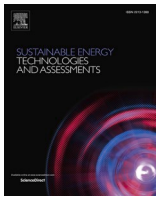
Sustainable Energy Technologies and Assessments 52 (2022) 102039

Contents lists available at ScienceDirect

Sustainable Energy Technologies and Assessments

journal homepage: www.elsevier.com/locate/seta



A comprehensive survey on blockchain technology

Arun Sekar Rajasekaran [a,*], Maria Azees [a], Fadi Al-Turjman [b]

[a] Department of Electronics and Communication Engineering, GMR Institute of Technology, Rajam 532127, Andhrapradesh, India
[b] Artificial Intelligence Engineering Department, Research Center for AI and IoT, AI and Robotics Institute, Near East University, Mersin 10, Turkey

ARTICLE INFO

Keywords:
Blockchain
Decentralization
Distributed ledger
Immutability
Peer to peer (P2P) network

ABSTRACT

In recent years of development, the interest in Blockchain technology and the essentials of its application have made it popular. The efficiency and availability of this technology have made it a widely accepted technology. Blockchain technology has completely changed the present-day concept of centralization. Different methodologies are used for the purpose of interfacing and monitoring the transactions in blockchain technology. Decentralization, immutability, transparency, and peer to-peer communication help to address the current trends effectively. This paper presents a comprehensive survey of blockchain technology, describing its features, classification, blockchain wallets, and applications.

Introduction

Blockchain is a unique technology that came into existence in the year 2009, and this new concept was first coined by Satoshi Nakamoto [1]. A blockchain consists of blocks with a growing list of records that are linked using cryptography to resist the alteration of the data. Each block in the blockchain possesses a cryptographic hash value of the previous block, a fresh timestamp, and transaction data. Because all blocks in the blockchain are decentralised and distributed in nature, any involved block in the blockchain cannot be modified retroactively without affecting all subsequent blocks. Blockchain technology contains its own key features such as security, transparency, decentralization, immutability, and programmability. Moreover, it doesn't depend on any centralized trusted authorities to process data transactions. In addition, there is no need for any intermediate third party to verify and validate the data transactions. This phenomenon allows users to easily verify and review the transactions independently and inexpensively. Once the data transactions are completed in a successful manner, the valid transactions are hashed and encoded into a Merkle tree [2–4] in the block. The new blocks are added in the block chain onto the old blocks in such a way that they are extended as new blocks rather than being overwritten onto old blocks to significantly reduce the probability of an entry becoming outdated.

For the implementation of a distributed ledger, one of the probable technologies is Blockchain [5–7]. During the implementation of a distributed ledger, the records are grouped together to form the blocks. The data present in the blocks is cryptographically secured to make it tamper resistant. To achieve this level of security, the contents of the blocks are hash valued and added to the header of the block. Finally, the blocks are chained together in such a way that the cryptographically secured hash value of the previous block is linked with the current block. Thus, each block not only depends on its own data content but also on the previous block's hash value. The time taken for block creation and block size are important factors related to scalability. The block creation time should be decreased to increase the performance of the network, but there may be a probability of a security threat. The number of transactions performed is directly related to block size, and the larger the block size, the more transactions, but there is an increase in security threat. These two parameters should not be modified blindly, which may lead to several security threats. Care should be taken while modifying these parameters. Sharding is a technique related to scaling in which blockchains are parallelized. This technique is mostly used to execute a large number of transactions. The information in the transactions is partitioned into a small number of pieces called "shards." Attention should be given while partitioning the information. If careful attention is not provided, it may lead to several possible attacks.

There are several recent developments within blockchain, such as stable coins, DeFi, etc., A cryptocurrency called Stablecoin is equivalent to a commodity like gold or a currency like the dollar. Moreover, they have a more stable nature. Since they are stable, their value does not fluctuate like other cryptocurrencies. They are mostly used in crypto exchanges. Defi refers to decentralised finance in which stablecoins are

* Corresponding author.
E-mail addresses: arunsekar.r@gmrit.edu.in, rarunsekar007@gmail.com (A.S. Rajasekaran), azeesmm@gmail.com (M. Azees), fadi.alturjman@neu.edu.tr (F. Al-Turjman).

https://doi.org/10.1016/j.seta.2022.102039
Received 13 August 2021; Received in revised form 7 December 2021; Accepted 25 January 2022
Available online 9 February 2022

used for several applications. The stablecoin owners give their tokens and benefit in return.

Blockchain technology provides number of applications [8–13] ranging from healthcare, finance, distribution, etc. There is no centralized authority during peer to peer transactions between two parties. Security [14] and trust are the two important criteria in blockchain technology. But all these trustfulness and security services [15] are fulfilled using cryptography. Blockchain technology-enabled trust among the unknown peers by creating the communication between the peer to peer [16] in the decentralized network. In blockchain technology security is ensured by using public and private keys. Public key is the common address that everyone in the network knows, similar to the email address of the user. The private key is the unique address, only the user has the knowledge similar to the user's password for the email address.

Verification and validation are performed by using software programmes in the blockchain. Several new innovative technologies are added to this blockchain as the computational elements to make the transactions simpler and easier. These transactions are recorded in the distributed ledger [17] where transparency and immutability are maintained. Even though blockchain plays a key role in current digital technology, there are some constraints associated with blockchain technology. The number of transactions performed in the network is limited due to the small size of the blocks. The time taken for the creation of the block size is more, which in turn reduces the throughput of the network.

Full node and lightweight node are the two important concepts in blockchain technology. The important functionality in the blockchain is carried out by full node. The entire history of the blockchain is stored in the full node. Moreover, during transaction verification and decision making are performed by full node. On the other hand lightweight node is a payment verification node for simple transaction process. In addition they are more feasible and consumes minimum resources.

In blockchain technology, cryptocurrencies [18] take a vital role. Cryptocurrency is a virtual currency that is used as the medium of exchange between the end users. Cryptocurrency is similar to our real-world currency except that it does not have any centralized authority to control over it. Cryptocurrency includes the facilities like no transaction cost, 24/7 access of money, no limits on purchases and withdrawal, freedom for anyone to use, and faster international access. The well-known first cryptocurrency-Bitcoin has its origin from the Blockchain technology. There is no centralized system for this digital currency and the transaction takes place between the users in a bitcoin [19] network is done in a decentralized way with- out the involvement of any third party. Bitcoin verified transactions are recorded in the distributed ledger called as blockchain. The time taken for the network to create a new block in the blockchain is called as block time. The average block time for the bitcoin is around 10 min and the maximum extend to produce bitcoin is limited to 21 million. The new bitcoin will be generated, only when the miner has successfully accomplished the task of mining the block.

Ethereum network platform [20] is a decentralized open source cryptocurrency platform where more than 1900 cryptocurrencies are used. On this platform, a general scripting language is used, which will be helpful for developing many applications. To reward the Ethereum miners for successfully adding the new blocks to the Ethereum network platform, Ether, the second largest virtual cryptocurrency is designed and used in the capital market. The block time for Ether is around 13 s, and the Ethash algorithm is used for its proof of work.

The main contribution of this survey article is to deal with preliminary concepts of blockchain technology. Moreover, the various features, such as blockchain structure, miner decisions, types of forks, and applications of blockchain are described briefly. Eventually, the goal of this survey article is to provide an insight into the technical concepts and research developments in blockchain technology.

The paper is organised as follows: Section II gives a structural overview of blockchain technology. Section III explains the features of the blockchain. The classification of blockchain is explained in section IV. Section V describes the miner's decision to add the block. Forks are explained in Section VI. Section VII elucidates blockchain wallets. Applications of blockchain technology are described in section VIII. Section IX concludes this survey paper.

Blockchain Structural Overview

The transactional flow in the blockchain technology is detailed in Fig. 1.

A. Node

The core part of the blockchain architecture [21] is the node. The user or the highly configured computers are defined as a node, and they play a key role in the transactions involved in the blockchain. A copy of the entire blockchain ledger is maintained in each node.

B. Miners

The specific nodes with the capability of adding a new block to the blockchain are called miners [22]. The miners perform the processes of authentication, verification, and validation of both end users. Once the transaction is validated and authenticated by the miners, the amount is deducted from the sender's wallet and credited to the receiver's wallet.

C. Block

A block [23] is similar to a container that holds an aggregated set of transaction details. If any new record or transaction is initiated in the blockchain, it implies the building of a new block. The blocks can be added to the blockchain, only if they are successfully verified by the miners. A block has two major parts, namely the header and transaction details.

Block header

The block header contains the block version number, previous hash value, timestamp, merkle root hash value, difficulty target value, nonce and hash value of the block. The block version number is a 4-byte sequential number of the block. The previous hash is the 256-bit resultant hash value of all the transactions in the previous block, including the header in the blockchain. This will be helpful in linking two consecutive blocks. The time at which the block was created is mentioned in the time stamp, and its size is 4 bytes. A Merkle root hash is a 32-byte hash value of all the transactions structured in the Merkle or binary tree. The difficulty level of the proof of work for that particular block is mentioned in the difficult target value, and its size is 4 bytes. The nonce is a 32-bit random string of whole numbers that is varied to create a unique hash value for that particular block which satisfies the proof of work. This unique hash value is the hash value of the entire block, and the miners are supposed to find this value by trying out all the possible values of nonce. If there is any modification to the transaction by an attacker, then the unique hash value of that particular block is also changed. Moreover, this unique hash is also linked with the succeeding block's previous hash value. Once the miner successfully varied the nonce value and found the unique hash of the block, he will be rewarded, and the block will be added to the blockchain. Fig. 2 shows the linkage of two blocks based on block hash values.

Transaction details

Transaction details contain sender and receiver information and the amount to be transferred. It is considered the smallest building block in the block system that holds the information, records, etc., The Merkle root hash is calculated as shown in Fig. 3. The list of transactions is passed through the hashing algorithm and the hash values are obtained. Then the hashes of each transaction are paired and, once again, they are passed through another hashing algorithm until only one hash value is left. This will be the merkle root hash.

