International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 7 July 2023, pp: 427-433 www.ijaem.net ISSN: 2395-5252

Securing Blockchain and Cryptocurrencies: Exploring Attack Vectors and Countermeasures

Heng Zhi Yong[1], Mohamad Fadli Zolkipli[2]
[1] *Awang Had Salleh Graduate School, School of Computing, Universiti Utara Malaysia, Kedah, Malaysia*
[2] *School of Computing, Universiti Utara Malaysia, Kedah, Malaysia..*

Date of Submission: 10-07-2023 Date of Acceptance: 20-07-2023

ABSTRACT: Blockchain technology and cryptocurrencies have revolutionized industries by offering decentralized and transparent solutions for financial transactions. However, they also introduce new security challenges and vulnerabilities. This study analyses existing hacking techniques in the context of blockchain and cryptocurrencies and evaluates future hacking trends. Attack vectors such as 51% attacks, Sybil attacks, double-spending, smart contract exploitation, phishing and social engineering, and malware and ransomware attacks are examined. Countermeasures include network decentralization, alternative consensus mechanisms, robust identity verification, secure coding practices, and system audits. Collaboration among industry stakeholders and ongoing research are emphasized. By understanding vulnerabilities and implementing proactive measures, blockchain technology and cryptocurrencies can be utilized securely, ensuring their continued adoption and successful implementation.

KEYWORDS: Blockchain technology, cryptocurrencies, security challenges, hacking techniques, countermeasures

I. INTRODUCTION

Blockchain technology and cryptocurrencies have delivered giant changes to numerous industries. They allow monetary transactions and records control to happen in a decentralised manner, that means no unmarried authority controls the whole lot. This decentralisation guarantees transparency and removes the want for intermediaries, along with banks, in economic transactions.

These advancements have many benefits. For instance, transactions may be completed quicker and at lower fees. Also, the transparency of the blockchain makes it less difficult to trace and verify transactions, lowering fraud and corruption.

However, together with those blessings, there are also new security dangers and weaknesses that want to be taken into consideration. Malicious people are usually searching for approaches to make the most of those structures for his or her private benefit. They may additionally try to hack into blockchain networks, manage transactions, or scouse borrow cryptocurrencies.

To address these demanding situations, it's important to perceive the various methods wherein these assaults can arise and develop powerful countermeasures. This involves imposing sturdy security measures, consisting of encryption techniques, multi-thing authentication, and regular device audits. Additionally, ongoing studies and improvement within the subject of blockchain protection are important to stay in advance of emerging threats.

By understanding the potential vulnerabilities and taking proactive measures to deal with them, we can ensure that blockchain technology and cryptocurrencies continue to offer the advantages they promise while minimising the dangers related to them.

Blockchain technology and cryptocurrencies have revolutionised various industries by offering decentralised and transparent solutions for financial transactions and data management [1, 2]. According to[3], blockchain technology also supports secure transactions of NFTs in modern computer games. However, along with their numerous advantages, they also introduce new security challenges and vulnerabilities. Malicious actors are constantly seeking ways to exploit these systems for personal gain, making it imperative to explore the different

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 7 July 2023, pp: 427-433 www.ijaem.net ISSN: 2395-5252

attack vectors and develop effective countermeasures.

The aim is to examine the different ways in which blockchain technology and cryptocurrencies can be targeted by attacks and to propose countermeasures to enhance their security. It is essential to understand the vulnerabilities and risks associated with these technologies in order to develop strategies that can protect blockchain networks and ensure the safety of digital assets.

The introduction provides an overview of the growing importance of securing blockchain and cryptocurrencies. It highlights the increasing adoption of blockchain technology and the rise of cryptocurrencies, emphasising the need for robust security measures. The potential consequences of successful attacks on blockchain networks, such as financial losses, compromised data integrity, and decreased trust among users, are also discussed.

The objectives of this study are:

1. To analyse existing hacking techniques in the context of blockchain and cryptocurrencies.
2. To evaluate future hacking trends and their potential impact on blockchain security.

