IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Doublespending Attack Prevention Using A Novel Method

[1]Aaryan Singh Suryan, [2]Gursimar Singh, [3]Mayank Dutt Pathak, [4]Dr. Christy Jackson J

School of Computer Science and Engineering (SCOPE),

[1]Vellore Institute of Technology (VIT) Chennai, Tamil Nadu, India

Abstract: This paper presents a custom blockchain system designed to detect and prevent double-spending attacks, which are a significant threat in decentralized digital currencies. The blockchain incorporates a cryptographic framework using elliptic curve cryptography (secp256k1) for secure transactions, along with a unique double-spending detection mechanism. The system continuously monitors transaction patterns and compares them with the account balances to identify any discrepancies or fraudulent attempts at re-spending the same coins. Upon detecting a potential attack, the system isolates and removes the conflicting transactions to maintain the integrity of the blockchain. The paper also introduces a peer alert system to notify the network of suspicious activity and automatically mitigate risks by adjusting the affected blockchain state. Through various tests, including transaction validation, block mining, and attack detection, the system demonstrates robust functionality in a simulated environment. Future work includes performance comparisons with existing blockchain systems, focusing on accuracy, time efficiency, and scalability. The findings aim to contribute to the development of more secure and efficient blockchain frameworks, enhancing their reliability for practical use in cryptocurrency networks.

Index Terms **- ECC, PoW, PoS, PoA, PoSA, BTC**

1. INTRODUCTION

Double spending poses a significant threat to the integrity and trust of decentralized digital currencies by allowing the fraudulent reuse of digital assets. Unlike physical currencies, digital assets can be easily replicated, necessitating robust cryptographic and consensus-based safeguards. Blockchain technology addresses this issue through decentralized ledgers maintained by a network of nodes that validate transactions using consensus mechanisms like Proof of Work (PoW) and Proof of Stake (PoS). These mechanisms ensure each transaction is uniquely verified, timestamped, and immutably recorded, preventing attacks such as race attacks, Finney attacks, and 51% attacks. Advanced cryptographic techniques, including digital signatures, Merkle trees, and Byzantine Fault Tolerance (BFT), further enhance transaction authenticity and integrity. Practical implementations like Bitcoin, Ethereum, Cardano, and Solana demonstrate the effectiveness of these measures in maintaining transactional integrity and preventing double spending. Continuous advancements, such as multi-signature wallets, layer-2 scaling solutions, adaptive difficulty adjustments, and privacy-preserving technologies like Zero-Knowledge Proofs (ZKPs), strengthen blockchain security. Additionally, decentralized governance and interoperability protocols contribute to the resilience and scalability of blockchain networks. Together, these strategies ensure secure, reliable, and trustless peer-to-peer transactions, fostering the widespread adoption of blockchain-based currencies and applications across various industries.

1.1. Objectives

1.1.1. Develop a Secure Blockchain Architecture

Integrate elliptic curve cryptography (ECC) and digital signatures to ensure transaction authenticity. Utilize Proof of Stake (PoS) or Proof of Authority (PoA) with adjustable difficulty and secure hash functions like SHA-256. Implement multi-layered security protocols, including TLS/SSL and decentralized storage, to protect against attacks and unauthorized access.

1.1.2. Implement Double-Spending Attack Detection Mechanism

Establish a real-time monitoring system using machine learning to identify suspicious transaction patterns. Apply graph analysis and anomaly detection to compare transactions with account histories. Automatically flag and isolate potentially fraudulent transactions to prevent double spending.

1.1.3 Validate Blockchain Integrity

Maintain blockchain integrity through cryptographic verification of block links and Merkle trees for transaction validation. Conduct regular integrity and consensus checks to detect and correct tampering. Use multi-signature schemes and decentralized key management to secure transaction processes.

1.1.4 Evaluate the Efficiency and Accuracy of Detection Algorithms

Benchmark detection algorithms for speed, resource use, and scalability under various network conditions. Perform stress tests with high transaction volumes to ensure real-time detection. Assess accuracy with metrics like precision and recall, and optimize algorithms for better performance.

1.1.5 Analyze System Performance under Different Conditions

Test system performance by varying parameters such as transaction rate, block size, and network latency. Use simulations and real environments to evaluate detection accuracy and throughput. Identify and address bottlenecks with optimization techniques like dynamic difficulty and layer-two solutions.

1.1.6 Enhance System Resilience and Trust

Deploy PeerAlert for real-time security notifications and automatic threat mitigation. Implement workflows to quarantine nodes or adjust consensus in response to attacks. Maintain transparent, immutable logs and provide forensic tools to ensure accountability and build trust in the blockchain's security.

2. LITERATURE SURVEY

Double spending remains a critical threat to blockchain security, undermining the trustworthiness of decentralized digital currencies by allowing the same cryptocurrency to be spent multiple times before verification. Bitcoin's Proof-of-Work (PoW) mechanism, introduced by [1], ensures decentralization and security but is vulnerable to double-spending attacks, especially in fast-payment scenarios where rapid transaction confirmations are required. The [2] demonstrated that such attacks could be executed with significant probability and minimal cost, challenging the perceived robustness of PoW and highlighting the need for enhanced security measures. Additionally, the transparency of public ledgers can compromise user privacy through address-linking and network analysis, as highlighted by [3], raising concerns about the balance between transparency and privacy in blockchain systems.