On the sender side, the transaction message is passed through the hash function [24,25] and the hash value is generated. This hash value is encrypted using the user's private key to form the signature. The

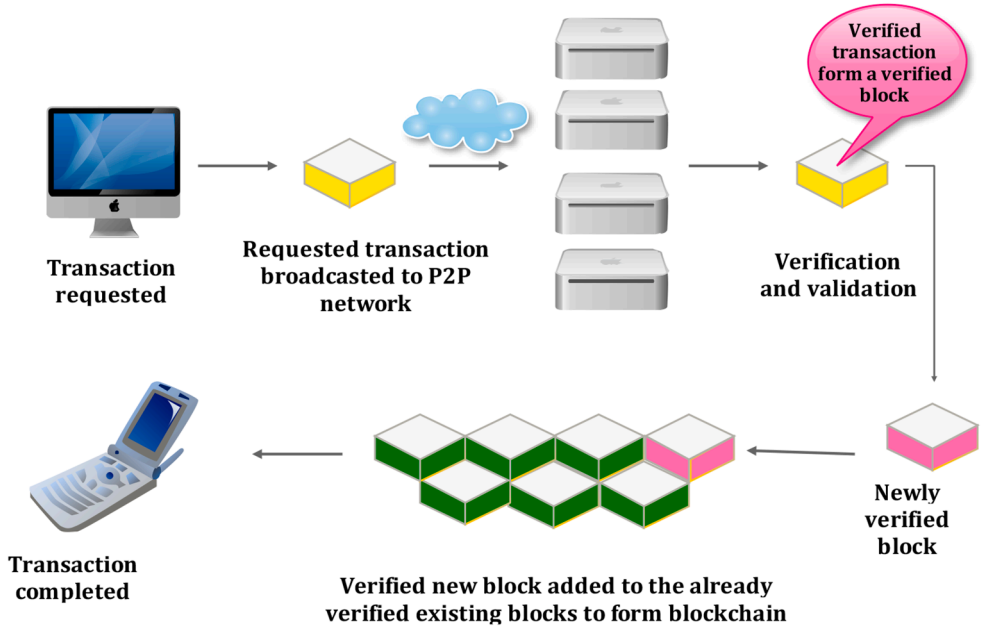


Fig. 1. Transaction Flow in Blockchain technology.

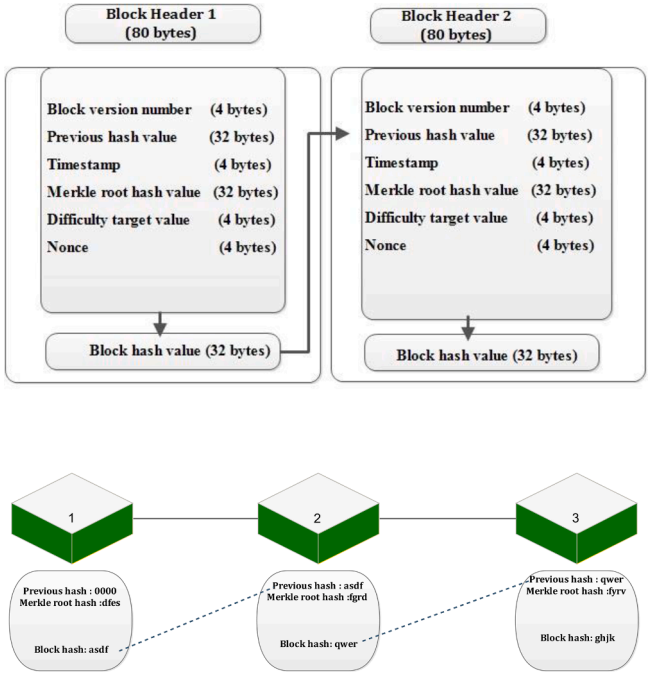


Fig. 2. Linkage of two Blocks based on block hash value.

transaction message is appended with the signature to form the digitally signed message, and it is broadcast worldwide. The entire flow at the sender side is shown in Fig. 4. During validation at the receiver's side, this digitally signed message is segregated into transaction message and signature. The transaction message is passed through the hash function to generate the hash. At the same time, the signature is decrypted using the public key to get another hash value. Both the hash values are compared to authenticate the user. If the hashes are equal, then the signature is valid. The flow at the receiver side is shown in Fig. 5.

Double spending is the concept in which the same digital money is used for two different transactions. In bitcoin technology, even though the same digital money is assured for two different users, only the

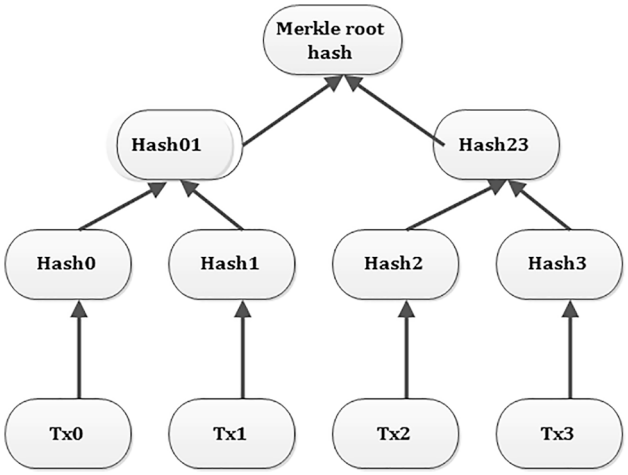


Fig. 3. Calculation of Merkle root hash.

verified transaction of the authorised entity is accepted.

D. Consensus protocol

A set of rules and regulations that are followed during the transactions in the blockchain technology is called as Consensus protocol [26]. As the blockchain technology follows the consensus algorithm, there is a level of trust in terms of updating or transferring data between the end-users. The trust between the end-users is preserved, as the data transmission takes place in an anonymous manner in the form of a blockchain address.

E. Mining

Mining [27] is the process of adding a block to the blockchain. The first person to find the nonce value that satisfies the proof of work will be rewarded and permitted to add his block to the blockchain. Currently, each miner is rewarded with 12.5 bitcoin for adding a new block to the blockchain. But the reward for the miners is reduced every four years. So, at the end of the next four years, the reward will be reduced by 6.25 bitcoins. Several strategies are involved to decide which miner wins in adding the block to the blockchain. Some popular methods are: proof of work, proof of stake, proof of space, proof of importance, trust measure,

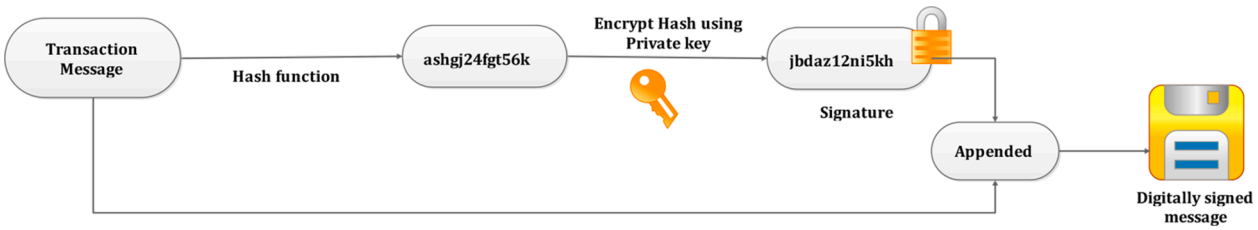


Fig. 4. Flow at the Sender side.

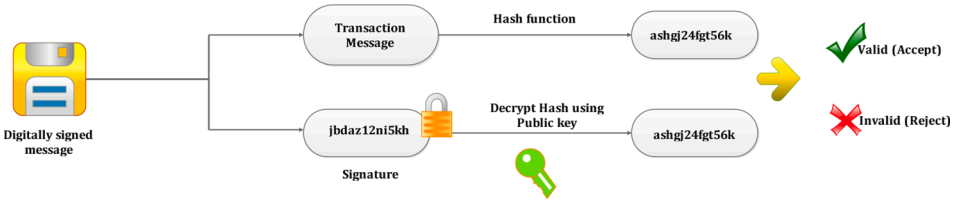


Fig. 5. Flow at the receiver side.

and minimum block hash. These approaches are described in the following section.

a) Proof of work

Miners are involved in the process of proof of work [28]. They are the people working in the blockchain network all over the world using highly efficient computers for performing computations. These competing miners around the world try to solve the mathematical puzzle. The miners who solve the puzzle first will be rewarded and are allowed to add the block to the blockchain. The miners are awarded, since they are investing in the resources. A mathematical puzzle is the hash value that satisfies predefined conditions. In-order to find that hash value, the miners use nonce field in the header of the block. To find the output that falls within the difficulty target value, the miners keep on changing the nonce value to obtain the hash. Immediately after finding the nonce, the miner broadcast that he has found the nonce, that satisfies the target requirement. Once it is revealed, then all the other miners validate and verify nonce and add the corresponding block to the existing block forming the blockchain. The proof of work algorithm is very hard to generate the nonce and get the hash value. But it is very easy to verify the transaction by the other miners.

b) Proof of stake

In the proof of stake [29], there is no need for the miners to solve the mathematical puzzle, which is computationally complicated. Moreover, miners are selected pseudo randomly. Moreover, based on their wealth or stake, the miners are deployed. In other words, the miner node that has the most money will be selected to mine the block. The old version of the Proof of Stake does not have any rewards, but the extended versions have some rewards for the miners who successfully mine the block and add it to the blockchain. The main drawback is that the wealthier mining node always gets the opportunity to mine the block, and this is similar to a single account taking control over all the nodes, leading to uneven distribution. Another method of selecting the mining node is based on the coin age-based approach. In this approach, the mining node that has not created any blocks for the past month is given preference to mine the block.

