on the part of the concrete evaluation on the part of their effectiveness.

## References

1. Lerner J (2006) The new new financial thing: The origins of financial innovations. *J Financial Econ* 79(2):223–255, 2006, [online] Available: <http://search.proquest.com.ezproxy.lib.usf.edu/docview/231721046?accountid=14745>
2. Frame W, White L (2004) Empirical studies of financial innovation: Lots of talk little action? *J Econ Literature* 42(1):116–144. [online] Available: <http://www.jstor.org/stable/3217038>
3. Swan M (2015) *Blockchain: blueprint for a new economy*. O’Reilly Media, Inc.
4. Kitchenham B, Charters S (2007) Guidelines for performing systematic literature reviews in software engineering
5. Wiesche M, Jurisch MC, Yetton PW, Krcmar H (2017) Grounded theory methodology in information systems research. *MIS Quart* 41(3):685–701
6. Coinmarketcap, *Crypto-Currency Market Capitalizations* (2016) Accessed 24 Mar 2016. <https://coinmarketcap.com/>
7. Bitcoin NS (2012) A peer-to-peer electronic cash system. Consulted 2008(1):28
8. Kondor D, Pósfai M, Csabai I, Vattay G (2014) Do the rich get richer? An empirical analysis of the Bitcoin transaction network. *PLoS one*. 9(2):e86197. pmid:24505257
9. Herrera-Joancomart J, Research and challenges on bitcoin anonymity. In: Garcia-Alfaro J, Herrera-Joancomart J, Lupu E, Posegga J, Aldini A, Martinelli F, et al (eds) *Data privacy management, autonomous spontaneous security, and security assurance*, vol 8872 of *Lecture Notes in Computer Science*. Springer International Publishing, pp 3–16. Available from: [http://dx.doi.org/10.1007/978-3-319-17016-9\\_1](http://dx.doi.org/10.1007/978-3-319-17016-9_1)
10. Judmayer A, Stifter N, Krombholz K, Weippl E, Bertino E, Sandhu R (2017) *Blocks and chains: introduction to bitcoin, cryptocurrencies, and their consensus mechanisms*. Morgan & Claypool
11. Bitcoincharts (2016) Accessed 24 Mar 2016. <https://bitcoincharts.com>
12. Housley R (2004) In: *Public key infrastructure (PKI)*. Wiley & Sons, Inc. Available from: <http://dx.doi.org/10.1002/047148296X.tie149>
13. Double-spending (2016). Accessed: 24 Mar 2016. <https://en.bitcoin.it/wiki/Double-spending>
14. Bitcoin wiki (2015) Accessed 24 Mar 2016. <https://en.bitcoin.it>
15. Wang Y, Hugh Han J, Davies PB (2018) *Understanding blockchain technology for future supply chains: a systematic literature review and research agenda*, vol 24, pp 62–84
16. Antonopoulos AM (2014) *Mastering Bitcoin: unlocking digital cryptocurrencies*. O’Reilly Media, Inc.
17. Proof-of-Stake (2016) Accessed 24 Mar 2016. [https://en.bitcoin.it/wiki/Proof\\_of\\_Stake](https://en.bitcoin.it/wiki/Proof_of_Stake)
18. Mingxiao D, Xiaofeng M, Zhe Z, Xiangwei W, Qijun C (2017) A review on consensus algorithm of blockchain. In: *2017 IEEE international conference on systems man and cybernetics*
19. Borenstein J (2016) A risk-based view of why banks are experimenting with bitcoin and the Blockchain. *SpotlightonRisk Technology*, 18 Sept 2015. Web. 03 May 2016
20. Barski C, Wilmer C (2014) The blockchain lottery: how miners are rewarded—CoinDesk. *CoinDeskRSS*. CoinDesk, 23 Nov 2014. Web. 03 May 2016
21. Wild, Jane, Martin Arnold, and Philip Stafford. “Technology: Banks Seek the Key to Blockchain -FT.com.” *FinancialTimes.N.p.*, 1 Nov. 2015. Web. 03 May 2016
22. Driscoll S (2013) How bitcoin works under the hood. *Imponderable Things*, 14 July 2013. Web. 03 May 2016
23. Kelly J (2015) Nine of world’s biggest banks join to form block-chain partnership. *Reuters*. Thomson Reuters, 15 Sept 2015. Web. 03 May 2016
24. Kalra V, Rashmi A (2019) Challenges of text analytics in opinion mining. In: *Extracting knowledge from opinion mining*. IGI Global, pp 268–282
25. Why NASDAQ Private Market. *Nasdaq Private Market l. N.p.*, n.d. Web. 03 May 2016
26. Chain | Enterprise Blockchain Infrastructure. *N.p.*, n.d. Web. 03 May 2016
27. Bhushan D, Rashmi A (2020) Security challenges for designing wearable and IoT solutions. In: *A handbook of internet of things in biomedical and cyber physical system*. Springer, Cham, pp 109–138



28. Bhushan D, Rashmi A (2020) The Internet of Things: looking beyond the hype. An industrial IoT approach for pharmaceutical industry growth, vol 2, p 231
29. Infante A (2014) Quantum computers: the end of cryptography?—Make Use Of. N.p., 16 Nov 2014. Web. 03 May 2016
30. Lee TB (2015) Bitcoin's value is surging. Here are 5 charts on the growing bitcoin economy. Vox. N.p., 03 Nov 2015. Web. 03 May 2016
31. Rivera J (2015) Gartner's 2015 hype cycle for emerging technologies identifies the computing innovations that organizations should monitor. N.p., 18 Aug 2015. Web. 03 May 2016
32. Gupta N, Rashmi A (2018) NoSQL security. In: Advances in computers, vol 109. Elsevier, pp 101–132
33. Gupta V (2017) A brief history of blockchain. Harvard Bus Rev. [online] Available: <https://hbr.org/2017/02/a-brief-history-of-blockchain>
34. Nærland K, Müller-Bloch C, Beck R, Palmund S (2017) Blockchain to rule the waves—Nascent design principles for reducing risk and uncertainty in decentralized environments. In: Proceedings of 38th International Conference on Information System. [online] Available: <https://aisel.aisnet.org/icis2017/HCI/Presentations/12/>

# Cloud Computing Security Using Blockchain Technology



Santosh Kumar Singh , P. K. Manjhi, and R. K. Tiwari

**Abstract** In 2006, cloud computing existed after Amazon's deployment of the first of its category of cloud services. Cloud computing is now simply the topmost in every record of existing theme as a research topic, for computer science in view of the fact that of its across-the-board implications in various areas in computing and which has become present day's most recent research area because of its capability to decrease the operational costs linked with computing. A rapid growth in cloud computing adaptation has been observed but, still, the data security concerns have not been fully countered. Data security anxiety is still an obstacle to the expansion of cloud computing to some extent and needs to be determined. Earlier we have used techniques for cloud environment security in our research work like two-factor authentication (OTP), AES algorithm, RSA cryptography, elliptic curve cryptography (ECC), hyperelliptic curve cryptography (HECC), homomorphic encryption, steganography, usage control (UCON) collective with encryption and the digital watermarking technology. Apart from used techniques, blockchain has come into view as a key technology to ensure security particularly in aspects of authenticity confidentiality and integrity. Therefore, this time we have selected blockchain technology to avoid the security concerns of the cloud environment. This time we will review the various features of security in blockchain and further analyze the application of blockchain in cloud environment for computing security.

**Keywords** Cloud computing · Blockchain · E-wallet · Security · Cloud services · Cryptography · Authentication

---

S. K. Singh (✉)

University Department of Computer Applications, Vinoba Bhave University, Hazaribag, Jharkhand, India

e-mail: [Santosh.trinity17@gmail.com](mailto:Santosh.trinity17@gmail.com)

P. K. Manjhi

University Department of Mathematics, Vinoba Bhave University, Hazaribag, Jharkhand, India

e-mail: [19pankaj81@gmail.com](mailto:19pankaj81@gmail.com)

R. K. Tiwari

Department of Computer Science and Technology, R.V.S. College of Engineering and Technology, Mango, Jamshedpur, Jharkhand, India

e-mail: [rktiwari@rvscet.com](mailto:rktiwari@rvscet.com)

## 1 Introduction

Blockchain technology was made by a person (or group of people) named Satoshi Nakamoto that provides the open business manuscript to the cryptocurrency bitcoin. The development of the digital ledger for virtual currency (bitcoin) prepared it the foremost electronic money to resolve the risk of digital currency which can be spent twice, i.e., double spending difficulty not having the requirement of reliable officials or essential servers. Blockchain is a rising file of records, known blocks, which are connected with cryptography. Every block holds a digital fingerprint or a hash value of the preceding block, operational information, and sequence of information as a time stamp usually displayed as a Merkle tree.

Intentionally, a cryptographic ledger is opposed to the tempering of the facts. Basically it is a public transaction ledger that is able to store the business details among the two parties proficiently also in a provable plus everlasting technique. To employ as a cryptographic ledger, a distributed ledger is normally headed by a (p2p Web) or peer-to-peer arrangements jointly hold on to a procedure in support of inter-node transmission as well as to authenticate latest blocks [1].

Blockchain has pulled focus as the succeeding production monetary machinery because of its safety that suits the computerization age. Particularly, it gives protection through the validation of peers to dispense virtual money, encryption, and the generation of a hash value that identifies the contents. Following the worldwide monetary business, the future merchandise for safety-based digital ledger technology is possible to grow up near about US Dollar twenty billion in 2020.

Blockchain is able to supply advanced security compared to keeping the entire information into a centralized database. In the case of the records repository space as well as managing features, database damage from attacks can be prohibited. Furthermore, seeing as the public transaction ledger has unrestricted features that can make available transparent with some condition in information at what time apply to region indispensable to exposé the data. Blockchain has a number of facilities, so it can be fruitful if utilized in different sectors including the monetary area and the Internet of things (IoT) background as well as we are expecting to increase its applications [2–5].

The public transaction ledger completes business records during the required work verification procedure, once a human being who lending digital money creates a block by merging the dealings over the related network.

The highly unique hash code is next produced by confirming it moreover linking the preceding record of the transaction block. Each block could be recognized by a hash which is created using the SHA256 algorithm that blocks at regular intervals simplified and reflected on the electronic money operation facts contribute to the main current business transaction detail block. This course of action provides safety to the business transaction of electronic cash and allows utilizing of dependable machinery [6–8].

Cloud customers demand for the services from the cloud service providers. CSPs are third parties that provide cloud storage services to their customers. Several other

third-party service providers are Third Party Auditor and Attribute Authority that are hypothetical to provide safety functionalities in the cloud. As we all know that safety and faith are the most significant and essential issues while benefitting the organizations and institutions with cloud [9, 10].

Cloud customer's data are on the highest threat which can be misplaced, revealed, or attacked but they do not have any choice to come out of this substandard position. Cloud customers do not even know of to whom they are interacting with or sharing their valuable data. Transparency is also a very serious concern, and cloud customers do not have any idea about the users of their data and how the data is roaming within the cloud. Cloud environment-based computing has been implemented in several information technology-based environments because of its effectiveness as well as accessibility. Furthermore, cloud safety plus confidentiality concerns have been discussed in respect of significant protection elements like privacy, righteousness, validation, admittance control, and many more [11].

Our research work studies and surveys the blockchain machinery by analyzing generic (provide services in software applications) technology and research trends. The outcome of this study could provide significant base information in the study of digital ledger. Hence we can motivate and encourage the improvement in future expectations of distributed ledger machinery by comprehension of the inclination of public transaction ledger safety measures in the cloud environment.

The rest of the research work in this chapter is structured in the following manner. In the chapter of Sect. 2, we are establishing the basic concept of blockchain. Section 3 presents a detailed argument on blockchain security as well as improved blockchain. Sections 4 and 5 proposes secure blockchain solutions in cloud computing. In the end, we conclude our study in Sect. 6.

## 2 Structure of Blockchain

A cryptographic ledger is a not centralized, ledger in distributed form, and frequently public transaction ledger, a digitalized ledger that is used to hold transactions across various computers so that any concerned record cannot be misrepresented. This permits the participators to test and audit transactions autonomously and comparatively inexpensive. A blockchain database is handled autonomously using a network and a distributed time stamp server. The use of a cryptographic ledger takes away the feature of unlimited duplicability from a digital ledger. It approves that every value of the unit is transmitted merely one time, removing the time-consuming standing difficulty. A cryptographic ledger can maintain title rights and has portrayed as a protocol of value-exchange [12]. The digital ledger is a mechanics that permits each associate to maintain a book holding the whole business transaction information and to revise their books to preserve reliability when there is the latest business transaction. Each and every one associate to validate the dependability of a business transaction which is possible just because of Internet and encryption technologies. The blockchain has

agent-free features since rights of the business deal information by several individuals make hacking complicated, safety expenditure is reduced, business transactions are mechanically accepted as well as keep recorded by a group of members, plus swiftness be guaranteed. Furthermore, the scheme could be simply executed, linked also extended with the help of public resource plus operation files could be publically retrieved to put together the operations open and minimize authoritarian expenditure [13].

The public transaction ledger, primarily blockchain which is a rising list of files also called blocks and linked using cryptography, i.e., an arrangement that is the combination or composed of a block body with a block header. Block header incorporates the code of hash values of the preceding and recent record books plus number which is difficult to find, meets the difficult level restrictions, i.e., nonce (number used only once added to hashed or encrypted block) value. Using the index function, the record book data are explored in the database, even though the record book does not include the code of hash value of subsequent record book as displayed in Fig. 1. As the code of hash values kept in every peer inside the record book is pompous through the previous values of record books, this is not easy to forge as well as modify the recorded records [14].

In the above Fig. 1, blockchain block holds the main data which depends on the code of hash value of current record book, the code of hash value of previous record book, time stamp which is the duration of record book creation, and other information, i.e., nonce value, the user defines data and block signature.

Verification based on public key with a hash function is used to offer safety in the cryptographic ledger. Algorithm of curve digital signature permitted the digital signature produced for the period of a business transaction among persons is used to provide evidence that the business transaction facts have not been altered [15]. Using blockchain there are various in-progress studies to make stronger safety in the cloud environment. The main significant part of the digital ledger is associated with the personal key utilization in encryption for safety. An aggressor attempts a “reuse attack” and an additional ambush in order to crack the bitcoin to acquire the

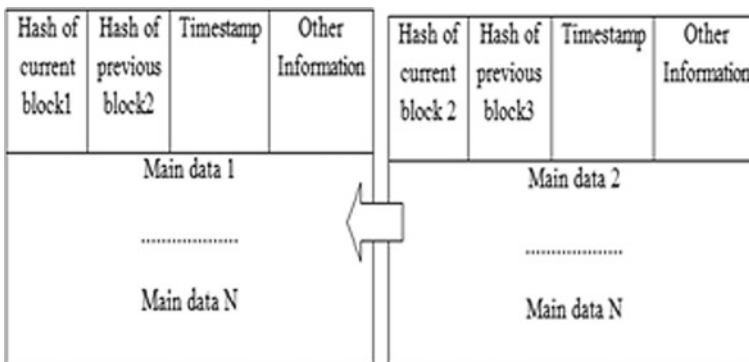


Fig. 1 Blockchain structure

personal key deposited in a peer's gadget. If the attacker can obtain the personal key, the information may be leaked and the attacker can crack the bitcoin [16].

### 3 Blockchain Security: Challenges

The digital ledger technique has been applied as electronic cash or cyber money. Still, a variety of safety issues is happening in digital ledger contracts, basically business transactions, e-wallet, and computer programs or freeware-based issues have been raised. We are trying to check the tendency of safety matters upraised to date and the safety measure of the existing public transaction ledger.

Security challenges are as follows:

- (a) Blockchain contract
- (b) Transactions security
- (c) Wallet security
- (d) Software security.

#### 3.1 *Blockchain Contract*

Blockchain is the collection of nonparallel association of produced record books. A digital ledger might be separated into two record books or blocks for the reason that the two most recent record books could be produced momentarily if two dissimilar peers are successful in operating the response used for producing the record book altogether. This type of situation, the record book particularly not selected as the most recent record book by the most of peers into the network of a virtual currency (is a peer to peer P2P payment network which working on a cryptographic protocol) to keep on extracting will become worthless. This is to say, the virtual currency will go after the preponderance of peers who have fifty percent or extra operating competence. Hence suppose an aggressor has fifty-one percent operating capability, a “fifty-one percent Attack,” in which the hackers have the command of the digital ledger and they may incorporate fallacious business transactions, may be a setback. In keeping with toward an investigation, a hacker may perceive unlawful grow with just twenty-five percent functioning potential through a malevolent excavating procedure in its place of fifty-one percent. Since the existing operating capacity of the whole bitcoin network is measured to be complex. However, pooling of resources by miners, who distribute their processing authority over a network that pools the links of mining peers have been dynamically pooling the recourses to enhance the possibility of pooling the recourses. Hence this threat has to turn out to be a dilemma. The chances of influencing the digital ledger are connected to the fundamental protections of the virtual currencies and such protection terrorization has momentarily exaggerated the financial component just because of the features of the virtual currency, i.e., bitcoin [17, 18].

### **3.2 *Transactions Security***

Many transaction forms can be designed using a flexible programming language, i.e., scripting language for inputs and outputs to manage safety issues. A bitcoin agreement [19] is a process of requesting virtual currency for the prevailing verification, validation, and economic services. The broadly used process necessitates generating an agreement using a scripting system for transactions that involves various existing signature techniques to prove ownership of the private key also known as multisig. Even though the systems of scripts are used to resolve a broad series of virtual currency troubles, the chance of an inappropriately arranged operation has also amplified as a complication of a scripting system enlarges. A virtual currency with an inappropriately arranged Pub KEY script is rejected because no one can apply it as the unlocking script (that satisfies or solves the condition placed by a locking script) cannot be produced. In order to achieve an aim, some studies who suggest that modeling of virtual currency agreement kind dealings to validate the correctness of characters made use of in operation [20].

### **3.3 *Wallet Security***

The address of personal key information holds by the bitcoin wallet like to be used for the generating of unlocking script. It shows with the intention of the thrashing of data/information into the wallet helps to hammer virtual currency because the data or information is necessary for using the virtual currency. Consequently, the virtual currency wallet has to turn out to be the most important issue of virtual currency assault through hacking [21].

Multisig for multiple signatures has been introduced to ensure the security of the bitcoin wallet services. In particular, if multisignature (which require multiple keys to give permission a bitcoin transaction) locate in an online virtual currency wallet and is set up to necessitate the owners digital signature added to the digital signature of the Internet wallet site at any time business transaction is carried out from wallet, destructive virtual currency withdrawal may be banned because the personal key of owners is not saved, even when online wallet position is obsessed by a hacking harass. Furthermore, multisignature is developing into facilities that permit departure from the virtual currency wallet simply in the course of biometric statistics or detach device using a two-factor authentication (2FA) plus other measures [22].

### **3.4 *Software Security***

Software used in bitcoin is very important and its concern is major. The bug or any technical issue of the freeware or computer program used in virtual currency can

be crucial. Even though the administrative authorized virtual currency developer documentation site, [bitcoin.org](http://bitcoin.org) describes every digital currency process and digital currency's main freeware is still successful as the recommendation because complete processes of the early digital currency system have been set on throughout the software developed by Mr. Satoshi Nakamoto [23]. However, even the virtual currency dedicated freeware or computer programs, that should be highly trustworthy than any type of things, is not independent of the setback of the computer program or freeware break down. The most popular freeware virus is the integer value overflow in wxBitcoin and bitcoin incident (CVE-2010-5139) having little resistance, i.e., vulnerability that materialized in August 2010 [24].

The requirement for the safety measures of virtual currency based on digital ledger has amplified because illegally gains right of entry to a computer system and occasionally tampers with its data or information plus hacking issues were disclosed so we are with improved blockchain.

## 4 Improved and Secured Blockchain

Seeing as the existing transfer of funds by online payment system is too much difficult and business transaction supporters are distributed, the points chosen through safety measures attacks are rapidly growing. A client planning to buy and sell currency will pay the fee for a yearly membership to obtain a card and utilize this card to buy products or use against services. Buyers' banking services and the seller's banking services operate together with one another to resolve the charge and a store or shop set up to use the card obtains it from a bank and utilizes it for the buy of products and to avail the services. A generalization of business transactions is essential because the majority of people use smart phones to buy products or to avail the services as revealed in Fig. 2 [25].

Peer-to-peer-based operation with blockchain is not merely trustworthy and provable but also profitable because there are no any mediators or third parties involved. Furthermore, a business transaction using digital ledger may be finished extra rapidly in this case distance does not matter, while traditional business transactions over the boundary can be extremely time-consuming. Furthermore, traditional, centralized management of business transactions is in danger to the disclosure of significant information at what time the functioning computing server machine is hacked. By comparison, it is extremely complex to attack or hack cryptographic ledger-based business transactions as every significant data or information is scattered or distributed and hackers must have to hack and modify fifty-one percent of the business transactions of peer-to-peer (P2P) network. As a result, the enhanced and secured cryptographic ledger, i.e., blockchain should be utilized for business transactions to resolve the trouble of usual all business transactions [26].

One of the major inconveniences of virtual currency using the cryptographic ledger is the risk of a dual business transaction. The effort of transferring the virtual or digital currency to two or more than two accounts for destructive ambitions is the



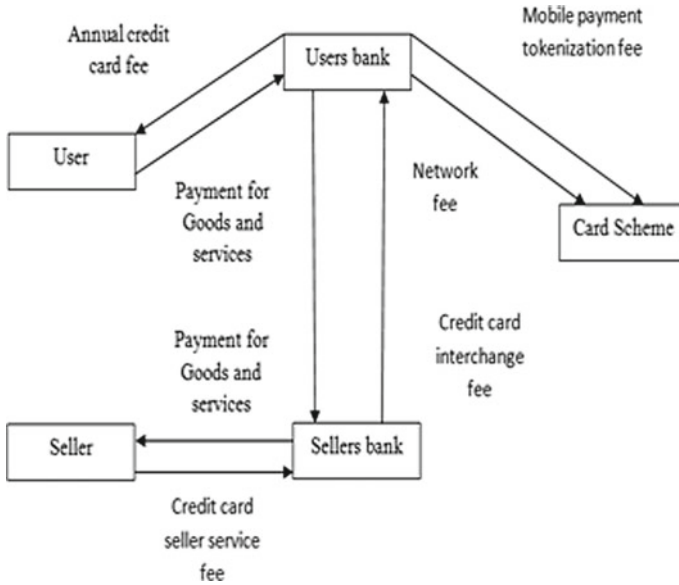


Fig. 2 Basic payment process system

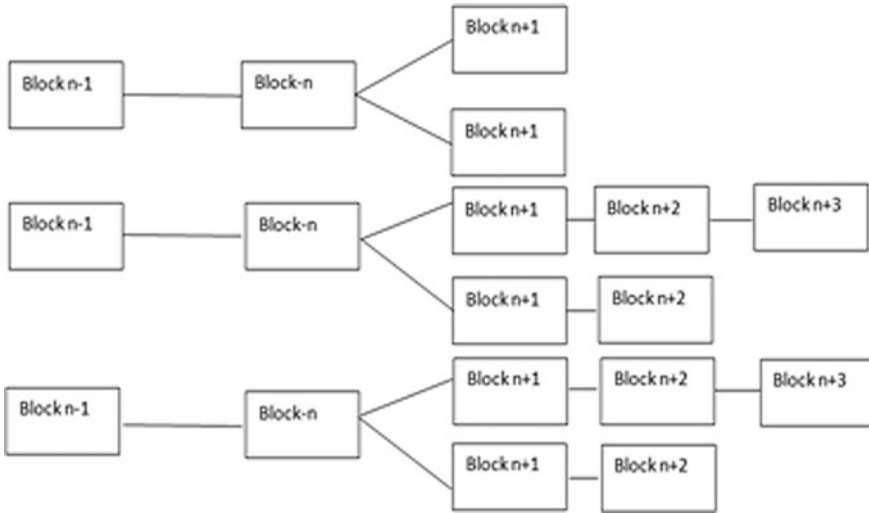
key job of a dual transaction. Basically longest chain and total currency wins and both are utilized as technologies for avoiding it. The longest chain rule ensures that the network will identify the chain with most jobs as the chief chain. Longest chain rule wins technology generates the subsequent block primarily once a digital ledger is now split by dual transaction and the largest chain along with the majority jobs will constantly win [27].

## 5 Blockchain Solution for Cloud Environment

Users’ sensitive information due to the monetary leak as well as psychological damages may occur in the environment of cloud computing. Cryptographic ledger is a representative technology for ensuring anonymity. Customer secrecy can be secured if the digital distributed ledger procedure is utilized in the cloud computing environment. Basically once using the blockchain technology e-wallet is installed and if e-wallet is not appropriately removed, the customer data or information may be left which may be utilized to estimate or conclude the customer information.

To avoid such an issue, we contemplate a solution that establishes plus removes the e-wallet strongly. The double spending trouble can be dealt with through prevention techniques as revealed in Fig. 3.

A secure wallet is required to resolve the above security problem. Basically e-wallet is installed and used in the PC. The safety of digital wallets in cellular phone



**Fig. 3** Technique for double spending prevention

plus in any digital gadgets should be confirmed because mobile phones have turned out to be extraordinarily accepted. Now the safety of a business transaction can be established only if both the reliability and accurateness of a time stamp produced in a smart phone are guaranteed [27, 28].

A digital wallet also called e-wallet mentions to software programs, online service, or electronic device, and to utilize a digital wallet efficiently, all clients must complete the installation process of digital wallet properly on their personal computer and the platform communicates digital wallet and information to set up safe and sound surroundings. The client must download as well as install the digital wallet freeware properly to make good use of the virtual currency through public transaction ledger along with the platform public key (is used to make certain that you are the holder of an address that can accept funds) is sent to the digital wallet as soon as the installation is completed. The e-wallet or digital wallet transfers the certificate distributed during improvement to the platform, and that confirms the power of the certificate in the digital wallet. The platform and digital wallet swap the key using the Diffie–Hellman technique, with everyone accepting the shared key. Money should be deposited in the e-wallet earlier to any business transactions or any bank account can be attached to the e-wallet. It made basic financial transactions as well as validates the holder’s credentials. As a client desires a business transaction linking to utilize a virtual currency, the book data holding the time stamp information among the digital card and the platform are enciphered through the shared key and then finally transmitted. At what time demand for discarding is carried out, the certificate of clients establishes and removed from the digital wallet after that the completed message is transferred to prove that it has been strongly abandoned. Furthermore, every related file is deleted so that the residual data are strongly isolated as shown in Fig. 4.

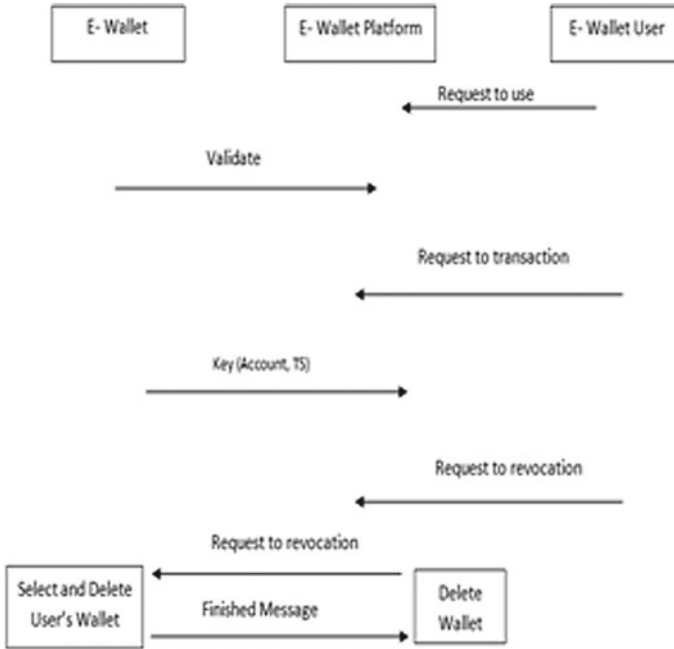


Fig. 4 Process of secure bitcoin

This process utilized a digital wallet based on public transaction ledger in a cloud computing environment. A public transaction ledger procedure is utilized to eliminate the data/information of the customer who makes use of the cloud. This process implements and utilizes a digital wallet and deletes it usually. The digital wallet is strongly deleted by transfer the completed message. Client information can be prevented from revealing only when the digital wallet is entirely deleted.

We compared the processes by existing studies with regard to confidential issues, integrity issues, anonymity issues, residual information protection problems, and privacy protection issues as displayed in Table 1.

The secured cryptographic ledger solution enhances safety by giving remaining data/information security since it uses the public key to encrypt the data/information moreover confirms the entire deletion of the digital wallet.

## 6 Conclusion

We examined the blockchain technique and interrelated core technologies. A variety of existing issues should be speculated to employ digital ledger within the environment of cloud computing. The secrecy of client information has to be guaranteed when utilizing digital ledger in the environment of cloud computing and the client

**Table 1** Comparison of related techniques

	Fifty-one percent attack case [28]	Authentication case [27]	Secure blockchain solution
Confidentiality	Yes	–	Yes
Integrity	Yes	Yes	Yes
Anonymity	Yes	Yes	Yes
Availability	–	Yes	Yes
Privacy protection	Yes	Yes	Yes
Residual information	–	–	Yes
Protection	–	–	Yes

data/information must be completely removed when deleting the dealing. In case the client data or information is not removed but left, as a result, the client information or data may be predicted from the remaining data/information. For that reason, this learning discussed the technique of giving safety measures by introducing a technique of protected public encrypted transaction ledger, i.e., blockchain utilization and deletion method. Hence it has been established that blockchain can be a suitable and powerful tool to provide security in the environment of cloud computing.

## References

1. Narayanan A, Bonneau J, Felten E, Miller A, Goldfeder S (2016) Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press, Princeton
2. Beikverdi A, Song J (2015) Trend of centralization in Bitcoin’s distributed network. In: 2015 IEEE/ACIS 16th international conference on software engineering, artificial intelligence, networking and parallel/distributed computing (SNPD). IEEE, pp 1–6
3. Huang H, Chen X, Wu Q, Huang X, Shen J (2018) Bitcoin-based fair payments for outsourcing computations of fog devices. *Future Gener Comput Syst* 78:850–858
4. Christidis K, Devetsikiotis M (2016) Blockchains and smart contracts for the internet of things. *IEEE Access* 4:2292–2303
5. Zhang J, Xue N, Huang X (2016) A secure system for pervasive social network-based healthcare. *IEEE Access* 4:9239–9250
6. Johnson B, Laszka A, Grossklags J, Vasek M, Moore T (2014) Game-theoretic analysis of DDoS attacks against Bitcoin mining pools. In: International conference on financial cryptography and data security. Springer, Berlin, Heidelberg, pp 72–86
7. Moreno-Sanchez P, Kate A, Maffei M, Pecina K (2015) Privacy preserving payments in credit networks. In: Network and distributed security symposium
8. Li J, Jia C, Li J, Chen X (2012) Outsourcing encryption of attribute-based encryption with mapreduce. In: International conference on information and communications security. Springer, Berlin, Heidelberg, pp 191–201
9. Hur J, Noh DK (2010) Attribute-based access control with efficient revocation in data outsourcing systems. *IEEE Trans Parallel Distrib Syst* 22(7):1214–1221
10. Singh A, Chatterjee K (2017) Cloud security issues and challenges: a survey. *J Netw Comput Appl* 79:88–115
11. Bheemaiah K (2015) Block chain 2.0: the renaissance of money. *Wired*

12. Park JH, Park JH (2017) Blockchain security in cloud computing: use cases, challenges, and solutions. *Symmetry* 9(8):164
13. Bonneau J, Miller A, Clark J, Narayanan A, Kroll JA, Felten EW (2015) Sok: research perspectives and challenges for bitcoin and cryptocurrencies. In: 2015 IEEE symposium on security and privacy. IEEE, pp 104–121
14. Aitzhan NZ, Svetinovic D (2016) Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Trans Dependable Secure Comput* 15(5):840–852
15. Tschorsch F, Scheuermann B (2016) Bitcoin and beyond: a technical survey on decentralized digital currencies. *IEEE Commun Surv Tutor* 18(3):2084–2123
16. Hari A, Lakshman TV (2016) The internet blockchain: a distributed, tamper-resistant transaction framework for the internet. In: Proceedings of the 15th ACM workshop on hot topics in networks, pp 204–210
17. Vasek M, Thornton M, Moore T (2014) Empirical analysis of denial-of-service attacks in the Bitcoin ecosystem. In: International conference on financial cryptography and data security. Springer, Berlin, Heidelberg, pp 57–71
18. Möser M, Böhme R (2015) Trends, tips, tolls: a longitudinal study of Bitcoin transaction fees. In: International conference on financial cryptography and data security. Springer, Berlin, Heidelberg, pp 19–33
19. Meiklejohn S, Orlandi C (2015) Privacy-enhancing overlays in bitcoin. In: International conference on financial cryptography and data security. Springer, Berlin, Heidelberg, pp 127–141
20. Gkaniatsou A, Arapinis M, Kiayias A (2017) Low-level attacks in bitcoin wallets. In: International conference on information security. Springer, Cham, pp 233–253
21. Bamert T, Decker C, Wattenhofer R, Welten S (2014) Bluewallet: the secure bitcoin wallet. In: International workshop on security and trust management. Springer, Cham, pp 65–80
22. Haber S, Stornetta WS (1990) How to time-stamp a digital document. In: Conference on the theory and application of cryptography. Springer, Berlin, Heidelberg, pp 437–455
23. Sapirshstein A, Sompolinsky Y, Zohar A (2016) Optimal selfish mining strategies in bitcoin. In: International conference on financial cryptography and data security. Springer, Berlin, Heidelberg, pp 515–532
24. Kogias EK, Jovanovic P, Gailly N, Khoffi I, Gasser L, Ford B (2016) Enhancing bitcoin security and performance with strong consistency via collective signing. In: 25th {usenix} security symposium ({usenix} security 16), pp 279–296
25. Karame GO, Androulaki E, Capkun S (2012) Double-spending fast payments in bitcoin. In: Proceedings of the 2012 ACM conference on Computer and communications security, pp 906–917
26. Stinson DR, Paterson M (2018) Cryptography: theory and practice. CRC press
27. Mann C, Loebenberger D (2017) Two-factor authentication for the Bitcoin protocol. *Int J Inf Secur* 16(2):213–226
28. Bastiaan M (2015) Preventing the 51%-attack: a stochastic analysis of two phase proof of work in bitcoin. <http://referaat.cs.utwente.nl/conference/22/paper/7473/preventingthe-51-attack-a-stochasticanalysisoftwo-phase-proof-of-work-in-bitcoin.pdf>

# An Introduction to Blockchain Technology and Their Applications in the Actuality with a View of Its Security Aspects



Reinaldo Padilha França, Ana Carolina Borges Monteiro, Rangel Arthur, and Yuzo Iano

**Abstract** Blockchain, in this innovative context of digital transformation, is nothing more than a chain of digital blocks, in which each block has a specific data and a code that connects to the previous block, and consequently, a chain is created that protects the information. The relationship between Blockchain and information security comes from the decentralization to store information with greater security, still considering the ability to enable the secure tracking of transactions, offering transparent access to information. Still evaluating the aspect of cybersecurity as one of the advantages of Blockchain, after all enabling the tracking of information, it also allows for a more secure decentralization of data storage than other known technologies. Still reflecting that in addition to authenticity, it is possible to optimize the signing of online contracts, thus preventing fraud in the registration of contracts from being made and generating losses. Guaranteeing the basic properties of Confidentiality, Integrity, and Availability (CIA) and concerning natural protection with blockchain distributed digital ledgers (once in the ledger, occurs after mining by users of the blockchain network validators) and consensus rules. Thus, Blockchain is a technology, and it is an efficient alternative to protect critical and sensitive information, capable of encrypting, tracking, and certifying any information, with potential in relation to cybersecurity that allows recording digital transactions. Therefore, this chapter aims to provide an updated overview of Blockchains, showing its relationship as well as approaching its success, with a concise bibliographic background, addressing its applications, and fundamental concepts, synthesizing the potential of technology.

---

R. P. França (✉) · A. C. B. Monteiro · R. Arthur · Y. Iano  
School of Electrical and Computer Engineering (FEEC), University of Campinas—UNICAMP,  
Av. Albert Einstein - 400, Barão Geraldo, Campinas, SP, Brazil  
e-mail: [padilha@decom.fee.unicamp.br](mailto:padilha@decom.fee.unicamp.br)

A. C. B. Monteiro  
e-mail: [monteiro@decom.fee.unicamp.br](mailto:monteiro@decom.fee.unicamp.br)

R. Arthur  
e-mail: [rangel@ft.unicamp.br](mailto:rangel@ft.unicamp.br)

Y. Iano  
e-mail: [yuzo@decom.fee.unicamp.br](mailto:yuzo@decom.fee.unicamp.br)

**Keywords** Blockchains · Encryption · Ledger · Information · Cryptocurrencies · Security · Cybersecurity · Encryption · Transparency

## 1 Introduction

Blockchain technology is nothing more than a public ledger that records a virtual currency transaction (the most popular of which is Bitcoin), so that this record is reliable and unchanging. It is a chain of blocks, hence the name, that is part of a collective registration system. This means that the information is not stored in one place, because instead of being stored in a single computer, all blockchain information is distributed among the various computers connected to it. That is, the blockchain records information such as the number of bitcoins (or other currencies) traded, who sent it, who received it, when this transaction was made, and wherein the book is recorded. This shows that transparency is one of the main blockchain predicates [1].

It stores this information, this set of transactions, in blocks stamping each block with a time stamp. Each period (10 min in the blockchain), a new transaction block is formed, which binds to the previous block. This way is possible only to access this database from the owner's computer and see a negotiation that took place between two people, for example, being in distant places, one in China and one in Germany [1, 2].

More and more companies use data as a source for efficient management, being used as a basis for strategic decision making. Keeping this information secure is crucial to keeping the company's branded value and sensitive information secure. The blockchain provides a broader view of information security, rather than traditional endpoint protection tools. This broader view includes the security of the user's identity, transactions, and communication infrastructure through transparent processes [1, 3].

The details about who is involved cannot be known as everything is encrypted. But it is well known that that transaction took place and that it is written to the blockchain forever, since it is spoken "forever" in the literal sense. After all, it is not possible to undo or change a transaction after it is entered into the system [4]. Several segments of the economy have already shown interest in the technology; there are already records in ports where loads of soybeans sent from the USA to China became the first agricultural loading that had all its blockchain stages. Another example that mixes applications and virtual currencies is ether. It is a cryptographic currency that feeds Ethereum, a blockchain of connected applications, which are programmable that run as long as someone supplies them with ether [5, 6].

Blockchain is one of the emerging technologies that have been gaining prominence in the world's technological scenario. Initially designed to enable secure transactions between Bitcoins, its technological potential has been reaching other applications that are not restricted to cryptocurrencies, attracting the interest of banks, companies, and governments [6].

How this technology can be used for information security? It is possible to use three terms for this action concerning decentralization; tracking; and cutting-edge encryption. The blockchain decentralizes data and stores it more securely. Thus, it enables the tracking of information, and cybersecurity is one of the main results. This is possible because its blocks are spread over thousands of computers around the world and, thus, a change can only be made when accepted by all systems belonging to your network [7].

Smart contracts are small programs that automatically make multi-party agreements when certain conditions are met. Because these mini-programs run on the blockchain, there are no intermediaries to manage the transaction or charge fees. Sending and receiving payments is the most popular blockchain application today, as its beginning was directly related to cryptocurrencies [5, 8].

In a centralized database, which is currently used by companies, just one “door” is enough for the attacker to be able to enter the server and have access to the data, often without leaving a trace. With blockchain, an attacker would have to have control of 51% of the nodes in the chain; that is, he would have to invade multiple machines to validate a change. Besides, all movement would be traceable [9].

In addition, the blocks are stored on several computers around the world. Even though they were geographically distant, they are interconnected, and when a change is made to the blocks, it is only accepted if the systems that make up the network allow it. This means that if a hacker manages to enter a single machine from a company to hijack the data, the other computers that make up the block will act, invalidating the action. This action that the blockchain provides will also be important for safe web browsing and password protection, for example [10].

Cloud storage will be another blockchain application that companies can benefit from. Within this context, blockchain can be used by companies to provide reliable, decentralized, encrypted, and uneditable databases [11].

Because it is a public and decentralized structure, the blockchain makes transactions in an encrypted, secure, and agile way. Still considering that through the blockchain, companies can consider that their data will never be erased or changed; transactions and interactions will be done with reliable rules; there will be proof of time, ownership and rights; there will be resistance against a single point of failure and censorship; there will be transparency and selective privacy [12].

This vision is increasingly necessary in today’s connected world. In a world where companies reinforce their defenses against security breaches, fraud, and hackers, blockchain can be an alternative to digital transactions. The feature eliminates intermediaries and transactions to take place in real time. In addition to providing security, blockchain reduces the risk of fraud as the data is auditable and verifiable. Therefore, IT management must start to see the relationship between blockchain and data security as an alternative to protecting your information [13].

Therefore, this chapter aims to provide an updated overview of Blockchains, addressing its evolution, applications, and fundamental concepts, showing its relationship as well as approaching its success, with a concise bibliographic background, categorizing and synthesizing the potential of technology.



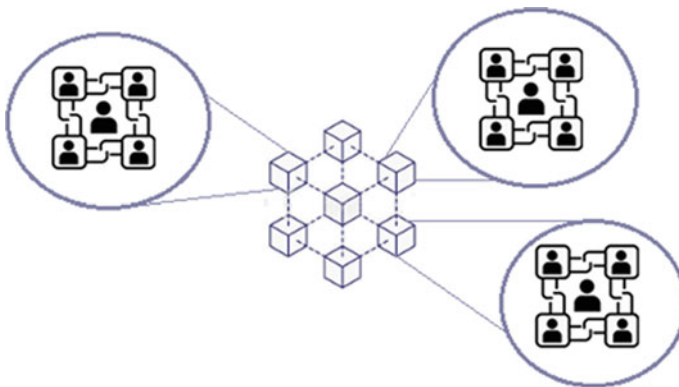
## 2 Methodology

This study was developed based on the analysis of scientific articles and scientific journal sources referring to Blockchains toward security issues, aiming to gather pertinent information regarding thematic concerning evolution and fundamental concepts of technology. Thus, it is also possible to boost more academic research through the background provided through this study.

## 3 Blockchain Background

When thinking about Blockchain, it is commonly associated with the universe of bitcoin and other cryptocurrencies; after all, it was in this innovative context of digital transformation that technology emerged and gained popularity. What it is nothing more than a chain of digital blocks, in which each block has a specific data and a code that connects to the previous block (Fig. 1), and consequently, a chain is created that protects the information [1, 14].

Blockchains can be divided into two categories: public, relating that any user can participate, where, in general, there is some incentive mechanism to encourage new members. An open blockchain, in general, is a huge chain, which with this demand is a necessary complex data processing, which requires high computational capacity, considering the biggest example regarding Bitcoin; and private, relating that in general, it is restricted to invite or authorize users, making the entry need to be validated by the person who started the chain or by rules predetermined by him. Consequently, once an entity has joined the network, it becomes part of the decentralized maintenance of the blockchain. What, for example, a system with these properties can be used by employees of a company or members of an organization. Thus, the difference between public and private Blockchains is respective to the



**Fig. 1** Connected blockchain Illustration

groups that are allowed to participate in the network, execute the consensus protocol to certify the transactions, and preserve the shared record [15, 16].

The unit of information in the Blockchain (Fig. 2) is called a transaction, relating that each user and each transaction has its own identification, so that without this data, it becomes impossible to know who is behind a certain process. Thus, within the Blockchain, these transactions are grouped into forms of data blocks. In this sense, for the blocks to be made, it is necessary to respect some rules, such as the maximum size of transactions that a block can hold and contain only transactions that are verified as valid, for example [17].

Still evaluating that while the transactions wait to be added in some block, they are temporarily in a structure called a pool. What is more, it is perfectly possible to trace the origin of any block from the fingerprint of only one of the parts. In short, the information can be certified and validated with great agility and security [17, 18].

Blockchain is known as a trust protocol, it is a chain of blocks; that is, it is a database formed by interconnected and decentralized blocks, and it is a technology that eliminates the need for intermediation by third parties in various types of transactions. It works as a kind of public register of witnesses who authenticate certain information.

Through Blockchain, data security for storage is provided due to encryption and the miners who check each block. Unlike a centralized database, in which an administrator is certifying and validating the data, in Blockchain technology this validation

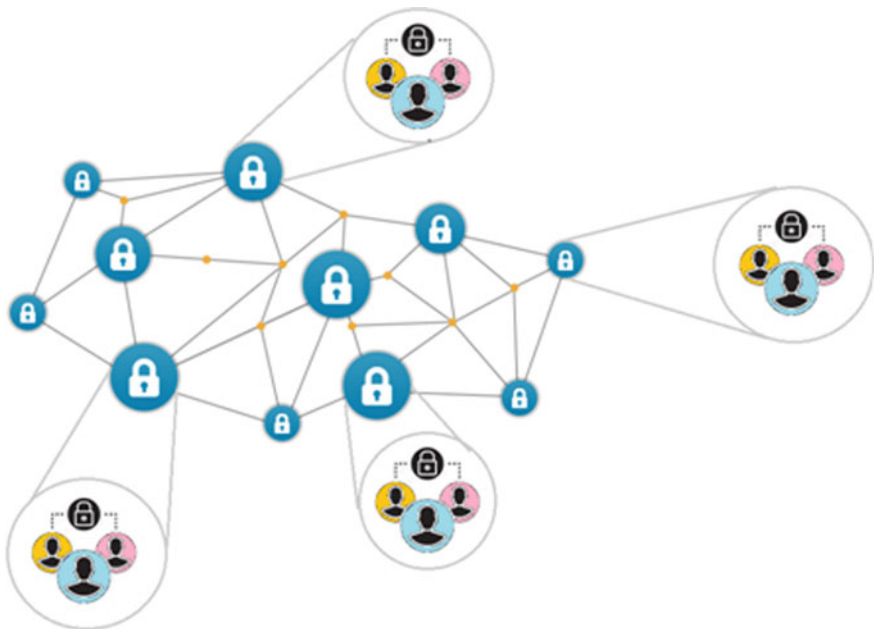
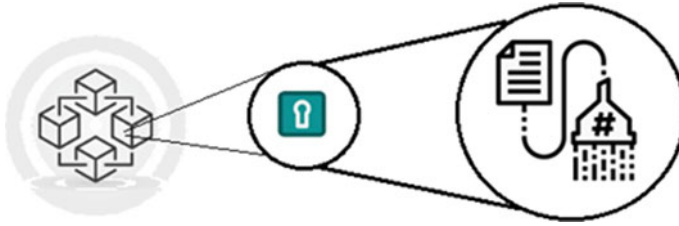


Fig. 2 Blockchain illustration



**Fig. 3** Hash illustration

is done by the nodes of that block, which are formed by computers spread across the web. So, for any transaction to be considered valid, it needs to be validated by the majority, at least 51% of the chain [17, 18].

In Blockchain, validation is done without the need for people to act as a mediator, but by computers around the world. What happens only when the machines that keep the code confirm the authenticity of the information, through a kind of encrypted digital signature, enabling the validation of the data and the guarantee of the origin of digital documents, products, financial transactions, among several others [19].

With respect to the encryption of each block generated on the Blockchain, each one carries a hash, which is respective to a sequence of letters and numbers. The Blockchain hash (Fig. 3) is encryption that stores the contents of the current block plus the previous one, making all blocks store information from the entire chain. And in this sense, it prevents adulteration with a simple invasion, since every transaction must be validated by the majority, that is, 50% + 1 [12, 20].

The hash is the cryptographic guarantee that the information in that data block has not been breached. This means that each time a new block is created, it has its own hash and loads the hash of the previous block, literally meaning a “chain of blocks” (blockchain). Relatively, any computer that connects to the Blockchain interface is considered a node. And so, the full nodes are the ones that really provide support and security to the Blockchain, since, in general, they are the ones that download a copy of the Blockchain [21].

And in practice, therefore, the Blockchain is not centralized in a single place, considering that interconnected computers are responsible for “auditing” transactions, which means that each network has groups of independent machines, which can be accessed from any location a place that has Internet access. And so, each block is created in constant time, about 10 min, exemplifying bitcoin and making the Blockchain network adjust to demand more or less from the nodes [3].

All changes made to a block are recorded forever, which facilitates tracking, a characteristic that can be used in the validation and certification of documents, contracts, reducing costs, and bureaucracy with the breakdown of the intermediary [21].

Transaction registration in relation to Blockchain is that it works in a totally decentralized and distributed way; that is, any allowed user (digitally signs his information using his private key) can have a copy on his computer, and this procedure works

as a cryptographic operation on all transaction information, generating a key (represented by another large set of numbers and characters), while also mentioning the characteristic related to ensuring that all data is always under secrecy and privacy [22, 23].

In this sense, for all transactions made to become anonymous, Blockchain uses the principle of addresses, starting from the use of individual private keys and with the application of cryptographic operations, generating several addresses that are formed by a large set of characters and numbers. With the use of addresses, whenever there is a new transaction, the use of a new address is made, which is not possible to discover the identity of the individuals who are inserted in the transaction, ensuring the anonymity of both. Still evaluating the use of keys, which can and should be kept in safe places, users are able to have control over these addresses [20, 22, 23].

In a typical Blockchain application, the loss or theft of the cryptographic key is equivalent to the loss of identity on the network. In this respect, the criticality is great, since the identity of any entity is a fundamental part of the transactions, be they access permissions, financial or legal. Thus, in any system, an identity must be able to be created, modified, stored, distributed, disseminated, and destroyed, both of the associated identifiers and the attributes [9, 14, 24].

The traditional model of identity management has characteristics that make it difficult to establish trust relationships between different entities, through Blockchain, with the centralization of the identity bases for each specific entity, especially the Internet of Things (IoT). An identity more adherent to the idea of personalization, that is, more uniform and reusable in different silos, while preserving privacy and security [25].

Thus, the use of Blockchain for the establishment of digital identity becomes more difficult to be stolen because it starts to be monitored publicly, and even from a reputation system, it is an important step toward the use of secure applications. Since it is not subject to forgetfulness, it has inviolable time parameters (time stamp), giving individuals greater control over who owns what portions of their personal information and how they are accessed, allowing the use of these principles in transactions that reinforce trust and also the authorship of accesses and transactions, without the need for a centralized entity for the creation or validation, with control by the device or person [26].

When a Blockchain transaction is made, it needs to go through a validation process. So, first, it stays in a temporary area awaiting its inclusion in the Blockchain, when it finally becomes official. In general, an analysis is made of all transactions that are in that temporary area, and then, they are evaluated by a miner (checks the authenticity of each of the transactions, as well as the validity of the signature and if it corresponds to the transaction data, confirming the last step of making the transaction official), which is nothing more than a computer connected to the network, which goes through a mathematical competition, and if it wins, it will have the right to introduce the transaction to the Blockchain. Considering the aspect of the digital signature that deals with types of fraud concerning whether the transaction was actually made or whether someone simply did a generation of fake addresses, simulating that way fake transactions for their own account [17, 18].

Blockchain authentication is transactional in nature; it is centralized, usually with a base of passwords or biometric references that are unique or that work in federations, and the objective is to validate the identity and allow entities to relate and carry out different transactions (permissions of access, financial or legal) in a safe and private manner. In addition to centralization, traditional authentication is fragmented, which makes the authentication process problematic in relation to the user experience, with different methods and the need for multiple registrations to access each service [27].

Traditional, centralized, and fragmented authentication is also not adherent to the reality of IoT, in which billions of smart devices connect in different ways and need an authentication method that is homogeneous, secure, and efficient. In general, devices have used authentication mechanisms that work, but do not scale and do not have adequate security, which is one of the concerns in cybersecurity related to IoT [28].

With the use of distributed protocols such as those employed through Blockchain technology, together with cryptographic techniques that add reputation and trust in authentication and also with the use of security algorithms, it has the properties of generating a balance between the user experience, security, and privacy. Assessing that in addition to authentication, it is necessary to define access control models that include the layers of authorizations and permissions, which impact the privacy and confidentiality of information. At this stage, it is made official through an official time stamp, from the date on which the transaction was carried out and in which the miner signs the due transaction by developing more cryptographic processes, generating, for each of the transactions (transaction id), related to the key that identifies an official transaction [29].

The transactions carried out on the Blockchain are immutable, regarding the existence of the hash, consisting of a mathematical function used on the information of the Blockchain, and generating an encoding for each version of it. That is, whenever there is any change, the hash will also change. This hash feature is essential to prevent any user from forging transactions on the Blockchain, which adds much more reliability and credibility to the system [23].

The advantages of Blockchain are related to **transparency**, that is, anyone can check and audit registered movements; **decentralization**: it evaluates the aspect that eliminates the need for agencies to approve transactions or determine rules, even related that from this property Blockchain networks do not have a central point of failure and are more resistant to malicious attacks; **immutability**: it consists of a record that cannot be altered, revised, or altered, even by those who operate the database; **reliability**, for the validation of a transaction, requires that other participants' computers enter into a consensus to enable it to occur; **respective automation**: there is no duplicity or conflicting information, and transactions that do not respect this rule are not registered within the block; **speed** with respect to traditional bank transactions can take up to days to be cleared and actually carried out. What with respect to Blockchain transactions are carried out in minutes and are processed 24 h a day, 7 days a week, still considering the aspect of **empowerment** regarding users being in control of all their information and transactions [2, 6, 30].

## 4 Blockchain Security

The relationship between Blockchain and information security comes from the decentralization to store information with greater security, still considering the ability to enable the secure tracking of transactions. Aligned with the objective of offering a model that adds confidence to unreliable environments, in the same sense that reduces business interruptions by offering transparent access to information available in the chain [8, 31].

This is possible because its blocks are spread across thousands of computers around the globe, so a change can only be made when accepted by all systems belonging to your network, still evaluating the transparency and immutability offered by Blockchain and getting a file system with Blockchain technology to be distributed with respect to participants maintaining copies of the file and agreeing to changes in consensus. As far as this file is made up of blocks, each includes a cryptographic signature from the previous block, creating an immutable record and thus, concluding a more secure option than any other current information system for negotiating information digitally [32].

If information was made to be visible, then multiple copies mean there is less chance of losing and stealing it. Assessing the context of any cyber threat that attempts to invade any of the computers on the network, the others will notice the malicious behavior and may prevent the attack. As technology is very flexible, the idea is that any element can be placed in Blockchain, whether in need of anonymity or public accessibility. In this context, companies can carry out their applications automatically and more safely, especially those related to the movement of digital assets, the sharing economy, or even with respect to decentralized services [33].

Given that through Blockchain, companies can expect that data will never be erased or changed, there will be proof of time, ownership, and rights; transactions and interactions will be done with reliable rules; there will be resistance against a single point of failure and censorship, still evaluating that there will be transparency and selective privacy [34, 35].

This technology can be used in different applications and contexts within a given organization, such as in the identity management of corporate systems. Since thinking about Blockchain, a broader view of security is assessed information, rather than traditional endpoint protection tools. Considering that this broader view includes security of the user's identity, and even communication infrastructure through transparent processes and transactions [34–36].

With regard to identity management, Blockchain can be used to establish identity and create a reputation system. Regarding that through this type of efficient mechanism, digital identity becomes more difficult to be stolen, as it starts to be monitored publicly, not to be forgotten, and to have inviolable time parameters. Still, pondering the factor related to the use of Blockchain-based identities allows users to have greater control over who has access to your personal information and how it is used [34–36].

