Azerbaijan Journal of High Performance Computing, Vol 5, Issue 1, 2022, pp. 33-51
https://doi.org/10.32010/26166127.2022.5.1.33.51

Blockchain Concepts, Architecture, Characteristics and Challenges: a Survey

Zahra Tayyebi Qasabeh[1], Seyyed Sajjad Mousavi[2]

[1]Payame Noor University of Guilan, Guilan, Iran, tayyebi.shiva@gmail.com
[2] Pol Talshan Azad University, Gilan, Iran, Sajjad_dwj@yahoo.com

*Correspondence:
Zahra Tayyebi Qasabeh,
Payame Noor university of Guilan, Iran,
tayyebi.shiva@gmail.com

Abstract

The blockchain is a revolutionary technology transforming how assets are managed digitally and securely on a distributed network. Blockchain decentralized technology can solve distrust problems of the traditional centralized network and enhance the privacy and security of data. It provides a distinct way of storing and sharing data through blocks chained together. The blockchain is highly appraised and endorsed for its decentralized infrastructure and peer-to-peer nature. However, much research about the blockchain is shielded by Bitcoin. But blockchain could be applied to a variety of fields far beyond Bitcoin. Blockchain has shown its potential for transforming the traditional industry with its essential characteristics: decentralization, persistency, anonymity, and audibility. Undoubtedly, blockchain technology can significantly change the global business environment and lead to a paradigm shift in the functioning of the business world. However, to unlock the tremendous potential, various challenges in the adoption and viability of blockchain technology must be addressed before we can see the legal, economic, and technical viability of this technology in the operation of various business applications. In this study, the fundamental concepts of blockchain are discussed at the beginning, and the way it works and its architecture is mentioned, and since all technologies face challenges, this technology is no exception and has challenges based on the works related to the challenges It is mentioned.

Keyword: Blockchain Concepts, Architecture, Characteristics, Challenges.

1. Introduction

The first public blockchain behind Bitcoin was developed with specific functionality, namely decentralized currency and peer-to-peer electronic cash applications. The Bitcoin whitepaper introduced the blockchain concept to solve the double-spending problem when executing a transaction over a communication medium without relying on a trusted third party like a financial institution or a bank (Gamage, H. T. M., Weerasinghe, H. D., & Dias, N. G. J., 2020). Therefore, the Bitcoin blockchain was practically challenging to customize and had shallow programmable support using a scripting system called Script for other purposes. Vitalik Buterin noticed this difficulty and introduced the Ethereum blockchain platform with a built-in, Turing-complete programming language, allowing anyone to write programs called smart contracts and run decentralized applications. Protocols like currencies, identity systems, and reputation systems can be implemented with minimal code to run on the Ethereum platform (Gamage, H. T. M., Weerasinghe, H. D., & Dias, N. G. J., 2020).

Blockchain is the central and the underlying technology of cryptocurrencies, is one of the examples of innovations that is pivotal to the business management revolution movement, and is an emerging and utilitarian technology that has the potential to have a significant impact on the functioning of a large number of business organizations (Pal, A., Tiwari, C. K., & Haldar, N., 2021). Satoshi Nakamoto first introduced blockchain technology in November 2008. The idea was to make transactions electronically without central authority at a low transaction fee. In a typical banking environment, central agencies implement a concurrency control mechanism to avoid double spending, but this approach suffers from issues like a single point of failure, high transaction fees, trust issues, and malicious attacks. Despite the absence of central authority, the blockchain architecture is efficiently designed to maintain security, confidentiality, and traceability (Kaushal, R. K., Kumar, N., & Panda, S. N., 2021, August).

In the blockchain, data are kept in a distributed ledger. Blockchain technology provides integrity and availability that allows participants in the blockchain network to write, read, and verify transactions recorded in a distributed ledger. However, it does not allow the deletion and modification operations on the transactions and other information stored on its ledger. The blockchain system is supported and secured by cryptographic primitives and protocols, e.g., digital signatures and hash functions. These primitives guarantee that the transactions recorded into the ledger are integrity-protected, authenticity-verified, and non-repudiated. Further, as a distributed network, to allow the entire set of participants to agree on a unified record, blockchain technology also needs a consensus protocol, which is essentially a set of rules to be followed by every participant, to achieve a globally unified view. In a trustless environment, blockchain provides users with desirable decentralization, autonomy, integrity, immutability, verification, fault-tolerance, attracted great academic and industrial attention in recent years, anonymity, auditability, and transparency.

Blockchain technology has attracted great academic and industrial attention in recent years with these advanced features. To help and benefit someone to understand the blockchain technology and blockchain security issues, especially for users who use blockchain to do transactions and for researchers who be developing blockchain technology and addressing blockchain security issues, we put in our effort and time to conduct a comprehensive survey and analysis on blockchain technology and its security issues. First, we identify keywords, blockchain, survey, consensus algorithm, smart contract, risk, and blockchain security, to search publications and information on the Internet. Second, we survey papers related to blockchain published in top security conferences and journals, e.g., USENIX Security Symposium, IEEE Symposium on Security and Privacy, and IEEE Transactions journals. In this way, we have surveyed as many papers as possible to overcome the study and result biases. Our survey paper presents the comprehensive findings from other research work (Guo, H., & Yu, X., 2022).

1.1. Blockchain concept

Blockchain is an immutable distributed digital ledger, secured using advanced cryptography, replicated among the peer nodes in the peer-to-peer network, and uses a consensus mechanism to agree upon the transaction log, whereas control is decentralized. With this definition, the paper identifies the following concepts as the core concepts to unwrap the meaning of blockchain—immutable, distributed, digital ledger, cryptography, peer-to-peer network, consensus mechanism, and decentralization. In accounting, a ledger is a place to record and store all the transactions concerning an entity. A digital ledger could be a computer file, database, or even a distributed database like a blockchain, where transactions are recorded electronically. The blockchain transaction ledger is unique to other ledgers, which ensures that the transaction log is computationally impractical to change, as long as honest nodes in the network control the majority of CPU power, thus making it immutable. The origins of the ledger can be traced back to over 5000 years ago in Mesopotamia. The Earliest and simplest form of recording transactions is called single entry accounting, which enters transactions into a list to keep track of adding or deducting assets. Owners or family members managed the single entry accounting, as this kind of recording is error-prone and difficult to track down when recorded fraudulently. Double entry accounting added a clear strategy to identify and remove errors, where two entries are recorded against each transaction so that the ledger is balanced all the time. Grigg proposed triple entry accounting in 2005, an alternative to traditional double-entry accounting, which secures transactions using cryptography to make them difficult to change. Blockchain implements a triple-entry accounting concept to permanently store transactions in the blockchain, ensuring that the sender has the authority to execute non-reversible transactions using public-key cryptography (Gamage, H. T. M., Weerasinghe, H. D., & Dias, N. G. J., 2020).