To achieve these objectives, this study utilises a combination of literature review, case studies, and analysis of existing security mechanisms. By synthesising the current knowledge in the field and building upon it, this research aims to contribute to the development of more secure and resilient blockchain and cryptocurrency ecosystems.

II. LITERATURE REVIEW

i. Background

Blockchain technology isdecentralised and disbursed ledger gadget that lets in steady and obvious transactions without the want for intermediaries. This utilises cryptographic techniques to ensure records integrity and consensus amongst community members. The concept of blockchain was first brought in 2008 with the guide of the Bitcoin whitepaper by Satoshi Nakamoto, which outlined a peer-to-peer digital coins system based totally on blockchain technology.

Digital or virtual currencies that operate on blockchain networks and use cryptography for security are known as cryptocurrencies. Bitcoin, the first and most well-known cryptocurrency, emerged in 2009 as a decentralised virtual foreign money that facilitated peer-to-peer transactions. Since then, numerous cryptocurrencies have been advanced, each with its very own features and use instances. According to [4], Regulators from all over the world are putting more pressure on cryptocurrencies like Bitcoin to use less energy.

ii. History

The records of blockchain generation dates again to the early 1990s while researchers and cryptographers explored the concept of decentralised systems and cryptographic techniques. The introduction of the hash cash evidence-of-work set of rules by Adam Back in 1997 laid the foundation for the computational consensus mechanism utilised in blockchain networks.

The publication of the Bitcoin whitepaper in 2008 marked a tremendous milestone in the records of blockchain generation. Satoshi Nakamoto added the idea of a decentralised, thrustless, and transparent machine for undertaking financial transactions. Bitcoin's underlying blockchain architecture served as the foundation for subsequent blockchain-based applications and cryptocurrencies. According to [5], in Bitcoin, the blockchain enabled customers to be pseudonymous. This technique approach that customers are nameless, but their account identifiers are not. In addition, all transactions are publicly seen. This has effectively enabled Bitcoin to provide pseudo-anonymity because debts may be created with none identification or authorization way (such tactics are generally required thru Know-Your-Customer (KYC) prison guidelines).

Following the success of Bitcoin, developers and entrepreneurs recognized the potential of blockchain technology beyond cryptocurrencies. The development of Ethereum in 2015 introduced the idea behind smart contracts, enabling programmable transactions and the creation of decentralised applications (dApps) on the blockchain. This development sparked a wave of innovation and exploration of blockchain applications in various sectors, including supply chain management, healthcare, finance, and more. By market capitalization, Ethereum is the second-largest cryptocurrency. Proof of Work (PoW) was superseded by an alternative called evidence-of-stake on September 15, 2022, as part of an occasion called The Merge.[4].

iii. Blockchain Security

Blockchain security focuses on the core principles and mechanisms used in blockchain technology to safeguard data integrity, establish consensus, and defend against attacks. It encompasses essential topics like cryptographic hashing, consensus algorithms such as Proof of

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 7 July 2023, pp: 427-433 www.ijaem.net ISSN: 2395-5252

Work (PoW) and Proof of Stake (PoS), and decentralised network structures. According to[6], Just a few academics venture beyond the purely technical perspective, whereas the majority of articles focused primarily on the technical elements of blockchain security. Researchers have investigated the vulnerabilities and potential attacks on blockchain systems and proposed various security measures and enhancements.

iv. Cryptocurrency Attack

Cryptocurrency attacks make a speciality of the unique vulnerabilities and assault vectors focused on cryptocurrencies. It delves into principles such as 51% assaults, in which a malicious actor profits from manipulation of the majority of the community's computational energy, allowing them to manipulate transactions. Other assaults consist of double-spending, Sybil assaults, and pockets vulnerabilities. According to[7], there have several taxonomy of attacks on cryptocurrency such as Goldfinger attack, Hard Fork, DNS Hijack, BGP Hijack, Eclipse Attack, Wallet Attack, DDoS and Dusting Attack. Researchers have examined the underlying mechanisms of these attacks, their effect on the safety and integrity of cryptocurrencies, and proposed mitigation strategies.