This vision is increasingly necessary in today's modern connected world, since technology can be an alternative to digital transactions, just as companies reinforce their defenses against security breaches, fraud, and digital intruders. Another effective way to use it in corporate security is to decentralize data storage, considering that through it, the blocks are kept on different computers interconnected with each other (Fig. 4). Regarding that in addition to tracking, Blockchain breaks with the current model of centralized data storage and is based on decentralization [34–36].

Regarding the blocks being “deposited” on thousands of computers, but interconnected, it is relative to the integrated work of the machines, meaning that any change made to the Blockchain is only accepted if all computers “allow.” In practice, this means that, even if one machine is invaded, the others will notice the change and stop the attack, making it even more difficult to attempt to invade such a system [37, 38].

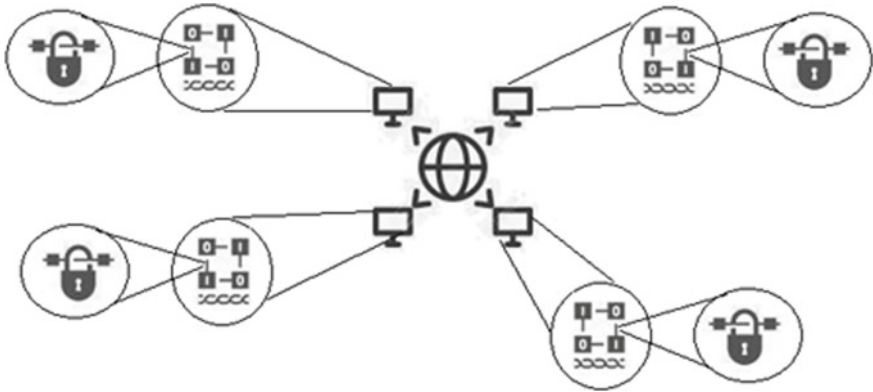
Cybersecurity is one of the advantages of Blockchain; after all, in addition to enabling the tracking of information, it also allows for a more secure decentralization (Fig. 5) of data storage than other known technologies. This is because despite being geographically distant, the blocks are “kept” scattered around the world, but even so, they are interconnected with each other; still, pondering the virtue of integrated work with regard to the change made is accepted with permission [37, 38].

Consequently, a system with this technology can help corporations to carry out proofs of authenticity for web content. Evaluating that through a plugin that is installed in the browsers of the employees' devices, it is possible to generate a report with information from the online page, providing a respective time stamp to when that content was published [39–41].

Still reflecting that in addition to authenticity, it is possible to optimize the signing of online contracts, thus preventing fraud in the registration of contracts from being made and generating losses. This is possible because if a document certified with Blockchain technology is changed, the fraud is quickly identified, which permeates the sense and the certainty that the document that was signed is safe [39–41].



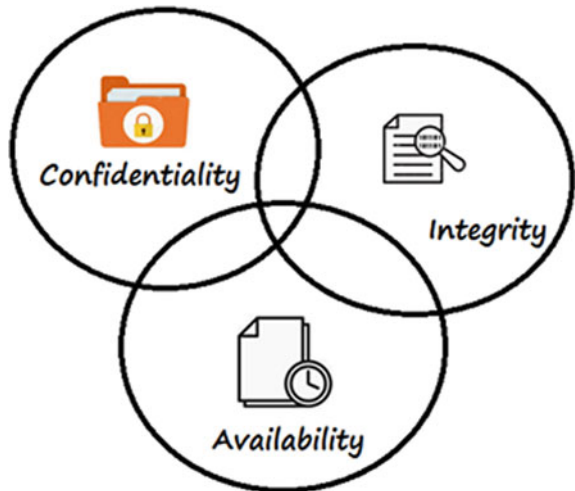
**Fig. 4** Blockchain interconnected with each other illustration



**Fig. 5** Blockchain decentralization illustration

Information security means guaranteeing the basic properties of Confidentiality, Integrity, and Availability (CIA) (Fig. 6), and with regard to natural protection with blockchain, distributed digital ledgers (once in the ledger, occurs after mining by users of the blockchain network validators) and consensus rules (data can no longer be erased or changed; that is, integrity is guaranteed), intrinsically guaranteeing the security of stored information, with regard to integrity and availability. And, as this data is distributed, repositories are decentralized and there are no single points of failure, which are valuable for protecting against denial-of-service attacks (availability is guaranteed) [39–41].

**Fig. 6** CIA properties illustration





It is worth mentioning that the consensus rules play a fundamental role, relating the methods for obtaining the respective consensus to the Practical Byzantine Fault Tolerance (PBFT), Proof-of-Work (PoW), Proof-of-Stake (PoS) algorithms, and Delegated Proof-of-Stake (DPoS), among others, when validating transactions before being permanently written to the blockchain ledger and still mentioning that digital platforms based on blockchain ensure the protection of corporate data, with protected and fully automated platforms, which allow the user to obtain certification and verify the authenticity of any document online [42, 43].

As well as considering a deeper view into the issue of intrinsic security, regarding the importance of consensus rules, which reinforces the importance of a Blockchain application project that takes security into account. Regarding the types of attack of 51%, with respect to when a single node of the blockchain network has more computational resources than the rest of the nodes of this network, this criterion means that in addition to controlling the contents of the network, this malicious node dominates the checks and approvals of transactions, resulting in the Blockchain network being manipulated, duplicate transactions, or the insertion of fraudulent transactions, or even theft of assets from members of the network [29, 39, 41].

Sybil attack types can also be considered, which relate an entity that can fill a Blockchain network with specific customers, which can lead to transaction manipulation, exploiting flaws in identity validations, since it starts to control multiple nodes of that network. Even so, in addition to the 51% attack and the Sybil attack (which are dealt with by consensus rules), there are denial-of-service attacks, which cause large amounts of data to be sent to miners, and may remain unable to process legitimate transactions, which makes that blockchain unavailable [44].

The need for blockchain security, in itself, can be considered safe and guarantees the integrity and availability of the information that becomes part of the distributed ledgers, arising from the natural protection of the stored data and against the typical attacks of distributed systems. Even so, assessing an additional need in relation to the points that become the primary natural targets of attacks, essentially executing the interface between the user and the functions of the blockchain, implies that Blockchain applications need specific security mechanisms [39–41].

However, it is worth mentioning that what cannot be considered inherently secure is the rest of the information manipulation process before the application of blockchain technology (not being able to ignore potential vulnerabilities) be validated to do part of the distributed ledger, considering that Blockchain technology is not capable of detecting fraudulent activities on its own, with regard to the performance of malware or even cases of identity theft that exploit transactions before their validation, which requires a development process safe [45].

## 5 Blockchain Applications

Blockchain is a technology capable of encrypting, tracking, and certifying any information, with important potential in relation to cybersecurity; considering that the

technology allows recording digital transactions, it is an efficient alternative to protect critical information, which needs to be verified by certain people, but not they can be publicly accessible, i.e., any digital interaction, in a safe, transparent way, highly resistant to external interventions. Considering the sophisticated level of authentication and security added to the ease of implementation in other scenarios, it makes technology a promising alternative, for both public and private sectors [46].

Despite emerging with Bitcoin cryptocurrencies, the technology behind Blockchain is not tied exclusively to digital currency. The innovation potential of technology makes it possible to apply it in different segments and industries, which revolutionizes all sectors that make use of digital payments [34, 35, 47].

Through the Blockchain, it is possible to manage health information online, such as exams and consultation history, and patient data, making all of this data and processes registered in the blockchain and also relating that the technology's capacity, through its secure network, is able to inform the doctor only what is necessary. Since the blockchain does not register only assets and transactions, but practically anything (data), therefore, the protocol is already being used to register and verify the authenticity of various types of documents [48–52].

Still reflecting on the application in the health area, it is also possible to combine technology with health by offering applications for mobile devices that are encrypted and structured in the blockchain, relating that the user can view their shared information, in relation to patient profiles, as well as their medical records and the like, especially when attending clinics, hospitals, or even research institutions [53–56].

Through the Blockchain, it is possible to track products, an important task to certify the veracity of the information, tracking the grains (in the agricultural area) safely (through a QR Code, for example) and guaranteeing their quality. As a result, customers are able to access any detail about the path the grain took from its origin to its commercialization to retail [34, 35, 57].

The signing of contracts is another activity that benefited by the application of Blockchain, relating that as it is an often-fraudulent registration, something that brings many losses for organizations from the most diverse areas. Blockchain can certify a document, and if any changes happen, as there are many ways to defraud that record, it will be possible to detect it. In this sense, signing online contracts with the Blockchain identity, it is possible to use the chaining of blocks for more secure browsing on the Internet, protecting passwords, and among other factors. This would result in the replacement of notaries by Blockchain systems, replacing systems for regulating contracts between parties, which would authenticate documents (digital payments) automatically [57].

Blockchain can also be used to generate more legal security, with respect to property related to Blockchain identity, which employs encryption of asymmetric keys in an application, doing the validation of users' identity. In general, listing three stages is related to registration by application and preliminary validations; automatic search in public networks; and even automated validation and manual verification in case of discrepancies. After these steps, the system will create a unique blockchain identity for a given user, who will be able to perform various actions on the Internet,

such as profile registration on sites without filling out forms, or even login on sites without using a password, among other features [34, 35].

Still, with respect to the use of Blockchain in the sale of digital property, it is possible to issue numbered prints on all types of artwork in their digital format. Evaluating that technology helps, protects, and manages creative work, as well as sharing art, for example. In this respect, it favors the purchase and sale of art digitally and fosters the art market, allowing art lovers to digitally collect the works without the artists suffering any damage related to copyright [35].

With regard to retail and food logistics, Blockchain allows the traceability of the products sold, in the sense that they collect data on the origin, security, and authenticity of the food sold. With this, the final consumer has the possibility to know better the input he is buying, with regard to the planting place, the date of harvest, and the path taken to reach the supermarket shelf, among other properties and characteristics that can be considered in the production chain [58].

An essential aspect of Blockchain is related to digital payments, reflecting on the confidentiality of bank information and personal data, which naturally brings several concerns to the online consumer. In this scenario, an online page employing technology transmits more security and reliability, guaranteeing more sales.

With Blockchain, it is possible to generate fewer expenses and eliminate existing bank costs, in addition to making it possible to carry out unique and totally secure transactions, impossible to change. This allows, for example, banks to monitor payments in real time as they pass between banks in different countries, in an international transaction context, which is seen as simplifying transactions and lowering costs. With technology, it is still possible to adopt Blockchain in the possibility of creating new land registration systems, eliminating problems of fraud in deeds and with the lack of regulation [1, 4, 47].

Applied in the context of the stock exchange, Blockchain also allows implementing a system to record transactions between private companies securely. What it means in international payments, benefits include, for example, settlement in real time and the change or replacement of traditional bank correspondence, making the process faster and less costly.

In addition considering proof of authenticity for web content, considering those slanderous and threatening content on social networks, fake news, and/or website pages that may harm the image of a person or a particular company. Faced with such scenarios, Blockchain helps in information security through a plugin available for browsers, in order to generate a report with a “print” of the page in question, in addition to providing a time stamp of when that content was published [17, 18].

The potential of Blockchain for marketplaces is linked in that it can transform existing business models; assessing the potential to break paradigms, establishing a direct route between those who carry out operations, inhibiting agent fees and interventions, preventing fraud, and preventing sensitive data are intercepted improperly. Therefore, companies have invested in Blockchain as a trust protocol, to improve the digital infrastructure of online payments, which enables agile transfers of values between users of the platform, without the need for intermediaries to ensure transparency in transactions [34].

One of the great advantages of the system is the ability to record the complete history of operations, in the context in which detailed data of those involved in the transactions and validations of the blocks is available to users, allowing traceability, since a new block is only created from a previous block with valid transactions. This reflects in the aspect that when a new chain of transactions appears, it is born with a totally reliable history [2, 9, 22, 30].

Assessing that hacker attacks bring great damage to organizations, information security has become an extremely important issue in the corporate world, where, in this context, Blockchain is a disruptive technology, which demonstrates digital security by decentralization of storage. In it, the blocks are stored in many computers that are interconnected, since there is no one coordinating, that is, an owner [29].

In the web context with the application of Blockchain, domains will be shielded against attacks related to the most common invasion model of flooding a server, data center, or domain with thousands of simultaneous accesses, bringing down the IT structure of any company. Associated with the decentralized nature of the technology that requires it, in case of attempted invasion, it will be necessary to obstruct all the nodes of the block network and not a single domain, which is practically unviable [37, 38].

Still evaluating the context of cryptocurrencies, Blockchain was originally developed, which allows two people who do not know each other to transfer money to each other without necessarily being an intermediary bank to guarantee the legitimacy of the payment. Through efficient authentication, the Blockchain system itself through advanced encryption and a network of connected users (miners) in order to carry out checks and confirm that everything is right for that transaction to proceed [40].

## 6 Discussion

Even though Blockchain is currently separating from bitcoin, it is not possible to ignore that the technology originated with cryptocurrency. Considering that the cryptocurrency was born in a time of real estate bubble and global economic crisis, with the function of avoiding increasing the credibility of financial transactions in the digital environment, in the same sense as avoiding the duplicate spending of values. From this context, Blockchain decentralizes data and stores it more securely, ensuring digital security, enabling information tracking and cybersecurity as one of the main results.

However, from their properties linked to security and distributed environments, blockchain applications enable digital transformations with regard to the cybersecurity needs of the financial sector, the sharing economy, or decentralized services. Assessing that the world is transactional, Blockchain technology matches this criterion, still reflecting on the aspect of information security related to identity management, authentication, or security monitoring.

Expressing that the growth of cloud computing and the popularization of the Internet and mobile devices are facilitating banking, shopping, evaluating the invaluable time and accessibility gains that these solutions offer, fostering home office work, and providing mobility for access to business systems, however, in this context, there is also a growing concern with the security of these operations in a digital environment. However, based on this technology, a safer world is provided, due to the combined use of Blockchain with other security technologies, such as self-protection algorithms, cognitive security, or the detection of anomalous behaviors.

The way Blockchain is able to validate, store, and record data so that it is safe is linked to the development of information security solutions that are always among the priorities of a modern and digital society, which is in line with the guidelines of Blockchain to manage electronic guarantees, in association with access to information and product support, in a simple and secure way.

Currently, the important and confidential data of companies is stored digitally, which makes the concern with information security extremely important, being necessary the use of protective measures and tools, since the risk of cybercriminals accessing this information, which in general can cause data loss or damage. In this sense, Blockchain benefits information security through the use of three principles for this action, which is decentralization; tracking; and cutting-edge encryption.

In general, a centralized database is used by most companies, which is related to only one “port” for an attacker to be able to enter the server and have access to the data, most of the time without leaving a trace. In this context, Blockchain represents that when there is an attempt to invade an environment, it is necessary that it is done on several machines to validate a change, to have control of 51% of the current nodes; in addition, all the movement would be traceable. Consequently, the invasion is eliminated by Blockchain technology.

The advancement of Blockchain technology meant that a large part of the business processes started to be made by electronic means, which means that it provides in addition to the importance of safe web browsing and password protection; for example, if a hacker succeeds in logging in a single machine of a company in order to hijack the data, the other computers that make up the block will act, invalidating the action.

Since the focus on using data as a source for efficient management, being used as the basis for strategic decision making for a company, it is necessary to keep this information safe and crucial to keep the company’s branded value and confidential information safe. In this sense, it is important that IT management starts to see the relationship between Blockchain and data security as an alternative to protect your information.

Just as the Internet has revolutionized technology and the way how people live and do business, Blockchain is seen as a trend that companies have adopted to reduce costs and practically end bureaucracy, with the decrease in the use of papers, migrating to the digital environment—combined with technologies such as cloud computing and the growing use of mobile devices to access corporate systems, providing organizations with a more practical way of working, given the ease of access by employees, and allowing the option to work from anywhere.

As a result, it is necessary to protect these accesses to prevent this from being the way in which criminals can access corporate data. This allows the use of Blockchain as a strategic tool for various business sectors, providing that your transactions are validated through technology. Thus, it is not necessary to issue documents or intermediate financial entities for the business to be concluded.

Thus, as presented in this chapter, the technology works through a chain of blocks, which is a way to guarantee this security, considering that it is related to each other (blocks), so that each new block needs the validation of the previous blocks. And so, the technology works as a distributed network, in which there is no single central administrator. In this sense, if an attacker manages to enter a point on the network, there is no way to go ahead, since there is a need for the validation of the other blocks.

Still evaluating that there are several tools that guarantee protection to the system and that companies should invest, such as antivirus, firewall, and antispyware. Also considering these digital protection tools that should be installed on all devices used by the corporation, such as notebooks, smartphones, and tablets. And even so, with the addition of the use of blockchain technology, it allows the configuration of the devices that will access the network, as well as the definition of the allowed connections, which are essential to mitigate DDoS attacks and prevent ransomware attacks. As long as it is possible to halt a hacker attack, since, when invading a network node, the others will not allow the invasion to continue.

Blockchain has an impact both on specific areas of companies and on users' lives; since the growing demand for services and products offered by the Internet, the way of making payments has gained new parameters. What, in the context of the chain of information created to protect storage, plays an important role in digital security, linked to simple tasks such as shopping over the Internet, is already part of the routine of many consumers worldwide. Still highlighting the e-commerce segment as one of the fastest-growing segments in recent years, and in this scenario, Blockchain gains more and more space as a promise for the future of payments and financial transactions.

Still, assessing the scenario of the number of purchases made over the Internet is growing more and more around the world. This directly reflects digital payments, which are a major source of concern for consumers, mainly because they do not trust the confidentiality of bank information and personal data provided. In this context, through the application of Blockchain, the blocks containing this information are stored on several computers around the world. This means that even if they were geographically distant, they are interconnected, and when a possible change is made in these blocks, it is only accepted if the systems that integrate the network allow it. Still appreciating that when records are made in the interconnected blocks, it is not possible to remove or add information individually. For that, it would be necessary to break the encryptions, to carry out any type of modification in the blocks, and still demonstrate to the machines of the Blockchain network that this is correct.

Technological evolution is moving quickly toward preventing fraud and preventing sensitive data from being unduly intercepted, as it is a public and decentralized structure, carrying out transactions in an encrypted, secure, and agile way.

Even so, Blockchain is a promise of disruption for the long term, as the associated technologies are still immature, but under development.

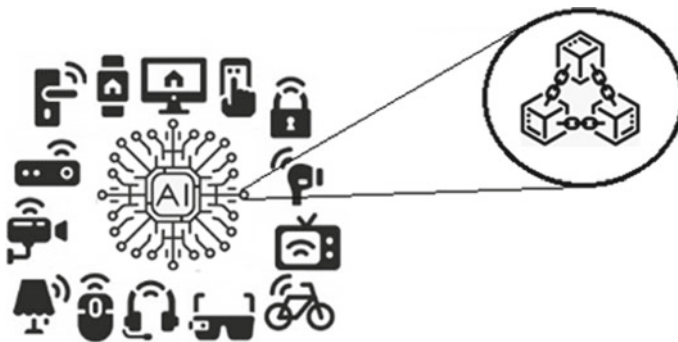
## 7 Trends

One of the major challenges for artificial intelligence (AI) to gain an even greater scale in relation to IoT is precisely the quality of the data. In what is derived from the collection, the data can be manipulated, edited, or deleted, still evaluating the possibility of being used to feed intelligent machines, through machine learning techniques. In that sense, Blockchain is an interesting solution while the technology brings the encryption that protects the data, and the AI works with intelligent algorithms to protect the encrypted data (Fig. 7) [50, 55].

Tokenization (a mechanism that detects the holder/owner of the asset that the token represents) of real assets is related to digital tokens, digital currencies, and even digital currencies backed by Central Banks from different countries, still evaluating the aspect of the possibility of using a digital contract issued using Blockchain and linked to a legal document that represents a real asset. In the sense of tokenizing assets and bonds, converting them into digital tokens and carrying out trading, exchange, and custody of these digital assets, using Blockchain is transforming the efficiency, security, and productivity of these capital markets [59].

The adoption of Blockchain with regard to the creation of an incorruptible data chain can be used for predictive analysis, since the blockchain data can be analyzed like any other type of element, with this data analyzed being organized in a decentralized manner, which can increase the power to obtain information and the scope of the analysis [57].

Through the Blockchain, the B2C relationship (companies for end customers) can be intensified, through the creation of a relationship in which the customer trusts the system and offers their personal and consumption data, feeding the business Big Data



**Fig. 7** AI+IoT+blockchain illustration

directly. This would allow new ways of working with blockchain, through data chains in several markets as a solution for real, incorruptible, decentralized data transitions that streamline the flow of information [35, 60].

The blockchain should allow for the ease of use of everything that companies need, regarding the infrastructure in which their data is hosted, in hybrid cloud computing environments, evaluating the multi-cloud and local character and, in this way, making technology allow a greater digital transformation of companies and industries [49].

Adjacent technologies such as IoT, 5G, AI, and edge computing can combine with Blockchain to generate added value for network participants, as blockchain solutions capture millions of data points and spread across the world; they open the door for new capabilities. For example, from this technological combination, it will be possible to create accelerators for blockchain-enabled markets in the future, relating that the most reliable Blockchain data will better inform and strengthen the algorithms. Signaling that Blockchain technology is no longer considered disruptive and is increasingly integrated into people's daily lives [61].

## 8 Conclusions

Blockchain is considered a disruptive technology and the engine of a great current revolution, evaluating its characteristics on what constitutes the basis of cryptography, guaranteeing a series of important properties linked to the possibilities of significant advances with respect to information security with its use, in fact, essential for the digital world increasingly being built assessing security needs in applications.

With the use of Blockchain, the stored information is immutable, inviolable, durable, resilient, stable, transparent, and distributed (Fig. 8). Reflecting that these

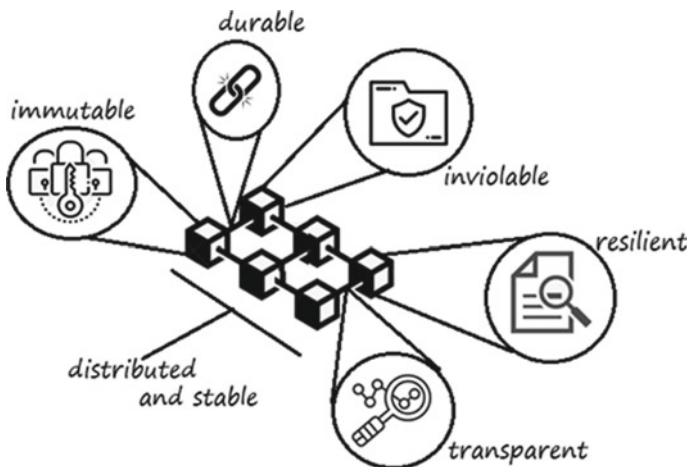


Fig. 8 Blockchain summary illustration



are properties that add up to resources that eliminate intermediaries and transactions occurring in real-time, providing security, reducing the risk of fraud, as the data is auditable and verifiable. Also considering the use of the distributed ledger and the consensus rules, which make many applications become viable automatically and safely, especially those related to the sharing economy, the movement of digital assets, or decentralized services.

In addition to bringing advantages to financial transactions, this Blockchain technology can be an ally to strengthen the protection of corporate data, which is a disruptive technology that has been gaining space in the corporate world and capable of securely recording and storing digital financial transaction data using any type of currency. Also considering the advantages related to the practicality and decentralization of operations, standing out, mainly, for offering digital security in its operations.

Information security has become an extremely important issue in the corporate world, since it optimizes data management and traceability, especially with regard to data protection, with regard to management regarding traceability in various economic sectors. The technology protects recorded data, preventing it from being deleted or altered. Given this context, Blockchain is not just for cryptocurrencies, but the technology takes data storage and security to another level, as long as the transactions carried out by companies are done in a secure, fast, inexpensive, transparent, autonomous, and very secure and efficient way.

## References

1. Drescher D (2017) Blockchain basics, vol 276. Apress, Berkeley, CA
2. Van Rijmenam M, Ryan P (2018) Blockchain: transforming your business and our world. Routledge
3. Prusty N (2017) Building blockchain projects. Packt Publishing Ltd
4. Crosby M et al (2016) Blockchain technology: beyond bitcoin. *Appl Innov* 2(6–10):71
5. Biswas K, Vallipuram M (2016) Securing smart cities using blockchain technology. In: 2016 IEEE 18th international conference on high-performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS). IEEE
6. Zheng Z, Xie S, Dai H, Chen X, Wang H (2017) An overview of blockchain technology: architecture, consensus, and future trends. In: 2017 IEEE international congress on big data (BigData Congress). IEEE, pp 557–564
7. Khan MA, Salah K (2018) IoT security: review, blockchain solutions, and open challenges. *Future Gener Comput Syst* 82:395–411
8. Tse D et al (2017) Blockchain application in food supply information security. In: 2017 IEEE international conference on industrial engineering and engineering management (IEEM). IEEE
9. Tasatanattakool P, Techapanupreeda C (2018) Blockchain: challenges and applications. In: 2018 International conference on information networking (ICOIN). IEEE
10. Fernández-Caramés TM, Fraga-Lamas P (2018) A review on the use of blockchain for the internet of things. *IEEE Access* 6:32979–33001
11. França RP et al (2020) Intelligent applications of WSN in the world: A technological and literary background. In: *Handbook of wireless sensor networks: issues and challenges in current scenario's*. Springer, Cham, pp 13–34

12. Kosba A et al (2016) Hawk: the blockchain model of cryptography and privacy-preserving smart contracts. In: 2016 IEEE symposium on security and privacy (SP). IEEE
13. Kaushik A et al (2017) Blockchain—literature survey. In: 2017 2nd IEEE international conference on recent trends in electronics, information and communication technology (RTEICT). IEEE
14. Weber RM (2018) An Advisor's Introduction to blockchain. *J Financ Serv Professionals* 72(6)
15. Daneshgar F, Sianaki OA, Guruwacharya P (2019) Blockchain: a research framework for data security and privacy. In: Workshops of the international conference on advanced information networking and applications. Springer, Cham
16. França RP, Iano Y, Monteiro ACB, Arthur R (2020) Improvement of the transmission of information for ICT techniques through CBEDE methodology. In: Utilizing educational data mining techniques for improved learning: emerging research and opportunities. IGI Global, pp 13–34
17. Gupta S, Sadoghi M (2019) Blockchain transaction processing. 366–376
18. Zhao D (2020) Cross-blockchain transactions. In: Conference on innovative data systems research (CIDR)
19. Witchey NJ (2019) Healthcare transaction validation via blockchain, systems and methods. U.S. Patent No. 10,340,038. 2 July 2019
20. Chen L et al (2019) Blockchain-based searchable encryption for electronic health record sharing. *Future Gener Comput Syst* 95:420–429
21. Applebaum B et al (2017) Low-complexity cryptographic hash functions. In: 8th Innovations in theoretical computer science conference (ITCS 2017). Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik
22. Lu Y (2018) Blockchain and the related issues: a review of current research topics. *J Manag Anal* 5(4):231–255
23. Schmidt CG, Wagner SM (2019) Blockchain and supply chain relations: a transaction cost theory perspective. *J Purchasing Supply Manag* 25(4):100552
24. Xu X, Weber I, Staples M (2019) Architecture for blockchain applications. Springer, Heidelberg, pp 1–307
25. Huh S, Cho S, Kim S (2017) Managing IoT devices using blockchain platform. In: 2017 19th international conference on advanced communication technology (ICACT). IEEE
26. Gupta SS (2017) Blockchain. Wiley
27. Garcia P (2018) Biometrics on the blockchain. *Biometric Technol Today* 2018(5):5–7
28. Delgado-Mohatar O et al (2019) Blockchain and biometrics: a first look into opportunities and challenges. In: International congress on blockchain and applications. Springer, Cham
29. Halpin H, Piekarska M (2017) Introduction to security and privacy on the blockchain. In: 2017 IEEE european symposium on security and privacy workshops (EuroS&PW). IEEE
30. Golosova J, Romanovs A (2018) The advantages and disadvantages of the blockchain technology. In: 2018 IEEE 6th workshop on advances in information, electronic and electrical engineering (AIEEE). IEEE
31. Zhang R, Xue R, Liu L (2019) Security and privacy on blockchain. *ACM Comput Surv (CSUR)* 52(3):1–34
32. Padilha R et al (2018) Betterment proposal to multipath fading channels potential to MIMO systems. In: Brazilian technology symposium. Springer, Cham
33. Babkin AV et al (2018) Automation digitalization blockchain: trends and implementation problems. *Int J Eng Technol (UAE)* 7.3.14(14):254–260
34. Tapscott Don, Tapscott Alex (2017) How blockchain will change organizations. *MIT Sloan Manag Rev* 58(2):10
35. Tapscott A, Tapscott D (2017) How blockchain is changing finance. *Harvard Bus Rev* 1(9):2–5
36. Cahill D et al (2020) I am a blockchain too: how does the market respond to companies' interest in blockchain? *J Bank Finance* 113:105740
37. Singer PW, Friedman A (2014) Cybersecurity: what everyone needs to know. OUPUSA
38. Conti M, Somani G, Poovendran G (eds) (2018) Versatile cybersecurity. vol 72. Springer

39. Parizi RM et al (2020) Blockchain in cybersecurity realm: an overview. In: *Blockchain cybersecurity, trust and privacy*. Springer, Cham, pp 1–5
40. Attaran M, Gunasekaran A (2019) Blockchain and cybersecurity. In: *Applications of blockchain technology in business*. Springer, Cham, pp 67–69
41. De Angelis S et al (2019) Blockchain and cybersecurity: a taxonomic approach
42. De Angelis S et al (2018) Pbf vs proof-of-authority: applying the cap theorem to permissioned blockchain
43. Bach LM, Mihaljevic B, Zagar M (2018) Comparative analysis of blockchain consensus algorithms. In: *2018 41st International convention on information and communication technology, electronics and microelectronics (MIPRO)*. IEEE
44. Mishra AK et al (2018) Analytical model for sybil attack phases in internet of things. *IEEE Internet Things J* 6(1):379–387
45. Sharma P, Jindal R, Borah MD (2019) Blockchain-based integrity protection system for cloud storage. In: *2019 4th Technology innovation management and engineering science international conference (TIMES-iCON)*. IEEE
46. Iovane G et al (2019) A novel blockchain scheme combining prime numbers and iris for encrypting coding. In: *2019 IEEE international conferences on dependable, autonomic and secure computing, international conferences on pervasive intelligence and computing, international conferences on cloud and big data computing, international conferences on cyber science and technology congress (DASC/PiCom/CBDCCom/CyberSciTech)*. IEEE
47. Ulrich F (2017) Bitcoin: a moeda na era digital. LVM Editora
48. França RP et al (2020) Improved transmission of data and information in intrusion detection environments using the CBEDE methodology. In: *Handbook of research on intrusion detection systems*. IGI Global, pp 26–46
49. França RP et al (2020) Lower memory consumption for data transmission in smart cloud environments with CBEDE methodology. In: *Smart systems design, applications, and challenges*. IGI Global, pp 216–237
50. França RP et al (2020) Potential proposal to improve data transmission in healthcare systems. In: *Deep learning techniques for biomedical and health informatics*. Academic Press, pp 267–283
51. França RP et al (2019) Potential model for improvement of the data transmission in healthcare systems
52. França RP et al, A methodology for improving efficiency in data transmission in healthcare systems. In: *Internet of Things for healthcare technologies*. Springer, Singapore, pp 49–70
53. Monteiro ACB, Iano Y, França RP (2017) Detecting and counting of blood cells using watershed transform: an improved methodology. In: *Brazilian technology symposium*. Springer, Cham
54. Monteiro ACB et al (2018) A comparative study between methodologies based on the Hough transform and watershed transform on the blood cell count. *Brazilian Technology Symposium*. Springer, Cham
55. Monteiro ACB et al (2020) Development of a laboratory medical algorithm for simultaneous detection and counting of erythrocytes and leukocytes in digital images of a blood smear. In: *Deep learning techniques for biomedical and health informatics*. Academic Press, pp 165–186
56. Monteiro ACB et al (2019) Medical-Laboratory algorithm WTH-MO for segmentation of digital images of blood cells: a new methodology for making hemograms. *Int J Simul Syst Sci Technol* 20 (2019)
57. Cheng J-C et al (2018) Blockchain and smart contract for digital certificate. In: *2018 IEEE international conference on applied system invention (ICASI)*. IEEE
58. Tian F (2016) An agri-food supply chain traceability system for China based on RFID & blockchain technology. In: *2016 13th international conference on service systems and service management (ICSSSM)*. IEEE
59. Mazzei D et al (2020) A blockchain tokenizer for industrial IOT trustless applications. *Future Gener Comput Syst* 105: 432–445

60. Krisztina K, Hahn I (2017) Mobile payment analysed from the aspects of Kano model
61. Padilha RF (2018) Proposta de um método complementar de compressão de dados por meio da metodologia de eventos discretos aplicada em um baixo nível de abstração=Proposal of a complementary method of data compression by discrete event methodology applied at a low level of abstraction

# Blockchain-Based Cyber Security



Snehlata Barde

**Abstract** The term cyber security is referred to as security of information technology. Major goal of cyber security is to provide the protection of computers, networks, programs, and data and keep safe from unauthorized person and does not allow them to access or change the data and information. Cybercrime can be classified into three categories like cybercrime against individual, crime against property, and cybercrime against organization. Application development is a process that reduces human effort in doing the things manually such as ticket booking and banking. It is a new technology known as a next-generation solution to a wide variety of transactional blockchain. It is a collection of records which are called blocks, which are linked and secured using cryptography. Blockchain technology increasingly receives attention and recordkeeping problems. The core ideas behind blockchain technology emerged in the late 1980s and early 1990s by STUART HABER and W. SCOTT STORNETTA. Blockchain can be defined into four categories such as data structure, immutable, validated by distributed network and cryptography for security. There are two types of blockchain available public and private. In this chapter, we have described the problem with current system and their solution with the help of distributed system, block identifiers and different terms that is supported by blockchain technology such as smart contracts.

## 1 Introduction

Today we cannot imagine the world scenario without the computer and communication devices, network between devices increases every time and every day, Internet provide the facilities where every person can access any type of information from the net within a small part of time. It is huge storage of information and supports communications technology in order to the human race. World growth increases remarkable day to day by the use of Internet. Where the Internet is helpful in human progress, the Internet has also given rise to heinous crime like cybercrime [1].

---

S. Barde (✉)  
MSIT, MATS University Raipur (CG), Raipur, India  
e-mail: [v.snehabarde@gmail.com](mailto:v.snehabarde@gmail.com)

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2021  
R. Agrawal and N. Gupta (eds.), *Transforming Cybersecurity Solutions Using Blockchain*,  
Blockchain Technologies, [https://doi.org/10.1007/978-981-33-6858-3\\_4](https://doi.org/10.1007/978-981-33-6858-3_4)

This type of crime is technology based and done by the technocrats. That required the need for strong computer security also becomes increasingly necessary and important. The boost in the computer network system has exposed many networks to various kinds of Internet threats, and with this exposure, one can see that the need of improved network security is vital and important in every term [8].

Cyber word related to all electronic equipments such as computer and mobile and security means protection from unauthorization. Cyber security means not only to protect data and information but also to protect all electronic and network devices from attacker. We define in other way cyber security as information security and network security technology [2].

Cybercrime perpetrators are very intellectual; their purpose is to commit crime in customer as well as in public and private organization. Cybercrime is caused by the lack of some innovation of cyber security, its responsible computers, and people who operate computers. We can provide the security at different level such as [3].

(a) **Network Security**

Network security is dealt with the problems of network and computers inside network. The network security problem can be of any size dealing with external issues, problems from users inside the network, etc. [9]. Network security problems arise in issues of client server models.

(b) **Internet Security**

Internet security deals with malware and hackers. Internet is an open zone where anyone can occupy web space by creating their own Web site and put malware to place in your computer or in server.

(c) **Port scanning**

Port scanning is the technique ports on your computer or server are accessed by hackers. They keep on trying, once locate the open port, they can read access and manipulate data from computer.

(d) **Accidental Data Losses**

Accidental data loss part is applicable to networks, computers nodes in networks and standalone nodes whether connected or not with Internet [10]. A sudden crash of hard disk and network failure during transmission creates problem of data loss.

(e) **Computer Security in standalone system**

Standalone computers refer to computers that are not connected to any network (but may be connected to Internet) [11]. For standalone computers, major types of computer security are factors affecting on data. The major threat is stealthy techniques.

## 2 Classification of Cybercrime

There are different types of cyber attacks these terms used in several of contexts and it can be divided into following categories as shown in Fig. 1 [4].

### A. Cybercrime against Individual:

- E-mail spoofing: A spoofed e-mail means duplicate e-mail its look like at original masses and person thinks that it has been coming from actual source but it is not true because it has been sent from false source [12]. It is also called as e-mail forging. The main goal of attacker is to interrupt the service of the e-mail sender for which he sends e-mails repeatedly as shown in Fig. 2.
- Phishing: Phishing is a type of forgery where a cyber criminal creates same webpage to fool people through the Internet in which people enter with their user id and password and fill the personal information for accessing the account [13]. Cyber criminal uses this secrete personal information and

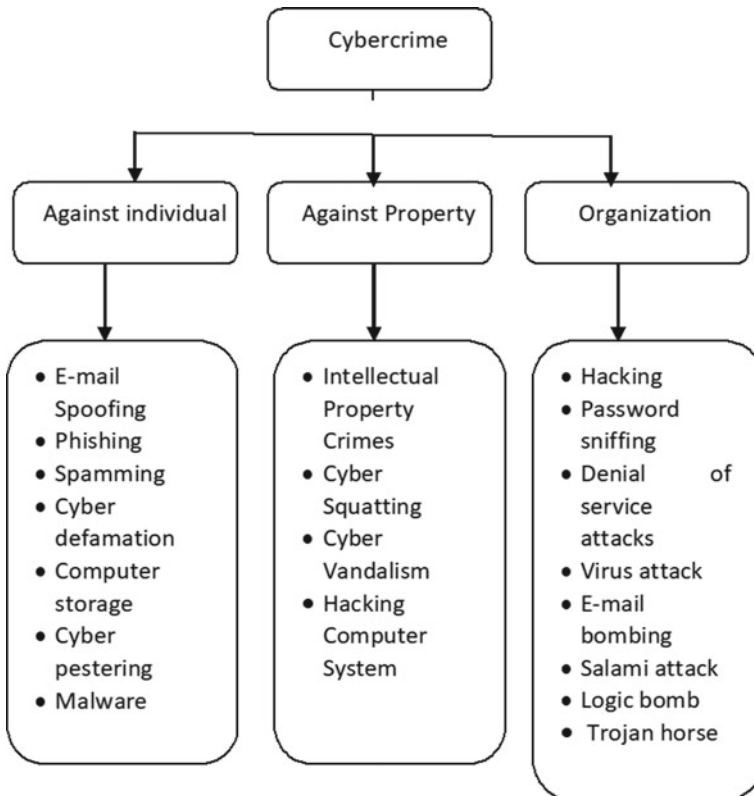
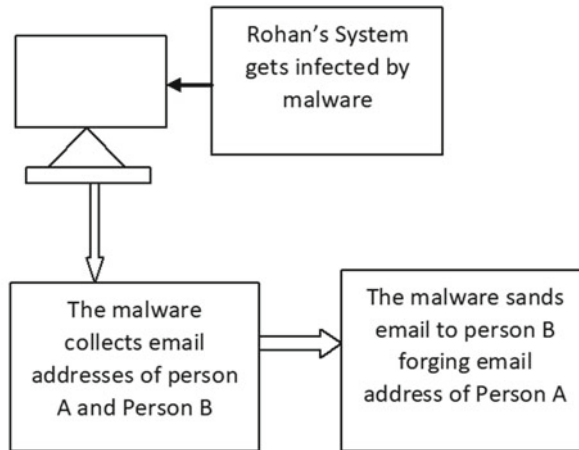


Fig. 1 Classification of cybercrime



**Fig. 2** E-mail spoofing

financial information of person in illegal way and gets the profit from them; without knowledge of customer, criminal does the forgery from his account.

- **spamming:** Spamming is the sending of multiple unsolicited e-mails or text messages, usually for marketing purposes, commercial advertising, or for any prohibited purpose (especially for the fraudulent purpose of phishing).
- **Cyber defamation:** The purpose of this crime is to damage the image of well-known person by using his mail and send the vulgar message from their account that degrade the dignity of person in society [14].
- **Cyber pestering:** Cyber pestering means harass the other person or organization through the Internet. This type of crime generally could be sexual in nature.
- **Computer sabotage:** Computer sabotage means disturbing the normal process of system by the harmful viruses and worms through the use of Internet.
- **Malware:** Malware is software whose purpose is to infect network system. It damages not only client side activities but also server side without client and server knowledge. Malware takeover all the controls of any individual system and spreads the bug from that to other system. Malware remotely controls all the network services which is used to send the viruses and spam [4].

## B. Crime against property

- **Intellectual property crimes:** Any unlawful act by which the owner is deprived completely or partially of his rights is a crime. The most common



type of crimes are software piracy, infringement of copyright, trademark, theft of computer source code, etc.

- Cyber squatting: It involves two persons claiming for the same domain name either by claiming that they had registered the name first. For example two similar names, i.e., [www.yahoo.com](http://www.yahoo.com) and [www.yahhoo.com](http://www.yahhoo.com).
- Cyber vandalism: Vandalism means damaging property of another. Thus cyber vandalism means destroying or damaging the data or information stored in computer when a network service is stopped or disrupted.
- Hacking computer system: Hacking in simple terms means an illegal intrusion into a computer system and/or network. Hacking attacks include famous social networking sites such as Facebook, Twitter, blogging platform by unauthorized access/control over the computer. Due to the hacking activity there will be loss of data as well as computer system. Also research especially indicates that those attacks were not mainly intended for financial gain too and to diminish the reputation of particular person or company [15].

### C. Cybercrime against Organization

- Hacking: It means unauthorized control/access over computer system and act of hacking completely destroys the whole data as well as computer programs.
- Password sniffing: Password sniffers are programs that monitor and record the name and password of network users as they login, at site.
- Denial-of-service attacks: DoS is an attack to shutdown a machine or to make inaccessible for intended users or imposing it for crash. DoS attacks often target web servers. Flooding and crashing are two most common DoS attacks [5]. Flood attacks when server needs too much load for buffering, causing their performance slow down and stop. Most common flood attacks are buffer overflow attacks, ICMP flood, and SYN flood. Crashing is done by bugs in the target that crashes or severely destabilizes the system from user access or by being used.
- Virus attack: A computer virus is a malware program that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be “infected.”
- E-mail bombing/mail bomb: E-mail bomb refers to sending a large no. of e-mails to the victim to crash victim’s e-mail account or server crash.
- Salami attack: These attacks are used for committing financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed, e.g., a bank employee inserts a program into bank’s servers that deducts a small amount from the account of every customer.
- Logic bomb: A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are available. For example, a programmer may hide a piece of code that starts deleting files should they ever be terminated from the company.

- Trojan horse: Trojan horse is another type of e-mail virus it creates duplicity itself; the purpose of this virus is to damage the system and get the information from the system, or harm the computer system [6]. “Trojan,” enters into system disguised as a normal, harmless file or program to trick users into downloading and installing malware. As soon as install a Trojan, it is giving cyber criminals access to the system. This allows the cyber criminal to steal data install more malware, modify files, monitor user activity, destroy data, and steal financial information.

### 3 Types of Security Attacks

There are many high-risk web application vulnerabilities such as:

- (a) SQL injection: SQL injection is a procedure of susceptibility where the attackers have right to change backend and it is possible through the SQL statements that are manipulated by the user input [7]. It occurs when the user input accepted by the web applications is directly placed into a SQL statement and does not properly clean out unsafe characters.
- (b) Cross-site scripting(XSS): Cross-site scripting (also called as XSS) is a vulnerability which allows an attacker to upload, post, or send malevolent contents such as comments, images, and messages (usually in the form of JavaScript) [6]. Since a browser cannot know whether the script should be trusted or not, it will execute the script in the user context allowing the attacker to perform unusual action like phishing, running a set of commands, or even stealing login session cookies.
- (c) Sensitive data exposure: This type of errors occurs when the application lacks the protection of the sensitive data means an application does not effectively protect sensitive data. These data can be unencrypted passwords, credit card details, database backup, etc.
- (d) Malicious file upload: It is referred to an opportunity where an attacker is uploading a file from narrow or remote resources and execute arbitrary script code in it with the privileges of the web server.
- (e) Security misconfigurations: Directory listing or directory traversal is a vulnerability that allows an attacker to access confidential directories and perform commands from outside of the web server’s root directory [8].

### 4 Blockchain

Any application development is the process which reduces human effort in doing the things manually such as ticket booking and banking. According to Satoshi Nakamoto “A blockchain is a collection of records which is continuously growing; these records are called blocks, that are linked together and used cryptography for



Fig. 3 A Block

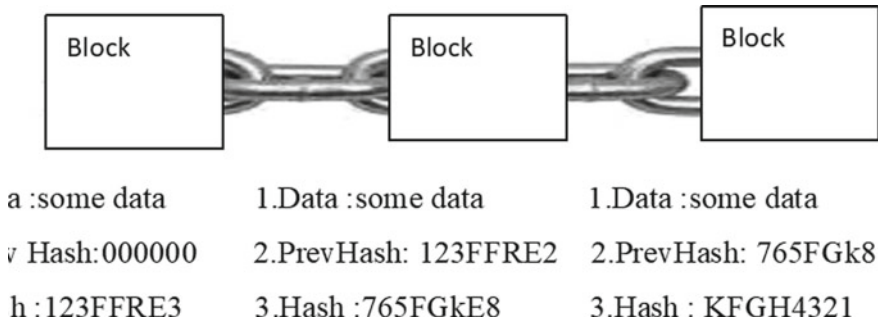


Fig. 4 Blockchain

security purpose.” Blockchain technologies offer a solution of huge variety of transaction in future and manage the problem of record storage for a next generation. The basic dream behind to develop a blockchain technology between 1980s and 1990s by the STUART HABER and W. SCOTT STORNETTA. Blockchain has collection of blocks; Fig. 3 shows the block that has three values data, pre-hash value and hash value and Fig. 4 shows the diagram of blockchain [8].

### 4.1 Hash Function

A cryptographic hash function takes an input (or message) and returns a fixed size string of bytes. The string is called hash value or checksum.

$$F_{\text{hash}}(\text{Message}) = \text{Output}_{\text{fixed length}}$$

{Public key}= {Receipient address}  
 {Private key}= {Receipient password}

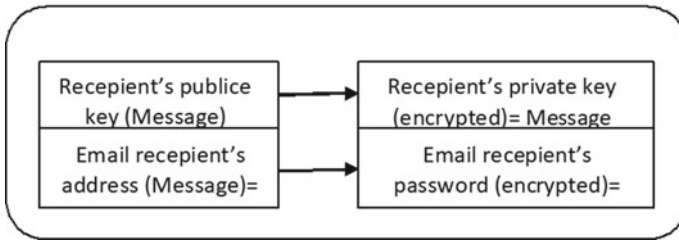


Fig. 5 Message transmission

### 4.2 Ledger

A ledger is a record-keeping book that stores all the transactions of an organization. Once the transaction is verified it is stored in a shared ledger across the network unconfirmed transaction will be store in main pool area and from there miner will pick and create the block in blockchain for the transaction.

### 4.3 Cryptography

In cryptography, original message before being transformed is called plain text keys used in cryptography are private and public key in asymmetric-key cryptography work on two keys one public and second private. They have a special relationship to each other public key is used for encryption, it is shared on the network and derived from private key while private key is used for decryption, it is not shared on network and not derived from public key shown in Fig. 5.

### 4.4 Digital Signature

Sender must require authenticity before sending his information means message. Sender's address plays a role of public key and private key is sender's password defined in Fig. 6.

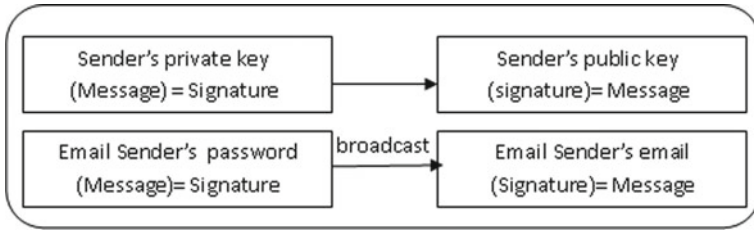


Fig. 6 Authenticity of transmission (digital signature)

## 5 Block Structure

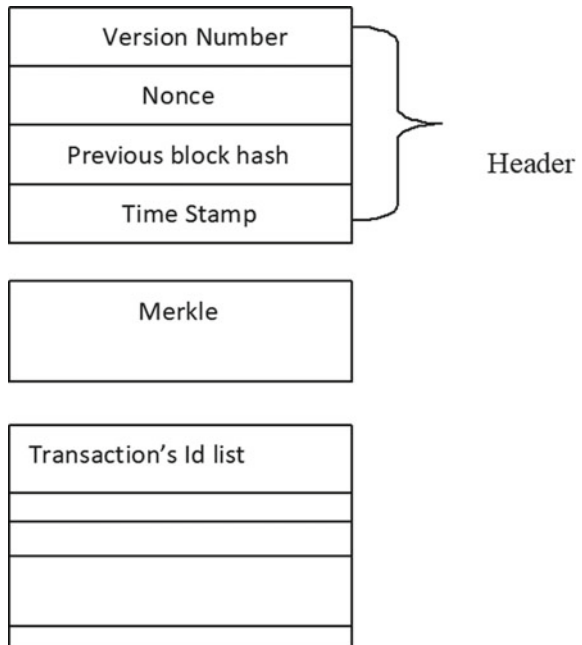
Blockchain blocks are shown in Fig. 7 which is divided into three parts.

Header: Contains version info, nonce, previous block id, and time stamp

Merkle: A hash built from a block's transaction identifiers.

List of record's: Identification hashes that were included into the block's Merkle tree

Fig. 7 Block structure



## 5.1 Characteristics of Blockchain

Blockchain is a new word we are listing nowadays everywhere frequently, many people correlate the term bitcoin and blockchain vice versa. But bitcoin is a digital currency which is used in blockchain technology [7]. Blockchain has data structure, immutable, validated by distributed network and cryptography for security characteristics.

- Data structure: Fundamental unit is a block consist of a header, transaction, and market root structure for every block is consistent each block maintains the reference to the parent block
- Immutable: Data once written to the blockchain cannot be changed. If wrong data has been written to the chain, it will exist on chain and another transaction is needed to correct the state maintaining audit trail of wrong data.
- Validated by distributed network: The nodes in the distributed network individually validate the data. The data is only written to blockchain once the network reaches an agreement or consensus.
- Cryptography for security: Hashing is used to ensure data is not tempered with asymmetric public key infrastructure is used to ensure transaction authenticity and validity.

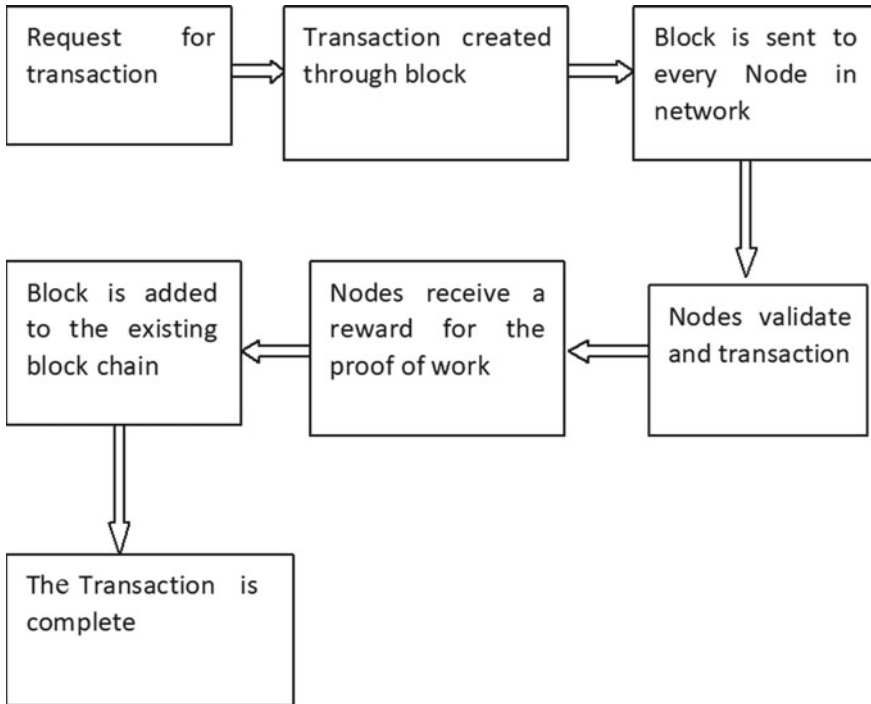
## 5.2 Types of Blockchain

There are three types of blockchain public, private, and consortium and Table 1 indicates feature differences of public and private blockchain [5].

- Public: Public blockchains are a collection of ledgers which is able to be seen by everyone that is available on the Internet and provide the facilities to anyone that can add a number of block into the blockchain for transactions and verify the block. Bitcoin, Ethereum, and Factom are an example of public blockchain [6].
- Private: All permissions are kept centralized to an organization private blockchain allow only specific people in the organization to verify and add transaction blocks but everyone on the Internet is generally allowed to view.

**Table 1** Difference between public blockchain and private blockchain

Features	Public	Private
Access	Open read/write access to database	Permission read and/or write access to database
Speed	Slower	Faster
Security	Proof of work/proof of stake	Pre-approved participants
Identity	Anonymous/pseudonymous	Known identities
Asset	Native assets	Any asset



**Fig. 8** Work process of blockchain

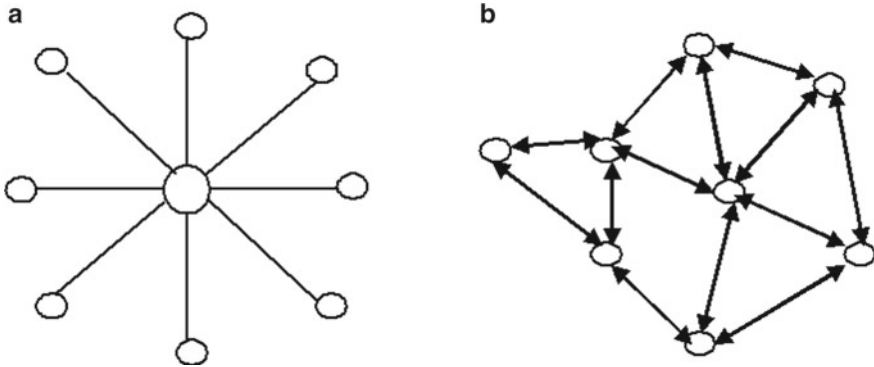
- Consortium: A collection of nodes that is used to write the data or block which is controlled by the members of consortium. Example: Ripple, R3, and hyperledger1.0.

### 5.3 *Process of Blockchain*

Blockchain completes their work in the following steps shown in Fig. 8.

### 5.4 *Problems with the Current System*

- Customer has to pay fees when he want to transfer a money from the banks and other parties;
- The transaction costs is increased by the mediator;
- Transaction is limited for the minimum size;
- Financial process of exchange is very slow. It takes few days to complete the services due to low cost wire;



**Fig. 9** **a** Centralized network, **b** distributed network

- System does not provide the fairness and transparency.
- Central authority over use the power and control to create money as per their own choice.

## 5.5 *Distributed System*

Distributed system provides the facility where computers create a network between them and arrange the large amount of data as a record of book keeping through the Internet. It is an open system not hold the command of single party but available in one ledger that is distributed transversely the network and give the solution of problems with current system. [5]

A collection of two or more than two nodes in a system achieves the target of same output by the coordination of between them. A role of node as an identity processing entity is defined in a distributed system. All nodes have a capability to send and receive the messages from each other. The sender and receiver see the distributed system in terms of a single logical model; Fig. 9 shows centralized network and distributed network.

