ISSN 1533-9211

DOI: 10.5281/zenodo.10209791

# AN OVERVIEW OF BLOCK-CHAIN TECHNOLOGY AND RELATED SECURITY ATTACKS: SYSTEMATIC LITERATURE REVIEW

**SELIN UZELALTINBULAT**

Faculty of Engineering and Architecture, World Peace University, Nicosia, TRNC.
Email: selin.kocyigit@wpu.edu.tr

**Dr. SAHAR EBADINEZHAD***

Assistant Professor, Department of Computer Information Systems, Near East University, Nicosia, North Cyprus. Computer Information Systems Research and Technology Center (Cisrtc), Near East University, Nicosia, North Cyprus. *Corresponding Author Email: sahar.ebadinezhad@neu.edu.tr, ORCID: https://orcid.org/0000-0001-9782-4820

### Abstract

Blockchain technology, a transformative innovation with diverse applications, raises concerns about the security and integrity of its networks. This article provides a comprehensive review, introducing blockchain concepts such as consensus algorithms, distributed ledgers, and cryptographic methods. Understanding these fundamentals is crucial for grasping the operational and security aspects of blockchain systems. The research delves into real-world applications across industries like energy, supply chain, healthcare, and banking, examining both benefits and challenges. Additionally, this study addresses cyberattacks on blockchain networks, identifying and analyzing prevalent types like double spending, Sybil attacks, 51% assaults, and smart contract vulnerabilities. The findings enable the design of robust security measures to safeguard blockchain networks.

**Keywords**: Blockchain Technology, Security Attacks, Cryptocurrency, Cybersecurity, Cryptographic Techniques, Privacy in Blockchain.

## 1. INTRODUCTION

There is no denying that blockchain technology is becoming more and more popular. It has had a significant impact on the world beyond just gaining popularity. Blockchain is a distributed, decentralized system for logging and tracking online activity (Khalil et al., 2022). In addition to facilitating bitcoin transactions, the blockchain has the potential to empower the development of decentralized applications without intermediaries and serve as the foundation for integral components of internet security infrastructures (Taylor et al., 2020). There are three distinct types of blockchain: public, private, and consortium, as identified in studies by Mohanta et al. (2019) and Islam (2023). The blockchain exhibits essential characteristics, including decentralization, immutability, traceability, and autonomy, as noted by Chen et al. (2022). The blockchain technology comprises of consensus algorithm, smart contract, cryptography for blockchain (Guo, and Yu, 2022). Internet of Things (IoT), data storage and sharing, network security, protection of private user data, and improving the usability and dependability of the World Wide Web are just a few examples of domains where blockchain applications with a security focus can be found (Taylor et al., 2020). Blockchain technology are susceptible to various risks and attacks, which includes double spending, privacy breaches, vulnerabilities in private key security, mining attacks, and balanced attacks, 51% vulnerability attack, transaction privacy leakage, DAO attack, BGP hijacking attack, Sybil attack ((Mohanta et al., 2019; Singh et al., 2021). By conducting a systematic literature, this study aim to provide a comprehensive understanding of the fundamental principles, applications, and security challenges associated with blockchain technology. In order to carry out this function 3 research questions has been formulated. To address these research questions, the systematic literature review explores relevant research papers, published within 2018-2023. This ensures that the results of this study is based on the most recent advancements and insights in the field of blockchain technology and security.

By combining current research, detecting developing patterns, and pointing out potential research areas, the results of this review will add to the body of existing knowledge. In the end, this research intends to improve our comprehension of blockchain technology and enable the creation of future blockchain systems that are more reliable and secure.In this context, we proposed three research questions as follow:

RQ1: What are the fundamental principles and components of blockchain technology?

RQ2: What are the applications of blockchain?

RQ3: What are the most common types of cyber-attacks targeting blockchain networks?

## 2. LITERATURE REVIEW

After comparing different types of blockchain, it is further elucidated that blockchain possesses certain characteristics such as the ability to grant read permissions, efficiency, immutability, consensus determination, and process that ultimately leads to decentralization (Vivekanadam, 2020). According to Idrees et al., (2021), blockchain may consist of various additional elements, but the fundamental and essential components that need to be comprehended for gaining a deeper understanding of the technology are block, hash pointer, markle tree, digital signature, transactions, and consensus mechanism.

Puneeth and Parthasarathy (2021) provided an overview of diverse scalability solutions and security-privacy techniques aimed at enhancing the efficiency of blockchain technology. These security-privacy techniques encompass various approaches such as mixing, group signature, homomorphic encryption, attribute-based encryption, secure multi-party encryption, and trusted execution environment.

Abed and Manaa (2020) suggest a blockchain-based secure file approach to safeguard sensitive and personal data from unauthorized access. By utilizing immutable and secure log files, this approach offers evidence of log manipulation and non-repudiation. To assess its efficacy, the researchers conducted experiments by comparing server attacks with and without the implementation of blockchain technology. The findings demonstrate that the adoption of blockchain technology can effectively prevent log file manipulation and enhance the security of sensitive information.

ElMamy et al., (2020) perform a comparative evaluation of the most relevant studies focusing on the utilization of blockchain technology in Industry 4.0. This assessment is based on various factors, including confidentiality, integrity, availability, privacy, and the incorporation of multifactor authentication features. The researchers also propose a classification framework for categorizing the most significant cyber-attacks observed in the past decade, categorized into four classes such as scanning, local to remote, power of root, and denial of service (DoS). The findings of the analysis indicate that the implementation of blockchain technology in the industrial sector can effectively uphold data availability and privacy, while concurrently ensuring data confidentiality and integrity.

