EAI/Springer Innovations in Communication and Computing

H L Gururaj · V Ravi Kumar
Sam Goundar · Ahmed A Elngar
B H Swathi *Editors*

Convergence of Internet of Things and Blockchain Technologies

EAI
RESEARCH MEETS INNOVATION

Springer

EAI/Springer Innovations in Communication and Computing

Series Editor

Imrich Chlamtac, European Alliance for Innovation, Ghent, Belgium

Editor's Note

The impact of information technologies is creating a new world yet not fully understood. The extent and speed of economic, life style and social changes already perceived in everyday life is hard to estimate without understanding the technological driving forces behind it. This series presents contributed volumes featuring the latest research and development in the various information engineering technologies that play a key role in this process.

The range of topics, focusing primarily on communications and computing engineering include, but are not limited to, wireless networks; mobile communication; design and learning; gaming; interaction; e-health and pervasive healthcare; energy management; smart grids; internet of things; cognitive radio networks; computation; cloud computing; ubiquitous connectivity, and in mode general smart living, smart cities, Internet of Things and more. The series publishes a combination of expanded papers selected from hosted and sponsored European Alliance for Innovation (EAI) conferences that present cutting edge, global research as well as provide new perspectives on traditional related engineering fields. This content, complemented with open calls for contribution of book titles and individual chapters, together maintain Springer's and EAI's high standards of academic excellence. The audience for the books consists of researchers, industry professionals, advanced level students as well as practitioners in related fields of activity include information and communication specialists, security experts, economists, urban planners, doctors, and in general representatives in all those walks of life affected ad contributing to the information revolution.

Indexing: This series is indexed in Scopus, Ei Compendex, and zbMATH.

About EAI

EAI is a grassroots member organization initiated through cooperation between businesses, public, private and government organizations to address the global challenges of Europe's future competitiveness and link the European Research community with its counterparts around the globe. EAI reaches out to hundreds of thousands of individual subscribers on all continents and collaborates with an institutional member base including Fortune 500 companies, government organizations, and educational institutions, provide a free research and innovation platform.

Through its open free membership model EAI promotes a new research and innovation culture based on collaboration, connectivity and recognition of excellence by community.

More information about this series at http://www.springer.com/series/15427

H L Gururaj • V Ravi Kumar
Sam Goundar • Ahmed A Elngar • B H Swathi
Editors

Convergence of Internet of Things and Blockchain Technologies

Springer

EAI
RESEARCH MEETS INNOVATION

Editors
H L Gururaj
Vidyavardhaka College of Engineering
Mysuru, Karnataka, India

Sam Goundar
Victoria University of Wellington
Wellington, New Zealand

B H Swathi
Vidyavardhaka College of Engineering
Mysuru, Karnataka, India

V Ravi Kumar
Vidyavardhaka College of Engineering
Mysuru, Karnataka, India

Ahmed A Elngar
Computers and Artificial Intelligence
Beni-Suef University
Egypt, Egypt

ISSN 2522-8595 ISSN 2522-8609 (electronic)
EAI/Springer Innovations in Communication and Computing
ISBN 978-3-030-76215-5 ISBN 978-3-030-76216-2 (eBook)
https://doi.org/10.1007/978-3-030-76216-2

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

Preface

Almost a year back, the authors/editors organized an international conference in the organization and met two very knowledgeable, enthusiastic researchers, Dr. Sam Goundar and Dr. Anand Nayyar, in the domains of blockchain technology and Internet of Things, respectively. After listening to the keynote address, the editors got inspired to combine these technologies and decided to create a collaborative book, where you can bring the thoughts of various researchers to apply the concepts of blockchain and IoT together to help society. The authors of Chaps. 1 and 2 are present game-changing technology in many functional sectors of society. These chapters are written for educators, practitioners, and professionals who want an overview of blockchain technology that provides insights of understanding of blockchain technology and its impact on economy. This chapter walks through the foundation of blockchain technology by highlighting its development history, blockchain framework, challenges, other application areas of blockchain technology which transforms society and so on. Finally, the future of blockchain with Internet of Things (IoT) in industrial applications along with some case studies, is discussed.

The **next five chapters** present the convergence of blockchain technology with IoT in various fields like sewage cleaning, home automation, smarts city, agriculture, and PalCom Middleware. The authors have focused on the health of sewage cleaners. They face a high risk because of the release of poisonous gases or oxygen insufficiency. Here, a continuous monitoring system will be built to monitor environmental parameters such as temperature, carbon monoxide (poisonous gases,) and humidity. The parameters are continually detected by different sensors; the admin will take appropriate measures to handle the situation if any irregular condition occurs. For the registration of new IoT devices and users, blockchain networks will help in authentication and identification. Blockchain technology also manages the sensitive events happening in the IoT network system and notifies users. In automation home systems, the blockchain can be used with IoT to enhance the innovation strategy to provide more privacy, security, and decentralized instruments for information utilization in smart homes.

The smart city application uses blockchain, IoT, Fog computing, and Cloud computing to form sustainable development of innovative applications for intellectual data processing, control systems, and communications between heterogeneous network infrastructures. This chapter discusses a conceptual framework with the dimensions: (1) technology, (2) human and (3) organization. Here, the authors are reconnoitring the challenges of digital technologies with the support of blockchain-based fog computing model that reduces energy consumption and latency in data communication and improves security features.

The PalCom directives use the commands/parameters in a limited version to access online patients. It aims to deliver a compiled working of blockchain to keep secure and safe digital relationships using private key cryptography and authentication. The challenges include fragmented patient data, medical record integrity, smart contract security, and privacy. This work includes using the Hyperledger and authentication algorithm to solve the issues of provided data-intensive domain, i.e. healthcare system, the research shows the benefit and performance based on the cryptography algorithm and provided with the adherence to data regulations and standards.

The next three chapters include the applications of blockchain in Indian economy and some areas with respect to a few other countries. Due to the involvement of lot of untrusted actors in the real estate market, real estate cannot be trusted blindly. A blockchain-centred policy has been proposed in this work for real estate operations, which prevents property fraud cases and ensures transparency, safe traceability, and trust. Since blockchain is not a centralized system, the use of blockchain avoids forgery or tampering of the real estate documents as the information or data will be stored in the form of blocks. We use smart contracts for property registration process. The 7/12 asset tracking system using blockchain technology will use the fingerprint of the person who was going to sell a property and the customer will have access to the server. All the property information is going to be displayed using a centralized system in government offices. This will help find the legal property papers and avoids the need for any third parties for property deals in between. This system provides secure and fraud-free handling of property documents.

The year 2020 has witnessed a deadly outbreak caused by a novel coronavirus. The unexpected and rapid spread of COVID-19 globally has increased the death rate to a very high rate, and the transmission rate found in rich countries is much higher than in other countries. With the available hospitals, diagnostic centres, and deprived disease surveillance systems in a limited manner, it is very tedious to tackle with COVID-19 outbreak. In such situations, the latest emerging technologies like blockchain and IoT have capable solutions for combating coronavirus pandemic by enabling early detection of outbreaks and ensuring reliable medical supply chain during the outbreak tracking and to strengthen security and bring transparency in data collected from various external devices by using IoT. The authors of Chaps. 11 and 12 have presented the use of these technologies by classifying the blockchain-based IoT applications into four major segments, namely, Smart Healthcare, Government, Banking, and supply chain management to sustain in these difficult times. They have shed light on a collective survey of COVID impact on

above-mentioned four segments and then discussed measurable preventive actions that blockchain with IoT can provide.

The **final chapter** introduces the various challenges to implement blockchain in the Jordanian Public Sector. The proposed factors of this chapter can be used by the public sector as a reference point for the efficient adoption of blockchain technology and by scholars for further practical and theoretical research into blockchain technology.

Mysuru, Karnataka, India H. L. Gururaj
V. Ravi Kumar

Acknowledgements

We would like to take this opportunity to thank all contributors of this book and all people involved in the organization of this edited book.

Contents

Part I
The Convergence of Internet of Things and Blockchain Technologies

Chapter 1
Blockchain: A New Era of Technology

J. Sudeep, S. C. Girish, Karthik Ganapathi, K. Raghavendra, Hong Lin, and P. Subramanya

1.1 Introduction

The role of technology has presented a significant part in everyone's life. With the rapid growth of Internet and communication technologies, people around the world are doing transactions digitally across various domains like banking, healthcare, and business. The revolution of technologies happens very often; one such technology is called "blockchain" which will be a game-changer in many functional sectors of the society. Today, people are more conscious when they hear about the word "money." It has become an integral part of people's life. It can take the form of a banknote, plastic card, or coins. Quite often, you might have visualized the image of the banknote, some coins, or credit cards. It is just an object which has an intrinsic value to do transactions.

J. Sudeep (✉) · S. C. Girish
Department of Information Science and Engineering, NIE Institute of Technology, Mysuru, Karnataka, India
e-mail: sudeep@nieit.ac.in; girishc@nieit.ac.in

K. Ganapathi
VSG Software Solutions Private Limited, Mysuru, Karnataka, India
e-mail: karthik@vsgsoftwares.com

K. Raghavendra
Department of Computer Science and Engineering, NIE Institute of Technology, Mysuru, Karnataka, India
e-mail: raghavendrak@nieit.ac.in

H. Lin
Department of Computer Science, University of Houston-Downtown, Houston, TX, USA
e-mail: linh@uhd.edu

P. Subramanya
DevOps Engineer, Akuna Capital, Greater Chicago, IL, USA

H. L. Gururaj et al. (eds.), *Convergence of Internet of Things and Blockchain Technologies*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-76216-2_1

Imagine you are going to a restaurant along with your family and ordering food items. The waiter serves the order and provides a bill that needs to be paid. The payment is digitally done with the interventions of the third-party agents. There is no direct communication between the payer and the receiver. This eventually led to the invention of new technology, where there is direct communication between the sender and the receiver. Before the invention of money into financial and economic system to do transactions, the concept of barter system was introduced in the era of 1920 by the Mesopotamian tribes for the exchange of materials, for instance, if two people want to exchange goods, i.e., a bag of wheat with a set of leather boots. There will be a direct communication for exchanges of goods. However, conflicts might arrive, if there is an opinion difference among a person who complies with other persons concerning the transactions. Therefore, money acted as a desire for the economy which enabled all types of transactions to be carried out in detail. The concept of Blockchain technology is analogous to a barter system, except that the transactions are digitally done without face-to-face involvement of individuals and interventions of third-party agents.

1.1.1 What Is Blockchain and How It Works?

One of the important valuable assets in the digital world is data which needs to be protected and managed. With skillful criminal people, there is always a threat to steal data. In the past, several methods are proposed to protect the valuable data. One such approach is the use of Blockchain technology. In simple terms, a Blockchain refers to a chain of blocks that store data. Every data cached inside the block depends on Blockchain types. The main intent is to encode the sequence of characters in digital documents using cryptographic algorithms so that it's not possible to antecede them or to mess with them [1]. A Blockchain is a digital ledger that is spread completely to anyone who is intended to learn and use it. It becomes very difficult to change it once data is archived inside a Blockchain. Every block contains data, the hash of the current block with hash of previous block. The transaction details of the sender and receiver and number of coins are stored in a Bitcoin Blockchain. Each block has a long sequence hash key which is unique that makes it difficult to break by felony hackers. Once the block is created, its hash is counted. Any changes made inside a block cause the hash to change. Often, hashes are very useful when we want to detect changes to blocks. The next element inside each block is the hash of the previous block [2, 3].

As shown in the Fig. 1.1a [4], let's assume that we have a chain of three blocks in a Blockchain network. Each block has a hash and hash of the previous block. So block number three points to hash of block number two, and block number two points to hash of block number one. The first block is a special block which is called "genesis block" which can't point to the previous block. Now, let's say that we tamper the second block as shown in Fig. 1.1b [4]. These changes the hash block. Consecutively, it makes adjacent blocks unacceptable as it points to tampered block.

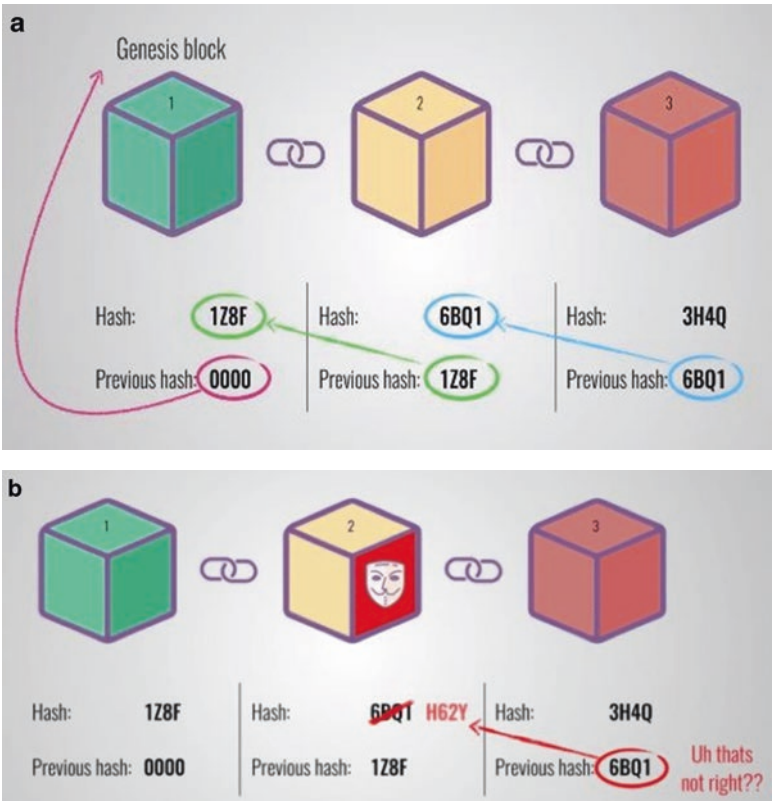


Fig. 1.1 (**a**) Genesis block. (**b**) Tampered block

Nowadays, supercomputers are fast enough to compute millions of hash codes per second, so we cannot rely solely on hash concept to avoid tampering. To alleviate this problem, Blockchain has a concept called "proof of work." This method delays the process of new block creation. It takes nearly ten minutes to compute the essential proof of work in the case of Bitcoins to insert into the Blockchain [3]. Any alteration in a single block results in recomputation of proof of work. So the proof of work and use of hash concept make the Blockchain more secured. The peer-to-peer network concept is also used by Blockchain where anybody can get the full copy of Blockchain when they join to that network. The existing nodes of the Blockchain examine the new block which is created by somebody. Each node verifies that block to make sure that it hasn't been tampered with. All nodes mutually ensure a "consensus" to add new block to its chain. They comply which are valid and invalid blocks. Blocks that are meddled will be rejected by other nodes in the network. So to effectively tamper a Blockchain, all blocks on that chain need to be meddled, recalculate the proof of work for each block, and take control of peer-to-peer network. Then, only the tampered block become accepted by everyone.

Blockchain is constantly evolving. One of the most recent developments is the creation of "smart contracts" which makes a Blockchain more secure [4].

1.1.2 Basic Framework of Blockchain

In the previous sections, we gave a brief outline of Blockchain and introduced how a Blockchain works. We take a deep dive into the Blockchain framework by explaining the different Blockchain types along with its structure. This section also describes the role of smarts contracts, centralized and decentralized networks, and challenges faced by Blockchain. So let's get started.

1.2 Types of Blockchain with Its Structure

Let's take a look at three major types of Blockchain in detail:

- Public Blockchain.
- Private Blockchain.
- Hybrid Blockchain.

Public Blockchain. As the name itself signifies, it is one type of Blockchain which is open to everyone who is interested to participate as users, miners, developers, and any other stakeholders. The Blockchain transaction which happens is fully transparent and can be examined by anyone regardless of details of the transactions. These are designed to be completely decentralized with "no individual or entity control" where the transactions are recorded in the Blockchain or the order in which they are processed. A public Blockchain is highly resistant since it is open to join networks regardless of location, nationality, etc. This makes it hard for the authorities to shut the network down. Lastly, these have a token with them designed to motivate and reward the stakeholders in the network. Some examples of public Blockchain are Bitcoin and Ethereum [5]

Private Blockchain. Unlike a public Blockchain, private Blockchain are focused on specific stakeholders or organizations who want to collaborate and share data but don't want their sensitive business information visible on the public domain. By nature, they are more centralized. In a private Blockchain, each stakeholder needs the consent to join the peer network or group. All the transactions are available to the stakeholders of the private local ecosystem which has been permitted to join that network. Private Blockchain may or may not have token associated with the chain. The entity running the chain has complete control over the participants or the governance structures. Some examples of private Blockchain are Hyperledger and R3 Corda [5, 6].

Hybrid Blockchain. As the name itself signifies, it is another type of Blockchain that combines the features of the above two Blockchain, i.e., private and public. It

combines the privacy and transparency benefits of public and private Blockchain which offers the flexibility to the businesses to select what type of data makes it public and private. In this type, the user will have the complete control of data that needs to be stored and provides some restrictions to gain access to other data. The only selected portion of data will be sent to the public while keeping other data in a private network. In a hybrid Blockchain, any users can easily join the public network, while all the transactions in the private network are completely verified within that network. Some example of hybrid Blockchain is the Dragonchain [5, 6]. Now, let's take a closer look at the basic structure of the Blockchain along with its components.

A Blockchain is a network of computers connected with every node in the network. There is a specific protocol imposed on the data in which every node has to agree and follow the constraints imposed on the shared data in the network. This makes the Blockchain structure very unique from other networks. As seen in Fig. 1.2 [7], every block in a Blockchain has two pieces of information, namely, the header block and transaction counter block. Every block in the header has one parent block which has a previous block hash value. Each block header has the following piece of information:

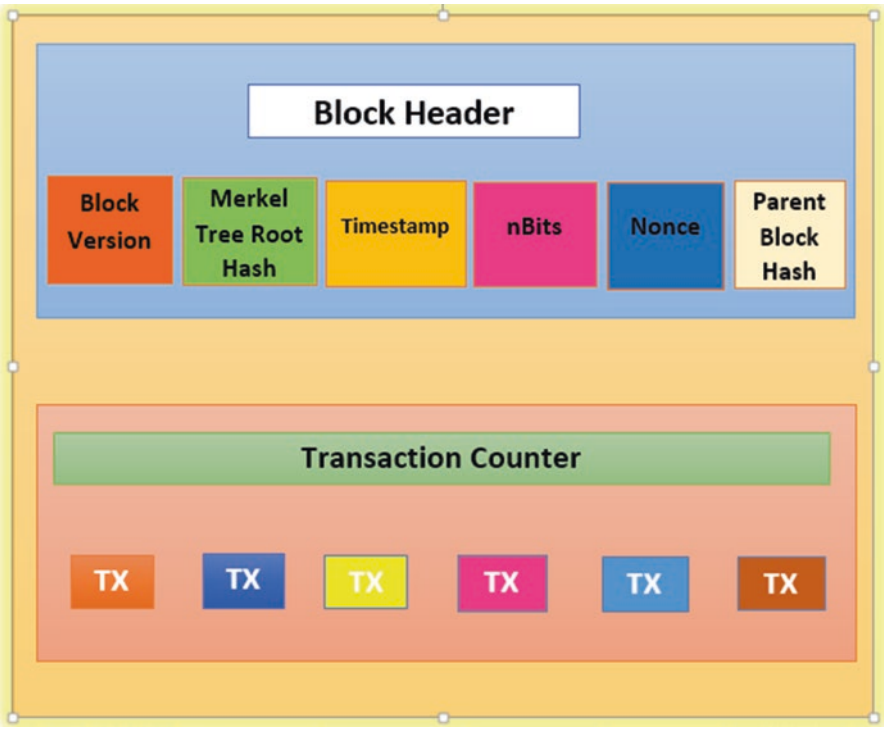


Fig. 1.2 Structure of Blockchain

Block version: It specifies the version of the block used for validating the block.
Merkel tree root hash: It basically has all the hash values for all types of transactions in a block within a Blockchain.
Timestamp: It represents the present time in unit seconds.
nBits: It represents the original value of the available block of the hash.
Nonce: It is a random nonrepeated four-byte field which starts with zero and increases with every calculation.
Parent block hash: This block points to the previous block which has a previous hash value of 256 bits depending on the type of cryptographic algorithms used [7].

1.3 Smart Contracts and Its Benefits

The idea of a smart contract was the brainchild of Nick Szabo in the year 1993 who is a computer scientist and a cryptographer. It can be simply defined as a small computer program which runs on top of Blockchain network. A smart contract provides a very powerful capability of code execution for embedding business logic on the Blockchain. These are the set of instructional codes that are stored on a Blockchain network which will be executed automatically based on some conditions. Smart contracts work on the basic principles of "simple if then else." At the simplest level, it is just a piece of code or program which is executed automatically based on some predetermined conditions. It is some type of agreement or a contract that gets automatically executed without any human involvement.

One of the better ways to understand the smart contract is through an example. Let's assume that you are buying a car from a dealer through a financial scheme. This involves a series of steps, wherein you need to interact with several people like financer, broker, lender, sales representative, and banker. This could be a tedious and frustrating process as it requires a lot of involvement from several people. One smart idea to streamline this process is to use a smart contract which eases the workflow of this system. With smart contracts, it's possible to create trust among the several stakeholders with ease of transactions. Since complete data is stored on the Blockchain network, the identity of the buyer with all his credentials is within the block which enables the lenders to quickly decide the credit. Smart contracts could be created between the bank, dealer, and lender so that the funds can be automatically released to the various stakeholders based on agreed terms and conditions. With this, the transfer of ownership will be automatic, and the complete transactions are recorded in the Blockchain network which can be verified anytime [8, 9]. Now, let's look at some of the benefits of smart contracts [8]

Transparency. One of the key aspects of any system to operate is completely dependent on the information. Automation played a crucial role in processing and managing digital data. It is possible to have full access and visibility of terms and conditions to concerned individuals without any disputes.

Accuracy. One of the primary goals of smart contracts is to maintain the records of all terms and agreements in a precise manner. It is an important aspect, as omissions will result in transaction errors. So smart contracts try to avoid the pitfalls and improve the accuracy of the transactions.

Speed. With the rapid growth of communication technologies and wide usage of the Internet, smart contracts run as a freeware code that can execute the transactions quickly. This saves the time required to do the transactions when compared to traditional business processes.

Storage and Backups. One of the key aspects of smart contracts is the ability to store complete transaction details in a single Blockchain which can be used for future reference. So whenever there is a loss of data, all the data attributes can be completely covered from storage. thereby providing full support for complete backup.

1.4 Centralized and Decentralized Networks

So far, we have seen the different types of Blockchain and understood the role of smart contracts along with its benefits. Now, it's time to understand the importance of different types of networks supported by Blockchain technology. Let us understand the concept in simple terms.

As seen in Fig. 1.3 [10], the Blockchain networks can be broadly classified into two types, namely, centralized and decentralized.

Centralized Networks. In this type of network, all nodes are connected to the centralized hub. This hub acts as an information server. All data are routed through a centralized server. When a message is transferred from one node to another node, it passes through the central hub. This is also called as "private network" as only authorized users are allowed to use this network due to entry restriction [11].

Decentralized Networks. This network is similar to that of a centralized network except that there is a single network connected to a centralized hub, whereas in decentralized networks, there is a chain of networks, i.e., multiple networks are

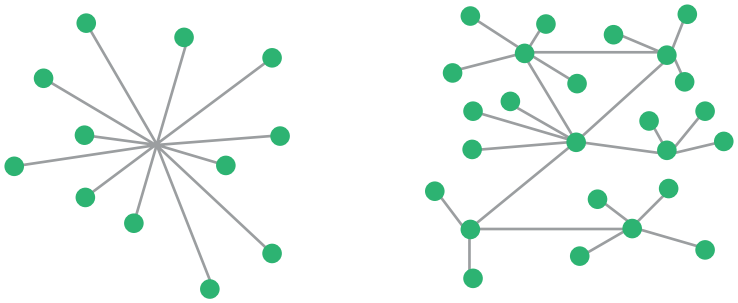


Fig. 1.3 Types of networks in Blockchain

connected to a centralized hub which enables the proper exchange of messages between them.

1.5 Blockchain Challenges

Even though Blockchain has a wide variant of applications, still, there are few challenges faced in terms of deployment and adaptability in industrial applications and other sectors. Some of them are given below [12].

Scalability. The biggest challenges of implementation of Blockchain are the inability of the technology to scale as large number of users is managed at a single time. Multiple users get connected through a chain of Blockchain structure. Different algorithms are used to process the transactions which seems to be a tedious task. The Bitcoin Blockchain can handle 3–7 transactions per second, On the other hand, Ethereum Blockchain can handle 15–20 transactions. This makes it not feasible to work for large industrial applications.

No Common Standard. With numerous platforms available in Blockchain environment, there is no common standard defined that can be used for project implementation. Many active projects use different platforms which have its own protocols, coding language, and consensus mechanism that make it difficult to use in industrial applications. Many organizations are working toward building a standard version in Blockchain to reform cross-platform collaborations.

Privacy. Another challenge that needs to be addressed is privacy concern in public Blockchain. All transactions of electronic ledgers in public Blockchain are visible to all servers which are more vulnerable to attacks. Some degree of modification is required in public Blockchain to restrict access to authorized persons only. For example, under any circumstances, the patient medical records can't be disclosed to the public.

Security. One of the major concern in the public Blockchain is that these are more vulnerable to attacks. As per [12], all the transactions in a Blockchain network are verified by miners which are present in the same network. Any miner which gains control of 51% of nodes on that network will restrict other miners to create a block and delay validating new transactions. These types of attacks decreases the number of miners that want to join the Blockchain network.

1.6 History of Blockchain

Initially, the origin of Blockchain started with the concept of adding timestamp to digital documents in the year 1991, by two data scientists Stuart Haber and W. Scott Stornetta, for avoiding the backdated and tampering of documents. This system got an upgradation in the year 1992 by the addition of cryptographic algorithm, providing security for the chain of digitally stored documents according to the timestamp.

Later in the year 2008, a paper related to peer-to-peer, decentralized network-based digital cash was proposed by Satoshi Nakamoto called Bitcoin. This was the first cryptocurrency that came to the market with the functionalities of Blockchain as the backbone.

Later in the year 2013, the upgradation with respect to Bitcoin happened with a scripting language as addition for building decentralized applications. This cryptocurrency got its name as "Ethereum." Presently, there are more than 20000+ cryptocurrencies available in market, which works on Blockchain technology.

1.7 Comparison of Blockchain with Notebook

In simpler terms, a Blockchain is compared to notebook as shown in Fig. 1.4 [13]. A blockchain is a distributed immutable ledger. Every entry in a notebook will take one line when anything is written into it. Similarly, Blockchain can be viewed as a notebook where entries will be written but can't be erased. Each page in a notebook is compared to a block on a Blockchain, and entries in a page are blockchain transactions. When Blockchain is compared to a notebook, it is precise to adopt that not all Blockchains are created equal just as all notebooks are equal. For example, the handling of transactions in Ethereum is somewhat different from Hyperledger Fabric with respect to ordering and validation. Blockchain is a revolutionary way of

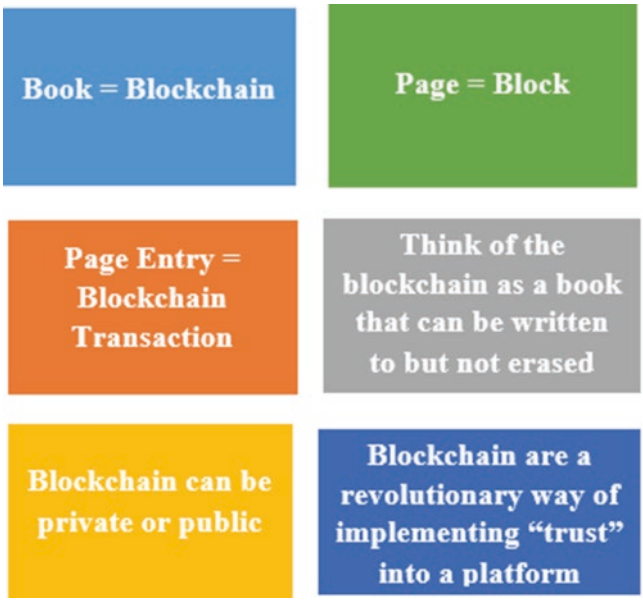


Fig. 1.4 Blockchain comparison to a notebook

implementing trust which removes third-party agents. It is transaction backend database which is secure which is read by everyone in the database. If anything needs to be changed in the database, transactions are created which should be accepted by all in the network; Blockchain is a fully robust technology, while database is not a robust technology [13].

1.8 Future of Blockchain in Industrial Applications

The usage of cryptocurrency has made Blockchain one of the promising technologies in the digital world. The revenue of industrial application can be improved through operational implementation by sharing data across multiple sectors. In this section, two applications are discussed that provide benefits to society [14, 15].

1.8.1 Telecommunication

Extreme competition and pressure to innovate are often faced by few industries in telecom domain. With billions of subscribers worldwide, telecom sectors employ different strategies to attract the brand-new customers, satisfying the current one and replacing the old. Demand for 5G network created impact for high-speed data. Technologies like AI and Internet of Things (IoT) are creating pressure to industries. Blockchain employs strategic levels to handle data privacy and operational challenges in 5G telecommunication networks which are as follows.

Data Privacy. Blockchain secures the privacy of data by protecting data and reducing annoyance through user preferences and immutable records. For example, Bharti Airtel in collaboration with IBM are working together to protect 250 million users' data from spam callers. Airtel uses Blockchain scrubbing process to protect users' mobile numbers from telemarketers. Immutable record of user preference is the next step to handle personal data and secure privacy.

Customer Experience. The customer experiences can be improved by creating new avenues and expanding business opportunities in industries. Smartphones and digital wallets are now merged rapidly that created pathways to offer financial services. Many banking applications use smartphones to make digital payments. There are three key ingredients to perform operations—a mobile platform to host application, customer relationship for postpaid billing, and meet Know Your Client (KYC) standard. All that is missing is a secure transaction with acceptance of payments; Blockchain overcomes this problems. TBCASoft and SoftBank in collaboration with IBM Blockchain are working together to build Cross-Carrier Payment System (CCPS) where payments can be made to local trader by single unified global payment platform. Immutable record and distributed ledger technology is adapted by TBCASoft to optimize transactions. CCPS uses smartphone access to provide over-the-top (OTT) payments [16].

1.8.2 Healthcare

Pharmaceutical sector is one of the prime departments in healthcare domain which focuses on patient safety through quality medicines. Blockchain revolutionizes healthcare enterprises by enabling new ecosystem with increased quality care. Several governments and other organizations collaborate to ensure safety of medicines with quality ingredients. Innovation requires continues evaluation, manufacturing with proper distribution, and technical approach to provide solution.

Different organizations like IBM, Walmart, Merck, and KPMG propose a Blockchain solution in response to FDA pilot program to accept this technology for verifying and tracking pharmaceutical product. Several challenges of the pharmaceutical supply chain are addressed through Blockchain technology with its immutable data, sharable ledger, and ability to track drug origin. Pilot program was devised to allow quick alert to supply chain partners. The process of notification is manual and fragmented using diverse systems which increased the response time and number of patients [17].

The pilot program proposed two objectives to check if Blockchain technology would be suitable to address pharmaceutical supply chain needs which are as follows:

- To achieve interoperability requirements in a secure way, Blockchain provides a common record of product movement connecting different systems and organizations.
- Improve safety of patient by bringing about product alerts and increasing visibility to suitable supply chain partners in the product investigation.
- The Blockchain successfully exhibited the above objectives.

1.9 Case Studies of Blockchain

Even though Blockchain has evolved as a disruptive technology, it has provided opportunities to scholars and industry personnel to explore this technology in detail, which contributes solutions to the society. This section will throw light about some case studies [18] and how it can be solved using the Blockchain technology in interdisciplinary fields like the judicial system and land and revenue sectors.

1.9.1 Judicial System of India with Its Issue and Blockchain Solutions

The judicial system is one of the main pillar of Indian democracy which indicates the rules in how democracy works. The judiciary is the institution which provides justice and executes the new laws and amendments passed by the government. The

Table 1.1 Pendency of cases in Indian judicial system

Court (as on)	Pending cases		Cases pending for more than 10 years	
	Civil	Criminal	Civil	Criminal
Supreme court (19 February 2016)	48,418	11,050	1132	84
High court (31 December 2014)	3,116,492	1,037,465	589,631	187,999
Subordinate courts (31 December 2014)	8,234,281	18,254,124	611,658	1,432,079

purpose of justice is defeated over years due to the pendency of cases. Still, millions of cases are still pending in Indian courts for the past 10 years. Many persons have struggled to seek justice and lost their lives in legal trials. Even though the judicial systems are considered to be the powerhouse of the system, still, there are a lot of loopholes in the current system. Key stakeholders like police, advocates, judicial officials, and individuals are utilizing these existing loopholes for their own benefits. In fact, over a period of time, stakeholders will lose faith and trust in the judicial systems. According to [19], regarding the ease of doing business operations, World Bank ranks India at 77th out of 190 countries concerning the trait of judicial standards. What are the prime reasons for many cases pending in the courts? A report from the supreme court and other chief judicial officials stated that the delay was due to the acute scarcity of judges which lead to the pendency of cases. The details of the pending cases in various courts are shown in Table 1.1 [20].

A report submitted by the Law Commission in 2009 states that in Delhi high court, to clear the pendency cases, it would require around 464 years with the available strengths of judges. However, we can't say that shortage of judges is the only reason for justice being delayed [20]. A study conducted by Vidhi Centre for legal policy states that 8086 orders are cleared by Delhi high court between 2011 and 2015. They categorized it as delayed cases if it is pending for more than 2 years. There are two prospects of delay, i.e., court side and counsel side delays. Finally, the survey summarizes that 82% of the delays caused could be credited to counsellor [21].

If gouged deeper with a reality check, the current records include statements of stakeholder getting pieces of evidence updated, modified, misplaced, or sometimes deleted to defeat opponent, thus destroying the justice. Is it possible to provide justice to all using current technology and solve the core judicial issues to speed up the judicial process? The answer is yes and it is possible through Blockchain technology. Even if there is a 1% improvement in the current judiciary, it hits the minds of crores of people to gain faith in the judicial system.Some of the challenges of the current Indian judicial systems is as follows:

Provenance: The origin of data has lacked currently in Indian judicial systems. The original data can be easily forged by any external agency which needs to be questioned.

Transparency: Besides having the copies of certified legal documents, the judicial systems lack transparency as a result of dereliction conducted by lawyers and other court officials which doesn't prevail justice.

Data integration: Many judicial representatives will have the information of particular zones. It's a better opportunity to integrate criminal records across the country so that it can track offender with their data to impede undue events in the future.

Scalability: Existing legal system is not scaled to maintain case records uniformly across different parts of states.

The abovementioned challenges can be tackled completely using Blockchain technology. As a part of the solution, different stakeholders like police, court officials, individuals, lawyers, and judges need to register their credentials on a Blockchain as shown in Fig. 1.5 [20].

After successful registration, each stakeholder will be granted an authenticated and unique wallet identifier with an address. To log into the wallet, a two-factor authentication like wallet ID, a password is required. This wallet ID is a combination of alphanumeric characters which will be used as a username through which all transactions are recorded. A unique hash key is generated to a block for validating the transactions. To send funds from wallets, the recipient address or QR code is required. All these details will be stored on the Blockchain, and the stakeholder can access credentials like a case number, court number, date of proceedings, advocate, judge and investigation officer details, and next hearing dates. The events will be automatically executed by smart contracts which are notified to the convict regarding the petition filed through email. Figure 1.6 [20] shows Blockchain solution for Indian judicial system.

In current scenarios, intermediaries in the judicial system have a fair chance to intervene and affect the processes of judicial systems. Let's take a close look at it one by one.

Next Date. As per the present court proceedings, the hon'ble judges in the current judicial system allocate the next hearing date for the proceedings of case. However, the officials of court who sit adjacent to the judge will record the next date on the document ledger. The proponent of the court who has a good harmony with these officials enables court officials to bribe them and ask them to pen down the next date as per their wish, e.g., hon'ble magistrate might have given the next date as 15 September, but the court official might note down the next date as 15 October. This is a major loophole in the judicial system as there is a prohibition of audio and video recordings in court which is a major loss to a victim in terms of delay with court proceedings. One solution using Blockchain technology is to design an efficient algorithm for the next date generation based on court type, type of case, different Indian Penal Code (IPC) and Criminal Procedure Code (CrPC) sections, case age, FIR number, advocate name, etc. This information should be intimated to all the individuals through email for the next date.

Warrant Issuance. In the present court proceedings, the hon'ble judge in the judicial systems issues an order to recover the fine. As a part of this process, the judge passes an order with the issuance of a warrant against the complainant or respondent for the recovery of the fine. The court officials direct the concerned police station to issue the warrant to take necessary action and report back within a

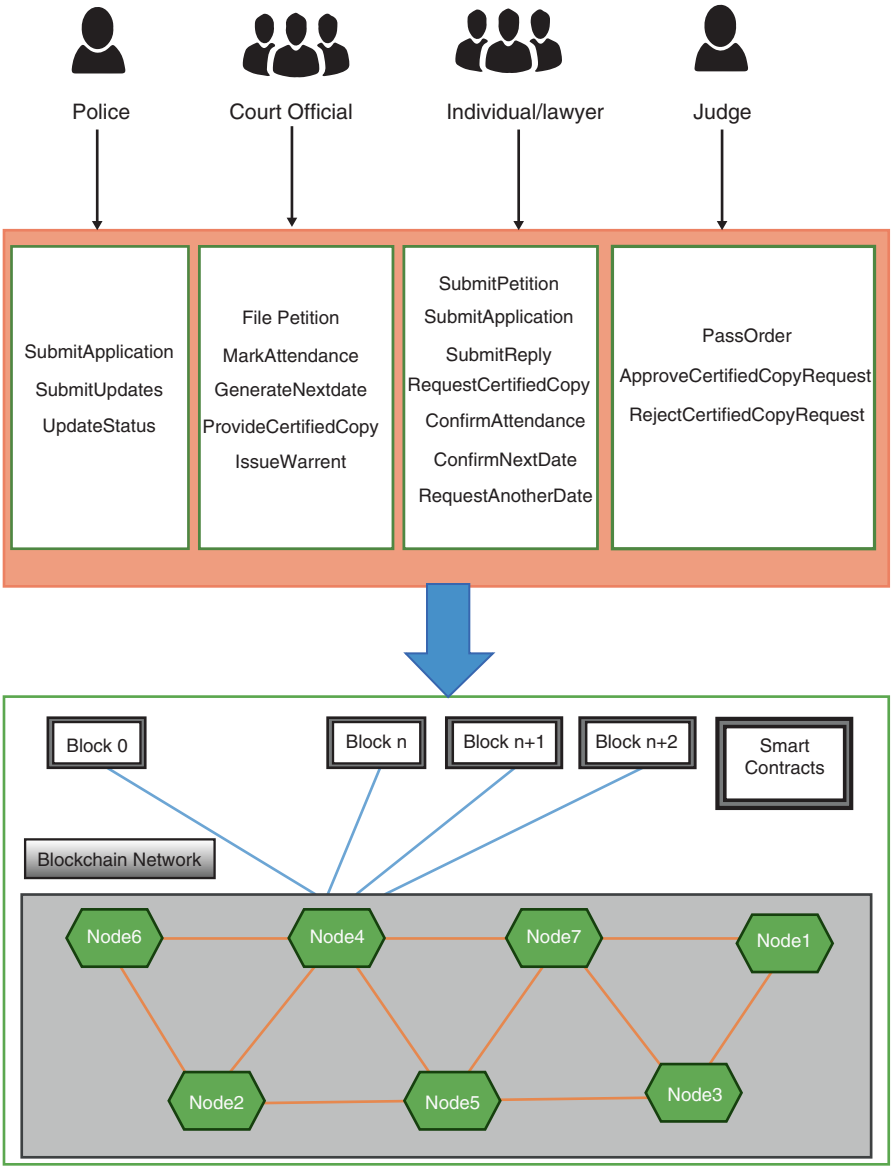


Fig. 1.5 Proposed Indian judicial system

scenario	New Individual
Invoked By	Court Official
Input	Name,Age,Gender, Address, ContactNumber, emailaddress, PANcardNumber
Output	wallet address
Trigger Event	Email wallet address to individual
Event Details	wallet address

scenario	File Protection
Invoked By	Court Official
Input	Case type,Current year, PetitionIPFSHash, sections, lawyer
Output	Casenumber, courtNumber, nextDate
Trigger Event	Intimate accused
Event Details	Complainant,CaseType, CaseNumber,CaseYear, sections,courtNumber, nextDate,petitioncopy

scenario	Mark Attendance
Invoked By	Court Official
Input	CaseType,CaseNumber, CaseYear, Individual/lawyer present
Output	attendanceUpdated
Trigger Event	Intimate concerned individuals to confirm Attendance
Event Details	CaseType, CaseNumber, CaseYear, Individual/lawyer present

scenario	Issue Warrant
Invoked By	Court Official
Input	CaseType,CaseNumber, CaseYear, applicationIPFSHash, orderIPFSHash
Output	exhibitNumber
Trigger Event	Issue Warrant as applicable and intimate concerned police officials
Event Details	warrant

scenario	Assign Next Date
Invoked By	Court Official
Input	CaseType,CaseNumber, CaseYear
Output	nextDate
Party present	confirmDate or requestAnotherDate
Party absent	automaticConfirmDate
Trigger Event	Intimate concerned individuals by email
Event Details	CaseType,CaseNumber, CaseYear, nextDate

scenario	Request Certified Copy
Invoked By	Individual/Lawyer
Input	CaseType,CaseNumber, CaseYear,exhibitNumber
Output	certifiedCopyNumber
Trigger Event	Judge Approval
Event Details	CaseType,CaseNumber, CaseYear,exhibitNumber
Approved	Trigger Event for Applicant to pay charges
Charges paid	Trigger event to email Certified Copy
Rejected	Intimate reason for rejection

scenario	Inward Entry
Invoked By	Court Official
Input	CaseType,CaseNumber, CaseYear,sender,sentDate,subject, documentIPFSHash, receiver,receivedDate
Output	InwardEntryNumber
Trigger Event	Intimate concerned individuals by email
Event Details	InwardEntryNumber,sender, sentDate,subject, receiver,receivedDate

scenario	Outward Entry
Invoked By	Court Official
Input	CaseType,CaseNumber, CaseYear,sender,sentDate, subject, documentIPFSHash,receiver
Output	outwardEntryNumber
Trigger Event	Intimate concerned individuals by email
Event Details	outwardEntryNumber,sender, subject, receiver,sentDate

Fig. 1.6 Blockchain solution for Indian judicial system

certain time period along with recovery details for further actions. However, sometimes, the court officials do not issue the recovery warrants to concerned individuals or police stations for several months or years unless it is followed up by the individuals or the advocate if not traced. Even if it is dispatched to the police, it will be difficult enough to keep track of when it was dispatched to the police to take further actions. In turn, the police may delay these actions for several reasons defeating the purpose of justice. The solution to this problem is achieved through Blockchain technology. The state government issues the predefined warrant format for different Indian Penal Code (IPC) and Criminal Procedure Code (CrPC) sections. Here, smart contracts can be used effectively to automatically generate the warrant upon the issuance of the order and add an action for police Blockchain. A report can be submitted to the court by the police through Blockchain which cannot be altered or deleted.

1.10 Maintenance of Land Records Using Blockchain

Keeping a secure data and storing it in real time are considered as some of the biggest challenges of the revenue department. Several issues related to land records arise due to inadequate information in different sections of the department and having no proper record management. Currently, registration of lands is done through

paper format which is more vulnerable and can be tampered easily. Due to unavailability or limited support of database, tracking changes of records in real time complicates the land issue registry. This problem can be solved using the Blockchain technology which is immutable, scalable, and more secure. With Blockchain, it's possible to store any information in real time. Any person can now sell, buy, or transfer the assets which are owned with less or no interventions from third-party agents like brokers making the system more transparent, secure, and cheaper.

1.10.1 Current Scenarios

In India, across all states, there are around two to three departments which take care of property-related registration and land-related documents. They are as follows.

Department of Stamps and Registry (DoSR). This department has the responsibility to maintain land registration along with verification during transfer of documents. This handles different types of deeds such as transfer of immovable property, marriage registration, bond paper, and other land-related documents. There are several different ways of acquiring immutable property like inheritance, through will, property purchase, property granted by court, or court. All the work of registration process and public interaction takes place at the Office of Sub-Registrar (OSR) which has the responsibilities like estimating value of the property, registering and preserving copies of sale deeds, collection of stamp duties, and issuing registration certificate

Department of Revenue (DoR). This department has the responsibility of preparing and maintaining records or transaction. Apart from these, it has complete authority of verifying transaction to handle disputes from revenue courts and any other governing agencies.

Survey and Settlement Department. This department has the responsibility of maintenance of cadastral and other survey maps [22]. Globally, many organizations have developed numerous platforms for maintenance of land records through Blockchain. Propy [23] is one platform which uses website and distributed application (dApps) for providing solution using Blockchain. Testbed [24] is another Swedish project which provides solution through Blockchain.

1.10.2 Blockchain Solutions

Even though digitization has improved the maintenance of property documents of land records, still, security, privacy, and transparency are major concerns for the revenue department. This problem can be solved using Blockchain technology which uses smart contracts for land record maintenance. Different stakeholders like the buyer, seller, bank, and government are involved in carrying out a Blockchain transaction. User details (buyers, sellers) are registered on a web portal to buy or sell

the property, and all the transactions are recorded on each different block in a Blockchain. The various roles of stakeholders are as follows:

Government: Any unowned land or property is registered by the government with details of land with its location (area per square feet).
Buyer: Using the website, the buyer registers details on a portal. The buyer is one who plans to buy assets.
Seller: The seller registers details on a portal using a website. The seller is one who wants to sell the property and notifies if there is any appeal from the buyer.
Bank: The bank acts as middle agent to authenticate the status of the buyer and seller.

Any user who needs to buy or sell the property needs to go through with the registration process. Figure 1.7 [10] describes the registration process where stakeholders like buyers, sellers, bank, and government create an account and get a private transaction key. Each user has unique key and address for website created by the Blockchain. Using this private key and address, user can log into the website for undergoing transactions [23].

After successful registration, the user can sell or buy single or multiple properties. Figure 1.8 [10] portrays the process of selling the land property where the buyer sends a request to the seller. The trade will be successful if the seller accepts

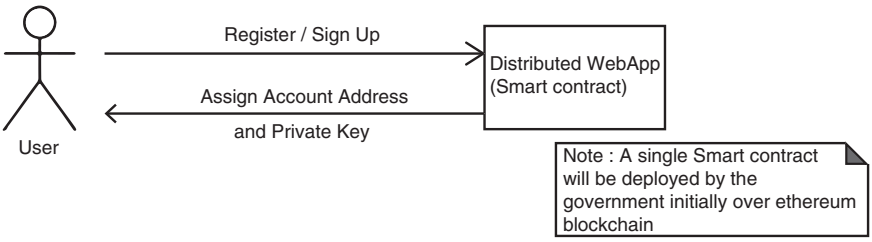


Fig. 1.7 User registration process for web app

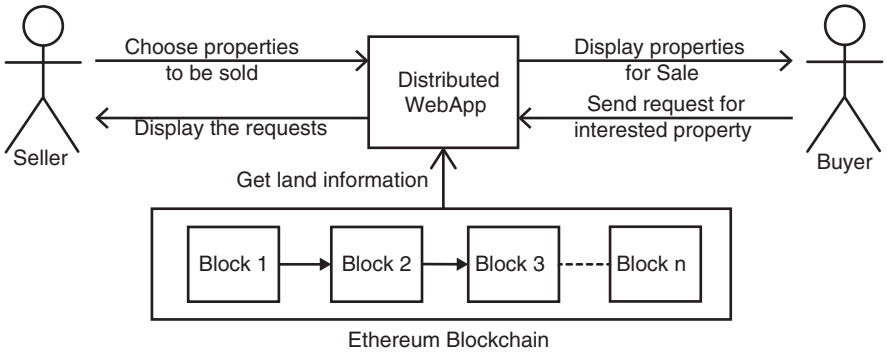


Fig. 1.8 Process of selling land property using Blockchain

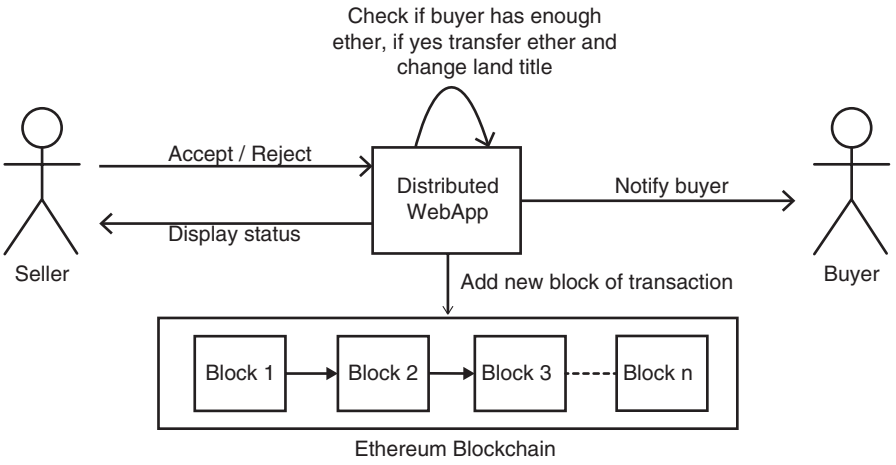


Fig. 1.9 Process of buying land property using Blockchain

request from the buyer and the buyer has sufficient ethers. The seller puts the property information that needs be sold on the application display with the property cost as digital currency ethers. The trade would be successful if all rules are satisfied as per the contract terms.

The buyer can buy the saleable property according to the price and owner details along with location of the land. Figure 1.9 [10] describes the process involved in buying property. Using the digital signature of the web app, the buyer makes a request to the seller to buy a property. The seller can accept or reject the request depending upon his interest. If the seller accepts request of the buyer, the smart contract will be automatically executed to check if all conditions are agreed and the consent is sent with money transfer in form of ethers. The buyer affirms it using digital signature, and the transaction is completed with land transferred to the buyer [23].

1.11 Conclusion

Blockchain is considered as one piece of emerging technology which has created an impact on the digital world. Even though this technology is not known to many people, it revolutionized and created an impression in the industrial world. This Blockchain technology has made life simpler by storing the information on a block by which some traditional transactions are transformed to being smooth and protected.

This chapter shows a brief insight about the fundamentals of Blockchain technology and how it works and explains the role of genesis block and other blocks in Blockchain. The different Blockchain types are discussed and the role of smart contracts to create trust and ease the transactions without third-party interventions. This chapter addresses solutions to industrial applications using blockchain technology in telemedicine and healthcare sectors which benefits society. This chapter concludes that functioning of Blockchain is secure and how it is implemented in many areas by considering two important case studies in the field of judicial and revenue systems.

References

1. Chakravarty, S. R., & Sarkar, P. (2020). *Introduction to blockchain: An introduction to algorithmic finance, Algorithmic trading and blockchain* (pp. 137–143). Emerald Publishing Limited. https://doi.org/10.1108/978-1-78973-893-320201017.
2. Chen, L., Cong, L., & Xiao, Y. (2019, August 10). *A brief introduction to blockchain economics*. https://doi.org/10.2139/ssrn.3442691.
3. Laurence, T. (2019). *Introduction to blockchain technology*. Van Haren Publishing. https://www.vanharen.store/amfilerating/file/download/file_id/4.
4. *Web Article: Blockchain & how it works*. Retrieved May 2018, from https://steemit.com/Blockchain/@suraj.blogit/what-is-Blockchain
5. Ratta, P., Kaur, A., & Sharma, S. (2020). A secured decentralized technology on blockchain. *IJAST, 29*(108), 2851–2859. Retrieved June 5, 2020, from https://www.researchgate.net/publication/341930378_Blockchain_secure_Decentralized_Technology.
6. *Web Article: Different Blockchain types*. Retrieved March 2018, from https://dragonchain.com/blog/differences-between-public-private-Blockchains
7. Kaur, A., et al. (2020 May). *Blockchain: A path to future, cryptocurrencies and Blockchain technology applications* (pp. 25–42). https://doi.org/10.1002/9781119621201.ch2.
8. *Web Article: Smart contracts on Blockchain*. Retrieved July 2018, from, https://www.ibm.com/blogs/Blockchain/2018/07/what-are-smart-contracts-on-Blockchain/
9. Raghavendra, K., & Ramesh, B. Managing the digital identity in the cloud: The current scenario. In *2015 IEEE International Conference Electrical, Computer and Communication Technologies (ICECCT)* (pp. 1–4).
10. Bhorshetti, H., Ghuge, S., Kulkarni, A., & Bhingarkar, S. (2020). Land record maintenance using Blockchain. In D. Patel et al. (Eds.), *IC-BCT 2019. Blockchain Technologies* (pp. 205–214). Singapore: Springer. https://doi.org/10.1007/978-981-15-4542-9_17.
11. Van Hijfte, S. (2020 July). *Blockchain platforms: A look at the underbelly of distributed platforms*. Morgan & Claypool Publishers. https://doi.org/10.2200/S01022ED1V01Y202006CSL011.
12. *Blog Article: key challenges to be addressed for adoption of Blockchain*. Retrieved November 29, 2019, from https://cyfuture.com/blog/8-key-challenges-to-be-addressed-for-adoption-of-Blockchain/
13. Joseph Holbrook, J. (2020). *Introduction to blockchain technologies: Architecting enterprise blockchain solutions* (pp. 1–26). https://doi.org/10.1002/9781119557722.ch1.
14. *Web Article: Explore Industry Applications on Blockchain*. Retrieved July 2018, from https://www.ibm.com/in-en/Blockchain/industries
15. IBM. (2020). FDA DSCSA Blockchain interoperability pilot project report. Available via DIALOG. Retrieved February 2020, from https://www.ibm.com/downloads/cas/9V2LRYG5

16. Astarita, V., Giofrè, V. P. et al (2020): A review of blockchain-based systems in transportation information 2020, 11, 21. DOI https://doi.org/10.3390/info11010021.
17. Mezquita, Y., Casadovara, R., et al. (2020 September). *Blockchain based architecture for the control of logistics activities: Pharmaceutical utilities case studies*. https://doi.org/10.1093/jigpal/jzaa039.
18. Farshidi, S., Jansen, S., & Verkleij, J. (2020). *Decision support for blockchain platform selection: Three industry case studies, IEEE transactions on Engineering management* (pp. 1–20). doi: https://doi.org/10.1109/TEM.2019.2956897.
19. Press Information Bureau, Government of India, Ministry of Commerce and Industry, India Improves Rank by 23 Positions in Ease of Doing Business. (2018). https://dipp.gov.in/sites/default/files/press_release_EODB_20112018.pdf
20. Khairwal, N., & Shah, R. (2020). Current Indian Judicial System: Issues and Blockchain Solutions. In D. Patel et al. (Eds.), *IC-BCT 2019. Blockchain Technologies* (pp. 229–239). Singapore: Springer.
21. Nitin K., Shalini S, Sumathi C. (2017) *Inefficiency and judicial delay. New Insights from the Delhi High Court*. Vidhi Centre for Legal Policy (pp. 1–32) India.
22. Case study. (2019). Land records on Blockchain. Retrieved February 22, 2019, from https://www.emudhra.com/
23. Propy Team. (2017). *White paper, Global property store with decentralized title registry*. Retrieved July 17, 2017, from https://assets.whitepaper.io/documents/
24. Kairos Future. (2017). A development project with lantmateriet, Landshypotek Bank, SBAB, Telia Company, Chromaway and Kairos Future. In: *The land registry in Blockchain – testbed*. Available via DIALOG. Retrieved March 2017, from https://static1.squarespace.com/static/Blockchain_Landregistry_Report

Chapter 2
Blockchain Applications that are Transforming the Society

C. V. Ravishankar and K. S. Kavitha

2.1 Introduction to Blockchain Technology

Latest technological developments in the field of electronics and computer engineering field remarkably changed the human and computer interactions and the world in general. Such developments in technologies improve the way the human society works. Various advancements in mobiles, computers, and Internet facilities give us the power of high-speed data transfer and data quality at its best; at the same time, the cybercrime rate also increased drastically as these technological developments are used by criminals.

Criminal activities in the cyber world are increasing day by day because of many reasons; for example, the latest computer and electronics products were extensively used by everybody, but in the same rate, the problems associated with it are not known by all the people as they are not aware of these technologies, but they are using the products which are made user-friendly; the cost of such products are decreasing day by day, and therefore, everybody intended to use those products irrespective of their economic background, as these products are mainly used for communication and entertainment and as the digital transaction is becoming more and more popular due to reasons like keeping large amount of hard cash currency is not advisable, due to duplicate currency circulation, everyone wants to do digital transactions for purchase of products and services and to pay for any transactions by means of credit cards, debit cards, and UPI transactions like Google Pay and Paytm, if users are using computers like PC or laptop or mobiles and using many apps

C. V. Ravishankar (✉)
Sambhram Institute of Technology, Bangalore, Karnataka, India

K. S. Kavitha
Global Academy of Technology, Bangalore, Karnataka, India

H. L. Gururaj et al. (eds.), *Convergence of Internet of Things and Blockchain Technologies*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-76216-2_2

related to bank software applications or by online usage of related bank web portals for transfer of money.

Many times, the messages received or sent by the users or by banks are by SMS or emails, which are all under threat now due to large scams and software glitches and also due to how good the attackers or hackers are in accessing the users' contact and communication details which leads to siphoning of bank accounts without notice of the real user. Generally, documents used for various purposes including bank documents, land documents, agreements, legal documents, court documents, and government and private transactions were documented for future references and clarifications; such documents are to be protected against various attacks by cybercriminals for changing the documents' contents and misuse. Various scientific researches, defense documentation, government secret documentations, and documents related to private and public organizations and companies have to be secured against hackers and cyberattacks.

The technology which protects the people, organization, and governments with regard to financial transactions and sensitive and confidential documents against cyberattacks and cybercrimes is blockchain technology. This is the latest and most trusted technology as to date which allows the user to protect his or her confidential and secret data, government authenticate documents, original documents, and communication and correspondence history against cybercrimes.

With this technology, no user or person can deny that the service, facilities, and transactions done or received are not done by them; that means this technology offers nonrepudiation, secrecy, confidentiality, and denial of service so that any user can be confident about their documents and transactions by using this technology. Then, what is blockchain technology? Blockchain is the digital, distributed, and decentralized ledger keeping track of all transactions without any mediator. A blockchain is also defined as immutable time-stamped records distributed and managed by virtual group of computers; here, each block in the block chain is actually digital information that pieces and stores information related to transaction date and time, origin details, participating parties, and identification details about each blocks as code. As far as blockchain technology is concerned, it does not matter who runs a blockchain and who owns it; that means it is important whether, functionally, the data and programs stored on a blockchain will be safe or not against removal [1].

The idea behind blockchain is creating a record which cannot be rewritable or editable but can be distributed. Stuart Haber and W. Scott Stornetta had this idea in 1991, but it became useful during the launch of Bitcoin in 2009. As to date, more than 1000 scientific papers are indexed only by Web of Science [2], and also more than thousands of paper on blockchain technologies were written in reputed journals; this itself gives an account of vastness of blockchain-technology-related research and developments. Still, in the world, people think that blockchain technology is meant only for cryptocurrencies, but beyond this, blockchain is used for many applications. Generally, the term distributed ledger is a consensus of shared, replicated, and synchronized digital data which spread across the globe; instead of the term distributed ledger, the term "blockchain" is used frequently as it is the only

data structure which offers maximum level of security . The Bitcoin blockchain, which uses the concept of "Proof-of-Work mining," is the most accepted method used to achieve distributed consensus. Similarly, few prominent blockchain platform solutions are Ethereum, OpenChain, Ripple, IOTA, Hyperledger, NEO, MultiChain, IBM Blockchain, Tezos, Quorum, Dragonchain, Corda, EOS, Stellar, OpenLedger, R3, Eris, and Hedera.

A blockchain is based on nodes, where nodes are formed by the network of multiple devices which are connected to each other through the Internet. It stores the records in a distributed peer-to-peer (p2p) method and later verified by all participating nodes. This type of ledger works on pre-defined rules which are agreed by all the participating nodes of the network. These rules are also called as protocols. The blockchain technology is based on many protocols related to various features like security, accuracy, and tolerance. One such important protocol is consensus protocol. It gives guarantee of the fault tolerance and security for blackchain systems [3]. This consensus is governed by an algorithm fed into the protocol layer of blockchain. An identical copy of each transaction is given by the blockchain to all peers which eliminates trust, thus making a trustless and distributed network.

2.1.1 Blockchain Advantages

Blockchain advantages include limitless decentralized record-keeping. Complete removal of human participation including third party in verification also helps in cost reduction. The advantage also includes the documents or blocks being tough to tamper, and because of this, the documents become highly private, transparent, and secure and become confidential. It allows the smart devices to communicate faster with high accuracy. Blockchain also offers accountability of every individual and every device involved; hence, the issue of manipulation is almost eliminated. The major characteristics of blockchain are decentralization, openness, and transparency [4]; therefore, the cryptocurrencies by blockchain technology will hand over the currency value controlling power and decision from the government to the public, which also reduces the middleman and intermediate documentation activities. The information and data once entered into the blockchain-based systems were immutable, hence avoiding the fraud on history and manipulation of the data. Accuracy of the technology is really appreciable, and to date, no such technology offers this much high level of security to the data. Cost reduction is another best feature of implementation of this technology for the long run. Decentralization with efficient, transparent, private, and secure transactions is also one of the best features of this technology especially for cryptocurrency, and all these became possibility because the backbone of blockchain is artificial intelligence, machine learning, data mining, and its hack susceptibility, and because of this, the blockchain can be used in almost all the places where the need of privacy and secret exists.

2.1.2 Blockchain Disadvantages

At the same time, blockchain technology also got few disadvantages like very low transactions of cryptocurrencies per second; using cryptocurrency in various illegal activities like drug trade, terrorist funding, block money laundering, illegal land purchases and criminal activities by crime syndicates; and its susceptibility to being hacked, because no technologies are hack-proof, so it is not disclosed by anybody to date that blockchain is breakable; if it was done, nobody announced it publicly. Another major issue related to blockchain technology is scalability and security problems [5] which actually decide the application area using blockchain technologies.

It is also observed that huge electric power is required to go through all the transactions in the chain. Another major threat to the blockchain technology is its private key; when the secret of private key is protected, it is immune from other people that has much security for the blockchain. And at the same time, losing the private key by forgetting or by accidentally erasing it from the secret file or storage device becomes costlier that it is almost a situation of losing all your data or cryptocurrency permanently as it is not at all retrievable in any way. This problem is also solved in few cases by having backup or secondary private key so that if the primary private key is lost, the user has an option of secondary private key to gain the documents and cryptocurrency, but at the same time, safeguarding and protecting both primary key and private key are even more complicated against the cyberattack and the brute force techniques wherein both the primary and secondary private keys are linked.

As it is very much clear that blocks in a chain are to be verified by the distributed network, it can take time which automatically leads to issue of transaction speed, scalability, and privacy leakage [6] that are other technical drawbacks. Other blockchain technology disadvantages include technology cost, speed inefficiency, and illegal activity, and central/reserve bank rules and conditions.

2.2 About IOT and IOT Devices

Various processes are controlled by devices through the Internet, which is called Internet of Things (IOT). Even though it is not new, for many years, it is at the initial stage of development as the Internet slowly entered into the digital controlling of day-to-day equipment and instruments, for example, present-day refrigerators, house automation, street lighting, traffic signal control, and drainage systems. As IOT devices are of machine to machine type initially, now and in the future, it is now machine-human-machine type, because of biosensors and DevOps along with AI and neural network-related developments that contribute high-level IOT systems. IOT is the outcome of combination of various technologies like sensor technology robotics, AI, wireless networks, embedded systems, machine learning, and automation and control.

To know these developments, the various threats, and its mechanisms, intrusion techniques and prevention process should be explored; IOT has got applications in various fields including medical and healthcare, transportation, consumer electronics, smart city, smart home and smart village, building and home automation, manufacturing and process industries, agriculture, sericulture, fisheries, horticulture, energy and power management, water management, environmental management, and transportation management. IOT devices look like independent device system, but practically, it is not; individually, no device offers fullest automation providing the area of application and place where it is being used.

2.2.1 Challenges and Constraints

Various security challenges are clipping the growth of IOT, and continuous connectivity between the starting and ending points is a must, but due to present-day communications and power restrictions and limitations, it is not able to fully establish the continuous connectivity. Similarly, this authenticates the services and endpoints and increases the privacy, integrity, and confidentiality issues for the users. At the same time, IOT installation and usage at urban areas are more complex as Wi-Fi networks and mobile networks are all used at various level of IOT usage which gives rise to IOT device security issues.