Cryptography can be defined as techniques used for secure communication to protect confidential information in the presence of adversaries. Blockchain uses concepts from vital public cryptosystems to verify the user's authority to execute transactions and cryptographic hash functions to achieve consensus between network nodes on blockchain data. The use of public key cryptosystems to provide digital signatures was suggested by Dife and Hellman (Eyal, I., & Sirer, E. G., 2018). Digital signatures, whether based on public key cryptosystems, conventional encryption functions, probabilistic computations, or other techniques, share several essential properties in common, such as an easier way for the sender to generate the personal digital signature, a convenient way for the receiver to verify the sender of the message, but must be impossible to generate someone else's digital signature by others.

In public key cryptography, there exist two keys called, public and private, and a function or cipher algorithm to encrypt the original text into ciphertext using the private encryption key.

This public essential cryptography technique is used in blockchain to verify the ownership of coins or tokens whenever transferring coins or tokens. The sender or owner generates the public-private key pair and keeps the private key as the secret key to encrypt information; the public key is distributed to anyone to verify that the original owner digitally signs the information. One another important concept used in blockchain to secure its data integrity is the cryptographic hash function—a one-way function that maps strings of arbitrary size into a bit of fixed size called Hash using a mathematical algorithm. An algorithm required for blockchain hash functions has three main properties—the same input should always result in the same output hash, given the Hash, no algorithm could produce the original input, and small changes in input results in a completely different output hash. Bitcoin uses the SHA-256 hash function, Ethereum uses Ethash, and Litecoin uses Scrypt when hashing its block data (Gamage, H. T. M., Weerasinghe, H. D., & Dias, N. G. J., 2020).

Blockchain technology has attracted much attention among these emerging technologies. Blockchain is a digital head office with transparent, visible, and tamper-resistant exchanges with a decentralized data center and distribution worldwide. Transactions in blockchain are done without the presence of a third party (such as banks, governments, or companies) between the seller and the buyer. While the trading system is usually centralized, and all data and information are controlled and managed by a third-party organization, not the two prominent people involved in the transaction. These intermediaries also control data security and data privacy ultimately. Blockchain technology was created to solve this problem to create a decentralized environment where no third party is in control of transactions and data. A notable feature of blockchain is that public passwords are never associated with a real identity and are activated without disclosing the identities of individuals, although transactions can be tracked if necessary. This event significantly differs from Fiat currency transactions in which individuals usually have legal personalities. The business logic that blockchain works with is defined in terms of smart contracts. Smart contracts specify all the conditions that must be met before making a transaction). The first and most common digital currency based on blockchain was Bitcoin. Blockchain technology is the basis of modern cryptocurrencies due to the widespread use of cryptocurrency functions. A cryptocurrency economic system is an economic system independent of geographical location, political structure, or legal system that is based on reliable cryptography. Currency encryption technology was initially designed for information security systems but has been developed in various fields over time (Aghababayi, H., Nikabadi, M. S., Kafaki, S. B., & Rahmanimanesh, M., 2022).

1.2. History of Blockchain

In 1982, Chaum was the first known person to propose a blockchain-like protocol in his Ph.D. thesis. In 1991, Haber and Stornetta described a secured chain of blocks cryptographically. In 1993, Bayer et al. incorporated Merkle trees into the design. In 1998, ‘‘bit gold’’—a decentralized digital currency mechanism, was designed by Szabo. In 2008, Nakamoto introduced Bitcoin, electronic cash with a purely peer-to-peer network. It was also in 2008 that the term blockchain was first introduced as the distributed ledger behind Bitcoin transactions. In 2013, Buterin proposed Ethereum in his whitepaper. In 2014, the development of Ethereum was crowdfunded, and on July 30, 2015, the Ethereum network went live. The emergence of Ethereum implied that blockchain 2.0 was born because, different from all the various blockchain projects that focused on developing altcoins (other coins which are similar to Bitcoin), Ethereum enables people to connect through trustless distributed applications on its blockchain. In other words, while Bitcoin is developed for a distributed ledger, Ethereum is developed for distributed data storage plus intelligent contracts, which are small computer programs. Ethereum 2.0 upgrades the Ethereum network, aiming to boost the network’s speed, scalability, efficiency, and security. The upgrades have 3 phases crossing from 2020 to 2022. In 2015, the Linux Foundation announced the Hyperledger project, open-source blockchains software. Hyperledger blockchain frameworks differ from Bitcoin, Ethereum, and Intend to build enterprise blockchains. Under Hyperledger, there are eight blockchain frameworks, including Hyperledger Besu, Hyperledger Fabric, Hyperledger Indy, Hyperledger Sawtooth, Hyperledger Burrow, Hyperledger Iroha, Hyperledger Grid, and Hyperledger Labs, five Hyperledger tools, including Hyperledger Avalon, Hyperledger Cactus, Heperledger Caliper, Hyperledger Cello, and Hyperledger Explorer, and four libraries, including Hyperledger Aries, Hyperledger Quilt, Hyperledger Transact, and Hyperledger URSA. The history of blockchain is summarized in Fig. 1. Bitcoin and Ethereum are public blockchains since anyone can participate in their blockchain networks, also called permissionless blockchains. The various Hyperledger blockchain networks are private blockchains since the participants must be verified first before joining the network, also called permissioned blockchains (Guo, H., & Yu, X., 2022).

