Revisiting Blockchain Technologies and Smart Contracts Security: A Pragmatic Exploration of Vulnerabilities, Threats, and Challenges

ABSTRACT

Aim: This study aims to offer a comprehensive examination of the security vulnerabilities associated with blockchain technology, with the aim of identifying critical challenges and formulating strategic solutions to bolster system integrity and enhance user trust.
Methods: The study employs a combination of literature review and case study analysis to explore specific vulnerabilities such as re-entrance attacks, transaction malleability, and the risks associated with third-party integrations. Various recommendations are offered to address the outlined vulnerabilities in blockchains and smart contacts.
Conclusion: Securing blockchain platforms against emerging threats requires a multidisciplinary approach that encompasses technological innovation, stringent regulatory oversight, and comprehensive user education. It advocates for ongoing research and collaborative efforts to develop robust security measures that ensure the sustainable integration of blockchain technology into global digital infrastructures, thereby maximizing its transformative potential while minimizing associated risks. Enhancing the understanding of blockchain's security needs and continuously adapting to emerging threats are crucial for the technology's future resilience and widespread adoption.

Keywords: Blockchain, smart contracts, cryptocurrency, decentralization, immutable record, distributed ledger

1. INTRODUCTION

Blockchain technology (BT) is a decentralized digital ledger that records transactions across multiple computers in such a way that the registered transactions cannot be altered retroactively. This technology has been utilized in various digital currencies and can typically be to anything of value, like contracts, personal data, or property. BT is built on an append-only data structure where each block in the network contains a link (hash) to its predecessor, forming a continuous chain back to the genesis block [1]. This structure, alongside the replication of databases and execution of code across multiple nodes, enhances the security of blockchain systems. The decentralization and cryptographic hashing of blockchain technology ensure the authenticity of the record keeping, which inherently makes it significantly secure from falsified information and hacks [2]. The integrity and transparency of blockchain not only reduces fraud but also facilitate transactions and information exchange in a trustless environment. However, despite these robust security features, including the use of cryptographic techniques like hash functions, symmetric and asymmetric cryptography, and digital signatures, blockchains are not completely immune to security breaches. Both internal and external attackers can exploit various potential vulnerabilities, underscoring the need for continuous security assessments and enhancements. Thus, robust security measures and continuous vulnerability assessments is essential for maintaining trust and functionality.

On the other hand, smart contracts are self-executing contracts with the terms of the agreement between buyer and seller being directly executed via blockchain technology. The code and agreements therein exist across a distributed, decentralized blockchain network [3]. These contracts automatically execute transactions when predefined conditions are met, eliminating the need for third-party verification and streamlining processes. They permit trusted transactions and agreements to be carried out among disparate, anonymous parties without a central authority, legal system, or external enforcement mechanism [3]. While smart contracts facilitate both traditional applications and distributed data storage on blockchains, acting as autonomous agents in decentralized applications, they are not without risks. Smart contract vulnerabilities can lead to significant financial losses if exploited and unauthorized access to critical information, potentially undermining the integrity of entire blockchain networks. This highlights the crucial importance of rigorous security protocols to safeguard transactions and maintain the integrity and functionality of blockchain networks.

Research Problem

Despite the inherent security features of blockchain technology, it remains susceptible to a range of sophisticated vulnerabilities and attacks that can significantly compromise its integrity, reliability, and trustworthiness. These vulnerabilities encompass re-entrancy attacks, transaction malleability, and risks associated with third-party integrations, among others. As blockchain technology continues to gain traction across multiple industries, these security breaches can result in substantial financial losses, operational disruptions, and a severe erosion of user trust. Thus, there is a pressing need to systematically identify, analyze, and address these vulnerabilities through a comprehensive and multidisciplinary approach.

Aim of the Study

This study aims to thoroughly examine and analyze the security vulnerabilities inherent in blockchain technology and smart contacts and evaluate the associated risks that these vulnerabilities pose to various applications of blockchain across multiple industries. Afterward, the study proposes comprehensive strategies and best practices to mitigate these risks, focusing on enhancing the security, reliability, and overall trustworthiness of blockchain systems, ensuring their safe integration into business processes and effective operation in environments demanding high security and privacy standards.

Scope of the Study

This research focuses on identifying and analyzing key security vulnerabilities in blockchain technology and smart contracts, assessing their impact on various blockchain applications, and proposing comprehensive strategies and best practices for mitigating these risks. The study encompasses both technical and regulatory aspects, aiming to provide a holistic framework for enhancing blockchain security.

2. CASE STUDY: RECENT BREACHES AND IMPLICATIONS

The DAO hack in 2016 exposed vulnerabilities in Ethereum's smart contracts, resulting in a loss of $50 million, while the Parity Wallet hack in 2017 saw over $150 million in Ether frozen due to a bug in a smart contract library [4,5]. During Ethereum DAO, an external contract was called back into the DAO contract before the first transaction was completed, leading to multiple withdrawals and a significant loss of funds. This attack not only caused a substantial financial loss—3.6 million ETH, valued at approximately $50 million at the time—but also had profound implications on the Ethereum blockchain, leading to a drastic drop in the price of ether and eventually resulting in the split of Ethereum into Ethereum and Ethereum Classic [25, 41]. A 51% attack on Ethereum remains an ongoing concern, where an attacker could rent computational power to potentially take over the network, posing a significant financial threat given Ethereum's substantial valuation [7].

Snegireva et al. highlighted nearly 200 weaknesses in blockchain systems identified by CloudSecurityAlliance, half of which are unique to blockchain systems compared to other public databases [8]. These vulnerabilities extend to various blockchain systems, including issues related to Ethereum's ethash mining, DDoS attacks, and flaws in the Ethereum virtual machine and Hyperledger's transaction and block signature validation [8]. Additionally, the CVE-2010-5139 bug in Bitcoin created about 184 billion bitcoins due to an integer overflow error, further demonstrating the critical nature of these security flaws [8,9]. Over 70% of the transactions on the Bitcoin network were controlled by just four Chinese companies as of April 2016, indicating the vulnerability of well-established cryptocurrencies like Bitcoin to the 51% attack [10].

On the smart contract front, Prasad et al. detail notorious attacks such as DAO, Govern Mental, and Parity Multisig, with a special focus on the Rubixi smart contract, which was exploited due to a change in the contract name that did not correspond with changes in the constructor name, leading to a permanence bug that facilitated the theft of substantial amounts [13]. Further, the significant impact of the DAO attack is notable, as it compromised 40.01% of the $150 million managed by the DAO and led to a loss of $50 million [14, 15]. Between 2016 and 2018, millions of dollars in assets held by smart contracts were stolen or frozen due to attacks such as the DAO attack, Parity Multi-Sig Wallet attack, and integer underflow/overflow attacks, attributing these incidents to technical flaws in software design and implementation [16]. These examples underscore the ongoing and evolving threat landscape in blockchain technology and emphasize the need to develop robust security measures to protect against known and emerging vulnerabilities.

The numerous high-profile security breaches have underpinned the need for robust security protocols and continuous improvement. Blockchain systems are susceptible to various attacks, including those targeting the consensus algorithm, flaws in smart contract programming languages, and vulnerabilities in the blockchain framework itself, which can lead to potential operational security breaches such as private key or host system compromises [6]. A significant challenge is the lack of dedicated Security Information and Event Management (SIEM) systems for permissioned blockchains, which hampers the ability to monitor and respond to threats effectively due to the complexity of blockchain nodes [6]. Similarly, the attack areas of blockchain can be categorized into three main areas: cryptographic constructs, the distributed architecture of systems, and the application context of blockchain technology [11]. Yi et al. present a comprehensive dataset of 1,037 vulnerabilities and their 2,317 patches, highlighting that a significant portion of these vulnerabilities were traditional in nature, thus indicating that blockchain systems are not immune to conventional security threats. They also developed 21 distinct blockchain-specific vulnerability patterns, which are crucial for identifying and mitigating similar threats on other blockchain platforms like Dogecoin, Bitcoin SV, and Zcash [12].

Each vulnerability presents unique challenges and risks, necessitating a comprehensive approach to identifying and mitigating potential threats in Ethereum-based smart contracts. Current research has only covered a few of the flaws, and there is a need to address as many vulnerabilities as possible in both smart contracts, in particular, and blockchain, in general.