## 5.6 *Block Identifiers*

There are two identifiers block header hash and block height shown in Table 2.



**Table 2** Block identifiers

Block header hash	Block height
The primary identifier of a block is its cryptographic hash	It is the position of the block in the blockchain
A digital fingerprint made by hashing the block header twice resulting 32-byte hash	The first ever block created is at block height zero
The block hash identifies a block uniquely	Each block added on the top has one position higher in the blockchain
The block hash not included inside the block's data structure	It is also not a part of the block's data structure

### 5.7 Blockchain Technologies

(a) **Smart contracts**

An agreement or bound between two people or organization is known as contract shown in Fig. 10. Smart contract is a small computer program given by Nick Szabo in 1994. Smart contract program developed using solidity which is a programming language the syntax of solidity language is similar to the JavaScript [6].

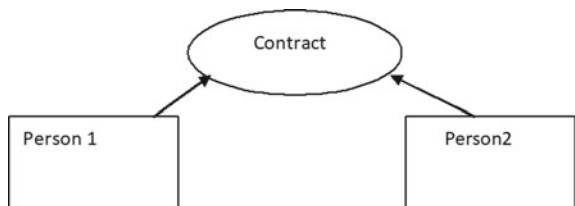
Smart contract executed the terms of contract and behave like transaction protocol roll of smart contract in blockchain as a self operating program that execute automatically when all specific conditions are met.

An option contract in a blockchain is written in the form of code between parties where they are involved individually and public ledger is used to write the contract. Date of termination and smack of price is treated as triggering event hit and the contract automatically executed itself when the code is generated [3]. Regulators can the blockchain to understand the activity in the market while maintaining the privacy of individual actor's position.

(b) **Ether**

The value token of the Ethereum blockchain is termed as Ether. It is remarked as crypto means secure currency and used in ETH, the Ethereum get charges on the exchange services when computational and transaction services would be performed. A contract is executed every time and GAS is used as a token in Ethereum.

**Fig. 10** Contract between two people



- **GAS:** The requirement of GAS in an Ethereum blockchain to be compensated for performance of any operation. A few amount of Ether has been charging as a fee of transaction and is directly deducted from the account of originator who had the transaction, and miners include fee that is paid for transaction. The more about fee, the miners pick up this transaction detail in future in the block [8]. Providing too little gas may result in the transaction failure.
- **Ethereum Virtual Machine:** Ethereum virtual machine is the engine in which transaction code gets executed, it enables the development of thousands of different applications at one platform. Contracts are written in a smart contract-specific programming languages which are later compiled into “bytecode,” which could be read and executed by EVM. All the nodes execute this contract using their EVMs [7].
- **Solidity:** The solidity source code is passed to the solidity compiler and the compile returns the EVM bytecode which is deployed to the Ethereum blockchain and to the contract Abstract Binary Interface (ABI). There are many solidity compilers available such as: remix browser-based compiler, command line solc compiler.

ABI is list of contract’s function and arguments and it is in JSON format. It known at compile time generated from source code through compilation. If we do not have the source code we cannot generate the contract ABI than only from the bytecode using reverse engineering. Anyone that wants to interact with the contract must have access to the contract ABI.

ABI is defined as the procedure of calling a functions within the contract and publicly access data in a bytecode from the contract. It is saved on the blockchain and cannot be encrypted because it must be run by every Ethereum node;

Opcodes are the human readable instructions of the program. It can be easily obtained from bytecode. There are tools like porosity that can reverse engineer the bytecode to source code. Contract source code does not have to be public.

Solidity is a high-level, statically-typed smart contract programming language and is similar to JavaScript, solc is the solidity command line compiler. Solidity is case-sensitive every line must end with a semicolon it uses curly braces { } for delimiting the blocks of code most of the control structures are available: if, else, while, for, break, continue, return [9].

## References

1. Sarmah A (2017) A brief study on cyber crime and cyber law’s of India. *Int Res J Eng Technol (IRJET)* 4(6):1633–1641
2. Dashora K (2011) Cyber crime in the society: problems and preventions. *J Altern Perspect Soc Sci* 3(1):240–259
3. Barde S, Tikariha N (2020) Cyber crime problems and prevention effect on society. *J Inf Comput Sci* 13(1):29–36
4. Barde S, Tikariha N (2020) Study on Cyber Laws of India. *Int J Res Appl Sci Eng Technol* 8(6):385–389

5. Melanie S (2015) Blockchain: blueprint for a new economy. 'O'Reilly Media, Inc
6. Marco J, Lakhani K (2017) The truth about blockchain. *Harvard Bus Rev* 95(1):118–127
7. Michael C et al (2016) Blockchain technology: Beyond bitcoin. *Applied. Innovation* 2:6–19
8. Aste T, Tasca P, Di Matteo T (2017) Blockchain technologies: the foreseeable impact on society and industry. *Computer* 50(9):18–28
9. Zheng Z, Xie S, Dai H, Chen X, Wang H (2017) An overview of blockchain technology: architecture, consensus, and future trends. In: 2017 IEEE international congress on data (bigdata congress), pp 557–564
10. Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system. [Www.Bitcoin.Org](http://www.Bitcoin.Org), (Online). Available: <https://bitcoin.org/bitcoin.pdf>
11. Wood G (2014) Ethereum: a secure decentralized generalized transaction ledger yellow paper. Ethereum Project Yellow Pap 1–32
12. Buterin V (2014) A next-generation smart contract and decentralized application platform. Ethereum, (Online). Available: <http://buyxpr.com/build/pdfs/EthereumWhitePaper.pdf>
13. Androulaki E et al (2018) Hyperledger fabric: a distributed operating system for permissioned blockchains. In: Proceedings of the thirteenth eurosys conference, pp 30:1–30:15
14. Kan L, Wei Y, Muhammad AH, Siyuan W, Linchao G, Kai H (2018) A multiple blockchains architecture on inter-blockchain communication. In: 2018 IEEE international conference on software quality, reliability and security companion (QRS-C), pp 139–145
15. Miller D (2018) Blockchain and the internet of things in the industrial sector. *IT Prof* 20(3):15–18

# Secured Storage and Verification of Documents Using Blockchain Technology



Soma Prathibha , T. R. Sona , and J. Krishna Priya 

**Abstract** In today's world, producing fake documents is becoming more common. As the fake ones accurately look like the originals, it is impractical for a common man to identify the real and the duplicate one. To verify the documents, it is required to seek vast data. Personal documents are mandatory to be shown in every organization and handling it manually may damage the documents as they exist only once. They may also get lost in the mail. Fake documentation has been a current issue in both public and private sectors where all the verification processes have to be done manually. The verification method is complicated. This downside may be solved by storing the digital certificates in a blockchain. This technology is used for a selected task of storing a digital signature of assets that prove their validity. In our work, we tend to solve the problem of verifying the validity of digital assets such as a birth certificate, academic certificates, housing documents and soon by creating a digital fingerprint that would convert the uploaded file into a hash code by using the hash function. With the help of a digital fingerprint, a digital signature is created using JSON web tokens. Both the finger print and signature are stored in the blockchain and the document shall be shared through any file sharing platform. For the verification process, the digital fingerprint is checked and the request reaches the blockchain. The signature for that particular fingerprint is checked against the public and private keys stored in the block. For authorization of the institution that generates the document, an SSL certificate shall be issued and can be checked for legitimation. The existing system does not guarantee the records and depends on third-party agencies.

**Keywords** Cryptography · Hash function · Hashing tool · Extended validation · RSA keys · Jason web tokens · Blockchain

---

S. Prathibha (✉) · T. R. Sona · J. Krishna Priya  
Sri Sairam Engineering College, Chennai 600044, India  
e-mail: [prathibha.it@sairam.edu.in](mailto:prathibha.it@sairam.edu.in)

T. R. Sona  
e-mail: [trsona1998@gmail.com](mailto:trsona1998@gmail.com)

J. Krishna Priya  
e-mail: [krishnapriyajaganathan28@gmail.com](mailto:krishnapriyajaganathan28@gmail.com)

## 1 Introduction

Blockchain is a buzz word in recent years. Blockchain is a supplementing list of records, referred to as blocks that are connected using cryptography and are made up of digital pieces of information. One block will readily store up to one MB of information. Once a block stores new information, it is superimposed to the blockchain. Blockchain consists of multiple blocks that are connected. Once a new block is superimposed, it becomes publicly visible on the market for anyone to look at and it is additionally terribly troublesome to alter the contents of the block that has been already stored. That is because every block has its own hash value and the hash value of the previous block. If that specific information is altered, the hash code also changes. The standard application of blockchain is bitcoin and various sectors such as health care, food supply chain management system, information sharing, real estate, banking, and smart appliances. Blockchain helps us in achieving the security of documents and eliminates fraudulent activities. In recent days, verification of documents is very much essential to avoid forgery. Using blockchain technology will even reduce the cost and increase efficiency.

In the proposed work, by using the blockchain technology hash value will be generated for every document. Only if the hash value matches with the document, it will be considered as an original one. For all enrolments in government institutions and organizations, original documents are being required for verification. Forging certificates commonly takes place. Even there may be a chance of documents getting broken while handling. Therefore, if the certificate gets digitalized and verified through blockchain technology, forging will be impossible. The original documents that are to be given must be validated with the organization's verification method. The verification of certificates has to be done with less time consumption without manual interruption. No third party shall be concerned about accessing or modifying the information. The existing system stores only the educational information, marksheets, and course completion certificates. In the proposed system, the certificates and documents are additionally validated and verified.

## 2 Evolution of Blockchain

In 1991, Stuart Harber and W Scott Stornetta for the first time described the cryptographically secured chain of blocks and in 1998, Nick Szabo, a computer scientist worked on a "bit gold", which is a decentralized digital currency. Stefan Konst in 2000 published his work on the theory of cryptographically secured chains and its idea of implementation. Satoshi Nakamoto and the developers under him released the model for a blockchain. Nakamoto in 2009 implemented the first blockchain as a public ledger for transactions by using bitcoin. The first generation of blocks was purely based on cryptocurrencies and secured financial transactions using blockchain technology. Because of its immutable data storage and secured phenomenon made

blockchain as public. “Anyone can view the data but no one can alter the data”. The second generation has introduced a new key concept “Smart contracts”, it made blockchain impossible to tamper or hack it. Ethereum blockchain succeeded to implement smart contracts. The third generation moved on to decentralized applications (DApps). Storage and communication have been decentralized. Most of the applications run their back-end code on the decentralized peer-to-peer network, a blockchain. The application can have front-end code and user interfaces in any language and can also call them to the back-end code. The Dapp includes both the frontend and the smart contracts. The fourth-generation solutions and approaches of the blockchain had made them solve other problems other than bitcoin. After releasing the usage of blockchain, it moved from bitcoin to various sectors especially Industry 4.0. Industry demands a high degree of trust and privacy protection. Industry 4.0 includes automation, enterprise resource planning and integration of systems health care, supply chain management, financial transaction, IoT applications, condition-based payment and asset management are a few examples of the application of blockchain.

### **3 Literature Survey**

An enumerated study on the applications of blockchain technology, the algorithm used, merits and demerits in various domains has been analyzed and discussed in this section.

#### **3.1 Banking**

The assorted works of blockchain in the field of banking are discussed as follows:

- In [1], a credit analysis framework for economical financial systems using blockchain has been projected by the authors for gathering information, analyzing the eligibility and scheming the customer’s credit score.
- The authors in [2] have used an epidemic algorithmic program in blockchain-based financial service which offers the potential for the creation of new transaction platforms.
- The authors have proposed a blockchain-based framework in [3] for automating the cheque clearance operations which are handled by blockchain in financial establishments.

#### **3.2 Supply Chain Management System**

The various works of blockchain technology in the supply chain field are discussed as follows:

- In [4], a supply chain quality management frame using blockchain technology has been proposed by the author to overcome information asymmetry, costs and limitations of supply chain members.
- The authors in [5] have examined the desegregation effects of blockchain and resource designing systems.
- In [6], the authors have recommended integrating IoT and blockchain technologies which improve the potential and digitalize the availability supply chain and asset management.
- In [7], the power of a blockchain-based supply chain has been delineated by the authors to integrate the supply chain design architecture.
- The authors have projected in [8] to explore future implications on managerial practices and educational research.

### ***3.3 Food Safety and Food Chain Management***

The assorted works of blockchain in food chain management system are discussed as follows:

- In [9], food safety primarily based on supply chain traceability system has been proposed by the authors to provide a platform for providing information to all the supply chain members.
- In [10], the authors proposed a systematic literature network analysis for reviewing blockchain technology to enhance the performance of the agri-food value chain.
- In [11], the authors projected a blockchain algorithm that incorporates a high potential.

### ***3.4 Healthcare System***

The works of blockchain technology in the field of the healthcare system are discussed as follows:

- The authors propose a blockchain network in [12] with users having permission and valid patients and medical officials.
- The authors propose a novel prototype medrec in [13] that provides patients blockchain-based decentralized and immutable logs for sharing their health data.
- Authors proposed in [14], storage of health care-related data using decentralized blockchain networks. The applications of blockchain in various domains are represented in Fig. 1.

With the results of the detailed study, we have found that blockchain technology has already been implemented in various sectors but its need in document and certificate verification has not yet been implemented or discussed in detail.

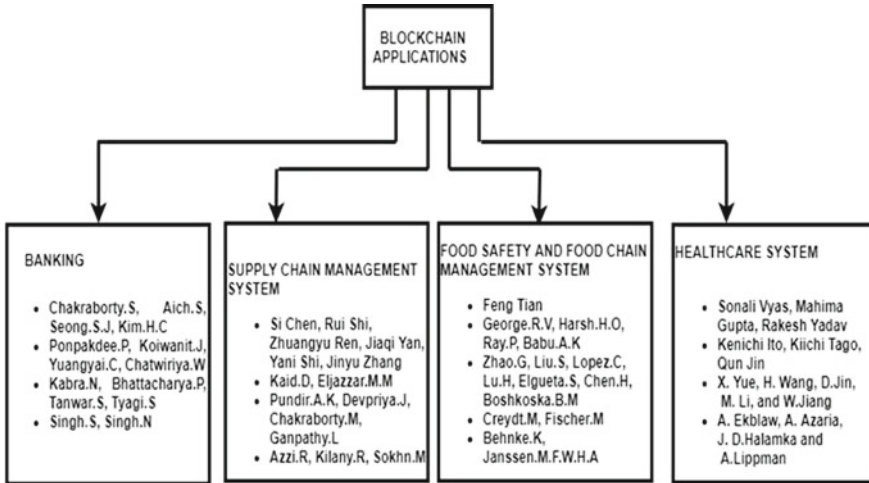


Fig. 1 Applications of blockchain technology

### 4 Existing System

A study on the existing system of verifying documents using blockchain technology has been interpreted in Fig. 2. The existing system only acts as a container for storing the documents but it does not verify whether it is an original or a duplicated one.

### 5 Proposed System

The proposed solution deals with storing the digital document that has been licensed by an institution on the blockchain. The legitimacy of a digital asset can be verified by evaluating it using the proof that is provided. Hence, the solution is such that blockchain provides an immutable storage container for those proofs. Initially, the document is digitized by scanning its QR code. After the digital asset has been created, the signature which is the digital proof is stored in the blockchain. The digital asset is transferred through an email or sharing the file. The signature that gets stored in the blockchain is validated and the institution which issues the asset is investigated. Even the person who is concerned about generating the fingerprint will not know how the key is generated.

The solution that is proposed includes these steps:

- Creation

The digit asset is created and the digital proof (signature) is held on to the blockchain.



PAPER TITLE	SCOPE	PRIVATE/ PUBLIC BLOCKCHAIN	ALGORITHM	LIMITATIONS
Secure E- Documents Storage using blockchain	Authors propose a mechanism which stores the document in a blockchain such that it cannot be tampered, mutable and provides availability to the documents .	Public blockchain	SHA-256	This system does not know to whom the document belongs and does not verify the document whether it is valid or invalid.
Tamper-Proof Certificate Management System	This system proposes a secure anti-forge mechanism using <b>hyperledger</b> that generates the document and encrypts it using asymmetric encryption.	Private blockchain	IPFS protocol	This system does not have a centralized system for generating documents and can only store the document safely.
SPROOF: A platform for issuing and verifying documents in a public blockchain	The authors propose a platform for issuance, management and verification of digital documents in a blockchain. The platform can be accessed by anyone.	Public blockchain	SPROOF protocol	This paper focuses on the issuance and verification of documents but these are only the proposal of the protocol and not the prototype.
Blockchain based framework for educational certificates verification	The authors propose a framework for verifying educational certificates focusing on authentication, authorization based on <b>hyperledger fabric</b> .	Private blockchain	SHA-256	This framework is only a proposed system and does not have a single platform for performing every steps.

Fig. 2 Existing system

- Transmission

The digital asset is transmitted or shared (email, file sharing, etc.)

- Validation

The digital asset is validated using the signature that gets stored on the blockchain and authorization of the establishment that issued the asset.

## 6 System Architecture

The system architecture of the proposed system is shown in Fig. 3.

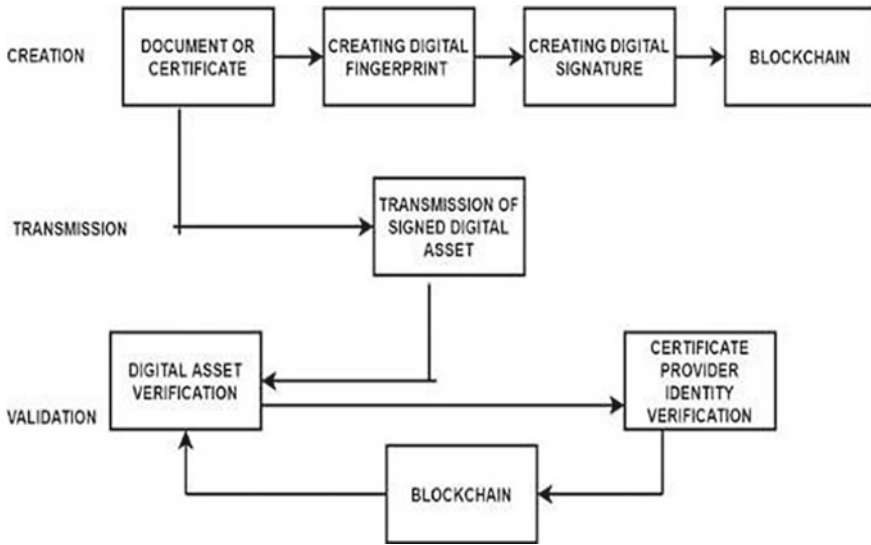


Fig. 3 System architecture

### 6.1 Conceptual Diagram

From the issuer’s perspective, the issuing organization has to be provided an SSL certificate for legitimation. The institution has to generate a digital fingerprint using a hash algorithm for that document. By keeping the fingerprint as an input, a digital signature has to be generated using JSON web tokens. Both the fingerprint and the signature are put into the blockchain which is explained in Fig. 4.

The user is someone who submits his/her digital document. The digital fingerprint for that document will be fetched and will be checked against the signature which has been inserted into the block by the issuer. Only when it matches the key pair, the document is considered as a valid one which is explained in Fig. 5.

The algorithm of the project is given in Fig. 6.

### 6.2 System Design

The system design explains the various steps involved in developing the proposed system. Data-flow diagram (DFD) explains the flow of information between various stages of the process. Figures 7, 8, and 9 represent the Level 0, Level 1, and Level 2 flow diagrams of the proposed secured document verification system.

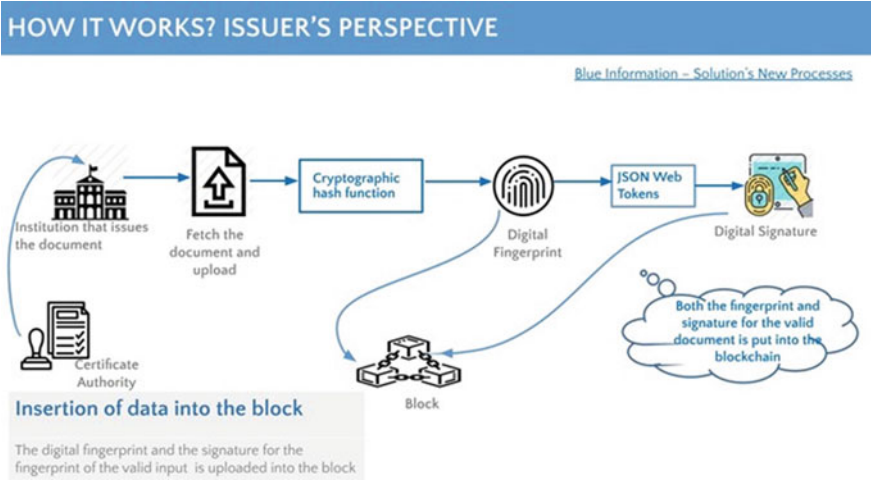


Fig. 4 Conceptual diagram—issuer's view

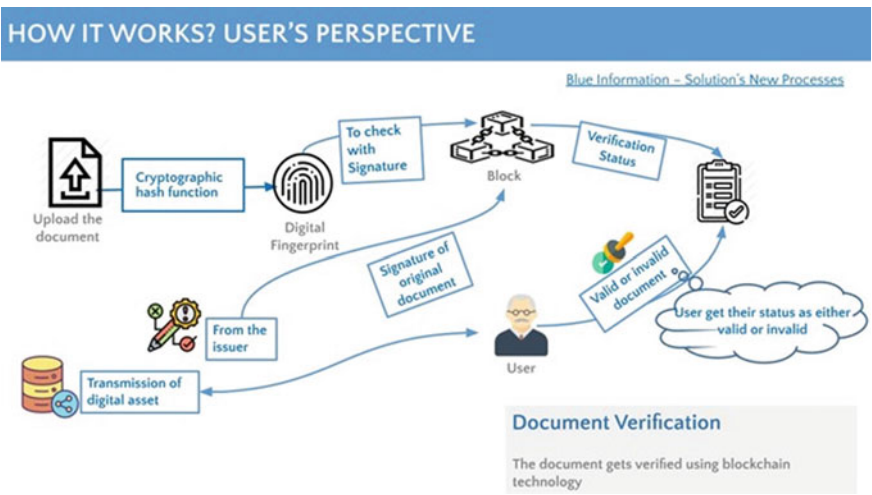


Fig. 5 Conceptual diagram—user's view

## 7 Module Description

The proposed system consists of six modules each of which enables enacting a proper interface. The modules are as follows:

```

Algorithm 1
AssignRoles:
function Define Roles (New Role, New Account)
  add new role and account in
  roles mapping
end function
AddData:
function Add User Record(contains variables to add data)
  if (institution==SSLcertificate) then
    add data to particular user's record
  else
    Abort session
  end if
end function
RetrieveData:
function View User Record
  if (msg.user==password | dataowner) then
    if privatekey==true then
      retrieve document from the database(id) return
      (document) to the account that requested the
      retrieve operation
    else
      Abort session
    end if
  end if
end function
UpdateData:
function Update User Record (contains variables
  to update data)
  if (msg.sender==dataowner) then
    if (id==ownerid&&name==dataowner) then
      update data to particular user's record
      return success
    else
      return fail
    end if
  end if
  Abort session
end if
end function
InvalidData:
function Invalid Document Record
  if (msg.sender==user) then
    if (id!=privatekey) then
      indicate invalid user record
      return fail
    else
      return success
    end if
  else
    Abort session
  end if
end function
    
```

Fig. 6 Algorithm

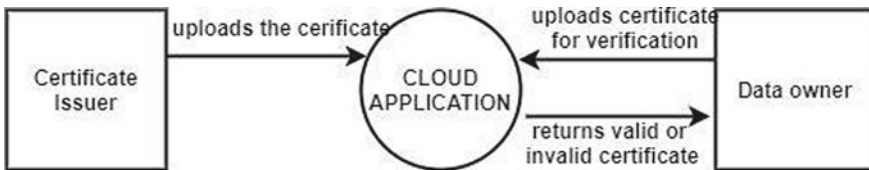


Fig. 7 Level 0 data flow diagram

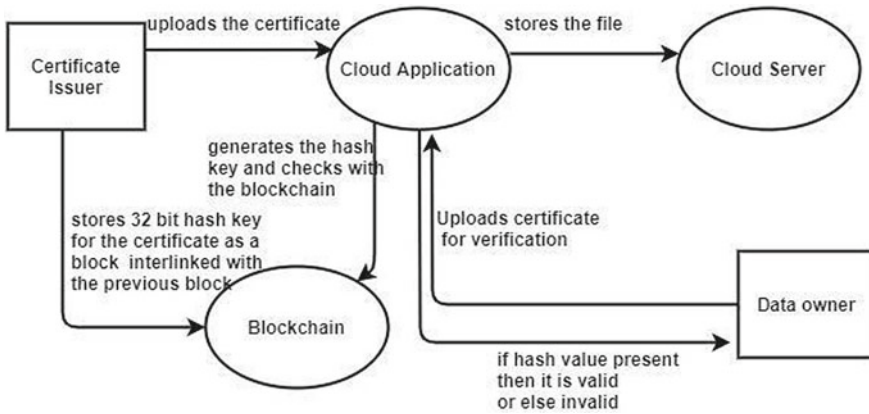


Fig. 8 Level 1 data flow diagram

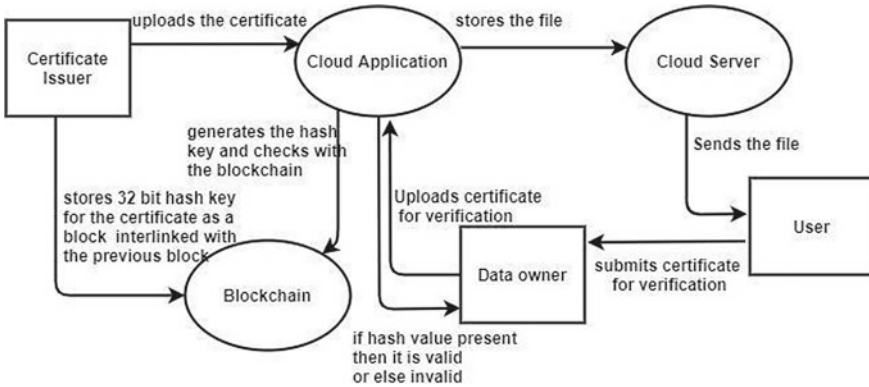


Fig. 9 Level 2 data flow diagram

• **Creating Digital fingerprint**

The certificate to be verified is made digital by converting it into a file of a word, excel, PDF, or image. Using the cryptographic hash functions, the fingerprint of digital assets is created. These functions produce a string of letters and characters as an input which is created by taking the file of virtually any size as an input parameter. A digital fingerprint which is 32-character long is displayed when a file is getting verified.

• **Creating Signature**

The public-private key pairs are passed as an input parameter to realize the digital fingerprint. The digital signatures are created using JSON web tokens as this process is straight forward. This token is created using an online tool referred to as jwt.io.

- **Committing Fingerprint and Signature to blockchain**

The digital fingerprint and also the JSON token are both uploaded to the blockchain. The information in the digital asset and the signature is getting stored in the blockchain. The data contained in the digital asset is only stored in the blockchain.

- **Transmission of Digital asset**

The digital asset can be sent to any party using email or any other files having platforms. If the digital asset gets modified, it would no longer match with the signature thereby the file would be considered as a fake done. It is not necessary to share the digital fingerprint, only the asset is to be shared.

- **Verification of Digital asset**

A digital fingerprint is created to verify if the digital asset is authenticated using the hashing tool from the received file. A request to the blockchain is raised to retrieve the signature for the corresponding fingerprint. Finally, the RSA public key corresponding to its private key is applied for signature verification confirmation and digital asset validation.

- **Identity Verification of the Certificate provider**

The organization that creates the digital asset has to be verified for legitimation. This process of validation is referred to as extended validation where the certificate authority conducts a complete verification of the organization. This verification is done by verifying the legal existence of the entity and the matching of the official records with the identity of the entity. The URL which is specified in the JWT has to be verified with the SSL certificate issued by the organization.

## **8 Result Discussion**

In this section, we discuss the hardware and software used for implementing and validating the proposed system which is given in Fig. 10.

The verification is implemented using the blockchain. The digital asset has the visual information of the address of the blockchain that is generated by the organization or the establishment (i.e., the QR code) shown in the document. The Jason web token and its signature are superimposed to the contract of the blockchain for storage. As soon as the code is generated from the digital asset, an own contract is deployed by the institution over the blockchain. This serves as an unalterable container for all the signatures of the digital assets of the organization. Whenever the deployment of code occurs on the blockchain, a contract is being created at a 42-character distinctive long address. The extended validation SSL provides the highest level of trust within the organization's legitimation.

S.No	Hardware/Software Requirements	
<b>Hardware</b>		
1	Processor	Intel i5
2	RAM	4GB
3	Hard Disk	260GB
<b>Software</b>		
4	Operating System	Windows 7/8/10
5	Scripting Lang	Javascript
6	Front End	HTML,J2EE
7	Database	MySQL
8	Contract Language	Solidity

Fig. 10 Hardware and software details used for the experiment

The document that is uploaded by the user is stored as a block. Each block is linked with the hash value of the previous block that gets stored in the present block. Thus, it forms a chain-like structure and hence the name, blockchain. The process of extracting data from the block and verifying is called the process of mining. It is a process of verifying and validating transactions by grinding through an enormous cryptographic search. The data which is stored in the block is in the form of hash code. They contain a mixed set of letters and numbers. These values are used to index a fixed-size table which is known as a hash table.

The registration of the organization who uploads the document and a user who already has a login needs to enter his username and password is given in Fig. 11.

The profile of the user and the field to upload the file are shown in Figs. 12 and 13.

DATA OWNER REGISTRATION

Your Server	<input type="text" value="CSP3"/>
Name	<input type="text" value="yoga"/>
E - Mail ID	<input type="text" value="yoga@gmail.com"/>
Password	<input type="password" value="****"/>
Your Credit Card Number	<input type="text" value="0987654321342589"/>
<input type="button" value="CLEAR ALL"/>	<input type="button" value="CREATE ACCOUNT"/>

DATA OWNER LOGIN

E - Mail ID	<input type="text" value="yoga@gmail.com"/>
Password	<input type="password" value="****"/>
<input type="button" value="RESET ALL"/>	<input type="button" value="LOGIN"/>

Fig. 11 Registration page

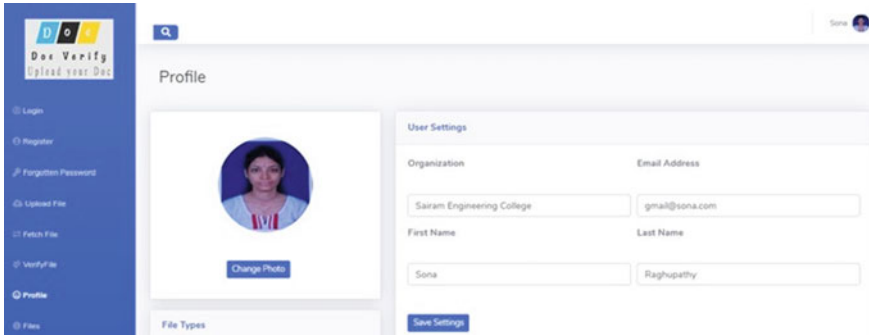


Fig. 12 User profile

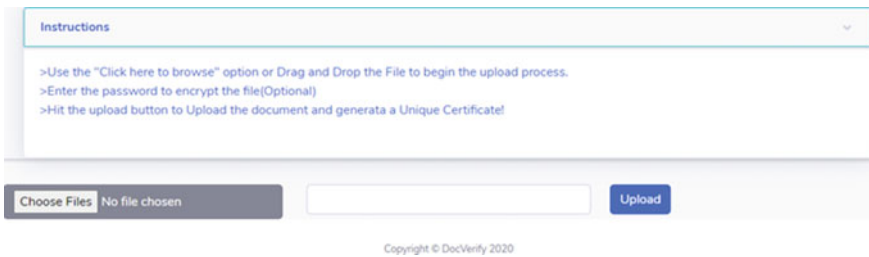


Fig. 13 Document uploading page

If an already uploaded document gets uploaded again, deduplication will be identified as shown in Fig. 14.

If a user wants to verify his file, a request will be sent and the verified and the non-verified status shall be seen which is shown in Fig. 15.

The status of the files which are uploaded can be viewed by the data owner in Fig. 16.

The digital signature of the document will be visible to the signed user which is shown in Fig. 17.

If the data owner validates the document, the public key can be sent to the user as shown in Fig. 18.

Once the document is unique, the public key will be sent to the user through the mail for viewing his file and he can also download which is displayed in Fig. 19.

The document which is uploaded once cannot be changed as it is connected to a chain of blocks as shown in Fig. 20.

The extraction of data from the block is shown in Fig. 21.

The digital signature of an uploaded document is shown in Fig. 22.

An example of the generation of public and private keys is shown in Fig. 23.



sample.txt File is Already Exists With 100.0% Matching

---

**Upload New File**    **Verified Files**    **Not Verified Files**

**UPLOAD NEW FILE**

File Type	Select File Type
File	Browse... No file selected.
Encryption Key1	dmoSAEuyN
Encryption Key2	S1NNJFG8I
<b>UPLOAD FILE</b>	

**Fig. 14** Matching status

**File Info**

Show 10

Search

Name	Hash	Date	Size(MB)
EduSign.pdf	58c14cbf02c452b2a13f4cc99ba3b60617207575dacee3d81606f644fab9a3ea	2020-01-27	1.7
EduSign Class Diagram.png	d622dc6cfa004f92227ab27bf13c0e85255c1ae41fff1f79d11123e3d0d1772f	2020-01-27	1.1
upload.json	89f491141de603cfb69c57f5936702a5b252c9e0a5f9d350d5412d598adabe75	2020-01-26	0.5
trial.json	2d627a60af9c4c78e211a5470280a2aac6028290ef35af231f317314f2485a84	2020-01-26	41

**Fig. 15** File verification process

### 8.1 Evaluation

The number of transactions per second is analyzed and interpreted through Apache JMeter. The throughput of the proposed framework is given in Fig. 24.

The delay in the system which is called latency is noted and analyzed using Apache JMeter. The latency of the proposed work is shown in Fig. 25.



Fig. 16 Status of files

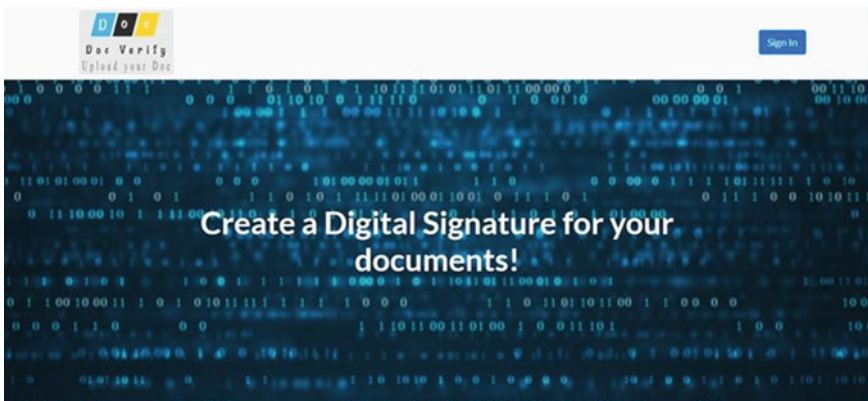


Fig. 17 Digital signature

## 9 Conclusion and Future Work

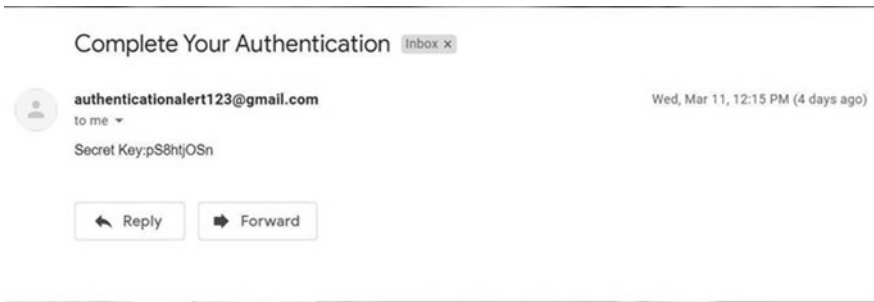
The intrinsic purpose of any technology is to improve the quality of living and ease of work. Blockchain is a large public ledger where the same data is stored and saved in

<

User name : 7  
Crop : code proof of work.txt  
mail Id : krishnapriyajaganathan28@gmail.com  
Send Key :

---

**Fig. 18** Key transmission



**Fig. 19** Public key

every node of the network. Blockchain ensures security, confidentiality, and validity. Forgery of documents shall be eradicated using this transparent system.

The future enhancements involve adding additional features such as time stamping of signatures and establishing an interface for signed digital asset verification. JSON web tokens can be replaced with the digital fingerprints for optimized storage. The URL can be stored within the blockchain contract and a standard can be established for verification using the interface base contract.

```

OUTPUT  TERMINAL  DEBUG CONSOLE  PROBLEMS

Microsoft Windows [Version 10.0.18362.657]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\saisi\Documents\SavjeeCoin> node example.js
{
  "chain": [
    {
      "index": 0,
      "timestamp": "01/01/2017",
      "data": "Genesis block",
      "previousHash": "0",
      "hash": "4373c7fb1437035365d9228c77eca2cfd240523e274163e78c1eba11effd8b38"
    },
    {
      "index": 1,
      "timestamp": "10/07/2017",
      "data": {
        "amount": 4
      },
      "previousHash": "4373c7fb1437035365d9228c77eca2cfd240523e274163e78c1eba11effd8b38",
      "hash": "c37ff893464874ffb4cfb0e0da1961786a0fd14ed68157af3a468944d098ecad"
    },
    {
      "index": 2,
      "timestamp": "12/07/2017",
      "data": {
        "amount": 10
      },
      "previousHash": "c37ff893464874ffb4cfb0e0da1961786a0fd14ed68157af3a468944d098ecad",
      "hash": "dda01bd5f98a793cc0134e3194d8b9b6ca5fa4b001607f5b716bbaad079f7978"
    }
  ]
}

```

Fig. 20 Blockchain storage

```

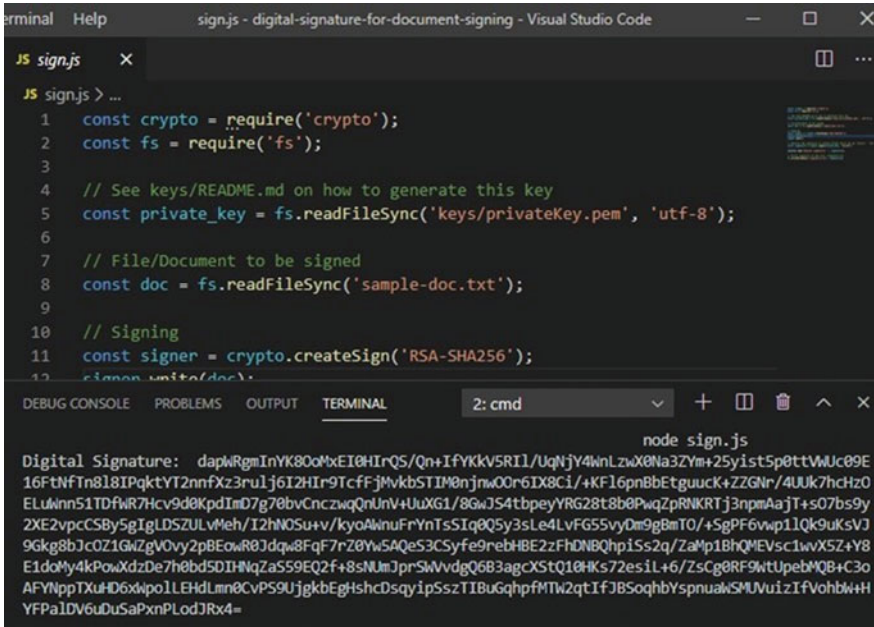
OUTPUT  TERMINAL  DEBUG CONSOLE  PROBLEMS

Microsoft Windows [Version 10.0.18362.657]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\saisi\Documents\SavjeeCoin> node example2.js
Mining block 1....
Block mined: 00765ca58c6b20d507a618ffe2e590d347154af541cc1b13d34aa3d931a06ea5
Mining block 2....
Block mined: 00dc27162eb7b8c3447358c137f47e093f8e9067238cbbf2d74142cb4c3f7261

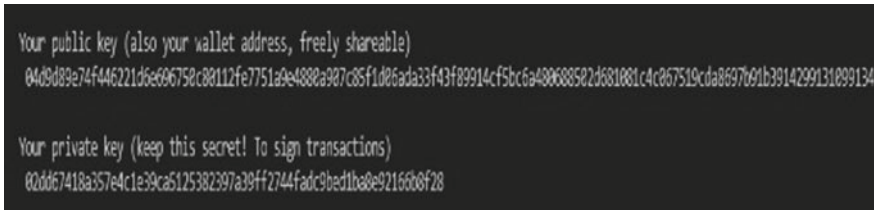
```

Fig. 21 Blockchain mining



```
terminal Help sign.js - digital-signature-for-document-signing - Visual Studio Code
JS sign.js X
JS sign.js > ...
1 const crypto = require('crypto');
2 const fs = require('fs');
3
4 // See keys/README.md on how to generate this key
5 const private_key = fs.readFileSync('keys/privateKey.pem', 'utf-8');
6
7 // File/Document to be signed
8 const doc = fs.readFileSync('sample-doc.txt');
9
10 // Signing
11 const signer = crypto.createSign('RSA-SHA256');
12 signer.update(doc);
13
14 node sign.js
Digital Signature: dapwRgmInYk80oMxEI0HrQS/Qn+IfYKkV5RI1/UqNjY4MnLzwX0Na3ZYm+25yist5p0ttWwUc09E
16FtNfTn818IPqktYT2nnfXz3rulj6I2HIR9TcFfJmVkbSTIM0njnw00r6DX8Ci/+KF16pnBbEtguuK+ZZGNr/4Uuk7hcHz0
ELuWnn51TDfWR7Hcv9d0KpdImD7g70bvCnczwaqQnUnV+UuXG1/8GwJ54tbpeyYRG28t8b0PwqZpRNKRTj3npmAajT+s07bs9y
2XE2vpcCSBy5gIgLDSZULWmeh/I2hN0Su+v/KyoAWnuFrYnTsSIq0Q5y3sLe4LvFG55vyDm9gBmTO/+SgPF6vwp11Qk9uKsVJ
9Gkg8bJc0Z1GwZgV0vy2pBEowR0Jdqw8FqF7rZ0YwSAQeS3Csyfe9rebHBE2zFhDNBQhpiSs2q/ZaMp18hQMEVsc1wvX5Z+Y8
E1doMy4kPowXdzDe7h0bd5DIHnqZaS59EQ2f+8sNUmJprSWvdgQ6B3agcXstQ10HKS72esiL+6/ZsCg8RF9wtUpebMQB+C3o
AFYnppTXuHD6xipolLEhdLmn0CvPS9UjgkBEghshcDsqiypSszTIBuGqhpffMtW2qtIfJBSoqhbYspnuakSMUVuizIFvohbW+H
YFPa1DV6uDuSaPxnPlodJRx4=
```

Fig. 22 Digital signature

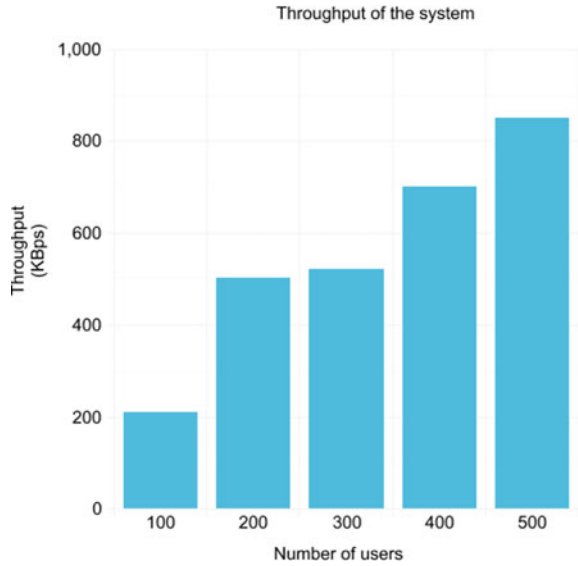


```
Your public key (also your wallet address, freely shareable)
04d0d89e74f44621d6e696750c80112fe7751a9e4880a907c85f1d06ada33f43f89914cf5bc6a408688582d681081c4c067519cda0697691b3914299131099134

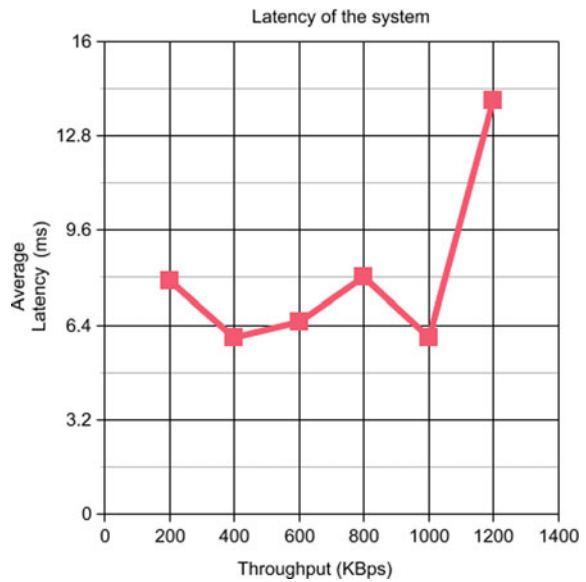
Your private key (keep this secret! To sign transactions)
00dd67418a357e4c1e39ca5125382397a39ff2744fad93bed1ba0e9216608f28
```

Fig. 23 Key pairs

**Fig. 24** Analysis of throughput



**Fig. 25** Analysis of latency



## References

1. Chakraborty S, Aich S, Seong SJ, Kim H-C (2019) A blockchain-based credit analysis framework for efficient financial systems. In: 2019 21st international conference on advanced communication technology (ICACT). IEEE, pp 56–60

2. Poonpakdee P, Koiwanit J, Yuangyai C, Chatwiriya W (2018) Applying epidemic algorithm for financial service based on blockchain technology. In: 2018 international conference on engineering, applied sciences, and technology (ICEAST). IEEE, pp 1–4
3. Kabra N, Bhattacharya P, Tanwar S, Tyagi S (2020) MudraChain: blockchain-based framework for automated cheque clearance in financial institutions. *Future Gen Comput Syst* 102:574–587
4. Minnens F, Luijckx NL, Verbeke W (2019) Food supply chain stakeholders' perspectives on sharing information to detect and prevent food integrity issues. *Foods* 8(6):225
5. Kaid D, Eljazzar MM (2018) Applying blockchain to automate installments payment between supply chain parties. In: 2018 14th international computer engineering conference (ICENCO). IEEE, pp 231–235
6. Pundir AK, Devpriya J, Chakraborty M, Ganpathy L (2019) Technology integration for improved performance: a case study in digitization of supply chain with integration of internet of things and blockchain technology. In: 2019 IEEE 9th annual computing and communication workshop and conference (CCWC). IEEE, pp 0170–0176
7. Saberi S, Kouhizadeh M, Sarkis J, Shen L (2019) Blockchain technology and its relationships to sustainable supply chain management. *Int J Prod Res* 57(7):2117–2135
8. Guo Y, Liang C (2016) Blockchain application and outlook in the supply chain industry. *Financ Innov* 2(1):24
9. Tian F (2017) A supply chain traceability system for food safety based on HACCP, blockchain, and Internet of things. In: 2017 international conference on service systems and service management. IEEE, pp 1–6
10. Zhao G, Liu S, Lopez C, Lu H, Elgueta S, Chen H, Mileva Boshkoska B (2019) Blockchain technology in agri-food value chain management: a synthesis of applications, challenges, and future research directions. *Comput Ind* 109:83–99
11. Creydt M, Fischer M (2019) Blockchain and more-algorithm driven food traceability. *Food Control*
12. Ito K, Tago K, Jin Q (2018) i-Blockchain: a blockchain-empowered individual-centric framework for privacy-preserved use of personal health data. In: 2018 9th international conference on information technology in medicine and education (ITME). IEEE, pp 829–833
13. Ekblaw A, Azaria A, Halamka JD, Lippman A (2016) A case study for blockchain in healthcare: “MedRec” prototype for electronic health records and medical research data. In: *Proceedings of IEEE open and big data conference*, vol 13, p 13
14. Vyas S, Gupta M, Yadav R (2019) Converging blockchain and machine learning for healthcare. In: 2019 amity international conference on artificial intelligence (AICAI). IEEE, pp 709–711

# Blockchain-Based Access Control System



P. Leela Rani, A. R. Guru Gokul, and N. Devi

**Abstract** Access control assures protection of resources against illegal access. This is implemented using policies, which enforce stringent mechanisms to protect highly confidential information. Blockchain is an apt technology for providing access control. Blockchain-based access control will offer security and transparency. It would also be helpful in avoiding a third party involvement. Blockchain-based access control system, in spite of providing confidentiality to the data, also ensures the integrity of the same. Blockchain technology is tamper-proof by its default implementation and access control increases the security of the data stored in the devices.

**Keywords** Access control · Blockchain · Attribute · Smart contracts · Cryptography

## 1 Introduction to Blockchain

A blockchain [1] is a decentralized distributed ledger of records that are cryptographically secured. A collection of records is grouped as a block. As shown in Fig. 1, the blockchain will grow as new blocks are added along. Every block in the blockchain will comprise of hash of the preceding block, collections of records of its own, and hashed value of records known as Merkle tree. Using hashing technique in an efficient way ensures integrity in blockchain and improves the security of the data stored in it. After the records are added to block and appended to the existing chain, it is infeasible to change any records in future.

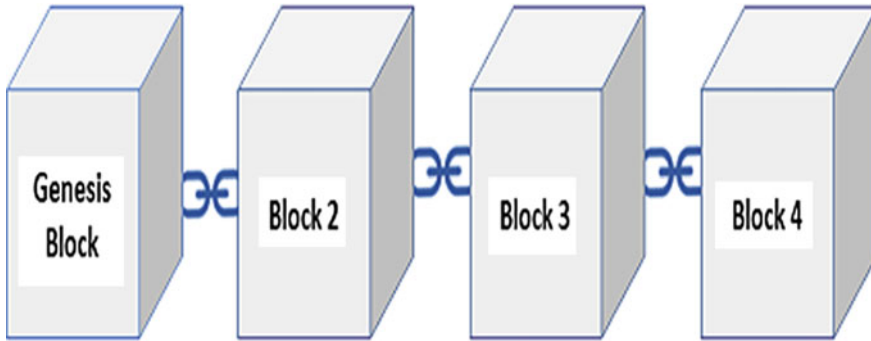
---

P. Leela Rani (✉) · A. R. Guru Gokul · N. Devi  
Department of Information Technology, Sri Venkateswara College of Engineering,  
Sriperumbudur, India  
e-mail: [28leelarani@gmail.com](mailto:28leelarani@gmail.com)

A. R. Guru Gokul  
e-mail: [gurugokul007@gmail.com](mailto:gurugokul007@gmail.com)

N. Devi  
e-mail: [nds@svce.ac.in](mailto:nds@svce.ac.in)





**Fig. 1** Basic blockchain structure

### ***1.1 Contents of a Block***

A block in a blockchain is a collection of various items such as the hash of its preceding block, the Merkle root and its own records. A Merkle tree for a block is formed by placing the hash of the individual records of that block as the leaf nodes and the non-leaf nodes as the combined hash of their own children. Hashing ensures data integrity and correctness of the data.

The first block is called as genesis block and is created at the beginning with the set of records and its Merkle root. In blockchain, once the block is created it is computationally infeasible to change the record in that block as it is connected to its subsequent block, which in turn, is connected to its next and so on. This dependency between the new and the old blocks in a blockchain ensures data integrity and prevents unauthorized data modification. The basic blockchain structure is shown in Fig. 1.

### ***1.2 Distributed Ledger***

A blockchain is a collection of immutable blocks in a transaction. This blockchain of records is referred to as ledger. This ledger is distributed among all the peers connected in the network and is updated regularly. The type of the transactions may vary from financial to medical records based on the blockchain application.

### ***1.3 Smart Contract***

A smart contract is a defined set of rules agreed upon by two nodes to perform a transaction. A transaction cannot be completed without satisfying all the set of rules defined in the smart contract. Any association of third party in the blockchain is

removed by the implementation of smart contract and they are consequently activated when a transaction is being done [2, 3].

### ***1.4 Consensus Protocol***

As the blockchain is a distributed ledger, it is mandatory to keep track of all the nodes and their records in a synchronized manner. To maintain this uniformity, various consensus mechanisms are employed in blockchain. In consensus mechanism, decision is made based on the acceptance by majority of nodes which eliminates the possibility of single controller of the network. Some of the consensus mechanisms like Proof of Work (PoW), Proof of Stake (PoS), Proof of Concept (PoC), etc. are widely used in blockchain.

### ***1.5 Cryptography Used in Blockchain***

The cryptographic techniques employed in blockchain ensure the security and integrity of the network and its data including the transactions. The most common techniques employed in blockchain are: Secure Hash Algorithm-256 (SHA-256), Rivest-Shamir-Adleman (RSA) public key cryptography, Digital Signature Algorithm (DSA), Elliptic Curve Digital Signature Algorithm (ECDSA), and various encryption techniques such as Attribute-Based Encryption (ABE) and Data Encryption Standard (DES) [4, 5]. The usage of blockchain technology is rapidly increasing due to its wide range of applications and the level of security provided. By enforcing a reliable and authorized access control over the resources, the data between peers can be exchanged in a secure way and can also be controlled using smart contracts.

### ***1.6 Permissioned Versus Permissionless Blockchain***

Based on the permission obtained by the user to participate in the consensus process or in some cases even to join the blockchain, it can be classified as permissioned or permissionless. In the permissioned blockchain, the access to the blockchain is limited to the set of users who are already known to the system. Those users can provide the identity to authenticate them to the system and can access the data. This type of blockchain is also called as private chain as it is limited to a collection of users and the ledger data is made available only to those registered users.

In permissionless blockchain, any user can join anonymously and take part in the consensus process to add a new block to the blockchain. The chain is also called as public chain as there is no limit on the users who are allowed to join the chain. The ledger copy will be available with all the anonymous users. A hybrid model that

makes a part of blockchain as publicly available and the remaining as a private one is also available.

## **2 A Study on Existing Access Control Methods**

Access control refers to cautious restriction to access a resource or information in the computer context. Certain crucial information like data, services, storage space, etc., cannot be granted access to everyone. There should be a mechanism to control the handling of this crucial information by users. Whenever a user is requesting access for a subject, the system should evaluate certain procedures related to the policies before it provides control over the subject. This section covers the various access control methods that are in practice to protect information assets from unauthorized access by users.

### ***2.1 Discretionary Access Control***

In Discretionary Access Control (DAC) system, the owner of the resource will decide about the access privileges provided for every user of the system either physically or digitally. DAC is the minimal secure model of access control as the user has control over any subject and its connected programs that are provided with access. The user is also provided with the control to enable and modify the security settings which may lead to unauthorized access without the knowledge of the data owner itself.

### ***2.2 Attribute-Based Access Control***

Attribute-based access control (ABAC) can be provided based on the attributes related to the subject or the user. These attributes can be a combination of the following like employee ID, company ID, designation, and name of the project he is related to and so on. These access controls can be transferred to some other subject or the user based on the current person who is handling the subject and the policies that are allowed for the user. Most of the access control systems are granting a resource based on the identity of the user requesting it. In ABAC, the access for a resource is given to the user who has been authenticated in the vicinity.

