Journal of Engineering Science and Technology Review 17 (3) (2024) 201- 216

Review Article

JOURNAL OF
**Engineering Science
and Technology Review**

www.jestr.org

Exploring the Landscape of Blockchain Technology: History, Applications, Challenges and Future Directions

Debarati Dutta and Priya G. *

School of Computer Science and Engineering, VIT, Vellore, Tamil Nadu - 632014, India.

Received 17 November 2023; Accepted 3 January 2024

Abstract

In several companies throughout the world, blockchain technology is gaining greater attention and implementation. In this article, first of all, we conduct an in-depth survey of blockchain technology, focusing on its history, phases, types, technologies, consensus algorithms, frameworks, and layers. Further, it describes its extensive list of applications for blockchain in several industries, including asset management, stock exchange, healthcare, insurance, digital identity, data storage and management, IoT, supply chain, voting, DNS services, etc. Blockchain has various advantages, including decentralisation, anonymity, immutability, integrity, auditability, and transparency. These features encourage the adoption of blockchain in every sector. In spite of these advantages, it has some challenges which as not letting it to accepted by common people. In this paper, we describe those challenges into two categories: security and attacks on blockchain and explain them thoroughly. Unlike other blockchain documents that focus on topics like cryptocurrencies, IoT, and security, this paper highlights the cutting-edge advancements and widespread implementation of blockchain technology, particularly in areas beyond digital currencies. Finally, it discusses the potential future research areas and objectives for blockchain technology.

Keywords: Consensus mechanisms, Smart contracts, Security issues, Blockchain attacks.

1. Introduction

Blockchain can be defined as a continuously growing chain of blocks or records maintained in a distributed ledger. Whenever a new record comes, it is added to the new block and that new block is added at the end of the chain. Except for the first (Genesis) block, every block contains a block number, the previous block's hash value, and nonce as a difficulty value. Besides these, it contains timestamp and data. Blockchain is created using Merkle tree structure and consensus protocol, which describe how data or transactions are added to the block and how that can be verified. Blockchain is a disruptive technology, that is going to be implemented in every sector. Nowadays the Internet has access to every sector. But there is one problem with the internet which is trust. This problem will be solved by blockchain technology easily.

Due to the rapid usage of blockchain technology, a lot of review papers are available, which have examined the technology in a variety of depths and contexts. The majority of these analyses or reviews concentrate on cryptocurrencies, consensus protocols, IoT integration, and the security concerns of various blockchain-based applications[1]–[4]. Many surveys are available where a single subject or a small number of topics are solely taken into account, some of them identify few drawbacks, and some of them have shown ways to overcome those. This article presents a broad and detailed picture of blockchain technology, concentrating particularly on security issues, its challenges, cryptography in the blockchain, and various attacks. This article examines the progress and current status of blockchain technology, as well as recent developments in its utilization and integration beyond cryptocurrency.

The remaining sections are structured in the following manner: Section 2 outlines the fundamentals and characteristics of blockchain technology, encompassing its generational evolution, various types, forks, and an overview of blockchain nodes. In Section 3 we describe the technologies and frameworks used in Blockchain like consensus algorithms, smart contracts, and its layers. Then Section 4 gives some idea about the blockchain applications. Security issues and various attacks on blockchain are described in Section 5. To demonstrate our contribution, Section 6 summarises the relevant survey works. Section 7 delves into potential future trajectories, while Section 8 brings the entire paper to a close.

2. Overview of the Blockchain:

David Chaum was the pioneer to propose a system resembling blockchain in his 1982 doctoral thesis [5]. Subsequently, the concept of a cryptographically secured chain of blocks was put forth by W. Scott Stornetta and Stuart Haber in 1991 [6]. After that Merkle trees were included in the design by Dave Bayer and his team in 1993 [7]. Szabo developed the decentralized digital money system known as "bit gold" in 1998 [8]. However, it wasn't until 2008, with the introduction of Bitcoin by Satoshi Nakamoto, that blockchain technology truly gained prominence [9]. Blockchain was the backbone of Bitcoin, cryptocurrency, and its applications [10]. Then it does not become restricted to the financial sector, slowly its application extends beyond the cryptocurrency and spreads to every sector of science where trust problem is involved. Today, blockchain technology has permeated every sector. Its

*E-mail address: gpriya@vit.ac.in

ISSN: 1791-2377 © 2024 School of Science, DUTH. All rights reserved.
doi:10.25103/jestr.173.21

widespread appeal stems from the fact that this open, distributed ledger system fosters decentralization, maintains data integrity, and ensures transparency.

2.1 Phases of Blockchain

The open-source nature of Bitcoin's code, allowed other programmers to update and enhance it. There have been several stages of development for blockchain technology [11].

Blockchain 1.0 generation:

The first iteration of blockchain technology is centered around digital currency, facilitated by the adoption of Distributed Ledger Technology (DLT). Bitcoin is the digital money that initially made blockchain technology known to the world. A complicated set of cryptographic techniques is used to link the blocks together, where transaction data is kept in encrypted form. Using PoW technology, several other digital currencies have developed in the blockchain.

Blockchain 2.0 generation:

Second-generation digital currencies were expanded by smart contracts, which created a digital economy. The smart contract will be automatically executed or activated by a transaction when the buyer and seller are satisfied with an agreement. Since the code is public and verifiable, it facilitates easier scrutiny by other nodes, enabling them to anticipate contract outcomes. Smart contracts find application in a range of industries like corporate agreements, mortgages, insurance, and supply chains. Ethereum is notably the leading blockchain platform in the phase 2.0 context.

Blockchain 3.0 generation:

The third-generation expands a wide range of non-financial and non-monetary uses. It avoids centralised infrastructure and concentrates on decentralized applications, which in contrast to conventional applications, communicate and store data via decentralised servers and storage. By utilising resources wisely, it creates smart cities with the facility of smart governance that in turn creates a smart economy. In order to conduct smart transactions and payments without the assistance of third parties, the integration of IoT with blockchain has been done. Blockchain 3.0's objective was to spread awareness of blockchain technology in established industries including government, healthcare, and education.

Blockchain 4.0 generation:

It offers strategies and tactics that may satisfy a number of business requirements of Industry 4.0, which include resource planning, automation, and integration of diverse execution programs.

2.2 Types of Blockchain

Blockchain manifests in diverse forms, contingent on factors like its purpose, network scale, employed consensus mechanism, availability, and user accessibility. The most prevalent blockchain varieties that are on the market are listed below:

Public: - A public blockchain is one where anyone can participate without restriction or permission. Most of the cryptocurrencies run on this platform. Anyone may join, view or publish their data as it is an open and decentralised ledger. It uses a public distributed ledger technology, allowing anybody with internet access to sign up and become a legitimate miner for a block. On the public blockchain also, the identity of the user address is created by a hash value that is pseudo-anonymous. Fully decentralised public blockchains are susceptible to 51% attacks, selfish mining, and privacy concerns[12],[13]. Currently, the widely recognized public blockchains encompass Litecoin [14], Bitcoin [9], and Ethereum (public) [15].

Private: - A private blockchain is alternatively labeled as a permissioned or restricted blockchain. It is a closed network that is distributed but centralised, which is used to operate it on the basis of a few access control principles. This private blockchain is the complete opposite of public blockchain, where anyone needs permission to participate, as the full control is restricted to a single person or organization. Although security risk is higher in this kind of blockchain, but the handling of the documents is easy and it has low transaction costs. Typically, a private blockchain is utilised by a single corporation with discrete departments that may function as blockchain nodes for the automation of business processes.

The private blockchain is more scalable. It has no difficulties with the 51% attack, selfish mining, and privacy concerns while being less secure and centralised. A trusted third-party organisation has control over the security, availability, authorization, and permissions. It finds application in various scenarios such as electronic voting, supply chain management, digital identity verification, data conservation, and managing asset ownership, among others. Some examples of this blockchain include Quorum [16], Hyperledger Fabric [17], Blockstack, and Multichain [12].

Consortium: - It is also known as federated Blockchain. This kind of blockchain may be described as being both partially centralised and partially decentralised. It is employed by several organisations rather than just one. It is not possible to directly access the network without being a member previously, because it is only open to groups of already registered nodes. One organisation cannot engage in illegal behaviour on a consortium blockchain, since it is impossible to carry out any action without the cooperation of other entities. Here security risk is lower than in private blockchain.

Consortium blockchains as a whole were developed to support enterprise collaboration for business improvement. It is commonly employed by financial institutions, governmental bodies, and similar entities. Independent companies that share information without much confidence utilise consortium blockchains. However, they do not experience a 51% attack and have fewer privacy and security problems. Corda [18], and Hyperledger [19], Energy Web Foundation [20] are examples of consortium blockchains.

Table 1. Comparing different blockchain categories

Property	Private	Public	Consortium
Permission	Required	Not required	Required
Security	High	Highest	Higher
Scalability	Low	High	Average
Centralization	Centralized	Decentralized	Partial
Efficiency	Enhanced	Limited	Elevated
Read access	Open/Restricted	Open	Open/Restricted
Consensus Establishment	Restricted to organization	Entire miner network	Selected node group
Examples	Ripple, Blockstack	Bitcoin, Ethereum	Corda, Quorum
Application	Electronic voting	Cryptocurrency	Banks

Tab. 1 outlines the distinctions between the three categories of blockchains: public, private, and consortium.

The combination of the private and public blockchain can be considered as a hybrid blockchain where users can control access. In this blockchain's operation, only a specific portion of data or records is permitted to be public, while the remaining information is kept confidential within the private network. The adaptability of hybrid blockchain technology is evident as users can seamlessly integrate multiple public blockchains with a private one.

Tab. 2 provides a comparative analysis of different blockchain platforms, namely Bitcoin, Ethereum, and Hyperledger Fabric. The main function of Bitcoin is to store transaction data and work as cryptocurrency. Anyone may take part as it is written in script and has open-source access on GitHub. It relies on Bitcoin (BTC) as its core currency, featuring a block release interval of 10 minutes, an average transaction size of 250 bytes, and a transaction rate of 3 transactions per second (TXN/sec). Proof of Work serves as the foundation for Bitcoin mining. Whereas the main function of Ethereum is to perform and store smart contracts and to keep digital assets and transaction data. Anyone can participate here also by accessing the source code through GitHub and it is built in Solidity or Serpent. It uses Ether (ETH) as its primary currency with a block release time of 12 seconds. The Ethash method is used for Proof of Work mining in Ether. The main function of Hyperledger fabric is to create an industrial blockchain, as well as the storage of smart contracts and chain codes. Anybody may take part after registration for identification to network and it is developed in the Go programming language.

Table 2. Comparative analysis of various blockchain platforms

Types	Bitcoin	Ethereum	Hyperledger fabric
Purpose	Cryptocurrency	Run smart contracts	Create for industries
Type of data store	Transactions	Digital assets, smart contracts, records	Chain code, smart contracts
Language	Script	Solidity, serpent	Go
Permission	Open to everyone	Open to everyone	Not open to everyone
Participate through	Github source code	Github source code	User source code, registration
Block release timing	10 minutes	12 second	Configurable
Native currency	Bitcoin (btc)	Ether (eth/etc)	N/a
Managed public key infrastructure	Not supported	Not supported	Not supported
Average transaction size	250 bytes	No theoretical maximum	Customizable
Mining	Proof of work	Proof of stake	Not applicable
Transaction rate	3 TXN/sec	Theoretically unbounded	Surpassing 10,000 TXN/sec

2.3 Key Characteristics

Blockchain has advantageous qualities that make it useful. The success of Bitcoin has given focus to the power and potential characteristics of blockchain. By April 2021, the market capitalization of Bitcoin had surged to an unprecedented level, exceeding a trillion USD in growth [21]. Following are notable characteristics, qualities, and the importance of blockchain.

Distributed:
Blockchain networks follow the Distributed Ledger Technology (DLT) where various users or nodes simultaneously store the blockchain data. Since there is a copy of the blockchain with other nodes on the network, if one node malfunctions or loses its data it can recollect the block again from other nodes of the network. This function stops double-spending in bitcoins, data loss, and record manipulation.