Based on the findings of Schlatt et al., (2023), the article offers a thorough research framework and agenda for information systems research on blockchain cyber security, highlighting the reciprocal relationships between users, developers, and attackers of both blockchain applications and infrastructure. Blockchain technology has a wide range of applications. The advantages and difficulties of applying blockchain technology in the healthcare sector are studied by Wenhua et al., (2023), illustrating how the inherent security properties of the blockchain, like as decentralization and cryptography, can preserve patient data privacy and enhance medical operations. They also highlight the security concerns and difficulties associated with implementing blockchain in healthcare, such as the potential for data breaches and the have to adhere to regulatory norms.

## 3. METHODOLOGY

This study was carried out using Kitchenham's (2007) suggested methods for a systematic literature review. A systematic review is a method for locating, assessing, and interpreting all research studies that are relevant to a certain research question or area of interest (Kitchenham, 2007). Three steps of the review process with associated activities are:

a. Making the review plan: To determine whether a review is necessary, the review protocol must be specified, including the search keywords and resources to be used, the inclusion and exclusion criteria, the study selection process, the data extraction plan, and the data synthesis process.

b. Carrying out the review: Locate a sizable number of primary studies that are relevant to the study issue, and learn about the primary studies' caliber, data extraction, discussion, and conclusions.

c. Reporting the evaluation: To construct the report document and write up the review's findings.

### 3.1 Search Logic

The following keywords are considered during searching the databases. “blockchain” OR “blockchain technology” OR “block chain technology” OR “block chain” OR “block chain security” OR “distributed ledger” AND “Cyber security” OR “security” OR “network security” AND “Attacks” OR “risks” OR “cyber-attacks” OR “security attacks” OR “vulnerabilities” OR “threats”

ISSN 1533-9211

DOI: 10.5281/zenodo.10209791

### 3.2 Inclusion and exclusion criteria

The studies that satisfied the requirements were chosen after several criteria were taken into consideration when choosing acceptable studies for this research. This is depicted in Table 1. Therefore, the following points are the prerequisites for inclusion are.

a. The search is limited to research released between 2018 and 2023.

b. Only papers from international conferences and journal publications were included.

c. Omitted articles that had not yet been released.

d. Incorporated papers that were authored exclusively in English.

e. Searched for pertinent studies based on abstract, title, and keywords.

f. Studies that do not thoroughly explain the keywords chosen for this research were disregarded.

**Table 1: Inclusion and exclusion criteria**

| Inclusion criteria | Exclusion criteria |
|---|---|
| Already published articles | Articles not in English Language |
| Open access available online | Not open access articles |
| Research articles and conference papers | Not research articles |
| English language only | Studies that do not match the keywords |
| Peer-reviewed Journal articles | Duplicate articles within the databases |

### 3.3 Selection process

During the study selection process, the most appropriate reporting method was utilized. The criteria for the PRISMA as illustrated in Figure 1, were established to simplify and facilitate the selection process of acquiring results from databases. The first search through the two databases generated a total of 8,958 results. After the inclusion and exclusion criteria were defined, a total of eighteen papers that were judged relevant to the study's scope were found. These articles were chosen because they answered the research questions posed in this study and were pertinent to the subject. These articles were distributed from reliable sources, such as Science Direct (with 8 papers) and the Institute of Electrical and Electronics Engineers (IEEE), which had 10 papers.

### 3.4 Quality assessment

To raise the overall rating of the planned publication study, the researchers carefully analyzed the assessment rules. The researchers closely monitored the allocation of tasks, planning process, and methodology review to ensure that only high-quality papers were selected for the study. They also considered the research questions and purpose during the inclusion and exclusion selection phase.