### ***2.3 Mandatory Access Control***

Mandatory Access Control (MAC) is popularly used in places where confidentiality and secrecy of data are more important. Rather than allowing the users to have control over the subject, it allows only the owners to have control over it and offers them with procedures and policies for managing the access controls. MAC will categorize the users and allow them access based on the defined security policies.

### ***2.4 Role-Based Access Control***

Role-Based Access Control (RBAC) is also referred to as Rule-Based Access Control. It is largely accepted and implemented model in today's business world. In RBAC, the access privileges for the users of the organization are provided by the security manager rather than by a collection of individuals. The notable factor in RBAC is that the manager, who provides the privilege, has default control permissions assigned. The system administrator can then provide access privileges for various subjects and the users based on the job requirements and responsibilities.

## **3 Access Control System Based on Blockchain**

Blockchain was initially designed to use cryptocurrencies in finance. According to a research, blockchain technology can be extended to many applications apart from finance domain. It is evident that availability of decentralized data provides trusted robust third party services. In blockchain access control system, the right to access a resource is defined by the resource owner in a transaction. The merits of storing this information are:

- Easy transfer of rights from the last accessed user to another user. There is no need of control to be exercised by the resource owner for the transfer.
- All the transactions that represent the transfer of rights are published in the blockchain.

It is possible to keep track of the users who are provided with rights to perform an action on the resource that is currently accessed [6]. An entity is entrusted with the job of providing the access for various resources. If a user is denied the access for a resource, the user is provided with the privilege to verify the credibility of access denial by the entity.

ABAC policy as shown in Fig. 2 is a standard way of assigning access rights to a resource. In ABAC, the main components are rules and attributes. The attributes of the environment or the resources form the collection of attributes. Conditions over the set of attributes are mentioned as the set of rules. In order to get an access to

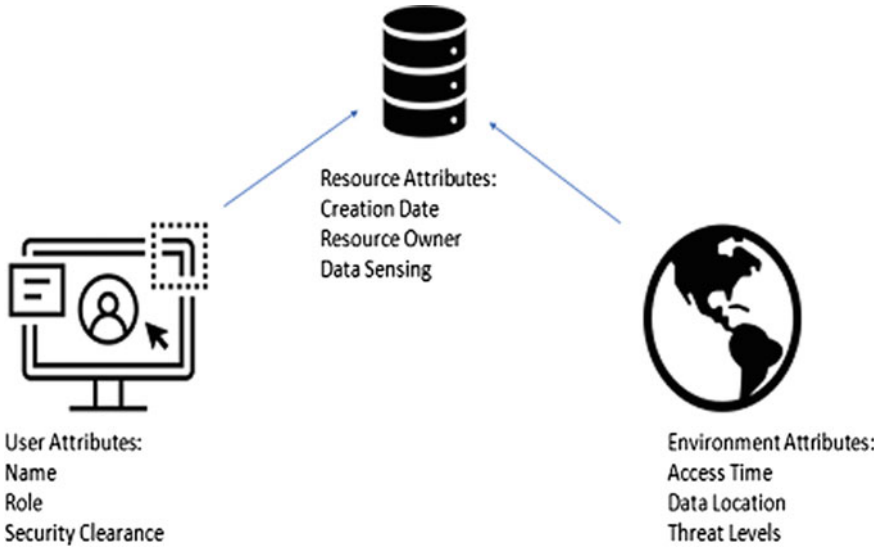


Fig. 2 ABAC policy

a resource, the rules must be satisfied. OASIS consortium has defined eXtensible Access Control Markup Language (XACML) as the policy definition language for ABAC [7].

Every resource is associated with a unique resource owner who controls the policy for each of the resources. The resource holder is responsible for creating, updating, and revoking the policies. The user of the resource should have appropriate rights to perform actions on resources. The users can also reassign the rights abided by the policies. This reassignment of rights can be done either partially or as a whole by the user.

The role of the resource holder and the user are mutually exclusive. Let us denote the resource owner as RO, the resource as R and the user of the resource as U who is assigned a unique ID. RO defines the set of policies to be satisfied by U to access R. RO may update the policy as and when the user is currently granted access to the resource even if the modification results in revoking the rights. Similarly, the resource owner has no control over transfer of rights to access a resource.

### 3.1 Operations on Policy

The following operations can be defined on a policy:

- Create
- Update
- Revoke.

A transaction used to create a policy is stored in the blockchain called as Policy Initiator (PI), which allows the RO to update the same as and when required that can be revoked at any time.

Every policy defines the user ID and the conditions to define the allowable values for the attributes of user, resource and environment based on which the access will be granted. Any right holder is given the privilege of modifying the rights when the rights are transferred to the other users. The current right holder is allowed to:

- Transfer the rights as such
- Add new conditions in addition to the old ones
- Segregate the set of values sanctioned for an attribute.

There are a few points to be noted when a condition is added to a policy or updated. The user has rights to add new conditions. This new condition is added along with the conditions that are already defined in the policy. While adding a condition, the user cannot modify existing conditions. Whenever the rights are transferred, the new user can only add to already existing conditions. The RO is responsible for updating the existing policies. RO has the privilege to entirely change the conditions defined in the policy. If more than one user wants to access a resource, RO is supposed to create a separate policy for those users. Each user will be provided with a distinct policy.

A blockchain is a decentralized repository. It is to be noted here that in a blockchain, the mode is append only mode. After a new block is added to the blockchain, it is practically impossible to remove that block from the blockchain. This feature provides the restriction that the data to be added in a blockchain should be an essential information.

XACML requires a set of formal structures. Policies written using XACML tend to be quite lengthy. If these policies are stored in the blockchain, it may lead to space issues. To avoid this space constraint, the policies can be stored in an external source. A link referring to this source and a hash of the policy could be stored in blockchain. This approach would result in making the activity of policy as constant irrespective of the length of the policies. Since the policy itself is not stored in blockchain, there would be serious security issues.

Blockchain-based access control technique is much cheaper and more secure than other technologies. It also allows the user to be in control of the data.

There are two solutions for implementing blockchain access control. One solution is to make password obsolete. Secure Socket Layer (SSL) certificates are stored on each node instead of a password and the password data is implemented as a blockchain. Another solution is IBM's blockchain access control that allows only the certified users to access online platforms for certifying diamonds. It also eliminates any security threats.

Blockchain is publicly available, decentralized and secure. In typical access control model, the access policy is usually stored in the server. The concept of having servers makes the blockchain as a centralized one. The security of the blockchain can be compromised as the attackers can gain illegal access to the policy and control operations of the users.

A blockchain-based access control should eliminate the security threats and allows the policies to be distributed over the network. A blockchain-based access control provides an additional level of security to existing applications. Unauthorized access to a resource may be gained by an attacker. To prevent unsanctioned access, imposing several levels of security is highly important.

### 3.2 *Attribute-Based Encryption*

Attribute-Based Encryption (ABE) and Identity-Based Encryption (IBE) can be used for access control mechanism. This approach combines Attribute-Based/Id-Based Encryption and sign (C-AB/IB-ES) along with blockchain techniques to ensure integrity. In Ethereum blockchain, smart contracts can be defined. The policies can be encoded in the smart contracts as follows:

- The first step is defining the policies,
- The second step is defining Policy Enforcement Architecture (PEA).

PEA is the set of components involved in verifying a current access request against the stored policies. If the policy is not stored as a smart contract, then the enforcement would be implemented as XACML. Policies in XACML are compressed and OP\_RETURN and Multi-Signature (MULTISIG) transactions are used to store policies in blockchain. The attribute required for access request can be accessed by Lightweight Directory Access Protocol (LDAP).

The conditions that are newly added by user are quite different from the updates that are done by the RO. The conditions that are added by user are appended along with the existing ones using AND operator which, in turn, makes the existing policy as a more restrictive one. While the update is performed by user, it may sometimes lead to an entirely new set of policy compared to the existing one. On the other side, the RO is supposed to confine the policy rights but not expand them and the role of user is to only append extra rights over the current resource so that they cannot be removed or changed by new user who is currently accessing the resource.

The rule defined in a policy will comprise of all the existing conditions of the policy which are appended with each other using AND and OR logical operators. The access can be granted for several users and several resources at the same time depending on the capacity of the system. Blockchain is a distributed collection of records that is available with all the users. It is also tamperproof by its structure of implementation. It is impossible to delete a data from the blockchain without modifying the contents of its related or subsequent blocks.

The data stored in the blockchain should be minimized for an effective implementation of the same. The policies that are defined using XACML are quite big and consume a large amount of space. An alternative for this approach would be saving the contents of a policy in an external resource that assures integrity of the data and storing that reference as a link or as a file descriptor alone as the data in the blockchain [8].

This model reduces the amount of data to be stored in the blockchain and benefits the policy creator to have a flexible policy description as there is no memory constraint on the external resource. On the other side, as the policies are stored in the external source, the basic requirements of blockchain like availability, integrity and security issues must be addressed.

### ***3.3 Traceable ABE***

The secret key generated in traceable ABE model [3] can always be traced to the source and the issues can be recorded in the blockchain that improves the security of ABE scheme. The secret key generated during data sharing will not have the details of users who generate them to ensure anonymity. The attribute authority may also generate the secret key from the available attribute set. If there is an issue pertaining to the secret key, the same cannot be identified whether it originated from the user or the attribute authority. Effortless implementation of the access control methodologies lead to sensitive data leakage. However, the traceable ABE scheme implemented using blockchain ensures integrity and non-repudiation of data in addition to privacy preservation.

### ***3.4 Attribute-Based Security***

In attribute-based security (ABS) [9], the ciphertext is associated with the attributes. The private key is connected to the predicate which is the access tree of the proposed model and a policy is defined for the decryption of ciphertext along with its keys [10]. When the secret key is used in the process based on the rights provided for the user, the access tree is generated and the data are encrypted using the attributes. A model that associates the tree with the private key [11] where the user has the privilege of storing either the Key or the Cipher text along with the policy and ABE is implemented over it.

In this model, the access tree is used to encrypt the data and the secret key for the user is produced using the attributes. The decryption is possible only when the attribute satisfies the access tree of the user. The ABS model has the following process flow starting from algorithm set up, followed by extraction of private key then signing the data and finally verifying it.

### ***3.5 Hybrid Approach to Store Attributes in Blockchain***

A hybrid approach that allows the users to store the policy in the blockchain but also ensures that there are no redundant data. The policies are compacted and written in



a specific format to be stored in the blockchain. The approach they have used is to segregate the policy into three parts as the attribute on both side and the operand used to connect them. AND/OR operations are used to append multiple conditions into an exclusive condition.

A mapping is created between all the operands and a code defined by the policy. The map is also maintained to add new policies or symbols during the future upgrades. A similar kind of approach can be used by the policy owner for mapping the attributes with numerical values. The available set of attributes can be made available publicly by the owner. The owner should make use of the same identity to create new policies in future. The hash of this mapping list is also stored as a data along with the policy to avoid fabricating a new policy or unintentionally modifying an active one. The owner still has control over this mapping which can be removed as it is stored in an external source. In future, if there is any inconsistency, it same can be verified with the hash of the policy and the signature stored along with it during its inception.

This model has advantage of allowing the user to store the information about the policy attribute unlike the previous model that had only a reference to the external resource. By applying this model, the left side operand can be represented as a reference or as a constant in a compacted format. This model also allows the user to store the attributes in specific types based on their value rather than using a common type to store all kind of attributes.

### ***3.6 RBAC-Based Smart Contract in Blockchain***

RBAC is an exclusive model that can be used for Smart Contract environments in the blockchain [12]. The Smart Contract (SC) and Challenge Response Protocol are the two main components of SC-based RBAC model. The roles for the users are created competently and effectively in a secure manner using a variety of functions provided by SC and stored in the blockchain. By storing the data in blockchain, anonymity of the data is ensured and it can be verified, since the data is always transparent in the blockchain. SC is a programmable asset that executes as instructed to do so in an exact manner and stores the results and the actions performed in the blockchain. The following actions can be performed by the organizations using the SC:

- Issuing role to the users
- Manage and modify the information as and when needed in a transparent way
- Revoke the roles as and when needed
- Provide access to users for issuing roles to other users and revoke them as well.

Authentication for the possession of roles and approval of user's role assignment in this model is done by the challenge response protocol. The protocol has the following sequence:

- Verifying the data related to the user and announcement of the user role
- Challenging the user

- Receiving response from the user for the challenge
- Validation of the user's response.

The challenge response model is designed such that there is no need of interaction among various organizations and it is not necessary to enforce the same always.

### ***3.7 Enhanced RBAC Model***

To improve the security of the data accessed by various entities such as people, system or devices an enhanced RBAC model [13] is implemented that enables the access of data in a secure manner with the help of web services. The access controls are placed in a hierarchical manner that enables the user to store even the relation between various users and their roles. This implementation improves the security and efficiency of RBAC systems implemented in blockchain for more improved data access mechanisms.

## **4 Access Control-Based Blockchain for Internet of Things**

The phenomenal growth of the Internet has given rise to a large set of connected devices that can communicate among themselves to carry out tasks. The invention of various technologies like Wi-Fi, Bluetooth, and other wireless protocols has made the connectivity much faster. One such product of these growing technologies is the Internet of Things (IoT) that connects the physical world with the Internet [14]. The IoT devices are connected to each other over the Internet and are able to share the data, resources, and information among them without the interference or assistance from human. Due to the minimal human intervention and higher processing capacity, the connected devices are growing exponentially in today's world.

### ***4.1 Merging Blockchain and SC in IoT***

As blockchain is a decentralized trustless network used for transactions between the users, it helps to achieve the settlement between the users in a faster way. The underlying cryptographic model enhances the security of the data. On the other hand, SC can be triggered and executed or can be made to execute on its own. Combining blockchain and SC with IoT [15, 16] enables the users to automate the process and allure the users toward them.

Amalgamation of blockchain with IoT is to enhance the security issues faced by IoT systems and to overcome the problems associated with dependence of IoT devices on a centralized cloud environment. Many companies including IBM are integrating

blockchain into the supply chain environment. Upon integration, it allows the users to load a part of the data to the permissioned blockchain which can be added in transactions. It also has an inbuilt capability to convert the device data into a form that is acceptable by the blockchain API's. The implementation platform takes care of the data conversion job from the devices to blockchain and it also sends only the data from the devices, not their particulars. Rather than a common storage, the data is shared with the entities that are a part of the transaction. Most of the organizations are integrating blockchain into their supply chain and other frameworks.

## ***4.2 Challenges in IoT***

The frequent challenges faced by IoT devices are the illicit sharing of data, unauthorized access of data or access by unauthorized users or failure of the centralized controller that is the backbone of the network. To overcome these challenges, the IoT system can be connected along with tamper-proof blockchain technology which elevates the security and also addresses the challenges in real time.

## ***4.3 ABAC Using Blockchain for IoT***

The conventional access control technologies that are used to provide access for the device are no longer applicable for the development of largely interconnected IoT devices. The multifaceted and extensive structure of the connected devices posts new challenges and security threats to them which can be addressed by ABAC system for IoT [17]. To ensure the integrity of the data and to avoid centralized failure in the network, Blockchain is used to store the details which are distributed over all the nodes and an in built tamperproof model.

### **4.3.1 Components of ABAC-Based Blockchain for IoT**

The components of the model are attribute authorities and IoT devices. The role of attribute authorities is to dispense, store, and maintain attributes in the blockchain. These attributes will be stored as transactions in the blockchain. Further, the attribute authority also verifies the validity of the data before it is stored in the chain as it is infeasible to alter the data once stored in the blockchain. There is a provision for updating the chain later based on the consensus arrived between the authorities. During registration, the attribute authority also takes care of the process of generating the keys that will be used to identify the IoT devices in the system. The key distribution process helps the devices to authenticate themselves before data transfer and also to concur on a shared key.

The IoT devices will collect, process, and share the data to the system. The privilege of read access in the blockchain is only provided for the devices and they will not involve in the process of verifying the transactions. To ensure confidentiality and security, the requester of the data should obtain appropriate authorization from the data owner before the exchange. The data owner can access the data after successful authentication of attributes themselves to match the access policy defined by the attribute authority.

#### ***4.4 SC-Based Access Control for IoT***

A framework that is based on SC has been implemented for providing access control in IoT [18]. The components of this model comprise of multiple contracts for access control and other contracts used for registering and approving the same. The role of contract is to implement access right verification by validating the activities of the subject. The contract used for approval will validate the access control contracts dynamically. If any such access control contract is found to deviate from the purpose, the approval will not be granted.

If a subject is found to deviate from its purpose, the approving contract has the rights to impose a penalty on that subject. The role of the registering contract is to provide and manage the functions like registration, modification, and removal of various subjects to register them in the blockchain. This approach defines a secure model of communication among IoT devices using the blockchain.

#### ***4.5 Identity and Access Management Systems in IoT***

The security of the IoT system can be improved to a greater extent with the help of blockchain-based access management systems [19]. Various details like identity, credentials, and access rights can be stored in the blockchain and resist changes as long as the data is original. One challenge to be addressed in this system is the security and reliability of the data stored in the system. In permissioned blockchain, the hash data about the device and its configuration can be stored in an eternal manner which can be used to verify the legitimacy of the device while a connection request is processed.

### **5 Smart Contract-Based Access Control Policy**

When a resource is accessed by several users, it is necessary to provide security to that resource by enforcing a policy. This section describes the access control policy based on roles. In RBAC system in smart contract, roles have an identifier and can be

created dynamically. A description that details the addresses of users can be created and stored along with its related secondary role. This secondary role has the privilege to add or remove users. Role-Based Access Control System in smart contract allows creation of new roles at runtime. It has an administrator to add and remove members to the role. It can also be used to identify existing roles and their bearers.

### ***5.1 Implementation of RBAC***

RBAC can be implemented in any of the existing blockchain network. Ethereum is permissionless distributed blockchain network that is used to implement real-time applications. The organizations that require only access by authenticated persons can implement the blockchain on Hyperledger framework which is private blockchain restricted only for registered users.

The sample implementation and testing of RBAC reproduced from [20, 21] is given in Appendix 1.

### ***5.2 Testing of RBAC***

This contract is made available as public contract.

Contract: RBAC

RBAC

- addRootRole creates a role.
- hasRole returns false for non-existing roles.
- hasRole returns false for non-existing bearers.
- addRootRole adds msg.sender as bearer.
- addRole doesn't add msg.sender as bearer with an admin role.
- addBearer throws on non-existing roles.
- addBearer throws on non-authorized users.
- addBearer does nothing if the bearer is in the role.
- addBearer adds a bearer to a role.
- removeBearer throws on non-existing roles.
- removeBearer throws on non-authorized users.
- removeBearer does nothing if the bearer is not in the role.
- removeBearer removes a bearer from a role.

## **6 ABAC in Hyperledger Fabric**

ABAC restricts access to a specific user with a certificate. The processes of creating a certificate are Registration and Enrollment. Enrollment is the process by which a

user requests and obtains a digital certificate from a given CA. Registration is done by a Registrar, telling a CA to issue the digital certificate. A registrar is enrolled in CA. Then the admin receives the signing key and certificate. The admin then registers user1 into the CA with proper information. The CA provides a secret key. This secret key is then used to enroll user1 to the CA. User1 gets the certificate and key. USER1 is registered by specifying the attributes.

```
fabric_ca_client.register({enrollmentID: username, affiliation:
'org1.department1', role: 'client', attrs: [{name: 'role', value: 'approver',
ecert: true}]}, admin_user);
```

In fabric-ca-client to register a user, the array of key-value pair should be specified. The role of user1 is approver. The next step is enrollment.

```
fabric_ca_client.enroll({enrollmentID: username, enrollmentSecret: secret,
attr_reqs: [{name: "role", optional: false}]});
```

While enrolling, optional attribute should be false. After successful completion of the two steps, the certificate gets generated.

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

37:19:35:f4:f9:90:a4:f9:a7:b9:fb:df:85:26:79:1a:5a:2f:ab:72

Signature Algorithm: ecdsa-with-SHA256

Issuer: C = US, ST = California, L = San Francisco, O = org1.example.com, CN = ca.org1.example.com

Validity

Not Before: Jan 25 18:37:00 2020 GMT

Not After : Jan 24 18:42:00 2021 GMT

Subject: OU = client, CN = pavan

### 6.1 Go Smart Contract

Chaincode is a program, written in Go, Node.js, or Java that implements an interface. Chaincode runs in a secured Docker container isolated from the endorsing peer process. Chaincode initializes and manages ledger state through transactions submitted by applications.

A chaincode handles business logic agreed to by members of the network. Ledger updates created by a chaincode are scoped exclusively to that chaincode and cannot be accessed directly by another chaincode. However, within the same network, given the appropriate permission, a chaincode may invoke another chaincode, to access its state.

```
import "github.com/hyperledger/fabric/core/chaincode/lib/cid"
```

The above statement should be included as there are multiple functions available in client identity (cid) package that should be used in the chaincode. The business logic can be implemented in restricted smart contract function.

## ***6.2 Node Smart Contract***

Import fabric-shim package. The business logic implementation is done in the smart contract. Smart contracts can be written in any language.

# **7 Issues to Be Addressed in Blockchain-Based Access Control**

Blockchain is rapidly accepted by many organizations due to its efficiency and the level of security provided for the data stored in it. Integrating blockchain with IoT enhances the potential of various devices that are connected over the network. It also improves the security issues that are faced by them during the data transfer or data storage. The following are some issues to be addressed in blockchain-based access control systems.

## ***7.1 Operational and Regulatory Issues***

Although blockchain is known for its efficiency and the level of integrity provided for the data, it is yet to be widely accepted in many of the countries due to its unexplained challenges of principles and guidelines [22]. Due to the rapid growth of blockchain technology, the guidelines to be followed should be mandated and established as the application scope varies from financial to supply chain. On implementing the guidelines and the assurance provided by them will enable a universal acceptance of the implementation of blockchain and thereby unleashing the full potential.

## **7.2 *Memory Requirements***

Blockchain is a distributed network that requires a lot of memory to store and handle all the data in the peer level. Another issue to be addressed is the scalability of the peer nodes in the event of expanding an existing network [23]. As new devices are added in the network, every node in the blockchain should be able to accommodate the entire set of data generated which may be a curb for the users. As the blockchain is widely accepted and integrated with various applications in the future, it may generate a large volume of data that needs to be processed and handled by the devices which may be a bottleneck for the end users.

## **7.3 *Sustainability in the Long Run***

Even though the blockchain has attracted interest of numerous companies, the state-of-the-art model of the blockchain implementation is yet to be achieved, which raises a question on the sustainability of this model [24]. As an infant model, it still faces issues in its functionality. The implementation of this model requires massive infrastructure, a collection of stake holders and variety of governments and their norms. Given these issues, the sustainability of this technology is still unanswered.

## **8 *Future Scope***

Making use of artificial intelligence (AI) and machine learning (ML) in blockchain technology can address issues faced by applications that make use of blockchain. The blockchain is a tool to store, execute, and verify transactions and its related data based on the application. AI along with blockchain [25] will help in the process of decision making and the judgment about the data an easier one. Additionally, the ML techniques can improvise the process of decision making without the need for any intervention and it could also help in the process of granting access rights for the users or the systems. As the block sizes are increasing rapidly, the blockchain is growing in a swift manner. The blockchain application implemented for access control-based systems will be storing the data that represent the access rights for various users and systems. The past data can be analyzed to find out various suspicious behaviors and attributes which can be used to identify and alert the system before granting the access. Identifying these malicious users before granting access will enhance the security of the application and data stored in the blockchain.



## Appendix 1

```

pragma solidity ^0.5.0;

/**
 * @title RBAC
 * @author Alberto Cuesta Canada
 * @notice Implements runtime configurable Role Based Access
Control.
 */
contract RBAC {
    event RoleCreated(uint256 role);
    event BearerAdded(address account, uint256 role);
    event BearerRemoved(address account, uint256 role);

    /**
     * @notice A role, which will be used to group users.
     * @dev The role id is its position in the roles array.
     * @param description A description for the role.
     * @param admin The only role that can add or remove bearers
from this role.
     * To have the role bearers to be also the role admins you should
pass
     * roles.length as the admin role.

```

```

    * @param bearers Addresses belonging to this role.
    */
    struct Role {
        string description;
        uint256 admin;
        address[] bearers;
    }

    /**
     * @notice All roles ever created.
     */
    Role[] public roles;

    /**
     * @notice The contract constructor, empty as of now.
     */
    constructor() public {
    }

    /**
     * @notice Create a new role.
     * @dev If the _admin parameter is the id of the newly created
    role
     * msg.sender is added to it automatically.
     * @param _roleDescription The description of the role being
    created.

```

```

    * @param _admin The role that is allowed to add and remove
bearers from
    * the role being created.
    * @return The role id.
    */
function addRole(string memory _roleDescription, uint256
_admin)
    public
    returns(uint256)
    {
require(_admin <= roles.length, "Admin role doesn't exist.");
    uint256 role = roles.push(
Role({
        description: _roleDescription,
        admin: _admin,
        bearers: new address[](0)
    })
) - 1;
emit RoleCreated(role);
if (_admin == role) {
    roles[role].bearers.push(msg.sender);
    emit BearerAdded(msg.sender, role);
}
return role;
}
/**

```

```

* @notice Verify whether an address is a bearer of a role
* @param _account The account to verify.
* @param _role The role to look into.
* @return Whether the account is a bearer of the role.
*/
function hasRole(address _account, uint256 _role)
    public
    view
    returns(bool)
{
    if (_role >= roles.length ) return false;
address[] memory _bearers = roles[_role].bearers;
    for (uint256 i = 0; i < _bearers.length; i++){
        if (_bearers[i] == _account) return true;
    }
    return false;
}

/**
* @notice Add a bearer to a role
* @param _account The address to add as a bearer.
* @param _role The role to add the bearer to.
*/
function addBearer(address _account, uint256 _role)
    public
{

```

```

require(_role <roles.length, "Role doesn't exist.");
require(
hasRole(msg.sender, roles[_role].admin),
"User not authorized to add bearers."
);
    if (hasRole(_account, _role) == false){
        roles[_role].bearers.push(_account);
        emit BearerAdded(_account, _role);
    }
}

/**
 * @notice Remove a bearer from a role
 * @param _account The address to remove as a bearer.
 * @param _role The role to remove the bearer from.
 */
function removeBearer(address _account, uint256 _role)
    public
{
require(_role <roles.length, "Role doesn't exist.");
require(
hasRole(msg.sender, roles[_role].admin),
"User not authorized to remove bearers."
);
address[] memory _bearers = roles[_role].bearers;
    for (uint256 i = 0; i < _bearers.length; i++){

```

```

        if (_bearers[i] == _account){
            _bearers[i] = _bearers[_bearers.length - 1];
            roles[_role].bearers.pop();
            emit BearerRemoved(_account, _role);
        }
    }
}
}
}
}

```

## References

1. Swan M (2015) Blockchain: blueprint for a new economy. O'Reilly Media, Inc.
2. Zhang L, Luo M, Li J, Au MH, Choo KK, Chen T, Tian S (2019) Blockchain-based secure data sharing system for internet of vehicles: a position paper. *Veh Commun* 16:85–93
3. Wu A, Zhang Y, Zheng X, Guo R, Zhao Q, Zheng D (2019) Efficient and privacy-preserving traceable attribute-based encryption in blockchain. *Ann Telecommun* 74(7–8):401–411
4. Zhang X, Chen X (2019) Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network. *IEEE Access* 7:58241–58254
5. Chen L, Lee WK, Chang CC, Choo KK, Zhang N (2019) Blockchain based searchable encryption for electronic health record sharing. *Future Generation Computer Systems*. 95:420–429
6. Maesa DD, Mori P, Ricci L (2017) Blockchain based access control. In: IFIP international conference on distributed applications and interoperable systems 2017 June 19. Springer, Cham, pp 206–220
7. Standard OA (2013) Extensible access control markup language (xacml) version 3.0. 24 Sept 2011. [http://docs.oasis-open.org/xacml/2.0/access\\_control-xacml-2.0-core-spec-os.pdf](http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf)
8. Pilkington M (2016) Blockchain technology: principles and applications. In: Research handbook on digital transformations. Edward Elgar Publishing
9. Khan S, Khan R (2018) Multiple authorities attribute-based verification mechanism for blockchain microgrid transactions. *Energies* 11(5):1154
10. Sahai A, Waters B (2005) Fuzzy identity-based encryption. In: Annual international conference on the theory and applications of cryptographic techniques. Springer, Berlin, pp 457–473
11. Goyal V, Pandey O, Sahai A, Waters B (2006) Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of the 13th ACM conference on computer and communications security, pp 89–98
12. Cruz JP, Kaji Y, Yanai N (2018) RBAC-SC: role-based access control using smart contract. *IEEE Access* 6:12240–12251
13. Zhang G, Tian J (2010) An extended role based access control model for the Internet of Things. In: 2010 International Conference on Information, Networking and Automation (ICINA), vol 1. IEEE, pp V1–319
14. Sultana T, Almogren A, Akbar M, Zuair M, Ullah I, Javaid N (2020) Data sharing system integrating access control mechanism using blockchain-based smart contracts for IoT devices. *Appl Sci* 2:488
15. Christidis K, Devetsikiotis M (2016) Blockchains and smart contracts for the internet of things. *IEEE Access* 4:2292–2303

16. Kshetri N (2017) Can blockchain strengthen the internet of things? *IT Prof* 19(4):68–72
17. Ding S, Cao J, Li C, Fan K, Li H (2019) A novel attribute-based access control scheme using blockchain for IoT. *IEEE Access* 7:38431–38441
18. Zhang Y, Kasahara S, Shen Y, Jiang X, Wan J (2018) Smart contract-based access control for the internet of things. *IEEE Internet Things J* 6(2):1594–1605
19. Banafa A (2017) IoT and blockchain convergence: benefits and challenges. *IEEE Internet of Things*
20. Alberto Cuesta Canada Role based access control for the ethereum blockchain. <https://www.techhq.io/8105/blockchain-development-rbac-ethereum-blockchain/>. Accessed 6 May 2019
21. Adhav P Attribute-Based Access Control (ABAC) in hyperledger fabric. <https://medium.com/coinmonks/attribute-based-access-control-abac-in-hyperledger-fabric-1eb81330f67a>. Accessed 26 Jan 2020
22. Cermeño JS (2016) Blockchain in financial services: regulatory landscape and future challenges for its commercial application. *BBVA Res Paper* 16:20
23. Decker C, Wattenhofer R (2015) A fast and scalable payment network with bitcoin duplex micropayment channels. In: *Symposium on self-stabilizing systems*. Springer, Cham, pp 3–18
24. Wang H, Chen K, Xu D A maturity model for blockchain adoption. *Financ Innov* 2(1), 12
25. Ali A, Latif S, Qadir J, Kanhere S, Singh J, Crowcroft J (2019) Blockchain and the future of the internet: a comprehensive review. *arXiv preprint* [arXiv:1904.00733](https://arxiv.org/abs/1904.00733)

# A Comparative Investigation of Consensus Algorithms in Collaboration with IoT and Blockchain



Alankrita Aggarwal , Shivani Gaba , and Mamta Mittal 

**Abstract** One of the large and emerging technologies nowadays is blockchain which has the impending potential to renovate the approach of contributing the large amount of data and information along with that it is also boosting confidence among the users. The drastic expansion in data creates security, privacy with assurance issues in the period of the Internet. The proposal is built to examine the nitty-gritty of blockchain technology and consensus algorithms also with the assessment of consensus algorithms and their area of relevance. With the appearance of Internet of Things (IoT), the enormous significant information is obtainable from the Internet. For doing cryptographic analysis and hashing procedures. This is a kind of challenge for the researchers to provide secure data without involving a third-party intervention for central environment. We can also reduce the transmission announcement expenditure of consensus for connected nodes with the assistance of restricted remembrance.

**Keywords** Blockchain · Consensus · IoT · Cryptography

## 1 Introduction

A consensus algorithm is a procedure in computer discipline to attain a union on a piece of sole information for the significance between scattered systems or processes. In consensus algorithms, there are different types of unreliable nodes and the network is designed to accomplish trustworthiness in a network. This chapter aims at solving the concern with the same issue of connecting and collaborating

---

A. Aggarwal (✉) · S. Gaba

Department of Computer Science and Engineering, Panipat Institute of Engineering and Technology, Samalkha 132101, Haryana, India  
e-mail: [alankrita.agg@gmail.com](mailto:alankrita.agg@gmail.com)

S. Gaba

e-mail: [sgsgknl@gmail.com](mailto:sgsgknl@gmail.com)

M. Mittal

Department of Computer Science and Engineering, G.B. Pant Government Engineering College, Okhla, New Delhi (under Government of NCT Delhi), India  
e-mail: [mittalmamta79@gmail.com](mailto:mittalmamta79@gmail.com)



a disseminated network computing using multi-agent systems and also the fundamentals of blockchain technology, IoT along with the consensus algorithms, their assessment of significant agreement algorithms, and their area of submission. To implement this realism, it can be presupposed that some of the processes or nodes may not be available and the exchanges will be lost. Therefore, consensus algorithms ought to be robust and fault-tolerant. The main requirement of such networks and algorithms is that most of the network nodes must respond perfectly but not a few. Some of the consensus algorithms support a lot of real global systems that are the synchronization of controlling drones, clock, smart grids, the ranking of the page, balancing load. Commonly known types of consensus algorithms are realistic convoluted error acceptance algorithm, evidence of hazard algorithms, and the delegated proof of stake algorithm, evidence of job, and the dual agreement. The consensus algorithm is categorized into three types: synchronous, asynchronous, and semi-synchronous. In synchronous consensus algorithm within a stipulated amount of time, messages much reach all the nodes when networks can have limited capacity whereas in an asynchronous algorithm this condition is not applicable and guarantee in producing the result but are inefficient and applications are also limited. Whereas a semi-synchronous algorithm establishes a relationship where messages can be delayed and be probabilistic within a time frame [1–3].

Various applications of the consensus algorithms are as given below:

1. To designate a particular node in some distributed environment as an organizer.
2. To decide that a distributed transaction has been properly committed to a database.
3. All the different technologies working in order along with a consensus algorithm.

## ***1.1 Consensus***

First of all, they let us take an idea of a distributed system that consists of networking of components that cooperate to achieve and solving a general objective. Here idea is to design the systems that are verifiable secure despite the omnipresence of distributed systems and their susceptibility to opponent attacks. The area of concern in consensus is to increase the influence of communication capacity on the computability of attainment of iterative fairly accurate consensus. The stretched topological circumstance on the networks for consensus is difficult to achieve [20, 21].

## ***1.2 Blockchain***

The blockchain technology has emerged as the prime technologies having a lot of possible prospective to convert the technique of distribution of a large amount of information and also by amplifying the faith. In today's world, it is a known fact that

the blockchain is the largest scattered account coupled utilizing bitcoin dependent on agreement algorithms for reaching the agreement among units. Block's chain preserves and uphold in a network unit by the interconnected peer-to-peer network. Here nodes can be considered as standalone systems that contribute as put in and perform a task on them and an amount is produced. It also divides partition in its entire workload between the balanced participants. If one of the participants goes down, there are many other available nodes form which data can be downloaded. A decentralized database is looked after by distributed computers on a one-to-one network where they preserve a replica to avert a sole end of the breakdown. With time over time, each updation and validation are reflected in all copies. The main purpose of using one-to-one **network is file allotment or file torrenting. In the traditional client-server system, it is** tremendously slow and reliant on the strength of the service as it also faces bowdlerization. Here is the comparison between the two scenarios as depicted in Fig. 1 [4, 5].

The design of combining one-to-one network with money expensive scheme has modernized economics business by the invention of cryptocurrency. **The main motivation for increasing approbation of blockchain is that:**

- (a) **It is decentralized and it is not a single owned unit.**
- (b) **The data inside is secure as it is stored cryptographically.**
- (c) The blockchain is unchallengeable so that nobody can meddle statistics.
- (d) The chain of blocks network is also see-through systems if someone wants to do that. However, it is still challenging to deploy IoT applications on blockchain systems. First, the architecture of an IoT-blockchain system needs to support an enormous number of IoT devices. Second, the consensus, a mechanism to ensure data integrity among peers in the blockchain, needs to be specifically

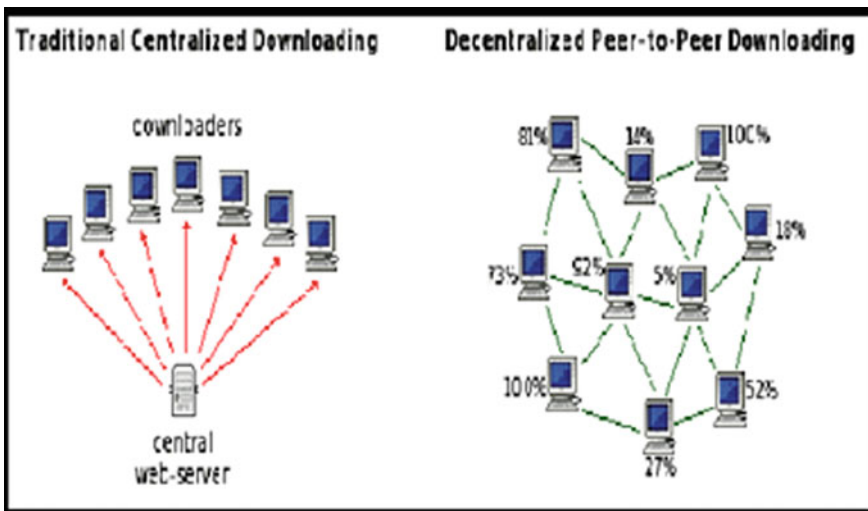
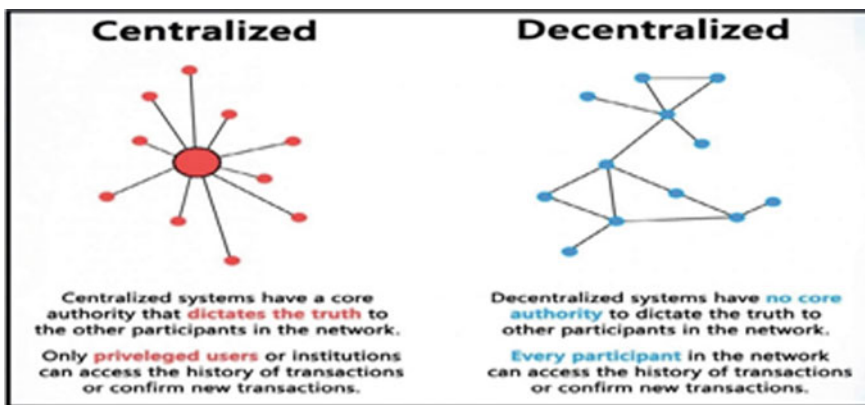


Fig. 1 Two scenarios of networks

**Table 1** Comparison between centralized and decentralized networks [6, 7]

S. No.	Traditional centralized client server network	Decentralized peer-to-peer network
1	Slow	Fast
2	One failure point	No one failure point
3	High bandwidth usage for the server	All downloaders are also uploaders
4	Is the core authority that dictates the truth to the other participants of the system	Decentralized systems have no such core authority
5	Privileged users have the authority to access the transactions or access new transaction	Every participant has the authority to access the transactions or access new transaction



**Fig. 2** Difference between centralized and decentralized systems [22]

designed for IoT blockchain because of the inadequate storage and the figuring out the ability of Inter of things devices. Table 1 depicts the various advantages of peer-to-peer network over traditional networks

Third, traffic modeling of a blockchain network is needed to realize high system performance in IoT blockchains. A deep understanding of a traffic model can reveal clues for optimizing communication processes and protocols. Shown below is the scenario of the centralized, as well as decentralized networks, are shown in Fig. 2.

### 1.3 Pillars of Blockchain

**There are some of the properties of** blockchain technology which have helped this technology to gain extensive praise. These are **Decentralization, Transparency, Immutability.**

(a) **Pillar 1: Decentralization**

Before the introduction of blockchain, a centralized body that stores the data and interaction is done exclusively with the unit to any type of information is required to receive the data. The second type of federal organization like banking where the change is stored and anyone receives amount after going to the bank location. Now after the invention of bitcoin and BitTorrent came along decentralization came into the process.

When we search for something on any web search engine, it is sent a query and sever bring the result utilizing the pertinent data called a simple client–server. But the centralized system is susceptible to many threats like these systems are centralized and data is stored in one place which makes hackers target some of the areas. One more problem area of the centralized systems is whenever there is an update in the system else the whole system would halt. The conventional client–server representation in Fig. 3 is an instance of this.

(b) **Pillar 2: Transparency**

**One of the** concepts in the blockchain is transparency means it give privacy as well as keeps system transparent. Any person of account holder identity as hidden through the complex cryptography and it is viewed as public address. For Example: “JOHN sent 3 THOMAS” it will be seen as “2MgKFP780hsfdjfgjjgHJSI sent 3 THOMAS.” Here a person’s identity is secure and all the transactions done can be seen by their public address. This type of accountability is needed by some of these largest organizations. If we talk about the **cryptocurrency**, if the public address of any of the large companies is known all the engaged transactions can be enquired.

(c) **Pillar 3: Immutability**

**Immutability is the perspective of** blockchain is that anything which has joined cannot be changed. It is valuable for the financial institutes and many misappropriate cases can be exposed by using a **cryptographic hash function** which takes a sequence of some duration and producing any sequence as output. The transactions are inputted and executed through a hashing algorithm. Let’s

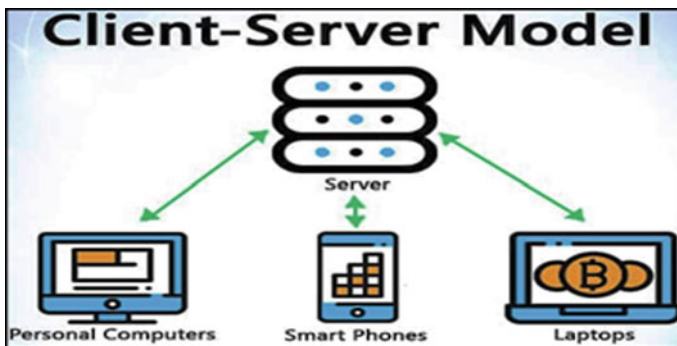


Fig. 3 A scenario of the traditional client–server system (centralized)

us exemplify cryptocurrencies like bitcoin which uses an encryption algorithm SHA-256 and produced an output of a fixed length. The blockchain can be implemented as numbers and a hash function pointing to its previous block or blocks and creates a chain. Here a pointer contains the address of the preceding chunk but also data inside the previous block. The feature makes blockchains so wonderfully dependable. Let us understand this scenario with the example: Because of the hashing properties and through what blockchains attain immutability, suppose a hacker attacks block number 3 and a little change in information will modify the hash significantly. Changes made in block number 2 can convert the hash stored in block number 1 and onwards. The impossible task is to change the chain.

(d) **Applications of Blockchain**

Proof of work algorithm is used for ensuring security in a network that is not trusty by comprising methods to ensure that attempt of the effort of drawing information is presented the chunk given by the miner. Using the different programs miners accesses the capacity to solve business-related algorithms. Any party can put forward a chain of blocks to the ledger and resources needed to a bogus agreement, besides it is valuable for looking after a dishonest party [8].

## ***1.4 Internet of Things***

The present era is of connected things on Internet having a large audience having provisions of performance and decisive responsibility in nearly all areas of health care, social, economic be it in education. This weeping growth in data is creating trust, solitude, and security issues in this age. The Internet of Things is now well known nowadays in an uninterrupted extension. Whenever a concept of smart or intelligent cities or similar applications requires communication among the nodes which generally require less or medium microcontrollers, IoT system also uses a communication system based on a client-server where different devices are recognized, considered as legitimate nodes, and are linked through servers having a large amount of calculation and storage space. Connected devices contain an exclusive individuality linked through the Internet. Due to the increasing population of several IoT devices and nodes, this communication strategy is not being used in present scenarios. The first scenario is to use centralized servers to make the link between billions of devices and require maintenance and it results in high cost. The second scenario is to use decentralized methods that may answer the high costs of and also provide solutions to issues related to large IoT systems. In this calculative authority and storing necessities mutual between the strategy in the network. The communication in the one to one network tries to solve issues like isolation, protection, legalization, and to make an agreement. A rational database keeping all the information must be needed for all the nodes to operate within the cooperative nodes. An effective explanation for this to use blockchain technology as discussed above as

uninterrupted increasing of the blocks or public records are added. Here the scattered can be increased and preceding blocks cannot be removed without replicating the complete chain without any elevated expenses. Also, every contributor must keep a replica of the blockchain and a fresh chunk will be inserted in the sequence simply after a consensus among contributors is acquired. The central catalog which is the operation on the Internet and uses the client–server arrangement of structural design where the client can modify information on a central server with permission. Control over the database can be maintained by essential power. Here the major concern is the protection of the network. For example, it is the central system any of the nodes distorted are at the same time at risk. But a database in blockchain information of each node is updated to make sure that a consensus is built with all the nodes for providing security to the complete network. But in the blockchain scheme, the nodes are connected through diverse topologies maybe it stars or one to one in a distributed system and each node tries to be connected to be part of using agreement algorithms. Two main concerns by using this arises are:

- (a) To make the complex consensus algorithm effective, all the resources which are in a limited number must be chosen intelligently
- (b) To keep the power consumption low, the network weight should be kept minimum as required. So there must be focused research on the association of realistic methods to make sure the agreement IoT-based system.

The accountability of information technology is guaranteeing the solitude and safety at gigantic arriving data outstanding for the progression of the Internet of Things and chain of blocks in more approaching years. A trustful network for decentralized or distributed surroundings without calling a faithful third party can be a technical situation and challenge for researchers. With the appearance of IoT, there is a large amount of information available on the Internet which reduces the trust over the data, security, and privacy matters [10, 11].

## 2 Literature Review

AliDorri et al. [1] proposed a system in which a smart IoT-based system can be made flexible to security attacks along with packet delays and expenses are also reduced. It uses a lightweight scalable blockchain that provides end to end security too.

Abdellatif et al. [2] suggested that in healthcare there are certain emerging technologies which are moving the patient care industry. There are different types of patient data from different resources newer methods to improve the radical medical services can be used. They presented a smart healthcare system which used edge computing and blockchain technologies to discover the epidemics, monitor, and emergency response. This model permits the exchanging the national as well as international secure data of medical between the health care related. A blockchain-based system is developed which helps in optimizing the data sharing and also fulfill the diverse levels of Quality of Service (QoS).

Lin et al. [3] proposed an analytical model in which a user entry method can improve the network performance by scheming the user access of all the mobile applications used by the user thereby using a multi-stage interference occurred by a portable device client and if any attendance of the client in the chain of scam to decide the admission of the client.

Li et al. [4] proposed a method based on neural networks models which supported the large data for using the high-end IoT devices so that multi-agent models can be used with the help of scalable fully distributed algorithms which get better the detection of attacker and performance is improved.

Hosseini et al. [5] proposed an integration of sources of renewable energy. Enquiring about the concepts of environmental resources technology and a large number of consensus algorithms have been investigated and also a discussion about the public, private, and consortium blockchain so that a large number of problems can be solved using the above combination.

Kenyeres et al. [6] implemented and tested in nesC a distributed algorithm on wireless sensor networks along with a consensus algorithm by creating a derivative to enhance the development of hardware devices in which a time planned admittance to various devices and nodes are allowed so that there is no collision is done.

Ni, X et al. [7] experimentally designed a practical and dependable tally system that solves the large database preservation costs using a CNN, blockchain employing a classification method and reducing feature extraction.

Wu et al. [8] proposed a lively organization, arrangement of the consensus in a blockchain necessary because IoT application is highly dynamic. Also, an Internet of things network node is frequently utilized again by applications in various blockchain because the IoT node switches to traverse consensus in the various blockchain.

KuoLi et al. [9] threw light on the consensus algorithms in a chemical nuclear reactor system for consensus problem for a group of the indistinguishable non-linear moment in a moment of hindrance by multi-agent systems.

Liu et al. [10] presented a hyper ledger fabric framework based on blockchain with IoT access control environment. There is a combination of the attributed-based access control (ABAC).

Mittal et al. [11–13] discussed about the role of big data in IoT, blockchain and maintaining consensus algorithms with the help of machine learning algorithms.

Chaudhry et al. [14] proposed a distributed ledger that is used in many applications and started implementing the blockchain solutions for their application and services. It is done by studying the gap between designing and evaluating to achieve a better consensus algorithm so that the consensus procedure can be made between the peer nodes of a blockchain network.

Pu et al. [15] investigated the bitcoin blockchain which is a storage, unchangeable, correct and exceptional record on net in a decentralized system. But there are certain disadvantages like Bitcoin and other virtual currencies function as approximate instruments rather than as mediums of exchange for illegal business.

Sabato Manfrediet al [16] designed a fast-dynamic consensus algorithm gain when a different type of delays which affect the multiple hops in a wireless sensor

networks by employing AODV protocols to reduce the packet collision with the help of simulation experimentation.

Sagirlar et al. [17] proposed and designed a hybrid IoT for decentralizing with the help of multiple blockchain for IoT specially designed for Hybrid-IoT architecture. It consists of many PoW blockchains to realize distributed consensus between IoT devices. In addition, framework is inter-connector to accomplish all the transactions between sub blockchains.

Singh et al. [18, 19] proposed IoT dependent intelligent robot for various disasters monitoring and prevention with visual data manipulating as well as the application of iCloud and wireless sensor network in environmental parameter analysis for maintaining the consensus environment.

Shi et al. [20] suggested that in ecosystem of IoT every unit operational from identification to communicate to achieve the performance. Also studied showed that IoT has high potential to be one of the most popular paradigms in the era of net computing also it has been discussed that IoT deployments can be that large scale, large or medium scale for the implementation of connected cars or smart cities and renamed as Internet of Multimedia Things. Such networks have a great capacity for shared trust between stakeholders.

Zoican et al. [21] presented a paper that tells the performance of the algorithms used in a blockchain system using the Internet of Things. Such a scenario emphasis is on the time requirements are minimized. An IoT node is adapted for different consensus algorithms using the ContikiIoT operating system and consensus was achieved in few fractions of seconds. Also focused on the assessment of the performance of consensus algorithms used by a blockchain system and Internet of Things network so that the time duration for achieving this is less by using a combination of consensus algorithms which evaluate in diverse scenarios. A hybrid solution is proposed so that any type of IoT node can adjust in a variety of consensus algorithms and done using ContikiIoT operating system.

Tao Dong et al. [22] tell that in a distributed computing system an average consensus algorithm is which is dependent on the functional Laplace noise and differential privacy. A novel differentially private average consensus algorithm is proposed by them to preserve the privacy of the state of each agent in the whole process of consensus computation for the convergence and consensus condition for network agents is checked.

Wenbo Zhanget et al. [23] proposed an Industrial Internet of Things a lightweight scenario that uses a data consensus algorithm an improved blockchain technology for the secure data communication where the correctness of data, security, and consistency of IoT is also verified.

Wang et al. [24] presented a paper on present technologies with an importance on the IoT and blockchain applications.

Yadav et al. [25] combined the idea of big data and machine learning and where IoT, blockchain is an important responsibility in areas likes healthcare, social, education, political in the present scenarios. It was discussed the basics of blockchain technology, consensus algorithms, comparison of consensus algorithms and areas of applications which is a challenge for researchers.



Zhang et al. [26] suggested an IoT security-based blockchain model so that data storage can be done, transmission encryption using consensus algorithms to solve the security problem of IoT to build a trust between devices for dependable data transfer.

### 3 Objectives of Work

The prime objective of the work is to list and summarize all the consensus algorithms available in the market to summarize their areas of application. After the judgment of the work of all the algorithms, it can be concluded how and which algorithm is best suited for the application to IoT and blockchain applications for decentralized network.

#### 3.1 Proof of Work (PoW)

Application of PoW is bitcoin where it is used as one to one e-payment system. The role of the consensus algorithm is to for solving the two peers in a decentralized system thus making a balance between the nodes. Here blockchain or any other application can control the problem of sending the trusted data and not send data to untrusted one shows how a consensus mechanism solves in disseminated circumstances. The issue of consistency has laid the foundation for the security of the bitcoin system. Algorithm for fitting consensus algorithm into the blockchain technology is as given as follows:

- (a) The new operation is broadcast to the whole network of candidates.
- (b) Each candidate finds a possible explanation and broadcasts the chunk to the entire network.
- (c) The remaining candidates verify the chunk of the block.
- (d) Any transaction is right then the hash joins the obligation and the longest block with truthful nodes will construct the next block.

**Pros and Cons:** The advantage of PoW is a higher degree of decentralization where the algorithm is easier to float and nodes can enter freely and a higher degree of decentralization. If there is certain damage to the system, it will be high therefore the security is very high. The type of trust in a piece of equipment provided by the producers of chunk solving hash function. In this process, no human involvement is required, and nodes achieve consensus without exchanging extra knowledge. Along with advantages some disadvantages are Pitable Expansion, extended verification time, sometimes waste of resources.

### 3.2 *Proof of Stake (POS)*

In this algorithm, the procedure is to select a leader randomly by a suitable candidate also called miner follows a fixed procedure and the other candidate releases the new chunk or block. Here the user of a group of users controls the accounts for a longer time. The process of impartial qualifications procedure selects the next candidate dependent on the percentage of contribution of each person in the process of consensus. The basic reason for selecting this idea is to if a candidate owns a large number of shares higher returns will be in the form of dividends so there is no additional requirement of any such resource. In this way, the blockchain properties have the usual price increases in this financially viable society.

**Pros and Cons:** The above consensus saves energy, as well as the confirmation of chunk, is quick as mining of nodes does not require any actual calculations, and proof of the calculation is done a required thing which lessens the consensus time. The main disadvantage is the bad security system as many humans are involved which increases the loopholes in security. Also, there is a need for this procedure to help in moving to the final position. The book-keeping problem of nodes and withdrawal by nodes in the mentioned algorithm is not reducing the cost of power along with the reduction in encouragement for miners are very limited. The attack called nothing at stake attack is used because of success if high of fork attack and it can be initiated.

### 3.3 *Delegated Proof of Stage (DPOS)*

In this algorithm, the holder is allowed to polling of nodes and surrogate for authentication and bookkeeping. It is a variation of POS in which the node selects representative nodes validated and allocated by the representation. Here if bit share is used it allows only three categories of persons to cast vote: witnesses, delegates, workers. People in witnesses will be paid if they are deal with business and maintain blockchains. The delegates cannot be updated if an initiate request for updating bit share. The category of workers can recommend whatever they wanted to do and will be paid only if the project is voted. In this, if there are enough of the blockchain properties then the majority of the votes are with you. Here the everlasting node having taken the vote and top of all the witnesses are saved. Several witnesses are rotated at different intervals and have to accept more than fifty percent of votes. All the witnesses of the block are paid for the number of blocks they produce. The identity of a witness may lose if they do not produce any block and hence, they will have no revenue. This algorithm is simple and straightforward and quite efficient also as it neither requires node verification nor requires mining.

**Pros and Cons:** This algorithm is considered as proficient as it lessens the number of participating and accounting nodes for the second stage verification. It requires only the main nodes to validate the network. The algorithm is highly scalable for the next level of authentication along with the faster blocking out in a network. The main

disadvantage is that consensus procedure based on token and it does not apply to many business requirements. Also, by reducing the particular number of verification nodes but not the global node, the algorithm deviates and creates a conflict of the theme of blockchain by the introduction of centralization.

