Blockchain for Smart Cities

Saravanan Krishnan
Valentina Emilia Balas
E. Golden Julie
Y. Harold Robinson
Raghvendra Kumar

ELSEVIER

Blockchain for Smart Cities

Edited by

Saravanan Krishnan
Assistant Professor, Department of Computer Science and Engineering, Anna University Regional Campus, Tirunelveli, India

Valentina Emilia Balas
Full Professor, Department of Automatics and Applied Software, Faculty of Engineering, “Aurel Vlaicu” University of Arad, Arad, Romania

E. Golden Julie
Department of CSE, Regional campus, Anna University, Tirunelveli, India

Y. Harold Robinson
Post Doctoral Fellow, School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, India

Raghvendra Kumar
Associate Professor, Department of Computer Science and Engineering, GIET University, Gunupur, India

ELSEVIER

Chapter 1

Introduction to blockchain and distributed systems - fundamental theories and concepts

Neha Sharma[1], Madhavi Shamkuwar[2], Sakthi Kumaresh[3], Inderjit Singh[4], Amol Goje[5]

[1]*Analytics and Insights, Tata Consultancy Services, Pune, India;* [2]*Zeal Institute of Business Administration, Computer Application and Research, Savitribai Phule Pune University, Ganesh Khind, Pune, Maharashtra, India;* [3]*M.O. P. Vaishnav College for Women, Chennai, Tamil Nadu,India;* [4]*Vara Technology Pvt Ltd, Pune, India;* [5]*Society for Data Science, Pune, India*

Chapter outline

Blockchain for Smart Cities. https://doi.org/10.1016/B978-0-12-824446-3.00002-8

1. Introduction

The speed with which the new technologies are being created due to fourth industrial revolution cannot be compared with any period in the history and is certainly exponential. The previous revolutions can be said to have evolved ata linear rate, with thefirst industrial revolution starting in 1765, followed bysecond in 1870 and third in 1969. The fourth industrial revolution happeningright now is boosted by the emergence of Internet and digitization. Internetcame in 1990s and unlike previous revolutions, within just 30 years a host oftechnologies like Internet of Things (IoT), Cloud Computing, etc., haveemerged out of Internet itself. Hence, we can see more and more technologiessupporting each other and being the reason for the emergence of some othertechnology. Technological revolution has placed the world at the threshold thatwill change the way the world is progressing. The change will be such that itsscale, sophistication, and transformation will be unlike the world has ever seenbefore, blurring the lines between digital, physical, and biological spheres.Mankind can only vision what developments this technological revolution willunravel, but to leverage it to the maximum the global leaders in technology,governments, and business should join hands to come to a consensus.

Technology does miracles toward the business growth and societal devel-opment, but at the same time poses major risks associated with dataflow, security, privacy, and integrity. In traditional system, generally system administrator is the centralized single trusted authority responsible for providing access rights to different users across the network. To make changesin the system is easy in this case as a single person is responsible for the sameand changes done are irreversible. System controlled by a single person is thussusceptible to changes and vulnerable to risks in terms of privacy, integrity,and security. When a system is person oriented there may be lot of data ad-versaries and the system is more prone to single-point-of-failure. To overcomethis, there is a need of technology which will eliminate the requirement ofhuman intervention and related threat. Blockchain is a solution to the aforesaidproblems where dependency on the centralized human authority is notrequired thus providing security from single-point-of-failure, along with otherbenefits like data immutability, reliability, and verifiability (Casado-Vara, Prieto, De La Prieta, & Corchado, 2018a; Dabbagh, Sookhak, & Safa, 2019;Reyna, Mart´ın, Chen, Soler, & D´ıaz, 2018). The transactions performed withblockchain are executed, stored, and monitored on decentralized networkinfrastructure (Aste et al., 2017). The emergence of the blockchain technologyinitially was forfinancial transactions, but later it emerged as the most promising technology in multiple domains such as electronic voting, health-care, education smart system, and certificate authorities (Henry et al., 2018).

The blockchain is the generic name for the database and transaction pro-cessing capabilities, which does ordinary things in amazing ways. Blockchaintransactions are transparent, secure, and free, which encourages multipleapplications to be built forfinancial and nonfinancial domain. Transferring the money without the need of third party is the most popular application,

e.g., Bitcoin (Dwyer, 2015). Implementing the contracts in neutral and unbi- ased way for achieving ethical practices in business is possible through anotherblockchain use case called Smart Contract. Blockchain can be used to store theidentity and accomplishments of the individuals in secured way so that it cannot be altered or stolen. It can also be used to store vast information in encrypted manner on distributed network and save on charges for cloud storage, which is heavy as we pay to the intermediaries, i.e., cloud owners for using the services. Blockchain also keeps the proof of provenance whichhelps in tracking the origin of the record and presents the credible record ofthe whole process (Becker et al., 2013; Peters & Panayi, 2016) (Hawlitschek, Florian, Benedikt, & Timm, 2018; Sara, Mahtab, & Joseph, 2018). Block- chains can become a very useful base to provide communication within a certain company or system, by creating a platform called ADEPT (Auton- omous Decentralized Peer-to-Peer Telemetry), which implements block- chains to form a base for cheap autonomous communication between all machines involved. In the other words, it is a successful attempt to create a blockchain-based Internet of Things (a system of electronic devices, whichare connected to the Internet, and interconnected among themselves) (Utilization of Blockchain Technology to Overthrow the Challenges in Healthcare Industry et al., 2015).

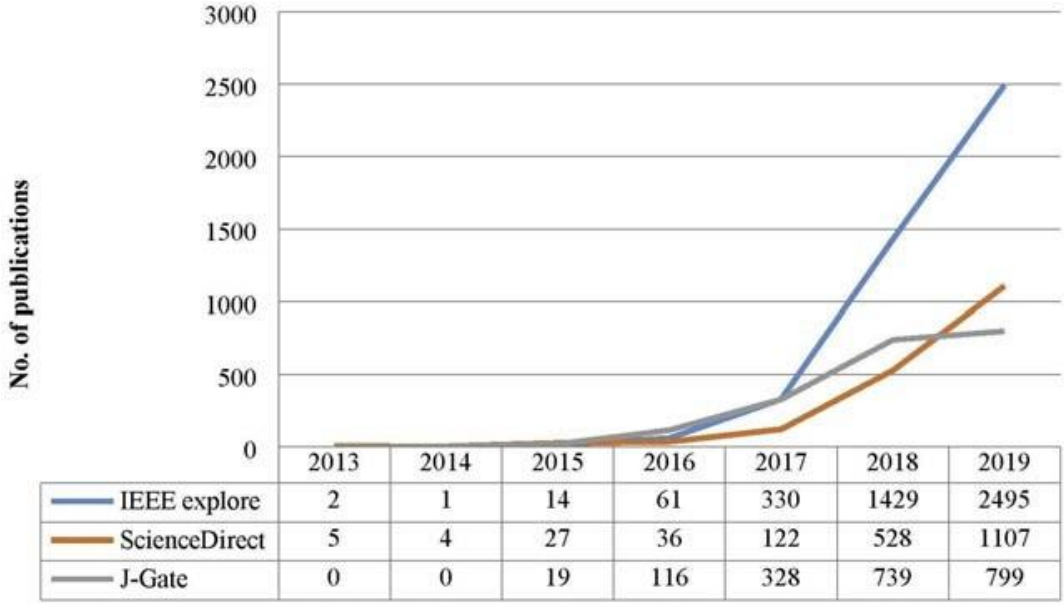
In this chapter, the endeavor is to systematically present all the concepts that have been adopted in a blockchain to make it a disruptive technology of this era. The next section focuses on the current research status with state-of- art review, highlighting systematic literature review and evolution of block- chain. Section 3 appraises the blockchain concepts like operations, networks, features, and consensus mechanisms, whereas Section 4 discusses types of blockchain and various platforms. Sections 5 and 6 present various interestingapplication and challenges, respectively. Finally, this chapter is concluded withprobable future of the technology.

2. Literature review

This section is further divided into two subsections. First subsection presents a systematic literature survey, whereas second subsection presents the journey of evolution of blockchain technology.

2.1 Systematic literature review

Thefirst step toward literature study is to identify related articles and carry outa systematic literature review. The authors of this chapter were keen to know the origin of blockchain concepts and its reflections in various articles types. From the study of research database IEEE explore, Science Direct and J-Gate,it is evident that the actual publication of the concept has emerged in the year 2013 (IEEE, nd). The concept has gained popularity over the years and same isdepicted in the increased number of (Fig. 10.1) publications with time as depicted in Fig. 10.1.



	2013	2014	2015	2016	2017	2018	2019
IEEE explore	2	1	14	61	330	1429	2495
ScienceDirect	5	4	27	36	122	528	1107
J-Gate	0	0	19	116	328	739	799

FIGURE 10.1 Year-wise publications in research database IEEE explore, Science Direct and J-Gate (IEEE, nd; ScienceDirect.com | Science, health and medical journals; J-Gate∈Largest e-Journal Gateway | Journal Finder | Journal).