Decentralization:
Blockchain eliminates the need for central authority and intermediaries, rendering it well-suited for trustless systems. This allows systems to operate autonomously and without reliance on a central authority, which typically entails verification and validation, leading to heightened computational expenses and communication delays. Every member of this distributed network, or node, actively engages in transactions due to this decentralised server [22]. However, although being partially or completely centralized, private blockchains are still beneficial from other blockchain capabilities.

Immutability and integrity:
Prior to inclusion in the block, the data undergoes a verification process [23]. Subsequently, transactions are permanently inscribed on the blockchain. The information within each block remains immutable [24]. The data in every block is interlinked by a hash key, and altering the data would render subsequent blocks invalid. This ensures that any endeavor to tamper with the data would be promptly discerned. A vast blockchain network makes it nearly implausible for an adversary to prevail, as they would need to modify the data of individual nodes across multiple blocks.

Traceability and transparency:
All the records and transactions are transparent to every node on the network as records have a time-stamp and it maintained in all the full nodes of the network. All nodes of any network can access this data since it is trustworthy and available to all of them. Each block is connected to the preceding blocks by their hash key in the blockchain network [25]. It also makes it appropriate as a tool of audit that provides public services, as well as detects fraud [25], [26].

Efficiency:
By eliminating intermediary subsystems, blockchain enables independent and more streamlined operations. This sought-after advantage has prompted many companies across various countries to adopt blockchain technology.

Interoperability:
Blockchain provides a secure platform for sharing data, allowing for secure service synchronization and data exchange among different parties. This feature is particularly valuable for businesses like banks and insurance companies, as it facilitates the exchange of data to improve interoperability [27].

Anonymity:

Data security on the blockchain is achieved through the use of asymmetric encryption methods. Every payment has a digital signature to verify the recipient. The sender employs the blockchain to generate a distinctive set of addresses, ensuring their identity remains confidential. Consequently, a centralized authority safeguards the genuine identities of users and takes all necessary measures to safeguard the sender's anonymity from disclosure [28].

2.4 Fork

As a public blockchain is a decentralised network, all the participants of that network have to agree on the shared state. When most of the nodes in the network agree, then a single blockchain is created with verified data that the network claims to be valid. But sometimes the network nodes are unable to agree on a single position on the blockchain's future state. This kind of situation is known as forking, which is the point from where a single ideal chain breaks into more than one equally valid chain of blocks. The following diagram Fig. 1 describes different types of forks.

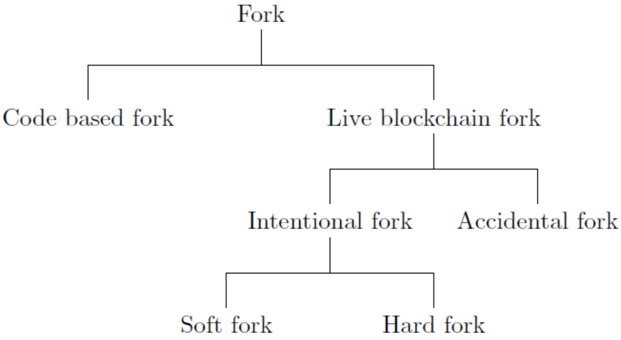

Fig. 1. Types of fork

As per the diagram, we can see that fork can be categorised broadly in two ways. Those are code-based fork and live blockchain fork. Due to a code-based fork new blockchain can be created starting from the blank ledger. It leads to changes in the coding of old cryptocurrency and new cryptocurrency is created. Some examples of code-based fork are Doge and Litecoin. Whereas, in a live blockchain fork both the chains share the history of the ledger till the fork. The Live blockchain fork can be intentional or accidental. If two miners mine blocks at the same time then it is categories as the accidental fork, which can be solved using longest chain rules. The intentional fork can be further divided into soft fork and hard fork. In soft fork new rules do not clash with the old rules and rules are tightened. Previously valid rules become invalid here, like a software update. But in the case of a hard fork new rules clash with the old rules and rules are loosened here. Due to this kind of fork previously invalid rules become valid here and a new cryptocurrency is made. Examples of hard fork are Bitcoin Cash, Ethereum Classic, etc.

2.5 Nodes in Blockchain

The computer device that operates on the blockchain environment and take part in P2P (peer-to-peer) networks are known as nodes in the blockchain network. Based on the service and functionality, these nodes can be classified. Those are:

Full nodes:

A full node authenticates recently added blocks and links them across the blockchain network upon publication. When publishing, it is their duty to authenticate transactions up to the Genesis block. A node earns the designation of a super node based on the volume of transactions a full node generates. Super Nodes interconnect all remaining full nodes, ensuring their connection and distribution across the network.

Light Nodes:

Light nodes behave similarly to full nodes; however, they only hold a small percentage of the entire block. If a full node becomes hacked and retains damaged data, then the light node can provide all the information regarding the node which helps to decide what should be kept and it can reject the fake blockchain. This helps the network to become more decentralized as they don't take up much data space, and they can travel far distances for less cost as compared to full nodes.

Mining nodes:

The creation of blocks within the blockchain is consistently carried out by mining nodes. These nodes, also called miners, are solely responsible for confirming which blocks should be incorporated into the list during the mining process, without any obligation for maintenance.

Broadcast nodes:

These nodes carry out the blockchain's operating protocols, verify, and disseminate the transaction records, and block data.

3. Technologies in Blockchain

3.1 Consensus Mechanisms

The structure of a blockchain resembles a linked list, where each new block is attached to the one before it. Every node in the network must confirm the validation of a block before it can be added to the blockchain. Consensus is an algorithm that facilitates cooperation among network nodes to establish the sequence for processing transactions and identify and eliminate fraudulent ones. The consensus protocol in the blockchain is a set of broad guidelines that all of the nodes follow to synchronize, update and maintain the blockchain network and ledger. Additionally, the decentralized nature of the blockchain network makes it challenging for miners to follow the consensus [23]. The Byzantine general issue is typically used by blockchain for its consensus. A set of blockchain nodes uses a consensus mechanism to make decisions, and the remaining nodes must abide by those decisions. The majority of the blockchains' consensus method is the vote of most of the participants. The following discussion includes some of the common consensus algorithms:

Proof-of-Work (PoW):

Cynthia Dwork and Naor Moni developed the concept of PoW in 1993 [29], while the phrase "proof of work" was first used by Markus Jacobson and Ari Juels in 1999 [30]. Here, in order to be eligible for producing a new block or new cryptocurrency coin, certain network nodes, known as miners, compete in computing labour by solving challenging mathematical puzzles, called Nonce. The Nonce, abbreviated from "number used once," is a pseudo-random or genuinely random number applied in authentication protocols to prevent the repetition of previous transmissions. The successful miner is the one who submits the new block and receives some extra bitcoin as compensation for obtaining the requisite result first [31]. The block's nonce needs to be changed for the subsequent hashing experiment if the required target value cannot be reached. This change for a particular block can be done until a particular time limit arrives. This time limit varies from platform to platform. For example, the difficulty of Bitcoin is, to add 1 block, every 10 minutes on average [32].

Network security is provided by PoW, which protects against DoS and double-spending attacks. Security issues in PoW networks include selfish mining and 51% attack. Nonetheless, PoW grapples with its substantial energy expenditure [33], which was estimated to be around 26.41 TWh to 176.98 TWh per year as of July 2021 [34]. This energy consumption aligns with that of countries such as Austria and the Czech Republic, and it even surpasses the combined energy consumption of 175 to 181 smaller nations taken individually [35].

Proof-of-Stake (PoS):
Unlike PoW, PoS validates a block using diverse, randomly chosen combinations of age or wealth, eliminating the need for miners to create a new block. Therefore, it consumes less energy than PoW. It establishes a number that results from multiplying the quantity of coins by the days they have been kept, which is called coinage. According to their coinages, the mechanism distributes relevant stakes to coin holders. In the PoS system, specialised nodes, known as validators, assemble transactions and produce new blocks. The stake (amount of coins/currency) of a validator determines his likelihood of adding a new block. There is a higher chance for new blocks to be submitted by validators with larger stakes. The reason is owners with huge stakeholders are unlikely to cause harm to the network. The stakeholder’s holdings of coins are reset to zero after successfully mining a block and receiving mining rewards, and the process of calculating its coinage is repeated.

The nothing-at-stake dilemma is the primary drawback of POS. A fork increases the likelihood of double-spending attacks since validators will gain nothing by adding to both chains. In most cases, a pseudo-random selection procedure is employed to choose the node allocation. This selection is unjust since the richest miner would start to dominate the rest of the network. The comparison of a miner's block count and a network's block count is used to recommend the majority of solutions. Many blockchains are in the process of gradually shifting from proof-of-work to Proof-of-Stake [36]. The Polkadot [37] and NEO [38] blockchains both employ PoS.

Delegated Proof-of-Stake (DPoS):
Unlike PoS, which operates on a democratic representative model, DPoS is characterized by a more direct form of democracy. The potential issue of accounts with substantial holdings exerting undue influence on block creation in PoS has been mitigated through the introduction of DPoS. It is used in cryptocurrencies like Blackcoin and Peercoin to increase security and prevent centralization. The consensus procedure is split into two phases, at the beginning each node votes to choose the trusted nodes. Secondly, these elected nodes carry out transaction accounting and verification. To verify a block and receive the appropriate transaction reward, delegates can cooperate [39]. Delegates hold the power to modify parameters such as block size and interval. Some blockchain initiatives that implement DPoS include Steem [40], Bitshares [41], and Tezos [42]. DPoS delivers excellent efficiency while reducing the verification nodes and energy use.

Practical Byzantine Fault Tolerance (PBFT):
The low-efficiency issue of the Byzantine fault tolerance problem is handled by the Practical Byzantine Fault Tolerance algorithm [43] which has been developed by allowing a distributed network to function even if some nodes are erroneous. In private blockchain and consortium blockchains, this voting-based consensus is employed, and even in some situations when chain codes are used, it can be quite successful [44]. Even if m out of x nodes are believed to be malicious the consensus function is secure, where x = (3m + 1) and m = (x - 1)/3. The system remains secure as long as the proportion of malicious nodes (m) is less than one-third of the total nodes (x). The quantity of participating nodes affects how effective PBFT is. When there are fewer nodes (for example, less than 100), it performs best [45]. In PBFT, there are primary and backup nodes. When a primary node gets a client request, a three-step process (pre-prepare phase, prepare phase, and commit phases) is carried out. Following this, the client receives a response. In this situation, PBFT necessitates familiarity across all network nodes.

The primary node initiates a pre-prepare message containing information like view number, block ID, primary ID, and block number. Once this message is acknowledged by a backup node, it sends a prepare message to signal the agreement on creating the new block to all backups, including the primary. The commit phase of a backup begins when it gets 2m + 1 prepare messages. Backups check and validate the proposed block's requests during the commit process. Then it notifies all other backups of a commit message if all requests are genuine. If a backup receives at least 2m + 1 identical commit messages, or if at least two-thirds of the nodes concur on adding the new block, it is eventually incorporated into the blockchain network. This newly added block is considered final as PBFT doesn't involve forks. Examples of PBFT include Hyperledger Fabric [17], Ripple [46], and Stellar [47].

Tendermint:
Another consensus protocol that uses voting is Tendermint. There is a similarity between Tendermint and PBFT algorithms. It also obtains without mining consensus, has finality, and zero energy waste. The selection of a proposer occurs when a new unverified block is introduced for dissemination in a given round. This process involves three stages: Prevote, Precommit, and Commit. During the prevote stage, validators make a broadcast prediction regarding the proposed block. Once a node receives prevotes surpassing two-thirds for the suggested block, it proceeds to the precommit phase. If the node gathers precommitments exceeding two-thirds, it engages in the commit process. The node broadcasts a commit message to the block after validating the block during the commit phase. The block will approve if the node obtains commitments of more than two-thirds. If detected cheating, validators face punishment. The Tendermint consensus is used by the Tendermint coin [48].

Ripple:
Ripple uses sub-networks inside the vast network that achieve trust collectively. In this network, there are two categories of nodes. The first is a participating server in the consensus process, while the second is a client that solely accepts money transfers. There will be a necessary Unique Node List (UNL) for each server which is used to determine the publication of transactions into the ledger. If the database received 80% or more of the nodes' votes in favour of publishing, it would pack the transaction in the ledger. The ledger will authenticate each UNL node as long as their proportion falls below 20%.