ISSN 1533-9211

DOI: 10.5281/zenodo.10209791

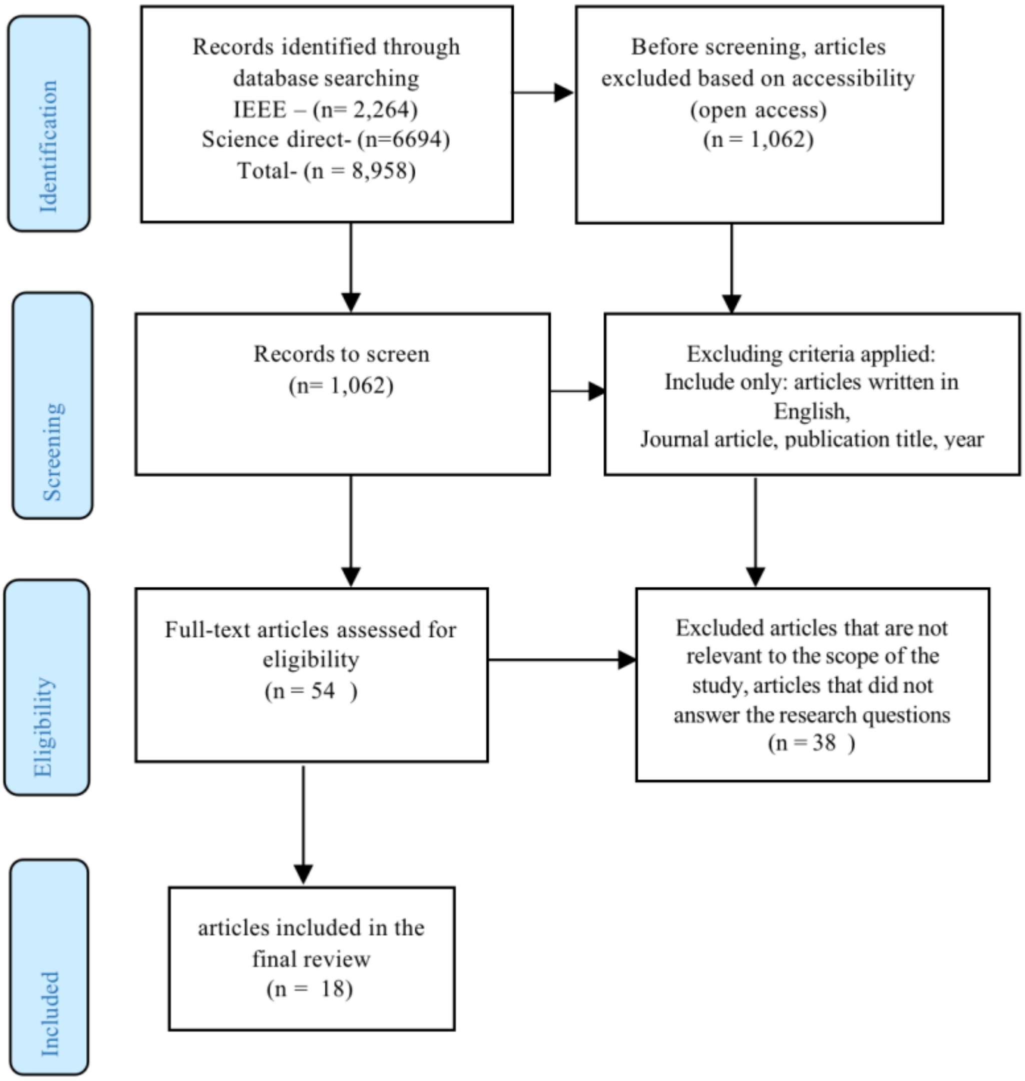
Identification
Records identified through database searching
IEEE – (n= 2,264)
Science direct- (n=6694)
Total- (n = 8,958)
Before screening, articles excluded based on accessibility (open access)
(n = 1,062)
Screening
Records to screen
(n= 1,062)
Excluding criteria applied:
Include only: articles written in English,
Journal article, publication title, year
Eligibility
Full-text articles assessed for eligibility
(n = 54 )
Excluded articles that are not relevant to the scope of the study, articles that did not answer the research questions
(n = 38 )
Included
articles included in the final review
(n = 18)

**Figure 1: PRISMA flow diagram of the article selection process**

## 4. RESULTS

### 4.1 RQ1: what are the fundamental principles and components of blockchain technology

Blockchain is an innovative method of handling and securing transactions through a decentralized database system. It ensures that transactions are validated and protected against unauthorized changes while maintaining consistency among a large group of participants referred to as nodes (Ali et al., 2021). Blockchain is a comprehensive technical system that consists of several different components rather than simply one technology. Distributed data storage, point-to-point communication, consensus techniques, and encryption algorithms are some of these elements. Blockchain builds a comprehensive foundation for safe and

The Seybold REPORT
ISSN 1533-9211
DOI: 10.5281/zenodo.10209791

decentralized transactions by combining these components (Vance, & Vance, 2019). Blockchain stores and verifies data using block-chain data structures. It uses decentralized methods for data generation and updating, utilizing distributed consensus techniques. Blockchain uses cryptography technology to guarantee data transfer and access security. Furthermore, it uses smart contracts—automated script codes—to program and carry out actions on the data. Blockchain is a strong and secure information management and processing system that is created by merging these different components (Li et al., 2021).

A "chain" of data is formed by connecting links between blocks in a distributed data structure called the blockchain. Each block has a timestamp. Blockchain is extremely resistant to block revisions and tampering due to its fundamental nature. This guarantees the data stored on the blockchain's immutability and integrity (Kim et al., 2022).

Public, private, and consortium blockchains are the three varieties (Mohanta et al., 2019; Ali et al., 2021; Lee & Kim, 2021; Islam, 2023). In a Public Blockchain, the ledger is accessible to the public, allowing anyone on the internet to verify and contribute a block of transactions. Private Blockchains, on the other hand, permit only specific individuals within an organization to verify and add transaction blocks, while still allowing general internet users to view the ledger. In Consortium Blockchains, verification and transaction addition are limited to a group of organizations, such as banks, with the option of either keeping the ledger open or restricting access to a select group.

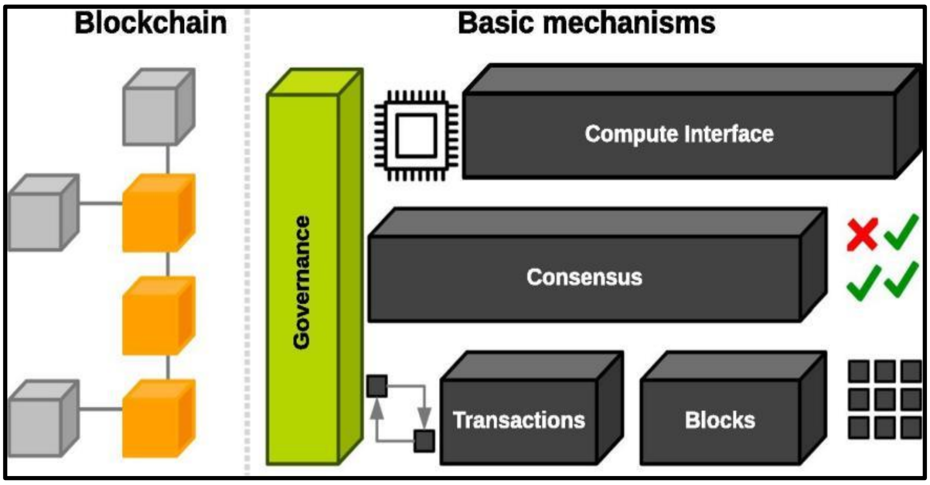

**Figure 2: Structure and Components that Constitute a Blockchain Network (Casino et al., 2019).**

### 4.1.1 Characteristics of Blockchain

Blockchain has several characteristics like decentralization, tamper proof, traceability, autonomy, (Chen et al., 2022), de-trusting, openness and transparency, (Li et al., 2021), non-repudiation, and anonymity (Huo et al., 2022).