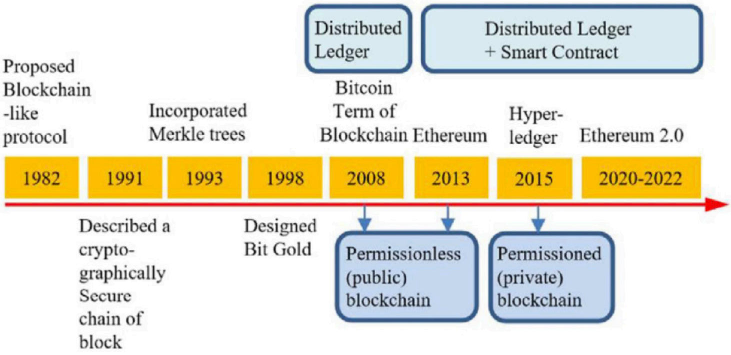
Distributed Ledger
Distributed Ledger + Smart Contract
Proposed Blockchain -like protocol
Incorporated Merkle trees
Bitcoin Term of Blockchain
Ethereum
Hyper- ledger
Ethereum 2.0
1982
1991
1993
1998
2008
2013
2015
2020-2022
Described a crypto- graphically Secure chain of block
Designed Bit Gold
Permissionless (public) blockchain
Permissioned (private) blockchain

Fig. 1. History of blockchain (Guo, H., & Yu, X., 2022)

1.3. The general structure of blockchain

A blockchain is a timestamped sequence of rigid transactions managed by a group of computers using unique algorithms. Each computer in this group is called a node, and each node shares the exact copy of data, called a digital ledger. Each node maintains the records of transactions in multiple consecutive blocks and uses the same algorithm to reach a standard agreement. These transactions are saved on every node in a distributed Peer to Peer (P2P) network. Figure 2 shows the general structure of a blockchain with essential block components. Each block consists of version information, nonce value, the previous block's hash value, timestamp, Merkle root, and transactions. The version number of the blockchain is used to maintain changes and updates during the whole duration of the protocol. A nonce is an arbitrary number that miners come across as a mining component. The nonce is a part of cracking the mathematical puzzle first to mine the block. Hash is a cryptographic function used o secure the chain. The timestamp is used to understand when a particular transaction has occurred. Merkle Root is obtained by hashing the transaction hashes again. A transaction list refers to the different transactions included in a particular block (Patil, P., Sangeetha, M., & Bhaskar, V., 2021).

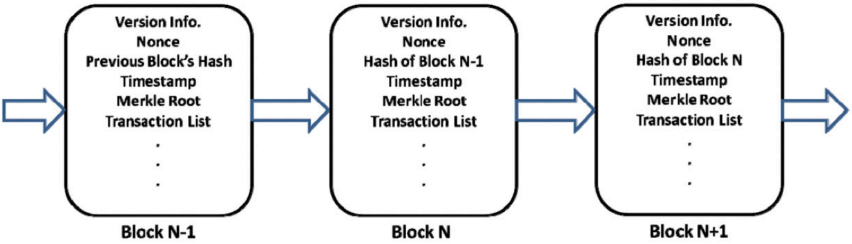

Fig. 2. General structure of blockchain

1.4. Functioning of the Blockchain

a P2P network needs to be created with the devices (users) interested in communicating through blockchain, In implementing Blockchain technology. Each participating device is referred to as a node. Two keys are generated for each node: namely, public and private. As the name implies, the public key is acknowledged to all, and the private key is undisclosed and is used by a user to produce a signature. In short, asymmetric cryptography is used to accomplish the security demand of the information. Private keys need to be kept protected to avoid possible misuse or tampering of data on a blockchain. A node initiates the transaction and, after signing it with the private key, publishes it in the network for getting verified by the peer nodes. These verification methods are known as consensus algorithms and vary in different blockchain platforms, depending upon the design objectives. After peer verification, the miner collects the transaction to create a block, and that block gets appended to the blockchain with the timestamp and unique ID (i.e., Hash) to avoid further alterations.

The newly added block gets linked up with the previous block using its Hash, and the upcoming block establishes a link with this block. Figure 3 below depicts the general workflow of blockchain based on the above description.

The consensus algorithm is the heart of Blockchain technology since it maintains the blockchain network's integrity and security. It is a protocol by which blockchain network nodes arrive at a standard agreement on the current records state of the ledger. Different blockchain platforms use different algorithms to reach a consensus, and of course, all of them differ in their operation and execution. Figure 4 shows the most popular consensus algorithms used in different blockchain platforms. The basic working principle behind these algorithms is as given below ((Patil, P., Sangeetha, M., & Bhaskar, V., 2021):

- Proof of Work (PoW) In PoW, nodes with more computing power administer the network.
- Proof of Stake (PoS) In PoS, nodes with more money administer the network.
- Proof of Authority (PoA) In PoA, arbitrarily chosen trustworthy nodes administers the network.
- Proof of Elapsed Time (PoET) In PoET, nodes who have finished a specific waiting period administer the network.
- Delegated Proof of Stake (DPoS) In DPoS, Nodes elected by delegates through voting administers the network.

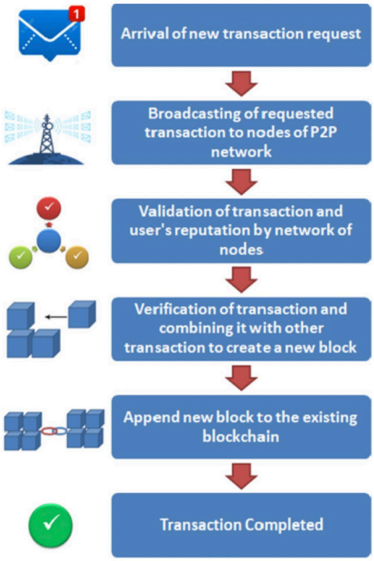
1
Arrival of new transaction request
Broadcasting of requested transaction to nodes of P2P network
Validation of transaction and user's reputation by network of nodes
Verification of transaction and combining it with other transaction to create a new block
Append new block to the existing blockchain
Transaction Completed

Fig. 3. General workflow of blockchain (Patil, P., Sangeetha, M., & Bhaskar, V., 2021)

