Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 5s (2025)

Optimizing IoT Security with Blockchain: Overcoming Computational Challenges

Hitesh Gehani[1], Shubhangi Rathkanthiwar[2], Siddhant Jaiswal[3], Arti Buche[4]

[1]Research Scholar, Department of Electronics Engineering, Yeshwantrao Chavan College of Engineering, Nagpur, India.
[1]hkgehani@gmail.com

[2]Professor, Department of Electronics Engineering, Yeshwantrao Chavan College of Engineering, Nagpur, India.
[2]svr_1967@yahoo.com

[3,4]Assistant Professor, School of Computer Science & Engineering, Ramdeobaba University, Nagpur, India.
[3]jaiswalsj@rknec.edu, [4]artibuche@gmail.com

Article History:

Received: *09-10-2024*

Revised: *27-11-2024*

Accepted: *07-12-2024*

Abstract:

The Internet of Things (IoT) has made its way into business and home applications, allowing for automation, monitoring, control, and analysis. Blockchain-based solutions use encryption, hashing, permanence, credibility, transparency, trustworthiness, and other security measures to protect IoT networks from numerous attacks. However, integrating blockchains involves complex computational tasks such as creating hashes, verifying hashes, mining blocks, etc, which adds extra computational burden on the system. This increased computational burden often reduces the quality of service for the system, making it less suitable for real-time and high-performance applications. To address this issue, this text introduces an AI algorithm for generating side chains. These side chains offer high security performance like regular blockchains but are generally less computationally complex. As a result, they can be used for secure real-time IoT applications.

Keywords: Blockchain, Security, IOT, Attack probability.

1. Introduction

The system will select an IoT application and begin with Keen Contract-based Ethereum blockchain usage for the application. It Store the data around the blockchain utilized, and its parameters on the chain itself. The system will analyse the length of the chain, complexity of mining, and traceability and alter the blockchain algorithm. Use profound nets and other AI procedures to memorize from the arrange structure and re-configure the blockchain. Perform the chaining and side-chaining based on the application chosen and assess its execution stack on the system. Apply an AI layer which is able assess on the off chance that the calculation must alter, and alter the framework parameters appropriately.

2. Literature Review

While navigating Online Social Networks (OSN) through suggestion engines. In addition, it increases a number of privacy-related issues. To guarantee the confidentiality and anonymity of user data, two smart contracts, SCSGI and SCSTI are created [1]. This study explores the use of sketches, such as Bloom Filter and HyperLog, to identify suspicious accounts without requiring the examination of the entire blockchain data. reduce the amount of memory used by the detection process by 90%-96% and reduce the time complexity by 86%[2]. Here author proposes a platform using federated learning and

private blockchain technology within a fog-IoT network. According to experimental results, the introduced implementation can effectively preserve a patient's privacy and a predictive service's integrity[3]. As blockchains have different types named public and private blockchains, we recommend private blockchains be implemented where no anyone can make transactions and mine the transactions. Patients, doctors, and hospital organizations care for their privacy, and authorized access to others' data, is the reason for the choice of the private blockchain[4]. Many proposals are recommended for advancement of decentralized blockchain applications. The work in [1] uses these rules to convey a decentralized cross breed on-and-off blockchain dependent on Ethereum-based shrewd agreements for further developed security and high QoS execution.

Here, diverse IoT applications that use sidechains for high velocity, high straightforwardness, and low energy are talked about[6] Resource trade can be performed on both permissioned and permissionless blockchains, however this work proposes a model for the previous one by means of the utilization of a compelling interruption location framework dependent on AI[7]. This work proposes the utilization of savvy contracts joined with cross breed blockchain model. The mixture model consolidates agreement calculations for public and union chains [8]. This work proposes the utilization of such a simultaneous mining calculation that utilizes repetitive calculation to track down measuring data about the shrewd agreement [9] The work in this paper proposes the utilization of sidechains for vehicular organizations, wherein a nuclear cross-chain trade-based administration framework a.k.a. ACSMS is characterized [10]. An exceptionally issue lenient organization can be practically reached out for performing activities like resource trade [11], token administration and information provenance [12].

The work in [12] proposes a n/2 shortcoming lenient component utilizing blockchain sharding, wherein the organization can recuperate information regardless of whether half of hubs are defective. Arrangement overheads of these numerous chain frameworks should be assessed as far as energy, postponement and cost required for access, stockpiling, move and token administration tasks. This expense assessment is done in [13], and should be utilized for any sort of blockchain organization that utilizes numerous chains for compelling overhead investigation. The work in [14] and [15] recommends utilization of AI models like Opti Shard, DAG, interleaving and OptChain separately.

