Al-Salam Journal for Engineering and Technology
Journal Homepage: http://journal.alsalam.edu.iq/index.php/ajest
e-ISSN: 2790-4822 p-ISSN: 2958-0862

An Overview of Blockchain Technology in Architecture and Consensus with Key Advances

Abbas Fadhil Mahdi[1]*, Furkan Rabee[1]

[1]Computer Science Department, Faculty of Computer Science and Mathematics, University of Kufa, Najaf, Iraq.

*Corresponding Author: Abbas Fadhil Mahdi

DOI: https://doi.org/10.55145/ajest.2025.04.01.020
Received November 2024; Accepted January 2025; Available online January 2025

ABSTRACT: Blockchain has revolutionized cryptocurrency since the advent of Bitcoin. Due to its decentralized nature, transparency, security measures, and ability to conduct transactions between untrusted parties, blockchain has received extensive attention recently. Consensus algorithms manage the blockchain and describe how peers achieve data consistency and integration. However, other hurdles persist for blockchain systems, including scalability and energy consumption, and they require to be overcome. The paper introduces a comprehensive overview of distributed ledger technologies (DLTs) with a deeper understanding of the blockchain. Moreover, we conduct a comparative analysis of the most widespread consensus mechanisms using various metrics. And briefly list potential threats, applications across several fields, and possible future directions.

Keywords: Distributed Ledger Technology DLT, Blockchain, Cryptocurrency, Bitcoin

1. INTRODUCTION

Since its introduction and implementation in 2009 by Satoshi Nakamoto, Bitcoin has sparked numerous discussions about its success as a pioneering cryptocurrency, its widespread adoption, and the technological aspects that contributed to it [1]. Bitcoin's underlying blockchain paradigm, which eliminates the need for a mediator and allows for the creation of collaborative financial models, shared storage, and agreement governance, has garnered great attention from many academics for its unique characteristic [2]. After Bitcoin's success, many cryptocurrencies followed Ethereum, ranked second in financial trading, and BNB third, reaching more than 9,000 cryptocurrencies worldwide, according to Statista [3]. At its core, Blockchain is a form of Distributed Ledger Technology (DLT) that allows for secure, transparent, and tamper-resistant storage of transactions across nodes within a P2P network. This innovative technology has transformed the handling of data and transactions in the digital realm [4]. Its applications go beyond cryptocurrency, impacting areas like e-voting, healthcare, the Internet of Things, government services, and agriculture, among other sectors [5].

Blockchain consists of a series of blocks, each containing a collection of transactions. Each block holds a unique hash, a timestamp, and the hash of the previous block, creating a cryptographically linked, continuous chain that resists tampering and fraud. This structure ensures that once a transaction is recorded within a block, it cannot be altered without affecting all following blocks. Additionally, it preserves data integrity and the chronological order of blocks, which rely on the consensus of the majority of network participants [6].

In blockchain technology, the consensus mechanism is a process that enables network participants to agree on the validity of transactions and the ledger's current state. This ensures that all copies of the blockchain remain accurately updated and verified. Nodes within the network, known as miners or validators, participate in this process by validating and approving transactions before they are added to the blockchain, using specific consensus algorithms [7].Typical consensus mechanisms include Proof of Work (PoW), Proof of Stake (PoS), and others, which help prevent fraudulent activities and ensure that transactions are validated by a majority of nodes, thus maintaining the blockchain's integrity and security. By requiring consensus from numerous independent participants, blockchain technology offers a trustless system that removes the need for a central authority [8].

*Corresponding author: abbassf.wahab@uokufa.edu.iq

2. DISTRIBUTED LEDGER TECHNOLOGY (DLT)

Distributed Ledger Technology (DLT) is a digital framework enabling decentralized and synchronized management of a shared database or ledger across multiple participants or nodes [9]. It aims to provide a transparent, secure, and immutable record of transactions or other data types. DLT operates on a decentralized peer-to-peer (P2P) network, where each participant holds a copy of the ledger and collaboratively verifies and updates its content through a consensus mechanism [10]. A defining feature of DLT is its decentralized structure across numerous nodes, eliminating the need for a central authority or intermediary to validate and store data. Figure 1 demonstrates the architecture of DLT.

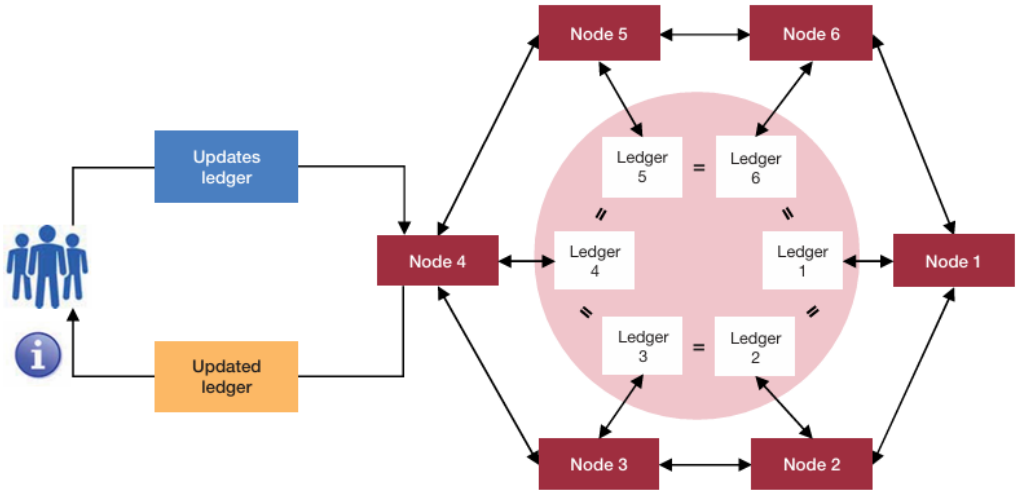

FIGURE 1. - Distributed Ledger Technology (DLT) platform [11]

This system's decentralized architecture enhances transparency, security, and resilience by reducing the risk of a single point of failure or potential manipulation [12]. Participants in a DLT network work together to uphold the ledger's integrity, ensuring the recorded data remains accurate and consistent. DLT often employs cryptographic techniques to protect data and transactions stored on the ledger, utilizing tools like cryptographic hashing, digital signatures, and consensus algorithms. These methods enable nodes to agree on the order and validity of transactions, safeguarding the system's reliability [13].

Figure 2 illustrates two types of network topologies commonly used in distributed systems. Figure 2 (a) illustrates a fully connected peer-to-peer network in which each node directly communicates with every other node, ensuring decentralized communication and redundancy, such as cryptocurrencies. In contrast, figure 2 (b) shows a centralized or hub-and-spoke model, where a central node coordinates communication with peripheral nodes, allowing data exchange but introducing a single point of control, such as a bank. These topologies represent different approaches to network design, with the former offering more distributed resilience and the latter providing more efficient, centralized coordination.

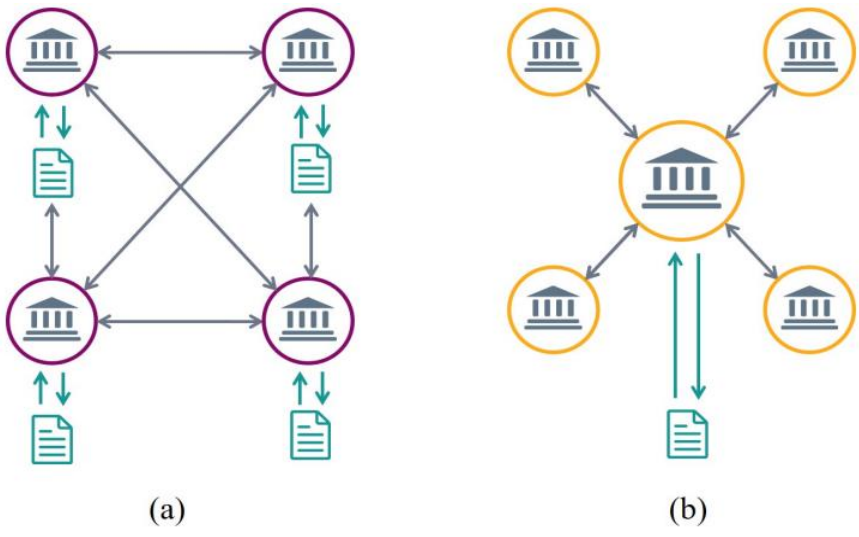

FIGURE 2. - (a) Distributed Ledger, (b) Centralized Ledger [14]

We can categorize distributed ledger technology, which encompasses a variety of mechanisms that enable the decentralized and synchronized management of a shared digital ledger, into two basic models as follows:

2.1 DLT PERMISSIONS MODELS

DLT can be categorized into four kinds based on permissions models, which determine the network's participants and their access to the ledger, Figure 3 demonstrates this categorized.

a. Public distributed ledger technologies

Public Distributed Ledger Technologies (PDLTs), such as Bitcoin and, function based on an open and permissionless framework. This means that any individual can become a participant in the network and verify transactions. These systems utilize consensus procedures such as Proof of Work (PoW) or Proof of Stake (PoS) to guarantee the integrity of the ledger [15].

b. Private distributed ledger technologies

Only authorized participants can view and participate in Private Distributed Ledger Technologies (PrDLTs) like Monax and Hyperledger Fabric, setting them apart from other systems. Authorized entities can only join the network and verify transactions, which makes it perfect for enterprise environments that prioritize privacy, scalability, and access control [16].

c. Consortiums distributed ledger technologies

Consortiums Distributed Ledger Technologies (CDLTs) can be described as a hybrid category that incorporates features from both public and private models. A CDLT involves a collective of organizations or entities that share the responsibility of governing the network and keeping the ledger. The participants, who possess equal rights and obligations, work together to reach an agreement and maintain the integrity of the ledger. R3 and Corda, when used in consortium mode, and certain Hyperledger Fabric implementations are examples of CDLTs. By uniting reliable organizations, CDLTs offer a compromise between public transparency and private control. This makes them well-suited for situations that demand secure cooperation and data exchange within a predetermined group [17].

d. Hybrid distributed ledger technologies

This kind of chain strives (HDLTs)to harness the benefits of both private and public models, striking a balance between transparency and control. It allows the public to access certain parts of the blockchain for transparency and verification while restricting other parts to specific participants for privacy and confidentiality. Hospitals and health centers manage healthcare data as an example of the hybrid model. The flexibility of the hybrid approach enables institutions to tailor blockchain designs to their specific needs, granting them control over chain participation and information access. Ripple(XRP) and XinFin (XDC Network) are examples of this approach [18].