### 3.4 *Practical Byzantine Fault Tolerance (PBFT)*

**The algorithm** helps in achieving an adequate consensus despite malevolent nodes of the system fails or propagates wrong information to peers' nodes in the network. The idea behind using this is to protect the disastrous system failures by extenuating the role these types of bad nodes play. PBFT is situation machine imitation duplication algorithm where examination model as a state machine and it performs replica duplication at diverse nodes of the scattered system. A duplicate of every state machine saves the state of the service implements the process of the service. The collection of the replicas is represented by an uppercase letter  $R$  where each copy is represented by an integer from 0 to  $|R|-1$ . If the copies of  $|R|$  are made then it will not help in improving the performance along with trustworthiness. The algorithm operates in a disseminated form and bears byzantine error. The primary node sends a calling request made by the client and master node multicast the request made by the client to the resultant node and executed and the reply is sent to the client again. The client node receives the  $f + 1$  reply that mean the client gets the requested data. In this algorithmic process, to set up the network all the nodes requirement should be known in advance and they cannot change while in execution enthusiastically which is mandatory in public chaining.

Pros and Cons: The network remains stable without a fork and there is a less range of application as it has limited application in market chaining whereas the system is poorly scalable and several nodes are fixed so it cannot deal with any open environment and also the network has low fault tolerance. The number of failures of nodes in a system shall not go beyond one-third of the nodes of the entire network [12, 13].

### 3.5 *Proof of Burn (POB)*

In this algorithm, the rather than investment into high-priced hardware equipment the validating nodes burn the coins to the area which is unsuspendable or place where they cannot retrievable sometimes known as eaters address and validators by the process of the random selection process can have an opportunity to excavate system based on a random selection of nodes. The idea proof-of-burn consensus is that the user burns the cryptocurrency for the long-term promise to the coin by blazing and receiving the gains at later stages because they are ***taking a short-term loss in exchange for an extended-term gain***. Here the miners might burn the native

currency just like bitcoin and if more coins they burn then there are more chances of being a selection for mining the next block. This algorithm wastes resources and mining power go to those who are willing to burn more in the form of hardware and electricity costs. Every transaction is recorded on the *blockchain* so that it ensures that coins cannot be spent again and the user burned the coins will be issued a reward.

**Pros and Cons:** Besides the burning of coins can be seen as less resource-intensive because the main resource is being used by the person's willingness to delay profits as if a user is patient enough for the gains this algorithm is best suited for him. Over time, the user of PoB will be able to receive rewards or he can earn privileges for mining the network. Similarly, if a user burns more coins, he will have a larger chance of mining and earning rewards.

### 3.6 *Proof of Elapsed Time (PoET)*

In this consensus, computing challenges are solved for the selection of random leader and it is designed by Intel and was released as a reference manual for programming the Software Guard Extensions (SGX). It is used in many private chaining blockchains, for example, Hyperledger *Sawtooth* which depends on a randomized timer system for network participate rather than making use of mining hardware used in Proof of Work (PoW). Here the important point to be noted is that every participating blockchain node is required to stay or a chance of chosen and which unit wins is the winner of the new clock and helps to invalidate it.

### 3.7 *Proof of Authority (PoA)*

It is an algorithm dependent on the reputation of trustworthy parties in a blockchain network. It was discovered by Ethereum who was also a co-founder and former CTO of *Gavin Wood in 2017*. The algorithm is based on the value of the identifiers, in a systems block and a network. Here validating nodes do not keep on stake the resources but in return stake their own identity and status. PoA blockchain networks are secured by trustworthy parties by the validating nodes chosen arbitrator. The algorithmic model is also scalable all the transactions are verified by previously accepted network participating nodes. Proof of Authority consensus algorithm is applicable in business networks and supply chain networks as the identification of all the nodes are acknowledged and trustworthy [14].

**Table 2** Summary of different consensus algorithms [16]

Consensus algorithms	Advantages	Disadvantages
Proof of Work (PoW)	<ol style="list-style-type: none"> <li>1. System of nodes are open</li> <li>2. Freedom of nodes are of high degree</li> <li>3. Steady and secure</li> <li>4. Very high level of decentralization</li> </ol>	<ol style="list-style-type: none"> <li>1. Weaker extensibility</li> <li>2. Near to the ground performance</li> <li>3. Hardware waste of resource</li> </ol>
Proof of Stake (PoS)	<ol style="list-style-type: none"> <li>1. Less power</li> <li>2. Very high level of decentralization</li> <li>3. System of nodes are open</li> </ol>	<ol style="list-style-type: none"> <li>1. Tough execution process</li> <li>2. Safety violation</li> </ol>
Delegated proof of stake (Dos)	<ol style="list-style-type: none"> <li>1. Less power</li> <li>2. Tall performance</li> <li>3. Definiteness</li> </ol>	<ol style="list-style-type: none"> <li>1. Fragile amount of decentralization</li> <li>2. Blocked node system</li> </ol>
Practical byzantine Fault Tolerance (PbfT)	<ol style="list-style-type: none"> <li>1. Higher performance</li> <li>2. Definiteness</li> <li>3. The system is highly secure</li> </ol>	<ol style="list-style-type: none"> <li>1. Fragile amount of decentralization</li> <li>2. Blocked node system</li> <li>3. Short fault acceptance</li> </ol>
Proof of Elapsed Time (PoET)	<ol style="list-style-type: none"> <li>1. Node is randomly chosen for a certain period</li> </ol>	<ol style="list-style-type: none"> <li>1. Random leader election</li> </ol>
Proof of Authority (PoA)	<ol style="list-style-type: none"> <li>1. Nodes are validated by arbitrators chosen</li> </ol>	<ol style="list-style-type: none"> <li>1. No Random selection</li> </ol>
Proof of Burn (PoB)	<ol style="list-style-type: none"> <li>1. Burn coins by sending them address</li> <li>2. Expensive hardware used</li> </ol>	<ol style="list-style-type: none"> <li>1. Waste of resources</li> </ol>

### 3.8 Proof of Capacity

This algorithm the validating nodes are required to spend the hard disk drive space as an alternative to investing in high-priced hardware or blazing coins. If there are more than enough hard drive space validators, then the chances of selection for mining the next block of chunk and incentive of earning and reward based on the selection are increased [15]. Table 2 given gives the comparison of different types of algorithms.

### 3.9 Hybrid Consensus

There are many hybrid consensus and regression of the PoW consensus that is offered for solving the public chain project. The table also gives a summary of the various consensus mechanisms currently applied for the solving and application of many public series projects. After comparing the agreement mechanisms of the IoT, chaining of every procedure ranging consumption of reserve, amount of centralization, throughput, performance, transaction rates, and their authentication time and

**Table 3** Major projects and their consensus mechanism [16, 17]

Public series project	Consensus mechanism designed
Aelf	In this, a combination of Pow and Pos is done and the main sequence adopted is the proof of stake procedure and the side surface series adopts the Proof of work agreement procedures. The problem is that Pos supervision is high in cost and is applicable to the main sequence and surface sequence uses the PoS to operate securely and separately
Zilliqa	In this, a mixture of Pow ad Pbft is taken. The safety of the Pow agreement procedure to validate the nodes is used for decision making and handed to the Pbft consensus mechanism
Aeternity	In this blend of Pow and Pos is done. The Pow system generates blocks and chief decisions are completed by assigning privileges to the token holders by the Pos mechanism
Bytom	In this a unification of Pow and artificial intelligence ASIC Chip-Friendly PoW Consensus Procedure

transaction confirmation time [23–25]. Some of the projects on which consensus algorithms are used are shown in Table 3.

The above-discussed algorithm is unique in design but due to security, they are not able to protect the Pow consensus mechanism. It can be concluded that despite large costs Pow consensus can be applied to the open and independent public chain environment but can be worn in most important decision-making methods like the selection of change and fork in a central network system. Here we have discussed the famous consensus algorithm which can be applied to the blockchain in terms of performance, requirements, and conditions along with their advantages and disadvantages.

## 4 Problems in Existing Work

### 4.1 Trust Issues

The blockchain environment network conforms to the byzantine general’s problem. A model should be constructed which must be suited to a general open business environment which is based on a realistic and enhanced agreement method based on Byzantine fault tolerance to solve diverse trade to increase the trust.

### 4.2 Delay

Some of the consensus algorithms also tell the chronological performance of units to optimize the protocols to solve the problem of lower agreement achievement velocity and huge traffic when facing faulty nodes. Past recognition can covert the agreement

procedure vigorous to resolve the problems related to diverse trade in the coalition sequence consent mechanism in the open industrial surroundings.

### 4.3 High Latency

As it is known fact that for the distributed payment systems various consensus algorithms are proposed for the byzantine general's problem, the main problem of high latency is introduced to accommodate all the nodes within the network so that they can be in touch in sync with each other. By using the principal technology of blockchain getting more and more awareness day by day applied to point distributed system and for solving the consensus of each node the agreement procedure scan be used. Combination of blockchain principles and applications of consent algorithms in a fault-tolerant technology in the area of distributed computing. One more problem that occurs is for solving the economic dispatch problem with the consequence of random delay where the algorithm is distributed and the supply-demand balance must always be satisfactory. Here the investigation by the algorithms must be done for the responsibility and impact of random time delay. The problem can be solved based on how much allowable delay bound for the efficiency of future algorithms. Another problem occurs when resource-controlled devices are used for sensing and also for doing judgment for applications like smart cities to ecological observation. Such devices are associated to generate real-time distributed networks known as the Internet of Things (IoT) coupled with edge and fog computing. In decentralized systems, the dependencies are ignored where the proof of work is gaining recognition for the security solutions but because of limitations of resources. This is also restrictions or constraints of the devices most of the time proof of work is not appropriate for blockchain-based security solutions. A consensus algorithm must be made which can suite both for personal and authorized blockchains in which there must be a proof of validation rather than a proof of work that can be used for when networks scale and want to sustain for a longer duration. The finite-time average consensus method can be used as an information fusion tool to construct the accurate Newtonian global gradient direction with some appropriate assumption such a method can be considered as a distributed implementation of the classical standard Newton method and eventually has a quadratic junction rate. The better supremacy needed an algorithm for the best convergence speed and performance must be devised may be through the modeling and assessment experimentation [18].

## 5 Simulation Study

After studying different types of algorithms Ontology introduced its VBFT which is a combination of Pos, VRF, and BFT consensus algorithm in recent years has gained momentum over the past two years. Ontology introduced its VBFT consensus

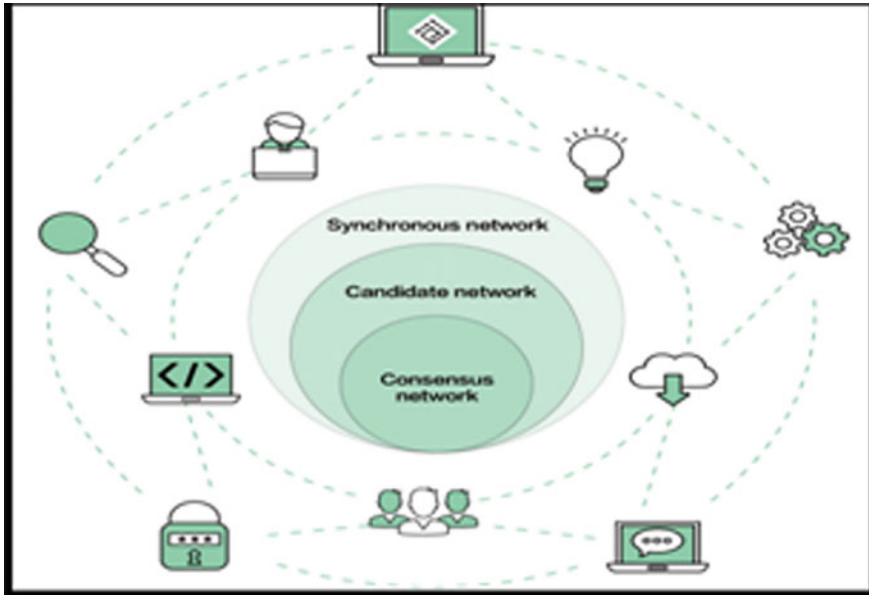


Fig. 4 The scenario of OVBFT consensus

algorithm in recent years and the project is continuously being elevated this is the great reports for the current algorithms in the blockchain industry are using proof of work and Byzantine fault tolerance which are the conventional algorithms used in public chaining.

In the future, the ontology-based on the VBFT algorithm is going to replace the old and obsolete methods and aims at solving problems. The above is the scenarios of ontology-based consensus algorithms as depicted in Fig. 4 [15].

### 5.1 VBFT Algorithm Based on Ontology

VBFT is an agreement procedure built with the combination of proof of stake, Verifiable Random Function, and Byzantine fault tolerance. VBFT is the main consensus algorithm of the ontology-based Consensus machines therefore named OVBFT. Ontology’s first part consists of mainly two components. The consensus network consists of the consensus nodes that are accountable for maintaining the blockchain, creating a block, assigning consensus blocks to synchronous node networks, and also looking after requested transactions. The second element of ontology’s center system is the consensus applicant network which remains synchronized with the consensus net and endlessly update the consensus blocks on the blockchain. This all happens in real-time which help ontology achieve top performance without sacrifice. The contender networks try to authenticate consensus blocks and scrutinize the



consensus network position which helps managing of the ontology network. The consumer and producer of the network can manage the size of the whole network via a smart contract. In the ontology network, OVBFT selects candidate units. After the block confirmation and authentication nodes completed by selecting a group of nodes ensuring certainty and equality to all users.

OVBFT algorithms are a model of the semi-synchronous network model type. OVBFT algorithm based on ontology is setting a new standard for blockchain and IoT consensus when we talk about the governance of IoT, autonomous and the administrative authority then it is with the blockchain-based intellectual circumstances framework which is based on IoT hardware solutions also called Chains of Things(CoT)working on projects with the help of the projects multiparty working group can select the essential and suitable governance algorithm that can convince the transaction and interaction between IoT, other things, blockchain and the persons in the research development of helping the factual financial system. CoT is the co-construction ecology of ontology. The feasible technological explanation of ontology communications is to construct and put into practice the main network technology architecture. The OVBFT consensus algorithm can meet the current intelligent cabinet integration scenario system and will also serve as the first chain of COT to build blockchain infrastructure based on the first batch of intelligent IoT infrastructure. It will formulate significant assistance and explorations to bend the barriers between intelligent hardware and to enhance the COT arrangement environment. The expansion of the majority of the agreement procedures continues to chase the tendency for improvisation in performance, extendibility, and transference of public networks. OVBFT agreement based on ontology alike aims thereby improving the efficacy and performance of blockchain systems. In the coming years, it will evident that all the jobs went with ontology and high performing agreement programs jobs. This algorithm aims at improving the performance and scalability of all public chaining whereas another guarantees the uncertainty and even-handedness of a consensus network and also help the app developers to create by removing the limitations of incompetent algorithms. Major improvements are being included in OVBFT to keep track of the new consensus algorithms which help in the sustainability of the long run and larger scale. The problem of the unpredictability and unsteadiness among the nodes in most of the inconsistent consensus algorithms can be improved by the reliability of data sets in a distributed system based on ontology VBFT for unreliable nodes can be built. As we have discussed earlier that consensus algorithms based on fault-tolerant capability categorized as crash error acceptance which is dependent on the node crash feedback. When the nodes are down and they violate the protocol then the crash fault tolerance will ensure the reliability of the closed distribution system of any organization. With the BFT algorithm, the system is reliable as errors come in a pre-defined ratio of nodes, therefore, fault tolerance algorithms such as OBFT suitable in open distributed systems. Before starting a new iteration of consensus of all nodes in the network ultimately recognize the agreement result by the corroboration unit. This is done to ensure that the algorithm runs effortlessly, rapidly also constantly. Ontology Consensus Management Smart Contract is responsible to build a consensus network that is built runs everlastingly for updating

the OVBFT algorithm. The users using the platform are always up to date whenever they are connected to the network and such networks contain very few malicious nodes. In recent years, the ontology-based algorithms have enhanced the association by escalating the number of agreement units ranges from ten to more.

The verifiable benzenes fault tolerance algorithm implements the addition of the consensus algorithm by a selection of a subset of nodes in the verifiable random function by enabling and definiteness of the resistant offensive characteristic of the algorithm done by unpredictability or randomness and PoS and the last stage is achieved by BFT alike algorithm. The VBFT algorithm is closely incorporated with the power representation of the blockchain network and provides decentralization and network hierarchy via random verification if it is compared with other consensus algorithms. Testing results have shown that the OVBFT algorithm shaped grades that surpass the results of other conventional public chains in terms of competence, authentication time, resource expenditure, and management.

The OVBFT consensus system is divided into three levels which are synchronized with the COT control authority model.

- (a) **Synchronous network:** The prime body of the CoT blockchain network which voluntarily and autonomously synchronizes and supervises the financial controls, synchronizes blocks, and the complete COT ecosystem. Synchronous networks always maintain the broader sustainability of decentralized cross-chain ecosystems.
- (b) **Candidate network:** In this, there is a set of candidate nodes that get together for the requirement of performance and can contribute to the agreement with supervision in consensus implementation association. Such candidate networks can at the same time administer the consensus implementation of multiple COT ecosystems.
- (c) **Consensus network:** This network is a purposeful network that takes part in the decentralization of the blockchain and also helps in reaching the consensus execution. The consensus network is also accountable for the implementation of a sole chain of ecology.

The definite functions of different networks of the first chain of COT are as given below:

Based on the diversity of business scenarios supported by the intelligent Internet of Things, the blockchain platform supporting diverse intelligent hardware also needs to have the characteristics of business diversity on the chain. Blockchain technology needs to meet different business characteristics and needs to find a balance between security, scalability, and performance. To meet different business characteristics, multiple blockchain network support is required. Therefore, the COT ecosystem requires a multi-chain solution. The VBFT consensus algorithm is one of the foundations for the establishment of a COT cross-chain solution.

The rules are as follows:

- The node worker operates on the COT node and one node operator can function on numerous nodes of the COT ecological sequence.

- A node operator can operate only on one node in a COT ecosystem.

In a distributed identity system, the cross-sequence business is based on atomic swap and subchain knowledge with COT as a link and for realizing the implementation of cross-chain node deployment in the COT multi-chain ecosystem as an operating platform is used. In the present era, the work is on for invention on an amalgamation of algorithms and a mixture consent method is a broadcaster follow a line of investigation and it is new. New method to make use of well-groomed connections to construct refined consent regulations. The prime function of the agreement applied to find a newer intruder attack will help in removing and recognizing the inadequacy of the present consensus algorithm. Public applications like the license chain, chargeable switchable, and in business scenario the applications involving the requirement of throughput, assumptions on security different types of essential consensus procedures are used [13, 14].

The algorithmic steps of OVBFT are listed below:

1. The first step is that the blockchain network node earliest applies for contribution in the network consensus through the stake.
2. The second step is to randomly selection of nodes from all consensus nodes by using a verifiable random number.
3. The third step is to propose candidate blocks and verifies the associated candidate.
4. In the fourth step after getting the support and approval of the verification grades, the consensus is achieved.

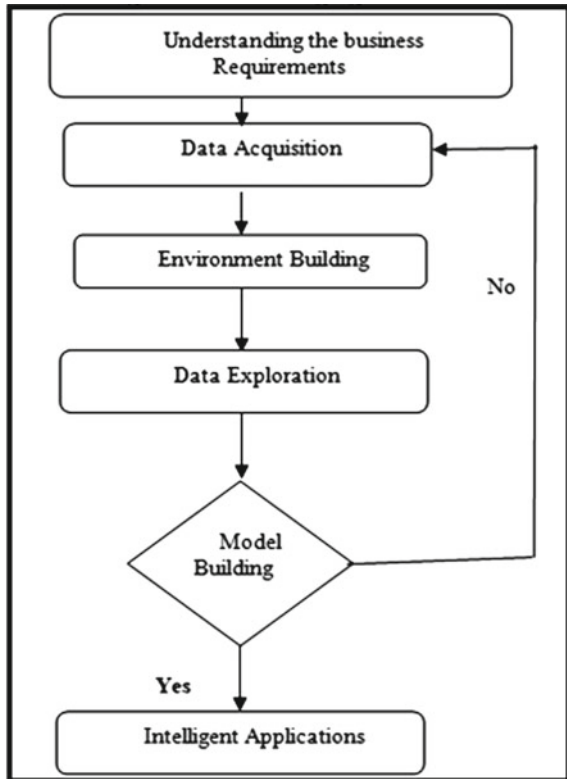
## 6 Proposed Methodology

After going through all the work in the previous years for developing the efficient the proposed methodology which can be applied to any application of the blockchain and IoT network which can be solved using a machine learning algorithm.

The software that can be used is python and datasets for the same can be created which can be collected from the various databases and after cleaning and analysis of the data acquired. This is depicted process in a flowchart as shown in Fig. 5. The following are the steps of the proposed algorithms are as follows:

1. Understanding the business requirements and requirements of the network to be established consisting of nodes (i.e., peer-to-peer nodes)
2. The next requirement is to acquire and understands the data. It consists of a collection of data from various sources. For example, collecting data from the transaction done by the customers in a blockchain network and that data might be stored in some database.
3. That data is pipelined and classified as streamed or batch data or it may a high or low-frequency data.
4. To provide the data the environment, i.e., it can be set up on-premises or it is a cloud-controlled environment. Data flow will be within the environment and

**Fig. 5** Algorithmic process of model building



will flow in a database or a data reservoir and it can be categorized as a small, average, or big data. This will help the network to update automatically.

5. Data acquired is the wrangling or it needs exploration or cleaning. It includes also differentiate between structured or unstructured data. Now the data needs to be validated, cleaning and how it can be visualized,
6. Now the modeling can be done with the help of feature engineering, built model can be trained by various algorithms best suited.
7. The built model can be evaluated by cross-validation and by applying various testing techniques.
8. After testing is done, the model is ready for deployment at the customer side with the customer acceptance. It can be controlled by scoring, performance testing, and monitoring procedures.
9. All these steps can be controlled with the help of web servers, storing the model, and intelligent applications.

## 7 Results and Discussion:

After going through and studying various types of different consensus algorithms are measured as the following parameters shown in Fig. 6.

- (1) The access types: public or permissionless
- (2) Decentralization: High, medium, Low
- (3) Scalability: High or Low
- (4) Latency: High, Medium, Low

Consensus method	Access	Decentralization	Scalability	Latency	Output	Adversary tolerance	Computing overhead	Network overhead	Storage overhead
PoW	Public, PL.	High	High	High	Low	<25% Computing Power	High	Low	High
PoC	Public, PL.	High	High	High	Low	<50% Storage Space	Low	Low	Very High
PoET	Private, P. or PL.	Medium	High	Low	High	N/A	Low	Low	High
PoS	Public P. or PL.	High	High	Medium	Low	<51% Stakes	Medium	Low	High
DPoS	Public, PL.	Medium	High	Medium	High	<51% Validators	Medium	N/A	High
LPoS	Public PL.	High	High	Medium	Low	<51% Stakes	Medium	Low	High
Pol	Public PL.	High	High	Medium	High	<51% Importance	Low	Low	High
PoA	Public, PL.	High	High	Medium	Low	<51% Online Stakes	High	Low	High
Casper	Public, PL.	High	High	Medium	Medium	<51% Validators	Medium	Low	High
PoB	Public, PL.	High	High	High	Low	<25% Computing Power	Medium	Low	High
PBFT	Private, P.	Medium	Low	Low	High	<33% Faulty Replicas	Low	High	High
dBFT	Private, P.	Medium	High	Medium	High	<33% Faulty Replicas	Low	High	High
Stellar	Public, PL.	High	High	Medium	High	Variable	Low	Medium	High
Ripple	Public P.	High	High	Medium	High	<20% Faulty UNL nodes	Low	Medium	High
Tendermint	Private, P.	Medium	High	Low	High	<33% Voting power	Low	High	High
ByzCoin	Public, PL.	High	High	Medium	High	<33% Faulty Replicas	High	Medium	High
Algorand	Public, PL.	High	High	Medium	Medium	<33% Weighted Users	Low	High	High
Dfinity	Public, P. or PL.	High	High	Medium	N/A	N/A	Low	N/A	N/A
RSCoin	Private, P.	Low	High	Low	High	N/A	Low	Medium	High
Elastico	Public, PL.	High	High	High	Low	<25% Faulty Validators	Medium	High	High
OmniLedger	Public, PL.	High	High	Medium	High	<25% Faulty Validators	Medium	Medium	Low
RapidChain	Public, PL.	High	High	Medium	High	<33% Faulty Validators	Medium	Low	Low
Raft	Private, P.	Medium	High	Low	High	<50% Crash Fault	Low	N/A	High
Tangle	Public, PL.	Medium	High	Low	High	<33% Computing Power	Low	Low	Low

Fig. 6 Comparisons of different consensus methods

- (5) Output: High or Low
- (6) Adversary Tolerance: In the range of Nil-above 50%
- (7) Computing Overhead: High or Low
- (8) Network Overhead: High or Low
- (9) Storage Overhead: High or Low

On the basis of blockchain comparisons on the various criteria as shown below in Fig. 7.

- (1) Implementation Criteria
- (2) Hyperledger Fabric
- (3) Hyperledger Sawtooth
- (4) Ethereum
- (5) Corda
- (6) Iota

Major consensus algorithms comparison on the basis of type, throughput, scalability, finality, adversary tolerance, Vulnerability shown in Fig. 8.

Implementation	Hyperledger Fabric	Hyperledger Sawtooth	Bitcoin	Ethereum	Corda	Iota
Consensus method	Pluggable (PBFT generally)	Proof of elapsed time	Proof of Work	Ethash (PoW) Casper (PoS)	Pluggable (Raft generally)	Tangle
Accessibility	Private	Private	Public	Public	Private	Public
Mode of operation	Permissioned	Permissioned or Permissionless	Permissionless	Permissioned or Permissionless	Permissioned	Permissionless
Decentralization	Partially	Partially	Yes	Yes	Partially	Partially
Compute-intensive	No	No	Yes	Partially	No	No
Network-intensive	Yes	No	No	No	No	No
Scalability	Low	High	High	High	Partially	High
Throughput	High	High	Very low	Low	High	High
Latency	100 ms	Very Low	10 Minutes	12 Seconds	Very Low Not Measured	10 ms
Immutability	Low	Low	High	High	High	High
Adversary tolerance	33.33% Faulty Replicas	Unverified	<25% Computing Power	<51% Stakes	unverified	33.33% Computing Power
Privacy	High	High	Low	Low	High	Low
Smart contract	Yes	Yes	Limited	Yes	Yes	No
Currency	None but Tokens possible	None but Tokens possible	Bitcoin (BTC)	Ether (ETH), Tokens possible	None	Iota

Fig. 7 Comparisons of various blockchain implementations

Consensus Method	Type	Throughput	Scalability	Finality	Adversary Tolerance	Vulnerability
BFT	P	1	0	Deterministic	33.3% Replicas	33% Attack
PBFT	P	1	0	Deterministic	33.3% Faulty Replicas	33% Attack
PoW	PL	0	0	Probabilistic	50%	Selfish Mining
					Computing Power	Long Range Attack
PoS	PL	0	0	Probabilistic	50% Stake	Selfish Mining
PoC	PL	0	0	Probabilistic	50% Space	Single Point Failure
PoA	PL	0	1	Probabilistic	50% of Online Stake	Single Point Failure
PoI	PL	0	0	Probabilistic	50% Stake	Denial-of-
PoB	PL	0	0	Probabilistic	50% Coins	Spending
DAG	P	1	1	Probabilistic	33.30%	Attack
					Computing Power	Sybil Attack
Ripple	PL	1	1	Deterministic	20% Faulty Nodes	Single Point Failure

Where PL refers to PermissionLess, P means Permissioned, 1 refers as High and 0 as Low

Fig. 8 Comparison of consensus algorithms

## 8 Conclusion

The combination of blockchain, IoT, and consensus algorithms is a hot and emerging technologies used in each and every application where automation, security, scalability is required. If absolute consensus is fitted the combination is a winner. The proposed methodology based on theoretical justification is entirely different as it also based on the latest machine learning techniques using datasets of application are taken and where a model is built and can prove a benchmark for the large-scale networks.

## References

1. Dorri A, Kanhere SS, Jurdak R, Gauravaram P (2019) LSB: a Lightweight Scalable Blockchain for IoT security and anonymity. J Parallel Distrib Comput 134:180–197

2. Abdellatif AA, Al-Marridi AZ, Mohamed A, Erbad A, Chiasserini CF, Refaey A (2020) ssHealth: toward secure, blockchain-enabled healthcare systems. *IEEE Netw* 34(4):312–319
3. Lin D, Tang Y (2018) Blockchain consensus-based user access strategies in D2D networks for data-intensive applications. *IEEE Access* 6:72683–72690
4. Li G, Wu SX, Zhang S, Li Q (2020) Neural networks-aided insider attack detection for the average consensus algorithm. *IEEE Access* 8:51871–51883
5. Hosseinian H, Shahinzadeh H, Gharehpetian GB, Azani Z, Shaneh M (2020) Blockchain outlook for deployment of IoT in distribution networks and smart homes. *Int J Electr Comput Eng* 10(3):2787
6. Kenyeres J, Kenyeres M, Rupp M, Farkas P (2011, April) WSN implementation of the average consensus algorithm. In: 17th European wireless 2011-sustainable wireless technologies. VDE, pp 1–8
7. Ni J, Chen X, Yan Y, Hu R, Zhu Q (2018, October) A tally system based on CNN and blockchain. In: 2018 17th international symposium on distributed computing and applications for business engineering and science (DCABES). IEEE, pp 68–71
8. Wu J, Dong M, Ota K, Li J, Yang W (2020) Application-aware consensus management for software-defined intelligent blockchain in IoT. *IEEE Netw* 34(1):69–75
9. Li K, Hua CC, You X, Guan XP (2020) Output feedback-based consensus control for nonlinear time delay multiagent systems. *Automatica* 111:108669
10. Liu H, Han D, Li D (2020) Fabric-IoT: a Blockchain-Based Access Control System in IoT. *IEEE Access* 8:18207–18218
11. Mittal M, Balas VE, Goyal LM, Kumar R (eds) (2019) Big data processing using spark in cloud. Springer, Berlin
12. Mittal M, Balas VE, Hemanth DJ (eds) (2018) Data intensive computing applications for big data, vol 29. IOS Press
13. Mittal M, Singh H, Paliwal KK, Goyal LM (2017, December) Efficient random data accessing in MapReduce. In: 2017 international conference on infocom technologies and unmanned systems (trends and future directions) (ICTUS). IEEE, pp 552–556
14. Chaudhry N, Yousaf MM (2018, December) Consensus algorithms in blockchain: comparative analysis, challenges and opportunities. In: 2018 12th International Conference on Open Source Systems and Technologies (ICOSST). IEEE, pp 54–63
15. Pu S (2020) Industrial applications of Blockchain to IoT data. In: *Blockchain and Crypt Currency*. Springer, Singapore, pp 41–58
16. Manfredi S (2013) Design of a multi-hop dynamic consensus algorithm over wireless sensor networks. *Control Eng Prac* 21(4):381–394
17. Sagirlar G, Sheehan JD, Ragnoli E (2020, March) On the design of co-operating blockchains for IoT. In: 2020 3rd International Conference on Information and Computer Technologies (ICICT). IEEE, pp. 548–552
18. Singh R, Gahlot A, Mittal M (2019) IoT based intelligent robot for various disasters monitoring and prevention with visual data manipulating. *Int J Tomogr Simul* 32(1):90–99
19. Singh R, Gehlot A, Mittal M, Samkaria R, Choudhury S (2017) Application of icloud and wireless sensor network in environmental parameter analysis. *Int J Sens Wirel Commun Control* 7(3):170–177
20. Shi P, Wang H, Yang S, Chen C, Yang W (2019) Blockchain-based trusted data sharing among trusted stakeholders in IoT. *Prac Experience, Software*
21. Zoican S, Vochin M, Zoican R, Galatchi D (2018, November) Blockchain and consensus algorithms in Internet of Things. In: 2018 International Symposium on Electronics and Telecommunications (ISETC). IEEE, pp. 1–4
22. Dong T, Bu X, Hu W (2020) Distributed differentially private average consensus for multi-agent networks by additive functional Laplace noise. *J Franklin Inst* 357(6):3565–3584
23. Zhang W, Wu Z, Han G, Feng Y, Shu L (2020) Ldc: a lightweight data consensus algorithm based on the blockchain for the industrial internet of things for smart city applications. *Future Gener Comput Syst* 108:574–582



24. Wang X, Zha X, Ni W, Liu RP, Guo YJ, Niu X, Zheng K (2019) Survey on blockchain for Internet of Things. *Comput Commun* 136:10–29
25. Yadav AK, Singh K (2020) Comparative analysis of consensus algorithms of blockchain technology. In: *Ambient communications and computer systems*. Springer, Singapore, pp 205–218
26. Zhang H, Lang W, Liu C, Zhang B (2020, June) A blockchain-based security approach architecture for the Internet of Things. In: *2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, vol 1. IEEE, pp 310–313

# Smart Contract Deployment in Ethereum Learning Made Easy



Mayank Aggarwal, Vishal Goar, and Nagendra Singh Yadav

**Abstract** Information technology has seen quite a few marvels of invention and new discoveries in terms of technology. Until now this was a revolutionary era in which change was something which is not accepted easily. Blockchain is the example of that change, which no one has thought of a technology that keeps and upholds the long-term record keeping. However, the adoption of technology is quite risky and requires a lot of analysis. The chapter covers Blockchain's brief summary in terms of its evolution from its origin, why we should opt for blockchain as a technology, a brief introduction to blockchain, types of blockchain Platform, how blockchain is driven by consensus mechanism along with its listed objectives which play an important role. There are several consensus mechanisms listed and explained with the conceptual point of view. The chapter enlists the smart contract, which is required to drive the business based upon some business rules. Alongside, blockchain implementation with its types is explained with their brief steps followed. Blockchain implementation is explained with the help of Ethereum in-depth with dedicated steps with deeply explained.

**Keywords** Blockchain · Blockchain platforms · Consensus mechanism · How to implement Browser-based blockchain · MetaMask · Ethereum · Smart contract

## 1 Blockchain—The Future Is Here

How we should protect our data? Why blockchain is considered most secured way to store data? What is blockchain? How to deploy our own blockchain? These types of questions are always keeping our mind occupied. The chapter is all about to answer these queries along with the complete practical idea of how one can deploy a smart contract using Solidity in Ethereum.

---

M. Aggarwal (✉)  
Gurukul Kangri Vishwavidyalaya, Haridwar, Uttarakhand, India  
e-mail: [mayank@gkv.ac.in](mailto:mayank@gkv.ac.in)

V. Goar · N. S. Yadav  
Government Engineering College Bikaner, Bikaner, Rajasthan, India

Blockchain transactions occur in real-time, used for any application or any business

## ***1.1 Background***

Blockchain uses the concept of distributed ledger. Though block chain is still in budding stage but distributed ledger concept was introduced around the 1990s for the first time [1].

Blockchain technology was introduced for the first time in 1991 when two of the research scientists, named as Stuart Haber and W. Scott Stornetta, comes up with a computation phenomenon which assures that no one can temper the Digital Document, or changes to the document cannot be made. This was the cryptography-based secured chain of blocks [2].

In the year 2004, computer scientists introduced a system called as “RPOW,” which stands for Reusable Proof of Work. The was designed to accept hashcash-based proof of work (PoW) token and as a result, which produced RSA Signed token. This was transferred from person to person.

By the year 2008, bitcoin was introduced which was a new decentralized peer-to-peer Electronic Cash System. On Jan 3, 2009, Digital gold termed as bitcoin was born due to the mining performed by Satoshi Nakamoto (pseudoname) [3]. Satoshi Nakamoto introduced the concept of blockchain, which demolished the concept of centralization by focusing upon decentralized ledger, being maintained by anonymous consensus. The first vendors in terms of cryptocurrency implementation were bitcoin (record priced at \$19,843.1094), ripple (represented by XRP symbol), and Litecoin (targeted number of tokens to be circulated is \$84 million) [4]. Litecoin is said to be the little sister of bitcoin.

On August 2014, the bitcoin blockchain file which was keeping records of all transactions reached 20 GB. Later attention shifted toward blockchain by which hundreds of new cryptocurrencies were issued [5].

In the year 2015, a blockchain project named “Hyperledger” was funded after the Linux Foundation announced the creation of the Hyperledger project [6].

Blockchain 1.0 was transactions based, which included the deployment of cryptocurrency in those applications, which are related or operate on cash, which is furthermore seen into currency transfer and digital payment systems. Early vendors operated using blockchain 1.0 were OneName, Open Bazar, Streamium, and Factorn.

In 2018 the power of blockchain became evident and it was called blockchain2.0. It was contracts based which included financial markets and applications, which operates on blockchain beyond cash transaction. All the transaction on this version of blockchain was smart contract-based transaction [7]. The goal shifted from digital

currency mining to applications, which can be used in any business. This started the use of blockchain-based solutions into health care, supply chain, and finance.

### **Why Blockchain?**

Say, for an example, if all the records lie on a centralized computer, in the case of failure, no one will be able to access the records [8]. To ensure the availability of data at any point of time, we have to opt for distributed storage instead of keeping all the data at one single place.

The decentralization ensures the availability of data at any point of time, resulting into reducing the centralized databases dependency. But decentralization itself has a shortcoming of security of data. We can protect data loss but we cannot say that data is fully secured. Using the concept of decentralization blockchain was introduced which made it secure, tamperproof, reliable, and transparent [9].

Blockchain promises to record or keeping a record of everything whenever a transaction occurs [10]. Now a transaction can be a financial transaction as well as storing data in the database can be termed as a transaction as well. Everything in the blockchain is transparent in terms of records keeping.

Blockchain protects us from all the defects related to security. Below are the key attributes of blockchain technology which derives its more capability by describing that blockchain is not just a technology, using this we can drive almost everything in information technology and digital world:

**Accessibility**—It's an open network. Accessible to everyone who wants to access the digital ledger. Anyone can add a new block to the chain by mining, upon which a transaction is recorded and the entire blockchain will have a record of it. Blockchain maintains the distributed ledger in a back end database.

**Disruptive**—Blockchain is said to be a Disruptive technology when we compare it to the Internet, as blockchain promises innovation in financial and commercial aspects when compared with the impact of web on communication [11]. Blockchain has revolutionized the transaction processing and its storage in the database, using below concepts:

**Track data and its storage**—Blockchain is a decentralized and distributed ledger whose transactions are recorded on each and every computer locked on the blockchain network, making the transaction data safer by tracking its data changes over time.

**Trust**—Trust is the key concept when we talk about blockchain. The data is accessible in real time and all the computers verify the transaction-related changes, this results in building up trust in data. Blockchain maintains the trust between individuals and businesses so that they can transfer information to each other using the uniquely identified address.

**Peer-to-peer transaction approach**—There are no third-party involvements when it comes to transaction processing using blockchain. Unlike regular transaction processing where we require our banks to verify and validate transaction, using blockchain no such dependencies exist on the third parties' institutions. It is a new way to authenticate and access transaction systems.

**Protects Identity**—All the transactions are anonymous by securing the identity of all the parties. There will be no name displayed in the transaction, unlike a banking transaction system. Instead, it uses a hexadecimal address which is a unique address and hard to remember.

**Decentralization**—The records kept on blockchain all recorded on each node over the network. This eliminates further dependency on a central authority.

**Secure**—All the transactions on the blockchain are secured as it uses cryptography algorithms that are based on private or public key encryption mechanisms. Blockchain maintains the repository of contracts and assets without containing them physically.

**Real-time Operations**—Blocks in blockchain are verified and added in real-time, which reduces the risks associated with data synchronization.

It is the trust and reliability feature of blockchain, which has made it so popular for all applications.

### **What is Blockchain?**

As we have already learnt why it is required, how fast it is growing. Let us now learn what is it?

To understand it in simple terms let us assume blockchain as link list that you must have learned in Data Structures. Just like linked list, blockchain have blocks in place of nodes of linked list. These blocks are joined with each other in somewhat similar manner as nodes of linked list. It is similar to the concept of data storage in a linked list. Like linked list nodes have two fields data and address, blocks in blockchain have namely three fields data, hash(address), and nonce. A node is connected with previous node using cryptography function called SHA-256 which makes it secure [12]. Nonce is a unique random number used to generate the hash (address) of previous block. Genesis is the name given to the first block created on blockchain. The two blocks on blockchain are linked to each other using hash. Blockchain system generates a unique number, typically termed as “Hash” [12]. If anything went wrong, as a result, a new block is created and added ensuring that no one is able to delete the previous block. Figure 1 explains the working of blockchain.

Blockchain is a ledger that contains all the transactions capable of transmitting any information securely. To ensure the authenticity in blockchain, it uses cryptography and digital signatures along with proof of identity ensuring read or write access rights are imposed. A blockchain is a moving network on which transactions take place without the involvement of any third-party institutions [13].

The structure of the block consists of three attributes, which are block header, block identifier, and Merkle trees. A block header contains hash of the previous block, mining details, i.e., timestamp, and binary hash tree root. Block Identifier contains a cryptographic hash. Merkle trees are the transaction in a block.

The blockchain-based ledger permanently holds the transaction records along with interactions that occurred between participants who have accessed the blockchain network. Each block on blockchain holds the transaction details and the currency type [14].

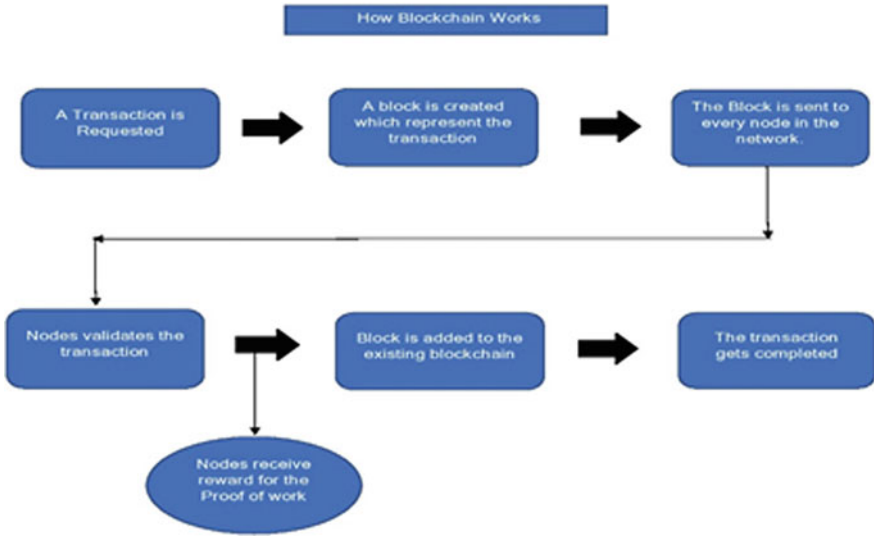


Fig. 1 Blockchain flow

In the implementation of blockchain, peer-to-peer network is adopted. Peer-to-peer ensures that every entity or a person or user contains some records or data. Mutual consent is required before the execution of any transaction [15].

In blockchain, every user should contain the data along with the ownership of the data, which they store with them, ensuring data is distributed across the network and synced

In a permission-based database for blockchain, data and records are stored inside the database with applied permissions granted to some specific set of users [16].

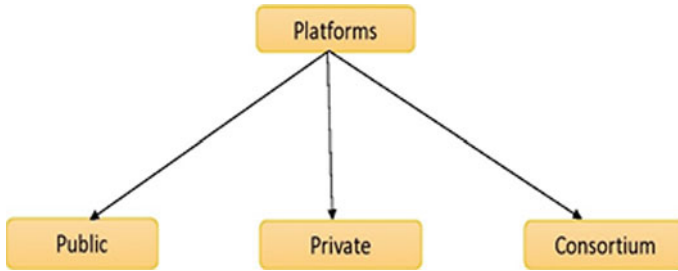
Blockchain ensures that no one should be able to delete or modify a data or transaction in the database. The number of operations performed on a blockchain is termed as transaction. A transaction can be adding a record or retrieval of an existing record.

Blockchain build trust, integrity, and security [17]. Data is decentralized, meaning it is shared and secured inside log files. Cryptography is used to encrypt a number of records inside a block. This technology is completely dependent on the Internet in order to maintain the distributed ledger. Blockchain mining nodes perform three operations for a block which are executed, verify, and store the data in the block [18].

Consensus algorithms are used in blockchain in order to ensure if and when something in terms of record is added up in the chain. Everyone before proceeding with addition of blocks on chain should sign off a common agreement.

Suppose nick wants to send some money to jack, below are the transaction steps performed before the completion of actual transaction:

Unconfirmed transaction—Transaction request will be sent to peer-to-peer network from the node to MEMPOOL.



**Fig. 2** Platforms in blockchain

Validation of transaction—The network of nodes will validate the transaction using an algorithm.

Proof of work 1—When the transaction is validated, it will be grouped into a single block and sent to the miner.

Proof of work 2—Miners starts to unravel difficult math problem supported Merkle root and nonce.

Transaction confirmation—A new block will be added to blockchain and transactions inside the block will be marked as confirmed.

Types of platform in blockchain (Fig. 2)?

**Public**—Accessible to everyone. Permission less blockchain, which is accessible to the public, allows any users to access at any point of time. A completely public blockchain allows anyone to view and access the data.

**Private**—Permission-based blockchain is accessible to users who have been granted permission to access a private network on a private blockchain. This could be considered as a group of selected users of an institution or organization who has access to view and edit the data.

**Consortium**—Combination of Public and private platform.

Blockchain transaction takes place in real-time, to drive an application or business.

### **Consensus Mechanism in Blockchain**

The consensus is a way to reach agreement in a group dynamically [18]. This mechanism ensures that an agreement reaches which should benefit the entire group itself. When a consensus decision making is obtained it is termed as “consensus mechanism.”

Objectives of consensus mechanism:

**Agreement seeking**—A consensus mechanism should cause the maximum amount agreement from the group as possible.

**Collaborative**—All the participants should put the group interest at the first place with aim to work together.

**Cooperative**—All the participants should work, as a team rather than putting own interests at first place.

**Equal rights to everyone**—This means that everyone’s vote in the group has equal importance and weightage.

**Inclusive**—Maximum number of people’s participation should be there is consensus process. It should not be as a normal voting where people feel like their vote will not have much weightage in terms of long run.

**Participation**—Consensus mechanism ensures that everyone should participate in overall process.

Each blockchain protocol is programmed with a consensus mechanism that is responsible for the verification and updating of transactions on the distributed network-based ledger. It is used to monitor records or transaction. Different type of consensus mechanism exists, out of which some are explained below:

### **POW (Proof of Work)**

POW in simple words termed as “Proof-Of-Work” aims to solve mathematical problems which are complex and harder to solve. A block is added to the chain because of voting. POW validates the nodes in larger quantity, later these nodes mine the block upon solving complex mathematical problems and hash code is divided to read those transaction exists on the blockchain. New block is added into the chain after the blocks are mined, for which the miners are rewarded. When 51% of the nodes are able to solve the mathematical problem on the network, then new transaction and its associated data is added to the blockchain. Miners to mine the block, because of which a new block is added, solve the cryptographic puzzles. This process intakes a huge amount of energy with computational usages. The puzzles are formed to ensure, it becomes really hard on the system. A block is shared on the network for its verification when miner successfully solves the puzzle. Verification of block, if it belongs to chain or not is a quite simple process, for example bitcoin uses proof of work Protocol.

### **POS (Proof of Stake)**

The system chooses the miner randomly. Here miners are called validators. This is how POS works:

As a stake, the validators will lockup some of their coins.

Validators will start the validation of the blocks, if they think that a particular block can be a fit on the chain in terms of adding a block, a bet will be placed to validate it.

Validators will be rewarded based upon their proportion of their bets, only if the block is appended.



POS is more resource friendly when compared to POW. In POW we have to waste lots of resources.

### **BFT (Byzantine Fault Tolerance)**

BFT termed as “Byzantine Fault Tolerance” aims to obtain consensus even if some nodes are unable to respond in a network. BFT focuses on the prevention, which leads to the failure of system or systems. In order to obtain BFT, we have to ensure that all the working nodes in the network should reach the agreement. In certain amount of time, if no message is received, we can conclude that the message from a specific node is said to be faulty. If most of the nodes are able to respond with a correct value there on, we can proceed with assigning a default response. There are two types of Byzantine Failures:

Fail—Stop Failure

Arbitrary node Failure

POAC (Proof of activity)

POAC is a one among various blockchain consensus algorithm to make sure that blockchain-based transactions are genuine and every one user reaches a consensus of the general public ledger [19].

POAC may be a mixed approach which uses two opposite commonly used algorithms—named as proof of work and proof of stake. The mining process in POAC begins as typical proof of work process alongside various miners attempting to outpace each other using high computation power to hunt out replacement blocks. Whenever a replacement block is mined or discovered, the system switch back to POS, along with new discovered block, which contains a header and thus the reward address of the miner.

Based upon provided header details, replacement random group of validators from blockchain network is chosen. The larger crypto coins a validator owns, the greater chances they have to be selected as signer. When all validators have signed for the newly discovered block, it is identified and results into addition to the blockchain network, because of which transactions are recorded.

### **POB (Proof of Burn)**

It focuses on addressing the POW problems related to energy consumption. In order to mine the blocks, miners have to buy a virtual mining rig. To achieve that miners, have to burn their coins. POB is an alternative consensus algorithm introduced to overcome or address POW system issues in terms of high-energy consumption. POB works on the principle, which allows miners to burn virtual currency tokens. The miners give rights for writing the blocks based upon the coins burnt. The miners burn their coins to purchase virtual mining rig, allowing them to mine the blocks. The bigger will be virtual rig, if the miner burns more and more coins.

### **POET (Proof of Elapsed Time)**

The POET focuses to follow a lottery system, in order to prevent higher resources and energy utilization. In other words, we can say that POET is a consensus algorithm

which forestalls highest utilization of resource and consumption of high energy. The method becomes more efficient by following a fair lottery system [20].

This is how the POET algorithm works:

Every participating node within the network is required to attend for a randomly chosen period of time; therefore, the first one to finish the designated waiting time wins the new block. Each node within the blockchain network generates a random wait time and goes to sleep for that specified duration. The one to awaken first—that is, the one with the shortest wait time—wakes up and commits a replacement block to the blockchain, broadcasting the required information to the entire peer network an equivalent process then repeats for the invention of subsequent block.

### **POC (Proof of Capacity)**

The algorithm focuses to use the space available on miner’s hard drive so that mining rights can be decided [21]. Proof of capacity (POC) is consensus mechanism utilized in blockchains which permits the mining devices within the network to use their available disk drive space in order to make a decision on mining rights, rather than using the mining device’s computing power (as within the proof of labor algorithm) or the miner’s stake within the crypto coins.

### **POA (Proof of Authority)**

The POA algorithm uses “authorities” which are the nodes who have access to create new block and to secure blockchain. They should have the required permission in order to delete a record. In other words, this consensus algorithm provides the efficient and practical solution for a private blockchain network. In 2017, Gavin Wood introduced this [22].

Proof of authority is a highly scalable system as the model itself is dependent on a limited number of block validators. Pre-approved participants verify the transaction and blocks, which act as mediators to the system.

## **2 Smart Contracts**

Smart contracts are program which are event driven executed on blockchain with enforcing some business rules, which is capable to take the control over an asset which exist on the ledger.

Blockchain consist of smart contracts, which are computer protocols, who serves as facilitator and verifies transaction beyond the purchase and selling of currencies. Smart contract is an agreement between one or more entity when they want to complete a transaction. Therefore, both the parties have to agree upon a mutual consent before any transaction. This contract contains “code of law.”

Let us take a look at the example of land registry system. Registry of land proves the authenticity that Mr. XYZ holds the property legally which proves the ownership. Now the government can implement the blockchain to maintain the records of land registry data. Therefore, this can be the combination of hybrid system, where there

is a public network, on which any person can see the property and find out about its boundaries and expansions. The other network, which contains all the private information to which only government official has access.

In case of purchase and sell of the property, the operations are carried out with the help of smart contract, which are simple, fast, and cheaper. This eliminates the need of intermediary authority to register a property. When a seller has received the full payment for the property by agreeing upon a smart contract, ownership rights and property get transferred to the new owner. This will add a new block of property information on the blockchain with containing the previous details and history of property.

### 3 Blockchain Implementation—Browser Based

After studying the basics of blockchain and what is smart contract, we will learn how we can deploy our smart contract in Ethereum blockchain.

Before proceeding with any transactions on blockchain, we must have an account or a wallet, which should have some cryptocurrencies [23]. So, first step is to have an account to hold cryptocurrencies. These are called wallets. These types of accounts are called Externally Owned Accounts (EOA). There are many types of wallets, in this chapter we will use MetaMask which is a browser-based wallet, i.e., its extension is embedded in our browser and we can use it from our browser directly [24]. Let us learn the complete process step by step:

Step 1: Install Metamask (Browser-based wallet)

- Using chrome web store, query for MetaMask in search option, and get it installed in your browsers extension (Fig. 3).

Step 2: Once the MetaMask Extension is added and installed in the web browser. Click on GET STARTED Button and then Click on Create a Wallet button in order to start using MetaMask (Fig. 4).

Step 3: The user is required to create a password as per the password specific rules (Fig. 5).

Once user has successfully created a password, the user will be navigated to a page where a user is required to arrange the phrase in order to form a sentence; this is termed as secret phrase. The user is required to remember the phrase, so that if a user has lost the password, the account can be unlocked with help of secret phrase. Once user has obtained the content of secret phrase, click on Next button.

User is required to confirm the secret phrase to get finished with account creation. Once phrases of word are arranged in correct sequence, click on Confirm Button.

Once a user has finished all the steps as stated in above steps, user would navigate to the web page as shown in Fig. 6. The address 0x406A73c2A92D50ac8d43Ac4E1636c7804E0B1d3B uniquely identifies the created account; it is unique for every account. You will see a different address, which represents your address in EOA. It can be considered as your account number.





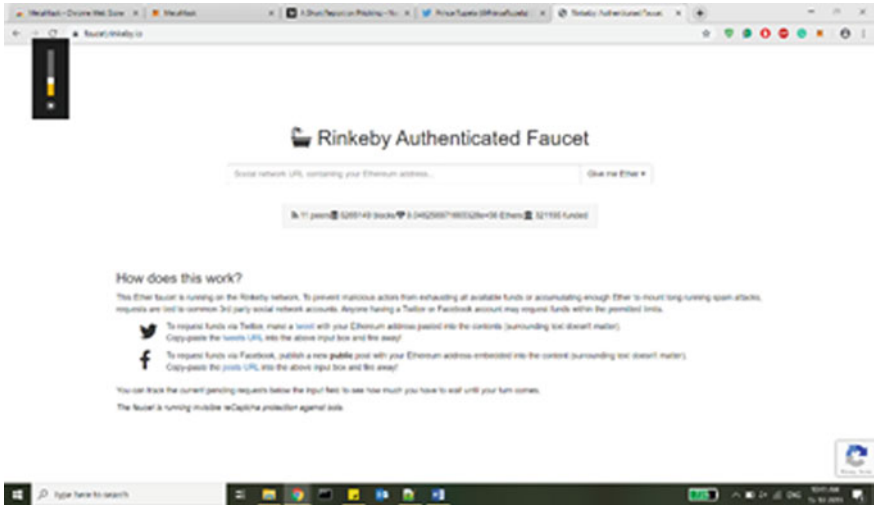


Fig. 7 Authentication

Step 4: Rinkeby Authenticated Faucet (To get Ether in your wallet).

Now we have a wallet, but we do not have any cryptocurrency added in the wallet. We use Rinkeby Authenticated Faucet to add the cryptocurrency to wallet. This website helps us to obtain Ether based on request. In order to request Ether, we are required to have a Twitter or Facebook account. We will use Twitter in our chapter.

Login to your Twitter account. If you do not have one create it.

Step 5: A user should be logged into Twitter account, once a user is logged into Twitter account, the user is required to navigate into Rinkeby Authenticated Faucet using URL—<https://faucet.rinkeby.io/> [25]. A user can request the Ether funds with the help of Twitter account by clicking on tweet Hyperlink given on page shown in Fig. 7.

