Journal of Distributed Computing and Systems(JDCS)
Vol.6, Issue 2, 2024, Pages 39-52

Blockchain Security: A Comparative Analysis of Threats and Countermeasures

Ehsan Abedini*, Amir Jalaly Bigly, Mohsen Nickray
Department of Computer Engineering, University of Qom, Qom, Iran

Article History:
Received: January 01, 2024
Received in revised form: March 01, 2024
Accepted: March 15, 2024
Available online: March 20, 2024

Abstract

Blockchain technology, as one of the transformative innovations of the last decade, has garnered significant attention across diverse domains such as financial services, healthcare, supply chain management, energy, the Internet of Things (IoT), and smart contracts. Characterized by key features such as transparency, immutability, decentralization, distributed and advanced traceability, blockchain serves as a powerful tool for transforming informational infrastructures and fostering trust among stakeholders. However, alongside these advantages, blockchain faces critical security challenges that threaten its widespread adoption, including data breaches and risks to data integrity. This study examines the structure and architecture of blockchain, identifying major security threats such as DDoS attacks, phishing, majority attacks, Sybil attacks, and other critical vulnerabilities. Additionally, it analyzes existing countermeasures to address these threats, evaluating their strengths, limitations, and areas for improvement. Furthermore, through comparative analysis, this research provides a comprehensive and practical perspective for researchers, developers, and decision-makers to enhance blockchain resilience and applicability.

Keywords: Blockchain, Security, Comparative Analysis, Attacks, Threats.

I. Introduction

Since its introduction by Satoshi Nakamoto in 2008 and the publication of the seminal paper on Bitcoin [1], blockchain technology has emerged as one of the most groundbreaking innovations in the field of information and communication technology. Blockchain, with its unique features—decentralization [2], transparency, immutability, distributed and high trustworthiness—has rapidly attracted the attention of researchers and various technological sectors. It has found extensive applications in areas such as finance, supply chain management, the Internet of Things (IoT) [3], healthcare, and smart contracts. These features have made blockchain an efficient tool for enhancing security and reducing the need for intermediaries in data exchanges.

Security in blockchain is a critical factor influencing its widespread adoption and utilization [4]. Its decentralized structure, reliant on consensus algorithms and advanced cryptographic techniques [3], ensures trust and transaction security without the need for central authorities. However, this reliance on distributed structures also exposes blockchain networks to a wide range of security threats and attacks [5]. Complex attacks, such as 51% attacks, double-spending, and smart contract manipulation, exemplify these threats, potentially undermining user trust and disrupting system functionality.

These threats target not only traditional blockchain structures but also newer architectures such as consortium and private blockchains [6]. Therefore, a comprehensive analysis of blockchain system attacks and their countermeasures is essential for understanding vulnerabilities and developing effective security solutions.

This paper begins with an overview of the fundamental concepts and security features of blockchain, followed by an exploration of known attack types and their respective countermeasures. Finally, through various comparative analyses, it introduces research trends and challenges in the field to outline potential future research directions.

In conducting this study, we have utilized reputable and up-to-date sources. Figure 1 presents the distribution of articles by publication year. Moreover, in selecting references, we have prioritized the use of recent and relevant studies to ensure the accuracy and timeliness of the analysis.

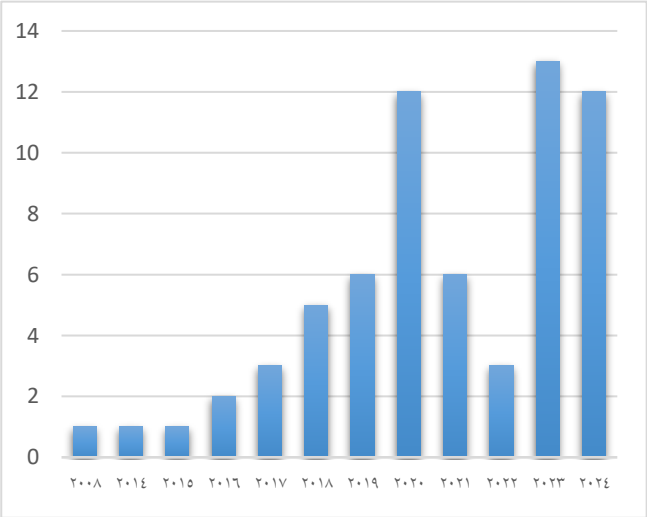

Fig. 1. Distribution of the utilized articles by year of publication

Table 1 also presents the statistics of the referenced articles based on their publishing journals.

* Corresponding Author: Ehsan Abedini (e.abedini@stu.qom.ac.ir)

TABLE I. STATISTICS OF REFERENCES BASED ON THE PUBLISHING JOURNAL

Publisher Name	Number of Articles
IEEExplore	21
ScienceDirect	16
ACM DL	8
MDPI	4
Other Publishers	١٦

II. OVERVIEW OF BLOCKCHAIN TECHNOLOGY

Since its inception, blockchain technology has achieved significant advancements, offering diverse models and mechanisms for various applications. At its core, blockchain is a distributed ledger technology [7] that enables multiple parties to securely and transparently access shared information. Its decentralized nature eliminates the need for a central authority [8] and fosters trust among participants [2].

Blockchain serves as a public, distributed database that maintains an encrypted ledger. Acting as a global system, it allows users worldwide with internet access to benefit from its functionalities [9]. Unlike traditional databases managed by central entities such as banks or governments, blockchain is not owned or controlled by any single individual or organization [10]. Instead, it operates collectively and in a distributed manner, making it exceedingly difficult to forge data, records, or transactions.

The technology stores data permanently across multiple network nodes and maintains it in a decentralized and distributed fashion [11]. Each node retains a local copy of the blockchain, which is regularly updated to ensure synchronization among all network participants [12]. Blockchain functions as a platform for distributed computing and data sharing, enabling untrusted nodes to collectively reach decisions [7].

In centralized systems, a single point of failure poses risks to availability and reliability. In contrast, decentralized systems address this issue by incorporating multiple coordination points. In a distributed architecture, every node contributes to the collective execution of system tasks [13]. The fundamental architecture of blockchain consists of nodes that are interconnected in a distributed network. Each node maintains an up-to-date copy of the blockchain [14], enabling activities such as initiating and validating transactions or performing mining operations [15].

Figure 2 illustrates the decentralized and distributed architecture of blockchain. In this network, no central node exists, and communications are established directly between nodes [16]. Additionally, all nodes are equal, with no node having superiority over others [17].

A. Blockchain Categorization

Blockchain can be categorized into three main types [11]. This classification, along with examples of each type, is illustrated in Figure 3.

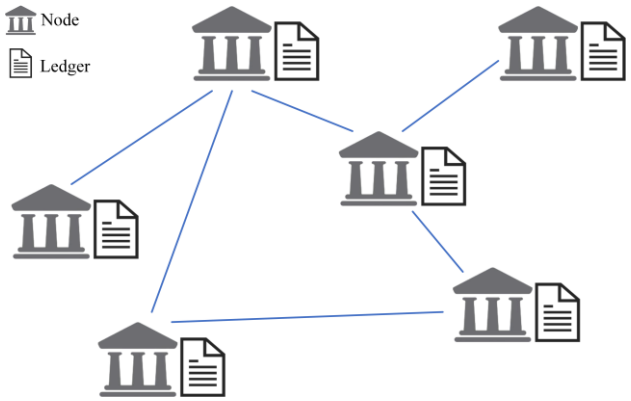

Fig. 2. Decentralized and distributer architecture of blockchain

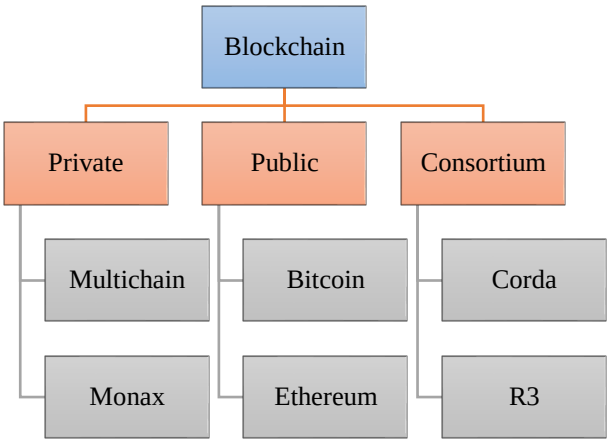

Fig. 3. Blockchain categories and examples

- **Private Blockchains:** These blockchains are restricted to specific participants [6]. Access control mechanisms determine who can join the network and participate in the consensus process [18]. This model is typically used in enterprise applications where privacy and confidentiality are of high importance.
- **Public Blockchains:** These blockchains are open to everyone, allowing anyone to join and participate [11]. They are usually secured through consensus mechanisms like Proof of Work (PoW) or Proof of Stake (PoS), which ensure that transactions are validated and added to the ledger in a trustworthy manner [12].
- **Consortium Blockchains:** This type involves multiple organizations collaborating to maintain a shared ledger [12]. It combines elements of both public and private blockchains, enabling joint governance while preserving some levels of access control [13].