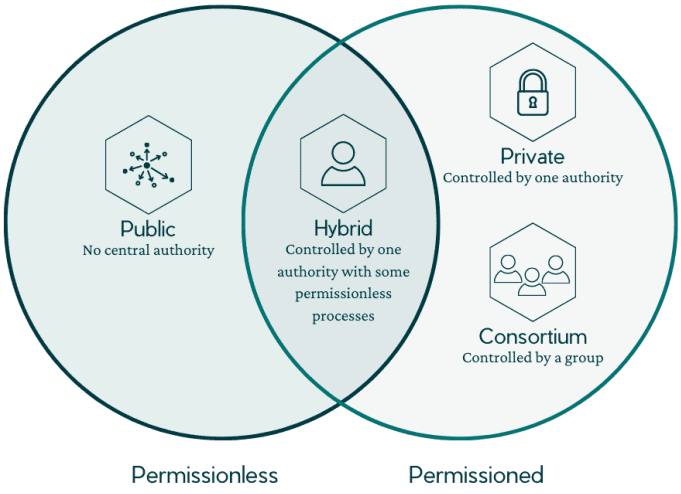

FIGURE 3. - The models of DLTpermissions [19]

The main difference between consortiums and hybrid chains is governance and control. Consortium chains are subject to shared control by a specific set of entities, while hybrid chains combine the advantages of both public and private chains, providing transparency and selective privacy. Table 1 describes the characteristics of DLT permissions models.

Table 1. - Characteristics of DLT permissions models [20]

Category	Permissioned	Permissionless
Access	Controlled by one authority or managed shared among two or more individuals or companies	Open to everyone
Secure	Less secure	More secure
Decentralized	Partially	Full
Read permission	Could be public or restrict	Public
Efficiency	High	Low
Privacy	Exclusive membership	transparent and open to all
Cost	cost-effective solution	Highly costly
Immutability	Could be impacted	Extremely difficult to manipulate
Energy	More Environmental	Energy consumption
Consensus determination	One authority or pre-selected participants	All miners
Consensus mechanisms	PBFT, Raft, etc.	PoW, PoS, DPoS, etc.

Table2. - Comparison of a few cryptocurrencies [21]

Permission Type	Trust Level	Cryptocurrency	Consensus Algorithm
Permission	Trust	Neo	Delegated Byzantine Fault Tolerance
	Trust	Icon	Loop Fault Tolerance
	Trust	WTC	Hybrid Proof of Work\Stake
	Trust	EOS	Delegated Proof of Stake
	Trust	Ark	Delegated Proof of Stake
	Trust	Lisk	Delegated Proof of Stake
	Trust	VeChain	Proof of Authority
	Trust	Nuls	Proof of capacity
	Distrust	Hashgraph	Asynchronous BFT
Permissionless	Distrust	Bitcoin	Proof of Work
	Distrust	Litecoin	Proof of Work
	Distrust	Dogecoin	Proof of Work
	Distrust	Monero	Proof of Work
	Trust	Stellar	Practical Byzantine Fault Tolerance
	Trust	XRP	N/A
	Distrust	Nano	Proof of Stake
	Distrust	Cardano	Delegated Proof of Stake
	Distrust	Decred	Hybrid Proof of Work\Stake
	Distrust	Zilliqa	Practical Byzantine Fault Tolerance
	Distrust	Elastos	Delegated Proof of Stake
	Distrust	IOTA	N/A

Table 2 categorizes various cryptocurrencies based on their permission models, trust levels, and consensus mechanisms. Permissioned cryptocurrencies generally operate in a trusted environment, relying on specific consensus mechanism such as DPoS, PoA, or other unique models like dBFT for Neo. These systems require some degree of control or verification by known participants [22]. On the other hand, permissionless cryptocurrencies, which include Bitcoin, Ethereum, and Litecoin, use Proof of Work (PoW) and function in a trustless, open environment, allowing any user to participate without prior approval. Other trustless systems use innovative approaches like DAG for IOTA or DPoS for Cardano to secure their networks. There are also hybrid systems, such as Decred, that integrate PoW and PoS, combining the advantages of both to achieve security and scalability. The distinction in permission and trust levels ultimately reflects different priorities in decentralization, scalability, and control among these cryptocurrencies.

2.2 DLT STRUCTURE MODELS

The underlying data structure that DLTs use is the second aspect of the categorization model, which is explained briefly and shown in Figure 4.

a. Blockchain

The most renowned kind of DLT employs a sequence of blocks, each of which has a roster of transactions. Cryptographic hashes connect the blocks to create an unchangeable ledger. They use efficient consensus techniques like PoW, PoS, PBFT, etc., to authenticate and add new blocks to the chain [23].

b. Directed acyclic graph (dag)

DAG is another type of distributed ledger technologies DLTs that deviates from the linear structure of blockchain. DAG-based ledgers depict transactions as nodes within a graph, with edges indicating the interdependencies between transactions. DAG-based systems seek to enhance scalability and expedite transaction processing by facilitating parallel processing rather than following a linear chain structure and eliminating the requirement for conventional miners. And are considered a very efficient approach for IoT infrastructures [24].

c. Hashgraph

Swirlds developed Hashgraph, which uses a unique consensus method and data structure to efficiently validate and sequence transactions. Hashgraph employs a gossip protocol in which nodes swiftly distribute information regarding transactions among each other [25]. By engaging in multiple rounds of gossip and virtual voting, Hashgraph nodes reach a collective agreement on the sequence of transactions, thereby attaining consensus without relying on resource-intensive proof-of-work procedures. Key advantages of this approach over previous DLT alternatives are high throughput, low latency, and fairness in transaction sequencing [9].

d. Holochain

Holochain is an innovative framework for DLT that distinguishes itself with its agent-centric architecture and focus on peer-to-peer networking principles. It grants more independence to network users and ensures data integrity using cryptographic security measures. Within the Holochain framework, every individual node has its own hash chain, which contains data that is pertinent to its engagements with other nodes. The decentralized method of data management allows for scalability enhancements, as nodes are not required to process and store the complete ledger [26].

e. Radix

The architecture of the radix depends on the concept of sharding, which divides the participant's network into smaller pieces called shards and manageable parts called shards, which enable it to process transactions in parallel. The radix stores transactions through a non-linear graph structure and maintains a global ledger that is synchronized via the shards. Tempo is Radix's consensus mechanism designed to provide deterministic finality to transactions by tracking the logical order of events [27].

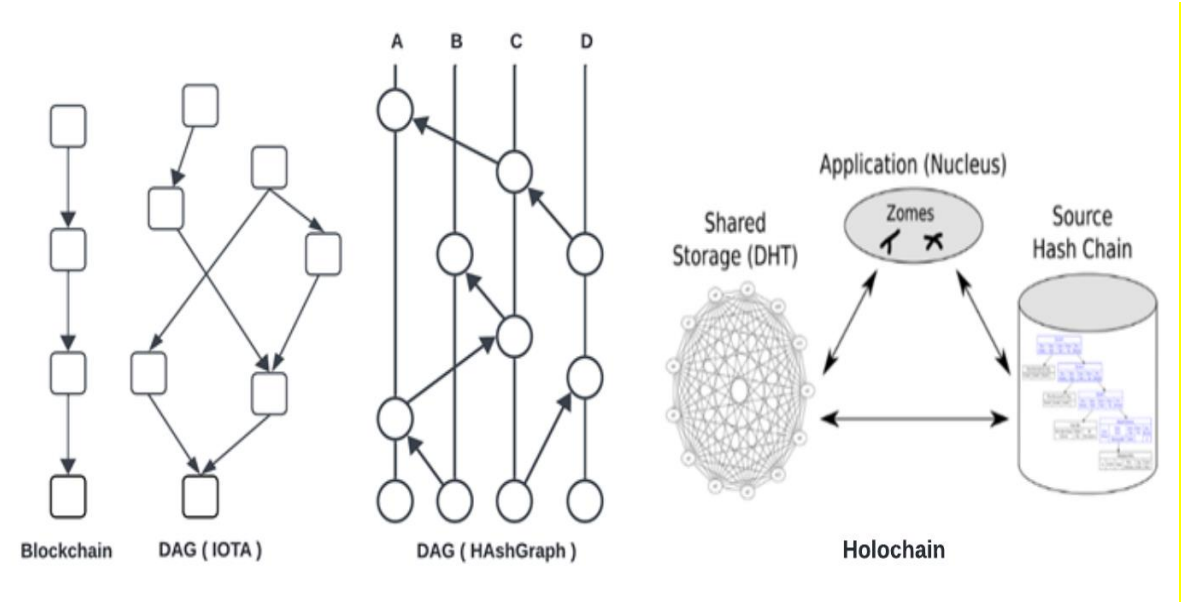

FIGURE 4. -The models of DLT structures [27, 28]

3. BLOCKCHAIN OVERVIEW

Stuart Haber and W. Scott Stometta introduced the term "blockchain" in 1991 under the title of the article ("How to time-stamp a digital document") [27]. It involves a dynamic growth of data structures, known as blocks, that are connected and secure cryptographically with each other. The blockchain distributes information in a decentralized manner, preventing tampering and maintaining its immutability and transparency. Bitcoin, followed by Ethereum, are the most notable applications of this technology [29].

Unlike traditional centralized systems, blockchain is characterized by its decentralization, transparency, immutability, and security. Decentralization entails the absence of a singular authority managing the network, which fosters cooperation, eliminates single points of failure, and enhances data integrity. Transparency allows all transactions to be visible to all network participants, thereby promoting trust. Immutability guarantees that once a transaction is stored, it becomes exceedingly challenging to change or remove, thereby ensuring that the ledger remains secure and resistant to tampering. Cryptographic techniques such as hashing and digital signatures ensure the blockchain's security [30].

Blocks within the blockchain include valuable information in addition to a link to the preceding block. A hash256, a fixed-length cryptographic hash function, typically represents this connection and acts as a unique identifier for the block. Figure 5 illustrates the "Genesis Block," which is the first block of a blockchain that acts as the fundamental building block for the whole chain.

