

AN INVESTIGATION AND OVERVIEW OF BLOCKCHAIN TECHNOLOGY: ARCHITECTURE, CONSENSUS, AND ITS FUTURE TRENDS

By

Priyadharsini, A.

Assistant Professor, Department of Computer Applications, Nallamuthu Gounder Mahalingam College, Pollachi, Tamil Nadu, India.

Abstract

A digital database or ledger that is distributed among the nodes of a peer-to-peer network is blockchain. Bitcoin cryptocurrency (BTC), a virtual currency designed to act as money and a form of payment outside the control of any one person, group, or entity, and thus removing the need for third-party involvement in financial transactions, lays the foundation for blockchain technology. A blockchain is a distributed database or ledger shared among a computer network's nodes. They are best known for their crucial role in cryptocurrency systems for maintaining a secure and decentralised record of transactions, but they are not limited to cryptocurrency use and are expected to be used in many other fields, like banking, voting, health care, and property records. Blockchain technology achieves decentralised security and trust in several ways, but challenges are still awaited in scalability and security. This paper includes an overview of blockchain architecture and a comparison of some typical consensus algorithms used in different blockchains. It concludes with future trends for blockchain, technical challenges and advancements are discussed briefly.

Keywords: *blockchain, architecture, decentralisation, consensus, scalability, and technical challenges.*

Introduction

A blockchain is a *distributed database or ledger* shared among a computer network's nodes. They are best known for their crucial role in cryptocurrency systems for maintaining a secure and decentralized record of transactions,

but they are not limited to cryptocurrency uses. Blockchains can be used to make data in any industry immutable the term used to describe the *inability to be altered*. Because there is no way to change a block, the only trust needed is at the point where a user or program enters data. This

aspect reduces the need for trusted third parties, which are usually auditors or other humans that add costs and make mistakes. Since Bitcoin's introduction in 2009, blockchain uses have exploded via the creation of various cryptocurrencies, decentralized finance (DeFi) applications, non-fungible tokens (NFTs), and smart contracts. Increasing popularity of crypto currency, Bitcoin has enjoyed a huge success with its capital market reaching 10 billion dollars in 2016. With a specially designed data storage structure, transactions in Bitcoin network could happen without any third party and the core technology to build Bitcoin is blockchain, which was first proposed in 2008 and implemented in 2009. Blockchain could be regarded as a public ledger and all committed transactions are stored in a list of blocks. This chain grows as new blocks are appended to it continuously. Asymmetric cryptography and distributed consensus algorithms have been implemented for user security and ledger consistency. The blockchain technology generally has key characteristics of decentralization, persistency,

anonymity and auditability. With these traits, blockchain can greatly save the cost and improve the efficiency. Since it allows payment to be finished without any bank or any intermediary, blockchain can be used in various financial services such as digital assets, remittance and online payment. Additionally, it can also be applied into other fields including smart contracts, public services, Internet of Things (IoT), reputation systems and security services. Those fields favour blockchain in multiple ways. First of all, blockchain is immutable. Transaction cannot be tampered once it is packed into the blockchain. Businesses that require high reliability and honesty can use blockchain to attract customers. Besides, blockchain is distributed and can avoid the single point of failure situation. As for smart contracts, the contract could be executed by miners automatically once the contract has been deployed on the blockchain. Although the blockchain technology has great potential for the construction of the future Internet systems, it is facing a number of technical challenges. Firstly, scalability is a huge concern. Bitcoin block size is limited to 1 MB now while a block is

mined about every ten minutes. Subsequently, the Bitcoin network is restricted to a rate of 7 transactions per second, which is incapable of dealing with high frequency trading. However, larger blocks means larger storage space and slower propagation in the network. This will lead to centralization gradually as less users would like to maintain such a large blockchain. Therefore, the trade-off between block size and security has been a tough challenge. Secondly, it has been proved that miners could achieve larger revenue than their fair share through selfish mining strategy. Miners hide their mined blocks for more revenue in the future. In that way, branches could take place frequently, which hinders blockchain development. Hence, some solutions need to be put forward to fix this problem. Moreover, a blockchain is on a really basic level a scattered information of records or open record everything thought of or modernised occasions that are dead and shared among sharing parties. Every exchange the excellent network record is genuine by accord of Associate in Nursing an excellent deal of the individuals within the structure.