Step 6: User must navigate back to MetaMask wallet. The user is required to copy his unique address which can be found listed under Details button on the Dashboard. As in our case unique address is 0x406A73c2A92D50ac8d43Ac4E1636c7804E0B1d3B. Then paste the address, replacing the highlighted string in your Twitter account as shown in Fig. 8 [24].

Just to connect with all readers we request to follow @mayankcloud on Twitter [26]

Step 7: The user is required to navigate back to the home page of Twitter account. Under your tweets section, click on “Copy link to Tweet.” This is the one in which a user has requested ether in order to get real-time fund (Fig. 9).

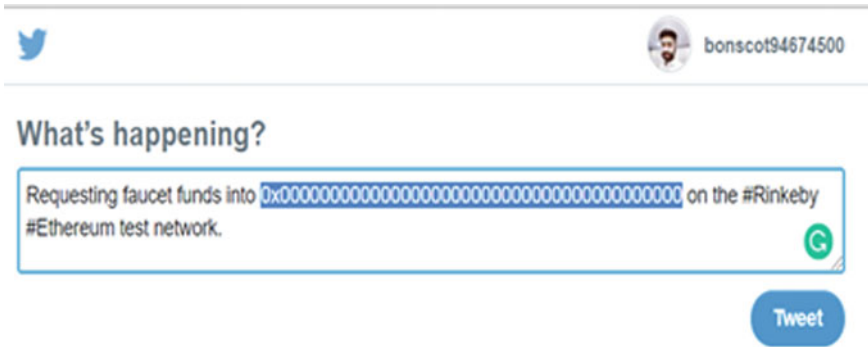


Fig. 8 Twitter account

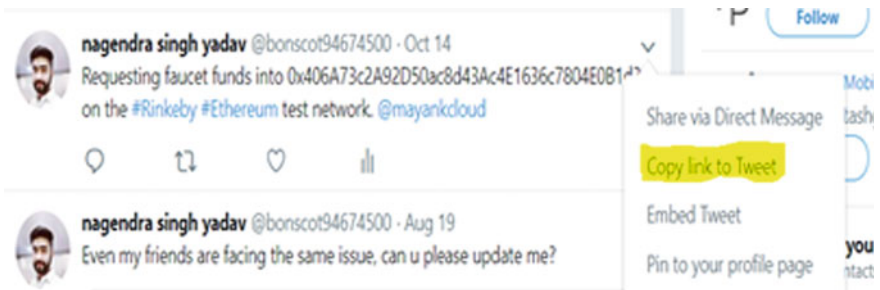


Fig. 9 Navigation

Step 8: Once user has completed the step 7, User must navigate back to Rinkeby Authenticated Faucet web page, and on the same web page, user is required to paste the URL as demonstrated in Fig. 10 and user has to select an option from Give me ether dropdown.

Step 9: User must navigate back to MetaMask wallet and refresh the page to validate the funds availability in the wallet. Strange! A user may not see any changes to the wallet because by default Main Ethereum Network is selected, from network options choose Rinkeby test network as shown in Figs. 11 and 12. Rinkeby Test

Fig. 10 Demonstration







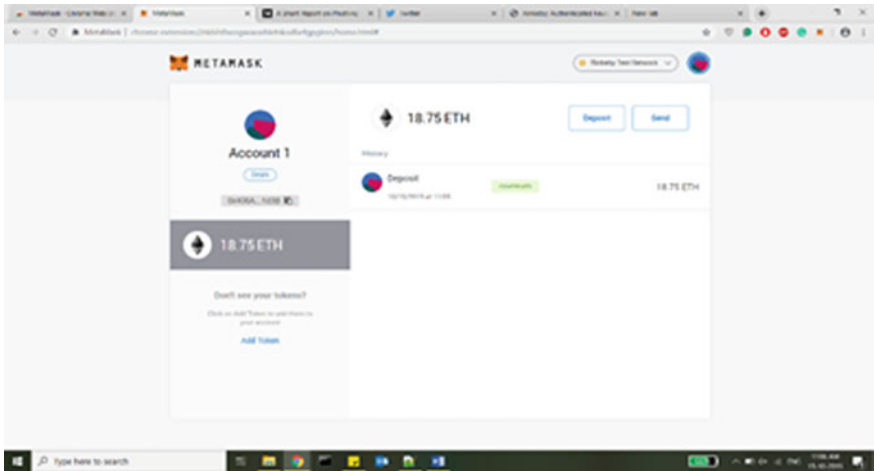


Fig. 13 Step 10

Step 11: Now as ethers are added, we need to deploy and compile our smart contract. We are assuming that you know how to write a Smart Contract using solidity and we will cover easiest way to deploy your smart contract on Ethereum test network [27]. Online compiler remix is used to compile and deploy the contract finally. Open <https://remix.ethereum.org/>:

Step 12: Choose solidity in Environments (Fig. 14).

Step 13: Click on Create new File button, which is located in the Browser storage explorer button as shown in Fig. 15.

Step 14: Assign some name to the File by default it will take Untitled. Sol.

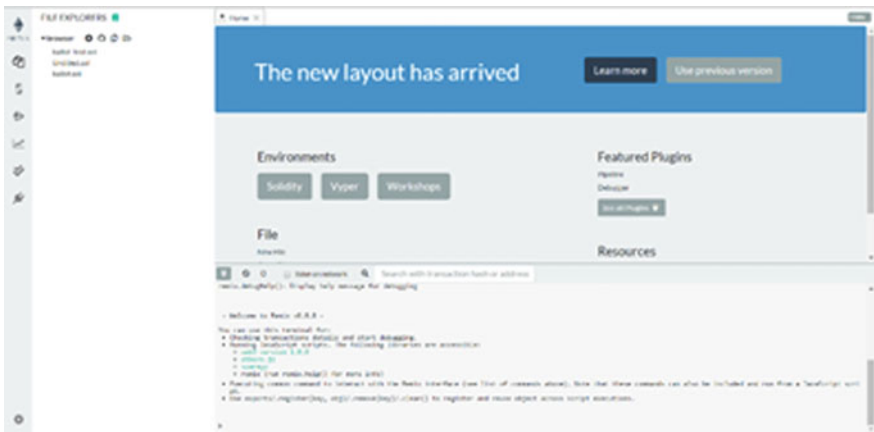


Fig. 14 Step 12

**Fig. 15** Step 13

Step 15: Write your smart contract here. Or for testing you can copy paste from [www.mayankagr.in](http://www.mayankagr.in). [28].

Sample Smart Contract:

```
pragma solidity ^0.4.0;

contract person
{
    string private name;
    uint private age;

    function setName(string newName) public
    {
        name=newName;
    }
    function getName()public constant returns(string)
    {
        return name;
    }
    function setAge(uint newAge) public
    {
        age=newAge;
    }
    function getAge()public constant returns(uint)
    {
        return age;
    }
}
```

Step 16: Go to compiler and choose compiler version as per your smart contract for copied smart contract, version is 0.4.25. Click on compile and if no error smart contract is compiled and bytecode is generated as shown in Figs. 16 and 17.

Step 17: After compiling deploy the smart contract. Select deploy and run transaction icon. At environment there are three options to deploy on Rinkeby test network select Inject web3 option as shown in Fig. 18.

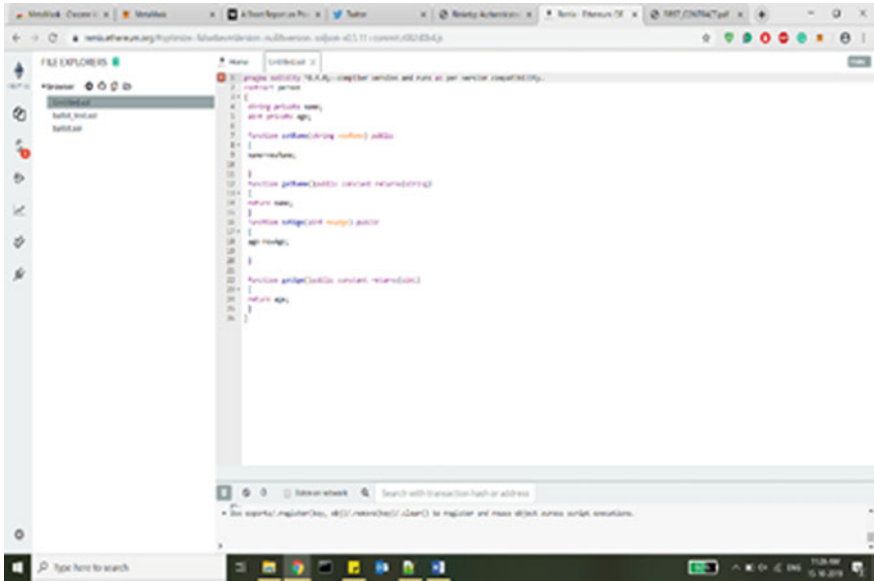


Fig. 16 Step 15

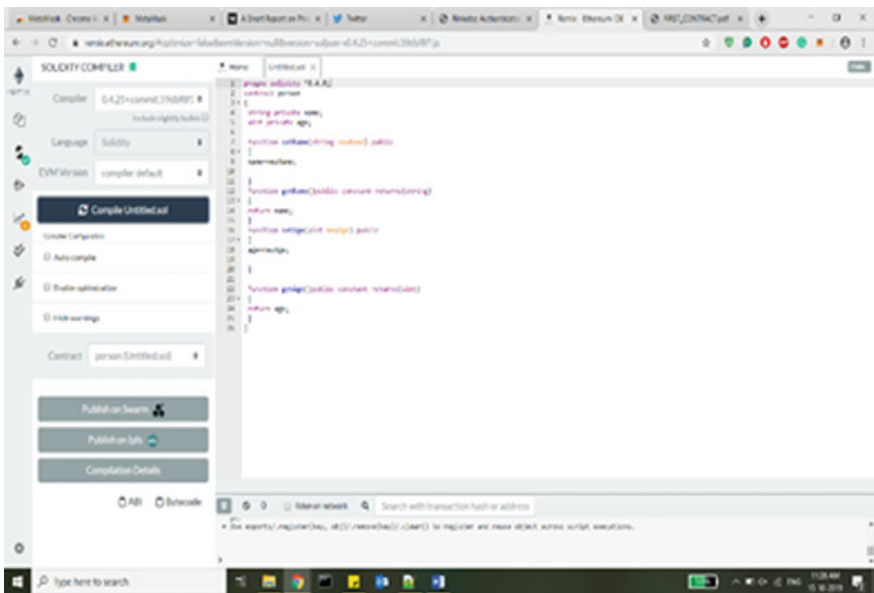
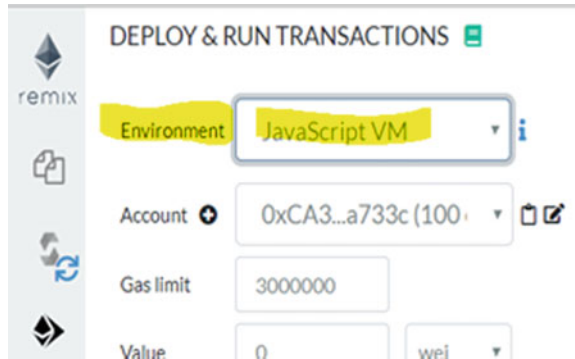


Fig. 17 Step 16

Fig. 18 Step 17



Step 18: Then deploy by clicking on Deploy button and contract will be shown under deployed contracts as shown in Fig. 19.

Step 19: One can see the deployed contract in metamask also as shown in Fig. 20.

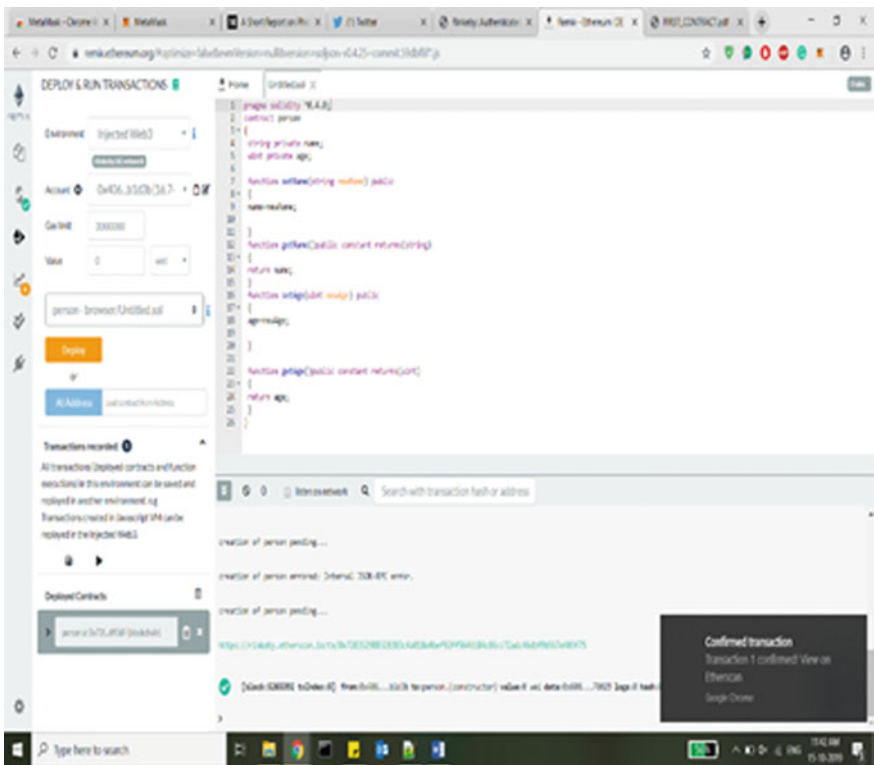
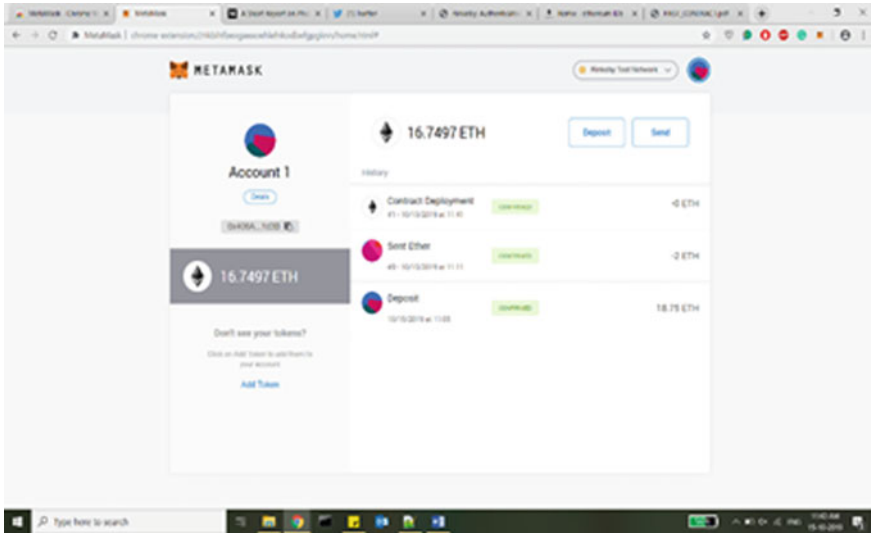


Fig. 19 Step 18



**Fig. 20** Step 19

The smart contract is successfully deployed in Rinkeby test network of Ethereum which can also be viewed on etherscan [29]. To make an application for the deployed contract below section describes how to use Oneclickdapp an easy way to make a decentralized application for your deployed contract.

Step 20: Navigate to Oneclickdapp by using URL as mentioned below [30]—<https://oneclickdapp.com/>

Step 21: Click over a button “Create a dApp for free” as shown in Fig. 21.

Step 22: Provide an application name of your choice (Fig. 22).

Step 23: Open the remix Ethereum page then open the contract written choose compile option. From the previously compiled code copy ABI and paste on Oneclickdapp window as shown in Fig. 23.

Step 24: Put metamask address in Address field and choose Rinkeby in Network field.

Step 25: Then click on Next button. Thereafter user must Click on Createdapp Button (Fig. 24).

The app is created successfully as shown in Fig. 25. On clicking set age one can input age.

## 4 Conclusion

In this chapter, we discussed the smart contract, which is required to drive the business based upon some business rules. Alongside, blockchain implementation with its types is also explained with their brief steps followed. Blockchain implementation



Fig. 21 Step 20

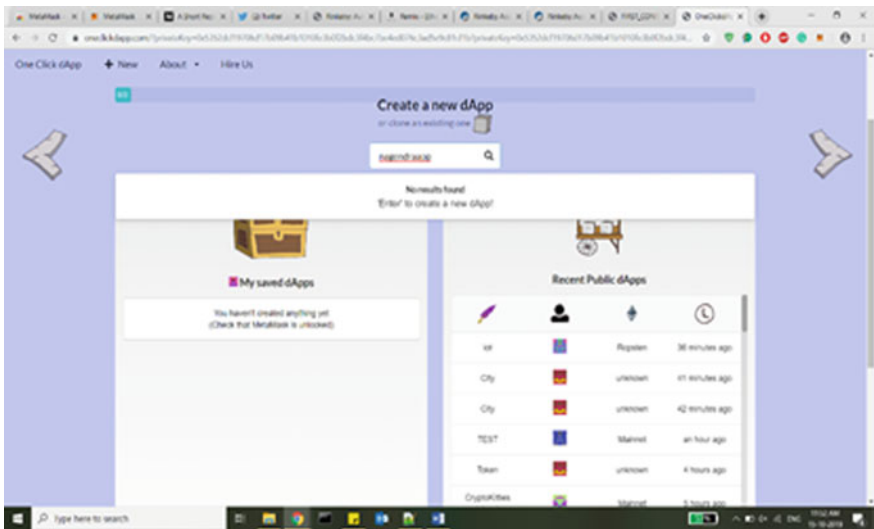


Fig. 22 Step 22

is explained with the help of Ethereum in-depth with dedicated steps with deeply explained.

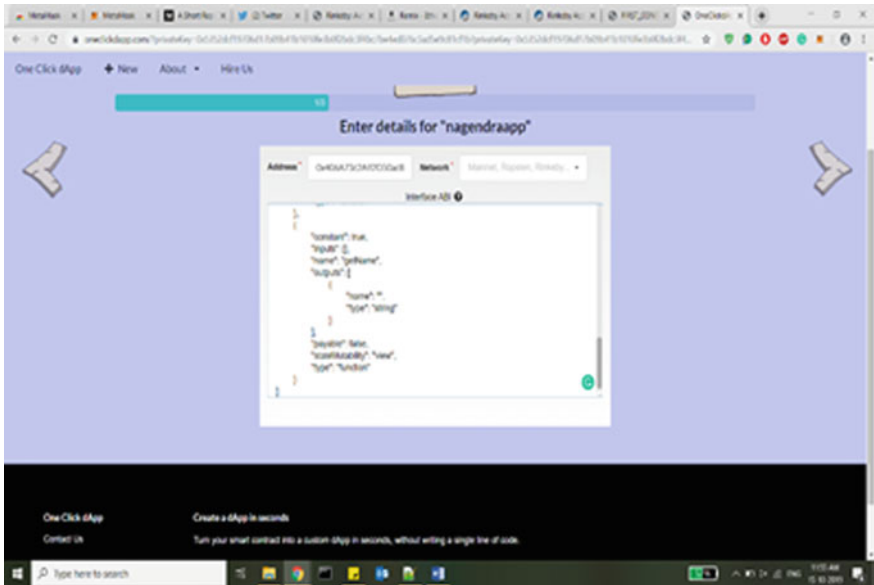


Fig. 23 Step 23

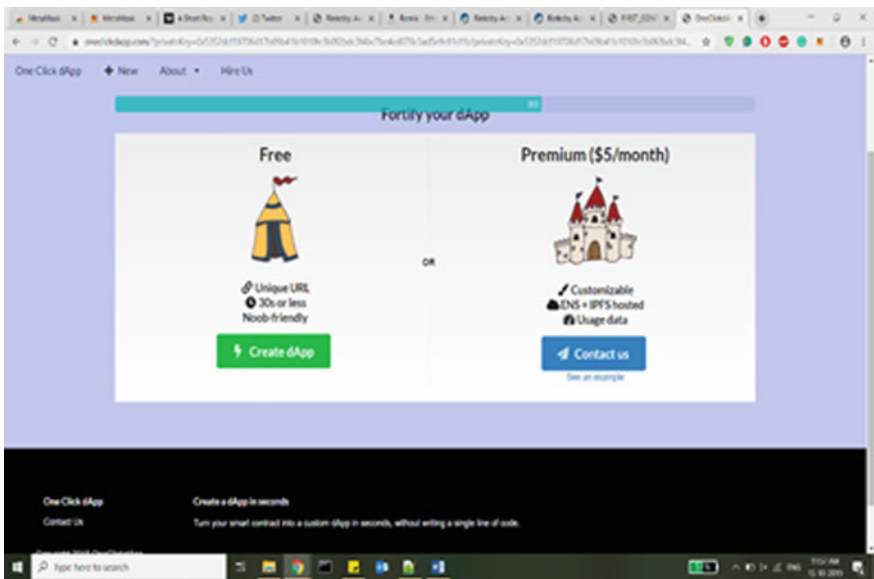


Fig. 24 Step 25

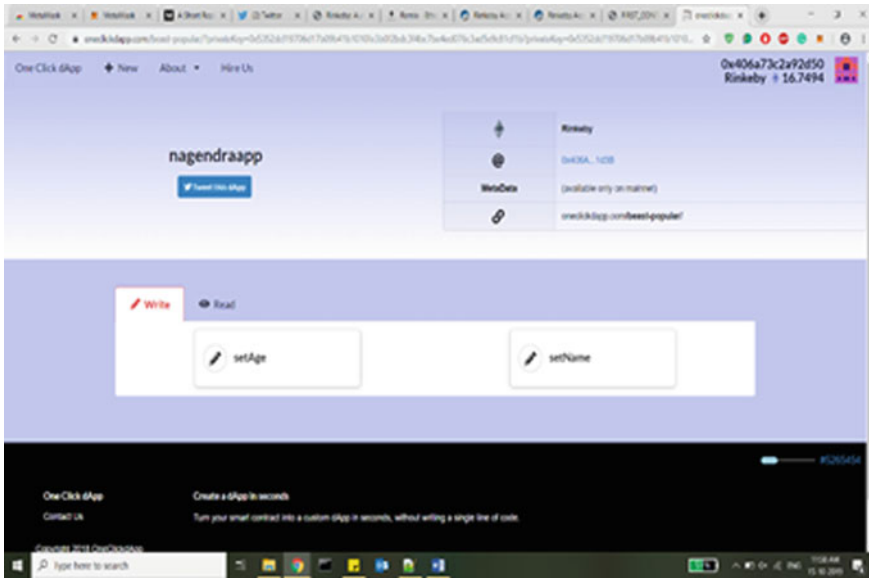


Fig. 25 Final Step

## References

1. Wikipedia (2020) Blockchain. Available on <https://en.wikipedia.org/wiki/Blockchain>. Accessed on 27 Apr 2020
2. Binance academy (2020) History of blockchain. Available on <https://www.binance.vision/blockchain/history-of-blockchain>. Accessed on 27 Apr 2020
3. Orcutt M (2017) It's getting harder to hide money in bitcoin-MIT technology. Review Available on <https://www.technologyreview.com/2017/09/11/149211/criminals-thought-bitcoin-was-the-perfect-hiding-place-they-thought-wrong>. Accessed on 27 Apr 2020
4. Newby TG, Razmazma A (2019) An untraceable currency? Bitcoin privacy concerns—fintech weekly. Available on <https://www.fintechweekly.com/magazine/articles/an-untraceable-currency-bitcoin-privacy-concerns>. Accessed on 28 Apr 2020
5. Mike I, Nathaniel P (2019) Facebook plans global financial system based on cryptocurrency—the New York times. Available on <https://www.nytimes.com/2019/06/18/technology/facebook-cryptocurrency-libra.html>. Accessed on 28 Apr 2020
6. Chowdhury N (2019) Inside blockchain, bitcoin, and cryptocurrencies. 1st ed. CRC Press. ISBN 978-1-00-050770-6
7. Neale S (2018) Getting married and divorced on blockchain. Available on <https://www.libertarianism.org/building-tomorrow/getting-married-and-divorced-blockchain>. Accessed on 29 Apr 2020
8. Yadav NS (2019) Blockchain-the future is here. Available on <https://medium.com/the-capital/blockchain-the-future-is-here-feadbcdbbfa0>. Accessed on 29 Apr 2020
9. Josh C (2019) Facebook announces Libra cryptocurrency: all you need to know. Available on <https://techcrunch.com/2019/06/18/facebook-libra/>. Accessed on 29 Apr 2020
10. Köhler S, Pizzol M (2019) Life cycle assessment of bitcoin mining. Environ Sci Technol 53:13598–08



11. Lucas M (2019) Linux Hyperledger to give developers supply chain building blocks. Available on <https://www.computerworld.com/article/3336036/linux-hyperledger-to-give-developers-supply-chain-building-blocks.html>. Accessed on 30 Apr 2020
12. Sanders J (2019) Blockchain-based unstoppable domains is a rehash of a failed idea. Available on <https://www.techrepublic.com/article/blockchain-based-unstoppable-domains-is-a-rehash-of-a-failed-idea>. Accessed on 30 Apr 2020
13. Hsieh Y-Y, Vergne J-P, Anderson P, Lakhani K, Reitzig M (2019) Correction to bitcoin and the rise of decentralized autonomous organizations. *J Organ Des* 8:3
14. Janssen M, Weerakkody V, Ismagilova E, Sivarajah U, Irani Z (2020) A framework for analysing blockchain technology adoption: integrating institutional, market and technical factors. *Int J Inf Manage* 50:302–307
15. Koens T, Poll E (2019) Parallel processing workshops. *Lect Notes Comput Sci* 11339:535–546
16. Kloch RC, Little SJ (2019) Blockchain and internal audit. Internal audit foundation
17. Agrawal R et al (2020) Blockchain technology and the internet of things: challenges and applications in bitcoin and security
18. Li J (2020) Blockchain technology adoption: examining the fundamental drivers. In: *Proceedings of the 2nd international conference on management science and industrial engineering*. ACM Publication, pp 253–260
19. Stoll C, Klaaßen L, Gallersdörfer U (2019) The carbon footprint of bitcoin. *Joule* 3:1647–1661
20. Frankenfield J (2018) Proof of elapsed time (Cryptocurrency). Available on <https://www.investopedia.com/terms/p/proof-elapsed-time-cryptocurrency.asp>. Accessed on 03 May 2020
21. Frankenfield J (2018) Proof of capacity (cryptocurrency). Available on <https://www.investopedia.com/terms/p/proof-capacity-cryptocurrency.asp>. Accessed on 03 May 2020
22. Parity technologies documentation on wikipedia (2020) Proof-of-authority chains. Available on <https://wiki.parity.io/Proof-of-Authority-Chains>. Accessed on 05 May 2020
23. Yadav NS (2019) Blockchain hands-on (browser-based). Available on <https://medium.com/the-capital/blockchain-hands-on-browser-based-38e27d5b241a>. Accessed on 5 May 2020
24. Metamask (2020). Available on <https://metamask.io>. Accessed on 06 May 2020
25. Rinkeby Authenticated Faucet (2020) Available on <https://faucet.rinkeby.io/>. Accessed on 06 May 2020
26. Aggarwal M (2020) Twitter account. Available on <https://twitter.com/mayankcloud>. Accessed on 06 May 2020
27. Remix IDE (2019) Available on <https://remix.ethereum.org/>. Accessed on 06 May 2020
28. Aggarwal M (2015) First contract. Available on [http://mayankagr.in/images/FIRST\\_CONTRACT.pdf](http://mayankagr.in/images/FIRST_CONTRACT.pdf). Accessed on 07 May 2020
29. Etherscan (2020) Available on <https://etherscan.io/>. Accessed on 07 May 2020
30. One Click dApp (2018) Available on <https://oneclickdapp.com/>. Accessed on 07 May 2020

# Blockchain-Based Smart and Secure Healthcare System



Sheikh Mohammad Idrees , Iflah Aijaz , Parul Agarwal ,  
and Roshan Jameel 

**Abstract** The healthcare data today is scrappy and not stored properly at a single location. However, some of the records are not even made digital that leads to different researches. The number of substandard medicines in the market is increasing, so is the deceitful insurance claims. Moreover, the patient-centric models are in high demand, because the patients are becoming more aware of all the aspects and requesting an infrastructure that gives most of the controls to patients themselves. Such systems would reduce the need for intermediaries, and also keep the confidentiality and anonymity of the patient data intact. The desired framework is supposed to safely handle the Electronic Health Records (EHRs), insurance claims and regulatory policies, promote researches and medicinal discoveries, etc. The healthcare data is big and heterogeneous that is usually stored in the cloud environment. However, the number of attackers on the cloud is increasing; therefore, a framework is required where the data privacy is maintained. In this chapter, a smart healthcare system based on blockchain technology is discussed, which would have the ability to provide real-time data access in a transparent, traceable, and trustful manner. The blockchain has transformed several industries including finance, manufacturing, e-commerce, education, etc. and is making its way into the healthcare industry as well. The blockchain is a distributed technology based on peer-to-peer decentralized network, which does not have any central authority controlling the system. The data within the blockchain network is represented in the forms of blocks. Cryptographic algorithms

---

S. M. Idrees

Department of Computer Science (IDI), Norwegian University of Science and Technology

(NTNU), 2815 Gjøvik, Norway

e-mail: [sheikh.idrees99@gmail.com](mailto:sheikh.idrees99@gmail.com)

I. Aijaz · P. Agarwal (✉) · R. Jameel

Department of Computer Science and Engineering, Jamia Hamdard, New Delhi 110062, India

e-mail: [pagarwal@jamiahamdard.ac.in](mailto:pagarwal@jamiahamdard.ac.in)

I. Aijaz

e-mail: [iflah.iflah1@gmail.com](mailto:iflah.iflah1@gmail.com)

R. Jameel

e-mail: [roshijameel@gmail.com](mailto:roshijameel@gmail.com)

are also applied to maintain the integrity of the data. Thus, making it the appropriate choice for healthcare applications.

**Keywords** Healthcare system · Electronic health records (EHRs) · Blockchain technology · Distributed technology · Decentralized network · Cryptographic algorithms

## 1 Introduction

The decentralized peer-to-peer connection-based blockchain technology was introduced by Satoshi Nakamoto [1] in a white paper in the year 2008 for handling first-ever cryptocurrency named Bitcoin. Since then, the blockchain has transformed almost every industry and is becoming one of the most innovative technologies available today. The researchers and organizations are attracted to this technology because of the trust offered by the blockchain-based distributed environment [2]. Besides industries including marketing, supply chain, finance, operations, etc. are adapting this fastest-growing technique to leverage their businesses [3]. Primarily the blockchain was introduced as a digital currency (substitute to actual currency), which can be used throughout the globe. The blockchain is based on peer-to-peer connectivity that allows the users to make transactions without any third party intermediation [1]. Blockchain technology facilitates the time stamping that provides an additional layer of security by monitoring the transactions that provide the user with trust and transparency. Thus making it best suitable for the healthcare industry, as data security and privacy are the main concerns for the users as the medical data is considered to be confidential [4, 5].

The open-source implementation of blockchain was released online that permitted the researchers and organizations to use it to generate various applications. This promoted the exploration of technology apart from the finance industry. The properties of blockchain such as a decentralized-distributed network with time stamping that keep the record of all the transactions happened so far, makes it the most eligible technology for exchanging any kind of information. The application areas of blockchain are spreading across multiple industries [6] including health care where several prototypes have been designed and implemented recently. The healthcare industry does not have a proper way to store the digitized medical data, the communications are also delayed at times that make it very difficult to maintain the health records of the patients. Using blockchain-based infrastructure would help in gathering useful patient details while maintaining the transparency in the network along with bringing all the stakeholders together through a single data exchange window [7]. The most advantageous feature of the blockchain-based system is ‘no third party intervention’ that decreases the implementation cost and time.

The blockchain network applies cryptographic algorithms for deriving its several properties. The participants of the network are called nodes and each of the nodes

owns their pair of private and public keys that are used as the address and authentication purposes respectively. When a transaction is requested, it consists of the public keys of the sender and receiver along with the actual information. The transactions are secured by applying a digital signature and then broadcasted over the network. This is how a single transaction is completed. A blockchain is a chain of blocks connected and one block consists of multiple transactions. This chain of blocks containing transactions is unbreakable and allows the execution of transactions openly and securely. Furthermore, blockchain technology also provides interoperability among the multiple existing systems and provides irreversible transactions. The participating nodes of the network assure the legitimacy of the transactions, which are called miners. There are several types of blockchain implementations; in the public blockchain, any node is allowed to join the network whereas, in permissioned blockchain, the nodes need to get verified first to join the network. Every node in the public blockchain can become miner, while in permissioned blockchain only a few nodes can act as miners. The permissioned blockchain is usually smaller in size and faster as compared to the public blockchain. There is also a third category of blockchain called consortium blockchain, which has the properties of both the public as well as permissioned blockchain.

The blockchain infrastructure is based decentralized-distributed network that makes it a good choice for healthcare applications, as the network is not dependent on single authority thus protecting the integrity of the data. Moreover, the immutable nature of blockchain assures that no data can be altered at any time. If a change is required, a new transaction is requested instead of modifying the existing one. The healthcare industry gives a good number of prospects for the implementation of blockchain technology. There could be several stakeholders such as patients, healthcare practitioners, medical researchers, medical insurance providers, hospitals, pharmacies. There are a huge number of events of information exchange among these stakeholders, and therefore, it becomes necessary to make sure that there is no misuse of the data like tampering, stealing, etc. Blockchain technology can provide several use cases within the healthcare industry such as supply-chain management of pharmaceutical companies [8] maintaining Electronic Health Records (EHRs) [9] monitoring insurance policies issuance [10] health research [11]. to name a few. The security and privacy of medical data are the biggest concern of healthcare organizations. Several blockchain-based models have been proposed to securely store and transact data among the stakeholders. One such system is called BloCHIE [12] which assures that the data is tamperproof and private. Furthermore, the real-time collection of the medical data is also required which can also be handled using blockchain-based architecture. The blockchain can also influence medicinal researches as it allows the easier storage, sharing, tracking, and analysis of the healthcare data in real time [13]. The blockchain-based infrastructure would increase the reliability of the system and would act as a facilitator in improving the quality of the research by providing trust and transparency to the system. The data exchange between the systems also raises the concern of data privacy, however, there are predefined standards and protocols available for the same but still maintaining it becomes costly.

## 2 Healthcare System

The healthcare system is a technique of delivering healthcare services to the population in an organized manner. It deals with various domains related to the healthcare industry. These systems have a different structure in different countries throughout the world. This structure depends on the type of healthcare provided, type and level of funding available, society to be served, technological infrastructure, environmental factors, etc. However, a healthcare system is required to provide an efficient framework to handle all these aspects [14]. The ‘United Nations International Standard Industry Classification’ classifies the healthcare system must constitute hospitals where medical and dental procedures are performed under the supervision of nurses, doctors, pathologists, physiotherapists along other health-related professions. The main focus of healthcare industries is to provide improved and efficient health services by preventing, diagnosing, and treating diseases and disorders [15–17]. The proper functioning of the healthcare system is dependent on several professions that work together in codependence. As per the World Health Organization (WHO), the objective of the healthcare systems should be providing good health to the citizens of the country, giving responses following the expectations along with fair funding.

### 2.1 Types of Healthcare

The requirement of every individual is unique which depends on the medical conditions and history. Therefore, there are three types of healthcare namely primary, secondary, and tertiary for handling different scenarios, but the primary objective is the same for all, i.e., to provide effective and efficient healthcare on time.

#### Primary Healthcare:

The primary healthcare primarily emphasizes on providing the health policies irrespective of social or economic background. The focus is to provide consultation and care to the patients with all types of diseases to all age groups within the local community. The healthcare professionals within this group do not constitute specialists they are more like generalists or physicians that can deal with various domains including social, physical, psychological issues, etc. The primary healthcare services are the first place of contact for a patient’s consultation. The number of such centers is increasing day by day to meet up with the increased number of cases of non-communicable chronic diseases like cervical, hypertension, diabetes, depression, etc.

#### Secondary Healthcare:

The specialists in various domains like dermatologists, gynecologists, urologists, etc. provide secondary healthcare. The secondary healthcare is either referred by the primary healthcare practitioner or taken if the problem is persisting or serious.

The process of getting secondary healthcare varies from country to country. In some countries, the reference from the primary doctor is necessary, while in some countries one might consult the secondary practitioner directly in case of an emergency. The secondary healthcare systems can be divided into two subcategories:

- (i) **District Health System:** The district health system constitutes of district hospitals and healthcare centers focusing on maternity and child health care. These centers remain open for 24 h, seven days a week, and provide services such as emergency care, neonatal units.
- (ii) **Community Health System:** The community health systems get referrals from primary practitioners or district health centers. The services provided in such healthcare centers cover vast domains including women's care, family planning, pathological testing, internal medicines, etc. These centers are also open for 24 h every day.

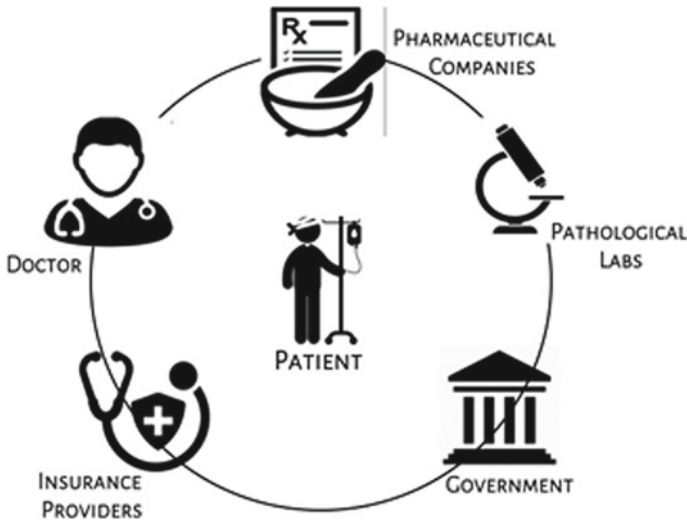
#### Tertiary Healthcare:

The tertiary healthcare sector is a specialized consultative unit that can only be consulted after getting referred from the primary or secondary health care for more sophisticated diagnosis and treatment. Services included under such systems are cardiac issues, handling severe burns, cancer, or other surgical procedures. The providers of such healthcare sector are usually national level hospitals. These centers also act as a training platform for newly educated doctors and researchers. These centers are also open throughout the week for 24 h.

## ***2.2 Components of Healthcare System***

The functioning of the healthcare industry requires the participation and contribution of different types of stakeholders. These stakeholders could be any person who is involved completely or partially in the implementation and functioning of the industry directly or indirectly. Regarding the healthcare industry, the major stakeholders are patients, healthcare practitioners, health insurance providers, pharmacists, pathological laboratories, and government. The current demand of the healthcare industry is a patient-centric model, as the outcomes of this approach are efficient in terms of the quality of healthcare provided to the patients. Moreover, in terms of business, it is observed that the patient-centric approach gives patients more satisfaction that provides positive feedbacks and overall stability in the industry. Figure 9.1 shows the components and schema of a patient-centric healthcare system.

- **Patient:** Patients are the most important component of the healthcare industry. They are the central stakeholders, and the health-related regulations and policies should always be generated in a patient-driven manner. Because today, everybody is health-conscious and if the framework is designed per the demands of the patients, the resultant efficiency would be high. The blockchain-based framework



**Fig. 9.1** Patient-centric healthcare system

for healthcare management would be apt for patient-centric care as the healthcare records would be available on a distributed platform and would provide anytime anywhere access to the users [18]. Moreover, having a decentralized system would also preserve the security and privacy of the data. The time stamping would keep the record of the transactions intact while immutability and hashing would assure the integrity of the healthcare data.

- **Doctor:** The doctors or healthcare practitioners play a fundamental role in the healthcare system by guaranteeing the quality of healthcare received by the patients. They act as a balancing factor between the patient and other stakeholders within the industry. The doctors are proficient enough to make decisions for the patients regarding complexities or uncertainties. Moreover, the doctors are responsible for promoting the health of individuals at the community level based on their expertise and experiences. With the advancement in technology, the roles of doctors are also evolving. The lifestyle of today's generation has changed entirely, which has led to an increased number of people with diseases, making it difficult for doctors to efficiently handle them all. The blockchain implementation in healthcare domain would make the job of the doctors much easier. As all the medical details would be available online in an organized manner, the diagnosis and consultation would become simpler.
- **Pharmaceutical companies:** The pharmaceutical companies also play an important role as a stakeholder in the healthcare industry as the patients depend on their products. These companies research, develop, manufacture, and sell the medical products including drugs that are required by the patients for their treatment. The government bodies to assure the standard of the drugs and prices imply a set of rules and regulations. Since, the companies are investing a lot in the

conduction of researches, supply-chain management, and marketing, the prices of the products are increasing. Nevertheless, this industry has faced problems like the fabrication of drugs or low-quality supplies globally [19] which could lead to severe complications to the patients. Therefore, surveillance is required in this domain [20] as the medicines had to go through several vendors before reaching the final user. Therefore, using a blockchain-based framework for the supply-chain management would assure the quality of the medicines as it provides traceability, immutability, and time stamping as its default features.

- **Pathological Laboratory:** The pathological laboratories provide pieces of evidence and materials that help in maximizing the efficiency of the healthcare system. It is the responsibility of the laboratories to produce results with accuracy, thus helping in diagnosis. Pathological laboratories are a vital part of the healthcare system, as they help in making correct and timely decisions. The doctors and patients can both communicate with this stakeholder. As the world is continuously changing, new types of diseases are taking over with time, and to deal with the spread and quick diagnosis, the latest technology is required. Implementing blockchain-based architecture would assure the integrity of the generated reports. Moreover, the reports would be made available online which can be accessed from anywhere, that is going to save time as well as expenses of printing and would eliminate the need of carrying them along.
- **Government:** The government's influence on the healthcare system has been expanding from the past few decades [21]. The government has been playing a very important part in spreading awareness about the preventive and precautionary measures to avoid chronic diseases, which in return saves lives as well as expenses. Moreover, it is the responsibility of the government to make a budget for the healthcare sector, design policies for providing quality healthcare, and fill the present inefficiencies and gaps [22]. The healthcare industry is becoming complex every passing day, aging, chronic diseases, and pandemics have been creating the demand for the services. Because of the unavailability of a proper communication channel among the stakeholders, the management has become difficult. As the healthcare industry not only needs the diagnosis and prognosis, it also needs a safe and secure platform for keeping the patient's information. For which the government should design the regulations and compliances, to manage the healthcare industry efficiently.
- **Insurance providers:** Health insurance covers the medical expenses of the purchaser based on the type of policy they have bought. The insurance providing companies design plans that cover the payments for injuries or illness. These companies could be government or private. In today's world, it has become necessary to purchase insurance as the medical expenses are hiking and chronic diseases are prevailing. Insurance organizations have to go through a lot of paperwork, which can cause human error. Moreover, there are fair chances of getting fraudulent claims or tampered patient history. Therefore, implementing the blockchain-based system would eliminate such inadequacies and denationalize personal data. It will also speed up the process and reduce the cost of management.



### ***2.3 Issues and Challenges in Traditional Healthcare System***

It is challenging for the healthcare industry today to continuously improving the quality of the health care provided, increasing the generated revenue, and reducing the implementation costs [23]. However, there are several technologies available to deal with these challenges, but the integrity, security, and privacy of the data are still the concern. Notwithstanding all the advancements made so far, the incompetence still exists in the sector that might cause danger to the patients. As the data generated by healthcare industries is confidential, its security from the attackers is very crucial [24]. The existing healthcare systems are centralized, that makes them easy target by the attackers. Therefore, using a blockchain-based decentralized network would eliminate the vulnerability of data leakage or hacking. Furthermore, the overall reliability of the system would be enhanced as the blockchain provides immutability, traceability, time stamping, and distributed ledgers as default features.

Interoperability is also a requirement of healthcare organizations, which allows the sharing and exchanging of Electronic Health Records (EHRs), information, and technologies among several systems as well as organizations [25]. The interoperability allows the flow of the information through the organizations securely while maintaining the trust among the involved parties. The protected sharing of data would be effective in cooperative treatment and patient care by assisting in prognosis and diagnosis using collective opinions [26]. Moreover, it would also reduce inadequacies in appointment scheduling and make the collection and sharing of electronic healthcare data between the patient and doctors easier and faster while maintaining the trust. The healthcare sector is moving toward value-based care from volume-based systems. The quality of care is taking over the traditional way of measuring healthcare by the quantity of care provided. The quality-based healthcare systems are patient-centric and treat the patients with utmost importance, and keep them informed and involved in every decision.

It is necessary to control the accessibility of the data. The patients should be able to know the extent to which their data is being shared with whom. Though such features are not provided by the current healthcare systems. Traditionally, once the data is given to the healthcare provider, the patient loses all its right and the data is gone. The patient cannot take the data or rights back from the provider, which means if someone visits more than one providers in his lifetime, all of them would be holding his data permanently forever, which affects the confidentiality and privacy of the data, and make it more prone to the attacks or theft. The healthcare data is heterogeneous and big; it contains data in various formats including images of reports, documents, EHRs, diagnostic codes, etc. It is very difficult to manage this huge amount of heterogeneous data online, as no such system framework is available today that allows the storing, sharing, and retrieving of the data across the organizations and among the stakeholders. Moreover, the providers should be able to maintain trust by following the safety regulations designed by the government. The relationship between the parties should be made based on mutual trust and effective communication to assure no standards of compliance are compromised.

Furthermore, the escalating price of healthcare is also a challenge for the medical industry. This includes different services such as doctor's consultation, drugs, pathological tests. The cause of this rise is the non-existence of an appropriate framework that can track everything, and benefit each stakeholder equally. It would also help in tracking the genuineness of the medicines throughout supply-chain management. Also, it would enhance the billing and insurance claiming system by eliminating manipulation in the data and ensuring no fraudulent claims neither by the hospitals to patients nor by the patients to insurance providers. The blockchain-based healthcare systems would deliver the system that can eliminate such claims and eradicate the intermediaries, which would also reduce the administration and management costs [27]. Clinical trials or researches are also important aspects of the healthcare industry. As the new diseases are coming up every other day, it is really important to have an infrastructure that efficiently deals with the data. Since, the blockchain provides features such as immutability, time stamping, and traceability that keeps all the transactions intact and facilitate effective clinical research. It would also promote the equal participation of the stakeholders while maintaining trust and transparency.

### 3 Blockchain Technology

The blockchain technology gained wide attention when cryptocurrency Bitcoin came into existence in 2008 [1]. Since then, its application areas are evolving and several industries are adopting the network for different use cases. Researchers and scholars are investigating new dimensions and possibilities every day. Blockchain is a distributed publically available ledger that has the capability of storing transactional records immutably on a peer-to-peer-based network [28]. The implementation and concepts of such distributed networks were first demonstrated in a research work [29] in which the blocks of data that are secured using cryptography are generated and connected to form a tamperproof chain with time stamping. The concept was improvised by applying the Merkel Tree model to upgrade the storing capacities as well as the system efficiencies [30]. Though, the concepts of blockchain escalate the developments in the technology after the release of Bitcoin.

The blockchain technology has transformed several industries, a report by Price Waterhouse Cooper (PwC) mentions that the changes brought by the technology are maximum in the financial sector as compared to other sectors including industrial manufacturing, media, energy, government, health care, and consumer goods [31]. The UN has used the blockchain in its World Food Program (WFP) to create the identities of the Syrian refugees digitally and provided them with nutritional support [32]. Moreover, Walmart in collaboration with IBM has also designed a supply-chain system based on blockchain to enhance the traceability of items [33]. The healthcare industry can also be benefitted from the blockchain; the health records of the patients are confidential and needs continuity for better diagnosis and treatment. Moreover, any single error could lead to severe damage to the patient's health, therefore, the healthcare systems need to maintain the integrity of the data, which can be assured by

blockchain network as it facilitates the immutability and traceability. Furthermore, the blockchain has been successfully used in the financial sector, which would help in handling the billing and insurance claiming as well. Additionally, the ability of blockchain to keep the track of historical data would aid in clinical researches and audits.

### 3.1 Blockchain Concepts

The blockchain is a distributed decentralized network that was first used in the implementation of cryptocurrencies [1] which allows transactions between two parties without the participation of any intermediaries. The blockchain network is aided with the cryptography that assures the integrity and immutability of the transactions [34]. Moreover, the cost of implementation is also reduced in such systems as the third party is eliminated. Blockchain networks are distributed in nature that eradicates the control of any centralized authority, and also removes the fear of single point of failure that might occur in centralized networks (where the entire network crashes if the central node fails). A difference between the distributed and centralized networks is depicted in Fig. 9.2.

The records in the centralized network are kept at a central node, which is connected to all other nodes. In Fig. 9.2, the node 1, 2, 3...  $n$  are multiple ledgers that are all connected to the central node. If any discrepancy is noticed within the system, then the central node is consulted for the final decision. Whereas in a distributed system, there is one ledger only and all the nodes hold a copy of the transactions and have equal rights and access to the information. In such systems, consensus protocols are used to deal with the discrepancies, i.e., majority of the nodes agreeing on something to achieve consensus. There are several ways of achieving consensus.

The blockchain capacity is limited and its size is static because the number of blocks permitted in the blockchain is limited. The first block is known as the header

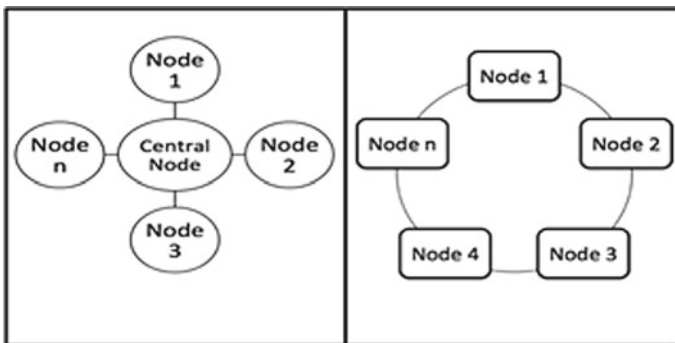


Fig. 9.2 Centralized versus distributed network

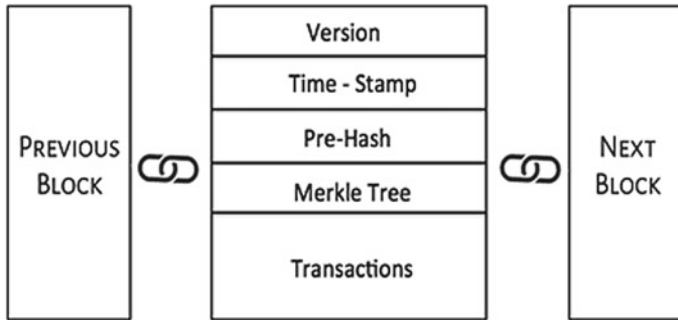


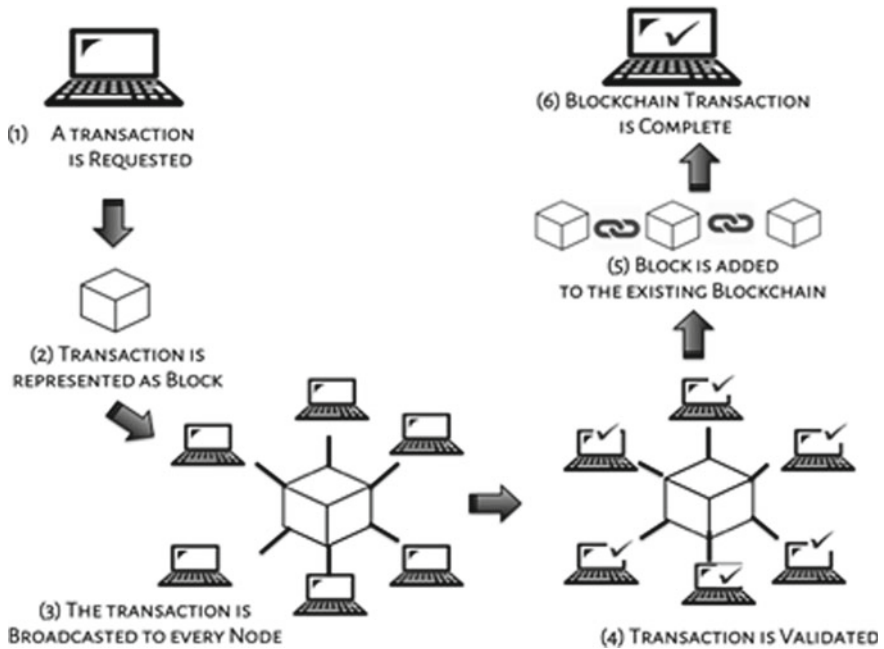
Fig. 9.3 Block structure within blockchain

block. At the time of generating a block, the data is kept in local memory within the block. Then a Merkle tree (having root value in the header block) is generated containing the transactional information. The blocks consist of a hash value that is created by applying cryptography to the previous node’s header. This also assures the connectivity among the blocks to form a chain. When the hash value is generated, the time stamping of the block is done, and the block is added to the blockchain. A basic structure of a block can be seen in Fig. 9.3.

Though the blockchain-based network is ruling the cryptocurrencies, its ability to maintain transparency during the transactions, and keeping the history of the records has made it a choice of interest in other areas as well [35]. The concept of smart contracts has made it more appealing. The smart contracts are some code that is solved automatically if the predefined terms and conditions are met. They are used for automating the transactions in the blockchain, hence eliminating the intermediaries that might be required for the same while maintaining the trust among the parties. The nodes of the blockchain-based network are peer-to-peer format and all these nodes run a function to process the transactions, and the nodes are rewarded in return. When a new transaction is made, the entire network has to agree on the consensus protocol to allow the generation of a new block; which makes it difficult for the hacker to attack the network. As to hack a block of the network, the attacker would have to attack all the blocks following it, which is impractical as would take a lot of resources.

### 3.2 Blockchain Transactions

The blockchain-based systems work distinctly for different types of applications. However, whatever be the system the flow of the data and working of the system is quite the same. The transfer of information from one node to another is termed as a transaction in the blockchain network, which follows a series of steps as shown in Fig. 9.4:



**Fig. 9.4** A blockchain transaction

Step 1: A node requests a transaction for which digital signature and the private key of the preceding transaction is used.

Step 2: A block is formed to represent the transaction.

Step 3: This newly formed data block is broadcasted to every node within the network.

Step 4: All these nodes of the network validate the transaction by solving some complex codes.

Step 5: When the code is cracked, the solving node shows all the transactions of the block that happened so far along with the time stamping to the network. Afterward, the data block is tested in context with the timestamp by all other nodes.

Step 6: In the final step, the transaction is accomplished if the transaction and time stamping are verified otherwise it is rejected.

### ***3.3 Blockchain Applications in Healthcare Domain***

To understand the application areas of blockchain technology in the healthcare industry, previous researches and works need to be analyzed and understood. From previous works, it can be found that several prototypes are still only proposed and not working in real time [36] which gives the guidelines to potentially understand

the gaps in the domain that are existing today. For the implementation of blockchain in the healthcare industry, several changes have been made to develop an equipped model. One of the most prominent application areas of the healthcare industry is the management of EHRs. The healthcare data is considered to be sensitive for the maintenance of the integrity of the records as well as sharing among the stakeholders because of the accessing permissions. Blockchain provides the default features such as trust, traceability, and transparency achieved via time stamping, cryptography, and hashing techniques. The blockchain can be used effectively for the implementation of the General Data Protection Regulation (GDPR) for maintaining data integrity during the healthcare data transactions [37].