These models target assessing ideal size for the sidechains to further develop generally speaking framework execution while keeping up with undeniable degree of safety in the organization. Here, specialists have used equal handling on DAGs to additionally lessen postponement of mining, subsequently further developing framework throughput [16]. Ethereum based shrewd agreements are utilized alongside heuristics based sharding for dealing with the blockchain [17]. Here, various access tokens are overseen on various blockchains to improve interoperability [18]. Here, specialists have proposed the utilization of exchange history for planning information to shards with compelled memory limits, which permits evacuation of redundancies in the framework [19]. The work in [20] and [21] proposes conventions for compelling shard portion. Issue identification and expulsion from blockchain organizations can be performed by powerful shard designation, and trust foundation.

The work in [22] proposes a convention for trust the board to configuration shortcoming open minded organizations. Mix of these models can help with further developing the adaptation to internal failure capacities of the framework, and subsequently improving QoS execution for the organization. Here, examined DAG utilizes verification of-work (PoW) as an agreement calculation for approval [23]. The

security execution of these blockchain executions can be additionally reached out by option of protection upgrade procedures like Garlic steering and onion directing [24]. Here, author proposes a shortened hashing engineering that assesses security level of square fields, and hashes just those fields which require significant degree of protection [25] The work in [26] examines distinctive agreement conventions like Proof-of-Stake (PoS), Proof-of-Space (PoSp), Proof-of-Authority (PoA), and so forth These conventions can be utilized with the current DAG-based sidechain model to assess its continuous exhibition [26]. This work proposes the utilization of Two-Phase Cooperative Bargaining Game Approach to lessen postponement of confirmation through choosing restricted arrangement of sidechains for block check [27]. This idea is utilized [28] for conveying elite execution and enhanced security banking applications with sidechains. It is seen that blockchain QoS execution is improved through the utilization of sidechaining, this work proposes different essential and optional execution compromises which should be dealt with while planning sidechaining applications [29].

3.Methods

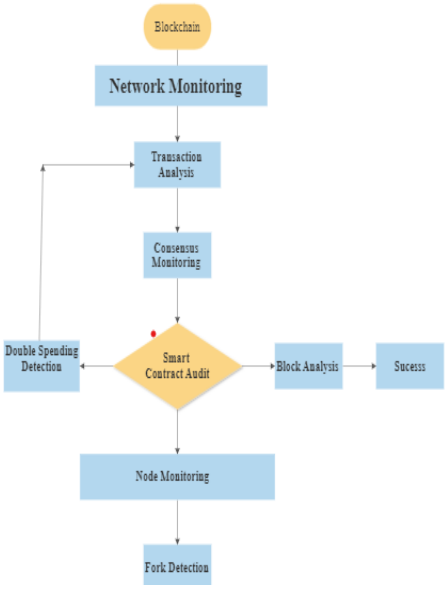

Fig 1: Blockchain security Model

Blockchain is the starting point of the process. Network Monitoring will be performed by the blockchain network. It Leads to Transaction Analysis and Consensus Monitoring. After computing the results from Transaction Analysis, it Evaluates transactions for irregularities or inconsistencies. According to the outcome the Feedback loop is given to Network Monitoring if issues are detected. At the last step it ensures the network's consensus mechanism operates correctly. Which Leads to Smart Contract Audit and again checks smart contracts for vulnerabilities. If issues are detected, leads to Double Spending Detection and if no issues then proceed to Block Analysis. The Double Spending Detection is used to identify and prevents duplicate spending of digital assets. The Feedback loop is then sent to Transaction Analysis and then to Block Analysis for Validating the block data that Leads to Success upon completion. The Node Monitoring is used to track the health and performance of network nodes which Leads to Fork Detection. After fork detection the system detects splits in the blockchain network to maintain integrity and finally it concludes the process.

Calculation Of Delay:

Time stamp 2(ts2) = Time taken at instant 1. Time taken at instant 2

(D) = (Time stamp 2 (ts2) - Time stamp (ts))

AD = Delay / Len(blockchain)

Where, ts2: Ideal time stamp, D: Delay calculation, AD: Average Calculation, Len(blockchain): Length of current Blockchain

By adjusting the difficulty target, the Nakamoto consensus protocol helps regulate the rate at which new blocks are added to the blockchain, contributing to the security and stability of the blockchain network.