Likewise, once entered, data will ne'er be eradicated. The blockchain contains an explicit and clear record of every and each exchange whenever created. To utilize a foremost equivalence, it's not at all troublesome to require a treat from a treat thump, unbroken in an exceedingly confined place than taking the treat from a treat knock unbroken in an exceedingly business centre, being seen by a monster range of people. Bitcoin is that the most recommended perspective that's remarkably related to blockchain progression. It's likewise the foremost off from being clearly true one since it empowers a multibillion-dollar normally market of unclear exchanges with no body management. On these lines it must administer distinctive body problems together with national governments and fund affiliations. The benefits of Blockchain advancement trounce the executive problems and centred inconveniences. One key creating use event of blockchain headway consolidates "splendid contracts". Sharp contracts area unit primarily computer programs that may during this manner execute the terms of a comprehension. Sharp Property is another connected plan that is

regarding dominant the requirement with relevance property or resource by methods for blockchain utilizing sensible Contracts. The property will be physical, for instance, auto, house, phone and rarity or it should be non-physical, for instance, offers of Associate in Nursing affiliation. It have to be compelled to be noted here that even Bitcoin is not usually a money - Bitcoin is tied in with dominant the commitment with reference to.

Blockchain architecture

Blockchain is a type of shared database that differs from a typical database in the way it stores information; blockchains store data in blocks linked together via cryptography. Different types of information can be stored on a blockchain, but the most common use for transactions has been as a

ledger. In Bitcoin’s case, blockchain is decentralized so that no single person or group has control—instead, all users collectively retain control. Decentralized blockchains are immutable, which means that the data entered is irreversible. For Bitcoin, transactions are permanently recorded and viewable to anyone. Blockchain is a sequence of blocks, which holds a complete list of transaction records like conventional public ledger. Figure 1 illustrates an example of a blockchain. With a previous block hash contained in the block header, a block has only one parent block. It is worth noting that uncle blocks (children of the block’s ancestors) hashes would also be stored in ethereum blockchain. The first block of a blockchain is called genesis block which has no parent block. We then explain the internals of blockchain in details.

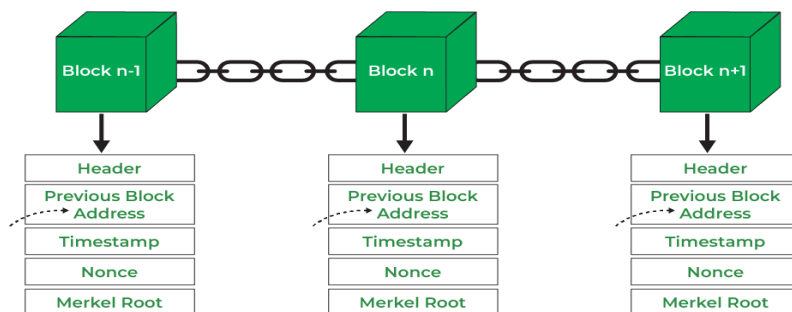


Figure1. Structure of Blockchain

Consists of the block header and the block body as shown in Figure 1 In particular, the block header includes:

- (i) **Block version:** indicates which set of block validation rules to follow: It is used to identify the particular block in the entire blockchain. It handles all blocks in the blockchain. A block header is hashed periodically by miners by changing the nonce value as part of normal mining activity, also Three sets of block metadata are contained in the block header.
- (ii) **Merkle tree root hash:** the hash value of all the transactions in the blockIt is a type of data structure frame of different blocks of data. A Merkle Tree stores all the transactions in a block by producing a digital fingerprint of the entire transaction. It allows the users to verify whether a transaction can be included in a block.
- (iii) **Timestamp:** current time as seconds in universal time since January 1, 1970. It is a system verify the data into the block and assigns a time or date of creation

for digital documents. The timestamp is a string of characters that uniquely identifies the document or event and indicates when it was created.

- (iv) **n Bits:** target threshold of a valid block hash.
- (v) **Nonce:** An 4-byte field, which usually starts with 0 and increases for every hash calculation (will be explained in details in Section III). A nonce number which uses only once. It is a central part of the proof of work in the block. It is compared to the live target if it is smaller or equal to the current target. People who mine, test, and eliminate many Nonce per second until they find that Valuable Nonce is valid.
- (vi) **Parent block hash:** a 256-bit hash value that points to the previous blockIt is used to connect the i+1th block to the ith block using the hash. In short, it is a reference to the hash of the previous (parent) block in the chain.

The block body is composed of a transaction counter and transactions. The maximum number of transactions that a block can contain depends on the block size and the size of each transaction. Blockchain uses an asymmetric cryptography mechanism to validate the authentication of transactions. Digital signature based on asymmetric cryptography is used in an untrustworthy environment. We next briefly illustrate digital signature.

Digital Signature

Each user owns a pair of private key and public key. The private key that shall be kept in confidentiality is used to sign the transactions. The digital signed transactions are broadcasted throughout the whole network. The typical digital signature is involved with two phases: signing phase and verification phase. For instance, an user Alice wants to send another user Bob a message. (1) In the signing phase, Alice encrypts her data with her private key and sends Bob the encrypted result and original data. (2) In the verification phase, Bob validates the value with Alice's public key. In that way, Bob could easily check

if the data has been tampered or not. The typical digital signature algorithm used in blockchains is the elliptic curve digital signature algorithm (ECDSA).