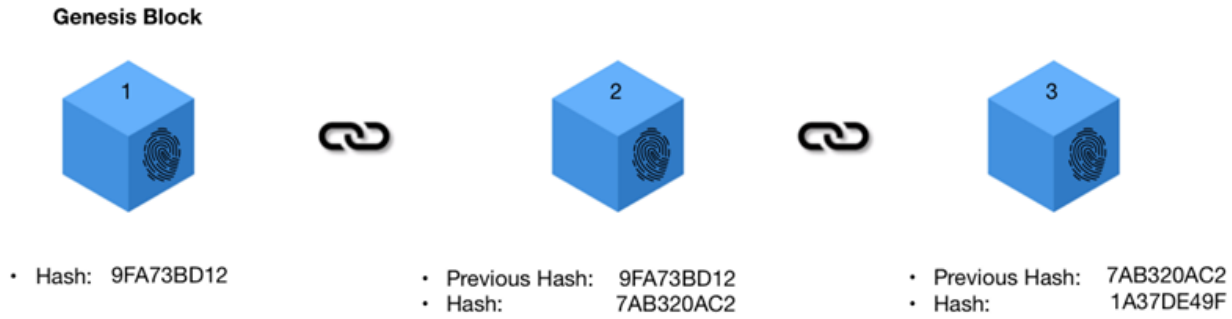

FIGURE 5. - Blockchain general architecture [30]

3.1 THE FUNDAMENTAL COMPONENTS OF BLOCKCHAIN

The key elements of blockchain will be explained in detail as follows:

1. Block

Each block in a blockchain has a similar structure, but the data it contains differs. To understand a blockchain block, we can break it down into two main components [31]:

a. Block Header

- Block Number: This indicates the block's position in the blockchain sequence.
- Previous Block Hash: This is the hash value of the preceding block, ensuring the integrity and immutability of the blockchain.
- Current Block Hash: The hash value of the current block after validation.
- Timestamp: The exact time the block was created, helping to arrange the blocks chronologically.
- Difficulty Target: This adjusts the required number of leading zeros in the block's hash to regulate the rate of block creation based on network conditions.
- Nonce: A variable used by miners to find a hash value that satisfies the network's difficulty target during mining.
- Merkle Root: The top hash in the Merkle tree, summarizing all transaction hashes in the block, ensuring data integrity with a 256-bit hash.

b. Block Body

- List of Transactions: This contains the validated transactions added to the block, with each transaction including:
- Sender and Receiver Address: Public addresses of the participants involved in the transaction.
- Digital Signatures: A cryptographic signature confirming the authenticity of the transaction, ensuring it is tamper-proof.
- Amount: The quantity of coins or data transferred.
- Transaction Fee: The fee paid to miners for including the transaction in the block.
- Transaction ID: A unique identifier generated by hashing, used to reference the specific transaction.
- Merkle Tree Structure: A hierarchical structure of transaction hash values, used for efficient verification of the integrity of the transactions.

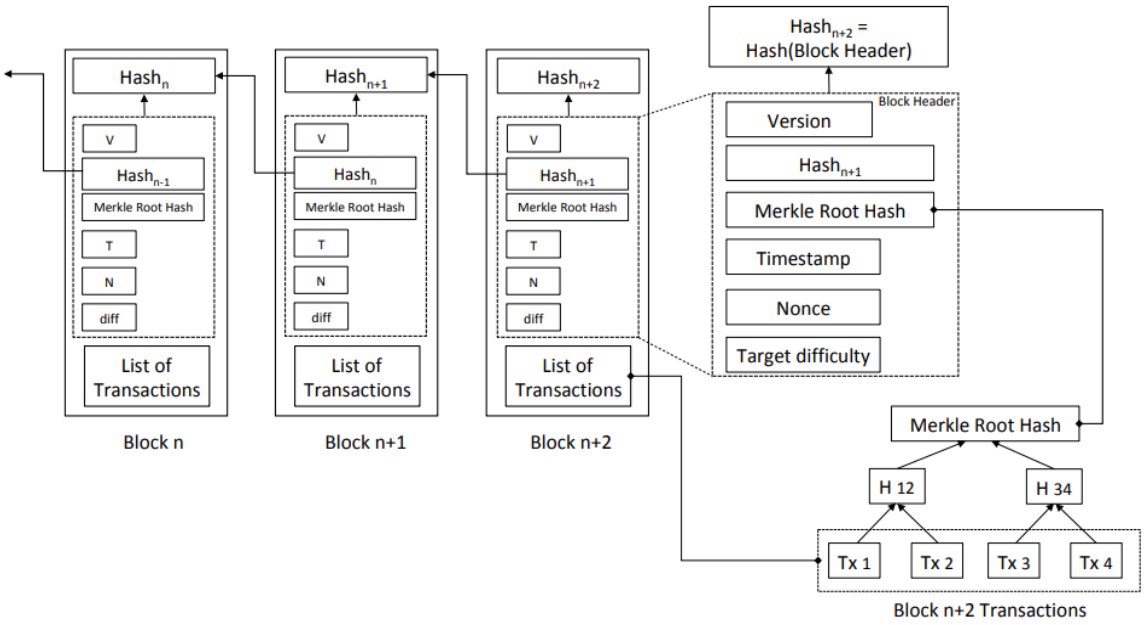

FIGURE 6. - Blockchain general architecture [32]

Figure 6 illustrates the structure of sequential blocks within a blockchain, where each block contains a header and a series of transactions. The block header consists of fields such as the version, the hash of the previous block (creating a link to the prior block), the Merkle root hash (which summarizes all transactions within the block through a Merkle tree), the timestamp, the nonce (utilized for Proof of Work), and the target difficulty level. The hash of each block header acts as a unique identifier and is referenced by the subsequent block to maintain a secure, continuous chain. For instance, block n+2 includes four transactions (Tx1, Tx2, Tx3, Tx4), whose hashes are merged to create a Merkle root. This setup preserves data integrity and immutability by cryptographically connecting each block, making unauthorized alterations difficult to achieve.

2. Miners

It is an individual or organization that uses computational power to collect transactions from the network, validate them, and form blocks to append later in the blockchain. The validation process involves verifying the legality of transactions, verifying the sender's sufficient balance, and confirming that the transactions comply with network requirements. Miners are crucial to ensuring the network's security and functionality [33]. Figure 7 shows the sequential steps of the miner's role in dealing with transactions.

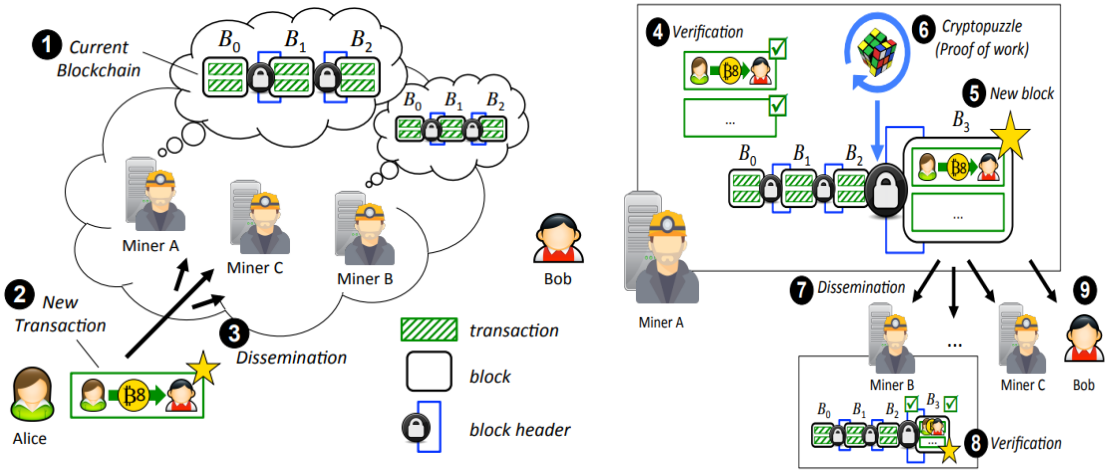

FIGURE 7. - life cycle of transaction and the role of a miner [34]

3. Consensus algorithms

In distributed systems, network participants, known as "Full nodes or Miners," use consensus protocols to reach an agreement on the system's state. These protocols are considered essential to maintaining the integrity and reliability of data without the need for a central authority and can be classified into two basic parts: voting-based consensus and

proof-based consensus, both of which have different kinds of mechanisms, as shown in Figure 8 Consensus protocols are distinguished by the following features:

- Agreement: ensuring all honest nodes agree on the same data.
- Fault Torrance: It ensures that the system continues to operate even if one of the nodes fails or behaves maliciously. Although various types of failures or malicious behaviors may occur, the system remains secure and available.
- Incentives: Through the reward system, nodes are encouraged to follow the network protocol honestly.

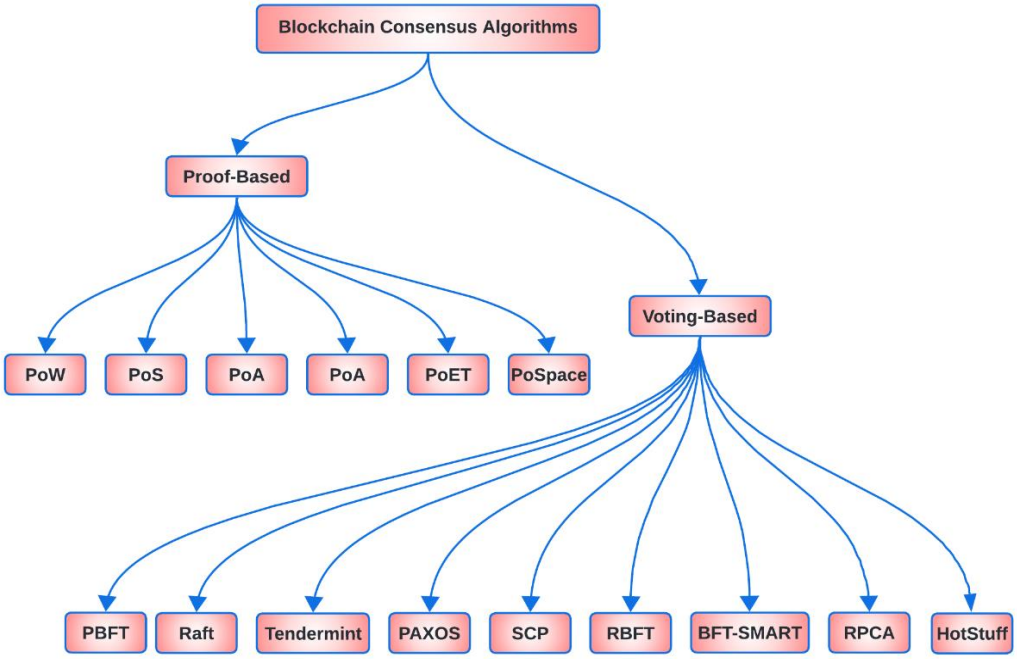

FIGURE 8. -The categories of consensus algorithms [35]

a. Proof of Work

Nakamoto proposed PoW as the first consensus algorithm to verify blocks in the Bitcoin network. PoW is a competitive mechanism that requires miners to meet a specific degree of difficulty in order to validate a particular block. This involves attempting to create a hexadecimal number that is less than the level target pre-set by the network using the SHA256 hash function. A single miner or miner pool accepts a block as true when the hash value of the entire block falls below the hash difficulty. Despite its ability to withstand the 51% attack and Sybil attack, the PoW algorithm consumes a significant amount of computing power, necessitates high resources, exhibits slow transaction processing efficiency, and contributes to increased carbon emissions and water consumption. Estimates suggest that Bitcoin mining consumed 1573.7 gigalitres of water in 2021, in addition to electronic waste, amidst growing concerns over the impacts of climate change [36]. Figure 9 shows a mechanism for creating blocks and verifying their validity based on PoW consensus.