Proof-Of-Authority (PoA):

PoW and PoS have been combined to create PoA [49]. It appreciates a stakeholder's reputation and identity. A stakeholder is therefore indirectly supported by their reputation rather than a stake. As a result, reliable and trustworthy individuals are responsible for protecting the blockchain's building blocks. Microsoft Azure implemented this method.

Proof of Vote (PoV):
Compared to other consensus techniques, the Proof of Vote algorithm is slightly unique. To establish transaction blocks a group of businesses must mutually exchange their business data in the blockchain. So, they choose a group of third parties for their work. To ensure the blockchain's decentralised nature, the team will send the block to every organisation participating in the network for voting-based verification. The owners of businesses occasionally increase the scope of the job performed by the hired staff. The purpose of developing this method was for consortium blockchains [44].

Proof-of-Importance (PoI):
The miner is picked according to productivity in PoI [50] rather than the quantity of labour or stake he has. Users who make more transactions into their accounts will receive the incentive instead of those with a high balance. The PoI network assigns a trust score to every user. The probability of receiving a reward increases with value. This algorithm is utilised by the NEM [51] blockchain network.

Other protocols:
There are several other suggested consensus algorithms. For example, Proof of Burn [52], Proof of Activity (PoA), Proof of Space (PoS), Proof of Bandwidth (PoB) [53], Proof of Capacity (PoC) [54], Federated Byzantine Fault Tolerance (FBFT), Proof of Publication (PoP), Directed Acyclic Graph (DAG) [55], Proof of Elapsed Time (PoET) [56], Raft, Proof of Existence (PoE), Scalable Byzantine Consensus Protocol (SCP) [57], etc [58]–[63].

3.2 Smart contracts

Smart contracts were first introduced by Nick Szabo as an automated transaction mechanism in 1994. A set of promises or conditions in digital form can be described as a smart contract [23]. When a certain condition is satisfied on each of the network's nodes, the smart contract permits self-execution [64]. Smart contracts were conceptualized prior to the emergence of blockchain technology. The inclusion of smart contract data within the blockchain ensures resistance against counterfeiting and unauthorized alterations. Execution of the smart contract depends on the code, as there is a digital signature that can be verified easily and it also aids the parties to forecast the results [25]. It has the ability to manage smart assertions and assertion transactions. Additionally, they are beneficial in loan, mortgage, and business-to-business agreements. According to certain studies, smart contracts have efficiency, accessibility, and scalability. The greatest platform for creating smart contracts is Ethereum [65].

Smart contracts are computer applications created for various blockchain platforms that will be automatically adopted by government agencies, healthcare, and other institutions [66]. The removal of intermediaries, fraud, and trust issues in financial transactions is the purpose of smart contracts. A smart contract and a conventional commercial agreement are different from each other. Both are equivalent in theory; however, smart contracts provide the automated implementation of the preset agreement and may be used simultaneously by various corporate groups.

3.3 Blockchain frameworks

Blockchain technology combines elements of cryptography and peer-to-peer (P2P) systems. It is characterized by a sequence of time-stamped blocks linked by cryptographic hashes. Each block typically comprises transaction records that have been validated by peers, often known as miners. Continuously more blocks are added to the chain and the chain increases simultaneously. Each block is created to ensure immutability, transparency, and anonymity [67].

3.3.1 P2P Network

In the blockchain network, a peer, often termed as a node, not only installs the system for personal benefit but also bolsters the system as a whole by offering resources such as bandwidth, storage, and computational capacity. This is similar to how a BitTorrent network works [68]. The node of the network is either accessible to everyone or limited to fewer users depending on the type of blockchain network. The advantage for blockchain nodes is, that their identity is protected as only the public key of the user is made visible to the other nodes in the network. Nodes also perform the role of miners, approving transactions before they are added to the blockchain.

3.3.2 Cryptography

The integration of current cryptographic ideas with consensus protocols makes blockchain technology so beautiful. Cryptographic ideas like hashing, Merkle trees, and digital signatures, are used to support and secure blockchain technology. The main application of cryptographic accumulators, zero-knowledge proofs, and commitments is to improve privacy [69], [70].

- **Hashing:**

Hashing is a mathematical pseudo-random one-way operation. Hash functions are employed to convert a large volume of data into a unique identifier, known as a hash key. This identifier is then stored in a data structure called a hash table.

- ➢ Any dataset fitting into this table is processed by the hash function, resulting in a fixed-length hexadecimal string that appears random. This string is referred to as the hash code or hash value [71].
- ➢ The hash function must be collision-free in order to provide different hash outputs from various inputs (message digest).
- ➢ It is impossible to get back the input from the message digest, the one-way property makes sure it.
- ➢ A new message digest is produced by even little input changes.

In the blockchain, hashing is used to produce addresses, transactions, and data integrity (security). Hashing is also necessary for digital signature and the PoW consensus technique. The Merkle root and block hashes, which are generated by hash functions, are used to identify transactions and the hash of blocks.

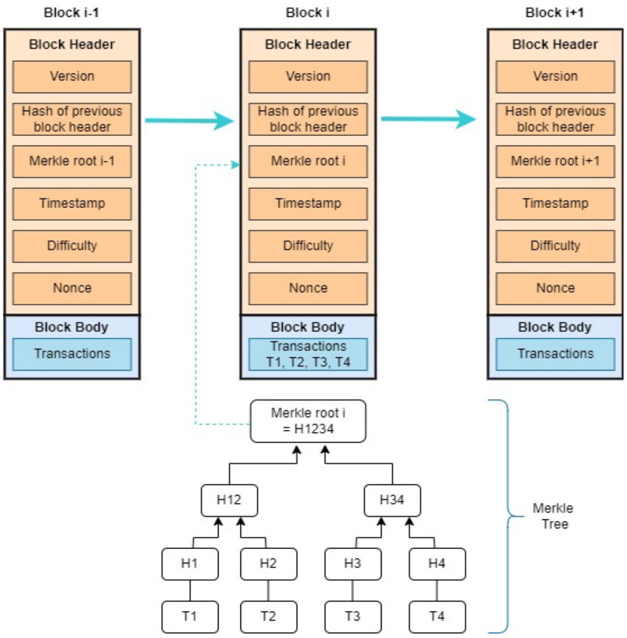

Fig. 2. Structure of blocks and Merkle tree in blockchain

Fig. 2 demonstrates how the hash function offers a mechanism to connect every block on the blockchain network. Examining the block header of block i-1, you'll find the storage of the hash of the preceding block (i-2). Similarly, in block i, it contains the hash of the prior block (i-1). This pattern continues, with block i+1 holding the hash of block i, and so forth.

- **Merkle tree:**

The hashes of all the transactions are amalgamated in a tree-like structure, resulting in the Merkle root, which is the ultimate hash output. This Merkle root stands as a single, crucial hash in the blockchain and is stored in the block header. Any alteration to transaction data is easily detectable, as the updated Merkle root will diverge from the previously recorded one. Simplified Payment Verification (SPV) nodes rely on this Merkle root to verify the existence of a claimed transaction in the blockchain. These nodes exclusively retain block headers, omitting transaction specifics. They request transaction hashes and Merkle branches from a blockchain server, subsequently computing the Merkle root. If it aligns with the Merkle root in the block header, the transaction is validated and incorporated into the blockchain.

Fig. 2 shows there are four transactions T1, T2, T3, and T4 in the block body of block i. The hash of T1 is H1, the hash of T2 is H2, and the hash of the combination of H1 and H2 is H12. In the same way hash of T3 is H3, the hash of T4 is H4, and the hash of the combination of H3 and H4 is H34. The resulting hash, H1234, is derived from the final combination of H12 and H34. This value is designated as the Merkle root and is stored in the header of block i. Any modification or tampering of these transactions will be readily detectable, as it will cause an automatic change in the Merkle root.

- **Digital signature:**

To ensure no data loss the digital signature is used, which is the digitally signed data delivered from one person to another. Digital assets like documents, software, massages, etc. gain validity and integrity due to a digital signature. Transactions can be authenticated using this asymmetric cryptography even when there is no trust [72]. Private and public keys will be there for each client. To establish communication, a client must initially generate a hash from the transaction values and then encrypt it using their private key. This process is termed "digital signing" and the act itself is called "signing". Once the transaction is signed, it is then distributed to all other network peers for validation. All of the peers of that network receive the distributed ledger of transactions that have been digitally signed. Then they subsequently confirm it using the publicly accessible transaction originator's public key. This stage is referred to as the verification phase.

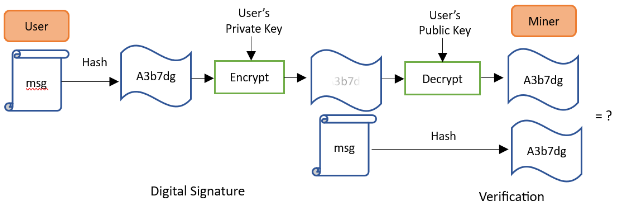

Fig. 3. Digital signature used in transaction

For example, in Fig. 3 we can see the user first applies the hash function to the message, then encrypts that using the private key of the user. This is called digital signature. After that user sends this digital signature along with the original message to the network. Next, the miner will use the user's public key to decrypt the received digital signature and generate the hash value A. Again, the miner will apply the hash function of the received message and produce the hash value B. Lastly miner verifies whether the value of A and the value of B are equal or not.

For signing and verifying transactions, Bitcoin and most blockchain applications employ the Elliptic Curve Digital Signature Algorithm (ECDSA) [73]. On the other hand, Monero and NaiveCoin utilize the Edwards-curve digital signature algorithm (EdDSA) [74]. Ring signatures are used for anonymity in RingCoin and several other cryptocurrencies. In a few applications, like Monero, Borromean ring signatures (BRS) and one-time ring signatures (OTS) are occasionally employed alone with ECDSA or EdDSA. In addition to ECDSA or EdDSA, the majority of blockchains now employ multi-signature for increased security and anonymity [69]. If the signature of the transaction is approved by the highest number of nodes on the blockchain, the transaction is included in a new block; otherwise, it is disregarded.

3.4 Blockchain layers

The blockchain operates without a hierarchical structure. It is structured into four layers according to its protocols:

- **Layer-0:**

The network hardware, which includes the internet and any linked devices, coexists at layer zero. This layer also permits communication across blockchains, enabling inter-chain operability [75]. It offers a vital framework for dealing with issues related to layer scalability in the future. The remaining layers are constructed on top of it as their base.
Some examples of blockchain layer 0 are Avalanche, Cosmos, and Polkadot.

- **Layer-1:**

A lot of tasks to maintain the core functions of blockchain networks, including consensus, dispute resolution, programming languages, limitations, etc. are done at Layer 1. Yet, scalability proves to be a concern within this layer. Any alterations or issues with the new protocol at layer 0 will inevitably have repercussions on layer 1. This layer is commonly referred to as the execution layer.

Some examples of blockchain layer 1 are Ethereum, Bitcoin, Ripple, and Binance Smart Chain [76].

- **Layer-2:**

It is also referred to as the execution layer. It eliminates the scaling restrictions of the previous layer with the integration of third-party. Many sectors have currently started utilising layer two technology.

As an example, blockchain layer 2 is implemented on the Lightning Network in Bitcoin [9].

- **Layer-3:**

Another term used for this is the application layer. Along with user interfaces, this layer also offers the usefulness of inter-chain and intra-chain operability. This layer's primary function is to host the decentralised apps (DAapps) and several other protocols that support other apps. It is the smallest and most effective method created to separate from blockchain in order to achieve the goal of true interoperability.

Some examples of blockchain layer 3 are decentralized exchanges of cryptocurrency like Uniswap and Pancake Swap. Coinbase and Binance are examples of wallet providers [21].

4. Applications

Cryptocurrencies were the first to use blockchain, and Bitcoin was the first successful application of it. Fig. 4, summarises some of the numerous blockchain applications that are available nowadays.