These characteristics are explained as follows.

A. Decentralized: In contrast to the centralized data management of usual apps, the blockchain enables several nodes to charge accounting, and it employs the consensus method to ensure consistency among the nodes. It prevents the involvement of outside credit agencies and the invasion of a data center. Additionally, it considerably reduces the resource waste caused by the plausibility of a transaction (Chen et al., 2022).

B. Tamper Proof: The information stored in the blockchain is hard to alter since each block contains the hash of the one before it and is structured in the form of unique structures like hash chains. As tampering with the data in any block will change its hash value and cause it to be disconnected from the blockchain, this assures irreversibility and immutability (Alladi et al., 2022).

C. Traceability: Blockchain incorporates the most recent transaction consensus result when establishing a new block and combines it with the hash value of the previous block to form a blockchain data structure. As a result, we swiftly track down any pertinent historical transaction data going back to the block time when examining a certain condition (Chen et al., 2022).

D. Autonomy: Blockchain facilitates the exchange, recording, and updating of data among all nodes in the network within a trustworthy environment. This is achieved through the utilization of consensus-based specifications and protocols. By leveraging these mechanisms, blockchain ensures the accuracy and authenticity of every transaction recorded on the blockchain, eliminating the need for human intervention. This enhances the reliability and integrity of the data stored on the blockchain (Chen et al., 2022).

E. De-trusting: The blockchain system establishes trust by employing cryptography, verification processes, and various other methods. This trust allows all nodes to engage in secure transactions without the need for third-party assurances or guarantees (Li et al., 2021).

F. Openness and transparency: Within a brief timeframe, the block is replicated across all nodes in the cluster, ensuring data synchronization throughout the network. Furthermore, each node has the ability to trace and access comprehensive transaction history (Li et al., 2021).

G. Non-repudiation: Every node upholds the ledger, and the consensus mechanism is supported by resilient correlation structure and cooperative group activities. This ensures data consistency and significantly minimizes the possibility of tampering, making the data verifiable and traceable. This characteristic simplifies the establishment of endorsements during data sharing and enables seamless integration with multiple centralized services. Consequently, it enhances overall efficiency and reduces costs (Huo et al., 2022).

The Seybold REPORT

ISSN 1533-9211

DOI: 10.5281/zenodo.10209791

### 4.1.2 Blockchain Technologies

Blockchain technology acts as an unchangeable distributed ledger that stores transactions in a sequential chain of blocks. These blocks are connected through hash values, forming a chronological record of transactions (Huo et al., 2022). In the whitepaper outlining the fundamentals of Bitcoin, S. Nakamoto first introduced the idea of blockchain, but it is now being used in a variety of industries, including finance, unmanned aerial vehicles (UAVs), the Internet of Things (IoT), smart cities, smart grids, supply chain management, and vehicular ad hoc networks (VANETs). Its potential applications in these domains are increasingly recognized due to the unique characteristics of blockchain, such as decentralization, transparency, security, and immutability (Alladi et al., 2022). The blockchain technology comprises of consensus algorithm, smart contract, cryptography for blockchain (Guo, and Yu, 2022).

A. *Consensus algorithm*: These consensus algorithms leverage the shared interest of the majority of blockchain users in maintaining the integrity of the blockchain. By employing a consensus algorithm, a blockchain system establishes trust and securely stores transactions within blocks. Consequently, consensus algorithms can be seen as the crucial component that drives all transactions within blockchain networks. The inclusion of smart contracts adds another valuable dimension to blockchain technology. It goes beyond merely providing a decentralized and immutable record of various events. *Smart contract:* Smart contracts enable the creation of objective computer code that precisely defines the management of processes and specifies the actions to be taken when specific events take place. This feature enhances the reliability and precision of blockchain-based operations. *Cryptography for*

B. *Blockchain:* Blockchain establishes a trust layer that facilitates secure and reliable records and transactions among parties who may not trust each other initially. This trust layer ensures the integrity and authenticity of the information exchanged, allowing for a secure environment for interactions to take place.

   It is important to understand the overall layered technical framework of the blockchain technology as illustrated in Figure 3. The frameowrk includes application layer, control layer, consensus layer, data layer and network layer.

C. *Network layer:* The network layer plays a crucial role in facilitating the transfer of data (Wen et al., 2021). Zig Bee, Wi-Fi, Bluetooth, and 3 G are examples of data transfer technologies (Thabit et al., 2023).

D. *Data layer*: The data layer encompasses elements such as the data structure, data model, and block storage. This foundational layer forms an essential part of the blockchain architecture, serving as a distributed ledger responsible for storing transaction or account information (Li et al., 2021).

E. *Consensus layer:* Every node within the blockchain network is required to uphold an identical ledger. However, since nodes generate data at different intervals and the data

ISSN 1533-9211

DOI: 10.5281/zenodo.10209791

source is unknown, there exists a potential for intentional dissemination of incorrect data by a node. Such actions can give rise to security vulnerabilities like Sybil Attacks and Double-Spending Attacks (Huo et al., 2022). Therefore, the layer of consensus incorporates a range of consensus mechanisms that determine the selection of the entity authorized to assemble the subsequent block (Wen et al., 2021).