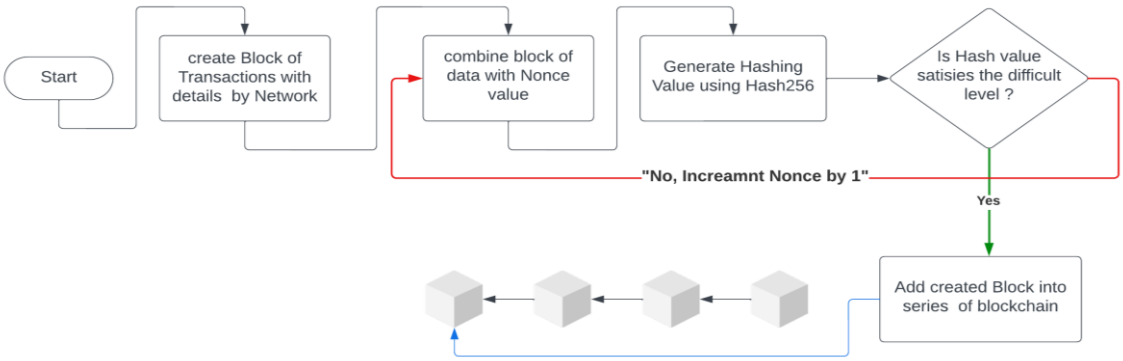

FIGURE 9. - Conventional (PoW) mining structure [37]

b. Proof of Stake

S. King and Scott Nadal proposed proof of stake (PoS) in the peercoin cryptocurrency in 2012 as a performance-oriented alternative to PoW [38]. PoS chooses a validator for each block depending on the stake amount and duration (coin age). Nodes with a larger coin stake than the rest of the network are more likely to mine blocks, but if they act as malicious nodes or fail to validate the transactions correctly, they will lose part or all of their stakes. PoS does not require a huge amount of computational power and, therefore, is considered energy-efficient compared to PoW, leading to faster block generation and increased throughput estimated at thousands [39]. Validators with more coins (or "stakes") are more likely to create blocks and collect rewards for the rich-get-richer problem. It may concentrate money and power among a few validators, and this vulnerability can be exploited to launch a majority attack [40]. It's worth noting that the coin (peercoin) operates on a decentralized P2P network using a unique hybrid model that combines proof of work for initial coin distribution and proof of stake for network security, as shown in Figure 10.

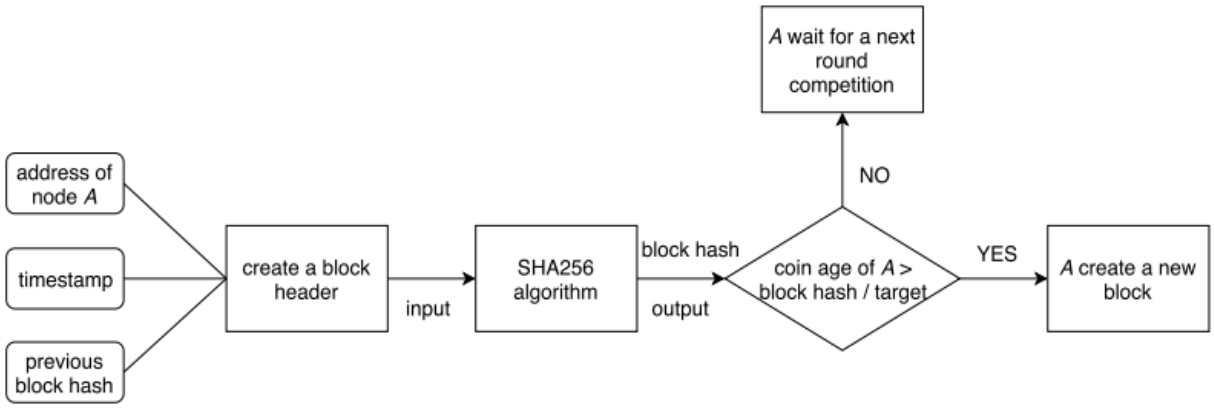

FIGURE 10. - Conventional (PoS) mining structure [41]

c. Practical byzantine fault tolerance

Miguel Castro and Barbara Liskov proposed the algorithm (PBFT) in early 1999 to operate in distributed systems susceptible to Byzantine faults. Byzantine faults refer to nodes that behave arbitrarily, maliciously, or disconnect, resulting in the provision of incorrect information to other nodes in the network that impacts correct consensus decisions [42]. Using the majority rule, the PBFT ensures system stability and work continuity as long as the number of malicious nodes does not exceed one-third of the network. It is characterized by processing transactions faster because it does not require any intensive computational operations, but increasing the number of nodes in the network may limit its ability to expand due to the increased density of communication between nodes, which leads to increased overhead. In general, the algorithm includes three main phases: pre-prepare, prepare, and commit, as shown in figure11. The most prominent cryptocurrencies that use the PBFT are Hyperledger Fabric and Tendermint.

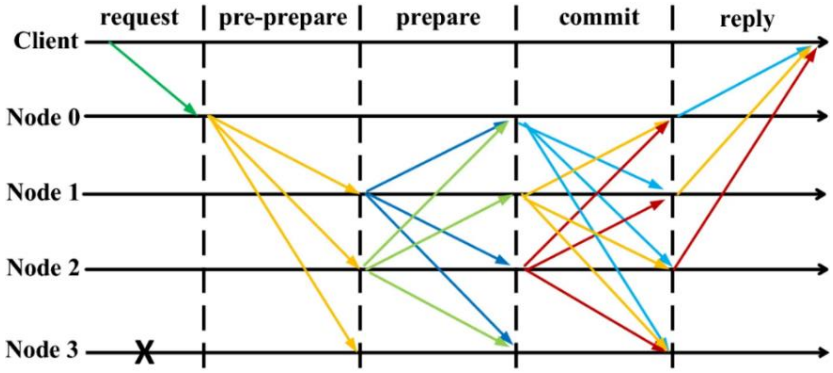

FIGURE 11. - Practical Byzantine Fault Tolerance (PBFT) [43]

d. Delegated Proof of Stake consensus

DPoS is derived from the voting-based consensus algorithm (PoS), which aims to achieve consensus in the network without the need for intensive computational power, but it differs in how the validator is selected. Stakeholders do not participate directly as verifiers, but they vote for a limited number of delegates, sometimes called witnesses, who are responsible for verifying transactions and producing the block. Validators can eliminate poorly performing or malicious delegates, and because the community of verifiers is larger than the delegates, they are rewarded less than the delegates. BitShares, Steemit, and EOS are projects that use DPoS [44]. Figure 12 reflects the steps in selecting and assigning nodes based on stakeholder votes to validate blocks in a DPoS blockchain system.

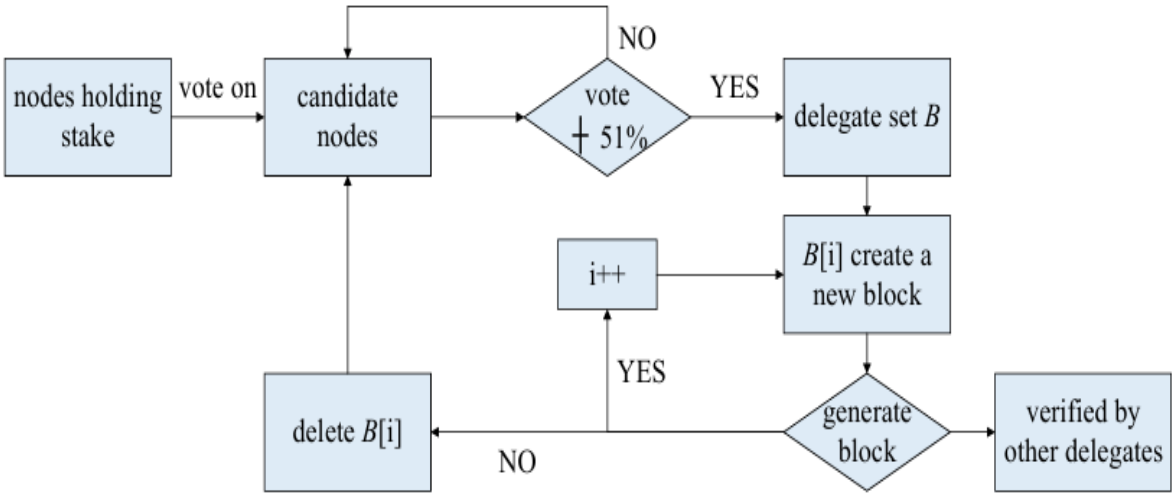

FIGURE 9. - Delegated Proof of Stake consensus (DPoS) [44]

e. Proof of Authority consensus

This type of algorithm is very suitable for private or permissioned blockchains in which the participants are known and trusted. The POA chooses the verifiers based on their identity and reputation, which they have earned over time by participating in the network, rather than their computational power or stake. The governing authority of the private network or consortium usually approves them in advance. Every time a new block joins the chain, it receives an incentive value that enhances its reputation. On the other hand, if they engage in any suspicious act or activity, their reputation suffers [45]. PoA is considered one of the most important strategies to mitigate the severity of common Sybil attacks because it uses trustworthy relationships between participants to perform collaborative tasks, but there are doubts about its resistance to these attacks in an environment devoid of permissions [46].