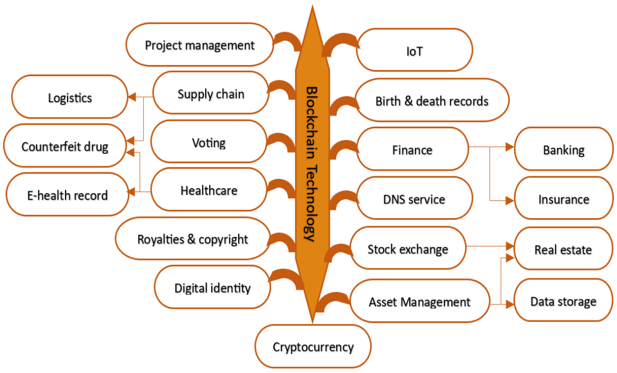

Fig. 4. applications of blockchain

Cryptocurrencies: The two most widely used cryptocurrencies are Bitcoin and Ethereum. Currently, there are almost 1200 different cryptocurrencies, including Litecoin, Bitcoin-cash, Ethereum classic, Doj, Ripple, etc. are present. Now Cryptocurrency payments are accepted for goods and services at many companies. Many nations are working to develop their central bank for their own digital currencies to be utilised primarily for government transactions and inter-bank operations. Numerous papers have been written about cryptocurrencies, particularly Bitcoin. A scaling mechanism for Bitcoin called Bitcoin-NG was introduced to support large transaction rates.

Stock exchange: Traditional methods of purchasing and selling stocks and assets entail several unwanted charges, trusts, and middleman involvements. These expenses might be avoided using blockchain technology. Microsoft predicted that blockchain technology will soon revolutionise the marketing of stock exchanges [77]. Banks don't sell shares directly, but secondary markets use blockchain to purchase and sell shares. Blockchain has been used for stock exchanges and marketing by NASDAQ, Augur, Bitshares, and Coinsetters [78]. Blockchain integration efforts have been ongoing at the LSE (London Stock Exchange) and the ASX Ltd [79]. (Australian Security Exchange). V-Chain [80] is a platform built on the blockchain that is designed to offer leasing services for cars quickly and effectively.

Healthcare: The present healthcare system has a number of problems, including inconsistent data, duplication of records, and most of the patients are unable to understand and manage their own information. Blockchain and smart contracts have a significant influence on healthcare. If properly used then it can solve healthcare data sharing and security related problems. Without difficulties caused by several databases and separate central agencies, various healthcare organisations might cooperate. Additionally, it assists in maintaining the privacy rules of HIPAA, which guarantees confidentiality and public access to patient information. The first nation to do so is Estonia, which has posted its medical information on the blockchain. Its application in the healthcare industry can be divided broadly into four categories. Those are the management of medical records, biomedical research, medical insurance, and connection of healthcare provider applications [76]. Based on the blockchain and ACP concept Wang et al. [75] developed a parallel healthcare system. According to Griggs [81], a healthcare system based on blockchain would allow for safe, autonomous, and remote patient monitoring. For the secure and scalable clinical data exchange, Zhang et al. [82] developed the blockchain architecture FHIRChain. For the integration of healthcare data OmniPHR [83] and for the protected health information (PHI), Healthchain [84] is developed. The blockchain in healthcare is surveyed by Abujamra [85] and McGhin [86].

Insurance: Increasingly, insurance firms are utilising blockchain technology. By adding insurance data to the blockchain, insurance providers may share and interact with data, preventing fraud. This stops individuals from making several insurance claims for the same policy. For the history of diamond certification, an organisation called Everledger employs blockchain technology. Other examples of blockchain applications in the insurance sector include MedRec, Etherisc, and Insurwave [78]. For the provision of insurance services, Raikwar et al. [87] created a safe blockchain infrastructure.

Birth and Death Records: In the world, especially in underdeveloped nations, a large number of people lack a valid birth record. As per UNICEF, 70% of all the children were found to lack a birth certificate. Furthermore, the issue with death certificates is the same. An alternative approach could be to use blockchain technology, which provides a secure repository for verified birth and death certificates, accessible only to authorized individuals.

Digital identity verification and management: In the absence of online verification and authentication, executing any online financial transactions becomes impractical. On the contrary, blockchain has the potential to streamline the online identity verification process, allowing users to share their identity with any desired service provider after a one-time verification with blockchain. In addition, users may select from a variety of identity verification techniques, including user authentication and face recognition. Generally, government agencies and organisations issued identities, like aadhaar-cards, I-card, passports, or certificates, are very susceptible to fraud, theft, and losses. Zero-knowledge proof and blockchain work together to provide a safe and private way to claim and verify the identities recorded on the blockchain. Currently, blockchain identification experiments are being conducted in several nations, including the USA, India, Japan, Switzerland, and other countries. A blockchain platform called tykn offers services and maintenance of digital identities [88].

Internet of Things: The "Internet of Things" (IoT) is a network of interconnected devices that communicate and gather data to enable informed decision-making. Because IoT devices operate autonomously and exchange data without human intervention, blockchain technology has gained attention for its potential applications in this field. A prominent example of IoT is the Smart Home, where various household items like lights, smoke alarms, air conditioners, and thermostats can be linked together on a unified platform. These appliances and IoT devices can self-update, upgrade, and troubleshoot. The use of blockchain is essential to secure this widely dispersed system, ensuring that the data collected by IoT devices remains protected and accessible only to authorized individuals.

Logistics and supply chain: With blockchain logistics and supply chains can operate more quickly, securely, and transparently. As the availability of data on a secured distributed immutable public ledger, it provides easier communication between participants, as well as it provides enhanced data integrity and security. Blockchain is a cost-effective and secure alternative for the logistics sector. It can be used in assigning recently arriving items to various shipping containers, and following the movement of products in real-time as they pass through the supply chain. Without depending on centralised authority, who may behave maliciously, the information is obtained faster. Almost half of all worldwide shipping businesses presently participate in a blockchain-based network for the supply chain, TradeLens [89]. Medicine supply chain also is one of the most common applications of blockchain [90]. Grainchain [91] utilises blockchain to track agricultural goods like grains as well as to sell, purchase, and exchange them.

Royalties and copyright: Blockchain technology can be used for the purposes of streamlining and managing content production and sharing, licensing, and distributing those, payments, copyright, and artist royalties. Blockchain technology can aid in reducing piracy as one of its most important concepts is to ensure that the same content cannot exist in any other location. Additionally, utilising smart contract blockchain can monitor playbacks on streaming platforms and distribute rewards, which can increase transparency and ensure that artists are paid what they deserve. Blockai and Copyrobo exemplify the fusion of blockchain technology and artificial intelligence to swiftly aid artists in safeguarding their online creations.

Voting: The ability to conduct elections in a free and fair way is a problem in many nations, especially developing countries. Voting in any meetings, organizations, and even within the nations might be made transparent with the use of blockchain technology. A few initiatives that offer effective blockchain voting architectures include BitCongress, AgoraVoting, and Remotengrity [78]. The blockchain-driven electronic voting system, tested in sixteen countries, advocates for an unalterable record of democratic elections, ensuring their fairness and integrity. To enable voting by its affiliated enterprises, Slock.it created Hutten for Siemens, a decentralised digital organisation built on blockchain [92].

Data storage: Data security and centralization are two risks associated with the current cloud storage services offered by organisations like Google and Dropbox. Traditional centralized systems pose a vulnerability as a sole point of failure for privacy and data security breaches. Therefore, personal data is stored using blockchain in a decentralised way under the complete control and supervision of the data owners. Blockchain storage offers advantages like speed, security, flexibility, and affordability. Storj, a blockchain-based decentralized cloud storage, provides a user-friendly, private, and secure solution [93]. Additionally, there's another BlockStack blockchain storage option named Gaia [94]. IPFS, Swarm, Sia, and SAFA networks are some other blockchain storage networks [95]. Li et al. [96] presented an IoT data storage system based on blockchain that does not require certificates.

DNS services: Blockchain technology is harnessed in Domain Name Services (DNS) to mitigate security threats, censorship, and potential abuse by centralized entities or governmental bodies governing internet DNS services. The October 2016 DoS attack on Dyn DNS provider underscored the necessity for robust security protocols in DNS services. EmerDNS [97] stands as a blockchain-driven alternative to DNSSec, with Namecoin [98] and Blockstack [99] offering DNS services integrated with blockchain. Karaarslan [94] delved into research on DNS and PKI systems anchored in blockchain technology.

Project management: Conventional contract management is full of threats, inefficient, and comes at an elevated expense to the business. Numerous businesses currently provide blockchain platforms and solutions for managing contracts. Platforms are used by contractors as well as their clients for effective contract tracking and management. The solutions are employed to accomplish construction and various other operations. At present, a lot of efficient project management solutions and platforms based on blockchain are offered by Corda, Konfidio, Monax, Oracle, and Icertis.

There are several more uses for blockchain, including in the public sector, the building industry, Energy management, trust administration, finance and banking, the music industry, the education sector, cybersecurity, and others.

5. Challenges with Blockchain

Blockchain is an innovative technology that has a lot of potential and benefits, but there are certain obstacles to overcome. The utilization of blockchain is sometimes restricted by these issues. Within this section, we'll delve into some of the most common security challenges and attacks that pertain to blockchain.

5.1 Security issues

Because of its decentralized nature, operating without the need for a third party and relying on the establishment of trust within a trustless infrastructure, it is valuable to delve into the security challenges of blockchain [25]. Consensus procedures, data management, chain systems, storage, regulation, governance, and other issues are only a few of the issues that exist [100]. Some of the major difficulties are:

Scalability:
One of the major problems with blockchain is scalability, especially in public blockchains. The main scalability problem with blockchain is its poor throughput (tps) and massive storage data [101]. For instance, 3-4 tps are handled by Bitcoin, and 20 tps are handled by Ethereum. In contrast, 24,000 and 193 transactions are managed by PayPal and Visa, respectively [102]. Only seven transactions can be processed per second by blockchain due to the lengthy block interval and tiny block size, which is a poor throughput rate, in contrast to Google, which can handle 85,830 queries per second, Blockcypher can handle 3 queries per second [103]. The block size and interval must be balanced in order to achieve the best throughput. On the flip side, the substantial storage capacity of blockchain presents a deterrent to running full nodes, particularly for IoT devices with their limited memory resources. Due to miners' preference for transactions with larger transaction fees, many tiny transactions may be delayed since the blocks' real capacity is insufficient. As a result, scalability is a serious issue. Various strategies, including sharding, sidechains, the lightning network, Jidar, Segregated Witness (SegWit), compact block relay, DAG, and advanced consensus algorithms, have been put forward to bolster the scalability of blockchains [104].

Security issues:
While blockchain is renowned for its robust security features, various security threats and weaknesses have been identified in certain blockchain applications, particularly in the public blockchain realm predominantly utilized for cryptocurrencies. Private and consortium blockchain systems, owing to their restricted access, tend to be more secure. Commonly reported security concerns encompass scams, malware attacks, denial of service (DoS) incidents, vulnerabilities in applications, Sybil attacks, and network susceptibilities. Large-scale security issues are also caused when private keys are lost because of carelessness, accidents, or attacks [105], [106], [45]. Since 2017, exchanges have been the primary target of $2 billion worth of cryptocurrency theft [107]. Attacks against Ethereum, Bitcoin, and other cryptocurrencies were reported, with the most well-known ones on MtGox and DAO costing 450 million and 60 million dollars, respectively. Border Gateway Protocol (BGP) attacks might potentially be used to steal money from cryptocurrencies [106]. BGP attacks were estimated to have cost about 83,000 USD in just two months. The 51% attack vulnerability exists for blockchain's implementing PoW consensus. Attacks like double-spending, eclipse attacks, and denial-of-service attacks might be carried out by the 51% attacker in addition to transaction censorship. Another issue with blockchain security is selfish mining. In smart contracts and blockchain programming can also have vulnerabilities. 8,833 Ethereum smart contracts out of 19,366 were discovered to have security flaws [108].

Privacy issues:
Even though blockchain employs a pseudonymous method, it is feasible to deduce a user's real-world identity through meticulous scrutiny of transactions originating from a particular node or by analyzing data and network behavior within the blockchain. As an alternative, privacy violations can be done by retrieving the IP addresses of users and connecting them to their wallets [45]. In his demonstration, Goldfeder [109] has shown how browser cookies can be used to reveal the true identity of users when they made cryptocurrency payments online. To avoid privacy detection, an intermediate entity is utilised to swap the identity for another identifier, such as a voucher [96]. While some studies provide brand-new strategies for blockchain privacy provision, some researchers suggest ways to improve the current privacy approaches [110].