2. BLOCKCHAIN VULNERABILITIES AND THREATS

2.1 Overview

The various security vulnerabilities present significant risks to the technology and its users. Data privacy breaches threaten the confidentiality and integrity of data as they traverse multiple network hops, alongside the susceptibility of IoT devices to attacks such as denial-of-service, jamming, Sybil, and replay attacks, significantly hamper IoT service functionality [17]. These IoT devices are particularly vulnerable due to their limited computational, storage, and network capacities compared to more robust systems like smartphones or computers.

The challenge of maintaining security grows as blockchain systems scale up in user numbers and services. This scalability-security trade-off often leads to vulnerabilities such as the draining of funds, execution inconsistencies, locked funds, transaction manipulation, and programming errors exploitable by attackers [18]. The security of blockchain hinges on the robustness of its software and hardware implementations, protocols, and consensus mechanisms, which paradoxically become targets for attacks [19]. The immutable nature of blockchain also complicates matters, as illicit blocks, once added, persist indefinitely, posing ongoing challenges to the integrity of the system.

Consensus delays due to DDoS attacks, selfish mining, orphaned blocks, and double-spending attacks have also become common in blockchain technology [20]. There also exist risks associated with the concentration of network processing power in single regions, which can lead to collusion and threaten the democratic nature of blockchains [21]. Moreover, the open-source nature of blockchain can be exploited through zero-day or time-jacking attacks, where attackers manipulate the blockchain's timestamp to create forks for double-spending [21].

The role of administrators as potential single points of failure due to their ability to manipulate the configuration of blockchain peers and initiate updates for smart contracts is particularly concerning, as it can introduce new vulnerabilities or backdoors [6]. Many vulnerabilities in blockchain stem from coding errors, stressing the importance of thorough testing in identifying and mitigating potential security risks [8]. Brute-force attacks are also significant threats that aim to overpower the network to alter transaction history, as well as Balance and Goldfinger attacks, where the attacker manipulates or seeks to destabilize the blockchain for financial gain or to disrupt the system [35]. In the Goldfinger attack, the goal is to destabilize the blockchain without direct financial gain, highlighting the existential threats that such motivations pose to blockchain stability across different consensus mechanisms.

These issues highlight the difficulties in maintaining the integrity and reliability of blockchain systems as they expand. The threat model for blockchain systems includes a variety of actors such as transactors, peer orderers, and certificate authority administrators, each capable of posing threats either as malicious insiders or external attackers.

2.2 Proof of Work Vulnerability & 51% Attack

While foundational to many blockchain networks, the Proof of Work (PoW) consensus mechanism presents significant vulnerabilities, particularly the risk of a 51% attack. This attack occurs when a single entity or a group gains control of more than 50% of the network's hashing power, enabling them to manipulate transaction verifications and potentially introduce fraudulent actions such as double-spending. PoW architectures are decentralized and facilitate transparency, reducing double spending risks under normal circumstances [22].

The potential for a 51% attack remains a critical vulnerability in blockchain systems, as miners with the majority of the network's power can alter transaction data, reverse transactions, and disrupt the validation process [18, 23, 24, 25]. For instance, attackers can exclude or modify the order of transactions, hamper other miners' operations, and impede the confirmation of legitimate transactions [24]. The risk is heightened in networks where hashing power is concentrated, as demonstrated when the mining pool ghash.io neared this majority threshold, sparking widespread concern within the Bitcoin community. The formal verification of consensus mechanisms has been suggested as a prevention technique to identify and mitigate these vulnerabilities.

The implications of a 51% attack extend beyond mere transactional integrity. Such an attack can undermine the democratic nature of decentralized networks by allowing attackers to reject valid blocks, introduce malicious ones, and execute double-spending [26]. These attacks challenge the integrity and reliability of blockchain systems; as such, no single miner or pool should control more than half the network's hash rate [20,27]. Moreover, the energy

consumption associated with maintaining PoW mechanisms is another significant concern. The energy demands are so substantial that they are comparable to those of a small country, which raises sustainability concerns [28]. This high energy consumption, combined with slow processing speeds exacerbated by the increasing number of network participants, presents further challenges to public blockchains [29].

The majority of attacks can even allow attackers to rewrite almost the entire transaction history of a blockchain, thereby indicating the profound impact such attacks could have on the historical integrity of blockchain records [19]. Collusion, which was once considered unlikely, has emerged as a realistic threat due to the potential manipulation of network operations by those controlling significant hashing power [10, 30]. Advancements in quantum computing severely threaten the cryptographic algorithms used in blockchain. Quantum algorithms could potentially break the cryptographic backbone of blockchain, enabling attackers to forge digital signatures and compromise user privacy [31, 32].

This evolving nature of the 51% attack shows the urgency of developing more robust security measures and exploring alternative consensus mechanisms, such as Proof of Stake (PoS), which might offer lower risks of 51%-type attacks and reduce energy consumption, aligning with broader environmental sustainability goals. The 51% attack represents one of the most severe vulnerabilities in blockchain networks that utilize the Proof of Work (PoW) consensus mechanism. This attack allows malicious actors who control the majority of the network's hashing power to alter the blockchain's integrity by enabling transaction reversals, double-spending, and the introduction of fraudulent blocks.

Such dominance not only undermines the decentralization and security that blockchains are designed to offer but also poses significant risks to the transactional and historical accuracy of these systems. The potential for these attacks is exacerbated by the concentration of mining power and the substantial energy demands associated with PoW systems. As blockchain technology continues to evolve, addressing these vulnerabilities through enhanced security measures, consensus mechanism innovations, and integrating quantum-resistant cryptographic solutions will be crucial for maintaining trust and functionality in blockchain networks.

2.3 Double Spending Attacks

Double spending is a significant security risk in blockchain systems, exploiting the time it takes for transactions to be confirmed to make multiple uses of the same digital assets. In blockchain, particularly Bitcoin, transactions require about 10 minutes to confirm [22]. During this window, an attacker can issue two transactions using the same inputs but directing them to different recipients [22]. The network typically confirms only the first transaction it receives, enabling attackers to manipulate transaction timing to their advantage.

Double-spending can occur in various ways, such as Race attacks, where an attacker sends two conflicting transactions in quick succession; Finney attacks, which involve pre-mining a transaction into a block and then spending the same coins before releasing the block; and Vector76 attacks, combining elements of Race and Finney attacks [27]. The PoW vulnerability makes blockchains prone to 'Race Attacks,' where an attacker could make a payment to a merchant and simultaneously send a conflicting transaction into the network [33, 34]. The network might validate the latter, leading to the merchant not receiving the payment despite delivering the service or product.

The issue of double spending represents a fundamental challenge to the security and reliability of blockchain transactions, particularly in systems based on the Proof of Work consensus mechanism. The ability of attackers to exploit the confirmation times of transactions to conduct fraudulent activities highlights a critical vulnerability within blockchain architectures. Effective mitigation requires a combination of technological enhancements, such as improved detection methods and modifications to consensus protocols, alongside strategic network practices,

including waiting for multiple confirmations and implementing alert systems. As blockchain technology continues to evolve and expand into various sectors, addressing the risk of double spending is crucial for maintaining trust in digital transactions and ensuring blockchain networks' long-term stability and security.

2.4 Selfish Mining Attacks

Selfish mining attacks represent a subtle yet potent threat to blockchain networks, particularly those employing a Proof-of-work consensus mechanism. In a selfish mining strategy, malicious miners withhold newly mined blocks instead of broadcasting them to the network. They continue to mine secretly on their private blockchain branch, revealing it only once it becomes longer than the public chain. This deceptive tactic allows them to replace the existing public chain with their version, thereby claiming a disproportionate share of mining rewards and potentially invalidating the legitimate mining efforts of others [19].

The implications of selfish mining extend beyond mere economic gains for the attackers. By disrupting the blockchain's normal operation, selfish miners can erode trust in the system's fairness and security. This can lead to centralization tendencies within the network, as fewer miners control more of the computational power, thereby contradicting one of the foundational principles of blockchain technology: decentralization. Addressing selfish mining is crucial for maintaining the integrity and robustness of blockchain networks. Ensuring that no single group can disproportionately influence the blockchain or its rewards system is essential for preserving the decentralized, democratic ethos that makes blockchain technology uniquely valuable and transformative.

