Enhancing Blockchain Security: A Novel Algorithmic Approach to Preventing 51% Attacks

Emad Shafie[1] & Fawaz A. Mereani[2]

[1]Department of Engineering and Applied Science, Applied College, Umm Al-Qura University, Mecca, Saudi Arabia | Email: Eashafie@uqu.edu.sa

[2]Corresponding Author | Department of Computer and Applied Science, Applied College, Umm Al-Qura University, Mecca, Saudi Arabia | Email: famereani@uqu.edu.sa

Abstract

Many studies have shown that blockchain is not as secure as it was thought to be despite its components and operations involving many algorithms. Therefore, researchers searched and found many novel algorithms to enhance blockchain security. This study aimed to enhance blockchain security using a novel algorithmic approach to prevent at least 51% of attacks, with three objectives. The novel algorithm was termed Dynamic Node Contribution (DNC), which dynamically adjusts mining power distribution based on node reliability and historical contribution to the network. The DNC algorithm employs a reputation system, where each node earns a reputation score based on its mining history, transaction validation accuracy, and consistency. Comparing the baseline tests and tests after the introduction of DNC into the system, overall, it can be concluded that the DNC algorithm has the potential to fortify blockchain networks against 51% of attacks while maintaining efficient operation with an effective reputation-base system. The algorithm's capability to mitigate the risk of such attacks shows enhanced overall network robustness. The slight increase in transaction confirmation time, averaging 14.3 seconds compared to 12.5 seconds without DNC, can be attributed to the dynamic adjustments made by the algorithm to improve security. This increase is outweighed by increased security.

Keywords: Blockchain, Novel Algorithms, Dynamic Node Contribution (DNC), Prevention of 51% attacks

Introduction

Enhancing blockchain security is crucial for ensuring decentralised transaction networks' longevity, integrity, and confidentiality. This can be achieved by utilising cryptographic data encryption and verification techniques, implementing strong consensus protocols to thwart tampering, and applying network security strategies to counter external threats. Furthermore, the security of smart contracts, access control strategies, and adherence to regulatory standards are vital for strengthening blockchain ecosystems. By embracing a multi-faceted approach that tackles technical, operational, and regulatory challenges, blockchain systems can improve their security stance and build trust among users and stakeholders (Leong, Leong, & Leong, 2024).

Algorithmic approaches

Velmurugadass, Dhanasekaran, Shasi Anand, and Vasudevan (2021) created an innovative framework to monitor activities on specific data evidence. This includes a Cloud-based Software Defined Network (SDN) with 100 mobile nodes (IoT devices), an open flow switch, blockchain-based controllers, a cloud server, an Authentication Server (AS), and an investigator. Users register with the AS to receive a secret key through Harmony Search Optimization (HSO). Packets in mobile nodes are encrypted using the Elliptic Curve Integrated Encryption Scheme (ECIES) and sent to the cloud server. The SDN controller uses a blockchain to protect evidence and user signatures based on the SHA-256 Cryptographic Hash Algorithm. The investigator conducts identification, evidence collection, analysis, and report generation using the Logical Graph of Evidence (LGoE). The authors present results that include response time, evidence insertion and verification times, computational overhead, total change rate, hash computation, key generation, and encryption and decryption times relative to the number of users. Ultimately, investigators can obtain evidence from the controller and compile it as a Logical Graph of Evidence (LGoE). Experimental results showed the system excelled in response time, accuracy, throughput, and security parameters. However, no percentage reduction in attacks was given in this paper.

Sharma, Upadhyay, and Sharma (2024) present a hybrid algorithm for detecting malware attacks to enhance cybersecurity in blockchain systems by addressing issues such as Byzantine fault tolerance, re-entrancy, and DDoS attacks. This framework integrates SHA-256 and DSA to analyse these malware attacks and has been developed to reduce malicious activities within a single block. The approach improves computational efficiency and accelerates processing in node networks. The authors tested the framework on the NSL-KDD dataset, achieving a precision of 64.29%, a recall of 73.33% and an F1 score of 68.03%. To ensure effective mitigation, an analysis of time and space complexity showed a combination of constant and linear time operations. The results indicated that the algorithm successfully detects and mitigates targeted attacks while maintaining optimal performance across different attack vectors. Thus, the algorithm was useful to detect 64.29% of the three types of attacks. This paper did not deal with prevention.