IOT devices and its operating system (OS) resource management mechanisms such as Contiki, TinyOS, and Reredos (real-time operating systems) really helped in a larger way to understand the OS resource management in IOT system and to look upon the implementation of advanced and smaller-size security software so that IOT devices are self-reliable and against any attacks. The microcontrollers work with low memory and hence cannot hold large software, so implementing security software within the IOT devices is not possible, and developing exclusively advanced and highly potent security software with possibility of requiring low-memory space is the main constraint. If the attack on IOT devices which are used in advanced processing industries, refineries, high-rise buildings, and other processing industries creates serious issues of functioning of these organizations, frankly speaking, drones are also a type of IOT device which can also be controlled through the Internet and remote console. Managing the IOT devices against cyberattacks is a really big task; in present-day situation, the possible weak points of any IOT devices are the sensors and password mechanisms; if the sensors are hacked and the wrong information was fed, then nobody can imagine the havoc created by IOT devices. For example, if the whole IOT system was hacked at the home/city/industry, then all the controls of IOT locking, entertainment, and control systems were under control of the hacker, with this control, the hacker can do anything on the IOT system which is really dangerous to the residents and workers and also may lead to large-scale devastation. Few IOT devices having advanced password or operating mechanisms like voice identification and/or image identification will create havoc in some cases

like if the user/house owner got throat infection/surgery, then no IOT devices can listen to him/her or recognize his/her voice commands.

2.2.2 Standards Related to IOT

As per the National Institute of Standards and Technology (NIST), US standards are given for IOT activities in two categories: IOT work and IOT-related work. In IOT work, these are technical needs and specific uses, where technical needs include lightweight encryption, advanced networking, cybersecurity for cyber physical systems, systems Bluetooth, security guidelines on RFID, and industrial control system (ICS) security guide and specific uses include connected transportation, smart cities, cybersecurity for smart grid systems, and wireless medical infusion pumps.

In IOT-Related Work. Cybersecurity framework an manufacturing profile, National Vulnerability Database, Security of Interactive and Automated Access Management Using Secure Shell (SSH), Systems Security Engineering (SSE), Digital Identity Guidelines (DIG), Security Content Automation Protocol (SCAP) standards and guidelines, standards and guidelines for software assessment management, information sharing on cyber threats, Supply chain risk management, and cloud security.

As per the NIST, Considerations for Managing IOT, Cybersecurity, and Privacy Risks (NISTIR 8228) is the first document in the series which NIST is developing to help IOT users protect their data and networks from unexpected compromise. The aim of NIST 8228 is to achieve protecting device security, protecting security of data, and protecting individual's privacy as its three risk mitigation goals.

In India, the Board of Indian Standards as to date contains overall published standards in all the 20,905 areas, and in the area of Electronics and Information Technology Department (LITD), total published standards are 1773. But in serial number 25, Committee No. LITD27 on Internet of Things and related technologies to date published only one standard. Similarly, in serial number 27, Committee No. 29 on blockchain and distributed ledger technologies to date published no standards, while the LITD27 standard ISO/IEC/JTC1/TC41/SC41 (P), Internet of Things and related technologies; does not state any standard procedures and regulations but directly refers to the International Standards Organization (ISO).

The International Standards Organization states that the standard is created in 2017 and mentioned that the scope of this standard ISO/IEC JTC1/SC41 is supported administratively by the International Electrotechnical Commission (IEC) which is handling international standards and conformity assessment for all related technologies.

All the information related to ISO/IEC/JTC1/SC41 is available on the IEC website under work program ISO/IEC/JTC1/SC41 with 19 listed project reference, 27 publications, and 47 project files. Under this, the total member of countries are 39 in that two countries, Kenya and Iceland, are associate members and the remaining 37 countries are full members. Here, all the 39 countries are categorized into two

groups, 27 as participating countries and 12 as observer countries, where India is acting as participating country along with the United States, Russia, Italy, Australia, the United Kingdom, Germany, and other prominent nations. It has various groups called as working groups, joint working groups, advisory groups, and ad hoc groups, where the three working groups are handling IOT architecture, IOT interoperability, and IOT applications; two joint working groups handling system interface between industrial facilities and the smart grid and IEC Smart Energy Roadmap; five advisory groups handling industrial IOT, utilities IOT, IOT trustworthiness, and IOT use cases; and finally, four ad hoc groups handling communication, IOT personnel positioning management system (PPMS), and trustworthiness interoperability.

As the aim of this chapter coincides with how technologies are transforming the society, the IOT technology and IOT devices are changing the dimension of society by providing a lot of facilities to the people; in this context, the few project references which are looking into human social interaction dynamics dealt in PWI TR JTC1-SC41-2 ED1, and trust worthiness principles are dealt in PNW JTC1-SC41-172. Based on the above points, still, worldwide accepted IOT standards are to be developed in various IOT areas especially IOT security and applications.

It is estimated by Cisco that around 50 billion IOT devices are in operation at the end of year 2020, whereas in 2016, the IOT devices in operation were 5.5 billion only; that means IOT is changing all the traditional technologies into advanced and more human-friendly by embedding with IOT, and it is creating an ecosystem of IOT through which all the needs of human society will be served whether it is handling refrigerator or managing high-power grids. The awareness in the people over the IOT is also rapidly changing; just few years back, nobody can thought of revolution of engineering process by IOT, and people awareness about IOT is really amazing; based on national IOT survey report by Tata Communications, as per economic times, around 54% of India's youth, that is, one out of two Indian youth in the age range between 18 and 25 years, have IOT-enabled smart homes and smart phones [7].

The IOT is also changing day by day by allowing other technology into its lap; already a lot of researches and implementation and development are happening very fast that artificial intelligence, edge computing, and quantum computing technologies were embedded and various technical implementations were started so that all these implementations contribute to increase in various characteristic features of IOT technology and IOT devices; for example, IOT can change the prospects and dimensions of cyber physical systems, because the major focus on smart cyber physical systems is to intelligently automate a variety of functions, with the main goal of hiding that complexity from the user [8]. In this way, the IOT devices can change any existing technology and its applications; that means the challenges with IOT devices and technology are to monitor and confirm the high service quality parameters like efficiency, real-time analytics, responsiveness, scalability, accuracy, security, adaptability, network latency, interoperability, storage handling, data memory, compactness, compatibility with advanced 5G communication infrastructure, privacy, surveillance, society ethics, handling confidentiality, and secrecy. When analyzing the history of IOT, the evolution of IOT is divided into different stages, namely, pre-Internet, Internet of Content, Internet of Services, Internet of

People, and Internet of Things. As per the survey by Extreme Networks, IOT is barreling toward the enterprise, but still, many organizations are highly vulnerable to IOT-based attacks.

2.2.3 Future of IOT

Artificial intelligence, robotics, fuzzy logic, blockchain technology, DevOps, cloud computing, cyber physical systems, data mining systems, big data analytics, drone technologies, nanotechnology, wireless sensor networks, biosensors, agile, business analytics, and sensor technologies are all getting integrated in one way or another way with IOT, which is broadening the application areas of IOT devices. The future of IOT technology is very bright; as the world is changing so fast and people wants to handle various data systems and gadgets from distance, the demand related to IOT product manufacturing, marketing, supply, service, research and development, and consultancy will be increasing drastically from 2020 onward.

In conclusion, IOT is the new mantra in the present world; all big companies are spending billions of dollars into research, development, manufacturing, and marketing of IOT product and solutions; developing robust IOT system which can work in various platforms simultaneously in real system environment is challenging. Protecting against cybercriminals is a Herculean task as the technology is changing so rapidly that every day, new features are added and new devices are developed, so another challenge of IOT devices is sustainability and long-run usage in order to use IOT technology in a practical approach, and real-time analysis of the environment where IOT systems are installed is to be done meticulously. The users and people who are using the IOT system must be sanitized so that the attacks should not happen by the insider.

2.3 Present Technological Challenges Faced by Society

The world is changing very fast due to rapid changes in the technology; in turn, the direct effect is on the society, where newborn child and aged person are in one way or the other facing this technological advancements both in positive and negative way; with the tonics, syrups, tablets, and capsules to space technologies and at the same time communication to agriculture, so many inventions and innovations are changing the lifestyle of every person in remote village or in modern cities.

The dynamics of societies whether it is in India, China, the United States, or Africa are in many ways affected by developments in technologies; cloth to automobiles are making people think differently as the technology changes the economic status of all, so latest equipment and devices like mobiles, TV, refrigerator, dish TV, smart vehicles, and computers can be used by almost everybody whether he or she is rich or poor. At the same time, the knowledge, information, and news are

transferred and disseminated to the last person of the society very easily; all daily day-to-day activities were changed due to this; various natural disasters like flood, volcano, hurricanes, and earthquake can be predicted almost accurately and early so that financial, life, and livestock losses can be drastically minimized.

The actual challenges for the society are how efficiently the technology can be used in their daily life and at the same time to reduce and save the human involvement, energy, and time for doing the repeated works or complicated works or the works which cause health or life trouble for human beings. As the population increases, food and water scarcity creates unrest in the society, and efficient utilization of water and fertilizer and cultivation of land to increase the food grain production; efficient handling of drinking water to avoid wastage and loss; good yield of crops; and storage and transportation and distribution of agricultural and nonagricultural, perishable and nonperishable, and commercial and noncommercial crops can be handled efficiently by using technology. At the same time, technology will not solve all the problems where human decisions and natural causes are involved; to overcome again these types of problems to certain extent, the technologies like AI, neural networks, and robotics can be of good help.

If the population statistics of the United States based on its 2010 census status [9] is considered, then out of total population of around 11,6716,292, the rural population is 22,772,300 only. Similarly, if the diversity of India is considered, especially rural and urban areas, as per the 2011 census of India [10], out of total Indian population of 12,105,69,573, the rural population is 833,463,448, and it is approximately 68.84%, and compared to 2001 census, the rural population was 742,490,639 which shows an approximate increase of 9% which is a positive sign, but at the same time, the problems associated with the villages and rural areas with respect to urban areas are getting wider day by day especially related to communication, transportation, connectivity, digital banking, food distribution and marketing, weather and price forecasting, and education which narrowly create a barrier for the economic growth at the rural levels and even at the stage where the whole country is poising toward 5G and beyond with advanced technologies, but it is an enigma for the rural people toward development.

As per the data from the World Bank—IBRD and IDA [11]—the rural population in India in percentage out of total population in 1960 was 82.076; during 1970, it was 80.24; during 1980, it was 76.902; during 1990, it was 74.453; during 2000, it was 72.333; during 2010, it was 69.07; and in latest data for 2019, it was 65.528, which clearly shows the decline in rural population, which also affects the equilibrium of resource distribution and technology implementation both at urban and rural population. At the same time, the decrease in population in rural areas directly affects the production of agricultural produce which indirectly hits the Indian economy. Below table gives the percentage of rural population with respect to respective total population at a glance as per the World Bank data spread from 1960 to 2019 for India, the United States, China, Australia, and Russia. Referring to Table 2.1, it is clearly visible that every decade, leaving few random cases, the rural population of all these countries is decreasing drastically, wherein the maximum decrease in

Table 2.1 Comparison table of rural population in top countries of the world

Country	Year							Percentage variation during 1960 and 2019	
	1960	1970	1980	1990	2000	2010	2019		
India	82.076	80.24	76.902	74.453	72.333	69.07	65.528	↓	16.55
The United States	30.004	26.398	26.262	24.7	20.943	19.228	17.541	↓	12.46
China	83.797	82.6	80.642	73.558	64.123	50.774	39.692	↓	44.10
Australia	18.471	16.001	14.448	14.567	15.765	14.818	13.876	↓	04.59
Russia	46.269	37.529	30.249	26.606	26.65	26.313	25.413	↓	20.85

rural population with reference to its total population is with China and least is Australia.

It is also an indicator of how technology changes the life of rural society and need of various facilities and infrastructure to attract the people to settle in rural areas; this is only possible when the governments take initiative of educating the rural people with latest technologies and its application and usage in their day-to-day life to solve their inevitable problems with low investment. People leaving the rural area leads to downfall of rural life expectancy in terms of economy, culture, and heritage of that area; in such scenario, the main sufferer is the agriculture and related farming; if population reduces, the implementation of technology in these areas will also drastically be reduced and make the people at rural areas become poorer day by day, so proper blend of people, facility, infrastructure, and technology must exist in rural areas which in turn definitely attracts more people to live in rural areas, which will make the country prosper.

In this context, considering all the aspects of present-society requirement, the problems associated with technological challenges for the society are as follows:

- Communication connectivity to remote areas is still not available.
- Good transportation and vehicle facility to all the areas is not available.
- Good drinking water facilities, medical facilities, and education facilities are not provided to all especially to the poor and village people of the society at almost free of cost.
- Proper solution to cultivating, producing, transporting, storing, distributing, and reducing the wastage and loss of the agricultural products is not yet successful.
- Digital technology is not available to all people of the society.
- Proper forecasting of weather and other climate situations is still a distant possibility.
- Introducing the latest technical advancements to agriculture, pharmacy, fertilizer, and pollution control, similar to defense, to other areas is not fully done.
- Providing modern and digitally enabled education to all the students in rural areas.
- To reduce infant mortality rates, good medical facilities for both people and animals especially at the villages is a distant possibility as of now.
- Water, milk, soil, seeds, food items, grains, and fertilizers' impurity or contamination testing, checking, and monitoring.
- Automated billing or maintaining and distribution of water, electricity, food, fertilizer, seeds, and other items from the farmers to buyers.
- Providing weather, flood, rain, and wind forecasting to avoid economic loss to the people.
- Preventing loss of human and agricultural crops and products due to wild animal intrusion and attacks.
- Land mapping and surveying and agricultural land and forest lands, irrigation, and barren lands assessment and to suggest proper crop farming.
- Assessing suitability of land and climate for commercial crop cultivation.
- Providing proper advanced and latest technology-based storage facility for perishable and nonperishable food and crops.

In all the above cases, the engineering and technology solution is not given to the fullest extent which made the society always turn toward engineers and scientists for better solutions for the problems, in order for the people to be happy in a society. Now, new developments of technologies in the area of blockchain technology, IOT, artificial intelligence (AI), neural networks, drones, 3D printing, automation, virtual reality, and other technologies really impact the society in many ways and provide advanced cybersecurity options for all types of usage and applications of both hardware and software.

2.4 Applications of Blockchain Technologies in Cryptocurrencies and in IOT

Before understanding the applications of blockchain technologies in cryptocurrencies, it is very important to know the concept of cryptocurrencies. Cryptocurrencies, also called as digital cash, are the opposite of hard cash or currencies like paper or coin type. As we trace the history of money, in earlier civilization, barter system was more prominent, and later, various types of money model came into picture; the first known currency form dated back to 5000 BC by Mesopotamian and later around 650 and 600 BC; the Lydians introduced the coins made of silver and gold. Similarly, the Chinese people first started to use the paper money in the seventh century by Tang Dynasty, and the earlier Chinese used copper coins.

The world's oldest currency in use is British pound, which is 1200 years. The American dollar is introduced in 1775 and called as continental currency and from 1792 called as US Dollar. The history of Indian currency dates back to many thousands of years, but it was identified back in the sixth century BC by the republic kingdoms of ancient India; later, at various rulers' period, it had various shapes and sizes and was of silver, gold, copper, and lead during the period of the Mughals; after defeating Humayun, Sher Shah Suri introduced silver coin named as Rupiya, and later in British rule, also, the currency was issued by using gold, silver, and copper; later in the eighteenth century, paper currency was introduced. Then, after setting up the Reserve Bank of India in 1935, it first introduced paper currency rupees in 5 January 1938. After their independence in 1947, the first paper currency printed by RBI is Rupees one note in 1949. And later, different denominations, sizes, colors, and designs of paper notes and coins were introduced.

In the world, various types of currency are in use which include paper and plastic notes, but still, fake currency or counterfeit currency is in use along with the original currency. This type of fake currency is introduced in any country for various reasons including political, economical, and military reasons by outside enemies like enemy country, terrorists groups, drug lords, external military agencies and similarly internal enemies like terrorists, religious groups, economic offenders groups, drugs- and real estate-interested persons, and political and religious peoples with only one intension of destabilizing the economy of any country. There exists a big difference

between fake money and black money, wherein fake currency or money is not the original currency issued by the government whereas the block money is unauthorized storing and circulating of the real currency kept against by nonpaying taxes toward the source of the income.

In the world, the counterfeit currency making dates back many years, but the earliest known instance is making counterfeit money by Germany's Nazi army during World War II, by making counterfeit money of British pounds and American dollars. Now also as per latest information, one in ten thousand dollars is a counterfeit currency; similarly, Indian rupees also got counterfeit currency which is damaging the economy seriously, For example, if we consider the counterfeit currency report of 2017 from the National Bank of Serbia [12], it clearly shows that 8% of US dollar, 49.2% euro, and 40.7% dinar are the total discovered counterfeits of the listed counterfeit currencies in Serbia.

All discussions lead to only one point, that is, even after various security options are taken care about the printing and distributing of the government currency by incorporating secret inks, secret design patterns, and different security provisions, it does not limit the making of counterfeit currency, which is a perennial problem not only in India but also throughout the world. To control this, only one possibility is introducing the digital money or virtual currency. Even though this has many advantages, this is not enough to convince the government and people as being the trusted money or currency due to many reasons; for example, it is not controlled by the government; it is not visible; it can be in the hands of block money operators; it can be destroyed without leaving proofs, if the person dies or losses the password or pass code, then that money cannot be transferred or retrieved permanently; if anybody knows the passwords, then they can do cybercrime very easily and the effect of this is devastating to not only to a single country but for the whole world; the digital money is universal in nature, so present money system which are offered differently by different countries will vanish; and another serious issue will be that due to this digital currency, the rich or poor country will be weighed the same, and economic structure of the world may become critical. For example, as per the RBI publication RBI WPS (DEPR): 03/2013: Estimation of Counterfeit Currency Notes in India—Alternative Methodologies [13], in India, during 2007–2008, out of 44,225 million number of currency notes, the number of counterfeit notes detected are 195,811, and it goes on in increasing numbers during 2011–2012, and out of 69,382 million number of currency notes, the number of counterfeit notes detected are 390,432. But, based on the advantages of having digital money on safety, antitheft mechanisms made it slowly acceptable by various countries.

As the online business, transactions, and money transfer became more and more prominent in the recent years, the hard paper or plastic currency transactions became less, and also, in transferring of huge money in terms of lakhs and crores, the digital transfer is found very safe, but still, many online frauds and hacking are active which create huge problem in online money transfer; all these cases lead to inventing digital money or cryptocurrency. The cryptocurrencies are nothing but the digital currencies, and in reality, it is virtual money generated, transferred, and saved in terms of cryptographic code and password mechanisms. These digital currencies

were fully safe, and codes are unbreakable provided it is supported by blockchain mechanism.

The blockchain can also be seen in IOT especially at the security level of both the IOT hardware and software, wherein the IOT devices and systems are openly used at all levels of usage from ordinary door opening to grid control, and at all of these areas, the input data, processing data, and output information have to be accessed and transmitted for next level of process or used by next level of IOT devices, and also normally, the inputs are coming from the sensors and sensor devices to the IOT devices for processing and related actions; the hacking and systematic attacks happen on the data, sensors, and software which have to be avoided; and also in almost all the cases, when multiple IOT devices are connected in different combinations, at each stage, the data repudiation and data authenticity are very much important so that the attack on any IOT device should not damage and jeopardize the whole IOT environment in any process. As software is more prone to get attacked than hardware in IOT systems due to the various limitations of software length, memory size, and security feature implementation, the best suited technology to handle IOT operating system features and application level software is blockchain technology. There exist various challenges to address the integration of the IOT with blockchain [14]; few to be seriously considered are the possible topologies to the integration and evaluation of blockchain nodes in IOT devices and systems.

In the same way, a new IOT server platform is proposed [15] by introducing a blockchain to store the sensor data. Mobius selected IOT server platform and authenticates IOT devices conforming to one machine to machine (M2M) communication standard, which receives a real-time sensor data and stores information in MySQL server and manages it efficiently. Another major problem associated with IOT is the protection of the privacy of data in IOT operation especially in real-time operations; in such scenarios, there is no other technology except blockchain that supports the IOT users against leaking of private data, as is [16] showed by applying zero-knowledge proof to a smart metering system to prove without disclosing the information such as public key.

In industrial automation and digital process environment, the requirement of security options and processing methods is different compared to nonsecured and non-IOT systems. But in both the situations, the security is at risk, and it is answered only by implementing blockchain security features because the blockchain-based systems exhibit decisive characteristic features of decentralization, security, and auditability [17] and build centralized IOT models to solve security challenges.

Another major threat to IOT system security is its vulnerability at the data collection stage; the proper analysis of data and authenticity of the data are most important as it is a deciding factor of the outcome of the IOT systems as [18] a scalable and configurable data collection infrastructure for data-driven IOT security emphasizes the collection of data from different elements of IOT systems, including individual devices and smart objects, edge nodes, IOT platforms, and entire clouds.

As IOT devices are not only connected physically but also virtually through the Internet, the IOT systems require its own software mechanism which handles online real-time data and its transferring and processing with highly secured environment;

this can be most successfully achieved by software-defined networking (SDN) technology also called as transport SDN (T-SDN), which improves the network performance and security options by offering better control on network traffic. The T-SDN is an SDN-based architecture for control and management of transport networks that could involve multilayer, multi-domain, and multi-vendor scenarios. In place of physical network devices, the SDN layer acts as a virtual software switch or router. The SDN-based IOT deployment models [19] further elaborated SDN-based IOT security solutions to present the comprehensive overview of software-defined security (SDSec) technology.

2.5 Other Application Areas of Blockchain Technology Which Transforms Society

The blockchain technologies are applied to improve the performances and security of the existing processes or to ensure new technologies are implemented for various applications. From digital currency to Internet of Things, the blockchain technology offers various application areas by allowing new innovation ideas and widely got applications in supply chain; business; healthcare; IOT; privacy and data management [20]; diamond and gold jewelry industry; health devices and services; customs; advertising and publishing; digital verification; baggage checking; loyalty points; automobile supply chain; vehicle insurance clearance; track and trace information of car; beauty product authenticity; big data security; data ownership; modern workforce handling; digitization of documents; carbon emission or foot printing; charity; clinical research and trails; connecting cars by IOT; dairy industry; defense; education certificates; government scheme implementation; combating fake news; fashion industry—apparels, designs, and fine arts, if real or fake; electronic health records; helping farmers—insurance and land documents; hotel industry; human resources; IOT and smart homes; IOT and logistics; IOT and data market places; KYC process in land registration; poultry industry; refugees; sports industry; robotics; vehicle registration; voting, transparency and any place voting; reduced order modeling (ROM); food safety; identity management; pharma industry for drugs duplicate; international trade: insurance, taxes, point of sale, share and share trading, MF trading, and transactions; buying and selling of electric power; telecom portability; fishing and fish concentration; wine industry; utility services, auto billing; IOT industrial cases; genome sequencing, bio-DNA; health insurance; smart city; smart village and smart factory; and many other unending list of areas where anyone can trust involvement of blockchain technology to offer good and smart transformation in the daily life of people in any society.

The latest buzzword is smart city concept, where maximum utilization and implementation of the latest technologies were adopted for all the related requirements so that the efficiency and accuracy of data or information, cleanliness, and other related maintenance with low cost and loss and less communication features

can be implemented, and at the same time, large mechanisms and systems based on IOT, computer networks, the Internet, and other digital systems require online and continuous monitoring mechanisms along with highly secured environment, so that no such untoward incidents of cybersecurity threats are to happen, and this can be achieved by implementing blockchain in IOT.

2.6 Conclusion

The blockchain technology definitely changes the direction of the modern world in almost all fields where computer technologies were in use; whether it is agriculture or astronomy, the main aspect is to protect the data and information from the hands of unwanted and unauthorized persons or entity and also to eliminate the middle-men concept whether it is government organizations or private organizations and to ensure the safety and privacy of the information and documents. Various day-to-day problems got solutions from IOT, so that it can be widely used from smart gadgets to smart cities, such as sowing the seeds or spraying the pesticides, transporting the precious organs for transplantation, shipment of emergency medicines, transportation of perishable items, and safeguarding precious items, and also, by the use of blockchain technologies, anyone can assure the safety and security of both the gadgets and users against any attackers or attacks.

References

1. Peck, M. (2017) Reinforcing the links of the block chain, White paper in IEEE future directions block chain initiative white paper blockchain incubator. IEEE.org.
2. Dabbagh, M., Sookak, M., et al. (2019). The evolution of Block chain- A bibliometric study, IEEE access.
3. Zhanga, S., & Leeb, J. H. (2020). Analysis of the main consensus protocols of blockchain KICS, Science Direct. *ICT Express, 6*, 93–97.
4. Hao, Q., et al. (2020). Research on the application of block chain technology in electricity trading system, E3S Web of Conferences 185, 01074 (2020). *ICEEB*, 2020.
5. Sun, J., Yan, J., et al. (2016). *Blockchain-based sharing services: What blockchain technology can contribute to smart cities*. https://www.researchgate.net/deref/http%3A%2F%2Fdx.doi.org%2F10.1186%2Fs40854–016-0040-y.
6. Zheng, Z., Xie, S., et al. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *2017 IEEE 6th International Congress on Big Data*. https://www.researchgate.net/deref/http%3A%2F%2Fdx.doi.org%2F10.1109%2FBigDataCongress.2017.85. DOI: https://doi.org/10.1109/BigDataCongress.2017.85.
7. ET Bureau. (2018). *The Economic Times*. https://economictimes.indiatimes.com/tech/internet/one-of-two-indian-youth-think-iot-is-about-smart-homes-tatacommunications/articleshow/66136302.cms?utm_source=contentfinterest&utm_medium=text&utm_campaign=cppst.
8. Craggs, B., & Rashid, A. (2017) Smart cyber-physical systems: Beyond usable security to security ergonomics by design. *IEEE/ACM 3rd International Workshop on Software Engineering for Smart Cyber-Physical Systems*.

9. United Census Bureau. https://www.census.gov/programs-surveys/decennial-census/decade.html
10. The India Profile - Census Info India. (2011). Office of the Registrar General & Census Commissioner, India, Ministry of Home Affairs, Government of India.
11. The World Bank-IBRD-IDA. https://data.worldbank.org/indicator/SP.RUR.TOTL.ZS?end=1960&start=1960&view=bar.
12. National Bank of Serbia. (2018, January). Counterfeit Currency Report, January – December 2017, Cash Department.
13. Sanjoy, B., & Abhiman, D. (2013). RBI WORKING PAPER SERIES Estimation of Counterfeit Currency Notes in India – Alternative Methodologies.
14. Reyna, A., Martín, C., et al. (2018). Blockchain and its integration with IoT challenges and opportunities. *Future Generation Computer Systems*, 173–190.
15. Jeon, J. H., Kim, K.-H. et al (2018), Block chain based data security enhanced IoT Server Platform. *IEEE International Conference on Information Networking*.
16. Lee, C. H., Kim, K.-H. (2018) Implementation of IoT System using Block Chain with Authentication and Data Protection, International Conference on Information Networking.
17. Ali, M. S., et al. (2019). Applications of blockchains in the Internet of Things: A comprehensive survey. *IEEE Communications Surveys & Tutorials, 21*(2) second quarter 2019.
18. Roukounaki, A., Efremidis, S., et al. (2019). Scalable and configurable end-to-end collection and analysis of IoT security data: Towards end-to-end security in IoT systems, Global IoT Summit.
19. Iqbal, W., Abbas, H., et al. (2020). An in-depth analysis of IoT security requirements, challenges and their countermeasures via software defined security. *IEEE Internet of Things Journal*.
20. Casino, F., Dasaklis, T. K., et al. (2019). A systematic literature review of blockchain- based applications: Current status, classification and open issues. *Telematics and Informatics, 36*. Elsevier, 55–81.

Chapter 3
Blockchain-Enabled IoT Integrated Autonomous Sewage Management System

G. B. Janardhana Swamy, D. R. Janardhana, C. P. Vijay, and Vinayakumar Ravi

3.1 Introduction

In any sector of sewage plant, chemical industry, and mining industry, protection is a very important factor. To reduce dangerous event and increase safety features for sewage cleaners, this project proposes to develop an intelligent safety device which is able to detect unsafe incidents in the sewage system. Sewage cleaners are not provided with any safety devices such as face mask or hand gloves. They are intended to clean by their bare hands. This is a very big problem. Because of this, the sewage cleaners suffer from many severe diseases such as diarrhea and viral fever, and sometimes, it goes to the abnormal changes in health condition, etc. Many people have died because of improper handling of sewage. The sewage contains many harmful poisonous gasses. When the person jumps to depth to clean the sewage without any proper safety device, there may be a chance of inhaling the poisonous gasses. This causes severe problem. We have many death incidents that have occurred recently. By observing all these consequences, we planned to implement a safety device for the sewage cleaners; it can be a helmet or any other wearable device. In this project, we are going to design a continuous monitoring system that measures parameters of the system, such as temperature, CO_2, poisonous gasses and humidity, and also, it continuously checks the health condition of the person such as

G. B. Janardhana Swamy (✉) · D. R. Janardhana
Sahyadri College of Engineering and Management Adyar, Mangaluru, Karnataka, India
e-mail: janardhana.is@sahyadri.edu.in

C. P. Vijay
Department of Information Science and Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India

V. Ravi
Assistant Research Professor, Center for Artificial Intelligence, Prince Mohammad Bin Fahd University, Khobar, Saudi Arabia

H. L. Gururaj et al. (eds.), *Convergence of Internet of Things and Blockchain Technologies*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-76216-2_3

heartbeat and pulse rate. For this, we are using some sensors such as temperature sensor and gas sensor. If any abnormal condition occurs, it will inform the person by making buzzer sound.

3.1.1 Blockchain Technology

A blockchain is a distributed ledger and without any intermediary; it conducts operations more securely. In the Internet of Things (IoT) sector, blockchain techniques are becoming more common to fix security and privacy issues. So, blockchain techniques are widely used to protect various IoT applications from attacks. Distributed architecture of blockchain helps to solve privacy and security issues of IoT applications in various ways:

- Blockchain can be used to protect sensor data from the malicious data by avoiding duplication.
- Distributed architecture will be well suited for IoT devices by providing identification and authentication and for secure data transfer.
- Intermediate not required for IoT data exchange purposes.
- Blockchain can prevent data tampering.
- Efficiently, blockchain manages the identity and integrity of the data and provides one-to-one communication.
- Blockchain technology is more cost-effective in the field of IoT deployment and from its operations.
- Blockchain addresses IoT devices directly with the history of connected devices.

Blockchain-based methods support to foster the IoT security. How will blockchain be the solution for IoT system? Blockchain is the architecture in the form of distributed ledger, and it contains the number of data blocks linked together with the help of cryptographic techniques and forms the chain. Blockchain makes computationally robust and infeasible to change the data in particular block. This technique makes sure that its immutable, decentralized, transparent, and it builds trust. In the blockchain, there are numerous forms of consensus mechanisms that are as follows:

- Networks for public blockchains
- Private networks for blockchains
- Permissioned networks with blockchain
- Blockchain of consortium

In public blockchain networks, anyone can join the network and participate, e.g., Bitcoin. But the main drawback of this is no privacy in transaction and weak security. In private blockchain networks, a single organization governs the entire network to allow participants in the network and execution of the consensus protocol and maintain the shared ledger. This significantly increases the trust and courage among the participants. In permissioned blockchain networks, businesses which run

privately can deploy the permissioned blockchain network, and participants seek invitations from the organization to join the network.

Multiple entities may share the responsibilities of managing the blockchain within consortium blockchain networks. Blockchain is necessary for IoT to improve reliability, scalability, interoperability, privacy, and security. Interoperability means communication takes between different IoT systems by exchanging the information. Checked spatial and temporal information from the data blocks stored in the blockchain can be traced to IoT data. Reliability can be achieved through the implementation of cryptographic mechanisms to protect the integrity of IoT data. Without the interference of third parties, IoT systems may communicate with each other.

3.1.2 Architecture of IoT

The stages shown in the Fig. 3.1 are explained here.

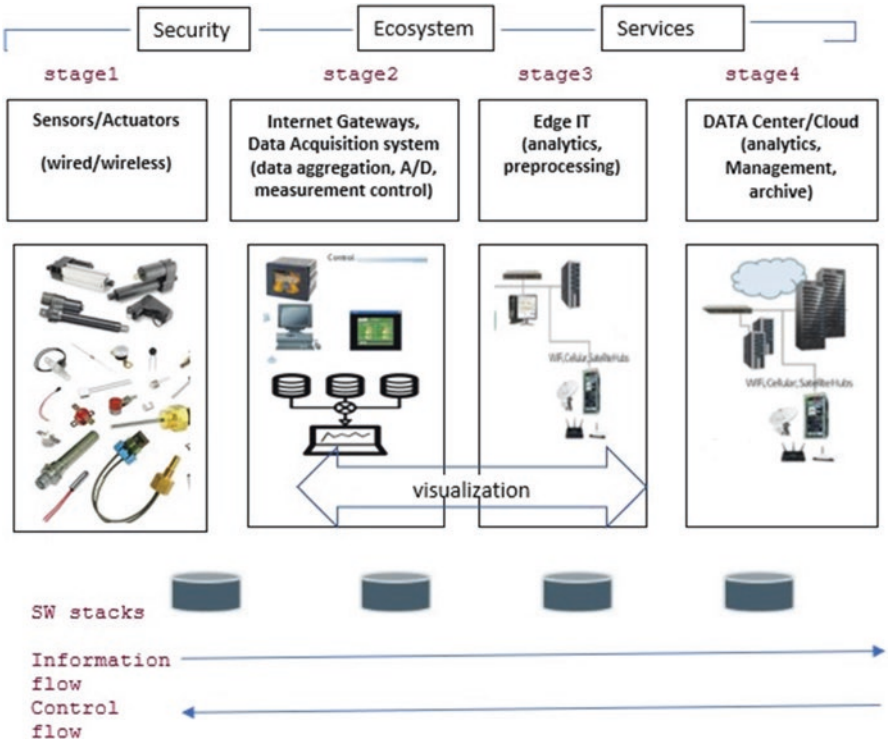


Fig. 3.1 Architecture of IoT [1]

3.1.2.1 The First Stage: Things that Are Networked (Wireless Sensors and Actuators)

The outstanding feature of sensors is their ability to transform the data collected for analysis in the outside world into data. In other words, in order to get information in an appearance that can be actually interpreted, it is important to start with the inclusion of sensors in the four stages of an IoT architecture system. For actuators, the process goes much further; these devices are able to interfere in the physical reality. For example, the light can be turned off, and the temperature in a room can be changed. Thus, the sensing and actuating stage covers and changes anything required for further study in the physical world to obtain the necessary insights.

3.1.2.2 The Second Stage: Aggregation Networks of Sensor Data and Transfer of Analog to Digital Data

Although this IoT architecture process still means working in close proximity to sensors and actuators, there are also Internet getaways and data acquisition systems (DAS). Specifically, though Internet getaways operate via Wi-Fi and wired LANs and perform more processing, the latter link to the sensor network and aggregate performance.

The critical importance of this stage is to process and squeeze the enormous amount of knowledge gathered at the previous stage to the optimum size for further study. Besides, here occurs the requisite conversion in terms of timing and structure. Stage 2 renders data both digitalized and aggregated, in short.

3.1.2.3 The Third Stage: Edge IT Applications Presence

During this time, the prepared knowledge is transferred to the IT environment between the stages of IoT architecture. In particular, edge IT systems perform enhanced analytics and preprocessing here. It applies to machine learning and visualization technology, for instance. At the same time, before the stage of entry into the data center, some more processing may occur here.

Similarly, Stage 3 is closely linked to the previous phases of IoT architecture development. Because of this, the edge IT systems' location is similar to the one where sensors and actuators are mounted, making a cable closet. At the same time, it is also possible to work in remote offices.

3.1.2.4 The Fourth Stage: Data Processing, Administration, and Storage

In the data center or cloud, the main processes take place in the last stage of the IoT architecture. Specifically, it allows in-depth processing, along a follow-up examination for data. Here, the skills of both IT and operational technology (OT)

professionals are required. In other words, the stage already contains the top-rated analytical abilities, both in the digital and human worlds. The data from other sources can also be used here to ensure an in-depth review. After following all the quality criteria and specifications, the data is returned to the real world but still in a processed and precisely examined appearance.

3.1.2.5 IoT Architecture Stage 5?

In fact, by adding an extra stage in it, there is a choice to broaden the process of building a sustainable IoT architecture. It refers to initiating the control of a user over the structure if, of course, only your result does not involve full automation. Visualization and management are the key assignments here. The device becomes a circle after the inclusion of Stage 5, where a user sends commands to sensors/actuators (Stage 1) to perform certain acts.

3.2 IoT Applications

Configuring a smart world and self-conscious autonomous devices, such as smart living, smart products, smart health, and smart cities, are the key goals of the IoT [2]. The following section addresses IoT implementations in the fields of industry, medicine, and home automation.

3.2.1 In Sectors IoT

The IoT has provided a fair opportunity to create huge modern frameworks and applications [3]; the approved person will screen the current area and creation of a vehicle in a savvy IoT transportation system. Likewise, the authorized person will predict his future area and street traffic. The word IoT was used in the previous process to differentiate one kind from RFID products. To date, specialists have correlated the term IoT with sensors, tools, mobile phones, and actuators of the Global Positioning System (GPS). Recognition and management of emerging IoT technologies are mainly focused on information protection and data security. The IoT provides various items that are linked, monitored, and observed, resulting in valuable data and private information obtained. Security assurance is an increasingly fundamental problem in IoT conditions as opposed to conventional systems since the amount of IoT attacks is high.

3.2.2 IoT in Personal Medical Devices

The basic goal of medical care is to guarantee the safety of the system in order to keep patients safe from pernicious attacks. They have their predefined targets at the stage where attackers target mobile phones. Typically, their point is to take the data, attack gadgets to use their properties, or shut down certain programs that check the condition of patients. There are various forms of attacks on medicinal gadgets that involve stealthy listening in which the patient's protection is spilled, uprightness error in which the message is altered, and usability problems that include battery-depleting assaults. Some advanced security threats associated with the protection, security, and prosperity of patient remedial data are discussed as follows:

- For any errand that uses battery power, PMDs are fundamental. Therefore, restricted encryption must support these gadgets. If the device is a component of different systems, there will be a high risk of confidentiality, accessibility, protection, and trustworthiness at that point.
- Because PMDs have no remote correspondence validation instrument. So, the information put away in the gadget could be effectively accessed by unapproved individuals.
- In addition, the absence of safe validation exposes the gadgets to various other security dangers that can contribute to vindictive assaults. Denial of service (DoS) attacks can be dispatched by an adversary.
- Patient information is transmitted through the communication medium, which may be changed by unapproved parties, so a patient's protection may be unfortunate.

In Smart Home IoT. The IoT brilliant home administrations are expanding step by step [4]; advanced gadgets can adequately speak with one another using Internet protocol (IP) addresses. In a keen home environment, all savvy home gadgets are associated with the web. As the quantity of gadgets rises in the shrewd home state, the chances of pernicious attacks also increase. If savvy home gadgets are run autonomously, the chances of vindictive assaults would also decrease. Wherever and wherever, keen home devices can be reached across the network. It generates the chances of malignant attacks on these gadgets in this way. There are four parts of a vibrant home: administration level, brilliant gadgets, home door, and home system. Numerous devices are connected to the brilliant home and exchange knowledge using a home device cleverly. Therefore, there is a home portal that governs the advancement of the data between the external system-related gadgets. The administration process utilizes specialist coop administrations that relay different administrations to the home system.

3.3 Review of Literature

The Internet of Things (IoT) is one such technology that has emerged with a tremendous growth in recent times, while there are some issues associated with security. The other conventional methods also failed to overcome the issues [5]. Blockchain (BC) is a new emerging technology that makes use of the concept of Bitcoin, which is now being used to overcome privacy and security issues in peer-to-peer networks [6].

Security has been the main concern in IoT since it has been hindered in large-scale deployment. IoT devices often suffer distributed denial of service (DDoS) which makes it a threat to security [6]. Even scalability is a current threat to IoT networks. Normally, when a number of nodes are connected to IoT, each node needs to be authenticated and authorized. Authentication and authorization will be done by centralized system in regular. When number of IOT device increases, the centralized system may go in difficult phase for the process [7]. IoT scalability challenges can be handled by another breakthrough technology, that is, blockchain or distributed ledger technology (DLT) along with security measures. Blockchain is an information game changer due to its unique capabilities and benefits. Hackers would be avoided by adding another layer of security. Using blockchain to store IoT data would add another layer of security which would contribute to decrease in security threats.

The main objective is to understand if the IoT and blockchain design can be used to encourage decentralized applications. As it is one of the initial phases of examining procedure, a survey on IoT engineering and its current issues along with its countermeasures for vulnerabilities in IoT design are discussed. We have found the countermeasures that tend to assault in the IoT engineering. Another constantly growing ledger is blockchain also known as distributed ledger technology; it plays a major role in IoT security field to secure the data more precisely without an intermediary. Blockchain changes the world of information due to its unique features and advantages. A blockchain system includes a distributed digital ledger that keeps the record of transactions more securely shared between participants in the system that is over the Internet. All the transactions are certified and recorded in the ledger and cannot subsequently be amended or removed. Using blockchain to store IoT data would be a tremendous technique and add another layer of security that hackers would need to bypass to get access to the network.

In IoT, there exist access management technologies, but they are formed on centralized system which has the technical issues related to security faced worldwide. Thus, to make it more secure, it requires decentralized mode for there is no involvement of third party. The new system is a completely distributed ledger technology and decentralized network that there is no centralized authority involvement, so that IoT technology has more security with the involvement of blockchain technology [7] (Fig. 3.2).

In spite of IoT being in its peak of its career, privacy and security are major challenges. The blockchain-based IoT architecture handles efficiently most of the privacy and security constraints, and it provides the best possible methods to avoid

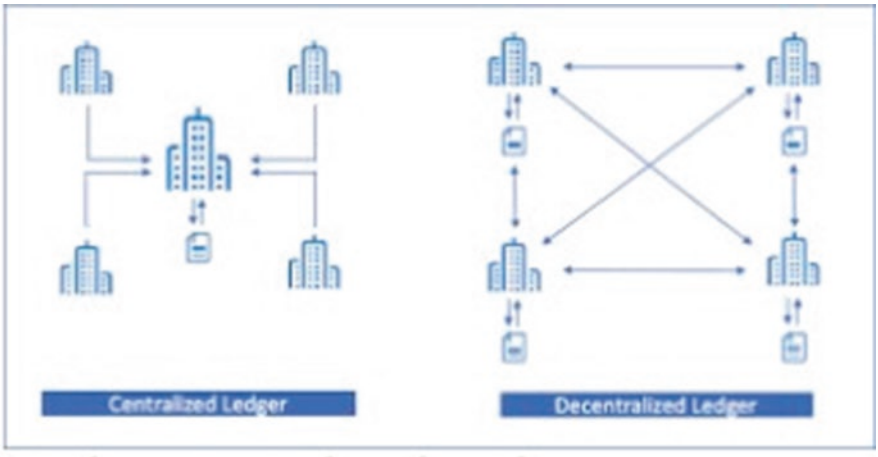


Fig. 3.2 Centralized and decentralized ledger

overhead delays. In IoT, there are many threats to be solved such as the modification attacks and denial of service (DOS) attacks. However, along with the questions, so many effective answers unfold such as decentralization and intrinsic broadcast medium with which we can achieve accuracy [8]. However, this architecture stays as a basement for further studies in this regard by giving efficient privacy and security in the field of IoT while preserving to have most of blockchain technology [9, 10].

New applications based on IoT are being developed for the user, but low security measures may lead to critical issues. Since these data are stored in a centralized manner, sensitive user data can be used, thus leading to a break of privacy. Blockchain has shown significant promise in the recent years in achieving the abovementioned goals as it has intrinsic security. Blockchain being "Secure by Design" can justify risks involved in security by providing data encryption, immutability, and transparency [11]. Tracking the devices connected to IoT can be done with blockchain by improving extensibility, dependability, transparency, and confidentiality. This is also used to enable or coordinate transaction processing [12]. Three layers are mainly involved in IOT; they are service, enterprise, and device layers. The physical components are present in device layers. The service layer has hardware and software. Service management and business applications are at enterprise layer. Blockchain can be engaged at the device level or at the service layer. Because of the limitations in storage and computational power of IoT devices, deploying blockchain at service layer provides more flexibility [4]. Integrating blockchain in the context of IoT is not straightforward and has several significant challenges like to do a proof of work. It requires high resources, transaction confirmation takes time, and scalability is also less. Implementation of blockchain is by eliminating the concept of proof of work. This proposed framework depends on ranked structure and distributed trust to maintain privacy and security and make it suitable for IoT-based projects.

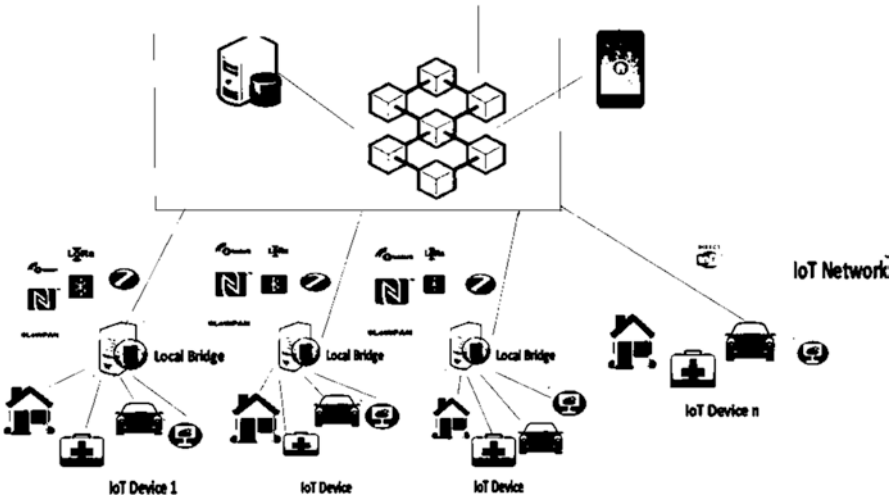


Fig. 3.3 A conceptual scenario [13]

Figure 3.3 shows the conceptual scenario of IoT blockchain combined system for secured architecture where all IoT sensor data are connected decentralized data store [13].

Internet of Things (IoT) leads to number of challenges in the area of decentralization and is weak in interoperability, privacy, and security concerns. So, integration of blockchain technology in IoT may augment the features. Based on the requirements for IoT blockchain, architecture may be proposed [14]. Integrating blockchain with IoT systems leads to greater opportunities, such as increasing the interoperability operations in the IoT systems by converting and loading the data into the blockchain. Security can be augmented in each block of the data by using encryption process in the blockchain.

In IoT systems [2], major challenges are security and privacy due to large-scale deployment of IoT devices in distributed nature. Blockchain approaches provide better security and privacy of data. Initiating lightweight cryptographic techniques in blockchain can improve the feature of IoT systems. In blockchain, miners will preserve the private and secure blockchain used for various auditing and controlling the communication. Miner is a device which processes all the incoming and outcoming transactions. Control over the transactions can be done by sharing the key to the devices connected in the network among each other directly. Key will be shared by the miner device in the network. Security requirements that need to be addressed in the blockchain are confidentiality, availability, and integrity. Confidentiality ensures the authorized users only able to read the data. Integrity ensures that data sent at the sender side should be available same at the receiver's side without changing the information, and availability makes sure that data or the service should be available all the time whenever customers need it.

Security is the major concern in the IoT use cases [15]. Many blockchain-based techniques emerged to address the security issues using intrusion detection and prevention system. Security architecture is designed on the basis of network structures, key management, control access, trust management in IoT, and the application used. Privacy is another issue in the IoT system; to address these, robust cryptographic measures are used to protect against third parties and provide access to the authorized users. Major drawback of the blockchain technology on IoT system is resource-constrained devices. Security architecture divided it to three level to implement blockchain technology in the IoT systems. In the first level, IoT devices generate the data that can be hashed using SHA-256 algorithm and then finally stored in the third level called cloud.

The authors of [16] have carried out a report on the method of coal mining and its implications. They have seen the obstacles faced by coal miners. To improve the safety characteristics of coal miners, they developed a smart helmet project. This helmet was able to identify three of the most dangerous incidents in the mining area, such as air pollution, miners' removal of helmets, and head collisions.

By incorporating networking technology, the authors in [17] tried to make the helmet even safer. The added network is used around the mining workers to sense the environmental circumstances. Using IOT, all real-time values are changed wirelessly on the network.

A system developed by the authors [3] consists of a processing segment that takes input, processes it, and provides output. For the purpose of detection and alteration, they built an embedded device with ARM-Acorn RISC Machine (ARM) micronutrient and various gas sensors that help to remove the risk in people's lives.

The authors in [18] defined the implementation and design role of IoT applications' Underground Drainage and Manhole Monitoring System. A system for monitoring water level and ambient temperature and pressure within a manhole and to check if a manhole lid is open is given in the proposed model. It also tracks electric power mounted underground.

3.4 Proposed System

The sewage cleaners are not having sufficient knowledge about poisonous gasses, chemicals, etc.; they are not provided with any safety devices. They are intended to clean by their bare hands. This is a very big problem of sewage cleaning people. Because of this, the sewage cleaners suffer from many severe diseases such as diarrhea and viral fever, and sometimes, it goes to the abnormal changes in the health condition, etc. Many people have died because of improper handling of sewage. When person jumps to depth to clean the sewage without any proper safety device, there may be a chance of inhaling poisonous gasses. This causes severe problem. We have many death incidents that have occurred recently.

In Fig. 3.4, IoT network of sewage cleaning system is connected to admin through gateway and also device registration, and sensitive data are managed

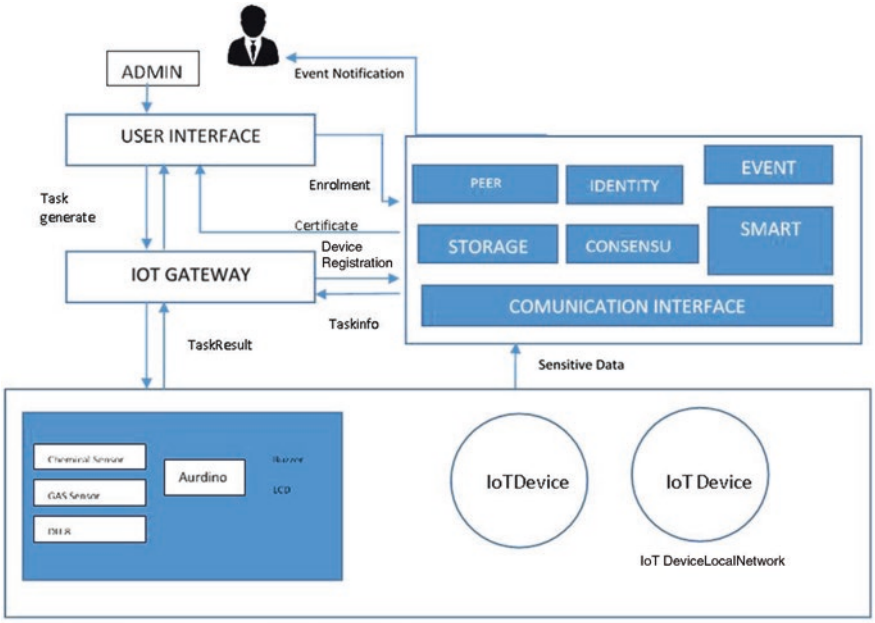


Fig. 3.4 Proposed system

through the blockchain technology. Sensor critical data are stored in blockchain network. In the proposed system, blockchain technology used are peer management, storage management, consensus, smart contract, and event management.

3.4.1 System Design

3.4.1.1 Arduino Uno

Figure 3.5 depicts Arduino Uno which is an ATmega328-based (datasheet) microcontroller board. It has 14 digital input/output pins, 6 analog inputs, a 16 MHz ceramic resonator, a USB link, a power jack, an In-circuit serial programming (ICSP) header, and a reset button (of which six can be used as Pulse Width Modulation (PWM) outputs). It includes all the microcontroller needs for support; just connect it to a computer with a USB cable, or power it to get started with an AC to DC adapter or battery.

3.4.1.2 Gas Sensor

Figure 3.6 shows gas sensor module that consists of a steel exoskeleton under which a sensing element is housed. This sensing element is subjected to contemporary through connecting leads. This modern day is known as heating modern day via it;

Fig. 3.5 Arduino Uno

Fig. 3.6 Gas sensor

the gases coming near the sensing element get ionized and are absorbed by using the sensing element.

3.4.1.3 DH8

The DH8 is a digital output; relative humidity and temperature sensors can be used as a monitoring and preventive measure in homes for people with illnesses that are affected by humidity. They are also found as part of home heating, ventilating, and air-conditioning systems. Humidity sensors measure and report both moisture and air temperature. Figure 3.7 shows the DH8.

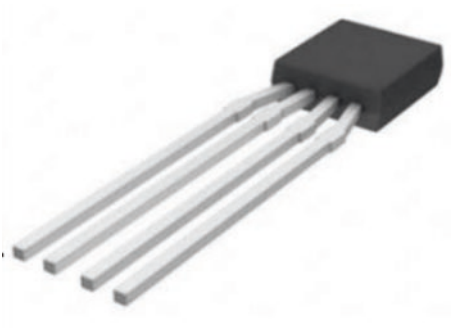


Fig. 3.7 DH8

Fig. 3.8 Chemical sensor

3.4.1.4 Chemical Sensor

Chemical sensors isolate and detect specific chemical elements/compounds along with their concentration within the environment (in this case, sewage) in order to extrapolate the sample concentrations to the larger environment. The chemical and biomedical sensors are most frequently used for detecting and monitoring the physical or chemical properties of various substances. Figure 3.8 shows the chemical sensor.

3.4.1.5 Buzzer

A buzzer or beeper is an audio signaling device, which may be mechanical, electromechanical, or piezoelectric. Typical uses of buzzers and beepers include alarm devices, timers, and confirmation of user input such as a mouse click or keystroke. The buzzer is shown in Fig. 3.9.

3.4.1.6 LCD Display

Figure 3.10 depicts LCD display; liquid crystal displays (LCDs) are a commonly used to display data in devices. It is a flat-panel display or other electronically modulated optical device that uses the light-modulating properties of liquid crystals.

Fig. 3.9 Buzzer

Fig. 3.10 LCD display

Liquid crystals do not emit light directly, instead using a backlight or reflector to produce images in color monochrome.

3.5 Implementation

To reduce dangerous event and increase safety features for sewage cleaners, this project proposes to develop an intelligent safety device which is shown in Fig. 3.11, which is able to detect unsafe incidents in the sewage system. Sewage cleaners are not provided with any safety devices such as face mask or hand gloves. By using blockchain technology, we try to fight against denial of service attack by using different levels. At the beginning level, it will block the attacker who tries to install the malware on our network, and moreover, these devices are not directly accessible. Miner node will monitor all the transaction happening in our network. At the second level, the process takes place on the outgoing traffic by analyzing the packet header. Since any header is constituted by the DDoS attack, then they would be blocked from the current network.

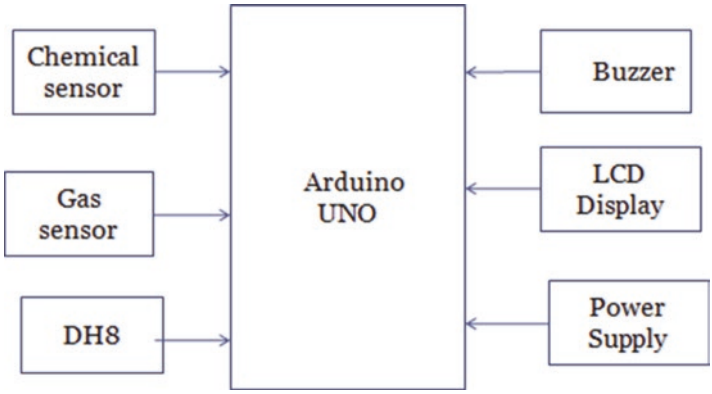


Fig. 3.11 Sewage alert monitoring system

3.6 Conclusion

The blockchain-enabled IoT that integrated autonomous sewage management system described in this chapter presents great security enhancement and efficient monitoring of the sewage system. When these smart devices are built, various features such as reliability, affordability, damage prevention, and maintenance issues are addressed. Smart device is developed and implemented for the sewage cleaning people's continuous monitoring and warning system and also gives people knowledge of sewage gases and chemicals. In addition, the device acquires real-time data, and buzzer displays it for warning on the LCD. Blockchain technology has been integrated with IoT systems to protect data exchange from external attacks.

References

1. Fuller, J. R. (2016). *The IoT liftoff*. https://techbeacon.com/enterprise-it/4-stages-iot-architecture.
2. Dai, H. N., Zheng, Z., & Zhang, Y. (2019). Blockchain for internet of things: A survey. *IEEE Internet of Things Journal, 6*(5), 8076–8094.
3. Vijayalakshmi, R., & Sengeni, D. D. (2017, November). IOT based smart detection system for harmful gases in underground sewages. *International Journal for Research in Applied Science & Engineering Technology (IJRASET), 5*.
4. Dorri, A. L., Kanhere, S., Jurdak, R., & Gauravaram, P. (2019). *Blockchain for IoT security and privacy: The case study of a smart home*.
5. Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems, 88*, 173–190.
6. Madumidha, S., SivaRanjani, P., Rajesh, S., & Sivajumar, S. (2018). Blockchain security for internet of things: A literature survey. *International Journal of Pure and Applied Mathematics, 119*(16), 3677–3686.
7. Novo, O. (2018). Blockchain meets IoT: An architecture for scalable access management in IoT. *IEEE Internet of Things Journal, 5*(2), 1184–1195.

8. Coetzee, L., & Eksteen, J. (2011, May). The internet of things-promise for the future? An introduction. In *2011 IST-Africa Conference Proceedings* (pp. 1–9). IEEE.
9. Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017, March). Blockchain for IoT security and privacy: The case study of a smart home. In *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)* (pp. 618–623). IEEE.
10. Lavanya, R., Singhal, A., & Gupta, S. (2019, January). A systematic survey on Blockchain for IoT security. *Journal of Advanced Research in Dynamical and Control Systems, 11*(03).
11. Miraz, M. H., & Ali, M. (2020). Integration of blockchain and IoT: An enhanced security perspective. *Annals of Emerging Technologies in Computing (AETiC)*. Print ISSN, 2516–0281.
12. Firoozjaei, M. D., Lu, R., & Ghorbani, A. A. (2020). An evaluation framework for privacy-preserving solutions applicable for blockchain-based internet-of-things platforms. *Security and Privacy, 3*(6), e131.
13. Hang, L., & Kim, D. H. (2019). Design and implementation of an integrated iot blockchain platform for sensing data integrity. *Sensors, 19*(10), 2228.
14. Conoscenti, M., Vetro, A., & De Martin, J. C. (2016). *Blockchain for the internet of things: A systematic*.
15. Roy, S., Ashaduzzaman, M., Hassan, M., & Chowdhury, A. R. (2018, December). Blockchain for iot security and management: Current prospects, challenges and future directions. In *2018 5th International Conference on Networking, Systems and Security (NSysS)* (pp. 1–9). IEEE.
16. Manusmare, A., et al. (2017). Study based on intelligent brain helmet for coal miners safety. *International Journal of Science, Engineering and Technology Research (IJSETR), 6*, 1278–1280.
17. Borkar, S. P. (2018). IoT based smart helmet for underground mines. *International Journal of Research in Engineering Science and Management (IJRESM), 1*, 52–56.
18. Muragesh, S. K., & Rao, S. (2014). Automated internet of things for underground drainage and manhole monitoring system for metropolitan cities. *International Journal of Information & Computation Technology, 4*.

Chapter 4
e-Reside: A Case Study on Blockchain for IoT in Home Automation Using Raspberry Pi

Prashanth Kambli, A. Ashwitha, and G. Shruthi

4.1 Introduction

There is a rapid development in the area of Internet of Things and it is growing in a vast aspect. It mainly refers to the billions of computing devices connected to the Internet worldwide in order to transfer data more efficiently and effectively. As data transfers via the web with the devices that are embedded with sensors and many other peripherals with connectivity over the Internet, there is a chance of misuse or hack of data. Due to violations in security policies, more security problems rise on this condition. This can be achieved by the usage of blockchain technology, as it was first popularized in bitcoin growing nowadays to the great extent. Also, in using of blockchain, some of the security issues can be resolved. One way that can be done is to make secure communication between IoT devices.

Since limited resources are available like storage space and low computing performance, network composed on lightweight devices gives a lot of problems. The applications of technology for robust security that helps in reduction of security performance will pose many significant challenges. In order to overcome this problem and have a better solution, the use of blockchain with strong security is much more suitable for IoT-based problems that have weaker security. In this context, many more research activity is being performed for improvement in security and more precise and better effectiveness of IoT network considering blockchain on IoT [1].

Internet of Things and blockchain are two different technologies, attaining their popularity from the time of their origin. IoT will have an influence in almost all the devices we use every day, and it would be expected to increase in the upcoming

P. Kambli (✉) · A. Ashwitha · G. Shruthi
Department of Information Science and Engineering, M S Ramaiah Institute of Technology, Bangalore, Karnataka,, India
e-mail: prash.kambli@msrit.edu; ashwitha.a@msrit.edu; shruthigmysore@msrit.edu

H. L. Gururaj et al. (eds.), *Convergence of Internet of Things and Blockchain Technologies*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-76216-2_4

days. At the same time, there can be more threat in misuse of technology, as existing technology still needs to be more advanced to handle the current situation. One of the best solutions for this would be blockchain technology to provide better security issues related to IoT [2].

Today's world is full of automation and digitization; it has made the life of every human simpler by replacing all old manual systems into automated ones. IoT has created a platform where all the supporting devices are interconnected and are controlled remotely across the various architectures made on network. IoT is focused on the concept of home automation with the use of computers and monitored through smart phones. The IoT devices can even monitor and control the various electronics and mechanical devices used in the entire building. Here, the devices are even connected to the cloud for storage and maintained through admin configurations. With this, it really helps in monitoring of all devices securely and remotely [3].

In the current trend of automation, all the manually controlled devices are made to work simply by sending data to controlled station by applying IoT technology in a sensor network node [4]. IoT applications are becoming more dominant with the use of the Internet and improvisation in mobile technology along with improvised standards in mobile communication. All these support IoT to reach a great extent [5].

IOT mainly works by receiving the input by sensors, today in market we can find many sensors that supports IOT usage. Virtual devices need to be developed to control these devices that need to have more portability in the form of support and the operating systems installed [6]. An IoT-based system installed in a building for a smart wireless security system will send alert or command to the owner, if there is any intruder within the designated area, by receiving the message from other peripheral sensors in the specified network architecture that are connected [7]. Combining the analysis of data received from different cameras and various sensors connected should provide good security in communication interface and is essential to provide technological solutions and to have individual security in focus [8].

New technology is incorporated for automating the entire house with the use of IoT-based technology along with household activities that is more comfortable and convenient with healthy nature and also more safe and economical [9]. Another form of IoT-based remote control application can also be made applicable with the methodology that uses the system on gesture recognition built by sensors that are visualized and wearable [10]. Some of the devices from the network of IoT that are being used for various applications are mainly embedded such that they are all in small sizes with some computational resources that are restricted and mainly have energy constraints [11].

The objective of the work e-Reside is to have a secured home monitoring all the time, have temperature sensing, and identify gas leakage through sensors and also for any water leakage to be detected and intimated to the user. It also focusses on reducing the usage of power consumption with the help of light-detecting resistors (LDR) and finally the usage of cameras to watch the home round the clock. All these devices will be monitored by Raspberry Pi device.

4.1.1 Blockchain in IoT

Literally speaking, blockchain is just the chain of various blocks. This means that the digital information in the form of blocks that gets stored in a database that can be public is the chain of information. Blockchain gets added with new data from the various blocks that get stored of these data. As a result, there will be multiple blocks getting threaded on each other. In order to add a new data to the block, a certain transaction needs be occur and its verification to be made and then stored in a block with the given hash.

Blockchain was introduced firstly for decentralized transaction and management of data for bitcoin cryptocurrency. From 2008, many started using concept of blockchain interest in has its development increased to a great extent, because of having facility for security, privacy, and integration of data in controlled transactions avoiding third-party association. Because of this, it has created more interest in the area of research, mainly toward technological challenges and its limitations [12].