2.5 Network Traffic Attacks

Network traffic attacks, particularly Distributed Denial of Service (DDoS), pose a significant threat to the stability and functionality of blockchain networks. These attacks involve flooding the network with overwhelming traffic, which can overload the system and cause legitimate transactions to fail. This method is used not only to disrupt the normal operation of the network but also as a competitive tactic among miners. Mining pools might launch DDoS attacks against rival pools to eliminate competition and gain a larger share of mining rewards [36]. Despite blockchain's decentralized architecture, which typically provides higher security against many forms of cyber-attacks, it is not immune to network-based threats. The decentralized nature of blockchain makes a DDoS attack more challenging to execute, as there is no single point of failure. However, specific blockchain components, such as mining pools and individual nodes, can still be targeted, making them vulnerable to such attacks [30].

Other network traffic attacks, like DNS attacks and mempool attacks, also present substantial risks. Attackers can exploit these vulnerabilities by flooding blocks with transactions [29]. This attack can congest the network and, in severe cases, allow attackers to gain majority control if they can manipulate the transaction flow effectively. This can lead to a disruption in the processing of transactions and potentially compromise the integrity of the blockchain.

The threat of network traffic attacks underscores the need for continuous improvements in blockchain security protocols. Enhancing the resilience of blockchain networks against such attacks involves strengthening the infrastructure, implementing more robust consensus mechanisms to handle unexpected surges in network load, and deploying preventive measures such as rate limiting or transaction scrutiny to mitigate the effects of these aggressive strategies. Protecting blockchain from these vulnerabilities is crucial for maintaining its reliability and trustworthiness as a digital transaction platform.

2.6 Eclipse Attack.

Eclipse attacks represent a sophisticated network security threat within blockchain systems, specifically targeting the network connectivity of individual nodes. An attacker can filter and

manipulate the victim's view of the blockchain by isolating a node from the rest of the network and monopolizing its network connections. This effectively "eclipses" them from the rest of the network and facilitates other malicious activities, such as double spending and selfish mining. This deprivation of accurate, decentralized network information significantly undermines the integrity and functionality of blockchain systems, and studies have shown the feasibility of such attacks in both Bitcoin and Ethereum networks [33].

In the context of Ethereum-based networks, eclipse attacks can be particularly detrimental as an attacker can exploit the synchronization process of a node [23]. When a node encounters a block with a higher difficulty level than its current total, it attempts to synchronize with the sender of that block. By initiating a synchronization attack, an attacker can prevent the node from properly syncing with the blockchain, thereby isolating it and keeping it in a state of misinformation and vulnerability for as long as the attack persists.

The eclipse attacks can be part of broader network threats such as Sybil attacks, where attackers create multiple false identities to saturate the network with malicious nodes [30]. These deceptive strategies isolate a node and monopolize its inputs and outputs within the network, further compounding the potential for fraud and manipulation within blockchain transactions. Alongside other network disruptions like partitioning attacks, which involve isolating a subset of nodes, eclipse threats can lead to severe consequences such as double spending, de-anonymization of users, and general disruption of the blockchain's operations [36]. Additional vulnerabilities, such as packet sniffing and delay or tampering attacks, also compromise the integrity and functionality of the network by manipulating the data transmitted between nodes.

The eclipse attacks within blockchain networks underscore the need for robust network security measures. Protecting against such attacks requires enhanced network monitoring, rigorous node verification processes to prevent the formation of malicious connections, and the implementation of countermeasures that ensure redundancy and diversity in peer connections. These strategies are essential to maintaining blockchain networks' decentralized integrity and security, safeguarding them against direct and indirect network threats.

2.7 Blockchain Forking

Blockchain forking is the process where a blockchain splits into two separate chains due to changes in its protocol or disagreement among participants. Forks can happen for various reasons, such as protocol upgrades or community disagreements, and they have significant implications for the network's stability and governance. Forking represents a pivotal challenge and risk within decentralized networks, as highlighted by several researchers who delve into the technical aspects and the broader implications of such events. Systems like Bitcoin are vulnerable to speculation and misinformation due to the absence of a central coordinating entity [37]. This decentralization, while fostering innovation and adaptability, also makes the system prone to instability during events such as development forks. These forks can create confusion and uncertainty among users, which in turn impacts the trust and reliability of the blockchain [37]. Thus, the decentralized nature of blockchain is a double-edged sword that presents both strengths and weaknesses, demonstrating the complex dynamics at play in blockchain-based payment platforms.

There are two main types of forks: soft forks and hard forks. Hard forks occur when the blockchain diverges into two separate and incompatible chains, creating two distinct blockchains [26]. Soft forks, in contrast, also involve a split but are designed such that only one chain is eventually continued by the majority of nodes [26]. Forks can be triggered by various factors, including network upgrades or malfunctions, and create inconsistent states within the network. Adversaries can exploit these inconsistencies to conduct fraudulent transactions or sow distrust among users, thereby undermining the blockchain's integrity.

These insights underpin the need for a balanced approach to managing blockchain technology. While forks can introduce vulnerabilities and uncertainties, understanding their dynamics and preparing with appropriate technical strategies can significantly enhance the security and stability of blockchain networks. These findings emphasize the importance of continuous research and development to mitigate the risks associated with blockchain forking, thereby ensuring the technology's long-term viability and reliability.

2.8 Deanonymization and Transaction Pattern Linkability

The perceived anonymity and privacy of blockchain transactions are often overstated, posing significant risks due to various deanonymization techniques and transaction pattern linkability. Network analysis, for instance, can reveal user identities by studying the flow of data within the transaction network [38]. Each transaction node and their data connections can be analyzed to trace back to the individuals involved [38]. Address clustering, another common method, groups multiple addresses believed to be controlled by the same entity, potentially exposing the activities and identities of involved parties. This clustering can inadvertently reveal sensitive information useful for market research or law enforcement.

There are various risks associated with transaction pattern linkability, where analyzing transaction flows and patterns on the public blockchain network can reveal statistical data about cryptocurrency distributions and regulations [38]. Techniques like transaction graph analysis can achieve high accuracy in unmasking user identities. Even web-based cryptocurrency payments are not entirely secure, as consumer identities can potentially be linked to real identities through browser cookies, undermining privacy measures like CoinJoin. Further, wallet owners sometimes voluntarily disclose their identities for legitimate reasons, such as fundraising by charities or political groups [10]. However, this practice also has a darker aspect, as evidenced by ransomware attackers who provide Bitcoin addresses for victims to send payments, demonstrating how blockchain's transparency can be exploited maliciously.

Moreover, the identity of a wallet owner can sometimes be deduced from collateral information like a signed blog post [10]. While knowing a public address does not directly lead to fund theft, it allows attackers to observe and analyze the transaction network of the address owner. This surveillance can disclose not just personal transactions but also sensitive business dealings, highlighting the security risks associated with the transparency of blockchain transactions.

2.9 Transaction Malleability

Transaction malleability represents a notable vulnerability within the Bitcoin network, highlighting inherent weaknesses in the protocol's design that attackers can exploit. It involves adversaries altering an unconfirmed transaction's hash ID [34]. By doing so, they can deceive the transaction sender into believing the transaction has failed. Misled by this false failure, the sender might initiate the transaction again, potentially leading to a situation where the adversary can exploit this confusion to their advantage [34]. This attack does not involve direct control over the transaction issuing process but exploits the malleability of transaction IDs to achieve similar outcomes as double-spending. Transaction malleability is thus a critical area of concern that necessitates continuous improvement and adaptation of blockchain protocols to safeguard against evolving network threats and ensure the reliability and security of cryptocurrency transactions.

2.10 RFID & QR Code Vulnerability

The vulnerabilities associated with RFID and QR code technologies, particularly in the context of blockchain and cryptocurrency transactions, pose significant security risks. Scammers often exploit the convenience of QR codes, commonly used to represent complex Bitcoin addresses [39]. Fraudulent QR code generators can deceive users by substituting legitimate Bitcoin

addresses with those controlled by attackers. When scanned during transactions, these QR codes direct funds to the attacker's address instead of the intended recipient. Sophisticated scammers might even design these QR codes to partially mimic legitimate addresses or temporarily display the correct address during verification attempts, making them appear trustworthy and increasing the likelihood of successful fraud. This type of scam can be particularly effective at cryptocurrency ATMs, where users might quickly scan a QR code, unwittingly sending their funds to a scammer.