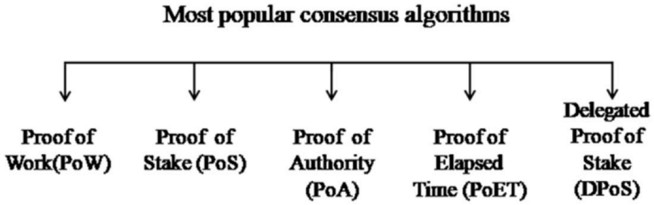
Most popular consensus algorithms
Proof of Work(PoW)
Proof of Stake (PoS)
Proof of Authority (PoA)
Proof of Elapsed Time (PoET)
Delegated Proof of Stake (DPoS)

Fig. 4. Most popular consensus algorithms (Patil, P., Sangeetha, M., & Bhaskar, V., 2021)

1.5. Functioning of the Blockchain

Since the publication of Bitcoin, the most famous peer-to-peer (P2P) payment system presented, in 2008, the concept of blockchain has spread worldwide. E blockchain technology is well known for leading to increased transparency, decentralization, and tamper resistance. In recent years, these benefits have motivated the broad application of blockchain to almost all industry segments, including cryptocurrencies, the Internet of ings, supply chain finance, social welfare, government affairs, and artificial intelligence. Blockchain (the technical logic architecture shown in Figure 5, including seven layers) is regarded as another disruptive technology after cloud computing, the Internet of ings, and Big Data. It is highly concerned by governments, financial institutions, and technology companies in various countries. However, the scalability issue of blockchain has always been the industry's focus, whether the era of large-scale commercial usage of blockchain comes. In particular, Bitcoin can only process 7 transactions per second, Ethereum can process 15 transactions per second, and EOS can process up to hundreds of transactions per second. ,e number of transactions that can be processed per second, that is, throughput is far from the actual transaction processing requirements. Improving transaction throughput has become a stuck-neck problem for blockchain to be implemented in multiple scenarios. By contrast, Visa can process 1 700 transactions per second. At is, the scalability issue of blockchain needs to be solved urgently.

In the past literature, scalability was not well defined. However, Vitalik Buterin, the co-founder of Ethereum (Xi, J., Zou, S., et al., 2021), firstly described the well-known scalability trilemma, stating that tradeoffs are inevitable between three significant properties of blockchain: decentralization, security, and scalability. Decentralization is the core and the intrinsic nature of blockchain, and security is an essential property, whereas scalability is the main challenge. We can only have two of either decentralization, security, or scalability simultaneously (i.e., we can pick just one side of the triangle shown in Figure 6). , us, tradeoffs are almost inevitable (Xi, J., Zou, S., et al., 2021).

2. Blockchain Ecosystem

Mempool is a memory block available on every single node on the network. The end users can initiate transactions in the blockchain ecosystem after creating a wallet. These transactions are kept on the mempool until picked and mined by the miners. A fee is

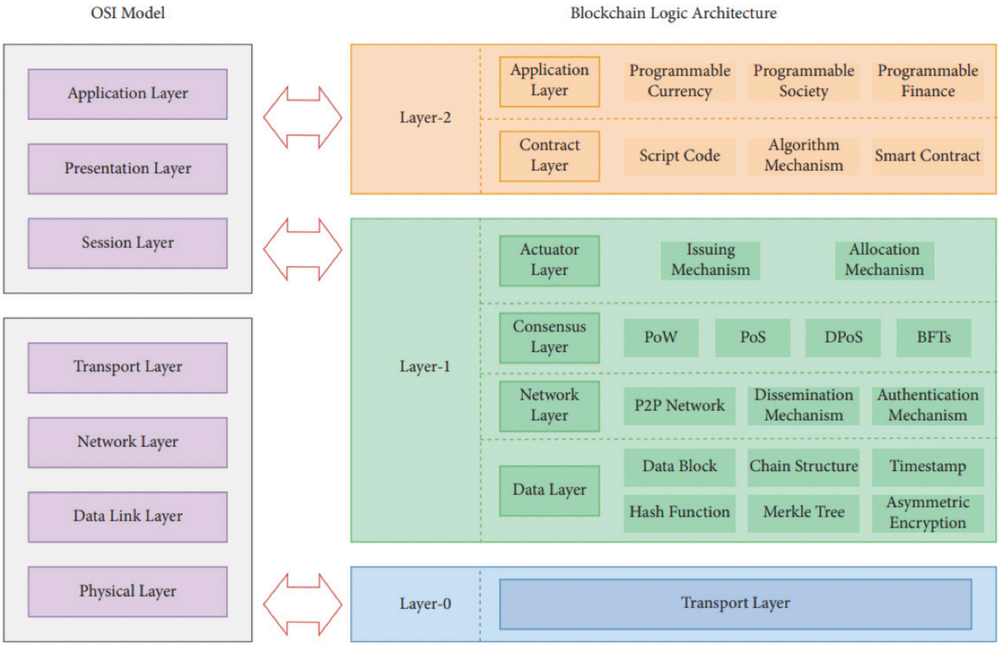

Fig. 5. Blockchain technical logic architecture (Xi, J., Zou, S., et al., 2021)

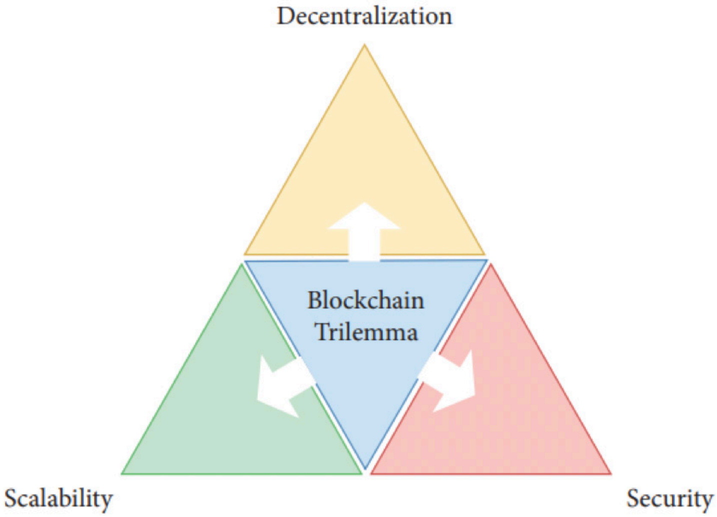

Fig. 6. Blockchain trilemma (Xi, J., Zou, S., et al., 2021).

associated with these transactions, and the miners pick high fee transactions from the mempool to put them on the block. A single block can accommodate approximately 2000 transactions. The blockchain ecosystem is depicted in Figure 7 (Kaushal, R. K., Kumar, N., & Panda, S. N., 2021, August).

