World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Blockchain Security: Vulnerabilities and Protective Measures

Ahsan Umar and Muhammad Zeeshan Zafar *

Department of Computer Science, Bahauddin Zakariya University, Multan, Punjab, Pakistan.

World Journal of Advanced Research and Reviews, 2025, 25(03), 1056-1058

Publication history: Received on 03 February 2025; revised on 12 March 2025 accepted on 14 March 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.25.3.0791

Abstract

Blockchain technology offers a decentralized and tamper-resistant framework for secure transactions. However, its growing adoption across industries—from finance to supply chain management—has also exposed it to critical security vulnerabilities. Issues such as smart contract flaws, 51% attacks, and Sybil attacks can undermine the integrity of blockchain applications, resulting in financial losses and diminished trust. This paper reviews the current state of blockchain security by examining key vulnerabilities, their impacts, and existing protective measures. It proposes a comprehensive security framework that integrates formal verification methods, enhanced consensus mechanisms, and international collaboration to mitigate these risks. The feasibility of these measures is discussed with regard to computational overhead and scalability challenges. Through real-world case studies, the review underscores the urgency of robust, multi-layered defenses and calls for collaborative efforts among developers, researchers, and regulators.

Keywords: Blockchain Security; Smart Contracts; 51% Attacks; Formal Verification; Consensus Mechanisms; Collaborative Security

1. Introduction

Blockchain technology, initially popularized by Bitcoin, has expanded well beyond cryptocurrencies into sectors such as finance, healthcare, and supply chain management. According to Statista, the global blockchain market is projected to reach 1,235 billion U.S. dollars by 2030 [1]. Despite its promise of decentralization and immutability, blockchain systems are not immune to vulnerabilities. Significant issues—ranging from smart contract bugs to 51% attacks—have led to considerable financial losses; for instance, blockchain-related hacks resulted in over $3.8 billion in losses in 2022 as reported by Chainalysis [2]. Moreover, security measures originally designed for centralized systems are often inadequate for addressing the unique challenges posed by decentralized ledgers. This review discusses the vulnerabilities inherent in blockchain systems, their real-world impacts, and protective measures designed to enhance security.

2. Related Work

Research in blockchain security has revealed several persistent vulnerabilities. Studies indicate that a substantial number of Ethereum smart contracts contain exploitable bugs—a phenomenon detailed in surveys such as that by Atzei et al. [5]. Additionally, the risk of 51% attacks, wherein an attacker gains control of the majority of a network's computational power, has been demonstrated in cases like the Verge network attack reported by CoinTelegraph [3]. These challenges highlight the need for new security paradigms. Enhanced consensus mechanisms like Proof of Stake (PoS), as discussed by Buterin and Griffith, offer promising alternatives by not only reducing energy consumption compared to Proof of Work but also by addressing some risks of 51% attacks [4]. Collectively, these findings call for a multi-layered security framework that integrates advanced technical measures with broader collaborative strategies.

* Corresponding author: Muhammad Zeeshan Zafar

3. Blockchain Security Overview

Key Vulnerabilities

3.1. Smart Contract Bugs

Vulnerabilities in smart contracts, such as those exploited in reentrancy attacks, remain a major concern. Surveys of Ethereum smart contracts reveal that many contain flaws that could be exploited if not rigorously tested and formally verified [5].

3.2. 51% Attacks

In a 51% attack, an entity controlling a majority of the network's computational power can manipulate transactions or double-spend funds. For example, the Verge network experienced a 51% attack in 2018, resulting in a loss of approximately $1.8 million [3].

3.3. Sybil Attacks

These attacks involve the creation of multiple fake identities to subvert the consensus mechanism. While the exact impact varies, the threat is well recognized in decentralized networks.

3.4. Phishing for Private Key

Social engineering tactics, such as phishing, have been linked to a significant portion of blockchain-related financial losses. Chainalysis reports that phishing remains one of the critical vectors for compromising private keys [2].

