Grenze International Journal of Engineering and Technology, January Issue

Blockchain Security: A Comprehensive Review of Current Threats and Solutions

Rupanshi Agarwal[1], Akash Sanghi[2], Priyanka Vishwakarma[3] and Gaurav Agarwal[4]
[1]Assistant Professor, Department of CSE, Invertis University, Bareilly, Uttar Pradesh, India
Email: rupanshi.aggarwal28@gmail.com
[2, 4]Associante Professor, Department of CSE, Invertis University, Bareilly, Uttar Pradesh, India
Email: sanghiakash@gmail.com, priyankavishwakarma210@gmail.com
[3]Assistant Professor, Department of CSE, Kamla Nehru Institute of Physical and Social Sciences, Faridipur, Sultanpur, Uttar Pradesh, India
Email: gaurav.a1@invertis.org

***Abstract*—Block chain technology has become a ground-breaking and revolutionary invention that is transforming a number of industries by offering a transparent and safe way to record and validate transactions. This research paper introduces the fundamental principles, architecture, security aspects of block chain technology and provide some countermeasures to security is-sues. The study delves into the decentralized aspect of block chain technology and clarifies its fundamental elements, such as distributed ledgers, consensus methods, and cryptographic concepts The paper's major focus is on block chain security, highlighting how crucial it is to preserve data availability, integrity, and confidentiality within distributed ledgers. It examines security problems like double-spending, 51% assaults, and smart contract weaknesses, clarifying the possible dangers that block chain ecosystems might face. This paper examines cutting-edge block chain security innovations and solutions in response to recognized security issues. By integrating an introduction to block chain, a detailed examination of its security mechanisms and a critical assessment of its solutions, this research paper aims to provide a comprehensive understanding of the current state of block chain technology.**

***Index Terms*— Block chain, distributed ledgers, consensus methods, double spending.**

I. INTRODUCTION

Within the modern information technology landscape, block chain technology has become a disruptive force that is transforming conventional ideas about security, trust, and decentralized governance [1]. Block chain technology, originally conceptualized as the underpinning technology for the digital currency Bitcoin, has rapidly evolved into a revolutionary force with transformative implications across various industries. At its core, block chain represents a decentralized and distributed ledger system that enables secure, transparent, and tamper-resistant recording of transactions [2].

At its essence, block chain introduces a paradigm shift by offering a decentralized and distributed ledger system [2]. Unlike conventional centralized databases, which rely on a single authoritative entity for transaction validation, block chain leverages a network of nodes to achieve consensus. This departure from centralization not only ensures transparency but also fortifies the security and integrity of recorded transactions [1].

The fundamental components of block chain encompass distributed ledgers, cryptographic techniques, and

Grenze ID: 01.GIJET.11.1.406

consensus mechanisms. Distributed ledgers, maintained across a network of nodes, serve as a tamper-resistant record of transactions [3]. Cryptographic principles ensure the security of data, and consensus mechanisms, such as Proof of Work (PoW) or Proof of Stake (PoS), enable agreement among participants, fostering trust in a trust less environment [1].

However, the integration of block chain is not without challenges. Scalability concerns, energy consumption, and the imperative for interoperability are persistent areas of research and development [4]. Acknowledging these challenges is pivotal to comprehending the full scope of block chain technology and sets the stage for an in-depth exploration of security mechanisms, emerging trends, and potential solutions in subsequent sections of this research paper [1].

As block chain technology continues to evolve and permeate diverse industries, this research contributes to the foundational understanding essential for navigating its multifaceted landscape. The subsequent sections will unravel the intricate layers of block chain, shedding light on its security features, ongoing developments, and the transformative impact it holds for the future of digital transactions and decentralized ecosystems.

II. Working Method of Blockchain

In addition to serving as a chronological series of blocks housing recorded transactions, the block chain is commonly recognized as a public ledger. With the consistent addition of new blocks at regular intervals, the chain undergoes continuous expansion. The following detailed explanation outlines the fundamental components and processes involved in the working of a block chain.

A. Nodes

Nodes are standalone computers or other devices that make up the block chain network. A duplicate of the complete block chain ledger is kept by every node. Nodes could be either non-mining users or miners, who are in charge of approving transactions and building new blocks. Transactions: A transaction is a basic data item in a block chain that symbolizes the transfer of data or products between network users. Within the block chain network, a transaction is a digital record that details the transfer of assets or information from a participant to another.