Another application area within the healthcare domain is managing the pharmaceutical supply chain. As the number of substandard drugs is increasing in the market, it is necessary to have a system that can provide traceability throughout the lifecycle; from manufacturing to the pharmacists and then to the send-users. Since blockchain provides time stamping and immutability, it becomes easier to track the origin and avoid any kind of discrepancy/modifications. Furthermore, the blockchain could help in clinical researches, by keeping the records of trials while maintaining anonymity. Another associated application could be medical training based on data analysis and insights. IoT-based real-time monitoring of patient's health can also be implemented using a blockchain network, in which the data could be collected in real time through the IoT devices, and can be stored and analyzed on the blockchain to provide reliable and robust Patient Monitoring. The default characteristics of blockchain such as traceability, traceability, and auditability offer applications in healthcare insurance policies management. The blockchain-based infrastructure would maintain the trust between the insurance provider and the insurance holder. With all these application areas, the blockchain can be utilized in multiple ways within the healthcare sector. Moreover, it can also be integrated with other prominent technologies like Machine Learning (ML), Artificial Intelligence (AI), Big Data, and Natural Language Processing, etc. to generate more use cases within the healthcare domain to benefit the businesses and end-users.

### ***3.4 Blockchain-Based Framework for Smart Healthcare System***

The applications of blockchain technology are in several industries like finance, banking, IoT, education, etc. It can also revolutionize the healthcare sector with its advanced features [11]. The blockchain can transform the way the health records are made and stored and the businesses are organized. Blockchain is based on a distributed and decentralized environment that benefits the patients as well as other stakeholders in many ways. The use cases of blockchain technology in the healthcare industry include the management of the EHRs, health insurance claims, reporting of clinical trials, and researches for the benefits of the society globally. The security

and privacy of the data are of the utmost importance in blockchain-based systems; the data is stored in the form of blocks and within the blocks, the data is kept in encrypted form. The following are the default feature of the blockchain technology that separates it from the other leading technologies and makes its the best choice for the systems where the transparency is required.

**Decentralized Management of Data:** The blockchain network is distributed, and all the nodes within the network, having no central power or controlling authority, hold a copy of data.

**Data Provenance:** Every activity within the network is time-stamped and recorded, hence allowing the easy tracking.

**Data Availability:** A copy of data is held by every node within the network. Therefore, the data remains accessible and available all the time.

**Data Immutability:** This feature of the blockchain technology ensures that the data can never be modified within the network. Whenever a change is required, the original block remains the same, and a new block with the new information is created.

**Data Privacy and Security:** The blockchain is known for its ability to maintain the security of the data by applying encryption. Moreover, the data is kept in a distributed manner that makes it difficult for the attacker to gain access or modify the data.

Blockchain technology can model and deploy healthcare data in an efficient manner. It provides unique features such as time stamping and immutability that maintain transparency during data transactions. It can be utilized for generating several distinct application areas within the medical industry. The blockchain infrastructure can be divided into four levels as depicted in Fig. 9.5. The data is collected in different forms from various sources such as path laboratories, pharmacies, trials at the bottommost layer called raw healthcare data. The next layer is blockchain technology that consists of application platforms, protocols, consensus algorithms, etc. where the infrastructure is generated that enables secure data transactions. The third layer is the healthcare application layer, in this layer; the technologies are combined to form a single application. These applications could allow the handling of EHRs, managing supply chains, supervising telemedicine, etc. The uppermost layer is the one where stakeholders such as patients, doctors, researchers reside. In this layer, the end-users get the benefits from the applications generated in the third layer.

### ***3.5 Data Sharing in Blockchain Smart-Based Healthcare System***

There are various aspects and use cases of the blockchain-based healthcare system, resulting in distinct jobs and responsibilities including basic tasks such as generating and storing EHRs to the complicated ones like generating discharge summary or performing surgeries, etc. However, there is one thing common in all these jobs, i.e., generation and transmission of data. As it is known that the healthcare data is quite

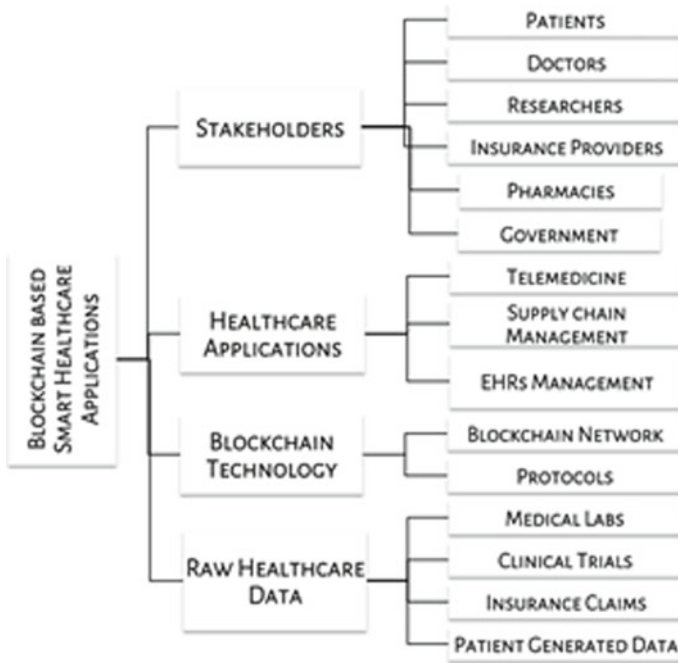
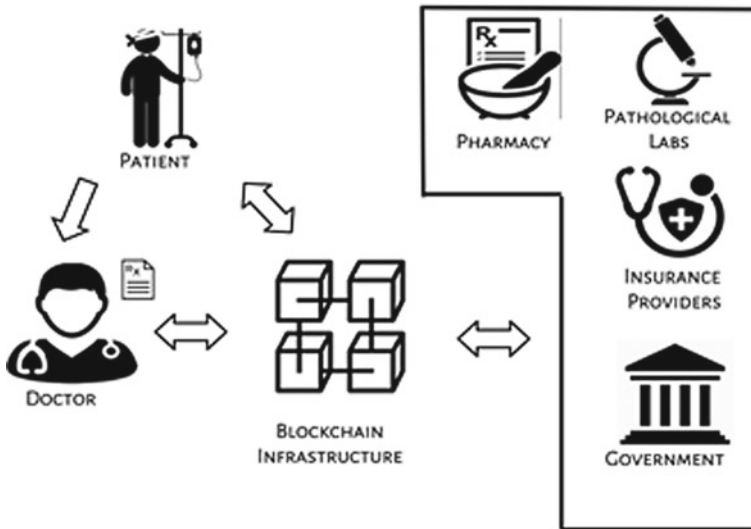


Fig. 9.5 Workflow of blockchain-based healthcare applications

complex and sensitive, the blockchain network could be used to handle the transactions while maintaining the privacy of the data and securing it from breaches and attacks. The very first step, in any medical trial, is the generation of the prescription by the doctor, based on information and history provided by the patient. The prescription could then be kept on the blockchain network, which would allow its access by the pharmacies for issuing drugs, pathological laboratories to conduct tests, insurance providers to reimburse claims, government to assure the implication of regulations along with the patient himself as shown in Fig. 9.6. Moreover, if the prescriptions would be made available on the network, the pharmacies would be able to issue medicines accordingly and maintain their inventory. Besides, if the path laboratories perform certain tests, the reports could also be made available on the network itself, which would eradicate the need for printing or carrying them. Furthermore, if all the details of the trials are stored on the blockchain network itself, it would be easier for the insurance companies to keep the track of all the procedures performed, which would decrease the number of fraudulent cases of insurance claims. The insurance providers and government would also put their regulations and policies over the network, which would make it easier for the users as well as insurance providers to verify the genuine procedures and would also provide services on time and in a transparent manner.





**Fig. 9.6** Data sharing in blockchain smart-based healthcare system

## 4 Conclusion and Future Directions

The information within the healthcare domain is of utmost importance, as the patient data is sensitive and confidential, therefore the healthcare systems are supposed to be implemented in such a way that the data is managed efficiently and effectively. The primary motivation for designing a healthcare system is to have the capability to maintain the privacy and security of the data. The healthcare data is heterogeneous, as it comes from different sources and there is no such standard system available today that can handle the data records safely.

The blockchain technology has changed a lot from its evolution. It started as a revolutionizing technology for handling cryptocurrencies but now has taken over several industries because of the features provided like transparency, authentication, traceability, time stamping, etc., which has gained the attention of various application areas and business organizations. In this chapter, an overview of the blockchain technology is presented in context with the healthcare domain. A brief discussion is made regarding the different types of healthcare along with the various components required for implementing a patient-centric model. The challenges that are faced by the traditional healthcare systems today and the ways to resolve them are also reviewed. A basic introduction of blockchain technology is made in brief that shows how it is different from traditional technologies. The blockchain-based transactions and applications in healthcare are also illustrated that would make it easier to understand how the data is transferred within the system and how the technology would transform the healthcare industry. The blockchain-based smart healthcare system is discussed next, that describes the infrastructure in tier format, followed by a brief

discussion, on how the blockchain would be placed among the stakeholders, and how the transactions would be made.

The blockchain in the healthcare domain is still in the developing phase, to make it successful, it is highly required for the researchers to start implementing instead of proposing or idealizing. Because it is not possible for now, to assess the performance of the blockchain-based applications from prototypes only. The other aspect of future work could be analyzing the interoperability; researches should be conducted to facilitate the easier sharing of the data by effectively generalizing the consensus protocols and smart contracts. Since the size of the blockchain is fixed, the other area of research could be making blockchain-based systems scalable. If all these challenges would be mitigated successfully, the blockchain-based healthcare systems would become more powerful and stabilized.

## References


1. Nakamoto S (2008) Bitcoin—open source P2P money. In: Bitcoin.org. <http://bitcoin.org/bitcoin.pdf>. Accessed 21 Aug 2020
2. Ølnes S, Ubacht J, Janssen M (2017) Blockchain in government: benefits and implications of distributed ledger technology for information sharing. *Gov Inf Quart* 34:355–364. <https://doi.org/10.1016/j.giq.2017.09.007>
3. Beck R, StenumCzepluch J, Lollike N, Malone S 2016 Blockchain—the gateway to trust-free cryptographic transactions
4. Zubaydi H, Chong Y, Ko K et al (2019) A review on the role of blockchain technology in the healthcare domain. *Electronics* 8:679. <https://doi.org/10.3390/electronics8060679>
5. Idrees SM, Alam MA, Agarwal P, Ansari L (2019) Effective predictive analytics and modeling based on historical data. In: Singh M, Gupta P, Tyagi V, Flusser J, Ören T, Kashyap R (eds) *Advances in computing and data sciences. ICACDS 2019. Communications in computer and information science*, vol 1046. Springer, Singapore. [https://doi.org/10.1007/978-981-13-9942-8\\_52](https://doi.org/10.1007/978-981-13-9942-8_52)
6. Androulaki E, Barger A, Bortnikov V, Cachin C, Christidis K, De Caro A, Enyeart D, Ferris C, Laventman G, Manevich Y, Muralidharan S (2018) Hyperledger fabric: a distributed operating system for permissioned blockchains. In: *Proceedings of the thirteenth EuroSys conference*, pp 1–15
7. Kuo TT, Ohno-Machado L (2018) Modelchain: decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks. arXiv preprint [arXiv:1802.01746](https://arxiv.org/abs/1802.01746)
8. Tseng J, Liao Y, Chong B, Liao S (2018) Governance on the drug supply chain via gcoin blockchain. *Int J Environ Res Public Health* 15:1055. <https://doi.org/10.3390/ijerph15061055>
9. Ivan D (2016) Moving toward a blockchain-based method for the secure storage of patient records. In: *ONC/NIST use of blockchain for healthcare and research workshop*. ONC/NIST, Gaithersburg, Maryland, United States, pp 1–11
10. Culver K (2016) Blockchain technologies: a whitepaper discussing how the claims process can be improved. In: *ONC/NIST use of blockchain for healthcare and research workshop*. ONC/NIST, Gaithersburg, Maryland, United States
11. Linn LA, Koo MB (2016) Blockchain for health data and its potential use in health it and health care related research. In: *ONC/NIST use of blockchain for healthcare and research workshop*. ONC/NIST, Gaithersburg, Maryland, United States, pp 1–10

12. Jiang S, Cao J, Wu H, Yang Y, Ma M, He J (2018) BlochIE: a blockchain-based platform for healthcare information exchange. In: 2018 IEEE international conference on smart computing (smartcomp). IEEE, pp 49–56
13. Benchoufi M, Ravaud P (2017) Blockchain technology for improving clinical research quality. *Trials*. <https://doi.org/10.1186/s13063-017-2035-z>
14. Walsham G, Sahay S (2006) Research on information systems in developing countries: current landscape and future prospects. *Inf Technol Dev* 12:7–24. <https://doi.org/10.1002/itdj.20020>
15. Agrawal R (2019) Predictive analysis of breast cancer using machine learning techniques. *Ingeniería Solidaria* 15(3):1–23
16. Chaudhary P, Agrawal R (2020) Non-dyadic wavelet decomposition for sensory-motor imagery EEG classification. *Brain-Computer Interfaces* 1–11
17. Chaudhary P, Agrawal R (2018) Emerging threats to security and privacy in brain computer interface. *Int J Adv Stud Sci Res* 3(12)
18. Jiang S, Cao J, Wu H et al (2018) BlochHIE: a blockchain-based platform for healthcare information exchange. In: IEEE international conference on smart computing (SMARTCOMP)
19. Sylim P, Liu F, Marcelo A, Fontelo P (2018) Blockchain technology for detecting falsified and substandard drugs in distribution: pharmaceutical supply chain intervention. *JMIR Res Protoc* 7:e10163. <https://doi.org/10.2196/10163>
20. Coelho F (2018) Optimizing disease surveillance with blockchain. <https://doi.org/10.1101/278473>
21. Straube B (2013) A role for government. *Am J Prev Med* 44:S39–S42. <https://doi.org/10.1016/j.amepre.2012.09.009>
22. Tang N, Eisenberg J, Meyer G (2004) The roles of government in improving health care quality and safety. *Jt Comm J Qual Saf* 30:47–55. [https://doi.org/10.1016/s1549-3741\(04\)30006-7](https://doi.org/10.1016/s1549-3741(04)30006-7)
23. Emanuele J, Koetter L (2007) Workflow opportunities and challenges in healthcare. In: BPM and workflow handbook, vol 1, p 157
24. (2018) 5 Major challenges facing the healthcare industry in 2019. In: Medium. <https://medium.com/@MailMyStatement/5-major-challenges-facing-the-healthcare-industry-in-2019-60218336385f>. Accessed 21 Aug 2020
25. Fanjiang G, Grossman JH, Compton WD, Reid PP (eds) (2005) Building a better delivery system: a new engineering/health care partnership. National Academies Press
26. Castaneda C, Nalley K, Mannion C et al (2015) Clinical decision support systems for improving diagnostic accuracy and achieving precision medicine. *J Clin Bioinform*. <https://doi.org/10.1186/s13336-015-0019-3>
27. Rabah K (2017) Challenges and opportunities for blockchain powered healthcare systems: a review. *Mara Res J Med Health Sci* 1(1):45–52
28. Yli-Huumo J, Ko D, Choi S et al (2016) Where is current research on blockchain technology?—A systematic review. *PLoS ONE* 11:e0163477. <https://doi.org/10.1371/journal.pone.0163477>
29. Haber S, Stornetta WS (1992) Method for secure time-stamping of digital documents
30. Bayer D, Haber S, Stornetta WS (1993) Improving the efficiency and reliability of digital time-stamping. In: *Sequences II*. Springer, New York, NY, pp 329–334
31. (2018) Blockchain is here. what’s your next move?. In: PwC. <https://www.pwc.com/jg/en/publications/blockchain-is-here-next-move.html>. Accessed 21 Aug 2020
32. Zambrano R, Young A, Verhulst S (2018) Connecting refugees to aid through blockchain enabled Id management: world food programme’s building blocks. *GovLab* October
33. Galvin D (2017) IBM and walmart: blockchain for food safety
34. Peterson M (2018) Blockchain and the future of financial services. *J Wealth Manag Summer*. <https://doi.org/10.3905/jwm.2018.21.1.124>
35. Crosby M, Pattanayak P, Verma S, Kalyanaraman V (2016) BlockChain technology: beyond bitcoin. *Appl Innov Rev*
36. Agbo C, Mahmoud Q, Eklund J (2019) Blockchain technology in healthcare: a systematic review. *Healthcare* 7:56. <https://doi.org/10.3390/healthcare7020056>

37. Idrees S, Nowostawski M, Jameel R (2021) Blockchain-based digital contact tracing apps for COVID-19 pandemic management: issues, challenges, solutions, and future directions. *JMIR Med Inform* 9(2):e25245. <https://medinform.jmir.org/2021/2/e25245>. <https://doi.org/10.2196/25245>

# Blockchain for Automotive Security and Privacy with Related Use Cases



M. Karthiga , S. S. Nandhini , R. M. Tharsanee , M. Nivaashini ,  
and R. S. Soundariya 

**Abstract** Nowadays, smart vehicles are getting manufactured in such a way that it can communicate with other smart devices or smart vehicles through wired or wireless technologies. Such high range of communication expressed by the smart vehicles makes many existing tasks easier to the vehicle owners and also introduces new features to increase the ease of the vehicle usage for the owners. Further, this high degree of communications also paves road for security threats which makes the smart vehicles highly vulnerable to privacy attacks like location tracking, remote hijacking of the vehicle. Such security attacks on smart vehicles not only questions the security of the vehicle, it also has greater effects in the safety of the passengers. Also, it is obvious that smart vehicles do have lot of sensors, cameras, devices like GPS and others which produce huge volume of data to be sent to the drivers or to the other sensor or devices connected to it. Such data carries sensitive information that needs to be protected to avoid privacy breach. So security is very important in dealing with smart vehicles. Traditional security and privacy strategies used in smart vehicles are not efficient to meet the threats that the vehicles are fronting mainly because they follow centralized mechanism to extend the security. Blockchain technology provides a decentralized, distributed ledger technology that maintains a chain of blocks to provide security and privacy. Blockchain provides security from all dimensions, and hence, it is popular in crypto-currencies, smart contracts. Each communication is referred as transaction in blockchain technologies and the transaction will be broadcasted to all participating nodes of the transaction for the verification and

---

M. Karthiga (✉) · S. S. Nandhini · R. M. Tharsanee · M. Nivaashini · R. S. Soundariya  
Bannari Amman Institute of Technology, Sathyamangalam, Tamil Nadu, India  
e-mail: [karthigam@bitsathy.ac.in](mailto:karthigam@bitsathy.ac.in)

S. S. Nandhini  
e-mail: [nandhiniss@bitsathy.ac.in](mailto:nandhiniss@bitsathy.ac.in)

R. M. Tharsanee  
e-mail: [tharsanee@bitsathy.ac.in](mailto:tharsanee@bitsathy.ac.in)

M. Nivaashini  
e-mail: [nive19794@gmail.com](mailto:nive19794@gmail.com)

R. S. Soundariya  
e-mail: [soundariya@bitsathy.ac.in](mailto:soundariya@bitsathy.ac.in)

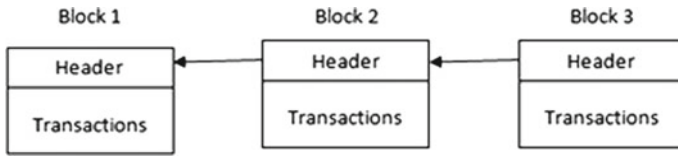
once verified the transaction will be added as new block to already existing blocks. To overcome the drawbacks in the traditional automotive security, blockchain technologies can be implemented to meet the requirement for the automotive security and privacy. The blockchain is formed by chaining the time-stamped blocks one after the other and a block includes the hash of the previous block in the blockchain. Hence, any changes made in a block will be notified easily by propagating changes in the hash of the following blocks. This feature makes the blockchain a better technology for automotive security. Additionally, blockchain enables the user to have flexible public key system, which makes the tracking ability of the user a tough task and hence protects the privacy of the user. Moreover, blockchain has its own reasons, why it cannot be implemented readily in automotive industry. The reasons be like, delay in getting verifications from participating nodes, where vehicles cannot wait so long to make decisions if there is delay. Other reasons may include scalability issues when there are more nodes involved in a transaction and what if there is increase in the number of nodes. This chapter reveals about the utilization of blockchain in automotive security in automobile sectors.

**Keywords** Automotive industry · Blockchain · Vehicles · Digitalization · Vehicle security · Automotive security · Vehicle tracking · Data sharing · Smart contract · Vehicle security attack · Privacy, security · Supply chain · Intermodal transport

## 1 Introduction

Nowadays the people possessing the vehicles experience a wide variety of sophisticated services offered by smart vehicles which are capable of connecting with each other. Whenever there is enhancement in technology, there will also be a security issue related to the technology. Similarly, the increased capability of the vehicle makes them exposed to security problems that may include tracking the location of the vehicle without their consent or controlling the vehicle. Blockchain—as a technology—serves many more applications like smart contracts, virtual currency, etc., and the same technology can be used to address the security issues of the smart vehicles. This includes tracking and maintaining all the small details about the vehicles like updating software in the vehicle, insurance renewable, approval and claiming process and such related activities.

Roadside infrastructures are highly updated to cope with the smart vehicles on road, and hence, the vehicles can establish connection with traffic management, other vehicles around, other smart devices, and obviously the Internet. Thus, the vehicles contribute to the Internet of Things and the security in doubt. The security issues are not only related to the vehicle but it may also affect the safety of the passengers. When the smart vehicle establishes a connection with other device or vehicle and shares information, then the sensitive information about the vehicle is at high risk like the location of the vehicle.



**Fig. 1** Basic structure of blockchain

The traditional methods and technologies used in securing the vehicles from security attack have become obsolete because of the advancements in technologies. For example, the security of the current smart vehicles is maintained in a central server may be a cloud. Here, the security is in doubt since it is centralized and also handling the security of highly increasing number of smart vehicles is not possible. Also, the vehicles require identification, authorization and authentication to maintain the security through connected vehicles or devices. Also, a smart vehicle that involves certain level of automation in driving has to highly secure. The traditional security system has no system to preserve the privacy of the automation in driving and thus will have high impact on the safety of the passengers.

To overcome the main security threat that all associated data being centralized, blockchain would be the best choice. It follows decentralized databases to store and process the vehicle associated data. As already discussed, blockchain has a series of blocks chained together as shown in Fig. 1 and it was successfully implemented in bitcoin. Blockchain provides good security and privacy, and hence, it can be used in automotive industry to meet the challenges.

Each node in the chain is identified by a public key and all the data transfer among the nodes are done by encrypting the data using the public key of the node. So it authenticates the sender node to all the other nodes in the network of blockchain. This is how blockchain provides security and privacy to the vehicles and hence decentralizing the sensitive data associated with the smart vehicles.

Among the collection of pending transactions, set of transactions will be grouped and a block will be created and notified to the entire network of nodes. So once the blocks are created and entered the network, then it cannot be modified. The node may change its public key after each transaction to ensure higher level of security. The anonymity of the public key used by the nodes provides good privacy.

## ***1.1 Challenges***

Besides the security provided by blockchain, it also has its drawback in getting deployed in automotive industry and they are the following.

- Scalability;
- Computational power;
- Latency;

- Throughput.

### **Scalability**

Since all the transactions and the newly created blocks have to be broadcasted to all the nodes in the blockchain, the transaction overhead will be high. Also, the number of nodes will get increased rapidly and hence the blockchain will have scalability issues and also the bandwidth of the smart vehicles would be too low to manage the broadcasting overhead.

### **Computational Power**

The algorithms maintaining the blockchain need more computational power and smart devices possess very low computational power, and hence, there would be a big gap in computational power when implementing the blockchain in automotive industries.

### **Latency**

The verification for the completed transaction needs a stipulated amount of time where it takes almost thirty minutes in the case of bitcoins. But adjusting to this high latency is not possible when the interconnected smart vehicles are very close to each other that is in very close proximity.

### **Throughput**

The efficiency will be computed based on the number of transactions mined per second in the blockchain. The interconnected smart vehicles will produce large number of transactions, and hence, the mining time would be high and in turn it decreases the throughput.

## **2 Blockchain Requirements in Automotive Industry**

Recent advancements in automotive industry include blockchain in semi- or fully automated vehicles, their security and privacy as discussed already. This brings in real-time monitoring systems to monitor the vehicles and to achieve the reliability and scalability in data sharing. Blockchain technology can change or can ease areas in automotive industry like supply chain, selling, rentals and many more important functional areas in automotive industry. The main requirements for blockchain in automotive industry are many and few are discussed here.

Supply chain management—it covers all the activities, stakeholders, from manufacturing to delivery. Blockchain can be used in all the steps in supply chain management systems of automotive industry. For example, take a use case where there is a failure in a vehicle and if the vehicle is manufactured from automotive industry with



blockchain involved supply chain, then it is easy to trace back to the actual cause which leads to the failure of the entire vehicle and again the same failure will be stored as a transaction and hence it helps in identifying the further break downs of the same vehicle.

Truthfulness and security—this ensures the trust ability of the system where the transactions that are done previously will not be changed. Also, it ensures that no attempt will be made to change the past data to overcome the present challenges and problems. Also whatever new transactions are made then that are made as a new block and updated to the chain as discussed already.

Mobility—this ensures that the framework should actually allow the smart vehicles to initiate and perform data sharing in all situations without being affected. This scenario is not possible with system being deployed in centralized systems and hence decentralized autonomous system is a solution to achieve mobility.

Uncompromised security—as the term states security should not be compromised in any of the extreme situations that are not expected to happen. With smart vehicles being more autonomous, data sharing among the connected vehicles are very common and hence the security is in threat. Blockchain technology will ensure the uncompromised security in all the situations among the connected vehicles during the data transfer. Again the data is chained as blocks and hence sharing and storing everything would be transparent.

Verification—verifying the blocks in blockchain is important since it is immutable. Once the blocks are created and added to the chain, then it is not possible to modify the block and hence verification of the blocks is possible and very easy when it is implemented using blockchain technology.

Maintenance and services—ensures the services after the delivery. If blockchain-enabled automotive industry delivers a smart vehicle, then it ensures the automation in billings and payments and insurance related issues and claims. Hence, the maintenance and service tracking will be made easy for the company people.

Transparency—when there is a centralized system, it is not possible to provide transparency of data for the involved parties. In decentralized systems, since there is no centralized control over the data, it is possible for all the stakeholders to access to the required data and also the same will be immutable as we have seen already.

Speed and cost management—if a system is implemented in a centralized architecture, then the control will be in a single entity and hence there will be more burdens on the entity to process all the lined up requests to be reflected in the centralized system. Since the blockchain provides a decentralized environment, the control will be distributed and hence all the processing will be in different entities and so the burden will not be on a single entity. This will decrease the time required to do the process and improves the speed.

### 3 Technologies in Automotive Industry

One of the biggest technologically advanced industries by means of hybrid vehicles, self-driving cars and electric vehicles is the automotive industry which highly relies on Industrial IoT (IIoT) for the latest innovations on connected vehicles. According to the paradigm of Industry 4.0, automotive industries are completely undergoing digitalization that in turn leads to inefficient operation and security breaches leading to cyber-attacks, losses, overblown prices for parts and expensive services. These issues are faced by industrial sectors to individual vehicle owners in automotive life cycle.

With the evolvement of Industry 4.0, there has been a tremendous growth in automotive industry with respect to modern sensors, big data application techniques, improved connectivity and computational perspective, new machine learning techniques to increase the smartness of the vehicles, new computational aspects like fog computing, edge computing, smart interfaces for humans and machines [1–3], updation in IIoT, advancements in robotics and emergence of 3D/4D printing technology. The advancements of automotive sectors in increasing the connectivity and approaching towards autonomous vehicles in turn enhance the security concerns which are a big challenge to cyber security. A vehicle could be endangered with malicious attacks which not only affects the vehicles but also with the passengers 'safety as well'. An attack is proposed by Miller and Valasek [4] on a Jeep with a wireless system thereby attacking and controlling the vehicles' core functions remotely. Providing strong security is a must in these kinds of autonomous and controlled systems.

The future automotive investments according to Frost and Sullivan forecast [5], the automotive IIoT expenditure is tend to increase to 36.7 dollars by 2025 with 11.5% increase in Compound Annual Growth Rate (CAGR). Added to it, the automotive digital retail of IoT spend will grow at a rate of 29.1% CAGR and data analytics business will enhance at a rate of 35% in 2025. Furthermore according to a strategy from original equipment manufacturers, the road map reveals that the digital transformation will change the business models from using Car as a Service (CaaS) to Mobility as a Service (MaaS) in the near future around 2030 where the vehicles are positioned as things in the connected systems.

Nowadays, blockchain techniques revolutionized the Internet, facilitating the usage of Internet rather as an information source to a value source by formation of new peer-peer distributed and shared economy [6, 7]. By 2029, nearly 10% of the gross domestic product (GDPs) worldwide will be saved through blockchain technique as per the report from World Economic Forum survey [8]. Blockchain technology facilitates a decentralized platform for the automotive sectors in maintaining the information related to insurance, ownership records, repairs, maintenance of the assets securely and recording/tracking the ownership of tangible/intangible assets.

The blockchain ledgers are integrated and this ensures the transactions among the customers of automobile industries in a secure manner. The accurateness and immutability facility of the blockchain facilitates efficient smart contract solutions

and maintenance of concrete supply chain. Big empire of opportunities and business systems like automation through IoT [9–13], smart-charging of electric vehicles, peer-peer lends, predictive maintenance and forensics advancements, leasing, financing and new models like MaaS are ensured through the facility of verifying the data and accessing it in real time by blockchain.

In [14], the authors' details about the security breaches handled by blockchain. Access control through cloud is focused in [15]. Management of user-identity in cloud-based blockchain applications are proposed in [16]. In smart-grid communications, the security is guaranteed through the use of blockchain as suggested in [17]. In [19], secure payment through cyber-physical system (CPS) [18] is proposed. When informations are shared across multiple industries, lot of cyber-attacks are possible and the way to avoid it is presented in [20]. The reviews about blockchain techniques specific to content-centric networking for increasing the security in 5G vehicles are illustrated in [21].

## 4 Supply Chain Management

Planning, manufacturing of product to delivery, marketing information and customer services are integrated in supply chain management or logistics in manufacturing industries. Logistics is more like a framework involving the product flow and related information for a business whereas supply chain framework deals with the management of business including the upstream and downstream relations among the customers and suppliers with an overall objective to deliver superior products to the customer at a low cost [22]. Supply chain also includes two major criteria: value chains and demand chains. Value chain involves effective management of the business with an aim of satisfying in all aspects with greater value. Demand chain insights the importance of delivering value products to the end customers [23].

One of the important aspects in the supply chain is transportation since all the manufactured products have to be delivered to various sectors of the industries finally reaching the end customer. Since the manufacturing sectors and business sectors are rarely located in the same location, transportation plays a significant role in supply chain management [24]. Product costs reduction and quality improvements with speedy manufacturing and delivery are one area that could be achieved by integrating transportation in the supply chain process as per [25]. Integrating transportation in supply chain management is one of the most important tasks to reduce the costs and to improve the customer satisfaction according to [26].

According to researchers, intermodal transportation is more like process cycle description [27], while some narrates it as value delivering strategy with a result of delivering customer decisive end-product and service [28]. Intermodal transportation is more like a service than technology as suggested by [29]. Different definitions

and aspects from diverse researchers insist the importance of intermodal transportation in supply chain sectors. Nowadays intermodal transports have grown a lot in manufacturing industries due to the advancements in shipping and door delivery services.

This triggers the development of infrastructure, vehicles and equipment with an aim of delivering the quality product to the customers [30]. Four factors that drive the revolutionary change in intermodal transportation include hyper-competition, end-user requirements, advancement in information and communication technology (ICT) and administration and combination of infrastructure and possessions [31]. Blockchain plays an important in managing and maintaining the processes of supply chain in an effective and secure manner thereby facilitating end-to-end customer service and satisfaction.

In disparity to the references cited above, the chapter projects a holistic strategy to blockchain in automotive sectors including the design of block chain-based strong cyber security applications and a thorough analysis on deployment and optimization of blockchain techniques for automobile industries. Added to it, the aim of blockchain in transforming the automotive industry worldwide by tackling the challenges associated with it is also presented.

Blockchain has attracted good attention in the field of automotive industry in the recent years. All of the concepts concerning the application of blockchain in automotive industry are in theoretical phase and need to be transferred to real-time products or services in order to generate growth in the production of various business cases. The major issues in the automotive industry are concerning security and privacy of the data shared in the blockchain network. Smart contracts in blockchain have the capability to resolve the security issues posed due to data sharing in connected vehicles.

## **5 Data Sharing in Connected Vehicles**

In coming years, vehicles are anticipated to interact more with the internet thus gaining more ability to transfer with each other and with the infrastructure of the road in the surroundings. This technological innovation would enable vehicles to accumulate sensible information regarding conditions of the road that the vehicle is passing by and to identify the traffic situations that persist in the current scenario. Additionally, this type of connection of vehicles with Internet will progressively facilitate a widespread range of accessibility services to the consumers, to collect instant map as well as traffic data for the current city and to even find an accident. This type of connected vehicles through Internet will also be able to transmit data which is being gathered by itself through sensors to storage like cloud. This data in turn can be used for a variety of applications and would attract more attention from various service providers. There are two important factors to be taken care with respect to data sharing in connected vehicles, one being the advantage gained by the vehicle's owner with the collected data and the second factor is the severe privacy

problems that can be incurred due to this shared data. There are possibilities for the transmitted information to be used in ways to exploit the privacy of the vehicle owner directly to investigate the behaviour of the user.

There are three specific ways in which this collected information could be used in an effective way.

- (i) *Benefits for vehicle owner:* The information gathered through connected vehicles could be used in such a way that it reaps some benefits to the vehicle owner who has consented to reveal the vehicle information
- (ii) *Monetary benefits:* The vehicle data will be of more interest to third-party companies who would utilize this data as inputs for their current applications and algorithms. This in turn can produce monetary benefits to the owner.
- (iii) *Benefits for Service providers:* Service providers can make use of this information to existing services or can plan for new services based on the vehicle information.

Besides this, there are lot of improvements made in the automotive industry through digitalization, development of autonomous cars that runs on the road and the advent of Internet of Things which involves sensors which communicate information via Internet. The downsides still exist in the automotive industry with respect to the safety and security of the information that are being collected from the vehicles.

## **5.1 Vehicular Data Sharing Environment (VDSE)**

The key entities of vehicular data sharing environment are manufacturer of the vehicle, owner/user of the vehicle, insurance provider and data consumers who act as the stakeholder for this system. All stakeholders will not be interested in the same type of vehicular data as there are several aspects involved such as information pertaining to vehicle driver, information pertaining to vehicle itself, information pertaining to the usage of the vehicle. For instance, considering the case of a map provider it is evident that information regarding vehicle driver/vehicle itself is of less importance to them and information regarding usage of the vehicle is most significant.

Information particularly about the specifics of the vehicle will be more useful to vehicle developers/manufacturers that will not show much interest towards vehicle owner data. Thus, it is clear from the proposed vehicular data sharing environment that data required by services varies according to the needs and only certain data can be enabled according to the specific services. In this manner, privacy is a major concern in a connected vehicle as the entire collected dataset will not be shared with a service provider but relatively only the data which is explicitly essential for the service to be offered.

## 5.2 Security Issues in Sharing Vehicular Data

The growth of connected vehicles in the worldwide market is significant for the recent past years due to the revolutions that occur in the automotive industry. This also poses a serious threat to the security concerns as there are many sensors embedded in vehicles. There is a high potential for theft of personal information. The potential hackers will take charge of the operational aspects of the vehicle like braking and steering systems. As the automotive manufacturers are highly dependent on supply chains for the different parts of the system, there is a high risk for security vulnerability. Poor cryptographic key management system from the manufacturers end is also another reason contributing for the security problems.

## 5.3 Privacy Issues in Sharing Vehicular Data

As previously stated, driver of the vehicle will be compensated by service providers through monetary benefits for sharing the vehicular data. In certain cases, connected vehicles and service provider may transfer data in an insecure way when the service providers engage in malevolent activities by making wrong use of the collected information. Thus, there arises a primary need to address the issues concerning security and privacy in a vehicular data sharing environment. A service provider should be given permission to acquire only the appropriate vehicular data as per the service requirements [32].

In certain cases, the performance of the driver while driving the vehicle can have negative behaviour leading to legal or social concerns. Violent driving nature will create bad consequences socially if the data is shared to everyone. Secondly, it can also take legal effects when the information is passed on to police officials. When drivers realize these details, they may not be willing to share the data collected from the vehicle owing to the negative reverberations. The state-of-the-art regarding privacy and trust is discussed in few existing literatures. In [33], Walter et al. briefly focussed on the necessity of a mechanism for privacy-aware data sharing.

Privacy concerns on vehicular data can be resolved by sharing the data to service providers in one of the following four stages of information sharing,

- (i) *No sharing*: This type of sharing is adopted when no data regarding the vehicle will be shared to anyone.
- (ii) *Semi sharing*: This type indicates sharing only the primitive data for performing statistical analysis but not more than that.
- (iii) *Partial sharing*: This category signifies sharing the data about the vehicle without revealing the personal identity of the user.
- (iv) *Full sharing*: This type of sharing involves making all the data publicly available.

## 6 Proposed Schemes

In order to deal with the security and privacy problems involved in sharing the vehicular data, the proposed system makes use of blockchain technology to facilitate secure as well as privacy-aware way of sharing the data about the connected vehicles. The first approach concentrates on securing the messages while the second approach concerns about the maintenance of privacy between the parties involved in sharing and using the vehicular data such as the vehicle owner and service provider. The following sections highlight the techniques proposed to implement the secure and privacy-aware methods of sharing vehicular data.

### 6.1 Workflow of Blockchain-Based Secure Vehicular Data Sharing

In this proposed system, the vehicles are tracked based on the geographic locations. This system comprises of components such as connected vehicles, traffic administrator, publisher and prober. Figure 2 shows the architecture model of blockchain-based secure vehicular data sharing. Each location consists of publishers to provide the essential authorizations for the connected vehicles using suitable signature schemes. Once the authorizations are provided, the vehicles become capable enough to produce signed messages. A secret key will be given by the probers of each cluster  $probe_{set}$  using a secret distribution scheme. Whenever a fraudulent message is identified, then  $probe_{set}$  will be requested to provide the credentials about the source of the message.

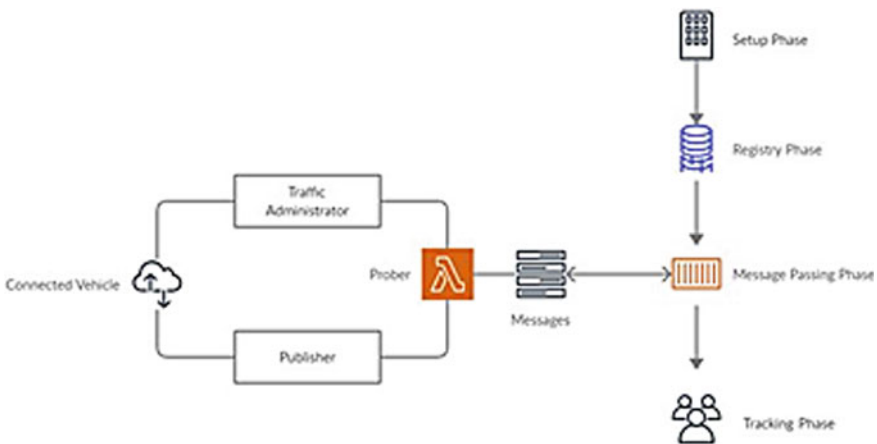


Fig. 2 Secure vehicular data sharing model

This scheme consists of two types of blockchain namely primary blockchain and supplementary blockchain. The primary blockchain is connected to all the components involved in the system architecture while the supplementary blockchain is connected to the specific locations. A smart contract exists between the primary and supplementary blockchain to assure the data reliability. The workflow of secure vehicular data sharing comprises of four phases namely setup phase, registry phase, message passing phase and tracking phase.

## **6.2 Setup Phase**

This phase begins by initializing the primary and supplementary blockchain and deploying a smart contract to ensure data reliability between the two blockchains. The next step is to select the publishers and probers for each location. The publisher generates the set of public keys  $\{P_{k1}, P_{k2}, P_{k3}, \dots, P_{kn}\}$  and these keys will get stored in the primary blockchain.

## **6.3 Registry Phase**

This phase is for registering the vehicle details soon after it gets into the system. The vehicle information under goes a verification process to ensure the authenticity of the details. Once the vehicle passes the authentication test, it will be provided with the public key already generated and stored in the primary blockchain.

## **6.4 Message Passing Phase**

Different types of messages will be transacted to the primary or supplementary blockchain depending on the scenarios. Connected vehicles usually gather information regarding the current conditions of the road via sensors. The collected information is broadcasted as messages, and there are chances for counterfeit messages to be broadcasted. A vehicle owner will be rewarded or punished based on the legitimacy of the messages transacted to the blockchains. The reward or punishment will be on the basis of monetary benefits. The message generated from particular location goes into the supplementary blockchain associated with that region.



## **6.5 Tracking Phase**

This phase is essential when severe consequences like accidents occur due to the counterfeit messages broadcasted by vehicles. In such cases, to track the identity of the involved stakeholder, the public key associated with the vehicle will be fetched based on which the details of the vehicle owner will be tracked down.

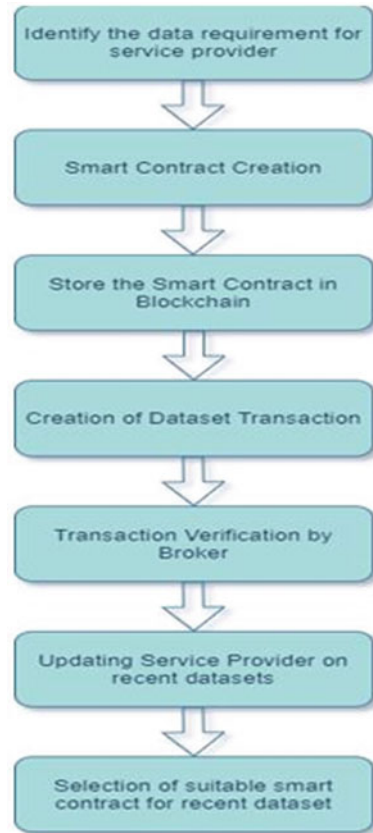
## **6.6 Workflow of Blockchain-Based Privacy-Aware Vehicular Data Sharing**

This section sketches the idea about the workflow of privacy-aware vehicular data sharing based on blockchain technology rather than providing the architecture or highlighting any tools. It is evident from the prior discussions that a vehicle can produce a huge amount of data and the owner of the vehicle may choose to share the collected data with the service providers based on sharing schemes discussed in previous section. The proposed idea as shown in Fig. 3 makes use of the concept of smart contracts in blockchain in order to identify the service that needs to access the data from a particular vehicle and what type of data should be shared.

This smart contract is similar to an agreement which will be signed between the vehicle owner and service provider. The role of blockchain technology is to assure that the smart contract is not fiddled and to make this contract accessible to the brokers. Brokers in turn are responsible for creating an online repository for storing the data gathered from the vehicles in a more secure manner. These brokers are also responsible for deciding upon the access rights for the service providers to fetch the data for the particular service without violating the smart contracts. In addition to that, the brokers are also required to administer safe connections for transfer of data from the vehicle to the online repository along with ensuring secure connection while transmitting the data from the online repository to the service provider. In order to ensure such type of safe and secure data connections, appropriate protection mechanisms such as Transport Layer Security will be adopted.

To accomplish the tasks stated earlier, more than one broker will be involved and the vehicles will also be permitted to move from one broker to other to transfer data to brokers located at different places. The main motive of employing blockchain technology is to provide tamper-resistant loading of smart contracts and transactions. Also, to guarantee the legitimacy of the data that is stored in the online repository which is gathered from the vehicles. In order to ensure the legitimacy of stored data, every transaction is incorporated with a hash performed on the gathered information. These types of transactions can act as a prompt to inform the service providers about the recent vehicular data that is available. From the technological perspective, it is actually not advisable to store data right into the blockchain. It should also be taken into account that smart contracts signed initially between the involved parties can be

**Fig. 3** Workflow of the smart contract blockchain



retracted or withdrawn and a different contract may be created between the owner of the vehicle and the service provider.

There are two important components that will be stored into the blockchain, such as smart contracts and the transactions. Smart contracts are used to store the information regarding the vehicular data that is exchanged with the service provider and it also contains the information about the reward for that particular data exchange. This contract will carry the broker information on which broker holds the data collected from the vehicle and also denotes the duration for which the service will be provided the right to use this data. As a thumb rule, the smart contract should be signed by the owner of the vehicle and service provider before it is loaded into the blockchain. Another significant component that will be stored in the blockchain is the transaction which is a hash of the vehicular data and stored in the online repository. This transaction should also be signed by the owner of the vehicle and by the broker before it gets stored in the online repository.

The proposed vehicular data sharing environment provides a safe and secure interconnection between the vehicle providing data and the service provider in a way

to preserve the privacy. To assure this secure connection, brokers are used to control the access of the service provider to the vehicle information.

Figure 3 depicts the workflow of the process carried out to store the vehicular data into blockchain. The various steps involved in the storage and retrieval of vehicular data using blockchain can be summarized as the following. These are the important phases for distributing data from a vehicle to a service provider in the proposed vehicular data sharing environment.

- (i) *Identify the data requirement for service provider:* In this stage, the service provider who is in requirement for data will get in contact with the owner of the vehicle after identifying the specific data requirements for certain service. This is an important step as the data requirements for a particular service must be well defined in order to facilitate the appropriate service.
- (ii) *Smart contract creation:* The user analyses the requirements stated by the service provider and agrees upon to sign a contract stipulating the connection between the owner of the vehicle and the service provider and thus acknowledging to share the vehicular data with respect to the requirements of the service provider.
- (iii) *Storing the smart contract:* Once the smart contract is signed between both the parties such as vehicle owner and service provider, the next step is to store the created contract onto a blockchain for providing a safe and secure way of transmitting the vehicular data.
- (iv) *Creation of Dataset Transaction:* When the vehicle is in the running status, it will automatically collect data and this data will further be separated into datasets. These individual datasets are then transmitted in an encrypted format to the online repository created by the broker. Every dataset that is transmitted to the repository will have two entities namely the digital signature of the owner of the vehicle along with the hash of the transferred dataset.
- (v) *Transaction Verification:* The role of the broker is to authenticate that there is no alteration made in the dataset that is transmitted. Broker should also be very cautious not to make any changes in the received dataset as it would affect the signature of the vehicle owner which is on-hand. On completing the successful verification of the dataset, the broker will include his own signature and pass the transaction on to the network of blockchain.
- (vi) *Updating Service Provider on Recent Datasets:* Blockchain will be regularly monitored by the service provider in order to identify if any latest datasets are available which are applicable for their service requirements. If the service provider finds a suitable transaction, then the broker will be immediately contacted to request for the vehicular data.
- (vii) *Selection of suitable smart contract:* Once the recent dataset is found, then the appropriate smart contract corresponding to the dataset will be selected on the blockchain network. Thus, the service provided gains right to use the data applicable as per the smart contract. If the relevant smart contract is not available then, the request made by the service provider will be rejected.

## 7 Privacy and Security in Driver-Specific Automotive Blockchain

Nowadays private blockchains are utilized in many private organizations where data is more sensitive and valuable. Like other industries, the automotive industries also gain setting of private blockchains for handling its sensitive data like maintaining its drivers' records and driving capabilities for producing quality drivers to the public. By closely supervising the driver's activities, the owners could issue notice in case of anomalies detected from the data. These private blockchain assures in maintaining the driver's data in a more secured manner and the confidentiality of records become the basic building architecture of these private blockchains.

The driver's details-specific blockchain would collect the data, closely monitor the data and diagnose anomalies from the performance of the active driver. The usual anomalies are like exceeding the speed limit, crossing the borders, smoking, drunk and drive, etc., and if these are diagnosed, indispensable actions are taken against the drivers. The data regarding the vehicles is captured from various resources and stored in separate blocks as mentioned in Fig. 4. The data measured in this blockchain is speed of the vehicle and location of the vehicle. The speed of the vehicle data is measured periodically using special speed monitoring sensors and those collected are stored in individual blocks. Similarly, the location of the vehicle is captured through GPS and stored in respective blocks. Headers are used for identifying the data stored inside the blocks and these are used during data retrieval. Other data like crossing

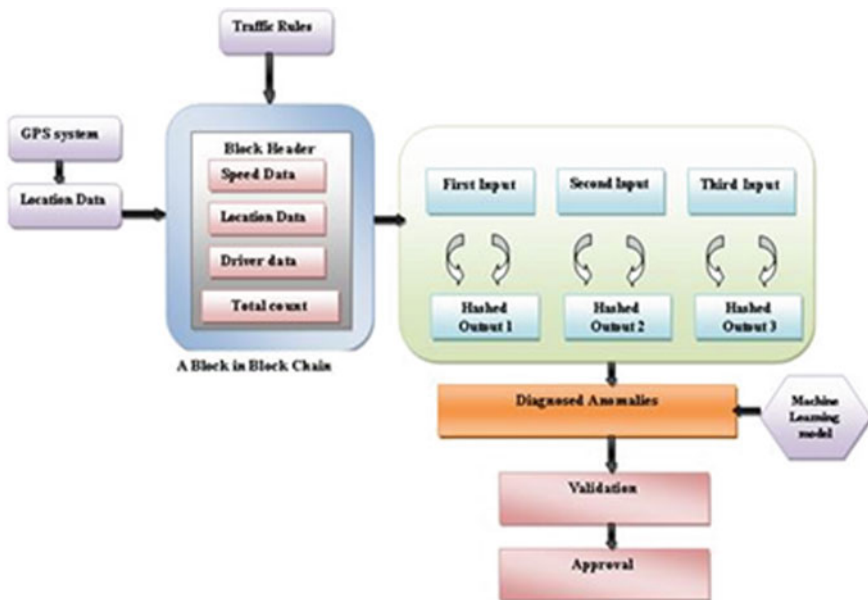


Fig. 4 Operational workflow of private driver-specific blockchain

the speed limit in particular areas, violating the traffic rules, are also maintained in separate blocks. The old data that are gathered in the blockchain is moved periodically to the cloud and removed after a particular time frame to satisfy the space issue. Each transaction in the blockchain keeps track of the data that is coming in and out. The data that is gathered under each transaction is the combination of speed as well as location data. The data gathered is rehabilitated into block hash periodically. The block hash reveals about the details of the data collected at every single instance. Further the data is collected and stored using the previous hash value which adds an additional advantage in blockchains. The output is nothing but a result of machine learning model which compares the actual data with collected data to diagnose the anomalies in the data and these are provided as recommendations from the blockchains.

The data is gathered from various sensors in the vehicles and then stored in the blocks of the blockchain for analysis like maximum speed limit allowed, following traffic rules properly and location of the vehicles by comparing with collected data and recommended data. The gathered data includes current speed of the vehicle, duration taken to reach the destination, current condition of the road used and location. This data is analysed in the blocks using some machine learning algorithms like support vector machines to diagnose the anomalies. After diagnosing the anomalies, the respective driver details are collected and checked. Once obtaining the driver details, the data is sent to the authorities for validation and action. The whole process is taken place within a single blockchain and within few seconds. The data is secured by hashing the data with a unique hash code. The data is transferred only among the respective authorities and this holds a unique feature of private blockchains.

## ***7.1 Transactional Data***

The data is collected from the vehicles and from real-time GPS system and compared with allowable traffic rules within a single block of the blockchain. The time period for collecting the data can be set according to the user requirements. Data from each vehicle is saved in individual and unique block nodes and the type of data collected with respect to time differs according to the vehicles. The individual nodes never exchange their data with other block nodes this in turn adds security and avoids data duplication in private blockchains. The data that is gathered at a particular time frame is stored in blocks and hashed to produce block hash. Block hash is a function for collecting data and stores it together under a common string value inside a block. The data is always appended with the previous blocks hash value so any change in the data could easily be identified in the blocks. Adding block hash protects the data with high security and this hash code is generated with more computational power which is difficult to break in case of attacks.

## 7.2 Data Analysis

Data collected from blocks is undergone to anomaly detection using any machine learning models. The machine learning models detect outliers for the new incoming data if it does not fall under a particular distribution. The machine learning model is trained well with lot of training data to increase the accuracy. The model is trained with different kinds of data to best suit any circumstances. If any anomaly is detected for a new incoming data, the details are immediately transferred to the respective authorities for validation and action. The data is transferred to the third party periodically or once detecting an anomaly.

After diagnosing an anomaly, the third-party agency compares it with current traffic rule and decides upon the issue of action or not against the driver. The driver's historical data is also compared in this case before issuing the notice. This kind of manual checking also adds accuracy to the complete system. Then, the driver is noticed by the respective government agencies after back checking process. Once notice is issued, the details are updated in the blockchain for future reference by creating a label. This data can be further reviewed by the government agencies in future while issuing vehicle licence or driver's licence renewal. The data collected across such private blockchains in automotive sectors are tamper-proof as the data is gathered directly from the vehicles and false-proof. This system is more accurate and reliable compared to camera-based system.

## 8 Applications of Blockchain Technology—Explore New Use Cases

Business utilizations of blockchain innovation have an application pace of over 25% across ventures from banking to medicinal services. As it were, the straightforwardness and inventiveness of blockchain applications are transforming numerous commercial productions. The most generally utilized real-world application is in cryptographic forms of money and digital individuality administration. A blockchain system's capacity to deal with protected trade exchanges provides incomparable worth in numerous ventures.

Every now and then, the manner in which organizations work changes. In this day and age, general clients request more straightforwardness and safety for the exchanges they are engaged with. Studies demonstrate that financial specialists and clients are progressively disposed towards decentralized trade plans, tokenized trade plans and decentralized utilizations. Blockchain innovation with its innate characteristics like straightforwardness, unchanging nature, and responsibility empower a few organizations to embrace decentralized items, stages to serve its clients better.

The accompanying subsections give an exhaustive clarification of different uses of the blockchain innovation together with its utilization cases.

## **8.1 *Banking and Financial Industry***

Uses of blockchain for banking commerce and monetary commerce are utilized by creating the money-related exchanges quicker, less expensive, straightforward and progressively safe. Blockchain innovation would disturb these enterprises in a remarkable way. The fundamental standards of blockchain innovation make it truly adaptable, and accordingly, it can provide answers on the way to make business activities progressively proficient, safe and consistent. The innovation, which supports cryptographic forms of money, like bit coin, was primarily given with incredulity by banks. Still, this has transformed drastically. This distributed innovation permits us to do cross-fringe settlements spilling out of one nation to another with modest exchange expenses and enormously decreasing the period needed for it. Then again, one of the most exceptionally foreseen utilizations of the blockchain, smart agreements makes the offer exchanging more safe than conventional agreement law. Additionally, it can remove the broker in exchanges and in this way, it decreases the quantity of exchange costs related with contracting. The principles of the smart agreement are documented in PC code and cannot be easily deciphered by ‘the plan of the agreement’, however just as indicated by the exacting significance. Let us find insight concerning the distinctive utilization cases of blockchain for banking and money commerce.