To address these vulnerabilities, various solutions have been proposed. Real-time detection mechanisms aim to balance privacy with accountability, enhancing security without compromising Bitcoin's decentralized nature [4]. These mechanisms often involve monitoring transaction patterns and implementing automated responses to suspicious activities. Enhanced consensus protocols, such as hybrid Proof-of-Work and Proof-of-Stake (PoS) models, seek to improve both security and efficiency by combining the strengths of different consensus algorithms [5]. This hybrid approach can provide better resilience against attacks while reducing the energy consumption associated with traditional PoW.

Machine learning techniques are being employed to identify and prevent suspicious transaction patterns indicative of double spending, with frameworks like the Multistage Secure Pool (MSP) integrating AI-driven

analysis for real-time monitoring and defense [6]. These advanced analytical tools can detect anomalies and adapt to evolving attack strategies, providing a dynamic defense mechanism. Emerging technologies, including multi-party computation (MPC) and zero-knowledge proofs (ZKPs), offer promising enhancements to transaction validation processes, addressing limitations of traditional consensus mechanisms by enabling secure and private verification without revealing sensitive information [7].

Additionally, studies have focused on mitigating risks associated with mining pools by implementing decentralized blacklist management strategies to effectively isolate malicious nodes [8]. By identifying and excluding compromised or malicious participants, these strategies help maintain the integrity and security of the blockchain network. Performance evaluations under adaptive double-spend attacks (ADSA) indicate that increasing the number of confirmation blocks can significantly enhance blockchain resilience [9]. This approach ensures that transactions receive sufficient confirmations before being considered final, reducing the window of opportunity for double-spending attempts.

Simulation-based approaches, utilizing frameworks like Shadow, have been crucial in validating the scalability and effectiveness of these countermeasures under practical network conditions [10]. These simulations provide valuable insights into how proposed solutions perform in real-world scenarios, enabling the refinement and optimization of security measures. Overall, while significant advancements have been made in preventing double-spending through improved consensus algorithms, real-time detection, and advanced cryptographic techniques, ongoing research is essential to address evolving attack vectors and ensure the continued security and reliability of blockchain networks.

Equations

PoS depends on two factors: Value of a coin, Age of the coin. Let say, each node in the blockchain has a set of coins with different values. Let value of i^{th} coin of node N be C_i. Let the age of i^{th} coin of node N be Ai.

Assuming a node N puts n coins at stake. So,

$$\text{PoS} = \sum_{i=1}^{n} C_i \times A_i \qquad (1)$$

PoA depends on three factors: Time since node N is doing validations, Frequency at which node N has done validations in a given timestamp T, Percentage of Correct Validations done by node N.

Let the time since node N is doing validations be τ. So,

$$\text{PoA}_1 = \tau \qquad (2)$$

Let frequency at which node N has done correct validations in time stamp T be F_T. Let percentage of correctness be P. We will give exponential preference to the percentage of correctness. More the correctness, more the score. To reduce the computation complexity, we will normalize the percentage from the scale of 0-100 to 1-5. Thus, after normalization we get,

$$y = \frac{4P}{100} + 1 \qquad (3)$$

Thus,

$$\text{PoA}_2 = F_T \times e^{\left(\frac{4P}{100}\right)+1} \qquad (4)$$

From (2) and (4) we get,

$$\text{PoA} = \tau + F_T \times e^{\left(\frac{4P}{100}\right)+1} \qquad (5)$$

From (1) and (5) we get:

$$S = \tau + F_T \times e^{\frac{4P}{100}} + \sum_{i=1}^{n} C_i \times A_i$$

For each validator node N, this "S" value must be calculated. Whichever validator node gets the maximum score, gets the chance to do the mining.

3. RESEARCH METHODOLOGY

To address the shortcomings of both PoA and PoS, we propose a novel hybrid algorithm that leverages the strengths of each while mitigating their weaknesses. In this system, PoS is used to select a group of validators based on their stake, ensuring decentralization and reducing the wealth centralization issue. PoA is then employed within this selected group, where trusted validators are responsible for block creation, ensuring fast transaction processing.

This hybrid approach balances the decentralization of PoS with the efficiency of PoA, while also mitigating the risks of validator corruption and over-centralization in either system. Validators are regularly rotated to prevent collusion and maintain security, ensuring a robust defense against double spending and other attack vectors.

4. CONCLUSION

The culmination of this project represents a significant advancement in addressing the double-spending problem within blockchain networks through the innovative development and implementation of a hybrid Proof of Authority (PoA) and Proof of Stake (PoS) consensus algorithm. This hybrid consensus mechanism strategically combines the strengths of both PoA and PoS, creating a more secure, efficient, and reliable blockchain framework. By leveraging PoA's capability for rapid block validation through a trusted group of validators and PoS's ability to enhance network security by incentivizing stakeholders to stake their assets, the proposed solution achieves a balanced approach between swift transaction processing and decentralized trustworthiness. This balance is essential in mitigating double-spending attacks, which exploit vulnerabilities in transaction validation and consensus protocols to illicitly duplicate digital assets.