The difficulty adjustment algorithm works as follows:

Target Block Time (Tb): The network sets a target block time, which is the desired time interval between the creation of consecutive blocks. In Bitcoin, the target block time is approximately 10 minutes.

Current Block Time (Tc): The time taken to mine the last few blocks is measured, and the average block time (Tc) is calculated.

Difficulty Adjustment: The difficulty target is adjusted based on the difference between the current block time (Tc) and the target block time (Tb). The adjustment is made approximately every 2016 blocks (approximately every two weeks in Bitcoin).

If Tc > Tb: The network assumes that blocks are being mined too quickly, and the difficulty target is increased. This makes mining more challenging and, in turn, increases the time it takes to find a valid block, helping to bring the block time closer to the target.

If Tc < Tb: The network assumes that blocks are being mined too slowly, and the difficulty target is decreased. This makes mining easier and reduces the time it takes to find a valid block, aiming to bring the block time closer to the target.

Different types of attacks on security:

Malware Attacks: Malicious software that includes viruses, worms, Trojans, ransomware, spyware, adware, and more. Malware is designed to harm or exploit computer systems and data.

Phishing Attacks: Social engineering attacks that trick users into revealing sensitive information like login credentials or personal data through fake websites or emails that appear legitimate.

Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks: These attacks overload a target's server or network with excessive traffic, rendering it unavailable to legitimate users.

Man-in-the-Middle (MitM) Attacks: An attacker intercepts and potentially alters communication between two parties without their knowledge, allowing them to eavesdrop or manipulate data.

SQL Injection: Attackers inject malicious SQL code into input fields to manipulate or access unauthorized data in a database.

Password Attacks: Techniques like brute-force, dictionary attacks, or rainbow table attacks to guess or crack passwords.

4.Results

Module 1: Design a blockchain based system for different number of blocks.

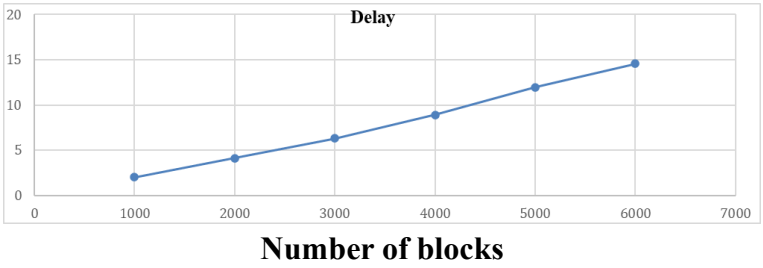

Fig 2: Graphical representation of Delay for mining different number of blocks

Module 2: Design a blockchain based system for testing the security of the application If number of blocks mine are 1000 then results is as shown below, for different value of attack probability.

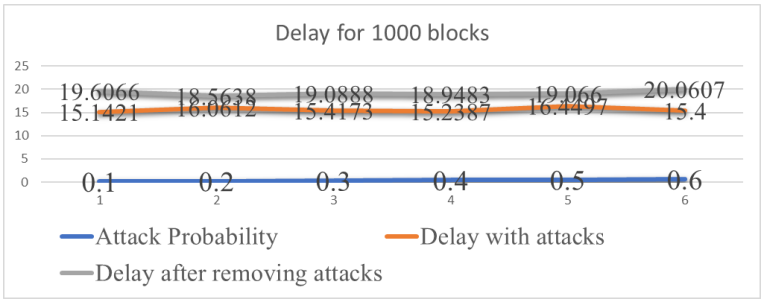

Fig 3: Graphical Analysis of Delay with attacks and after removing attacks

If number of blocks mine are 2000 then results is as shown below , for different value of attack probability.

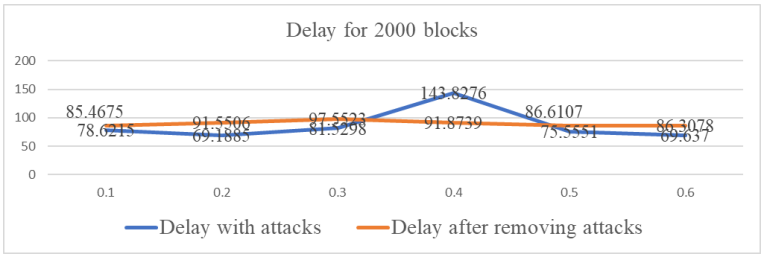

Fig 4: Graphical Analysis of Delay with attacks and after removing attacks

By implementing these steps, blockchain administrators and security teams can enhance their ability to detect and respond to potential attacks on blockchain security effectively.