c) Proof of space or proof of capacity

In the proof of space or proof of capacity approach [30], the space required for storing the complex mathematical puzzle is large. This approach is similar to that of proof of work, except that high storage capacity is required. The miners use the empty space on their hard drive to store the different possibilities of the hash value. So, the larger the hard drive space, the more possible values of the hash are stored, which in-turn increases the probability for the miner to match the required hash from the stored list and to win the reward. Even though many practical solutions have evolved regarding the proof of space, it has proved to be a great challenge when compared to the proof of work.

d) Proof of importance

In Proof of Importance [31], the highest priority is given to the node based on the transaction details of that mining node. If the transaction amount (strength) and the balance of the node are higher, then the node will be called the significant node and will be given priority. In this approach, the priority is assigned to the significant node based on the hash calculation. Once the priority is assigned, the corresponding mining node is allowed to mine the new block.

e) Trust measures

In the trust measure concept [32,33], the mining nodes are selected based on the trust level. The node that has the highest trust is given the highest priority and allowed to mine the block. The measure of trust is calculated based on the mining node's behaviour. If the behaviour of the node satisfies the trustworthiness of the network and follows certain protocols, then the corresponding node will be selected to mine the block. Moreover, trustworthiness depends on the history of the mining node.

f) Minimum block hash

In this minimum block hash approach [34], the mining node is selected randomly based on the minimum hash value that is generated in the network. The wealth, stake, or resources of the mining node is not considered. The selection procedure randomly takes place, and there is a minimum or zero probability of selecting the same node. Although energy is saved considerably, this approach is not widely practiced.

Features of blockchain

There are six main features of blockchain technology that make it popular. The six important features of blockchain are described as follows.

g) Decentralization

Blockchain technology uses the concept of decentralization. Decentralisation is the process in which there will be no centralised authority to plan or make decisions for an organisation to perform transactions. A decentralised system [35,36] does not store the information in a single node and everyone in the network can access the information. Moreover, if we want to do a transaction with another entity, there is no need for a third party (i.e., a trusted authority). We can directly interact with the corresponding end user and do our transactions, but we are solely responsible for the transaction. The peers can make direct transactions with the end users irrespective of their location without revealing their real identity. Since no central authority is available, there is no central

point of failure. Moreover, the history of the entire transaction is known by all the participants in the network. Before the existence of blockchain technology, we were mostly addicted to centralised services. However, in the centralised system, it is very simple and easy. There is a centralised trusted authority that is responsible for all our transactions. Since they are centralized, it is easy for hackers to corrupt the data that is available on a single node. If there are any errors in the centralised TA, no one can access or process data in the network. Moreover, only the registered participants have the privilege of accessing the history of their transactions. Thus, to overcome these drawbacks, the concept of decentralisation is employed in blockchain technology.

h) Transparency

Transparency [37] and privacy are the two different concepts used in the blockchain technology. Some interpret the blockchain as transparent, but some represent it as privacy. But when we see the transaction history in the blockchain technology, only the dummy identity of the user is represented instead of their real identity. So, the real identity of the user is secured even though the transaction is performed using a public address. But in the view of cryptocurrency, if the public address is known by an intruder, then he/she can retrieve the original number of transactions involved between the end users. So, in order to avoid the intruder's actions, cryptocurrencies are integrated with blockchain technology to maintain privacy.

i) Immutability

Once a transaction has been initiated and data has been inserted into the distributed ledger, it cannot be edited or deleted [38].These additions made to the blockchain are permanent and immutable. Once registered, they cannot be modified and are available for validation and verification. If there is any modification of data in any one of the blocks in the blockchain, then this modification is reflected on other ledgers in the network. In addition, the particular modified node is identified and rectification takes place.

j) Peer to peer network

Peer-to-peer (P2P) networks [39,40] are interconnected collections of all nodes in which the entire load is distributed among all participants known as peers. However, the peers are distributed and decentralized. The main benefit of using the P2P network is file sharing. The download mainly depends on the strength of the server. When we download any file based on the centralised server, then it depends on censorship. But the censorship can be completely avoided if we prefer a decentralised P2P network. In the decentralised P2P network, if one of the peers fails to operate, the other peers in the network assume the role and perform the required function. Fig. 6a and Fig. 6b represent the centralised and decentralised peer-to-peer networks, respectively.

k) Distributed ledger

The database of each transaction is broadcast to all the nodes in the P2P network, and the same identical copy of the database is maintained in the ledgers of all the nodes. If any data is updated, then all the distributed ledgers are updated uniformly. For instance, let us consider a situation where data is shared uniformly among three users. If there is only one document and one of them modifies the data in it, it will be difficult for the others to be notified of the changes. However, if each of them has a copy of the document, even if someone changes the data, the others will find the change within the data. Blockchain works on this basic principle [41]. Since the data inside the block is accessible to everyone; any modification can be easily retractable. Therefore, being part of the network, the entire history of the transaction is accessible by all the nodes.

l) Irreversibility

Irreversibility is the process where, once the task is executed, it cannot be retraced. In blockchain, the variable length of data/information, or transactions is passed through the hash function to get a fixed, encrypted output. Since the hash function is deterministic, it will produce the same output for the same input. Even a small change in the information may cause a drastic change in the hash output. Moreover, the hash function is a one-way function, and so it is difficult to retrace the original data from the hash output.

Classification of blockchain

A blockchain may be classified into two categories based on access controls, such as permission-less and permissioned blockchain. The pictorial representation of the classification of blockchain is shown in Fig. 7.

m) Permission-less blockchain

In a permission-less blockchain [42], anyone can access the blockchain network. The public blockchain is the best example of this type of blockchain.

1. Public blockchain

In public blockchain [43], anyone can access the network. The participants can enter and exit the network at any time. It is open source, and the transaction blocks are publicly visible, though the transactions take place in an anonymous form. Furthermore, everyone has a copy of the blockchain, so no one can alter the data in the blockchain. Even though, if there is a change in the blockchain, the other nodes in the blockchain can come to know that a change has happened in the node.

n) Permissioned blockchain

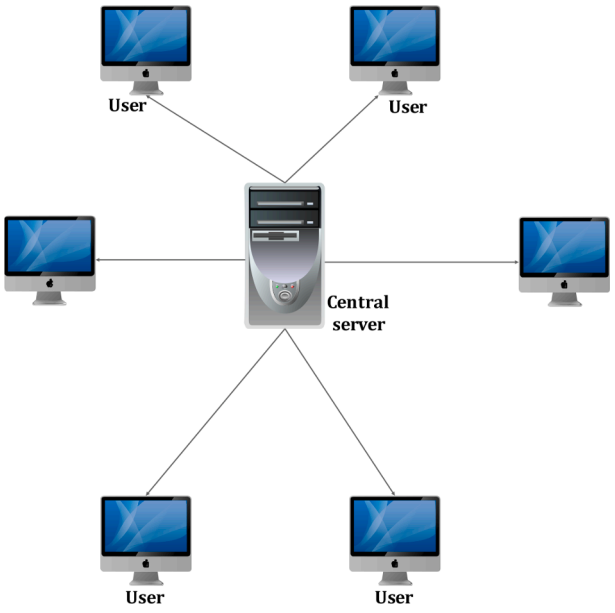


Fig. 6a. Centralised network.

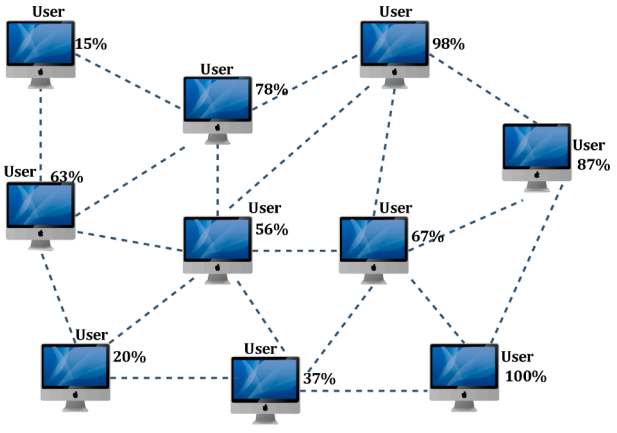


Fig. 6b. Decentralised P2P network.

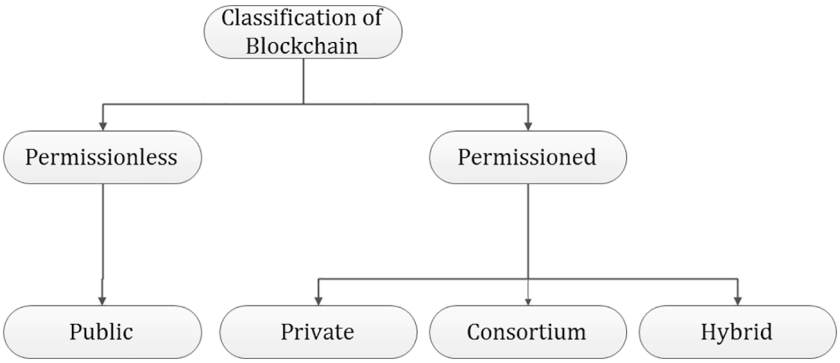


Fig. 7. Classification of blockchain.

In a permissioned blockchain [44], only the nodes that have the permission provided by the network can access the blockchain network. Only certain identifiable nodes are allowed to perform certain tasks. They provide an additional blockchain security system. The identity of each node in the blockchain network is maintained. Anyone can join the permission blockchain once their identity and roles are defined. Such nodes are called "permissioned nodes." Furthermore, only permissioned nodes are permitted to perform blockchain transactions. It is classified into private, consortium and hybrid blockchain.