Education, manufacturing, medicine, finance, etc. are the various sectors that have incorporated the use of blockchain applications to gain the unique bundle of characters of this application. In the aspect of security, it even promises providing benefits in trust, collaboration, organization, identity, credibility, and transparency in the use of application. Analysis has been made in order to show the usage of blockchain technology along with its properties on open science that can be benefited. Comparison on open science ecosystem and characteristics of blockchain technology prove the technology that suits its infrastructure [13].

As blockchain is the core technology of bitcoin, it has gained a lot of popularity. Utilization case is growing toward various fields that include IoT with security, banking sector, industries, and many medical centers. Among these, IoT has vastly expanded in accepting the blockchain technology due to its deployment on smart homes and other city development across the world. As IoT-based network devices mainly operate on limited power in computing with its low capacity toward storage and network bandwidth, for example a camera can be controlled remotely using a mobile phone consuming less bandwidth, they are close to attacks on the other end points, which are PCs, cell phones, and other digital gadgets [14]. Common operating picture gets enabled with IoT for various applications in today's living world. As more advancements are seen in wireless sensor network devices, common operating picture is achieved in network through exchange of information and analysis of various performances. With the use of central server only, the IoT applications exchange information and authenticates the data that leads to security and privacy concerns [15].

IoT devices are drastically increasing in both civilian and military concepts, among the various smart cities and smart grids. Daily upgradation is seen in technology, in order to meet the requirements of a human in this data-driven society. As there seems to be more advancement in semiconductor and communication technology, it allows multiple devices to connect on a network, such that the people can connect and communicate with machines.

The technology is also considered as Internet of Everything, involving the Internet of Things (IoT), Internet of Medical Things (IoMT), Internet of Battlefield Things (IoBT), Internet of Vehicles (IoV), and many more [16].

Serverless record-keeping method is one of the features of blockchain. To make a decentralized form of IoT in communicating with the use of blockchain, to reduce the requirement of centralized form, many more efforts are being put by the researchers, resulting into having an idea on the core research interest as blockchain-based IoT [17].

4.1.2 Raspberry Pi and Its Usage

"Raspberry Pi" is a low-cost, small size, maybe of a credit card size, computer that can be plugged into a monitor, connected with all other peripherals of a computer device. As the size of the device is small, all aged people can work and explore in computing and even in learning to create a program in languages such as Scratch and Python. One of the specialty of the device is insertion of an SD card to the provided slot in the board of Pi, which resembles hard disk for the device. Requirement of power can be supplied through the USB and through HDMI port for connection to a monitor with a cable. It can be inserted with keyboard, Wi-Fi, Bluetooth, and mouse through USB slots. Raspberry Pi is designated as a microprocessor and a microcontroller. It can be classified as a system on chip (SOC) as shown in Fig. 4.1 with a multicore processor, ROM, and GPU; I/O peripherals are all on a single board.

Considering the vision of IoT applications, its usage in diverse range of research work has increased, even with its few disadvantages with the current existing prototype for IoT technology [18]. For blockchain technology, the low-cost minicomputers can be used. Based on the hardware resources usage, it can be fitted for many applications that relate to technology of blockchain. Raspberry Pi is used as a minicomputer along with the technology of blockchain as an open source, blockchain-based, decentralized software (Ethereum) platform [19]. Decentralized form of

Fig. 4.1 Raspberry Pi 3 Model B Board

Ethereum used as a platform in running the contracts that are smart. Applications are running precisely as programmed without any option of interruption, restriction, scam, or third-party interference. Raspberry Pi is among the perfect fit for running an Ethereum node since it can run on its own till the time we decide to stop it.

As discussed, automation plays a vital role for all workplace and at even homes mainly when it comes into the concept of security. Currently, these automation techniques can be implemented over embedded microcontroller devices with its associated sensors. Like a minicomputer, Raspberry Pi systems function with small setup, as it contains GPIO and USB ports that take action of connectivity. With the help of these ports, the various other peripherals are interconnected and can be used in multipurpose activities [20]. With the help of Wi-Fi technology, smart phones get connected to Raspberry Pi through its IP address. These wireless applications will always be user-friendly with which it improves the efficiency and lifestyle of human users. With this mode, the system has overcome all the drawbacks that were observed using Bluetooth and Zigbee technology. Raspberry Pi is used in IoT applications that are connected in order to control and manage all the intelligent objects through their own IP address [21].

4.2 Home Automation

The interconnection of various peripheral devices and sensors to a software implanted in the house for security measure becomes a home automation. With the help of connectivity over network, there will be usage of exchanging the collected data among the peripherals and storage. In building automation, various control systems will be planted for utilization and have a clear view of residential extension. Many switches and sensors are connected to the modern systems through a central post called "gateway," such that the user can view all data in mobile phones, PCs, or any other gadgets through user interface. These data will be able to view in video formats and even sometimes used in storing the data in the cloud [22].

In today's scenario, home automation is quite common in controlling all the home appliances of electrical and electronic devices using smart phones. With the use of relay circuit, IoT technology can even control various home appliances through its on wired or wireless mode of connection [23]. For the control of all the devices at home, the technology with Bluetooth can also be used. The usage of it is with Bluetooth module that is HC-05 and a controller for Bluetooth that has an interaction from the mobile to various appliances [24] (Fig. 4.2).

In today's market, there are many industries working on the concept of home automation in order to provide an excellent service to all its vendors. Some of the applications even connects to the cloud and can be mainly used in storage activity.

Fig. 4.2 Smart home automation system

4.3 Related Work

There has been a lot of work carried out on home automation using Raspberry Pi devices, also deployed for the result in the cloud, and then, it is accessed on web page control. Day by day, the entire world is changing very fast in the form of advancement in technology, human being's comfort, and need of automation work on mobile technology. Table 4.1 shows some of the literature work mentioned for home automation work on different forms.

4.4 Case Study Implementation

Here, the case study being implemented uses Raspberry Pi technology and cloud platform over the blockchain of IoT to have a private, secure, and decentralized information in smart home. Earlier systems were controlled through Bluetooth and Zigbee devices, where the connectivity was for limited area. It was difficult to control devices from remote place through the Internet because of device compatibility, and embedded c platform was not supported for others.

To overcome these issues, a model was designed that applies new ideas to the existing systems and improves upon that. The system uses Raspberry Pi technology to overcome existing issues, and we control external devices even from remote

Table 4.1 Literature work on various applications for smart home

Sl. no.	System	Communication interface	Applications	Benefits	Year
1.	IoT with Raspberry Pi for smart home automation [25]	SMS and alarm	A web application that gets integrated with cameras and motion sensors	Human interactions is reduced, absolutely an affordable system	2015
2.	IoT-based smart home security system [26]	Open-source hardware platforms	Mobility sensors, heat sensors, and gas sensors along with web-based camera for security	Up-to-date sensor architecture as a reference for further applications is developed	2019
3.	IoT-based smart home automation system using WSN [27]	Wireless sensor networks	Wi-Fi module, TBSA algorithm	Energy-efficient for data encryption than all approaches	2017
4.	Risk analysis for smart home automation [28]	Tools in analyzing the integrated and automated risk development	Smart home with imposed system of security with improvised privacy form	For a system with smart home automation, risk with threats to be analyzed	2016
5	Smart home automation for IoT-based system using sensor node [29]	MCU ESP8266-based node along with Arduino Uno	Most of the house electronic appliances controlling and monitoring	Energy efficiency with less cost and flexible device	2018
6	District of smart, through IoT and blockchain [30]	ICT, IoT, and BC	Integrated on smart grid, smart service, and smart house	IoT and BC approach for a replicable model and can be implemented	2018
7	Problem of compatibility in smart homes with platform updation [31]	Use of JSON prototype	For healthcare, AI, and ambient assisted living	To have networks that are heterogeneous for a system for unified control	2020
8	To have smart home for the development of smart cities [32]	Arduino, with application-based Wi-Fi	For development of smart systems	To have smart house	2020

areas. The user having no knowledge toward electronic devices also can still easily control external devices using this technology. The intention in choosing Raspberry Pi technology is to overcome power consumption issues than earlier systems that use minimum of 5 V. It also supports almost all platforms and is much compatible with all programming languages. Here, we use the cloud with Raspberry Pi technology to overcome disadvantage of existing system where devices are controlled within a restricted area using Bluetooth, Wi-Fi, and proprietary protocols. To remotely control devices, we use Amazon's cloud service.

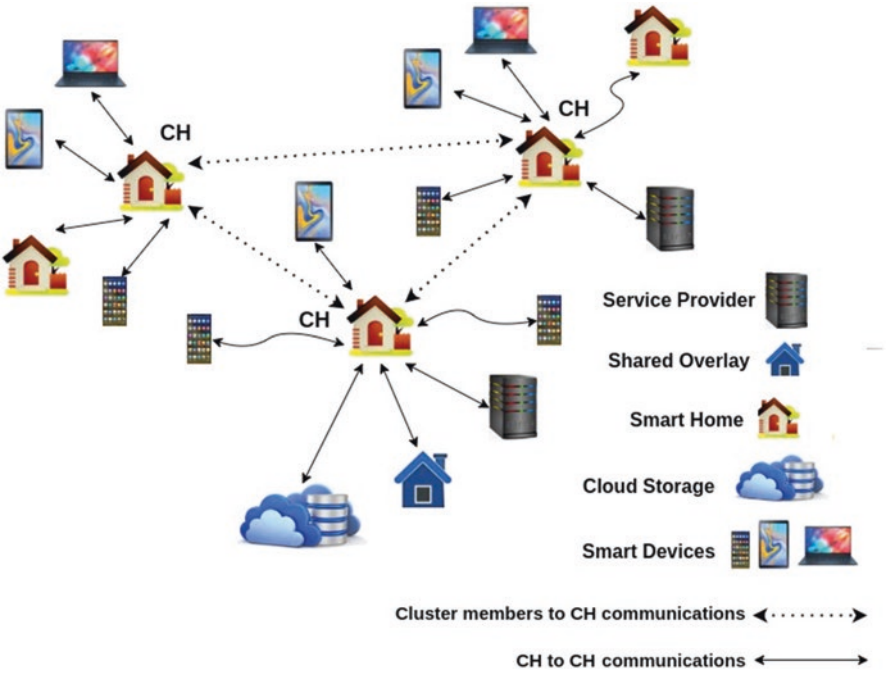


Fig. 4.3 Overview of the bitcoin-based architecture [33]

Our proposed framework has smart home, cloud storage, and overlay as three main components. Smart home contains smart devices which form an overlay network with cloud storage, smart devices, and service provider which is shown in Fig. 4.3; all the nodes in the network are grouped into different clusters, and every group nominates a cluster head (CH) to avoid network impediment. Cluster heads in the overlay network use requester and requested key lists in accordance with bitcoins. Requester key list has the details of user and has access to the smart homes with their public keys. Records of public keys of smart homes connected to the cluster are sanctioned to be accessed in the cloud to store the information of the smart home [33].

4.4.1 Implementation Requirements

In order to implement the abovementioned case study, the technologies and devices used are the following:

- Raspberry Pi 3 Model B 64-bit Quad Core ARM CPU with Wi-Fi
- Amazon S3 cloud server

- PuTTY configuration that enables user to connect to Pi server and user using static IP address
- Web-based application supported by Tomcat web application server.

4.4.2 Architectural Design

Figure 4.4 represents framework that is the calculated outline that characterizes the structure and conduct. It characterizes the segments or building pieces mentioned in the framework that give an arrangement of items required for built up and help in cooperation in executing the general form. It is also capable of controlling all sensors associated in design remotely and displaying and storing data and also even visualizing the sensor data.

The component of the system is as follows.

A grouping chart demonstrates the members in collaboration and the succession of messages between them. A succession chart demonstrates the communications of the framework with its on-screen characters to perform all part of a utilization case.

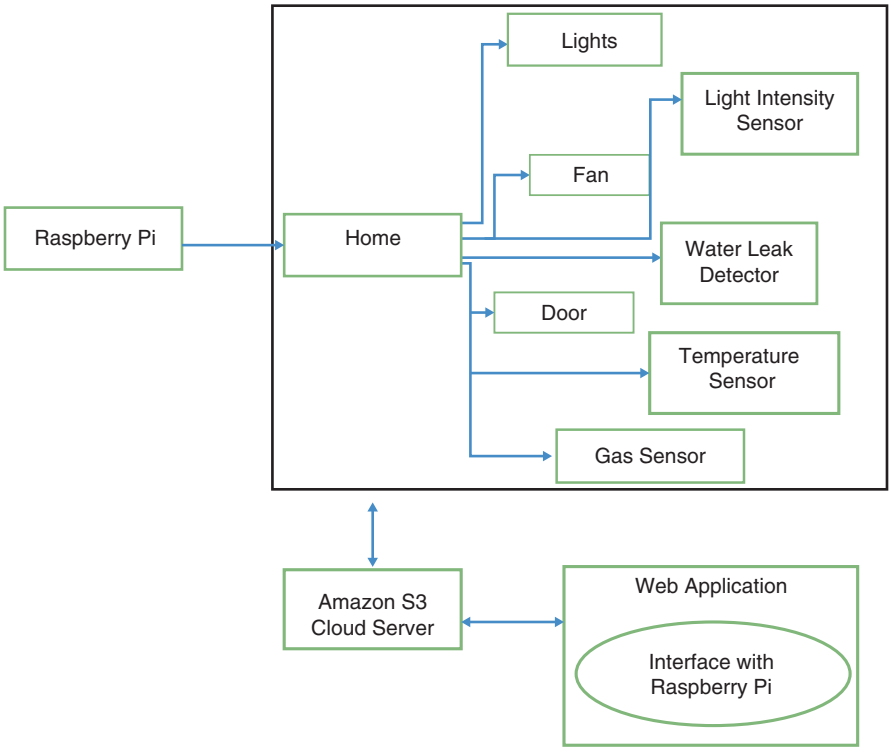


Fig. 4.4 System architecture

Here, the user sends the signals to the cloud server and from the cloud fetches the data and files through Raspberry Pi. Raspberry Pi controls the devices through relay, and that relay that controls electronic devices supports the user. Here, the three main cases involved are listed below:

- In order to initiate a signal to the server deployed on the cloud, user will be an actor.
- Uploading of files and data to the server deployed on the cloud is taken care by the user.
- Controlling of all the peripheral devices through Raspberry Pi device is done by thee user.

In order to understand the working principle more clearly, below are the two dataflow diagram explained in level; refer to Figs. 4.5 and 4.6.

Level 1

This level has an interface among the user and the server. It shows how the user will initiate the signals through devices and the digital signals will send the file and that file will upload to Amazon's cloud server.

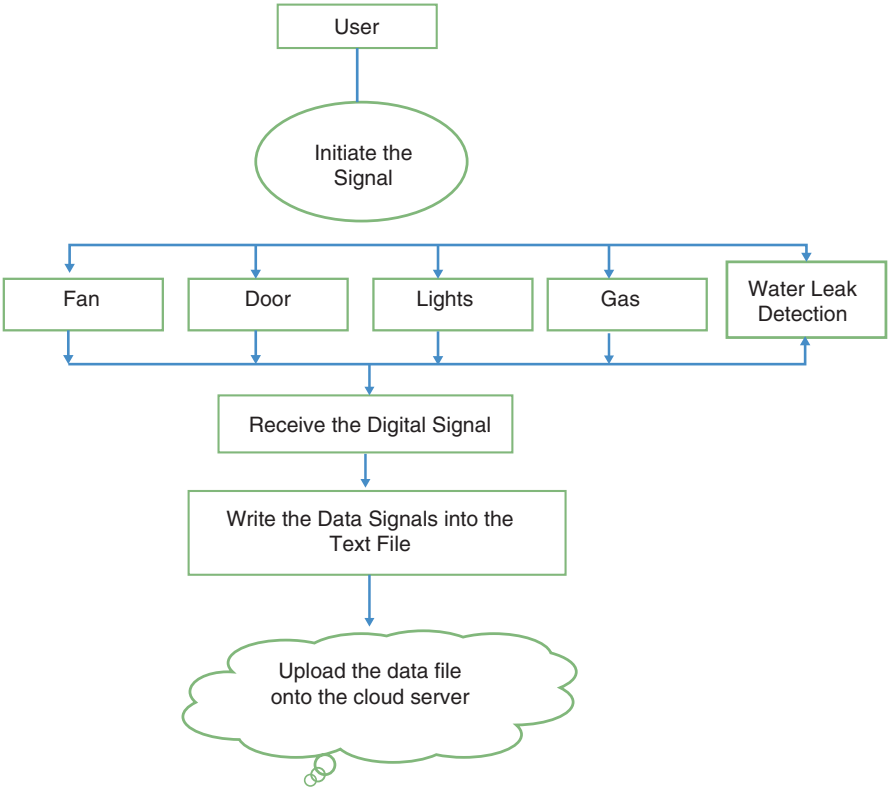


Fig. 4.5 Flow of data—level 1

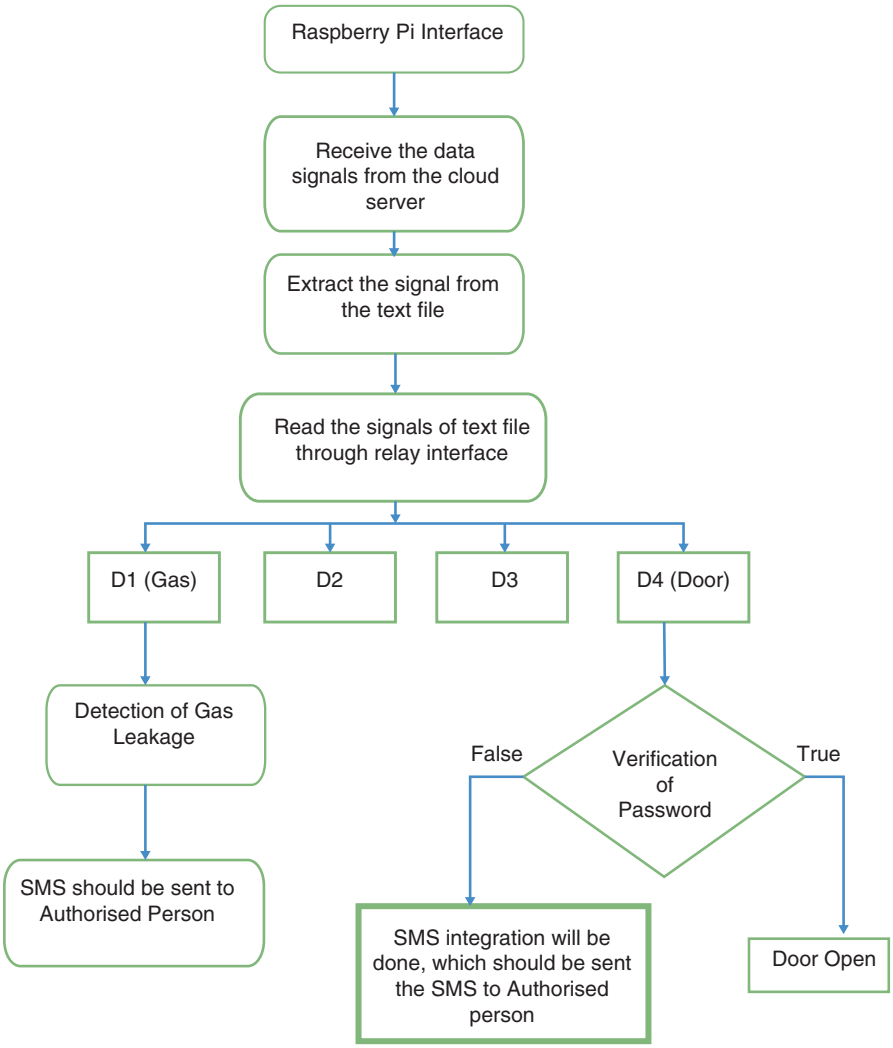


Fig. 4.6 Dataflow diagram—level 2

In the level 2, the interface between the Raspberry Pi and electronic devices is depicted. The Pi retrieves the signals from the cloud server and fetches the data from the cloud. The relay will interface with the Pi and control the signals to devices, and through relay, we can control the external devices.

4.4.3 *Implementation Procedure of Study*

Initially, PuTTY configuration is enabled that helps in connecting the Raspberry Pi server and user with a static IP address. It is displayed in Fig. 4.7a, b showing that PuTTY software configuration is enabled for SSH of X1 forwarding.

Figure 4.8 shows how the Raspberry Pi is connected to the model for execution purposes. It is connected to the various sensors to have a validated and exact result for the sensing format.

Pi prompt enables the user to compile and run the program and will download file from the cloud server and initiate signal to Pi server to control external device according to signal initiated by the user as shown in Fig. 4.9a, b.

Figure 4.10 shows the web application through which we can control external devices using Amazon S3 cloud server.

Transactions are the interactions involving neighboring devices or overlay nodes. To serve many functions of smart home, various varieties of transactions are used. There are five kinds of transactions such as store, access, monitor, genesis, and remove. Nodes use store transactions to store the data. House owner and service provider use the access transaction to access the cloud. To regularly supervise the device, data house owner uses monitor transaction. Genesis is used to insert novel transaction, and the same is eliminated using remove; private blockchain is provided to store all forms of transaction. Each local blockchain has two sections such as header and transaction; further, two kinds of headers are block header and policy header. To retain the irreversible nature of the blockchain, block header will keep the hash of the preceding block, and authorizing the devices is the task of the header. Figure 4.11 shows the outline of smart home. Upper table shows the four attributes of the policy header that indicates the requesters, requests for what type of resource,

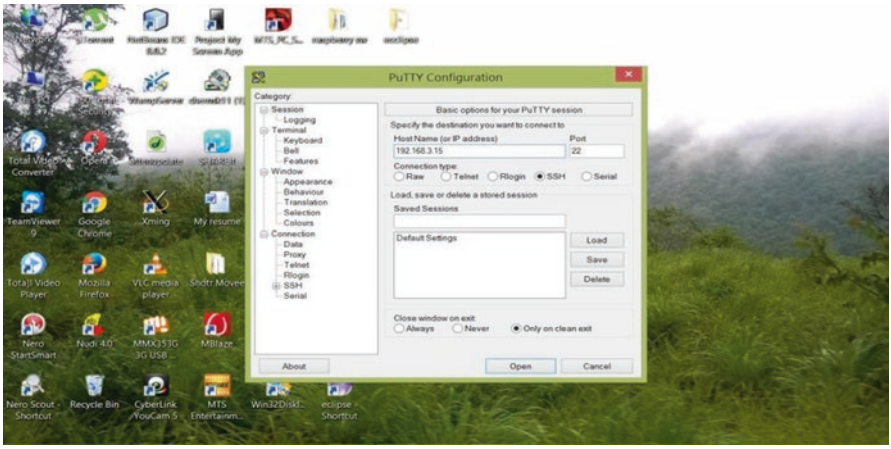


Fig. 4.7 (**a**) PuTTY which enables user to connect Pi server. (**b**) PuTTY configuration enabling the SSH of X1 forwarding

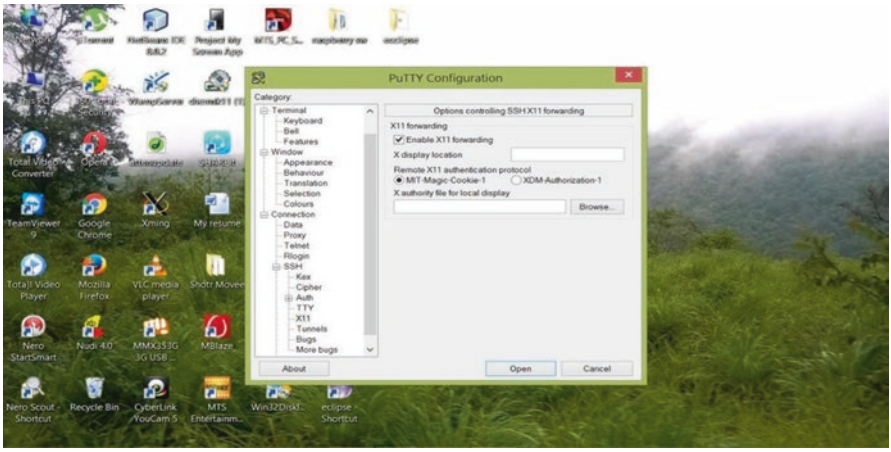


Fig. 4.7 (continued)

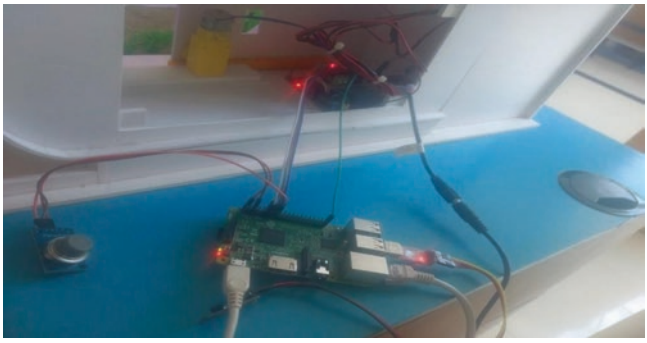


Fig. 4.8 Raspberry Pi connection to the model

device identification, and action whether to give access to the resources or not. In addition to the headers, every block has various transaction attributes like transaction number, transaction types (genesis, access, storage, add, and remove), and unique device authentication

Home miner is a gadget that manipulates arriving and departing transactions to the smart home and vice versa. Miner is situated between the gateway and devices. It also performs tasks like creating genesis transactions, allocating and revising keys, and altering the communication organization.

The miner supervises home storage space to offer extra capability. Local storage is a device which is used to perform home storage which acts as backup gadget. This is associated with the miner and sometimes can be the separate device. This utilizes first-in first-out (FIFO) technique to store the data.

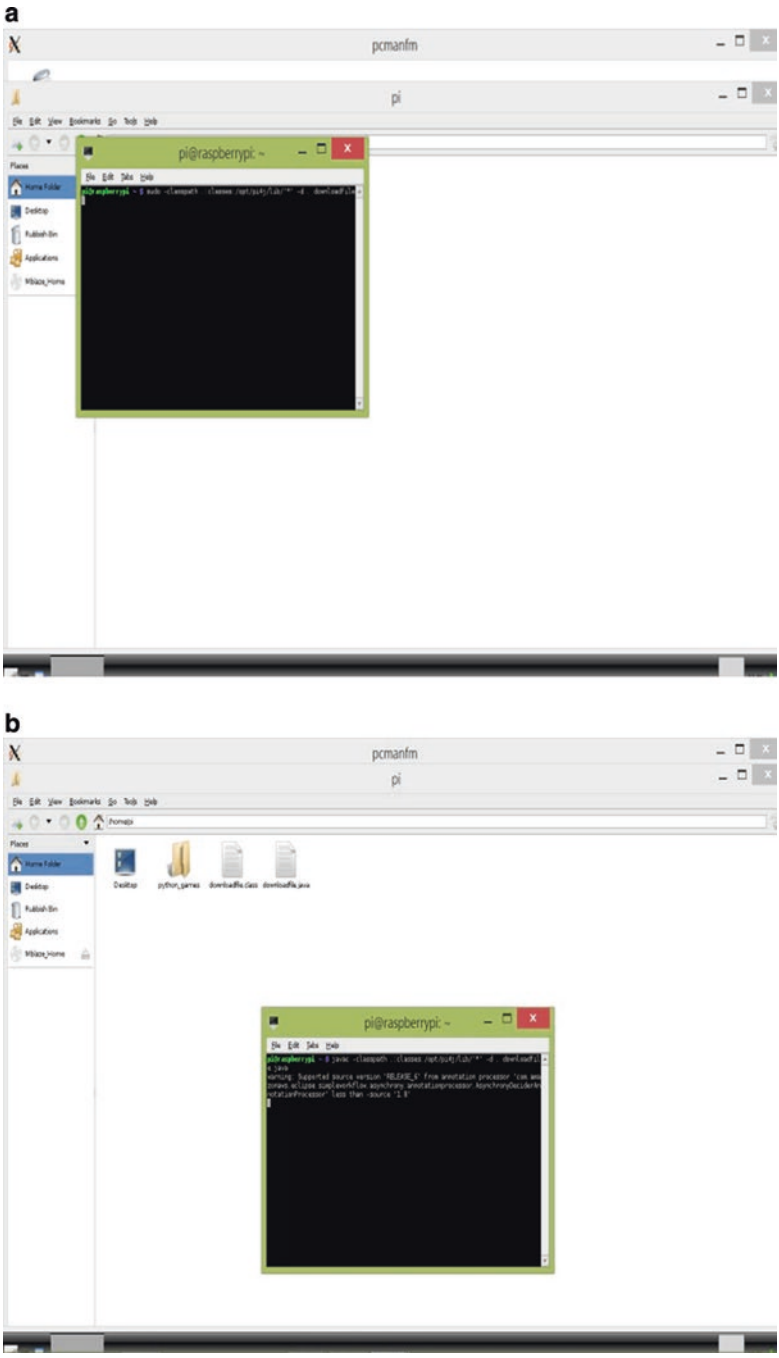


Fig. 4.9 (**a**) Pi prompt 1. (**b**) Pi Prompt 2

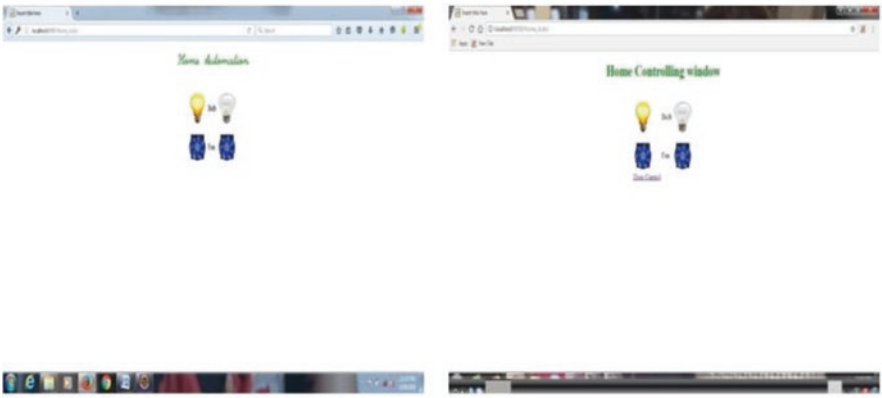


Fig. 4.10 Web application through which the model is controlled

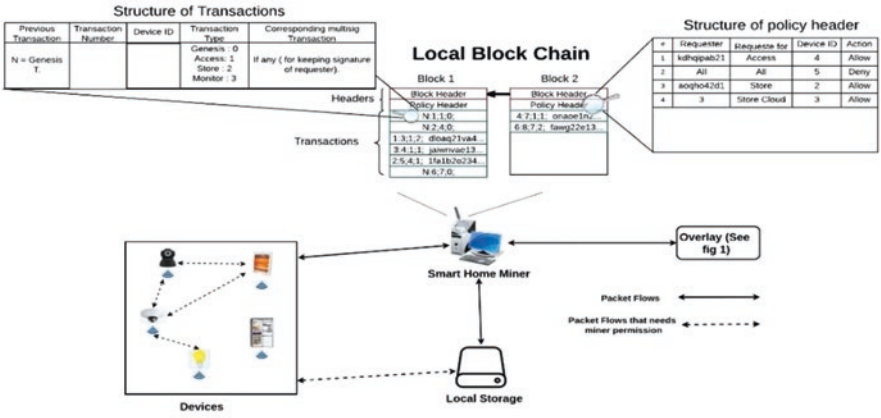


Fig. 4.11 Overview of the smart home

4.5 Evaluation and Results

Evaluation of the working principle discussed above has been mentioned below in the flow diagram shown in Fig. 4.12. Measure has been taken clearly in the execution procedure.

Figure 4.13 shows the result via SMS for identifying one of the applications as a leakage of gas at home to the user mobile, providing alertness about the incident.

Fig. 4.12 Flow diagram

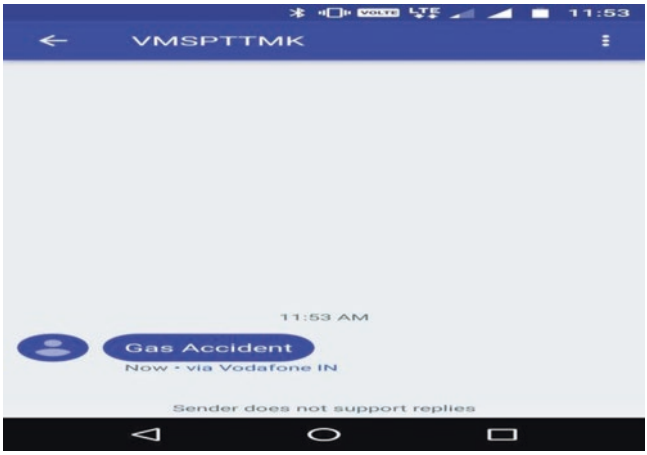


Fig. 4.13 Gas leakage detected alert via SMS

4.6 Conclusion

Home automation systems are required to control the various electronic devices remotely to avoid human errors like not switching off the home appliances that are in no use, and in this case, the solution is to utilize the power effectively and also in a secured manner by means of blockchain. The model describes Raspberry Pi module and presents its potential deployment in smart home environment. In this perspective, Raspberry Pi is an emerging network technology and controlling many devices and is capable to satisfy such requirements. Work involves the incorporation of blockchain to provide authorization and authentication of information obtained from IoT sensors; peripherals have been designed successfully in a system communicating with mobile device like smartphone or a laptop by Raspberry Pi in controlling a door sensor, lights, and other electronic devices with appropriate applications that could benefit the end users.

References

1. Wu, M., Wang, K., Cai, X., Guo, S., Guo, M., & Rong, C. (2019, October). A comprehensive survey of blockchain: From theory to IoT applications and beyond. *IEEE Internet of Things Journal, 6*(5), 8114–8154.
2. Boudguiga, A., et al. (2017). Towards better availability and accountability for iot updates by means of a blockchain. In *Security and Privacy Workshops (EuroS&PW) 2017 IEEE European Symposium*.
3. Dey, S., Roy, A., & Das, S. Home automation using internet of thing. In *IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference* (p. 2016). New York: UEMCON.

4. Yashiro, T., Kobayashi, S., Koshizuka, N., & Sakamura, K. An internet of things (IoT) architecture for embedded appliances. In *International conference* (p. 2011). Yichang: IEEE.
5. Malagund, K., Mahalank, S., & Banakar, R. (2015). Evolution of loT in smart vehicles: An overview. In *IEEE Computer Society*.
6. Suyama, T., Kishino, Y., & Naya, F. (2014). Abstracting IoT devices using virtual machine for wireless sensor nodes. In *Internet of things (WF-IoT)* (p. 2014). Seoul: IEEE World Forum.
7. Kodali, R. K., Jain, V., Bose, S., & Boppana, L. IoT based smart security and home automation system. In *International Conference on Computing, Communication and Automation* (p. 2016). Noida: ICCCA.
8. Pereira, P. P., Eliasson, J., Kyusakov, R., Delsing, J., Raayatinezhad, A., & Johansson, M. (2013). Enabling cloud-connectivity for Mobile internet of things applications. In *IEEE Seventh International Symposium on ServiceOriented System Engineering*.
9. Tseng, S.-P., Li, B.-R., Pan, J.-L., & Lin, C.-J. (2014). An application of internet of things with motion sensing on smart house. In *IOCT*.
10. Jing, L., Yamagishi, K., Wang, J., Zhou, Y., Huang, T., & Cheng, Z. (2011). A unified method for multiple home appliances control through static finger gestures. In *IEEE/IPSJ International Symposium on Applications and the Internet*.
11. Coelho, C., Coelho, D., & Wolf, M. An IoT smart home architecture for long-term care of people with special needs. In *IEEE Conference*.
12. Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016, October). Where is current research on Blockchain technology?—A systematic review. *PLoS One, 11*(10).
13. Leible, S., Schlager, S., Schubotz, M., & Gipp, B. (2019). A review on Blockchain technology and Blockchain projects fostering open science. *Frontiers in Blockchain, 2*. ISSN: 2624-7852, 16.
14. Sultan, A., Mushtaq, M. A., & Abubakar, M. (2019, March). IOT security issues via Blockchain: A review paper. *ICBCT 2019: Proceedings of the 2019 International Conference on Blockchain Technology*.
15. ManojKumar, N., & Mallick, P. K. (2018). Blockchain technology for security issues and challenges in IoT. In *Procedia computer science*.
16. Banerjee, M., Lee, J., & Choo, K.-K. R. (2018). A blockchain future for internet of things security: A position paper. *Digital Communications and Networks*.
17. Ali, M. S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., & Mubashir Husain, R. (2019). Applications of Blockchains in the internet of things: A comprehensive survey. In *IEEE Communications Surveys & Tutorials*.
18. Maksimović, M., Vujović, V., Davidović, N., Milošević, V., & Perišić, B. Raspberry pi as internet of things hardware: Performances and constraints. In *IcETRAN* (p. 2014). Vrnjacka Banja: Serbia.
19. Fernando, E., Meyliana, & Surjandy. (2019). Blockchain technology implementation in raspberry pi for private network. In *International Conference on Sustainable Information Engineering and Technology (SIET)*.
20. Patchava, V., Kandala, H. B., & Ravi Babu, P. A smart home automation technique with raspberry pi using IoT. In *International Conference on Smart Sensors and Systems* (p. 2015). Bangalore: IC-SSS.
21. Venkatesh, K., Hemaswathi, S., Balakrishnan, R., & Rajkumar, P. (2018). IoT based home automation using raspberry pi. *Journal of Advanced Research in Dynamical and Control Systems*, 1721–1728.
22. Jeyapadmini, J., & Kashwan, K. R. (2015). Effective power utilization and conservation in smart homes using IoT. In *International Conference on Computation of Power, Information and Communication*
23. Gupta, P., & Chhabra, J. (2016). IoT based smart home design using power and security management system. In *1st International Conference on Innovation and Challenges in Cyber Security (ICICCS)*.

24. Mandula, K., et al. (2015). Mobile based home automation using Internet of Things (IoT). In *International Conference on Control Instrumentation, Communication and Computational Technologies (ICCICCT)*.
25. Patchava, V., Kandala, H. B., & Ravi Babu, P. (2015). A smart home automation technique with raspberry pi using iot. In *International Conference on Smart Sensors and Systems (IC-SSS)*.
26. Hoque, M. A., & Davidson, C. (2019). Design and implementation of an IoT-based smart home security system. *International Journal of Networked and Distributed Computing*, 85–92.
27. Pirbhulal, S., Zhang, H., Alahi, M. E. E., Ghayvat, H., Mukhopadhyay, S. C., Zhang, Y.-T., & Wu, W. (2017). A novel secure IoT-based smart home automation system using a wireless sensor network. *Sensors, 17*(3), 606. PMC5298642.
28. Jacobsson, A., Boldt, M., & Carlsson, B. (2016). *A risk analysis of a smart home automation system. Future generation computer systems* (pp. 719–733). ACM.
29. Singh, H., Pallagani, V., Khandelwal, V., & Venkanna, U. (2018). IoT based smart home automation system using sensor node. In *4th International Conference on Recent Advances in Information Technology (RAIT)*.
30. Lazaroiu, C., & Roscia, M. (2017). Smart district through iot and blockchain. In *EEE 6th International Conference on Renewable Energy Research and Applications (ICRERA)*.
31. Phan, L.-A., & Kim, T. (2020, May). Breaking down the compatibility problem in smart homes: A dynamically updatable gateway platform, mdpi. *Sensors, 20*(10), 2783.
32. Alam, T., Salem, A. A., Alsharif, A. O., & Alhejaili, A. M. (2020). Smart home automation towards the development of smart cities. *APTIKOM Journal on Computer Science and Information Technologies, 5*, 152–159.
33. Dorri, A., Kanhere, S. S., & Jurdak, R. (2016). Blockchain in internet of things: challenges and solutions. arXiv preprint arXiv:1608.05187.

Chapter 5
Blockchain-Based Fog Computing Model (BFCM) for IoT Smart Cities

R. Venkadeshan and M. Jegatha

5.1 Introduction

With the recent improvement in the urban lifestyle, the smart cities originated for the improvement of the quality of living and to optimize the utilization of cities' resources [1]. There are a lot of improvements that have been carried out on infrastructure and different services which elevated the eminence of life. All these could be possible with the support of the Internet, telecommunication, and advancement in the information technology field [2]. The expectation from the awareness of smart cities includes smart transportation, efficient society services, and better infrastructure results in on-demand accessible and effective interactive services. With the support of the Internet of Things (IoT), the vision of the smart city becomes reality. As a result, many IoT applications have been built up for the smart cities services to interact with the people anytime and anywhere.

The smart cities are deployed with physical objects interconnected with the IoT system. This system emphasizes four pillars in IoT concepts such as things, data, objects, and processes. Hence, the integration of IoT concepts with smart city domain will facilitate the promising services in the near future. Big data analytics is an emerging technique to analyze the massive data generated by IoT-connected devices which could help to sort out the issues of data storage and processing. Fog computing, also referred to as edge computing or fogging, extends the cloud computing services to the enterprise network's edge. It allows the edge devices to transfer a significant amount of data to compute, store, and communicate for the local decision and forward over the Internet.

This chapter discusses a conceptual framework with the dimensions (1) technology, (2) human, and (3) organization and reconnoitering the challenges of digital

R. Venkadeshan (✉) · M. Jegatha
University of Technology and Applied Sciences – Shinas, Shinas, Sultanate of Oman
e-mail: venkadengg@gmai.com

H. L. Gururaj et al. (eds.), *Convergence of Internet of Things and Blockchain Technologies*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-76216-2_5

technologies with the support of blockchain-based fog computing model (BFCM) for smart cities [3]. This model reduces energy consumption and latency in data communication and improves security features. The convergence of blockchain and Internet of Things (IoT) technologies in smart cities ensures the security and privacy of data captured and stored in a cloud-based infrastructure. In the IoT application execution of fog computing, the node called fog node (FN) acts as a basic fundamental entity and an intermediate layer between the cloud and edge devices [4]. Emerging IoT applications require the support of mobility, low latency, geo-distribution, and location awareness. The BFCM architecture targeted to improve the efficiencies of the above parameters by handling most of the data at the network edges rather than transferring to cloud always. Another important service to address is the security of data and devices which could be enhanced by using the blockchain technology. The blockchain technology [5, 6] is organized as a series of blocks and chains of records stored in a shared database which could be secured by cryptographic hash functions. Each block is a group of transactions that had occurred for a while.

5.2 IoT Technologies in Smart Cities

In recent decades, there are several researchers that worked on IoT-related smart cities. Smart cities are one of the rapidly progressing technological revolution and escalation of Internet of Things development in every possible aspect of urban lifestyle [7]. A smart city is designed for providing solutions for the environment, traffic, and other energy management problems by integrating various technologies such as Internet of Things, big data, and blockchain. Simply, the smart city is a network of environment with objects, people, and services sharing the information with one another through the communication technologies like 3G, 4G, and Wi-Fi. Due to the blended heterogeneous devices with different technologies, the deployment of smart cities becomes very much complicated [8]. The large-scale network exponentially increases the difficulties of object's management and tracking which results in an intruder or attacker easily performing security breaches. By taking all these in mind, building a basic infrastructure for a smart city in urban areas needs support from various sensors and technologies [9]. The Internet of Things (IoT) is one among them, considered as a key builder in the development of smart city. The fundamental components and concepts of smart city are given in Table 5.1.

An emerging smart city objective is to make use of the resources like energy and electricity in an effectual way to provide a suitable and comprehensive infrastructure for the human society in day-to-day life. Therefore, the impact of IoT is magnified in various services of smart cities [10]. The smart city is a network of six components: smart environment, smart people, smart governance, smart mobility, smart economy, and smart living (Fig. 5.1). Some of the applications and services where IoT technologies and smart city projects de facto overlap are listed below [11]:

Table 5.1 Fundamental components and concepts of smart city [36]

Components	Descriptions
Policy and purpose	Environmental sustainability: environment pollution, energy efficiency, and resources Economic requirements: education, public security, medical care, social stability, and healthcare Happiness of citizens: asset, new job formation, and system modernization
Key industry	Smart buildings, smart transportation, smart government, smart facilities, and so on
City infrastructure	Sensor networks, operation systems, sensors, and smart devices Telecommunication platforms, data analysis, control systems, and interactive web services

Fig. 5.1 Smart city components [12]

Public services such as public transportation management, citizen services, tourism services and healthcare sector administration, and information services

Sustainability which includes smart wastage management and recycling system, smart metering, smart energy, smart water, and environmental monitoring

Infrastructure services that deal with smart building's structural health monitoring, smart lighting, smart irrigation, smart schools, etc.

Transportation services that handle smart traffic management, coordinating the connected vehicles on the road, smart road system, pollution and noise control management, and so on

Safety services which are video surveillance, disaster recovery system, environmental screening, and telemedicine system

IoT technologies in Table 5.2 provide IT solutions for automatic electricity services, telecommunication services and construction, vehicle telematics, smart healthcare, and other business services [12].

Table 5.2 IoT technologies for smart cities

Technologies	Descriptions
User interface technology	Communication between sensors, objects, machines, and humans
Context awareness technology	Provide services based on the understandability of current situation data collected from various sensors, objects, and machines
Wired and wireless connection gateway	It's a home gateway technology used to provide communication between the different network platforms like Ethernet, 3G, 4G, LTE, Wi-Fi, and Zigbee
System-on-Chip (SoC) technology	It's a microcontroller for controlling and integrating with computers objects for sensing the environment. Mostly used in the mobile computing and edge computing markets
Optimized sensor design technology	It's a sensor technology used for collecting environmental values on object transformation and personal information.
Sensor fusion and converging technology	Used for converging more than one sensor's functionality in an object
Analytical technology	Sensors generating massive amount of data which are collected on cloud server for big data analytics

5.3 Fog Computing for Smart Cities

The Internet of Things (IoT) connects billions of everyday automation objects/things to collect and exchange massive amount of data over the Internet. All those collected data are pushed into the cloud for further analysis and knowledge discovery for future purpose [10]. Moreover, the amount of gathered data becomes overwhelming to store and manage, requiring high-processing computing devices to forward to cloud, and will have limitations such as resources wastage (e.g., storage, bandwidth), unreliable latency, and data security. The result of fog computing or edge computing offers different solutions to these limitations. The main goal of Fog computing technology is to improve the effectiveness and minimize the amount of information sent over the Internet to the cloud for analysis, processing, and storage by performing data analytics at the network edges [13]. Edge devices are easy to control, manage, and self-govern at the local network. Therefore, the network traffic and data processing have been reduced considerably by moving the services to the edge of the local network. In smart cities development, the fog computing plays a potential role in processing a variety of volume of data swiftly and most securely.

Figure 5.2 illustrates the various elements of smart city that applies fog computing technology to support low latency, location awareness, and mobility to the end users.

Smart cities achieve the below listed benefits through the incorporation of fog computing technology [14]:

Reduced the amount of data being sent to cloud: Fog computing uses intelligent sensing and filtering technique to allow only the useful and most needed information to the cloud; the remaining will be available at the local fog devices in the network premises.

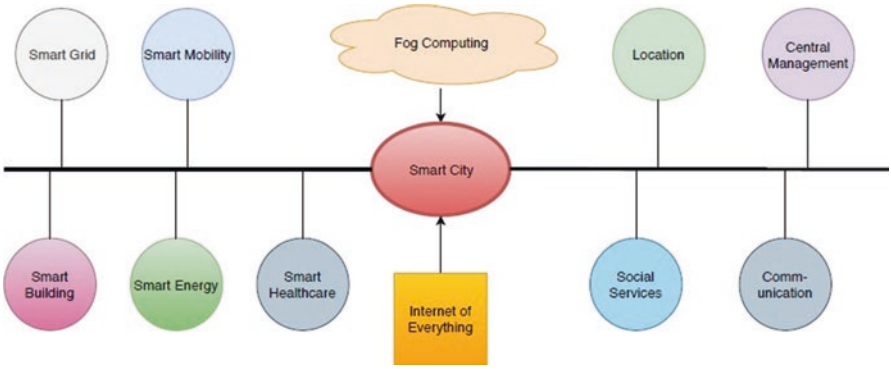


Fig. 5.2 Fog computing for sustainable smart cities [3]

Low latency: Fog devices are capable of data processing and decision-making and sending back results without depending on the remote cloud services. Especially, these characteristics save a lot of time considerably in IoT automated environment.

Reduced bandwidth: Forwarding and processing of sensed data require huge amount of bandwidth in cloud computing. But, in the case of fog computing, this issue does not exist because most of the data are stored and processed by the fog nodes inside the local network which significantly reduces the consumption of total network bandwidth.

Security enhancement: Fog computing restricts the outreach of most sensible and confidential data exposed to the vulnerable public network (Internet) which results safeguard the data from cyberattacks and hacking.

Henceforth, fog computing provides relief to the smart city components by achieving reliable and faster data communication. In succession, the urban areas called as fog (edge) computing smart city proliferate the communal sectors such as healthcare, manufacturing, education, transportation, energy, and utilities [15].

5.4 Blockchain-Based Fog Computing Model (BFCM)

The blockchain-based fog computing model (BFCM) for the smart cities is introduced to connect the Internet of Things (IoT) and fog nodes. This model is an on-demand service that provides high performance with low latency and secure device management and data privacy in a distributed form of infrastructure [16]. It will result in the improvement of lifestyle quality of the citizens and meeting the expectations of day-to-day activities.

5.4.1 Blockchain: A Study

A blockchain technology is a decentralized distributed database with special data structure which forms all transactions into blocks with secure distinctive hash code and transmits them to every node [17]. It works with different elements like network, authentication, and transactions to store the sensitive data. It also enables the network's authorized members to validate the transaction data at any time and to quickly store it as a digital information which is easy to manage against any forgery and attacks. A public key cryptographic technique is used to sign all the transaction on a distributed ledger linked blocks of records known as blockchain [18]. Once the data is transferred, it cannot be changed, and it provides better security to the information. For smart cities management, various frameworks support Internet of Things (IoT) technology but face multiple issues like security, resource management, heterogeneous devices and data, multiple application assistance, and platform independence. The BFCM-based infrastructure secures sensitive information with authentication, edge computing, encryption, and blockchain.

5.4.2 Structure of Blockchain

Generally, a blockchain is nothing but consecutive list of records, called blocks, that contains the detailed transactions linked using cryptography in a network. In Fig. 5.3, each record, or block, consists of a header and a body, where the header comprises the previous record or block's identity and the body portion encompasses stored data/transactions that are being transferred [6]. The chain of blocks is connected as linked list to transfer over the network.

Intuitively, blockchain technology offers desirable features such as decentralization, immutability, distributed ledger, and fault tolerance. Intrinsically, BFCM

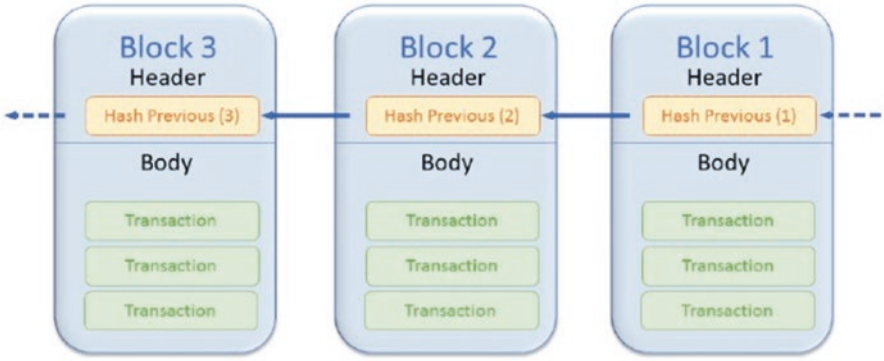


Fig. 5.3 Structure of blockchain [6]

promotes transparency and trust on smart city elements and helps to provide on-demand services to the citizens [19].

Decentralization—A blockchain technology is a decentralized database network which does not have any governing authority or entity at the framework to manage and control the transactions of data among the smart city components. So, the data storage and analytics integrate the security and trust on decision-making processes.

Immutability—It is one of the exciting key features of blockchain technology, where the network is permanent, uncorrupted, and unaltered. The chain of immutable blocks contains the secured data with digital ledger ensuring the validity and corruption-proof. IoT-enabled smart city infrastructure struggles with handling massive data being generated, safety and security of carrying sensitive information such as financial transaction, health-related data, traffic information, and so on. With the support of immutability in smart cities, the communication becomes tamper-free where an attacker would have to compromise all the devices within the network to alter any records in the blockchain.

Distributed Ledger—Generally, the term DLT stands for distributed ledger technology, used to keep multiple copies of single ledger in a distributed manner. So, all the ledger holders should ensure the data integrity and the data cannot be altered in between. The DLT provides data sharing and smart services in building a smart city infrastructure that are supported by blockchain and IoT.

Fault Tolerance—The distributed nature of blockchain technology allows the nodes to tolerate the malicious behavior for certain threshold. Blockchain peers will automatically reject the blocks if any tampering occurred. The fault tolerance servers are imperative in providing continuous services and operations to maximize the value of smart industries. Since the data are shared, replicated, and synchronized across the participating devices, any failure in one or more devices in a smart network does not affect the performance of entire system.

5.4.3 Blockchain and IoT Technology

Basically, the Internet of Things (IoT)-technology-supported network works as a centralized architecture for communication where the data is collected, processed, and analyzed in various forms from different millions of devices. Yet, this technology suffers with numerous issues like security and privacy of massive data, scalability of devices, and scarcities in resource management at IoT edge network. Fortunately, the blockchain technology with distributed nature offers countermeasures for all the above listed issues and secures the data from tampering embedded into real-time IoT applications [20]. Nevertheless, using blockchain technology in the smart city's infrastructure requires huge amount of energy to generate blocks of live records and to verify its integrity with the use of energy-constrained IoT devices. The smart city infrastructure enhances these technologies to support and provide sustainable solutions for the new era. The BFCM plays a prominent role in the rapid

moving environment of smart cities [21]. Blockchain technology could be incorporated in three ways:

- *Public* **blockchain:** It is also named as "Permissionless Blockchain"; a decentralized environment allows everyone to keep a replica of blocks and take part in validating new blocks.
- **Private blockchain:** It is referred as "Permissioned" or "Private" or "Closed" blockchain; the access to the blocks of records are restricted to some specific participants. It supports three types of permissions to setup a blockchain:

  Read—allows to access and see the transactions of ledger records
  Write—allows to access, modify, and see the transactions of ledger records
  Commit—allows the ledger records to update the state after modification

- **Consortium blockchain:** It is like private blockchain where the permission is required to access the blocks. The main role of consortium blockchain is to synchronize the distributed databases and to keep track of data exchanged between the participants in the network. It provides faster latency and more auditability for the chains of blocks in the networks.

5.4.4 Challenges in Blockchain-Based IoT

On the other side, there are some challenges in the integration of blockchain with IoT technology. The IoT technology visualizes the smart city as collection of connected smart devices or sensors or things that interacts and shares data with each other using smart applications. IoT-based solutions are being incorporated in many of the smart city components such as smart industries, smart grid, smart transportation, smart healthcare, and smart environment to optimize the performance and digitizing of the communication [22]. The smart applications that generate huge data require uninterrupted connectivity and continuous power that lead to excessive number of challenges. Integrating the blockchain with IoT technology will enrich the infrastructure by providing trustable sharing services; reliable information can be traceable at any point. The challenges [6] in an integration of both technologies are summarized in Table 5.3 [23].

5.5 BFCM-Based Smart City Architecture

The objective of BFCM-based model is to incorporate the IoT-based smart cities with blockchain and fog computing technologies to solve traffic-, energy-, and environment-related problems and to enhance and better the lifestyle of the citizens. The smart city network is composed of different components like smart healthcare, smart transportation, smart banking, and smart industries using different

Table 5.3 Integration challenges of blockchain and IoT [6]

Category	Challenges
Integration	Layer of integration of two different systems into single coherent model that supports energy constraints, compatibility, and heterogeneity
Device management and deployment	Building the infrastructure to provide failure recovery, remote monitoring and auditability, sensor's extensibility, and flexibility
Storage and scalability	Devices are being scalable every day in smart cities and generating gigabytes of data in a real-time environment which creates a barrier to blockchain technology to provide security
Security	Different formats of data from different devices in smart city component are very much hard to handle. There is no single security model to protect against all the cyberattacks and breeches
Anonymity	Smart city applications work mostly with sensitive and confidential data like healthcare and banking. The problems of providing data privacy is transparent, and the public blockchains of cryptographic security for software devices should be safeguarded

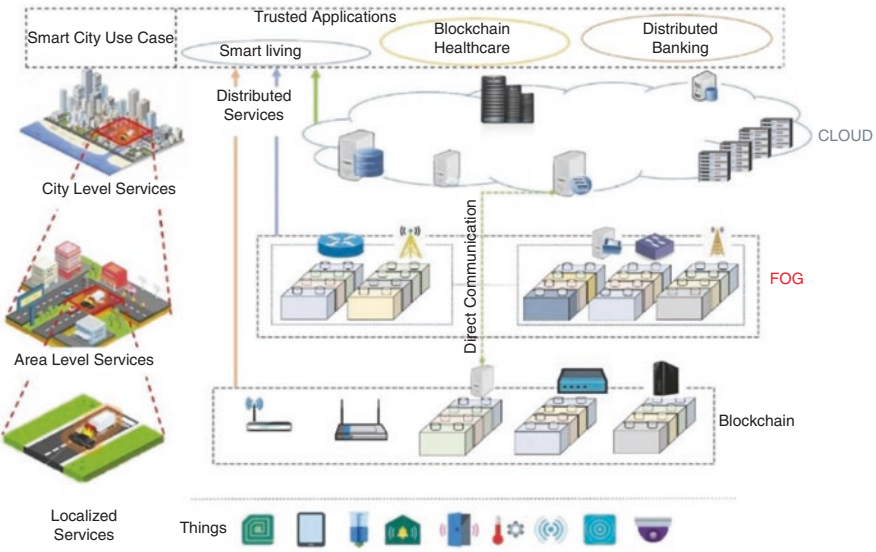


Fig. 5.4 BFCM-based smart city architecture [37]

communication model of IoT technology [24]. The smart city use cases are broadly categories into three levels of services as depicted in the Fig. 5.4, which includes (1) localized services, (2) area-level services, and (3) city-level services, to understand how the BFCM model is acting as digital technology transformation in data transmission and its communication [25]. The lower-level localized services are populated with the highly reliable, low-cost IoT smart objects and sensors like RFIDs, IR sensors, GPS, and cameras deployed across the smart cities horizontals such as generation, distribution, transmission, and consumption. The security to the data

generated by sensor devices is achieved through blockchain technology where the information is stored as blocks of records called ledger. The next level is the integration of computing services and blockchain technology to provide distributed area-level services for handling substantial amount of data communication and analysis through fog computing framework [26]. As shown in the figure, not all data are to be processed and handled at the network edge; some of the data as per the user's requirements can be transferred directly called as "Direct Communication" to the cloud storage and analysis without fog computing in the edge of network.

The blockchain provides guarantee to the data integrity and transactions between the local network and the cloud. Blockchain strengthens the security and privacy of the internal information by using SHA (Secure Hash Algorithms) [27]. Smart cities are growing exponentially with the emergence of Internet of Things (IoT) technology. Every edge device should cover up the sensors to perform local traces and instant analysis. The outcomes of fog layer may either have transferred fully to the smart city's IoT application processing at cloud or may be off-loaded in the network edges. The distributed environment at city-level services experienced massive raise of data storage and data processing. Cloud computing is a solution to handle huge amount of data storage and processing in on-demand and anytime and anywhere basis. It supports centralized monitoring and control of information with high performance and different behavioral analysis. The topmost level is the trusted event-driven applications that impeccably integrate the IoT technologies, spatiotemporal analytics, and complex-event processing for the different smart city's components present to the end users.

5.5.1 Blockchain IoT Applications and Platforms

Emerging technologies such as blockchain fog and cloud computing have been improvising the IoT applications particularly in security domain, e.g., data integrity and data reliability. This has resulted in an enlightenment of increasing electronic devices or smart devices deployment in many areas and stepping into the digital world. The smart devices can be able to sense, actuate, and communicate over the Internet without any human interventions [28]. The end users connected with the IoT applications, which are more specific in features and characteristics, generate large amount of data and expected high connectivity and electric power for long periods. The smart cities are the collection of different components such as smart healthcare, smart home, smart transportation, smart education, and smart grid [2]. Each component is embedded with IoT sensors that can communicate with each other using BFCM model. The presented figure is a multitier architecture that illustrates the detailed layout of smart city infrastructure with the technologies, Internet of Things (IoT), fog computing, blockchain, telecommunication, and cloud services (Table 5.4).

Table 5.4 Blockchain- and fog-based architecture network characteristics [3]

Type	Architecture	QoS	Technology	Latency	Bandwidth	Mobility	Storage	Delay
Primary	Centralized	High	Wi-Fi/4G/5G	Low	Medium	Yes	Yes	Very low
Inter- primary	Centralized	High	Zigbee/Bluetooth/Wi-Fi	Very low	High	Yes	No	Very low
Secondary	Distributed	Very	5G/4G	Low	Low	No	Yes	Low

5.5.2 Challenges and Security Features for Device Management in BFCM

A smart city is a network that consists of complicated and heterogeneous urban devices connected with the Internet that have the capacity to send and receive the data using Internet of Things (IoT) technology and can exponentially increase the security problems where the attackers can perform several cyberattacks [30, 31]. Some of the security measures for device administration security in a smart city are as follows.

Confidentiality. A wide range of devices across the smart cities will sense, collect, store, and process data that could contain more sensitive information [29]. Confidentiality means providing security and privacy over those data and enabling only authenticated and authorized entities to access that information. One of the general methods to provide confidentiality is relying on cryptography technique. Since the BFCM model uses blockchain technology, that integrates the cryptography with private and public keys in the list of records to strengthen the sensitive information.

Integrity. The data exchanged between the smart devices are reliable, accurate, consistent, and integrity to ensure the transferred data are delivered without any modification. The blockchain technology is designed to prevent the data modification using hash functions: the data does not get changed once it is added into the chain.

Availability. Sensors act as a backbone of smart cities, and continuous collection of massive data from different geographic areas requires high availability to the authorized entities. The BFCM model is deployed as distributed decentralized infrastructure and provides data availability with no single point of failure.

Accounting. Blockchain technology is a distributed P2P database system; the data is stored and managed as a record with timestamp called block. A block is a data structure that accounts all the records of transactions between the smart devices. So, the blockchain provides efficient accountability for data management.

Latency. In BFCM, the data are gathered and processed at the edge of the network in geographic proximity. Due to that, it enhances the performance of the network by reducing the latency and provides higher bandwidth in transaction.

Adaptability. The smart city operates on open interconnected heterogeneous smart devices and technologies that result in interoperability issues. But the BFCM enables decentralized architecture to manage cross-disciplinary IoT systems.

5.5.3 Privacy-Conserving Blockchain and Fog Computing

It is to all appearances that the main challenge in IoT is to overcome the downsides associated with privacy, security, and vulnerability aspects. Moreover, the blockchain technology requires enormous amount of energy to process and verify each

block of record that are difficult to handle with resource-constrained IoT devices and real-time data applications [32]. Due to the public ledger system, blockchain discloses the privacy of the stakeholder's data though it is secure from data alteration. Fog computing technology reduces the complexity of data privacy at cloud computing by populating the real-time applications data at the network edges. However, due to handling of massive data, distributed environment, and shortage of enough resources made, this model endlessly suffers from abundant security and privacy issues [33]. Remarkably, blockchain technique provides strong countermeasures to these security issues and protects data against any tampering even in distributed nature of IoT. It is very difficult to provide message delivery in end-to-end connectivity without the cooperation of network devices. But, some selfish devices in the network become reluctant in data transmission due to minimum resources utilization such as energy consumption [34]. The BFCM provides remote data integrity verification which allows the remote users to validate the reliability of the transmission data. The authors [31] proposed homomorphic encryption for data aggregation scheme in fog-assisted IoT devices. There are several articles that addressed the various techniques used to preserve the privacy of information through blockchain and fog computing. Some of them are listed below:

Identity privacy—A user's identity in IoT environment should be preserved and protected from impersonate attacks. The authors [30] present various pseudonym techniques to preserve identity privacy.

Data privacy—There are algorithms run between the fog and cloud services to preserve the information transferred. But the reality is this algorithm consumes massive amount of resources at the network edge devices. At the local edge, same encryption method can be deployed without decryption to allow privacy preservative collection [31].

Usage privacy—Additional important concern in blockchain-based fog computing model is user's resource usage privacy pattern. Let us consider that the smart energy meter in smart industry reads and stores a massive amount of data continuously that are user's private data, energy consumption, user unavailability, and other online and offline appliances status at home, which are threat to user's privacy [34].

Location privacy—However, the fog clients and remote monitoring nodes are in different location; there are rare possibilities that the path route may be revealed to fog nodes. One method to hide the fog node's location is to obscure the identity of fog client [35].