B. Verification

All network nodes receive broadcasts of transactions. Nodes use pre-established rules to confirm each transaction's legitimacy [2]. These regulations frequently entail verifying the digital signatures and making sure the sender has enough money.

C. Block Formation

A block is made up of all the valid transactions. The word "block chain" refers to the chain of blocks that is created when each block has a hash that links it to the preceding block.

D. Consensus Mechanism

A set of guidelines or protocols that guarantee network nodes agree on the legitimacy of transactions and the sequence in which they should be added to the block chain constitute a consensus mechanism in block chain technology [5]. They make it possible for nodes to cooperate, come to an agreement, and stop bad actors from exploiting the block chain.

E. Addition to the block chain

Once a block is validated and added to the block chain, it becomes a permanent part of the ledger [5]. The hash of this block is referenced in the subsequent block, creating a secure and tamper-resistant chain.

F. Transparency and Immutability

Because block chain is transparent, everyone can see the complete history of transactions.

Every transaction on a block chain must first pass through a number of crucial procedures. One can examine the block chain’s operation from Fig. 1. When authentication is necessary for a transaction on the block chain, a block containing the transaction's data is created. Next, every node or block chain participant receives the newly produced block [6]. Then the nodes validate the transaction. The transaction won't be recorded when the validation fails. The transaction is finished if validation is successful. Additionally, all of the nodes in that specific block chain network will receive the updates. Following that, the block is added to the block chain. The nodes are rewarded for their Proof of Work, typically with cryptocurrency.

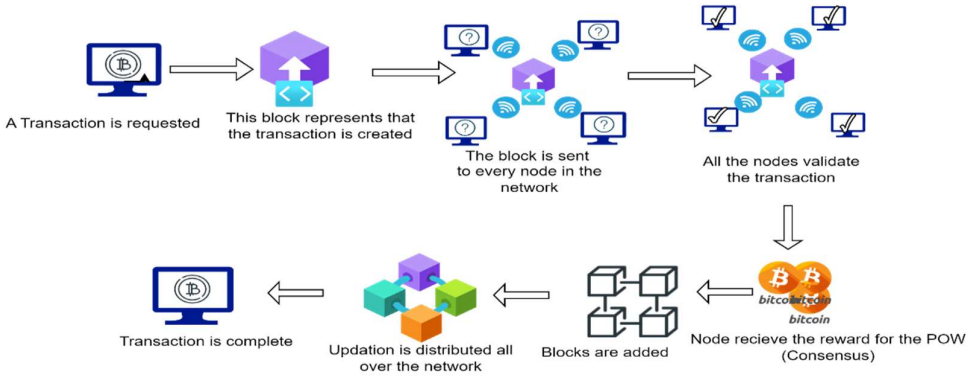

Figure 1. Working of Block chain

III. Proof of Work (PoW)

In block chain technology, Proof of Work (PoW) is a crucial consensus technique that is essential to both the decentralised preservation of a public ledger and the safe validation of transactions [7]. PoW is a consensus-building technique that was first included in the groundbreaking cryptocurrency Bitcoin. It eliminates the need for a central authority.

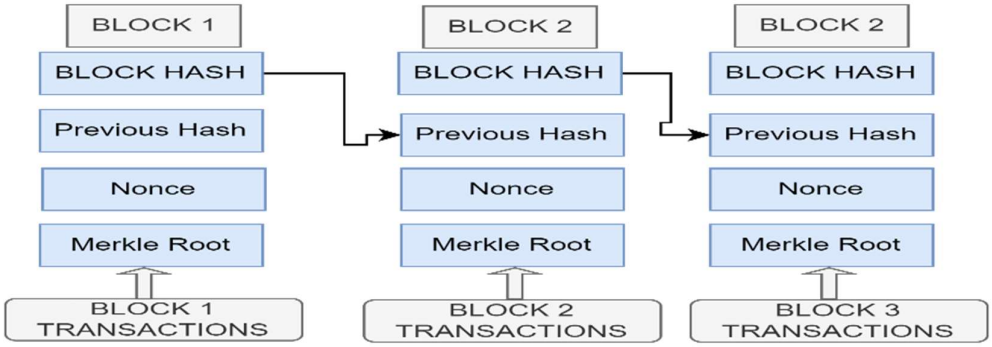

Figure 2. Block diagram of Block chain

Fig. 2 shows that each block in a block chain is made up of four headers, and those are:

A. Block Hash

In proof of work (PoW), the block hash is crucial since it needs to meet certain requirements in order to show that miners have put in a significant amount of processing power to produce a new block.