1. Private blockchain

Private blockchain [45] is applicable to smaller organizations. In a private blockchain, only a selected number of nodes can access the blockchain. These restrictions help to perform operations like block creation in a quicker manner. Furthermore, mining the block takes less than a minute. In a private blockchain, all the nodes do not have access to see the transactions. Only those who have access to the particular private blockchain network can see the transactions. So, a completely secure and trusting transaction takes place. Moreover, it is easy to identify the nodes involved in the transactions. If any mishap happens, the identity of the particular node can be traced. Only a few nodes are authorised to perform the transactions, so even if the network grows, it doesn't influence its speed and efficiency. But, in the private blockchain, there will be a single organisation controlling the network, and it will be like a centralised unit, which is the main disadvantage.

1. Consortium blockchain or federated blockchain

In consortium blockchain [46,47], there is no single organisation and the blockchain platform will be managed by more than one organization. Moreover, both public and private blockchain features are incorporated. Some important aspects of the organisations are made private, while others remain public. In order to access the ledger, the node should be a member of any one of the organizations, so it is called a permissioned blockchain. Since multiple organisations take the decision on the blockchain platform to validate the transaction, it is called a "decentralised based consortium blockchain."

2. Hybrid blockchain

A hybrid blockchain [48] is a combination of both private and public blockchains. It is similar to consortium blockchain, but the hybrid blockchain incorporates the best features of both public and private blockchain characteristics. Here, the consensus protocol can be changed according to our requirements. It offers good scalability since only a few nodes are authorised to validate the transaction.

Miners decision

The miners should make an important decision regarding which transactions should be added to the block. Before the transactions are added to the blocks in the blockchain, they are temporarily collected in a vessel called the memory pool [49]. The miners select the transactions from this pool, and they place them in a temporary block called the "candidate block." Then, the miner tries to be the first person to find the nonce value that satisfies the hash requirement. Once he becomes successful, he adds his candidate block to the blockchain.

Suppose someone in the blockchain wants to spread some wrong information. The Byzantine fault tolerance algorithm plays an important role in preventing the wrong spread. This tolerance algorithm will be helpful for preserving the right consensus of the network.

o) Byzantine fault tolerance-Blockchain

Byzantine fault tolerance problems [50,51] can be encountered in the blockchain. If an intruder tries to add an invalid transaction into the blockchain, he/she sends this false information to all the nodes in the blockchain. This would affect the reliability of the blockchain. But blockchain can achieve Byzantine fault tolerance with the help of proof of work. This is effective since we are adding the block to the blockchain using a complicated process involving the hashing algorithm. This process is very hard to decrypt and highly reliable, and its value depends on the previously existing hash value of the blockchain. This would cause the intruder to take a long time to produce enough proof of work to break the blockchain.

p) Simultaneously adding the blocks

Let us consider that two miners add a block to the blockchain at the same time. It is difficult to conclude which block will be added to the blockchain. However, in an ideal situation, the miner who initially finds the required hash value will add the block to the blockchain. Whereas in some complex circumstances, if both the miners find the required hash value that is less than the target predetermined value at the same time, then both the values are accepted.

The crucial situation is whether to connect Miner 1 block or Miner 2 block to the blockchain. In this scenario, 50% of the network accepts the miner's 1 block and the remaining 50% of the network accepts the miner's 2 blocks. Half of the network continues to function, believing miner's 1 block to be the correct block, while the other half continues to function, believing miner's 2 blocks to be the correct block. But this is practically impossible since only one blockchain is allowed to operate within the network. Two blockchains are not allowed to run simultaneously on the network. Suppose that if miner 3 adds his new block to the miner 1 block, then the miner 2 block is completely discarded and the block of miner 1 is accepted by the entire network. Fig. 8 shows the schematic of two miners adding the block at the same time to the blockchain. Fig. 9 shows the flow of the addition of a block by miner 3 to the miner's 1 block and the discarding of miner 2 block. Therefore, only one blockchain runs in the network, and this situation is called an accidental fork.

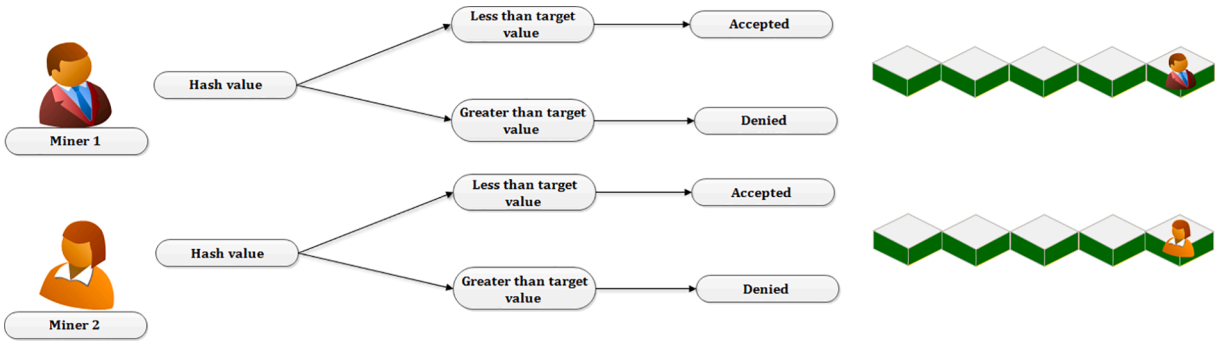


Fig. 8. Two miners adding the block at the same time to the blockchain.

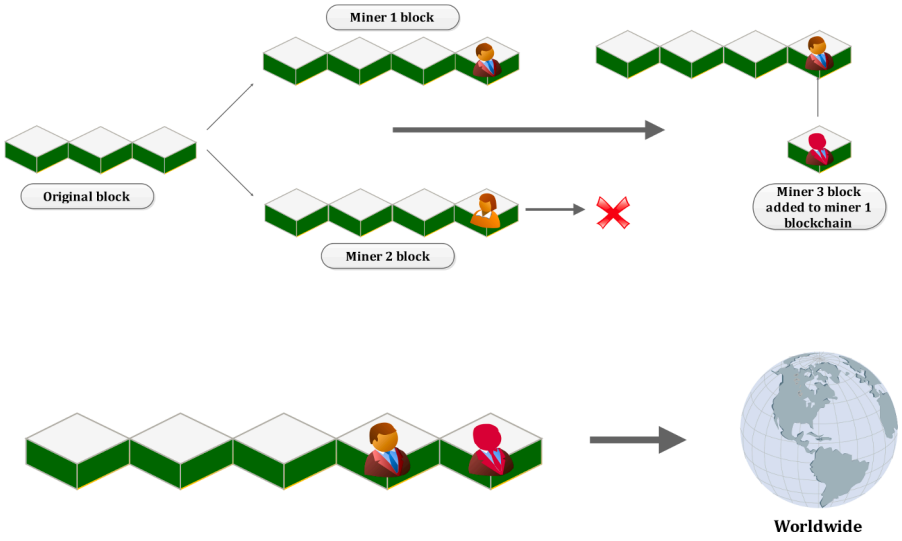


Fig. 9. Schematic of Miner 3 block added to miner 1 block.

Fork

The concept of a fork [52] exists when a blockchain diverges into two parts or when there is no definite conclusion/agreement regarding the network transaction details, or the new rules to validate the transaction. It may be classified into two types, as described below.

q) Soft fork

A new block is added to the blockchain due to the change in the software protocol following a new set of rules. This is called a "soft fork." This change in the new rules should be accepted by the majority of network users.A soft fork is mainly implemented to tighten the rules and to add some unique special features without affecting the framework.

r) Hard fork

A hard fork is formed by modifying some of the basic functions of the software protocol, which forces the development of a new blockchain. Here, the blockchain that is not updated remains in the network, and the blockchain that is upgraded with the new software protocol follows the new path. Moreover, both these blockchains are considered valid and legitimate. But in the soft fork, the blockchain that is not updated will be discarded. The best example of a hard fork is Bitcoin Cash.

Blockchain wallet

Blockchain wallet [53] is a cryptocurrency wallet that allows users to manage cryptocurrencies like bitcoin, Ethereum, etc. Blockchain wallet helps in the exchange of funds, securing transactions between different parties, and maintaining privacy. They can be easily accessible from the web or mobile devices.

A Blockchain wallet is very similar to the process of sending/receiving money through pay-pal or any other gateway, but instead it uses cryptocurrency.

The transactions were slower before the existence of the blockchain wallet. The transactions must pass through some trusted third party called banks, which may experience a central point of failure. It is difficult to track all the accounts and balances. There may be a possibility of data getting manipulated, modified, or corrupted.

s) Working of blockchain wallet

Private and public keys are used in the blockchain wallet. Whenever a blockchain wallet is created, private keys and public keys are also created and are associated with the blockchain wallet. The public key is known to everyone in the network and is shared with everyone to receive the funds. Whereas the private key is a top-secret key that is used to spend the funds and is known by the authorised users. For instance, if we want to transfer money to a friend, this transfer process is done through a blockchain wallet using cryptocurrencies.

A Blockchain wallet works similar to our email address. Even if anyone knows our email address, they will not be able to send the email through our email address unless the email password is revealed to them. The blockchain wallet follows a similar pattern: no one will be able to send crypto coins (e-mails) through our public key (e-mail address) until our private key (e-mail password) is revealed. But, if someone gets access to our private key, there will be a high possibility of our account being hacked and all our cryptocurrencies deposited in our account will be lost. UTXO refers to the unspent output transaction amount received by the bitcoin user, and this can be used in the near future. In the bitcoin wallet, the received output amount is stored as a

separate entity. Based on the requirements of the user, the unspent amount is unlocked and can be used.

t) Features of blockchain wallet

Certain important features of the Blockchain wallet are as follows: They are easy to use, high security, instant transactions throughout the world with a low transaction fee. Moreover, the blockchain wallet helps with transactions with multiple cryptocurrencies. So, payment can be done using different cryptocurrencies, which helps with easy currency conversion.

u) Types of blockchain wallet

A Blockchain wallet is a software programme used for transactions using bitcoins. Moreover, the wallet contains the private key used to access the bitcoin address to carry out the transactions. The blockchain wallet is classified into two major types. The different types of blockchain wallets are schematically represented in Fig. 10.