v. Smart Contract Security

Smart contracts are agreements that automatically carry out their terms after being instantly encoded in blockchain code. Security for smart contracts addresses the flaws and vulnerabilities included in those automatic contracts. It discusses not unusual vulnerabilities, which include re-entrancy, integer overflow, and unchecked external calls, and explores auditing practices, stable coding recommendations, and tools to enhance clever settlement safety. According to [8], smart contract security can also spotlight the capability blessings of the proposed system, inclusive of reducing fraud, casting off intermediaries, and offering a greater green and reliable land registration procedure.

vi. Existing Security Measures

Existing security measures examine the approaches and techniques implemented in blockchain systems to enhance security. It covers network-level security, data privacy, identity management, access controls, and encryption methods. According to [9], there are 6 layers of security measures of blockchain technology and there are application layer, contract layer, incentive layer, consensus layer, network layer and data layer. Researchers have proposed and evaluated various security mechanisms, consensus algorithms, cryptographic techniques, and protocols to protect blockchain systems from attacks.

III. EXISTING HACKING TECHNIQUE

51% Attacks

A 51% attack takes place whilst a malicious actor or institution gains manage of more than 50% of the computational energy in a blockchain network. This allows them to exploit the consensus mechanism, probably permitting them to alter transaction history, opposite transactions, or double-spend coins.Such attacks are particularly relevant for blockchains that rely on a proof-of-work consensus algorithm. Mitigation strategies for 51% attacks involve enhancing network decentralisation, implementing alternative consensus mechanisms, and monitoring network activity[10].

Sybil Attacks

In Sybil attacks, several fraudulent identities or nodes are created with the goal of taking over or influencing a blockchain network. A large number of nodes under the attacker's control allow them to alter consensus rules or damage network reputation. Preventive measures for Sybil attacks include establishing robust identity verification mechanisms, implementing reputation systems, and employing consensus protocols that are resistant to Sybil attacks[11].

Double-Spending

Double-spending attacks exploit the inherent nature of digital currencies, where it is possible to spend the same cryptocurrency more than once. This occurs when an attacker successfully spends a certain amount of cryptocurrency and then quickly creates an alternative version of the transaction that directs the same funds elsewhere. Mitigation strategies involve the implementation of secure consensus algorithms, real-time transaction verification, and the use of additional security layers to prevent double-spending attacks [10].

Smart Contract Exploitation

The self-executing contracts known as "smart contracts" are created using blockchain technology. Smart contract exploitation involves identifying vulnerabilities in the code and exploiting them to gain unauthorised access, manipulate contract conditions, or steal digital assets. Common vulnerabilities include re-entrancy

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 7 July 2023, pp: 427-433 www.ijaem.net ISSN: 2395-5252

attacks, integer overflow, and unchecked external calls. To mitigate smart contract exploitation, rigorous auditing and testing processes, adherence to secure coding practices, and the use of vulnerability detection tools are recommended [12]

Phishing and Social Engineering

Phishing and social engineering attacks target individuals involved in blockchain and cryptocurrency transactions. According to[13], Phishing attacks can be launched through messaging services, social media plateforms, or emailwith disastrous results such as identity theft and financial loss. Attackers use deceptive techniques, such as fake websites, emails, or impersonation, to trick users into revealing their private keys, login credentials, or other sensitive information. Preventive measures include user education, employing multi-factor authentication, and promoting secure communication channels to mitigate the risk of falling victim to phishing and social engineering attacks. According to [14], Social engineering attacks distinguish into 3 categories and there are technology-based attacks, human-based attacks and hybrid attacks.