The hybrid PoA-PoS model significantly enhances the security posture of blockchain systems. PoA contributes by limiting block validation to a pre-approved set of validators, thereby reducing the attack surface and minimizing the risk of Sybil attacks and other malicious activities. Concurrently, PoS introduces an economic deterrent against malicious behavior by requiring validators to stake cryptocurrency, aligning their incentives with the network's integrity and discouraging attempts to manipulate the system for personal gain. This synergistic effect ensures the network is resilient against both internal threats from validators and external threats from potential attackers seeking to exploit consensus weaknesses.

REFERENCES

[1] Karame, G. O., Androulaki, E., Roeschlin, M., Gervais, A., & Čapkun, S. (2015). Misbehavior in Bitcoin: A study of double-spending and accountability. ACM Transactions on Information and System Security, 18(1), Article 2.

[2] Podolanko, J. P., Ming, J., & Wright, M. (2017, April). Countering double-spend attacks on bitcoin fast-pay transactions. In Proc. Workshop Technol. Consum. Protection (pp. 1-3). https://www.ieee-security.org/TC/SPW2017/ConPro/papers/podolanko-conpro17.pdf

[3] Begum, A., Tareq, A., Sultana, M., Sohel, M., Rahman, T., & Sarwar, A. (2020). Blockchain attacks analysis and a model to solve double spending attack. International Journal of Machine Learning and Computing, 10(2), 352-357. https://www.ijml.org/vol10/942-M114.pdf

[4] Nicolas, K., & Wang, Y. (2019). A novel double spending attack countermeasure in blockchain. In 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) (pp. 0383–0388). IEEE. https://doi.org/10.1109/UEMCON47517.2019.8992991

[5] Akbar, N., Muneer, A., Elhakim, N., & Fati, S. (2021). Distributed hybrid double-spending attack prevention mechanism for proof-of-work and proof-of-stake blockchain consensuses. Future Internet, 13(11), 285. https://doi.org/10.3390/fi13110285

[6] Zheng, J., Huang, H., Zheng, Z., & Guo, S. (2024). Adaptive double-spending attacks on PoW-based blockchains. IEEE Transactions on Dependable and Secure Computing, 21(3), 1098–1110. https://doi.org/10.1109/TDSC.2023.3268668

[7] Pérez-Solà, C., Delgado-Segura, S., Navarro-Arribas, G., & Herrera-Joancomartí, J. (2019). Double-spending prevention for Bitcoin zero-confirmation transactions. International Journal of Information Security, 18(4), 451–463. https://doi.org/10.1007/s10207-018-0422-4

[8] Wang, J. L., Liu, Q., & Song, B. (2022). Blockchain-based multi-malicious double-spending attack blacklist management model. Journal of Supercomputing, 78(12), 14726–14755. https://doi.org/10.1007/s11227-022-04370-1

[9] Kumar, A., Kumar Sah, B., Mehrotra, T., & Rajput, G. K. (2023). A review on double spending problem in blockchain. In 2023 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES) (pp. 881–889). IEEE. https://doi.org/10.1109/CISES58720.2023.10183579

[10] Ramezan, G., & Leung, C. (2020). Analysis of proof-of-work-based blockchains under an adaptive double-spend attack. IEEE Transactions on Industrial Informatics, 16(11), 7035–7045. https://doi.org/10.1109/TII.2020.2977689

[11] Fahim, S., Rahman, S. K., & Mahmood, S. (2023). Blockchain: A comparative study of consensus algorithms PoW, PoS, PoA, PoV. Int. J. Math. Sci. Comput, 3, 46-57. https://www.mecs-press.org/ijmsc/ijmsc-v9-n3/IJMSC-V9-N3-4.pdf

[12] An, A. C., Diem, P. T. X., Van Toi, T., & Binh, L. D. Q. (2019, November). Building a product origins tracking system based on blockchain and PoA consensus protocol. In 2019 international conference on advanced computing and applications (ACOMP) (pp. 27-33). IEEE. https://ieeexplore.ieee.org/abstract/document/9044220

[13] Pawar, A., Barthare, D., Rawat, N., Yadav, M., & Shirole, M. (2021, October). BlockAudit 2.0: PoA blockchain based solution for secure Audit logs. In 2021 5th International Conference on Information Systems and Computer Networks (ISCON) (pp. 1-6). IEEE. https://ieeexplore.ieee.org/abstract/document/9702378

[14] Iqbal, M., & Matulevičius, R. (2021). Exploring sybil and double-spending risks in blockchain systems. IEEE Access, 9, 76153-76177. https://ieeexplore.ieee.org/abstract/document/9435780

[15] Nicolas, K., Wang, Y., Giakos, G. C., Wei, B., & Shen, H. (2020). Blockchain system defensive overview for double-spend and selfish mining attacks: A systematic approach. IEEE Access, 9, 3838-3857. https://ieeexplore.ieee.org/abstract/document/9308934