Table 3. - Comparison of common consensus mechanisms [44]

Aspect	PoW	PoS	DPoS	PBFT	RAFT
Decentralization	Complete	Complete	Complete	Incomplete	Incomplete
Numbers of nodes	Unlimited	Unlimited	Unlimited	Limited	Unlimited
Energy consumption	High	Low	Low	Low	Low
Block generation	Long	Short	Short	Short	Short
Transaction confirmation	long	Short	Short	Immediate	Immediate
Scalability	High	High	High	Low	Low
Throughput	Low	Low	High	High	High
Consistency	Probability	Probability	Probability	Finality	Finality
Fault tolerance	50%	33% or 50%	50%	33%	50%
Permission	No	No	No	Yes	Yes
example	Bitcoin	Peercoin	EOS	Tendemint	Etcd

Table 3 compares different consensus mechanisms, highlighting their unique attributes and trade-offs. Proof of Work (PoW), used by Bitcoin, is highly decentralized with high energy consumption and probabilistic consistency, while Proof of Stake (PoS) and Delegated Proof of Stake (DPoS) both reduce energy needs and improve transaction speeds, with DPoS specifically enabling higher throughput. Practical Byzantine Fault Tolerance (PBFT), used in Tendermint and RAFT and utilized in distributed systems like Etcd, is more suited for permissioned environments. PBFT offers immediate transaction finality and high fault tolerance with limited scalability, whereas RAFT focuses on consistency and fault tolerance for distributed databases. Each algorithm serves different use cases, balancing decentralization, energy efficiency, and transaction finality according to specific needs.

Table 4.- The throughput of few cryptocurrencies and the time consumed to create a block [18, 21]

Consensus algorithms	Cryptocurrencies	Algorithm	TPS	Block Time Minutes	Transaction Confirmation Time	#of confirmation block
PoW	Bitcoin	SHA256	7	10	78 minutes	6
	Ethereum	Ethash	15	0.25	6 minutes	30
	Litecoin	ECCAK256 Scrypt	28	2.3	30 minutes	12
	Monero	Cryptonight	30	2	30 minutes	15
	Zcash	Equihash	27	2	60 minutes	24
PoS	Waves (LPoS)	LPoS	100	1	N/A	N/A
	Qtum	POS3.0	70	2	60 minutes	24
	Nxt	SHA256	100	1	N/A	N/A
	Blackcoin	Scrypt	0	1	N/A	N/A
DPoS	Nano	Blake2b	7000	Instant	N/A	N/A
	EOS	DPoS	4000	0.5	1.5 seconds	N/A
	Cardano	Ouroboros (DPoS)	257	0.33	5 minutes	15
	TRON	DPoS	2000	0.05	5 minutes	N/A
	Lisk	DPoS	3	0.284	N/A	N/A
	BitShares	DPoS	100000	0.05	N/A	N/A
PBFT	Ripple	N/A	1500	0.06	4 seconds	N/A
	Stellar	N/A	1000	0.08	5 seconds	N/A
PoC	Zilliqa	Keccak	0	45s to 4 m	N/A	N/A
	Burst	Shabal256	80	4	N/A	N/A
DAG	IOTA	Curl-P	1000	Instant	3 minutes	N/A
	Byteball (Obyte)	DAG	10	0.5	N/A	N/A
	Travelflex	DAG	3500	1	N/A	N/A
PoA Hybrid PoW/PoS	Dash	X11	56	2.5	15 minutes	6
	Decred	BLAKE256	14	5	N/A	N/A
	Komodo	Equihash	100	1	N/A	N/A
	Peercoin	SHA-256	0	10	N/A	N/A
	Espers	HMQ1725	0	5	N/A	N/A
dBFT	NEO	RIPEMD160	1000	0.25	N/A	N/A
Pol	NEM (XEM)	Ed25519	10000	1	N/A	N/A
PoB	Slimcoin	Dcrypt	0.00003	1.5	N/A	N/A

The table summarizes cryptocurrencies by their consensus algorithms, highlighting metrics such as transactions per second (TPS), block times, confirmation times, and confirmation blocks across diverse models like PoW, PoS, DPoS, PBFT, PoC, DAG, and hybrids. It compares the performance and efficiency of each approach.

4. FEATURES OF BLOCKCHAIN TECHNOLOGY

Blockchain technology has several important features that make it unique and enhance its worth for diverse applications. Figure 13 summarizes these primary characteristics.

1.Decentralization

A core feature of blockchain technology is its decentralized nature, where numerous computers—referred to as full nodes—maintain a shared ledger. These nodes collectively manage the peer-to-peer network, ensuring the validity of transactions in a decentralized manner [7]. As a result, two parties can transact directly without an intermediary, enhancing both fairness and security. Consensus protocols facilitate operations such as storage, updating, verification, and maintenance, ensuring data consistency and safeguarding against corruption. Consensus is achieved when enough

nodes agree on the data to be recorded in the blockchain. This trust-building process occurs independently of any centralized authority and often involves mathematical algorithms or voting mechanisms [47]. Each node in the network operates autonomously, with equal rights and responsibilities, meaning that issues at the node level do not compromise the entire network. By distributing information across multiple nodes, the blockchain mitigates risks associated with data loss or destruction by avoiding a single point of failure. Decentralization also strengthens user privacy, reduces information misuse, and overcomes bottlenecks typically seen in centralized systems, effectively removing the need for a middleman [48].

2.Immutability

Terms like persistency, tamper-proofing, and unforgeability are often used to describe the concept of immutability in blockchain. This principle ensures that once data is added to a verified block and incorporated into the blockchain, it cannot be altered, deleted, or tampered with. The hash256 algorithm cryptographically connects each block to the next, so even the slightest modification produces a different hash in all subsequent blocks, immediately revealing any change. This linkage secures the shared ledger across the network, making it truly immutable [47].

3.Transparency

Transparency, often referred to as "auditability," is a defining feature of blockchain technology that allows anyone to view transaction data at any time [7]. This openness enhances the integrity and accountability of the system, ensuring that no information is altered improperly or fraudulently. The transparent nature of blockchain enables easy transaction history tracking through public addresses accessible to all, providing a high level of trust in the system [49].

4. Autonomy

In the traditional system, all transactions are processed based on the parties' trust and commitment to fulfilling them. On the contrary, blockchain provides a system that does not consider trust to be a problem and operates on a peer-to-peer network that does not necessitate a trusted party to ensure a specific procedure. Some have called these "systems trustless," but this expression is inaccurate and has negative connotations, as the consensus algorithm is the basis for trust [50].

5.Security

The blockchain's security surpasses that of a central authority, which is more than 50% vulnerable to hacking, thanks to its protection by hash256 encryption, consensus algorithms, and the simultaneous monitoring of distributed ledgers across network nodes. As a result, a hacker must break the encryption chain and change all copies of the data distributed across hundreds or thousands of nodes, making data forgery impossible [51].

a. Privacy

Blockchain technology enables user anonymity, protecting against intrusion and unauthorized access. Transactions are authenticated without disclosing personal information, ensuring that parties involved in data exchanges remain anonymous [52].

b. Programmable

The blockchain is considered open-source technology that allows developers to create decentralized applications using smart contracts to automatically execute contract terms when pre-defined conditions are met [48, 52].

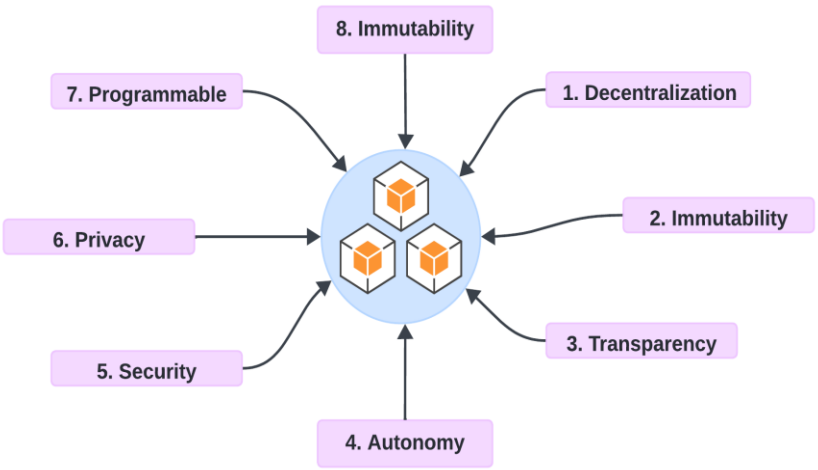

FIGURE 13. - Features of blockchain technology [53]

5. THE METRICS OF BLOCKCHAIN EVALUATION

Blockchain usually uses several metrics to evaluate its performance, which we can summarize and illustrate in Figure 14.

- Throughput

Definition: the total amount of processed transactions per second by miners in a blockchain network referred to as Transaction Per Second TPS

Important: High throughput indicates the blockchain's capability to handle a larger volume of transactions and its ability to scale [54].

$$TPS = \frac{Number \text{ of Transactions per Block}}{Block \text{ Time}} \quad (1)$$

- Scalability

The extent to which the system can grow without significant performance loss, increased costs, sacrifice of security, and decentralization

- Latency

Definition: Also known as "finality," the duration required to process a transaction from its moment of creation to its completion throughout the blockchain network.

Important: Lower latency is critical for improving blockchain performance because it reduces transaction confirmation delays [55].

$$Latency = \text{Pr}opagation \text{ time} + \text{Block time} + \text{Validation time} \quad (2)$$

- Fault tolerance

Indicate the ability of the existing blockchain system to tolerate the maximum number of nodes that may act arbitrarily or maliciously or be subject to failure or interruption without affecting the consensus mechanism or the continuity of the system. It is measured in percentages [56].

- Energy consumption

Definition: The amount of energy consumed to process transactions in the network.

Important: Energy-efficient blockchain systems are more sustainable, less polluting, and have lower operating costs [57].

$$E = W \times N \times T \quad (3)$$

Where symbol E the total electrical energy consumed for all nodes, W Denote power consumption in Watts per node, N Indicate the number of nodes and T Time taken to complete the work per node.

- Storage

As blockchain grows, efficient data storage and management are critical to reducing bloat and long-term system sustainability [58].

- Cost transaction

Transaction fees critically play a role in measuring the performance of a blockchain system because they directly affect the transaction confirmation time and thus impact throughput and latency, as is happening now in Bitcoin [7].

- Nodes

More full nodes by miners in the network mean extra replicas, increasing security and decentralization, but they can also increase energy consumption and raise communication costs [59].

- Size block

Definition: number of transactions (usually measured in megabytes) that are included in a single block

Important: Larger block sizes increase the blockchain's throughput by allowing more transactions within the block, but they also take longer to propagate because a heavier block requires more time, computational resources, and bandwidth to transmit across the network.

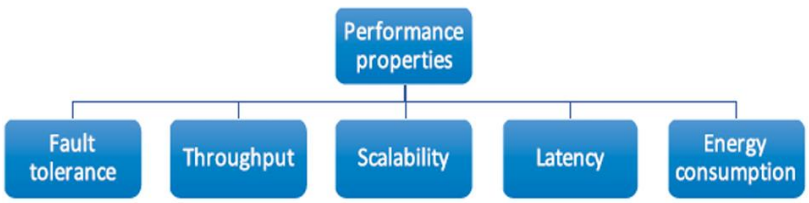

FIGURE 14. - Performance properties of blockchain [60]

6. THE BLOCKCHAIN LAYERS

Many articles have classified the blockchain layers into five, as shown in Figure 15, and we will explore each with a sufficient explanation.