B. Applications of Blockchain

As shown in Figure 4, blockchain technology, with its unique features, has widespread applications across various fields [19]. Below are some of these applications:

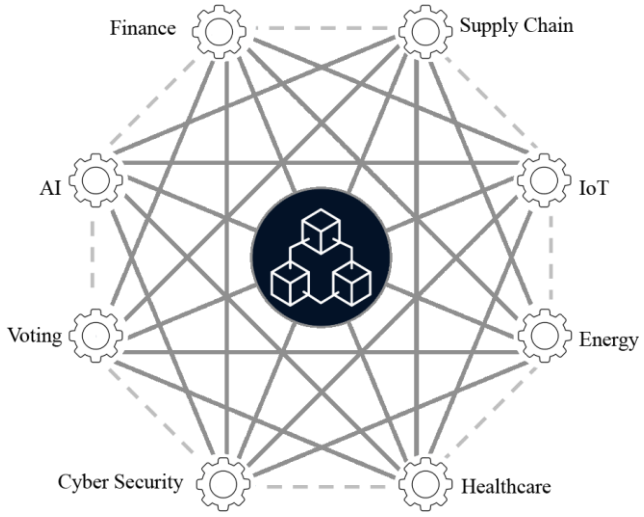

Fig. 4. Applications of blockchain

In the financial, this technology enables peer-to-peer transactions without intermediaries, which helps reduce costs and enhance security [19]. In supply chains, blockchain ensures transparency and accurate tracking of stages, and through the use of smart contracts, payments are made automatically [20]. In electronic voting, blockchain guarantees security and transparency, preventing fraud [21]. Additionally, in healthcare, this technology enables the secure storage of medical records and improves data sharing [16]. In artificial intelligence, blockchain enhances data transparency and security in machine learning and facilitates collaborative learning models [19].

In the energy, blockchain aids in improving the management of energy distribution networks through transparent and immutable data records, enabling the tracking of renewable energy sources and facilitating peer-to-peer energy transactions between consumers. It also increases efficiency in energy markets and reduces operational costs and intermediaries [22]. Furthermore, in cybersecurity, blockchain, with its decentralized structure and strong encryption, prevents cyberattacks and intrusion into sensitive systems, significantly enhancing the security of digital infrastructures. In the Internet of Things (IoT), blockchain enables decentralized management and automation of interactions between devices, contributing to the security and efficiency of networks [3]. These applications demonstrate the high potential of blockchain in enhancing security, transparency, and efficiency across various sectors.

C. Consensus Mechanisms

Consensus mechanisms, the most important of which include PoW and PoS, play a critical role in the security of blockchain networks. These protocols verify the validity of transactions through agreement among nodes and prevent data manipulation [6]. For example, in PoW [23], miners must solve complex mathematical problems, while PoS selects validators based on the amount of stake they hold [7].

Blockchain is recognized as a secure and tamper-resistant technology, but in order to maintain this level of security and withstand new challenges, continuous improvement is necessary. A thorough examination of security challenges and the development of innovative solutions can facilitate the adoption of this technology in various applications. In the next section, we will examine these challenges in detail.

III. TYPES OF ATTACKS AND THREATS IN BLOCKCHAIN

Blockchain, due to its unique characteristics, is considered an innovative solution in the field of information and communication technologies. However, this technology presents numerous security challenges that hinder its widespread adoption in various sectors. These challenges arise from inherent vulnerabilities in its architecture [24], the complexity of applications, and the evolving nature of cyber threats [25]. Understanding these issues is crucial for developing robust solutions to enhance blockchain security. In this section, we will explore the various significant attacks in blockchain and the solutions to mitigate them.

A. Majority Attack

The majority (51%) attack is a significant security threat in blockchain networks, where an attacker or group of attackers gains control of more than 50% of the network's computational power [26]. This allows them to perform malicious actions such as preventing transaction confirmations, executing double-spending attacks, and altering the transaction history. Particularly in networks based on consensus algorithms like PoW, such as Bitcoin, which relies on computational power for security, this attack represents a serious threat [2]. Although executing a 51% attack in large networks with high computational power, like Bitcoin, is difficult and costly due to the high expense of controlling the majority of the network, this threat is significantly greater in smaller networks or those with less distributed computational power. Figure 5 illustrates this attack, where the red blocks (attackers), having control over more than 50% of the network, are capable of launching malicious actions against the blue blocks (honest participants).

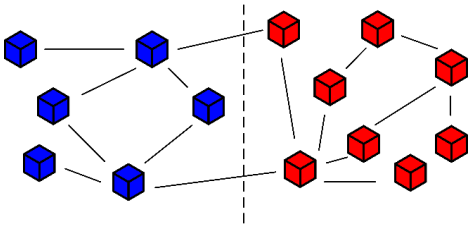

Fig. 5. Majority attack

To counter this attack, the use of enhanced consensus protocols or the transition to PoS algorithms has been suggested, which reduce the need for high computational power and increase the cost of executing such an attack. Also transitioning to consensus algorithms such as hybrid algorithms like Delegated Proof of Stake (DPoS) [27] or Proof of Authority (PoA) [28] can also be employed. In DPoS, network members elect representatives who are responsible for validating transactions. This approach not only reduces the need for high computational power but also significantly increases the cost of executing a 51% attack. Similarly, in PoA, only verified and authorized nodes are permitted to participate in the consensus process, making it

nearly impossible for a malicious entity to take control of the network.

B. Double-Spending Attack

In a double-spending attack, which is one of the common threats in blockchain systems, a digital unit is spent more than once. This attack is especially problematic in decentralized networks that rely on consensus to validate transactions, as it can undermine user trust and disrupt the system's functionality [19]. In this attack, the attacker might make an initial transaction to purchase goods or services, and then manipulate the blockchain's history to spend the same currency in a second transaction.

In high-security networks with decentralized consensus algorithms such as Proof of Work or Proof of Stake, transaction validation is performed in an immutable manner, significantly reducing the likelihood of double-spending attacks [26]. However, in smaller networks or those with less computational power, the risk of such attacks is higher.

To mitigate the risk of Double-Spending attacks, in addition to introducing delays in transaction confirmations [29], multi-stage verification mechanisms [30] can be implemented. For instance, in some networks, transactions are considered valid only after being confirmed by multiple independent nodes (e.g., six confirmations in Bitcoin). Moreover, employing faster consensus algorithms such as Practical Byzantine Fault Tolerance (PBFT) [31] can reduce transaction confirmation times and decrease the likelihood of successful attacks.

C. Sybil Attack

In a Sybil attack, the attacker creates multiple fake identities [4] to influence the network's consensus processes. In this attack, the attacker simulates fraudulent nodes using limited resources in order to impact voting, network decisions, and consensus protocols, ultimately aiming to gain control of the network [32]. In networks based on consensus algorithms such as Proof of Work and Proof of Stake, this attack becomes particularly dangerous when the attacker is able to increase their computational power or staking resources. Figure 6 illustrates an example of this type of attack. In this figure, the red blocks represent compromised blocks.

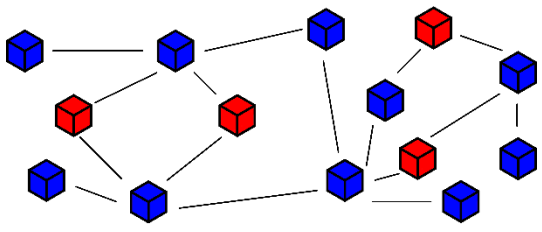

Fig. 6. Sybil attack

To counter Sybil attacks, blockchains employ various mechanisms that impose high costs for creating fake nodes [3]. Specifically, in PoW networks, creating fake nodes requires significant computational power, while in PoS networks, actual staking is required to participate in the consensus process, making the creation of fake identities more difficult. In addition to increasing the cost of creating fake nodes, reputation-based systems [33] can be employed. In these systems, nodes are scored based on their activity history within the network, and only high-reputation nodes are allowed to participate in the consensus process, preventing the influence of malicious nodes. Furthermore, identity-based consensus algorithms can require real identity verification for participants, effectively deterring the creation of fake nodes. These approaches increase the cost of generating multiple fake identities and significantly reduce the likelihood of a successful Sybil attack.

D. Attacks on smart contracts

Attacks on smart contracts are significant threats in blockchains that can lead to serious abuses. Smart contracts, which are executable codes on the blockchain, may be vulnerable to various attacks due to weak designs or coding errors [34]. Among these attacks are reentrancy attacks, where the attacker exploits design flaws to access contract resources before the status update is completed [5]. This type of attack, known as DAO, was observed in the Ethereum blockchain [22]. Incomplete transaction attacks occur when an attacker disrupts the contract's execution logic by injecting incorrect values, which can lead to exploitation in financial contracts.

For example, the DAO attack in 2016 was a real-world instance of this type of attack. In this attack, attackers exploited a vulnerability in the DAO smart contract code to steal over $50 million worth of cryptocurrency. This attack led to the division of the Ethereum network into two separate chains.

To counter these threats, using verified code, conducting thorough security audits, and employing monitoring models to detect suspicious behavior are essential. Additionally, enhancing smart contract design standards, such as Ethereum's ERC-20, can help improve security and prevent such attacks. Additionally, the use of static and dynamic analysis tools such as Mythril and Slither is highly effective. These tools can identify potential vulnerabilities in smart contract code. Moreover, advanced security standards like ERC-721 [35] and ERC-1155 [36] provide enhanced security features, helping to prevent common attacks on smart contracts.