B. Previous Hash

This hash address is where the previous block is located. A block's reference to the block before it is also present. The hash before this one makes reference to it.

C. Nonce

In order to find a legitimate hash that meets the difficulty requirements, miners must modify a nonce, which is a numerical value.

D. Merkle Root

The Merkle root is an essential part of the block header in the Proof of Work (PoW) consensus process used by block chains. It is a synopsis of all the transactions contained in a block provided by a cryptographic hash.

IV. Types of Blockchain

There are various kinds of block chains, each intended to fulfil particular functions and handle various use cases. Among the primary kinds of block chains are:

A. Public block chain

Anybody having a base asset can use a public block chain, which is a fully decentralized block chain. An open, permission less distributed ledger that is available to anybody wishing to participate is called a public block chain. Users from all around the world can validate transactions and participate in the consensus process because to its decentralised operation. Examples are cryptocurrencies like Ethereum and Bitcoin [5].

B. Private block chain

A private block chain is a permissioned distributed ledger system that is only accessible by a specific set of users or organisations. It places a strong emphasis on data privacy by limiting access to sensitive information to authorised users only [4].

C. Consortium Block chain

A consortium block chain combines elements of a public and private block chain. It permits shared governance and restricted ac-cess among a chosen set of organisations. A consortium block chain is a permissioned distributed ledger system created by several entities working together to keep the network up to date [8]. Only the participating entities have access to the consortium block chain, guaranteeing a permissioned environment. Consortium block chains, as opposed to public block chains, offer a compromise between control and decentralisation by enabling recognised parties to cooperatively verify transactions and oversee the network [9].

V. APPLICATIONS OF BLOCKCHAIN

Blockchain technology has completely changed a number of businesses by offering a decentralised, transparent, and safe way to manage data and record transactions. Its applications cut across several industries and provide novel answers to enduring problems. Here, we examine some of the most important uses for blockchain technology, emphasising both its practical applicability and importance.

A. Financial Services

The financial services sector has been significantly impacted by blockchain technology, which provides creative solutions for safe and effective transactions [10]. Some of the financial services which are provided by blockchain technology are:

(a) Cryptocurrencies: Cryptocurrencies, which enable peer-to-peer transactions without the need for middlemen like banks, are based on blockchain technology [10][11].

Bitcoin: The original cryptocurrency [1][10], it allows for safe, open transactions on a distributed ledger.

Ethereum: Ethereum uses smart contracts to expand the capabilities of blockchain technology and enable the development of decentralised apps (dApps) [12].

(b) Cross-Border Payments: The time and expense of international transactions are greatly decreased by blockchain technology.

Ripple (XRP): Ripple's blockchain technology streamlines and lessens the need for conventional banking networks by enabling quick and inexpensive cross-border payments [11][13].

Decentralised Finance (DeFi): DeFi uses blockchain technology to provide typical middlemen-free financial services like lending, borrowing, and trading.

Compound and Aave: These DeFi platforms let users lend and borrow assets in a transparent and safe manner by utilising smart contracts [14].

B. Supply Chain Management

Supply chain operations are improved by blockchain technology through increased efficiency, transparency, and traceability [12][14].

(a) Traceability and Transparency: Blockchain guarantees the authenticity and quality of items by improving supply chain traceability and transparency.

IBM Food Trust: Using an open supply chain to guarantee safety and authenticity, this blockchain network follows food goods from farm to table [14].

(b) Anti-Counterfeiting: Blockchain contributes to the prevention of supply chain fraud and counterfeiting by offering an unchangeable record of every transaction [14][15].

Everledger: This blockchain technology ensures the authenticity and combats fraud by tracking the provenance of valuable commodities like diamonds.

C. Medical Care

Blockchain helps the healthcare industry by enhancing data security and improving patient care.
(a) Management of Medical Records: Blockchain ensures data integrity and privacy while protecting patient records and facilitating easy sharing between healthcare professionals [14].
MedRec: A secure, all-inclusive medical history accessible to physicians and patients via a blockchain-based medical record management system [14].
(b) Pharmaceutical Supply Chain: By monitoring the manufacture and distribution of medications, blockchain protects the integrity of the pharmaceutical supply chain.
Chronicled: By offering an unalterable and visible trail of medications' travel from producer to customer, this blockchain technology guarantees the legitimacy of pharmaceuticals.