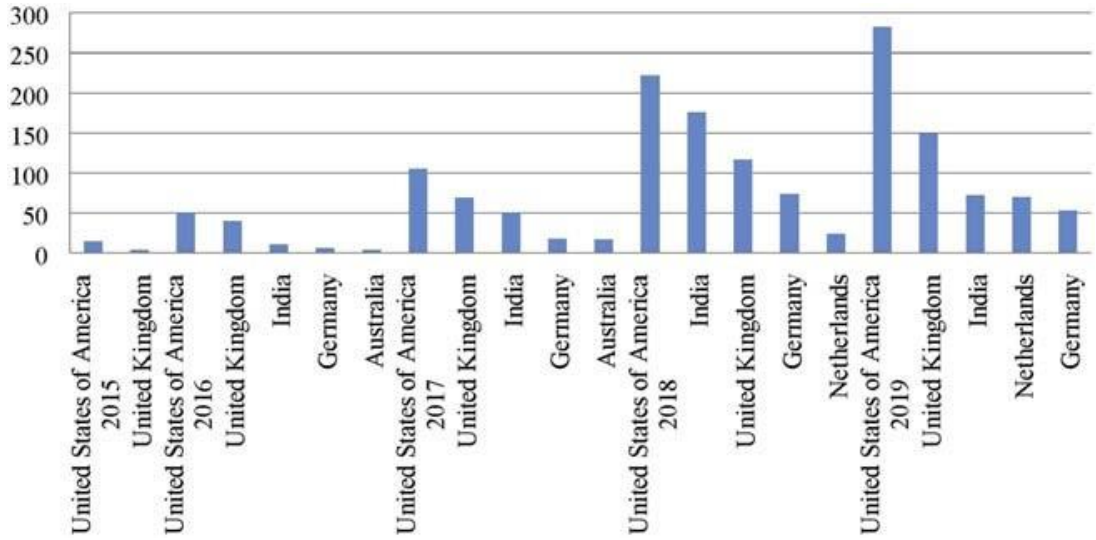


FIGURE 10.2 Country-wise publications in research databases J-Gate (J-Gate∈Largest e-Journal Gateway | Journal Finder | Journal).

The authors were also curious to know the country-wise publications related the "blockchain" concept and hence research databases J-Gate and IEEE explore were explored as shown in Figs. 10.2 and 10.3.

The Gartner hype cycle shown in Fig. 10.4 was published in the year 2019 (Gartner: Global Research and Advisory Company). It clearly suggests that blockchain technology is emerging and will reach its maturity not before next decade. So, it holds lots of opportunity to experiment and innovate.

Finally, to know the research interest of community toward blockchain technology, Google worldwide trends were studied for last 17 years, i.e., fromyear 2004 till current date (Google Trends). The trend shows rise in the searchof the term "blockchain" over a period of time as clearly evident in Fig. 10.5.

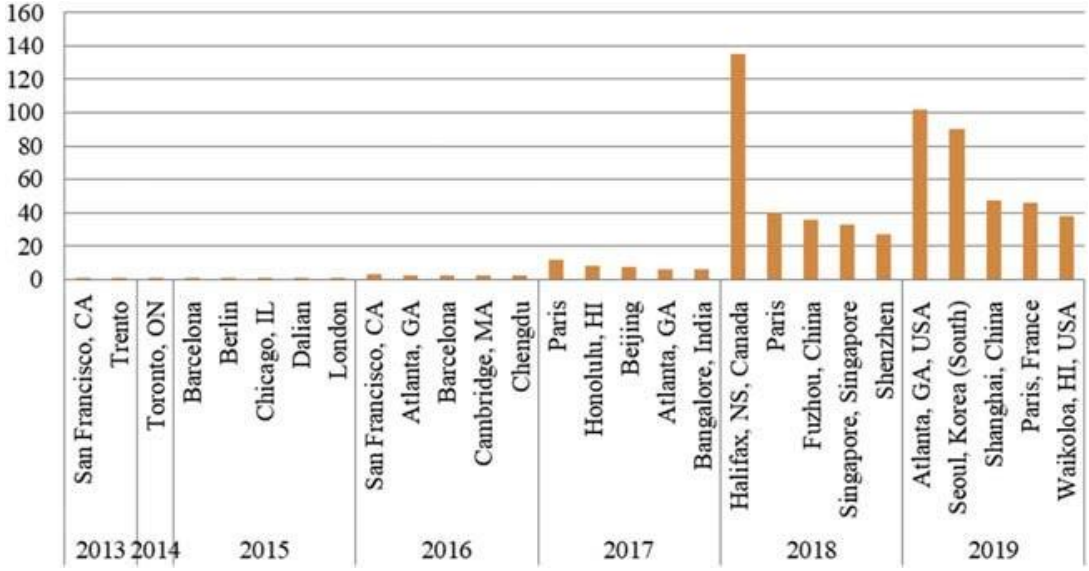


FIGURE 10.3 Country-wise publications in research database IEEE explore (IEEE, nd).

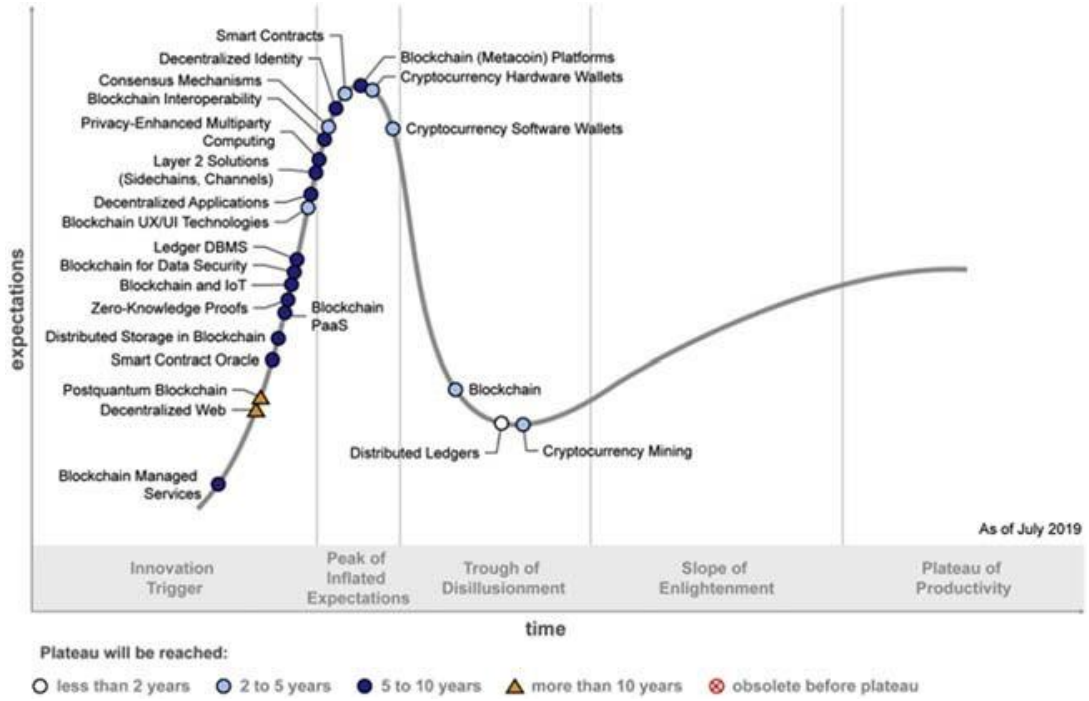


FIGURE 10.4 Blockchain and Gartner Hype cycle (Gartner: Global Research and Advisory Company).

2.2 Evolution of blockchain

Blockchain technology has evolved immaculately since early 1990s and isbeing successfully applied fromfinancial to nonfinancial applications like manufacturing, sales, education, etc. In this section, the evolution of block-chain is presented systematically.

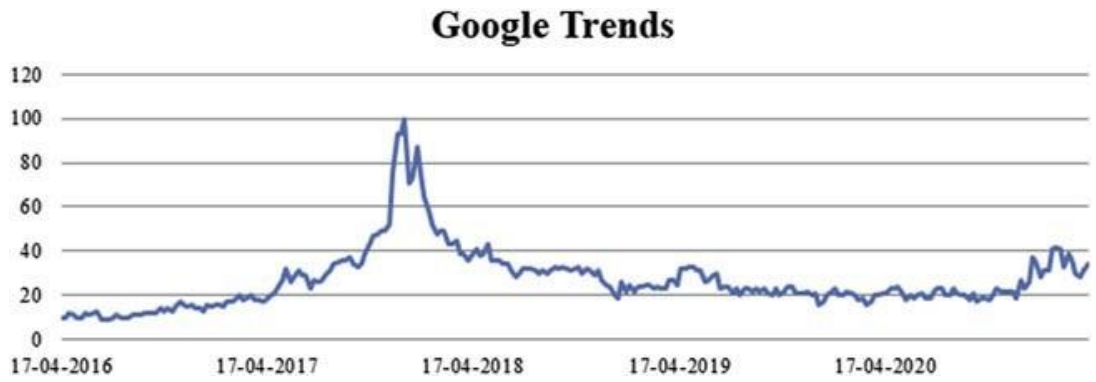


FIGURE 10.5 Google Worldwide trends for search term "blockchain" from 2004 till July 2020 (Google Trends).

It is very important to know from where you have come, in order toappreciate where you are and where do you want to go? The term "block-chain" came into light for thefirst time when a paper titled "Bitcoin: A peer-to-peer electronic cash system" was published online in 2008 by ananonymous person or group of people known as Satoshi Nakamoto (Naka- moto, 2008) and then with the implementation of Bitcoin in 2009. The paperrevolutionized the way data are stored and transactions are done. The data arepackaged in the block and block is added to the chain after approval. Once theblock is there on the network, it cannot be altered. The change can be reflectedonly by adding new block to the chain.