- Network layer

A blockchain system relies on a mechanism to distribute data among participants. This mechanism, known as the peer-to-peer (P2P) network layer, allows nodes to discover and connect with each other, facilitating the dissemination of transactions and blocks while synchronizing the blockchain's current valid state. Nodes in the network are categorized into full nodes and light nodes. Full nodes, often referred to as miners, uphold the system's trust by verifying transactions and blocks according to the consensus rules and maintaining complete copies of the blockchain. Light nodes, on the other hand, focus on generating parameters and transmitting them across the network. The network layer is essential for distributed ledgers, as it enables intensive communication for peer identification and state synchronization among nodes. Efficiency in this layer is largely determined by the speed of these operations [61].

- Consensus layer

It also refers to the data manipulation layer, which ensures reaching a coordinated agreement or decision between synchronized nodes on a single block of transactions in a decentralized environment with a trustless system [2]. This layer encompasses various consensus algorithms, categorized into three main sections: the first section comprises proof of work-based consensus algorithms, like PoW in Bitcoin and PoS in Ethereum, which offer high security but demand intensive computational effort, resulting in low transaction processing efficiency. The second is consensus algorithms based on voting that provide relatively high performance, such as PBFT, but require intensive message exchange between participants and high communication costs, especially in a large network. The third is the hybrid approach, which combines the two previous approaches with the aim of improving performance and enhancing security, such as Tendermint, which combines PoS and PBFT, and EOS, which combines DPoS and PBFT algorithms [62].

- Data layer

The data layer encompasses various data-related components, including transaction models, data structures, Merkle trees, hash functions, and digital signatures. There are two primary transaction models for managing digital asset ownership: the unspent transaction output (UTXO) model used by Bitcoin, which focuses on spending outputs from previous transactions, and the account-based model employed by platforms like Ethereum, which updates balances within individual accounts. Different data storage structures, such as linear chains and Directed Acyclic Graphs (DAGs), are used to organize transaction data. Merkle trees play a vital role in summarizing all transactions within a block, creating an encrypted digital fingerprint to ensure data integrity. By repeatedly hashing pairs of transactions, a single hash known as the Merkle root is produced. Digital signatures, particularly those based on Public Key Cryptography (PKC), provide a secure method for verifying data authenticity and ensuring its integrity [61].

- Execution layer

This layer is responsible for executing the contract or bytecode, which is low-level machine code in the runtime environment that contains the compilers and containers and is installed on the DLS network nodes. Ethereum has Ethereum virtual machines (EVM), akin to the Java virtual machine (JVM), for executing instructions. Hyper Ledger Fabric, on the other hand, supports the execution of smart contracts using Chaincode, but Bitcoin lacks this feature due to its reliance on a simple scripting system for transaction execution [62].

- Application layer

The application layer, also referred to as the presentation layer, serves as the interface connecting decentralized applications (dApps) to the underlying blockchain network via smart contracts. Developers utilize specialized programming languages to design scripts, APIs, and user interfaces, specifying the requirements that the blockchain system must meet. For example, Solidity is widely used on the Ethereum platform to develop smart contracts, enabling the verification and enforcement of contract execution [61].

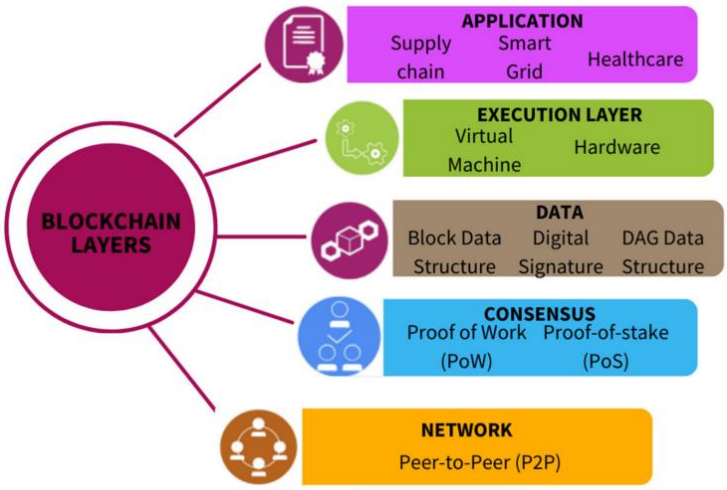

FIGURE 15. - Applications of blockchain [14]

7. BLOCKCHAIN CONSENSUS VULNERABILITIES

The reliability and resilience of blockchain technology are largely determined by the consensus algorithms responsible for validating transactions and blocks. This section highlights the most significant attacks that could potentially compromise the security of a blockchain system. While there are various other threats across different categories, this discussion focuses on summarizing the most common ones. Figure 16 provides an overview of these attacks.

7.1 THE MAJORITY ATTACK

A 51% attack, also known as a majority attack, occurs when an entity gains control of more than 50% of the network's total computing power or nodes. This dominance allows the attacker to disrupt the consensus mechanism by introducing malicious content or blocking the addition of legitimate blocks. Often referred to as hijacking consensus, this type of attack poses a greater risk to public blockchains, which rely on open participation without requiring permissions or trust among participants. These networks typically depend on proof-of-X consensus mechanisms.

To mitigate majority attacks in proof-of-work-based systems, one potential strategy is to increase the computational difficulty arbitrarily, making it infeasible for an attacker to amass the required computational power. The specifics of such attacks and the measures needed to counter them depend on the blockchain's architecture and the consensus algorithms it employs [63]:

- PoW: need more than 51% of computation power.
- PoS: need more than 51% of the committed stake.
- PBFT: more than 33% of all synchronized nodes, or enough to take over the primary node.

7.2 SYBIL ATTACK

A Sybil attack seeks to dominate network participants by generating numerous fake identities that appear as legitimate nodes, allowing attackers to gain majority influence and control over decision-making processes. These attacks often target voting mechanisms, enabling the manipulation of validator selection, consensus protocols, or network modifications to favor the attacker's goals.[63].

An eclipse attack, while similar to a Sybil attack, differs in its approach. It isolates a specific node by surrounding it with malicious nodes, cutting it off from the rest of the network. This isolation allows the attacker to mislead the targeted node, either by convincing it to approve fraudulent transactions or by withholding updates from the broader network. In this way, the attacker can control the information seen by the isolated node and manipulate its actions without necessarily affecting the entire network. Permissionless systems that are highly resistant to Sybil attacks typically implement proof-of-work or proof-of-stake principles. Conversely, mechanisms with weaker resistance often rely on reputation systems to counter such threats [64].

7.3 DOUBLE SPENDING ATTACK

An attacker exploits weaknesses in the consensus process to create a situation where he can spend the asset multiple times. There are several ways to double-spend, as follows.[63]:

a. Race attack: The attack begins when two different transactions are created in rapid succession to spend funds that are only enough for one transaction: one for the merchant and the other for himself or someone else. He hopes that both transactions will be validated and included in the blockchain. Double spending will occur if the merchant accepts the transaction before its confirmation.

b. Finney attack: This type requires the attacker to mine a block as one of the miners. The attacker prepares a block that contains a transaction, sending coins to either his own address or another address under his control. The attacker then sends a second transaction containing the same amount of coins to a different recipient, such as a store or service, using the normal network protocol. Once the recipient receives or confirms it, the attacker releases the pre-prepared block containing the initial transaction, leading the network to believe it contains the actual and correct transaction and adding the block to the blockchain. Consequently, the network invalidates the second transaction because the initial transaction has already used up the coins. The attacker will succeed in recovering his money, along with the goods or services provided by the store or merchant.

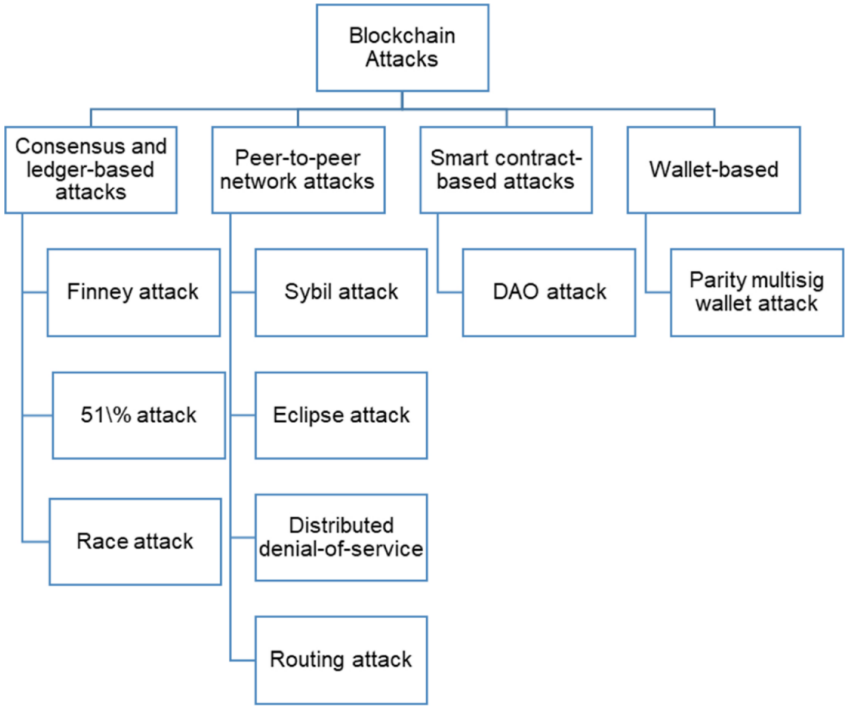

FIGURE 16. - Kinds of blockchain attacks [65]

8. APPLICATIONS OF BLOCKCHAIN TECHNOLOGY

Because of its fundamental principles of decentralization, transparency, and security, blockchain technology has significantly transformed from being the foundation of cryptocurrencies like Bitcoin to a potent tool that spans various fields in the real world, as shown in Figure 17. It offers a promising solution to numerous challenges. In this section, we will explore some of these fields.

- Healthcare

Health data security is crucial for pharmacy companies, as it is valuable and often stored on hospital servers. Blockchain-based IoT technology can help prevent misuse and misuse of health data by allowing doctors to access it only if the patient permits it, in addition to releasing patients from the hospital's centralized structure and keeping in constant contact with doctors. This system ensures proper security for personal information [66].

- Education

Implementing blockchain technology as a secure storage solution for educational certification systems to enhance document security, minimize fraud, and shorten authentication time. Leveraging blockchain allows for the replacement of traditional systems, paving the way for a new model in student information sharing [67].