D. Real Estate

Blockchain technology guarantees secure property ownership records and streamlines real estate transactions.
(a) Property Transactions: Blockchain makes real estate transactions easier by facilitating quicker, more secure ownership transfers and minimising paperwork.
Propy: Propy is a blockchain-based platform that uses smart contracts to automate and minimise the need for middlemen in real estate transactions [15].
(b) Title Management: A tamper-proof record of property ownership is provided via blockchain, which helps to thwart fraud and title disputes.
Ubitquity: This platform ensures accurate records of property ownership by using blockchain technology to provide transparent and secure title administration.

E. Voting Systems

Blockchain ensures the integrity of elections and other decision-making processes by providing transparent and safe voting alternatives [16].
(a) Election Security: Elections may be conducted securely and transparently with blockchain, guaranteeing that votes are cast and counted correctly.
Voatz: A blockchain-based mobile voting technology that secures election data to guarantee voting process integrity and facilitate safe absentee voting [16].
(b) Corporate Governance: Blockchain technology is used by businesses to conduct transparent and precise vote counting during shareholder meetings.
Nasdaq's Linq: This blockchain platform offers improved security and transparency for corporate governance functions including shareholder voting [13].

VI. Blockchain Security

Ensuring the availability, confidentiality, and integrity of data within a block chain network is reliant upon block chain security. In this research paper, important factors for block chain security to take into account are:

A. Cryptography

Block chain mostly uses cryptographic methods to protect data. Cryptographic algorithms provide privacy, digital signatures verify transactions, and hash functions guarantee the immutability of blocks [9].

B. Decentralization

Block chain's decentralised structure adds to its security. A dispersed network of nodes resists malicious assaults and single points of failure by validating and approving transactions [4].

C. Consensus Mechanisms

Consensus algorithms, like Proof of Work (PoW) or Proof of Stake (PoS), are essential to block chain security because they stop double-spending and guarantee that all participants agree on the ledger's current state [1].

D. Smart Contracts Security

On the block chain, smart contracts are self-executing code that needs to be thoroughly audited in order to find and fix problems. Smart contract security holes may result in monetary losses or the block-chain network being exploited [10].

E. Governance

The collaborative maintenance, security, and advancement of the block chain network can be ensured through the establishment of efficient governance systems. Participants' security and trust are increased by well-defined policies and processes[13]. This section insights the various performance parameters used for the analysis and evaluation of proposed scheme and its comparison with the performance of existing routing protocols. Total number of nodes in the network are designated by N.

VII. BLOCKCHAIN SECURITY ISSUES AND COUNTERMEASURES

The structure of block chain is extremely hardy and intricate. Despite this, there are a number of security-related issues and difficulties with this technology. In addition to double spending, which is always possible with Bitcoin, there are other types of attacks that may be carried out against the system, such as client-side security, DDoS, eclipse, and Sybil attacks as well as mining attacks like 50%, block withholding, and bribery. Various security issues associated with blockchain are discussed in table 1.

TABLE I: PARAMETER VALUES USED IN SIMULATION

Security Issue	Issue Description	Counter Measure
51% attack	When one person or organisation has control over most of the network's processing capacity, they can falsify transactions, double-spend cryptocurrency, or otherwise interfere with the network. This is known as a 51% assault[1].	Implementing a consensus mechanism that requires a majority of network participants to agree on the validity of transactions[1].
Double Spending	Ensuring that every transaction is distinct and impossible to replicate by using cryptographic techniques such as digital signatures[1][3].	The practice of using the same cryptocurrency tokens more than once is known as "double spending.[3]" By making sure that every transaction is safely recorded and validated, this may be avoided.
Sybil attack	In a Sybil assault, several fictitious identities are created in an attempt to take over a network. By demanding proof of work or proof of stake from participants, Proof of Work and Proof of Stake technologies assist avoid this[2].	Putting into practice strategies like Proof of Stake (PoS) and Proof of Work (PoW) to guarantee that users have a stake in the network[2].
Smart Contract Vulnerabilities	Smart contracts are prone to errors or weaknesses that could be used to control or syphon off money[10]. Formal verification, secure coding techniques, and thorough code audits can all be used to detect and reduce these risks.	Putting secure coding practices into practice, carrying out exhaustive code audits and testing, and applying formal verification methods[10].
Wallet Management	Safeguarding private keys and controlling access to bitcoin funds are two aspects of wallet management. Strong authentication procedures, hardware wallets, and secure storage options all aid in preventing theft and unwanted access[3][10].	Using hardware wallets, enabling two-factor authentication, implementing secure storage methods, and routinely updating wallet software[10].
Eclipse Attack	Isolating a node by severing its connections to the rest of the network is known as an eclipse attack. Eclipse attacks can be avoided or at least lessened with the implementation of strong peer discovery techniques and the upkeep of a diversified network of connections[13][15].	Putting in place peer discovery techniques that lessen the possibility of malevolent nodes controlling a victim's network connections[13].
Transaction Malleability	Because of transaction malleability, attackers can alter transaction data before it is verified, which can result in problems like double spending. Using distinct transaction identifiers and implementing stringent validation guidelines are examples of preventive measures[1][13].	Putting policies in place such requiring stringent validation guidelines for transaction inputs and employing unique transaction identifiers[1][13].

