IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 27, Issue 5, Ser. 4 (Sept. – Oct. 2025), PP 61-64
www.iosrjournals.org

Security Designing Aspects Of Blockchain Technology

Mrs. Pallavi Mahendra Jain, Mrs. Chanchal Aniruddha Rapatwar,
Mr. Pratik Sunil Jaiswal
Assistant Professor Deogiri Instittute Of Technology & Management Studies, Chh. Sambhajinagar (M.S) India

Abstract
Blockchain, or Distributed Ledger Technology (DLT), is an immutable digital ledger system implemented in a distributed fashion without a central repository or authority, gaining significant traction across various industries, including finance, healthcare, and IoT. While the technology offers reliable and expedient services, the security and privacy issues and challenges remain a critical concern. This paper focused on introducing blockchain technology, its models (Public and Private), its working mechanism, and its architecture. Blockchain records cryptographically signed transactions grouped into blocks, where each new block is cryptographically linked to the previous one after validation via a consensus decision. The architecture involves a sequence of blocks, each containing a block header (with elements like Parent Block Hash, Merkle Tree Root Hash, and Nonce) and a list of transactions. The process relies on network-wide validation, often using consensus algorithms like Proof-of-Work (PoW), to ensure that the ledger is permanent and immutable.

Keywords: *Distributed Ledger Technology (DLT), Cryptographically Signed Transactions, Ethereum, Bitcoin.*

Date of Submission: 04-10-2025 Date of Acceptance: 14-10-2025

I. Introduction

Distributed ledger technologies or Block chains are immutable digital ledger systems implemented in a distributed fashion (i.e. without a central repository) and usually without a central authority[1]. This technology became widely known in the beginning of 2008 when it was applied to enable the emergence of electronic currencies where digital transfers of money take place in distributed systems. Various digital currency systems such as Bitcoin, Ethereum, Ripple, and Litecoin are only an example of this technology. Infact, this technology is broadly useful and can be used for variety of applications[2]. Block chains are distributed digital ledgers of cryptographically signed transactions that are grouped into blocks. Each block is cryptographically linked to the previous one after validation and undergoing a consensus decision. As new blocks are added, older blocks become more difficult to modify. New blocks are replicated across all copies of the ledger within the network, and any conflicts are resolved automatically using established rules. Presently, there are mainly two types of block chain: Public Blockchain validate transactions and bundle them into blocks to add to the ledger[3]. Any computer connected to the internet can join the party. Private blockchains, on the other hand, typically only permit known organizations to join. Together, they form a private, members-only "business network." This difference has significant implications in terms of where the (potentially confidential) information moving through the network is stored and who has access to it. Bitcoin is probably the most well-known example of a public blockchain and it achieves consensus through "mining." In Bitcoin mining, computers on the network (or 'miners') try to solve a complex cryptographic problem to create a proof of work[4].

Problem Statement

Blockchain is gaining popularity and may be considered one of the most popular subjects nowadays. Although skeptics dispute its scalability, security, and sustainability, it has already changed many people's lifestyles in certain ways owing to its enormous effect on industries and enterprises[5]. While the advantages of blockchain technology promise more dependable and efficient services, it is critical to evaluate the security and privacy concerns and obstacles that lie beneath the new technology. Blockchain applications span a wide range of industries, including finance, healthcare, automotive, risk management, the Internet of Things (IoT), public and social services. Several research focus on using the blockchain data structure in different applications. This presentation subject focuses mostly on the introduction of blockchain technology, its models, and numerous security concerns, as well as countermeasures to combat such threats in the blockchain context[6].

Working Of Blockchain Technology

The blockchain is a database or a ledger that provides a way for information to be recorded and shared by a community. In this community, each member keeps his or her copy of the information, and all members must

validate any updates collectively. It's distributed in nature, meaning that there is no central server holding the entire database or chain, but instead, the participating nodes have a copy of the ledger[7]. The new records are appended to the ledger. Typically, from record perspective, blockchain consists of two types of elements. Transactions are the actions created by participants in the blockchain network. Blocks record these transactions and make sure they are in right sequence and have not been tampered. Blocks also record the timestamp when the transactions were added. Each block has one or more than one transaction[8].

Let us suppose A wants to send money to B. First, a block is created online and represents the transaction. Then this block is broadcasted to every participant in the blockchain network and set of participants approves the transaction and validates it[9]. Once the block is validated, it is added to the chain which provides a permanent, non-reputable and transparent record of the transaction. Finally, B receives the money from A. The above steps are shown clarified in Figure 1.