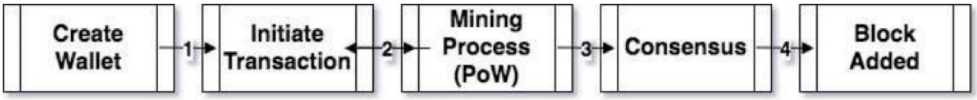

Fig. 6. Blockchain ecosystem (Kaushal, R. K., Kumar, N., & Panda, S. N., 2021, August).

Each block has a block number, protocol version, timestamp, previous block hash, nonce, difficulty target, transactions, and Merkle root. The Hash of a previous block is required to link all the blocks to form a chain. The transaction field holds transaction details, and the Merkle root is the cumulative Hash of these transactions. The timestamp file records the exact time when the block was mined. The nonce and difficulty target is the most important fields and vital for mining. The difficulty target is a hash with some leading zeros. The protocol sets these leading zeros, and more leading zeros make it more challenging to mine. In October 2020, the difficulty target was nineteen leading zeros. To successfully mine a block, the miners must find a nonce value (an editable field in the block), which then combines with the other fields to produce a cumulative hash just below the target difficulty.

This event is the cryptographic puzzle. To achieve this, the brute force technique requires millions and billions of iterations as the only way to find the correct nonce. These efforts are well known as Proof-of-Work (PoW). The verified mined block is broadcasted on the blockchain network to get the consensus. This event is accomplished with a consensus algorithm. Different protocols may use different consensus algorithms. Bitcoin protocol uses a Proof-of-Work consensus algorithm. At least 51% of nodes must verify and agree to add the newly mined block to the blockchain. Complex cryptographic puzzle and slow consensus algorithm is the primary cause of enormous electricity consumption and slow transaction rate. On average, every block in bitcoin is mined in approximately 10 minutes (Kaushal, R. K., Kumar, N., & Panda, S. N., 2021, August).

3. Types of Blockchain

Private and public blockchains are the two types of blockchains. However, there are many blockchains, such as consortium and hybrid ones. Before we go into the details of each blockchain, it is crucial to understand what they all have in common. Each blockchain comprises nodes connected by a peer-to-peer (P2P) network. Every node in a network has a copy of the shared ledger, which is updated regularly. Each node can validate transactions, send and receive them, and create blocks. To aid in comprehension, Figure 8 illustrates the various forms of blockchains (Joshi, S., Pise, A. A., et al., 2022).

Public Blockchain: A public blockchain is a distributed ledger technology that is permissionless and nonrestrictive. Anyone with access to the Internet can join a blockchain platform and become an authorized node, joining the blockchain network.

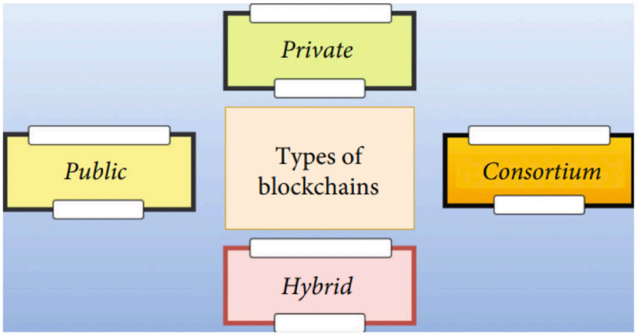

Fig. 8. Types of blockchains (Joshi, S., Pise, A. A., et al., 2022).

The following are the main characteristics of public blockchains (Joshi, S., Pise, A. A., et al., 2022):

- The primary purpose of public blockchains is to make Bitcoin mining and trading more accessible to the general population. On a public blockchain, a node or user can view current and historical data, validate transactions, conduct proof-of-work on incoming blocks, and mine. As a result, Bitcoin and Litecoin have become the most widely utilized public blockchains.
- Public blockchains are frequently secure if users strictly follow security rules and procedures. However, it is only dangerous when players do not strictly follow the security procedures.
- People from all walks of life can join, transact, mine, and read and write on the blockchain in this category. None of these variables are constrained, and anyone using permissionless blockchains is free to conduct transactions, keep a copy of the distributed ledger, and participate in verifying and adding new blocks to the chain.
- Furthermore, the blockchain is decentralized and transparent; no preset group of validators exists, and any user can contribute new blocks to the network by solving computationally complex puzzles or staking their own money. Because each node keeps a full copy of the blockchain, it is secure and immutable.
- Moreover, because each transaction is associated with a processing fee, this sort of blockchain is resistant to tampering, preventing the public ledger from being hacked because changing its contents would be prohibitively expensive.

Private Blockchain: This type of blockchain is frequently used to enable private data sharing and trade among known members of a specific organization. Because external users cannot access or participate in private blockchains unless they have been granted permission, they are also known as permissioned blockchains. The following are the primary characteristics of private blockchains:

- Rules or an access-controlling network controls users' involvement. This event concentrates the network while weakening the purported key blockchain characteristics of complete decentralization and openness.
- When nodes join a private blockchain system, they contribute to the network's

decentralized operation by keeping a copy of the ledger and working together to establish consensus on updates. (c) However, unlike public blockchains, writing is limited. A private blockchain is a permission-based or restricted blockchain that only exists within a closed network.

- Private blockchains are widely used within organizations or enterprises because only a few individuals participate in the blockchain network. The controlling organization determines the amount of security, authorizations, permissions, and accessibility.
- As a result, private blockchains operate similarly to public blockchains but with a more limited network. Private blockchain networks are used for various purposes, including voting, supply chain management, digital identity, and asset ownership.