E. BGP Attack

The BGP attack is one of the significant threats in blockchain networks, which can lead to traffic rerouting and disrupt the transaction validation process. The BGP protocol, due to its basic design and lack of encryption, is vulnerable to various attacks. In these attacks, the attacker is able to alter routing paths and direct transactions or data to their own servers, which can result in data manipulation, information theft, or transaction forgery. Additionally, denial-of-service (DoS) attacks can cause severe disruptions by directing traffic toward specific nodes or sending incorrect information to the network [37]. As shown in Figure 7, the compromise of a router in the network causes routing disruptions, resulting in the creation of a custom path (the red path) toward a specific node (the red block).

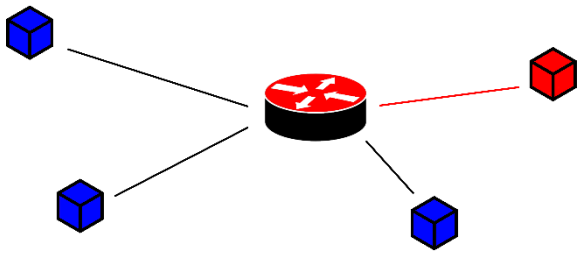

Fig. 7. BGP attack

To counter these threats, the use of advanced security protocols such as BGPsec and RPKI is essential. BGPsec focuses on the encryption and validation of BGP routes, preventing unauthorized changes to routing paths, while RPKI strengthens blockchain network security by validating and verifying the resources of these paths. Additionally, overlay networks such as Tor or I2P can be utilized. These networks route traffic through encrypted pathways, making it difficult for attackers to manipulate network routes [38]. Furthermore, continuous monitoring of route changes can help detect potential route hijacking attempts. These measures can effectively mitigate the threats posed by BGP attacks, enhancing the security and reliability of blockchain networks.

F. Private Key Attack and Key Theft

Private key attacks and key theft are serious threats in blockchain that can lead to the loss of digital assets. In blockchain, private keys are crucial for accessing assets and performing transactions. If an attacker gains access to a user's private key, they can freely access their assets and conduct fraudulent transactions. Common methods for stealing these keys include phishing attacks, malware, and hacking of software and hardware wallets [39]. In phishing attacks, the attacker deceives the user into entering their private key on a fake website or application. Malware, such as spyware or keyloggers, can also infiltrate user devices and steal private keys.

To mitigate these threats, it is recommended to use hardware wallets that store private keys in separate devices, protecting them from online access. Additionally, multi-factor authentication can help enhance security. In addition to these measures, multi-signature algorithms can be employed. In this approach, executing transactions requires authorization from multiple private keys [40], making it impossible for attackers to access assets even if a single private key is compromised. Educating users to recognize phishing and malware attacks is also an essential part of strategies to prevent private key theft [41].

G. Distributed Denial of Service (DDoS) Attack

A Distributed Denial of Service (DDoS) attack in blockchain refers to attacks aimed at disrupting user access to the blockchain network. These attacks typically use many different devices (often under the attacker's control) to send a high volume of unwanted requests to the network. As a result, system resources, such as bandwidth or processing servers, are severely strained, and service to legitimate users is disrupted. These attacks can have negative impacts on the performance of blockchain networks and can even halt their operations [9].

In blockchain, DDoS attacks can occur in two main forms: 1) Attacks on network nodes, and 2) Attacks on smart contracts. In attacks on nodes, the attacker's goal is to create high traffic to consume bandwidth and computational resources, which can result in reduced efficiency and slower transactions [2]. In attacks on smart contracts, the attacker may try to exploit network capacities by sending complex requests to disrupt smart contract operations [3].

To mitigate these attacks, methods such as using advanced firewalls, DDoS protection services, and increasing network capacity are recommended. Additionally, some blockchain networks enhance their security by using decentralized consensus algorithms and identity verification mechanisms to become more resistant to DDoS attacks [42]. Fault-tolerant networks can also be utilized in this context. In such networks, even if some nodes are attacked, other nodes are able to continue the network's operation. Additionally, increasing network capacity and employing faster consensus algorithms can mitigate the impact of these attacks.

To protect blockchain nodes against DDoS attacks, advanced firewalls such as Firepower or Palo Alto Networks can be utilized. These firewalls have the capability to detect and block malicious traffic. When configuring these firewalls, security policies should be set to ensure:

- Allowing only traffic from authorized ports, such as port 80 for HTTP and port 443 for HTTPS, to minimize the attack surface.
- Enabling Intrusion Prevention System (IPS) to detect and block potential network attacks.

Additionally, DDoS protection services such as Cloudflare or Akamai can be deployed. These services should be configured to ensure that incoming traffic to blockchain nodes is routed through a Content Delivery Network (CDN), effectively filtering out malicious requests and mitigating volumetric attacks.

H. Eclipse Attack

The Eclipse attack in blockchain is a security threat aimed at disrupting communication between network nodes. In this attack, the attacker creates a private network of their own nodes, cuts off the communication of the targeted node, and intentionally alters or intercepts the information they are seeking. This type of attack is particularly dangerous for blockchain networks that use consensus algorithms based on random nodes. By controlling a large number of nodes, the attacker can send false or fake information to the target node, which may result in the target node sending incorrect data to the network or failing to validate legitimate transactions [43]. This attack can significantly affect data synchronization processes and transaction validation. For example, as shown in Figure 8, the compromised node (red block) disrupts the communication of the target node(s) with the entire blockchain network, causing synchronization issues with the network.

To counter Eclipse attacks, in addition to using resilient communication protocols, random node assignment can be employed. In this approach, nodes are randomly connected to one another, making it difficult for attackers to control the communications [44]. Moreover, utilizing multiple nodes for

data verification can prevent information manipulation by attackers.

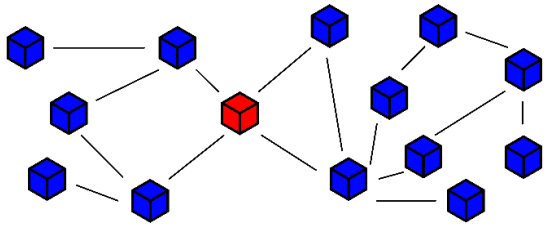

Fig. 8. Eclipse attack

I. *Timejacking Attack*

The timejacking attack is a security threat in blockchain networks where an attacker manipulates the network's system time to disrupt the consensus process. The goal is to deceive nodes into receiving incorrect time data, which can affect the order and validity of transactions. By manipulating time, the attacker can disrupt the blockchain synchronization process, allowing illegal or fraudulent transactions to be accepted as valid [4]. This type of attack is particularly dangerous for blockchain networks that rely on precise timing and node synchronization for transaction validation. To counter this threat, various methods are used, including the use of tamper-resistant timestamps, time-independent consensus algorithms like Proof of Stake, and advanced synchronization protocols [45]. Additionally, the use of time-independent consensus algorithms, such as Proof of History (PoH) [46], can be effective. These algorithms rely on an internal timestamp sequence, which is nearly impossible for attackers to manipulate. These methods help the network prevent incorrect time changes and ensure that even if an attacker changes the time of one node, the network can detect and correct this error.

J. *Dusting Attack*

In blockchain, a dusting attack refers to sending small amounts of cryptocurrency to a large number of different addresses to identify the real identities behind these addresses. The purpose of this attack is to collect data from transaction behavior and analyze user patterns for identification and tracking. The attacker usually sends tiny amounts of cryptocurrency, known as dust, to various addresses and uses transaction analysis to link these addresses to a specific identity [47]. To counter this attack, one of the solutions is to use multi-signature addresses and avoid reusing addresses for different transactions. Additionally, users can use privacy services like CoinJoin and zero-knowledge proofs. These services conduct transactions anonymously, making it difficult for attackers to analyze transaction behavior.

K. *Phishing Attack*

A phishing attack in blockchain, similar to internet phishing attacks, is an attempt to deceive users into revealing private keys, account information, or passwords related to digital wallets. These attacks usually occur through emails or fake websites that resemble official blockchain service websites [25]. The goal is to trick the victim into entering sensitive information on a fraudulent page [48]. To protect against phishing attacks, users should always use reputable and well-known websites, avoid clicking on unknown links, and implement two-factor authentication to enhance the security of their accounts. Additionally, educating and raising awareness among users can play an important role in reducing the success of these attacks. Also AI-based phishing detection technologies can be employed [49]. These technologies are capable of identifying fraudulent websites and emails, alerting users to potential threats.

L. *Liveness Attack*

One of the complex threats in blockchain networks is the liveness attack, which aims to delay transaction confirmations and disrupt the process of recording them in the public ledger. In this attack, the attacker manipulates the growth process of the blockchain, preventing transactions from reaching public confirmation. The liveness attack consists of three stages: 1) The attack preparation stage, where the attacker temporarily dominates the miners by creating a private chain longer than the public chain. 2) The transaction denial stage, where the attacker keeps the block containing the target transaction private to prevent it from being registered in the public chain. 3) The blockchain slowdown stage, where the attacker continues to build and release the private chain, reducing the public chain's growth rate and delaying the target transaction [22].
To combat this attack, the use of more resilient consensus mechanisms like Proof of Stake or hybrid algorithms, which are less affected by liveness attacks, is recommended. Additionally, strategies like fast synchronization and transaction confirmation by multiple miners can be implemented to prevent delays in establishing transactions and ensure the blockchain's growth speed. These measures can help prevent transaction confirmation delays and network disruptions [50].