A) Hot wallet

A hot wallet, or software wallet [54], is an application downloaded to a device either on a desktop or mobile and accessed online. It is similar to our regular wallet and is user-friendly. Hot wallets are online wallets through which cryptocurrencies can be transferred easily. Moreover, private keys are stored in the cloud for faster transfer. It can be easily accessed through desktop/mobile since it is available online (24*7), but it has the risk of unrecoverable theft when hacked. Hot wallets are vulnerable to government regulations. Some of the hot wallets are mobile wallets, online/web wallets, and desktop wallets, which are described below.

- *Desktop wallet*

The desktop wallet is a hot wallet mounted on the desktop where private keys are stored on cold servers. Since the private keys of the wallet are located on the desktop, they can be unplugged from the internet and the transaction can be carried out offline. Eventually, they can be brought online after the transaction is completed. Moreover, the cold server (desktop server) is used as a backup server when the main server is lost. These wallets can be downloaded on any computer, but they can be accessed only from the installed system. So, protection and privacy should be maintained while using a desktop wallet. In addition, these wallets are cost-efficient.

- *Online wallet*

Online or web wallets are hot wallets running on the cloud. Users can access these wallets via a web browser on any computer, such as a tablet, laptop, etc. The private keys are stored online and are managed by the third party. So, we must depend on a third-party service to get the private key.

- *Mobile wallet*

Mobile wallets are similar to online wallets, but are designed for mobile phone use only. These wallets are user-friendly, and they provide an easy to use graphical user interface for transactions.

B) Cold wallet

A cold wallet [55] is similar to a vault, where cryptocurrencies are stored with a high level of security. Cold wallets are digital offline wallets where the transactions are signed offline and later disclosed online. So, they are not maintained in the clouds on the internet. Moreover, private keys are stored on separate hardware that is disconnected from the internet and stored on the paper-based document. This method of transaction helps to protect the wallet from unauthorised access and other online vulnerabilities. Some of the cold wallets are hardware wallets and paper based wallets. They are described as below.

- *Hardware wallet*

A hardware wallet is a type of cold storage device that stores the user's private key in a secure hardware device. These wallets are like portable devices that can be connected to the computer. It is less prone to malware or malicious attacks. In order to complete the transaction, we must ensure that our wallet is connected to the computer system.

- *Paper-based wallet*

A paper-based wallet is an offline method for storing cryptocurrencies. This wallet is a printed paper consisting of a private and public key address that can be accessed using the QR code. Since these wallets are encrypted, they are commonly used to store many cryptocurrencies. To perform transactions, paper wallets work with software wallets. To transfer funds from our software wallet to the public address shown in our paper wallet (i.e., QR code), first the funds are stored in the online software wallet, and then they are transferred from the online software wallet to the paper wallet.

Applications of Blockchain technology

As blockchain technology is growing rapidly, there are several applications. Some of the important applications of blockchain technology are briefly discussed in the following section. Fig. 11 shows the diagrammatic representation of blockchain applications.

v) Cryptocurrency

The first and foremost application of blockchain technology is the Bitcoin cryptocurrency [56]. Cryptocurrency is based on a cryptographic method that uses encryption and decryption for secure communication. Some of the benefits of using cryptocurrencies are as follows: There is no transaction cost; the money can be accessed 24*7; there is no limit on purchases and withdrawals; anyone can use it; and international transactions are quicker. Bitcoin is a form of digital cryptocurrency that is decentralised without a central bank. It uses blockchain technology to perform transactions on a peer-to-peer network. Ether is another form of cryptocurrency that is accepted on the Ethereum network. Ethereum works on blockchain technology to create an open source for designing and implementing decentralised applications. The main difference between bitcoin and ether is that bitcoin is used to transfer money to someone in the real world. Moreover, bitcoin transactions are manual. It takes 10 min to perform a transaction. Bitcoin uses

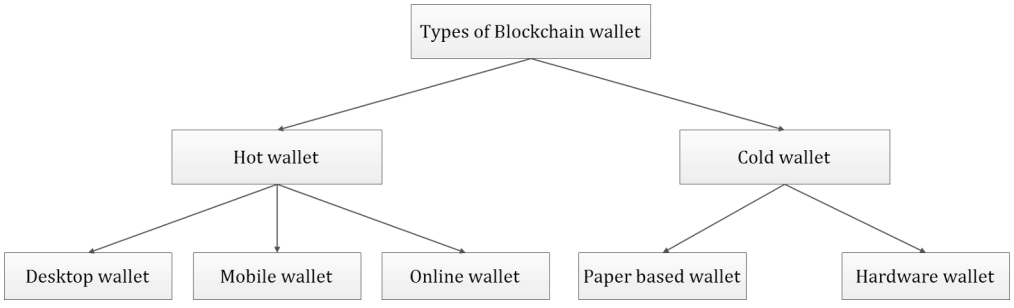


Fig. 10. Schematic representation of blockchain wallet types.

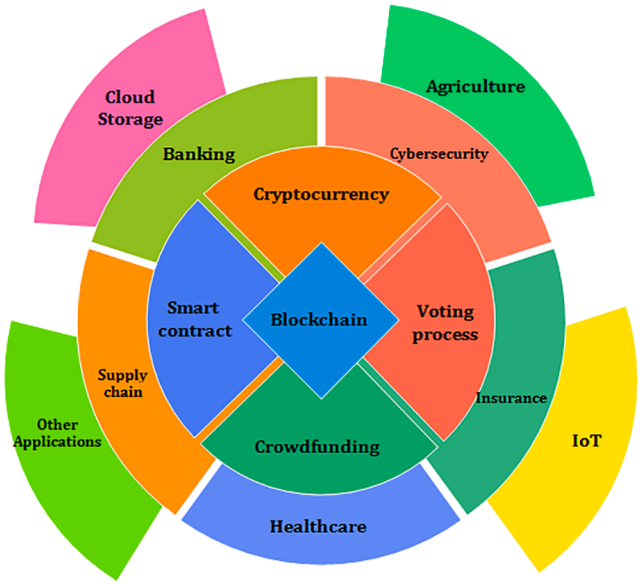


Fig. 11. Blockchain applications.

the SHA256 algorithm for hashing, whereas ether is used as a currency on the Ethereum network. Transactions are either manual or automatic. They are programmable and become executable when certain conditions are satisfied. It takes 14 s to complete the transaction. For hashing, Ethereum uses the ethash algorithm. Futurists believe that by 2030, cryptocurrencies will occupy 25% of the national currency. There are almost 3000 cryptocurrencies in the market. Some other important cryptocurrencies are Litecoin, Zcash, Dash, Ripple, Stellar, etc.,

w) Smart contracts

Smart contracts [57,58] are self-executing contracts without any intermediaries that contain the terms and conditions of the agreement between the parties. The terms and conditions of the agreement are written in code and implemented on the decentralised Blockchain platform. These agreements facilitate the exchange of any type of digital asset, which may be digital currency, shares, property, etc. The blockchain based decentralised platform offers an autonomous framework where transactions are authorised by the majority of the users and the true identity of the users is also kept anonymous. The process of execution of a smart contract is explained as follows.

A smart contract is formed on the basis of certain terms and conditions. Based on the code, a smart contract holds the transaction document, money, or shares until a certain condition is satisfied. This smart contract is submitted to the nodes in an Electronic Virtual Machine (EVM) for evaluation. All the nodes in the network executing the EVM code must come to the same result, since all the EVM use the same copy of the smart contract. These results are recorded in the distributed ledger. If the condition is not satisfied, then the smart contract will be self-executed, and the compensation will be given to the peers. This is the main objective of the smart contract, (i.e.,) without any paperwork, third party, manual process and all of this has been bypassed and the compensation is directly given to the peers. The bugs in the smart contract are immutable and irreversible. There is no direct way to rectify the bugs that is established in the smart contract application of blockchain. Eventhough, there is a possibility of rectifying the bugs it may significantly decrease the performance of the blockchain architecture. Therefore, smart contracts are designed with safe software protocol before come into execution.

In the conventional smart contract system, if two parties enter into a contract, they can use the services of a third party whom they trust to get the contract executed. Now, with the new approach of smart contracts, the third-party dependency is completely removed, and the automation of the contract is executed. Table 1 shows the comparison between the conventional contract and the smart contract in detail.

Table 1
Comparison of Conventional contract with Smart contract.