Blockchain privacy can be improved by using zero-knowledge proofs like ZK-SNARKs, AZTEC, and Idemix [111]. While Merve [112] provides a thorough survey of anonymity and privacy in cryptocurrencies that are similar to Bitcoin, Conti [113] provides an overview of privacy concerns with Bitcoin. To extend asset transfers on Ethereum to 500 tps, Vitalik Buterin suggested using ZK-SNARKs [114]. Zk protocol is used by an API for privacy solutions on Ethereum [115]. For privacy, a zk variation protocol is used by Hyperledger Fabric and Indy which is the identity mixer (Idemix) [116].

Usability:
Swan [117] asserted that while specific software can dissect and retrieve data from the blockchain, its APIs pose challenges for developers. Simplifying blockchain APIs would be beneficial for programmers.

Quantum computing issue:
In quantum computing, there are several projects and research. The goal of certain companies, including Google, IBM, and Microsoft, is to develop quantum computers for commercial purposes that operate at speeds that are far faster than those of the existing computers. According to a Google announcement from October 2019, a work that would have taken supercomputers to complete 10,000 years, is achieving quantum supremacy in 200 seconds. A practical quantum computer for commercial purposes is still a long way off from being ready [118]. With the help of a modified Shor's algorithm [118], the ECDSA, which is used by the majority of blockchains, may be broken by quantum computers. According to Kiktenko et al. [119], blockchain signatures will take one day to be broken by quantum computer attacks. Consequently, they suggested a digital signature of post-quantum whose security is hypothetical and mostly untested.

Regulatory issues:
One of the biggest problems preventing blockchain adoption globally, especially by the central authorised banks, is the absence of rules. Regulatory difficulties were cited by 48% of 600 respondents in the PWC study, as the biggest obstacle to the use of blockchain technology [120]. Because of worries about illegal actions and the possible impact of cryptocurrencies on their official currency, many governments are hesitant to oversee blockchain operations, particularly those involving cryptocurrencies. Due to this, many nations are thinking of developing their own digital currencies. Many societal changes, including the legal and judicial systems, have been altered by the advent of blockchain. Due to inadequate legal oversight during its early phases, blockchain gave rise to a number of legal problems. Once there is a thorough comprehension of blockchain's characteristics, suitable guidelines can be refined. The majority of nations began implementing blockchain by tightening regulatory controls [23].

Lack of knowledge of blockchain:
A major hurdle to the widespread adoption of blockchain technology is the lack of knowledge. As many people believe it is being utilised for unfair purposes, they do not trust it or think it is challenging to utilise blockchain technology. According to a poll of 576 Asia-Pacific companies (except China), 68% of them have no trust in blockchain since they do not understand the technology [121]. Deloitte's poll of 1386 executives found that among the specialists 28% saw the main obstacle to blockchain adoption as being a lack of awareness [122].

Reluctance to switch current systems:
Changing to a new system before it has fully grown, it is normal to experience some resistance. This characteristic also affects Blockchain technology. Many organisations are hesitant to upgrade or replace their current systems with blockchain. Deloitte polled 1386 executives, and 30% of them said that the biggest obstacle to adopting blockchain technology is the unwillingness to switch to a new system [122].

5.2 Blockchain Attacks

51% Attack:
This attack is also known as the majority attack, enabling a perpetrator with more than 51% of the computational power of the network to freely manipulate blocks [123]. Miners can make an orphan block to the target block by controlling transactions in it if they have at least 51% of the network's computational power. Spending the same UXTO (Unspent Transaction Output) in two transactions is called the double-spending technique which is also used in the 51% attack. Because of the delay in confirmation of any transaction of block consensus, double-spending may induce.

Selfish Mining Attack:
Miners with malicious intent and powerful computing power could withhold the publication of legitimately mined blocks until they manage to compile an exceedingly lengthy chain of unchallenged blocks. By integrating their own mined blocks into this new chain, it gains the status of being the longest and is acknowledged as the primary chain. Consequently, the honest miners who had previously mined other valid blocks before the selfish miners find their contributions disregarded. As a result, honest miners are discouraged from mining and suffer losses. Therefore, with fewer miners and more selfish miners, the network's scalability and security are compromised [124]. Selfish mining refers to the practice of a miner or a pool of miners not publishing and distributing its recently mined block while simultaneously mining the next block and retaining its mining market's top position [125]. Selfish mining harms the clarity and transparency of the blockchain network by placing bets on mining successfully utilising hashing power.

Block Withholding Attack (BWA):
The block withholding attack involves targeting the mining pool [126]. When a miner successfully completes a block, instead of broadcasting he holds it, which is preventing the mining pool from receiving the mining reward. However, in accordance with the mining pool's allocation guidelines, the miner who launches the BWA may share the block mining rewards earned by others. As a result, the BWA has few negative effects such that, the miner suffers from financial loss and the attack cost is relatively cheap.

Sybil Attack:
When an illegal node displays several identities to the outside of a network then it is known as a Sybil attack and these node identities are commonly referred to as Sybil nodes. In a blockchain, as there is no fee to generate new identities, the attacker can create a false identity to connect to the network and can use this vulnerability to start the Sybil attack. Once the attacker has monitored several identities, he or she is free to engage in malicious behavior [127].

Denial-of-Service (DoS) Attack:
Attacks against system protocols that are intentionally flawed or direct resource exploitation of an attacked item are referred to as "Denial of Service" attacks [128]. While creating a block in systems, malicious miners might use some resources and produce illegal blocks repeatedly in the system for denial-of-service attacks. Attackers may also engage in malicious actions to prevent honest miners from generating a profit from mining, which would prevent them from continuing to mine and would cause the blockchain to stop functioning.

New attacks, such as block withholding attacks and fork after withholding attacks, are encouraged by the competitiveness between mining pools. Fig 5 summarises some of the blockchain attacks.

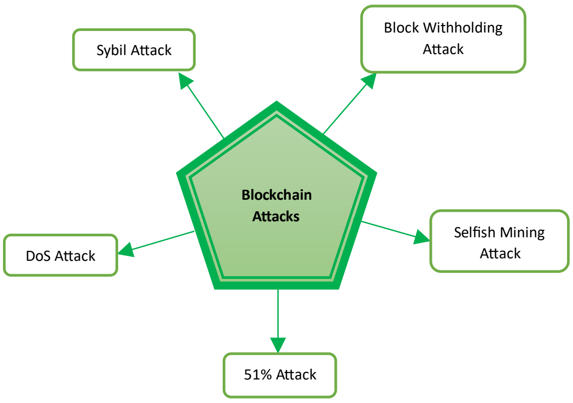

Fig 5. Blockchain attacks.

6. Related Work

Numerous academic works delve into the realm of blockchain technology. In 2017, Sankar et al. introduced three broad categories of blockchains and provided a qualitative analysis comparing Hyperledger Fabric, Corda, and Stellar consensus protocol [129]. Ji.H. Park and Jo.H. Park, also in 2017, conducted a study on the structure of Bitcoin's blockchain, highlighting security concerns such as 51% attacks, transaction security, wallet security, software security, and the integration of blockchain in cloud computing [130]. Lin and Liao, in the same year, discussed security challenges, including the 51% attack, as well as difficulties like the fork problem, issues with confirmation time, rules, data synchronization, and cost-related matters [12]. In 2018, a paper from Kennesaw State University proposed the utilization of blockchain and cryptography to ensure authenticity, data confidentiality, privacy, and integrity across various blockchain applications, emphasizing the need for additional security measures beyond what is inherent in the blockchain itself [131]. Another survey in 2018, conducted by Zheng et al., covered consensus algorithms, challenges, privacy concerns, selfish mining, various applications, and future directions in blockchain technology, including testing, artificial intelligence, robust security measures, and big data analysis [100]. Monrat et al. conducted a comprehensive survey in the same year, addressing various aspects of blockchain technology such as block structure, features, transaction processes, types of blockchains, consensus algorithms, applications, and potential areas for future research [48]. Lastly, in 2019, Dave et al. conducted a survey on the adoption of blockchain across diverse industries, including healthcare, education, agriculture, supply chain management, and more [132]. Development trends of blockchain were assessed by Dasgupta et al. in 2019 along with possible blockchain vulnerabilities [133].

Aguiar et al. conducted a study and employed blockchain technology in 2020 to improve patient privacy and strengthen healthcare security [60]. In another survey paper in 2020, Gamage et al. discussed blockchain technology, its applications, scalability problems, and recommended solutions [59]. A thorough assessment of the attack surface of blockchain technology was published by Saad et al. in 2020 [106]. For the purpose of identifying the research gap and outlining potential future paths for blockchain security research, Leng et al. evaluated blockchain security perspectives of different levels like data, process, and infrastructure in 2020 [135]. The survey report by Berdik et al. on blockchain's role in ensuring information security and integrity was presented in 2021 [58]. In 2021 Bhushan et al. proposed a survey that has given some insights into the security threats of blockchain, emphasizing the privacy requirements for contemporary applications [136]. In 2021 an in-depth analysis of the cryptography underpinning the blockchain was done by Sanka et al. and showed some future direction in their survey paper [78]. Bhutta et al. took a closer look at development frameworks, architecture, security risks, and research challenges in 2021 [137]. Rajasekaran et al. did a comprehensive survey in 2022 by describing the features, applications, classifications, and wallets of blockchain technology [138]. In 2022 H Guo, and X Yu have done a survey on the blockchain where they discussed quantitative comparisons of consensus algorithms, cryptography functions, applications, security, and risk analysis [139]. C Zhu et al. proposed a survey in 2023 that integrates blockchains with databases [140].

7. Future directions

There is a huge research scope on blockchain as it is going to be adopted by almost every sector. Research on how to increase the scalability of blockchain is highly desirable. It is necessary to further address latency and throughput problems with blockchain. The volume of data in blockchain makes it possible to do big data analysis on it. For space, quicker accessibility, and other advantages, alternative large data storage methods might also be improved to save and process data effectively in blockchain networks. Other than these blockchain legitimacy verification needs efficient and safe technologies. Blockchain is something that many businesses desire to use, but they are unwilling to replace their current systems without significant issues. The optimum manner for the blockchain to integrate with an organization's current systems has to be analysed. There is also scope for research on the efficient collaboration of various blockchain systems for mutual gain. Consensus protocols of blockchain have a lot of research opportunities. The emergence of quantum computers poses a potential threat to blockchain security. Therefore, it is imperative to develop robust and rigorously tested post-quantum digital signature systems, along with conducting relevant research. There are some future research possibilities to enhance the efficiency, usability, and trust of post-quantum digital currencies against the risks of quantum computers. Future studies on the blockchain may also lead to more innovative solutions for some of the issues mentioned here. In the future, for widespread use of the technology, infrastructure, and connectivity must be developed for blockchain. The lack of understanding among the stakeholders is one of the main barriers to the adoption of blockchain, and it has to be addressed properly in the future.

8. Conclusion

Blockchain is an exciting new technology that offers a wide range of advantages, including data security, integrity, cost savings, efficiency, anonymity, interoperability, traceability, verifiability, transparency, and most important part is the immutability and removal of middlemen. Holding data by the building blocks which is connected to the chain is blockchain technology. Each block contains the preceding block header which serves as a connection or chain between adjacent blocks. Blockchain is the cause of a digital revolution by leading several sectors. In addition to cryptocurrencies, blockchain now has a wide range of uses and has been adopted by several nations and businesses. As the technology develops and several studies show promising outcomes, further adoptions are anticipated. The implementation of blockchain-based government services by Smart Office in Dubai serves as a groundbreaking model. It is expected that blockchain will eventually attain broad recognition and adoption worldwide. Here, we have done a survey on the evolution, adoptions, and current situation of blockchain technology, encompassing significant advancements in its applications, security issues, and attacks. We also provided an in-depth analysis of the cryptography utilized by the blockchain technology. The future direction shows some ideas that might be used as a source for related studies in the future. Potential scholars can create some new model or structure by compiling all relevant publications, their contributions, and the limits mentioned here. We believe that our work will aid in the understanding of blockchain technology and its state of the art. We also anticipate that our work will be useful to researchers conducting more research on blockchain technology and resolving challenges mentioned.

References

[1] J. Sengupta, S. Ruj, and S. Das Bit, “A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT,” *J. Netw. Comput. Appl.*, vol. 149, Art. no. 102481, Jan. 2020, doi: 10.1016/j.jnca.2019.102481.