In a review of the security and privacy techniques to achieve security in blockchain-based systems, Leng, Zhou, Zhao, Huang, and Bian (2020) discussed the representative consensus algorithms, hash chained storage, mixing protocols, anonymous signatures, non-interactive zero-knowledge proof, and a few others.

The above three papers show that algorithms were used only to detect the attacks rather than reduce or prevent them by enhancing blockchain security systems. Based on this gap, the following aim and objectives were formed for this study.

Aim-

To enhance blockchain security using an algorithmic approach to prevent at least 51% of attacks.

Objectives-

a) To survey the literature for available approaches.
b) To select a suitable algorithmic approach based on the literature review.
c) To use the selected approach and evaluate whether the aim of preventing at least 51% of attacks.

Literature Review

Many papers discuss algorithmic approaches to enhance blockchain security. There are consensus mechanisms like Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Practical Byzantine Fault Tolerance (PBFS) and Hybrid Consensus. Cryptographic Hashing uses Hashing Algorithms and Hash Chains. Digital signatures use Key Pairs or Encryption and Decryption. Other algorithms include Snake Optimisation Algorithm (SoA), Elliptic Curve Integrated Encryption Scheme (ECIES) and Two-Stage Encryption (TSE). Ferdous, Chowdhury, Hoque, and Colman (2020) discussed PoW and PoS algorithms in detail. Ferdous, Chowdhury, and Hoque (2021) noted that a crucial component of any blockchain system is its underlying consensus algorithm, which determines its performance and security in many ways. They extended their previous work beyond consensus algorithms, considering hybrid consensus algorithms like proof of research and proof of burn. To protect the privacy of patients in shared health records, Hussein, et al. (2018) used a genetic algorithm with a cryptographic hash key generator to optimise the queuing optimisation technique. Tests showed the algorithm-used system to be robust, efficient, immune and scalable.

In a cloud computing IoT environment, Velmurugadass, Dhanasekaran, Shasi Anand, and Vasudevan (2021) used an Elliptic Curve Integrated Encryption Scheme (ECIES) and the SHA-256 Cryptographic Hash Algorithm to enhance blockchain security.

Shrivastava, Alam, and Alam (2023) created a blockchain-based modified infinite chaotic elliptic cryptography (MICEC) to enhance and strengthen security in cloud computing. The process consists of three phases: authentication protection, ownership safeguarding, and validation of identity mapping. Initially, MICEC is utilised for the authentication procedure, integrating infinite elliptic curve cryptography with a modified chaotic neural network for key generation and data encryption. Furthermore, a hash function is produced using the enhanced message digest five algorithm. Next, the enhanced Message Content Recommendation Algorithm utilising Latent Dirichlet Allocation is employed to evaluate the score values. Finally, the validation process is conducted based on the digests using cosine similarity matching criteria.

Venkatesan and Rahayu (2024) proposed hybrid consensus algorithms that integrate machine learning (ML) techniques to address vulnerabilities in blockchain networks, focusing on cyber-attack prediction, anomaly detection, and feature extraction. These methods enhance the security, trust, and robustness of consensus protocols. The research explores various ML techniques alongside hybrid algorithms, such as Delegated Proof of Stake Work (DPoSW) and Delegated Byzantine Proof of Stake (DBPoS), for improved security and decision-making. The methodology was validated within decentralised networks using the ProximaX blockchain platform, demonstrating energy efficiency and adaptability. However, practical implementation of these ML-based models faces challenges like scalability, latency, and potential adversarial attacks, which need resolution for real-world applications. The authors provided only descriptive results without quantitative data.

Hash algorithms can be used to make blockchain integration safe, and many of them can solve problems with data integrity and security that arise when using blockchain technology. However, they can also have problems with time, lack of resources, and use too much memory. To solve these problems, Ali, Hazar, Mabrouk, and Zrigui (2023) developed an algorithm to create a hash based on a chaos key using logistic maps, and lightweight cryptography is proposed (Hamming Bird 2). Hash outputs were tested in terms of time and hardness to guess using cryptanalysis tools. The proposed algorithm was tested using a cryptanalysis site based on brute force attacks. The result showed that the site could not identify the modified hash using all the cryptanalysis settings that generated a strong hash against attacks. The authors observed that SHA-1, SHA-2, and SHA-256 are the hash algorithms that provide the greatest level of safety and dependability in blockchain technology.