M. *Balance Attack*

A balance attack in blockchain allows low computational power attackers to temporarily disrupt communications between subgroups with similar computational power. In this attack, the blockchain is transformed into an unconstrained graph where nodes represent blocks, connected through directed edges [51]. The attacker initially introduces delays between correct subgroups with similar computational power, issuing transactions in one subgroup (transaction subgroup) and mining blocks in another subgroup (block subgroup). This causes the block subgroup tree to dominate the transaction subgroup tree, and even if the transactions are recorded, the attacker can rewrite the corresponding blocks [3]. The balance attack effectively violates the chain's prefix continuity and poses a double-spending risk.
To counter this attack, in addition to using more resilient consensus algorithms such as PoS, advanced synchronization mechanisms can be employed [51]. For instance, time-based synchronization algorithms can prevent artificial delays by ensuring precise synchronization of nodes. Moreover, using delay-resistant communication protocols can enhance network security against such attacks. Furthermore, parallel transaction [52] verification by multiple independent subgroups can prevent one subgroup from dominating the

others. This approach ensures that even if one subgroup is affected by an attack, other subgroups can continue the network's operation.

N. Selfish Mining Attack

A selfish mining attack is carried out by attackers to gain illegitimate rewards or waste the computational power of honest miners. In this attack, the attacker privately mines new blocks and creates a private chain longer than the public chain [5]. When honest miners discover a new block, the attacker publishes their private blocks, attempting to present the private chain as the valid one [25]. This attack undermines the decentralization of the blockchain, causing honest miners to perform extra computations without receiving rewards, while attackers can strategically release their blocks to gain more advantages. Research has shown that this attack is effectively executed in PoW-based blockchains with only 25% of the network's computational power. Figure 9 shows an illustration of the Selfish Mining attack.

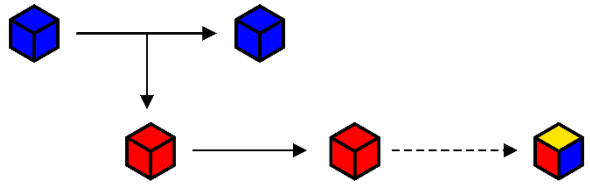

Fig. 9. Selfish mining attack

To counter this attack, network difficulty can be increased, and more resilient consensus algorithms such as PoS can be employed [53], alongside penalty mechanisms. For instance, in some PoS networks, if a node attempts to secretly mine blocks, a portion of its stake is confiscated. This significantly reduces the attackers' incentive for selfish mining. Moreover, increasing the speed of block propagation across the network can help prevent the success of such attacks. By utilizing faster communication protocols and improving network infrastructure, it can be ensured that new blocks are quickly disseminated throughout the network, leaving attackers with insufficient time to create a private chain.

Additionally, hybrid consensus algorithms [54] like PoW/PoS can enhance network security against these attacks. In these algorithms, block mining is a combination of computational power and stake, making it more difficult for attackers to control the network.

IV. COMPRATIVE ANALYSIS

Given the complexities of vulnerabilities present in blockchain systems, a precise understanding and analysis of different types of attacks is crucial for enhancing the security of this technology. In this section, we compare and analyze the various attacks previously discussed.

A. Comparison of Threats

The attacks introduced in Section III vary depending on their type, objective, complexity, and required resources. Table 2 provides a comprehensive comparison of different blockchain attacks, covering various aspects. The purpose of this comparison is to highlight the characteristics of these attacks, so that more effective solutions can be developed and suitable security strategies can be adopted to address each type of threat.

TABLE II. COMPARISON OF BLOCKCHAIN ATTACK TYPES

Attack Type	Required Resources	Common Vulnerabilities	Preventive Measures	Effect on Privacy	Predictability and Prevention
Majority Attack [26]	Control 51% of computational power	Consensus protocols	Increase network computational power	Decreases privacy	Detectable through strong consensus
Double Spending Attack [19]	Network resources for fake transactions	Simultaneous transactions	Faster verification systems	Decreases security and privacy	Simulatable with specialized tools
Sybil Attack [32]	Creation of fake nodes in the network	Fake node creation	Strengthen consensus protocols	Exposure of personal data	Simulatable
Smart Contract Attack [34]	Exploiting code vulnerabilities	Weak contract code review	Code auditing, formal verification	High if private data is involved	Detectable through proper audits
BGP Attack [37]	Internet routing control	Internet routing vulnerabilities	Secure routing protocols	Low to moderate impact	Detectable through routing table analysis
DDoS Attack [9]	Botnets, high traffic generation	Bandwidth limitations	Rate limiting, anti-DDoS measures	Minimal	Traffic analysis
Eclipse Attack [9]	Isolating network nodes	Peer-to-peer networks	Network diversity, IP restriction	Moderate impact	Detectable through network monitoring
Time-jacking Attack [4]	Manipulating network timestamps	Network time protocol	Secure time synchronization	Low to moderate impact	Continuous timestamp monitoring
Dusting Attack [47]	Sending small amounts to wallets	Repeated use of wallet addresses	Mixing services, address change	High impact on privacy	Monitoring small transactions
Phishing Attack [25]	Social engineering, fake websites	Human error	User education, two-factor authentication, secure links	High impact	Strong user education
Liveness Attack [22]	Network manipulation	Consensus protocol	Strengthened consensus rules	Low impact	Detectable through consensus analysis
Balance Attack [51]	Network partition	Partitioned networks	Stronger consensus protocols	Moderate impact	Network monitoring systems
Selfish Mining Attack [53]	Maintaining a private chain	Mining power centralization	Block reward mechanism adjustments	Minimal	Detectable through mining analysis

B. Threat Analysis

Security threats in blockchain systems can damage the infrastructure of this technology in various ways due to their complexity and diversity [6]. Unlike direct attacks such as double spending and 51% attacks, many threats infiltrate the network's different layers, including communication protocols, key management, and social interactions, often in

a hidden manner [10]. One of the main challenges in threat analysis is identifying malicious behavioral patterns amidst the network's normal activities. To counter these threats, the use of advanced methods such as behavior analysis, machine learning, and continuous network monitoring is crucial [55]. These approaches can help create more effective defensive strategies, reducing vulnerabilities before they escalate into severe attacks. The threat analysis and comparison of different attack characteristics addressed in this section assist in identifying the weaknesses of blockchain networks and providing more effective countermeasures, ultimately ensuring security and increasing trust in decentralized systems.

Attacks Based on Their Impact on the Network: Table 3 presents a set of common attack types in blockchain networks, focusing on the type of impact on the network and including real-world examples [22, 4]. This analysis significantly aids in better identifying vulnerabilities in blockchain-based systems and finding effective measures to reduce security risks.

TABLE III. ATTACKS BASED ON THEIR IMPACT ON THE NETWORK

Attack Type	Example	Amount	Impact on Network
Majority Attack	Bitcoin Gold Attack (2018)	Millions of dollars	Destruction of network integrity and transparency
Double Spending Attack	Bitfinex Attack (2016)	Millions of dollars	Reduced transaction credibility, double spending, insecurity
Sybil Attack	Tor and Bitcoin network (2014)	Unspecified	Disruption in consensus, reduced security
Smart Contract Attack	DAO Vulnerability in Ethereum (2016)	Around $60 million	Financial loss, contract execution flaws
BGP Attack	Amazon Route 53 (2018)	Around $150,000	Data flow interception and modification, transaction speed reduction
Private Key Theft	Mt.Gox (2014)	Millions of dollars	No direct impact on the network
DDoS Attack	Ethereum (2016)	Unspecified	Network slowdown or failure
Eclipse Attack	In Simulations	Unspecified	Consensus change and transaction validation issues
Timejacking Attack	In Simulations	Unspecified	Delay in consensus and transaction confirmation
Dusting Attack	Tron Network (2023)	170,000 USDT	Reduced user privacy
Phishing Attack	Binance (2020)	Around $40 million	Asset loss, data theft
Liveness Attack	In Simulations	Unspecified	Network operation halt
Balance Attack	In Simulations	Unspecified	Potential double spending, network halt
Selfish Mining Attack	In Simulations	Unspecified	Destruction of decentralization, wasted honest miners' efforts

Attacks Based on Impact Severity: Cyberattacks can significantly affect the performance of blockchain networks, leading to reduced efficiency, increased latency, data loss, or even complete network shutdowns [7]. In Figure 10, various types of attacks are compared based on the severity of their impact on blockchain networks. This analysis is aimed at providing a comprehensive view of the level of damage each attack can cause. A precise understanding of these attacks and their potential impact allows decision-makers to allocate resources more effectively and adopt preventive strategies to protect networks.