F. *Control layer:* The control layer serves as the central hub where different applications and the ledger interact. It encompasses components such as the processing model, control contract, and execution environment (Huo et al., 2022).

G. *Applicattion layer:* The application layer encompasses a wide range of application scenarios, including programmable currency, programmable finance, and programmable society (Wen et al., 2021). Users can access various applications defined within the application layer by utilizing the standard interface offered by the application layer (Li et al., 2021).

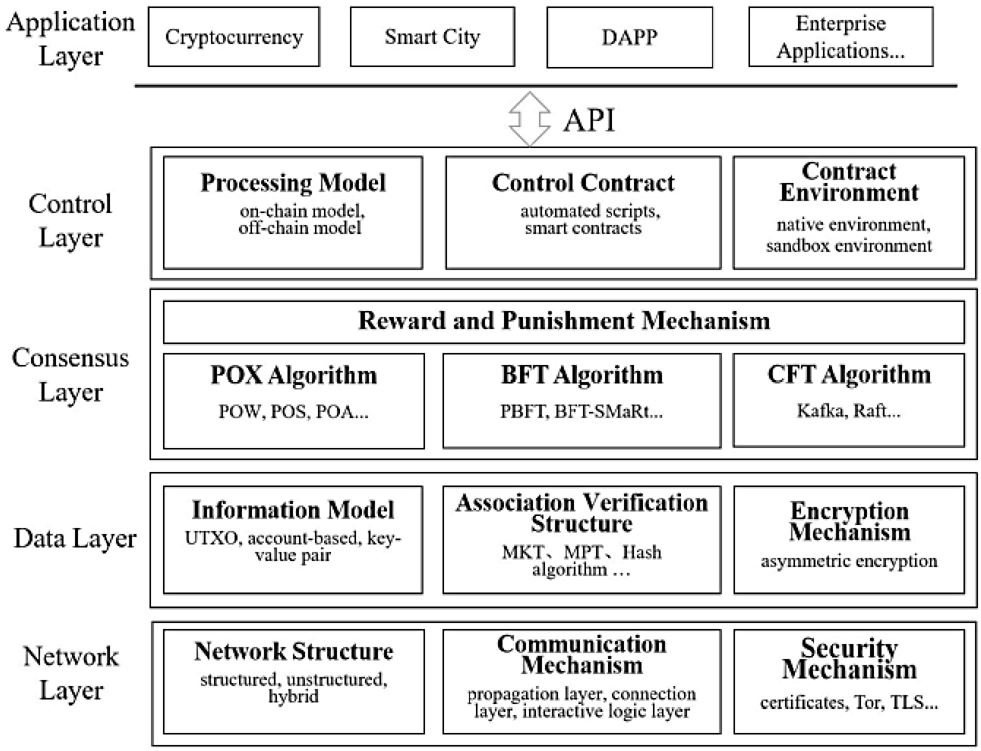
Application Layer
Cryptocurrency
Smart City
DAPP
Enterprise Applications...
API
Control Layer
Processing Model
on-chain model, off-chain model
Control Contract
automated scripts, smart contracts
Contract Environment
native environment, sandbox environment
Consensus Layer
Reward and Punishment Mechanism
POX Algorithm
POW, POS, POA...
BFT Algorithm
PBFT, BFT-SMaRt...
CFT Algorithm
Kafka, Raft...
Data Layer
Information Model
UTXO, account-based, key-value pair
Association Verification Structure
MKT、MPT、Hash algorithm ...
Encryption Mechanism
asymmetric encryption
Network Layer
Network Structure
structured, unstructured, hybrid
Communication Mechanism
propagation layer, connection layer, interactive logic layer
Security Mechanism
certificates, Tor, TLS...

**Figure 3: The Overall Layered Technical Framework of Blockchain Technology (Huo et al., 2022).**

## 4.2 RQ2: What are the applications of blockchain

The foundational idea of Blockchain technology originated from the Bitcoin cryptocurrency, and subsequently, this concept has been adopted in various domains (Mohanta et al., 2019). Applications of blockchain span across finance, IoT and edge computing, society services (Li et al., 2021), healthcare, integrity verification (provenance and counterfeit, insurance, and intellectual property), governance, privacy and management, business and industrial applications (supply chain management), education, data management (Casino et al., 2019), manufacturing sector (Ali et al., 2021), power grid, transport system, commercial world, cloud computing, reputation (Mohanta et al., 2019). An overview of the blockchain applications are represented in Figure 4.