4. Impacts

Blockchain vulnerabilities not only result in immediate financial losses but also erode user trust and hinder mainstream adoption. High-profile incidents like the Verge attack and historical events such as the DAO hack serve as stark reminders of how technical flaws can lead to long-term reputational damage. As regulatory bodies begin to scrutinize blockchain operations more closely, inconsistent global regulations further complicate efforts to secure blockchain environments.

4.1. Protective Measures

To address these vulnerabilities, several protective measures have been proposed and implemented:

4.2. Formal Verification

The use of formal verification tools—such as those designed to analyze smart contracts—has been shown to significantly reduce the occurrence of exploitable bugs. Although these methods may increase development time and costs, they provide a crucial safeguard for mission-critical applications [5].

4.3. Enhanced Consensus Mechanisms

Transitioning from energy-intensive Proof of Work to more efficient consensus models like Proof of Stake can reduce the risk of 51% attacks while also lowering energy consumption. The Casper protocol, for example, has been proposed as a way to secure PoS systems [4].

4.4. Global Collaboration

Addressing blockchain security challenges requires coordinated efforts among developers, industry stakeholders, and regulators. Establishing international standards and collaborative frameworks is vital for ensuring a secure and trustworthy blockchain ecosystem.

5. Case Studies

5.1. The Verge 51% Attack (2018)

In 2018, the Verge network suffered a 51% attack in which attackers gained control over the network's hash rate, enabling them to manipulate transactions and steal funds totaling approximately $1.8 million [3]. This incident

underscored the vulnerabilities inherent in smaller Proof-of-Work blockchains and spurred discussions on the adoption of alternative consensus mechanisms.

5.2. Smart Contract Exploits

High-profile smart contract failures—exemplified by incidents like the DAO hack—demonstrate the critical need for robust testing and formal verification. Studies have shown that a significant number of Ethereum contracts contain vulnerabilities that could be exploited if not adequately verified [5].

6. Discussion

The evolution of blockchain technology brings with it both immense promise and substantial risk. On one hand, enhanced protective measures such as formal verification and advanced consensus mechanisms can dramatically reduce vulnerabilities. On the other hand, the high costs associated with these measures and the complexity of achieving global regulatory alignment remain significant challenges. Addressing these issues will require not only technical innovation but also sustained collaborative efforts across multiple domains.

7. Conclusion

Blockchain security is at a critical juncture. As the technology continues to expand into diverse industries, the vulnerabilities inherent in its design—ranging from smart contract flaws to 51% and Sybil attacks—must be addressed proactively. This review has outlined the primary challenges, assessed their impacts, and presented a multi-layered security framework that integrates formal verification, enhanced consensus protocols, and international collaboration. By drawing on insights from industry-leading reports and academic research, this paper calls on developers, researchers, and regulators to work together in forging a secure path forward for blockchain technology.To further enhance blockchain security, adopting a centralized collaborative framework to address cryptographic threats and attacks—similar to the web security framework proposed by Muhammad Zeeshan Zafar in "The Punisher: A Collaborative Framework for Global Web Security"—could be beneficial [6].

Compliance with ethical standards

Disclosure of conflict of interest

The author declares no conflict of interest.

References

[1] Statista. Blockchain Market Size Worldwide from 2018 to 2025. 2024. Available from: https://www.statista.com/statistics/647231/blockchain-market-size-worldwide/.

[2] Chainalysis. The 2023 Crypto Crime Report. 2023. Available from: https://go.chainalysis.com/2023-crypto-crime-report.html.

[3] CoinTelegraph. Verge Suffers 51% Attack, Loses $1.8M in XVG Tokens. 2018. Available from: https://cointelegraph.com/news/verge-of-disaster-200-days-transactions-wiped-from-blockchain.

[4] Buterin, V. & Griffith, V. Casper the Friendly Finality Gadget. 2017. Available from: https://arxiv.org/abs/1710.09437.

[5] Atzei, N., Bartoletti, M., & Cimoli, T. A Survey of Attacks on Ethereum Smart Contracts (SoK). In: Principles of Security and Trust; 2017. DOI: 10.1007/978-3-662-54455-6_8.

[6] Muhammad Zeeshan Zafar. The punisher: A collaborative framework for global web security. World Journal of Advanced Research and Reviews. Available from: The Punisher.