Parameters	Conventional contract	Smart contract
Third party	Government, lawyers etc.,	Not required
Processing time	In days (slow)	In minutes (fast)
Remittance	Manual process	Automatic process
Transparency	Not available	Available (24*7)
Automation	Manual	Fully automated
Accuracy	Less accurate	Highly accurate
Archiving	Difficult (as records are paper based and offline)	Easy traceable
Security	Limited	Cryptographically secured
Cost	Expensive	Cheap
Signature	Manual	Digital signature

HTLC stands for hashed timelock contract. It is mainly used in smart contract-based blockchain technology applications. It is a time-bound protocol in which the consumer acknowledges the conditional payment before a scheduled deadline. As a result, the counterparty risk is completely eliminated as the transactions are time constraints.

x) Voting process

Blockchain implementation in the voting process [59] can eliminate malpractices. A centralised voting system faces a lot of problems when it comes to tracking votes. There may be a possibility of manipulation of identity, counting, being unbiased in decision making, etc. A blockchain-based contract is introduced in the voting process, and certain predefined conditions are set in the contract. No voter can vote based on the digital identity of the other voter. Counting is performed automatically when every vote is registered on the blockchain network. So, there is no intermediate third party or manual process. Moreover, each identity should be attributed to one vote. Validation is performed by the nodes in the blockchain. So, the voting process takes place on the decentralised public blockchain, where there is 100% transparency and each voting transaction is recorded. Therefore, every vote of the voter is documented in the public ledger using an anonymous identity and the information cannot be modified.

y) Crowdfunding

Crowdfunding [60] is the concept in which the fund is provided by a group of people. The critical scenario is how the fund is provided by the people to the new person whom they don't trust. The solution comes in the form of blockchain. For instance, if we want to start a business, a lot of funding is required. But who would lend money to someone they don't trust? Blockchain plays a significant role in such issues. A crowdfunding contract is developed with Blockchain technology that keeps the funds of donors until a given date or target is reached. If the condition is satisfied, the fund will be released to the contract owners depending on their satisfactory results, or it will be sent back to the contributors (donors). The centralised crowdfunding system has many drawbacks. Therefore, a decentralised autonomous organisation (DAO) is utilised for crowdfunding. The terms and conditions are set out in the contract. Every individual participating in crowdfunding is given a token, and the token is credited if the target is satisfied by that individual. Every contribution from the DAO to the individual investor transactions gets recorded on the blockchain network. This helps to track and check the amount of funds received from the investors, whether the target amount has been received or not, how much percentage of shares belongs to the investors and how much percentage has been distributed already, and so on. Therefore, everything can be tracked using the provisions present in the crowdfunding.

z) Banking

One of the main applications of blockchain technology is in the banking sector [61]. For instance, if we wanted to transfer money from one person in one location to another person in another location, there would be a definite transaction fee. This transfer fee can be both

expensive and time-consuming. Because of the exchange rate and other hidden fees involved, sending money overseas gets much more complicated. Blockchain disrupts this current system by offering a peer-to-peer payment system with high protection and low fees. Moreover, the peer to peer payment system eliminates the need for central authority. It provides fast, cheap, and borderless payments across the world. Moreover, blockchain technology records all the transactions in a decentralised ledger that is publicly accessible by end users.

aa) Cybersecurity

Cyberattacks [62] are a major treat for the public. Blockchain is an effective solution to secure our data against unauthorised access and tampering. Blockchain is a decentralised framework, making it ideal for environments that require high security. All the stored information is verified and encrypted using a cryptographic algorithm. In the blockchain technology, each node has a copy of the ledger (data), and cryptography protects the transaction against any changes by making it immutable. With blockchain technology, data is distributed among multiple nodes and is secured by cryptography. This ensures that there is no single point of entrance for a wide-scale attack. Moreover, it's easy to identify malicious attacks due to peer-to-peer connections, where the data cannot be altered or tampered with. Blockchain provides a protected and secure way of tracking transactions without disclosing our private information to others.

ab) Supply chain management

Blockchain technology can facilitate traceability across the entire process of a supply chain. In supply chain management [63], blockchain provides permanent transparency and validation of transactions shared by multiple supply chain partners. For instance, if any product is produced at the producer end, it is possible to track the entire traceability of the product from the production end, distributor, retailer, and purchaser (customer). All blockchain entries are permanent and transparent, which makes it easy for a customer to view the transaction history of a product. Since each transaction is recorded in the block, anyone can verify the authenticity or status of the product being delivered.

ac) Healthcare

The data related to healthcare [64,65] is highly confidential and should be secured. Since the patient data is stored in the common physical memory of the centralised system, it can be easily hacked by an intruder. The intruder not only hacks the data but also modifies the data. But with the help of blockchain technology, central authority is eliminated, which results in rapid access to data. The confidential records of the patient are highly secured, encoded and stored in the blockchain using a private key. Access will be given only to specific individuals based on request. Moreover, doctors can only check the data of the patient with his public key. In addition, all the servers are interconnected and distributed across the nodes. So, corrupting the secured data is highly impossible. Another problem in healthcare is forged medicines. They are difficult to distinguish from the original, genuine medicines. Blockchain solves this problem with supply chain management, where the medicine's provenance can be traced.

ad) Insurance

Insurance companies can use blockchain technology to detect false claims and prevent forgeries by utilising a decentralised blockchain system. The distributed ledger records the data of the insured person to check the history of his transactions. This would help the insurer to prevent, detect, and counter fraud. For the insured person and the insurer, there are two viewpoints on insurance. According to insured individuals, filing an insurance claim is a complex and difficult task. The procedure of withdrawing the claim is also a difficult process for the insured person. From the insurer's perspective, rules and regulations are rigid and it is difficult to process a false claim. According to the current scenario, 400 million euros were lost due to false claims. Blockchain technology would be helpful to prevent this situation. Blockchain can be used by insured individuals and insurance companies to manage claims in a transparent and immutable manner. All the claims claimed by the insured person are recorded in the public distributed ledger. Moreover, it is validated by the network, ensuring only valid claims are paid to the insured people. For a single accident, if multiple claims are made by the insured person, then blockchain technology would know that the claim has been made already and would reject the multiple claims. Further, the claim amount is refunded to the genuine insured person automatically. If blockchain technology is adopted in the wider sector of the insurance industry, then handling claims would be very easy, streamlined and efficient. Not only will it help with customer satisfaction, but it will also reduce or completely prevent false claims [66].

ae) Agriculture

With the implementation of blockchain technology in the agriculture sector [67], data essential to farmers, such as soil moisture, seed quality, climate and environmental conditions, demand and sale price, harvest and yield, and so on, is stored in the distributed ledger. So, all these important activities in agriculture can be recorded using the blockchain technology. The world's agricultural market depends on population growth and the demand for high-quality products. Providing high-quality products to the increasing population is possible only with blockchain technology. Blockchain technology streamlines the sales process by eliminating all intermediaries between the producer and the customer. The producer has the sole right to fix the price of his product, and once it is fixed, it will be recorded, and no one will be able to modify it. Because blockchain provides certification for manufactured products, it will be beneficial for trusted retailers to use it. Some of the advantages of blockchain technology in the agricultural sector are transparent supply chains, fraud prevention, attractiveness for investment, smart contract availability, and easy money transfer for farmers.

af) Internet of things

Although the Internet of Things (IoT) [68] has millions of applications, the security of the information collected is of primary importance. As the technology is growing, several sensors are used for remotely monitoring and controlling different activities using IoT. A high level of security is required to make this process successful. The blockchain integrated with IoT helps to secure the data without any interruption. Only legitimate, trusted users would have access to the information recorded in the ledger. Moreover, the ownership and transferability are secured by the encryption of IoT devices on blockchain technology.

ag) Cloud storage

With the advancement of Internet innovation, the volume of data is increasing enormously. To handle a large volume of data, numerous organisations are trying to increase their storage capacity with the assistance of cloud platforms [69,70]. But, before storing the data on an untrusted cloud platform, some steps should be adopted to guarantee data protection. But by using blockchain technology, data can be effectively stored in the cloud. Clients can segment their own records into encoded information pieces and arbitrarily transfer that information into P2P network hubs. With high speed and low cost, videos, archives, documents, files, images, databases, contacts, financials, etc., are stored in the cloud storage. Thus, storage happens in the decentralised network, making it less prone to attacks. The transactions are performed by the clients without the intervention of third-party agents, following certain protocols. Illegal access to the data is prevented, as it provides the information only to legitimate users based on recorded history.

ah) Power and energy systems

With the advent of blockchain technology, in addition to its de facto application, which is cryptocurrency, the application of this technology in various fields has increased. The power and energy sectors are no exception. The proliferation of Distributed Energy Resources (DERs) in the Smart Grid network enables two-way power flow that leads to various challenges as well as opportunities to manage the energy needs of demand-side entities in an efficient manner. The major demand-side entities are the residential, commercial, industrial, and transportation sectors. The residential sector includes homes and buildings. The commercial sector includes hospitals, banks and financial institutions, educational institutions, etc. The industrial sector includes manufacturing units, factories, and companies. Thus, one of the critical

tasks in effectively managing energy requirements in a smart grid is optimal management of DERs [71]. Since, energy trading is required to manage the overall load profile of the sectors just mentioned, it can be achieved using blockchain, which offers a transparent, tamper-proof, and secure way of management. A block chain is basically a distributed ledger that records transactions that happen between entities in a seamless manner. The electricity needs can be better managed using Demand Response (DR) services [72]. Many examples of energy trading operations exist. For example, if an electric vehicle (EV) has excess power, then it can trade its energy with the electric grid via a charging station (CS) to meet the demand during peak hours [73]. Smart home systems can negotiate their excess energy with a utility service provider using energy trading [74]. Some use cases are defined in European Parliament resolutions on using blockchain technology in the energy sector, such as democratising the energy sector by allowing exchange of green energy generated by households with different parties, improving the integration of DERs into the Smart Grid network by offering additional network services, alternative government sponsored renewable investment schemes, alternative payment and donation mechanisms, contributing to consumption of less energy and being eco-friendly, etc. Based on the resolutions of the EU parliament, more applications of blockchain technology in the energy sector are under research. Some of the scenarios are as follows:

- Blockchain technology can be used between interconnected microgrids to achieve secure and efficient energy trading mechanisms for reliability and economic benefits [75].
- It provides a new technology for fully automated smart grid environments outfitted with renewable energy systems to address various challenges such as energy production, peer-to-peer (P2P) energy markets, carbon certificates and trading, and so on [76].
- Offering cryptocurrency rewards for the generation of renewable energy [77].
- The use of smart contracts, which act as a *code of law* in blockchain technology for price negotiation, automatic settlement, and payment after use [78].
- Decentralized storage and control in power grids, privacy in P2P energy trading, and EV charging in the transportation sector are all examples of energy-related issues [79].

ai) Microgird and smartgrid

Because they both deal with energy, microgrids and smart grids are inextricably linked [80,81].Microgrids powered by blockchain can provide a lossless, environmentally friendly energy transfer to nearby locations. The stored energy in the microgrid is either from the central grid or autonomously generated, and this energy can be used for smaller applications like invertors, etc., and it is a small-scale distributed generation. Whereas in smart grids, energy transactions are verified and recorded. Moreover, blockchain offers immutable transactions with a traceable transaction history, which helps to solve any dispute in smart grids.