[2] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, “A Survey of Distributed Consensus Protocols for Blockchain Networks,” *IEEE Commun. Surv. Tutor.*, vol. 22, no. 2, pp. 1432–1465, 2020, doi: 10.1109/COMST.2020.2969706.

[3] T. Fernández-Caramés and P. Fraga-Lamas, “Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks,” *IEEE Access*, vol. 8, pp. 21091–21116, Jan. 2020, doi: 10.1109/ACCESS.2020.2968985.

[4] B. Bhushan, C. Sahoo, P. Sinha, and A. Khamparia, “Unification of Blockchain and Internet of Things (BIoT): requirements, working model, challenges and future directions,” *Wirel. Netw.*, vol. 27, pp. 55–90, Aug. 2020.

[5] D. L. Chaum, *Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups*. Electronics Research Laboratory, University of California, 1979. Accessed: Oct. 11, 2023. [Online]. Available: https://nakamotoinstitute.org/literature/computer-systems-by-mutually-suspicious-groups/

[6] S. Haber and W. S. Stornetta, “How to time-stamp a digital document,” *J. Cryptol.*, vol. 3, no. 2, pp. 99–111, Jan. 1991, doi: 10.1007/BF00196791.

[7] D. Bayer, S. Haber, and W. S. Stornetta, “Improving the Efficiency and Reliability of Digital Time-Stamping,” in *Sequences II*, R. Capocelli, A. De Santis, and U. Vaccaro, Eds., New York, NY: Springer, 1993, pp. 329–334. doi: 10.1007/978-1-4613-9323-8_24.

[8] R. Sharma, “Bitgold: Meaning, Overview, Differences From Bitcoin,” Investopedia. Accessed: Oct. 14, 2023. [Online]. Available: https://www.investopedia.com/terms/b/bit-gold.asp

[9] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” *Decentralized Bus. Rev.*, Aug. 2008, doi: 10.2139/ssrn.3440802.

[10] R. Karjian, “A Timeline and History of Blockchain Technology,” WhatIs.com. Accessed: Oct. 14, 2023. [Online]. Available: https://www.techtarget.com/whatis/feature/A-timeline-and-history-of-blockchain-technology

[11] Unibright.io, “Blockchain evolution: from 1.0 to 4.0,” Medium. Accessed: Oct. 14, 2023. [Online]. Available: https://unibrightio.medium.com/blockchain-evolution-from-1-0-to-4-0-3fbdbccfc666

[12] I.-C. Lin and T.-C. Liao, “A survey of blockchain security issues and challenges,” *Int. J. Netw. Secur.*, vol. 19, no. 5, pp. 653–659, Sep. 2017, doi: 10.6633/IJNS.201709.19(5).01.

[13] C. Cachin and M. Vukolić, “Blockchain Consensus Protocols in the Wild.” arXiv, Jul. 07, 2017. doi: 10.48550/arXiv.1707.01873.

[14] “Litecoin - Open source P2P digital currency.” Accessed: Oct. 14, 2023. [Online]. Available: https://litecoin.org/

[15] “What is Ethereum?,” ethereum.org. Accessed: Oct. 14, 2023. [Online]. Available: https://ethereum.org

[16] “Consensys Quorum,” Consensys. Accessed: Oct. 16, 2023. [Online]. Available: https://consensys.net/quorum/

[17] E. Androulaki *et al.*, “Hyperledger fabric: a distributed operating system for permissioned blockchains,” in *Proceed. Thirteenth EuroSys Conf.*, in EuroSys ’18. New York, NY, USA: Association for Computing Machinery, Apr. 2018, pp. 1–15. doi: 10.1145/3190508.3190538.

[18] R. G. Brown, “The Corda Platform: An Introduction,” 2018.

[19] S. Aggarwal and N. Kumar, “Chapter Sixteen - Hyperledger☆☆Working model.,” in *Advances in Computers*, vol. 121, Aug. 2021, pp. 323–343. doi: 10.1016/bs.adcom.2020.08.016.

[20] “Why we exist - Energy Web.” Accessed: Oct. 16, 2023. [Online]. Available: https://www.energyweb.org/why-we-exist/

[21] “Bitcoin’s Market Capitalization History (2013 – 2023, $ Billion),” GlobalData. Accessed: Oct. 16, 2023. [Online]. Available: https://www.linkedin.com/company/globaldataplc/

[22] A. V. Barenji, H. Guo, Z. Tian, Z. Li, W. M. Wang, and G. Q. Huang, “Blockchain-Based Cloud Manufacturing: Decentralization,” *IOS Press*, Vol. 7, pp. 1003 - 1011, Jan. 2019, doi: 10.3233/978-1-61499-898-3-1003.

[23] L. Zhu, K. Gai, and M. Li, “Blockchain and Internet of Things,” in *Blockchain Technology in Internet of Things*, L. Zhu, K. Gai, and M. Li, Eds., Cham: Springer International Publishing, 2019, pp. 9–28. doi: 10.1007/978-3-030-21766-2_2.

[24] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, “Integration of Blockchain and Cloud of Things: Architecture, Applications and Challenges,” *IEEE Commun. Surv. Tutor.*, vol. 22, no. 4, pp. 2521–2549, Apr. 2020, doi: 10.1109/COMST.2020.3020092.

[25] Y. Lu, “The blockchain: State-of-the-art and research challenges,” *J. Ind. Inf. Integr.*, vol. 15, pp. 80–90, Sep. 2019, doi: 10.1016/j.jii.2019.04.002.

[26] “Distributed ledger technology: beyond block chain,” GOV.UK. Accessed: Oct. 16, 2023. [Online]. Available: https://www.gov.uk/government/news/distributed-ledger-technology-beyond-block-chain

[27] A. Narayanan and J. Clark, “Bitcoin’s academic pedigree,” *Commun. ACM*, vol. 60, no. 12, pp. 36–45, Nov. 2017, doi: 10.1145/3132259.

[28] D. Wang, J. Zhao, and Y. Wang, “A Survey on Privacy Protection of Blockchain: The Technology and Application,” *IEEE Access*, vol. 8, pp. 108766–108781, Apr. 2020, doi: 10.1109/ACCESS.2020.2994294.

[29] C. Dwork and M. Naor, “Pricing via Processing or Combatting Junk Mail,” in *Adv. Cryptol. — CRYPTO’92*, E. F. Brickell, Ed., in Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 1993, pp. 139–147. doi: 10.1007/3-540-48071-4_10.

[30] M. Jakobsson and A. Juels, “Proofs of Work and Bread Pudding Protocols(Extended Abstract),” in *Sec. Inform. Netw.:*, vol. 23, B. Preneel, Ed., in IFIP — The International Federation for Information Processing, vol. 23. , Boston, MA: Springer US, 1999, pp. 258–272. doi: 10.1007/978-0-387-35568-9_18.

[31] R. Qin, Y. Yuan, and F.-Y. Wang, “Research on the Selection Strategies of Blockchain Mining Pools,” *IEEE Trans. Comput. Soc. Syst.*, vol. 5, no. 3, pp. 748–757, Sep. 2018, doi: 10.1109/TCSS.2018.2861423.

[32] Y. Wang, C. Tang, F. Lin, Z. Zheng, and Z. Chen, “Pool Strategies Selection in PoW-Based Blockchain Networks: Game-Theoretic Analysis,” *IEEE Access*, vol. 7, pp. 8427–8436, Oct. 2019, doi: 10.1109/ACCESS.2018.2890391.

[33] K. Bendiab, N. Kolokotronis, S. Shiaeles, and S. Boucherkha, “WiP: A Novel Blockchain-Based Trust Model for Cloud Identity Management,” in *2018 IEEE 16th Intl Conf. Dependable, Auton. Sec. Comput., 16th Intl Conf Pervas. Intellig. Comput., 4th Intl Conf. Big Data Intellig. Comput. Cyb. Sci. Techn. Congr. (DASC/PiCom/DataCom/CyberSciTech)*, Athens: IEEE, Aug. 2018, pp. 724–729. doi: 10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00126.

[34] V. Kohli, S. Chakravarty, V. Chamola, K. S. Sangwan, and S. Zeadally, “An analysis of energy consumption and carbon footprints of cryptocurrencies and possible solutions,” *Digit. Commun. Netw.*, vol. 9, no. 1, pp. 79–89, Feb. 2023, doi: 10.1016/j.dcan.2022.06.017.

[35] S. Corbet, B. Lucey, and L. Yarovaya, “Bitcoin-energy markets interrelationships - New evidence,” *Resour. Policy*, vol. 70, p. 101916, Mar. 2021, doi: 10.1016/j.resourpol.2020.101916.

[36] D. K. Tosh, S. Shetty, X. Liang, C. Kamhoua, and L. Njilla, “Consensus protocols for blockchain-based data provenance: Challenges and opportunities,” in *2017 IEEE 8th Ann. Ubiquitous Comput., Electron. Mob. Communic. Conf (UEMCON)*, Oct. 2017, pp. 469–474. doi: 10.1109/UEMCON.2017.8249088.

[37] G. WOOD, “Polkadot — A heterogeneous multi-chain framework,” *White paper*, vol. 21, no. 2327, p. 4662, Nov. 2016.

[38] www.allcryptowhitepapers.com, “NEO Whitepaper,” The Whitepaper Database. Accessed: Oct. 16, 2023. [Online]. Available: https://www.allcryptowhitepapers.com/neo-whitepaper/

[39] L. Daniel, “DPOS Consensus Algorithm - The Missing White Paper,” *Bitshare whitepaper*, May 29, 2017. Accessed: Oct. 16, 2023. [Online]. Available: https://steemit.com/dpos/@dantheman/dpos-consensus-algorithm-this-missing-white-paper

[40] C. Li and B. Palanisamy, “Incentivized Blockchain-based Social Media Platforms: A Case Study of Steemit,” in *Proceedings of the 10th ACM Conf. Web Sci.*, in WebSci ’19. New York, NY, USA: Association for Computing Machinery, Jun. 2019, pp. 145–154. doi: 10.1145/3292522.3326041.

[41] F. Schuh and D. Larimer, “Bitshares 2.0: General Overview,” in *Cryptonomex, Cryptonomex.com*, 2017. [Online]. Available: http://docs. bitshares. org/downloads/bitshares-general. pdf

[42] L. M. Goodman, “Tezos—aself-amendingcrypto-ledger Whitepaper,” *White Pap.*, vol. 4, pp. 1432–1465, Sep. 2014.

[43] Castro, Miguel and Liskov, and Barbara, “Practical Byzantine Fault Tolerance,” in *OsDI*, vol. 99, in 1999, vol. 99, 1999, pp. 173–186. Accessed: Oct. 16, 2023. [Online]. Available: https://pmg.csail.mit.edu/~castro/osdi99_html/osdi99.html

[44] K. Li, H. Li, H. Hou, K. Li, and Y. Chen, “Proof of Vote: A High-Performance Consensus Protocol Based on Vote Mechanism & Consortium Blockchain,” in *2017 IEEE 19th Int. Conf. High Perform. Comp. Communic.; IEEE 15th Int. Conf. Smart City; IEEE 3rd nt. Conf. Data Sci. Sys. (HPCC/SmartCity/DSS)*, Dec. 2017, pp. 466–473. doi: 10.1109/HPCC-SmartCity-DSS.2017.61.

[45] X. Wang *et al.*, “Survey on blockchain for Internet of Things,” *Comput. Commun.*, vol. 136, pp. 10–29, Feb. 2019, doi: 10.1016/j.comcom.2019.01.006.

[46] F. Armknecht, G. O. Karame, A. Mandal, F. Youssef, and E. Zenner, “Ripple: Overview and Outlook,” in *Trust and Trustworthy Computing*, M. Conti, M. Schunter, and I. Askoxylakis, Eds., in Lecture Notes in Computer Science. Cham: Springer International Publishing, 2015, pp. 163–180. doi: 10.1007/978-3-319-22846-4_10.

[47] “Stellar | A Blockchain Network for Payments and Tokenization,” Stellar.org. Accessed: Nov. 17, 2023. [Online]. Available: https://stellar.org/

[48] A. A. Monrat, O. Schelén, and K. Andersson, “A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities,” *IEEE Access*, vol. 7, pp. 117134–117151, Apr. 2019, doi: 10.1109/ACCESS.2019.2936094.