Bitcoin or blockchain did not start in 2008 or 2009, but is a part of larger movement. This is a technological solution to a social and political problem, which will continue to evolve in a greatest possible way. However, we cannot deny their origins. The philosophies from various electronic cash or digital cash paved the way for cryptocurrencies in general and bitcoin in particular. The movement from cash to digital started around 1990s. The fundamental requirement from any e-cash system is that it should address anonymity and accountability (Danezis and Diaz, 2008).

David Chaum has proposed many cryptographic concepts and protocols in his contributions from 1981 to 1990, like blind signature where the content isblinded before signature, anonymous communication network which was alsocalled mix network where message and sender are encrypted that can bedecrypted by the receiver for whom the message is meant, and secret sharingwhich is about detecting the use of same e-cash token twice (double spending),that built up the foundation for blockchain (D. Chaum, 1985; D.L. Chaum,1981; Danezis & Diaz, 2008; Nakamoto, 2008). He is the originator of digitalcash system, which took care of two fundamental requirements from anye-cash system and addressed anonymity and accountability. David Chaumfound afirst electronic cash company known as "Digicash" in 1990 and the first virtual currency was created in 1995 (Greenberg, 2012). The US-basedbank located at Missouri, Mercantile bank, which acquired the Mark Twain

Bank, was thefirst and only US bank to support DigiCash systems. Deutsche Bank, based in Germany, was the second backing bank of DigiCash systems (DigiCash's eCash to be Issued by Deutsche Bank - David). Digicash was ahead of its time and focuses on making transactions anonymous; however, the problem for solution offered was not evident as online trades and e-commercewere not popular. Chaum stated in an interview in 1999 that the DigiCash project, and its technology system, entered the market before e-commerce wasfully integrated within the Internet [26]. In 1998, DigiCashfiled a Chapter 11 bankruptcy and in 2002 the company was sold for assets to eCash Technol- ogies, another digital currency company, which was acquired by InfoSpace onFeb. 19, 2002. (Pitta, 1999) (A Cypherpunk's Manifesto - Activism.net).

Eric Hughes a mathematician from University of California, Berkeley; John Gilmore a computer scientist who was Sunmicrosystems'fifth employee,Tim May, a retired businessman who worked for Intel and many others, came together in late 1992 to form a group called "Cypherpunks." The grouppublished a "Cypherpunk Manifesto" which was written by Eric Hughes in 1993 highlighted the basic idea of the movement. The manifesto says that "Privacy is not Secrecy" and to achieve privacy the society requires anony- mous transaction systems and cryptography as well as it should be part of social contract. Privacy is about revealing the identity only when it is desired (Back, 2002).

The next attempt was made in 1997 by Dr. Adam Back, who developedHashcash system (AALWA: Ask any LessWronger anything - LessWrong).The system is also known as proof of work system which uses hash cryp-tography and allows anonymous communication basically to control emailspams and denial-of-service attack. Every email is added with a hashcashstamp as a header to prove that substantial amount of CPU time andcomputational power is used to calculate the stamp. The idea is to deter andmake sending spam mails difficult and expensive. The header is prepared bythe sender who initializes a random number and appends a counter to theheader and computes 160-bit SHA-1 hash of the header. The header isacceptable iffirst 20 bits, i.e., 05 most significant digits are all 0s, else the counter is increased and hash algorithm is applied again. Only 2^{140} hash valuessatisfy the criteria out of 2^{160} possible hash values, therefore probability of arandom selected header to have a hash with 20 leading 0s is one in 2^{20} orapproximately one in million and approximately one second of time is neededto compute the hash. A legitimate email sender would not mind spending thismuch time and computational power to generate a hash; however, this issignificantly uneconomical for a spammer who has to send large number ofmails. The computation at receiver's end is pretty simple and has to justcalculate 160-bit SHA-1 hash of entire string received and takes 2ms in 1 GHz machine. The recipient computer checks date, email, and hash string to vali-date the mail received. Hashcash system is an efficient brute force approach tofind a valid header and is a basis for mining algorithm used in blockchain.

Wei Dai, who is a computer engineer and a cypherpunk, published an articleon B-Moneyоan anonymous, distributed electronic cash system, in 1998,which ignited interest in cryptocurrencies (Ridley, 2017; Decoding the Enigmaof Satoshi Nakamoto and the Birth of ; Bitcoin: The Cryptoanarchists' Answer to Cash - IEEE Spectrum). His paper on b-money suggested many coreconcepts that are used in cryptocurrencies, and more specifically bitcoin like

1) Proof of Work for every transaction, i.e., amount of time and computational power needed.
2) The transaction is verified by a group of people/community who update a
3) combined ledger book, and they are incentivized for their efforts and being honest. This is called as proof of stake (PoS), where the group of people invests their money in a special bank and will lose all their stakes if they attempt to process any fraudulent transaction.
4) All the transactions and fund exchanges are maintained in two ways, i.e.,
5) every participant maintains a separate ledger regarding the money that belongs to them and a collective bookkeeping is maintained by group of people. The transactions and fund exchanges are authenticated with cryptographic hashes.
6) Contracts are enforced through the broadcast and signing of transactions
7) with digital signatures (i.e., public key cryptography).

In the same year, i.e., 1998, Nick Szabo, a computer scientist, cryptog- rapher, and a legal expert, designed a concept of decentralized digital cur- rency called "bit gold," which was never implemented but played a vital role in the architecture of a bitcoin (O'Leary, 2015; Peck, 2012; Tschorsch & Scheuermann, 2015). Bit Gold introduces the concept of timestamping and creation of money using hashcash. Computer power is dedicated to solve cryptographic puzzles by the participants and the solved puzzles are sent to byzantine fault-tolerant public registry and a public key of solver is assignedto it. Each solution would become part of the next challenge, creating a growing chain of new property. This aspect of the system provided a way for the network to verify and timestamp new coins, because unless a majority of the parties agreed to accept new solutions, they could not start on the next puzzle (Szabo, 1998). However, there were certain features which were missing in bit gold like incentives to keep nodes honest, a way to keep tokens fungible (no agreed way to set difficulty, one token might be made with significantly more difficulty than the other).

As can be seen, various people from across the world have been working tirelessly on the blockchain technology and cryptocurrencies since the 1990s and there have been multiple attempts to solve the complex issues surroundingcryptocurrency, by arguably some of the most brilliant minds in this space.

3. Blockchain concepts

A blockchain is a list of transactions or a record that is kept up by a network ofclients, instead of a focal specialist. It is referred to as blockchain in light of the very fact that new exchanges are prepacked into “blocks” of information and composed onto thefinish of a “chain” of prevailing blocks depicting everyearlier exchange. The blocks are linked by joining the hash of the earlier blockto the recent block, the recent block to the subsequent block, and so on. Successive nested blocks undertake transactions in a serial order, thus a transaction cannot be changed antedated without changing its block and all thefollowing blocks. A subchain of the block is regarded only if it is larger than acompetitor chain. Honest nodes should produce fresh blocks quicker than an opponent’s attempt to do so. The scheme delivers this efficiency by imple- menting a proof-of-work system, which testifies that a node has invested the required funds to do a computationally challenging job.

A standard blockchain is an outstanding structure of information that stores historical statements and transactions. All nodes in the framework arein agreement with the operations and their order. In blockchain, the records are distributed in different blocks and each block is connected by a crypto- graphic pointer to its predecessor, and way back to its initial block. The basic structure of the blockchain is shown in Fig. 10.6, where each block has two main sections: block header and block body. Each block header has a unique identifier in the form of hash which is generated using hash algorithm. Apart from hash, the other components of block header are index, previous hash, number of transactions in the block, timestamp, and nonce as shown in Table 10.1. The body of the block is a collection of all transactions stored in various arrays and implemented using a data structure called Merkle tree. Hence, every block in the network is connected altogether, forming a chain of integrity. Transactions in an open blockchain are publicly visible, while the view is restricted in the case of personal blockchain or a blockchain consortium.

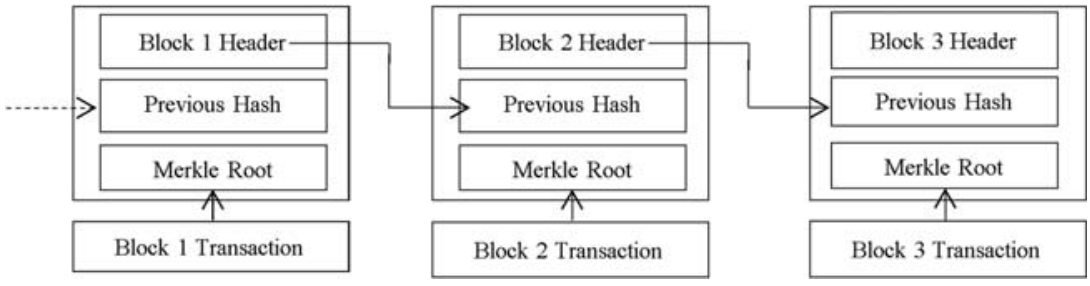


FIGURE 10.6 The structure of a blockchain.

TABLE 10.1 The component of the block.

Name of the component	Description
Index	It is a unique sequential number that informs about the block position in the blockchain. The index of thefirst block is “0.”
Hash	It is a cryptographically generated unique number, mainly used for quick identification of data.
Previous hash	It is the hash of the preceding block.
Time stamp	It stores the time of block creation.
NumTx	Number of transactions embedded in the block.
Nonce	It is the number which is used only once in the mining process.
Transaction	It is a data record that has to be saved on the blockchain.