Hybrid Blockchain: A hybrid blockchain combines private and public ledgers into a single digital ledger. The following are the primary characteristics of hybrid blockchains (Joshi, S., Pise, A. A., et al., 2022):

- It combines the benefits of both blockchains, allowing for private and public permission-based systems.
- By utilizing a hybrid network, users can control who has access to which data is stored on the blockchain.
- Only a subset of the data or records on the blockchain may be made public, with the remainder remaining private on the private network.
- The hybrid BCT is adaptable, allowing users to connect a private blockchain to several public blockchains easily.
- A transaction on a hybrid blockchain's private network is frequently confirmed within that network. Users can verify it by putting it on the public blockchain.
- Public blockchains increase the number of nodes involved in the verification process and improve hashing. This event improves the blockchain network's security and transparency.

Consortium Blockchain: A consortium blockchain is a semi-decentralized blockchain in which multiple entities administer the network. Several companies may operate as nodes in this blockchain, exchanging data and mining. On the other hand, a private blockchain was discovered to be owned by a single company. Financial companies, government agencies, and similar organizations frequently employ consortium blockchains. The following are the main characteristics of consortium blockchains (Joshi, S., Pise, A. A., et al., 2022):

- This event is a partially private and permissioned blockchain in which a preselected collection of nodes controls the consensus process and block validation rather than a single entity.
- These nodes determine who is allowed to join the network and participate in the consensus process. Due to the control exercised by a few selected validator nodes, it is a relatively centralized system.
- This type of blockchain, like private blockchains, has no processing fees, and publishing new blocks is computationally simple.
- While it provides auditability and decreased transaction latency because most

nodes control the consortium, it does not entirely ensure immutability and irreversibility, which could lead to blockchain manipulation.

Finally, we want you to use your knowledge to determine which blockchain is best for you. If you are part of a public blockchain network, all you have to do now is figure out how it works so you can make informed decisions in the future (Joshi, S., Pise, A. A., et al., 2022).

4. Characteristics of blockchain

As mentioned, blockchain is Bitcoin's underlying technology and facilitates transactions that occur within a global peer-to-peer network in a decentralized fashion. That makes Bitcoin a borderless, censorship-resistant digital currency. Blockchain is a trustless system that provides trust through the functions that propagate all the activities within the network. In general, the trust may be the primary concern regarding traditional centralized systems, such as banks, where people must put their solemn confidence in the system. This event is the sweet spot for public blockchain technology in that it does not require any trust while handing over the ownership of digital assets from one peer to another. Below are the characteristics of blockchain (Monrat, A. A., Schelén, O., & Andersson, K., 2019):

Decentralization: in conventional centralized transaction systems, each transaction must be validated through the central trusted agency (e.g., the central bank). Therefore, decentralization requires trust, which is the main issue, along with lift resilience, availability, and failover, where the decentralized peer-to-peer blockchain architecture could be a better solution. Unlike a centralized system, a transaction in the blockchain network can be conducted between any two peers (P2P) without authentication by the central agency. In this manner, blockchain can reduce the trust concern by using various consensus procedures. Moreover, it can reduce server costs (including development and operation costs) and mitigate the performance bottlenecks at the central server. In contrast, in many cases, blockchain has some tradeoffs. For example, in PoW cases such as Bitcoin and Ethereum, the server and energy cost are orders of magnitude higher, while the performance is also several orders of magnitude lower.

Persistency: blockchain provides the infrastructure by which truth can be measured and enables the producers and consumers to prove their data are authentic and not altered. For example, if a Blockchain consists of 10 blocks, then block no. 10 contains the Hash of the previous subsequent block, and the information of the current block is used to create a new block. Therefore, all the blocks are linked and connected in the existing chain. Even the transactions are related to the prior transaction. A simple update on any transaction significantly changes the block's Hash. If someone wants to modify any information, he has to change all the previous block's hash data, which is considered an astronomically tricky task considering the amount of work needed. In addition, after generating a block by a miner, it is confirmed by other users in the network. Hence, the network detects any manipulation or falsification of data. For this reason, blockchain is almost tamper-proof and considered an immutable distributed ledger.

Anonymity: it is possible to interact with the blockchain network with a randomly generated address. Blockchain provides a certain amount of anonymity through its trustless environment. A user can have many addresses within a Blockchain network to avoid the exposure of his identity. As it is a decentralized system, no central authority monitors or records users' private information.

Auditability: All transactions in a blockchain network are recorded by a digital distributed ledger and validated by a digital timestamp. As a result, it is possible to audit and trace 117138 VOLUME 7, 2019 A. A. Monrat et al.: Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities previous records by accessing any node in the network. For example, all the transactions could be traced iteratively in Bitcoin, which facilitates the blockchain's auditability and transparency of the data state. However, tumbling money through many accounts makes it tough to trace the money to its origin.

5. Challenges

Blockchain technology can also be used in various fields of business. One exciting implementation of Blockchain technology is in the healthcare system. This event satisfies all stakeholders such as Hospitals, Healthcare, and Health Authorities by meeting information consumers' needs and protecting patient privacy by using blockchain to pay fees with Bitcoin. In the paper system, if information consumers need to see a patient's health record, they must fill in a request form and send it to the registration office for approval. After receiving approval, the information consumer pays a copy fee to the cashier and obtains a bill of receipt. The information consumer then shows the receipt to the registration office to obtain a copy of the patient's health record. However, a patient's health records can be lost, or copies may be made for illegal purposes. The concept of an electronic health records system using Blockchain technologies is depicted in Figure 9 (Tasatanattakool, P., & Techapanupreeda, C., 2018, January).