Further, attackers can embed malicious QR codes in emails that impersonate legitimate cryptocurrency services [39]. These emails might alert recipients to unauthorized access attempts and prompt them to scan a QR code to "verify" or "secure" their account. However, this scan leads the victim to a fraudulent website where their wallet credentials are stolen, facilitating identity theft [39]. Fraudsters may also place double-sided stickers with their QR codes over genuine ATM QR scanners. Unsuspecting users scanning these tampered QR codes inadvertently send money directly to the fraudsters' wallets.

On the RFID front, the 'Hilt Shao attack' occurs during the initial phases of product registration with RFID tags. This attack involves cloning an RFID tag, altering its data, and then writing this false information to the blockchain [40]. Such actions can compromise data integrity within the supply chain, misleading the tracking and verification processes integral to food production and distribution industries. The ease with which RFID tags can be cloned and manipulated poses a severe risk, potentially allowing malicious actors to alter or fabricate data on the blockchain, thus undermining the entire system's security and reliability.

These vulnerabilities show the need for stringent security measures and robust verification processes to safeguard against these sophisticated types of fraud and attacks. Enhancing the security protocols surrounding QR code generation and RFID tag handling and educating users about potential scams are crucial steps in mitigating these risks and ensuring the integrity of transactions and supply chain information in blockchain applications.

3.0 SMART CONTRACTS DESIGN VULNERABILITIES

3.1 Overview

Smart contracts, which run on blockchain technology, represent a significant advancement in executing decentralized transactions and automated business processes. These contracts, written in code and stored on the blockchain, are used in various applications across industries such as finance, voting, digital rights, escrow, healthcare, IoT, and e-governance. The decentralized nature of blockchain allows smart contracts to operate independently of central authorities, providing a robust platform for executing and enforcing contract terms directly between parties.

However, the design and implementation of smart contracts are not without significant vulnerabilities. Since smart contracts are code-based and stored on an immutable blockchain, any errors in their development are permanently recorded and cannot be easily corrected. This immutability means that even minor bugs or oversights can lead to serious consequences, such as unauthorized actions or access, loss of funds, or other security breaches.

Flaws in smart contract design have led to severe financial damages. Notably, errors in a multi-signature contract resulted in the theft of 150,000 ethers, underscoring the financial risks [8]. Additionally, mistakes in a digital wallet service led to the accidental destruction of funds, illustrating how design flaws can lead to financial loss and irreversible damage to user trust and system integrity [8]. These vulnerabilities become especially critical because smart contracts often handle significant financial transactions and sensitive data.

3.2 External Calls & Gasless Send

Interaction with external systems introduces several key vulnerabilities that must be carefully addressed to maintain system integrity and security. In external calls in smart contracts, contracts interacting with external functions can inadvertently execute malicious code present in these functions [41]. Compounding these risks is the gasless send vulnerability, part of Ethereum's model. In Ethereum, transactions and dependent function calls require a certain amount of "gas" to execute, with insufficient gas leading to an out-of-gas exception [41]. Importantly, the spent gas is not reimbursed, posing a risk of financial losses, particularly when contracts interact with external contracts that may consume more gas than anticipated, as well as DoS attacks targeting block gas limits [8].

These insights underpin the intricate and high-risk nature of designing and implementing smart contracts on blockchain platforms. Developers must employ a comprehensive security strategy that includes diligent testing, adherence to established best practices and staying informed about the latest security advancements. This proactive approach is crucial for safeguarding smart contracts against a broad spectrum of known and emerging threats, ensuring their reliable and secure operation within the blockchain ecosystem.

3.3 Unhandled Exceptions & Transaction-ordering Dependence

Vulnerabilities such as unhandled exceptions and transaction-ordering dependence present significant challenges, particularly in smaller blockchain systems and decentralized applications (DApps). These vulnerabilities commonly manifest as coding errors that might result in infinite loops during transaction deployment. These flaws not only degrade the performance but can also be exploited by attackers to severely compromise the security of the entire blockchain system [23].

Mishandled exceptions, which often occur when different smart contracts interact, can lead to unhandled errors that disrupt the normal functioning of smart contracts [24]. These exceptions, if not properly managed, can halt the execution of contracts or lead to incorrect processing of transactions. Additionally, the reentrancy vulnerability is highlighted, where an attacker can make repeated calls to a smart contract, exploiting the contract's state before the initial transaction is finalized, potentially leading to unauthorized actions like the theft of Ether.

Transaction-ordering dependence, such as timestamp dependence vulnerability, arises from the fact that the execution order of transactions can affect the final state of the smart contract. Such dependencies can lead to unpredictable outcomes if the order of transactions is altered, whether intentionally by malicious actors or unintentionally due to network behaviors [24]. Smart contracts that rely on timestamps are particularly vulnerable because miners, who include transactions in blocks, can manipulate these timestamps to influence contract outcomes. This manipulation can lead to significant security breaches, especially in contracts that execute or validate actions based on specific times

3.4 Re-entrancy

Re-entrancy attacks pose a significant threat within the blockchain ecosystem, particularly in the context of smart contracts. This vulnerability is exploited when a contract function designated to transfer funds, such as a withdrawal function, calls an external, untrusted contract. Suppose the initial contract fails to update its internal state before making this external call. In that case, it can be manipulated to repeatedly execute the withdrawal, allowing funds to be withdrawn multiple times.

Further, re-entrancy can initiate new calls back to the calling contract before the initial execution is completed [14]. This can lead to unexpected behaviors that could, for instance, drain funds from the contract. They also highlight the risks of using **tx.origin** for authentication, unchecked external calls, and the implications of choosing **send()** over **transfer()** for transferring Ether [14]. The choice between **send()** and **transfer()** is particularly critical

because **send()** does not raise an exception on failure, which can lead to unverified transaction outcomes and potential financial losses.

The re-entrancy problems are a particular issue within Ethereum and Solidity, where the same function can be maliciously invoked multiple times [16]. Similarly, the critical nature of such vulnerabilities is notable, which include not only re-entrancy but also issues arising from external contracts using **tx.origin**, unchecked external calls, and the inappropriate use of **send()** instead of **transfer()** [14]. These functions, when misused, can further exacerbate the security risks associated with smart contracts.

3.5 Modular & Functional Problems

The modular and functional aspects present distinct vulnerabilities that can significantly impact the system's security and operational efficiency. The consensus module is a critical component of blockchain systems tasked with validating and adding new transactions or blocks to the blockchain [12]. With 265 identified vulnerabilities, this module demonstrates the substantial security risks inherent in the core mechanisms that govern blockchain operations [12]. This high number of vulnerabilities underscores the need for rigorous security measures and constant vigilance to ensure the integrity and functionality of the consensus process.

Further, the wallet and networking modules, which are fundamental to handling transactions and facilitating peer-to-peer communications, also show a high incidence of security flaws [12]. These modules are essential for transaction processing, data storage, and overall network communication within blockchain systems. The prevalent vulnerabilities in these areas indicate that critical aspects of blockchain functionality are susceptible to various security risks, necessitating dedicated efforts to enhance security protocols and mitigate potential threats.

Functional issues in blockchain systems can include problems like integer division errors, issues with locked money (where funds become inaccessible), integer overflow and underflow, dependencies on timestamps that can be manipulated, and unsafe type interfaces [12]. These issues complicate the execution and reliability of smart contracts and other blockchain functionalities, potentially leading to erroneous operations or security breaches.

From a developmental perspective, various issues can arise during the development phase of blockchain applications. These include violations of token APIs, inappropriate use of the private modifier, not fixing compiler versions, style guide violations, redundant fallback functions, and implicit visibility levels [14]. Each of these developmental issues can introduce vulnerabilities into the system, compromising the security and effectiveness of the blockchain application.

Operational issues further complicate the blockchain ecosystem, with vulnerabilities such as those related to handling byte arrays and costly loops in smart contracts [14]. These vulnerabilities can lead to performance inefficiencies and increased costs due to excessive computational needs, which might make blockchain operations economically unsustainable in certain contexts.