3.1 Blockchain operations

As discussed earlier, each block consists of some value, like the hash of theblock and also of the previous block. The value that is kept within a block isbased on the kind of blockchain. For instance, Bitcoin blockchain stores theinformation of transactions, like the sender, receiver, and quantity of coins.The mining process ensures the validity of the transaction (Gatteschi et al.,2018). A hash of the block is like afingerprint that uniquely identifies theblock and all its content. The hash is computed, once the block is formed.Altering anything in the block would result in changed hash, which means it isno longer the same block. Now, this block with new hash value needs to beupdated to the local copy of blockchain of every node in the network. So, thatblockchain architecture maintains a strong consistency among nodes in thenetwork.

A block is a container data structure with average size of 1e8 MB, and is large enough to handle huge number of transactions. The structure of block consists of two components such as block header and list of transactions. Block header consists of metadata about block such as previous block hash, mining statistics, and merkle tree root. Previous block hash is used to create the new block hash as represented in Fig. 10.7 (How does a blockchain work - Simply Explained?ᑯSteemit). If all the transactions in a block are arranged in a tree form, then it is called as merkle tree. In a merkle tree, every leaf node consists of the hash of the transactions, and the intermediate nodes consist of the combined hash values. The structure of merkle tree is presented in Fig. 10.8. At the root level, the merkle tree contains the combined hash of

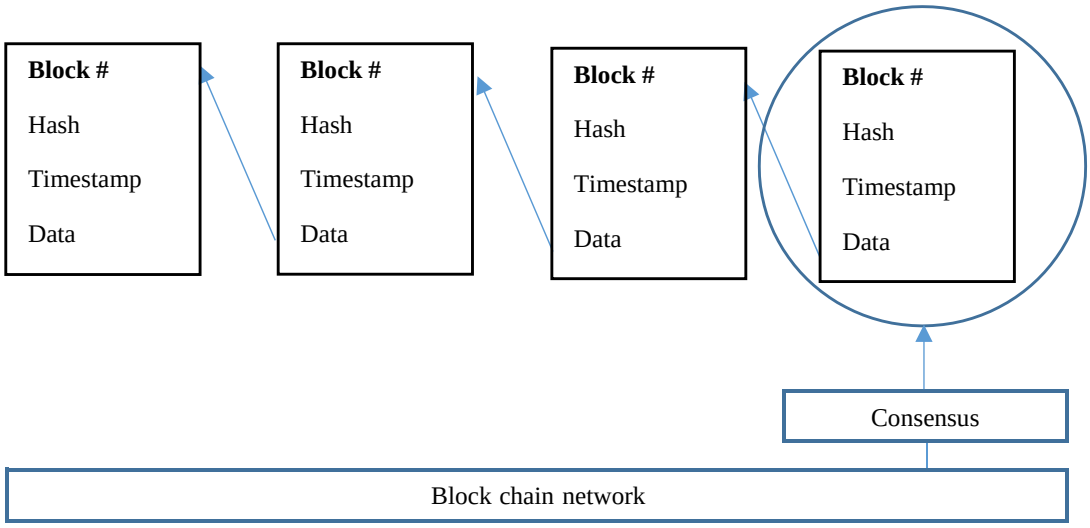


FIGURE 10.7 Blockchain operations.

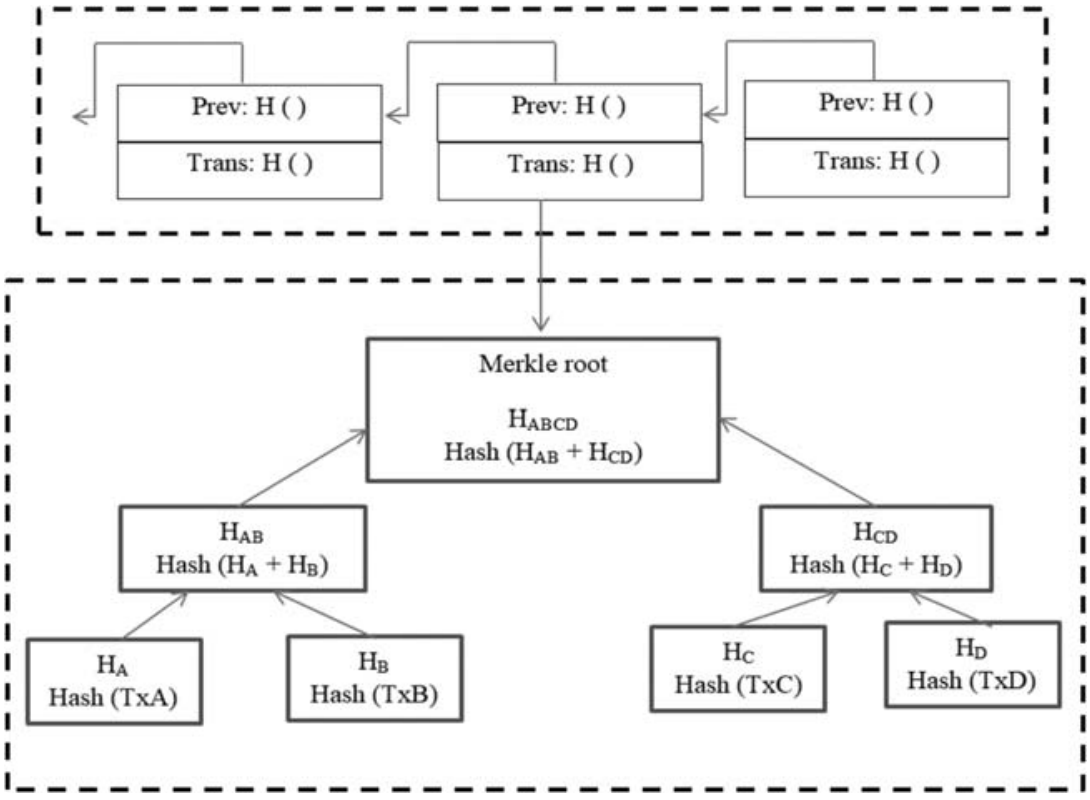


FIGURE 10.8 Merkle tree implementation of a blockchain.

the right tree and left tree. If anyone wants to change the transaction, the hash will get changed and at the same time the changes will be reflected in the root hash as well. If the root hash changes, the hash of the linked blocks will also change, which will lead to a tamper-proof architecture (Computer Science and Engineering - NOC _ - NPTEL).

Figure seven depicts an example of a blockchain which has a series of fourblocks and every block features a hash along with the hash of the previousblock, which binds them in a chain. Thefirst block is known as the genesis block as it does not direct to any previous blocks. Now, if the second blockgets tampered, the hash value of the block will get changed. Therefore, thehash value of the second block will not match with the previous hash value ofthe third block. This will result in making block three and every other blockinvalid as the blocks do not contain a legitimate hash of the previous block. So,altering one block can make the subsequent blocks invalid (conda).

However, utilizing hash values is not enough to stop tampering, as com- puters are powerful and very fast to compute tons of hash values per second. Incase of any tampering, it can compute all the hash values of other blocks to form the blockchain valid once again. So, in order to eliminate tampering, a concept of proof of work (PoW) is used, which is a procedure that slows downthe formation of latest blocks. In case of Bitcoins, it generally takes 8 to10 minutes to compute the desired PoW and add a brand-new block to the chain. This procedure makes alteration with the blocks, extremely difficult. Asa result, if a block is altered, the PoW will have to be recomputed for all the subsequent blocks.

There is another method which makes blockchains secure and that is by being distributed. Whenever any user joins the network, he will get the complete copy of the blockchain. The node will utilize this to check that everything continues to be in the sequence. Now, as a new block is generated, each and every node in the network receives a copy of it. The nodes then checkthe block to ascertain that it is not been altered or modified, and then include this block to their own network and produce an agreement regarding valid andinvalid blocks.

3.2 Blockchain network

The “blockchain” is the core principle behind Bitcoin digital currency (Hayden & Choi, 2019). It is decentralized, distributed technology that collectsa digital record of any event and store it in a distributed database that is sharedamong all the users connected with it. Every transaction in a blockchain is verified by the majority of the connected nodes of the system. Once infor- mation is inserted it cannot be erased or altered. Bitcoin which is the decen- tralized peer-to-peer (P2P) digital currency medium is among the list of majorly accepted and favored implementations of blockchain technology.

To understand decentralized, distributed P2P network which is the backbone of blockchain, there is a need to grasp the concept of various networking sys- tems, its functioning as well as its pros and cons. The network system is like a hierarchy in government administration or clientєserver architecture in data- base management systems. The basic difference in various network systems isthe concept of authority. There are some common definitions of authority, like

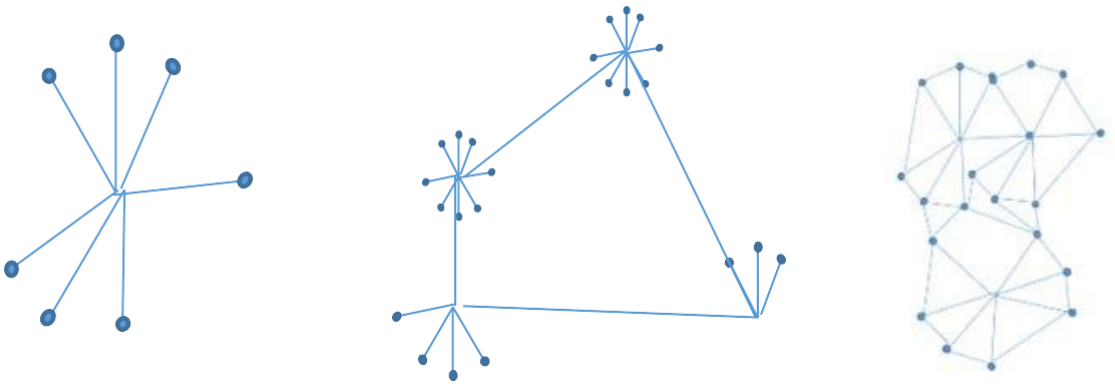


FIGURE 10.9 Types of network systemsd(A) centralized, (B) decentralized, (C) distributed.

the right to give commands, be in-charge, make decisions, and enforce obedi- ence in the organization or person, having control in a typically administrativesphere and the power to influence others. Therefore, on the basis of center of authorities, the network systems are divided into three types: centralized, decentralized, and distributed network systems as shown in Fig. 10.9.