- Cloud computing

Blockchain technology in the field of cloud computing has attracted the attention of many companies that require security, reliability, accountability, and audibility, as it provides complete tracking of data from modification, processing, storage, and use, and in the event of any unauthorized action, the responsible entity can be identified [37, 68].

- Voting

The trustworthiness of blockchain technology makes it an effective option for voting systems. The current traditional system cannot be trusted as long as it is managed centrally; therefore, it is vulnerable to vote tampering, has a single point of failure, and is more complex in use. A blockchain-based voting system can save effort and energy by allowing voters to cast their votes from anywhere and eliminate voter impersonation and double-voting [69].

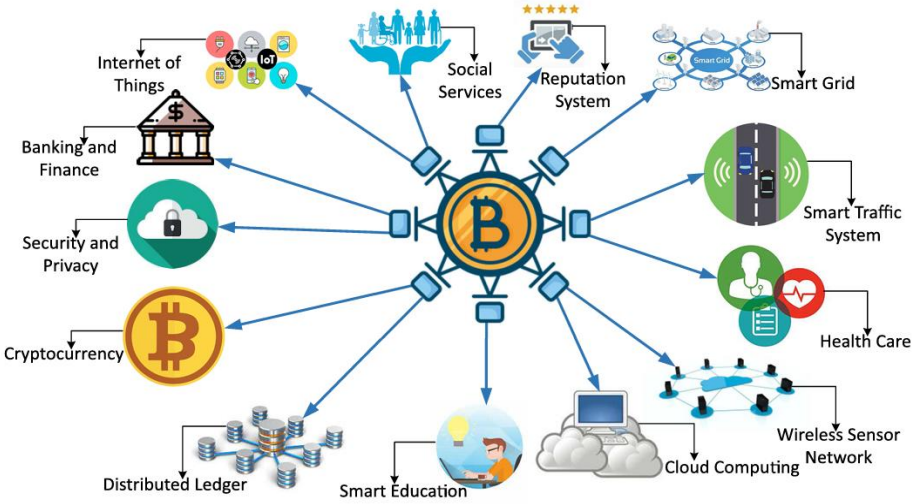

FIGURE 17. - Applications of blockchain technology [45]

- Financial

Blockchain technology has been extensively adopted in the financial and economic sectors for applications such as trade finance, insurance, money transfers, and stock trading. It facilitates real-time transactions without relying on intermediaries or banks. Additionally, blockchain enables the secure registration and transfer of asset ownership, such as vehicles and properties, and ensures the authenticity and integrity of critical documents and data [70].

- Supply chain

Blockchain technology can also be utilized in the food supply chain, a crucial sector for human health, food quality, and pricing. Tracking activities such as farming, processing, production, and distribution creates a tamper-proof record of food origins. This enhances the ability to identify contaminated supply chains, remove unsafe food before it reaches consumers, and cut out exploitative intermediaries, thereby improving quality of life and minimizing food safety risks [71].

- Other application

Various other fields have used blockchain technology to achieve goals that increase their efficiency and raise their level of performance, for example, but not limited to smart cities, energy trading, insurance, IoT, wireless networks, crowdfunding, and military purposes [18].

9. POSSIBLE FUTURE DIRECTIONS

Due to its unique potential and growing importance in academic and industrial circles, blockchain technology offers numerous promising directions for future development. We will briefly describe some of these directions.

- Scalability solutions

Blockchain has revolutionized cryptocurrency and completely changed the management of data and transactions in the digital world due to its decentralized nature, improved transparency, increased security measures, the ability to facilitate commercial trading between untrusted parties, and its contribution to preventing fraudulent activity. However, the primary issue with blockchain systems is their limited scalability, as they can only process a maximum of 7 Transactions Per Second (TPS) in Bitcoin and not exceed 30 transactions in Ethereum. Therefore, addressing or eliminating these constraints will be a significant milestone in advancing blockchain technology, enabling various applications without compromising or affecting system decentralization and security.

- Mobile Crowdsensing based on Blockchain

Many academic researchers have dedicated their endeavors to utilizing mobile crowdsensing MCS in combination with blockchain technology. The primary reason for this correlation can be attributed to shared factors mentioned as follows: First, blockchain technology depends on distributed ledger technology (DLT), which requires a significant number of MCSN participants. Second, blockchain's decentralized nature ensures that data collected from mobile devices remains tamper-proof. In MCS systems, ensuring that the sensed data is reliable and hasn't been modified by

any malicious entity is crucial. Blockchain's immutability and cryptographic security can protect data integrity by maintaining an auditable ledger of all data submissions. Third, blockchain enables the use of cryptocurrency tokens or other forms of rewards to incentivize participants. Smart contracts on the blockchain can automatically reward users based on predefined conditions, like data quality, quantity, or frequency of contribution. Fourth, blockchain can enhance privacy by allowing users to contribute anonymized data while proving its authenticity, thereby protecting the privacy of participants. Fifth, blockchain, especially in combination with reputation systems or proof-of-data mechanisms, can help verify the authenticity and reliability of submitted data by tracking the history of data contributions from individual users and their reputations within the system. Lastly, blockchains can help scale crowdsensing systems by allowing multiple participants to contribute data across different geographical locations or applications, such as environmental monitoring, traffic monitoring, or smart cities.

- Energy-efficient consensus mechanisms

In light of the growing concerns about the environmental impacts on climate security around the world caused by blockchain mining devices, which result in increased carbon emissions and a higher water footprint for Bitcoin in addition to consuming a large amount of electricity, many researchers are turning to find alternative solutions that would develop more efficient and energy-saving consensus algorithms.

- Integration with AI models

Blockchain technology can be a highly reliable data source for AI algorithms, secure training data, create auditable records, and enhance the accuracy of AI-driven processes such as supply chain tracking, predictive analytics, and medical diagnostics. Therefore, it can lead to enhanced AI outputs and increased transparency in decision-making processes.

10. CONCLUSION

The paper contributes a detailed review of blockchain technology's architecture, characteristics, and features based on an investigation of several research papers that focus their methodology on this technology. While blockchain overcomes the major limitations of traditional systems, It continues to encounter considerable obstacles regarding scalability and energy consumption. We have discussed the typical consensus algorithms that describe how peers achieve data consistency and integration and compared these mechanisms using diverse metrics. Moreover, the paper presents an analysis of the DLT, which provides clear insights into their suitability in different applications. Finally, future research must pivot on scalability solutions, developing consensus mechanisms that are energy efficient, and integrating blockchain technology with artificial intelligence that can expand its practical utility and revolutionize secure and decentralized systems.

FUNDING

None

ACKNOWLEDGEMENT

The authors would like to thank the anonymous reviewers for their efforts.

CONFLICTS OF INTEREST

The authors declare no conflict of interest

REFERENCES

[1] M. A. Fauzi, N. Paiman, and Z. Othman, "Bitcoin and cryptocurrency: Challenges, opportunities and future works," The Journal of Asian Finance, Economics and Business, vol. 7, no. 8, pp. 695-704, 2020.

[2] M. H. Tabatabaei, R. Vitenberg, and N. R. Veeraragavan, "Understanding blockchain: Definitions, architecture, design, and system comparison," Computer Science Review, vol. 50, p. 100575, 2023.

[3] R. d. Best, "Number of cryptocurrencies worldwide from 2013 to September 2024," Statista, 2024. [Online]. Available: https://www.statista.com/statistics/863917/number-crypto-coins-tokens/. [Accessed: Jan. 6, 2025].

[4] O. Labazova, "Towards a framework for evaluation of blockchain implementations," in Proc. of the [Conference Name], 2019.

[5] S. Tanwar, N. Gupta, P. Kumar, and Y.-C. Hu, "Implementation of blockchain-based e-voting system," Multimedia Tools and Applications, vol. 83, no. 1, pp. 1449-1480, 2024.

[6] W. Li, M. He, and S. Haiquan, "An overview of blockchain technology: applications, challenges and future trends," in 2021 IEEE 11th International Conference on Electronics Information and Emergency Communication (ICEIEC) 2021 IEEE 11th International Conference on Electronics Information and Emergency Communication (ICEIEC), 2021, pp. 31-39: IEEE.