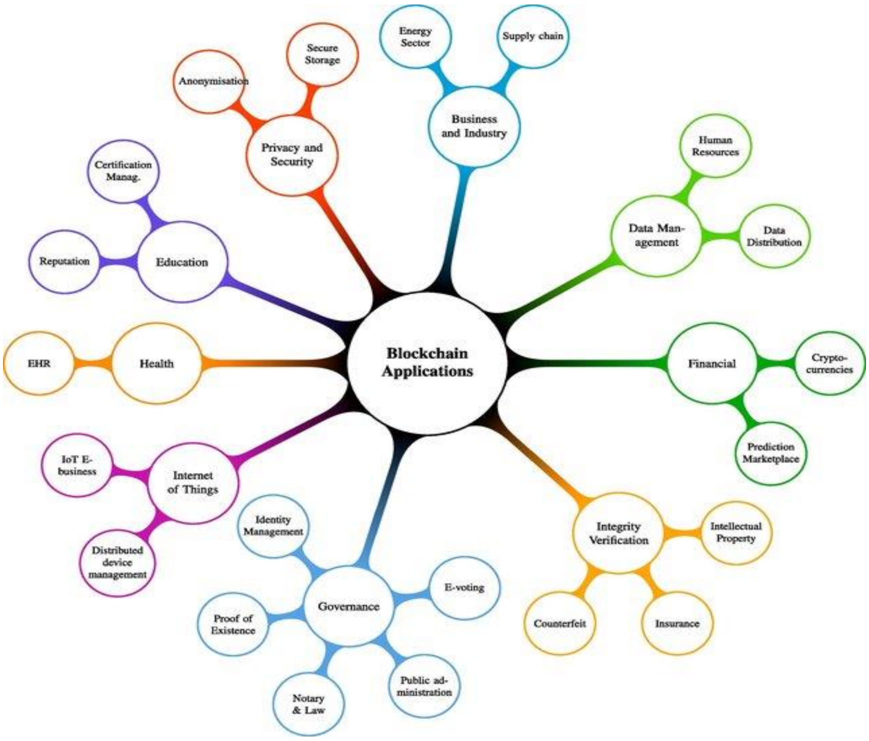

**Figure 4: Blockchain Applications (Casino et al., 2019).**

Blockchain applications with a security focus encompass areas such as Internet of Things (IoT), data storage and sharing, network security, protection of private user data, and enhancing the functionality and reliability of the World Wide Web (Taylor et al., 2020).

A. *IoT:* In the context of IoT, blockchain technology is utilized for authenticating devices connecting to the network, verifying end users accessing the devices, securely deploying firmware updates through peer-to-peer distribution, and implementing measures to detect threats and prevent malware.

B. *Data storage and sharing:* The objective is to guarantee the integrity of cloud-stored data, making it impervious to unauthorized modifications. This is accomplished through the utilization of hash lists, which enable secure storage and retrieval of data. Additionally, data exchanges are subjected to verification, ensuring consistency from the moment of dispatch to receipt.

C. *Network security:* In the context of network security, blockchain technology offers a decentralized and resilient method for storing crucial authentication data in light of the growing adoption of virtualized machines, software-defined networks, and containerized application deployment.

D. *Protection of private user data:* The safeguarding of private user data encompasses aspects such as preserving end user settings for wearable Bluetooth devices and ensuring the security of personally identifiable information shared with external parties.

E. *In terms of navigating and utilizing the World Wide Web*: Blockchain technology aims to validate the legitimacy of wireless Internet access points connected to a reference point. It also facilitates accurate DNS record management for precise web page navigation. Additionally, blockchain ensures secure usage of web applications and enables communication with others through encrypted and safe methods.

### 4.3 RQ3: What are the most common types of cyber-attacks targeting blockchain networks

While blockchain has made significant innovative strides, studies suggest that the technology still harbors security vulnerabilities. Although blockchain applications offer a robust approach to securing networked ledgers, it is important to note that the technology alone does not assure the security of individual participants or negate the necessity of implementing additional cyber security best practices (Vance, & Vance, 2019). These challenges pertain to cybersecurity concerns and threats, finding a balance between security and performance, as well as managing cryptographic keys and ensuring their effectiveness. As an example, robust security measures that effectively defend against governance attacks, such as 51% attacks, denial of service (DoS) attacks, sabotage through misleading actions, and strategies resembling the prisoner's dilemma, have either not been sufficiently developed or have not gained widespread adoption within open-source blockchains to undergo rigorous testing (Ali et al., 2021). Different applications of Blockchain technology are susceptible to various risks and attacks, including but not limited to double spending, privacy breaches, vulnerabilities in private key security, mining attacks, and balanced attacks (Mohanta et al., 2019), 51% vulnerability attack, transaction privacy leakage, DAO attack, BGP hijacking attack, Sybil attack (Singh et al., 2021).

A. *Double spending attack*: This issue arises when a successful transaction is replicated with identical funds, creating a potential weakness in digital currency systems, as the same digital token can be spent twice during such an attack. Despite the validation of all transactions by the blockchain's consensus mechanism, preventing double-spending entirely remains impossible. Attacks associated with double spending encompass various types such as race attacks, Finney attacks, 51% attacks, and Vector 76 attacks (singh et al., 2021).

B. *Sybil attack:* By executing a Sybil attack, the perpetrator can manipulate a blockchain system by launching a variety of threats to gain advantages. These threats may include attacks such as compromising the consensus protocol, generating fraudulent transactions, manipulating the reputation of nodes, and hijacking honest nodes, thereby causing the network to split into multiple disjointed groups (Iqbal & Matulevičius, 2021)

ISSN 1533-9211

DOI: 10.5281/zenodo.10209791

C. *51% vulnerability attack:* Li et al., (2020) stated that the distributed consensus mechanism plays a vital role in establishing trust within the blockchain. However, this mechanism is susceptible to a 51% vulnerability, which attackers can exploit to gain control over the entire blockchain. Particularly in PoW-based blockchains, if a single miner's hashing power exceeds 50% of the total hashing power, a 51% attack becomes possible. Consequently, concerns arise when mining power becomes concentrated in a few mining pools, leading to the potential scenario where a single pool controls more than half of the computing power. This vulnerability can be exploited by attackers to execute several types of attacks, including: -Reversing transactions and initiating double spending attacks (spending the same coins multiple times), -Manipulating the order and exclusion of transactions, -Disrupting the normal mining operations of other miners, -Obstructing the confirmation process of regular transactions. The 51% vulnerability attack is shown in Figure 5.