3.2.1 Centralized system

Centralized systems have just one point of authority and this is where all the control is concentrated. All the processes and decisions are carried out at the single location, which makes the system extremely susceptible to collapses, meaning any disruption at central server can collapse the whole system.
Advantages of Centralized System:

1) It is very easy to implement and helps in quick decision-making. Since single authority takes the decision, there is no consensus required.
2) With just one single authority, there is no chance of multiple authorities performing the same function and this reduces the economics of scale. Drawbacks of Centralized System:
1) There is dependence on one single authority for data and security. The
2) system is unsafe as any attack on the sole authority shall destabilize the system and might lose primary source of information.
3) It's bureaucratic in nature and thus it adds many layers and hierarchies.
4) It is not transparent and thus prone to fraud. The lack of transparency will induce irresponsibility at the top level since that is where the power is concentrated. Some examples of centralized network systems are abanking system, food franchises like McDonald's or Silversea.

3.2.2 Decentralized systems

The decentralized systems have several points of authority and thus power is more diversified. This makes the system less susceptible to downfalls as the fall of a single point of authority would not bring down the entire system. The hierarchy is thusflat compared to a centralized system.

Advantages of Decentralized System:

1) The decisions are now made much closer to the consumer. Thus, the decision-making authorities have more information about the end users.
2) Second the system is less susceptible to collapses because now there are multiple points of authority. The downfall of one point is not going to bring about a destabilization of the system as we saw in centralized systems.

Drawbacks of Decentralized System:

1) There are still the economies of scale as with multiple authorities the duplication of task problem persists.
2) Although they are safer than centralized system, they are still susceptible to collapses. Thus, they are not completely safe.

A few examples of these are supply chains like Johnson and Johnson's.

3.2.3 Distributed systems

In distributed systems, everyone has an equal authority which makes thesystem virtually unsusceptible to collapses. However, this does not guarantee that the system is safe from being hacked unless and until at least 50%authority is with the system. So, a distributed network has aflat hierarchy.

Advantages of Distributed System:

1) The biggest benefit that distributed systems introduce is that it removes the need for intermediaries.
2) The network is economical and unviable to bring down, which makes it extremely secure and safe system.
3) The complete transparency in the system prohibits fraud.

Drawbacks of Distributed System:

1) These systems are still new and the technology is still nascent. So, it will take a lot of time to stabilize.
2) There will be economies of scale with time; however, initial imple-
3) mentation of the system is very expensive.

A few examples of these are cryptocurrencies and blockchain networks.

3.3 Features of blockchain

A blockchain technology has many features and some of them are listed below:

(a) Decentralized:Each transaction in the centralized systems requires to be validated through the central trusted agency (e.g., the central bank),inevitably resulting in the cost and the performance bottlenecks at the central servers. Hence, instead of a single source, multiple participants areconsidered who agrees upon the transaction with the help of consensus algorithm (Croman et al., 2016). Besides, a transaction in the blockchain network can be conducted between any two peers (P2P) without the need of authentication by the central agency. In this manner, blockchain can significantly reduce the server costs (including the development cost and the operation cost) and mitigate the performance bottlenecks at the centralserver (Zheng et al., 2018).

(b) Security:The transactions in blockchain are encrypted and linked withthe previous transaction. Therefore, the criminal activities like hack, fraud,or unauthorized access of critical information can be prevented (Topfive blockchain benefits transforming your industry - IBM).

(c) Immutable:A blockchain follows the append-only ledger principle which makes it an immutable technology. If information in one block is changed,it will have a ripple factor, i.e., it will demand change in subsequent blocksmaking the overall working infeasible (Eyal & Sirer, 2014; Nakamoto, 2008). In this immutable ledgers, the consensus of the participants is verified, thus the transactions log created cannot be altered or replaced (Lemieux, 2016).

(d) Distributed Ledger:The blockchain shares undefined copies of all data. Participants approve data independently without an authority being integrated. The remaining nodes continue to work, even if one node fails, ensuring no disturbance (Lavanya, 2018).

(e) Scalability:The block rate consists of throughput and information propagation time. However, it depends on the consensus algorithm and the number of participants involved in the transaction. The large number of participants will lead to limit the desired high throughput (Croman et al., 2016). In blockchain every node holds the information of other blocks, so scalability becomes crucial when the data size is large (THE EUROPEAN UNION BLOCKCHAIN OBSERVATORY).

(f) Persistent:Every transaction expanding across the network has to be confirmed and registered in blocks shared within the network, which makes it infeasible to tamper. In addition to this, every broadcasted block will be verified by other nodes and help in identifying the spam, if any.

(g) Anonymity:All users can make communication with the blockchain network through a generated address. However, a user could also create

(h)
(i) more than one addresses to mitigate the exposure of identities. There is no centralized entity storing user's personal data. This characteristic pre- serves the privacy of the transactions. But to be noted, blockchain cannot ensure the 100% authorization due to the underlying limitations.
(j) Auditable:Since every transaction in the blockchain is attested and registered along with a timestamp, users can check and discover the past records with so much of ease. Users can do so through accessing any node in the distributed network. In Bitcoin, all the transactions within the
(k) network could be discovered to earlier transactions repeatedly. This in- creases the transparency of the data kept inside the blockchain.
(l) Transparency:Blockchain is a distributed ledger in which all the par- ticipants in the network share the same information. Hence, transactions become more transparent.
(m) Digital:Entire information in blockchain is digitized disposing of requirement for common documentation (Blockchainerevolutionary change or not? Cross sector use).

3.4 Different blockchain consensus mechanisms

Consensus mechanisms are protocols that make sure that all the nodes are synchronized with each other and agree on transactions which are legitimate and are added to the blockchain. These consensus mechanisms are crucial fora blockchain in order to function correctly and to minimize the risk of differenttypes of attacks. They make sure everyone uses the same blockchain. Everyone can submit the data to be added to the blockchain; therefore, it is essential to check the transactions constantly and to perform continuous audit of the blockchain by all nodes. There are many ways to reach consensus, so this section discusses the most popular ones.

3.4.1 Proof of work

Proof of Work (PoW) is thefirst blockchain consensus mechanism and was first used by Bitcoin. However, this has been adopted by many crypto-currencies successfully. The PoW creates a new block with the help of miningprocess which is carried out by the few special nodes in the network, which areknown as miners. Each miner competes with other miners to solve complexmathematical puzzles and get rewarded. However, it is important to note thatsolving the puzzle requires enormous amount of computational power as thereis no way tofind the solution except for continuously guessing it till the time we get the right answer, which might take lots of time. More computationalpower is needed to solve the puzzle in faster way, making the process furtherexpensive. Nevertheless, verifying the correctness of the solution is extremelysimple, which makes PoW process very popular.

3.4.2 Proof of stake

Proof of Stake (PoS) works on a philosophy that the miner who owns most coins in the blockchain network holds the authority to validate or mine thenew transaction of a block. In a system that uses PoS, a randomized processis used to determine the miner who gets to produce the next block. Userscan stake their tokens to become a validator (someone who can produce blocks), which means they lock their tokens up for a certain time. After doing so they are eligible to produce blocks. The factors affecting the process of deciding the next miner to produce the next block depends upon the design of the blockchain, maximum number of coins, and also the duration of coins being staked.

PoS is much more energy efficient than the PoW system. In a PoW system,a miner may not own any coins they are mining, which means they only seek to maximize their profits without actually improving the network, whereas in aPoS system, validators have a much bigger incentive to maintain the network as they actually hold the coins of the blockchain which they are validating.

3.4.3 Delegated Proof of Stake

Delegated Proof of Stake (DPoS) is one of the fastest consensus protocols where stake-weighted voting system mechanism is implemented for digital democracy. In a DPoS-based blockchain system, miner (participants/stake-holders) can vote for a certain number of delegates by staking their coins andthe weight of their vote depends on their stake. Hence, the stakeholdersdelegate or outsource their responsibility to a third party. For instance, if twominers stake 10 and 20 coins on two different delegates, respectively, then thevote of second miner weighs double than the vote offirst miner. So the au- thority to produce the block goes to the delegates that receive the highest votesand they are rewarded for the same. The number of delegates that gets apermission to create blocks depends on the blockchain design.

3.4.4 Proof of Capacity

The next consensus mechanism is Proof of Capacity (PoC) that makes use ofa process called plotting, where solutions are prestored. In PoW process, massive computational power is needed by the miners to guess the correct solution, whereas in PoC process, the digital storages like hard disks are used to prestore the solutions, and this process is called plotting. Once the storage has been fully plotted with solutions, then the particular miner can take partin the process of block creation. However, the miner who solves the puzzle first, gets the opportunity to create the new block. In PoC process, the emphasis is on storage capacity, as bigger storage allows stocking more solutions and thus increasing the chance for creating a block.