[7] D. Khan, L. T. Jung, and M. A. Hashmani, "Systematic literature review of challenges in blockchain scalability," Applied Sciences, vol. 11, no. 20, p. 9372, 2021.
[8] J. Xu, C. Wang, and X. Jia, "A survey of blockchain consensus protocols," ACM Computing Surveys, vol. 55, no. 13s, pp. 1-35, 2023.
[9] F. Masood and A. R. Faridi, "An overview of distributed ledger technology and its applications," Int. J. Comput. Sci. Eng, vol. 6, no. 10, pp. 422-427, 2018.
[10] X. Liu, B. Farahani, and F. Firouzi, "Distributed ledger technology," Intelligent internet of things: From device to fog and cloud, pp. 393-431, 2020.
[11] J. L. Romero Ugarte, "Distributed ledger technology (DLT): introduction," Banco de Espana Article, vol. 19, p. 18, 2018.
[12] M. Gorbunova, P. Masek, M. Komarov, and A. Ometov, "Distributed ledger technology: State-of-the-art and current challenges," Computer Science and Information Systems, vol. 19, no. 1, pp. 65-85, 2022.
[13] S. Barj, A. Ouaddah, and A. Mezrioui, "Cryptography in distributed ledger technologies from a layered perspective: A state of the art," in International Conference on Digital Technologies and Applications, 2023, pp. 210-220: Springer.
[14] J. Zheng et al., "An in-depth review on blockchain simulators for iot environments," Future Internet, vol. 14, no. 6, p. 182, 2022.
[15] S. Bouraga, "A taxonomy of blockchain consensus protocols: A survey and classification framework," Expert Systems with Applications, vol. 168, p. 114384, 2021.
[16] C. Mohan, "Tutorial: blockchains and databases," Proceedings of the VLDB Endowment, vol. 10, no. 12, pp. 2000-2001, 2017.
[17] A. Canciani, C. Felicioli, A. Lisi, and F. Severino, "Hybrid DLT as a data layer for real-time, data-intensive applications," arXiv preprint arXiv:2304.07165, 2023.
[18] A. Haque and M. Rahman, "Blockchain technology: Methodology, application and security issues," arXiv preprint arXiv:2012.13366, 2020.
[19] elevatex, "Permissionless vs. Permissioned Blockchains," 27-Jan-2022. [Online]. Available: [URL]. [Accessed: Jan. 6, 2025].
[20] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in 2017 IEEE international congress on big data (BigData congress), 2017, pp. 557-564: Ieee.
[21] S. M. H. Bamakan, A. Motavali, and A. B. Bondarti, "A survey of blockchain consensus algorithms performance evaluation criteria," Expert Systems with Applications, vol. 154, p. 113385, 2020.
[22] K. Wüst and A. Gervais, "Do you need a blockchain?," in 2018 crypto valley conference on blockchain technology (CVCBT), 2018, pp. 45-54: IEEE.
[23] Z. Zhang, "A survey of privacy protection in distributed systems based on blockchain," Journal of Electronics and Information Science, vol. 8, no. 5, pp. 26-30, 2023.
[24] C. Fan, H. Khazaei, Y. Chen, and P. Musilek, "Towards a scalable DAG-based distributed ledger for smart communities," in 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), 2019, pp. 177-182: Ieee.
[25] Modelling and Review," University of Surrey, 2021. [Online]. Available: [URL]. [Accessed: Jan. 6, 2025].
[26] S. Gaba et al., "Holochain: An agent-centric distributed hash table security in smart IoT applications," IEEE Access, vol. xx, no. xx, pp. xxx-xxx, 2023.
[27] N. El Ioini and C. Pahl, "A review of distributed ledger technologies," in On the Move to Meaningful Internet Systems. OTM 2018 Conf.: CoopIS, C&TC, ODBASE 2018, Valletta, Malta, Oct. 22-26, 2018, Proc., Part II, 2018, pp. 277-288.
[28] M. Khan, D. Schaefer, and J. Milisavljevic-Syed, "A review of distributed ledger technologies in the machine economy: challenges and opportunities in industry and research," Procedia CIRP, vol. 107, pp. 1168-1173, 2022.
[29] R. Ramadoss, "Blockchain technology: An overview," IEEE Potentials, vol. 41, no. 6, pp. 6-12, 2022.
[30] G. Bigini, V. Freschi, and E. Lattanzi, "A review on blockchain for the internet of medical things: Definitions, challenges, applications, and vision," Future Internet, vol. 12, no. 12, p. 208, 2020.
[31] T. Wang, X. Bai, H. Wang, S. C. Liew, and S. Zhang, "Game-theoretical analysis of mining strategy for bitcoin-ng blockchain protocol," IEEE Systems Journal, vol. 15, no. 2, pp. 2708-2719, 2020.
[32] M. Raikwar, D. Gligoroski, and K. Kralevska, "SoK of used cryptography in blockchain," IEEE Access, vol. 7, pp. 148550-148575, 2019.
[33] B. K. Mohanta, D. Jena, S. S. Panda, and S. Sobhanayak, "Blockchain technology: A survey on applications and security privacy challenges," Internet of Things, vol. 8, p. 100107, 2019.
[34] D. Frey, M. X. Makkes, P.-L. Roman, F. Taïani, and S. Voulgaris, "Dietcoin: shortcutting the Bitcoin verification process for your smartphone," arXiv preprint arXiv:1803.10494, 2018. [Online]. Available: [URL]. [Accessed: Jan. 6, 2025].

[35] W. Yao, J. Ye, R. Murimi, and G. Wang, "A survey on consortium blockchain consensus mechanisms," arXiv preprint arXiv:2102.12058, 2021. [Online]. Available: [URL]. [Accessed: Jan. 6, 2025]
[36] A. de Vries, "Bitcoin's growing water footprint," Cell Reports Sustainability, vol. 1, no. 1, 2024.
[37] A. F. Mahdi and F. Rabee, "A blockchain mining proof of work approach based on fog computing virtualization for mobile crowdsensing," in 2024 Third International Conf. on Distributed Computing and High Performance Computing (DCHPC), 2024, pp. 1-9.
[38] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake," Aug. 2012. [Online]. Available: [URL]. [Accessed: Jan. 6, 2025].
[39] L. Lao, X. Dai, B. Xiao, and S. Guo, "G-PBFT: A location-based and scalable consensus protocol for IoT-blockchain applications," in 2020 IEEE international parallel and distributed processing symposium (IPDPS), 2020, pp. 664-673: IEEE.
[40] S. Sayeed and H. Marco-Gisbert, "Assessing blockchain consensus and security mechanisms against the 51% attack," Applied sciences, vol. 9, no. 9, p. 1788, 2019.
[41] S. Zhang and J. Lee, "Analysis of the main consensus protocols of blockchain," ICT Express, vol. 1, 2019. [Online]. Available: https://doi.org/10.1016/j.icte. [Accessed: Jan. 6, 2025].
[42] M. Castro and B. Liskov, "Practical byzantine fault tolerance," in OsDI, 1999, vol. 99, no. 1999, pp. 173-186.
[43] M. Bosamia and D. Patel, "Comparisons of blockchain based consensus algorithms for security aspects," Int. J. Emerg. Technol, vol. 11, no. 3, pp. 427-434, 2020.
[44] M. Xie, J. Liu, S. Chen, and M. Lin, "A survey on blockchain consensus mechanism: research overview, current advances and future directions," International Journal of Intelligent Computing and Cybernetics, vol. 16, no. 2, pp. 314-340, 2023.
[45] T. A. Alghamdi, R. Khalid, and N. Javaid, "A Survey of Blockchain based Systems: Scalability Issues and Solutions, Applications and Future Challenges," IEEE Access, 2024.
[46] M. Platt, D. Platt, and P. McBurney, "Sybil attack vulnerability trilemma," Int. J. Parallel, Emergent and Distributed Syst., vol. xx, no. xx, pp. 1-15, 2024.
[47] 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, 2017.
[48] Y. Lu, "Blockchain: A survey on functions, applications and open issues," Journal of Industrial Integration and Management, vol. 3, no. 04, p. 1850015, 2018.
[49] Y. Xinyi, Z. Yi, and Y. He, "Technical characteristics and model of blockchain," in 2018 10th international Conference on communication Software and networks (ICCSN), 2018, pp. 562-566: IEEE.
[50] J. Xie et al., "A survey of blockchain technology applied to smart cities: Research issues and challenges," IEEE communications surveys & tutorials, vol. 21, no. 3, pp. 2794-2830, 2019.
[51] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," Future generation computer systems, vol. 88, pp. 173-190, 2018.
[52] M. N. M. Bhutta et al., "A survey on blockchain technology: Evolution, architecture and security," Ieee Access, vol. 9, pp. 61048-61073, 2021.
[53] A. Odeh, I. Keshta, and Q. A. Al-Haija, "Analysis of blockchain in the healthcare sector: application and issues," Symmetry, vol. 14, no. 9, p. 1760, 2022.
[54] G.-T. Nguyen and K. Kim, "A survey about consensus algorithms used in blockchain," Journal of Information processing systems, vol. 14, no. 1, 2018.
[55] X. Xu, G. Sun, L. Luo, H. Cao, H. Yu, and A. V. Vasilakos, "Latency performance modeling and analysis for hyperledger fabric blockchain network," Information Processing & Management, vol. 58, no. 1, p. 102436, 2021.
[56] M. S. Ferdous, M. J. M. Chowdhury, M. A. Hoque, and A. Colman, "Blockchain consensus algorithms: A survey," arXiv preprint arXiv:2001.07091, 2020. [Online]. Available: [URL]. [Accessed: Jan. 6, 2025].
[57] I. Konstantinidis, G. Siaminos, C. Timplalexis, P. Zervas, V. Peristeras, and S. Decker, "Blockchain for business applications: A systematic literature review," in Business Information Systems: 21st International Conf. BIS 2018, Berlin, Germany, Jul. 18-20, 2018, Proc., vol. 21, 2018, pp. 384-399. Springer.
[58] X. Wang et al., "Survey on blockchain for Internet of Things," Computer Communications, vol. 136, pp. 10-29, 2019.
[59] A. A. Mazlan, S. M. Daud, S. M. Sam, H. Abas, S. Z. A. Rasid, and M. F. Yusof, "Scalability challenges in healthcare blockchain system—a systematic review," IEEE access, vol. 8, pp. 23663-23673, 2020.
[60] M. S. Ferdous, M. J. M. Chowdhury, and M. A. Hoque, "A survey of consensus algorithms in public blockchain systems for crypto-currencies," Journal of Network and Computer Applications, vol. 182, p. 103035, 2021.
[61] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "A survey on the adoption of blockchain in iot: Challenges and solutions," Blockchain: Research and Applications, vol. 2, no. 2, p. 100006, 2021.
[62] C. Fan, S. Ghaemi, H. Khazaei, and P. Musilek, "Performance evaluation of blockchain systems: A systematic survey," IEEE Access, vol. 8, pp. 126927-126950, 2020.

[63] L. König, S. Unger, P. Kieseberg, S. Tjoa, and J. R. C. Blockchains, "The Risks of the Blockchain A Review on Current Vulnerabilities and Attacks," J. Internet Serv. Inf. Secur., vol. 10, no. 3, pp. 110-127, 2020.
[64] M. Platt and P. McBurney, "Sybil in the haystack: A comprehensive review of blockchain consensus mechanisms in search of strong Sybil attack resistance," Algorithms, vol. 16, no. 1, p. 34, 2023.
[65] A. Hamdi, L. Fourati, and S. Ayed, "Vulnerabilities and attacks assessments in blockchain 1.0, 2.0 and 3.0: tools, analysis and countermeasures," International Journal of Information Security, vol. 23, no. 2, pp. 713-757, 2024.
[66] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of things security: A top-down survey," Computer Networks, vol. 141, pp. 199-221, 2018.
[67] A. W. Reza, K. Islam, S. Muntaha, O. B. Abdur Rahman, R. Islam, and M. S. Arefin, "Education Certification and Verified Documents Sharing System by Blockchain," International Journal of Intelligent Engineering & Systems, vol. 15, no. 6, 2022.
[68] A. Lakhan, M. Ahmad, M. Bilal, A. Jolfaei, and R. M. Mehmood, "Mobility aware blockchain enabled offloading and scheduling in vehicular fog cloud computing," IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 7, pp. 4212-4223, 2021.
[69] T. Moura and A. Gomes, "Blockchain voting and its effects on election transparency and voter confidence," in Proc. 18th Annu. Int. Conf. Digital Gov. Res., 2017, pp. 574-575, Sao Paulo, Brazil: ACM.
[70] V. Chhabra, S. Bathla, and H. Maheshwari, "An overview of blockchain technology and comparison between various cryptocurrencies," J. Emerg. Technol. Innov. Res, vol. 6, pp. 68-71, 2019.
[71] A. Iftekhar, X. Cui, M. Hassan, and W. Afzal, "Application of blockchain and Internet of Things to ensure tamper‐proof data availability for food safety," Journal of Food Quality, vol. 2020, no. 1, p. 5385207, 2020.