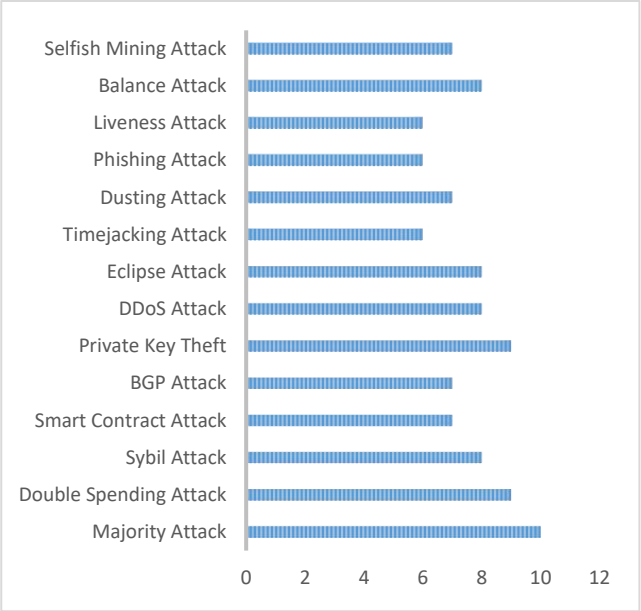

Fig. 10. Comparison of different types of attacks based on their impact severity on blockchain networks

Attacks Based on Different Criteria: Figure 11 examines attacks from various perspectives, including execution complexity, detectability, and the cost of these attacks in blockchain networks, providing a clear view of the threats and challenges facing blockchain technology. A thorough understanding of these aspects can significantly contribute to the stability of blockchain networks.

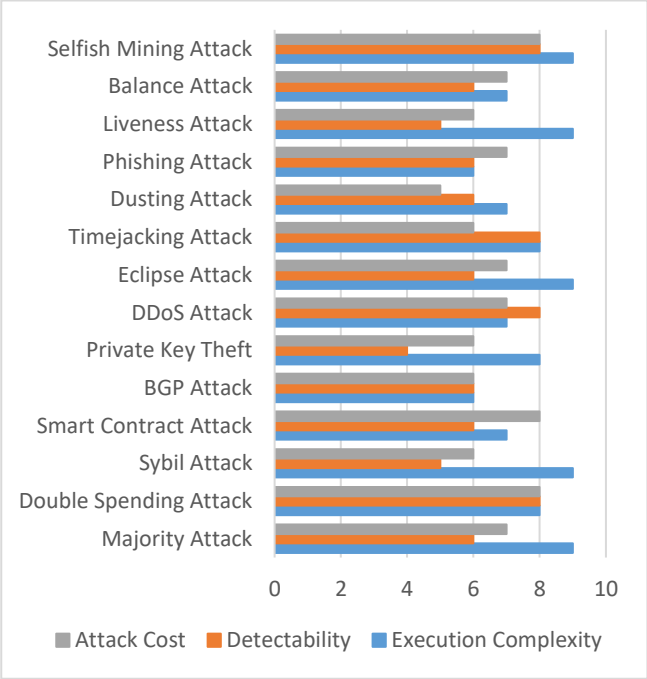

Fig. 11. Comparison of attacks based on various criteria

An analysis of blockchain attacks reveals that majority attacks, Sybil attacks, eclipse attacks, liveness attacks, and selfish mining are among the most complex to execute due to their reliance on advanced technical resources and in-depth knowledge. On the other hand, attacks such as double-spending, DDoS, selfish mining, and timejackein exhibit higher detectability due to the inherent characteristics of blockchain networks.

In terms of cost, attacks like double-spending, selfish mining, and smart contract attack are the most expensive, as they depend on substantial financial and computational resources. The findings suggest that high-complexity and high-cost attacks typically target larger and more valuable networks. In contrast, low-cost and easily detectable attacks, such as phishing, are executed more broadly due to their simplicity and high success rates.

This analysis underscores the necessity for multilayered strategies to effectively mitigate diverse threats in blockchain systems, ensuring the stability and security of decentralized networks.

Frequency of Blockchain Attacks: The distribution of common blockchain attacks based on their frequency of occurrence is illustrated in Figure 12. An analysis of the frequency of blockchain attacks reveals that attacks such as majority attacks, Sybil attacks, DDoS attacks, phishing, and double-spending are among the most prevalent threats. Several factors contribute to this frequency. Majority and double-spending attacks occur more frequently in weaker or less robust systems due to the decentralized nature of blockchain and its reliance on network consensus. Sybil attacks, which exploit the creation of fake accounts, are relatively simple to execute, making them common. Similarly, DDoS attacks, due to the widespread availability of tools to initiate such attacks, occur frequently and are widely employed in network-based attacks. Finally, phishing attacks leverage social engineering and the large pool of potential users to achieve high occurrence rates.

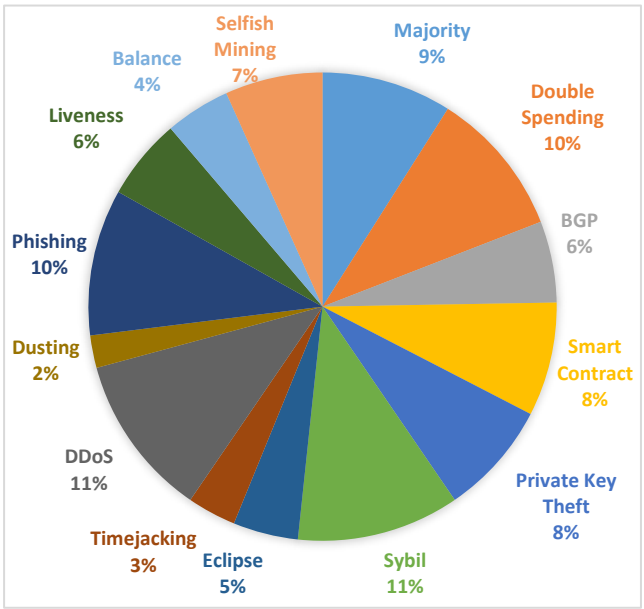

Fig. 12. Comparison of the distribution of common blockchain attacks

These patterns demonstrate that the frequency of attacks is closely tied to the low cost of execution, accessibility of appropriate tools, and security vulnerabilities in network infrastructures. To counteract these threats, blockchain developers must continuously enhance detection and prevention mechanisms.

Analysis of Countermeasures for Attacks: Given the complexity of attacks and their potentially destructive impacts on blockchain systems, implementing effective and efficient countermeasures is essential. Analyzing various mitigation strategies can significantly contribute to the stability and resilience of blockchain technology. Table 4 outlines the strengths and weaknesses of different countermeasures against various types of attacks. This table provides a detailed overview of the countermeasures for various blockchain attacks, highlighting their benefits and limitations. It emphasizes the importance of selecting appropriate strategies based on the specific attack scenario while considering the trade-offs involved in implementation.

TABLE IV. STRENGTHS AND WEAKNESSES OF COUNTERMEASURES AGAINST BLOCKCHAIN ATTACKS

Attack Type	Countermeasures	Strengths	Weaknesses
Majority Attack	Increasing mining power, Proof of Stake	Higher attack resistance, reduced success probability	High costs and resource demands
Double Spending Attack	Increasing transaction confirmation time, multi-signature wallets	Enhanced transaction security	Time-consuming for users
Sybil Attack	Reputation-based systems, Proof of Authority	Reduced likelihood of creating fake identities	Dependence on centralized validation models
Smart Contract Attack	Formal verification, smart contract audits	Detection and mitigation of contractual vulnerabilities	High implementation costs for small projects
BGP Attack	Prefix filtering, BGP monitoring and detection	Prevention of route hijacking	High technical complexity for implementation
Private Key Theft	Hardware wallets, two-factor authentication (2FA), secure key storage	Increased key security, reduced hacking likelihood	Dependence on specific hardware and higher costs
DDoS Attack	Rate limiting, CAPTCHA, bot reduction	Enhanced network resilience against attacks	May impose restrictions on legitimate users
Eclipse Attack	Network monitoring, time synchronization protocols	Reduced probability of node isolation	Requires diverse IP infrastructure
Timejacking Attack	Timestamp verification, random transaction delays	Reduced likelihood of timing errors in transactions	High cost of continuous monitoring
Dusting Attack	Transaction monitoring, pattern recognition	Improved user privacy	Limited effectiveness in highly dynamic environments
Phishing Attack	User education, email filters	Increased user awareness and security	Depends on user awareness and attack complexity
Liveness Attack	Redundancy, consensus protocol optimization	Maintains network stability under adverse conditions	High complexity in protocol design
Balance Attack	Regular balance reviews, miner activity monitoring	Reduced risk of partitioning and imbalance	Dependence on strict rules for resource allocation
Selfish Mining Attack	Isolating selfish miners, Proof-of-Work adjustments	Reduced profitability of selfish mining	May decrease miners' motivation

Figure 13 presents an evaluation of the countermeasures detailed in Table 4, scoring them from 1 to 10 across three

parameters: effectiveness, implementation cost, and resource requirements.