3.4.5 Proof of Elapsed Time

The last consensus mechanism is Proof of Elapsed Time (PoET), which is a random process to decide the miner who will create the next block on the basisof waiting time. In this process, a random wait time is assigned to each node and the opportunity to create the new block is given to the node whichcompletes its wait timefirst. PoET can work effectively if there exist a system to authenticate that multiple nodes are not run simultaneously and assignment of wait time is genuinely random.

4. Blockchain taxomony

In this section, different types of blockchains and various platforms have been discussed.

4.1 Type of blockchains

Depending on the requirements of applications, the blockchain can be broadly categorized into four types as shown in Fig. 10.10:

1. Public Blockchain
2. Private Blockchain
3. Consortium or Federated Blockchain
4. Hybrid Blockchain

4.1.1 Public blockchain

Public blockchains are publicly accessible and has no restriction on who willtake part, share, or be a validator. In this blockchain, nobody has the full

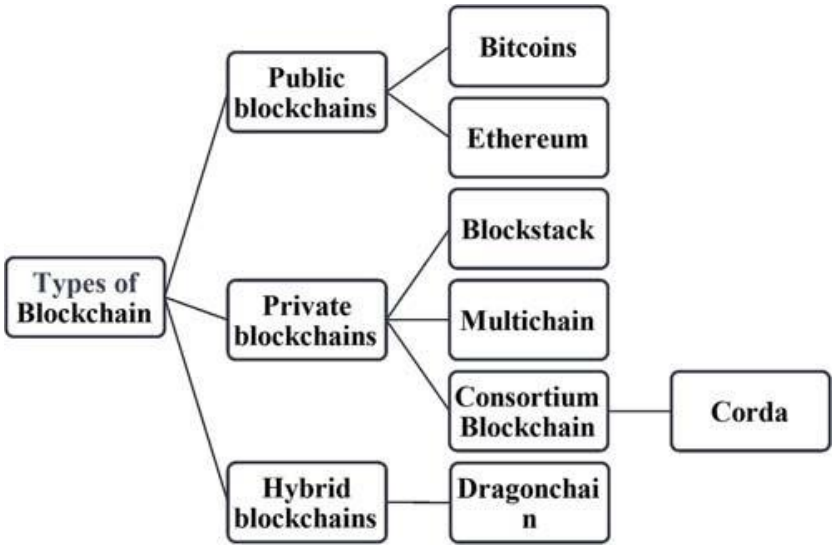


FIGURE 10.10 Types of blockchain.

control over the network but everybody can read or write. This characteristic ensures the security of data and helps to achieve immutability, as it becomes impossible for single individual to deceive this type of blockchain. The controlon the blockchain is equally distributed among each node in the network and hence is known as thoroughly distributed and fully decentralized network. They are majorly used for creating cryptocurrencies like Bitcoin, Litecoin, Ethereum by blockchain companies like Factom and Blockstream.

4.1.2 Private blockchain

Private blockchains are also referred as permissioned blockchain. It has certain limitations on who can access it and participate in the transactions. Only selective entities are permitted to access it, rather it can be said that only ownerbeing a centralized authority can access it or grant permission to make changesin it. The roles and access rights are defined at the time of building the blockchain application; however, network administrator can take care of assigning the rights to new user or to revoke it from an already created user. These blockchains are majorly implemented in private companies to efficiently manage the confidential data that should be accessible or available solely to the authorized person or people within the organization. Due to the very fact that private blockchain is nothing but a closed blockchain, the information is restricted within the organization's sphere and it is completely inaccessibleor unattainable to any unknown entities. Eris Industries, Blockstack, andMultichain are few example of private type of blockchain [53].

4.1.3 Consortium blockchain

Consortium blockchain is a type of private blockchain and is governed by a group rather that a single entity. It is a collaborative model that brings group oforganizations that work and compete with each other. This type of blockchain can be more efficient as some rights can be kept restricted to individual like data access rights in order to keep it secure from public access, whereas groupcan collaborate on some common aspects of the business. There can be two types of users of such blockchain:

i. The users who have full charge over the blockchain and who can select who should have the rights to access the blockchain.
ii. The users who will simply access the blockchain, like participants from bank, government, etc.

4.1.4 Hybrid blockchain

A hybrid blockchain draws its feature from public as well as private block- chain. The permission-based structure of a private blockchain system is combined with the security and transparency of a public permissionless system.This makes the hybrid blockchain veryflexible for the users, who can

effortlessly join a multiple public blockchains from private blockchain. Usually, in a hybrid blockchain, the transaction of a private network is verified within that network. However, it can also be verified in the public blockchain by increasing the hashing function with the help of more nodes to improve the transparency and security of the blockchain network. A popular example is Dragonchain.

4.2 Major blockchain platforms

The abovementioned types of permissioned and permissionless blockchains can be used to develop different interesting applications in different platforms discussed in this subsection.

4.2.1 Hyperledger

Hyperledger is an open-source project that aims to create a suite of tools for enterprises to deploy blockchain technologies quickly and effectively. The protocol is commonly used in blockchain software solutions because it comes with its libraries that help to speed up development. The Linux Foundation is astrong supporter of Hyperledger, and it has supplied significant expertise to accelerate the creation of the protocol. Hyperledger is also highly compatible with Linux, so it is designed to work effectively on the same servers that are widely used in today's business world.

4.2.2 Ethereum

Ethereum was proposed by a Russian∈Canadian coder, Vitalk Buterin in 2013.It is an open-source and distributed computing platform, mainly used for executing smart contracts. An Ethereum platform has a run-time environment, Ethereum Virtual Machine (EVM), which needs to run on each node. It is essentially a permisssionless platform that works on Proof of Work which makes it very slow. Ethereum ecosystem is fueled with the help of native cryptocurrency called Ether. Anyone who wishes to uses the platform for running an application and executing the transactions has to pay in Ethers.

4.2.3 Ripple

Ripple platform was discovered in 2012 to enable global payments by con- necting banks, digital asset management company, payment providers, cor- porates, etc., using RippleNet. It is an open-source distributed consensusledger that uses the native currency called Ripple or XRP that achieves the consensus between nodes using probabilistic voting. Ripple is faster and scalable in comparison to other blockchains as it is built on advanced tech- nologies. It has three prominent applications like xVia to send payments acrossmultiple networks, xRapid to reduce liquidity costs, and xCurrent for cross- border payments. Many industry giants are testing Ripple to integrate it totheir existing payment system.

4.2.4 IOTA

Internet of Things Application (IOTA) was founded by David Sønstebø,Sergey Ivancheglo, Dominik Schiener, and Dr. Serguei Popov of Germany in2015. It is a decentralized currency which is developed on a futuristic tech-nology known as Internet of Things and is not based on blockchain technology.Cryptocurrency based on blockchain technology is generated by miners bysolving complex puzzle, whereas IOTA eliminates this transaction cost asthere is no associated fee. An IOTA transaction is executed if the user verifiesother two random transactions in this decentralized environment ensuring afaster network. IOTA is different than existing blockchains as it uses ablockless distributed ledger called Tangle and incorporates direct acyclic graph(DAG) feature. IOTA coin cannot be purchased with the traditional cash andcan only be bought in the exchange of other cryptocurrencies like Ethereumand bitcoin. It's a global trend to maximize the sharing of resources like tools,appliance, drones, storage devices, processors, eBikes, wifibandwidth, etc., instead of keeping it idle. IOTA coins help to lease and share such resourcesand also can be used profusely for applications toward e-voting, e-governance,masked messaging, etc.

4.2.5 Chain core

Chain core is a blockchain infrastructure which uses a chain protocol toimplement a permissioned network. It is mainly used for issuance and transferof assets, especially related tofinance like derivatives, gift cards, securities, loyalty points, and coins. The developer edition of this blockchain is free;however, the commercial edition is available for the organizations which wantto run it in production environment. The process of asset creation, control, andtransfer among the participants is decentralized, but the network is mainlygoverned by designated set of entities known as a federation.

4.2.6 Corda

Corda was developed in 2015 by an association of world's leadingfinancial institutions called R3. It is a blockchain platform that uses a smart contract protocol to record, supervise, and synchronize thefinancial agreements be-tween regulatedfinancial institutions by removing costly frictions in business transactions. There is no built-in token or cryptocurrency in corda and is an open-source permissioned blockchain, where only approved participants are allowed to access the data, which certainly boosts privacy and offersfine-grained access control to digital records. It was initially designed for the financial sector by the consortium offinancial industry; however, now it has multiple applications in trade, supply chain, healthcare, government sector,etc. As per the record, more than 60firms including front runners use Corda blockchain platform and very heavy investments around 107 million USD into Corda.

5. Applications of blockchain

There are many applications that are built using blockchain technology for transforming society.

(a) Smart Contracts: It is a computer protocol or a program which controls the transactions of digital money among different parties with specific conditions. These contracts are stored on blockchain technology, whichintends to facilitate, check, and enforce the performance of contracts
digitally. In real-life scenario, an arbitrator makes sure that everybody follows the terms. The blockchain not solely waives the necessity for thirdperson or parties, but additionally make sure that all ledger participants have the fair knowledge of the contract details and that agreement terms implement mechanically once conditions are met. Smart contracts are often used for various things, like monetary services, insurance policies, property laws, legal documents related to crowd funding, etc.

i. One such application of smart contracts is drought insurance systems where the users are insurers and famers, who are engaged in the entireinsurance process where the farmers need weather-based insurance
programs. The applications are developed using NEO blockchain platform, executed on NeoVM and use Oracle as a Service to fetch theexternal data using Application Program Interface (API); the system calculates the compensation values for the farmers who become victim of extreme weather conditions (Nguyen et al., 2019).

ii. The next application discusses supply chain operations between Consumer and Provider of service in supply chain operations bycreating a Document of Understanding (DOU). To build Blockchainnetwork, Hyperledger Fabric was installed on Intel-based servers
running Red Hat Enterprise Linux 7 (Montes et al., 2019).