### **(a) *Quicker and easier cross-boundary expenses***

Cross-boundary expenses are presently a basic piece of a large number of lives so we progressed in the direction of a globalized ecosphere. Cross-boundary transmission of cash, esteem has consistently been a moderate procedure just as costly. As huge, cross-boundary expenses become increasingly normal, B2B dealers are searching for the more helpful and cost-proficient techniques. This has pulled in a greater amount of these exchanges to the network and portable stations when related with customary banks and specialists-based stations blockchain-based answer for doing digital currency exchanges can accelerate and shorten the expense procedure, removing a lot of the conventional brokers and furthermore lessens the expenses fundamentally. In this result, a computerized dispersed exchange record with matching duplicates is kept up on every one of the system’s individuals’ PCs. All gatherings can survey past passages and record new ones. Exchanges are assembled in blocks, documented in a steady progression in a chain of blocks. The connections among blocks and their substance are ensured by cryptography, so past exchanges cannot be crushed or faked. This implies the record and the exchange is trusted without a chief power.

## **8.2 *Broker-Free Stock Marketing***

Purchasing and marketing shares and stocks have consistently included numerous brokers, like mediators. These procedures include multifaceted systems which are tedious, cost incompetent and inclined to dangers. One of the most intensely foreseen

utilizations of the blockchain, smart agreement is a PC program that encourages and implements the procedure and execution of a contract. Numerous sorts of legally binding statements can be made self-performing or potentially self-authorizing utilizing smart agreements meanwhile these copies the basis of normal authoritative conditions. Smart agreement-based answer for stock exchanging is safer than conventional agreement law. Additionally, they can remove brokers in exchanges and therefore decrease various exchange expenses related with agreement. The guidelines of the smart agreement are documented in PC program and cannot be easily deciphered by ‘the purpose of the agreement’, however just as per exacting significance.

### ***8.3 Individuality Management Resolution***

Handling client individuality in real time is a costly and tedious procedure. The client needs to enlist online for the administration which may need extra advances like an up close and personal association as may be the situation with money-related establishments. The client ought to likewise validate their sign in this manner demonstrating that they are approved to get to that entryway. It turns out to be monotonous when the client needs to experience these equivalent paces with each original amenity supplier. Notwithstanding to be monotonous, it likewise increases safety worries as these amenity suppliers collect large measures of individuality data with them. Blockchain-dependent individuality management resolution takes care of this issue by removing all the outsiders. The client would enlist on the blockchain and, as essential, approved gatherings can basically get to that data on the system. This wipes out the requirement for the client to enrol with each original amenity supplier. Whereas finest procedures for this utilization are as yet being created, it demonstrates capability. Still, security stays a worry as soon as data is warehoused on blockchain; it is open to everybody in the system, that unlocks a novel path for further study.

### ***8.4 Crypto Reliable Coupons***

Traditional reliable and top projects do not understand its maximum capacity because of a few components such as inoperativeness of client account, least reclamation charges and period intervals in conveying prizes and focuses, maximum exchange price, maximum client obtaining expenses and least customer maintenance and so on. Blockchain as a confidence less distributed ledger permits reliability reward database suppliers, managers, framework directors, clients, and so on to converge and interface in one framework without any mediators and without trading off security or intensity. This arrangement upgrades the implementation and organization of remuneration programs with close to continuous straightforwardness, bringing about cost reserve funds. In this blockchain-dependent reliability program, on commencement of a reliable exchange, like the issuance, recovery or trade of a prize, the framework



makes a PC created reliable coupons, which is a basis for a wide range of remunerations, including focuses. The reliability coupon's remarkable identifiers can be refreshed on every member's record and made accessible over the system. A few real-time conventional guidelines oversee the manner in which the focuses behind these coupons work. Besides, the framework can be associated with online life and advanced wallets and can communicate with reliability rewards program stages via 'smart agreements' to give bother free conveyance of dependability focuses.

## 8.5 *Real Estate*

The real estate division is presently seeing developing enthusiasm from purchasers after almost a time of moderate development since the extraordinary downturn in 2008. Individuals are currently ready to contribute more, because of the improved money-related situation of economies and adaptable financial choices. Consequently, the expanded attention additionally carried with it a higher pace of fake practices. We regularly know about land tricks, like twofold marketing of a land, fake of records, name debates and so on. What could be possible to counter these wasteful aspects? We accept the answer and stay with blockchain. Joining blockchain in land can change the part. By encouraging computerized data to be distributed yet not duplicated, blockchain innovation set up a spine to share esteem. Despite the fact that the innovation was initially invented for the digital money, Bit coin, businesses globally are now discovering other possible usages for the innovation. Additionally, it turns out innovation which is the greatest fit to tackle huge numbers of the problems looked in the land business.

## 8.6 *Automation Using Smart Agreements*

Smart agreements are a lot of guidelines in an electronic organization that moves data and satisfies the agreement terms and conditions consequently. They act in a decentralized situation with no human impedance. It eliminates the boundary among the advanced and physical world. The advantages of smart agreement are as per the following:

- Automation of lease instalments;
- Automation of duty instalments from the exchanges;
- Automation of benefit sharing structure land bargains.

### (a) **Property Registries on Blockchain and Effective Name Proprietorships**

Property registry in blockchain structures tries to correct proprietorship debates in land by making the possessions name as a constraint credited to a coupon—which

can combine open library subtleties, like dimensions, GPS directions and development or buy year and so on. Trade of coupons can be followed at whatever point it transforms via a sequence of purchasers or financier businesses. At the point when the possessions are at last traded, the exchange yield for the past proprietor is documented and warehoused and an exchange yield for the recent proprietor is made. In this circumstance, whether someone wants to recognize the proprietor of a land, they could basically experience the exchange history—starting from the preliminary exchange and finishing at the open exchange yield. Likewise, the present proprietor would have the option to confirm possession by ‘marking a message’ with their confidential key related with that address on the blockchain.

The basic takeout at this time is, this tool gives a simple, safe approach to enrol and move possessions. To engage the total pattern of computerized land exchanges, certifiable digital signs of a property officer, in addition to signs of purchasers or dealers are utilized for move and offer of a land. This whole sequence can be effectively overseen by a blockchain-dependent library. Blockchain consequently can turn into a necessary piece of land enrolment businesses and can make a straightforward land administrative and consistence structure. Consistently universally, this can bring about investment funds cost billions of dollars, consequently joining of blockchain in land administrations are here to advance the development of this business in the upcoming years.

#### (b) **Escrow Open Expenses and Bank Transactions**

Conventionally, escrows are utilized for land exchanges to set up the aspect of faith among the purchaser and vender in an exchange. This is expensive in addition to tedious procedure. Regardless of whether there is an absence of faith among the two gatherings associated with an exchange, the blockchain can deal with the procedure without bringing on any strain. The exchange can be executed with a smart agreement, wherever an accord among the purchaser and vendor is needed to activate the agreement to discharge the assets to the vender. In a blockchain framework, every client has an exceptional character that implies the customer money related data can be distributed safely with different gatherings during exchanges. Regardless of whether the assets have been transmitted by the purchaser, it will not be discharged to the dealer while waiting for the exchange is officially finished. The safety offered by the blockchain accelerates the exchange executive’s procedure. Regardless of whether the purchaser and merchant are not in a similar spot, the property financing is accelerated by the presence of a money-related record for each gathering.

#### (c) **Tokenizing Possessions**

Tokenization is a technique to change privileges of a benefit into a digital token. By tokenizing resources, this present reality resource could be computerized in the blockchain. Essentially, tokenizing a possession implies creating a token on a smart agreement and provides an incentive to the token in resemblance to the genuine resource. Tokenization begins the entryway for additional interests in the land part. In spot where valuable individuals had the option to put resources into high-esteem

land bargains, tokenization opens the entryway for anybody to put resources into limited quantities. The advantages of tokenization are as per the following,

- Simpler to increase finances;
- Numerous purchasers can cooperatively purchase possessions;
- Easy to distribute proprietorship of income from resources.

## 8.7 Insurance

At first, blockchain was utilized distinctly as an open exchanges' record. Consequently, the innovation experienced adjustments when technical and business specialists understood the potential utilizations of blockchain in different commercial segments. Nowadays, blockchain is classified into the open blockchain, private blockchain and consortium blockchain (semi-decentralized). For a considerable length of time, a reasonable utilization of blockchain innovation in the insurance business has stayed just in principle. Though, now, with the correct usage of decentralized ledger innovation, functional in addition to efficient answers for improving numerous procedures in the insurance business is reasonable. In the insurance business, blockchain exhibited guaranteeing utilizations to improve areas like shared protection, small scale protection and parametric protection. Real-world utilizations of blockchain in the insurance business are disturbing the manner in which the protection exchanges are taken care of.

### (a) **Automobile/Possessions/Fatality Insurance**

The serious issue looked at by this part is collecting the important information to assess and process privileges. Currently, this is a mistake inclined procedure as it includes a great deal of physical information section. Additionally, it also needs appropriate synchronization among various gatherings. By permitting the policyholders and guarantors to follow and oversee physical resources carefully. Utilization of blockchain in the insurance business can systemize the cases preparing through smart agreements. It additionally retains a perpetual review trail, envision that an individual encounters with a mishap. To recuperate from the misfortunes, they need to present a case to the insurance agency. The insurance provider will at that point want to look at the case. In a blockchain system, when an individual takes an insurance policy, the insurance providers will have their identifications (smart agreements) incorporated with the blockchain—with the goal that the instalments will be activated depending on explicit circumstances. Subsequently, this permits policyholder cases to be handled effectively and dependably. At this time, all the gatherings engaged with the exchange implement its essential handling exercises utilizing pre-set up smart agreements.

### (b) **Health Insurance**

The individual well-being records of clients could be programmed and warehoused on the blockchain. It is finished with a confidential key, so they are just available by specific people, in this way guaranteeing security. By setting up a smart agreement among the patient and the insurance agency, the cases procedure can be rearranged. For the safeguarded, the smart agreement will self-execute once the clinical method has been finished. For this, all the constraints referenced in the agreement must be satisfied. The bills of hospitalization will be warehoused on the blockchain. At that point, it will be naturally directed to the insurance suppliers as evidence of conveyance (fills in as a proof of idea).

## **8.8 Health Care**

With the possibility to bring a progressive just as transformative changes, blockchain is relied upon to turn into a distinct advantage in the human services division too. Here, the need is to ensure that the patient's well-being is not undermined. The need of great importance for social insurance entrepreneurs is to cut out the superfluous cost that is related with maintaining the business without settling on the nature of administration they offer. The following sections discuss the different parts of blockchain innovation in the medicinal services segment.

### (a) **Public health monitoring**

Corner to corner we have emergency clinics and well-being establishments. A large portion of the information gathered from every one of these establishments is not shared outside, clearly because of security reasons. Be that as it may, approaching all the information consolidated from all the well-being foundations can assist specialists with deriving valuable data. For instance, the event example of an illness or the geological impact of a specific pandemic. We do not yet have such a framework which binds together information from all the sources since well-being associations are wary to share their information because of security concerns. Be that as it may, the arrangement is to construct a blockchain organization where all the well-being establishments can record information without uncovering touchy data. The system offers a seal just as permanent stockpiling. Blockchain innovation is an incredible asset to jolt a framework where trust is the key component. By utilizing blockchain innovation, administrative bodies can share the patient data without uncovering the personality of the patient or some other touchy data. This stream will assist specialists with identifying the pandemics or dangers so they can take fundamental activities to control the issue in a convenient way.

**(b) Data security**

Information security is a significant worry in the social insurance area. The objective of using blockchain in the social insurance area is to bind together and adjust the medicinal services encountered while supporting secure clinical record sharing. Clinical and well-being records have gone advanced in the previous barely any years and now it is undeniably increasingly defenceless against burglary—and unquestionably progressively significant to programmers, who can sell a total clinical record for more than \$1000 on the dark net. It is evaluated that everybody in the United States will have had their social insurance information undermined by 2024 if online robbery continues quickening at the current pace. Blockchain innovation presents the answer for protecting data and can keep unapproved access to data from an unapproved party. Blockchain can be utilized to separate information into pieces and store it in an appropriate arrangement, encode the information with the goal that solitary approved faculty to approach it and in addition, circulate records over a system so that all documents are accessible, regardless of whether some portion of the system is down. Building up such a framework will expand security in the clinical, pharmaceutical ventures.

**(c) Consent for information sharing**

Patient data is accumulated over a progression of individual exercises, well-being exercises, restorative assistance methods and furthermore from clinical and hereditary testing administrations. Every patient claims their remarkable electronic well-being chain (EHC). With blockchain innovation, the patients can pre-approve data imparting to real suppliers and specialists who can utilize the snippets of data at the hour of crises without really pre-sharing the information. They can give certain scrambled keys to the suppliers, research faculty who need to get to the information.

**(d) Simplified billing and claiming process**

Billing and maintaining claims are a procedure containing documenting and handling of clinical cases that are identified with the patient's analysis, medicines and drugs. Well-being establishments can offer straightforward and trustable charging to their client blockchain innovation. In such a framework, each charging occasion is recorded in the straightforwardly disseminated record which can be gotten to by patient, specialists and the administration. The administration cannot charge a penny extra to the patients since each demonstrative charging data is recorded in the system. The patient on other hand has straightforwardness of when they are charged for what sum. This framework can likewise be incorporated with the insurance agencies to such an extent that they would auto be able to start the protection claims dependent on the symptomatic data added to the system and the approvals given by the specialists for every one of the determination. The entire procedure of charging and guaranteeing can be computerized through keen agreements. This gives another experience to the patients as far as trust capacity.

## 8.9 *Automotive Industry*

Automobile industries have continually grasped earth shattering innovation answers for understanding difficulties in different sectors, for example, supply chain, manufacturing, logistics, client care, sales and everything in the middle. With 4.8% yearly development, this industry sees fast footing across geologies and is one of the hotbeds for innovation advancements. Blockchain can profit the car industry from multiple points of view. Utilizing smart agreements and IoT, businesses can robotize a few procedures engaged with vehicle deals, administration, guarantee (claims) preparation and considerably more. In addition, it helps the purchaser and lender to evade brokers or outsiders to include in exchanges or protection claims. This decentralized record innovation can assist with building a condition of serenity in clients, makers and administration focuses with its straightforwardness and unchanging nature. The utilizations of blockchain in the car business extend from crypto tokens to give reliability prizes to their clients to flexible chain perceivability arrangements that can hold the honesty or provenance of the vehicle. Keeping up a carefully designed log of all records, for example, administration logs, subtleties of mileage of extra parts and so forth can assist the producer with estimating the real resale estimation of the vehicle. Let us find in detail which parts in the car biological system are first going to be impacted by blockchain.

### (a) **Targeted vehicle recalls**

Vehicle makers regularly issue review notices to their clients when there is a deformity in the conveyed vehicle which could influence the travel security and safety. Tragically, most vehicle makers cannot remarkably distinguish each part in each vehicle sold, so they have to give the review for 1000 s of vehicles regardless of whether the faulty parts are introduced distinctly on a couple of vehicles. This procedure is lost cash to the producer; besides, it brings about upsetting 1000 s of clients. A blockchain-based framework that empowers the vehicle producer to particularly recognize each and every part will spare an immense measure of cash in the occasion a future review is required. Since the maker will realize which imperfect part was fitted to which explicit vehicle, they will have the option to give explicit reviews for individual VIN numbers. This could set aside a ton of cash and time for the makers.

### (b) **Identification of counterfeits**

Out of benefit, some assistance places and carports are purposefully fitting fake extra parts to vehicles. This, thus, influences the brand notoriety of the maker when these fake parts fail to meet expectations or even glitches. Utilizing a blockchain-based chain framework, the provenance or really of extra parts can be handily confirmed. The supply chain framework associated with IoT sensors and brilliant gadgets would empower administration focus, maker and the client to follow the realness of the extra parts by confirming each progression in the flexible chain to its unique assembling

date and area. Such a framework can give full recognizability of extra parts and furthermore help the protection and guarantee screen groups to distinguish fakes rapidly.

**(c) Automated Insurance Claim Processing**

Overseeing client identification online is a costly and tedious procedure. The client needs to enrol online for the administration which may require extra steps like an eye-to-eye connection as may be the situation with money-related organizations. The client ought to likewise confirm their sign in along these lines demonstrating that they are approved to get to that entryway. It becomes monotonous when the client needs to experience these equivalent strides with each new service provider. Notwithstanding being redundant, it additionally raises protection worries as these service providers store gigantic measures of personality data with them.

Blockchain-based identification management systems tackle this issue by removing all the outsiders. The client would enrol on the blockchain and as required, approved gatherings can basically get to that data on the system. This takes out the requirement for the client to enrol with each new service provider. While best practices for this application are as yet being created, it shows potential. Be that as it may, security despite everything stays a worry as once data is put away on blockchain; it is available to everybody in the system. That opens up another road for research.

**(d) Crypto loyalty tokens**

Reward programs are a typical instrument for driving client engagement, maintenance and extra income over an assortment of sectors, including the car sector. The failure of current unwavering programs causes the reward programs to go unutilized. Dedication programs are once in a while incorporated and the capacity to accumulate esteem is constrained. There is a requirement for a common database to oversee high volumes of exchanges and empower permission access and program execution so faithfulness commitment serves the two purchasers and the various associations with which they cooperate. On a blockchain-based faithfulness program, on commencement of a devotion exchange, for example, the issuance, reclamation or trade of a prize, the framework makes a PC produced dependability token, which is a base for a wide range of remunerations, including focuses. The faithfulness token's one of a kind identifiers can be refreshed on every member's record and made accessible over the system.

**(e) Faster transactions**

The process of payment for a vehicle buy is very tedious. The producer needs to hold up a long time before instalment for the delivery of vehicle is received. The postponement is brought about by numerous gatherings engaged with the instalment procedure, for example, a credit letter from buyer's bank or even receipt and archives confirmation process which includes a great deal of administrative work. The exact history of the data like important vehicle information, banking details, due investment

information, number of dues left, etc., could be easily managed and maintained by the vehicle producers using a blockchain framework.

(f) **Authentic service records**

Service record and maintenance of a vehicle assumes a significant job in assessing the resale estimation of the vehicle just as encourages producers to approve the protection claims. Be that as it may, the administration records are not totally secure.

These records can be produced, altered or controlled either by the client or outsiders to profit undeserving credits. A blockchain-based framework would authorize organization occasions subtleties to be put away in a common documentation that all gatherings move towards. Openness in data about a vehicle's administration history empowers the optional purchaser, or the maker to all the more likely assesses the vehicle. Also, genuine mileage enables the back suppliers to confirm about the usage level and the remaining usage estimation for a vehicle during the agreement date.

## 9 Future Enhancements

Availability of more blockchain architectures for different fields and organizations makes visible that it is easy to integrate to automotives. Also, it is to be noted that blockchain is still an emerging technology where there may be scope for many more surprising elements in the future which may do wonders in automotive companies. However, there are lot more dimensions to be considered for its deployment in an automobile industry.

Interoperable IoT platforms—IoT is widely used in many fields like home security, health care, smart city projects, transportation management systems and many more. Integrating this with blockchain may bring in significant improvement in security and maintenance of the data involved in the above said areas.

Customizable environment—users may be provided with an option to customize their needs based on the services offered. The user of the smart vehicle can decide what it is actually required and able to customize it based on the requirement is real joy for the users.

Smart contracts adaptability—many industries find difference and difficulty in maintaining the smart contract structure and standards as it involves so many to be hidden details that need not to be visible for their competitors and hence an adaptable smart contract structure will be very much useful.

Scalability—when there are more and smarter vehicles in future, then the length of the blockchain will be exponentially higher and to mine and maintain such larger blockchain requires a simpler system.



Standards—since blockchain is readily adaptable in all fields, it will be very helpful if there is a common standard like a government regulations for certain process. This will make all organizations to follow the standard instead of developing their own formats and structures.

## 10 Conclusion

Blockchain in automotive industry ensures security and also reduces the stress of being following up the business needs from other parallel industries and to other stakeholders involved in the supply chain of an automotive industry. Blockchain architecture provides a shared framework for all possible transactions in an industry and hence maintaining the data and worries of keeping the integrity of the data are minimalized since everything is transparent among the stakeholders of the business. Also, it increases the data sharing among the supply chain entities which reduces the time, cost and enhances product protection. On the other hand, since the entire system is decentralized, overhead on the single entity is highly reduced. Implementing blockchain in automotive industry enables the system to achieve unparalleled security amidst the challenges and requirements to implement it in the automotive industry.

## References

1. Blanco-Novoa O et al (2018) A practical evaluation of commercial industrial augmented reality systems in an industry 4.0 shipyard. *IEEE Access* 6:8201–8218
2. Fraga-Lamas P et al (2018) A review on industrial augmented reality systems for the industry 4.0 shipyard. *IEEE Access* 6:13358–13375
3. Fernández-Caramés TM et al (2018) A fog computing and cloudlet based augmented reality system for the industry 4.0 shipyard. *Sensors* 18(6):1798
4. Miller C, Valasek C (2015) Remote exploitation of an unaltered passenger vehicle. Black Hat, USA, p 91
5. Frost & Sullivan Digital transformation of the automotive industry digitalization spending to grow rapidly to \$82.01 Billion in 2020. Available online <https://store.frost.com/digital-transformation-of-the-automotive-industry.html>. Accessed on 3 August 2018
6. Tapscott D, Tapscott A, Cummings J (2016) Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world. Random House, LLC
7. Fernández-Caramés TM, Fraga-Lamas P (2018) Design of a fog computing, blockchain and IoT-based continuous glucose monitoring system for crowdsourcing mHealth. *Multi. Dig. Publishing Instit. Proc.* 4(1)
8. World Economic Forum. Deep shift technology tipping points and societal impact. Survey Report, September 2015. Available online [http://www3.weforum.org/docs/WEF\\_GAC15\\_Technological\\_Tipping\\_Points\\_report\\_2015.pdf](http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf). Accessed on July 2018
9. Hernández-Rojas DL et al (2018) Design and practical evaluation of a family of lightweight protocols for heterogeneous sensing through BLE beacons in IoT telemetry applications. *Sensors* 18(1):57

10. Froiz-Míguez I et al (2018) Design, implementation and practical evaluation of an IoT home automation system for fog computing applications based on MQTT and ZigBee-WiFi sensor nodes. *Sensors* 18(8):2660
11. Hernández-Rojas DL et al (2018) A plug-and-play human-centered virtual TEDS architecture for the web of things. *Sensors* 18(7):2052
12. Blanco-Novoa O et al (2018) A cost-effective IoT system for monitoring Indoor radon gas concentration. *Sensors* 18(7):2198
13. Fernández-Caramés TM, Fraga-Lamas P (2018) Towards the Internet of smart clothing: a review on IoT wearables and garments for creating intelligent connected e-textiles. *Electronics* 7(12):405
14. Dai F et al (2017) From Bitcoin to cybersecurity: a comparative study of blockchain application and security issues. In: 2017 4th international conference on systems and informatics (ICSAI). IEEE
15. Sukhodolskiy I, Zapechnikov S (2018) A blockchain-based access control system for cloud storage. In: 2018 IEEE conference of Russian young researchers in electrical and electronic engineering (EIConRus). IEEE
16. DeCusatis C, Zimmermann M, Sager A (2018) Identity-based network security for commercial blockchain services. In: 2018 IEEE 8th annual computing and communication workshop and conference (CCWC). IEEE
17. Mylrea M, Gourisetti SNG (2017) Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security. In: 2017 resilience week (RWS). IEEE
18. Fraga-Lamas P (2017) Enabling technologies and cyber-physical systems for mission-critical scenarios. Ph.D. dissertation, Dept. Electrónica y Sistemas, Univ. A Coruña, A Coruña, Spain
19. Zhao Y et al (2018) Secure pub-sub: Blockchain-based fair payment with reputation for reliable cyber physical systems. *IEEE Access* 6:12295–12303
20. Rawat DB et al (2018) iShare: blockchain-based privacy-aware multi-agent information sharing games for cybersecurity. In: 2018 international conference on computing, networking and communications (ICNC). IEEE
21. Ortega V, Bouchmal F, Monserrat JF (2018) Trusted 5G vehicular networks: blockchains and content-centric networking. *IEEE Veh Technol Mag* 13(2):121–127
22. Christopher M (2011) Logistics and supply chain management. Pearson Education Limited
23. Hoover Jr WE et al (2002) Managing the demand-supply chain: value innovations for customer satisfaction. Wiley
24. Chopra S, Meindl P, Kalra DV (2013) Supply chain management: strategy, planning, and operation, vol. 232. Pearson, Boston, MA
25. Mason R, Lalwani C (2004) Integrating transport into the supply chain to improve supply chain performance. In: Proceedings of the 9th logistics research network conference
26. Morash EA, Clinton SR (1997) The role of transportation capabilities in international supply chain management. *Transp J* 5–17
27. Muller G (1989) Intermodal freight transportation
28. Everett S (2002) Deregulation, competitive pressures and the emergence of intermodalism. *Aus. J. Public Adm.* 61(3):19–26
29. D'Este G (1996) An event-based approach to modelling intermodal freight systems. *Int J Phys Distrib Logistics Manag*
30. Hoyle BS, Knowles RD (eds) Modern transport geography. Belhaven Press, London
31. Dewitt W, Clinger J (2000) Intermodal freight transportation. Transportation in the New Millennium
32. Kaiser C et al (2018) Towards a privacy-preserving way of vehicle data sharing—a case for blockchain technology? In: International forum on advanced microsystems for automotive applications. Springer, Cham
33. Walter J, Abendroth B (2018) Losing a private sphere? A glance on the user perspective on privacy in connected cars. In: Advanced microsystems for automotive applications 2017. Springer, Cham, pp 237–247

# Blockchain Technology: Developers Cultivate Novel Applications for Societal Benefits



Sheetal Zalte and Rajanish Kamat

**Abstract** Blockchain, a buzz word in the second decade of the current century, is a decentralized technology enabling facilitation of distributed ledger with immutable transactions, updated time-to-time at every node. The beauty is such an absence of centralized authority, transactions, or digital assets that can be shared across a P2P network. This technology was conceived way back in the 90s by a group of researchers. Though the primary aim was for time-stamping documents, after two decades, in 2009, the first blockchain, i.e., bitcoin came into the market and soon became the talk of the time. Other popular cryptocurrencies in blockchain such as Ethereum, Litecoin, Ripple, and Stellar also emerged in the form of intangible currencies working on the very principle of cryptography. These days, Ethereum has become more popular since it is featured prominently for “smart contracts” for decentralized and self-executing agreements. There are so many advantages of blockchain over the traditional system. Blockchain is enriched by its dominating characteristics such as decentralized, distributed, secure and faster, transparent, immutable and insusceptible to tampering. Every node in blockchain can propose new transactions, to validate this transaction consensus mechanism play a crucial role in a structured way, i.e., proof of work and the proof of stake mechanism. Thus in a nutshell blockchain is a cutting-edge technology that proves it is time-saving, cost-saving, and rigid security. It is also advantageous over inefficient, expensive, and vulnerable transactions. It creates resistance against fraud, cybersecurity attacks without involving centralized authority. Moreover, it is secure with a cryptographic shield that contains a hash function, public-key cryptography, and digital signatures, and so on. Though phenomenal growth of blockchain in various applications like cybersecurity, supply chain, online data storage, networking, IoT, insurance, government, multimedia, and real estate is witnessed, few domains remain untouched by developers and tech savvies. The sole aim of this chapter is to focus on such untouched domains, besides showcasing the evolution of this novel platform. This chapter aims to cover the basic essence of

---

S. Zalte (✉) · R. Kamat  
Shivaji University, Kolhapur, India  
e-mail: [sheetal.zaltegaikwad@gmail.com](mailto:sheetal.zaltegaikwad@gmail.com)

R. Kamat  
e-mail: [rkk\\_eln@unishivaji.ac.in](mailto:rkk_eln@unishivaji.ac.in)

blockchain with basic architecture and working principles. The societal applications will be dealt with in-depth. The chapter will present a lucid flow of the blockchain technology details with the potential for further exploration.

**Keywords** Blockchain · Digital asset · Peer-to-peer network · Smart contract · Ethereum

## 1 Introduction

Blockchain has become synonymous with banking, investing, cryptocurrency, and so many other domains of business especially in the span of the last decade. The blockchain evolved from the bitcoin network is known for the key attributes mainly distributed, decentralized, and being used as a public ledger. Blockchain innovation is creating noteworthy enthusiasm over a wide scope of enterprises in India. As the field of utilizations for blockchain develops, industry pioneers are modifying and fitting the innovation to fit different use cases. The basic notion of the blockchain has been as diverse as the basic technology itself which is expressed as the chain of blocks wherein the blocks, i.e., digital information is stored in public databases viewed as a chain. Scholarly literature covers define blockchain in a variety of ways [1]:

The main attributes of the dimensions of blockchain technology are as shown in Fig. 11.1.

- Digital, public ledger that records online transactions
- Cryptocurrencies like bitcoin

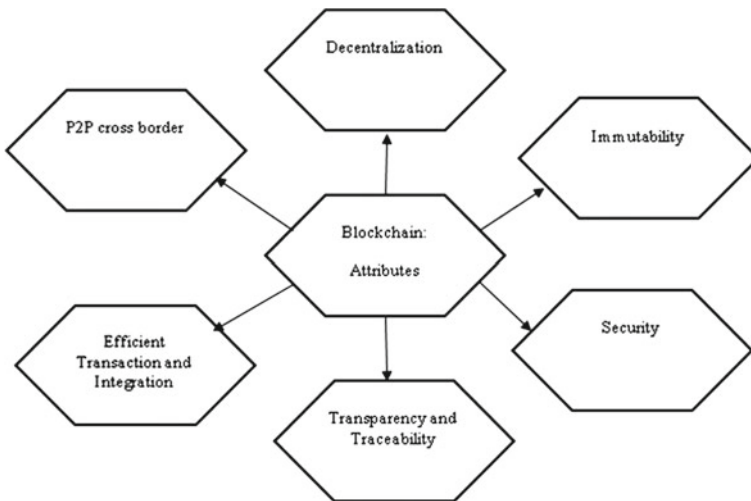


Fig. 11.1 Key attributes of blockchain technology

- Integration of a cryptocurrency through encryption, validation, and recording of transactions
- Openness as well as accessibility to the user [2].

### ***1.1 Blockchain: Key Attributes***

- (a) Decentralization
- (b) Immutability
- (c) Security
- (d) Transparency
- (e) Traceability
- (f) Efficient transactions
- (g) Simpler integration
- (h) P2P cross-border transfers.

Yet another fundamental revelation of the blockchain expressed in its basic definition is in the form of distributed ledger that marks permanent and most secure transactional data record by the way of its functioning as a decentralized database deployed on many servers in a peer-to-peer (P2P) network, each of them maintaining a copy to mitigate a single point of failure (SPOF). The beauty of the entire interface is simultaneous updating and validation of the records [3].

As a companion peer-to-peer arrangement joined with a dispersed time-stamping server, blockchain databases can be managed autonomously. There is no requirement for a different executive. As a result, the clients are the administrators. The distributed ledger technology that began with bitcoin is quickly turning into a publicly supported framework for a wide range of checks.

At present, the team has effectively gone live with blockchain applications which have been instrumental in demonstrating the plausibility and pragmatic advantages of executing blockchain. One such important execution was for a crowdfunding application for a social government assistance organization that was created utilizing the Ethereum stage empowering the application to get straightforward, changeless, and fabricate upgraded trust in the framework. Another arrangement that has been generally welcomed is birth and death registration utilizing blockchain for a district in West Bengal which improved, security and made it a misrepresentation free framework, making more prominent trust in administration applications. Blockchain has additionally been utilized as an apparatus for making more noteworthy network commitment and support in one of our tasks which included tokenizing web-based life movement. The group has additionally dealt with a pilot for Land Title Mutation in blockchain utilizing hyperledger fabric, which has planned to mechanize the procedure of land procurement and make an unchanging review preliminary.

Then again, the group is working on new use cases to infiltrate new markets utilizing blockchain. A portion of these utilization cases incorporate shared (P2P) banking arrangements, drug traceability, controls framework (blockchain evaluating apparatus), bank guarantee applications, to give some examples. We are on

a consistent post for new regions where blockchain can take care of the current issues or improve the current design. After covering the basic concepts regarding the blockchain technology, it will be logical to portray its advantages.

### ***1.2 What Are the Key Advantages of Blockchain?***

Blockchain innovation has a couple of key focal points over our present framework, which incorporates the way that it is above all else, decentralized, implying that there is no overseeing body over it. It is additionally totally straightforward and can be extremely simple to review or follow, in addition to it is liberated from information adjustment or altering. Also, the blockchain's information is scrambled, making it exceptionally difficult to hack into.

### ***1.3 What Challenges Does India Face with Blockchain Tech Adoption?***

While the eventual fate of blockchain appears to be splendid and promising, it is as yet viewed as in its early stages, with an excessive number of unanswered inquiries concerning how powerless blockchain applications and blockchain application improvement can be. Despite this, India is as yet pushing ahead with its appropriation and right now have the accompanying diligent difficulties with it. The Indian government does not have any characterized guidelines on distributed ledger technology or any guideline identifying with blockchain innovation. This absence of guidelines implies that there is an absence of consistency, making appropriation moderate. For there to be a fruitful verification of ideas for a huge scope, blockchain specialists must be recruited. In addition to the fact that this is costly current testing on blockchain applications is confined to cryptocurrency as it were.

For open-based or public-based blockchain applications, the expense of the system upkeep and the approval of the exchanges is not characterized to a particular individual, organization, or association.

Due to the innovation despite everything being viewed as new and the way that there is an absence of mindfulness about it, it implies that numerous potential merchants are not at the selection point yet. More digitization about blockchain innovation needs to happen first. From being executed, if there is to be a speedy acceptance of blockchain applications and the innovation, all in all, there should be more mindfulness spread and unmistakably characterized guidelines set up.

### ***1.4 Wrapping It Up: Blockchain Adoption Can Solve Major Problems in India***

If blockchain chain innovation was to be adopted in India, regardless of whether it is in the financial area, in the security division, or even over the medicinal services framework, it is ready to be progressive. Lamentably, India's economy experiences some extreme issues like information penetrates, budgetary record altering, and defilement, all of which might be moderated somewhat with bigger and adaptable blockchain application advancement. With the very nearly 20,000 blockchain designers arranged in India, the nation can turn into a pioneer where the blockchain is concerned.

The crucial property of the blockchain, which makes it so amazing, is unchanging nature. If one can envision a widespread record in the cloud which is shared by the individuals who reserve the options to get to, any section in the record gets included in the type of an extra block which must be confirmed by all members. That is the reason it is so troublesome if not out and out outlandish for programmers to get through the whole chain to get agreement from all members.

In the beginning it is generally accepted that the principal executive of present-day blockchain innovation originated from Satoshi Nakamoto. In 2008, an individual or gathering of individuals distinguished as Nakamoto distributed a paper, "Bitcoin: A Peer-to-Peer Electronic Cash System," which speculated a direct online payment starting with one party then onto the next without the utilization of a go-between outsider. The paper depicted an electronic payment framework dependent on cryptographic confirmation rather than trust [4].

The paper looked to take care of the issue of twofold or double spending. That is the very idea of digital cash which permits it to be effortlessly copied and spent more than once. The subsequent vulnerability was lethal to the appropriation of the innovation. The Nakamoto paper tackled this issue by connecting each exchange to the exchange going before it in an altered safe way. The tamper-resistant way portrayed by Nakamoto was the open record. With this record, a system can look at the exchange history of an electronic coin that a client submits for payment and can affirm that the coin has not as of now been spent, accordingly forestalling the "double spending" issue. Blockchain is a kind of database that is copied on numerous PCs or "nodes." All of the nodes have similar data on them. This is imperative to the achievement of the blockchain innovation. The data is put away in, as the name suggests, blocks. Each block can contain various exchanges, with every exchange having an interesting reference number, a time stamp, a pointer to the quickly past exchange, just as data on the exchanges themselves. Along these lines, every hub approaches every single past square down to the primary block of the chain called the "genesis" block. The time stamp gives each block an unchanging transient situation in the chain. A theoretical exchange epitomizes the way blockchain works. With regard to a deal, a vender consents to offer a gadget to a purchaser for one "coin." In a system of PCs, one node (purchaser) communicates code that will consequently deduct one coin from the purchaser's record and add it to the dealer's record when the merchant delivers a gadget to the purchaser. A smart agreement is conceived, i.e.,

called “Smart Contract.” That is, the execution some portion of contact was decreased to code that is actualized by nodes and confirmed by a network of nodes before it is changelessly added to the database. When the gadget is delivered, the smart contract is executed. Different nodes get the exchange and go to confirm it by guaranteeing that the purchaser in certainty has the coin it has offered to the vender for the gadget. The confirmation may involve taking a look at the most recent exchange of the purchaser’s record to ensure it holds adequate assets for the buy. The succession of the transaction is recorded in an immutable record, i.e., a blockchain, by constraining the nodes in the system to contend in taking care of a mathematical problem for the option to include the following block of exchanges to the chain, connecting the winner’s new block to the past block, restarting the opposition to include the following block each time an answer is found, and dismissing any endeavor to embed or supplant block prior in the chain. In that capacity, the purchaser cannot spend the coin he has given to the merchant once more, as everybody in the framework knows the purchaser no longer has the asset.

## 2 Basic Structure of Blockchain

In blockchain cryptographically link exists between all blocks. Blockchain is a mutual, distributed ledger that encourages the procedure of recording exchanges and monitoring tangible assets (property, house, vehicle) as well as intangible assets (advanced cash, protected innovation rights) in a system. Fundamentally, it stores data and records its developments in a distributed domain. How about we investigate its subtleties.

It is an open and dispersed database that keeps subtleties of assets and its developments/exchanges over a peer-to-peer network. Every transaction will be made sure about through cryptography and later all the transaction history will be gathered, what is more, put away like a block of information. At that point, the blocks are connected along with cryptography and made sure about from interruption. The entire procedure will make an unforgeable, and unchanging record of the transactions that occurred over the system. Also, these blocks of records are duplicated to each taking part nodes in the system, so everybody will approach it. The incredible preferred position of blockchain is that it can store any sort of asset, its possession subtleties, history of the possession, and area of advantages in the system, regardless of whether it is the bitcoin (digital cryptocurrency) or some other assets like a digital certificate, individual data, an agreement, title of ownership for, even the real-world objects.

The amazing element of blockchain is that we can make a belief over non-trusting elements. No need to verify trust between nodes in the blockchain because each node has capacity to validate and approve the chain for themselves. The incongruity is that the common doubt among member is the thing which keeps the blockchain secured.

The information in the blockchain is put away as an individual block, that is the reason it is called blockchain. The blockchain is an assortment of blocks connected



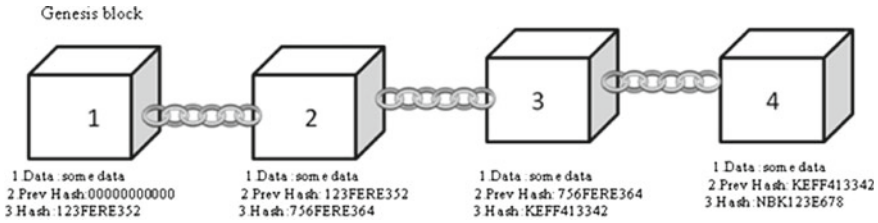


Fig. 11.2 Basic structure of blockchain

together as linked list. Each block in the blockchain will have the accompanying fields as shown in Fig. 11.2.

- a. Data: Stores the information
- b. Previous hash: Stores the hash of the past block
- c. Hash: Hash an incentive for the current block which can be utilized to allude this block.

The most significant thing is the data field which contains genuine information (like transaction subtleties, resource details, and so on) that are put away in this field. The past hash will store the hash estimations of the past block (think about it as a connection to the past block), the blocks are associated through this value.

### 3 Process of Transaction Get into the Blockchain

We saw that blockchain has its own remarkable data stockpiling structure, the information appropriation in a blockchain has additionally a different methodology. They do not follow the broadly embraced client-server model rather the peer-to-peer model. The companion to peer information appropriation approach gives the explanation for the free nature of blockchain; there is a lack of central authority. As there is no central control over the blockchain, validation of blocks can be done by the validation process as shown in Fig. 11.3. In the era of digitalization, hacking and data breaching are the common problems all businesses are facing. The development of this technology has changed the way business transactions were done in the past. It has not only given birth to the digital currency but also transforming the businesses and societies [5].

#### 3.1 Validation of Blocks

As we portrayed over, the asset and its transactions are put away as associated blocks in the blockchain. Only valid transactions are added to the blockchain. Actually saying, validation in blockchain is just the way toward finding the block hash. In a blockchain, only after validation all the blocks are added to the blockchain. At

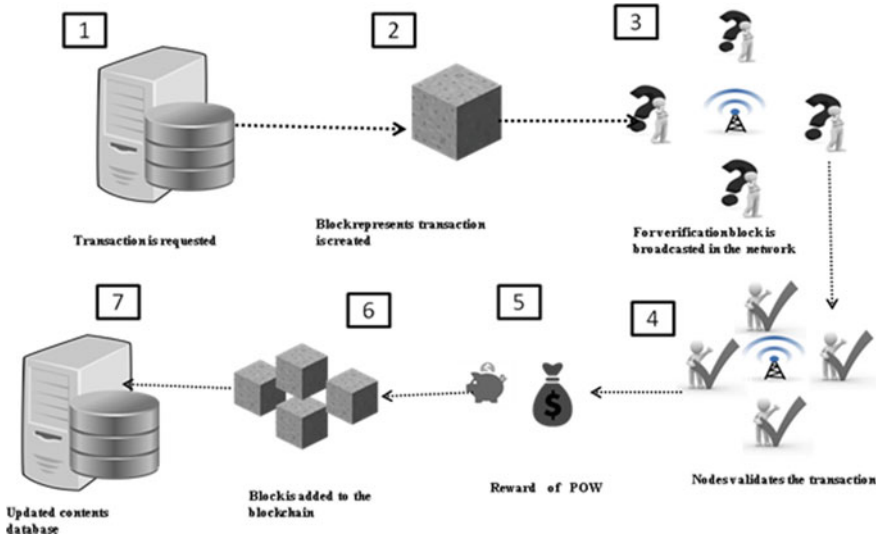


Fig. 11.3 Transaction validation process in blockchain

whatever point transaction takes place in the blockchain it will be added to a block; now and then one transaction for every block and in some cases a few transactions per block. It relies upon the block size and the idea of the arrangement. At the point when the transaction is added to the block, it must experience an approval process before it is being added to the blockchain as a valid block. The hash algorithm (like a 256) helps to evaluate hash value for the block.

The hash value has certain properties as well. The primary concern is that the hash worth ought to be sans crash for example no two blocks ought to have similar hash value. Since each block is spoken to utilizing the hash value it ought to be indistinguishable. The subsequent property is that the hash value ought to be irreversible. This implies the block data could not be retrievable from the hash value.

### 3.2 Proof of Work

It requires the individuals who own the PCs in the system to take care of a complex mathematical problem to have the option to add a block to the chain. The problem-solving method is known as mining, and “minors” are normally compensated for their work in digital money.

In any case, mining is not simple. The mathematical problem must be tackled by experimentation and the chances of a solving problem are around 1 in 5.9 trillion. It requires significant processing power which utilizes extensive measures of vitality. This implies the compensations for undertaking the mining must exceed the expense

of the PCs and the power cost of running them, as one PC alone would take a long time to discover an answer for the mathematical issue.

### ***3.3 Proof of Stake***

Later blockchain systems have embraced “proof of stake” approval consensus mechanism, where members must have a stake in the blockchain—as a rule by possessing a portion of the cryptocurrency to be in with an opportunity of choosing, checking, and approving transactions. As there is no need for mining, it recovers more processing power resources.

What is more, blockchain advancements have developed to incorporate “smart contracts” which consequently execute exchanges when certain conditions have been met [6].

### ***3.4 Smart Contract***

Smart contract is a set of rules in a blockchain and executed when conditions are matched. At the most fundamental level, they are programs that run as they have been set up to run by the individuals who created them. The advantages of smart contract are generally obvious in business collaborations, in which they are regularly used to authorize some kind of understanding so all members can be sure of the result without a third-party involvement [7].

The simplest approach to clarify what a smart contract does is through a model. On the off chance that you have at any point purchased a vehicle at a business, you know there are a few stages and it tends to be a baffling procedure. On the off chance that cannot pay for the vehicle out and out, you will need to get financing. This will require a credit look at and you will need to fill many forms with your own data for verification of identity. En route, you will need to communicate with different employees, including the sales person, fund dealer, and loan specialist. To repay their work, different bonuses and charges are added to the base cost of the vehicle.

What smart contract on a blockchain can do is smooth out this complicated procedure that includes a few mediators on account of an absence of trust among members in the exchange. With your personality put away on a blockchain, loan specialists can rapidly settle on a choice about credit. At that point, a smart agreement would be made between your bank, the seller, and the moneylender so that once the assets have been discharged to the vendor, the loan specialist will hold the vehicle’s title and reimbursement will be started dependent on the concurred terms. The exchange of proprietorship would be programmed as the transaction gets recorded to a blockchain, which is shared among the members and can be checked whenever.

## 4 Types of Blockchain

There are four different types of blockchain as shown in Fig. 11.4.

### 4.1 Public Blockchain

How about we investigate the various sorts of chains. Also, start with block blockchains, which are open source. They permit anybody to take an interest as clients, excavators, engineers, or network individuals. All transactions that occur on public blockchains are completely straightforward, implying that anybody can know details of transactions.

Public blockchains are intended to be completely decentralized, with nobody individual or element controlling which transactions are recorded in the blockchain or the request wherein they are prepared [8].

Public blockchains can be profoundly oversight safe, since anybody is available to join the system, paying little mind to the area, nationality, and so on. This makes it very difficult for authorities to close them down.

In conclusion, open blockchains all have a token related to them that is commonly intended to boost and prize members in the system.

**Examples** of public blockchain are Bitcoin, Ethereum, Litecoin.

### 4.2 Private Blockchain

Private blockchains are also called as permission blockchains and have various eminent contrasts from open blockchains. Members need to agree to join the systems.

All transactions are accessible to environment members that have been allowed to join the system. Private blockchains are more unified than open blockchains.

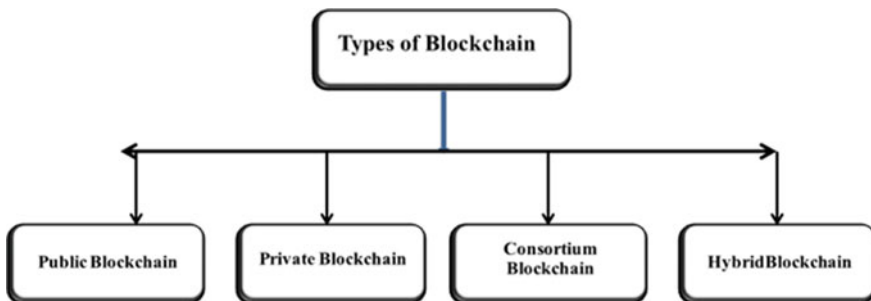


Fig. 11.4 Types of blockchain

Private blockchains are significant for undertakings who need to work together and share information, yet do not need their delicate business information obvious on a public blockchain. These chains, by their temperament, are progressively brought together; the entities running the chain have huge command over members and administration structures. Private blockchains could possibly have a token engaged with the chain.

**Examples** of private blockchain are Multichain and Hyperledger projects (Fabric, Sawtooth), Corda, etc.

### ***4.3 Consortium Blockchain***

Consortium blockchain is similar to private blockchain except private blockchain is managed by a single person and consortium blockchain is managed by group of people. Here, group of people can act as a node and deliver data or perform mining. Consortium blockchains are widely used by banks, government organizations, etc.

**Examples of** consortium blockchain are Energy Web Foundation, R3, etc.

### ***4.4 Hybrid Blockchain***

This signifies it strengthens the protection advantages of a permissioned and private blockchain with the security and transparency advantages of a public blockchain. That gives organizations critical adaptability to promote what information they need to make publicly open and what information they need to keep hidden. Hybrid blockchain permits us to handily correlate with other blockchain protocols, taking into account a multichain system of blockchains permission [9].

This usefulness makes it straightforward for organizations to work with the transparency they are searching for, without giving up security and protection.

Likewise, having the option to post to different public blockchains without a moment's delay builds the security of exchanges, as they profit by the joined hashpower being applied to the open chains.

**Example** of a hybrid blockchain is Dragonchain.

## **5 Blockchain Role in Social Impact Initiatives**

### ***5.1 Fraud and Risk Reduction***

Probably the greatest favorable position of blockchain for social effect is the decrease of fakes and dangers related with the project itself. A tremendous issue is corruption,

particularly at the administration level. This implies voracious individuals utilize the cash expected to give help to the penniless. This is made conceivable as a result of the traditional methods that are not straightforward enough to tackle corruption.

The most ideal approach to take care of every one of these issues is by utilizing blockchain. Blockchain offers a total sealed arrangement where every transaction is confirmed utilizing consensus techniques. There is no reliance on an incorporated position and henceforth is liberated from any sort of extortion. The data put away in the blockchain is additionally permanent, which implies that once put away, it cannot be altered or changed by a malicious user.

## ***5.2 Reduced Administrative Costs***

Charities require a ton of work to oversee appropriately. That implies going through a great deal of cash should be spent on authoritative expenses. With blockchain, these authoritative expenses can be decreased. With smart agreements, it is presently conceivable to oversee budgetary and legitimate middle people. Automation is consistently useful and consequently makes it simple for everything to manage viewpoints that are dull or non-innovative.

## ***5.3 Accountability and Transparency***

By utilizing blockchain, it is presently feasible for good cause to be responsible and straightforward. People are consistently doubtful of noble cause. In any case, with blockchain, contributors can make certain of what they are doing. They can perceive how their commitments are having any kind of effect.

## ***5.4 Faster Border Transfers***

Regular banking channels are not giving much performance with regard to moving cash globally. It can take anyplace between days to send cash. On head of that, there is likewise an expense related with the exchange. As most causes are worldwide, they are in consistent need to do global exchanges. The late reach can hamper their endeavors.

Without involving central authority, digital cash can be transferred over the network. With it, they do not need to pay the middle people and furthermore do not need to stand by excessively long for the exchanges to get finished.

## ***5.5 Improved Accessibility***

With blockchain, it will presently be workable for anybody to move or get value. They do not need to rely upon banking to have the option to do these. This is a blast for noble cause and NGOs that are attempting to help individuals from all foundations. By making this methodology, the foundations likewise do not need to do twofold exchange and decrease both settlement and cost times.

## ***5.6 Social Sectors That Are Impacted Using Blockchain***

In this section, we are going to go through the different sectors that are being impacted by blockchain from a social point of view. The statistics shared in the section are taken from the standard blockchain for social impact study.

## ***5.7 Agriculture***

Horticulture is one of those areas that require cautious consideration. It can affect a colossal populace over the world. The fundamental centre is to improve three key parts of the gracefully chain in agriculture. This incorporates improving straightforwardness, delectability, and effectiveness. It will ensure farmers are all around associated with the consumers.

A portion of the key features that are partaken in the investigation incorporates the accompanying

- New activities are under two years of age;
- None of the new activities have in excess of 1000 recipients;
- Some of the activities can arrive at a million recipients;
- Most of the applications are for-benefit.

With blockchain, these issues can be settled. Above all else, it can decrease pollution and fraud in food. This can occur with the assistance of blockchain proficiency and straightforwardness. Blockchain's job is to improve the outsider contribution by guaranteeing that they are following, gathering, and overseeing information in the most ideal manner. With blockchain farmers and wholesalers will get their installments quicker than any time in recent memory improving their capacity to take a shot at their next arrangement of activities quicker.

**Projects:** AgriDigital, Grassroots Cooperative, Bext360

## 5.8 *Democracy and Governance*

The following division where blockchain can assume a critical job is democracy and governance. At the present time, governments are open to blockchain and its job in improving majority rules system and administration.

Key features

- Governments began blockchain as right on time as 2008;
- 21 activities across democracy and governance;
- 81% of the activities have seen accomplishment by mid 2019.

Less than half of the activities are for-benefit.

Governments run on trust. Also, that is the place blockchain becomes an integral factor. With blockchain, governments can address security identified with the location information trade. What is more, it will likewise permit clients to cast a ballot by means of blockchain, which makes them in a flash countable and discernible.

By utilizing blockchain, the legislature can likewise store residents' information in a vastly improved manner. The information is unchanging, which implies that there is no resident information that can be wrongfully erased or altered. It additionally enables organizations to get to the information at whatever point they need. The absence of centralization additionally implies that there is no main issue of disappointment. The legislature can likewise run legitimate crowdfunding utilizing blockchain.

**Projects:** e-Estonia, Votem.

## 5.9 *Health Care*

Healthcare division is one of those parts that have huge amounts of activities by both for-benefit and non-benefit associations. With blockchain, human services can improve computerized social insurance records. It likewise improves pharmaceutical gracefully chain the executives. Obviously, blockchain offers a decentralized, productive, and secure arrangement.

The key advantages incorporate appropriate electronic well-being records, better protection usage, and fake medications.

Undertakings: Modium.io.

## 5.10 *Philanthropy and Aid*

Social effect can be best observed from the altruism and help division. At the present time, the guide and altruism do not arrive at their proposed use. This is a direct result of the immense wasteful aspects that the current stage endures with regard to help



and generosity. Indeed, even with such a great amount of speculation, there is as yet a requirement for extra assets to satisfy the need for fundamental human rights, destitution, and access to training.

Key features

- More than 80% of the activities are non-benefit;
- Over 55% of the activities are arriving at fewer than 1000 individuals.

Billions of dollars are put resources into helping the poor. Be that as it may, these guides are for the most part abused because of an absence of straightforwardness. Truth be told, the greater part of the guide never contacts the planned individuals. This has additionally driven individuals to not add to these non-benefit associations. Blockchain can take care of these issues and help hoist the trust in non-benefit in using the assets.

**Projects:** Ixo Foundation, Disperse, RootProject.

## 5.11 Insurance Segment

In the insurance segment, consider the head as the insurance agency. The objective of the insurance segment is to decrease his danger of payout and to gain the best yields based on the accessible items. At that point we have an agent whose objective is to gain the commission on sale of product.

At last, we have a client, whose objective is to lessen his monetary risk at the event of an occasion (e.g., sudden death, or, accident, or then again, flight delay). Each of the three members in the commercial center has totally various incentives and various arrangements of data. For instance, the insurance agency could model the specific hazard an item faces and could adjust costs as needs be. The specialist could just concentrate on selling the item with the most noteworthy insurance. Next, the customer would need to pick a protection item that would give the most noteworthy hazard confirmation in any event cost. The motivations of every one of the three players contrast essentially and differ as indicated by availability of data at the time of transaction.

## References

1. Investopedia (2020) Blockchain explained [online]. Available at: <<https://www.investopedia.com/terms/b/blockchain.asp>. Accessed 13 June 2020
2. Bankrate (2020) Blockchain definition | Bankrate.Com [online]. Available at: <https://www.bankrate.com/glossary/b/blockchain/>. Accessed 13 June 2020
3. SearchCIO (2020) What is blockchain?—definition from Whatis.Com [online]. Available at: <https://searchcio.techtarget.com/definition/blockchain>. Accessed 13 June 2020
4. Popovski L, Soussou G, Tyler W, Belnap P (2020) A brief history of blockchain. Retrieved from: <https://hbr.org/2017/02/a-brief-history-of-blockchain>. 15 June 2020

5. Houben R (2018) Cryptocurrencies and blockchain. European Parliament, Belgium, p 103
6. Potts J (2019) Blockchain in agriculture. SSRN Electron J
7. Schär F (2018) Decentralized finance: on blockchain- and smart contract-based financial markets. SSRN Electron J
8. Andreev R, Andreeva P, Krotov L, Krotova E (2018) Review of blockchain technology: types of blockchain and their application. *Intell Syst Proizv* 16(1):11
9. De Lara S, Grech C (2018) Blockchain and transaction regulation. *ITNOW* 60(4):24–25