[49] “POA Network Whitepaper,” GitHub. Accessed: Oct. 17, 2023. [Online]. Available: https://github.com/poanetwork/wiki/wiki/POA-Network-Whitepaper

[50] “What is POI,” NEM Documentation. Accessed: Oct. 18, 2023. [Online]. Available: https://docs.nem.io/pages/Concepts/what-is-poi/docs.en.html

[51] “Welcome to the NEM Documentation,” NEM Documentation. Accessed: Oct. 18, 2023. [Online]. Available: https://nemproject.github.io/nem-docs/pages/

[52] K. Karantias, A. Kiayias, and D. Zindros, “Proof-of-Burn,” in *Finan. Cryptogr. Data Sec.*, in Lecture Notes Computer Science, vol. 12059. Malaysia: Springer-Verlag, Jul. 2020, pp. 523–540. Accessed: Oct. 18, 2023. [Online]. Available: https://www.research.ed.ac.uk/en/publications/proof-of-burn

[53] M. Ghosh, M. Richardson, B. Ford, and R. Jansen, “A TorPath to TorCoin: Proof-of-Bandwidth Altcoins for Compensating Relays,” presented at the Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs), Jul. 2014. Accessed: Oct. 18, 2023. [Online]. Available: https://apps.dtic.mil/sti/citations/ADA621867

[54] A. Hayes, “Proof of Capacity (Cryptocurrency) Overview,” Investopedia. Accessed: Oct. 18, 2023. [Online]. Available: https://www.investopedia.com/terms/p/proof-capacity-cryptocurrency.asp

[55] “What Is a Directed Acyclic Graph (DAG) in Cryptocurrency?,” *Binance Academy*. Accessed: Oct. 18, 2023. [Online]. Available: https://academy.binance.com/en/articles/what-is-a-directed-acyclic-graph-dag-in-cryptocurrency

[56] “Sawtooth FAQ: Consensus Algorithms (including PoET).” Accessed: Oct. 18, 2023. [Online]. Available: https://sawtooth.hyperledger.org/faq/consensus.html

[57] L. Luu, V. Narayanan, K. Baweja, C. Zheng, S. Gilbert, and P. Saxena, “SCP: A Computationally-Scalable Byzantine Consensus Protocol For Blockchains,” *Cryptol. EPrint Arch.*, 2015, Accessed: Oct. 18, 2023. [Online]. Available: https://eprint.iacr.org/2015/1168

[58] D. Berdik, S. Otoum, N. Schmidt, D. Porter, and Y. Jararweh, “A Survey on Blockchain for Information Systems Management and Security,” *Inf. Process. Manag.*, vol. 58, no. 1, Art. no. 102397, Jan. 2021, doi: 10.1016/j.ipm.2020.102397.

[59] H. T. M. Gamage, H. D. Weerasinghe, and N. G. J. Dias, “A Survey on Blockchain Technology Concepts, Applications, and Issues,” *SN Comput. Sci.*, vol. 1, no. 2, Art. no. 114, Apr. 2020, doi: 10.1007/s42979-020-00123-0.

[60] E. Aguiar, B. Faiçal, B. Krishnamachari, and J. Ueyama, “A Survey of Blockchain-Based Strategies for Healthcare,” *ACM Comput. Surv.*, vol. 53, pp. 1–27, Mar. 2020, doi: 10.1145/3376915.

[61] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, “A survey on the security of blockchain systems,” *Future Gener. Comput. Syst.*, vol. 107, pp. 841–853, Jun. 2020, doi: 10.1016/j.future.2017.08.020.

[62] S. Zhang and J.-H. Lee, “Analysis of the main consensus protocols of blockchain,” *ICT Express*, vol. 6, no. 2, pp. 93–97, Jun. 2020, doi: 10.1016/j.icte.2019.08.001.

[63] Wenbo Wang *et al.*, “A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks,” *IEEE Access*, vol. 7, pp. 22328–22370, Jan. 2019, doi: 10.1109/ACCESS.2019.2896108.

[64] Shangping Wang, Xu Wang, and Yaling Zhang, “A Secure Cloud Storage Framework With Access Control Based on Blockchain,” *IEEE Access*, vol. 7, pp. 112713–112725, Jul. 2019, doi: 10.1109/ACCESS.2019.2929205.

[65] S. Nanayakkara, S. Perera, and S. Senaratne, “Stakeholders’ Perspective on Blockchain and Smart Contracts Solutions for Construction Supply Chains,” in *CIB World Building Congress*, Hong Kong SAR China, Jun. 2019, pp. 17–21. doi: 10.6084/m9.figshare.8868386.

[66] Martin Röscheisen, Michelle Baldonado, Kevin Chang, Luis Gravano, Steven Ketchpel, and Andreas Paepcke, “The Stanford InfoBus and its service layers: Augmenting the internet with higher-level information management protocols,” in *Dig. Libr. Comp. Sci.: The MeDoc Approach*, vol. 1392, in Lecture Notes in Computer Science book series, vol. 1392. , Springer Berlin Heidelberg, 2006, pp. 213–230. Accessed: Oct. 18, 2023. [Online]. Available: https://link.springer.com/chapter/10.1007/BFb0052526

[67] A. A. Mamun, S. R. Hasan, M. S. Bhuiyan, M. S. Kaiser, and M. A. Yousuf, “Secure and Transparent KYC for Banking System Using IPFS and Blockchain Technology,” in *2020 IEEE Region 10 Symp. (TENSYMP)*, Jun. 2020, pp. 348–351. doi: 10.1109/TENSYMP50017.2020.9230987.

[68] Ahmed Ghonima, “How do torrents work? (P2P networking),” LinkedIn. Accessed: Oct. 18, 2023. [Online]. Available: https://www.linkedin.com/pulse/how-do-torrents-work-p2p-networking-ahmed-ghanima/

[69] L. Wang, X. Shen, J. Li, J. Shao, and Y. Yang, “Cryptographic primitives in blockchains,” *J. Netw. Comput. Appl.*, vol. 127, pp. 43–58, Feb. 2019, doi: 10.1016/j.jnca.2018.11.003.

[70] A. N. Clark Jeremy, “Bitcoin’s Academic Pedigree.” Accessed: Oct. 18, 2023. [Online]. Available: https://cacm.acm.org/magazines/2017/12/223058-bitcoins-academic-pedigree/fulltext?mobile=false

[71] D. Tosh, S. Shetty, X. Liang, C. Kamhoua, and L. L. Njilla, “Data Provenance in the Cloud: A Blockchain-Based Approach,” *IEEE Consum. Electron. Mag.*, vol. 8, no. 4, pp. 38–44, Jul. 2019, doi: 10.1109/MCE.2019.2892222.

[72] E. Paul, “What is Digital Signature: How it works, Benefits, Objectives, Concept,” EMP Trust HR. Accessed: Oct. 18, 2023. [Online]. Available: https://www.emptrust.com/blog/benefits-of-using-digital-signatures/

[73] D. Johnson, A. Menezes, and S. Vanstone, “The Elliptic Curve Digital Signature Algorithm (ECDSA),” *Int. J. Inf. Secur.*, vol. 1, no. 1, pp. 36–63, Aug. 2001, doi: 10.1007/s102070100002.

[74] S. Josefsson and I. Liusvaara, “Edwards-Curve Digital Signature Algorithm (EdDSA),” Internet Engineering Task Force, Request for Comments RFC 8032, Jan. 2017. doi: 10.17487/RFC8032.

[75] S. Wang *et al.*, “Blockchain-Powered Parallel Healthcare Systems Based on the ACP Approach,” *IEEE Trans. Comput. Soc. Syst.*, vol. 5, no. 4, pp. 942–950, Dec. 2018, doi: 10.1109/TCSS.2018.2865526.

[76] Ahmad Akmaluddin Mazlan, Salwani Mohd Daud, Suriani Mohd Sam, Hafiza Abas, Siti Zaleha Abdul Rasid, and Muhammad Fathi Yusof, “Scalability Challenges in Healthcare Blockchain System—A Systematic Review,” *IEEE Access*, vol. 8, pp. 23663–23673, Jan. 2020, doi: 10.1109/ACCESS.2020.2969230.

[77] N. Biedrzycki, “Will blockchain transform the stock market?,” Medium. Accessed: Oct. 18, 2023. [Online]. Available: https://n-biedrzycki.medium.com/will-blockchain-transform-the-stock-market-d888c60aab00

[78] A. I. Sanka, M. Irfan, I. Huang, and R. C. C. Cheung, “A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research,” *Comput. Commun.*, vol. 169, pp. 179–201, Mar. 2021, doi: 10.1016/j.comcom.2020.12.028.

[79] “ASX CHESS replacement,” ASX services. Accessed: Oct. 18, 2023. [Online]. Available: https://www.asx.com.au/markets/clearing-and-settlement-services/chess-replacement

[80] K. O.-B. Obour Agyekum *et al.*, “V-Chain: A Blockchain-Based Car Lease Platform,” in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Comp. Commun. (GreenCom) and IEEE Cyber, Phys. Social Comput. (CPSCom) and IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1317–1325. doi: 10.1109/Cybermatics_2018.2018.00228.

[81] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, “Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring,” *J. Med. Syst.*, vol. 42, no. 7, p. 130, Jun. 2018, doi: 10.1007/s10916-018-0982-x.

[82] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, “FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data,” *Comput. Struct. Biotechnol. J.*, vol. 16, pp. 267–278, Jan. 2018, doi: 10.1016/j.csbj.2018.07.004.

[83] A. Roehrs, C. A. da Costa, and R. da Rosa Righi, “OmniPHR: A distributed architecture model to integrate personal health records,” *J. Biomed. Inform.*, vol. 71, pp. 70–81, Jul. 2017, doi: 10.1016/j.jbi.2017.05.012.

[84] S. Chenthara, K. Ahmed, H. Wang, F. Whittaker, and Z. Chen, “Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology,” *PLOS ONE*, vol. 15, no. 12, p. e0243043, Dec. 2020, doi: 10.1371/journal.pone.0243043.

[85] R. Abujamra and D. Randall, “Chapter Five - Blockchain applications in healthcare and the opportunities and the advancements due to the new information technology framework,” in *Advances in Computers*, vol. 115, S. Kim, G. C. Deka, and P. Zhang, Eds., in Role of Blockchain Technology in IoT Applications, vol. 115. , Elsevier, 2019, pp. 141–154. doi: 10.1016/bs.adcom.2018.12.002.

[86] T. McGhin, K.-K. R. Choo, C. Z. Liu, and D. He, “Blockchain in healthcare applications: Research challenges and opportunities,” *J. Netw. Comput. Appl.*, vol. 135, pp. 62–75, Jun. 2019, doi: 10.1016/j.jnca.2019.02.027.

[87] M. Raikwar, S. Mazumdar, S. Ruj, S. Sen Gupta, A. Chattopadhyay, and K.-Y. Lam, “A Blockchain Framework for Insurance Processes,” in *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, Feb. 2018, pp. 1–4. doi: 10.1109/NTMS.2018.8328731.

[88] Jeff John Roberts, “Microsoft and Accenture Unveil Global ID System for Refugees,” Yahoo Finance. Accessed: Oct. 19, 2023. [Online]. Available: https://finance.yahoo.com/news/microsoft-accenture-unveil-global-id-150051556.html

[89] C. DENMARK and A. NY, “TradeLens blockchain-enabled digital shipping platform continues expansion with addition of major ocean carriers Hapag-Lloyd and Ocean Network Express,” IBM Newsroom. Accessed: Oct. 19, 2023. [Online]. Available: https://www.maersk.com/news/articles/2019/07/02/hapag-lloyd-and-ocean-network-express-join-tradelens

[90] X. Xu, N. Tian, H. Gao, H. Lei, Z. Liu, and Z. Liu, “A Survey on Application of Blockchain Technology in Drug Supply Chain Management,” in *2023 IEEE 8th International Conference on Big Data Analytics (ICBDA)*, Mar. 2023, pp. 62–71. doi: 10.1109/ICBDA57405.2023.10104779.