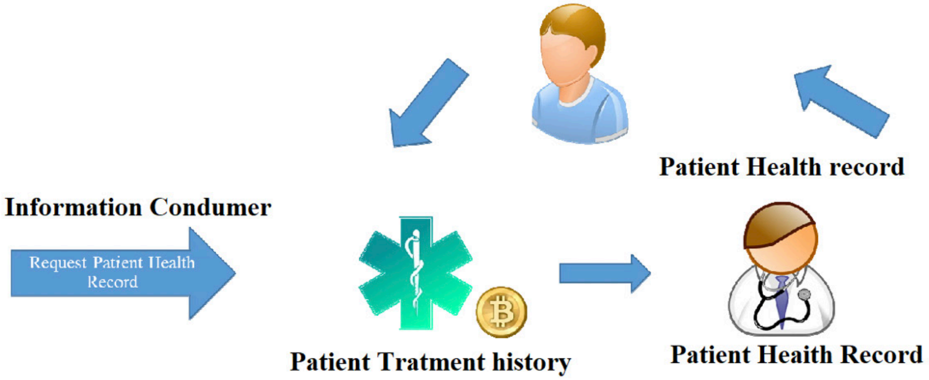

Fig. 9. E-health system using Blockchain (Tasatanattakool, P., & Techapanupreeda, C., 2018, January)

When an information consumer requests a patient's health records to an issuer (hospital or healthcare), and the issuer agrees with the information consumer, the Bitcoin is placed. Before sending a patient's health records to an information consumer, approval from a primary doctor and the patient is needed so that only specific records are sent, for example, mental health records. The details of this process are explained in subsequent research (Tasatanattakool, P., & Techapanupreeda, C., 2018, January).

As an emerging technology, blockchain is facing multiple challenges and problems. Three other blockchain challenges are mentioned below (Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H., 2018):

Scalability: The blockchain becomes heavy with the number of transactions increasing daily. Currently, the Bitcoin blockchain has exceeded 100 GB of storage. All transactions have to be Stored for validating the transaction. Besides, due to the original restriction of block size and the time interval used to generate a new block, the Bitcoin blockchain can only process nearly 7 transactions per second, which cannot fulfill the requirement of processing millions of transactions in a real-time fashion. Meanwhile, as the capacity of blocks is tiny, many small transactions might be delayed since miners prefer those transactions with a high transaction fee. However, a large block size would slow the propagation speed and lead T to blockchain branches. So scalability problem is quite challenging. There are many efforts proposed to address the scalability problem of the blockchain, which could be categorized into two types (Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H., 2018):

- Storage optimization of blockchain. To solve the bulky blockchain problem, a novel
- A cryptocurrency scheme was proposed by (Bruce, 2014). In the new scheme, old
- The network removes transaction records, and a database named account tree is
- Used to hold the balance of all non-empty addresses. In this way, nodes do not need
- To store all transactions to check whether a transaction is valid or not. Besides
- The lightweight client could also help fix this problem. A novel scheme named VerSum
- (van den Hooff et al., 2014) was proposed to provide another way of allowing
- L lightweight clients to existing. VerSum allows lightweight clients to outsource expensive
- C computations over significant inputs. It ensures that the computation result is correct by comparing results from multiple servers.
- Redesigning blockchain. in Eyal et al. (2016), Bitcoin-NG (Next Generation) was
- Proposed. The main idea of Bitcoin-NG is to decouple conventional blocks into two
- P parts: fundamental block for leader election and macroblock to store transactions. Miners are

- Competing to become a leader. The leader would be responsible for the macroblock
- G generation until a new leader appears. Bitcoin-NG also extended the heaviest
- (longest) chain strategy where only critical blocks count and micro blocks carry no
- W weight. In this way, blockchain is redesigned, and the tradeoff between block size and
- Network security has been addressed.

Privacy: leakage in the blockchain is believed to be very safe as users only make transactions with generated addresses rather than real identities. Users also could generate many addresses in case of information leakage. However, it is shown in (Meiklejohn, S., Pomarole, M., et al., 2013, October) and (Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C., 2016, May) that blockchain cannot guarantee transactional privacy since the values of all transactions and balances for each public key are publicly visible. Besides, a recent study (Barcelo, J., 2014) has shown that a user's Bitcoin transactions can be linked to reveal the user's information. Moreover, (Biryukov, A., Khovratovich, D., & Pustogarov, I., 2014, November) presented a method to link user pseudonyms to IP addresses even when users are behind network address translation (NAT) or firewalls. In (Biryukov, A., Khovratovich, D., & Pustogarov, I., 2014, November), each client can uniquely identified by a set of nodes it connects. However, this set can be learned and used to find the origin of a transaction. Multiple methods have been proposed to improve the anonymity of blockchain, which could be roughly categorized into two types (Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H., 2018):

- Mixing (Moser, M., 2013) In the blockchain, users' addresses are pseudonymous. But it is still possible to link addresses to the user's real identity as many users make transactions with the same address frequently. A mixing service is a kind of service that provides anonymity by transferring funds from multiple input addresses to multiple output addresses. For example, user Alice with address A wants to send some funds to Bob with address B. If Alice directly makes a transaction with input address A and output address B, the relationship between Alice and Bob might be revealed. So Alice could send funds to a trusted intermediary, Carol. Then Carol transfers funds to Bob with multiple inputs c1, c2, c3, and multiple outputs d1, d2, B, and d3. Bob's address B is also contained in the output addresses. So it becomes harder to reveal the relationship between Alice and Bob. However, the intermediary could be dishonest and reveal Alice and Bob's private information on purpose. It is also possible that Carola transfers Alice's funds to her address instead of Bob's address.
- Bitcoin (Bonneau, J., Narayanan, A., et al., 2014, March) provides a simple method to avoid dishonest behaviors. The intermediary encrypts users' requirements, including funds amount and transfer date, with its private key. Then if the intermediary did not transfer the money, anybody could verify that the intermediary cheated. However, theft is detected but still not prevented. Coinjoin depends on a central mixing server to shuffle output addresses to prevent theft. And inspired by Coinjoin, CoinShuffle

(Ruffing et al., 2014) uses decryption mix nets for address shuffling.

• *Anonymous.* In Zerocoin, a zero-knowledge proof is used. Miners do not have to validate a transaction with a digital signature but to validate coins that belong to a list of valid coins. Payment's origin is unlinked from transactions to prevent transaction graph analyses. But it still reveals payments' destination and amounts. Zerocash was proposed to address this problem. In Zerocash, zero-knowledge Succinct Non-interactive Arguments of Knowledge (zk-SNARKs) are leveraged. Transaction amounts and the values of coins held by users are hidden.