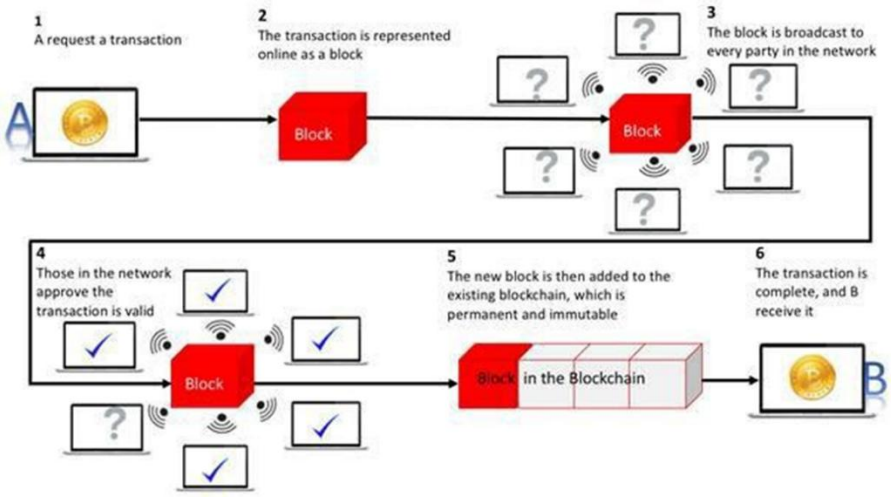

Figure 1: Working of Blockchain.

The following are the specific procedures involved in the blockchain network. Transaction. Data exchange refers to the exchange of digital assets such as money, products, contracts, medical records, consumer information, and more. The transaction is transmitted to all participants in the system. There are two sorts of transactions in Bitcoin. Users create conventional transactions that involve coins. Coinbase transactions, also known as Generation transactions, are made by miners to reward themselves. Miners receive a reward after successfully mining a block[10]. The current block reward is 12.5 Bitcoins per block, and the reward halves every 210,000 blocks, or roughly every four years ("Bitcoin Block Reward Halving Countdown," n.d.). In case of Bitcoin, only the UXTO (Unspent Transaction Output Set) is stored in the memory and the remaining data is stored on the disk ("Weaknesses–Bitcoin Wiki," n.d.). Once a client wants to process a transaction, before fetching transaction inputs from disk to memory, the client checks that all the inputs are unspent[11].

Verification: Depending on the blockchain network's characteristics, the transaction is either validated instantly or queued with other pending transactions (Piscini et al., 2016). The network's nodes use agreed-upon criteria to decide whether a transaction is legitimate or invalid.

Structure: The block includes the transaction or collection of transactions, and each block is recognized by a 256-bit hash value generated by the network's agreed-upon message digest algorithm. Typically, the SHA256 message digest method is utilized. A block typically consists of a header, a reference to the preceding block hash, and a collection of transactions.

Validation: Blocks must be verified before being added to the blockchain. Proof-of-Work (PoW) is the most common consensus mechanism for validating blocks. Miners solve a mathematical puzzle based on the block's header.

Mining involves using Proof-of-Work or other consensus techniques to solve mathematical puzzles. Once solved, blocks are verified. Mining is the process of finding an input to a cryptographic hash function that hashes less than or equal to a predetermined target value. The brute force method involves gradually changing the text to be hashed in each cycle to ensure a correct hash is obtained.

Block Chain Security

Blockchain is a complicated system consisting of distributed digital ledgers containing crypto graphically signed transactions organized into blocks. Blockchain has the following security features:

I. Blockchain technology uses a ledger to keep track of all financial transactions. Normally, this type of "master" ledger would be an obvious source of risk. A hacked ledger might cause a system meltdown. For instance, tampering with a record might lead to unlimited financial gain. Simply reading all transactions might expose crucial private information. The blockchain ledger is decentralized. This implies that no single computer or system has control over the ledger at any moment. Gaining access to the main ledger would require a sophisticated and coordinated attack on thousands of machines at once.
II. Another security principle is the chain itself. The ledger is a lengthy chain of encrypted consecutive chunks. Each link is a piece of the bigger puzzle. These records date back to the system's debut. This means that anybody attempting to modify a transaction must first modify all transactions before it, and do so precisely. This complicates the potential tampering procedure. Furthermore, it significantly raises the Overall security of the system.
III. In contrast to current payment systems, a block chain architecture involves hundreds to thousands of unique nodes. Each node has a full copy of the digital ledger. These can independently verify the transaction. If the nodes cannot agree, the transaction is canceled. This system keeps the ledger organized. Furthermore, the complicated mechanics make it difficult to conduct fraudulent transactions.
IV. Block chain exchanges utilize complicated cryptographic keys that require authority to decode.

Block Chain Security Issues And Challenges

Blockchain has a highly sophisticated and robust structure. However, there are security issues and obstacles with this technology. Bitcoin is vulnerable to several types of attacks, including wallet assaults (client-side security), network attacks (e.g. DDoS, sybil, eclipse), and mining attacks (e.g. 50%, block withholding, and bribery). Double spending is always a possibility.

Traditional Challenges

The use of a distributed ledger implies that data is shared between all counterparties on the network. On one side this could potentially have a negative impact on the confidentiality; while on the other, it has a positive impact on availability with many nodes participating in the Blockchain, making it more robust and resilient. Some of traditional security challenges are:

Key Management: Private keys are the direct means of authorizing activities from an account, which in the event they get accessed by an adversary, will compromise any wallets or assets secured by these keys.