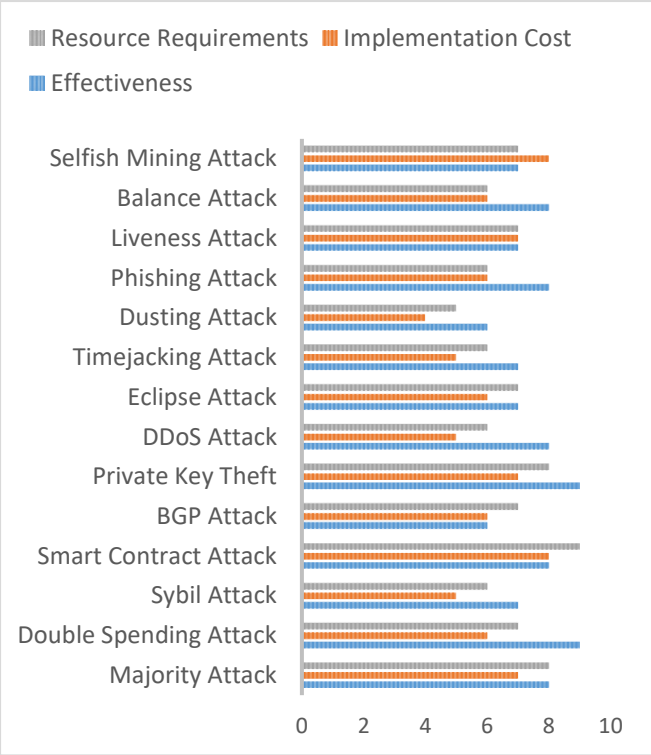

Fig. 13. Scoring of countermeasures from Table 4 based on effectiveness, implementation cost, and resource requirements

This comparison not only assists decision-makers and developers in selecting optimal security approaches but also provides a clearer understanding of the balance between effectiveness and cost.

V. Multifaceted Challenges in Blockchain Security

This section explores the various complex aspects of blockchain security. While cryptographic techniques and technical solutions play a crucial role in securing blockchain networks, other factors also significantly impact this security. These factors include privacy, regulatory and compliance challenges, as well as the influence of human and organizational elements. This section delves into these different dimensions and examines the importance of each in strengthening and maintaining blockchain security.

A. Privacy in Blockchain

Transaction privacy in blockchain is a fundamental challenge for this technology. Although blockchain enables transactions without revealing users' real identities, research has shown that transactions remain traceable. For instance, studies on Bitcoin have demonstrated that transaction histories can be linked to real-world identities [56]. Additionally, methods such as associating pseudonymous user addresses with IP addresses, as proposed in [57], highlight vulnerabilities in blockchain privacy. The primary reason behind this susceptibility is the public visibility of transaction details and the balances of all public keys within the blockchain network. Consequently, to prevent information leakage, privacy and security measures should be integrated from the initial design phase of blockchain applications.

To address these challenges, several approaches have been proposed in recent years. Solutions such as Hawk for executing private smart contracts [58], Obscuro for Bitcoin transaction mixing [59], and Ouroboros Crypsinous [60] for privacy-preserving PoS protocols have been introduced. Furthermore, blockchain networks like Bitcoin and Zcash employ one-time accounts and unique private keys for each transaction to obscure transaction linkages. In Monero, users can utilize decoy coins (Mixins) to prevent adversaries from identifying the connection between inputs and outputs in a transaction. Algorithms such as Zero-Knowledge Proofs, Ring Signatures, and Stealth Addresses, which are used in the Monero cryptocurrency, have also contributed significantly to improving user privacy. However, studies indicate that existing privacy mechanisms are not entirely robust; for example, research has revealed that 66.09% of Monero transactions lack mixins [61], leading to privacy leaks. Therefore, despite advancements in blockchain privacy, further research and development are required to enhance the resilience of privacy-preserving techniques in blockchain technology.

B. Regulatory and Compliance Challenges in Blockchain Security

Despite its significant security advantages, blockchain technology presents complex regulatory and compliance challenges. Given its inherently decentralized nature, which eliminates the need for a central authority, many traditional legal frameworks designed for centralized systems do not fully align with blockchain operations [62]. Globally, countries have adopted varying approaches to blockchain regulation, with some embracing the technology while others impose restrictions on its usage.

One of the most critical issues is balancing privacy protection with legal requirements such as Anti-Money Laundering (AML) and Know Your Customer (KYC) regulations. For instance, in 2021, the Binance exchange collaborated with regulatory bodies worldwide to comply with AML and KYC regulations. Binance employed transaction analysis tools such as Chainalysis and Elliptic to detect suspicious activities. Another example is the 2020 settlement between Ripple and the U.S. Securities and Exchange Commission (SEC) regarding the sale of XRP tokens as securities, highlighting the importance of financial compliance in the blockchain sector.

While some blockchains, such as Bitcoin and Ethereum, maintain transaction transparency, others, like Monero and Zcash, implement anonymization mechanisms that raise regulatory concerns over potential illicit activities. Additionally, attacks such as private key theft, phishing, and double-spending pose complex legal challenges, as assigning responsibility and enforcing regulations in a decentralized environment remains difficult. Furthermore, the legal frameworks for smart contracts are still evolving, as issues related to their enforceability and dispute resolution have not been fully addressed.

Therefore, blockchain security should not be examined solely from a technical perspective but also within the framework of international regulations, governance policies, and compliance standards. Future research should explore strategies to align blockchain security innovations with regulatory requirements, facilitating broader adoption of this technology in financial, commercial, and governmental sectors.

C. The Role of Human and Organizational Factors in Blockchain Security

Blockchain security is not solely dependent on technical measures but is heavily influenced by human and organizational factors. Many security breaches, such as phishing attacks and private key theft, occur not because of flaws in cryptographic algorithms but due to human errors or gaps in security policies. A primary challenge is the limited awareness among users regarding security threats, which can lead to social engineering attacks [63] and unauthorized access to digital assets. Comprehensive user education programs, coupled with security practices like multi-factor authentication and the use of hardware wallets, can significantly reduce these vulnerabilities.

At the organizational level, secure management of cryptographic keys is crucial, as improper storage or handling of keys can lead to asset loss. Solutions such as multi-signature and distributed key storage, along with adherence to security standards like NIST SP 800-57 [64], can effectively mitigate such risks. Additionally, weaknesses in smart contract implementation and the failure to follow secure programming standards can lead to attacks, such as the Reentrancy Attack witnessed in the 2016 DAO hack. Employing techniques like formal code auditing and enforcing security standards, such as ERC-1404 [65], can help prevent these vulnerabilities.

Furthermore, the way users interact with digital wallets and blockchain networks also impacts security. Research has shown that transaction data leaks in software wallets can reveal users' identities. Privacy-preserving technologies, such as CoinJoin, MimbleWimble, and privacy-oriented blockchains like Monero, can help reduce these risks.

VI. FUTURE WORK

Blockchain technology, as an innovative infrastructure, holds immense potential to transform various domains due to its unique features. However, numerous security challenges, particularly in maintaining data integrity and privacy, hinder its widespread adoption. Future research should focus on identifying and analyzing emerging threats and developing innovative solutions. Emphasizing user awareness and education about blockchain cybersecurity, especially in key management and recognizing social engineering attacks, can significantly enhance the security of this technology.

Given the rapid growth of blockchain technology and the increasing diversity of security threats and attacks, adopting novel and effective approaches to safeguard this ecosystem is crucial. Strengthening the security of blockchain networks will require continuous improvements and enhancements in various countermeasures.
Key strategies include:

- **Optimizing Consensus Algorithms:** Enhancing algorithms like PoS to mitigate 51% attacks, enabling better resource distribution, and reducing attack risks.
- **Secure Protocols:** Utilizing secure communication protocols such as TLS and public-key cryptography to improve node communication security and prevent man-in-the-middle attacks.
- **Intrusion Detection Systems:** Implementing intrusion detection systems and user behavior analysis to identify malicious activities in real time.
- **Key Management:** Improving private key management through secure storage techniques and multi-factor authentication to safeguard user assets.
- **Secure Smart Contracts:** Developing smart contracts with robust, secure code and ensuring regular software updates.
- **Mitigating Emerging Threats and Future Attacks, Including AI-Based and Quantum Attacks:** With the increasing use of artificial intelligence (AI) in blockchain networks [55], attackers may also leverage this technology to conduct advanced attacks. For instance, machine learning-based attacks can analyze transaction patterns and identify vulnerabilities within the network. To counter these threats, blockchain networks should implement AI-driven defensive algorithms capable of detecting and neutralizing suspicious activities in real time.Furthermore, with the advancement of quantum computing, current cryptographic algorithms used in blockchain systems may become vulnerable. For example, Shor's Algorithm can efficiently break private keys within a short period, posing a significant security threat to the network. To mitigate this risk, blockchain networks must transition toward post-quantum cryptography, which is designed to withstand quantum-based attacks.

Ongoing research and user education in this domain will enhance awareness and preparedness, paving the way for further innovations while addressing future challenges effectively.

VII. CONCLUSION

Given the growing importance of blockchain across various fields, the need for continuous research and development in the security of these systems is more critical than ever. This paper underscores the necessity of integrating technical and educational approaches to improve blockchain security. It suggests that future research should focus on identifying existing challenges and providing scientific and practical solutions to maximize the potential of this transformative technology.

REFERENCES:

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," ۲۰۰۸.

[2] Khoshavi, Navid, et al. "A Survey on Blockchain Security." 2019 SoutheastCon, 2019, pp. 1–8. IEEE Xplore, https://doi.org/10.1109/SoutheastCon42311.2019.9020646.

[3] Singh, Saurabh, et al. "Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network." IEEE Access, vol. 9, 2021, pp. 13938–59. IEEE Xplore, https://doi.org/10.1109/ACCESS.2021.3051602.