Key Characteristics of Blockchain

In summary, blockchain has following key characteristics.

- **Decentralization:** In conventional centralized transaction systems, each transaction needs to be validated through the central trusted agency (e.g., the central bank), inevitably resulting to the cost and the performance bottlenecks at the central servers. Contrast to the centralized mode, third party is no longer needed in blockchain. Consensus algorithms in blockchain are used to maintain data consistency in distributed network. Because of this distribution and the encrypted proof that work was done the information and history (like the transactions in cryptocurrency) are irreversible. Such a record could be a list of transactions (such as with a cryptocurrency), but it also is possible for a blockchain to hold a

variety of other information like legal contracts, state identifications, or a company's inventory.

- **Persistency:** Transactions can be validated quickly and invalid transactions would not be admitted by honest miners. It is nearly impossible to delete or rollback transactions once they are included in the blockchain. Blocks that contain invalid transactions could be discovered immediately.
- **Anonymity:** Each user can interact with the blockchain with a generated address, which does not reveal the real identity of the user.
- **Auditability:** Bitcoin blockchain stores data about user balances based on the Unspent Transaction Output (UTXO) model [2]: Any transaction has to refer to some previous unspent transactions. Once the current transaction is recorded into the blockchain, the state of those referred unspent transactions switch from unspent to spent. So transactions could be easily verified and tracked

Taxonomy of blockchain systems

Current blockchain systems are categorized roughly into three types: public blockchain, private blockchain and consortium blockchain. In public blockchain, all records are visible to the public and everyone could take part in the consensus process. Differently, only a group of pre-selected nodes would participate in the consensus process of a consortium blockchain. As for private blockchain, only those nodes that come from one specific organization would be allowed to join the consensus process. A private blockchain is regarded as a centralized network since it is fully controlled by one organization. The consortium blockchain constructed by several organizations is partially decentralized since only a small portion of nodes would be selected to determine the consensus. The comparison among the three types of blockchains.

- **Consensus determination:** In public blockchain, each node could take part in the consensus process. And only a selected set of nodes are responsible for validating the block in consortium blockchain. As for

private chain, it is fully controlled by one organization and the organization could determine the final consensus.

- **Read permission:** Transactions in a public blockchain are visible to the public while it depends when it comes to a private blockchain or a consortium blockchain.
- **Immutability:** Since records are stored on a large number of participants, it is nearly impossible to tamper transactions in a public blockchain. Differently, transactions in a private blockchain or a consortium blockchain could be tampered easily as there are only limited number of participants.
- **Efficiency:** It takes plenty of time to propagate transactions and blocks as there are a large number of nodes on public blockchain network. As a result, transaction throughput is limited and the latency is high. With fewer validators, consortium blockchain and private blockchain could be more efficient.

- **Centralized:** The main difference among the three types of blockchains is that public blockchain is decentralized, consortium blockchain is partially centralized and private blockchain is fully centralized as it is controlled by a single group.
- **Consensus process:** Everyone in the world could join the consensus process of the public blockchain. Different from public blockchain, both consortium blockchain and private blockchain are permissioned

Since public blockchain is open to the world, it can attract many users and communities are active. Many public blockchains emerge day by day. As for consortium blockchain, it could be applied into many business applications. Currently, Hyperledger is developing business consortium blockchain frameworks. Ethereum also has provided tools for building consortium blockchains.

Consensus algorithms

In blockchain, how to reach consensus among the untrustworthy nodes is a

transformation of the Byzantine Generals (BG) Problem. In BG problem, a group of generals who command a portion of Byzantine army circle the city. Some generals prefer to attack while other generals prefer to retreat. However, the attack would fail if only part of the generals attack the city. Thus, they have to reach an agreement to attack or retreat. How to reach a consensus in distributed environment is a challenge. It is also a challenge for blockchain as the blockchain network is distributed. In blockchain, there is no central node that ensures ledgers on distributed nodes are all the same. Some protocols are needed to ensure ledgers in different nodes are consistent. We next present several common approaches to reach a consensus in blockchain.