4.0 EXTERNAL CHALLENGES AND CONCERNS

4.1 Overview

A broad spectrum of challenges stems from the technology's inherent characteristics and the external environment in which it operates. Key issues such as interoperability difficulties with legacy systems, the need for improved privacy measures against potential leaks, and the continuous evolution of technology that may render existing blockchain solutions obsolete are critical concerns that need addressing. Moreover, the dependence on third-party vendors for blockchain implementations introduces additional risks, necessitating rigorous scrutiny and ongoing management to safeguard against potential breaches and failures.

Interoperability issues particularly underscore the complexity of integrating blockchain with diverse business processes and legacy systems, which often involves navigating technical discrepancies and compatibility problems. The seamless interaction of blockchain systems with existing ERP systems and traditional databases is crucial for achieving comprehensive digital transformation but is fraught with challenges that impede smooth integration. Auditors and IT professionals play a pivotal role in evaluating and ensuring that blockchain solutions are technically sound and align with organizational strategies and compliance requirements.

Further, the rapid pace of advancements in fields like quantum computing poses a significant threat to the security of current blockchain infrastructures. This technological evolution could potentially compromise the cryptographic foundations of existing blockchain networks, highlighting the need for proactive and adaptive security strategies that can respond to these advancements. Continuous research and development efforts are essential to stay ahead of potential vulnerabilities and ensure blockchain technologies' longevity and reliability.

4.2 Anonymity, Transparency & Privacy Concerns

Blockchain technology offers a degree of anonymity but fails to provide complete privacy protection, revealing inherent tensions between anonymity, transparency, and privacy. The public nature of blockchain means that transactions can leave traceable clues that potentially expose user identities. This traceability can occur through linking transactions to IP addresses or third-party applications that profile and track user data. Although various schemes have been proposed to enhance anonymity, the challenge remains in securing trading platforms and other third-party software that manage identities and cryptographic keys [19].

Despite the pseudo-anonymous nature of blockchain transactions, there is still a possibility of tracing transactions back to individual users through transaction graphs and related data [28]. This traceability may pose a greater risk to user privacy than traditional financial systems like credit cards, which typically provide more direct protections for user identity [28]. While blockchain transactions do not directly reveal identities, analyzing transaction graphs, especially in networks like Bitcoin, can sometimes link real identities to transaction activities [31]. This weak anonymity is compounded by user ignorance, as many individuals do not fully understand how to preserve their privacy within the blockchain environment or overestimate their anonymity.

4.3 Storage Constraints

As blockchain networks expand, particularly with the integration of IoT devices, storage constraints emerge as a significant challenge, potentially impacting the efficiency and scalability of these systems. Each node in a blockchain network is required to store the entire history of transactions [28]. The blockchain's immutable nature means that once data is added to the network, it cannot be altered or deleted, raising issues such as compliance with privacy regulations like the GDPR, which includes provisions like the right to be forgotten [44]. This requirement means that as the data volume grows, each node's storage demands increase correspondingly. Such growth can strain transaction times and may disproportionately affect nodes with limited storage capacity, potentially leading to network performance bottlenecks. These insights highlight a critical tension in blockchain development: the need to balance expansive data storage for transparency and immutability with transaction processing efficiency and compliance with evolving privacy norms [28,44].

4.4 Scalability

The inherent technical limitations in transaction performance and the slow block formation process hinder blockchain's efficiency. Scalability issues arise from the limited capacity of blockchain networks to process transactions rapidly [29]. The blockchain inherently faces a trade-off between maintaining robust security through intensive computational processes and achieving high transaction throughput. In certain blockchain implementations, transactions

can take up to 8 minutes to complete, with the network supporting only 2-3 transactions per second [28]. Such high latency and low throughput significantly impair the practicality of blockchain for applications that require quick transaction processing, such as financial services or real-time data management. This limitation is a significant bottleneck, particularly in systems that cannot compromise on security for performance.

4.5 Interoperability with Legacy Systems and Third-Party Vendor Risks

Integration with other systems is crucial for ensuring that blockchain technology does not operate in isolation but rather enhances and works alongside existing infrastructures to improve efficiency and transparency in business ecosystems. Interoperability challenges arise from the necessity for blockchain systems to seamlessly integrate with a variety of external systems. These include diverse business processes, legacy systems, traditional databases, and various modules of enterprise resource planning (ERP) systems [45]. The ability to interact with these systems without disruption is vital for blockchain to deliver its full potential, enabling enhanced data sharing, streamlined operations, and more robust security measures. However, achieving this level of integration is complex due to the differences in data structures, communication protocols, and security standards between blockchain technology and existing systems.

The risks associated with third-party vendor integrations further complicate the problem. Dependence on third-party applications for blockchain implementations introduces potential vulnerabilities, as these vendors might not adhere to the same rigorous security and operational standards as the blockchain system itself [45]. This can lead to data inconsistency, security breaches, and performance issues, which undermine the integrity and reliability of the blockchain network. Moreover, any weaknesses in third-party systems can directly and detrimentally impact the client's blockchain integrity. Additionally, the integration of blockchain with legacy systems presents its own set of risks. Legacy systems often use outdated architectures and proprietary data formats that are not directly compatible with modern blockchain frameworks [[46]. This incompatibility can result in significant data transformation issues, requiring extensive middleware solutions to bridge the gap. Furthermore, the security protocols in legacy systems might be obsolete, failing to meet the advanced cryptographic standards of blockchain technology, which could expose the entire network to vulnerabilities. Performance bottlenecks are another critical risk, as legacy systems may struggle to handle the high transaction throughput typical of blockchain operations, leading to delays and inefficiencies [46].

4.6 Private Key/Wallet Theft

The security of private keys and the potential for wallet theft are critical vulnerabilities in blockchains, posing serious risks to the integrity and privacy of user transactions. Private key security is vital, as these keys are instrumental in authenticating user transactions within the blockchain [36]. Wallet theft is identified as a high-likelihood risk with moderate impact, originating from various threats such as system hacking, software bugs, or malware. Further, the "Man-in-the-Middle" (Address Attack) risk, where an attacker alters the recipient's address during a transaction, also presents a high likelihood and moderate impact. Vulnerabilities in the cryptography used in blockchain, such as the Elliptic Curve Digital Signature Algorithm (ECDSA), though less likely, could have a high impact if exploited [36]. The potential for "Criminal Smart Contracts" in blockchain 2.0 could also facilitate illicit activities, posing high risks in terms of likelihood and impact.

Private keys authenticate transactions and control access to a participant’s assets [38]. Compromising these keys can result in severe privacy leaks and identity theft. Despite the control they provide over assets, securing and managing these keys rests solely with the user, underscoring a significant point of vulnerability [38]. The absence of efficient key recovery mechanisms in the event of loss further compounds this risk, highlighting an urgent need for

robust key management systems and recovery mechanisms within blockchain frameworks. address this vulnerability to enhance security and trust in blockchain systems.

4.7 Societal and Organizational Barriers

Integrating blockchain technology into societal structures and organizations faces several barriers, ranging from societal acceptance to regulatory and interoperability challenges. Various social threats exist, such as the resistance to the decentralization of sensitive information, exemplified by medical data, where privacy concerns are paramount [29]. The shift from traditional, trusted third parties to decentralized models can provoke skepticism and opposition due to perceived privacy and data security risks. Additionally, the lack of governance regulations and guidelines further complicates the adoption of blockchain within critical sectors like healthcare. This regulatory vacuum can stall the implementation and scaling of blockchain applications due to uncertainties about compliance and legal responsibilities [29].

On the organizational front, several obstacles impede the effective deployment of blockchain technology. Issues such as interoperability are significant where there is a pressing need for a seamless exchange of information between different organizations and systems [29]. However, achieving this is often hindered by limited trust among stakeholders and the absence of open standards that facilitate such integration [29]. Furthermore, the financial implications of adopting blockchain, such as high initial installation costs and ongoing transaction fees, pose additional burdens that can deter organizations from adopting this technology.

Without clear regulatory processes and strategic frameworks for blockchain, systems represent a critical systemic challenge [28]. For blockchain technology to gain broader acceptance and to function effectively across various domains, it is imperative to establish robust standards and governance mechanisms. These frameworks should address various issues, from security vulnerabilities and legal compliance to ensuring interoperability among disparate blockchain systems. Developing these regulatory processes and standards is essential not only for enhancing the security and functionality of blockchain applications but also for instilling confidence among users and stakeholders about the technology's reliability and legal standing

5. RECOMMENDATIONS

Addressing blockchain technology's myriad security vulnerabilities and concerns requires a multifaceted approach, emphasizing best practices, specialized methodologies, and innovative technological solutions.