5.6 Conclusions

With the support of emerging technologies like Internet of Things (IoT), fog computing, blockchain, and cloud computing, the world is moving toward the digital electronic era of communication. The smart city projects uplift the use of all these

technologies in a common citizen's day-to-day lifestyle to share information and data communication among the smart devices between cities. In smart cities, there are abundant Internet of Things (IoT)-related applications along with smart sensors, actuators, and controllers that provide energy-aware, scalable, and low-latency network to the society. We started with the impact of Internet of Things (IoT) technology in smart city's infrastructure which generate huge amount of data that should be handled by fog computing nodes at the network edges to provide state-of-the-art security and privacy to meet the limitations. In addition, next, we discussed the role of blockchain technology as an emerging solution to the security issues in fog-enabled IoT environment. At the end, we addressed some of the challenges in integration of blockchain-based fog computing model (BFCM) in the IoT platform. To conclude, BFCM provides many advantages in smart city infrastructure and networks in terms of data computation and information storage with minimal energy consumption.

References

1. Albino, V., Berardi, U., et al. (2015). Smart cities: Definitions, dimensions, performance, and initiatives. *Journal of Urban Technology*, 3–21. https://doi.org/10.1080/10630732.2014.942092.
2. Nguyen, D. C., & Pathirana, P. N. (2020). Blockchain for 5G and beyond networks: A state of the art survey. *Journal of Network and Computer Applications*. https://doi.org/10.1016/j.jnca.2020.102693.
3. Singh, P., Nayyar, A., et al. (2020). Blockchain and fog based architecture for internet of everything in smart cities. *Future Internet*. https://doi.org/10.3390/fi12040061.
4. Hussain, M., & Beg, M. M. S. (2019). Fog computing for internet of things (IoT)-aided smart grid architectures. *Big Data and Cognitive Computing, 2019*(3), 8. https://doi.org/10.3390/bdcc3010008.
5. Shen, C., & Pena-Mora, F. (2018). Blockchain for cities—A systematic literature review. *IEEE Access.* https://doi.org/10.1109/ACCESS.2018.2880744.
6. Aloqaily, M., & Otoum, S. (2020). Blockchain for managing heterogeneous internet of things: A perspective architecture. *IEEE Network*. https://doi.org/10.1109/MNET.001.1900103.
7. Sanchez, L., Muñoz, L., et al. (2014). IoT experimentation over a smart city testbed. *Computer Networks*, 217–238. https://doi.org/10.1016/j.bjp.2013.12.020.
8. Anton, R. (2018). Intelligent communication and patterning in smart cities. *IntechOpen*. https://doi.org/10.5772/intechopen.79629.
9. Biswas, K., & Muthukkumarasamy, V. (2016). Securing smart cities using blockchain technology. In *Conference: 14th IEEE International Conference on Smart City*. https://doi.org/10.1109/HPCC-SmartCity-DSS.2016.0198.
10. Karim, S., & Ahamed, F. A. S. (2019). Smart city architecture and applications based on IoT: A theoretical overview. *International Journal of Scientific and Engineering Research, 10*(1), 1815–1820.
11. Alvarez, M. G., Morales, J., et al. (2019). Integration and exploitation of sensor data in smart cities through event-driven applications. *Sensors*. https://doi.org/10.3390/s19061372.
12. Samih, H. (2019). Smart cities and internet of things. *Journal of Information Technology Case and Application Research*. https://doi.org/10.1080/15228053.2019.1587572.
13. Perera, C., Qin, Y., et al. (2017). Fog computing for sustainable smart cities: A survey. *ACM Computing Surveys*. https://doi.org/10.1145/3057266.

14. Neagu, I. M. (2018). Sustainable smart cities: A fog computing framework for a smart urban transport network. *Studia Universitatis Vasile Goldis Arad – Economics Series*. https://doi.org/10.2478/sues-2018-0021.
15. Yu, W., et al. (2018). A survey on the edge computing for the internet of things. *IEEE Access*, 6900–6919. https://doi.org/10.1109/ACCESS.2017.2778504.
16. Miraz, M. H. (2020). Blockchain of things (BCoT): The fusion of Blockchain and IoT technologies. In S. Kim & G. Deka (Eds.), *Advanced applications of Blockchain technology. Studies in big data* (Vol. 60). Singapore: Springer. https://doi.org/10.1007/978-981-13-8775-3_7.
17. Li, X., Jiang, P., et al. (2018). A survey on the security of blockchain systems. In *Future generation computer systems*. https://doi.org/10.1016/j.future.2017.08.020.
18. Tariq, N., Asim, M., et al. (2019). The security of big data in fog-enabled IoT applications including blockchain: A survey. *Sensors*. https://doi.org/10.3390/s19081788.
19. Oliveira, T. A., & Oliver, M. (2020). Challenges for connecting citizens and smart cities: ICT, E-governance and blockchain. *Sustainability, 12*, 2926. https://doi.org/10.3390/su12072926.
20. Iftikhar, M. Z., Iftikhar, M. S., et al. (2019). Efficient resource utilization using Blockchain network for IoT devices in smart city. *International Conference on Broadband and Wireless Computing, Communication and Applications BWCCA, 2019*, 521–534. https://doi.org/10.1007/978-3-030-33506-9_47.
21. Jang, S. H., Guejong, J., Jeong, J., & Sangmin, B. (2019). Fog Computing Architecture Based Blockchain for Industrial IoT. In J. Rodrigues et al. (Eds.), *Computational Science – ICCS 2019. ICCS 2019. Lecture Notes in Computer Science* (Vol. 11538). Cham: Springer. https://doi.org/10.1007/978-3-030-22744-9_46.
22. Lu, K., Heung, A., Lashkari, H., et al. (2017). A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT. *IEEE Access*, 3302–3312. https://doi.org/10.1109/ACCESS.2017.2677520.
23. Reyna, A., Martín, C., et al. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems*, 173–190. https://doi.org/10.1016/j.future.2018.05.046.
24. Košt'ál, K., Helebrandt, P., et al. (2019). Management and monitoring of IoT devices using blockchain. *Sensors*. https://doi.org/10.3390/s19040856.
25. Gong, S., Tcydenova, E., et al. (2019). Blockchain-based secure device management framework for an internet of things network in a smart city. *Sustainability*. https://doi.org/10.3390/su11143889.
26. Jayasinghe, D., Lee, G. M., et al. (2019). TrustChain: A privacy preserving block-chain with edge computing. Hindawi. *Wireless Communications and Mobile Computing*. https://doi.org/10.1155/2019/2014697.
27. Theodorou, S., & Sklavos, N. (2019). Blockchain-based security and privacy in smart cities. *Smart Cities Cybersecurity and Privacy*. https://doi.org/10.1016/B978-0-12-815032-0.00003-2.
28. Marsal-Llacuna, M.-L., Colomer-Llinàs, J., et al. (2015). Lessons in urban monitoring taken from sustainable and livable cities to better address the smart cities initiative. *Technological Forecasting and Social Change*, 611–622. https://doi.org/10.1016/j.techfore.2014.01.012.
29. Khan, M., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, 395–411. https://doi.org/10.1016/j.future.2017.11.022.
30. Lin, X., Sun, X., et al. (2008). TSVC: Timed efficient and secure vehicular communications with privacy preserving. *IEEE Transactions on Wireless Communications*, 4987–4998. https://doi.org/10.1109/T-WC.2008.070773.
31. Lu, R., Liang, X., et al. (2012). EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications. *IEEE Transactions on Parallel and Distributed Systems*, 1621–1631. https://doi.org/10.1109/TPDS.2012.86.
32. SmartCity. (2018). *Blockchain–train of innovative thoughts transforming smart cities*. Smart City Press. https://www.smartcity.press/blockchain-implementations-in-smart-cities/.

33. Nitti, M., Pilloni, V., et al. (2017). IoT architecture for a sustainable tourism application in a smart city environment. *Mobile Information Systems*. https://doi.org/10.1155/2017/9201640.
34. Pick, J. B. (2017). Smart cities in the United States and worldwide: A rich arena for MIS studies. *Journal of Information Technology Case and Application Research, 19*(3), 133–144. https://doi.org/10.1080/15228053.2017.1363597.
35. Lee, B., & Lee, J. H. (2017). Blockchain-based secure firmware update for embedded devices in an internet of things environment. *The Journal of Supercomputing, 73*, 1152–1167. https://doi.org/10.1007/s11227-016-1870-0.
36. Andrea, Z., Nicola, B., Angelo, C., Lorenzo, V., & Zorzi, Michele, Z. (2012). Internet of things for smart cities. *Internet of Things Journal, IEEE. 1*. https://doi.org/10.1109/JIOT.2014.2306328.
37. Jayasinghe, U., Lee, G. M., MacDermott, Á., & Woo Seop Rhee, W. S. (2019). TrustChain: A privacy preserving blockchain with edge computing. *Wireless Communications and Mobile Computing, 2019, 17*. https://doi.org/10.1155/2019/2014697.

Chapter 6
Role of Blockchain in Agriculture and Food Sector: A Summary

N. Kamalakshi and Naganna

6.1 Introduction

Agriculture is one of the most significant jobs not only in India but also everywhere in the entire world, for the most obvious reason – grow food and feed people. The concept of agricultural farming after the Stone Age has been evolving ever since the globalization and era of Internet of Things (IoT) and machine learning in post modern era, in spite of this, the humankind has not got rid of the agriculture sector. That shows the perennial nature of this profession. We as *Homo sapiens* have built our society on agriculture. Therefore, agriculture is the basis of a country's economy. And the farmer is the backbone of society. Agriculture has a major contribution and plays a significant role in the overall societal and economical foundation and steadiness. Progression and expansion in agriculture sector not only are crucial but also incur food security; it plays an important role in employment generation as well. However, growth of agriculture depends on various factors like investment which contributes the most. The issues and the challenges are ignorance and low priority in terms of public investment. Also, there is no proper guidance, security, and management maintenance training for farmers. Even though farmers work full days to get a good yield, they sleep without food, and every year, lakhs of farmers commit suicide due to nonpayment of loan, and in a day, more than lakhs of people are quitting agriculture profession due to loss, nonsecurity, and no turnover for his/her hard work and finally moving toward metropolitan cities in search of secure job with handful money. To address this issues and help the farmers with the emerging trend and technologies, the blockchain mechanism has been incorporated for agriculture [27–31].

N. Kamalakshi (✉)
Sapthagiri College of Engineering, Bangalore, Karnataka, India

Naganna
Dr. VRK Institute of Technology, Nookapalle, Telangana, India

H. L. Gururaj et al. (eds.), *Convergence of Internet of Things and Blockchain Technologies*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-76216-2_6

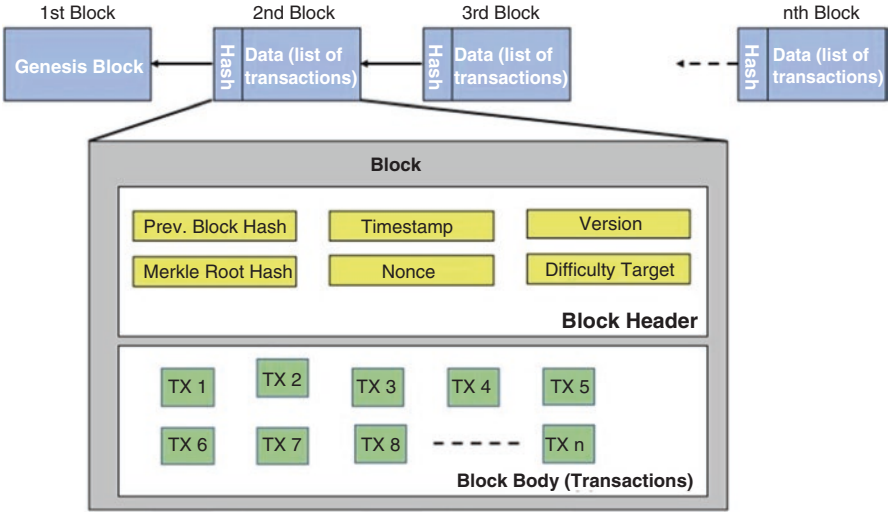


Fig. 6.1 Blockchain with transactions [1]

Blockchain is an emerging technology. It is a platform comprising the distributed ledger of transaction maintained by a network of multiple computing machines without the intervention of the trusted third party. Each transaction data files are termed as blocks; these blocks are operated using a definite software platform that permits the data to be transmitted, processed, stored, and represented in a manner that can be read by humans. In its first example, bitcoin model, there were several blocks, and each block is composed of a header with a time stamp, transaction data, and a link to the previous block. Every block generates a hash value based on its contents and then is referred in the heading of the subsequent block as shown in Fig. 6.1 [1]. Thus, any variation of a given block might result in a disparity in the hashes of all consecutive blocks case study.

6.2 Needs for Blockchain in Agriculture in India

Agriculture is a backbone of major nations of the world and also a very important sector for the survival of humankind. For a country like India, it has a major contribution and plays a significant role in the overall societal and economical foundation and steadiness. Progression and expansion in agriculture sector not only are crucial but also incur food security; it plays an important role in employment generation as well. However, growth of agriculture depends on various factors, and investment contributes the most. The issues and the challenges are ignorance and low priority in terms of public investment. Also, there is no proper guidance, security, and management maintenance training for farmers. Even though farmers work full days to get a good yield, they sleep without food, and every year, lakhs of farmers commit

Table 6.1 Agriculture contribution to GDP of India

Sl. no.	Year	Agriculture contribution to GDP in %
1	2019–2020	15.96
2	2018–2019	15.41
3	2017–2018	16.36
4	2016–2017	16.36
5	2015–2016	16.17
6	2014–2015	16.79
7	2013–2014	17.15
8	2012–2013	16.85
9	2011–2012	17.19
10	2010–2011	17.03

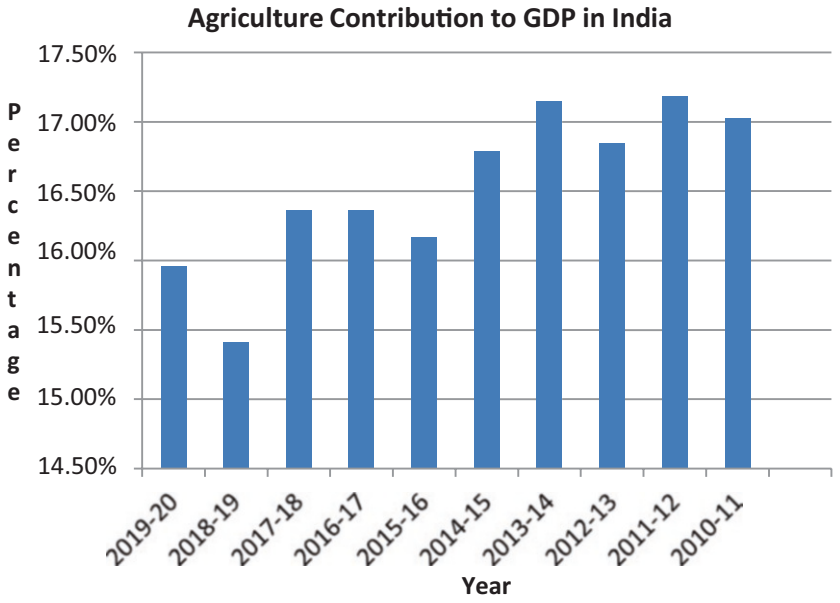


Fig. 6.2 Graph on agriculture contribution to GDP of India

suicide due to nonpayment of loan, and per day, more than lakhs of people are quitting agriculture profession due to loss, non-security, and no turnover for his/her hard work and finally moving toward metropolitan cities in search of secure job with handful money. Table 6.1 and Fig. 6.2 depict the agriculture contribution to GDP of India in tabular-wise and graphical representation, respectively. To address these issues and help the farmers with the emerging trend and technologies, the blockchain mechanism has been incorporated for agriculture [2]. Blockchain is a distributed and decentralized ledger transaction that has started to be employed in the

agriculture sector recently to help the farmers to reach customers directly, and also, this paper highlights applications and case study.

6.3 Challenges of Agriculture Sector

The agriculture sector has a major contribution to the worldwide trade and industry; in spite of that, the industry encounters extensive intimidation to its overall progress, invention, and sustainability. The major challenges encountered in the agriculture sectors are unpredictable climatic conditions, floods, drought, pests, and diseases.

There are innumerable intervention of brokers and agents between growers (farmers) and the consumer. The brokers and agents gain all the benefits while making the farmers suffer with least gain and customers with more expenses in buying the goods:

- The growers don't have direct approach to the banks. The money lenders usually lend money to the growers at a very privileged interest rate than the cooperative, nationalized, and international banks.
- In the developing countries like India, the increase in the interest of the overdue amount owed has led the farmers into depression, further resorting to drastic actions like committing suicide.
- The farmers have unclear land documents, and fragmentations have accomplished nothing but worsen the circumstances.
- In the developing countries like India, there is no proper mechanism for tracing the soil type so as to select the suitable crop and to get good yield of crop of the farmer's land, thus leading to loss of investment of the resources like finance, manure, and crops and decreased revenue for farmers.
- Lack of awareness of innovative and emerging technologies and latest agricultural equipment and benefits such as subsidy and insurance schemes.

6.4 Applications of Blockchain for Agriculture and Food Sector

The employment of blockchain has imparted high benefits to various sectors including the major sectors such has agriculture and food [3]: Major applications are the following: [4]

- Crop and yield insurance for farmers
- Smart agriculture farming
- Supply chain management
- Digital transactions of agricultural products

6.4.1 Crop and Yield Insurance for Farmers

Farmers being the backbone of most of the nations are always the prime target for the natural disaster. Either there will be floods or drought leading to climate extremes which in turn is a threat to the farmers for their yields and agricultural production, leading to breach of security of food. The weather variation is predicted to further exacerbate weather extremes in the future and thus lead to the adverse effects on the crop. In the past, most of country had adopted agricultural insurance schemes as a best tool to manage and recover financial crisis and the debt availed. Normally, here, insurance agency collects premium from the farmers before the commencement of cropping, and if there is any loss after that amount is paid, it's the whole and sole responsibility of the insurance company to bear and manage all the financial exposure due to weather extremes and also financial losses due to it [4].

Insurances for Damage Assessment. Here, committee panel and professionals assess the farmer's land to cover the incurred losses to the farmer; this approach can be called as indemnity-based insurances [5]. The demerits of indemnity-based insurance approach are asymmetrically distributed data on the riskiness of the agricultural outcome of the yield production and also various outcome production practices such as deductibles between farmer and insurer leading to very high expensive damage assessment and should focus on incorporating various course of actions to circumvent problems encountered from skewed information. Also, tackling immeasurable productions such as grazed meadows is a challenging task, as there cannot be any sort of insurance provided, further escalating to the monetary losses [4, 6].

The demerits of indemnity-based insurances have led to the development of index- based insurances [7]. Here, loss is depicted by measurable index, such as precipitation, by taking into consideration the weather station available nearby. Depending on the weather station's past historical weather data, eventually, both the farmer and the insurance company authorities have been provided with the identical information; agricultural farming traditions do not have any influence on the decision of the insurance. Hence, undesirable choice and proper risk do not play any role, and the technological method to activate a payment became significantly easy. Additionally, the coverage of the complete insurance without any further deductions is possible, and timely payments can be done without any delay and can be automated immediately after an undesirable climatic effect was recorded in the database [8].

In summary, index insurances are more challenging risk management tool for farmers. Blockchain aims to improvise index insurance in two aspects: first, to ensure on-time payment and also to furnish the automated weather data that triggers the expenditure as defined and, second, to gather various information such as weather and plant growth information in order to improve the decrease in risk and further make the payment procedure much more proficient [4, 9].

Examples of smart index insurance are Etherisc and WorldCover.

Further, usage of cryptocurrency payouts to reimburse farmers' needs has shown a lot of impact in the field. In fact, the farmers, in the major developing countries,

cannot way in to the essential facilities of communications to take part in a distributed blockchain-based insurance system.

6.4.2 Smart Agriculture

Smart agriculture plays a vital role in major nations by providing basic needs such data and information. It supports all forms of farming information flow although product flow takes the path from initial entry to final outcome through a range of value-adding phases and financial steps. Different community of people produces different data, and further, handling data and in sequence as per their requirements and capacities is very essential. In this aspect, utilization of ICT, emerging technologies such as Internet of Things (IoT), sensors, and many current data gathering and investigation technologies including unmanned aerial vehicles (UAV) and machine learning can lead to highest contribution. Security issue is a major concern that facilitates the utilization and organization of data. In the past, centralized data was managed, and this led to inaccurate data and chances for cyberattack [4].

6.5 Benefits of Blockchain in Agriculture Applications

The various benefits of blockchain in agriculture are the following:

- Traceability
  - Blockchain can be applied for traceability using digital transaction as well as to ease and lessen the burden of the farmers while managing the consumer details with precise write-up of the value chain that finally turned into their products. The reports are composed of valuable data regarding the crop harvested, shipping methods, the processors used, and the delivery and distribution of the output products to stores. The emerging blockchain technology platform can be thus applied to track the crops grown and provide verifiable relevant information to farmers, distributors, and consumers online; with this flexibility and transparency, stakeholders are able to without any difficulty, therefore, perceive and comprehend the complete process that may explain delays [10].
  - Blockchain in the field of agriculture sector can make it possible for stakeholders to collect logistical information to prevent fraud and middlemen intervention.
  - Blockchain ensures trustworthy data because of it's a tamper-proof ledger. It can track each transaction, with complete transparency [11, 12].

- Food safety and quality control
  - Blockchain integrated with IoT and with tracking can record data using sensors to examine the quality of the crop leading up to harvest while in storage and during delivery [13].
  - Blockchain keeps track of record of agricultural information that framers can grasp to inculcate smart and controlled irrigation, fertilization, and pest control while benefitting farmers with lower expenses and enhanced monetary gains [14].
  - Monitors the food production for any contamination, and identifies illness in order to ensure food safety and quality [3, 12, 15].
- Logistics
  - Blockchain emphasizes on flexible, efficiency, and quick delivery of agricultural products due to their short span of life. Also, it focuses on drastically reducing the wastage of the food and procurement costs.
  - Blockchain record-keeping also ensures that payment to the farmers is fair and in time based on yield of the crop rather than seasonal basis [4, 12].
- Transaction costs
  - Blockchain with its sophisticated peer-to-peer network can enable direct and transparent transactions between consumer and vendor, thus eliminating brokers and their commission fees.
  - Blockchain technology uses digitized contract documents and automated data matching to avoid expensive duplications and manual checks on agricultural product transactions.

It can also boost up the supply chain management and food retailers with the benefit from lower transaction costs, thus avoiding back and forth in processing permits and other legal documentation [4, 12]

- Farming resource management
  - Once a piece of agriculture machinery is embedded, a mechanic with blockchain access can update its status from multiple locations.
  - Blockchain in fact monitors the maintenance records dynamically to update the farmers which machinery is available in working condition and also which needs continuance and which is being repaired [12].
- Record encryption
  - Blockchain freezes the stored data so that it cannot be altered, assuring the stakeholder that none of the records have been falsified in any way. With its transparency characteristics, it provides and ensures reliable data to the farmers along with the legal information to all its stakeholders [12].

6.6 Use Cases of Blockchain Platform

6.6.1 Tracing of Food Products

The concept of blockchain in agriculture emphasizes on transparency and trust. Using blockchain, it is very easy to identify the best and suitable location for planting the grain of the crop and also the period for its harvesting and the pesticides to be applied. The blockchain stores minute information, which further can be kept transparent so as to be verified by the consumer before buying the product. It also combines the food supply chain management as per the delivery supply chain management. From this, further information can be tracked easily such as process for shipment; also, the particular broker involved and also the traces in reaching the retail store can be viewed [12].

6.6.2 Optimizing Agricultural Subsidies and Insurance

Blockchain technology in connection with latest emerging trends, IoT devices, machine learning, artificial intelligence, and scientific data analytics, can afford a larger and important depiction to the various financial support for the general insurance schemes. Smart contract is one of the applications that is constructed on blockchain platform. It can reform the intricate outline into a faster and computerized configuration. IoT devices with its appliances and sensors of IoT can be used to forecast and supervise the climatic conditions and to identify crop disease. The sensors play a vital role by straightforwardly feeding information to a smart contract in real time, by enabling automatic payment into the farmer's mobile wallet, hence reducing latency and manual work making the process transparent [12].

6.6.3 Yielding Maximum Crop Productivity

Agricultural land's crop productivity is reliant on various factors such as fertility of the soil; natural climate situation; use of fertilizers and organic fertilizer such as manure, dung, and compost, use of pesticides, and geological conditions. Further, using appropriate and necessary actions at precise conditions can make sure of gaining the highest profit. It also benefits the cultivator to receive utmost profit. Conventional cultivation methods aren't outfitted with advanced agricultural equipment especially in developing countries, who always face losses in crop production each year due to a massive amount of such factors. Blockchain in agriculture can afford a direct use case for optimizing data operation. It provides a safe platform to evaluate all the data gathered by current technological devices. It provides farmer with the feedback on the conditions that are best suited for the land to have good yield [12].

Table 6.2 Small farmer's reasons for suicide

Sl. no.	Reason for suicide	Percentage
1	Crop failure	16.84
2	Price crash	2.65
3	Debt burden	2.65
4	Borewell failure	0.88
5	Losses in nonfarm activities	1.77

6.6.4 Encouragement for Small Farmers

The small farmers are the backbone of the many countries across the world. Their farming purely depends on the nature of the region's land conditions; they vary in their trade and industry conditions. But, more or less, in any region in consideration, it is the smallholder farmer who receives very marginal profit. The brokers get the maximum gain from promotion and trade of farm goods. But the farmer gets the "last part" of the share. Farmers cannot approach the food markets directly due to lack of awareness. Hence, they are unable to utilize the chance that they lawfully deserve. Many of the farmers, involuntarily, missed out of the economic ecosystem. They do not have the facility to way in to the generic banking services and thus cannot avail the facilities of credit systems. Table 6.2 depicts the small farmer's reasons for suicide due to agriculture problem [12].

6.7 Blockchain Food and Agriculture Companies

With the rapid growth and upgradation of the cryptocurrency attracting many businesses, many renowned industries are using blockchain technology to provide solution to various real-world problems and issues. They are depicted in Table 6.3.

Provenance. This platform ensures each and every substantial product is represented with a digital "passport" that proves verification and validation by building an auditable documentation of all the phases of the physical products. The main benefit of this is to avoid the selling of bogus goods and also the difficulty of "double spending" of certifications available in existing system [16].

AgriDigital. It is a coherence of product organization solution for the worldwide food grains sector. This approach provides the combined high-end Indo-technical solutions to innovative ideas and intuitive work flows to provide flawless and perfect solution to complex products, with risk management issues. They are the worldwide leaders in software platforms designed to assist in the transaction and settlement of agricultural commodities and to manage supply chain risk by distributed ledgers and smart contracts. It also facilitates online transactions to farmers with increase competence for middlemen and adaptable supply chain for consumers and investors [17].

Table 6.3 Blockchain food and agriculture companies

Sl. no.	Name of the company
1	Provenance
2	AgriDigital
3	OriginTrail
4	Arc-net
5	Avenews
6	OwlChain
7	Foodcoin
8	TE-FOOD
9	Ripe.io
10	Agri10×
11	Sahyadri Farmers Producer Company
12	Agriota

OriginTrail. It enables professionals of information technology to associate blockchain for supply chain data sharing among many companies. It also helps to provide transparency and integrity for the data that leads to the product [18].

Arc-net. This platform ensures a secure, indisputable, reliable chain of custody for a product or asset. It uses the onion skin model of protection. The encryption uses high-grade keys which are stored and managed by a dedicated hardware security module (HSM). For each asset, it creates a universally unique identifier (UUID) for every asset, thus creating a digital DNA for every product [19].

Avenews. This emphasizes on direct digital trading, thus enabling verified businesses, farmers, cooperatives, and commercial consumers to interact directly locally and worldwide to minimize delivery cost, thus creating safety measures and simplicity [20].

OwlChain. This is a solution using AMIS blockchain structure which depicts apparent, secured, unchangeable, and inerasable characteristics of blockchain. It helps to track the animal's details as a node of blockchain, and even farmers and food companies can upload their details [21].

IBM Blockchain. It incorporates an optimal highly secured network that is a group of all the business transactions and trading relationships globally for business community. It encapsulates a shared distributed ledger that is reorganized and authenticated concurrently with the entire participant in the group. It provides equivalent visibility of the various activities of the group and furnishes the asset location and owner details.

Foodcoin. Foodcoin is a platform that accepts cryptocurrency aiming to reduce the expenses. It deals with the use of smart contracts. It is enriched with ample choice of appliance, such as an appropriate "smart" folder, a remote user recognition method, athletically configurable smart contracts, verification of the source of foodstuff, and an appropriate crypto disbursement processor, thus allowing the trade course of action participants associated to select the food and to do proper customization [22].

TE-FOOD. It provides a cost-effective, transparent, traceability tool solution for livestock food, including all strategy and food excellence venture and managing data for the supply chain aspects of farm animals and fresh food supply information [23].

Ripe.io. It is a platform that provides precision, confidence, and sincerity for agriculturists, vendors, distributors, and customers. It aims to change the basic food structure description by operating with each performer over the length of the food supply chain to construct a globe where channel into information equals reliability, endurable, protection, and foodstuff for all to have a better living. It encourages farmers to use emerging technologies such as IoT and sensors to computerize processes and proficiently meet the existing market requirements for the production of very high-quality, endurable products. It has a mechanism to track the food products, thus helping distributors to react transparently with online data for quick delivery and safety [24].

6.7.1 Indian-Based Blockchain

Agri10×. Agri10× is a Pune-based decentralized blockchain network platform firm. It avoids brokers or intermediate person in the farming trade to provide the farmers with good price for all their efforts to produce the agricultural products on time. This platform ensures secured data and fort and does not permit price manipulation. By using latest technology tools, there would be direct communication between the farmers and the traders. The trading fee charges are fixed 6–10% for start-up charges; this nominal fee is equally divided between farmers and customer. This blockchain-based company is also now expanding its operations to various states of India such as Telangana, Bihar, Madhya Pradesh, and Andhra Pradesh other than the Maharashtra [25]

Sahyadri Farmers Producer Company. It is one of India's largest farmers' companies that has combined blockchain technology in an attempt to introduce traceability and boost income. Sahyadri Farmers Producer Company will enable the customers to trace their produce from the farm to their dinner plate. The company has been digitizing its supply chain as it attempts to comply with food safety standards, the chairman Vilas Shinde said in a statement. Blockchain developed as most suitable for the company's requirements as it improves trust between all the stakeholders, he stated.

By utilizing blockchain, Sahyadri will give the customers greater choice as they will be capable of tracking their food, from the quality of the seeds utilized to the harvesting, packaging, and distribution. This will be done by the simple scanning of a QR code on the product. The benefits of blockchain will be not only for the customers but also for the farmers, Shinde said in a statement. The farmers will also get to track their produce along the supply chain, including such details as to where the product is sold and at what price.

Recently, the company guarantees farmers a 25% share of the retail price for the produce it sells. Nevertheless, by combining blockchain technology, it will be capable of giving the farmers up to 50% share of the final price. Blockchain will decrease the costs originating from friction along the supply chain and cut down the middlemen who take a big piece of the farmer's earnings.

The application of blockchain in agriculture has proliferated in recent years. According to Indian research firm Markets and Markets, the market has been increasing at a Compound Annual Growth Rate (CAGR) of 47.8%. The firm anticipated that this market would be worth $430 million in 2023. The Asia Pacific stands out as the region with the most active growth in this sector. For Australian farmers, blockchain will now be part of a one-stop farming solution experience following collaboration between Farm in One and MetaStreme. Farm in One allows farmers to manage all their processes on a single platform, from irrigation, to spraying, to mapping, to monitoring.

By associating with leading Bitcoin SV wallet service MetaStreme, the company will now penetrate the data-rich Weather SV. The platform will enable the farmers to use this data to shape their activities and, consequently, maximize their profits [26].

6.7.2 Blockchain-Based Agriota E-Marketplace Platform Connects Indian Farmers to Food Industry of the UAE

The blockchain-based supply chain management sector has led the food industry authorities in the United Arab Emirates to import agricultural goods directly from India. The agriculture sector shall start using Agriota E-Marketplace, a new platform that employs blockchain technology to collaborate and bridge the gap between Indian farmers and the major food industry.

Agriota provides simplicity and clarity by verifying the food supply chain from Indian farms to food processing companies, traders, consumer, and wholesalers in the UAE. This platform will allow Indian farmers to connect directly with food industry firms in the UAE.

In the year 2019, India was able to export worth more than one billion dollar of food products to the UAE as per the report of the data from the country's Agricultural and Processed Food Products Export Development Authority. In the year 2002, the government of Dubai introduced Dubai Multi Commodities Centre (DMCC) in collaboration with Indian company CropData Technology; Agriota will also ensure highly protected business communication through a multitier escrow structure. Its main aim is to provide monetary infrastructure and promote significance in the world commodities trade.

Coffee is one of the most favorite beverages of the people all over the world. Among all the countries in the world, India is the one and only country where the coffee plants are grown under shade, further handpicked, and sun-dried. It produces one of the best coffees in the world, produced by small coffee growers and tribal farmers. Indian coffee is highly renowned and has a market value in the global

marketplace and is sold as best top-level coffee. The percentage of share of farmers for all his/her efforts in the return on investment from coffee is very low as compared to the middlemen.

Blockchain-platform-based digital market plays a crucial part for trading of Indian coffee with the emphasis on bringing in simplicity and openness in doing the business of the nation, by maintaining the traceability of Indian coffee from initial stage of growing coffee beans to beverage drink of consumer cup so as to serve the consumer with the real flavor and taste of the Indian coffee, and here, the farmer is paid comparatively better for all his/her efforts for the coffee produced. This enterprise attitude will definitely benefit the nation in creating a trademark for the quality image on Indian coffee through traceability, thus avoiding growers' dependency on middlemen by providing a direct control to consumers and a reasonable cost for their produce, determining the platform for right coffee suppliers to exporters and within the specified time to meet the increasing requirements, and establishing an enhanced confidence and long-standing association due to improved *visibility* toward the aspects of traceability and simplicity of the produce. Blockchain-based coffee e-marketplace through video conferencing has been launched. This new approach which is first of its kind is a pilot project that will help integrate the farmers with markets in a transparent manner and lead to realization of fair price for the coffee producer; the blockchain will also reduce the number of layers between coffee growers and buyers and help farmers double their income.

The collaboration of the Coffee Board of India with M/s Eka Plus, one of the worldwide pioneers in digital product organization platforms for agriculture, led to the development of decentralized blockchain-based trade market application. The Eka Plus have designed and developed an application along with collaboration of group of coffee owners, farmers, exporters, roasters, importers, and retailers that are already registered on the platform from India and various countries across the world. It is one of its kind in which the blockchain-platform-based processor for coffee has been introduced after it has been introduced in France and Ethiopia and to the world.

The coffee community includes coffee farmers, traders, coffee curers, exporters, rosters, importers, and retailers registered on the blockchain platform that has been introduced to create trade and business. The coffee farmer registers basic credentials like location, type of coffee, elevation, quality, and any other relevant information pertaining to the coffee grown. The process starts by creating a block for each of the coffee sold by the farmer on the decentralized blockchain platform. The credentials and details of the block/lot of the farmers will be stored on the blockchain throughout its journey and are not able to be forfeited.

6.8 Conclusion

Blockchain technology has the great prospective to alter the area of agriculture and food at the same time also adding up great value to it. The main objective of this chapter was to accomplish a thorough exhaustive research literature concerning

employment of blockchain for traceability and food safety measures and few other techniques of the blockchain technologies and their combination in the agriculture and food sector. In spite of blockchain technology being an emerging technology of extensive research over the last decade, it is only in the last few years that some research avenues and also the studies on the realization and accomplishment of blockchain in agriculture and food sector have made their appearance. At the same point in time, an increasing trend on start-ups, ventures, and pilot applications is observed. Research review survey conducted in the background of this chapter has exhibited that using blockchains can beneficially help to attain traceability by irreversibly and immutably storing data. Blockchain technology creates a unique level of credibility that contributes to a more sustainable food industry.

This chapter provides a glimpses of the role of blockchain in agriculture and food sector. Initially, it provides the introduction to blockchain, challenges, applications, and use cases. Further, it also enlightens various start-up companies that are working on blockchain platform e-agriculture.

References

1. Kamilaris, A., Xavier, F., & Boldú, P. (2019). The rise of blockchain technology in agriculture and food supply chains. *Trends in Food Science & Technology*. https://doi.org/10.1016/j.tifs.2019.07.034.
2. Borah, M. D., Naik, V. B., Patgiri, R., & Bhargav, A. (2019). Supply chain management in agriculture using blockchain and IoT. In *Advanced Applications of Blockchain Technology*. https://doi.org/10.1007/978-981-13-8775-3_11.
3. Baralla, G., Ibba, S., Marchesi, M., Tonelli, R., & Missineo, S. (2018). A blockchain based system to ensure transparency and reliability in food supply chain. In *Proceedings of the europar: Parallel Processing Workshops, Turin, Italy* (pp. 27–28).
4. Xiong, H., Dalhaus, T., Wang, P., & Huang, J. (2020). Blockchain technology for agriculture: Applications and rationale. *Frontiers in Blockchain, 3*(7), 1–7. https://doi.org/10.3389/fbloc.2020.00007.
5. Just, R. E., Calvin, L., & Quiggin, J. (1999). Adverse selection in crop insurance: Actuarial and asymmetric information incentives. *American Journal of Agricultural Economics, 81*, 834–849. https://doi.org/10.2307/1244328.
6. Vroege, W., Dalhaus, T., & Finger, R. (2019). Index insurances for grasslands – A review for Europe and North-America. *Agricultural Systems, 168*, 101–111. https://doi.org/10.1016/j.agsy.2018.10.009.
7. Turvey, C. G. (2001). Weather derivatives for specific event risks in agriculture. *Review of Agricultural Economics, 23*, 333–351. https://doi.org/10.1111/1467-9353.00065.
8. Woodard, J. D., & Garcia, P. (2008). Basis risk and weather hedging effectiveness. *Agricultural Finance Review, 68*, 99–117. https://doi.org/10.1108/00214660880001221.
9. Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaría, V. (2018). Blockchain and smart contracts for insurance: Is the technology mature enough? *Future Internet, 10*, 20. https://doi.org/10.3390/fi10020020.
10. Lin, Q., Wang, H., Pei, X., & Wang, J. (2019). Food safety traceability system based on blockchain and EPCIS. *IEEE Access, 7*, 20698–20707.
11. Demestichas, K., Peppes, N., Alexakis, T., & Adamopoulou, E. (2020). Blockchain in agriculture traceability systems: A review. *Applied Sciences, 10*(12), 4113. https://doi.org/10.3390/app10124113.

12. Hammerich, T. (2018). Potential use cases for blockchain in agriculture. *Future of Agriculture*. https://futureofag.com/5-potential-use-cases-for-blockchain-in-agriculture88d4d2207e8.
13. Kamble, S. S., Gunasekaran, A., & Sharma, R. (2020). Modeling the blockchain enabled traceability in agriculture supply chain. *International Journal of Information Management, 52*, 101967.
14. Salah, K., Nizamuddin, N., Jayaraman, R., & Omar, M. (2019). Blockchain-based soybean traceability in agricultural supply chain. *IEEE Access, 7*, 73295–73305.
15. Lucena, P., Binotto, A. P. D., Momo, F. D. S., & Kim, H. (2018). A case study for grain quality assurance tracking based on a blockchain business network. In *Proceedings of the Symposium on Foundations and Applications of Blockchain*.
16. Provenance. (2015). *Blockchain: The solution for transparency in product supply chains (White Paper)*. Retrieved September 2020, from https://www.provenance.org/whitepaper
17. Xu, X., Weber, I., & Staples, M. (2019). *Case study: AgriDigital*. Springer, Cham: Architecture for Blockchain Applications. https://doi.org/10.1007/978-3-030-03035-3_12.
18. Rakic, B., Levak, T., Drev, Z., Savic, S., & Veljkovic, A. (2017). Origintrail. In *First purpose built protocol for supply chains based on blockchain*.
19. Childerhouse, P., & Towill, D. R. (2011). Arcs of supply chain integration. *International Journal of Production Research*. https://doi.org/10.1080/00207543.2010.524259.
20. Avenews-gt. (2018). https://www.avenews-gt.com/
21. OwlChain. (2017). https://www.owlting.com/obs
22. Foodcoin. (2017). *Foodcoin Ecosystem*. https://fcegroup.ch/
23. TE-Food. (2017). Making business profit by solving social problems, White Paper. Retrieved September 3, 2020, from https://www.te-food.com/te-food-white-paper.pdf
24. Ripe.io. (2017). http://www.ripe.io/
25. Agri10x. (2020). https://www.inc42.com/infocus/blockchain-this-week/blockchain-this-week-blockchain-startup-agri10x-to-work-with-indian-farmers-more/
26. SahyadriFarmers. (2018). https://www.manage.gov.in/publications/reports/Sahyadri-eport.pdf
27. Abelseth, B. (2018). Blockchain tracking and cannabis regulation: Developing a permissioned blockchain network to track Canada's cannabis supply chain. *Dalhousie Journal of Interdisciplinary Management, 14*.
28. https://www.techslang.com/blockchain-agriculture-getting-it-off-the-ground/Josh Cook, 12 blockchain food & agriculture companies in their own words. https://medium.com/lokaal/12-blockchain-food-agriculture-companies-in-their-own-words-71f8398252eb
29. OwlTing. (2017). https://www.prnewswire.com/news-releases/owlchain-launched-as-the-worlds-first-food-blockchain-provenance-system-300464467.html
30. Krishna, A. S., Voora, H., Hallikerehundi, M., Sharma, S., Agrawal, Y., & Thasmiya Noorain, A. N. (2019). *Modernizing enterprise business connecting application data with IBM blockchain*. IBM Developer. https://www.ibm.com/blockchain.
31. TE-Food and LAUREL. (2017). *The Largest Farm-to-Table Food Traceability Project in the World*. Retrieved September 3, 2020, from http://te-food.co.za/use_case.html

Chapter 7
PalCom Middleware-Based Blockchain Challenges on Healthcare System

Sonali S. Dash, V. Rajasekar, and Sam Goundar

7.1 Introduction to Blockchain

The worldwide emerging technology that is blockchain is one of the popular technologies having vast number of applications. The distributed network approved with decentralized environment is able to solve security issues without the use of third trusted party (TTP) in the blockchain. The blockchain researchers focus on healthcare system having challenges like fragmented information on patient and doctor. The decentralized view point causes patient-oriented services to be more delightful. All data are securely accessible from hackers as everything will be in cloud servers.

Healthcare is one of the applications which is possible for research as it has a strong impact for generating the opportunities for current healthcare system. The proper direction is necessary to interrogate in healthcare [1] for collecting all background information and existing information of healthcare systems. It is reviewed by using the latest methodology for which it has been stated. It focused on exploring the dynamic applications of latest blockchain technology which highlights the requirements of new era platforms such as trustworthy and transparent. The data-driven healthcare home-based system is considered as positive, effective environment for sustainable future.

The health service provider acts like a building block associated with healthcare system collaborating the emerging technology and infrastructure for patient records. The combination enables the distributed healthcare system to be very secure. Pivot

S. S. Dash (✉) · V. Rajasekar
AMC Engineering College, Bengaluru, Karnataka, India

S. Goundar
ICT (Cyber Security), British University Vietnam/University of Staffordshire, Hanoi, Vietnam

H. L. Gururaj et al. (eds.), *Convergence of Internet of Things and Blockchain Technologies*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-76216-2_7

system helps to share the patient-related data with service providers without creating conflict requirements. Integrity and uniqueness play vital role interoperability.

The medical records maintain uniqueness toward the patient or doctor data using blockchain, Hyperledger, and smart contracts. It helps to provide information using the distributed decentralized network and to achieve the conceptual way using efficiently interoperability mechanism effectively. The disjoint information uses handheld devices to improve the security toward positioning the preventative [2] and precision medicine. The greater individuals provide the access and control the data. The transparency and immutability promise to solve the interoperability and security issues using blockchain paradigm in healthcare system. Many papers have proposed the security purpose of blockchain technology to determine and identify the potential improvement in case of applications and challenges.

The work proposes toward the following:

- Presenting overall details related to blockchain technology health data systems
- Discussing the integrity, security and privacy, and performance
- Identifying the solution toward the research questions on healthcare data systems

The blockchain governance-based healthcare research provides the real-time deployment with unique key and efficient approach of smart contract security. The audit tools are used to adhere the healthcare data regulations and standards. The push message toward patient-driven interoperability [3] uses patient-mediated data exchange with patient-driven. The patient-centered interoperability has new challenges and requirements for integrity, security, and privacy. The scaling approach succeeded the technology, incentives, and governance for data sharing.

The mechanisms used to facilitate the transmission are as follows:

- Digital access signature
- Data aggregation values
- Data validity
- Patient integrity
- Data security

The barriers in patient-driven interoperability and patient engagement govern the rules toward data aggregation. It is a lightning swing toward healthcare system which gives several upcoming challenges and to be focused on facilitation part for transition suitability from home-based to patient/doctor/pharmacist-centric data divisions.

The healthcare interoperability focuses on information sharing approach between medical entities and patient entities. Healthcare is a data-sensitive domain where large volume of data monitoring happens in hospital. For clinical research, creating medical records and generating insurance claim report are the challenging role in the Internet of Things (IoT). The healthcare applications of blockchain use heterogeneous network for creating virtual tokens [4] which is the terminology for authorization of medical records in medical domain. It is a crucial research study where the technology is accompanied with a healthcare system for generating smart contracts support and challenges as a problem.

The healthcare domain compromises with the following:

- Report the results of medical information as a systematic literature review.
- To identify, extract, evaluate, summarize, categorize, and synthesize the studies.
- Existing benefits/challenges/feedback on incorporating blockchain.
- Provide a framework with all research activities,
- Establish the state of evidence with in-depth assignment.

7.1.1 Internet of Things (IoT)

The name defines dynamic self-configuring global network infrastructure which has the capability to be interoperable with all variety of communication channels through protocols with physical communication channels. They consisted with individual identities, attributes, and personalities. They use quick interface for integrating into the information network [5]. The IoT has a bright future toward real-time application in a growing market. It is recognized as sophisticated and sensible technology for the human health and privacy.

The IoT includes the set of somatic objects that are assisted with sensors, actuators, and electronic devices. All have been connected with communication channels and linked to a distributed network to provide the data transmission. The health-related information nowadays is transmitted through the gateway providing all the security [6]. They access all the information from the cloud servers to a one-way secure cloud-based platform. Imagine the scenario where a patient will be constantly monitored using the handheld devices like for hypertension, diabetes, asthma, or obesity. All parameters will be recorded in cloud-based platform in health management system.

The portable devices designed to receive the treatment from any of the organizations for all health checkup parameters. The data are gathered together from portable electronic devices and can stored in cloud servers, and each data set should be analyzed by the medical specialists. It helps to enable the location of patient to respond timely. With appropriate sensors, the alert can be enhanced in wireless technology. The solutions will support the patient in healthcare and medical environment. This is a packaging concept to integrate blockchain technologies.

This work represents the challenges, benefits, and feedback [7] needed to resolve using blockchain's latest technology in healthcare systems. Here, the smart contract is initiated for the use of blockchain-based healthcare system. It emphasizes on key which defines the predefined agreement within PalCom middleware and stakeholders. The analysis of the results concluded with a discussion on requirements and how blockchain could be benefited in the healthcare premises.

7.1.2 PalCom Middleware

The PalCom architecture is used to separate the computation from the assemblies and configuration of which services are present and the coordination to solve the services' interaction. A unified view for heterogeneous network in PalCom is established for the communication network and also to discover way of mechanisms to make assemblies reactive for a new changing environment where the services may come and go.

PalCom assembly is the service provider to mediate for design to be fitted and makes the outcome possible to combine into new unplanned way. It can be done without making any changes to the services and enables the original implementation of services for adjustments using the scripting language for the betterment of healthcare [6].

In view of PalCom middleware which is used in healthcare systems like blood flow meter, combining with proper equipment helps to enable all flexible combination with mobile devices with the help of AXIS cameras [8] and remote sensors; the development includes all variety applications for real-time control of mobile robots.

7.2 e-Health Abstraction

The e-health abstraction is being used to find the new era of attractive customers that associate with healthcare system which added the science and latest technologies with appropriate data. The communication channel is a key template to access the benefits/feedback of individual patients/doctors along with society. A very extensive research takes place to focus in distributed network that helps to improve the healthcare services with the reduction of the cost for all healthcare system. The network improves the quality and quantity of medical assistance with channel of communication between patients, doctors, and pharmacists. All health service providers and abstraction [9] bring the security in the health system.

A wide range of data is included in e-health through communication channel and the latest technology for applications. The goal is to improve management and security. The main use of information is to support the clinical processes in operational way with financial basis. The decision-making process is used to improve the delivery in health service. The e-health benefit includes the potential to increase the security access for information along with resources which increases the patient's ability for better improvement in medical healthcare and also improves the organizational processes. The safety measurement measures the quality of patient life issues with integrated e-health system for providing clinical information. Healthcare monitoring system is illustrated in Fig. 7.1.

The clinical problems regarding the reporting result test allow direct access to pharmacy orders, and it supports all telemedicine applications. The decision-making process of administrative along with financial officers plays a vital role. The

Fig. 7.1 Home monitoring system [7]

location of the patient from the distributed network can be in a hospital. The inventory management and financial and administrative officers can analyze the results which are associated with the treatments and with the formal procedures. The quality can be assured with all the clinical experiments implemented and supported by treatment protocols. All the scientific-related information can be accessed from digital scientific [10] libraries to support and to provide the access to all databases.

The potential applications of healthcare can be diverse in many ways:

Hospital which involves database of patient/doctors/nurses and the transactions between them will be through smart contact and other related pharmaceutical test.

Database which includes all transactional activities of protection, validation, and monitoring for prevention, early detection, quality, quantity, and security.

Management which includes all initial initiatives regarding the development and deployment of healthcare systems in smart and attractive way for securing data from traffic congestion systems.

7.3 Healthcare for Home Patient Monitoring System

The quality of health has impact on one's life which might raise the cost of medical care, and for chronic diseases, it is very high. As the elder people increases in number, society pressurizes the health services. The healthcare system is rapidly growing in terms of the powerful information and communication channels [11]. The new vast technologies help in service of healthcare for developing the large effective

information processing system and securing the large-scale data values. The effective communication is connected with large devices to improve the healthcare system for faster delivery using hand sensors. It is used to collect all the data from the cloud and various data centers and to analyze data appropriately.

All the healthcare service providers are vastly connected with handheld devices like mobiles, laptops, pamphlet, tablets, and smart devices through Wi-Fi using all switches and bridges. It helps to become proactive for health services' faster delivery. The wireless devices are used theoretically in order to use all wearable devices for collecting the real-time data from hospitals. Home monitoring devices provide the services for patients who require the constant health checkups from the comfort [12] of being at home rather than in hospital environment. The glucose meters and oximeter used for remote monitoring of patients are very difficult to provide accurate data to healthcare specialists.

The communication between doctor and patient improves the connectivity with real-time home-based monitoring of patient. The Romanian health system has impacted all European countries' the medical activity where Romanian medical sector has befitted with recent technologies for healthcare. The medical officers have the authority to access patient's medical records. The healthcare cost including the services seems to be high due to the emerging technology along with the vast population. It helps in increasing the demand in healthcare system.

The latest emerging healthcare system provides all the authentication to support doctors and patients with any kind of chronic diseases. It manages healthcare records to achieve the performance based on optimal status to avoid latency. The evolution in healthcare system combined the technologies to achieve the best result out of it and also to solve the problems of the health domain [13].

7.4 Architecture of Blockchain-Based Healthcare System

Remote patient monitoring in healthcare system helps to monitor the patients within the settled environment. It allows the patients to be intrinsic toward the service which can be connected with health providers if necessary. To reduce medical cost and to improve the quality of remote care, the service providers provide the RPM masses for explicit use of healthcare system. The component based on RPM system can be designed for monitoring the devices through smart phone by accessing the data using smart contract concept.

The handheld device features act similar to wearable devices. The component present plays a vital role in RPM application and helps to push the data into smart contract [14] for development. The patient health information is collected securely and transferred privately to hospitals or medical institutions by creating the blocks to facilitate the health monitoring remote-wise. Then, diagnosis of the diseases and sending for treatment play a role. The big data develops the scenario through all the patient-related data sent to blocks of data and finalizes the integrity and security. The handheld devices in healthcare use the smart device which includes the

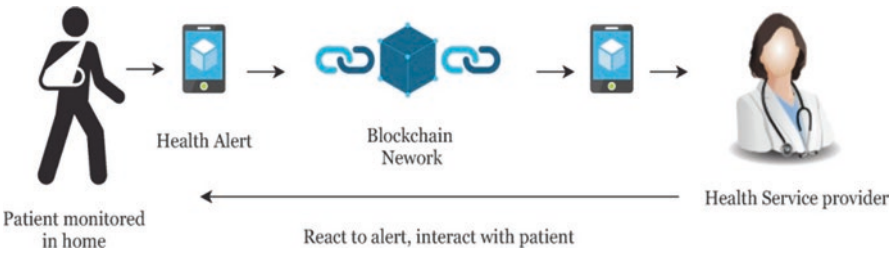


Fig. 7.2 Blockchain architecture for patient monitoring system [15]

microcontroller being embedded into the body like an accessory. It is a user-friendly command and well connected with advanced properties such as wireless data transmission. The alternation mechanism for real-time feedback collection provides the important information for calculating the blood pressure, pulses, and blood glucose. The healthcare wearable devices can be categorized into three types. Figure 7.2 shows the blockchain architecture for patient monitoring system:

- **Accessory devices**—Devices which can be used on a specific physical part of the body externally.
- **Embedded devices**—Devices which can be implemented physically and internally.
- **Handheld devices**—Devices used by the doctors provided for checking.

The handheld/wearable devices can be embedded like software, hardware, electronics, and sensors, and the connectivity helps to enable exchange of data. All the devices transmit the information to be kept on cloud centers securely.

The blockchain technology emerges to provide secure data which can be sharable [15] along with the doctor/patient data with other centers/organizations. It further demands the secure data sharing concept using the encrypted algorithms. The major risk arises by sharing private health data among the organizations. The current enthusiastic system approaches toward the protection of centralized architecture with centralized trust value.

Toward the solution part of each and every data, privacy and security [16] can be achieved by providing the blockchain technology. It provides robustness against the exposure of data along with failure. The shared data method is responsible to provide blocks of data for storing. Each blocks are connected with each other with chain. Genesis is the first block of chain. Each block has block header segmented with transaction counter and transaction ID. Figure 7.3 shows the healthcare blockchain system using smart contracts.

The proof of work or stock is based on blockchain security. The transaction is meant to be valid when the system obtains appropriate proof. The miner is responsible to create the blocks which has a constant gas limit for performance. To solve the cryptographic hash puzzles, it uses the blockchain computation. Mining is an important process for adding a new block to the blockchain accurately. The individual block of chain is segmented by hash in header having hash values [17]. Each

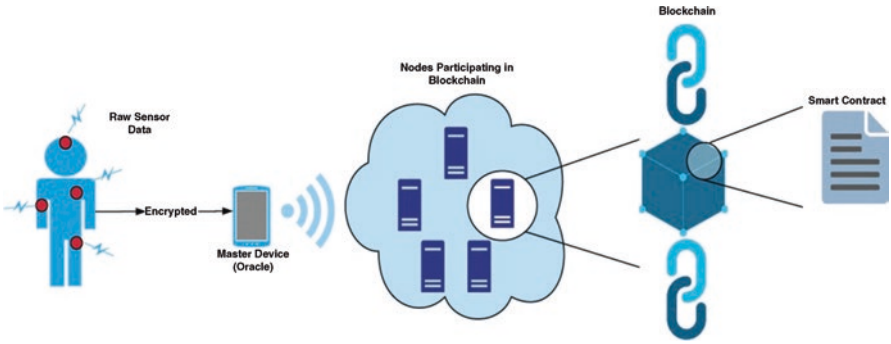


Fig. 7.3 Healthcare blockchain system using smart contracts [16]

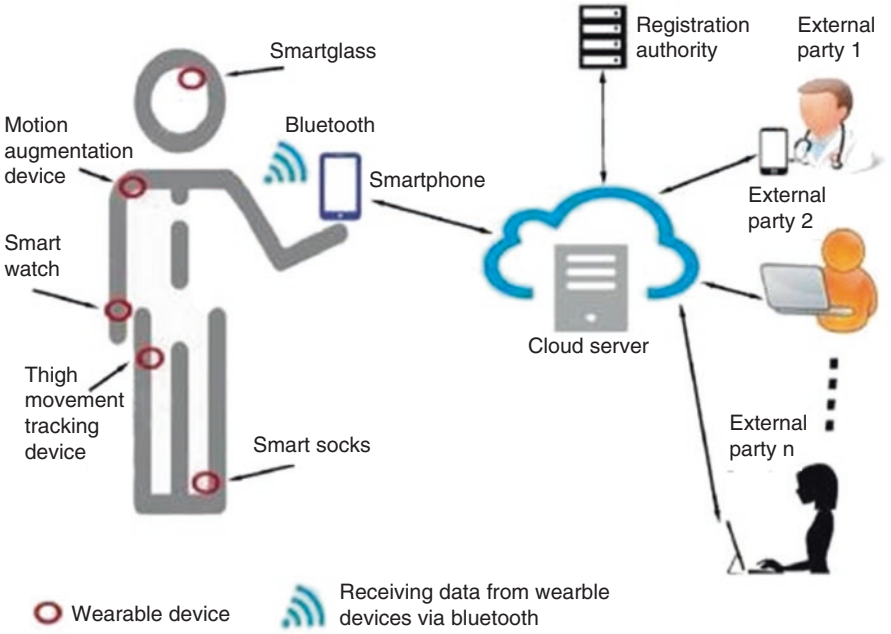


Fig. 7.4 Patient wearable devices [17]

hash value is unique and generated by the algorithm called Secure Hash Algorithm (SHA-256). This algorithm uniquely encrypts and decrypts any size of plain text and calculates a fixed size of 256-bit cryptographic hash value. The individual header contains the address of the previous block and connects to the next block of the chain. Deleting/altering/changing the information from the block is not possible because the blockchain is the best in the field of healthcare system. Figure 7.4 shows the typical patients' wearable devices.

7.5 Implementation

Examples of patient's handheld device are pulse oximeter, blood pressure machine, insulin pump, and injections. The random monitor for patient was impossible to connect with ubiquitous network. After verifying the identity of documents, they can connect to the network and can access the network. Health-related information from the cloud server can be accessible by smart device like smart phone, pamphlet, or tablet. They can format the data and aggregation [18] by the online/offline application. The well-formatted information from the cloud can be accessed by smart device like mobile phone or tablet by scripting the smart contract for analyzing the threshold values once completed. The threshold values are dependent *on normal* reading. The abnormal reading will occur with scripting smart contract when an event/fire is created.

The abnormal reading is stored into the cloud servers. The hash of the stored data is transferred from the cloud server to overlay network. While transferring the health record from the cloud server, the sender segmented the digital signature with the data. The overlay network within the distributed network sends ignition to the health service providers. The health reading data is not stored in the overlay network [19]. The data stored in the transaction alert toward the overlay network. The health ignition can be immaterial. The privacy is preserved inside the overlay network. This alerts with the transaction of data with the specific user by using the encrypted cryptographic techniques.

The flow of data moving toward the system uses the technical details for encryption/decryption algorithm from the sender, receiver, and network. The public key/private key contains all information placed inside the overlay network that has hash index of stored data in the cloud. An ignition will be received in the provider node, and then, it enables to access the full health reading of the patient. Each transmission of data is authorized over overlay network.

7.6 Security and Drawback of Home Monitoring System Using Blockchain

The major problem in home patient monitoring systems is security and privacy. All the medical data are efficiently transmitted. The medical data can be secured from hackers, and the security the data is the primary motivation. The primary target for cybercriminal [20] is to hack information. The cyberattacks on medical records are through wearable devices of patients. The blockchain technology concept brings the solution of preventing these issues by imposing to delete or change or alter the information present inside the blocks, which proves to be one of the best technologies for healthcare system. The below challenges prove the use of blockchain toward the IoT world.

7.6.1 Challenges

- **Distributed network:** The traffic flow congestion eliminates the robustness and scalability for decentralized system. Due to distributed system and decentralization, the single point of failure or information delay can be eliminated.
- **Digital signature:** The stored data is transferred from the cloud servers to blockchain networks. While transferring the data from one host to another host, the data can be lost. The tampered data can increase the burden toward security and integrity [21]. It can cause the loss of information of the patient. To protect these, the digital signature scheme can be utilized. The secured data is verified in the blocks with the help of user's digital signature on the receiver end and as an acknowledgment adds the receipt of data.
- **Integrity:** The IoT devices are very intensive resources. Distributed network has nodes. It helps to increase the scale value in nodes within blockchain. The proof of work concept helps to eliminate the consistency in overlay network. The similar clusters within a single chain will not be responsible for nodes by dividing inside the overlay network. The spread of clusters over the nodes relies on the distributed network and added the security and privacy toward the network.
- **Cloud storage:** The cloud storage over big data uses the cloud servers for all information to store, update, and delete in blockchain and helps to encrypt or decrypt data blocks. The cryptographic security using digital signature helps to solve high-standard definition encryption to huge data. The third trusted parties [22] cause the problem to store all huge data transactions in each variety of blocks. It helps to create hash value of each block encapsulated by the algorithm of Merkle tree to transfer over overlay network. The cloud data can be changed and detectable, and the cloud helps to store and to preserve all the data in decentralization over the networks.
- **Ring users:** The secure huge medical information of a patient may contain very delicate data. All the huge information are anonymized over the distributed network. The lightweight ring structure uses digital signatures for securing the data. The user uses the digital signature for securing the data known as ring signature. It allows the user to extract the data anonymously and uses the signature. All signature started mixed with other groups where it's signed by the message.
- **Encryption scheme:** The medical wearable or handheld devices encrypts [23] all the information, but due to hackers, health data must be secured and cannot be altered. The data can be saved from hackers by applying the double encryption scheme algorithm. The so-called algorithm double encryption uses two keys for encrypting the data. It used the encrypted lightweight algorithm SHA-256 and the public key of receiver. The Diffie-Hellman algorithm helps to exchange key for analyzing and securing data from hackers.

7.7 Solution Toward Security Issues of Home Monitoring System Using Blockchain

This home-monitoring-based system has six concepts. These are hash storage, distributed network, healthcare service providers, smart agreements, PalCom middleware, and handheld devices equipped with healthcare system.

7.7.1 Hash Storage

The cloud storage uses the data from the cloud server. The patient data create the hash values to keep it inside the blockchain. The patient information stored is all the grouped information [24] in each identical blocks having identical sequence number. The cloud storage is connected to distributed network. The single block is calculated by using each hash values and functions where the Merkle tree algorithm is associated. The head hash will always add the new generated block which associates with previous hash values and will be able to generate the new blockchain. The needed case uses the third-party trust where the data can be traceable.

7.7.2 Distributed Network

The distributed network is a heterogeneous [25] network which based on overlay architecture rather than homogeneous network. Every nodes are connected to each other through laptop, smart devices, tablet, or IoT handheld device. The distributed network has the nodes which are certified by valid certificate. The authorization can be given to each certified person who can access the data through distributed network very securely.

The probability increases inside distributed network and can able to avoid time delay. The nodes can be grouped with clusters, and each cluster head is used to take care of public keys. If latency [26] comes, then each node can change with the cluster, and along with that, the cluster head will also change. Generally, the cluster head has the public keys of sender which come from the service providers, and they can access all the specific data.

When the patient wants to access or share the personal information with the specific doctor, then the node will not allow access till they submit the digital signature. This is the job of cluster head which has authenticity to verify the details using the private key along with the digital signature [27] of doctors. The transaction will broadcast to other clusters for verification. If the nodes cannot be verified with the public key, then it will not broadcast the same and also will not allow to transfer any data to the cluster heads.

The cluster head is also responsible to keep all the hash values inside the cloud server securely. The cluster has the capacity to keep all the hash of previous value block in each new allocated block. The capability of each cluster is to decide for new blocks' availability. The cluster main head adds the new automated link to each new hash so that it will broadcast. The rest of the clusters verify the necessity to maintain trust rating in distributed network.

7.7.3 Healthcare Service Providers

The healthcare service providers keep all the necessary information of medical treatments in applying for insurance. It covers and maintains all variety of medical test. The service providers deal with all medical test of the patient happens inside the distributed network [28]. Each of the node within the network will have authentication to receive all securely based patient data.