The steps involved in the study by Rajawat, Goyal, Kumar, and Singh (2024) were a detailed examination of the current state of blockchain security mechanisms, the creation of a virtual blockchain, incorporating the SOM+LSTM algorithm and putting the algorithm through its paces to see its speed of detection and defence against different security risks. Using the SOM+LSTM technique, they were able to increase the detection rates of possible security risks, such as Sybil and DDoS attacks. Enhanced reaction times when compared to conventional security techniques for attack prediction and prevention. Tests demonstrated the ability of the algorithm to adapt and learn from new patterns of attacks, assuring long-term sustainability. The accuracy, precision, recall and F1 scores were above 94% for the proposed LSTM +SOM integrated with blockchain. All these values were higher than the other algorithms tested.

The well-known SHA256 algorithm has recently been targeted by attacks, leading to the creation of more secure hash functions. Salih and Kashmar (2024) introduced a new modification strategy to boost the efficiency of SHA256 by implementing an extended technique for producing a 288-bit message digest and cutting down the round count to 44 from 64, all while ensuring the data's diffusion is preserved through a complex iterative process that includes numerous rounds of bitwise and logical operations. This adjustment guaranteed that even minor changes in the input data resulted in significant differences in the output hash, thereby upholding its cryptographic characteristics. The proposed hash function, SHA288, provided enhanced security, collision resistance, and preimage resistance while also ensuring a quicker execution time than SHA256. The experiments conducted on this new algorithm demonstrated its impressive safety and resilience against attacks and showcased exceptional performance in random tests, further bolstering its security features.

The importance of 51% was illustrated by Park and Park (2017) using the Bitcoin example. In a Bitcoin environment, a 51% attack alters and falsifies 51% of the ledgers simultaneously. Consequently, coordinating such an attack is extremely challenging. The attacker needs to possess 51% or greater computational power of all participants, deliberately create two branches, and designate the intended branch as the authentic blockchain. To address this issue, an intermediary verification process should be implemented to avert any such manipulation.

Testing novel algorithms

Since this study is about testing a novel algorithm, some papers related to this topic are reviewed here. While Hussein, et al. (2018) tested a genetic algorithm, Xiong, et al. (2021) tested the Elliptic Curve Digital Signature Algorithm (ECDSA), and Ali, et al. (2022) used an attribute-based signing algorithm, an evaluation algorithm and an access control algorithm implemented through smart contracts, to enhance the security of shared health records. Qahtan, et al. (2022) tested a new version of the MCDM weighting method, s-FWZIC (fuzzy weighted with zero inconsistency), for weighing the security and privacy properties of blockchain-based IoT in the healthcare industry. The method was efficient, with good access control, low integrity, and good optimisation. To enhance the security, trustworthiness, reliability and confidentiality of the data in healthcare IoT (oHT), Ali, et al. (2022) proposed a novel group theory (GT)--based binary spring search (BSS) algorithm consisting of a hybrid deep neural network approach. The approach was effective in detecting the intrusion within the IoT network. Blockchain as a distributed database was proposed with a homomorphic encryption technique to ensure a secure search and keywords-based access to the database. Simulations based on the blockchain-based tools Hyperledger Fabric and OrigionLab for analysis and evaluation showed that the proposed framework led to better security and searchable mechanisms.

In a study using a novel deep learning and blockchain-based energy framework for Smart Grids (DeepCoin) Ferrag and Maglaras (2019) used Byzantine fault tolerance (PBFT) algorithm to achieve a consensus inside the blockchain-based energy network.

The Quantum Signature Validation Algorithm (QSVA) was tested by Torres, Ortega, and Martin-Delgado (2025) as a novel approach based on quantum technology has been developed to improve the detection of altered transactions within blockchain networks. By harnessing the significant capabilities of quantum computing, particularly in the context of transaction-oriented blockchains, the QSVA aims to exceed traditional techniques in terms of both speed and effectiveness. The QSVA employs a quantum walk method combined with PageRank-based algorithms, offering a strong system for pinpointing fraudulent transactions. Simulation findings indicated that QSVA outperforms the randomised search ranking approach.