Table 1 Type of attacks in categories

Categories	Type of Attacks
Technology-based attacks	• Spyware • Adware • Keylogger • Ransomware • Trojan • Worm
Human-based Attacks	• Tailgating • Eavesdropping • Pretexting • Quid pro quo
Hybrid Attacks	• Baiting • Trolling • Phishing

Malware and Ransomware

Malware and ransomware attacks target users' computers or devices to gain unauthorised access to their digital assets or compromise the security of blockchain systems. According to [15], malicious software, such as keyloggers or remote access tools, can be used to steal private keys or login credentials. According to [16], ransomware encrypts users' data or digital assets and demands a ransom payment for their release. Preventive measures include using reliable security software, practising secure software and wallet management, and regularly updating systems and applications.

IV. FUTURE HACKING TREND

Artificial Intelligence and Machine Learning Attacks

As artificial intelligence (AI) and machine learning (ML) technologies advance, they have the potential to be used by hackers to develop more sophisticated and automated attack techniques. AI-powered attacks can analyse vast amounts of data, identify patterns, and adapt their strategies to exploit vulnerabilities.According to [17],attacks include model poisoning, adversarial attacks, evasion attacks, and data poisoning. Each attack type is explained, highlighting its potential impact on the integrity and security of blockchain systems.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 7 July 2023, pp: 427-433 www.ijaem.net ISSN: 2395-5252

For example, AI can be utilised to generate highly convincing phishing emails, launch automated malware attacks, or bypass security systems by learning and evading detection mechanisms. Defending against AI and ML attacks will require the development of AI-based defence systems, robust anomaly detection algorithms, and constant monitoring to detect and mitigate emerging threats

Social Engineering and Psychological Manipulation Techniques

Social engineering and psychological manipulation techniques have always been effective tools for hackers, and they are expected to continue evolving in the future. Hackers manipulate people into divulging sensitive information or doing actions that endanger security by taking advantage of human psychology and trust.. According to [18], techniques such as pretexting, baiting, phishing, and impersonation will likely become more sophisticated, tailored, and personalised. Besides that, psychological manipulation techniques such as identity theft, financial fraud, unauthorized access to personal information, and manipulation of user behaviour and emotions. Combating these techniques will require ongoing user education, awareness programs, and the implementation of multi-factor authentication and stringent identity verification processes.

Quantum Computing and Blockchain Security

Quantum computing is poised to revolutionise various fields, including cryptography and blockchain security. While quantum computers offer tremendous computing power, they also pose a threat to traditional cryptographic algorithms used in blockchain networks. Quantum computers can potentially break commonly used cryptographic schemes, compromising the security of blockchain systems. According to [19], to mitigate this threat, researchers are exploring quantum-resistant cryptographic algorithms, such as post-quantum cryptography, which can withstand attacks from quantum computers. Additionally, the development of quantum-secure consensus mechanisms and the integration of quantum-resistant encryption in blockchain networks will be essential to ensure future blockchain security.

V. DISCUSSION

Emerging Technologies and their Security Implications

This discussion area delves into the security implications of emerging technologies that intersect with blockchain and cryptocurrencies. It explores how advancements in fields such as Internet of Things (IoT), artificial intelligence (AI), and decentralised finance (DeFi) can impact the security of blockchain networks. According to [20], potential risks such as data breaches, hacking attacks, smart contract vulnerabilities, and the misuse of decentralized systems. It emphasizes the importance of addressing these security concerns to ensure the successful adoption and implementation of these technologies. For example, the integration of IoT devices with blockchain introduces new attack surfaces and data privacy concerns. The discussion may cover potential vulnerabilities, attack vectors, and recommended security measures to mitigate risks associated with these emerging technologies.

Regulatory Challenges and Policy Considerations

Blockchain technology and cryptocurrencies operate in a rapidly evolving regulatory landscape. This discussion area examines the challenges and considerations related to the regulatory framework for blockchain and cryptocurrencies. It addresses topics such as legal frameworks, data privacy, anti-money laundering (AML) regulations, and consumer protection. The discussion may explore the need for harmonised international regulations, the challenges of enforcing compliance in decentralised systems, and potential policy recommendations to ensure the responsible and secure adoption of blockchain technology[21].