7.7.4 Smart Agreements

The smart agreements allows the smart contract to be created in any of the handheld devices. Some conditions are to be applied to find out the exact measurement of blood pressure in high-level or low-level conditions. Depending on the reading, the handheld device will decide range it falls in, and the smart contract will have authenticity to provide the patient data to authorized healthcare providers. The storage of all the readings will be the cloud server [29]. Figure 7.5 shows the typical structure of smart contract for healthcare system.

7.7.5 PalCom Middleware

The PalCom middleware contains all assemblies which propagated with all possible services and parameters. This is done when the commands can be added to the services without changing the environment's capability. It helps with scripting language where the user having no knowledge can implement the information in the healthcare system.

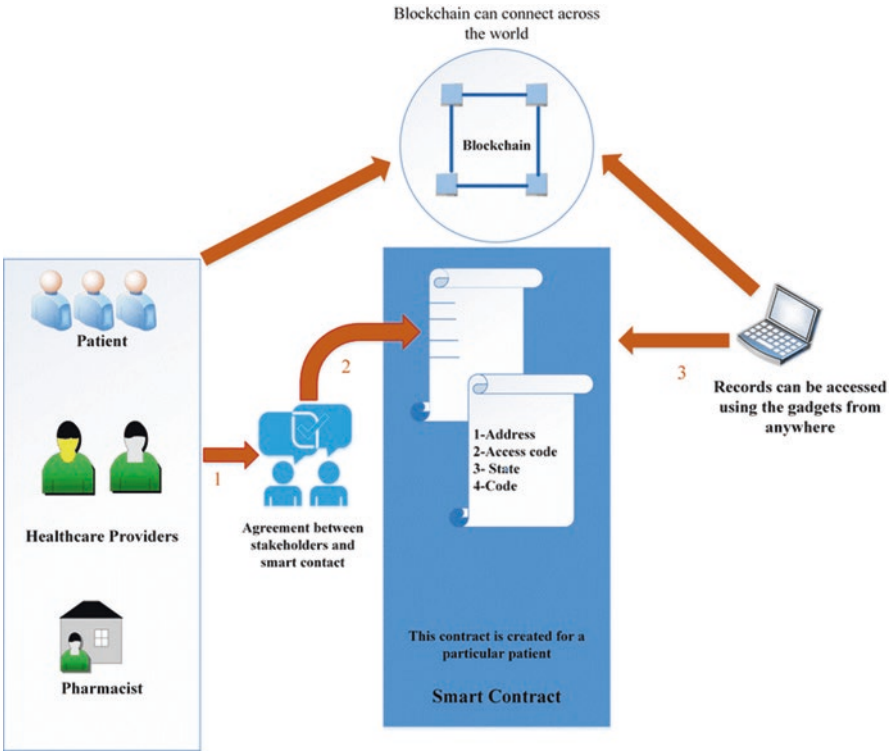


Fig. 7.5 Smart contract for healthcare system [30]

7.7.6 Handheld Devices

The handheld devices help to collect the information from the patient. The data can be collected through IoT devices from heart rate and blood pressure. The data can be stored in the cloud server and can be accessed [30] securely using authentication. The data can be insured through insurance service providers.

7.8 Future Work

This paper brings the actual usage toward the IoT model which is accomplished with blockchain approach that helps toward providing secure authenticated information of home-based patient. The main agenda toward future aspect is to add the commands and parameters in PalCom middleware where the researchers will have the guarantee to secure all testable data from hackers using cryptographic component.

7.9 Conclusion

The huge and rapid transmission of information between the channels like patient, doctor, and pharmacist gives way to the use of Internet of Things in healthcare system. It intermediates the safety transaction of information using handheld devices. This is the continuous process of monitoring the people's healthcare data in a preventive and effective way. Here, the survey was taken to enrich the concept of safety toward the patient information system.

Internet of Things uses its many applications for the development of many platforms by implementing health monitoring system which enhances the rapid access in the field of blockchain systems. Now, the patient home monitoring system in medical environment is made very safely and securely.

The blockchain security is very useful toward healthcare and industry. There is third trusted party available which is the constraint factor of Internet of Things. The proposed architecture gives the idea toward security and privacy where the hackers cannot access the information without authorization. In this paper, the hybrid approach uses encryption technique, blockchain, and smart contract for cryptographic primitives. It is used to develop all authorized patient data where medical records are kept.

References

1. Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. La Vergne, TN: BN Publishing.
2. Malina, L., Hajny, J., Dzurenda, P., & Ricci, S. (2018, July 26–28). Lightweight ring signatures for decentralized privacy- preserving transactions. In *Proceedings of the 15th international joint conference on e-business and telecommunications, Porto, Portugal* (pp. 526–531).
3. Mettler, M. (2016, September 14–17). Blockchain technology in healthcare: The revolution starts here. In *Proceedings of the 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), Munich, Germany*.
4. Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017, March 13–17). Blockchain for IoT security and privacy: The case study of a smart home. In *In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA* (pp. 618–623).
5. Zhang, J., Xue, N., & Huang, X. A. (2016). Secure system for pervasive social network-based healthcare. *IEEE Access, 4*, 9239–9250.
6. Zhu, X., & Badr, Y. (2018). Identity management systems for the internet of things: A survey towards blockchain solutions. *Sensors, 18*, 4215.
7. Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: Found healthcare intelligence on Blockchain with novel privacy risk control. *Journal of Medical Systems, 40*, 218.
8. Panarello, A., Tapas, N., Merlino, G., Longo, F., & Puliafifito, A. (2018). Blockchain and IoT integration: A systematic survey. *Sensors, 18*, 2575.
9. Srivastava, G., Dwivedi, A. D., & Singh, R. (2018). PHANTOM protocol as the new cryptodemocracy. In K. Saeed & W. Homenda (Eds.), *Computer information systems and industrial management* (pp. 499–509). Cham, Switzerland: Springer International Publishing.

10. Srivastava, G., Dwivedi, A. D., & Singh, R. (2018, July 26–28). Crypto-democracy: A decentralized voting scheme using Blockchain technology. In *Proceedings of the 15th international joint conference on e-business and telecommunications, Porto, Portugal* (pp. 508–513).
11. Buccafurri, F.; Fotia, L.; Lax, G. Social signature: Signing by tweeting. In Electronic government and the information systems perspective; Andrea Kő, Francesconi, E, Eds.; Springer International Publishing: Cham, Switzerland, 2014; pp. 1–14.
12. Buccafurri, F., Fotia, L., & Lax, G. (2015). A privacy-preserving e-participation framework allowing citizen opinion analysis. *Electronic Government, an International Journal, 11*, 185–206.
13. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access, 4*, 2292–2303.
14. Qu, C., Tao, M., & Yuan, R. A. (2018). Hypergraph-based Blockchain model and application in internet of things-enabled smart homes. *Sensors, 18*, 2784.
15. Dwivedi, A. D., Srivastava, G., Dhar, S., & Singh, R. (2019). A decentralized privacy-preserving healthcare blockchain for IoT. *Sensors, 19*, 326. https://doi.org/10.3390/s19020326.
16. Kumar, T., Ramani, V., Ahmad, I., Braeken, A., Harjula, E., & Ylianttila, M. Blockchain utilization in healthcare: Key requirements and challenges. In *2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom)*. 978–1–5386-4294-8/18/$31.00 ©2018 IEEE.
17. Irving, G., & Holden, J. (2016). How blockchain-timestamped protocols could improve the trustworthiness of medical science. *F1000Research, 5*.
18. He, W., Liu, X., Nguyen, H., Nahrstedt, K., & Abdelzaher, T. P. D. A. (2007, May 6–12). Privacy-preserving data aggregation in wireless sensor networks. In *Proceedings of the IEEE INFOCOM 2007—26th IEEE International Conference on Computer Communications, Anchorage, AK, USA* (pp. 2045–2053).
19. Li, N., Zhang, N., Das, S. K., & Thuraisingham, B. (2009). Privacy preservation in wireless sensor networks: A state-of-the-art survey. *Ad Hoc Networks, 7*, 1501–1514.
20. Li, M., Yu, S., Ren, K., & Lou, W. (2010). Securing personal health records in cloud computing: Patient- centric and fine-grained data access control in multi-owner settings. In S. Jajodia & J. Zhou (Eds.), *Security and Privacy in Communication Networks* (pp. 89–106). Berlin/Heidelberg, Germany: Springer Berlin Heidelberg.
21. Mandl, K. D., Markwell, D., MacDonald, R., Szolovits, P., & Kohane, I. S. (2001). Public standards and patients' control: How to keep electronic medical records accessible but private. *BMJ, 322*, 283–287.
22. Wu, J., Dong, M., Ota, K., Li, J., & Guan, Z. (2018). Big data analysis-based secure cluster management for optimized control plane in software-defined networks. *IEEE Transactions on Network and Service Management, 15*, 27–38.
23. Guo, L., Dong, M., Ota, K., Li, Q., Ye, T., Wu, J., & Li, J. (2017). A secure mechanism for big data collection in large scale internet of vehicle. *IEEE Internet of Things Journal, 4*, 601–610.
24. Wu, J., Ota, K., Dong, M., & Li, C. A. (2016). Hierarchical security framework for defending against sophisticated attacks on wireless sensor networks in smart cities. *IEEE Access, 4*, 416–424.
25. Dwivedi, A. D., Morawiecki, P., & Wójtowicz, S. (2018). Finding differential paths in ARX ciphers through nested Monte-Carlo search. *International Journal of Electronics and Telecommunications, 64*, 147–150.
26. Dwivedi, A. D., Morawiecki, P., Singh, R., & Dhar, S. (2018). Differential-linear and related key cryptanalysis of round-reduced scream. *Information Processing Letters, 136*, 5–8.
27. Dwivedi, A. D., & Srivastava, G. (2018). Differential cryptanalysis of round-reduced LEA. *IEEE Access*.
28. Dhar Dwivedi, A., Morawiecki, P., & Wójtowicz, S. (2017, July 24–26). Differential and Rotational Cryptanalysis of Round-reduced MORUS. In *Proceedings of the 14th International Joint Conference on e-Business and Telecommunications, Madrid, Spain* (pp. 275–284).

29. Dwivedi, A. D., Morawiecki, P. (2018). Differential Cryptanalysis in ARX Ciphers, Application to SPECK. Cryptology ePrint Archive: Report 2018/899. Retrieved January 9, 2019, from https://eprint.iacr.org/2018/899
30. Griggs, K. N., Ossipova, O., & Hayajneh, T. (2018). Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *Journal of Medical Systems, 42*(130). https://doi.org/10.1007/s10916-018-0982-x. , Corpus ID: 46969017.

Chapter 8
Blockchain Enterprise: Use Cases on Multiple Industries

T. Narayanaswamy, P. Karthika, and Kandappan Balasubramanian

8.1 Introduction

One of the biggest threats to transparency in the Indian government establishment is centralization of power and corruption within the system. Adopting blockchain technology can reduce corruption to a greater extent because it removes the need of middlemen [1]. Any centralized system or a process can be converted into a decentralized system using blockchain technology [1]. Wherever there are transactions including monetary between two persons/entities that lack trust among each other, blockchain technology facilitates smooth, fair transparency between them. This article explores key sectors where BCT can be very well applied to reap tangible benefits. Blockchain has been one of the most important innovations in the field of information technology for handling large volume of database in a seamless manner [2]. The commonly cited blockchain applications in the literature include cryptocurrency, financial transactions, and supply chain traceability of various business activities though it can be put to other uses. Moreover, the blockchain is used in combination with other technologies such as artificial intelligence (AI) and remote sensing technology (RST) for tracking various important parameters like temperature, time, weight, transactions, climatic conditions, compliance, human identity, quality, and other similar information. This kind of information is very vital to be tracked throughout the supply chain of any business organization ensuring

T. Narayanaswamy (✉)
School of Management Studies, REVA University, Bengaluru, Karnataka, India

P. Karthika
Department of Management Studies, Kongu Engineering College, Erode, Tamil Nadu, India

K. Balasubramanian
School of Hospitality, Tourism & Events, Faculty of Social Sciences & Leisure Management, Taylor's University, Selangor Darul Ehsan, Malaysia
e-mail: kandappan.balasubramanian@taylors.edu.my

H. L. Gururaj et al. (eds.), *Convergence of Internet of Things and Blockchain Technologies*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-76216-2_8

transparency, cost-effectiveness, and time effectiveness [3]. Many use cases/case studies on blockchain are found in the existing literature. Some of the interesting areas cited for use cases are insurance, document maintenance, food processing, fisheries, banking, and agriculture.

8.2 Use Cases in Insurance

Insurance Policy for Flight Delay: Fizzy. Fizzy is a blockchain technology that enables automated flight insurance policy facilitating customer to claim insurance in case of any delay of more than two hours in their flight arrival (the contents under this have been referred from AXA website content published in the year 2017 [4]). This system has brought a lot of benefits to the customer compared to traditional system (with which customers were facing a lot of difficulties in getting policy claims) of settling down claims. The benefits of fizzy are as follows:

- The policyholder is well aware of risks that are not covered under the insurance policy. This in turn leads to customer satisfaction.
- Customers will be able to know time of receiving insurance compensation/claims.
- The data such as proof of delay is automatically stored in the blockchain network. This in turn helps eliminate a cumbersome process of contacting the airline for providing proof of delay by the customer and sending to the insurer.

The working mechanism of fizzy blockchain (deployed by AXA) is shown in the Fig. 8.1. Flight delay insurance policy is fully automated with the help of blockchain called Ethereum that allows for compensating loss to the customers the

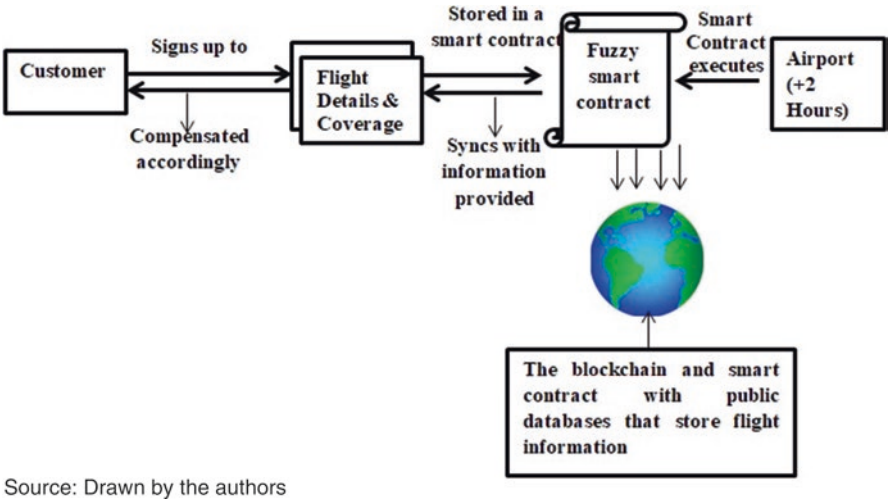


Fig. 8.1 Working mechanism process of fizzy blockchain for flight delay insurance policy

moment they reach their destination. This process has been fully automated, with the help of a smart contract which facilitates to check whether the customers are eligible for getting compensation claim due to delay. This clearly reveals that customers need not put any efforts to claim insurance for flight delay because of this automation process.

8.3 Use Cases in Agriculture

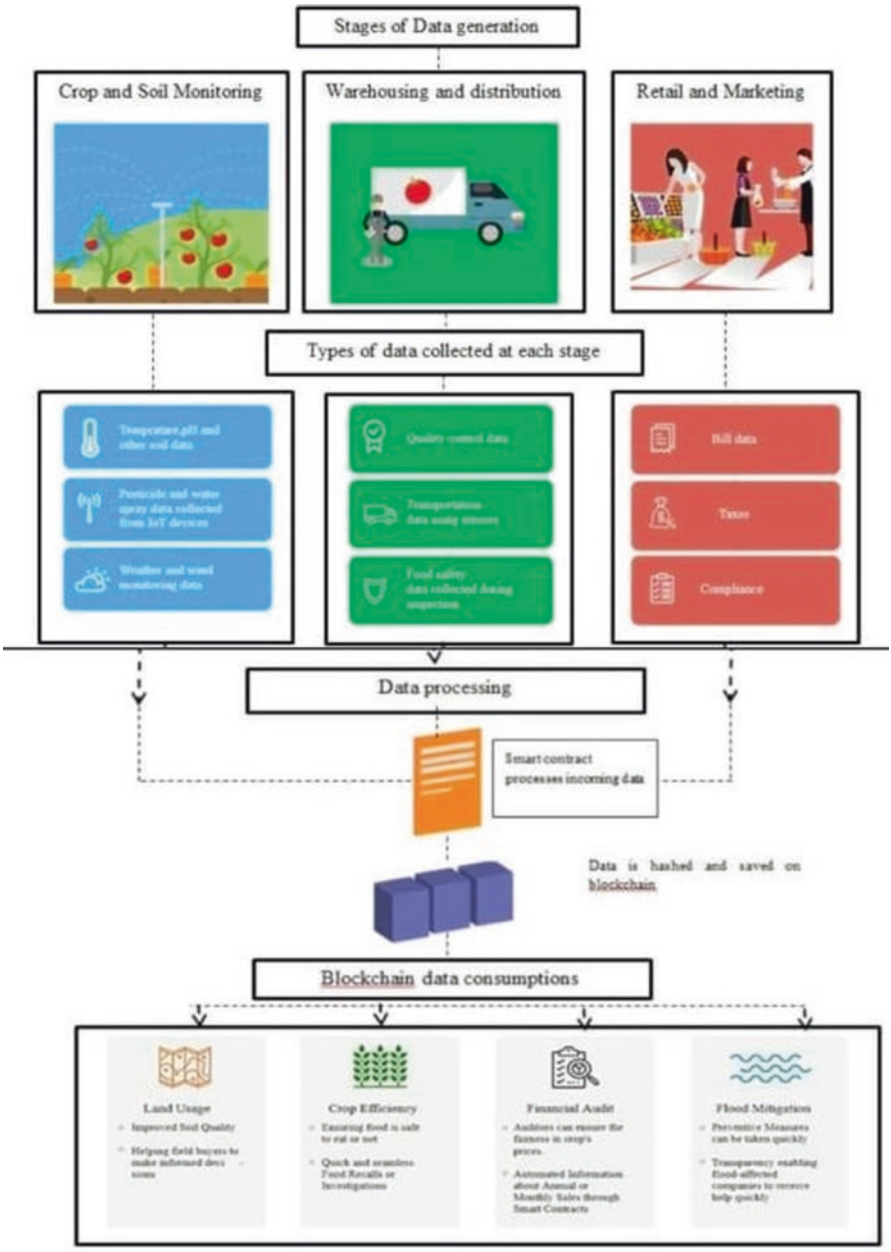
Millions of money is being invested by companies like IBM for creating precision agriculture by using Internet of Things which monitors agriculture-related factors such as the pests, soil quality, and irrigation that could greatly affect their crops. In Australia, blockchain is being used by some of the farmers for tracking their food production and reducing waste. The blockchain process is exhibited in Fig. 8.2 which is the basis for use cases discussed in this section [12].

8.3.1 Crop and Food Production

The growing population needs to be supplied by growing more food/crop with the use of minimizing resources. Agriculture should be carried out in such a way that it reduces the impact on the natural environment coping up with changing weather conditions. It is also important to ensure that the customer gets satisfied to a maximum possible extent by maintaining transparency across the supply chain as it guarantees reasonable income level to the farming community. Existing literature review discusses use cases based on blockchain combined with IoT and how blockchain technology will add value to the agriculture in different spheres such as generating, enriching, and saving the data which will help farmers to gather timely information about various things related to agriculture**.**

Effectiveness of blockchain to bring tremendous changes in the crop and food production is explained below.

IoT devices and sensors enable smart farming by keeping track of various data such as pH, soil moisture, temperature, humidity, and light in the crop field. This in turn helps the farmers to make informed decisions about the growth of crops. Information captured through IoT devices are initially structured and then stored. Data enrichment improves the quality of the collected/captured information. This involves two steps. Firstly, information such as demography, type, and time stamp is added for ensuring a structured data, and then, data collected through IoT is secured. Later, the data is well segregated/structured and then transformed into suitable machine-learning format. Insightful data is generated from these data by using machine-learning algorithms. For example, data pertaining to agricultural crops such as nature, type, yield, quality, and demand can be predicted accurately. Also, this data can also be made accessible to various parties in the agricultural supply



Source: Drawn by the authors

Fig. 8.2 Blockchain in agriculture

chain in a time and transparent manner which helps them to overcome the difficulties faced due to bottlenecks in the supply chain. The insightful data thus collected will be stored on a distributed storage platform on the blockchain. This information in turn will activate smart contracts depending upon the well-defined rules which are built into the blockchain system. This seamless information brings efficiency in crop/food production to various agricultural market participants.

8.3.2 Food Supply Chain Tracking

Food supply chain tracking helps in identifying the source of origination of food. It is important to make sure that supplied food products are safe to eat. With the advent of the blockchain, it becomes easy to develop trust and safety and ensure greater transparency in the supply chain of food and food products at all levels. The process of how blockchain enables food supply chain tracking is explained below:

- IoT sensors captures data as explained in the previous use case of food and crop production, or farmers can store data such as type of seed, crop quality, and weather conditions of cultivation using their mobile application.
- Once after the crops are ready for harvesting, food processing/manufacturing companies will use online bidding platform to complete price negotiations before purchasing them. Then, crops are taken to the refineries through IoT-enabled vehicles, which can track temperature-related parameters of items it carry.
- After validating the bids with the help of smart contracts, the crops are processed, and information captured about each step is stored on the blockchain. This information will enable wholesalers/retailers to confirm the quality of food being delivered. As the data stored blockchain is seamless, the compliance is monitored at every point in the food supply network.
- After the completion of food processing, wholesalers and retailers can bid through the bidding platform for the products they need. The food items are also distributed in the manner stated in step 2.

The consumers can look for the information such as source, transportation details, expiry date, storage temperature, and manufacturer details as they are digitally accessible using blockchain. This in turn helps consumers to know about the details of food products by tracing back to the supply chain.

The bidding architecture is shown in Fig. 8.3. The architecture comprises the following systems:

- Bidding parameters
- Create campaigns
- Serve ads
- Placement of bids
- Analysis of the outcome in terms of success or failure of the campaign
- Storage of bidding results

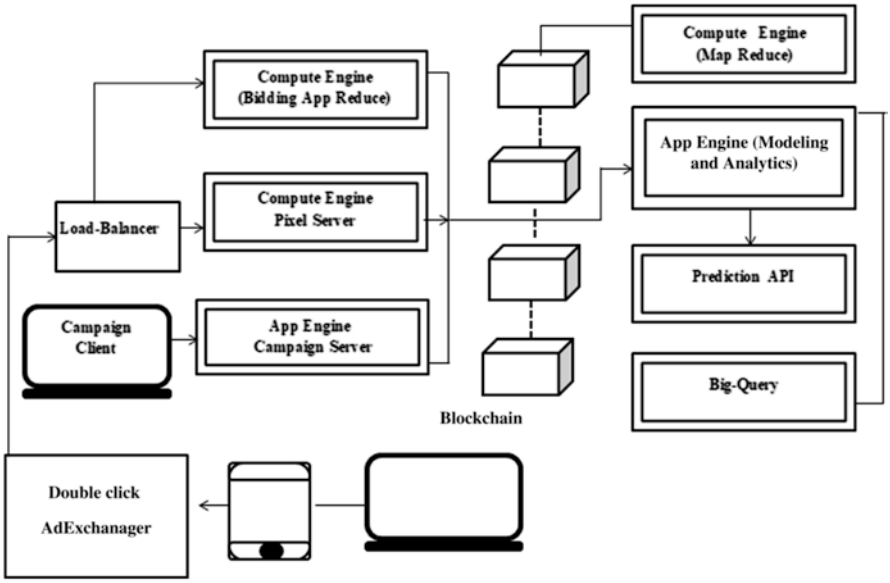


Fig. 8.3 Bidding platform architecture

The Google App Engine used for management of campaign has dashboards and facilities for reporting. Information about campaign is entered by various users of the bidding system, and the same will be stored in the blockchain ledger. When stakeholders access web content with the help of personal computer or any other related computer devices, request for placing advertisement gets activated either through Ad Exchange or DoubleClick. Load Balancer receives bid requests and sends the same to Bid Server for further examination, and accordingly, the bid is returned to compute engine. The ads can be stored directly in the blockchain, and the same would be available for retrieval at any time. Pixel Servers are used for fulfilling ad requests. Data on ads and campaign results can be thoroughly analyzed through data analytics tools and techniques to draw meaningful insights. Big Query is used for placing queries and loading necessary data to get insights about campaign's effectiveness. Prediction API facilitates incorporating machine-learning algorithms into the past information of bidding results that help stakeholders for making necessary improvements in the campaigns if required.

8.3.3 *Blockchain-Enabled Weather Control Process in Agriculture*

Smart agriculture helps farmers to understand the crop conditions with the use of (1) mapping fields and (2) sensors. Setting up weather stations within limits of agricultural farms will be helpful to generate key information such as rainfall, atmospheric pressure, solar radiation, and humidity. These parameters can be measured, recorded, and saved on the blockchain which in turn enables farmers and other stakeholders to access it in transparent manner and make better decisions related to farming. For example, farmers can initiate necessary actions/precautionary measures if needed, in case the data reveals the symptoms of heavy rainfall in the next few days. The blockchain also facilitates the farmers to apply for crop insurance without much delay in the event of damages to their crops during unfavorable climatic conditions such as heavy windfall and heavy rainfall. The insurance companies can also have access to the data captured through smart weather stations, and they can initiate smart contracts to process the claims on time. This in turn helps the farmers automatically receive the insurance claim amount directly in their bank accounts.

8.4 Blockchain Applications in the Financial Services Sector

Blockchain find its applications in various areas of financial services sector such as anti-money laundering (AML), trade surveillance, know your customer (KYC), settlements, and collateral management. During the period 2008–2012, bitcoin emerged, and cryptocurrency was used in place of cash-related transactions.

Later in the period 2012–2014, there was increase in bitcoin exchanges and startups dealings with bitcoins. Also in the same period, digital payment transactions were done using blockchain mechanism. In the year 2014–2015, venture capitalists and financial service firms started to invest in blockchain, and smart contracts emerged. In 2016–2017, manufacturing firms faced scalability issues which lead to more possible use cases in supply chain management, health care, and so on. Fintech firms speeded up their investment and develop a capability to operate through blockchain. From 2018 onward, efforts have been taken up in defining standards and protocols for using blockchain and also increase in initial coin offerings (ICOs), and privately held startups based on blockchain was observed.

Blockchain gained prominence during the year 2016. As per the National Association of Software and Service Companies (NASSCOM) data published in the business standard dated 27 July 2018, blockchain would create a value to the extent of 5 billion USD across all sectors. Blockchain is gaining momentum in the financial services sector across India in a way equal to other global counterparts. Numerous sector-related consortia are involved in the process of prototyping blockchain for different use cases. Besides banks, many insurance companies and a very few stock exchanges in India are also exploring the use of blockchain.

Since 2016, the following application areas have been in the top in terms of usage for providing financial services in India—viz., financing trade receivables, making payment between parties from different countries, discounting of bills receivable (B/R), digital identification of human beings, and supply chain financing.

With the increased use of Internet for financing, various online third-party payment platforms have paved the way for financial disintermediation. This in turn creates the need for the banks to minimize laborious process in providing banking services and also speed up the same. Though banks have adopted Internet technology to provide online banking services, the speed of Internet should be increased so as to handle large volume of transactions in a safe and secured manner [5]. Blockchain will be one-stop solution to overcome the problems in existing mode of delivering banking services because it can handle/store huge volumes of data in a decentralized manner and transmit the necessary data without tampering security features [6].

Blockchain technology can be used to monitor illegal/suspicious customers' monetary transactions on a real-time basis [7]. This means monetary transactions which pave the way for criminal activities such as terrorism, corruption, and smuggling can be traced effectively.

Blockchain technology is used to optimize the storage and retrieval of know your customer KYC) and financial transactions data pertaining to financial institutions [8]. The history of inflows and outflows of each of the financial transactions can be accessed at any point in time by means of using tamper-proof time stamp in the blockchain network. Then, the whole set of data and credit history of various participants associated with financial transactions are stored on every node in the blockchain, thereby ensuring information sharing on a timely basis happens.

The financial services industry is undergoing changes in terms of regulation, newly entering fintech firms, competition, and changing customer expectations. Also, minimizing frauds is one of major objectives in the sector.

Governments worldwide are differing in terms of using blockchain for various reasons. A few of the governments are very active in building a sustainable ecosystem for using blockchain technology. As per the World Economic Forum (2016–2017) [9] reports, 90 central banks and more than 30 governments are financing to building capabilities for using blockchain. The United States, Canada, China, and Australia are the countries where respective governments were able to set up blockchain hubs [10]. Next to these countries are Korea, Japan, Malta, Lichtenstein, and Gibraltar.

As per the World Economic Forum (Global Competitiveness Report 2016–2017) [9], worldwide usage and development of blockchain solutions are presented below:

- **European countries**—They had already set up European Blockchain Partnership for imitating the use of blockchain technology. More than 300 million euros would have been invested toward end of the year 2020.
- **Japan**—Blockchain-based platform for data sharing is announced for the trade industry.

- **United States**—Blockchain technology companies are allowed to issue exchange-traded funds via stock exchange.
- ***Switzerland***—Bitcoin is allowed to be used as a means for digital payment of up to 200 Swiss Francs.
- **Australia**—One of the stock exchanges in Australia has adopted the use of blockchain technology for clearing and settlement relating to buying and selling of securities.
- **South Korea**—Planned to invest more than 200 million USD by 2022.
- **Canada**—Permitted blockchain technology companies to issue exchange-traded funds on the stock exchange. Government utilizes blockchain technology for tracking and publishing information related to grant funding.

8.5 Blockchain Application Initiatives in India

The Indian government is exploring the use of blockchain technology in various areas listed below :

- Supply chain management
- Benefit distribution through various government schemes
- Land records
- Identity management
- Cross border finance
- Educational certificates
- Power distribution

Initiatives of the Indian government are underway for providing infrastructure that helps in building skills relating to blockchain, performing pilot testing in its internal systems, and developing interrelated platforms.

Andhra Pradesh in India has been the front-runner in pilot testing blockchain for its use in various areas of governance. As of now, two pilot tests have been done in the following areas:

- Maintenance and management of land documents/records for reducing property/asset-related disputes
- Vehicle registration process

As per the news article published in Business Standard in the year 2018, the Andhra Pradesh government had collaborated with a New York-based software company to build a sustainable ecosystem using blockchain. Chhattisgarh has successfully conducted its first Blockchain Challenge. For a period between 2016 and 2018, the IT nodal agency of Chhattisgarh, called as Chhattisgarh Infotech Promotion Society (CHiPS), had used blockchain technology for delivering proactive e-governance to their citizens [13]. A pilot test was also done in identity management by them in collaboration with experts in the year 2017. Similar projects

were also being initiated for land and e-health records maintenance in partnership with NITI Aayog [14].

8.5.1 Initiatives by NITI Aayog and IndiaChain Proof of Concept (PoC) Use Cases

NITI Aayog (based on the NITI Aayog report on blockchain in India published in January 2020) launched a blockchain project called IndiaChain, which is similar to Unified Payments Interface (UPI) project. This has an interoperable platform which supports for building scalable blockchain solutions. The objective of IndiaChain is to build a mechanism for minimizing, speed up enforcement of contracts, and ensure transparency [15].

NITI Aayog had pursued PoCs in four major areas to check the potential of blockchain technology for improved efficiency and attempt to understand possible obstacles during implementation. They are as follows:

- Tracking and tracing of drugs in the pharmaceutical supply chain
- Claim verification and approval for timely and transparent disbursal of fertilizer subsidy
- Certificate verification of university degrees
- Maintenance and transfer of land records

8.5.2 Fertilizer Subsidy Pilot Undertaken by NITI Aayog

For the fertilizer subsidy pilot undertaken by NITI Aayog, the major problem was reducing turnaround time to reimburse freight claims and subsidy payments. The existing process was burdened with inefficiencies as there are multiple systems of record, less visibility for inventory stocks, and less reliability of the data generated relating to subsidy and freight claims.

The Department of Fertilizers (DoF), India, issues fertilizers for agricultural purpose on subsidized rates. Subsidy amount is first paid to fertilizer producer once it completes the sales. Fertilizer subsidy occupies second place in terms of proportion of total amount of subsidy provided. Gujarat Narmada Valley Fertilisers & Chemicals (GNFC) is one of the largest fertilizer manufacturers selling across India. With large scalability and Presence Across Nation (PAN) India presence, GNFC is carrying out its operations through a large network of supply chain.

GNFC claims the subsidy in the following manner from DoF:

- **Subsidy claims:** GNFC claims subsidy based on the difference between the subsidized sales price and the cost of production of the fertilizer by showing sales record as an evidence for the sale of the product to the farmers. The sales record

is compiled from the retailers at point of sale (PoS) machines. Then, invoice generated is put in storage on GNFC's servers which uses an SAP-based system and is also made available on Integrated Fertilizer Management System (IFMS) of DoF on a real-time basis. To claim subsidy, invoices are compiled from GNFC-IFMS system on a weekly basis, authorized by statutory auditor before submitting to DoF.

- **Freight claims:** Freight claims are the charges incurred for transportation of fertilizers. Freight claims are produced by compiling the received quantity by the warehouses. After receiving fertilizer stock in the warehouse, zero claim subsidies are submitted to IFMS.

The consolidated freight claim data is sent to DoF on a monthly basis. Due to the presence of several unnecessary processes and inefficiencies in the form of paper-based systems and participation of multiple agencies, it takes 3–4 months for GNFC to receive subsidy, and also, it incurs substantial working capital cost.

The pain point/issue GNFC faced was the linking of final retail sales invoice with the challan prepared at the time of shipment leaving GNFC's factory. Besides, a unified system of record maintenance is required for the inventory/stock with all supply chain members who will take lead of GNFC. NITI Aayog collaborated with PwC and Intel and performed a pilot testing to optimize supply chain dealing with fertilizer subsidy distribution with the use of blockchain technology. The project is aimed at restructuring this supply chain by ensuring transparency and maintains tamper-proof records of ledger for tracking and tracing of fertilizer products throughout the value chain and speeds up subsidy payments by properly linking various transaction records.

8.5.3 Blockchain Use Case Application for Handling Fishery Supply Chain

Tsolakis et al. [11] conducted a case study research about the data accuracy issues in the fishing sector. The issues include incorrect number of registered vehicles which the vehicles which are not there in the port are used for illegal activities. Though the number of vessels used for local fishing facilities increases three times every year, 11–26 million tons of fishes caught are not all recorded anywhere. As logbook information about vessels is not shared on a real-time basis due to technical difficulties, 20% tolerance is acceptable on the amount of fishes caught. The author had proposed a supply chain that can be designed using blockchain to overcome the above-stated issues. A few of the recommendations by author to improve supply chain design in the fisheries sector are as follows:

- Creation of a decentralized database (blockchain) for gaining access to real-time data

- Use of onboard smart weighting system to ensure the weighting accuracy of fishes caught and thereby transfer the information about weight to the blockchain
- Implementation of e-logbook where catch data can be recorded on real time and made accessible to the government authorities

8.6 Conclusion

In this chapter, use cases of a blockchain enterprise have been presented more with reference to Indian context and less with reference to global context. A review of literature on blockchain applications in different sectors has been provided. This work can be extended to develop prototype of blockchain usage for solving many issues related to transparency and traceability. Several case studies can be conducted on blockchain by using the contents of this chapter. Agriculture being a backbone of Indian economy currently faces so many challenges with respect to climatic conditions and tracking them in supply chain. The blockchain application is still under the development stage with respect to agriculture. The application of blockchain in agriculture discussed here will help stakeholders to develop blockchain prototypes and implement them after thoroughly studying the pros and cons of the same.

References

1. Kapoor, R.(2020). *Blockchain technology – Some India use cases*. Retrieved from https://timestech.in/blockchain-technology-some-india-use-cases/
2. Abeyratne, S. A., & Monfared, R. P. (2016). Blockchain ready manufacturing supply chain using distributed ledger. *International Journal of Research in Engineering and Technology, 5*(9), 1–10.
3. Senyo, P. K., Liu, K., & Effah, J. (2019). Digital business ecosystem: Literature review and a framework for future research. *International Journal of Information Management, 47*, 52–64.
4. AXA goes blockchain with fizzy. (2017). Retrieved from https://www.axa.com/en/magazine/axa- goes-blockchain-with-fizzy
5. Chang, V., Baudier, P., Zhang, H., Xu, Q., Zhang, J., & Arami, M. (2020). How blockchain can impact financial services–the overview, challenges and recommendations from expert interviewees. *Technological Forecasting and Social Change, 158*, 120166.
6. Mu, Q. (2016). *Report on survey of blockchain technology: Potential to disrupt all industries*. Retrieved October 3, 2018, from https://www.chainnode.com/doc/415
7. Lai, K. (2018). Blockchain as AML tool: a work in progress. *International Financial Law Review*. Retrieved April 5, 2020, from https://www.iflr.com/Article/3804315/Blockchain-as-AML-tool-awork-in-progress.html.
8. Mashelkar, R. A. (2018). Exponential technology, industry 4.0 and future of jobs in India. *Review of Market Integration, 10*(2), 138–157.
9. The Global Competitiveness Report 2016–2017. Retrieved from https://www.weforum.org/reports/the-global-competitiveness-report-2016-2017-1. World Economic Forum report-2016, 2017
10. Where are the world's blockchain hubs actually located?, Cryptodisrupt, 15 July 2018.

11. Tsolakis, N., Niedenzu, D., Simonetto, M., Dora, M., & Kumar, M. (2020). Supply network design to address United Nations sustainable development goals: A case study of blockchain implementation in Thai fish industry. *Journal of Business Research*.
12. Blockchain in Agriculture – Improving Agricultural Techniques. Retrieved from https://www.leewayhertz.com/blockchain-in-agriculture/
13. Sharanya, H. (2018). This Indian City is embracing Blockchain Technology- Here's Why. Retrieved from https://www.forbes.com/sites/outofasia/2018/03/05/this-indian-city-is-embracing-blockchain-technology-heres-why/?sh=75656da18f56
14. Bhumika, K. (2018). Andhra Pradesh govt. signs MOU for blockchain innovation in the state. Retrieved from https://inc42.com/buzz/andhra-pradesh-govt-mouconsensys-blockchain/
15. Blockchain: The India Strategy-Part I. (2020). Retrieved from https://niti.gov.in/sites/default/files/2020-01/Blockchain_The_India_Strategy_Part_I.pdf

Chapter 9
Application of Blockchain Technology for 7/12 Asset Tracking System

Y. V. Parkale, M. D. Buchake, S. P. Gaikwad, and M. R. Gawade

9.1 Introduction

A blockchain is an emerging technology in the age of the Internet and is employed in different areas such as fintech, healthcare, finance, pharmaceuticals, insurance, and digital security. A blockchain is an emergent list of registers termed as blocks that are connected through cryptography.

The researcher Christidis et al. [1] concluded that blockchain technology and IoT are a powerful combination and result in significant transformation in industries. Moreover, it creates new distributed business models. The researchers Rangel and Kleinschmidt [2] proposed a consensus algorithm based on a blockchain architecture. This architecture cogitates data composed in the wellness and health ecosystem. The researcher Hasan et al. [3] proposed a blockchain-based solution for locating and following the spare part details from the manufacturer. The researchers Hinckeldeyn and Kreutzfeldt [4] proposed a smart storage container for supply chain uses founded on blockchain technology. The researcher Ren et al. [5] proposed an intelligent traffic system based on blockchain which enhances and optimizes the traffic system. The researcher Singla et al. [6] developed a leave management system based on blockchain. The researcher Kang et al. [7] proposed blockchain-based smart homes. The researcher Schmitt et al. [8] proposed the Hyperledger Fabric blockchain technology to an IoT network. The result demonstrates the improved security and privacy of IoT communication with smart contracts [9–25].

The various systems in the government offices to find legal property documents are very complex. The state-of-the-art system for document handling has many

Y. V. Parkale (✉) · M. D. Buchake · S. P. Gaikwad · M. R. Gawade
Department of Electronics and Telecommunication Engineering,
SVPM'S College of Engineering, Malegaon (Bk), Baramati, Maharashtra, India

H. L. Gururaj et al. (eds.), *Convergence of Internet of Things and Blockchain Technologies*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-76216-2_9

intermediaries, and due to this, trustless transaction is very difficult. Moreover, lawyers and third parties make frauds in the property selling and buying.

The solutions over the existing system are blockchain-based smart contracts. The blockchain innovation will supplant legal counselors and brokers. This framework is a decentralized framework that exists between totally allowed parties, there's no compelling reason to pay delegates, and it spares your time and clashes. Smart contracts help you exchange money, property, and shares in a transparent form and fraud-free and trustless way to avoid fraud.

In this chapter, we have proposed the 7/12 asset tracking system using blockchain technology. This system is developed to monitor, enhance, and develop secure, trustless, and fraud-free property document handling.

The chapter is coordinated as follows: Sect. 9.2 depicts the block diagram and working of the proposed system. Section 9.3 depicts the algorithm, flowchart, software used, circuit diagram, and Printed Circuit Board (PCB) layout implementation. Section 9.4 presents the conclusions.

9.2 Proposed System

This part presents the square chart of the proposed framework. Figure 9.1 shows the square chart of the proposed framework. The support of the presented framework is composed of the accompanying fundamental squares:

- Arduino Uno (Atmega) microcontroller
- 16×2 LCD display
- Fingerprint sensor

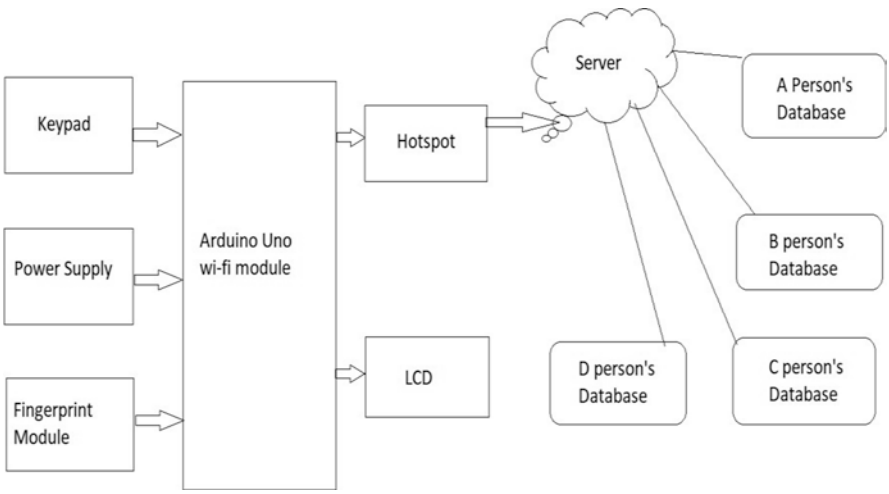


Fig. 9.1 Block diagram of the proposed system for 7/12 asset tracking using blockchain

- 4×4 matrix keypad

The details of each block are given as follows.

9.2.1 Arduino Uno (Atmega) Microcontroller

It is the heart of the system. It accepts the input from the 4×4 keypad and fingerprint module. Furthermore, it will perform the identification of the seller/buyer using the output of the fingerprint module and send the detailed information to the 16×2 LCD and the webserver.

9.2.2 16×2 LCD Display

All the information required about the property such as the name of seller/buyer and property details can be displayed using a 16×2 LCD display.

9.2.3 Fingerprint Sensor

The fingerprint sensor is used to fetch the image data and further send the data to the microcontroller. This module will store up to 162 fingerprints in the flash memory. Here, the fingerprint sensor is interfaced to the microcontroller through the serial protocol.

9.2.4 4×4 Matrix Keypad

This 16-button keypad gives a helpful human interface segment for microcontroller ventures. Advantageous cement backing gives a basic method to mount the keypad in an assortment of utilizations.

9.2.5 Working Principle

The proposed system creates a fraud-free blockchain-based property documents handling system. The data of actual documents are distributed on every user computer. The blockchain gives information from the origin. Also, while buying and selling the property, the third-party lawyers can be avoided. These results in the

saving of the number of fees paid toward the third-party lawyers. Additionally, for every buyer and seller, it's going to be a very trusted system. The proposed system uses a fingerprint sensor to check the property of the owner. The secret key is assigned to each seller/buyer so that whenever the user wants to sell and buy someone's property, they will get all the correct information about their property using the centralized system implemented in the government offices. The seller/buyer will get all correct information via SMS and call from the central authority, so he/she can trust anyone without getting lawyers in between.

9.3 Results

This section describes the algorithm and the flowchart of the proposed system. Furthermore, it presents the detail of the simulation software used, the circuit diagram, and the PCB layout of the proposed system.

9.3.1 Algorithm and Flowchart

This section describes the algorithm and flowchart of the proposed system. The different steps of the algorithm are as follows:

Start.
Initialize hardware; tap the fingerprint of the user.
Check whether the authentication is successful.
If yes, then check the distributed database on the server.
If no, then stop the process immediately.
Show information on display.
Stop.

Figure 9.2 describes the flowchart of the system.

9.3.2 Software Used

This section describes the different software used for programming the proposed system:

- **NodeMCU LUA:** The NodeMCU IDE is used to program the Wi-Fi module using the LUA programming language.
- **HTML editor:** The HTML editor is used to design the web page.
- **NetBeans IDE (PHP Website):** The NetBeans IDE is used to design the website for the server-side.
- **Arduino IDE:** It is used to program the Arduino microcontroller.
- **FileZilla Web client:** It is used for uploading our website to the server.

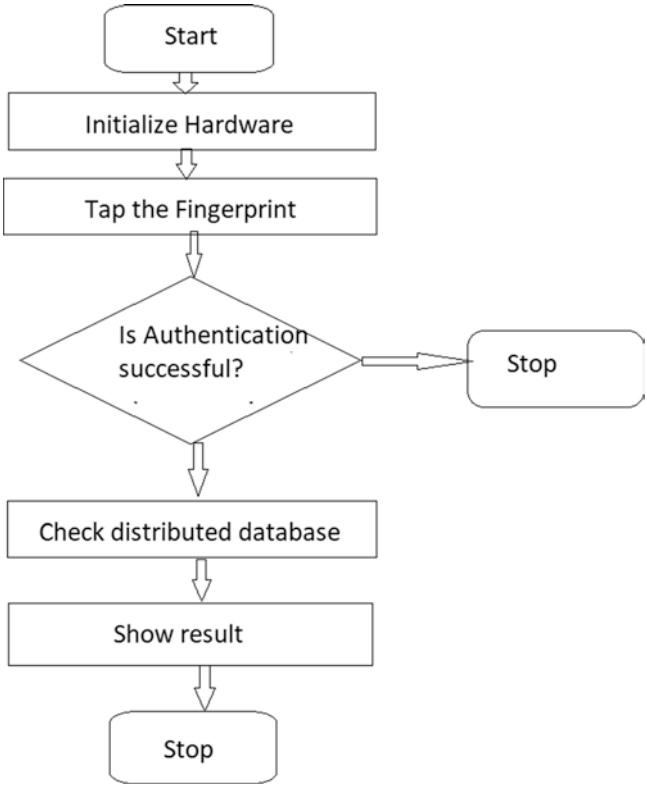


Fig. 9.2 Flowchart of the proposed system

9.3.3 Circuit Diagram and PCB Layout of the Proposed System

This part shows the circuit chart and the PCB format of the proposed framework. Figure 9.3 shows the circuit graph of the proposed framework. Further, Fig. 9.4 shows the PCB format of the proposed framework:

- **Inputs** keypad and fingerprint sensor.
- **Outputs** LCD and server.
- This fingerprint sensor module has four pins: (1) VCC, (2) GND, (3) TX, and (4) RX. The TX and RX pins are connected to the ATMEGA module.
- The LCD has VCC and GND pins that are connected to the A3 and A4 pins of the ATMEGA module.
- ESP8266 module to the SDA and SCL pins.
- The keypad is connected to the P0–P7 pins of the ATMEGA controller, respectively.

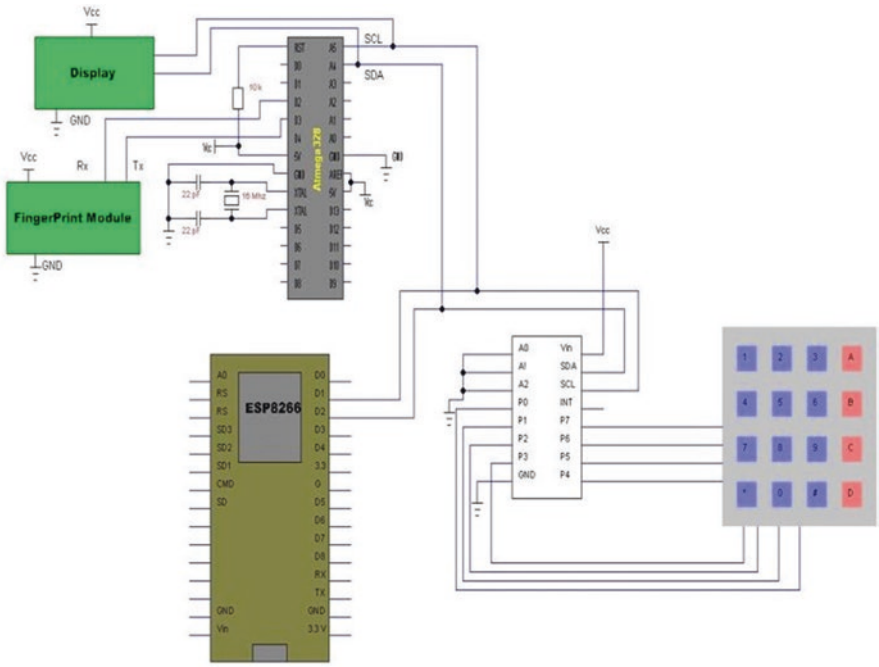


Fig. 9.3 Circuit diagram of the proposed system

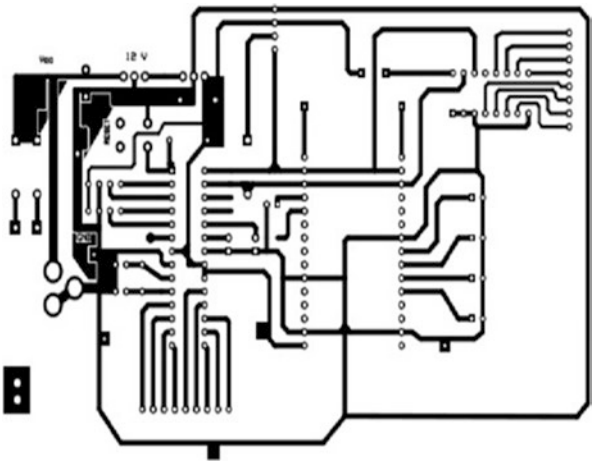


Fig. 9.4 PCB layout of the proposed system

9.4 Conclusion

In this chapter, we have proposed the 7/12 asset tracking system using blockchain technology. This system is developed to monitor, enhance, and develop secure, trustless, and fraud-free property document handling. In the state-of-the-art system, the dealing of legal property documents for buying and selling property is accomplished through the government offices. However, these systems result in various frauds due to the middle intermediaries and also have to pay for lawyers. In this work, we have proposed a secure system that provides distributed data on the computer of every customer. This will help to find the legal property papers and avoids the need for any third parties for property deals in between. The proposed 7/12 asset tracking using the blockchain is a promising advanced and more secure system that avoids frauds and makes a transparent deal. The proposed system has many advantages and applications in fintech, healthcare, finance, insurance, digital systems, security, and smart contracts.

References

1. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. *IEEE Access-Special Section on the Plethora of Research in the Internet of Things (IoT), 4*, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339.
2. Rangel, P., & Kleinschmidt, J. (2020). Sharing health and wellness data with blockchain and smart contracts. *IEEE Latin America Transactions, 18*(6), 1026–1033. https://doi.org/10.1109/TLA.2020.9099679.
3. Hasan, H. R., Salah, K., Jayaraman, R., Ahmad, R. W., Yaqoob, I., & Omar, M. (2016). Blockchain-based solution for the traceability of spare parts in manufacturing. *IEEE Access, 4*. https://doi.org/10.1109/ACCESS.2020.2998159.
4. Hinckeldeyn, J., & Kreutzfeldt, J. (2018). Developing a smart storage container for a blockchain-based supply chain application. *IEEE Computer society-Crypto Valley Conference on Blockchain Technology*, 97–100. https://doi.org/10.1109/CVCBT.2018.00017.
5. Ren, Q., Man, K. L., Li, M., & Gao, B. (2019). Using blockchain to enhance and optimize IoT based intelligent traffic system. *IEEE-International Conference on Platform Technology and Service (PlatCon)*. https://doi.org/10.1109/PlatCon.2019.8669412.
6. Singla, V., Malav, I. K., Kaur, J., & Kalra, S. (2019). Develop Leave Application using Blockchain Smart Contract. In *IEEE-11th International conference on Communication systems and network (COMSNET)* (pp. 547–529). https://doi.org/10.1109/COMSNETS.2019.8711422.
7. Ali, J., Ali, T., Musa, S., & Zahrani, A. (2018). Towards secure IoT communication with smart contracts in a blockchain infrastructure. (IJACSA). *International Journal of Advanced Computer Science and Applications, 09*(10). https://doi.org/10.14569/IJACSA.2018.091070.
8. Schmitt, G., Mladenow, A., Strauss, C., & Schaffhauser-Linzatti, M. (2019). Smart contracts and internet of things: A qualitative content analysis using the technology- organization-environment framework to identify key-determinants. *The 10th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2019) November 4–7, 2019, Coimbra, Portugal, ScienceDirect-Procedia Computer Science, 160*, 189–196. https://doi.org/10.1016/j.procs.2019.09.460.

9. Salman, T., Jain, R., & Gupta, L. (2019). A reputation management framework for knowledge-based and probabilistic blockchains. In *2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA*. https://doi.org/10.1109/Blockchain.2019.00078.
10. Malik, S., Dedeoglu, V., Kanhere, S. S., & Jurdak, R. (2019). TrustChain: Trust Management in Blockchain and IoT supported supply chains. In *2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA*. https://doi.org/10.1109/Blockchain.2019.00032.
11. Wan, L., Eyers, D., & Zhang, H. (2019). Evaluating the impact of network latency on the safety of Blockchain transactions. In *2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA*. https://doi.org/10.1109/Blockchain.2019.00033.
12. Homayoun, S., Dehghantanha, A., Parizi, R. M., & Choo, K.-K. R. (2019). A Blockchain-based framework for detecting malicious mobile applications in app stores. In *2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), Edmonton, AB, Canada*. https://doi.org/10.1109/CCECE.2019.8861782.
13. Wutthikarn, R., & Hui, Y. G. (2018). Prototype of blockchain in dental care service application based on Hyperledger composer in Hyperledger fabric framework. In *2018 22nd International Computer Science and Engineering Conference (ICSEC), Chiang Mai, Thailand*. https://doi.org/10.1109/ICSEC.2018.8712639.
14. Zheng, W., et al. (2019). NutBaaS: A blockchain-as-a-service platform. *IEEE Access, 7*, 134422–134433. https://doi.org/10.1109/ACCESS.2019.2941905.
15. Linoy, S., et al. (2019). Scalable privacy-preserving query processing over Ethereum Blockchain. *2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA*. https://doi.org/10.1109/Blockchain.2019.00061.
16. Wang, R., et al. (2018). A privacy-aware PKI system based on permissioned blockchains. In *2018 IEEE 9th International Conference on Software Engineering and Service Science (ICSESS), Beijing, China*. https://doi.org/10.1109/ICSESS.2018.8663738.
17. Taş, R., & Tanrıover, O. O. (2019). Building a decentralized application on the Ethereum Blockchain. In *2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Ankara, Turkey*. https://doi.org/10.1109/ISMSIT.2019.8932806.
18. Fitwi, A., Chen, Y., & Zhu, S. (2019). A lightweight blockchain-based privacy protection for smart surveillance at the edge. In *2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA*. https://doi.org/10.1109/Blockchain.2019.00080.
19. Seol, Y., et al. (2019). Query-chain: Fast and flexible blockchain-based platform for diverse application services. In *2019 International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Korea*. https://doi.org/10.1109/ICTC46691.2019.8939801.
20. Wang, S., et al. (2019). A novel Blockchain Oracle implementation scheme based on application specific knowledge engines. In *2019 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), Zhengzhou, China*. https://doi.org/10.1109/SOLI48380.2019.8955107.
21. Suriya Praba Devi, G., & Miraclin Joyce Pamila, J. C. (2019). Accident alert system application using a privacy-preserving Blockchain-based incentive mechanism. In *2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), Coimbatore, India*. https://doi.org/10.1109/ICACCS.2019.8728507.
22. Niya, S. R., et al. (2019). A platform-independent, generic-purpose, and blockchain-based supply chain tracking. In *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Korea*. https://doi.org/10.1109/BLOC.2019.8751415.
23. Ehmke, C., Wessling, F., & Friedrich, C. M. (2018). Proof-of-property - a lightweight and scalable Blockchain protocol. In *2018 IEEE/ACM 1st International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB), Gothenburg, Sweden*.

24. Shudo, K., Kanda, R., & Saito, K. (2018). Towards application portability on blockchains. In *2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), Shenzhen, China*. https://doi.org/10.1109/HOTICN.2018.8605977.
25. Gong, X., Liu, E., & Wang, R. (2020). Blockchain-based IoT application using smart contracts: Case study of M2M autonomous trading. In *2020 5th International Conference on Computer and Communication Systems (ICCCS), Shanghai, China*. https://doi.org/10.1109/ICCCS49078.2020.9118549.

Chapter 10
Blockchain Technology for Property Sales and Registration

Shrayas Ranjan Sinha, H. S. Madhusudhan, N. Mahima Pai, Saloni Jain, K. Ujwal, and Hong Lin

10.1 Introduction

Land is not only an important asset but also unique as it is not movable and its value depends on its location. Since the population is growing continuously, its demand is also increasing continuously although the supply remains constant. The access to land has a great effect on the place where it is present and the work that is going on there like malls and schools. Land registration is always a problem for the people of India as there are a lot of government procedures. It also results in the corruption from people like brokers. Majority of people in India are not aware of the land laws due to which a lot of corruptions such as fake registration happen. Some stringent actions should be taken as to improve trust, immutability [1], and transparency. That's where blockchain eradicates all such problems. It not only solves the problem of trust and immutability but also the secure transfer of money. Smart contract is the key for all the trust operations.

Now, many people fear fake land certificates which are used by the fraudsters to fool the buyers. The fraudsters are actually taking advantage of old and poor management of land records. Often, such disputes have dragged the people to the court for the required settlement. It is also a surprise to know that such cases of land frauds are actually covering 66% of the total cases pending in the court. Also, after so many hardships, it is not evident that justice is served because in many cases it is seen that the police are actually humiliating the innocent people who become the victims of land frauds.

S. R. Sinha · H. S. Madhusudhan (✉) · N. Mahima Pai · S. Jain · K. Ujwal
Department of Computer Science and Engineering, NIE Institute of Technology, Mysuru, Karnataka, India

H. Lin
Department of Computer Science, University of Houston, Houston, TX, USA
e-mail: linh@uhd.edu

H. L. Gururaj et al. (eds.), *Convergence of Internet of Things and Blockchain Technologies*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-76216-2_10

So now, we can realize the seriousness of the matter which is horrifying and shocking. But it can be improved if we use the current technologies of present time in which we are living in. The technology of blockchain will be the first choice to deal with this wherein it helps in keeping the land records safe and organized. It will demolish the old and ineffective methods of storing the records. The other benefits are it will fast-track the pending cases related to land disputes. Therefore, it will ensure that justice is served. At the same time, money and energy of the victims and the court will be saved.

10.2 Literature Survey

Blockchain technology has impressed the real estate market in several ways by introducing a new means for buyers and sellers to connect with each other. The need of brokers and intermediate people may lead to various kinds of mistakes while auditing [25]. That's where blockchain comes in scene to remove all such problems; also, it will reduce the cost. As blockchain is not centralized, it is very difficult to tamper with the data. Blockchain uses consensus algorithm [2] such as proof of work (POW), proof of stack (POS), and proof of burn (POB) [3]. The recent study shows that an advanced approach was used to expose land scams, property holdings, and pending cases of court. The actual purpose was to digitalize all the land records and poor maintenance of land record. The proposed method can be framed like "land" which is an important asset for the people will be registering through a distributed ledger (DLT) [4] and the agreement will be done through a set of software which is known as smart contact [5]. It will be executed, and all the negotiating terms and agreement will be present in it [6].

If we talk about the implementation of blockchain, it is seen in a recent survey that Sri Lanka [7] is using a decentralized ledger that is based on blockchain. It helps to provide a better way of managing the records instead of using the handwritten records. If this technology is adopted, then it will reduce the loopholes to a great extent. It will outsmart all the existing methods which are old and inefficient. In this, the records and assets are handled by linking them to a fundamental cryptocurrency [8].

Blockchain removes third-party access with the help of smart contracts concept with multiple gain which also involves a secure price token for every safe asset in RE market. If it is applied properly, then it will eliminate all types of frauds and will strengthen process integrity and network reliability [9]. Thus, smart contracts will also pave the way for many rising industries like Internet of Things (IoT) and financial management [10].

Blockchain also helps in reducing the corruption in many countries [11]. In this, the transactions are kept transparent and available to the public, thereby reducing the chances of modification by unwanted users. There are many other features of blockchain for creating a democratic, automatic, transparent, decentralized, and secure environments. By adopting all these features, we can improve smart city services too [12].

Ethereum offers smart contract [13] functionalities which is based on distributed computing platform. In order to execute smart contract, it requires a decentralized virtual machine to function in a runtime environment for creating Ethereum network. Its main aim is to create an alternative method for creating a decentralized application. It has a built-in Turing machine which allows the programmers to create a set of rules for the smart contract as well as the dApps. A special type of protocol which is known as WalliD is implemented so as to operate smart contract logic and to deal with digital certified and global trusted identities which results in the feature of transparency, decentralized networks privacy, and immutability [14].

10.3 Methodology

Land registration and sales using blockchain have been explored in this section. Blockchain is a prominent technology, and because of its strength in providing security, it has the ability to outclass the existing real estate management which uses the traditional centralized structure. Figure 10.1 describes about the functioning of our work in a simplified way.

The real estate and property systems are dependent on centralized registries of the countries to handle ownership, sales, and land locations. The Catasto (Italian system of land registration) of Italy handles properties ownership [15], and the notary handles the regulations. In the United Kingdom, HM Land Registry manages properties, and the seller responsible for the contracts for sale does not need a third-party interference [16]. An agency in the United States deals with the contracts, while a notary verifies the signature deal [17].

Blockchain introduction into real estate system can transform the roles of various notaries, financial support real estate agencies, and all other intermediaries existing in the current method or system.