[91] “GrainChain.” Accessed: Oct. 19, 2023. [Online]. Available: https://www.grainchain.io/

[92] Ravikant Agrawal, “DAO - Democratizing ownership of organization through smart contract on blockchain,” LinkedIn. Accessed: Oct. 19, 2023. [Online]. Available: https://www.linkedin.com/pulse/dao-democratizing-ownership-organization-through-smart-agrawal/

[93] “Globally Distributed Cloud Object Storage.” Accessed: Oct. 19, 2023. [Online]. Available: https://www.storj.io/

[94] E. Karaarslan and E. Adiguzel, “Blockchain Based DNS and PKI Solutions,” *IEEE Commun. Stand. Mag.*, vol. 2, no. 3, pp. 52–57, Sep. 2018, doi: 10.1109/MCOMSTD.2018.1800023.

[95] Vaibhav Saini, “StoragePedia: An Encyclopedia of 5 Blockchain Storage Platforms,” HackerNoon. Accessed: Oct. 19, 2023. [Online]. Available: https://hackernoon.com/storagepedia-an-encyclopedia-of-5-blockchain-storage-platform-8aa13c630ace

[96] R. Li, T. Song, B. Mei, H. Li, X. Cheng, and L. Sun, “Blockchain for Large-Scale Internet of Things Data Storage and Protection,” *IEEE Trans. Serv. Comput.*, vol. 12, no. 5, pp. 762–771, Sep. 2019, doi: 10.1109/TSC.2018.2853167.

[97] S. Al-Mashhadi and S. Manickam, “A brief review of blockchain-based DNS systems,” *Int. J. Internet Technol. Secur. Trans.*, vol. 10, no. 4, pp. 420–432, Jan. 2020, doi: 10.1504/IJITST.2020.108134.

[98] “Namecoin.” Accessed: Oct. 19, 2023. [Online]. Available: https://www.namecoin.org/

[99] G. Khachatryan, “Blockstack: A New Internet for Decentralized Apps,” Medium. Accessed: Oct. 19, 2023. [Online]. Available: https://grigorkh.medium.com/blockstack-a-new-internet-for-decentralized-apps-1f21cb9179b9

[100] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, “Blockchain challenges and opportunities: A survey,” *Int. J. Web Grid Serv.*, vol. 14, p. 352, Oct. 2018, doi: 10.1504/IJWGS.2018.095647.

[101] “Blockchain Size (MB),” Blockchain.com. Accessed: Oct. 19, 2023. [Online]. Available: https://www.blockchain.com/explorer/charts/blocks-size

[102] “Visa and Swift Team Up to Enhance Transparency, Speed and Security in Global B2B Money Movement,” Business Wire. Accessed: Oct. 19, 2023. [Online]. Available: https://kommunikasjon.ntb.no/pressemelding/18000543/visa-and-swift-team-up-to-enhance-transparency-speed-and-security-in-global-b2b-money-movement?publisherId=90063

[103] “1 Second - Internet Live Stats.” Accessed: Oct. 19, 2023. [Online]. Available: https://www.internetlivestats.com/one-second/

[104] Q. Zhou, H. Huang, Z. Zheng, and J. Bian, “Solutions to Scalability of Blockchain: A Survey,” *IEEE Access*, vol. 8, pp. 16440–16455, 2020, doi: 10.1109/ACCESS.2020.2967218.

[105] Y. Marcus, E. Heilman, and S. Goldberg, “Low-Resource Eclipse Attacks on Ethereum’s Peer-to-Peer Network.” 2018. Accessed: Oct. 19, 2023. [Online]. Available: https://eprint.iacr.org/2018/236

[106] M. Saad *et al.*, “Exploring the Attack Surface of Blockchain: A Comprehensive Survey,” *IEEE Commun. Surv. Tutor.*, vol. 22, no. 3, pp. 1977–2008, 2020, doi: 10.1109/COMST.2020.2975999.

[107] “Once hailed as unhackable, blockchains are now getting hacked,” MIT Technology Review. Accessed: Oct. 19, 2023. [Online]. Available: https://www.technologyreview.com/2019/02/19/239592/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/

[108] N. Atzei, M. Bartoletti, and T. Cimoli, “A Survey of Attacks on Ethereum Smart Contracts (SoK),” in *Principles of Security and Trust*, M. Maffei and M. Ryan, Eds., in Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2017, pp. 164–186. doi: 10.1007/978-3-662-54455-6_8.

[109] S. Goldfeder, H. Kalodner, D. Reisman, and A. Narayanan, “When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies,” *Proc. Priv. Enhancing Technol.*, vol. 2018, Aug. 2017, doi: 10.1515/popets-2018-0038.

[110] M. Wu, K. Wang, X. Cai, S. Guo, M. Guo, and C. Rong, “A Comprehensive Survey of Blockchain: From Theory to IoT Applications and Beyond,” *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8114–8154, Oct. 2019, doi: 10.1109/JIOT.2019.2922538.

[111] “What are zk-SNARKs?,” Z.Cash. Accessed: Oct. 19, 2023. [Online]. Available: https://z.cash/learn/what-are-zk-snarks/

[112] M. C. Kus Khalilov and A. Levi, “A Survey on Anonymity and Privacy in Bitcoin-Like Digital Cash Systems,” *IEEE Commun. Surv. Tutor.*, vol. 20, no. 3, pp. 2543–2585, 2018, doi: 10.1109/COMST.2018.2818623.

[113] M. Conti, E. Sandeep Kumar, C. Lal, and S. Ruj, “A Survey on Security and Privacy Issues of Bitcoin,” *IEEE Commun. Surv. Tutor.*, vol. 20, no. 4, pp. 3416–3452, 2018, doi: 10.1109/COMST.2018.2842460.

[114] vbuterin, “On-chain scaling to potentially ~500 tx/sec through mass tx validation - Applications,” Ethereum Research. Accessed: Oct. 19, 2023. [Online]. Available: https://ethresear.ch/t/on-chain-scaling-to-potentially-500-tx-sec-through-mass-tx-validation/3477

[115] “Privacy-first ZkRollup On Ethereum.” Accessed: Oct. 19, 2023. [Online]. Available: https://aztec.network/

[116] M. H. Au, W. Susilo, and Y. Mu, “Constant-Size Dynamic k-TAA,” in *Security and Cryptography for Networks*, vol. 4116, R. De Prisco and M. Yung, Eds., in Lecture Notes in Computer Science, vol. 4116. , Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 111–125. doi: 10.1007/11832072_8.

[117] M. Swan, *Blockchain: Blueprint for a New Economy*, 1st ed. O’Reilly Media, Inc., 2015.

[118] “How Will Quantum Supremacy Affect Blockchain?,” Consensys. Accessed: Oct. 19, 2023. [Online]. Available: https://consensys.net/blog/developers/how-will-quantum-supremacy-affect-blockchain/

[119] E. O. Kiktenko *et al.*, “Quantum-secured blockchain,” *Quantum Sci. Technol.*, vol. 3, no. 3, p. 035004, Jul. 2018, doi: 10.1088/2058-9565/aabc6b.

[120] PricewaterhouseCoopers, “Blockchain is here. What’s your next move?,” PwC. Accessed: Oct. 19, 2023. [Online]. Available: https://www.pwc.com/jg/en/publications/blockchain-is-here-next-move.html

[121] MARIE HUILLET, “EY: Blockchain Not Understood by Almost 70% of Firms in Asia-Pacific,” Cointelegraph. Accessed: Oct. 19, 2023. [Online]. Available: https://cointelegraph.com/news/ey-blockchain-not-understood-by-almost-70-of-firms-in-asia-pacific

[122] “Deloitte’s 2019 Global Blockchain Survey.” Accessed: Oct. 19, 2023. [Online]. Available: https://www.deloitte.com/za/en/Industries/technology/analysis/blockchain-gets-down-to-business.html

[123] S. Sayeed and H. Marco-Gisbert, “Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack,” *Appl. Sci.*, vol. 9, no. 9, Art. no. 9, Jan. 2019, doi: 10.3390/app9091788.

[124] C. Grunspan and R. Pérez-Marco, “On profitability of selfish mining.” arXiv, Jan. 22, 2019. doi: 10.48550/arXiv.1805.08281.

[125] M. Saad, L. Njilla, C. Kamhoua, and A. Mohaisen, “Countering Selfish Mining in Blockchains,” in *2019 Int, Conf. Comp., Network. Commun. (ICNC)*, Feb. 2019, pp. 360–364. doi: 10.1109/ICCNC.2019.8685577.

[126] S. Kim and S.-G. Hahn, “Mining Pool Manipulation in Blockchain Network Over Evolutionary Block Withholding Attack,” *IEEE Access*, vol. 7, pp. 144230–144244, Mar. 2019, doi: 10.1109/ACCESS.2019.2945600.

[127] A. Hafid, A. S. Hafid, and M. Samih, "A Tractable Probabilistic Approach to Analyze Sybil Attacks in Sharding-Based Blockchain Protocols," *IEEE Trans. Emerg. Top. Comput.*, vol. 11, no. 1, pp. 126–136, Jan. 2023, doi: 10.1109/TETC.2022.3179638.

[128] R. Chaganti *et al.*, "A Comprehensive Review of Denial of Service Attacks in Blockchain Ecosystem and Open Challenges," *IEEE Access*, vol. 10, pp. 96538–96555, Mar. 2022, doi: 10.1109/ACCESS.2022.3205019.

[129] L. S. Sankar, M. Sindhu, and M. Sethumadhavan, "Survey of consensus protocols on blockchain applications," in *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*, Jan. 2017, pp. 1–5. doi: 10.1109/ICACCS.2017.8014672.

[130] J. H. Park and J. H. Park, "Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions," *Symmetry*, vol. 9, no. 8, Art. no. 8, Aug. 2017, doi: 10.3390/sym9080164.

[131] T. T. Huynh, T. D. Nguyen, and H. Tan, "A Survey on Security and Privacy Issues of Blockchain Technology," in *2019 International Conference on System Science and Engineering (ICSSE)*, Jul. 2019, pp. 362–367. doi: 10.1109/ICSSE.2019.8823094.

[132] D. Dave, S. Parikh, R. Patel, and N. Doshi, "A Survey on Blockchain Technology and its Proposed Solutions," *Procedia Comput. Sci.*, vol. 160, pp. 740–745, Jan. 2019, doi: 10.1016/j.procs.2019.11.017.

[133] D. Dasgupta, J. Shrein, and K. D. Gupta, "A survey of blockchain from security perspective," *J. Bank. Financ. Technol.*, vol. 3, Jan. 2019, doi: 10.1007/s42786-018-00002-6.

[134] E. J. De Aguiar, B. S. Faiçal, B. Krishnamachari, and J. Ueyama, "A Survey of Blockchain-Based Strategies for Healthcare," *ACM Comput. Surv.*, vol. 53, no. 2, p. 27:1-27:27, Mar. 2020, doi: 10.1145/3376915.

[135] J. Leng, M. Zhou, J. L. Zhao, Y. Huang, and Y. Bian, "Blockchain Security: A Survey of Techniques and Research Directions," *IEEE Trans. Serv. Comput.*, vol. 15, no. 4, pp. 2490–2510, Jul. 2022, doi: 10.1109/TSC.2020.3038641.

[136] B. Bhushan, P. Sinha, K. M. Sagayam, and A. J, "Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions," *Comput. Electr. Eng.*, vol. 90, p. 106897, Mar. 2021, doi: 10.1016/j.compeleceng.2020.106897.

[137] M. N. M. Bhutta *et al.*, "A Survey on Blockchain Technology: Evolution, Architecture and Security," *IEEE Access*, vol. 9, pp. 61048–61073, Aug. 2021, doi: 10.1109/ACCESS.2021.3072849.

[138] A. S. Rajasekaran, M. Azees, and F. Al-Turjman, "A comprehensive survey on blockchain technology," *Sustain. Energy Technol. Assess.*, vol. 52, Art. no. 102039, Aug. 2022, doi: 10.1016/j.seta.2022.102039.

[139] H. Guo and X. Yu, "A survey on blockchain technology and its security," *Blockchain Res. Appl.*, vol. 3, no. 2, Art. no. 100067, Jun. 2022, doi: 10.1016/j.bcra.2022.100067.

[140] C. Zhu, J. Li, Z. Zhong, C. Yue, and M. Zhang, "A Survey on the Integration of Blockchains and Databases," *Data Sci. Eng.*, vol. 8, no. 2, pp. 196–219, Jun. 2023, doi: 10.1007/s41019-023-00212-z.