Early Detection of Threats: Continuous monitoring and analysis of network activities, transactions, and consensus mechanisms enable early detection of potential security threats or attacks.

Timely Response: With real-time monitoring and analysis, security teams can respond quickly to emerging threats, minimizing the impact and reducing the window of vulnerability.

Protection Against Double Spending: Implementing double-spending detection mechanisms protects against the fraudulent use of cryptocurrency within the blockchain.

Data Integrity Assurance: Analysing block data ensures that the blockchain's data remains tamper-resistant and maintains its integrity.

Collaboration and Community Support: Engaging with the blockchain community and collaborating with other stakeholders fosters knowledge-sharing, helping to collectively address security challenges.

Module 3: Design a blockchain based system for testing the security of the application Updated

If number of blocks mine are 2000 then results is as shown below , for different value of attack probability.

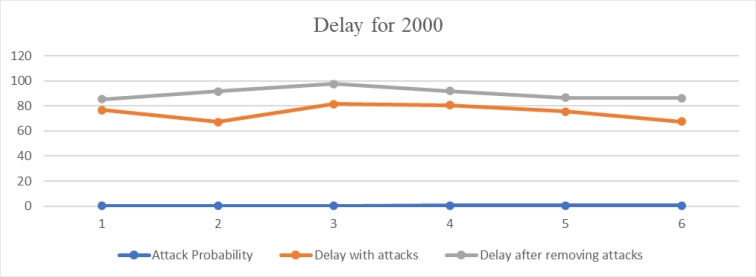

Fig 5: Graphical Analysis of Reduced Delay with attacks and after removing attacks

5.Discussion

An improvement in overall security of the IoT based blockchain network. Due to addition of AI, there might be a reduction in overall complexity of the network, as the network's dependency on a single blockchain algorithm will be reduced, therefore the rule satisfaction process of the algorithm (which is the most complex portion), will be relaxed, thereby reducing the complexity of the network. An increase in the overall QoS of the secure network

References

[1] A. Kumar, T. Vyas, S. Ahmed, N. Girdharwal, E. Vijayakumar and A. Thangavelu, "Security and Privacy Enabled Framework for Online Social Networks using Blockchain," 2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2023, pp. 641-647, doi: 10.1109/ICESC57686.2023.10193119.

[2] Deepa, V.V., Thamotharan, B., Mahto, D. et al. Smart embedded health monitoring system and secure electronic health record (EHR) transactions using blockchain technology. Soft Comput 27, 12741–12756 (2023). https://doi.org/10.1007/s00500-023-08893-4

[3] T. Voronov, D. Raz and O. Rottenstreich, "A Framework for Anomaly Detection in Blockchain Networks With Sketches," in IEEE/ACM Transactions on Networking, doi: 10.1109/TNET.2023.3298253.

[4] M. J. Baucas, P. Spachos and K. N. Plataniotis, "Federated Learning and Blockchain-Enabled Fog-IoT Platform for Wearables in Predictive Healthcare," in IEEE Transactions on Computational Social Systems, vol. 10, no. 4, pp. 1732-1741, Aug. 2023, doi: 10.1109/TCSS.2023.3235950.

[5] Liu, J., Yan, L. & Wang, D. A Hybrid Blockchain Model for Trusted Data of Supply Chain Finance. *Wireless Pers Commun* (2021). https://doi.org/10.1007/s11277-021-08451-x

[6] Woo, S., Song, J., Kim, S. *et al.* GARET: improving throughput using gas consumption-aware relocation in Ethereum sharding environments. *Cluster Comput* **23,** 2235–2247 (2020). https://doi.org/10.1007/s10586-020-03087-1

[7] Xu, Y, Huang, Y, Shao, J, Theodorakopoulos, G. A flexible *n*/2 adversary node resistant and halting recoverable blockchain sharding protocol. *Concurrency Computat Pract Exper*. 2020; 32:e5773. https://doi.org/10.1002/cpe.5773