aj) Renewable energy sources application in Blockchain

Biomass, geothermal, wind, and solar are some of the major renewable energy sources. These sources can be effectively used in the blockchain network for providing pollution free environment. When renewable energy sources are used, there is an effective transition from polluting fossil fuels to moving towards the long-term sustainable usage of clean resources. The biomass waste can be recycled and once again used for the production of energy. When blockchain technology is incorporated, biomass tracing, production, and thereby conserving resources can be easily achieved. This may lead to the development of a shared energy system. Research has been focused on the production of renewable energies in a decentralised manner, thus meeting the needs of small-scale energy producers. When blockchain technology is assimilated, it leads to a reduction in energy waste, an increase in transparency, and a monitoring capability of the clients. Traceability is the major advantage of using the blockchain. The source of renewable energy resources such as wind or solar can be easily traced and, thereby, linked to the specific point of consumption. A peer-to-peer energy trading model can be achieved using blockchain for renewable energy sources.

ak) Other applications

Blockchain technology enables traceability in the transportation [82] industry, where the shipment of goods can be easily traced. Deploying blockchain technology in real estate [83] increases the speed of the conveyance process and eliminates the necessity for money exchanges. Blockchain technology can increase security and transparency in the government's system. With blockchain technology, a fast and secure registration [84] process of any asset, like an automobile, land, etc., is possible. Utilizing blockchain technology with the notary's seal [85] can be a faster way to prove a document's authenticity. Deploying blockchain can result in quicker tax [86] payments, lower rates of tax evasion, and less effort in tax auditing. Blockchain 3.0 [87] is having a revolutionary impact on all industries. Apart from the development of blockchain in the financial sectors, markets, healthcare, economics, and so on, Advancement in blockchain technology opens doors for secure applications in industries too. Furthermore, blockchain 3.0 enables industries to have a global reach. It led to the development of industrial applications that are global in smart.

Conclusion

A detailed survey of blockchain technology is presented in this work. The implementation of blockchain technology builds trust between anonymous users and enables them to perform transactions without any third-party intermediary. This work clearly explains the structural overview, describing the role of the node, miner, and the contents of the block. Moreover, the transaction process and the blockchain consensus mechanism are also described. Furthermore, this work discusses key blockchain technology features such as decentralisation, transparency, immutability, distributed ledger, P2P network, and irreversibility. In addition, blockchain classification, features, functionality, and blockchain wallet types are also described. Finally, the various applications of the blockchain technology are enlightened. This study is envisioned to serve as a significant guide for knowing various blockchain consensus frameworks and areas of application for exploring possible directions for research, that can lead to promising findings in related fields. The future scope of blockchain technology can be incorporated into big data and standardization. Standardization should be followed when implementing blockchain technology in the business sector. Initially, the claims are verified, and a standard procedure is followed to obtain the best solution. The integration of blockchain technology with big data helps to keep confidential data secrets and copyright forms in the secured cryptographic layer. Moreover, they help in storing large volumes of data which are completely secured due to the immutable nature of blockchain.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

Funding details: There is no funding for this manuscript.
Data availability and ethical statement: None.

References

[1] Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System; 2009.

[2] Dhumwad S, Sukhadeve M, Naik C, MKN, Prabhu S. A Peer to Peer Money Transfer Using SHA256 and Merkle Tree, 2017 23rd Annual International Conference in Advanced Computing and Communications (ADCOM), Bangalore, India, 2017, pp. 40–43.

[3] Meva D. Issues and challenges with blockchain a survey. Int J Comp Sci Eng 2018;6 (12):488–91.

[4] Attaran, Mohsen, and Angappa Gunasekaran. Blockchain Principles, Qualities, and Business Applications. Springer Briefs in Operations Management Applications of Blockchain Technology in Business, 2019, pp. 13–20.

[5] Bhutta MNM, Khwaja AA, Nadeem A, Ahmad HF, Khan MK, Hanif MA, et al. A survey on blockchain technology: evolution, architecture and security. IEEE Access 2021;9:61048–73. https://doi.org/10.1109/ACCESS.2021.3072849.

[6] Xu LD, Lu Y, Li L. Embedding blockchain technology into IoT for security: a survey. IEEE Internet Things J 2021;8(13):10452–73.

[7] Tran QN, Turnbull BP, Wu H-T, de Silva AJS, Kormusheva K, Hu J. A survey on privacy-preserving blockchain systems (PPBS) and a novel PPBS-based framework for smart agriculture. IEEE Open J Comp Soc 2021;2:72–84. https://doi.org/10.1109/OJCS.2021.3053032.

[8] Mollah MB, Zhao J, Niyato D, Guan YL, Yuen C, Sun S, et al. Blockchain for the internet of vehicles towards intelligent transportation systems: a survey. IEEE Internet Things J. 2021;8(6):4157–85.

[9] Arasan A, Sadaiyandi R, Al-Turjman F, Rajasekaran AS, Karuppuswamy KS. Computationally efficient and secure anonymous authentication scheme for cloud users. Pers Ubiquit Comput 2021. https://doi.org/10.1007/s00779-021-01566-9.

[10] Subramani J, Maria A, Rajasekaran AS, Al-Turjman F. Lightweight privacy and confidentiality preserving anonymous authentication scheme for WBANs. IEEE Trans. Ind. Inf. 2022;18(5):3484–91.

[11] Subramani J, Maria A, Neelakandan RB, Rajasekaran AS. Efficient anonymous authentication scheme for automatic dependent surveillance-broadcast system with batch verification. IET Commun 2021;15(9):1187–97. https://doi.org/10.1049/cmu2.12152.

[12] Iqbal A, Rajasekaran AS, Nikhil GS, Azees M. A secure and decentralized blockchain based EV energy trading model using smart contract in V2G network. IEEE Access 2021;9:75761–77. https://doi.org/10.1109/access.2021.3081506.

[13] Subramani J, Nguyen TN, Maria A, Rajasekaran AS, Cengiz K. Lightweight batch authentication and privacy-preserving scheme for online education system. Comput Electr Eng 2021;96:107532. https://doi.org/10.1016/j.compeleceng.2021.107532.

[14] Curran K, Curran J. Blockchain security and potential future use cases. Blockchain for Cybersecurity and Privacy 2020:75–83.

[15] Conti M, Sandeep Kumar E, Lal C, Ruj S. A survey on security and privacy issues of bitcoin. IEEE Commun Surv Tutorials 2018;20(4):3416–52.

[16] Pal P, Ruj S. BlockV: a blockchain enabled peer-peer ride sharing service. 2019 IEEE International Conference on Blockchain. 2019.

[17] Bellini E, Iraqi Y, Damiani E. Blockchain-based distributed trust and reputation management systems: a survey. IEEE Access 2020;8:21127–51.

[18] Rehman MHU, Salah K, Damiani E, Svetinovic D. Trust in blockchain cryptocurrency ecosystem. IEEE Trans Eng Manage 2020;67(4):1196–212.

[19] Zaghloul E, Li T, Mutka MW, Ren J. Bitcoin and blockchain: security and privacy. IEEE Internet Things J 2020;7(10):10288–313.

[20] Toyoda K, Machi K, Ohtake Y, Zhang AN. Function-level bottleneck analysis of private proof-of-authority ethereum blockchain. IEEE Access 2020;8:141611–21.

[21] Tempesta, Stefano. Blockchain Architecture Reference. Introduction to Blockchain for Azure Developers; 2019.

[22] S. Dos Santos, C. Chukwuocha, S. Kamali, R.K. Thulasiram, An Efficient Miner Strategy for Selecting Cryptocurrency Transactions, 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019, pp. 116–123.

[23] Pyoung CK, Baek SJ. Blockchain of finite-lifetime blocks with applications to edge-based IoT. IEEE Internet Things J 2020;7(3):2102–16.

[24] Drescher D. Hashing in the real world. Blockchain Basics 2017:81–92.

[25] Almuttalibi RA, Yousif. Blockchain hash function for secure biometric system. J Eng Appl Sci 2019;14(11):3797–805.

[26] Xiao Y, Zhang N, Lou W, Hou YT. A survey of distributed consensus protocols for blockchain networks, IEEE Commun Surveys Tutorials, 22 (2), 1432–1465, Second quarter 2020.

[27] Klinkmüller, Christopher, et al. Mining Blockchain Processes: Extracting Process Mining Data from Blockchain Applications. Business Process Management: Blockchain and Central and Eastern Europe Forum Lecture Notes in Business Information Processing, 2019, pp. 71–86.

[28] Mittal, Anshul, and Swati Aggarwal. Hyperparameter Optimization Using Sustainable Proof of Work in Blockchain. Front Blockchain, 3, 2020.

[29] Saleh F, Jiang W. Blockchain without waste: proof-of-stake. Rev Financial Studies 2021;34(3):1156–90.

[30] Lu Y, et al. Car parker: a blockchain-based privacy preserving and accident-proof-preserving private parking space sharing system. Easy Chair Preprints 2018.

[31] Pohl M, et al. Proof of provision: improving blockchain technology by cloud computing. Proceedings of the 9th International Conference on Cloud Computing and Services Science. 2019.

[32] "Unpacking Blockchain Trust." The Blockchain and the New Architecture of Trust; 2018.

[33] She W, Liu Q, Tian Z, Chen J, Wang B, Liu W. Blockchain trust model for malicious node detection in wireless sensor networks. IEEE Access 2019;7:38947–56.

[34] Dietzfelbinger, Martin, Jörg Keller. Determining Minimum Hash Width for Hash Chains." Proceedings of the Third Central European Cybersecurity Conference on – CECC 2019, 2019.

[35] Hoffman, Michał R., et al. "Toward a Formal Scholarly Understanding of Blockchain-Mediated Decentralization: A Systematic Review and a Framework." Frontiers in Blockchain, vol. 3, 2020.