(b) Tokenization: For authenticating a singular physical item, the things are combined up with a corresponding digital token or stamp. This impliestokens are accustomed to link the physical and digital worlds. Thesedigital tokens are very helpful in terms of providing chain management, anticounterfeiting properties, and scam detections.

i. The research paper is based on real estate (RE) with having RE tokenization integrates the RE investors, tenants and sellers in theprocess. These tokens are "unit of account" with properties countable,fungible, and divisible. With such token properties, people tend to usethem to denote value of property assets they possess, these T-tokenshence become a "medium of exchange" (Latifiet al., 2019).

ii. Steemit is a Multi-Token Economy with three different economic activities: Steem, Steem Power, and Steem Dollars, the beneficiariesof these systems get benefitted by Steem and Steem Dollars. Both ofthese activities are economic activities and are responsible for external exchanges. This public content platform is entirely laid on blockchain and has much complicated token economy design (Kang et al., 2019).

(c) Interorganizational data management: Blockchain technology brought a revolutionary change in the way information is gathered and collected. Itis less regarding maintaining information and more about managing a system of records. Hence, this helps in management of interorganizationaldata with so much of ease.

(d) For governments: The components of blockchain technology can be implemented to maintain all the activities of government. Blockchaintechnology proves to be a possible way to enhance government servicesand stimulate additional clear governmentcitizen relations. The distrib-uted technologies can work to dramatically optimize various business procedures through more effective and secure sharing of data.

i. Blockchain is used for "reward checking system" for Thai Govern- ment where customer and lottery administrator play their role in thelottery wining process. The customer owns Ethereum address withdetails such asfirst-time lottery purchase, consequent purchase, award announcement, and create Ethereum wallet for customers (Saichuaet al., 2019).

ii. South Korean government proposesfive phasebased framework for National Digital ID based on the blockchain (NIDBC) for identity and authentication management. The procedure of NIDBC is explained with respect to national health insurance service of the National Health Security Office (NHSO) has been presented (Chakraborty,Aich, & Kim, 2019).

(e) Healthcare: Blockchain features a vast scope in healthcare industries. The blockchain technology facilitates the efficient and secure transfer ofmedical records of patients, manages the health supply chain, and helpsthe healthcare researchers or analyst to unlock the genetic code. Various companies use the concept of blockchain to improvise the way the medicaldata are shared and used. The integration of Internet of Things (IoT), Blockchain, and Machine Learning framework is responsible to detect anomaly in the patient's health such as heart beats, pulse rates, calories burns, sleep time monitoring using two networks, i.e., Personal Health Care (PHC) BlockChain and the External Record Management (ERM) Blockchain (Lee et al., 2019).

i. SHAREChain is a Smart healthcare data sharing framework which has five components Patient Identity Source, Consumer, Data Source, Repository, and Blockchain registry responsible for providing reliableand interoperable data to solve problems which arise due to data sharing process.

ii. Gem, a United Statesbased startup, prepares an ecosystem in healthcare using Ethereum Blockchain technology termed as Gem

Health Network. The system uses patient-centric approach where transparency of data and process exists among multiple stakeholders (Mettler, 2016).

(f) Financial Service: Blockchainfinancial services are redefining the pre- vailing rails of recentfinancial markets' infrastructure. This sector expe- riences vital activities that range from backend clearing and settlement to the worldwide capital markets' design. In a number of these cases, the distributed ledger systems do not require being completely decentralized, and various monetary establishments are gazing to build their own "private blockchains."

Besides, there are many application of blockchain technology like Abra which allows the money transaction without the need of bank account or paying transaction fee, whereas Guardtime ensures industrial cyber securityfor Estonian Project. Augur performs market prediction using blockchaintechnology, which can also be used for betting on sports, stocks, naturaldisasters, elections, etc. Ujo is an application that implemented smart contractsto bring transparency in music industry, whereas Ubitquity implements for ensuring provenance and avoid middle man in real estate industry. Storj is cloud-based decentralized storage which allows people to save their data in aneconomical way with more security. OpenBazaar employs smart contracts to establish connections between buyers and sellers.

6. Challenges of blockchain

Blockchain is still in nascent stage and there are many challenges which are listed in this section:

(a) Blockchain RegulationdIt is highly important to define the legal scope of blockchain as companies in various sectors are waiting to get concrete direction on regulation and legislation so that it can be implemented

(b) without any legal risks. There are areas such as Smart Contracts where there is a looming uncertainty on regulation and existing regulations do not cover Smart Contracts.

(c) Blockchain ComplexitydBlockchain uses complex technical jargon which could be difficult to understand by nontechnical users and hence efforts are taken to create glossaries and indexes to make it understand- able. Even though companies and organizations are using distributed

(d) ledger technology in a great deal, there is a shortage of skilled blockchain developers.

(e) Blockchain Security Issuesd51% attacks are one of the most known security vulnerabilities where blockchain's hash rate is controlled by malicious entities and these entities perform double spends by reversing the transactions and blocks the miners to confirm the blocks. Poor security

(f) practices also open security loopholes and hackers can easily attack on the

(g) cryptocurrency exchanges. Blockchain has been attacked by various types of malware such as crypto jacking where the malware consumes com- puter's resources to mine cryptocurrency.
(h) Blockchain ScalabilityдBlockchain's transaction history keeps growing on daily basis and thereby there is a constant risk of slowness in the system. Blockchain's scalability depends on various factors such as block size, response time, fees, etc. At the beginning, the capacity of a block in blockchain was 1 MB and each block could hold almost 2020 transactions. Over the time, the number of transactions has started to grow causing a scalability problem. Since every transaction goes through a validation process, the number of transactions need to stay up for an extended time in the queue to get validated causing slower response time and scalability concern.
(i) Cost and EfficiencydThe Blockchain technology is quite competent in cost reduction. But it still faces specific challenges while implementing the legacy systems. Setting up the initial blockchain infrastructure is expensive. Smallfinancial companies or banks would not prefer investing in something that does not hold a promising future. As we discussed, like scalability, many other factors contribute to high maintenance cost. With the increase in popularity of blockchain, validation process has become more expensive due to complication and increasing of mining resources. This has started to cause problem as the transactions waiting for validation need to wait for long time tofinish validation unless a higher processing fee is paid for quick validation.

7. Conclusions

This chapter shares the systematic literature review which showcases thesudden hype in the blockchain-related searches and thus foresees the future ofblockchain and its applications in various sectors. An overview on variousdimensions like types, taxonomy, features of blockchain, the exciting block-chain applications, and major challenges has been presented in detail.Blockchain is a revolutionary idea which brings the transparency amongdifferent users and has become very popular in no time. Blockchain technol-ogies and its applications are constantly evolving with time and its inventionculminates many people's interest. In almost no time, others realized that thistechnology might be applied for several other things conjointly, like storing and sharing the logs of patients in medical sectors, generating a digital registrar or collecting taxes infinancial sectors, etc. Blockchain's ability to support different business application makes blockchain one of the revolu-tionary technologies which would bring change in society, economics, busi-ness, and technology.

References

Aste, T., Tasca, P., & Di Matteo, T. (2017). Blockchain technologies: The foreseeable impact on society and industry.*Computer, 50*(9), 18e28. https://doi.org/10.1109/MC.2017.3571064.

Back, A. (2002). Hashcash- A Denial of Service Counter-Measure.*Technical report*. Submitted for publication.

Becker, J., Breuker, D., Heide, T., Holler, J., Rauer, H. P., & Böhme, R. (2013). Can we afford integrity by proof-of-work? Scenarios inspired by the bitcoin currency. In*The economics of information security and privacy*(pp. 135e156). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-39498-0_7.

Casado-Vara, R., Prieto, J., De La Prieta, F., & Corchado, J. M. (2018a). Blockchain framework for IoT data quality via edge computing. In*BlockSys 2018 - proceedings of the 1st blockchain-enabled networked sensor systems, part of SenSys 2018*(pp. 19e24). Association for Computing Machinery, Inc. https://doi.org/10.1145/3282278.3282282.

Chakraborty, S., Aich, S., & Kim, H. (2019). A Secure Healthcare System Design Framework using Blockchain Technology.*21st International Conference on Advanced Communication Technology (ICACT), PyeongChang Kwangwoon_Do, Korea (South)*, 260e264. https://doi.org/10.23919/ICACT.2019.8701983.

Chaum, D. L. (1981). Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM, 24*(2), 84e90. https://doi.org/10.1145/358549.358563.

Chaum, D. (1985). Security without identification: Transaction systems to make big brother obsolete.*Communications of the ACM, 28*(10), 1030e1044. https://doi.org/10.1145/4372.4373.

Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., et al. (2016). On scaling decentralized blockchains (A position paper). In*Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics)*(Vol. 9604, pp. 106e125). Springer Verlag. https://doi.org/10.1007/978-3-662-53357-4_8.

Dabbagh, M., Sookhak, M., & Safa, N. S. (2019). The evolution of blockchain: A bibliometric study.*IEEE Access, 7*, 19212e19221. https://doi.org/10.1109/ACCESS.2019.2895646.