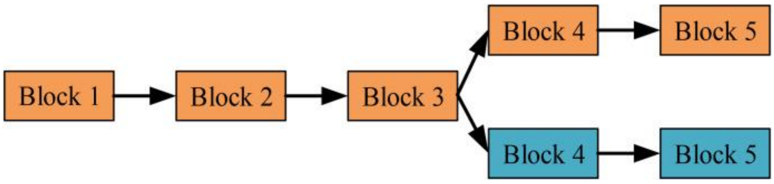

**Figure 5: 51% vulnerability attack in blockchain (Chen et al., 2023).**

D. *BGP hijacking attacks:* BGP hijacking attacks are classified as external routing protocol attacks that occur within the interconnected networks of the Internet. These attacks involve a malicious Autonomous System (AS) creating deceptive advertisements for specific network prefixes and broadcasting them to neighboring ASs. Consequently, the traffic intended for those destinations is redirected, granting control to the attackers and potentially disrupting the consensus mechanism. Furthermore, the attackers can manipulate information, such as transactions, within the network. By exploiting BGP hijacking attacks, the blockchain network can be fragmented into multiple independent networks that are unable to communicate with each other. This situation leads to the formation of parallel chains within the blockchain. Attackers can conduct transactions on these parallel forks, but ultimately, the longest chain will prevail while the transactions on the other forks will be discarded once the attack ceases (Wen et al., 2021). The blockchain security risks are categorized as network attacks, endpoint security, international misuse, code vulnerabilities, data protection, and human negligence (Guo & Yu, 2022).

## 5. DISCUSSION

The discussion section of this article presents a comprehensive analysis of the research questions posed in this systematic literature review on blockchain technology and related security attacks.

### 5.1 Fundamental Principles and Components of Blockchain Technology

The findings reveal that blockchain technology is built on several fundamental principles and components. The distributed ledger, which ensures data transparency and immutability, is a key component. Consensus algorithms are essential for building participant confidence and preserving the blockchain's integrity. Digital signatures and hashing are two examples of cryptographic algorithms that offer data protection and authentication. Self-executing and programmable transactions are made possible by smart contracts. Together, these tenets and elements support blockchain technology's decentralized and secure structure.

### 5.2 Applications of Blockchain

The report demonstrates how blockchain technology can be applied in a multitude of industries. Blockchain has the power to completely transform identity verification, cross-border transactions, and payment systems in the financial industry. Blockchain technology can help supply chain management by offering transparent, traceable records that guarantee product authenticity and lower fraud. Voting systems, decentralized energy grids, healthcare data management, and intellectual property rights management are a few other noteworthy applications. According to studies, there is continuous investigation into a wide range of fields on the possible applications of blockchain technology.

### 5.3 Common Types of Cyber Attacks Targeting Blockchain Networks

Several frequent categories of cyberattacks that target blockchain networks are identified by this systematic review. These include 51% attacks, in which a single entity gains majority control of the network's computational power; Sybil attacks, in which an attacker creates multiple fake identities to control the network; double spending, in which a user tries to spend the same digital asset more than once; and vulnerabilities in smart contracts, which can be used to carry out malicious or unauthorized actions. These attacks emphasize how critical it is to comprehend and manage the security concerns related to blockchain technology.

## 6. CONCLUSION

Finally, a thorough overview of blockchain technology and associated security threats is given by this systematic literature study. The decentralized, transparent, and safe nature of blockchain technology is revealed through an examination of its core ideas and constituent parts. The paper also looks at the various uses of blockchain technology, showing how it can revolutionize several sectors, including supply chain management, healthcare, and banking. In addition, the recognition and analysis of prevalent forms of cyberattacks directed at blockchain networks illuminated the susceptibilities and hazards linked to this technology. To counter these risks and safeguard the integrity of blockchain networks, it highlights the necessity of implementing strong security measures.

This comprehensive analysis of the literature adds to the body of knowledge already in existence by compiling and interpreting research results on blockchain technology and associated security threats. For scholars, professionals, and decision-makers looking for a thorough grasp of blockchain technology and the related security environment, it offers insightful information. This analysis lays the groundwork for future investigations and developments in blockchain security by answering the research questions and providing an overview of the major discoveries.

ISSN 1533-9211

DOI: 10.5281/zenodo.10209791

**Disclosure Statement:** The authors report there are no competing interests to declare.

**Data Availability Statement:** there is no data set associated with this paper.

**References**

1) Abed, F. N., & Manaa, M. E. (2020). A proactive secure file approach using a block chain technique. Journal of Discrete Mathematical Sciences and Cryptography, 23(6), 1235-1242. doi: 10.1080/09720529.2020.1727610

2) Ali, O., Jaradat, A., Kulakli, A., & Abuhalimeh, A. (2021). A comparative study: Blockchain technology utilization benefits, challenges and functionalities. *Ieee Access*, *9*, 12730-12749. DOI: 10.1109/ACCESS.2021.3050241

3) Alladi, T., Chamola, V., Sahu, N., Venkatesh, V., Goyal, A., & Guizani, M. (2022). A comprehensive survey on the applications of blockchain for securing vehicular networks. *IEEE Communications Surveys & Tutorials*. DOI: 10.1109/COMST.2022.3160925

4) Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and informatics*, *36*, 55-81. DOI: https://doi.org/10.1016/j.tele.2018.11.006

5) Chen, Y., Chen, H., Zhang, Y., Han, M., Siddula, M., & Cai, Z. (2022). A survey on blockchain systems: Attacks, defenses, and privacy preservation. *High-Confidence Computing*, *2*(2), 100048. https://doi.org/10.1016/j.hcc.2021.100048

6) ElMamy, S. B., Mrabet, H., Gharbi, H., Jemai, A., & Trentesaux, D. (2020). A Survey on the Usage of Blockchain Technology for Cyber-Threats in the Context of Industry 4.0. Applied Sciences, 10(21), 7545. https://doi.org/10.3390/app10217545

7) Guo, H., & Yu, X. (2022). A Survey on Blockchain Technology and its security. *Blockchain: research and applications*, *3*(2), 100067. https://doi.org/10.1016/j.bcra.2022.100067

8) Huo, R., Zeng, S., Wang, Z., Shang, J., Chen, W., Huang, T., ... & Liu, Y. (2022). A comprehensive survey on blockchain in industrial internet of things: Motivations, research progresses, and future challenges. *IEEE Communications Surveys & Tutorials*, *24*(1), 88-122.