[8] Abuidris, Y., Kumar, R., Yang, T. and Onginjo, J. (2021), Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding. ETRI Journal, 43: 357-370. https://doi.org/10.4218/etrij.2019-0362
[9] A. Mizrahi and O. Rottenstreich, "State Sharding with Space-aware Representations," 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, ON, Canada, 2020, pp. 1-9, doi: 10.1109/ICBC48266.2020.9169402.
[10] Yan Wang, Jixin Li, Wansheng Liu, Aiping Tan, "Efficient Concurrent Execution of Smart Contracts in Blockchain Sharding", *Security and Communication Networks*, vol. 2021, Article ID 6688168, 15 pages, 2021. https://doi.org/10.1155/2021/6688168
[11] Chaoxia Qin, Bing Guo, Yan Shen, Tao Li, Yun Zhang, Zhen Zhang, "A Secure and Effective Construction Scheme for Blockchain Networks", *Security and Communication Networks*, vol. 2020, Article ID 8881881, 20 pages, 2020. https://doi.org/10.1155/2020/8881881
[12] PolyShard: Coded Sharding Achieves Linearly Scaling Efficiency and Security Simultaneously, https://arxiv.org/abs/1809.10361
[13] Okanami N., Nakamura R., Nishide T. (2020) Load Balancing for Sharded Blockchains. In: Bernhard M. et al. (eds) Financial Cryptography and Data Security. FC 2020. Lecture Notes in Computer Science, vol 12063. Springer, Cham. https://doi.org/10.1007/978-3-030-54455-3_36
[14] Analysing and Improving Shard Allocation Protocols for Sharded Blockchains, https://www.semanticscholar.org/paper/Analysing-and-Improving-Shard-Allocation-Protocols-Han-Yu/13979b32449431c41ecc7bcd1450bf73c7b87495
[15] Yibin Xu and Yangyu Huang. 2020. An n/2 byzantine node tolerate blockchain sharding approach. In Proceedings of the 35th Annual ACM Symposium on Applied Computing (SAC '20). Association for Computing Machinery, New York, NY, USA, 349–352. DOI: https://doi.org/10.1145/3341105.3374069
[16] J. Yun, Y. Goh and J. -M. Chung, "Trust-Based Shard Distribution Scheme for Fault-Tolerant Shard Blockchain Networks," in IEEE Access, vol. 7, pp. 135164-135175, 2019, doi: 10.1109/ACCESS.2019.2942003.
[17] de Vos, M., Ileri, C.U. & Pouwelse, J. XChange: A Universal Mechanism for Asset Exchange between Permissioned Blockchains. *World Wide Web* (2021). https://doi.org/10.1007/s11280-021-00870-x
[18] Token Economy 101, or why Blockchain-powered decentralized networks are important, https://pentremont.medium.com/token-economy-101-or-why-blockchain-powered-decentralized-networks-are-important-310de1cc8bac
[19] Sigwart, M., Borkowski, M., Peise, M. *et al.* A secure and extensible blockchain-based data provenance framework for the Internet of Things. *Pers Ubiquit Comput* (2020). https://doi.org/10.1007/s00779-020-01417-z
[20] xLumi: Payment Channel Protocol and Off-chain Payment in Blockchain Contract Systems, https://arxiv.org/abs/2101.10621
[21] Blockchain technology in the energy sector: A systematic review of challenges and opportunities, https://www.sciencedirect.com/science/article/pii/S1364032118307184
[22] Chenkai Tan, Shaoyi Bei, Zhengjun Jing, Neal Xiong, "An Atomic Cross-Chain Swap-Based Management System in Vehicular Ad Hoc Networks", *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 6679654, 14 pages, 2021. https://doi.org/10.1155/2021/6679654
[23] Towards Automated Benchmark Support for Multi-Blockchain Interoperability-Facilitating Platforms, https://arxiv.org/abs/2103.03866
[24] S. Park, S. Oh and H. Kim, "Performance Analysis of DAG-Based Cryptocurrency," 2019 IEEE International Conference on Communications Workshops (ICC Workshops), Shanghai, China, 2019, pp. 1-6, doi: 10.1109/ICCW.2019.8756973.
[25] W. Wang et al., "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks," in IEEE Access, vol. 7, pp. 22328-22370, 2019, doi: 10.1109/ACCESS.2019.2896108.
[26] Sidechain technologies in blockchain networks: An examination and state-of-the-art review, https://www.sciencedirect.com/science/article/abs/pii/S1084804519303315
[27] Blockchain and Distributed Ledger Technology Use Cases, https://www.springer.com/gp/book/9783030443368
[28] Y. Pang, "A New Consensus Protocol for Blockchain Interoperability Architecture," in IEEE Access, vol. 8, pp. 153719-153730, 2020, doi: 10.1109/ACCESS.2020.3017549.
[29] Blockchain based Decentralized Applications: Technology Review and Development Guidelines,https://www.researchgate.net/publication/339971962_Blockchain_based_Decentralized_Applications_Technology_Review_and_Development_Guidelines