Industry Collaboration for Enhanced Security

Collaboration among industry stakeholders is crucial for strengthening the security of blockchain and cryptocurrencies. According to [22], the importance of industry collaboration, information sharing, and collective efforts to address security challenges. It may discuss the role of industry associations, consortiums, and standardisation bodies in promoting best practices, establishing security guidelines, and facilitating knowledge exchange. The discussion may also explore the potential benefits of public-private partnerships and cross-industry collaborations in enhancing the overall security posture of blockchain and cryptocurrency ecosystems.

VI. CONCLUSION

Blockchain technology and cryptocurrencies have revolutionized various industries by offering decentralized and transparent solutions for financial transactions and data

management. However, along with their numerous advantages, they also introduce new security challenges and vulnerabilities. Malicious actors are constantly seeking ways to exploit these systems for personal gain, making it imperative to explore different attack vectors and develop effective countermeasures.

In this study, we have examined existing hacking techniques in the context of blockchain and cryptocurrencies and evaluated future hacking trends and their potential impact on blockchain security. We have discussed various attack vectors, such as 51% attacks, Sybil attacks, double-spending, smart contract exploitation, phishing and social engineering, malware and ransomware attacks. Additionally, we have explored emerging hacking trends, including AI and machine learning attacks, social engineering and psychological manipulation techniques, and the potential impact of quantum computing on blockchain security.

To enhance the security of blockchain and cryptocurrencies, it is crucial to implement robust security measures. These measures include enhancing network decentralization, implementing alternative consensus mechanisms, establishing robust identity verification mechanisms, employing secure coding practices, and conducting regular system audits. Ongoing research and development in the field of blockchain security are essential to stay ahead of emerging threats and vulnerabilities.

Furthermore, industry collaboration and information sharing play a vital role in strengthening the security of blockchain and cryptocurrency ecosystems. Collaboration among industry stakeholders, including industry associations, consortiums, standardization bodies, and public-private partnerships, can promote best practices, establish security guidelines, and facilitate knowledge exchange.

In conclusion, securing blockchain technology and cryptocurrencies is of paramount importance to ensure their continued adoption and successful implementation. By understanding the potential vulnerabilities and taking proactive measures to address them, we can minimize the risks associated with these technologies and leverage their benefits in a secure and resilient manner. It is through collective efforts, continuous research, and collaboration that we can build a safer and more trustworthy blockchain and cryptocurrency landscape for the future.

VII. ACKNOWLEDGEMENT

The authors would like to thank all School of Computing members who were involved in this study. This study was conducted for the purpose of Ethical Hacking & Penetration Testing Research Project. This work was supported by Universiti Utara Malaysia.

REFERENCES

[1] M. I. Sidiq, W. S. Roth and T. Rusmanto, “Literature Study on the Effect of Blockchain Usage on Cryptocurrencies Looks at Comparisons of Previous Research,” in Proceedings of the 9th International Conference on Management of e-Commerce and e-Government, 2022, July.

[2] B. Lili, C. Du, Y. Li, L. Shaotian and A. W. Chwastek, “Research on Innovation of Online Financing Process based on Blockchain Technology,” in Proceedings of the 7th International Conference on Intelligent Information Processing, 2022, September.

[3] C. I. Paduraru, R. Cristea and A. Stefanescu, “Enhancing the security of gaming transactions using blockchain technology,” in Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering, 2022, October.

[4] A. D. Vries, “Cryptocurrencies on the road to sustainability: Ethereum paving the way for Bitcoin,” Patterns, vol. 4, no. 1, 2023.

[5] D. Yaga, P. Mell, N. Roby and K. Scarfone, “Blockchain technology overview,” arXiv preprint arXiv:1906.11078, 2019.