10.4 Overview

The different processes involved in property sales and registration using blockchain technology are as follows:

- Decentralized application
- Smart contracts
- Wallets
- Accounts
- Byte code
- Truffle

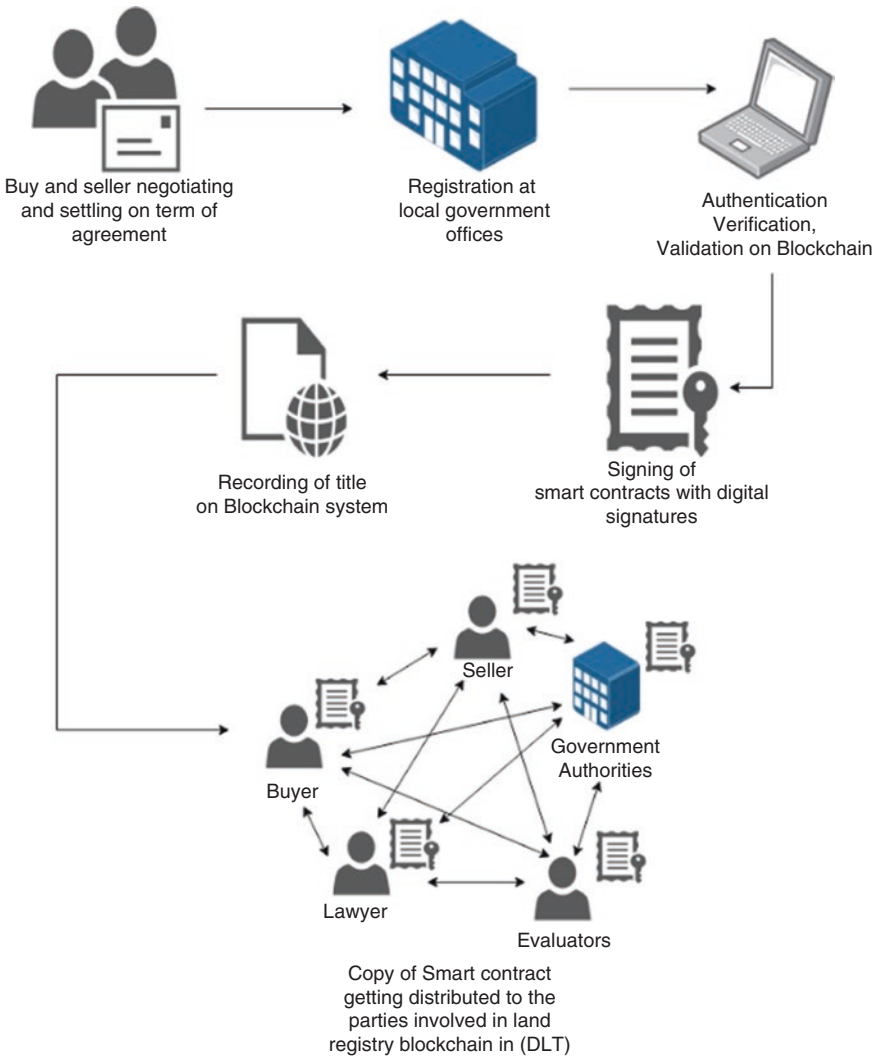


Fig. 10.1 Working mechanism

10.4.1 Decentralized Application

A decentralized application falls under application program category that follows peer-to-peer architecture in which application runs on network of nodes rather than a server or a single system. In peer-to-peer network, two or more systems are connected and share their resources without the need of a dedicated servers. A blockchain-aided website "dApps" provides smart contracts that can be used in blockchain which will be a replacement of traditional API connections. In

traditional websites, API calls are used to transfer data and use database to store the data, whereas in dApps, smart contracts are used to transfer data and a blockchain to store the data. Centralized applications use the dedicated server to run the back-end code, but dApps uses peer-to-peer network to run the code. Ganache is used for simulation and testing which offers blockchain for development of Ethereum in our personal system. Ganache is used to build applications, deploy application, and run tests on personal/local system. To deploy dApps network on local network, all essential requirements like Node.js [18], terminal, and Ganache need to be contended.

10.4.2 Smart Contracts

Crypto-contracts, also known as smart contracts, were introduced in the year 1994 by a computer scientist Mr. Nick Szabo, who invented virtual currency "Bit Gold" in the year 1998, 10 years earlier Bitcoin was announced [19, 20]. Smart contract is a set of codes which are self-executing and contains information regarding terms of agreement that exist between parties who are present in the contract. Blockchain network which is distributed and decentralized approach comprises the agreements and code. Smart contract is a self-executing component which will generate output after execution only if the set of predefined rules are satisfied. The decentralized automation is achieved through the code by enforcing and verifying the condition provided in an agreement. Anonymous parties can carry out trusted transactions and agreements among themselves without need of legal system or central authority. This permits smart contract to exchange money, property, shares, and so on in a very transparent mode and keep the system conflict-free. Smart contracts are transparent, irreversible, and traceable.

10.4.3 Wallets

To manage and store Ethereum accounts, Ethereum wallets are being used. They are the libraries or plugins to manage accounts. Two types of wallets are deterministic and nondeterministic wallets. In nondeterministic, public keys are generated using the given private key. There is no limitation on number of private keys that will be generated; nevertheless, relation between each pair of keys exists. In deterministic, serialized phrases called seeds which are human readable are used to generate key from a solitary starting point. Seeds let the user to generate public address without the awareness of the private key and allow the user to restore and backup their wallet.

10.4.4 Accounts

For each and every account, Ethereum blockchain [21] uses private and public keys. Public keys are visible to everyone and private keys should be kept secret. Private key represents the password for account funds. Ethereum ecosystem is composed of two types of accounts. First account is the externally owned account (EOA) which is the combination of private and public keys. This account is used to send or receive "ether" to/from another account or deliver transactions to smart contracts. In the second type of account, contract account doesn't have a corresponding private key. Here, accounts get generated after the smart contract is deployed to blockchain. Using these accounts, ether can be sent or received, and they have code linked with them unlike EOA. Only smart contracts or EOA can trigger the transactions. Figure 10.3 represents one of the ways of getting key required for transactions.

10.4.5 Byte Code

High-level programming languages like Solidity are used to create smart contract. While directing the smart contract to blockchain, smart contracts are compiled to get Etherium Virtual Machine (EVM) byte code [22]. The advantage of such conversion is that it lets the developer to adapt some other programming languages to go for implementation of smart contracts such as Pyramid Scheme, Vyper, LLL, HAssembly-evm, and Flint.

10.4.6 Truffle

Truffle is one of the frameworks used in Ethereum network. Even Embark is another framework the Ethereum can make use of. Truffle is generally used by Ethereum network developers. Truffle provides an abstract way of compiling and deploying smart contracts to blockchain. Truffle makes these tasks easier and also provides tools and testing frameworks to test contracts [23]. Figure 10.2 gives the overview of the blockchain system.

10.5 Practical Approach

10.5.1 dApps Smart Contracts

Ethereum blockchain supports numerous smart contract languages such as Vyper, and Solidity. In this work, Solidity smart contract is used which is most widely popular and properly documented. A smart contract entitled PropertyRegistration.

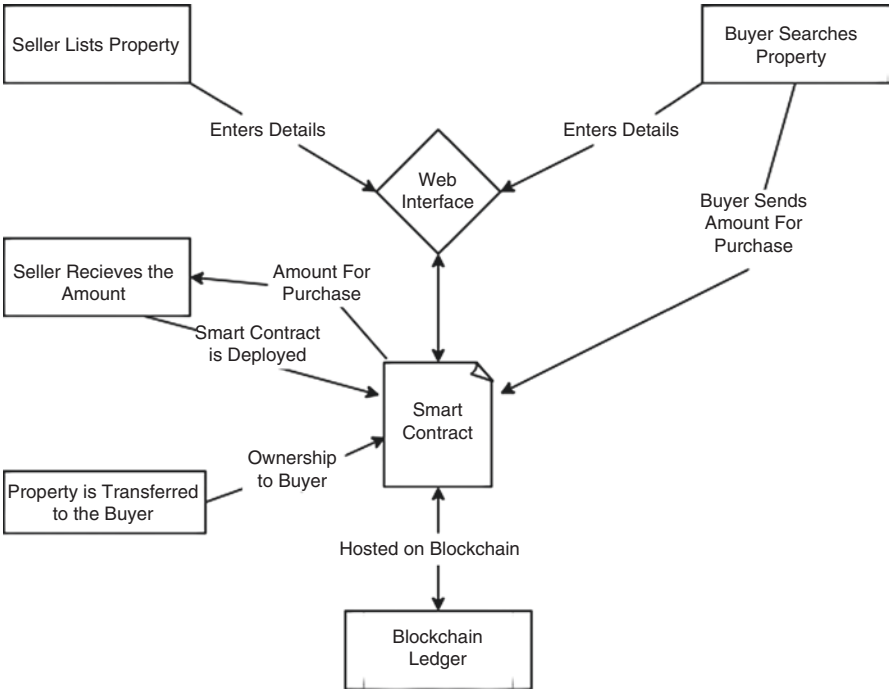


Fig. 10.2 Overview of the blockchain system

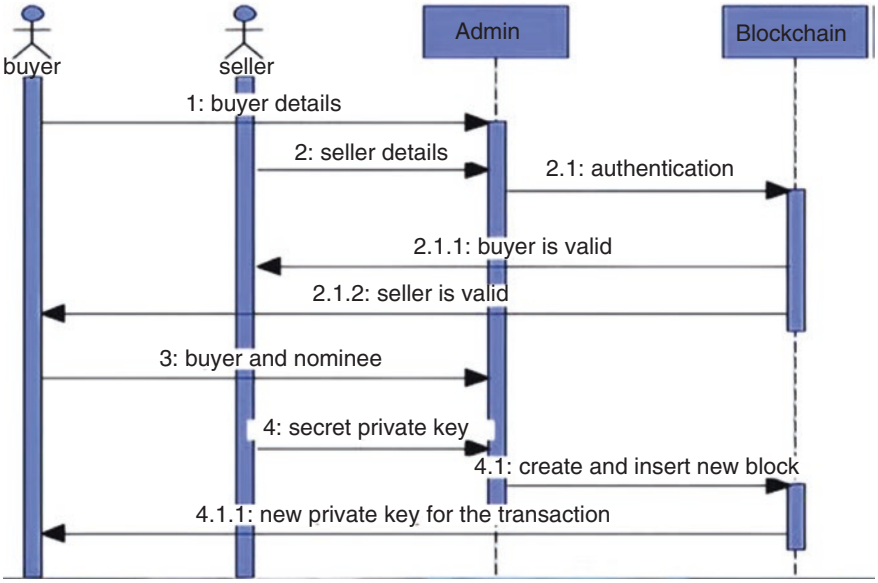


Fig. 10.3 Sequence diagram of the working

sol is formed. Solidity is a statically typed language. A unique type of data known as address is defined by Solidity. This address occupies 20 bytes in the storage. An address may belong to smart contract or to an account. Figure 10.3 gives the sequence diagram of the working of the dApps smart contract approach.

10.5.2 Comparative Analysis

Table 10.1 shows comparative analysis of different blockchain platforms. Analysis is performed on the basis of data scalability, data structure elasticity, and transactions per second (TPS) [3]. Though other platform like Hyperledger (HL) is promising, we have chosen Ethereum in our work since we are creating our own cryptocurrency.

10.5.3 Deployment

In the terminal, command "truffle compile" is executed, which compiles Solidity to byte code for EVM, after which a new migration script deploy_contracts.js is created in migrations directory, which is used to migrate compiled contract to the blockchain:

```
 pragma solidity ^0.4.24;
 contract Migrations {address public owner; uint public last_com-
pleted_migration; modifier restricted () {
 if (msg. sender == owner)
 }
 constructor () public {owner = msg. sender;
 }
 function setCompleted (uint completed) public restricted
 {last_completed_migration = completed;
 }
  function upgrade (address new_address) public restricted {
Migrations upgraded = Migrations(new_address); upgraded.
setCompleted(last_completed_migration);
 }
 }
```

Truffle defines a migration as a deployment script meant to move application's smart contracts from one state to another. Before we can run migration, we need to have blockchain running in our local machine. For this, we use Ganache, and by default, blockchain will be running on our identified port. Now, we can run "truffle migrate" in our terminal to migrate contract to the blockchain.

Table 10.1 Comparative analysis of blockchain platforms

Platform criteria	Bitcoin		Ethereum		HL		EOS	
Data structure elasticity	3	27	3	27	9	81	6	54
TPS	4.6		15		3500		50,000	
Data scalability	3	27	3	27	6	54	6	54

10.5.4 Front End

A group of libraries called Web3.min.js is used in this work, which enables the interaction with remote Ethereum node or local system. To retrieve user accounts and transfer transactions, it interacts with smart contract, and the Web3 function is used as shown in the algorithm. Here, MetaMask is used wherein Ethereum provider is added to the window object. Then, Web3 object will be created, and also, request access to the account will be done through ethereum.enable(). If no Ethereum object is present, then inject Web3 instance will be checked. Then, the corresponding provider is used to create the object; Web3 objects are created using Ganache in local system. Figure 10.4 shows how Web3 is used at both client end and in blockchain network.

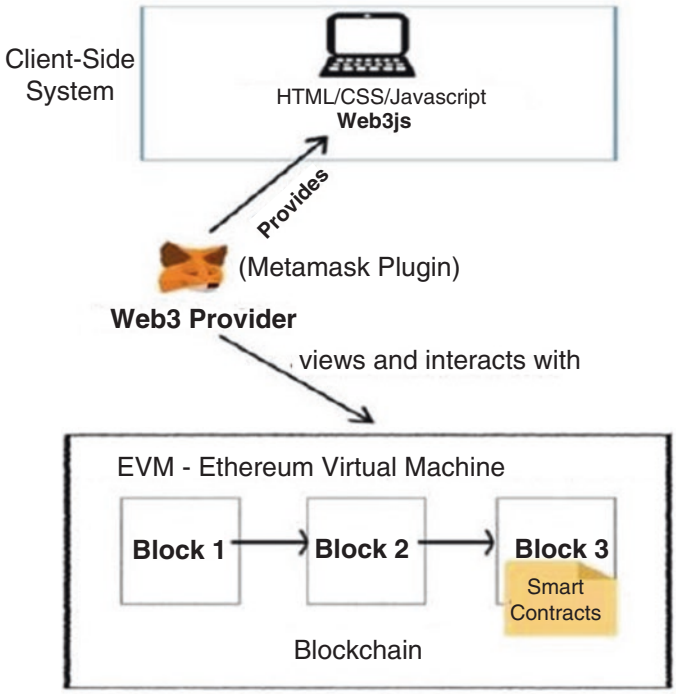


Fig. 10.4 Web provider

10.5.5 Overall Working

Figure 10.5 shows the working of blockchain ledger. Property owners and buyers are being handled by web application. Administrative work like checking and validating data would also be taken care through the web application. Web interface provides the provision to manage the actors of real estate like seller, buyer, admin, and their input and output of the transaction. The blockchain used here would store all necessary details or data, and administrator has the provision of monitoring this regularly. The exchange of monetary funds or contract deployments between seller and buyer is recorded in the chain which acts as a proof in blockchain ledger. Figure 10.5 reflects the idea of the use case scenario of our proposed work with the involvement of all the actors present in it. The use case diagram describes how a system interacts with outside actors; each use case represents a piece of functionality that a system provides to its users.

Figure 10.6 describes the layered approach of proposed system. This means that all the components are interconnected but do not depend on each other. Figure 10.7 describes the process flow of our work where buyer and seller are involved in the process of transactions but the admin which is the government in this case monitors everything as member of blockchain. Finally, after ownership verification and ownership recording in the Ethereum blockchain network, the transaction is made between the parties though the government-verified cryptocurrency (ether) in this case.

The following algorithm defines the approach followed for property sales and registration. Firstly, user registration is done and then property registration takes

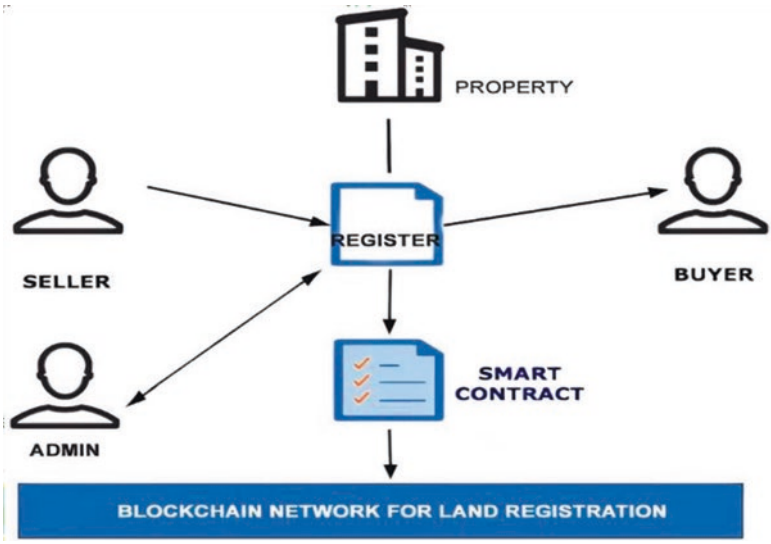


Fig. 10.5 Use case diagram of our proposed work

place. Both are validated. In the next step, any user can search for existing property for sale and get the details. All the actions of the user will be recorder in blockchain ledger. Validation of property can be done through the special code or identification number associated with it.

Algorithm

The approach taken in PropertyRegistration.sol

Input: User action

Output: action decisions

```
1 Procedure Registeruser()
2    if user already exists then
3       return user already exists
4    else
5       Register new user
6 Procedure RegisterProperty()
7    if property already registered then
8       return property already registered
9    else
10      Register new property
11 Procedure SearchProperty()
12    if Property exists then
13      return property details
14    else
15      return invalid property_id
16 Procedure TransferProperty()
17    if property exists
18      if owner.userID = _sellerID
19           string memory _transactionID <- strConcat(strConcat(uint2str(_propertyID), "."),
uint2str  (_property.prevOwners.length+2))
20          _property.currOwner <- Owner(_transactionID, _buyerID, _time, _amount)
21           properties[_propertyID] <- _property
22           Transfer Property
23 Procedure uint2str()
23    bytes memory bstr <- new bytes(length)
24    uint k <- length - 1
```

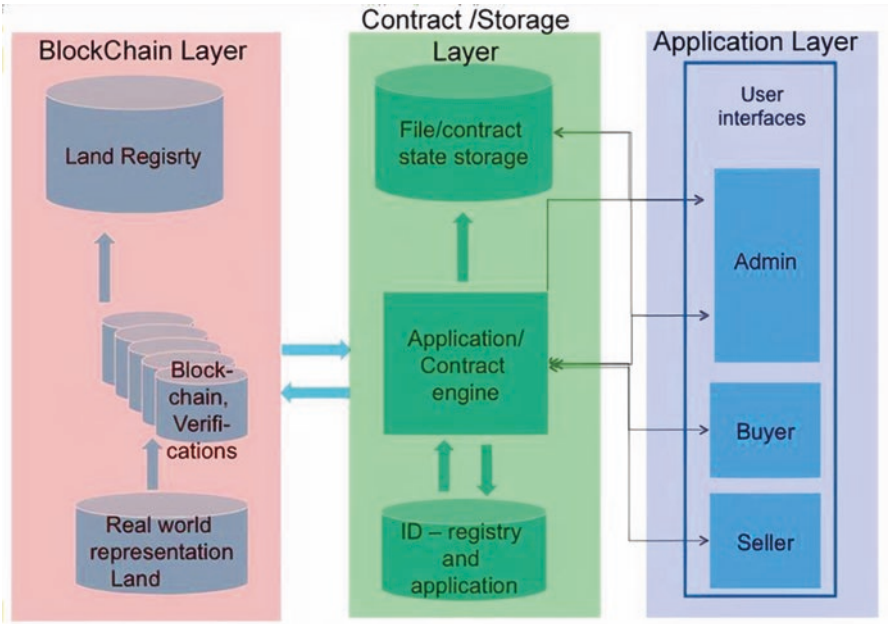


Fig. 10.6 Layered architecture of proposed system

10.6 Experimental Results and Discussion

Property sales and registration using blockchain proposed in this work start with proper compilation and migration (as discussed in the previous section).

Once migration is successful, the migrations will be deployed, and then, migrations along with artifacts are added to the chain. After successful deployment, browser-sync configuration is started to synchronize the contracts constructed to the browser to create interface, and MetaMask is used as plugin for wallets and its accounts.

To begin with, land owner should be registered as a new user to the application with the details and the identity proof along with username and password of their choice. After registration is successful, ETH is used (via MetaMask wallet), and this gets registered in blockchain ledger. Web interface is used for registration of real estate property. To register a property, all the necessary information like property owner details, username, and password should be submitted through interface. Here, MetaMask is used, and smart contract is created for the property or the land that is available for sale.

Any user who registers for the application can search for the property available using the web interface and choose a property the user is willing to purchase. To purchase the property, buyer uses cryptocurrency to send amount to the owner using owner address, and then, the buyer will be made as the new owner of the property.

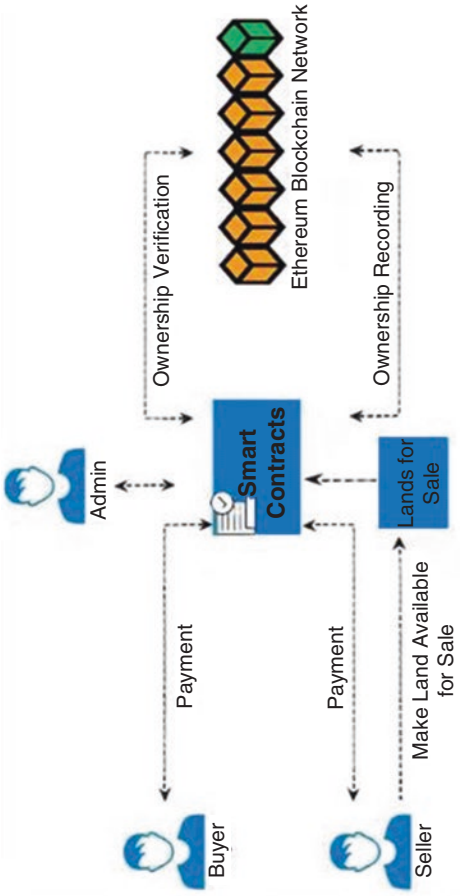


Fig. 10.7 Process flow diagram of our work

This process is done though deploying smart contract. Finally, the data regarding this transaction is saved in blockchain ledger, and the data cannot be tampered.

10.6.1 Involvement of Cryptocurrency

In our work, we have used our own cryptocurrency, which leads to secure transaction, and also, it is safe. In this work, Ethereum test network is used for demonstration and testing purpose which is achieved though MetaMask. This process resolves trust issues, and also, international transaction will be easier. In general, government will use their own cryptocurrency.

10.6.2 Is it Secure?

Some of the attacks like Distributed Denial-of-Service (DDOS) attack, Sybil attack, and 51% attack [10] are possible, yet it is not that fruitful as it is expected [24].

10.7 Conclusion

In this work, the blockchain technology is applied for the real estate domain which transforms the traditional on-paper work to the digitized registry process and also secures different operations such as purchase, sale, lease management, transaction, and financing. The approach proposed in this work uses Ethereum to perform operations which not only enhances security but also brings confidence in buyers. The solution will also increase authenticity of the land records.

References

1. https://security.cse.iitk.ac.in/sites/default/files/14807257.pdf by Gunda Abhishek
2. Fu, X., Wang, H., & Wang, Z. (2020). Research on block-chain-based intelligent transaction and collaborative scheduling strategies for large grid. *IEEE*, 151866–151877.
3. Kamkar, R., Adak, S., Arsheekhan, P. P., & Sampath, A. K. (2019). Land registry using blockchain. *IJSRD, 6*(11), 636–639.
4. Teja, J. R. (2020). Proposing method for public record maintenance using block chain. In *2020 International Conference on Mainstreaming Block Chain Implementation (ICOMBI), IEEE, Bengaluru, India* (pp. 1–5).
5. Liu, S., & He, S. (2019). Application of block chaining technology in finance and accounting field. In *2019 International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS), IEEE, Changsha, China* (pp. 342–344).

6. Saranya, A., & Mythili, R. (2019). A survey on blockchain based smart applications. *International Journal of Science and Research (IJSR), 8*(1), 450–455.
7. Yapa, I., Heanthenna, S., Bandara, N., Prasad, I., & Mallawarachchi, Y. (2018). Decentralized ledger for land and property transactions in Sri Lanka acresense. In *2018 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), IEEE, Malambe, Sri Lanka* (pp. 1–6).
8. Lemieux, V. L. (2017). A typology of blockchain recordkeeping solutions and some reflections on their implications for the future of archival preservation. In *2017 IEEE International Conference on Big Data (Big Data), IEEE, Boston, MA* (pp. 2271–2278).
9. Kan, L., Wei, Y., Muhammad, A. H., 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), IEEE, Lisbon, Portugal* (pp. 139–145).
10. Abbas, Q. E., & Sung-Bong, J. (2019). A survey of blockchain and its applications. In *2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), IEEE, Okinawa, Japan* (pp. 001–003).
11. Kshetri, N., & Voas, J. (2018). Blockchain in developing countries. *It Professional*, 11–14.
12. Xie, J., Tang, H., Huang, T., Yu, F. R., Xie, R., Liu, J., & Liu, Y. (2019). A survey of blockchain technology applied to smart cities: Research issues and challenges. *IEEE Communications Surveys & Tutorials, 21*, 2794–2830.
13. Mertz, L. (2018). (Block) chain reaction: A blockchain revolution sweeps into health care, offering the possibility for a much-needed data solution. *IEEE Pulse, 9*(3), 4–7.
14. Tavares, M., Guerreiro, A., Coutinho, C., Veiga, F., & Campos, A. (2018). WalliD: Secure your ID in an ethereum wallet. In *2018 International Conference on Intelligent Systems (IS), IEEE, Funchal - Madeira, Portugal* (pp. 714–721).
15. Wohrer, M., & Zdun, U. (2018). Smart contracts: Security patterns in the ethereum ecosystem and solidity. In *2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE), IEEE, Campobasso, Italy* (pp. 2–8).
16. Taş, R., & Tanrıöver, Ö. Ö. (2019). Building a decentralized application on the ethereum blockchain. In *2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), IEEE, Ankara, Turkey* (pp. 1–4).
17. Le, T., Kim, Y., & Jo, J. Y. (2019). Implementation of a blockchain-based event reselling system. In *2019 6th international conference on computational Science/Intelligence and Applied Informatics (CSII), IEEE, Honolulu, HI, USA* (pp. 50–55).
18. https://nodejs.org/en/docs/
19. Li, L., Arab, A., Liu, J., Liu, J., & Han, Z. (2019). Bitcoin options pricing using lstm-based prediction model and blockchain statistics. In *2019 IEEE International Conference on Blockchain (Blockchain), IEEE, Atlanta, GA, USA* (pp. 67–74).
20. Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (2017). Blockchain technology innovations. In *2017 IEEE Technology & Engineering Management Conference (TEMSCON), IEEE, Santa Clara, CA, USA* (pp. 137–141).
21. Harris, J. D., & Waggoner, B. (2019). Decentralized and collaborative AI on blockchain. In *2019 IEEE International Conference on Blockchain (Blockchain), IEEE, Atlanta, GA* (pp. 368–375).
22. Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., & Wang, F. Y. (2019). Block-chain-enabled smart contracts: Architecture, applications, and future trends. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, 49*(11), 2266–2277.
23. https://www.trufflesuite.com/docs/ganache/overview.
24. https://academy.horizen.global/technology/advanced/attacks-on-blockchain
25. Latifi, S., Zhang, Y., & Cheng, L. C. (2019). Blockchain-based real estate market: One method for applying blockchain technology in commercial real estate market. In *2019 IEEE International Conference on Blockchain (Blockchain), IEEE, Atlanta, GA* (pp. 528–535).

Chapter 11
An Exhaustive Survey of Blockchain Applications with the Internet of Things (IoT) to Combat COVID-19 Spread

K. C. Suhas, N. Mahesh, Asifullakhan, H. L. Gururaj, K. S. Vinayaka, and P. Subramanya

11.1 Introduction

The coronavirus disease 2019 (COVID-19), which begins with relentlessly sensitive severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) [1], initially got diagnosed in humans with the onset of symptoms at the beginning of December 2019 in Wuhan, China. This virus infects people of all ages. However, by clinical trials, it has been confirmed that two groups of people are at high risk of getting infected with this disease. They are people more than sixty years old and with some medical co-occurring like diabetes, high blood pressure, cardiac disease, kidney problem, cancer, and chronic respiratory disease and people below the age of 16. The most common symptoms of COVID-19 are fewer, dry cough, tiredness, sore throat, headache, and body pain. At the time of writing this paper, in the present scenario in the world, the total number of infected people is +3.7 crores, and the total number of death claims is +1.04 crores [2] as shown in Fig. 11.1.

As Fig. 11.1 shows the vast spread of coronavirus across the globe, preventive measures are to maintain a safe distance from one another, to improvise and strengthen medical care, and to facilitate the transparent, automated, and easy reach facilities and schemes provided by the government. In this regard, Blockchain can

K. C. Suhas (✉) · N. Mahesh · Asifullakhan
CIT, Gubbi, Karnataka, India
e-mail: suhas@cittumkur.org; mahesh.n@cittumkur.org; asifullakhan@cittumkur.org

H. L. Gururaj
Vidyavardhaka College of Engineering, Mysuru, Karnataka, India

K. S. Vinayaka
Network Engineer at Cywest Communications, Phoenix, AZ, USA

P. Subramanya
DevOps Engineer, Akuna Capital, Greater Chicago, IL, USA

H. L. Gururaj et al. (eds.), *Convergence of Internet of Things and Blockchain Technologies*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-76216-2_11

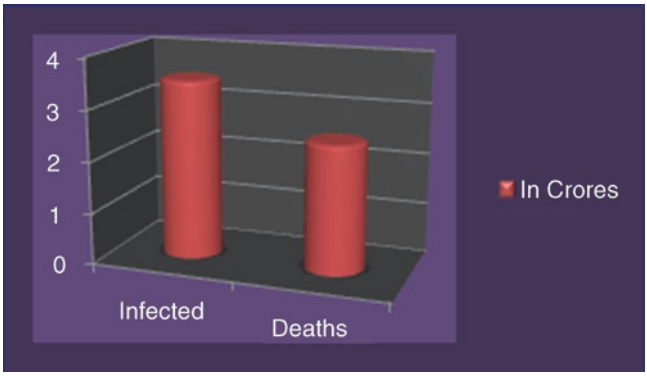


Fig. 11.1 Expansion of coronavirus

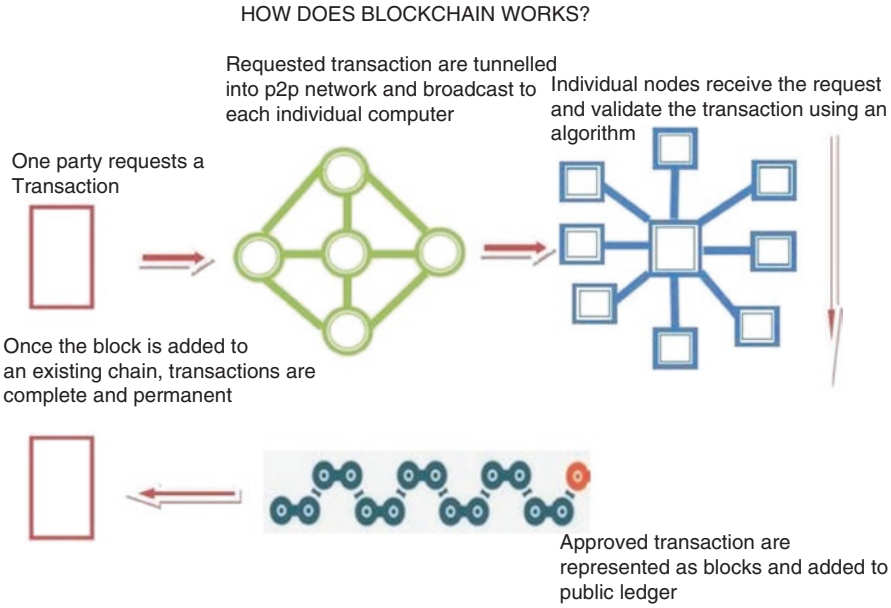


Fig. 11.2 Integrating IoT with Blockchain

be chosen as an effective technique to combat this difficult situation, but Blockchain alone makes it difficult to maintain secrecy and security of confidential data. Hence, we integrate IoT with Blockchain as shown in Fig. 11.2 which permits devices to transmit data to private Blockchain ledgers for incorporation in collaborative transactions which doesn't harm the records.

In this COVID-19 situation, Blockchain along with IoT [3] can transform several industries like banking, supply chain management, healthcare, and government sectors. Blockchain is a decentralized technique with many built-in aspects like

transparency and cryptic encryption tools. Blockchain is a type of spreadsheet which has data about transactions. Each transaction gives rise to a hash, and every block of data refers to a prior block and altogether creates a Blockchain. It is a peer-to-peer technology, which incorporates a distributed ledger technology (DLT) which permits data to get stored globally on servers by allowing anyone on the network to see everyone's entries in real time [4]. When Blockchain is used with IoT, it empowers the entire system by providing unique identifiers and the capacity to move data from one node to another node in a network without the need for interaction between person to person or person to computer.

11.2 Healthcare Application

Many countries have been affected by the sudden increase in COVID-19 cases, and it's troublesome for patients to approach doctors. To conquer this problem, we use IoT technology; in recent years, we have noticed many sensors, devices, and vehicles are attached through the Internet to medicate patients by remote patient monitoring [4].

Before the Internet of Things, patients had to visit the hospital; interactions with doctors were limited to visits and had less communication about the health details. Due to the rapid increase in COVID-19, there was difficulty in approaching doctors or going hospitals for doctors to observe patients' health constantly and make a suggestion; for that reason, RPM provides monitoring and care of patients through home quarantine, and it reduces medical cost and burden on government and also improves the quality of treatment.

Nevertheless, these technologies also showcase serious privacy concerns and security risks for data transfer and upholding data transactions. Hence, the above-proposed security and privacy issues of medical data may perhaps be the reason for a delay in treatment progression and also letting the patient's life in distress. Hence, we prefer to use the Blockchain mechanism which is the most promising one to provide secure management and to store, process, transfer, and monitor the patient data presented in various IoT sensor objects [5].

Remote patient monitoring (RPM) offers monitoring of outpatient concern outside the generally proven spot (house). First, it allows patients an in-house opportunity for the service. Patients know how to stay in touch with healthcare providers if needed. It moreover reduces treatment costs and improves the excellence of care. This is the major reason why healthcare providers are exploring ways to provide RPM to people. The key parts of the RPM system are a monitoring tool specifically designed for monitoring and transmission of health information on a smart contract and mobile devices using Internet connection. Mobile devices with IoT play a significant responsibility in RPM and the current development of wise cities [6]. The wearable devices gather patient health information and transmit it to hospitals or clinics for easy monitoring, diagnosis, and treatment. By doing so, we see the big

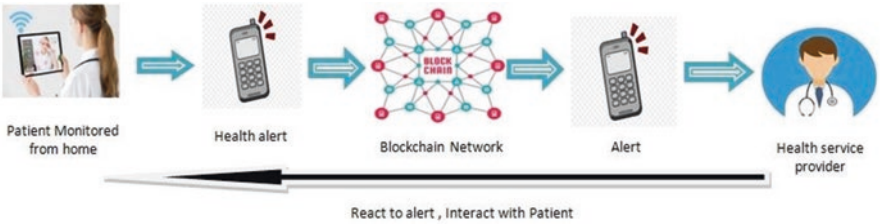


Fig. 11.3 Remote monitoring system

data situation grow through every patient data being analyzed and transmitted. Figure 11.3 shows the remote monitoring system.

The wearable devices for healthcare are smart devices with minimal controls embedded in outfits (clothes) or worn on the body as accessories [7]. These are anonymous, non-usable, and highly connected to advanced features such as wireless data transfer, real-time feedback, and device build methods for notification. These devices can provide important sequence to healthcare providers such as blood pressure, blood sugar levels, and respiratory patterns.

One of the characteristics of the IoT is a network of portable, embedded devices with software, electronics, sensors, actuators, and connecting devices that enable a portable device to connect and modify data. In the wise city of the future, we will not only see these clothes or devices send healthcare data, but it makes sense to think that wearable devices know how to share a lot of information as we connect these devices. Therefore, access to the thoughts expressed here in terms of wearable health devices and the use of Blockchain technology extends far beyond as shown or you can think here. To hold such patient information among additional facilities, such communications require secure data sharing. Health information is not to be disclosed, and data sharing can increase the risk of exposure. Also, the current data-sharing system uses a basic structure that requires moderate trust.

Shortly after the outbreak of COVID-19, countries began looking at ways in which smartphones could help enforce segregation policies and reduce the spread of the virus. Two main methods have been developed—using QR codes for electronic management of public access to public places, and location tracking based on GPS data from mobile phones. Both have shown good results but have also expressed their risks and limitations. Figure 11.4 shows the wearable devices for the patients.

One of the approaches to anti-COVID smartphones was in the city of Hangzhou, China [8], where authorities used QR codes to track the health status of each citizen as part of their health monitoring program. Based upon that information, everyone had to follow certain limits on where they'll go and how much time they spent outside. People also needed to measure and adjust their temperature in the app every day and keep their profile up to date. This strategy was reported to be very effective but also had its drawbacks:

- It requires a comprehensive infrastructure for QR testing centers and local recruitment.

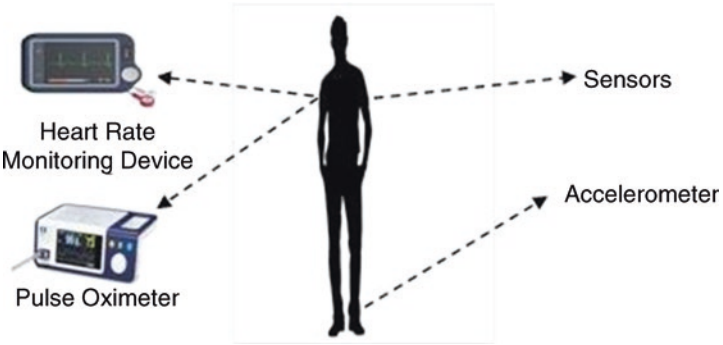


Fig. 11.4 Wearable devices for the patients

- It does not work well at a time when the person is not showing any symptoms.
- It requires everyone to have a smartphone and know how to use it.
- It does not work as expected if one chooses not to carry a smartphone when going out.

Location tracking was intended to address the above shortcomings of QR codes and uniform functionality. By touching GPS phone data, authorities can track your whereabouts and track your contacts as long as your smartphone is with you. It provides grim data to reduce the epidemic; however, it comes at the expense of everyone's data privacy. Figure 11.5 shows some of the Blockchain using IoT to combat the COVID-19 epidemic and its benefits.

Blockchain technology has been widely explored among researchers and other sectors in the recent years, particularly since the beginning of Blockchain 2.0 and Blockchain 3.0. Progressively, this technology is expanding its occurrence in almost all major domains, including supply chain management, banking sector, insurance sector, government sector, transportation sector, drone contact technology, and even the healthcare sector, and existing health problem, brought on by COVID-19 [9]. The COVID-19 epidemic left no room for concealment; people all over the world need to stand together to pass this problem. The epidemic itself is being spread in nature. Therefore, textbook technology, such as Blockchain, can be very helpful in terms of dealing with these circumstances. Blockchain technology empowers people and organizations from any part of the world to participate in a single interconnected network that facilitates secure data sharing. The disruptive feature of Blockchain evidence makes it challenging to unofficial changes, and concern of smart contract compliance reduces the distribution of fake and fraudulent data details. Requests for Blockchain can be processed for monitoring and managing COVID-19 patients, thus reducing the burden on hospital staff and other healthcare workers. The following is a few of the significant methods where Blockchain technology's know-how to help against COVID-19: assisting additional assessment and reporting details of COVID-18 patients, managing lockdown implementation, preventing the spread of fake news, enabling collaborative engagement, enabling

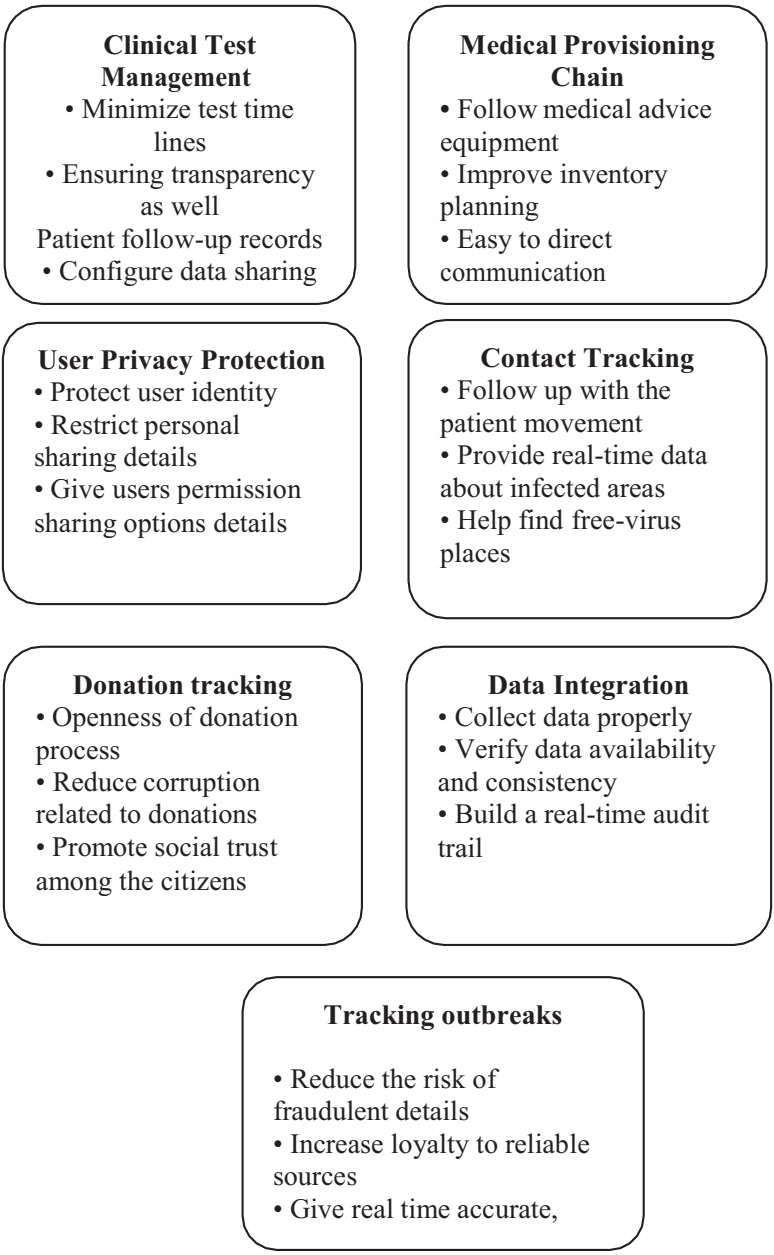


Fig. 11.5 Blockchain using IoT to combat the COVID-19 epidemic and its benefits

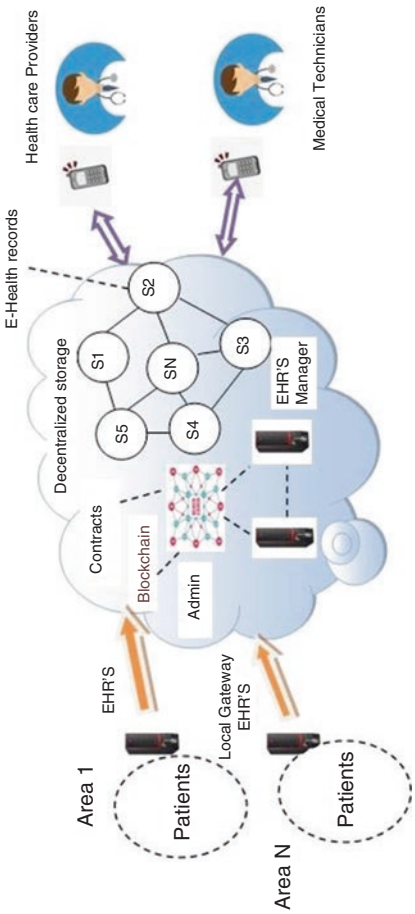


Fig. 11.6 Blockchain-based e-health system

platform for a secure donor support, and reducing procurement disruption. Figure 11.6 shows the Blockchain-based e-health system.

11.3 Blockchain with IoT for Banking

The banking domain is one of the many affected camps. It needs high-level security, and numerous solutions are developed that strive to address this problem [10]. Blockchain can remove the hazard of fraud in all banking environments, and this can apply fairly to the trading domain also. Besides, Blockchain will also solve issues such as operational hazards and administrative prices as they can be made clear and unchangeable. The tracking and persistent record that will be available on Blockchain to support each asset or item of sale will provide assurance and integrity throughout the entire sale process. So let's see the high usage cases of Blockchain that have proven their reasoning and effectiveness [11].

Blockchain authorizes IoT devices to improve safety and exposure to IoT environments. As per IDC, 20% of every IoT releases will make Blockchain-related solutions by 2020. Blockchain provides an awesome and shared ecosystem for IoT-related devices, principles, and applications. Banks and monetary institutions such as ING, HDFC Bank, and HSBC set up a Proof of Concepts (PoC) to ensure Blockchain methodology. In addition to monitory institutions, various companies are planning to exploit the power of the Blockchain. Conversely, the Internet of Things (IoT) exposes many chances for ventures to go ahead with smart jobs. All the equipment are now sensory, transmitting information onto the cloud. Hence, making these two methodologies work together can improve the performance of our system.

11.3.1 Working of Blockchain in Banking

Figure 3.1 shows the working of Blockchain in banking where a block stocks newer data; it will be appended into the Blockchain. As the name tells, Blockchain contains numerous blocks grouped. For any block needed to be added to the Blockchain, the following procedure takes place [12]. Figure 11.7 shows the working of Blockchain in banking:

- Transactions should take place. Let's take as an example Amazon shopping. After a quick click of multiple checkouts, you do the opposite of your best judgment and you will purchase. As per what we have seen above, in most of the cases, a single block will assemble more interactions; hence, Amazon shopping shall be included in the block and transaction information of other users as well.
- That transaction should be confirmed. After shopping, what you do should be confirmed. For more public records, go to someone who takes care of the new data entry tests, like the Securities and Exchange Commission, your local library,

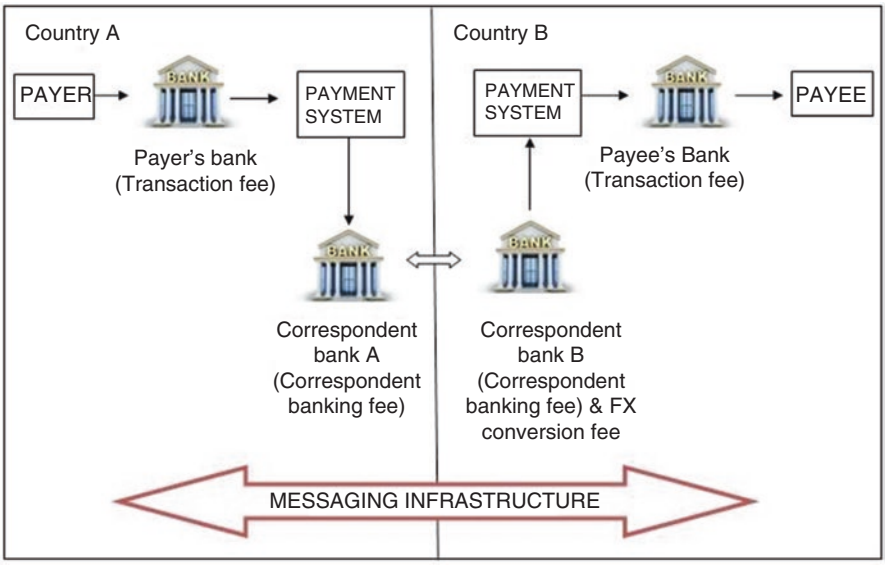


Fig. 11.7 Working of Blockchain in banking

or Wikipedia. Using Blockchain, that function is given to the computer network. When you shop on Amazon, that computer network quickly scans your deals in the same way you did. Besides, they verify purchase logs, transaction time, and the dollar price.

- What is being done should be maintained in that block. Once the transaction is authenticated as correct, it receives a green light. The transaction dollar amount and a digital signature of Amazon and yours will be kept in the block. Hence, transactions may become numerous.
- Every block of that type will be provided with a hash. As the angel who receives his colorful wings, after all the blocks have been authenticated, they will be given a separate, identifiable key named a hash. Every block will be given with a recent block hash added to the Blockchain. As much as you are quick, that block will be appended to the Blockchain.
- After that block has been appended to the Blockchain, it will be available in the public to everyone who can watch. If you consider the Bitcoin cryptocurrency Blockchain, you can observe that you have entry to each of the transaction details, also details of when ("time"), where ("rise"), and who ("transferred by") are added to the Blockchain.

11.3.2 Areas in Banking Where Blockchain Is Used

11.3.2.1 Quick Remittance

Finding out a cost-effective way for transactions, monetary organizations can use recent methodologies to smoothen payments, thus reducing the processing costs. By providing high safety and low cost of making and redirecting payments, banks can come up with a new kind of service, introduce new ventures, and be ready to go head to head with emerging start-ups. Also, by using Blockchain, banks can reduce the need for authentication from mediators and speed up processing times through normal bank transfers.

11.3.2.2 Drying and Seating Methods

Distributed ledger technology such as Blockchain can allow banking transactions to be more direct and secure compared to present protocols such as SWIFT. A standard bank deal takes 1 or 2 days to pay as it is done by the method of our financial framework. Globalization is a food contest for almost all banks. An easy banking transaction requires going through a complex method of mediators such as a depository before it moves to its destination. Besides, bank balances should be aligned with the financial system all over the globe, which includes a comprehensive monitory network, property managers, and vendors.

Let us take an example; if you would want to transfer the amount from an Indian bank account to another in Germany, such a movement of money would be made through the International Monetary Fund (SHIFT). Each day, SWIFT participants send 30 trillion messages to some 1,000,000 sites!

The cluster SWIFT protocol only executes payment orders. The real amount is executed through a mediator. Everyone comes with new costs and takes more time. Ledger used for business such as a Blockchain can allow banks to know the traces of everything publicly and openly. Banks may not depend on a network of storage assistance and authoritative bodies such as SWIFT. These bodies can simply adjust business directly to the general Blockchain.

11.3.2.3 Trading of Goods

By eliminating intermediate transfers and intellectual property rights, the Blockchain reduces interchange rates and minimizes the uncertainty of the conventional safety market. As per the sources, blocking secrets on the Blockchain will save $19–34 million every year on the cost of international trade.

Trading of assets such as stocks, items, or liabilities depends on keeping an eye on who owns all of them. Monitory markets achieve the above by a secured network of interchanges, mediators, real estate mediators, central bank deposits, and savings

banks; altogether, different groups are made up of the old paper proprietorship system. Altogether, you can see that the system will not only reduce its efficiency but also will be full of errors and frauds. Making those types of banking through computers is not safe as most of the time traders won't depend on the similar banks, and this does not always depend on reliable mediators to have all the ownerships. We have to observe that the German government will not allow monitorial institutions to provide cryptocurrency-related assistance. Ukraine also depends on the same. When you trade goods, the respective order will be forwarded to more mediator companies. Hence, interchange of ownership is complex. Observe that every group stores its sort of correctness in a different label. The operating organization is not only practical but also correct.

Blockchain transforms the monitory businesses by generating used datasets corresponding to digital properties. Distributed ledger permits the interchange of property rights by unreadable tokens that can replace those properties without a chain. Legal tenders like Bitcoin achieve that with digital properties, although more number of Blockchain companies are now functioning on results which will make us keep practical assets like gold or properties. Removing the middle person will also reduce interchange rates and accelerate the process.

11.3.2.4 Making Money

Making money by business financing is a very complex affair today. Almost all the time, it takes the following way: owners put the decks altogether; hold some meetings with their fellow members; go through lengthy discussions about equity; and, ultimately, decide to exchange their company by deciding on a fee. Blockchain organizations are speeding up actions by investing and raising money in many ways. This involves initial exchange offering (IEO), equity token offering (ETO), and security token offerings (STOs). STO is presently a more secure and popular method as it is legally safe. To use this method, projects need to go beyond the proper process. STO partners are Switzerland as well as Malta in which organizations such as Skerri and Concise Limited assist. The most promised and secure ETO trading domain is Neufund.

11.3.2.5 Debts and Credit

Conventional banking organizations apply for credits through a credit reporting organization. With Blockchain using IoT, we look into the upcoming peer-to-peer crediting, quicker and more confident borrowing methods, and even more sophisticated formal credits that can compare to a combined loan structure or cash loan [13].

Banks considering loan applications assess threats by considering credit scores, real estate ranking, or interest rate debt. To get this data, they want to request your credit status given by credit firms. In the United States, that is similar to three organizations. Abovementioned intermediate programs are sometimes dangerous for

customers because they may have incorrect data. Also, integrating these secure data in such tiny institutes makes data in danger. Let us take an example where, in the previous year, one of them, Equifax, was manipulated, revealing the debt details of more than 154 million people in America. This pays a way to know why Blockchain along with IoT makes it a much cheaper and safer application.

By the above working of Blockchain in banking and areas where Blockchain can be used for banking [1], we can conclude that Blockchain along with IoT can be cost-effective and efficient wherein Blockchain's capabilities are highly attractive to banks, facing rising costs of repairing or replacing their obsolete infrastructure and ensuring compliance with heavy regulatory responsibilities. Also, banks have to deal with growing economic instability. To that end, the solutions for Blockchain can save tens of billions every year, and secondly, it has given rise to new types of businesses wherein banks can use Blockchain-based systems to limit the control of medium-sized businesses or legacy infrastructure. Banks can develop these systems to create new business models that disrupt the financial system.

11.3.2.6 Blockchain in Education

Given that Blockchain technology is emerging, educational leaders, the same as the managers in some industries, require further proof of that common Blockchain application (beyond cryptocurrency). Many are aware of investing valuable resources in emerging technologies. But it has dangers in it. Organizations that are now beginning to understand the technology and the value it can bring with accurate charges of use will be appropriately set to reap its operational benefits [14].

11.3.2.7 Working of Blockchain in Education Domain

Student data are unlimited; using Blockchain, data such as attendance, tuition, tuition fees for the private school, marks, courses, and certificates can be included as their Blockchain data. Since these data can't be removed, this contributes to data safety as they cannot be changed. And it is for the student, not for the authorities of the school. Hence, using Blockchain, none of the members, even teachers or students, can modify the saved data. If the data is defective, a new dataset should be submitted for correction, and wrong and correct datasets can be seen. Nowadays, almost all educational organizations are thinking to use Blockchain-related pedagogies. If you are working in any educational institutions, knowing this will help you be informed about these changes and perhaps offer some helpful solutions. If you are associated with making any open-source software, then this can help you to know better and use Blockchain-related methodologies, and incorporating IoT to Blockchain gives extra ease of use to the participants [15]. Figure 11.8 shows the typical implementation of Blockchain with IoT for education.

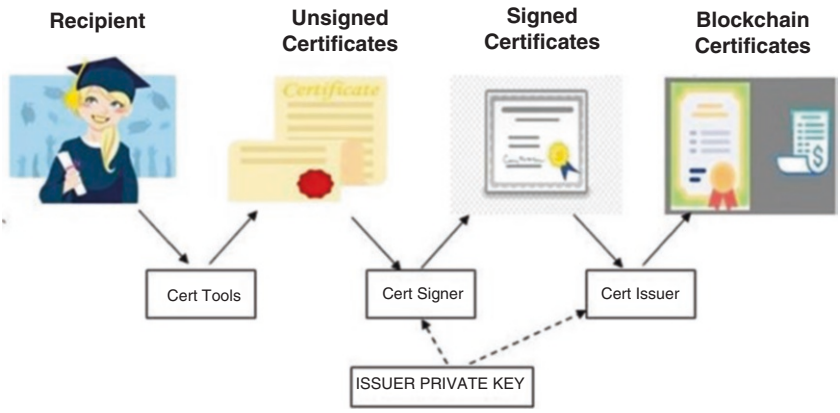


Fig. 11.8 Blockchain with IoT for education

11.3.3 Opportunities for Blockchain Along with IoT in Educational Systems

Remote classrooms are not beyond the thinking where they will be integrated with Blockchain and the Internet of Things technology. This technology will be the most important segment of scholars around the world soon. The question in front of us is, in what way will the program benefit us, employers and people related to teaching? And the reply is yes; to see the full impact of the Blockchain on the education system or find out that this will have an impact on both teaching group and student group, this will help to monitor how other domains have used this methodology to improve their ways and in what way organizations can do it someday

Follow their lead. The BC-IoT collaboration strategy has many opportunities in the education system. This opens two new windows next to each other. Several opportunities can be seen in the following way.

11.3.3.1 Building Trust Between Groups

Due to its very advanced features, the BC-IoT strategy can cultivate relationships between many intellectual devices. Only verified gadgets can share with the file system, and miners will begin to verify regularly transactional block, in which case they should join BC [16].

11.3.3.2 Low Cost

Such a plan can reduce costs as they come together successfully without a mediator. Hence, pullout every mediator members between the receiver and the people who send the data.

11.3.3.3 Reduce Time

Reduce the maximum of the time allowed. This method reduces business time from hours to microseconds. Let's take an example where students won't take a university entrance conventionally by paying more time to complete forms and wait for a response from the university administration.

11.3.3.4 Functions of the Institute of Education

Blockchains can also change certain roles in education institutions. The Blockchain will be a good format by providing degrees and knowledge that would be possible to remove the role of the facility administrator as a location for delivery. This will also reduce the flow of the facility profit; this can minimize costs or permit that help distribution everywhere. Presently, institutions of higher learning worldwide introduced their people to the Blockchain journey as they see the minimum number for advancement in the domain. So many countries have introduced Blockchain-education-affiliated organizations.

11.3.4 Challenges

11.3.4.1 Usability

BC can stop because of its huge transactions. Before 2021, digital currency storehouse has become so much accepted by people that more than 200 GB capacity Take the time IoT included in BC so that load will be more than that of the current circumstances.

11.3.4.2 Energy Conservation

An electronic notebook will be maintained by each IoT point. In each case, they have seized it, despite obstacles we can scarcely imagine. Size that would be hard work or be too heavy every other wireless device.

11.3.4.3 Incompetence

BC is now an emerging conversion methodology. Few humans all over the globe recognize this methodology.

11.3.4.4 Locating or Meeting

BC might have been found out by IoT in the first place. Finding an additional device in BC or IoT is an eye-opening task for every smart gadget. The Internet of Things can be found on each other, but they may have not found combing BC with other devices.

Finally, this study gives an overview of the methodology that can be used for Blockchain with IoT for the educational system along with a list of advantages and disadvantages for the same.

11.4 Application of IoT in Supply Chain Management

In recent times, Blockchain has been gaining a lot of attention in a variety of industries, starting from the economic zone, to the healthcare industry, to individuals, to the public sector. The reason intended for this attention is that applications in these industries only work through a trusted consultant. By adopting Blockchain, these industries can operate at a lower rate, lacking the need for a validation system, but can achieve the same amount of reliability. Additionally, utilizing cryptography in Blockchain ensures data security, given a large calculator to record everything users have done [16].

Blockchain supports peer-to-peer network design and development to get better security and growth in production. Also, the integration of Blockchain skill among agent knowledge ensures facts' integrity which provides precise resource execution to various stakeholders. This technology exist as a digital distribution system that ensures the visibility, tracking, and reliability, as well as intelligent contractual relations surrounded by worldwide supply chain networks, mainly disruptive technologies of construction, planning, processing, and all-purpose administration of supply chains. Blockchain technology provides promising opportunities to create circulated business proceedings. Generally, Blockchain is understood as a static digital recorder for records, prearranged by interconnected data blocks. Blockchain is secure due to the low-level secure transaction processes offered by computer networks that are used together in Blockchain operation and authentication processes. Blockchain applications in sales ensure the protected storage space of all business information. By installing Blockchain, submissions can be tracked and confirmed, and the destination and proof of each transaction can be retained.

In terms of security perspective, Blockchain is considered to be the most advanced skill. Although the use of Blockchain technology in the delivery and sale of goods is still in its early stages, this knowledge can be adapted and used in the supply chain. Technology is used more widely than others, from open production and in-house production, to make sure of scam prevention in a medical trial and the start-up of new businesses. When Blockchain is adopted, commodity managers can have a pure, transparent, consistent, and effective transaction for their operating systems. The entire application of Blockchain on universal provisioning networks can be summarized as follows: most Blockchain applications are related to cryptocurrency sets but are also increasingly leading to digital positive feature management. Skill analysis and resolution are the obvious continuity. As facts' consistency is guaranteed, this can be used to sign a transaction for the authenticity of an item, a bond, or a use right. These factors are taken into account in the administration register and the medical industry. Industrial uses reported inside the literature include open production facilities, IoT connectivity, originality, and product security.

The assistance of Blockchain programs is allocated system management as all stakeholders share the requirement intended for a consistent and transparent process. The certainity include high-quality business facts or complete certification related to the products, procedures or issuance of payments, and enhanced faith with increased visibility of acquisitions and acquisitions of fraud, a scary system that provides the basis in favor of the same profit [17]. Figure 11.9 shows the supply chain transaction in multi-vendor project logistics.

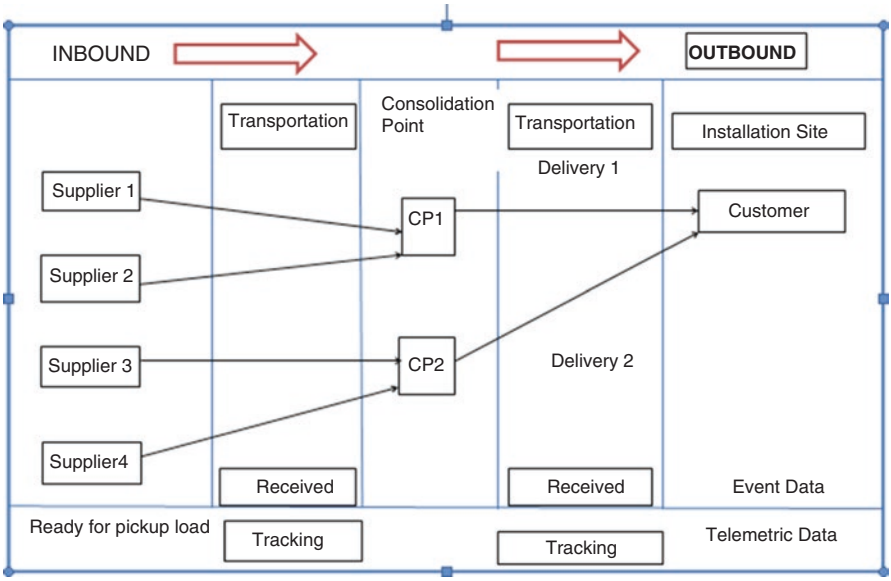


Fig. 11.9 Supply chain transaction in multi-vendor project logistics

11.4.1 Applications of Blockchain

- Blockchain load supply machinery is used to manage and approach information on foodstuff sales. It monitors and evaluates foodstuff purchases to record and verify transactions.
- The provision at aircraft procurement Blockchain helps to keep track of aircraft parts and monitor performance to reduce the risk of part starting the black market.
- Transport and asset management increases the visibility at procurement and improves the integration of contracts in travel contracts and improves general repair management in the company.
- Foodstuff supply together with RFID and Blockchain technology is used to track reliable data throughout the agri-food chain and to ensure fare security by distributing accurate agricultural food information on the production, use, storage, distribution, and marketing of links [18].
- The integration of digital delivery between cloud record and Blockchain technology is planned for interactive digital marketing to achieve troublesome transformations of information/data intended for various associations and systems.
- To learn IoT, a Blockchain-based solution has been submitted to meet the needs of the provision of services such as price reduction, quality improvement, high speed, low reliability, risk, improved stability and elasticity, and increased transparency and responsiveness.
- Pharmaceutical supply chain in the ration of IoT and Blockchain was developed to ensure data consistency and public access to temperature and humidity records for the sale of medicines by reducing operating costs.
- Agricultural provision is the agricultural procurement system to learn the organization of the two chains and take into account the security of transaction information and the time alone of the business information system.
- The customer electronics sector analyzes the general contact of Blockchain technology in the management of the customer electronics industry's supply chain to make the industrial sector transparent, safer, and more reliable.
- Construction industry explores the potential of Blockchain technology in a range of materials in the creative industry. A model is shown to provide an increased number of clients, transparency, and a network of improved services in the construction industry [19].
- Procurement management in the consumer industry using a Blockchain model is proposed to facilitate the notion of circle economics and coordination of all transactions that take place in the goods [20].
- Megacity supply sequence Blockchain technology is used to support the hunt and negotiation phase of an asset agreement. For comprehensive information structure and vendor motivation structure, resource management is also implemented with Blockchain technology.

11.4.2 Impact of COVID-19 on Procurement Decisions

The coronavirus epidemic has been a significant problem for almost all manufacturers and retailers. While the world tries to move from side to side in this hard times, many companies are striving to uphold a stable run of needed merchandise, whether stationary food and substance (i.e., paper), ventilators and mask, and other services. Many genres and frameworks that have been developed in existing literature have been clever to stop this disruption, and as a result, a firm has the appropriate strategy to contract and to employ it. Intended for the firm with composite supply options (i.e., production), it is very important to identify the strategy for an agreement with that critical situation. The aim is to provide information on the strategies firms are using in dealing with major problems and planning and options for firms to consider. The tweets records since NASDAQ 100 firms to breed themes about the problems facing the firm and the strategies they use using text analysis tools (Table 11.1).

Figure 11.10 shows the graphical representation of tweets concerning total words and occurrence which includes parameters like study, required, help, COVID and a total number of people that commented concerning the occurrence.

We find that firms face a challenge in terms of unwanted supply-demand, skill, and the construction of a solid supply chain. Also, moving beyond profits, the firm has experienced difficulty in building sustainable purchases. We provide a future strategic recommendation, rebuilding the supply chain.