1. Improving smart contract design by allowing re-addressability of other smart contracts' code used as libraries. This approach enables corrections and updates akin to versioning in traditional software, facilitating the introduction of new features and rectification of flaws. The absence of a Solidity-equivalent to JUnit, calling for robust testing techniques including manual and automated test generation.
2. Parallel Security in blockchain can be implemented to enhance the protection of user identities and transaction privacy [43]. This strategy involves using parallel intelligence and computational experiments to optimize security decisions in blockchain operations [43]. By constructing artificial blockchain systems and simulating various attack scenarios, this method aims to understand threat evolutions and develop effective countermeasures. Although this approach represents a strategic framework rather than an immediate solution, it underpins the necessity for ongoing modeling, experimentation, and adaptation to safeguard privacy within blockchain networks. Further, fail-safe encryption can be applied to protect personal information stored on the blockchain. By encrypting this data, the blockchain can effectively render it

inaccessible should the encryption keys be lost or deleted, thus approximating compliance with privacy rights while maintaining the integrity of the data stored on the blockchain.

3. Cold storage methods, such as USB drives, offline wallets, or paper-based wallets, are crucial for safeguarding private keys and significantly reducing the risk of online theft. Unlike hot storage solutions that keep private keys connected to the internet and thus susceptible to hacking, cold storage keeps private keys offline, away from potential cyber threats [47]. USB drives, for instance, can securely store private keys and only connect to the internet when necessary, minimizing exposure to online attacks. Offline wallets, including hardware wallets, provide an even more robust solution by storing private keys in a secure device designed to remain disconnected from the internet. These wallets often come with advanced security features like encrypted storage and multi-factor authentication, further protecting against unauthorized access. Paper-based wallets, which involve printing the private keys and storing them physically, offer a simple yet highly effective method for offline storage, provided the paper is kept in a secure location. By using cold storage methods, individuals and organizations can protect their digital assets from hacking attempts, malware, and other cyber threats, ensuring the integrity and security of their blockchain transactions and holdings.

4. Zero-Knowledge Proofs (ZKPs) offer a compelling method to enhance blockchain security by allowing one party to prove to another that a statement is true without revealing any additional information. ZKPs can be used to verify transactions and smart contracts without exposing the underlying data [48]. For example, in a blockchain-based voting system, ZKPs can verify that a vote is valid without revealing the voter's identity or choice. This approach ensures confidentiality while maintaining the transparency and trustworthiness of the process. Implementing ZKPs in blockchain systems can mitigate risks associated with data breaches and unauthorized access, enhancing overall security [48]. Alongside ZKPs, developing innovative testing protocols is crucial for identifying and addressing vulnerabilities in blockchain systems. These protocols include automated security audits, formal verification methods, and continuous monitoring systems that can detect and respond to potential threats in real time. By integrating these testing protocols, blockchain platforms can maintain a high level of security and reliability.

5. Establishing regulatory and legal frameworks is necessary to address losses due to code failures in permissionless blockchain environments [21]. Regulatory frameworks must include stringent guidelines for code development, testing, and deployment to mitigate these risks. Legal frameworks should clearly define liability and accountability in the event of such failures, ensuring that developers and operators adhere to best practices and are held responsible for any breaches or malfunctions. Additionally, these frameworks should establish protocols for dispute resolution and compensation mechanisms for affected parties, providing a structured approach to handling incidents of code failure. By fostering a well-regulated environment, these frameworks can enhance trust and confidence in blockchain technologies, encouraging broader adoption and integration into various industries. This approach not only protects users and investors but also promotes the development of more secure and reliable blockchain systems, ultimately contributing to the stability and growth of the blockchain ecosystem.

6. Sharding, off-chain processing, and the implementation of Directed Acyclic Graphs (DAGs) can be used to address scalability problems [43]. These methods aim to enhance the scalability of blockchain systems by distributing the load and allowing for more parallel processing. However, these solutions can compromise privacy due to their increased transparency, potentially exposing sensitive user data in environments that require confidentiality, such as healthcare.

7. To achieve seamless interoperability with legacy systems and third-party vendors, a comprehensive strategy is necessary. This strategy includes developing and adopting industry-wide standards for blockchain integration with legacy systems and third-party applications to ensure consistency and compatibility. Utilizing modular integration frameworks that allow easy addition or removal of components is essential, along with implementing rigorous interoperability testing protocols to identify and address integration issues before deployment [49]. Establishing continuous monitoring mechanisms to detect and resolve integration issues in real-time is crucial for ensuring ongoing seamless operation. Collaboration and education also play a critical role in this process. Additionally, data wrapping and transformation using middleware can transform data formats from legacy systems into blockchain-compatible formats, while implementing API gateways facilitates communication between legacy systems and blockchain platforms by translating requests and responses. Developing security adapters that bridge the gap between legacy security protocols and blockchain's encryption standards, and gradually upgrading the security protocols of legacy systems to match blockchain requirements while ensuring minimal disruption to operations, are also highly useful. Performance bottlenecks associated with legacy systems can be resolved by using parallel processing techniques to handle transactions on blockchain while ensuring that legacy systems can process them asynchronously, and offloading intensive computational tasks to off-chain processing units that interact with the blockchain only for essential operations.

8. Use of checks-effects-interactions pattern to mitigate re-entrancy vulnerabilities in smart contracts. This ensures that state changes occur before any external calls, reducing the risk of such attacks. This pattern can be applied by structuring smart contract code to first check for any required conditions, then perform all necessary state changes, and only afterwards make external calls [50]. This sequence minimizes the risk of re-entrancy attacks by securing the contract's state before interacting with other contracts. Developers can incorporate this pattern by auditing existing contracts for potential re-entrancy risks and refactoring them to follow this secure coding practice. Additionally, automated tools and static analyzers can be employed during the development process to enforce the checks-effects-interactions pattern, ensuring that new contracts adhere to this secure design.

9. Modifications to Bitcoin's protocol and lightweight detection methods can enhance the network's ability to identify and thwart double-spending and selfish mining attacks. [33,34]. These modifications aim to make it less profitable or more difficult for miners to execute selfish strategies without contributing positively to the network [33]. By using multiple confirmations and network alerts, adjusting how blocks are verified, or changing the reward distribution mechanism, the protocol can be tuned to discourage selfish behavior, promote a more cooperative mining environment, and ensure transaction integrity.

10. Ensuring the contract's state before executing external calls to prevent such vulnerabilities [25]. This procedural step is important in safeguarding against re-entrancy attacks by ensuring that the contract's state reflects any changes before any external interactions that could lead to recursive exploitation. It can be implemented by structuring smart contract code so that all internal state changes are completed

prior to making any external calls. Developers should review and refactor their contracts to follow this secure coding practice, checking conditions and updating state variables before interacting with other contracts. Using automated testing and static analysis tools can help identify any potential issues in the code that may allow re-entrancy. Additionally, integrating secure coding guidelines into the development process and conducting regular code audits can further ensure that contracts are safeguarded against recursive exploitation.

11. Applying the Bitcoin Improvement Proposal 62 (BIP 62) was introduced. BIP 62 aims to fortify the transaction verification process by implementing multiple verification metrics [34]. These new standards ensure that only transactions with non-malleable identifiers are validated and added to the blockchain, reducing the risk of such exploits. By tightening the criteria for transaction confirmation, BIP 62 helps to secure the network against the manipulation of transaction data and enhances the overall integrity of the blockchain.

12. For gasless send, there is a need for careful management of gas allocation and monitoring of contract interactions to avoid unexpected gas exhaustion [41]. Developers need to allocate gas meticulously, ensuring that each transaction or function call is assigned an adequate amount of gas to complete its execution. This involves anticipating the gas requirements of complex interactions and dynamically adjusting gas limits based on the transaction's complexity and expected computational workload. Additionally, continuous monitoring of contract interactions is essential to detect and address any anomalies in real-time. Implementing automated systems for gas management can help dynamically adjust gas allocations and provide alerts for potential gas depletion scenarios.