9) Idrees, S. M., Nowostawski, M., Jameel, R., & Mourya, A. K. (2021). Security aspects of blockchain technology intended for industrial applications. *Electronics*, *10*(8), 951. **https://doi.org/10.3390/electronics10080951**

10) Iqbal, M., & Matulevičius, R. (2021). Exploring sybil and double-spending risks in blockchain systems. *IEEE Access*, *9*, 76153-76177.

11) Islam, M. D. (2023). A survey on the use of blockchains to achieve supply chain security. Information Systems, 102232. DOI: https://doi.org/10.1016/j.is.2023.102232
Chen, H., Luo, X., Shi, L., Cao, Y., & Zhang, Y. (2023). Security challenges and defense approaches for blockchain-based services from a full-stack architecture perspective. Blockchain: Research and Applications, 100135. https://doi.org/10.1016/j.bcra.2023.100135

12) Khalil, A. A., Franco, J., Parvez, I., Uluagac, S., Shahriar, H., & Rahman, M. A. (2022, June). A literature review on blockchain-enabled security and operation of cyber-physical systems. In *2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)* (pp. 1774-1779). IEEE.

13) Kim, T., Ochoa, J., Faika, T., Mantooth, A.H., Di, J., Li, Q., Lee, Y. (2022). An Overview of Cyber-Physical Security of Battery Management Systems and Adoption of Blockchain Technology, *IEEE Journal of Emerging and Selected Topics in Power Electronics*, *10*(1), 1270-1281, doi: 10.1109/JESTPE.2020.2968490.

The Seybold REPORT

ISSN 1533-9211

DOI: 10.5281/zenodo.10209791

14) Kitchenham, B. (2007). Guidelines for performing systematic literature reviews in software engineering. *Version 2.3 EBSE technical report. EBSE-2007-01.*

15) Lee, S., & Kim, S. (2021). Blockchain as a cyber defense: opportunities, applications, and challenges. *IEEE Access*, *10*, 2602-2618. DOI: 10.1109/ACCESS.2021.3136328

16) Li, W., He, M., & Haiquan, S. (2021, June). 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)* (pp. 31-39). IEEE. DOI: 10.1109/ICEIEC51955.2021.9463842

17) 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. http://dx.doi.org/10.1016/j.future.2017.08.020

18) Mohanta, B. K., Jena, D., Panda, S. S., & Sobhanayak, S. (2019). Blockchain technology: A survey on applications and security privacy challenges. *Internet of Things*, *8*, 100107. https://doi.org/10.1016/j.iot.2019.100107

19) Puneeth, R.P., & Parthasarathy, G. (2021). A Comprehensive Survey on Privacy-Security and Scalability Solutions for Block Chain Technology. In Smart Intelligent Computing and Communication Technology, (pp. 173–178). IOS Press. https://doi.org/10.3233/APC210031

20) Schlatt, V., Guggenberger, T., Schmid, J., & Urbach, N. (2023). Attacking the trust machine: Developing an information systems research agenda for blockchain cybersecurity. *International journal of information management*, *68*, 102470. https://doi.org/10.1016/j.ijinfomgt.2022.102470

21) Singh, S., Hosen, A. S., & Yoon, B. (2021). Blockchain security attacks, challenges, and solutions for the future distributed iot network. *IEEE Access*, *9*, 13938-13959. DOI: 10.1109/ACCESS.2021.3051602

22) Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K. K. R. (2020). A systematic literature review of blockchain cyber security. *Digital Communications and Networks*, *6*(2), 147-156. https://doi.org/10.1016/j.dcan.2019.01.005

23) Thabit, F., Can, O., Aljahdali, A. O., Al-Gaphari, G. H., & Alkhzaimi, H. A. (2023). A Comprehensive Literature Survey of Cryptography Algorithms for Improving the IoT Security. Internet of Things, 100759. https://doi.org/10.1016/j.iot.2023.100759

24) Vance, T. R., & Vance, A. (2019, October). Cybersecurity in the blockchain era: a survey on examining critical infrastructure protection with blockchain-based technology. In *2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)* (pp. 107-112). IEEE. doi: 10.1109/PICST47496.2019.9061242.

25) Vivekanadam, B. (2020). Analysis of Recent Trend and Applications in Block Chain Technology. *Journal of ISMAC, 2*(4), 200-206. https://doi.org/10.36548/jismac.2020.4.003

26) Wen, Y., Lu, F., Liu, Y., & Huang, X. (2021). Attacks and countermeasures on blockchains: A survey from layering perspective. *Computer Networks*, *191*, 107978. https://doi.org/10.1016/j.comnet.2021.107978

27) Wenhua, Z., Qamar, F., Abdali, T. A. N., Hassan, R., Jafri, S. T. A., & Nguyen, Q. N. (2023). Blockchain Technology: Security Issues, Healthcare Applications, Challenges and Future Trends. *Electronics*, *12*(3), 546. **https://doi.org/10.3390/electronics12030546**