11.4.3 Challenges to Providing Demands During the COVID-19

The request for hesitation is one of the most important challenges that reflect in many tweets. Several sectors have set refuse inside the order, others contain to see an unexpected rise inside the order. While persons began to follow the “hang about

Table 11.1 Impact of COVID-19 on procurement decisions

Total words	Occurrence
Squad	2288
Study	1772
Require	1576
Holdup	1531
Particulars	1524
Ladder	1441
Help	1285
COVID	1223
Subsequently	1165
Support	1129

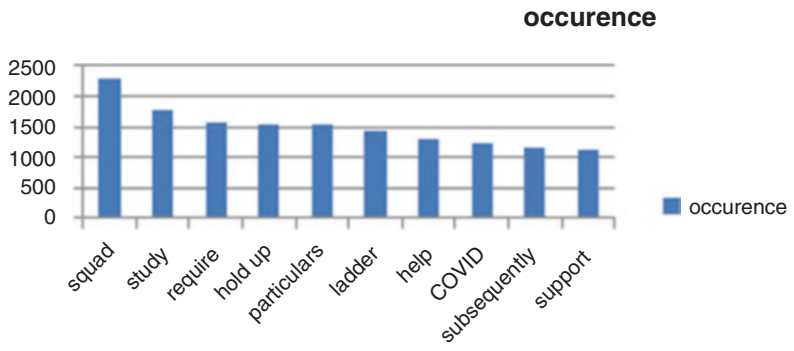


Fig. 11.10 Total words and occurrence

at house" instructions, other sectors such as automobiles and transport saw a drop in demand. In contrast, many skill companies have found an increase in the claim. The company is facing a daunting challenge of curbing this growing demand. Many tweets highlight the challenges the company is facing. PSD International, a management consultancy firm, wrote on Twitter (May 7, 2020), "Pandemic Lockdown & Stay Home has created unparalleled Supply Chain management features. To keep the forces organized a ken care of by driver safety, pressure, and ethics." Similarly, Biogenic wrote on Twitter (April 29, 2020), "Foodstuff insecurity is an everyday problem intended for many. At # COVID19, insist is growing."

Adjusted to meet demand, Cerner wrote on Twitter (on April 15, 2020), "around the world, physical condition mind influence is responding in the direction of the growing demand for tough and treatment related to the virus. Surveys capability show aim to assist our customers to organize, deliver, operate, and function in the middle of the increase of the bug. Likewise, unexpected changes can create a challenge in matching short-term demand and demand." As shown in many tweets, the company is compulsory to match equation-supply equations daily.

11.4.3.1 Technical Challenge in the COVID-19 Era

Skill has emerged as an important issue in determining the achievement or breakdown of a company through the COVID era. However, our analysis suggests that all firms may not be at the same level of technological readiness, which represents much concern related to employing the technology. Apart from technological willingness, safety breaches are too ordinary problems highlighted inside many tweets. Among the accepted technologies, firms use a wide range of technology that is able to give them visibility throughout the value chain as healthy because it helps in ease and efficiency.

11.4.3.2 Creating an Elastic Value Chain

Due to COVID-19, regarding the entire value chain, there is a rising dialogue between the firm and Akers about how to build a supply chain. Gitanjali Ghosh, leader of NASS COM, wrote on Twitter (6th April 2020), "nowadays we contain 90.0% + workers operational as of house, there are serious employees on university grounds to make sure there is a negative disturbance to customer business. With the help of the administration, the manufacturing has shown great flexibility as well as enthused to the copy. India and India's IT determination merely approach absent stronger!"

11.4.3.3 Sustainable Procurement Challenges

Although COVID-19 has been cause of the economic downturn, the focus of organizations is on the ongoing supply chain. Organizations are simply not listening carefully in maintaining financial stability, but many tweets indicate that "organization is now the opposite challenge related to social sustainability."

11.4.4 How to Overcome COVID Purchasing Challenges

Next-generation sales require a major adjustment in look; based on our examination, we advocate a firm to accept a modern move. These modern approaches must contain many aspects of the feed list including people, processes, and technologies. This will allow the firm to provide a sequence to be able to contest prospect shock. Other strategies that the firm may include are as follows:

- Firm needs to rethink real-time information retrieval strategies. The hard container plans its supply chain in such a method to be able to poise risks and functioning suppleness, manage procurement disruption, and keep agile chains fast.
- While skill is available to streamline procurement decisions, firms must incorporate advanced skills such as AI and in-depth tools base on learning in the procurement result structure. The installation of these instruments helps the firm decide and exclude market signals about the disruption and visibility of sales and firm with the essential performance toward existence of skill used. This can assist in reducing the unintended consequences of some unusual events because of COVID-19.
- The definite too desires to measure weaknesses in the entire procurement environment as the belongings COVID or alike abnormalities can exist found inside other parts of the sales service with might stay unknown. A single way to measure such vulnerabilities is to expand the case-based provisioning model and efficient lines. The firm can submit presented information and use imitation to

exclude all potential adverse event. This determination helps firm not only to assess risk but also to reduce danger and to carry on the business.

- Many firms had to lay workers throughout this difficult time due to changes in sickness practice with earnings margins. While this may be a temporary plan, the company thinks its extended-term impact. Such retrenchment could affect the entire factory price chain. Continuous ways firms can manage to haven activist staffing strategy involves the selection of critical staff who can deal with unrest in any surroundings and the hard manage them beneath any conditions. This conditional preparation keeps utilization and competence management.
- Firms also need to work in employing more stakeholders and have a clearer strategy for their provided chain organization approach. With no teamwork, raising a novel year's supply chain might not be viable for the company.
- Finally, there is a great need for the company to look beyond profit. Ensuring the well-being of not only the company's workers but also those working for the suppliers is essential if the company needs to keep away from the disruption of sales.

11.5 Application of IoT in Government

Technology combinations such as IoT and Blockchain and the public sector distribute cabs and help citizens. It helps to create a safe infrastructure.

IoT in government sectors helps to create a lot of opportunities such as city planning management; IOT helps to make complex aspect in city planning to a simple one. IoT even helps the nation by creating a lot of job opportunities; it also helps in analyzing economics. It creates opportunities for growth by overcoming the barriers. Any country in the present era should be strong in defense; IoT helps by allowing the use of automated defense systems which in turn help the country grow [21].

11.5.1 Impact on the Public Sector Due to COVID-19

The factories that are closed started to open, and the manufacturing sector in India is facing a lot of problems to reduce the amount, the state, make smaller humans the state of relying on, and become quieter to events that will happen. Industry experts believe that this will motivate companies to adopt smart processes enabled by different new technologies. Fighting changes are high in India; however, the final tailwinds are working in their favor. Companies want to secede from China and see India as a possible destination. The manufacturing sector is monitoring operations.

Governments around the world are demanding that companies reduce their reliance in China on finished products or parts thereof. Japan set a $2.2 billion economic recovery package to help its producers move their production from China.

Cabinet also announced the Production-Linked Promotion (PLI) scheme worth more than Rs 40,000 in the IT sector.

China is already at the forefront of spending on AI in manufacturing. From 2019, the market of AI in manufacturing in China will increase from $2 billion to $40 billion by 2025, according to a 2019 Deloitte report.

The manufacturing sector needs to be strengthened to launch a flawless partner ecosystem. Engagement with customers and channel partners can be the benchmark. Presently, AI is used in construction planned in favor of structural maintenance—to identify and report parts, machinery, or manufacturing processes in real-time. AI helps to optimize the supply chain by estimating claims and revenue. The information provided for the AI model comes since industrial IoT networks are deployed on the manufacturing floor. It consists of sensors installed on networked machines to gather real-time information on their performance and capabilities.

The industries are disappearing to accelerate the overall movement toward Blockchain 4.0. In the present, there is a lot of interest that can be completed to increase flexibility. Indian manufacturers should now begin to seriously consider automation. The mid-market segment has started to look at it seriously, and the automotive segment is looking at it on a large scale, said Lux Rao, director, Solutions and Consulting, NTT India.

The epidemic was also uncovered in the supply chain networks. By concerning all the stakeholders in the long network, Blockchain helps to identify the issues that are interfering with the organization by preparing them for any challenges in the future. “An advanced RPA can gather information on manufacturing ecological unit, including inventory, logistics, supplier and vendor systems, and use the sensing capability of the device to initiate activities that increase in the general efficiency of the whole ecosystem.” Venkateshwaran, superior vice president, Industrial and IoT Solutions, Percentage System. Blue Star, TVS Motor Company, JK Tyre & Industries, and Asian Paints are some of the companies already using AI solution with analytics platforms in their manufacturing units in India. “When getaway of the present situation, feel that the uniformity of a common market has been shaken and it will take a few months for it to become an integrated, homogeneous market. The areas that able to become powerful things for creating technology like Al,” said Rakesh Ridge, Cloud and Solution Sales Director and Microsoft Executive Director.

The COVID pandemic is a primary and the largest humanitarian tragedy. Likewise, 200 countries and territories comprise a complete effectual remedial case, which has been confirmed as an epidemic by the WHO. As of April 1, 2020, the recent global rate has been more than 1,200,000 COVID cases and more than 66,000 deaths. Have already agreed that India is a rising wealth, is difficult. With the calendar day shut out announcement by Prime Minister Narendra Modi on December 23, 2020, through demand frustration and high unemployment, it will slow down supply, exacerbate the recession, and endanger the financial well-being of millions. Increasing coronavirus cases, the administration closed transport services, restricting all public and private, factory w congestion. In recent studies, some media report that 40 million people (MRD report) have lost their jobs in the countryside, typically in the unorganized sector.

In this situation, they predict that India, which affects the unorganized sector, will go into recession, and people working in semiskilled jobs will lose their jobs. In this, we are referring to the time of the Ebola crisis in Africa, with declining confidence in countries and between nations—by countrywide guidance beneath the pressure of social conflict and financial conflicts between major powers.

The worker sector under MGN REGA, 2005, was negatively impacted as they may not be offered jobs, and most of the worker sectors are associated with building company and everyday earners. Tourism limitations and segregation affecting hundreds of core of people have migrated in a small supply of workers and parts, supply chains, and sales alerts to all technologies, automotive, customer, pharmaceuticals, and other industries.

Look at the latest events announced by the administration and RBI in the direction of reducing the impact of this epidemic; as stated by the RBI director, these are temporary and may not bring the preferred results as the problem is serious due to the advance shutdown.

Quarterly GDP has been steadily declining since Q4 FY 18. There is a Q4 defect of FY 19, significantly reducing the increased charge in the primary three quarters of FY. Given what has happened and the latest data, the sector apart from this is likely to fall sharply in the coming days as job production declines at an alarming rate by long-term closures and frail GDP.

With the start of the economic time, the results of the coronavirus affect the economic strength of 150 countries—endangering livelihoods, economies, businesses, and thinking of normal life that we have taken for granted. Reductions have harmed the service sector such as banks, restaurants, load, and providers of equitable load supply and health and nutrition, and we must also consider the health of the sick by combining capital and planning for job formation.

11.5.2 Category Result Restaurant Service

The NRAI representing fifty thousand nationwide has advised its members to close down fried service from Wednesday to March 31, 2020. This power affects the performance of thousands of restaurants and bars. Increasingly, load delivery like Swingy and Zomato work on their own—they are also very effective. Orders in Swingy and Zomato dropped by 60% during the epidemic.

11.5.2.1 Food and Farming

The foodstuff and agricultural sector contribute the most to GDP of 16.5.0 Celsius and 43.0 Celsius in the service segment. The bulk of the foodstuff giving out to industry is dairy (29.0 Celsius), edible oil (32.0 Celsius), and grains (10 Celsius). India also ranks first in dairy and spice products in the international arena (export).

11.5.3 Main Challenge of Test 19 Levels of Government

- Another major problem is how global health systems are prepared to respond to these outbreaks.
- Tracking a large number of infectious patients to stop the epidemic [22].
- Another need is to improve quality diagnostics, medications, and targeted therapies.
- Misconceptions and conspiracy are still circulating on social media.
- Several one when accessing tools where needed. There are not enough steps to apply it in an emergency.

11.5.4 How the IoT Overcomes the Challenges of the COVID-19 Epidemic

The global epidemic, which began in March 2020 and continued into modern times, is still causing us a lot of trouble. Billions of people who had intended to travel abroad or at least within their own countries were suspended and forced to stay at home. Health workers from different medical fields are now forced to deal with thousands of similar daily emergencies. Not to mention, they face the risk of infection as they try to save the lives of the same people from whom they could get the virus. In the commercial arena, many small- and medium-sized businesses and even large corporations that have been struggling for decades (or failed at others) have failed to adapt to new trends. Several of them condemned their losses by hacking their employees, selling their property, and closing their doors temporarily (or permanently) [23].

Despite the people who work on the Internet of Things (IoT), yes, the IoT industry was also disrupted by way if its distribution (e.g., installing 5G mobile infrastructure designed to help business operations); it was disrupted as corporate clients tried to resolve their financial crisis. Organizations and institutions turn to work remotely in hopes of so their nation's curve, these products, and similar names call on the IoT to get help immediately. They have realized that leading IoT solution providers such as RAK wireless are critical to continuously improving their efficiency, quality, and security. To learn more, listed below are some of how IoT joins the cause of stopping the spread of coronavirus [24].

11.5.5 Improving Touch Tracking

One critical step in reducing the global spread of the virus is finding out in real time who among us has been exposed to suspected and infected people. To do this, the nation must invest in high technology that can build a knowledgeable connected

network of information. And what better technology is available than this app? Working people to take health data from a various infected patients and manage all the data using a visual management system is a lot of work. For example, in China, a mobile app called Close Contact was designed for citizens to know their proximity to the corona-positive patient and urge them to take safety precautions when leaving their homes. As a result, China and other countries using similar applications such as Taiwan are already close to stopping the epidemic.

11.5.6 E-Government

E-government, the government, is focusing on greater use of information and communication technology (ICT) to sustain the provision of public and private service issued in the direction of citizens of the country. These services include necessary public services, pay payments, duty collection, wedding and divorce service, land register, elections, and entry permit processing. The e-government concept proposes digital inclusion in all particular sectors of these services. The use of an e-government Blockchain can ensure safety by promoting integrity, consistency, confidentiality, and data instability flanked by organizations. Besides, its employment improves efficiency by dipping processing and mitigation delays' operating costs. Key Blockchain, such as notarization, common database, and workflow automation, is helpful after using various aspects of working e-government programs. Such programs can be detected automatically for the location of errors and fraudulent attempts [25].

11.5.7 Challenges to Connecting Citizens to Cities

How citizens interact with cities affects excellence in general and their participation in communication. Unit decisions are very important in assisting with community decisions that affect supremacy, rule, and teaching. This interaction has the parts to grow inside the range of elegant and digital cities, particularly with the latest developments in Blockchain technology. This job presents details of how smart city ideas and new technologies can help society cope with daily challenges to improve citizen alertness. Digital technology can drive the public as well as economic development through information and communication technology (ICT) promotion. Management, in combination with an unsettling concept such as Blockchain, is a fundamental tool of democracy for countries. This policy is reviewing, discussing, raising, and presenting suggestions on the effective, crystal clear use of technology, used in opportunity cities [26].

11.5.8 Blockchain and Elegant City

Application-based technology is recognized too the same as in circulated literature. This has received attention because of the emergence of Bitcoin in cryptocurrency and also has the potential for cost reduction. For instance, in Brazil, the Brazilian Development Bank (BNDES) contains a smart public finance management contract where bidding occurs. Another case of use in Brazil includes medical records' privacy, elegance, and low cost. Also, it is used for issuance and tracking, and official verification of certificate/diploma has been the center of other Brazilian institutions and Spanish programs. Applications internally can promote transparency if used properly applications they were in the financial sector and, these days, including other upward markets, desire to incorporate it into different benefit organizations [27], within the background of SC, there are a small number of applications that be able to at rest available.

The achievement of Aggarwal et al. induces Blockchain use in architecture between various IoT geographical areas in "increasingly digital society (e.g., smarty)." The authors have spoken of a growing computerized society as well as the use of the elegant city, linking it to the need for a Blockchain to manage distributed IoT key component network devices. Commonly, a few applications were concerned with privacy, starting with the Blockchain provided, intended for the initial occasion within the past, and open-source infrastructure for cryptographic operations to enable privacy-related application, as the peer review process for methodical paper applications go further, such as Patel and Patel emphasizing that distributed applications (dApps) technology can manage urban data storage, data management, prudent contract, certifying authenticity, verifying and managing reliable transactions, and allowing pooled financial system. While emphasized with them, in the period of graceful cities, it is expected to ignore the knowledge that provides consistent and transparent messages between the people involved.

11.6 Conclusion

The unexpected incidence of COVID-19 has made almost all the major sectors of human life such as health, banking, supply chain, education, government administration a standstill. These important sectors need some automation and advancement in their operation to continue their service to the abovementioned sectors. Many end users recommend IoT and Blockchain-based solution and change the operation of the above sectors. Accordingly, this paper simplifies the choice of adopting Blockchain and the corresponding method to protect the IoT system for the real-time operation of the mentioned sectors which addresses the security, authenticity, and ease of use. In a comprehensive discussion of this post, we separated the various technological interventions made in the form of COVID-19 impact management. Our discussion focused on the use of emerging technologies such as IoT and

Blockchain, in the abovementioned sectors, which reduce the intervention of humans and thus prevent the spread of COVID-19. We believe that our timely research will enlighten us with Blockchain and IoT anti-COVID-19 research and encourage interested researchers and national administrators to make greater efforts to use this promising technology to fight future coronavirus-like epidemic. Finally, we discussed the Blockchain-based IoT system and its security issues in the real world.

References

1. Chamola, V., Hassija, V., Gupta, V., & Guizani, M. (2020, May). *COVID-19 Pandemic and the Role of IoT, Drones, AI, Blockchain, and 5G in Managing Its Impact*. 109/ACCESS.2020.2992341
2. https://www.worldometers.info/coronavirus.
3. Chendeb, N., Khaled, N., & Agoulmine, N. (2020). Integrating Blockchain with IoT for a secure healthcare digital system
4. Srivastava, G., Crichigno, J., & Dhar, S. (2019). *A Light and Secure Healthcare Blockchain for IoT Medical Devices*.
5. Nguyen, D. C., Ding, M., et al. 2019. Blockchain and AI-based solutions to combat coronavirus (COVID-19)-like epidemics: A survey
6. Jesus, E. F., Chicarino, V. R. L., de Albuquerque, C. V. N., & de Rocha, A. A. (2018). *A Survey of How to Use Blockchain to Secure Internet of Things*. Published 8 April 2018.
7. Khatoon, A. (2020). Department of Electrical & Electronic Engineering, National University of Ireland Use of Blockchain Technology to Curb Novel Coronavirus Disease (COVID-19) Transmission.
8. Dwivedi, A. D., Srivastava, G., Dhar, S., & Singh, R. (2019). *A Decentralized Privacy-Preserving Healthcare Blockchain for IoT*.
9. Khezr, S., Moniruzzaman, M., Yassine, A., & Benlamri, R. (2019). Blockchain Technology in Healthcare: A comprehensive review and directions for future research.
10. Dorri, A., Kanhere, S. S., & Jurdak, R. (2016). *Blockchain in Internet of Things: Challenges and Solutions*.
11. WHO. (2020, April 24). "Immunity passports" in the context of COVID-19 scientific brief. https://www.who.int/publications-detail/immunity-passports-in-the-context-of-covid-19.
12. https://www.leewayhertz.com/blockchain-iot-use-cases-real-world-products/
13. https://www.investopedia.com/terms/b/blockchain.asp
14. https://concisesoftware.com/10-use-cases-of-blockchain-in-banking/
15. https://www.iotsworldcongress.com/blockchain-technology-and-how-is-transforming-banking/
16. https://mdreducation.com/2018/08/20/blockchain-education/
17. Sahin, F., & Robinson, E. P., Jr. (2005). Information sharing and coordination in make-to-order supply chains. *Journal of Operations Management, 23*, 579–598.
18. Fayez, S., & Zomorodi, M. (2015). Supply chain management: Developments, theories, and models. In *Handbook of research on global supply chain management* (pp. 313–340). Hershey, PA: IGI Global.
19. Zantalis, F., Koulouras, G., Karabetsos, S., & Kandis, D. (2019). A review of machine learning and IoT in smart transportation. *Future Internet, 11*, 94.
20. Svorobej, S., Takako Endo, P., Bendechache, M., Filelis-Papadopoulos, C., Giannoutakis, K. M., Gravvanis, G. A., Tzovaras, D., Byrne, J., & Lynn, T. (2019). Simulating fog and edge computing scenarios: An overview and research challenges. *Future Internet, 11*, 55.

21. https://www.tutorialspoint.com/internet_of_things/internet_of_things_government_applications.html.
22. Meijer, C. R. D., (2016). Blockchain, financial regulatory reporting, and challenges. https://www.finextra.com/blogposting/13102/blockchainfinancial-regulatory-reporting-and-challenges.
23. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.
24. Chang, M. C., & Park, D. (2020). How can Blockchain help people in the event of pandemics such as the COVID-19? *Journal of Medical Systems, 44*(102).
25. SmartLog. (2016). https://smartlog.kinno.fi/
26. Wood, G. (2016). Smart contract yellow paper.
27. Worner, D., & von Bomhard, T. (2014). When your sensor earns money: exchanging data for cash with Bitcoin exchanging data for cash with Bitcoin, ACM, New York, USA.

Chapter 12
Role of Blockchain in Tackling and Boosting the Supply Chain Management Economy Post COVID-19

N. Kamalakshi and Naganna

12.1 Introduction

The novel coronavirus (COVID) belongs to coronavirus family of viruses (WHO/Europe). The transience rate of COVID-19 is a reduced amount rather than that of the severe acute respiratory syndrome (SARS) [1] and Middle East respiratory syndrome (MERS) coronavirus diseases. The coronavirus has created remarkable disorder globally disturbing human life and severely causing a huge number of deaths. It was first noticed in Wuhan, China, December 2019. By analyzing the severity of the epidemic for a larger scale, the World Health Organization (WHO) was obligated to announce it as a pandemic in a short span due to its large-scale spreading. Individuals infected with COVID-19 have had a wide range of symptoms reported, ranging from mild symptoms to severe illness. Patients infected with the disease may have symptoms from days 2 to 14 subsequently after the contact to the virus. The symptoms are depicted in Table 12.1 [2, 3, 22–48].

The global pandemic of novel coronavirus pneumonia affects the hearts of people across the world. Scientists worldwide are searching for a vaccine to counter the virus, which is spreading across the world. The *rapid* growth of COVID-19 has created numerous problems in the governments' state of being able to retort systems while projecting and showcasing an incompetence to gauge the solution as to the growth of the epidemic. Determining the root cause of an epidemic, quarantining the infected patients, managing serious patients, and avoiding cross infection between healthcare professional do entail tremendous manpower and an increased pandemic threat further leading to great challenges worldwide along with tracing

N. Kamalakshi (✉)
Sapthagiri College of Engineering, Bangalore, Karnataka, India

Naganna
Dr. VRK Institute of Technology, Hyderabad, Telangana, India

H. L. Gururaj et al. (eds.), *Convergence of Internet of Things and Blockchain Technologies*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-76216-2_12

Table 12.1 Symptoms of COVID-19 [2]

Sl. no.	Symptoms
1.	High body temperature
2.	Cough
3.	Difficulty in breathing
4.	Weakness
5.	Body ache
6.	Headache
7.	Loss of taste or smell
8.	Sore throat
9.	Congestion
10.	Nausea

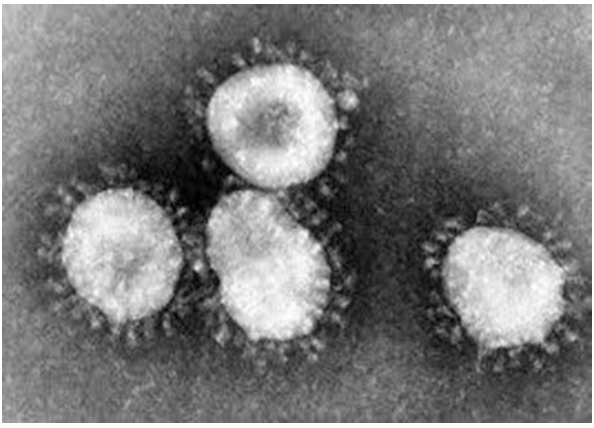


Fig. 12.1 Image of coronavirus

the origin of the epidemic to the first human infected, controlling and decreasing the infection of virus, and maintaining adequate medical resources to treat all the patients with severe symptoms. Figure 12.1 depicts the image of coronavirus.

Lots of contribution in terms of knowledge and expertise toward the implementations of government policies during this unprecedented and chaotic time was established [4]. The research community is striving very hard to invent vaccine and medicines to treat infected patients. Computer vision and image processing research community are working on medical image analysis to prevent and detect infectious patients using medical imaging techniques such as X-ray and computed tomography (CT). With the virus spread and continuous infection of people, most of the countries had declared lockdowns and curfews and social distancing as many of the sectors incorporated work from home to prevent, reduce, and control the infection of the disease. It has its impact on the global economy on various sectors such as supply chain, business, e-commerce, agriculture, transportation, and tourism [4]. As per the latest updates of the coronavirus pandemic, Table 12.2 depicts the total number of cases in the world.

Table 12.2 Total number of cases as of 24 October 2020 (Worldometer 2020)

Sl. no.	Content	Number of cases
1.	Confirmed cases	42,460,985
2.	Serious or critical	76,197
3.	Active cases	9,898,320
4.	Recovered/discharged	31,413,0176
5.	Deaths	1,148,689

The organization of this chapter is as follows: Section 2 introduces brief overview of blockchain technology used to combat the crisis in terms of supply chain management; section 3 presents a review of use cases and blockchain development toolkit; and finally, section 4 concludes the book chapter.

12.2 Blockchain Technology

Blockchain is a ledger of distributed decentralized secured transactions, by means of cryptocurrencies for all the industries and sectors. The technology has recently emerged as a key technology in the healthcare sector's digital transformation, and many research studies have identified the potential for blockchain to the healthcare ecosystem, and this provides patients as well as service providers with modern and digitized healthcare ecosystems [5, 6]. It is also exhibiting sufficient prospects to develop a fundamental quantity of being hostile for COVID-19 as it would support proficient tracing and observing solutions, ensure a transparent supply chain of vital products and donations, and secure payments. [2]

A peer-to-peer distributed ledger technology (DLT)-based platform "MiPasa" was launched by WHO in association with renowned software companies. The main objective of this association is to convey pandemic-related data to the community. It facilitates information among the public, state establishment, and healthcare organization. It aids in the early detection of the disease, its carriers, and occurrences across the world [7]. It helps in financial tracking and management, by providing an outlook mechanism for donors to see where there is financial urgency, and also entrusts by acknowledging the donor after it reaches the needy. Blockchain can also help to claim insurance for COVID-19-infected patients efficiently without human intervention, thus avoiding risk of infection. Blockchain-based platform can be used to trace the demand and the supply chains of medical supplies of epidemic prevention materials, such as masks, gloves, and other protective gear [6].

Blockchain data management systems build services for patients, physicians, and healthcare institutes in the fields of patient record access and monitoring, claims and payment processing, medical Internet of Things (IoT) protection management, clinical data verification and financial audit exchange, and transparency. Real-time updates to an encrypted, anonymous blockchain database are done in these applications to understand, track, and manage medical information. It also enables

restricting the unauthorized person's access to confidential information by healthcare organizations. Here, blockchain technology is used as a means to share reliable data of supply chain management in terms of supply of healthcare commodities and food for the needy during the outburst. It helps in tracking of appropriate information and assists in pace to complete the treatment process in terms of healthcare system. At the same time, it will preserve the person's identity.

In spite of all these advantages, there are certain drawbacks of blockchain technology such as the following [8]:

- High-energy consumption due to the requirement of high-end hardware resources.
- Scalability is the major issue of concern due to the fact that authentication necessitates time due to the authorization of transactions.
- The complication of blockchain aspects and the necessity of a wide-ranging network of users.
- Privacy preservation management is another big challenge [8].

12.2.1 Mathematical Model

The mathematical model frequently used with blockchain platform are the following:

12.2.1.1 Hash Function

A hash function is a function which transforms data of vast size into a predetermined size number. The main intension of a hash function is to distinguish an input using the output fixed size number [9]. The most famous hash function is SHA256, which transforms any message (a string) into a binary number of 256 bits SHA256 (blockchain) that is worth 625da44e4eaf58d61cf048d168aa6f5e492dea166d8bb54ec06c30de07db57e1 whereas SHA256 (blockchain) is worth ef7797e13d3a75526946a3bcf00daec9fc9c9c4d51ddc7cc5df888f74dd434 d1 [9].

12.2.1.2 Merkle Tree

A Merkle tree is a way of representing a potentially huge amount of data while providing the user with a simple way to check that the data have not been modified. To build a Merkle tree, let us consider a hash function H and a set of data: D = {d1, d2, . . . , dn}. Each leaf of the Merkle tree is represented by the hash values of the elements within D: H(d1), H(d2), etc. We can then build the tree recursively. Let us assume an entire layer L is known, the first node within the next layer is given by the hash value of the first two nodes within L, the second node is given by the hash value of the third and fourth nodes within L, etc. If there is an odd number of nodes

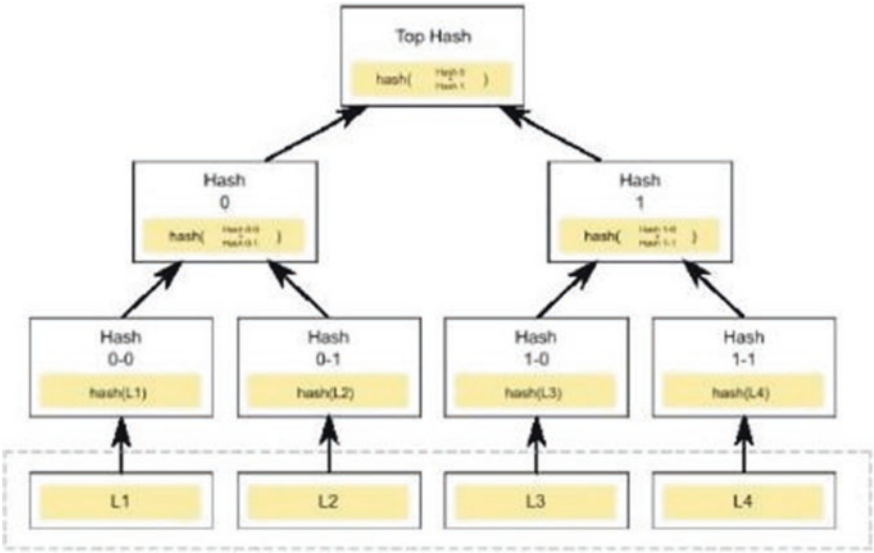


Fig. 12.2 Merkle tree [9]

within L, then the last node within the new layer is simply equal to the last node within L. To make the comprehension of Merkle trees easier, we provide the reader with a graphical example. We consider D = {L1, L2, L3, L4}, and Fig. 12.2 shows the corresponding Merkle tree [9].

12.2.2 Blockchain Supply Chain Management of Healthcare and Food

The global supply chain management system has a foremost impact across the world because of COVID-19 global supply chain. Due to lockdown, many of the healthcare industries are not able to manufacture adequate quantity of medicines. But blockchain with its sophisticated supply management systems will ensure that crucial medical equipment including vaccines, testing equipment, and other assistance aids are reachable to the suitable places in time and in the required quantities. It also keeps track of the supply chain by recording the shipments coming in and going out (Linda Lacina 2020).

With the worldwide pandemic catastrophe that has impacted all the company trade operations globally, the threat of foodstuff and basic necessity delivery is also imposing an enormous stress on food retailers over the entire world. In the inception of COVID-19, blockchain, being one of the emerging technologies, helps the food distributors in the midst of the epidemic and enable food distributors to work together with each other. The collaboration between agri-food distributors and other

logistics partners, to pilot blockchain for quicker international commodity trading in a short span of 5 days, initially focuses on the food crops such as wheat. The partnership and association have accomplished between the different continents product trade transaction of the food grain wheat from North America to Southeast Asia on a blockchain platform by a company called dltledgers, a Singapore-based company. The business deal of all the companies demonstrates the authority of partnership and association in ensuring the global agriculture supply chain delivers food in a time of uncertainty such as flood, drought, and pandemic. The trade transaction from the North America to Indonesia ensued with six trading partners participating on a blockchain platform [10].

12.2.2.1 Use Cases of Blockchain

The application of blockchain for curbing the coronavirus pandemic has been attracted and uncalculated from industry and research community with projects and use case trials. In this section, we provide an insight of the well-known popular use cases on blockchain used in China in response to fighting coronavirus.

12.2.2.2 Hashlog

Hashlog is a visualization tool of blockchain technology which provides interaction with Hedera Hashgraph's dispersed ledger transaction technology which works online to enable real-time logging and anticipation of data of the disease spread updates in time. This information is retrieved from the public data of the US Centers for Disease Control (CDC) and the World Health Organization (WHO). It provides real-time information for tracking the movement of infected person to prevent further spread of the disease. Hashlog was created by a Georgia-based health tech start-up Acoer [11, 12] (Linda Lacina 2020).

12.2.2.3 VeChain

VeChain, a blockchain-based platform, was used in China earlier; its main focus was to supervise vaccine manufacturing in China and to combat and tackle counterfeit face masks issue. It also monitors the manufacturing companies to ensure that new KN95 masks imported from China are genuine. All activities relating to medicine and pertaining to vaccine production from primary to concluding stages are kept track and further stored on distributed ledgers for later retrieval. It also aims to provide a reliable method to prevent and control the threat of manipulation of vaccine information [12, 13] (Linda Lacina 2020).

12.2.2.4 HyperChain

Managing transparency of information has been one of the furthermost thought-provoking responsibilities throughout the pandemic outburst. HyperChain is an enterprise blockchain and distributed ledger technology that concentrates on contribution and donation of fund tracking from the governments and various nonprofitable healthcare organization, and individuals to curb the pandemic outbreak. This platform emphasizes on ensuring that the donation process is indisputable, appreciable, and trustworthy. It provides a unique dashboard with an apparent digital portal that allows donors to inspect where their donated moneys are operating. By providing and collecting necessary proof of need and also proof of remit, this platform guarantees that the donations reach immediately to the authorized party [12, 14] (Linda Lacina 2020).

12.2.2.5 PHBC

PHBC stands for Public Health Blockchain Consortium. Its main objective is to monitor public health, free from the coronavirus outbreak, also concentrating on infection causers such viruses, bacteria, and fungi and implying control mechanism. This consortium concentrates and focuses on tracking the zones and areas of the cities with no confirmed cases of pandemic. It helps the healthcare systems in monitoring the movement of uninfected persons and helps in alerting and controlling and restricting their revisit back if they have visited infected regions and locations, in order to prevent the spread in safe zones [12, 15] (Linda Lacina 2020).

12.2.2.6 Blockchain Deployment Toolkit

Blockchain technology plays a vital role to overcome the supply chain issues of COVID-19 pandemic and further can enhance the recovery mechanism for economic process post COVID-19. Further, the World Economic Forum (WEF) introduced a kit called as "blockchain deployment toolkit" to progress outlook in pandemic preparedness and to speed up an economic rebound post COVID-19 [16]. It stated that the COVID-19 crisis significantly increases the demands on government, enterprises, and businesses sector to retain resilient supply chains. "The demand formed by the pandemic on worldwide operate systems insights a vital requirement for world wide collaboration to sustain and reinforce the resilience of worldwide supply chains," as stated by the WEF. It is supposed to enable influence in maximizing the benefits while minimizing the risks of the technology. Resilience mechanism in supply chains aspect mainly focuses on confidence, precision, and honesty; through the enhancement, it strives for the best deployment of blockchain technologies with real cause, according to the WEF. It further said that the current pandemic underscores the need for businesses. This concept was initiated and introduced by the World Economic Forum [16]; the details are in Table 12.3.

Table 12.3 World Economic Forum

Sl. no.	Contribution	Agency benefitted	Toolkit
1.	Center for the Fourth Industrial Revolution UAE	Government	The Abu Dhabi Digital Authority
2.	Port of Los Angeles	Companies	
3.	Latham and Watkins		
4.	Cardiff business school		
5.	University of Berkeley	Civil society	
6.	Tech Mahindra	International organizations	

Table 12.4 World Economy Forum organization [16]

Sl. no.	Name of the company	Toolkit	Country
1	IBM	Rapid Supplier Connect Initiative	USA and Canada

Details for blockchain start-ups that transform the supply chain sector are in Table 12.4.

- **Block Verify:** This start-up provides the insight on enhancing anti-counterfeit actions. It also tracks and checks the products, goods, merchandise, and transactions [17].
- **Everledger:** This blockchain-based platform start-up helps in tracking the provenance of rich goods such as diamonds. It also helps in detection of the fraud and risk reduction [17].
- **OpenPort:** A blockchain platform for supply chain management with improved performance and optimization. It also provides a direct connection between the shipment and delivery sector; keeping expenses reduction has a highest priority [17].
- **OriginTrail:** A blockchain-powered composed of protocol for ensuring exchange of data in interconnected supply chain management sector [17].
- **Provenance:** An emerging blockchain company emphasizing on transparent information and open access in the supply chain mechanism and for the sale purpose [17].
- **ShipChain:** A blockchain-based freight platform following smart contract applications which is best suited for logistics industry [17].
- **Skuchain:** Ensures protection and transparency for the global supply chain Bitcoin network [17].
- **SyncFab:** Ensures visible order tracking and procurement order management protected by blockchain [17].

Supply chain management challenges and issues are rising in complication and prohibiting the expansion of the intact business, comprising all the sectors related to the economy that are entangled with it, such as trade, industrialized, and logistics. In spite of all these issues, the supply chain management (SCM) market is predicted

Table 12.5 Blockchain start-ups transforming the supply chain industry [16]

Sl. no.	Content	Number of cases
1	Block Verify	Anti-counterfeit
2	Everledger	Provenance
3	OpenPort	Directly connecting shippers
4	OriginalTrail	Is composed of protocol for ensuring exchange of data in interconnected supply chain management sector
5	Provenance	Emphasizes on transparent information and open access in the supply chain mechanism and for the sale purpose
6	ShipChain	Freight platform pursuing smart contract applications
7	Skuchain	Cryptographic principles

to reach beyond the expectation through the process of automation of its operations, representing a significant role for blockchain novelties in the supply chain management sector (Table 12.5).

12.2.3 Impact of COVID-19 Effect on Supply Chain

The COVID-19 pandemic has impacted major demands and tension on supply chains, further raising challenges such as shortfall of the product, hindrance in delivery, and extra expenses and burden. At this juncture, the resilience of supply chains has attracted the business community both in digitally online and offline method platforms all over the globe, with several domain experts, business professionals, and manufacturing insiders having an expectation that the world will appear enormously diverse after the lockdown [17].

The prospect by various professional and experts in this field is the great progress by organizations toward a digitization approach where technology is a prime initiative force in upcoming policymaking. The new avenue of Industry 4.0 aspects contains prospective to start up new venture for developing various software tools and application to facilitate features which are apparent and observable and provide rapid relocation of refined data and business deals. For this, one such emerging technology is the blockchain which has the prospective to convey distinctive assessment to supply chain management sector. This distinctive way of creation of data storage helps in proficient and successful transport of commodities and services with minimal expenses. Further, supply chains continue to nurture, amalgamate, and lead to multifaceted ecosystems composed of many entities functioning jointly to accomplish consumer requirements by accumulating importance commencing from the initial stage to the concluding fulfillment procedure; the task of software tools and technological aspects in organizing the course of action has become a crucial aspect. Also, there is a prerequisite for informational transactions to match the trust and to provide simplicity and traceability with the supply chain sector, which is a mandatory aspect.

The expedition of blockchain within the supply chain sector will follow this purpose in the first instance. The blockchain platform upon proper implementation in a suitable manner is able to create provable, indisputable records of the communication within the supply chain, thus enhancing confidence and constructing information-resilient supply chains [18].

BelfricsBT and YoSync are blockchain-based start-up companies. They were developed at IIITB-IMACX Studios. A written-contract Memorandum of Understanding (MOU) was signed as a research collaboration with IIIT Bangalore to jointly develop BelYo, a COVID-19-tracking blockchain platform. The company Mphasis F1 Foundation came forward for proposal funding. The platform is currently being tested in a few clinics and will be reaching out to ICMR-approved government labs and private labs. BelYo aims to use the BelfricsBT Belrium block to convert COVID-19-associated medical and vaccination data of people presently from the raw data into digital effects which can be used by any contact-tracing apps like Aarogya Setu. Anyone can be able to scan and retrieve data through a QR code [19].

12.2.4 IoT Blockchain Platform Nodle Launches Coalition

Recently, a start-up company based on Internet of Things (IoT) technology named Nodle.io has launched Coalition, an app to trace the contact in order to avoid the spread of COVID-19 pandemic. The app emphasizes to preserve the privacy of the intended users by storing the contents locally on the phone. The app aims to use low-energy consumption of the company Nodle's Bluetooth. Its network can be used to create communication with neighboring devices. The user can download the app and further turn on Bluetooth; then, the app will start recording unidentified encounters with other Coalition users nearby.

A protocol called Coalition Whisper Tracing is used in the application to generate a random unidentified ID of the user's identity. If a user asserts that they are sick, the unidentified IDs from the phone are sent to the cloud for the storage. The app on another user's phone can then download these "infected" IDs and compare it with the IDs stored locally. This approach can help other users as well and is notified if they came in contact with an infected person [20].

12.2.5 Emerging Blockchain Pilots Post COVID-19 [18, 21]

In the recent years, few of the renowned companies, such as International Business Machine, Walmart Inc., Zurich Insurance Group, Maersk, Nestlé S.A., Unilever, and Amazon, have come forward and invested in pilot blockchain-based supply chain projects to design and develop software products and applications and also to test the technology for the benefit of various sectors as depicted in Table 12.6.

Table 12.6 Blockchain pilots post COVID-19

Sl. no.	Content	Number of cases
1	International Business Machine	FDA tracing prescription drugs and vaccines
2	Walmart	Food traceability
3	Zurich Insurance	Insurance payment Tracking
4	Maersk	Business environment which has seen record numbers of employees working from home for safety reasons while performing day-to-day operations. Record demand for online business transactions has increased the Maersk shipments app usage by nearly 90%
5	Nestlé	Chain of origin of the products

12.3 Conclusion

Blockchain is an emerging trend that can be used to combat COVID-19. The main focus of the blockchain technology is to fortify the processes of healthcare and thus patient outcomes to combat the infection (COVID-19). Blockchain can aid in many ways: minimizing transaction costs, medical supply chain management, and donation tracking. This chapter provides a glimpse of various use cases of blockchain and its deployment toolkit in supply chain management to boost up the economy post COVID-19, start-ups, and emerging blockchain pilots post COVID-19.

References

1. Lai, C.-C., Shih, T.-P., Ko, W.-C., Tang, H.-J., & Hsueh, P.-R. (2020). Severe acute respiratory syndrome coronavirus 2 (sars-cov-2) and corona virus disease-2019 (covid-19): The epidemic and the challenges. *International Journal of Antimicrobial Agents*, 105924.
2. Marbouh, D., Abbasi, T., & Omar, I. (2020, July). Blockchain for COVID-19: Review, opportunities and a trusted tracking system. *Arabian Journal for Science and Engineering*. https://doi.org/10.1007/s13369-020-04950-4. https://doi.org/10.36227/techrxiv.12609344.
3. Coronavirus Disease 2019 (COVID-19). (2020, May). *CDC Center for Disease Control and Prevention*. Retrieved June 2020, from, https://www.cdc.gov/coronavirus/2019-ncov/symptoms-testing/symptoms.html
4. Economic Outlook. (2020). https://www.oecd.org/economic-outlook/
5. Radanović, I., & Likić, R. (2018). Opportunities for use of blockchain technology in medicine. *Applied Health Economics and Health Policy, 16*(5), 583–590.
6. Vora, J., et al. (2019). BHEEM: A Block chain-Based Framework for Securing Electronic Health Records. In *2018 IEEE Globecom Work. GC Workshops 2018 - Proceedings* (pp. 1–6) https://www.worldometers.info/coronavirus/.
7. Nguyen, C., Ding, M., Pathirana, P. N., & Seneviratne, A. (2020). *Blockchain and AI-based Solutions to Combat Coronavirus (COVID-19)-like Epidemics: A Survey*. Preprint.

8. Sharma, A., Bahl, S., Bagha, A. K., et al. (2020). Blockchain technology and its applications to combat COVID-19 pandemic. *Research on Biomedical Engineering*. https://doi.org/10.1007/s42600-020-00106.
9. Coperneec. (2020). Blockchain through a mathematical model. *Coperneec, 2020*.
10. https://www.industrialautomationindia.in/articleitm/9715/How-Blockchain-is-Helping-Food-Supply-chain-During-Covid-19/articles
11. Acoer Coronavirus Tracker, Powered by HederaHashgraph, Now Freely Available to General Public with Added Clinical Trial Data. https://www.hedera.com/blog/acoer-coronavirustracker-powered-by-hedera-hashgraph-now-freely-available-to-generalpublic-with-added-clinical-trial-data
12. Gomez, M., Bustamante, P., Weiss, M. B., Murtazashvili, I., Madison, M. J., Law, W., Mylovanov, T., Bodon, H., & Krishnamurthy, P. (2020). *Is Blockchain the Next Step in the Evolution Chain of [Market] Intermediaries*? Retrieved June 25, 2020, from https://ssrn.com/abstract=3427506
13. VeChain Announces Blockchain Vaccine Tracing Solution for China. https://www.nasdaq.com/articles/vechainannounces-blockchain-vaccine-tracing-solution-china-2018-08-16.
14. HyperChain-Blockchain Charity Platform to Fight Against the Coronavirus. https://www.hyperchain.cn/en
15. Public Health Blockchain Consortium: PHBC. ttps://www.phbconsortium.org/
16. https://www.weforum.org/agenda/2020/04/blockchain-development-toolkit-implementation-supply-chains-in-a-post-covid-world
17. blockchain-council. (2020). https://www.blockchain-council.org/blockchain/blockchain-use-cases-to-fight-covid-19/?utm_source=organic&utm_medium=boolmarking&utm_campaign=seo
18. Startus 2020. http://www.startus-insights.com/innovators-guide/8-blockchain-startups-disrupting-the-supply-chain-industry/
19. EconomicTimes. (2020). Retrieved July 24, 2020, from https://economictimes.indiatimes.com/small-biz/startups/newsbuzz/covid-19-tracking-blockchain-platform-launched/articleshow/77146407.cms
20. LedgerInsights. (2020). https://www.ledgerinsights.com/covid-19-contact-tracing-iot-blockchain-nodle
21. Jabar, A., & Dani, S. (2020). https://boardagenda.com/2020/08/13/blockchain-supply-chains-and-the-post-covid-world
22. Abelseth, B. (2018). Blockchain tracking and cannabis regulation: Developing a permissioned blockchain network to track Canada's cannabis supply chain. *Dalhousie Journal of Interdisciplinary Management, 14*.
23. WHO/Europe | Coronavirus disease (COVID-19) outbreak. Retrieved June 28, 2020, from http://www.euro.who.int/en/health-topics/health-emergencies/coronavirus-covid-19
24. Linn, L. A., & Koo, M. B. (2016). Blockchain for health data and its potential use in health IT and health CareRelated research. *ONC/NIST Use of Blockchain for Healthcare and Research Workshop*, 1–10.
25. Kshetri, N., & Nir, K. (2018, 2018). Blockchain and electronic healthcare records. *IEEE, 51*.
26. Yaqoob, S., Khan, M., Talib, R., Butt, A., Saleem, S., Arif, F., & Nadeem, A. (2019). Use of block-chain in healthcare: A systematic literature review. *International Journal of Advanced Computer Science and Applications, 10*, 644–653.
27. Randall, D., Goel, P., & Abujamra, R. (2017). Blockchain applications and use cases in health information technology. *Journal of Health & Medical Informatics, 08*(03), 8–11.
28. Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. *Journal of Medical Systems, 40*(10), 1–8.
29. Kalla, A., et al. (2020). The role of blockchain to fight against COVID-19. *IEEE Engineering Management Review, 99*. https://doi.org/10.1109/EMR.2020.3014052.

30. Jayaram, R., Ellahham, S., Khatoon, A. (2020). *Use of Blockchain Technology to Curb Novel Coronavirus Disease (COVID-19) Transmission*.
31. Torky, M., & Hassanien, A. E., *COVID-19 Blockchain Framework: Innovative Approach*.
32. Wright, T. (2020). Blockchain app used to track COVID-19 cases in Latin America. In *Coin Telegraph: The future of money*. Retrieved May 29, 2020, from https://cointelegraph.com/news/blockchain-app-usedtotrack-covid-19-cases-in-latin-america.
33. Dragov, R., Croce, C. L., & Hefny, M. (2020). How blockchain can help in the COVID-19 crisis and recovery. In *IDC-Analyze the Future*. Retrieved May 27, 2020, from https://blog-idcuk.com/blockchain-help-in-the-covid-19-and-recovery/.
34. Blockchain and crypto firm VeChain utilized to confirm authenticity of coronavirus KN95 masks. Blockchain Magazine, 2020, April 20. Retrieved May 27, 2020, from https://www.blockchainmagazine.net/blockchainandcrypto-firm-vechain-utilized-to-confirm-authenticity-ofcoronaviruskn95-masks/
35. Singh, G., & Levi, J. (2020). MiPasa project and IBM Blockchain team on open data platform to support Covid-19 response. *IBM*. Retrieved May 27, 2020, from https://www.ibm.com/blogs/blockchain/2020/03/mipasaprojectand-ibm-blockchain-team-on-open-data-platform-tosupportcovid-19-response/.
36. Coalition: Help stop the spread. Retrieved May 27, 2020, from https://www.coalitionnetwork.org/.
37. Joshi, M. (2020). PHBC announces blockchain monitor to track virus-free zones. *Cryptopolitan*. Retrieved May 27, 2020, from https://www.cryptopolitan.com/phbc-blockchain-monitor-for-virus-free-zones/.
38. Chang, M. C., & Park, D. (2020). How can blockchain help people in the event of pandemics such as the COVID-19? *Journal of Medical Systems, 44*(102), 2020.
39. Zhang, J. (2020). Chinese startup launches blockchain platform to improve donation efficiency. Tech in Asia, 14 Feb. 2020. Retrieved May 27, 2020, from https://www.techinasia.com/china-blockchain-platform-donation
40. Acoer. (2020). Providing daily tracking and visualizations of the pandemic. *Coronavirus (COVID-19) Tracker*. Retrieved May 27, 2020, from https://www.acoer.com/coronavirus.
41. Buterin, V. (2013). A next-generation smart contract and decentralized application platform. *Ethereum White Paper*. Retrieved January 19, 2020, from http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_ generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf.
42. Hasan, H., & Salah, K. (2018). Blockchain-based solution for proof of delivery of physical assets. In *Proceedings of the International Conference on Blockchain (ICBC 2018). Springer LNCS, Seattle, USA, June 25–June 30, 2018*.
43. Piscini, E., Dalton, D., & Kehoe, L. (2017). *Blockchain & Cybersecurity Point of View*. Deloitte. Retrieved June 2, 2020, from https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Technology/IE_C_BlockchainandCyberPOV_0417.pdf.
44. Tlelo-Cuautle, E., Díaz-Muñoz, J., González-Zapata, A., Li, R., León-Salas, W., Fernán-dez, F., Guillén-Fernández, O., & Cruz-Vega, I. (2020). Chaotic image encryption using hopfield and hindmarsh- rose neurons implemented on FPGA. *Sensors, 20*(5), 1326.
45. Salah, K., Nizamuddin, N., Jayaraman, R., & Omar, M. (2019). Blockchain based soybean traceability in agricultural supply chain. *IEEE Access, 7*(1), 73295–73305. https://doi.org/10.1109/ACCESS.2019.2918000.
46. van den Hooff, J., Kaashoek, M. F., & Zeldovich, N. (2014). VerSum: verifiable computations over large public logs. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, New York*.
47. Solat, S., & Potop-Butucaru, M. (2016). ZeroBlock: Timestamp-Free Prevention of Block-Withholding Attack in Bitcoin.
48. Benchoufi, M., & Ravaud, P. (2017). Blockchain technology for improving clinical research quality. *BioMed Central, 18*, 1–5.

Chapter 13
Beyond the Bitcoin: Analysis of Challenges to Implement Blockchain in the Jordanian Public Sector

Abeer F. Alkhwaldi and Fairouz M. Aldhmour

13.1 Introduction

Information and communication technology (ICT) is a notable enabler for social relations and communication worldwide at an outstanding speed and reach compared to all earlier technologies in human history. For instance, the Internet has changed the human understanding of time and space, both intensifying and expanding human relations and organizations. It also turned the world into a global village [1]. Blockchain is a disruptive emerging ICT that is changing the interactive impact of human relations through supporting trust technologies. Blockchain (BC), as a general-purpose technology, is considered as one of the vital technology trends that will affect societies and organizations in the years to come [2]. In recent years, Blockchain technology (BCT), which first came into prominence by Satoshi Nakamoto in 2008, has been a subject of great interest in different fields and many countries [3]. In general, BCT is referred to as "…a distributed ledger that maintains a continually growing list of publicly accessible records cryptographically secured from tampering and revision" [4]; see Fig. 13.1.

Around the world, governments and public services entities are starting to investigate the potential benefits of integrating BCT applications into the public services sector. It is believed that BCT has great potential for use in government entities, such as transparency improvement, fraud prevention, data integrity and quality,

A. F. Alkhwaldi (✉)
Department of Management Information Systems, School of Business, Mutah University, Mutah, Jordan
e-mail: abeerkh@mutah.edu.jo

F. M. Aldhmour
Department of Innovation and Technology Management, Arabian Gulf University, Manama, Bahrain
e-mail: fairouzm@agu.edu.bh; fairouz@mutah.edu.jo

H. L. Gururaj et al. (eds.), *Convergence of Internet of Things and Blockchain Technologies*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-76216-2_13

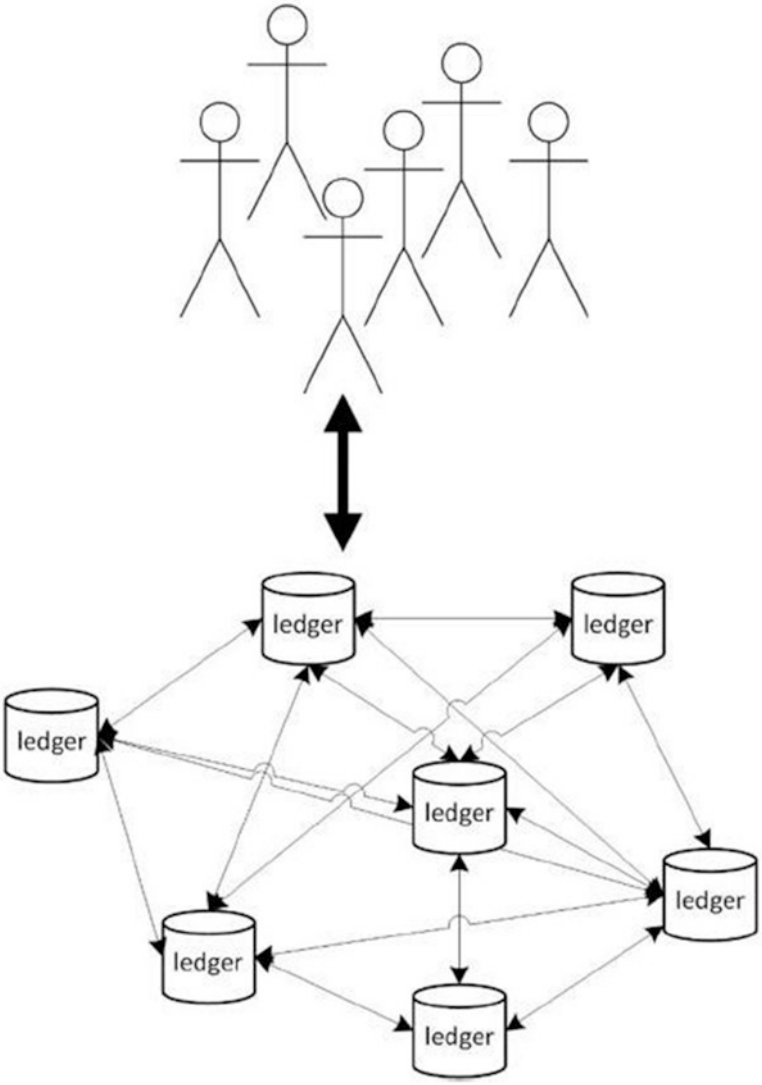


Fig. 13.1 Distributed ledgers (Blockchain technology) [2]

keeping sensitive information private and secured, corruption reduction, and trust enhancement [5, 6]. These benefits have attracted the attention of the public sector in many countries in terms of corruption elimination and transparency. Guided by pioneering initiatives in developed countries, such as the United Kingdom, the USA, Estonia, the Netherlands, and Sweden [7], BCT has successfully progressed toward being the next generation of innovative technology in the eGovernment context. Some of the BCT benefits, such as transparency and trust, can be particularly

beneficial for developing nations since they are more vulnerable to fraud, corruption, and lack of trust compared to developed countries.

Recently, governments in the developing countries, the Middle East (ME) in particular, have started to gear toward initiatives to actively explore BCT use in public services (e.g., the United Arab Emirates) [8]. However, a number of these countries are still at a rudimentary stage. In 2018, the Jordan government published its general policy for ICT; this policy aims to "seize the opportunities of the Fourth Industrial Revolution with the primary goal being the development of a digital economy leading to renewed economic development and increased income and wealth of individual Jordanians." The Jordanian government sector has long been striving to promote the development of online government services by using ICT (e.g., artificial intelligence (AI) and the Internet of Things (IoT) as well as Blockchain) in the public sector to accelerate digital transformation, along with technological and social development [9]. The use of BCT in the eGovernment system is part of this development. For instance, the Customs Department in Jordan has recently announced a pilot of the "TradeLens Blockchain supply chain platform" to offer advanced efficiency and transparency to the communication between trading counterparties, documentation processes, and exchange of goods [10]. However, regulators' reactions toward BCT initiatives in the ME vary from being very encouraging, such as in the United Arab Emirates, to having a kind of resistance, such as in Jordan. Data analysis in Ghazawneh's (2019) study indicated that in 2016, the Central Bank of Jordan issued a declaration that prevents its employees and the banks in HJK to deal with BCT [8].

Blockchain is a relatively new technology of the eGovernment system, yet it continues to progress quickly. This research intends to investigate the factors prohibiting the government organizations from having efficient use of BCT. Thus, the current study proposed here is to utilize the theoretical lens of the unified theory of acceptance and use of technology (UTAUT) to examine the original UTAUT variables and explore the relationships that lead to the factors affecting BCT adoption for eGovernment services in Jordan. As has been stated in recent literature, BCT can significantly contribute to making the government sector trusted and more open while unlocking the potentials of the public sector and citizens toward a more collaborative, secure, and managed service. However, since the BCT field is still in its infancy, multiple challenges (e.g., technical, organizational, and regulatory) exist, which demanded further investigation. This paper made a contribution in this direction; hence, the aim of this study is to identify the barriers of BCT application in the Jordanian public sector. These can be taken into account when developing a new theoretical framework and shaping the directions of future work in the Government 3.0 field.

13.2 The Challenges of Applying Blockchain Technology to the eGovernment System

Blockchain technology aims to contribute to setting up citizens' accounts to access eGovernment services and enhance governance. In addition, BCT can be used to provide individuals with access to trustworthy and reliable government information, which can support public sector credibility. BCT can be used to store information related to transactional data, such as birth/marriage certificates, educational certificates, vehicle registries, ownership of land registry, and loans [2, 11, 12]. However, a number of scholars indicate that there are many barriers encountered by government institutions that obstruct the realization of BCT-promised potentials and degrade its effective adoption in the public sector [4, 6, 13, 14]. Therefore, governments have the responsibility to overcome these hurdles. In spite of public sector efforts in this respect, the success of BCT initiatives is based likewise on IT employees' willingness to use and adopt Blockchain technology for eGovernment services.

The challenges of BCT adoption in the domain of eGovernment services are associated with some difficulties and are categorized and listed in Table 13.1.

Compared to a large number of research articles that address the challenges of BCT adoption from a technology perspective, relatively limited literature exists regarding different types of challenges influencing the adoption of BCT for eGovernment. Also, little has been done to understand the challenges of BCT in the ME region, Jordan in particular [8]. Thus, more empirical investigation is required to explore the barriers of the adoption of BCT in the Jordanian public sector. For this study, an online questionnaire was employed to achieve this aim.

13.3 Blockchain in Government

Evidence from the recent literature shows that BCT can be adopted for information exchange or for transactions that take place in the public sector [5]. The fundamental characteristics of BCT offer some prospective benefits in a wide range of public services, for example, asset registry, both physical (e.g., property) and intangible (votes and patents) assets [12, 16]. Some of these benefits are transparency, immutability, and distributed architecture, which might help to eradicate corruption and fraud in governments [4, 17]. The essence of BCT is that government organizations can keep track of a "distributed ledger" and that these organizations jointly create, develop, and keep track of one immutable history of public sector transactions as well as figure out successive events. Governments worldwide are managing pilots using BCT. If the promising benefits and significant challenges of BCT could be confirmed, it is possible that the technology would reach an inflection point and commence obtaining widespread acceptance and adoption by the public sector in general in the near future. Yet, Ølnes et al. [2] stated that the potential benefits of this innovative technology as well as its challenges have not been confirmed by

Table 13.1 Blockchain challenges in eGovernment

Challenges	Examples	References
Technical factors		
Cost	• Cost of establishing a new Blockchain • Based platform/cost-effectiveness	[4, 6]
Security and privacy	• The information security of Blockchain technology/cybersecurity issues • Cybercrime • Privacy leakage	[4–6, 13, 15]
Trust	• Trust of the technology	[5]
Information exchange and transactions	• Time to process transaction • Size of the block • Scalability • Standardization • Usability • Interoperability/compatibility • Reliability • Fixability • Computation efficiency • General application platform • Selfish mining	[2, 4–6, 11, 13]
Distributed ledger	• Design of the system/design variables • Newness	[6, 13]
Storage	• Storage size • Immaturity	[6]
Technical infrastructure	• Support infrastructure • Accessibility (the matter of the digital divide)	[2, 6]
Institutional/organizational factors		
Organization support	• Management responsibility of the Blockchain platform • Organizational readiness • Business model/organizational transformation	[4, 6, 11]
Norms and cultures	• Cultural resistance • Resistance to change/acceptability • Lack of understanding of Blockchain technology	[13]

(continued)

Table 13.1 (continued)

Challenges	Examples	References
Regulations and legislations	• The need for introduction of a new law • Ability of law enforcement agencies to deal with fraudulent activities • Confusion of policymakers in Bitcoin with Blockchain technology • Need to deal with taxation • Laws should take into consideration the nature of Blockchain technologies • Laws and regulations support • Legally binding • Applicability in terms of General Data Protection Regulation (GDPR)	[5, 13, 15]
Governance	• Government losing control • Using an appropriate governance framework • Risk of market manipulation and unfair practices	[2, 6, 11, 13]
	• Risk of error for complex business rules • New governance model • Implications • Trust • Auditing	
Market factors		
Market structure	• High degree of computerization increases in market volatility • Interconnectedness • Moving an existing contract to a new Blockchain technology methodology • Lack of clarity on smart contracts • Confusion of smart contracts with eContracts	[13]
Business processes	• Inability to apply traditional business processes for using Blockchain technology • Cost of adoption and implementation of Blockchain technology for businesses	[13]

empirical evidence. As a result, further interdisciplinary studies in broader aspects of BC, such as proposed theoretical models and extended variables, are needed. Therefore, this study reviewed the literature to map the challenges of BCT adoption in the government domain (see Table 13.1). In the following sections, these challenges will be proven empirically.

13.4 Acceptance and Adoption of New ICT: Theories and Models

IT/IS users' acceptance research addresses one of the most vital issues in the management information systems (MIS) field. So far, scholars have proposed many competing theoretical models to understand technology acceptance behavior: the theory of reasoned action (TRA), the theory of planned behavior (TPB), the theory of reasoned action (TRA), and so on [18]. A comprehensive theoretical model was needed with the aim of understanding users' acceptance of IT. In 2003, Venkatesh et al. developed UTAUT as integration and consolidation of the findings of previous research on this issue [18]. The UTAUT model incorporates four core antecedents (performance expectancy (PE), effort expectancy (EE), social influence (SI), and facilitating conditions (FC), which influence both behavioral intention (BI) and actual behavior. Age, gender, voluntariness, and experience have been found to moderate the relationships of the key constructs. The same is shown in Fig. 13.2.