13. To mitigate threats associated with external calls, the developers should treat contracts as untrusted by default and implement robust error-handling mechanisms to manage unexpected behaviors or revert operations when external calls fail. This precaution is essential to prevent potential security breaches that could compromise the entire blockchain system [41]. Enhancing security measures, such as improving transaction handling, refining exception management, and securing timestamp operations, are essential to safeguarding the integrity and reliability of smart contracts and, by extension, the broader blockchain infrastructure.

14. To address the vulnerabilities associated with third-party vendors and interoperability, thorough vetting of third-party vendors and continuous monitoring of these relationships is advised [45]. Auditors play a critical role in this context by assessing whether a client's business processes and systems are adequately prepared to integrate with blockchain technology. They must evaluate whether management's policies are robust enough to address potential interoperability issues, ensuring that the transition to or incorporation of blockchain technology aligns with the client's operational and strategic goals [45]. The complexity of achieving such interoperability without compromising the functionality or security of either the blockchain system or the existing IT environment poses a considerable challenge.

15. To address the 51% and other network attacks, protocols such as the PirGuard Protocol in Ethereum and the Delayed Proof of Work can be employed [30]. A combination of blockchain and network monitoring technologies is recommended for traffic attacks like DDoS. Implementing these protocols involves integrating specific safeguards within the blockchain infrastructure to detect and prevent malicious activities. The PirGuard Protocol enhances Ethereum's security by monitoring mining activities and identifying attempts to gain control of the network's hashing power.

Similarly, Delayed Proof of Work introduces additional layers of verification to ensure the integrity of transactions before they are fully validated. In tandem with these protocols, deploying a combination of blockchain and network monitoring technologies is crucial for mitigating traffic attacks like DDoS. This can be achieved by continuously analyzing network traffic patterns to detect anomalies, implementing rate-limiting measures to control the flow of transactions, and utilizing automated threat detection systems that can swiftly identify and respond to suspicious activities.

16. Blockchain anomaly detection systems and mutual authentication protocols in RFID systems can be used to mitigate injection or insider attacks. Anomaly detection systems can be deployed to continuously monitor blockchain transactions and network activities, identifying unusual patterns or behaviors indicative of potential security threats [51]. By employing advanced machine learning algorithms and real-time analytics, these systems can promptly detect and flag suspicious activities, allowing for immediate investigation and response to potential injection attacks. Simultaneously, mutual authentication protocols within RFID systems can enhance security by ensuring that both the RFID reader and the tag authenticate each other before any data exchange occurs. This can be achieved through cryptographic techniques and secure communication channels, which prevent unauthorized devices from accessing or injecting malicious data into the system.

17. A more analytical approach, such as large deviation theory to study the vulnerabilities caused by intentional forks in the blockchain network. This method provides a micro-level examination of the network's robustness. It reveals that adjusting certain network parameters can be more effective and cost-efficient than simply boosting computational power to mitigate vulnerabilities [33]. Through extensive experiments with the Ethereum protocol, this study validates the effectiveness of strategic technical and managerial adjustments to enhance the resilience of blockchain systems against forking attacks.

By adopting these recommendations and continuously evolving the technological and methodological frameworks, stakeholders can mitigate the inherent risks and maximize the benefits of blockchain technology.

4. CONCLUSION

Unlike traditional centralized systems, the decentralized nature of blockchain introduces new dimensions of security, trust, and reliability that are not fully understood or addressed in current research. This gap in understanding highlights the need for ongoing research to explore the implications of blockchain technology for various stakeholders, including users, developers, and regulatory bodies. A comprehensive understanding of blockchain technology is crucial for ensuring its deployment and evolution are secure, trustworthy, and beneficial for all parties involved. This calls for a concerted effort from the academic and technological communities to address the novel challenges posed by blockchain technology and to develop solutions to mitigate the risks associated with its adoption.

As blockchain continues to evolve and integrate into various sectors, from finance and healthcare to supply chains and public administration, its foundational promise of decentralization, transparency, and security faces critical tests. Key vulnerabilities such as smart contract flaws, private key theft, and scalability issues highlight the need for robust security protocols, rigorous testing, and continuous system enhancements. Additionally, the intrinsic challenges posed by rapid technological advances, such as quantum computing, necessitate proactive approaches to ensure blockchain infrastructure remains secure, efficient, and future-proof.

Addressing these challenges requires a multifaceted strategy involving technological solutions and regulatory and educational approaches. Adopting advanced cryptographic methods offers

promising pathways to enhance transaction security and privacy. Meanwhile, establishing clear regulatory frameworks and standards is crucial for mitigating risks related to interoperability and third-party integrations. Further, as blockchain systems become more prevalent, educating stakeholders, from developers to end-users, about the best practices for security and privacy will play a critical role in safeguarding the technology against potential breaches.

Further, the adoption of blockchain technology must be accompanied by thorough risk assessments and the implementation of tailored security measures. This includes vetting third-party vendors rigorously, employing cold storage options to secure private keys, and embracing innovative solutions like off-chain processing to address scalability and privacy concerns. Additionally, developing and deploying smart contracts should prioritize security from the outset, utilizing tools for automatic vulnerability detection and adhering to secure coding practices. As demonstrated by incidents such as the DAO attack, the financial and reputational ramifications of security lapses can be profound, underscoring the importance of a security-first approach in blockchain development.

While promising, the future of blockchain technology hinges on the collective efforts of developers, researchers, businesses, and regulators to comprehensively address its security vulnerabilities. By fostering an ecosystem that prioritizes security, privacy, and interoperability, blockchain can achieve its full potential as a transformative technology. As this study has shown, continued research and collaboration are essential for overcoming the current challenges and unlocking the innovative capacities of blockchain for secure, transparent, and efficient digital transactions across a myriad of applications.

REFERENCES

[1] Sarmah SS. Understanding blockchain technology. Computer Science and Engineering. 2018 Aug;8(2):23-9. 10.5923/j.computer.20180802.02

[2] Zheng Z, Xie S, Dai HN, Chen X, Wang H. Blockchain challenges and opportunities: A survey. International journal of web and grid services. 2018;14(4):352-75.

[3] Nzuva S. Smart contracts implementation, applications, benefits, and limitations. Journal of Information Engineering and Applications. 2019 Sep 30;9(5):63-75.

[4] Kissoon Y, Bekaroo G. Detecting vulnerabilities in smart contract within blockchain: A review and comparative analysis of key approaches. In2022 3rd International Conference on Next Generation Computing Applications (NextComp) 2022 Oct 6 (pp. 1-6). IEEE.

[5] Destefanis G, Marchesi M, Ortu M, Tonelli R, Bracciali A, Hierons R. Smart contracts vulnerabilities: a call for blockchain software engineering?. In2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE) 2018 Mar 20 (pp. 19-25). IEEE.

[6] Putz B, Pernul G. Detecting blockchain security threats. In2020 IEEE International Conference on Blockchain (Blockchain) 2020 Nov 2 (pp. 313-320). IEEE.

[7] Beck R, Becker C, Lindman J, Rossi M. Opportunities and Risks of Blockchain Technologies: Report from Dagstuhl Seminar 17132. Dagstuhl Reports. 2017;7(3).

[8] Snegireva DA. Review of modern vulnerabilities in blockchain systems. In2021 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS) 2021 Sep 6 (pp. 117-121). IEEE.

[9] Guo H, Yu X. A survey on blockchain technology and its security. Blockchain: research and applications. 2022 Jun 1;3(2):100067

[10] Keenan TP. Alice in blockchains: surprising security pitfalls in PoW and PoS blockchain systems. In2017 15th Annual Conference on Privacy, Security and Trust (PST) 2017 Aug 28 (pp. 400-4002). IEEE.