[36] Chohan UW. The Limits to Blockchain? Scaling vs Decentralization. SSRN Electr J 2019.

[37] Daoud E. Decentralizing of transparency: using blockchain to reduce counterfeiting. 17th International Conference on e-Society. 2019.

[38] Click, Kelly, et al. Immutable and Secure IP Address Protection Using Blockchain. Advances in Information Security Blockchain Cybersecurity, Trust and Privacy, 2020, pp. 233–246.

[39] Dhumwad S, et al. A peer to peer money transfer using SHA256 and Merkle tree. 2017 23RD Annual International Conference in Advanced Computing and Communications (ADCOM). 2017.

[40] Patwardhan, Anju. "Peer-To-Peer Lending." Handbook of Blockchain, Digital Finance, and Inclusion, Volume 1, 2018, pp. 389–418.

[41] Natarajan, Harish, et al., Distributed Ledger Technology and Blockchain; 2017.

[42] Deuber D, Magri B, Thyagarajan SAK. Redactable Blockchain in the Permissionless Setting, 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2019, pp. 124–138.

[43] Lai, Roy, David Lee Kuo Chuen. Blockchain – From Public to Private. Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2, 2018, pp. 145–177.

[44] Mitani T, Otsuka A. Traceability in Permissioned Blockchain, 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019, pp. 286-293.

[45] Huang D, Ma X, Zhang S. Performance analysis of the raft consensus algorithm for private blockchains. IEEE Trans Syst, Man, Cybernetics: Syst 2020;50(1):172–81.

[46] Al-Shaibani H, Lasla N, Abdallah M. Consortium blockchain-based decentralized stock exchange platform. IEEE Access 2020;8:123711–25.

[47] Zhang J. A multi-transaction mode consortium blockchain. Int J Performability Eng 2018.

[48] Z. Cui et al., A Hybrid BlockChain-Based Identity Authentication Scheme for Multi-WSN, in IEEE Transactions on Services Computing, vol. 13, no. 2, pp. 241-251, 1 March-April 2020.

[49] Chang S-Y, Park Y. Silent timestamping for blockchain mining pool security. 2019 International Conference on Computing, Networking and Communications (ICNC). 2019.

[50] Byzantine Fault Tolerance. Building Dependable Distributed Systems, 2014, pp. 239–287.

[51] Xu X, et al. Concurrent practical byzantine fault tolerance for integration of blockchain and supply chain. ACM Trans Internet Technol 2020.

[52] Misic VB, et al. On forks and fork characteristics in a bitcoin-like distribution network. 2019 IEEE International Conference on Blockchain (Blockchain). 2019.

[53] Chen P-W, et al. Blockchain-based payment collection supervision system using pervasive bitcoin digital wallet. 2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). 2017.

[54] Thota AR, Upadhyay P, Kulkarni S, Selvam P, Viswanathan B. Software Wallet Based Secure Participation in Hyperledger Fabric Networks, 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS), Bengaluru, India, 2020, pp. 1–6.

[55] Khadzhi AS, Zareshin SV, Tarakanov OV. A Method for Analyzing the Activity of Cold Wallets and Identifying Abandoned Cryptocurrency Wallets, 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), St. Petersburg and Moscow, Russia, 2020, pp. 1974–1977.

[56] Yuan Y, Wang F. Blockchain and cryptocurrencies: model, techniques, and applications. IEEE Trans Syst, Man, Cybernetics: Syst 2018;48(9):1421–8.

[57] 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, Cybernetics: Syst 2019;49(11):2266–77.

[58] Christidis K, Devetsikiotis M. Blockchains and smart contracts for the internet of things. IEEE Access 2016;4:2292–303.

[59] Shahzad B, Crowcroft J. Trustworthy electronic voting using adjusted blockchain technology. IEEE Access 2019;7:24477–88.

[60] Bogusz CI, Laurell C, Sandström C. Tracking the Digital Evolution of Entrepreneurial Finance: The Interplay Between Crowdfunding, Blockchain Technologies, Cryptocurrencies, and Initial Coin Offerings, IEEE Trans Eng Manage.

[61] Bagrecha NR, Mustafa Polishwala I, Mehrotra PA, Sharma R, Thakare BS. Decentralised Blockchain Technology: Application in Banking Sector, 2020 International Conference for Emerging Technology (INCET), Belgaum, India, 2020, pp. 1–5.

[62] Vance TR, Vance A. Cybersecurity in the Blockchain Era : A Survey on Examining Critical Infrastructure Protection with Blockchain-Based Technology," 2019 IEEE International Scientific-Practical Conference Problems of Info communications, Science and Technology (PIC S&T), Kyiv, Ukraine, 2019, pp. 107–112.

[63] Shakhbulatov D, Medina Chirinos J, Dong Z, Rojas-Cessa R. How blockchain enhances supply chain management: a survey. IEEE Open J Comp Soc 2020.

[64] Zhuang Y, Sheets LR, Chen Y-W, Shae Z-Y, Tsai JJP, Shyu C-R. A patient-centric health information exchange framework using blockchain technology. IEEE J Biomed Health Inf Aug. 2020;24(8):2169–76.

[65] Garcia PSR, Kleinschmidt JH. Sharing health and wellness data with blockchain and smart contracts. IEEE Lat Am Trans Jun 2020;18(06):1026–33.

[66] Vakilinia I, Badsha S, Sengupta S. Crowdfunding the Insurance of a Cyber-Product Using Blockchain. 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York City, NY, USA, 2018, pp. 964–970.

[67] Lin W, et al. Blockchain technology in current agricultural systems: from techniques to applications. IEEE Access 2020;8:143920–37.
[68] Novo O. Blockchain meets IoT: an architecture for scalable access management in IoT. IEEE Internet Things J 2018;5(2):1184–95.
[69] Wang S, Wang X, Zhang Y. A secure cloud storage framework with access control based on blockchain. IEEE Access 2019;7:112713–25.
[70] Gai K, Choo KR, Zhu L. Blockchain-enabled reengineering of cloud datacenters. IEEE Cloud Comput 2018;5(6):21–5.
[71] Wang K, Li H, Maharjan S, Zhang Y, Guo S. Green energy scheduling for demand side management in the smart grid. IEEE Trans Green Commun Networking 2018;2 (2):596–611.
[72] Golosova J, Romanovs A, Kunicina N. Review of the Blockchain Technology in the Energy Sector, 2019 IEEE 7th IEEE Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE), Liepaja, Latvia, 2019, pp. 1–7.
[73] Nsonga P, Hussain SMS, Garba A, Ustun TS, Ali I. Performance evaluation of electric vehicle ad-hoc network technologies for charging management, 2017 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC), Bangalore, 2017, pp. 1–5.
[74] Hussain SMS, Farooq SM, Ustun TS. Implementation of Blockchain technology for Energy Trading with Smart Meters, 2019 Innovations in Power and Advanced Computing Technologies (i-PACT), Vellore, India, 2019, pp. 1–5.
[75] Masaud TM, Warner J, El-Saadany EF. A Blockchain-Enabled Decentralized Energy Trading Mechanism for Islanded Networked Microgrids, in IEEE Access, doi: 10.1109/ACCESS.2020.3038824.
[76] Hrga A, Capuder T, Žarko IP. Demystifying distributed ledger technologies: limits, challenges, and potentials in the energy sector. IEEE Access 2020;8:126149–63.
[77] Huang Y, Yang P, Liu Z, Lyu Y, Chen Y. A design of photovoltaic plants financing platform based on blockchain technology, in Proc. Int. Conf. Power Syst. Technol. (POWERCON), Nov. 2018, pp. 4251–4256.
[78] Thomas L, Long C, Burnap P, Wu J, Jenkins N. Automation of the supplier role in the GB power system using blockchain-based smart contracts. CIRED Open Access Proc. J. Oct. 2017;2017(1):2619–23.
[79] Zhuang P, Zamir T, Liang H. Blockchain for cybersecurity in smart grid: a comprehensive survey. IEEE Trans Ind Inf 2021;17(1):3–19. https://doi.org/10.1109/TII.2020.2998479.
[80] Mollah MBet al., Blockchain for Future Smart Grid: A Comprehensive Survey, in *IEEE Internet of Things Journal,* vol. 8, no. 1, pp. 18-43, 1 Jan.1, 2021, doi: 10.1109/JIOT.2020.2993601.
[81] Bao J, He D, Luo M, Choo K-K-R. A survey of blockchain applications in the energy sector. IEEE Syst J 2021;15(3):3370–81. https://doi.org/10.1109/JSYST.2020.2998791.
[82] Mu Y, Rezaeibagha F, Huang K. Policy-driven blockchain and its applications for transport systems, IEEE Trans Services Comp, 13 (2), 230–240, 1 March-April 2020.
[83] Latifi S, Y. Zhang, L. Cheng, Blockchain-Based Real Estate Market: One Method for Applying Blockchain Technology in Commercial Real Estate Market,“ 2019 IEEE International Conference on Blockchain, Atlanta, GA, USA, 2019, pp. 528-535.
[84] Jiang N, Wang W, Wu J, Wang J. Traceable method for personal information registration based on blockchain. IEEE Access 2020;8:52700–12.
[85] Szalachowski P. PADVA: A Blockchain-Based TLS Notary Service, 2019 IEEE 25th International Conference on Parallel and Distributed Systems (ICPADS), Tianjin, China, 2019, pp. 836-843.
[86] Fatz F, Hake P, Fettke P. Towards Tax Compliance by Design: A Decentralized Validation of Tax Processes Using Blockchain Technology, 2019 IEEE 21st Conference on Business Informatics (CBI), Moscow, Russia, 2019, pp. 559-568.
[87] Leng J, et al. Blockchain-secured smart manufacturing in industry 4.0: a survey. IEEE Trans Systems, Man, Cybernetics: Syst 2021;51(1):237–52. https://doi.org/10.1109/TSMC.2020.3040789.