The UTAUT relationships have been extensively proved in the context of eGovernment systems [19–23]. Therefore, the unified theory (UTAUT) is suitable for understanding the acceptance of Blockchain technology for eGovernment services.

Blockchain technology acceptance literature has been relatively limited in terms of application to the public sector. Therefore, there is a need to gain empirical investigation for theoretical models of IT acceptance within the context of the public sector and to study technology utilization issues among IT employees to advance the success of technology implementation in this arena. The suggested model builds upon the existing UTAUT by integrating contextual characteristics as primary influencing constructs, based on the findings of this research. These constructs will be considered as enhancing factors to predict users' motivations to accept Blockchain technologies.

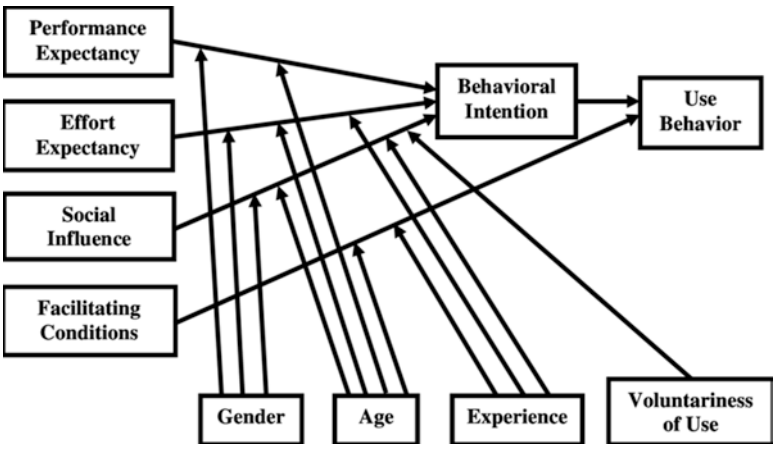


Fig. 13.2 Unified theory of acceptance and use of technology [18]

13.5 Research Methodology

A quantitative research method based on an online questionnaire was selected to meet the aims of this study. A survey questionnaire was used as it is low cost in terms of both money and time. It also has the ability to offer an inflow of collected data from a large sample with minimum bias from the researcher, and respondents' anonymity can be guaranteed [24]. After the initial design of the online survey, a pretest was conducted by postgraduate researchers, academic staff in the department of management information systems (MIS), and some of the IT staff in the Jordanian public sector. This was important to improve questions and check the respondents' understanding before the distribution of the final version of the questionnaire [25]. This resulted in some revisions to the wording of a few questionnaire items. The online survey was developed to determine what IT employees in the Jordanian public sector perceived to be challenges confronting the acceptance of BCT in eGovernment systems. Because Blockchain is a relatively new technology in developing countries, the researchers stated the definition of this new concept on the first page of the online questionnaire. The online questionnaire link was advertised to the targeted research sample through different communication channels, such as social media groups, personal emails, and official mailing lists. In general, the study sample can be classified as IT employees, such as software/system engineers, web designers, and programmers. Participants were approached to take part in this study if they had knowledge and experience in the field of Blockchain for eGovernment services. The survey is divided into two parts: part one is general participants' information, and part two is participants' perceptions about barriers facing the acceptance of BCT for public services.

13.6 Data Analysis and Findings

The following two sections highlight the key findings and present indications as to how the study questions could be answered by drawing on the data analysis. The first section presented an overview of the online questionnaire, and then, the following section illustrated the implications for the study questions in more detail.

13.6.1 Overview of the Online Questionnaire

As outlined above, the online questionnaire consisted of two parts. It was presented in both Arabic and English as the sample consisted of qualified IT employees. Although the native language in Jordan is Arabic, the English language is prevalent in the academic and ICT sectors. Involvement in the online survey was entirely voluntary, and informed consent was received through the first question in the

introduction page, indicating that explicit consent by the "yes" answer to the question. The survey was built using the online questionnaires' website (*forms.office.com*) and was available to all targeted study samples during February 2020. The review of the collected data led to discarding five straightliners and two incomplete responses for a total of 221 surveys. This resulted in 213 valid responses to be used in the data analysis. People who understood Blockchain technology (ICT employees in the public sector) were qualified respondents. This stems from the fact that this sample represents the adult population group who has basic knowledge and understanding of BCT for eGovernment services use. Furthermore, since the development of BCT in Jordan is in the early stage, the participants will be the main potential developers, adopters, and users. Accordingly, knowledge of their attitudes and perceptions is critical for the successful adoption of BCT in the Jordanian eGovernment context. The analysis findings are described below.

13.6.2 Demographics Statistics

Table 13.2 summarizes the participants' samples who completed the first section of the survey by providing their personal information. In this table, only selected demographic profiles, namely, gender, age, level of education, and awareness/knowledge level of Blockchain technology, were listed by the researchers.

Data showed evidence that about two-thirds (71.4 %) of participants were male and one-third (29.6%) were female. The bias toward males is due to the fact that HJK is one of the developing nations that is considered as a male-dominated society. For instance, females occupy around 30% of ICT sector jobs in Jordan [26]. The

Table 13.2 Personal data on the basis of survey

Description	Percentage (%)	Frequency
Gender		
Male	71.4	152
Female	28.6	61
Age		
21–30	39.9	85
31–40	54	115
41–50	6.1	13
Educational level		
Bachelor	62	132
Master's degree	30	64
PhD degree	8	17
Awareness/knowledge level of blockchain technology		
Beginner	3.8	8
Medium	67.1	143
Advanced	29.1	62

respondents' ages were mainly between 21 and 40 years old (93.9 %), which is consistent with the publications of the Jordanian Department Of Statistics concerning the population ages in 2019 [27]. Most of the participants held a bachelor's degree, which comes in agreement with the Ministry of Higher Education (MoHE) statistics [28]. In general, the participants were self-identified as having medium-level BCT knowledge and awareness.

13.6.3 Challenges of Applying Blockchain Technology in the eGovernment Context: Interpretation of the Research Question

According to the results, there are a number of barriers (e.g., technical, institutional, and market factors) that obstruct the adoption and use of Blockchain technology in the Jordanian public sector from the respondents' perspective (see Fig. 13.3). Table 13.3 shows these challenges; the responses were ranked based on a set of factors that the IT employees in public sector identified as being very challenging or challenging in BCT's successful adoption.

Challenges associated with technological aspects evidently dominate the findings from the online survey. Interestingly, security, privacy, and trust, as being the main strengths of BCT [1, 4, 6, 29], are still questioned by the study sample as well as some scholars. From the table above, it is clear that about 92% and 91% of the respondents cited security, privacy, and trust, respectively, as being significant concerns of BCT adoption in the Jordanian public sector, thus making them the first- and second-ranked barriers of BCT use.

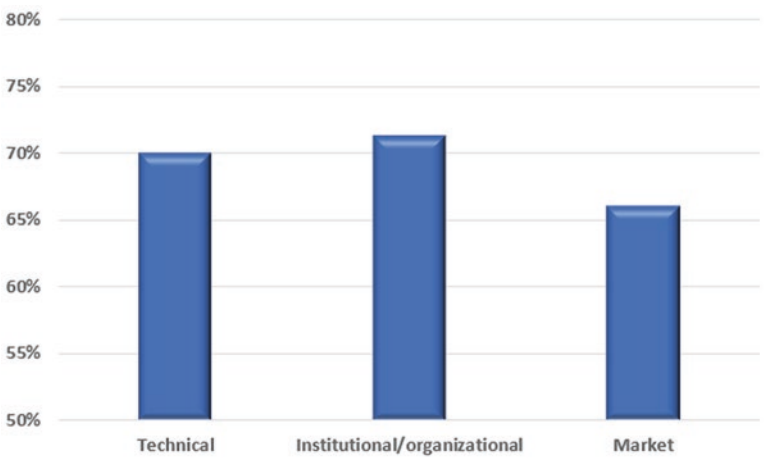


Fig. 13.3 Challenges to adopting BCT in the e-government context

Table 13.3 Challenges of blockchain technology

	Percentage of responses				
	Very challenging	Challenging	Natural	Less challenging	N/A
Technical factors					
• Cost	54%	9%	8%	31%	0%
• Security and privacy	76%	16%	2%	7%	0%
• Trust	71%	20%	4%	5%	0%
• Information exchange and transactions	63%	9%	10%	15%	3%
• Distributed ledger	52%	12%	10%	26%	0%
• Storage	36%	11%	11%	39%	3%
• Technical infrastructure	39%	22%	8%	20%	11%
Institutional/organizational factors					
• Organization support	45%	21%	6%	28%	0%
• Norms and cultures	68%	17%	5%	8%	2%
• Regulations and legislations	57%	22%	6%	15%	0%
• Governance	36%	19%	11%	27%	7%
Market factors					
• Market structure	26%	41%	6%	19%	8%
• Business processes	21%	44%	19%	14%	0%

Blockchain technology aims to change the way of establishing the authenticity of records and transactions to a system-based mode instead of reliance on a trusted third party [13]. According to Hou [4], "at present, the biggest danger actually comes not from system vulnerabilities, but from blind trust in the Blockchain on the part of Blockchain developers, lawmakers, law enforcement and the general public. This trust relies exclusively on the technology, rather than management to make sure the system is trusted and the records in the system are reliable." There is no guarantee that BCT will ever make any mistakes, and if this technology platform was extensively used in an eGovernment context for the services and transactions that contain personal and private information, one fault may result in serious consequences.

The main characteristics of decentralized transactions are security and privacy. The core aim of the records' management process in the public sector is to make sure that records and transactions can be trusted. The security system of eGovernment services using the BCT platform should include data security, physical security, secret key security, risk management, and application systems security. Building secure systems can increase the protection of normal operations to higher levels and also maintain the trustworthiness of a record within the platform.

13.7 Conclusion

Being a type of data management technology and decentralized transaction, Blockchain provides transparency, security, efficiency, trust, anonymity, and data integrity for services delivered by the public sector. A review of the academic literature shows that most of the extant studies on BCT adoption principally concentrate on technological perspectives. However, as addressed in this article, a more comprehensive view is required for Blockchain adoption by government organizations. The majority of the current studies on Blockchain have concentrated on the financial services, which limits the application of these studies' findings for other e-services. This study reviewed and investigated the state of existing knowledge in the adoption of BCT in the context of the Jordanian public sector and identified three categories of challenges, namely, technical factors (technical infrastructure, storage, distributed ledger, information exchange and transactions, trust, security and privacy, and cost), institutional/organizational factors (organization support, norms and cultures, regulations and legislation, governance), and market factors (market structure and business processes). The classification of the challenges was built upon the research work of Koppenjan and Groenewegen (2005) [30]. This is the first research work integrating and empirically validating a range of challenges for the adoption of BCT in the eGovernment services.

Findings of this study can play an instrumental role in promoting the understanding of government institutions, particularly in developing countries, of the key obstacles to adopt Blockchain and how designers, along with developers, may shape Blockchain technology within the public sector as it is still evolving and nascent. With respect to the cultural resistance and resistance to change, there is still a need for BCT enterprises and IT managers to effectively cooperate with each other, introduce novel solutions, and implement BCT applications. Therefore, the experience of the Jordanian government could be the first step toward the maturation of BCT-based eGovernment services. The main objective of this research paper is to draw upon current perspectives of Jordanian IT staff in the public sector regarding the challenges affecting the acceptance and adoption of BCT in the research context. This was carried out to support the decision-making process by stakeholders of the public sector. Understanding and mitigating barriers one by one help to implement a successful Blockchain-based platform in government organizations.

The current study identified challenges that influence the adoption of Blockchain technology; however, future research is still required in order to suggest solutions to these barriers. Analysis of the data collected helped garner some insights into the significance of these challenges and their sequence. For instance, security and privacy, along with trust, play a significant role in the adoption of BCT in the government context (first and second rank). Therefore, consideration of these barriers and their integration into a technology acceptance model are required for future research work. The proposed theoretical framework will be useful to show the relationships between these factors and their influence on BCT acceptance and adoption. Future research should test and refine these relationships empirically as well as assess the

framework based on practical evidence. Due to its high explanatory power compared to the previous theoretical models of IT acceptance and also its appropriateness to this study context, the UTAUT model would be a superior choice as a base for the future-proposed theoretical framework to address the acceptance of BCT in the Jordanian public sector. Future research could also employ other unique methods, such as interviews and qualitative studies, in order to identify novel challenges.

References

1. Frizzo-Barker, J., et al. (2019). Blockchain as a disruptive technology for business: A systematic review. *International Journal of Information Management*.
2. Ølnes, S., Ubacht, J., & Janssen, M. (2017). *Blockchain in government: Benefits and implications of distributed ledger technology for information sharing*. *Elsevier*.
3. Warkentin, M., & Orgeron, C. (2020). Using the security triad to assess blockchain technology in public sector applications. *International Journal of Information Management*, 102090.
4. Hou, H. (2017). *The application of blockchain technology in E-government in China*. *IEEE*.
5. Alexopoulos, C., et al. (2019) *Benefits and obstacles of blockchain applications in E-Government*.
6. Batubara, F. R., Ubacht, J., & Janssen, M.. 2018. Challenges of blockchain technology adoption for e- government: A systematic literature review.
7. White, M., Killmeyer, J., & Chew, B.. (2017). *Will blockchain transform the public sector? Blockchain basics for government*. Retrieved February 21, 2020, from https://www2.deloitte.com/us/en/insights/industry/public-sector/understanding-basics-of-blockchain-in-government.html
8. Ghazawneh, A. (2019). *Blockchain in the middle east: Challenges and opportunities*. In *Association for Information Systems*.
9. MoDEE. (2018). *General Policy for the Information & Communications Technology and Postal Sectors*. Jordan: Ministry of Digital Economy and Entrepreneurship.
10. Tiwari, A. (2020) Jordan: Customs Department to Pilot IBM, Maersk's Blockchain Platform. Retrieved February 21, 2020, from https://btcmanager.com.
11. Ølnes, S. (2016). *Beyond bitcoin enabling smart government using blockchain technology*. In *International Conference on Electronic Government*. Springer.
12. Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. O'Reilly Media, Inc..
13. Janssen, M., et al. (2020). A framework for analysing blockchain technology adoption: Integrating institutional, market and technical factors. *International Journal of Information Management, 50*, 302–309.
14. Biswas, B., & Gupta, R. (2019). Analysis of barriers to implement blockchain in industry and service sectors. *Computers & Industrial Engineering, 136*, 225–241.
15. Ahram, T., et al. (2017). Blockchain technology innovations. In *Technology & Engineering Management Conference*. TEMSCON, IEEE.
16. Khan, K. M., Arshad, J., & Khan, M. M. (2020). Investigating performance constraints for blockchain based secure e-voting system. *Future Generation Computer Systems, 105*, 13–26.
17. Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy, 41*(10), 1027–1038.
18. Venkatesh, V., et al. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 425–478.
19. Weerakkody, V., et al. (2013). Examining the influence of intermediaries in facilitating e-government adoption: An empirical investigation. *International Journal of Information Management, 33*(5), 716–725.

20. AlAwadhi, S., & Morris, A. (2008). *The Use of the UTAUT Model in the Adoption of E-government Services in Kuwait*. In *Proceedings of the 41st Hawaii International Conference on System Sciences*. IEEE.
21. ALKhwaldi, A., Kamala, M., & Qahwaji, R. (2017). From e-government to cloud-government challenges of Jordanian Citizens' acceptance for public services. In *The 12th International Conference for Internet Technology and Secured Transactions (ICITST-2017)*. IEEE.
22. Puspitasari, N., et al. (2019). An application of the UTAUT model for analysis of adoption of integrated license service information system. *Procedia Computer Science, 161*, 57–65.
23. Dwivedi, Y. K., et al. (2020). A meta-analysis based modified unified theory of acceptance and use of technology (meta-UTAUT): A review of emerging literature. *Current Opinion in Psychology*.
24. Gray, D. E. (2014). *Doing research in the real world* (Third ed.). London: SAGE Publications Ltd..
25. Saunders, M. N. K., Thornhill, A., & Lewis, P. (2019). *Research Methods for Business Students* (Eighth ed.). Harlow, Essex: Pearson Education Limited.
26. Jordantimes. (2019) *Women occupy around 30% of ICT jobs in Jordan — int@j*. Retrieved February 21, 2020, from https://jordantimes.com/news/local/women-occupy-around-30-ict-jobs-jordan-%E2%80%94-intj
27. DOS. (2019). *Department of Statistics: Population Estimates*. Retrieved February 21, 2020, from http://dosweb.dos.gov.jo/DataBank/Population_Estimares/PopulationEstimates.pdf.
28. MOHE. 2019. Ministry of Higher Education: Statistics.
29. Mohanta, B. K., et al. (2019). *Blockchain technology: A survey on applications and security privacy challenges*. *Internet of Things*, 100107.
30. Koppenjan, J., & Groenewegen, J. (2005). Institutional design for complex technological systems. *International Journal of Technology, Policy and Management, 5*(3), 240–257.

Chapter 14
Blockchain-Based Secure Method for Tiger Detection Using Machine Learning

D. B. Vishwas, M. Gowtham, A. V. Ajay, K. Raghavendra, Vinayakumar Ravi, and Sam Goundar

14.1 Introduction

The creatures assume a significant function in the decent variety of biological system and are among the high=level hunters that are available at the tip of the natural pecking order and go about as a mechanism for keeping the general equalization among the different members remembered for the evolved way of life. Nonetheless, these species are presently imperilled and, if not focused on, would be nearly terminated. One of the numerous helpful applications that have been given by PC researchers is to recognize specific substances and screen them, which are, for this situation, the tigers. Camera traps are utilized in public stops and woodlands, ending up being superior to the early strategy for utilizing hefty radio restraints on creatures. These gadgets recognize and photograph the creature moving along the woodland tracks. This strategy ends up being a useful instrument in checking these creatures. The methodology incorporates recognizing tigers and furthermore distinguishing explicit tiger among them by the method of design coordination.

The point of executing tiger discovery and recognizable proof is to have the option to identify and photograph these vertebrates while they move along the woodland tracks. From pictures or recordings caught by the cameras, the assignment of tiger identification expects to put tight jumping boxes around tigers. As the

D. B. Vishwas · M. Gowtham (✉) · A. V. Ajay · K. Raghavendra
Department of Computer Science and Engineering, NIE Institute of Technology, Mysuru, Karnataka, India

V. Ravi
Assistant Research Professor, Center for Artificial Intelligence, Prince Mohammad Bin Fahd University, Khobar, Saudi Arabia

S. Goundar
ICT (Cyber Security), British University Vietnam/University of Staffordshire, Hanoi, Vietnam

H. L. Gururaj et al. (eds.), *Convergence of Internet of Things and Blockchain Technologies*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-76216-2_14

recognition may run on the edge, both the discovery precision and the processing cost are utilized to gauge the nature of the finder.

The motivation behind this undertaking is to find an inventive methodology of having the option to recognize and distinguish the tigers so that the speed of the technique is expanded. Previously, a similar undertaking was performed by people, which used to be tedious and included a ton of exertion [1].

The tiger identification framework is set up as a private decline issue, that is, legitimately from the picture pixels to the bouncing boxes and the class probabilities. The calculation utilized in the framework is called You Only Look Once (YOLO); by utilizing it, it is conceivable to foresee whether tigers are available and where precisely they are, by looking only once at the picture. This includes the working of a proficient neural organization as the base of the framework. This organization is essentially run on another picture during the test time to anticipate the identifications. Further, the highlights from the organization of the creature's flank are separated, and a strategic relapse classifier is prepared to distinguish and perceive singular tigers. The cycle likewise includes consolidating various calculations to ascertain similitude scores between the examples from the pictures to mechanize the quest for a match to another picture. The surface model of a tiger is put away as a content document of three-dimensional directions, reaching out from the shoulders to the base of the tail, undermining the front and rear appendages.

The venture portrays how correlation of pictures broadly contrasting in camera edges and body stances is made conceivable by utilizing a three-dimensional surface model of a tiger for filtering the example tests [2].

14.2 Related Work

YOLO is introduced as another approach to manage object ID. Prior work on object acknowledgment repurposes classifiers to perform recognizable proof. Or maybe, object revelation is sketched out as a backslide issue to spatially disconnected hopping boxes and related class probabilities. A singular neural association predicts bouncing boxes and class probabilities honestly from full pictures in a solitary evaluation. Since the whole ID pipeline is a singular association, it will in general be smoothed out beginning to end clearly on the spot execution. YOLO gives three rule inclinations [2]:

- It is very quick.
- It reasons around the world about the picture when making expectations.
- It learns generalizable portrayals of articles.

A technique to recognize one tiger from another is by watching and contrasting non-impeded segments of their jacket designs. As the tiger personal ID list develops with populace change and movement from neighboring spots, the exertion needed to scan the whole index for matches to each new picture gets exorbitant. The quantity of visual examinations required can be decreased fundamentally by computing

comparability scores between each new picture and the pictures by which existing people are spoken to in the index. Visual examinations would then be able to be confined to those people for which the most extreme score surpasses a limit approval.

A system was created for programmed identification and acknowledgment of people in various designed species like tigers, zebras, and panthers. Quicker R-CNN object identification structure was utilized to identify creatures in pictures. Further, they separated highlights from AlexNet of the creature's flank and train a calculated relapse classifier to perceive the people. Both the tiger and the flank district are recognized by utilizing faster R-CNN. During preparing, both the picture and the jumping boxes are inputted in the organization. The organization is prepared to distinguish three classes: tiger, flank, and the foundation. For distinguishing proof, just flank locales are utilized on the grounds that they contain the data to interestingly recognize the designed creatures.

The highlights are invariant to picture scaling and turn and halfway invariant to change in brightness and 3D camera see point. The expense of removing these highlights is diminished by adopting a course-separating strategy, in which the more costly activities are applied uniquely at areas that finish an underlying assessment. The scale-invariant feature transform (SIFT) key focuses depicted in this paper are especially helpful because of their peculiarity, which empowers the right counterpart for a keypoint to be chosen from a huge information base of other central issues. This uniqueness is accomplished by gathering a high-dimensional vector speaking to the picture slopes inside a nearby area of the picture.

14.3 Implementation

The system architecture of tiger detection and pattern matching can be represented in a diagram as shown in Fig. 14.1. The tiger is considered as a symbol for preservation. Because of its imperilled and lead status, exact and solid populace gauges are the need of great importance. An exact and dependable framework is required for checking singular tiger in their regular living space and making their profile for better reconnaissance [3]. Every tiger has an example of stripes and facial markings interesting to singular creatures. This could be checked in the event that paper could recognize them particularly.

Tiger detection and identification are utilized to screen the tigers in the timberland territories and monitor their developments. The camera traps catch the pictures while the creatures move along the ways of woodland. A camera trap is a distantly enacted camera that is outfitted with a movement sensor or an infrared sensor or utilizes a light bar as a trigger. These camera catches are put away to decide different estimates, for example, finding the region of the creature and populace thickness.

The tiger identification measure is completed utilizing a calculation called "You Only Look Once" (YOLO). In this system, a solitary neural organization predicts bouncing boxes and class probabilities straightforwardly from full pictures in a single assessment. Subsequent to distinguishing a tiger, the recognized edge is

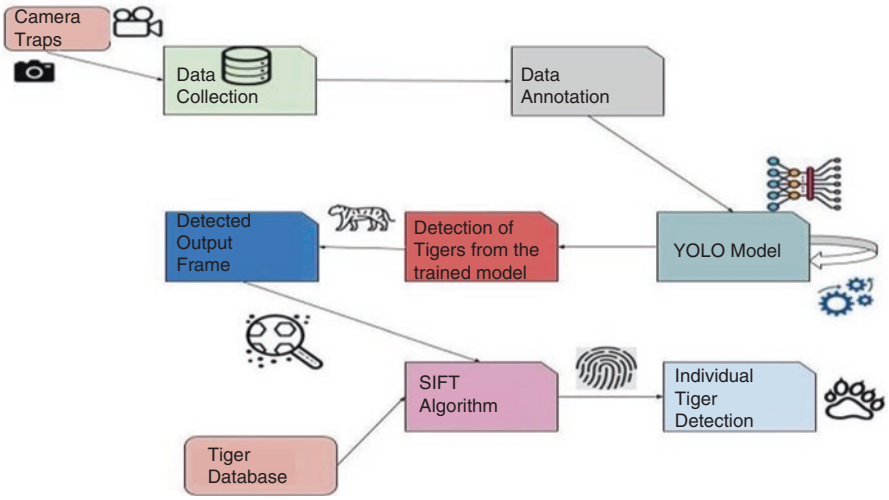


Fig. 14.1 System architecture

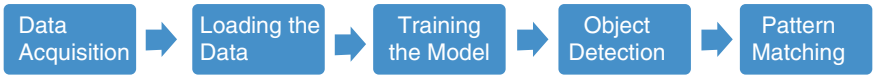


Fig. 14.2 Data flow diagram

utilized for design coordination for singular ID as examples are viewed as the proportion of uniqueness.

The implementation of tiger detection and pattern matching can be carried out in six main stages and can be represented in Fig. 14.2.

14.3.1 Stage 1: Acquiring Images

This stage includes getting pictures from the camera traps. Camera traps will be introduced in the region of the timberland territories to monitor creature's developments. It has v4 camera traps introduced wherever in the woodland which is set off when there is some movements there. Subsequently, the tiger pictures are acquired from these snares [4].

14.3.2 Stage 2: Loading the Information into the Organization

In the wake of getting the pictures from the camera traps, pictures are stacked into the organization to prepare the model on them, so the tiger's condition can be recognized progressively.

Initially, before stacking the dataset into the organization, the pictures are clarified for object discovery. This will expand the exactness of the model since paper will put the bouncing box just for the necessary item and eliminate the undesirable commotion in the information.

14.3.2.1 YOLO

YOLO is an organization for object location. The item identification task comprises deciding the area on the picture where certain articles are available and just as arranging those articles. YOLO is favorable contrasted with past article location strategies. Procedures like R-CNN and its assortments used a pipeline to play out this endeavor in various methods. This can be deferred to run and moreover hard to upgrade, considering the way that each individual section must be arranged freely. YOLO does everything with a lone neural association [5] (Fig. 14.3):

- The framework resizes the information picture.
- Runs a solitary convolutional network on the picture.
- Thresholds the subsequent identifications by the model's certainty.

YOLO first takes a data picture. By then, it parcels the image into grids S×S. Each grid cell predicts B ricocheting boxes similarly as C class probabilities as shown in Fig. 14.4. The hopping box estimate has five fragments (x, y, w, h, assurance).

The (x, y) masterminds address the point of convergence of the case, similar with the system cell territory. These headings are normalized to fall some place in the

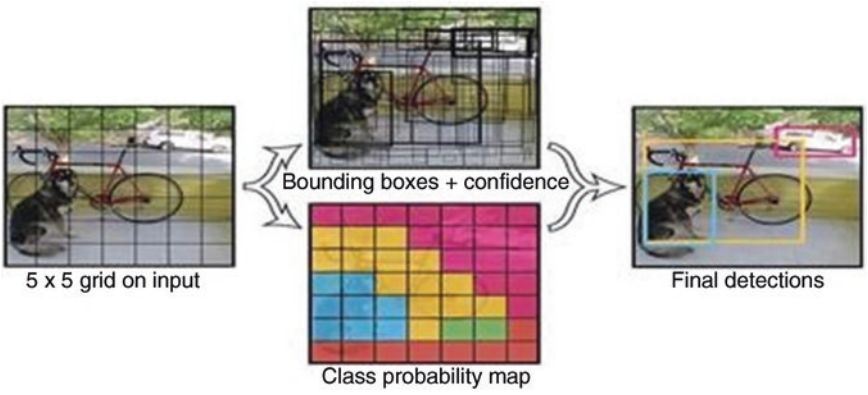


Fig. 14.3 Working of YOLO

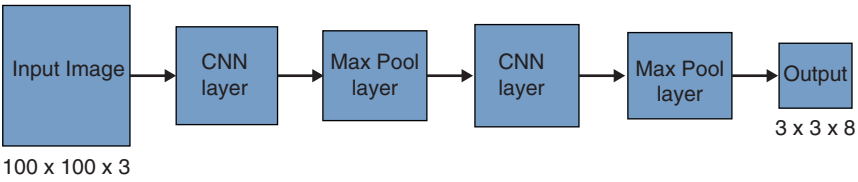


Fig. 14.4 YOLO network structure

scope of zero and one. The (w, h) box estimations are in like manner normalized to zero and one, near with the image size. Adding the class figures to the yield vector, paper gets an S×S×(B * 5 +C) tensor as yield.

Second, YOLO reasons all around the globe about the image when making desires. Unlike sliding window and region recommendation-based techniques, YOLO sees the entire picture during planning and test time, so it evidently encodes pertinent information about classes similarly as their appearance. Brisk R-CNN, a top recognizable proof procedure, bungles establishment patches in an image for objects since it can't see the greater setting. YOLO makes not actually a huge part of the amount of establishment bungles appeared differently in relation to fast R-CNN. Third, YOLO learns generalizable depictions of articles. Right when arranged on trademark pictures and it took a stab at compelling artwork, YOLO beats top ID methods like DPM and R-CNN by a wide edge. Since YOLO is uncommonly generalizable, it is less disposed to isolate when applied to new spaces or surprising information source [6].

14.3.3 Stage 3: Training the Model

YOLO utilizes total squared blunders between the forecasts and the ground truth to figure misfortune.

14.3.3.1 The Misfortune Work Involves Classification Misfortune

In the event that an item is identified, the order misfortune at every cell is the squared mistake of the class contingent probabilities for each class:

$$\sum_{i=0}^{s^2} 1_i^{\text{obj}} \sum_{c \in \text{classes}} \left(p_i(c) - \hat{p}_i(c)\right)^2. \qquad (14.1\$\ (14.1)\ \$)$$

where
$1^{\text{obj}} = 1$ if an object appears in cell i, otherwise O,
$\hat{p}i\ (c)$ denotes the conditional class probability for class c in cell i.

14.3.3.2 Localizations

The restriction misfortune gauges the blunders in the anticipated limit box area and sizes. Paper just tallies the container answerable for recognizing the item:

$$\lambda_{\text{coord}} \sum_{i=0}^{s^2} \sum_{j=0}^{B} 1_{ij}^{obj} \left[\left(x_i - \hat{x}_i \right)^2 + \left(y_i - \hat{y}_i \right)^2 \right] + \lambda_{\text{coord}} \sum_{i=0}^{s^2} \sum_{j=0}^{B} 1_{ij}^{obj} \left[\left(\sqrt{w_i} - \sqrt{\hat{w}_i} \right)^2 + \left(\sqrt{h_i} - \sqrt{\hat{h}_i} \right)^2 \right]$$

(14.2$$ (14.2) $$)

where $1^{\text{obj}} = 1$ if the jth boundary box in cell i is responsible for detecting the object, otherwise O,λ_{coord} increases the weight for the loss in the boundary box coordinates.

14.3.3.3 Confidence Misfortune

In the event that an article is distinguished in the crate, the certainty misfortune is as follows:

$$\sum_{i=0}^{s^2} \sum_{j=0}^{B} 1_{ij}^{\text{obj}} \left(c_i - \hat{c}_i \right)^2 \qquad (14.3\$ \ (14.3) \ \$)$$

where

$\hat{ci}$ is the box confidence score of the box j in cell i,

$1^{\text{obj}} = 1$ if the jth boundary box in cell I is responsible for detecting the object, otherwise O.

In the event that an article isn't distinguished in the crate, the certainty misfortune is as follows:

$$\lambda_{noobj} \sum_{i=0}^{s^2} \sum_{j=0}^{B} 1_{ij}^{noobj} \left(c_i - \hat{c}_i \right)^2 \qquad (14.4\$ \ (14.4) \ \$)$$

where

$1_{ij}^{\text{noobj}}$is the complement of 1_{ij}^{obj},

$\hat{c}_i$is the box confidence score of the box j in cell i,

λ_{noobj} weighs down the loss when detecting background.

The last misfortune includes limitation, certainty, and grouping misfortunes together:

$$\lambda_{\text{coord}} \sum_{i=0}^{s^2} \sum_{j=0}^{B} 1_{ij}^{obj} \left[\left(x_i - \hat{x}_i \right)^2 + \left(y_i - \hat{y}_i \right)^2 \right] + \lambda_{\text{coord}} \sum_{i=0}^{s^2} \sum_{j=0}^{B} 1_{ij}^{obj} \left[\left(\sqrt{w_i} - \sqrt{\hat{w}_i} \right)^2 + \left(\sqrt{h_i} - \sqrt{\hat{h}_i} \right)^2 \right]$$
$$+ \sum_{i=0}^{s^2} \sum_{j=0}^{B} 1_{ij}^{obj} \left(c_i - \hat{c}_i \right)^2 + \lambda_{\text{noobj}} \sum_{i=0}^{s^2} \sum_{j=0}^{B} 1_{ij}^{\text{noobj}} (c_i - \hat{c}_i + \sum_{i=0}^{s^2} 1_i^{obj} \sum_{c \in \text{classes}} \left(p_i(c) - \hat{p}_i(c) \right)^2$$

(14.5$$ (14.5) $$)

14.3.4 Stage 4: Detection of Tiger

In the wake of preparing the model, load the model from the most recent checkpoint, that is, the setup document that was utilized before for building the model. At that point, set burden as −1; it will stack the most recent checkpoint [7].

By calling load_from_ckpt() technique in International Tropical Fruits Network (TFNet), it will stack pre-prepare boundaries from the checkpoint that you simply determined in choices: tfnet2.load_from_ckpt().

At that point, the test picture can be given to check the expectation. On the off chance that the tiger is identified, it will give the certainty of the recognized tiger beside the jumping box arranges. Additionally, the model is run on the recordings which will help progressive situations.

14.3.5 Stage 5: Pattern Matching

Examples speak to the uniqueness in tigers. This is done as every tiger is recognized through discernable highlights which they have, for example, the dark stripes on the body. Subsequently, it is a significant perspective in distinguishing the tigers. Here, paper is utilizing a calculation called scale-invariant feature transform (SIFT) for coordinating examples. This calculation depicts picture that have numerous properties that make them reasonable for coordinating varying pictures of an article or scene. The highlights are invariant to picture scaling and turn and incompletely invariant to change in brightness and 3D camera perspective.

14.3.5.1 Scale-Invariant Feature Transform

The scale-invariant feature transform (SIFT) is a component acknowledgment count in PC vision to recognize and depict neighborhood features in pictures. Channel key motivations behind articles are first removed from a ton of reference pictures and set

aside in a database. A thing is seen in another image by independently differentiating every part from the new picture to this database and finding up-and-comer planning features subject to euclidean partition of their component vectors. From the full course of action of matches, subsets of focal issues that agree on the thing and its region, scale, and bearing in the new picture are recognized to filter through incredible matches.

The confirmation of unsurprising gatherings is performed rapidly by using a profitable hash table utilization of the summarized Hough change. Each pack at any rate of three features that yield to a thing and its stance are then subject to extra point by point model check, and in this manner, special cases are discarded. Finally, the probability that a particular plan of features shows the presence of an article is figured, given the accuracy of fit and number of conceivable counterfeit matches. Article organizations that breeze through all of these evaluations can be perceived as right with high sureness.

14.3.5.2 Scale-Space Top Selection

Genuine articles are basic precisely at a specific scale. You may see a sugar block consummately on a table. Regardless, in the event of taking a gander at the whole smooth way, by then, it in a general sense doesn't exist. This multi-scale nature of articles is fundamental in nature. Additionally, a scale space endeavors to copy this idea on electronic pictures.

The scale space of a picture is a cutoff L(x, y, σ) that is passed on from the convolution of a Gaussian kernel (blurring) at various scales with the information picture. Scale space is kept into octaves, and the measure of octaves and scale relies on the size of the essential picture. So paper produces several octaves of the chief picture. Every octave's picture size is a colossal aspect of the past one.

14.3.5.3 Keypoint Localization

Central issues made in the past improvement produce a ton of keypoints. Some of them lie along an edge, or they need more division. In the two cases, they are not as obliging as highlights. So paper disposes of them. The procedure looks like the one utilized in the Harris Corner Detector for clearing out edge highlights. For low-differentiation highlights, paper basically checks their powers.

They utilized Taylor plan extension of scale space to get a more exact region of extrema, and if the power at these extrema isn't really a cutoff respect (0.03 according to the paper), it is pardoned. Canine has a higher reaction for edges, so edges also should be slaughtered. They utilized a 2×2 Hessian organization (H) to deal with the main bend.

14.3.5.4 Direction Assignment

Straightforwardly, paper has ensured keypoints. They've been endeavored to be steady. Paper surely knows the scale at which the keypoint was recognized (it's proportionate to the size of the obscured picture). So paper has scale invariance. The thing to do is to commit an orientation to each keypoint to cause it to turn invariance.

A district is taken around the keypoint domain relying on the scale, and the inclination size and bearing are settled here. A direction histogram with 36 compartments covering 360 degrees is made. Expect the edge bearing at one point (around the "way plan area") to be 18.759 degrees; by then, it will go into the 10–19-degree compartment. Similarly, the "all out" that is added to the holder is relative with the size of the point by then. Exactly when you've done this for all pixels around the keypoint, the histogram will have a top unavoidably. The most basic top in the histogram is taken, and any top above 80% of it is additionally considered to compute the course. It makes keypoints with same zone and scale yet extraordinary heading. It adds to the adequacy of arranging.

14.3.5.5 Keypoint Descriptor

As of now, each keypoint has a region, scale, and bearing. Next is to enlist a descriptor for the nearby picture region about each keypoint that is unbelievably irrefutable and invariant as conceivable to collections, for example, changes in setting and light.

To do this, a 16 × 16 window around the keypoint is taken. It is isolated into 16 sub-squares of 4 × 4 size as shown in Fig. 14.5.

For each sub-block, eight-canister direction histograms are made as shown in Fig. 14.6.

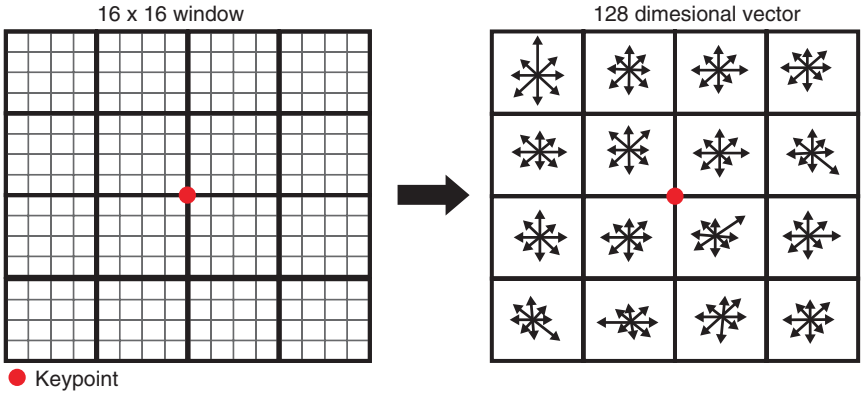


Fig. 14.5 Canister direction histograms

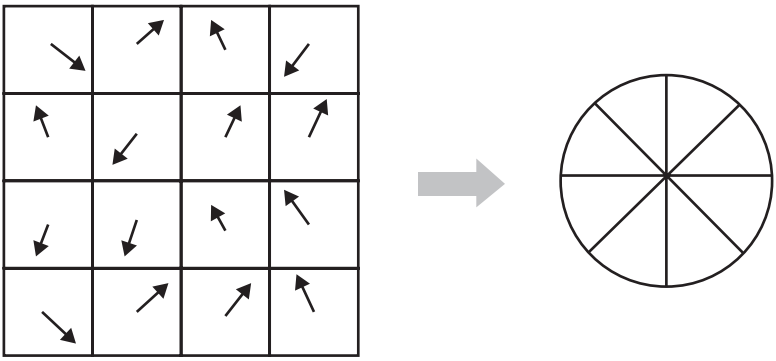


Fig. 14.6 4 × 4 × 8 bearings

So 4 × 4 descriptors in excess of 16 × 16 model bunch were used eventually. 4 × 4 × 8 headings give 128 canister regards. It is addressed as a segment vector to shape keypoint descriptor. This component vector presents two or three complexities. Paper needs to discard them before settling the remarkable imprint.

14.3.5.6 Central Issue Matching

Focal issues between two pictures are facilitated by perceiving their nearest neighbors. Regardless, on occasion, the second closest match may be uncommonly near the first. It may happen on the grounds for some various reasons. In light of everything, the extent of closest detachment to second-closest elimination is taken. If it is more noticeable than 0.8, they are excused. It takes out around 90% of false matches while discards so to speak 5% right matches, as indicated by the paper.

14.4 Results

14.4.1 Camera Traps and Data Collection

Camera traps, the one showed in Fig. 14.7, utilized by earthy people, producers, and specialists, are sent into the wild to screen creatures. These gadgets utilized in the timberlands are the primary wellspring of information for the identification framework. These cameras catch the creatures, for this situation the tigers, while they wander along the tracks in the forested areas. Set off by infrared sensors, camera traps can recognize development and self-sufficiently catch photographs and recordings of creatures. The recordings and pictures consequently caught by these cameras are then gathered and utilized for preparing the discovery model.

Fig. 14.7 A camera trap installed in a forest

To start the picture catch, essentially, all camera traps utilize passive infrared (PIR) movement identifiers which react when something with a surface temperature from the foundation moves in their field of view. Littler targets are harder to distinguish in light of the fact that less of the warmth they emanate arrives at the locator. Therefore, greater creatures are identified at longer ranges than littler ones.

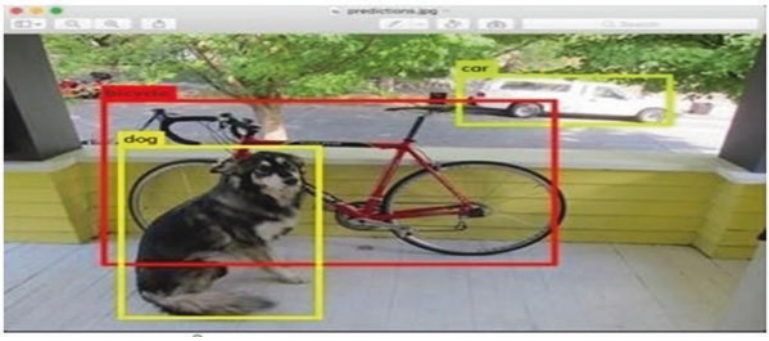
14.4.2 Annotation

When paper has gained the information from the camera traps, the following significant activity is to comment on those pictures. In machine learning or artificial intelligence, paper has to prepare the machine to distinguish different kinds of articles noticeable in the common habitat. Self-driving vehicles, robots, self-governing flying machines, and other such identification frameworks can't identify such items except if prepared with a specific cycle. Explained pictures make the object of intrigue discernible to machines.

14.4.3 Object Detection

Article discovery is a typical computer vision issue which manages recognizing and finding objects of specific classes in the picture. Deciphering the item localization should be possible in different manners, including making a jumping box around the article or by division, which is denoting each pixel in the picture which contains the item [19].

Article location was concentrated even before the breakout notoriety of convolutional neural networks (CNNs) in computer vision and, before deep learning, was a few stage measure, beginning with performing edge identification and highlight extraction on the picture, utilizing methods like SIFT and histogram of oriented gradients (HOG). The information pictures were then contrasted, and the current article formats, ordinarily at multi-scale levels, to identify and restrict objects




```
layer     filters    size              input                output
    0 conv     32  3 x 3 / 1   416 x 416 x   3   ->   416 x 416 x  32
    1 max          2 x 2 / 2   416 x 416 x  32   ->   208 x 208 x  32
    .......
   29 conv    425  1 x 1 / 1    13 x  13 x1024   ->    13 x  13 x 425
   30 detection
Loading weights from yolov2.weights...Done!
data/dog.jpg: Predicted in 0.016287 seconds.
car: 54%
bicycle: 51%
dog: 56%
```

Fig. 14.8 (**a**) Input. (**b**) Darknet output for the image given in (**a**)

present in the picture. In more conventional ML-based approaches, PC vision strategies are utilized to take a gander at different highlights of a picture to recognize gatherings of pixels that may have a place with an article. These highlights are then taken care of into a relapse model that predicts the area of the article alongside its mark. Then again, profound learning-based approaches utilize CNNs to perform from start to finish; solo article location, in which highlights don't, should be characterized and removed independently.

YOLO, which is utilized as the fundamental location framework in this venture, is written in Darknet. Darknet is a custom profound learning system. It is open source and is written in CUDA/C and fills in as the reason for YOLO. This can be executed by cloning the vault. Darknet prints out the object it detects, along with its confidence and how long it took to find them as shown in Fig. 14.8.

Figure 14.9 has plotted a graph between loss and number of training steps. As the model's number of training steps increases, the loss value drops near to zero.

14.4.4 IFT Algorithm

Scale-invariant feature transform (SIFT) is a procedure for eliminating feature vectors that are portrayed closed by fixes of an image. Not only are these component vectors scale-invariant, but also they are invariant to translation, turn, and light [1]. Figure 14.10 shows a sample and query input images for the SIFT algorithm.

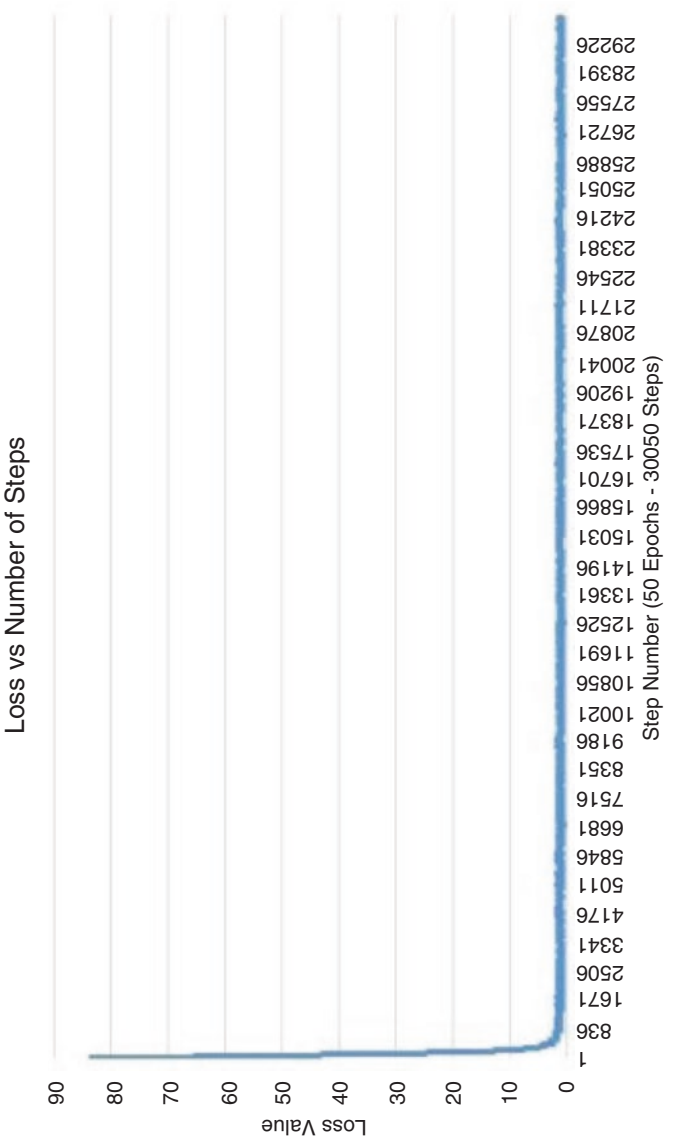


Fig. 14.9 Loss graph

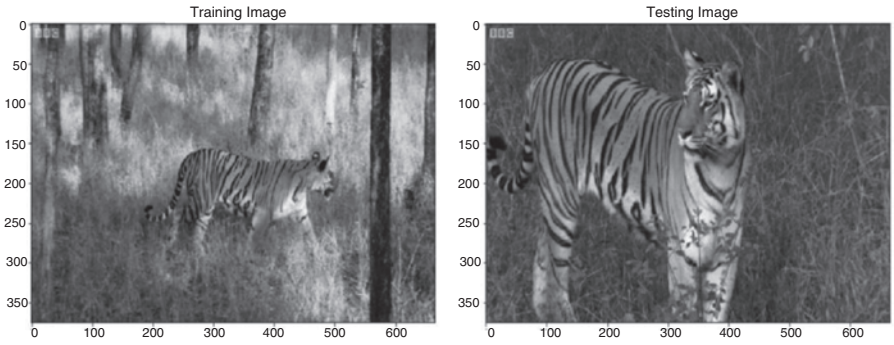


Fig. 14.10 Initial sample and query images given to the SIFT algorithm

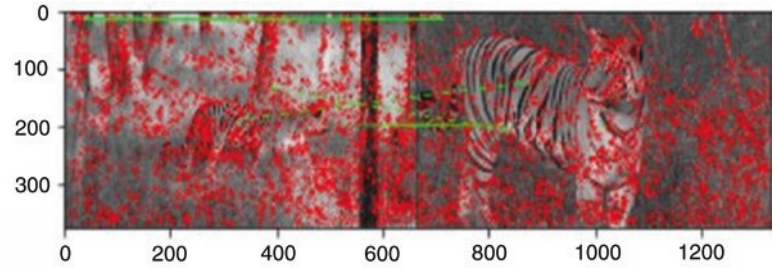


Fig. 14.11 Final result of SIFT algorithm

By and by to calculate the descriptor, OpenCV gives two strategies:

- Since you recently found keypoints, you can call sift.compute() which enrolls the descriptors from the keypoints paper has found, e.g., kp,des = sift. compute(gray,kp).
- If you didn't find keypoints, truly find keypoints and descriptors in a lone development with the limit, sift.detectAndCompute().

We will see the resulting procedure:

```
channel = cv.SIFT_create() kp,
des = sift.detectAndCompute(gray,None)
```

Here, kp will be an overview of keypoints and des is a numpy display of shape Number_of_Keypoints×128. So paper got keypoints, descriptors, etc. Directly, paper has to see how to facilitate keypoints in different pictures. By and by, paper set a condition that at least ten matches (portrayed by MIN_MATCH_COUNT) are to be there to discover the article. In any case, essentially, show a message saying insufficient matches are available.

On the off chance that enough matches are discovered, paper extricates the areas of coordinated keypoints in both the pictures. They are passed to locate the viewpoint change. When paper gets this 3 × 3 change network, paper uses it to change the edges of query image comparing focuses in train image. At that point, paper draws it. At last, paper draws our inliers (if effectively found in the article) or coordinating keypoints (whenever fizzled). Figure 14.11 shows the final result of SIFT algorithm with 3604 matching keypoints between the training and query images.

14.5 Providing Security by Using Blockchain

One of the significant important resources in the computerized world is information which should be ensured &amp and overseen. With handy crime individuals, there is consistently a danger to take information [8]. Previously, a few strategies are proposed to secure the important information. One such methodology is the utilization of blockchain innovation. In straightforward terms, a blockchain alludes to a chain of squares that store information. Each information reserved inside the square relies upon blockchain types. The principal goal is to encode the succession of characters in advanced reports utilizing cryptographic calculations, so it's unrealistic to preface them or to play with them [9]. A blockchain is an advanced record that is spread totally to any individual who is expected to learn and utilize it. It turns out to be hard to transform it, whenever information is documented inside a blockchain. [20] Each square contains information, the hash of the current square with hash of past square [10]. The exchange subtleties of the sender, beneficiary &amp, and number of coins are put away in a bitcoin blockchain. Each square has a long succession hash key which is interesting that makes it hard to break by lawful offense programmers. When the square is made, its hash is tallied. Any progressions made inside a square make the hash change. Frequently, hashes are helpful when we need to distinguish changes to blocks. The following component inside each square is the hash of the past square. Blockchain is the record-keeping development behind the bitcoin association [11].

Likewise, there's a fair chance that it just looks good. In endeavoring to get acquainted with blockchain, apparently, a definition like this is encountered: "blockchain is a passed on, decentralized, openly available report" [12]. In case this advancement is so mind boggling, why call it "blockchain"? At its most key level, blockchain is, from a genuine perspective, basically a chain of squares, which is not in the standard sentiment of those words [13].

Exactly as the words "square" and "chain" in this particular situation, we are truly examining automated information (the "block") set aside in a public database (the "chain"). "Squares" on the blockchain are included as progressed pieces of information. Specifically, they have three segments [14].

Squares store information about trades like the date, time, and dollar proportion of your most recent purchase from Amazon. (Note: This Amazon model is for illustrative buys [15]; Amazon retail doesn't work on a blockchain standard as of this

arrangement). Squares store information about who is participating in trades. A square for your luxurious use purchase from Amazon would record your name by Amazon.com, Inc. (AMZN). Instead of using your certifiable name, your purchase is recorded with no distinctive information using a standout "mechanized mark," like a username [16].

Squares store information that remembers them from various squares. Much like you and I have names to distinguish us from one another, each square stores a novel code called a "hash" that licenses us to uncover it isolated from another square. Hashes are cryptographic codes made by unprecedented figures. Assume you made your sumptuous use purchase on Amazon, notwithstanding, while it's in transit, you pick you can't evade and require a resulting one. Notwithstanding, with the way that the nuances of your new trade would look practically vague from your past purchase, we can recognize the squares because of their novel codes [17].

14.5.1 Creating Blockchain Using Python, Mining New Block, and Displaying the Whole Blockchain

- The information will be put away in JSON design which is extremely simple to execute and simple to peruse. The information is put away in a square, and the square contains numerous information. In every single moment, numerous squares are added, and to separate one from the other, we will utilize fingerprinting.
- The fingerprinting is finished by utilizing hash, and to be specific, we will utilize the SHA256 hashing calculation. Each square will contain its own hash and furthermore the hash of the past capacity with the goal that it can't get altered [21].
- This fingerprinting will be utilized to chain the squares together. Each square will be connected to the past square having its hash and to the following square by giving its hash [22].
- The mining of the new square is finished by offering and effectively finding the response to the evidence of work. To cause mining hard, the confirmation of work must be sufficiently hard to get abused [18].
- After mining the square effectively, the square will at that point be added to the chain.
- After mining a few squares, the legitimacy of the chain must be checked so as to forestall any sort of messing with the blockchain [23].
- Then, the web application will be made by utilizing flask and conveyed locally or freely according to the need of the client.

14.5.2 Usage Aspects of Blockchain for Wildlife Protection

The libraries and toolboxes can be introduced with Raspberry Pi or Arduino with existing Python utilizing pip installer. The blockchain innovation is exceptionally reliant and making use of the combinations with dynamic cryptography and encryption. For this, the hashlib library can be introduced utilizing the previously mentioned guidance [24].

The following is the situation of a made sure blockchain that is producing the hash esteems, so generally, exchanges and records will be profoundly made sure. In the accompanying code, the dynamic hash esteem is created that is the base of any blockchain with various exchanges in a chain and that makes the general blockchain:

```
 class Block:
 def init (this, myidx, ts, mydata, backsecuredhash):
 this.myidx = myidx this.ts = ts this.mydata = mydata
 this.backsecuredhash = backsecuredhash this.securedhash = this.
securedhashop() def securedhashop(this):
    shasecuredhash    =    securedhasher.sha256()    shasecuredhash.
update(mystr(this.myidx) + mystr(this.ts) + mystr(this.mydata) +
mystr(this.backsecuredhash))
 return shasecuredhash.hexdigest() def keyblock():
 return Block(0, date.datetime.now(), "Keyblock Block", "0") def
next_block(last_block):
 this_myidx = last_block.myidx +1.
 this_ts = date.datetime.now()
  this_mydata = "Block" + mystr(this_myidx) this_securedhash =
last_block.securedhash
 return Block(this_myidx, this_ts, this_mydata, this_securedhash)
blockchain = [keyblock()]
 IoT_Secured_Block = blockchain[0] maxblocks = 20
 for i in range(0, maxblocks):
   block_to_add   =   next_block(IoT_Secured_Block)   blockchain.
append(block_to_add)
 IoT_Secured_Block = block_to_add
  echo "Block #{} inserted in Blockchain".format(block_to_add.
myidx)   echo   "Securedhash   Value:   {}\n".format(block_to_add.
securedhash)
```

With the execution of the code, the following outcome is obtained that is having different hash values and provides higher degree of security using cryptography functions. Using these hash values, the attempt of hacking or sniffing the transaction will be almost impossible.

14.5.3 Generation of Hash Values Using Blockchain Implementation

```
 Gen in Blockchain Node 1:
                                    60afeff7f57bc04dc1c411763778f561d
9088c77d7789b4881a67d46557154ac Gen in
 Blockchain
 Node 2:
 8084d8e09b74f295082ea38cc3bbd892f27719b0fa9a732295fac34ed03debb9
 Gen in Blockchain
  Node 3: 247086d83f38210185aed834e4efe218822c6e1223e465321a80d3
d78f7ee803
 Gen in Blockchain
 Node 4: e7af556dd479088f4fb8cfb11f7648e192c8bb66835cdc748b039e0f-
c5fac646 Gen in Blockchain
 Node 5:
 439ed4470f39e44475852dee4j42e4474d535431b61807d02892af38e4a4395e
 Gen in Blockchain Node 6:
 452d166db9c397cac1870agfb08b462b00e15d7f5450485b03f7243a1a684b36
 Gen in Blockchain
 Node 7:
 301fabc673d1d29b0c18e0h8cf3c59d85051cf2a1eb4bd11c92abe0c0e531441
 Gen in Blockchain
 Node 8:
 bb876789e44fbd8d8d108d151cbde1b5d5d71cd5de388cdf2c0815c0e66a8635

 NodeBlock #19980 inserted in Blockchain Hash Value:
 58d86f4e14068cd1f56c5h27b7088a9894aceca01bd51bb304569b57c4e2a37e
 Node Block #19981 inserted in Blockchain Hash Value:
 d8d86d541ed3abb30bddg98d35b6f34d57958cb266aa70774251e5491e07d8ac
 Node Block #19982 inserted in Blockchain Hash Value:
 baf04029f374008683118534391e9a85f0af1593cad9b4d6e32088c5dcf4814d
 Node Block #19983 inserted in Blockchain Hash Value:
 43fa6ddebcc9b433711b3e616152223aea4ced529515a61b7b497a7f82fc0a86
 Node Block #19984 inserted in Blockchain Hash Value:
 b124ea343e9608f48b98cdh20835d6af14d492cbc60a2aff2809a12741f506a8
```

14.6 IoT-Enabled Blockchain for Secured Scenarios

As in the past model, the execution of hash work with the squares is done on independent structure. On the off chance that there ought to be an event of real blockchain, it is needed to be passed on with the objective that different customers can

Fig. 14.12 Executing the secured environment for IoT-based wildlife conservation

begin their trades and squares. For spread and electronic executions, there are different structures in Python. In blockchain programming, the proof of work (PoW) is one of the critical assessments. It is used to announce and uphold the trades with the objective that the new squares are intertwined with the blockchain. It is recommended as the key in understanding and figuring the checks and authenticity of the trades. In blockchain, different diggers take an energy for guaranteeing and completing the trades. For the productive backings, the diggers are repaid with the serious pushed sorts of cash as their pay.

This cycle also keeps up a key segment from the twofold encountering issue with the objective that the moved cash or trade is executed in attested manner. For example, if A sends a record or remote message to B, for this circumstance, that specific report or cash regards to the records of A that specifically need to be executed and after that should be reflected in the records of B. Overall, it is done by the remote regulator as extensively captivating. On the off chance that there ought to be an event of blockchain plan, it is executed where it is not comprehensively captivating, and it is grasped usually using express counts. If there are events of non-deleting the trade from sender, it will de-evaluate the remote message regardless of such a remote message.

As portrayed in Fig. 14.12, the execution of code and generally usage with all the records and exchanges can be broken down, so the straightforwardness of activities will be there with no endeavor of hacking. Utilizing proof of work (PoW), the honesty of exchanges is logged and submitted. With this methodology, the shrewd urban areas and keen homes or related parts of IoT can be made sure about utilizing blockchain-based innovations.

14.7 Conclusion

In conclusion, this paper presents the detection of tiger and pattern matching. The tiger is detected using YOLO network. It requires OpenCV and TensorFlow libraries in order to process the given dataset. Pattern matching is done using SIFT algorithm which is scale-invariant and rotation-invariant and sometimes even using illumination and orientation. This will help the forest department to keep track of tigers and avoid the harm causing to them. Definite contextual investigation on blockchain about IoT climate is used for checking and securing the natural life creatures like Tigers.

References

1. Redmon, J., Divvala, S., Girshick, R., & Farhadi, A. (2016). You only look once: Unified, real-time object detection. In *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*. University of Washington, Allen Institute for AI, Facebook AI Research.
2. Lex, H., Phil, L., Narendra, P., Narayanarao, K., Arjun, G., & Karanth, K. (2009). A tiger cannot change its stripes: Using a three-dimensional model to match images of living tigers and tiger skins. *Biology Letters, 5*, 383–386. https://doi.org/10.1098/rsbl.2009.0028.
3. Kumar, S., Gopalaswamy, A. M., & Karanth, K. U. (2011). Counting India's wild tigers reliably. *American Association for the Advancement of Science, 332*(6031), 791.
4. Cheema, G. S., & Anand, S. (2017). Automatic detection and recognition of individuals in patterned species. *Machine Learning and Knowledge Discovery in Database*, 27–38.
5. Iyer, N., Jayanti, S., Lou, K., Kalyanaraman, Y., & Ramani, K. (2005). Three-dimensional shape searching: State-of-the-art review and future trends. *Computer-Aided Design, 37*(5), 509–530.
6. Lowe, D. G. (2004). Distinctive image features from scale-invariant key points. *Computer Science Department, and University of British Columbia, 60*, 91–110.
7. Gowtham, M. Intrusion detection and avoidance for home and smart city automation in IoT. In *IoT: Security and Privacy Paradigm*. CRC Press, Taylor and Francis Group.
8. Bahga, A., & Madisetti, V. (2017). Blockchain applications: A hands-on approach. *Computers & Internet*.
9. Chondros, N., Kokordelis, K., & Roussopoulos, M. (2012). On the practicality of practical byzantine fault tolerance. *ACM/IFIP/USENIX International Conference on Distributed Systems Platforms and Open Distributed Processing*, 436–455.
10. Gowtham, M., Banga, M. K., & Patil, M. Secure internet of things: Assessing challenges and scopes for NextGen communication. In *2nd IEEE International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT-2019) at Vimal Jyothi Engineering College, Kerala*.
11. Heilman, E., Kendler, A., Zohar, A., & Goldberg, S. (2015). Eclipse attacks on bitcoin's peer-to-peer network. In *Proceedings of the 24th USENIX Conference on Security Symposium, ser. SEC'15. USENIX Association* (pp. 129–144).
12. Ohbuchi, R., Osada, K., Furuya, T., & Banno, T. Salient Local Visual Features for Shape-Based 3D Model Retrieval.
13. Gowtham, M. CL-PKA: Key management in dynamic wireless sensor network: A novel framework. In *3rd International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT-2018) at P.E.S College of Engineering, Mandya*. Springer-LNEE.

14. Deepak, T., Shetty, S., & Kevin, A. K. (2017). Security implications of blockchain cloud with analysis of block withholding attack. In *17th IEEE/ACM International Symposium on Cluster Cloud and Grid Computing (CCGRID)* (p. 458).
15. Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2016). *Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol*. Springer.
16. Swanson, T. Consensus-as-a-service: A brief report on the emergence of permissioned distributed ledger systems.
17. Duong, T., Fan, L., & Zhou, H. S. (2016). *2-hop Blockchain: Combining Proof-of-Work and Proof-of-Stake Securely*. Springer.
18. Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*, 151.
19. Ji, S., Cai, Z., Han, M., & Beyah, R. (2015). Whitespace measurement and virtual backbone construction for cognitive radio networks: From the social perspective. In *Sensing Communication and Networking (SECON) 2015 12th Annual IEEE International Conference on IEEE* (pp. 435–443).
20. Han, M., Yan, M., Li, J., Ji, S., & Li, Y. (2014). Neighborhood-based uncertainty generation in social networks. *Journal of Combinatorial Optimization, 28*, 561–576.
21. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture consensus and future trends. In *Big Data (BigData Congress) 2017 IEEE International Congress on IEEE* (pp. 557–564).
22. Min, X., Li, Q., Liu, L., & Cui, L. (2016, August). A permissioned blockchain framework for supporting instant transaction and dynamic block size. In *2016 IEEE Trustcom/BigDataSE/ISPA* (pp. 90–96).
23. Malkhi, D. (2012, January). Byzantine quorum systems. *Distributed Computing, 4*, 203213.
24. Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016, May). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In *IEEE Symposium on Security and Privacy* (pp. 839–858).

Index

H. L. Gururaj et al. (eds.), *Convergence of Internet of Things and Blockchain Technologies*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-76216-2