[11] Saad M, Spaulding J, Njilla L, Kamhoua C, Shetty S, Nyang D, Mohaisen D. Exploring the attack surface of blockchain: A comprehensive survey. IEEE Communications Surveys & Tutorials. 2020 Mar 2;22(3):1977-2008.
[12] Yi X, Wu D, Jiang L, Fang Y, Zhang K, Zhang W. An empirical study of blockchain system vulnerabilities: Modules, types, and patterns. In Proceedings of the 30th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering 2022 Nov 7 (pp. 709-721).
[13] Prasad B. Vulnerabilities and attacks on smart contracts over BlockChain. Turkish Journal of Computer and Mathematics Education (TURCOMAT). 2021 May 10;12(11):5436-49.
[14] Narayana KL, Sathiyamurthy K. Automation and smart materials in detecting smart contracts vulnerabilities in Blockchain using deep learning. Materials Today: Proceedings. 2023 Jan 1;81:653-9.
[15] Guggenberger T, Schlatt V, Schmid J, Urbach N. A Structured Overview of Attacks on Blockchain Systems. PACIS. 2021 Jul:100.
[16] Praitheeshan P, Pan L, Yu J, Liu J, Doss R. Security analysis methods on Ethereum smart contract vulnerabilities: a survey. arXiv preprint arXiv:1908.08605. 2019 Aug 22.
[17] Khan MA, Salah K. IoT security: Review, blockchain solutions, and open challenges. Future generation computer systems. 2018 May 1;82:395-411.
[18] Ahmed M, Pathan AS. Blockchain: Can it be trusted? Computer. 2020 Apr 9;53(4):31-5.
[19] Gao W, Hatcher WG, Yu W. A survey of blockchain: Techniques, applications, and challenges. In2018 27th International Conference on Computer Communication and Networks (ICN) 2018 Jul 30 (pp. 1-11). IEEE.
[20] Bhutta MN, Khwaja AA, Nadeem A, Ahmad HF, Khan MK, Hanif MA, Song H, Alshamari M, Cao Y. A survey on blockchain technology: Evolution, architecture and security. Ieee Access. 2021 Apr 13;9:61048-73.
[21] Zamani E, He Y, Phillips M. On the security risks of the blockchain. Journal of Computer Information Systems. 2020 Nov 1;60(6):495-506.
[22] Hasanova H, Baek UJ, Shin MG, Cho K, Kim MS. A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. International Journal of Network Management. 2019 Mar;29(2):e2060.
[23] Jonathan K, Sari AK. Security issues and vulnerabilities on a blockchain system: A review. In2019 international seminar on research of information technology and intelligent systems (ISRITI) 2019 Dec 5 (pp. 228-232). IEEE.
[24] Li X, Jiang P, Chen T, Luo X, Wen Q. A survey on the security of blockchain systems. Future generation computer systems. 2020 Jun 1;107:841-53.
[25] Amiet N. Blockchain vulnerabilities in practice. Digital Threats: Research and Practice. 2021 Mar 26;2(2):1-7.
[26] König L, Unger S, Kieseberg P, Tjoa S, Blockchains JR. The Risks of the Blockchain: A Review on Current Vulnerabilities and Attacks. J. Internet Serv. Inf. Secur.. 2020 Aug;10(3):110-27.
[27] Rathod N, Motwani D. Security threats on blockchain and its countermeasures. Int. Res. J. Eng. Technol. 2018 Nov;5(11):1636-42.
[28] Kadena E, Holicza P. Security issues in the blockchain (ed) world. In2018 IEEE 18th International Symposium on Computational Intelligence and Informatics (CINTI) 2018 Nov 21 (pp. 000211-000216). IEEE
[29] Abu-Elezz I, Hassan A, Nazeemudeen A, Househ M, Abd-Alrazaq A. The benefits and threats of blockchain technology in healthcare: A scoping review. International Journal of Medical Informatics. 2020 Oct 1;142:104246.
[30] Bamakan SM, Motavali A, Bondarti AB. A survey of blockchain consensus algorithms performance evaluation criteria. Expert Systems with Applications. 2020 Sep 15;154:113385.

[31] Cheng J, Xie L, Tang X, Xiong N, Liu B. A survey of security threats and defense on Blockchain. Multimedia Tools and Applications. 2021 Aug;80:30623-52.
[32] Kearney JJ, Perez-Delgado CA. Vulnerability of blockchain technologies to quantum attacks. Array. 2021 Jul 1; 10:100065.
[33] Wang S, Wang C, Hu Q. Corking by forking: Vulnerability analysis of blockchain. In IEEE INFOCOM 2019-IEEE Conference on Computer Communications 2019 Apr 29 (pp. 829-837). IEEE.
[34] Bhushan B, Sinha P, Sagayam KM, Andrew J. Untangling blockchain technology: A survey on the state of the art, security threats, privacy services, applications, and future research directions. Computers & Electrical Engineering. 2021 Mar 1; 90:106897.
[35] Ghosh A, Gupta S, Dua A, Kumar N. Security of Cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects. Journal of Network and Computer Applications. 2020 Aug 1; 163:102635.
[36] Morganti G, Schiavone E, Bondavalli A. Risk assessment of blockchain technology. In2018 Eighth Latin-American Symposium on Dependable Computing (LADC) 2018 Oct 8 (pp. 87-96). IEEE.
[37] Lindman J, Tuunainen VK, Rossi M. Opportunities and risks of Blockchain Technologies–a research agenda. Open Digital Services and Platforms (2017)
[38] Junejo AZ, Hashmani MA, Alabdulatif AA. A survey on privacy vulnerabilities in permissionless blockchains. International Journal of Advanced Computer Science and Applications (IJACSA). 2020;11(9):130-9.
[39] Averin A, Averina O. Review of blockchain technology vulnerabilities and blockchain-system attacks. 2019 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon) 2019 Oct 1 (pp. 1-6). IEEE.
[40] Hilt M, Shao D, Yang B. RFID security, verification, and blockchain: vulnerabilities within the supply chain for food security. In Proceedings of the 19th Annual SIG Conference on Information Technology Education 2018 Sep 14 (pp. 145-145).
[41] Mense A, Flatscher M. Security vulnerabilities in Ethereum smart contracts. In Proceedings of the 20th International Conference on Information Integration and Web-based Applications & Services 2018 Nov 19 (pp. 375-380).
[42] He D, Wu R, Li X, Chan S, Guizani M. Detection of vulnerabilities of blockchain smart contracts. IEEE Internet of Things Journal. 2023 Feb 1.
[43] Wenhua Z, Qamar F, Abdali TA, Hassan R, Jafri ST, Nguyen QN. Blockchain technology: security issues, healthcare applications, challenges, and future trends. Electronics. 2023 Jan 20;12(3):546.
[44] Joshi AP, Han M, Wang Y. A survey on security and privacy issues of blockchain technology. Mathematical foundations of computing. 2018 May 1;1(2).
[45] White BS, King CG, Holladay J. Blockchain security risk assessment and the auditor. Journal of Corporate Accounting & Finance. 2020 Apr;31(2):47-53.
[46] Singh, K.K., 2022. Application of Blockchain Smart Contracts in E-Commerce and Government. arXiv preprint arXiv:2208.01350.
[47] Barakat S, Hammouri Q, Yaghi K. COMPARISON OF HARDWARE AND DIGITAL CRYPTO WALLETS. Journal of Southwest Jiaotong University. 2022;57(6).
[48] Sun X, Yu FR, Zhang P, Sun Z, Xie W, Peng X. A survey on zero-knowledge proof in blockchain. IEEE network. 2021 Aug 20;35(4):198-205.
[49] Prewett KW, Prescott GL, Phillips K. Blockchain adoption is inevitable—Barriers and risks remain. Journal of Corporate accounting & finance. 2020 Apr;31(2):21-8.
[50] Thirulokachander VR. Impact of Design Patterns on Code Quality in Blockchain-based Applications (Doctoral dissertation, University of Windsor (Canada)).
[51] Hassan MU, Rehmani MH, Chen J. Anomaly detection in blockchain networks: A comprehensive survey. IEEE Communications Surveys & Tutorials. 2022 Sep 12;25(1):289-318.

[52] Liu, S., Roy, D., & Hennequin, S. (2020). Blockchains and Internet of Things for the Pooling of Warehouse Resources. South Asian Journal of Social Studies and Economics, 5(4), 1–16. https://doi.org/10.9734/sajsse/2019/v5i430153

[53] Abbasi, F. N., & Sidhu, S. M. (2021). The Implementation and Impact of Blockchain Technology in the Finance and Trade Sector of Economy of the Developing World. Asian Journal of Economics, Business and Accounting, 21(11), 70–73. https://doi.org/10.9734/ajeba/2021/v21i1130442

[54] Morkunas VJ, Paschen J, Boon E. How blockchain technologies impact your business model. Business Horizons. 2019 May 1;62(3):295-306