Danezis, G., & Diaz, C. (2008).*Survey of anonymous communication channels*.

Dwyer, G. P. (2015). The economics of Bitcoin and similar private digital currencies.*Journal of Financial Stability*, 81e91. https://doi.org/10.1016/j.jfs.2014.11.006.

Eyal, I., & Sirer, E. G. (2014).*Financial Cryptography and Data Security*. In Christin, N., & Safavi-Naini, R. (Eds.),*Majority Is Not Enough: Bitcoin Mining Is Vulnerable*(pp. 436e454). Springer, Berlin Heidelberg.

Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaria, V. (2018). To blockchain or not to blockchain: That is the question.*IT Professional, 20*(2), 62e74. https://doi.org/10.1109/MITP.2018.021921652.

Greenberg, A. (2012).*This machine kills secrets: How wikiLeakers, cypherpunks, and hacktivists aim to free the world's information*(Vol. 0525953205). Dutton Adult.

Hawlitschek, Florian, Benedikt, Notheisen, & Timm, Teubner (2018). The limits of trust-free systems: A literature review on block-chain technology and trust in the sharing economy. *Electronic Commerce Research and Applications, 29*, 50e63. Submitted for publication.

Hayden, C., & Choi, Y. (2019). Blockchain and Bitcoin: Concept, Functionality, and Security. *International Journal of Cyber Research and Education*, 27e37. Submitted for publication.

Henry, R., Herzberg, A., & Kate, A. (2018). Blockchain access privacy: Challenges and directions. *IEEE Security and Privacy, 16*(4), 38e45. https://doi.org/10.1109/MSP.2018.3111245.

https://ico.conda.online/the-crypto-guide-for-beginners-%E2%80%93-what-is-blockchain/. (Accessed 9 April 2021).
https://jgateplus.com. (Accessed 10 April 2021).
https://nptel.ac.in/courses/106105184/3/lec3.pdf. (Accessed 6 April 2021).
https://spectrum.ieee.org/computing/software/bitcoin-the-cryptoanarchists-answer-to-cash. (Accessed 10 April 2021).
https://steemit.com/blockchain/@thesumitbanik/how-does-a-blockchain-work-simply-explained. (Accessed 11 April 2021).
https://trends.google.com/. (Accessed 10 April 2021).
https://www2.deloitte.com/content/dam/Deloitte/in/Documents/strategy/in-strategy-innovation-blockchain-revolutionary-change-noexp.pdf. (Accessed 10 April 2021).
https://www.activism.net/cypherpunk/manifesto.html. (Accessed 7 April 2021).
https://www.chaum.com/ecash/articles/1996/05-07-96%20-%20DigiCash_s%20Ecash%20to%20be%20Issued%20by%20Deutsche%20Bank.pdf. (Accessed 7 April 2021).
https://www.eublockchainforum.eu/sites/default/files/reports/report_security_v1.0.pdf. (Accessed 10 April 2021).
https://www.gartner.com. (Accessed 10 April 2021).
https://www.ibm.com/blogs/blockchain/2018/02/top-five-blockchain-benefits-transformingyour-industry/. (Accessed 8 April 2021).
https://www.lesswrong.com/posts/YdfpDyRpNyypivgdu/aalwa-ask-any-lesswronger-anything. (Accessed 10 April 2021).
https://www.nytimes.com/2015/05/17/business/decoding-the-enigma-of-satoshi-nakamoto-and-the-birth-of-bitcoin.html. (Accessed 10 April 2021).
https://www.sciencedirect.com. (Accessed 10 April 2021).
IEEE. (n.d). ieeexplore.ieee.org.
Kang, S., Cho, K., & Park, K. (2019). On the effectiveness of multi-token economies. In*ICBC 2019 - IEEE international conference on blockchain and cryptocurrency*(pp. 180e184). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/BLOC.2019.8751242.
Latifi, S., Zhang, Y., & Cheng, L. C. (2019). Blockchain-based real estate market: One method for applying blockchain technology in commercial real estate market. In*Proceedings - 2019 2nd IEEE international conference on blockchain, blockchain 2019*(pp. 528e535). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/Blockchain.2019.00002.
Lavanya, B. (2018).*Blockchain technology beyond bitcoin: An overview*.
Lee, A. R., Kim, M. G., & Kim, I. K. (2019). SHAREChain: Healthcare data sharing framework using blockchain-registry and FHIR. In*Proceedings - 2019 IEEE international conference on bioinformatics and biomedicine, BIBM 2019*(pp. 1087e1090). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/BIBM47256.2019.8983415.
Lemieux, V. L. (2016). University of British columbia. In*Blockchain technology for record keeping: Help or hype?*(Vol. 1).
Mettler, M. (2016). Blockchain technology in healthcare: The revolution starts here. In*2016 IEEE 18th international conference on e-health networking, applications and services, healthcom 2016*. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/HealthCom.2016.7749510.
Montes, J. M., Ramirez, C. E., Gutierrez, M. C., & Larios, V. M. (2019). Smart contracts for supply chain applicable to smart cities daily operations. In*5th IEEE international smart cities conference, ISC2 2019*(pp. 565e570). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ISC246665.2019.9071650.

Nakamoto, S. (2008).*Bitcoin: A peer-to-peer electronic cash system*.

Nguyen, T. Q., Das, A. K., & Tran, L. T. (2019). NEO smart contract for drought-based insurance. In *2019 IEEE Canadian conference of electrical and computer engineering, CCECE 2019*. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/CCECE.2019.8861573.

O'Leary, M. (2015).*The mysterious disappearance of Satoshi Nakamoto, founder & creator of bitcoin*. The Huffington Post.

Peck, M. (2012). Bitcoin: The cryptoanarchists' answer to cash.*IEEE Spectrum, 49*(6).

Peters, G. W., & Panayi, E. (2016). Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. *New Economic Windows*, 239e278. https://doi.org/10.1007/978-3-319-42448-4_13.

Pitta, J. (1999).*Requiem for a bright idea*. Forbes. N.

Reyna, A., Mart´ın, C., Chen, J., Soler, E., & D´ıaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities.*Future Generation Computer Systems, 88*, 173e190. https://doi.org/10.1016/j.future.2018.05.046.

Ridley, M. (2017). The Bitcoin revolution is only just beginning. The Times. Retrieved 23 December 2017. In*The legal scholar and computer scientist Nick Szabo*.

Saichua, P., Khunthi, S., & Chomsiri, T. (2019). Design of blockchain lottery for Thai government. In*Ecti DAMT-NCON 2019 - 4th international conference on digital arts, media and technology and 2nd ECTI northern section conference on electrical, electronics, computer and telecommunications engineering*(pp. 9e12). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ECTI-NCON.2019.8692241.

Sara, S., Mahtab, K., & Joseph, S. (2018). Blockchain technology: A panacea or pariah for resources conservation and recycling?*Resources, Conservation and Recycling*, 80e81. https://doi.org/10.1016/j.resconrec.2017.11.020.

Szabo, N. (1998).*Secure property titles with owner authority*.

Tschorsch, F., & Scheuermann, B. (2015).*Bitcoin and beyond: A technical survey of decentralized digital currencies*.

Utilization of Blockchain Technology to Overthrow the Challenges in Healthcare Industry, Hemalatha, K., Hema, K., & Deepika, V. (2015).*Advances in intelligent systems and computing 1054, emerging research in data engineering systems and computer communications proceedings of CCODE*(pp. 199e208).

Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey.*International Journal of Web and Grid Services, 14*(4), 352e375. https://doi.org/10.1504/IJWGS.2018.095647.

Blockchain for Smart Cities

Blockchain and the Smart City: Infrastructure and Implementation uses case studies from around the world to examine blockchain deployment in diverse smart city applications, focusing on different tools, platforms, and techniques. The book begins by examining the fundamental theories and concepts of blockchain, looking at key smart cities' domains such as banking, insurance, healthcare, and supply chain management.

Using case studies for each domain, the book explores payment mechanisms, fog/edge computing, green computing, and algorithms and consensus mechanisms for the implementation of smart cities. This book illustrates tools such as Hyperledger, Etherium, Corda, IBM Blockchain, and Hydrachain, as well as policies and regulatory standards, applications, solutions, and methodologies.

While exploring future blockchain ecosystems for smart and sustainable city life, the book concludes with the research challenges and opportunities academics, researchers, and companies in implementing blockchain applications, representing a valuable resource for smart city academic researchers, scholars, and graduate students, as well as city planners and policymakers.

Key features:

- Independently organized chapters for greater readability, adaptability, and flexibility
- Examines numerous issues from multiple perspectives and academic and industry experts
- Explores both advances and challenges of cutting-edge technologies
- Coverage of security, trust, and privacy issues in smart cities

Edited by:

Saravanan Krishnan
Assistant Professor, Department of Computer Science and Engineering, Anna University Regional Campus, Tirunelveli, India

Valentina Emilia Balas
Full Professor, Department of Automatics and Applied Software, Faculty of Engineering, "Aurel Vlaicu" University of Arad, Arad, Romania

E. Golden Julie
Senior Assistant Professor, Department of CSE, Regional campus, Anna University, Tirunelveli, India

Y. Harold Robinson
Post Doctoral Fellow, School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, India

Raghvendra Kumar
Associate Professor, Department of Computer Science and Engineering, GIET University, Gunupur, India

ISBN 978-0-12-824446-3

9 780128 244463

ELSEVIER elsevier.com/books-and-journals