Selfish mining: the blockchain is susceptible to attacks of colluding selfish miners. Generally, it is convinced that nodes with over 51% computing power could reverse the blockchain and the happened transaction. However, recent research shows that even nodes with less than 51% power are still dangerous. In particular, Eyal and Sirer (Eyal, I., & Sirer, E. G., 2018) showed that the network is vulnerable even if only a tiny portion of the hashing power is used to cheat. In a selfish mining strategy, selfish miners keep their mined blocks without broadcasting, and the private branch would be revealed to the public only if some requirements are satisfied. As the private branch is longer than the current public chain, it would be admitted by all miners. Before the private blockchain publication, honest miners waste resources on a useless branch while selfish miners are mining their private chain without competitors. So selfish miners tend to get more revenue. Rational miners would be attracted to join the selfish pool, and the selfish could exceed 51% power quickly.

Based on selfish mining, many other attacks have been proposed to show that blockchain.

The trail-stubbornness is one of the stubborn strategies that miners still mine the blocks even if the private chain is left behind. In stubborn mining, miners could amplify their gain by non-trivially composing mining attacks with network-level eclipse attacks. Yet, in some cases, it can result in 13% gains compared to a non-trail-stubborn counterpart. Sapirshtein et al. (Sapirshtein, A., Sompolinsky, Y., & Zohar, A., 2016, February) show that selfish mining strategies' gains are relatively small.

Furthermore, it shows that attackers with less than 25% of the computational resources can still gain from selfish mining. To help fix the selfish mining problem, Heilman (Heilman, E., 2014, March) presented a novel approach for honest miners to choose which branch to follow. With random beacons and timestamps, honest miners would select more new blocks (Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H., 2018).

6. Conclusions

Blockchain has numerous benefits, such as decentralization, persistency, anonymity, and auditability. There is a broad spectrum of blockchain applications ranging from cryptocurrency, financial services, risk management, Internet of things to public and social services. Blockchain technology has attracted considerable interest in the last 15 years. It is argued that blockchain can sustain any transaction of value, be it monetary or information, in a manner that is secure and independent of interpersonal trust. Yet, there remains little understanding of whether and how this technology enables trust-free transactions. Blockchain has been increasingly used as a software component to enable decentralization in software architecture for various applications. Blockchain governance has received considerable attention to ensure blockchain's safe and appropriate use and evolution, especially after the Ethereum DAO attack in 2016. However, there are no systematic efforts to analyze existing governance solutions. Furthermore, it highlights the critical challenges in blockchain implementation and the potential of blockchain in managing the business. This technology, like the others, has challenges that are discussed in this study on the general concepts and challenges of blockchain.

References

Aghababayi, H., Nikabadi, M. S., Kafaki, S. B., & Rahmanimanesh, M. (2022). Challenges of using blockchain technology in the international markets. *Journal of Information Technology Management, 14*(Special Issue: The business value of Blockchain, challenges, and perspectives), 171-191.

Barcelo, J. (2014). User privacy in the public bitcoin blockchain. *URL: http://www. dtic. upf. edu/jbarcelo/papers/20140704 User Privacy in the Public Bitcoin Blockc hain/paper. pdf (Accessed 09/05/2016).*

Biryukov, A., Khovratovich, D., & Pustogarov, I. (2014, November). Deanonymisation of clients in Bitcoin P2P network. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (pp. 15-29).

Bonneau, J., Narayanan, A., et al. (2014, March). Mixcoin: Anonymity for bitcoin with accountable mixes. In *International Conference on Financial Cryptography and Data Security* (pp. 486-504). Springer, Berlin, Heidelberg.

Eyal, I., & Sirer, E. G. (2018). Majority is not enough: Bitcoin mining is vulnerable. *Communications of the ACM, 61*(7), 95-102.

Gamage, H. T. M., Weerasinghe, H. D., & Dias, N. G. J. (2020). A survey on blockchain technology concepts, applications, and issues. SN Computer Science, 1(2), 1-15.

Guo, H., & Yu, X. (2022). A Survey on Blockchain Technology and its security. *Blockchain: Research and Applications, 3*(2), 100067.

Heilman, E. (2014, March). One weird trick to stop selfish miners: Fresh bitcoins, a solution for the honest miner. In *International Conference on Financial Cryptography and Data Security* (pp. 161-162). Springer, Berlin, Heidelberg.

Joshi, S., Pise, A. A., et al. (2022). Adoption of Blockchain Technology for Privacy and Security in the Context of Industry 4.0. *Wireless Communications and Mobile Computing, 2022.* 4079781

Kaushal, R. K., Kumar, N., & Panda, S. N. (2021, August). Blockchain Technology, Its Applications and Open Research Challenges. In *Journal of Physics: Conference*

Series (Vol. 1950, No. 1, p. 012030). IOP Publishing.

Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016, May). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In *2016 IEEE symposium on security and privacy (SP)* (pp. 839-858). IEEE.

Meiklejohn, S., Pomarole, M., et al. (2013, October). A fistful of bitcoins: characterizing payments among men with no names. In *Proceedings of the 2013 conference on Internet measurement conference* (pp. 127-140).

Monrat, A. A., Schelén, O., & Andersson, K. (2019). A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access, 7,* 117134-117151.

Moser, M. (2013). Anonymity of bitcoin transactions. In Münster Bitcoin Conference (MBC), 10 pages

Pal, A., Tiwari, C. K., & Haldar, N. (2021). Blockchain for business management: Applications, challenges and potentials. The *Journal of High Technology Management Research, 32*(2), 100414.

Patil, P., Sangeetha, M., & Bhaskar, V. (2021). Blockchain for IoT access control, security and privacy: a review. *Wireless Personal Communications, 117*(3), 1815-1834.

Sapirshtein, A., Sompolinsky, Y., & Zohar, A. (2016, February). Optimal selfish mining strategies in bitcoin. In *International Conference on Financial Cryptography and Data Security* (pp. 515-532). Springer, Berlin, Heidelberg.

Tasatanattakool, P., & Techapanupreeda, C. (2018, January). Blockchain: Challenges and applications. In *2018 International Conference on Information Networking (ICOIN)* (pp. 473-475). IEEE.

Xi, J., Zou, S., et al. (2021). A Comprehensive Survey on Sharding in Blockchains*. Mobile Information Systems, 2021.* 5483243

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), 352-375.

Submitted: 14.01.2022
Accepted: 10.05.2022