[4] Guo, Huaqun, and Xingjie Yu. "A Survey on Blockchain Technology and Its Security." Blockchain: Research and Applications, vol. 3, no. 2,

June 2022, p. 100067. ScienceDirect, https://doi.org/10.1016/j.bcra.2022.100067.

[5] Li, Xiaoqi, et al. "A Survey on the Security of Blockchain Systems." Future Generation Computer Systems, vol. 107, June 2020, pp. 841–53. ScienceDirect, https://doi.org/10.1016/j.future.2017.08.020.

[6] Islam, Md Rafiqul, et al. "A Review on Blockchain Security Issues and Challenges." 2021 IEEE 12th Control and System Graduate Research Colloquium (ICSGRC), 2021, pp. 227–32. IEEE Xplore, https://doi.org/10.1109/ICSGRC53186.2021.9515276.

[7] Bhutta, Muhammad Nasir Mumtaz, et al. "A Survey on Blockchain Technology: Evolution, Architecture and Security." IEEE Access, vol. 9, 2021, pp. 61048–73. IEEE Xplore, https://doi.org/10.1109/ACCESS.2021.3072849.

[8] Li, Xiulai, et al. "Blockchain Security Threats and Collaborative Defense: A Literature Review." Computers, Materials & Continua, vol. 76, no. 3, 2023, pp. 2597–629. DOI.org (Crossref), https://doi.org/10.32604/cmc.2023.040596.

[9] Leng, Jiewu, et al. "Blockchain Security: A Survey of Techniques and Research Directions." IEEE Transactions on Services Computing, vol. 15, no. 4, July 2022, pp. 2490–510. IEEE Xplore, https://doi.org/10.1109/TSC.2020.3038641.

[10] AlFaw, Aysha, et al. "Blockchain Vulnerabilities and Recent Security Challenges: A Review Paper." 2022 International Conference on Data Analytics for Business and Industry (ICDABI), 2022, pp. 780–86. IEEE Xplore, https://doi.org/10.1109/ICDABI56818.2022.10041611.

[11] Mohanta, Bhabendu Kumar, et al. "Blockchain Technology: A Survey on Applications and Security Privacy Challenges." Internet of Things, vol. 8, Dec. 2019, p. 100107. ScienceDirect, https://doi.org/10.1016/j.iot.2019.100107.

[12] Iuon-Chang Lin and Tzu-Chun Liao. "A Survey of Blockchain Security Issues and Challenges." International Journal of Network Security, vol. 19, no. 5, Sept. 2017. Semantic Scholar, https://doi.org/10.6633/IJNS.201709.19(5).01.

[13] Morar, Catalin Daniel, and Daniela Elena Popescu. "A Survey of Blockchain Applicability, Challenges, and Key Threats." Computers, vol. 13, no. 9, Sept. 2024, p. 223. www.mdpi.com, https://doi.org/10.3390/computers13090223.

[14] Bansal, Pranshu, et al. "Blockchain for Cybersecurity: A Comprehensive Survey." 2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT), 2020, pp. 260–65. IEEE Xplore, https://doi.org/10.1109/CSNT48778.2020.9115738.

[15] Chen, Wubing, et al. "A Survey of Blockchain Applications in Different Domains." Proceedings of the 2018 International Conference on Blockchain Technology and Application, Association for Computing Machinery, 2018, pp. 17–21. ACM Digital Library, https://doi.org/10.1145/3301403.3301407.

[16] De Aguiar, Erikson Júlio, et al. "A Survey of Blockchain-Based Strategies for Healthcare." ACM Comput. Surv., vol. 53, no. 2, Mar. 2020, p. 27:1-27:27. ACM Digital Library, https://doi.org/10.1145/3376915.

[17] Liu, Jiajun, and Junhao Wu. "A Comprehensive Survey on Blockchain Technology and Its Applications." Highlights in Science, Engineering and Technology, vol. 85, Mar. 2024, pp. 128–38. Semantic Scholar, https://doi.org/10.54097/r0ggyr24.

[18] He, Zheyuan, et al. Large Language Models for Blockchain Security: A Systematic Literature Review. arXiv, 2024. DOI.org (Datacite), https://doi.org/10.48550/ARXIV.2403.14280.

[19] Monrat, Ahmed Afif, et al. "A Survey of Blockchain from the Perspectives of Applications, Challenges, and Opportunities." IEEE Access, vol. 7, 2019, pp. 117134–51. IEEE Xplore, https://doi.org/10.1109/ACCESS.2019.2936094.

[20] Zamani, Efpraxia, et al. "On the Security Risks of the Blockchain." Journal of Computer Information Systems, vol. 60, no. 6, Nov. 2020, pp. 495–506. DOI.org (Crossref), https://doi.org/10.1080/08874417.2018.1538709.

[21] Tripathi, Gautami, et al. "A Comprehensive Review of Blockchain Technology: Underlying Principles and Historical Background with Future Challenges." Decision Analytics Journal, vol. 9, Dec. 2023, p. 100344. ScienceDirect, https://doi.org/10.1016/j.dajour.2023.100344.

[22] Gupta, Neha. "Chapter 4 - A Deep Dive into Security and Privacy Issues of Blockchain Technologies." Handbook of Research on Blockchain Technology, edited by Saravanan Krishnan et al., Academic Press, 2020, pp. 95–112. ScienceDirect, https://doi.org/10.1016/B978-0-12-819816-2.00004-6.

[23] Gervais, Arthur, et al. "On the Security and Performance of Proof of Work Blockchains." Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Association for Computing Machinery, 2016, pp. 3–16. ACM Digital Library, https://doi.org/10.1145/2976749.2978341.

[24] Wang, Liangmin, et al. "Security and Privacy Issues in Blockchain and Its Applications." IET Blockchain, vol. 3, no. 4, Dec. 2023, pp. 169–71. DOI.org (Crossref), https://doi.org/10.1049/blc2.12051.

[25] Oksiiuk, Oleksandr, and Iryna Dmyrieva. "Security and Privacy Issues of Blockchain Technology." 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), 2020, pp. 1–5. IEEE Xplore, https://doi.org/10.1109/TCSET49122.2020.235489.

[26] Eyal, Ittay, and Emin Gün Sirer. "Majority Is Not Enough: Bitcoin Mining Is Vulnerable." Commun. ACM, vol. 61, no. 7, June 2018, pp. 95–102. ACM Digital Library, https://doi.org/10.1145/3212998.

[27] Li, Wangchun, et al. "Delegated Proof of Stake Consensus Mechanism Based on Community Discovery and Credit Incentive." Entropy, vol. 25, no. 9, Sept. 2023, p. 1320. www.mdpi.com, https://doi.org/10.3390/e25091320.

[28] Kasi, Nisanth Reddy, et al. "Chapter 1 - Blockchain Architecture, Taxonomy, Challenges, and Applications." Blockchain Technology for Emerging Applications, edited by SK Hafizul Islam et al., Academic Press, 2022, pp. 1–31. ScienceDirect, https://doi.org/10.1016/B978-0-323-90193-2.00001-6.

[29] Masteika, Saulius, et al. "Bitcoin Double-Spending Risk and Countermeasures at Physical Retail Locations." International Journal of Information Management, vol. 79, Dec. 2024, p. 102727. ScienceDirect, https://doi.org/10.1016/j.ijinfomgt.2023.102727.

[30] Yao, Yue, et al. "Blockchain-Based Multistage Continuous Authentication for Smart Devices." Applied Sciences, vol. 13, no. 23, Jan. 2023, p. 12641. www.mdpi.com, https://doi.org/10.3390/app132312641.

[31] Zhang, Zhujun, et al. "QPBFT: Practical Byzantine Fault Tolerance Consensus Algorithm Based on Quantified-Role." 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2020, pp. 991–97. IEEE Xplore, https://doi.org/10.1109/TrustCom50675.2020.00132.

[32] Swathi, P., et al. "Preventing Sybil Attack in Blockchain Using Distributed Behavior Monitoring of Miners." 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2019, pp. 1–6. IEEE Xplore, https://doi.org/10.1109/ICCCNT45670.2019.8944507.

[33] Biryukov, Alex, and Daniel Feher. "ReCon: Sybil-Resistant Consensus from Reputation." Pervasive and Mobile Computing, vol. 61, Jan. 2020, p. 101109. ScienceDirect, https://doi.org/10.1016/j.pmcj.2019.101109.

[34] Wu, Guangfu, et al. "A Comprehensive Survey of Smart Contract Security: State of the Art and Research Directions." Journal of Network and Computer Applications, vol. 226, June 2024, p. 103882. ScienceDirect, https://doi.org/10.1016/j.jnca.2024.103882.

[35] What Is ERC 721 Tokens: Explaining the Ethereum NFT Standard. 12 Feb. 2024, https://webisoft.com/articles/create-erc721-token/

[36] ERC-1155 Multi Token Standard - RareSkills. 10 Dec. 2024, https://www.rareskills.io/post/erc-1155.

[37] Qiong, Yang, et al. "Towards Blockchain-Based Secure BGP Routing, Challenges and Future Research Directions." Computers, Materials and Continua, vol. 79, no. 2, May 2024, pp. 2035–62. www.sciencedirect.com, https://doi.org/10.32604/cmc.2024.049970.