[6] V. Schlatt, T. Guggenberger, J. Schmid and N. Urbach, “Attacking the trust machine: Developing an information systems research agenda for blockchain cybersecurity,” International journal of information management, vol. 68, p. 102470, 2023.

[7] S. Ramos, F. Pianese, T. Leach and E. Oliveras, “A great disturbance in the crypto: Understanding cryptocurrency returns under attacks,” Blockchain: Research and Applications, vol. 2, no. 3, p. 100021, 2021.

[8] R. K. Yadav, R. Dabare, M. Ghyar, B. Shreya and M. Gautam, “Smart Contract-Based Land Registration System Using Blockchain,” in 2023 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), 2023, February.

[9] Z. Wenhua, F. Qamar, T.-A. N. Abdali, R. Hassan, S. T. A. Jafri and Q. N. Nguyen, “Blockchain technology: security issues, healthcare applications, challenges and future trends,” Electronics, vol. 12, no. 3, p. 546, 2023.

[10] V. Schalat, J. Sedlmeir, J. Traue and F. Völter, "Harmonizing sensitive data exchange and double-spending prevention through blockchain and digital wallets: The case of e-prescription management," Distributed Ledger Technologies: Research and Practice, vol. 2, no. 1, pp. 1-31, 2023.

[11] M. Platt and P. McBurney, "Sybil in the haystack: a comprehensive review of blockchain consensus mechanisms in search of strong sybil attack resistance," Algorithms, vol. 16, no. 1, p. 34, 2023.

[12] J. Wanqing, C. Qi, W. Jiaqi, A. S. V. Koe, L. Jin, H. Pengfei, W. Yaqi and W. Yin, "A novel extended multimodal AI framework towards vulnerability detection in smart contracts," Information Sciences, vol. 636, p. 118907, 2023.

[13] R. O. Ogundokun, M. O. Arowolo, R. Damaševičius and S. Misra, "Phishing Detection in Blockchain Transaction Networks Using Ensemble Learning," Telecom, vol. 4, no. 2, pp. 279-297, 2023, May.

[14] P. Weichbroth , K. Wereszko, H. Anacka and J. Kowal, "Security of Cryptocurrencies: A View on the State-of-the-Art Research and Current Developments," Sensors, vol. 6, no. 3155, p. 23, 2023.

[15] M. Gimenez-Aguilar, J. M. de Fuentes and L. Gonzalez-Manzano, "Malicious uses of blockchains by malware: from the analysis to Smart-Zephyrus," International Journal of Information Security, pp. 1-36, 2023.

[16] A. Alqahtani and F. T. Sheldon, "Temporal Data Correlation Providing Enhanced Dynamic Crypto-Ransomware Pre-Encryption Boundary Delineation," Sensors, vol. 23, no. 9, p. 4355, 2023.

[17] V. Chithanuru and M. Ramaiah, "An anomaly detection on blockchain infrastructure using artificial intelligence techniques: Challenges and future directions – A review," Concurrency and Computation: Practice and Experience, p. e7724, 2023.

[18] H. Yan, L. Yi Joy and C. Zhipeng, "Security and Privacy in Metaverse: A Comprehensive Survey," Big Data Mining and Analytics, vol. 6, no. 2, pp. 234-247, 2023.

[19] D. Peng and Z. Bo, "Post quantum identity authentication mechanism in blockchain," in Proceedings of the 8th International Conference on Communication and Information Processing, 2022, November.

[20] E. Ducas and A. Wilner, "The security and financial implications of blockchain technologies: Regulating emerging technologies in Canada," International Journal, vol. 72, no. 4, pp. 538-562, 2017.

[21] K. K. Guerra and K. A. Boys, "A new food chain: Adoption and policy implications to blockchain use in agri- food industries," Applied Economic Perspectives and Policy, vol. 44, no. 1, pp. 324-349, 2022.

[22] A. Polyviou, P. Velanas and J. Soldatos , "Blockchain Technology: Financial Sector Applications Beyond Cryptocurrencies," in Decentralized 2019, 2019.