Potentially different private keys could be used for signing and encrypting messages across the distributed ledger. An attacker who obtained encryption keys to a dataset would be able to read the underlying data. A private key is usually generated using a secure random function, meaning that reconstructing it is difficult, if not impossible. If a user loses a private key, then any asset associated with that key is lost. If a private key is stolen, the attacker will have full access to all assets controlled by that private key and once a criminal steals the key and transfer funds to another account, it cannot be undone.

If a user loses a private key, all connected assets are gone. If a private key is taken, the attacker gains access to any assets owned by that key. Once stolen, monies transferred to another account are irreversible.

Cryptography: Blockchains use cryptographically generated public and private keys. Cryptography requires strict rules and procedures for key management, encompassing people, processes, and technology. Cryptographic key generation software should provide robust and difficult-to-decrypt keys.

Privacy: Privacy is another concern that arises from the use of Blockchain technology. In a permission-less ledger, any counterparties can download the ledger, allowing them to view the whole transaction history, even if they are not members. Exploiting authorized agent or smart contract capabilities in a permissioned ledger may expose sensitive information, depending on the author's access rights.

The Majority Attack (51% Attacks)

With Proof of effort, the likelihood of mining a block is determined by the miner's effort (for example, CPU/GPU cycles spent checking hashes). Because of this process, users will want to band together to mine more blocks, forming "mining pools" where the majority of computational power is concentrated. Once it has 51% computer power, it can seize control of the blockchain. This might lead to security issues in a chain.

If someone possesses more than 51% processing power, he or she can determine the Nonce value faster than others, indicating that he or she has the ability to select which block is allowed. After this, the attacker can:

i. Modify the transaction data, which may result in a double-spending attack.
ii. Stop the block verification transaction.
iii. iii. To stop miner mining any available block.

II. Conclusion

Distributed Ledger Technologies (DLT) or blockchain has become one of disruptive technologies with great potential to change our economy, culture and society. DLT enables innovative financial/non-financial decentralized applications that eliminate the need for third party intermediaries. This technology is introducing new data management infrastructure that will accelerate a services revolution in industries (for example, banking and finance, government, healthcare and super logistics) based on telecommunications. These are a significant new avenue for technological advancements, enabling secure transactions without the need for a central authority. This technology will significantly influence telecom customers and sectors, including telecom service providers. This has the potential to significantly increase income for service providers. Identifying the roles and responsibilities of telecom consumers, operators, and service providers in the DLT context is crucial for security.

Reference

[1] Alex. R. Mathew "Cyber Security Through Blockchain Technology" International Journal Of Engineering And Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-9 Issue-1, October 2019
[2] Egelund-Müller, B., Elsman, M., Henglein, F., & Ross, O. (2017). Automated Execution Of Financial Contracts On Blockchains. Business & Information Systems Engineering, 59(6), 457–467.
[3] Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016). On The Security And Performance Of Proof Of Work Blockchains. In Proceedings Of The 2016 ACM SIGSAC Conference On Computer And Communications Security (CCS). Vienna, Austria.
[4] Goldfeder, S., Kalodner, H., Reisman, D., & Narayanan, A. (2018). When The Cookie Meets The Blockchain: Privacy Risks Of Web Payments Via Cryptocurrencies. Proceedings On Privacy Enhancing Technologies, 2018(4), 179–199 [5] Hyvärinen, H., Risius, M., & Friis,
[5] G. (2017). A Blockchain-Based Approach Towards Overcoming Financial Fraud In Public Sector Services. Business & Information Systems Engineering, 59(6), 441–456.
[6] Kumar, A., Fischer, C., Tople, S., & Saxena, P. (2017). A Traceability Analysis Of Monero's Blockchain. In Proceedings Of The 22nd European Symposium On Research In Computer Security (ESORICS) (Pp. 153–173). Oslo, Norway
[7] Mr. Pratik S. Jaiswal, Dr. Rameshwar R. Gaikwad, Mrs. Karuna Patel, "Integrating Blockchain Technology In Online Trading", International Journal Of Creative Research Thoughts (IJCRT) -Www.Ijcrt.Org Volume 13, Issue 4 April 2025 | ISSN: 2320-2882.
[8] W. Wang, And C. Su. "CCBRSN: A System With High Embedding Capacity For Covert Communication In Bitcoin." In IFIP International Conference On ICT Systems Security And Privacy Protection, Pp. 324-337. Springer, Cham, 2020.
[9] L. Zhang, Z. Zhang, W. Wang, R. Waqas, C. Zhao, S. Kim, And H. Chen, 2020. A Covert Communication Method Using Special Bitcoin Addresses Generated By Vanitygen. CMC-COMPUTERS MATERIALS & CONTINUA, 65(1), Pp.597-616.
[10] S. Li, F. Liu, J. Liang, Z. Cai And Z. Liang: Optimization Of Face Recognition System Based On Azure Iot Edge, Computers, Materials & Continua, Vol. 61, No. 3, Pp.1377-1389, 2019.
[11] D. Kim, S. Min And S. Kim: A DPN (Delegated Proof Of Node) Mechanism For Secure Data Transmission In Iot Services, Computers, Materials & Continua, Vol. 60, No. 1, Pp.1-14, 2019.