[38] Sun, Yixin, et al. "Counter-RAPTOR: Safeguarding Tor Against Active Routing Attacks." 2017 IEEE Symposium on Security and Privacy (SP), 2017, pp. 977–92. IEEE Xplore, https://doi.org/10.1109/SP.2017.34.

[39] Almadani, Mwaheb S., et al. "Blockchain-Based Multi-Factor Authentication: A Systematic Literature Review." Internet of Things,

vol. 23, Oct. 2023, p. 100844. ScienceDirect, https://doi.org/10.1016/j.iot.2023.100844.

[40] Han, Jongbeen, et al. "An Efficient Multi-Signature Wallet in Blockchain Using Bloom Filter." Proceedings of the 36th Annual ACM Symposium on Applied Computing, Association for Computing Machinery, 2021, pp. 273–81. ACM Digital Library, https://doi.org/10.1145/3412841.3441910.

[41] Pal, Om, et al. "Key Management for Blockchain Technology." ICT Express, vol. 7, no. 1, Mar. 2021, pp. 76–80. ScienceDirect, https://doi.org/10.1016/j.icte.2019.08.002.

[42] Chaganti, Rajasekhar, et al. "A Survey on Blockchain Solutions in DDoS Attacks Mitigation: Techniques, Open Challenges and Future Directions." Computer Communications, vol. 197, Jan. 2023, pp. 96–112. ScienceDirect, https://doi.org/10.1016/j.comcom.2022.10.026.

[43] Lin, Li, et al. "Eclipse Attack Defense Method Based on Distributed Storage and Reference Value System." 2023 IEEE 23rd International Conference on Communication Technology (ICCT), 2023, pp. 1231–36. IEEE Xplore, https://doi.org/10.1109/ICCT59356.2023.10419806.

[44] Vinta, Surendra Reddy, et al. "Dynamic Defense Model against Eclipse Attacks in Proof-of-Work Blockchain Systems." Procedia Computer Science, vol. 235, Jan. 2024, pp. 1202–12. ScienceDirect, https://doi.org/10.1016/j.procs.2024.04.114.

[45] Mollajafari, Sepideh, and Kamal Bechkoum. "Blockchain Technology and Related Security Risks: Towards a Seven-Layer Perspective and Taxonomy." Sustainability, vol. 15, no. 18, Jan. 2023, p. 13401. www.mdpi.com, https://doi.org/10.3390/su151813401.

[46] Weston, Georgia. "What Is Proof of History and How Does It Work?" 101 Blockchains, 24 Feb. 2023, https://101blockchains.com/proof-of-history/.

[47] Wang, Yunpeng, et al. "Anti-Dust: A Method for Identifying and Preventing Blockchain's Dust Attacks." 2018 International Conference on Information Systems and Computer Aided Education (ICISCAE), 2018, pp. 274–80. IEEE Xplore, https://doi.org/10.1109/ICISCAE.2018.8666834.

[48] Andryukhin, A. A. "Phishing Attacks and Preventions in Blockchain Based Projects." 2019 International Conference on Engineering Technologies and Computer Science (EnT), 2019, pp. 15–19. IEEE Xplore, https://doi.org/10.1109/EnT.2019.00008.

[49] Blancaflor, Eric, et al. "AI-Driven Phishing Detection: Combating Cyber Threats Through Homoglyph Recognition and User Awareness." Proceedings of the 2024 The 6th World Symposium on Software Engineering (WSSE), Association for Computing Machinery, 2024, pp. 226–31. ACM Digital Library, https://doi.org/10.1145/3698062.3698095.

[50] Camargo, Darcy, et al. "Mitigation of Liveness Attacks in DAG-Based Ledgers." 2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2023, pp. 1–9. IEEE Xplore, https://doi.org/10.1109/ICBC56567.2023.10174902.

[51] Natoli, Christopher, and Vincent Gramoli. "The Balance Attack or Why Forkable Blockchains Are Ill-Suited for Consortium." 2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2017, pp. 579–90. IEEE Xplore, https://doi.org/10.1109/DSN.2017.44.

[52] Chen, Guo, et al. "Parallel Execution of Blockchain Transactions with Sharding." ICC 2023 - IEEE International Conference on Communications, 2023, pp. 6559–64. IEEE Xplore, https://doi.org/10.1109/ICC45041.2023.10279242.

[53] Wang, Sheng-Wei. "Selfish Mining Attacks in Sharded Blockchains." 2024 International Conference on Computing, Networking and Communications (ICNC), 2024, pp. 106–10. IEEE Xplore, https://doi.org/10.1109/ICNC59896.2024.10556307.

[54] Wu, Yaqin, et al. "Hybrid Consensus Algorithm Optimization: A Mathematical Method Based on POS and PBFT and Its Application in Blockchain." Mathematical Problems in Engineering, vol. 2020, Apr. 2020, pp. 1–13. DOI.org (Crossref), https://doi.org/10.1155/2020/7270624.

[55] Bakar, Abdellatif, et al. "An Overview on Machine Learning Approach to Secure the Blockchain." Proceedings of the 6th International Conference on Big Data and Internet of Things, edited by Mohamed Lazaar et al., Springer International Publishing, 2023, pp. 486–500. Springer Link, https://doi.org/10.1007/978-3-031-28387-1_41.

[56] Ishmaev, Georgy. "Sovereignty, Privacy, and Ethics in Blockchain-Based Identity Management Systems." Ethics and Inf. Technol., vol. 23, no. 3, Sept. 2021, pp. 239–52. ACM Digital Library, https://doi.org/10.1007/s10676-020-09563-x.

[57] Biryukov, Alex, and Ivan Pustogarov. "Bitcoin over Tor Isn't a Good Idea." 2015 IEEE Symposium on Security and Privacy, 2015, pp. 122–34. IEEE Xplore, https://doi.org/10.1109/SP.2015.15.

[58] Kosba, Ahmed, et al. "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts." 2016 IEEE Symposium on Security and Privacy (SP), 2016, pp. 839–58. IEEE Xplore, https://doi.org/10.1109/SP.2016.55.

[59] Tran, Muoi, et al. "Obscuro: A Bitcoin Mixer Using Trusted Execution Environments." Proceedings of the 34th Annual Computer Security Applications Conference, Association for Computing Machinery, 2018, pp. 692–701. ACM Digital Library, https://doi.org/10.1145/3274694.3274750.

[60] Kerber, Thomas, et al. "Ouroboros Crypsinous: Privacy-Preserving Proof-of-Stake." 2019 IEEE Symposium on Security and Privacy (SP), 2019, pp. 157–74. IEEE Xplore, https://doi.org/10.1109/SP.2019.00063.

[61] Möser, Malte, et al. An Empirical Analysis of Traceability in the Monero Blockchain. arXiv:1704.04299, arXiv, 23 Apr. 2018. arXiv.org, https://doi.org/10.48550/arXiv.1704.04299.

[62] Buterin, Vitalik, et al. "Blockchain Privacy and Regulatory Compliance: Towards a Practical Equilibrium." Blockchain: Research and Applications, vol. 5, no. 1, Mar. 2024, p. 100176. ScienceDirect, https://doi.org/10.1016/j.bcra.2023.100176.

[63] Weber, Kristin, et al. "Exploiting the Human Factor: Social Engineering Attacks on Cryptocurrency Users." Learning and Collaboration Technologies. Human and Technology Ecosystems, edited by Panayiotis Zaphiris and Andri Ioannou, Springer International Publishing, 2020, pp. 650–68. Springer Link, https://doi.org/10.1007/978-3-030-50506-6_45.

[64] Barker, Elaine. Recommendation for Key Management: Part 1 – General. NIST Special Publication (SP) 800-57 Part 1 Rev. 5, National Institute of Standards and Technology, 4 May 2020. csrc.nist.gov, https://doi.org/10.6028/NIST.SP.800-57pt1r5.

[65] Mutual, Neptune. "What Is the ERC-1404 Token Standard?" Neptune Mutual, 17 Apr. 2024, https://medium.com/neptune-mutual/what-is-the-erc-1404-token-standard-a369c3bef4a2.

How to cite: E. Abedini, A. Jalaly Bidgoly, and M. Nickray
Blockchain Security: A Comparative Analysis of Threats and Countermeasure, Journal of Distributed Computing and Systems(JDCS), Vol 6, Issue 2, Page 39-52, 2024.

Ehsan Abedini is currently Ph.D. student in Department of Computer Engineering at the University of Qom. He received his M.Sc. degree in information technology engineering in 2016. His favorite research title includes computer networks and computer security.

Amir Jalaly Bidgoly received his M.Sc. degree in software engineering from the Iran University of Science and Technology (IUST) in 2009, and Ph.D. in software engineering from the University of Isfahan (Isfahan, Iran) in 2015. He is currently an Associate Professor with the Department of Computer Engineering at the University of Qom, Iran. His research interests include computer security and machine learning.

Mohsen Nickray received the BS.c., M.Sc., degree in computer engineering from Iran University of Science and Technology and University of Tehran in 2004, 2007, and Ph.D. degree computer architecture at University of Tehran respectively in 2012. Currently, he is an assistant professor in Department of Computer Engineering at the University of Qom, Iran. His recent research interests include resource management and task scheduling in Cloud and Fog computing.