Approaches to consensus

PoW (Proof of work) is a consensus strategy used in the Bitcoin network. In a decentralized network, someone has to be selected to record the transactions. The easiest way is random selection. However, random selection is vulnerable to attacks. So if a node wants to publish a block of

transactions, a lot of work has to be done to prove that the node is not likely to attack the network. Generally the work means computer

Current obstacles and latest breakthroughs

Obstacles

1. Scalability: Traditional blockchains like Bitcoin and Ethereum process only a few transactions per second (TPS), which is inadequate for large-scale applications.
2. Energy Consumption: Proof-of-Work (PoW) requires significant computational resources, making it environmentally and economically unsustainable.
3. Regulatory Uncertainty: Governments worldwide are still struggling to define legal frameworks, particularly around cryptocurrency and data privacy.
4. Interoperability: Lack of standardization hampers the interaction between different blockchain networks.

5. Latency: In public blockchains, transaction validation delays can affect real-time applications.

Despite the promising nature of blockchain technology, it faces several obstacles that hinder its large-scale adoption.

1. Scalability: One of the primary concerns is the limited number of transactions per second (TPS) supported by public blockchains like Bitcoin and Ethereum. As transaction volumes grow, current consensus mechanisms struggle to maintain efficiency, leading to network congestion and high fees.

2. Energy Consumption: Proof of Work (PoW), the most widely used consensus mechanism, is highly energy-intensive. The requirement for massive computational power has raised sustainability concerns, especially in light of global environmental goals.

3. Security Threats: Although blockchain is secure by design, it is not immune to threats like 51% attacks, double-spending, smart

contract vulnerabilities, and phishing attacks on users.

4. Regulatory Uncertainty: The lack of consistent legal frameworks and governance models across countries creates uncertainty. Many governments are still determining how to regulate blockchain, especially in areas involving cryptocurrencies and privacy.

5. Interoperability: Different blockchain platforms operate in silos. There is limited interaction between networks, making data exchange and asset transfers cumbersome.

Latest Breakthroughs Include:

- Layer 2 Scaling Solutions: Like Lightning Network (for Bitcoin) and Ethereum's Optimistic Rollups improve scalability by processing transactions off-chain.
- Green Consensus Mechanisms: Adoption of Proof of Stake (PoS) and Delegated PoS significantly reduces energy consumption.

- **Cross-chain Communication Protocols:** Technologies like Polkadot and Cosmos enable seamless interoperability between blockchains.
- **Zero-Knowledge Proofs (ZKPs):** Improve privacy while allowing secure data validation without revealing the actual data.

Emerging Trends and innovations

Blockchain is rapidly evolving, with new applications and innovations emerging across industries:

1. **Decentralized Finance (DeFi):** DeFi platforms offer traditional financial services such as lending, borrowing, and trading in a decentralized manner without intermediaries.
2. **Non-Fungible Tokens (NFTs):** NFTs represent ownership of unique digital assets and are revolutionizing industries such as gaming, art, and entertainment.
3. **Smart Cities and IoT Integration:** Blockchain is being integrated with IoT devices to enhance automation,

data security, and transparency in smart city applications.

4. **Identity and Access Management:** Blockchain offers secure, decentralized digital identity solutions that reduce fraud and empower users to control their personal data.
5. **Supply Chain Transparency:** Many industries are leveraging blockchain to track goods from origin to delivery, ensuring authenticity and ethical sourcing.
6. **Central Bank Digital Currencies (CBDCs):** Governments are exploring or piloting digital currencies using blockchain for more efficient and traceable monetary systems.

Conclusion

Blockchain technology is reshaping the way we envision trust, transparency, and security in digital interactions. From its roots in cryptocurrency to its expansion into finance, healthcare, governance, and logistics, blockchain is unlocking innovative solutions to long-

standing problems. However, its widespread adoption is contingent on overcoming technical and regulatory challenges. With ongoing research, collaborative standardization, and the

development of more sustainable and scalable platforms, blockchain is poised to become a foundational technology for the future digital economy.

References

Buterin, V. (2014). Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform.

Dai, H.-N., Zheng, Z., & Zhang, Y. (2019). Blockchain for Internet of Things: A survey.

Garay, J., Kiayias, A., & Leonardos, N. (2020). Proof-of-stake protocols: Security definition and improvements.

Gorenflo, C., Lee, S., Golab, L., & Keshav, S. (2020). FastFabric: Scaling Hyperledger Fabric to 20,000 Transactions per Second.

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on the security of blockchain systems.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—a systematic review.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends.

To cite this article

Priyadharsini, A. (2025). An Investigation and Overview of Blockchain Technology: Architecture, Consensus, and Its Future Trends. *John Foundation Journal of EduSpark*, 7(3), 1-13.

ABOUT THE AUTHOR



Priyadharsini Arumugam is an Assistant Professor in the Department of BCA at Nallamuthu Mahalingam College, Pollachi, Coimbatore District, Tamil Nadu, India. She holds a B.Sc. (Mathematics), MCA, and M.Phil. in Computer Science. She has actively participated in and presented papers at various national seminars and conferences.