VIII. CONCLUSION AND FUTURE SCOPE

To sum up, block chain technology has the potential to completely transform a number of industries by offering decentralized, transparent, and safe solutions. While there are undoubtedly difficulties and security concerns with block chain, like the possibility of 51% attacks, weaknesses in smart contracts, and privacy issues, these problems may be resolved by continuous research, development, and use of best practices.

To guarantee the long-term sustainability and security of block chain ecosystems, these problems can be resolved with proactive steps like strong encryption techniques and consensus procedures.

Block chain's potential applications in security are numerous and bright. We should anticipate additional use cases and applications as technology develops further, especially in fields like digital identity, voting systems, and supply chain management. Furthermore, the creation of fresh consensus algorithms like proof-of-stake and proof-of-authority might aid in resolving some of the present security issues with block chain technology. Future research and development initiatives should concentrate on quantum-resistant encryption, decentralized identification solutions, privacy improvements, interoperability standards, and scalability solutions. By addressing these issues, we can improve block chain technology's usability, scalability, and security and open the door for more innovation and industry revolution.

REFERENCES

[1] Moosavi, N., & Taherdoost, H. (2023). Blockchain Technology Application in Security: A Systematic Review. Blockchains, 1(2), 58-72. doi: 10.3390/blockchains1020005

[2] Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A Survey on Security and Privacy of Blockchain Systems. In 2017 IEEE 24th International Conference on Software Analysis, Evolution and Reengineering (SANER) (pp. 332-335). IEEE.

[3] Li, M., Li, Y., Li, Z., & Liu, Y. (2017). A Survey on Security Issues of Blockchain Systems. In 2017 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.

[4] Mougayar, W. (2016). The Business Blockchain: Promise, Practice, and Applica-tion of the Next Internet Technology. Wiley.

[5] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. In Proceed-ings of the 3rd Conference on Financial Cryptography and Data Security (FC) (pp. 1-12). Springer.

[6] Tseng, Y., & He, Y. (2019). A Survey on Blockchain Security: Attacks and De-fenses. In 2019 IEEE 19th International Conference on Trust, Security and Priva-cy in Computing and Communications (TrustCom) (pp. 103-110). IEEE.

[7] Zhang, Y., Liu, Y., & Wang, J. (2019). Blockchain Technology and Security: A Survey. IEEE Access, 7, 132799-132815.

[8] Conti, M., De Cristofaro, E., & Jajodia, S. (2018). Surveying Blockchain Security: A Comprehensive Review of Cryptocurrencies Attacks. IEEE Communications Surveys & Tutorials, 20(4), 2816-2842.

[9] Kshetri, N. (2018). Blockchain's Roles in Meeting Key Supply Chain Management Objectives. International Journal of Information Management, 39, 80-89.

[10] Emerging Topics in Blockchain Security and Privacy. (2023). Cryptography, Special Issue. doi: 10.3390/cryptography7020032.

[11] Wang, W. Y., & Zhou, H. (2020). Blockchain, Bank Credit and SME Financing. Journal of Financial Services Research, 57(1), 1-25.

[12] Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on the security of blockchain systems. Future Generation Computer Systems, 107, 841-853.

[13] Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., & Yang, C. (2018). The blockchain as a decentralized security framework [future directions]. IEEE Consumer Electronics Magazine, 7(2), 18-21.

[14] Casino, F., Kanakaris, V., Dasaklis, T. K., Moschuris, S., & Rachaniotis, N. P. (2021). Modeling Food Supply Chain Traceability Based on Blockchain Technology. IFAC-PapersOnLine, 54(13), 252-257.

[15] Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K.-K. R. (2018). Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? IEEE Cloud Computing, 5(1), 31-37.

[16] Morkunas, V. J., Paschen, J., & Boon, E. (2019). How Blockchain Technologies Impact Your Business Model. Business Horizons, 62(3), 295-306.