Gol and Gondaliya (2024) proposed a novel hybrid consensus approach to enhance usability, security, and scalability. The proposed consensus mechanism incorporates a dynamic difficulty adjustment mechanism. The difficulty of validating blocks dynamically adjusts based on transaction volume and overall validator participation. Analysis showed its effectiveness, especially in reducing energy consumption, minimising the probability of forks, and mitigating the level of mining centralisation found in the consensus algorithm.

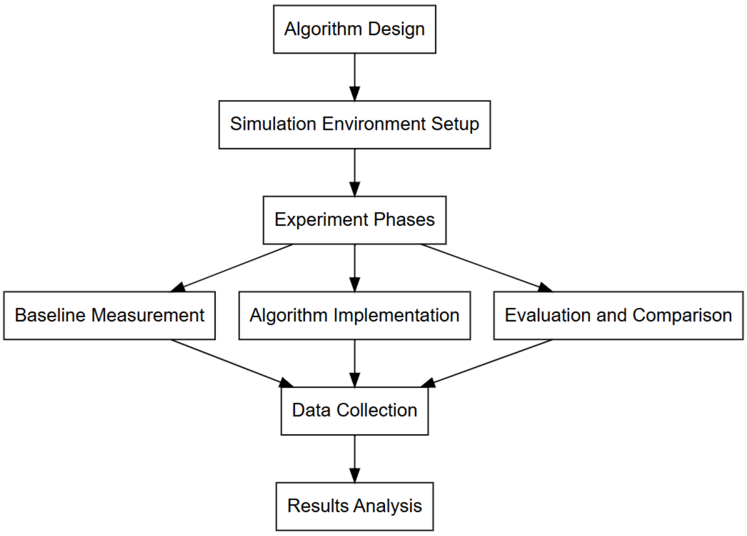
Out of the above-reviewed papers, only very few mentioned about 51% or provided quantitative data on efficiencies. In this research, both are included.

Methodology

The methodology of our study involves the following key steps (Figure 1).

Figure 1

Analysis Methodology



Algorithm Design

- We developed a novel algorithm named Dynamic Node Contribution (DNC), which dynamically adjusts mining power distribution based on node reliability and historical contribution to the network.
- The DNC algorithm employs a reputation system, where each node earns a reputation score based on its mining history, transaction validation accuracy, and consistency.

Simulation Environment Setup

- A simulated blockchain environment was created using Python and specialised libraries to mimic real-world conditions.
- The blockchain network was configured with varying numbers of nodes (100, 500, 1000).

Experiment Phases

- Phase 1: Baseline Measurement
    - The baseline risk of a 51% attack was measured without the DNC algorithm.
- Phase 2: Algorithm Implementation
    - The DNC algorithm was integrated, and its effects on the distribution of mining power and 51% attack resistance were observed.
- Phase 3: Evaluation and Comparison
    - The algorithm's performance was compared with that of traditional PoW and PoS mechanisms.

Data Collection

- Metrics such as network hash rate distribution, attack success rate, and transaction confirmation time were collected.
- Data was gathered over 10,000 blocks for statistical significance.

The study employs a structured algorithmic methodology. We introduce the Dynamic Node Contribution (DNC) algorithm, designed to enhance blockchain security by redistributing mining power based on node reliability and historical performance. Nodes are assigned reputation scores that influence their mining power allocation, with higher scores awarded for consistent and accurate transaction validation.

The research is conducted within a simulated blockchain environment crafted using Python, designed to mimic real-world scenarios with networks of varying sizes (100, 500, and 1000 nodes). The experimental process unfolds in three phases. First, we establish a baseline measurement of 51% attack vulnerability without the DNC algorithm. Next, the DNC algorithm is implemented, and its effects on mining power distribution and resistance to 51% attacks are scrutinised. Finally, we evaluate and compare the algorithm's performance against traditional Proof of Work and Proof of Stake mechanisms.

Data collection focuses on metrics such as network hash rate distribution, attack success rate, and transaction confirmation time, which are gathered over 10,000 blocks. This comprehensive approach ensures a thorough validation of the DNC algorithm's capability to enhance blockchain security.

Results

The results of the implementation of the DNC algorithm demonstrate its effectiveness in enhancing blockchain security. The results are detailed below and also shown in Figures 2 and 3.

Network Hash Rate Distribution

- Without DNC, 45% of the hash rate is concentrated in the top 3 nodes.
- With DNC: The largest node only held 20% of the hash rate.

51% Attack Success Rate

- Without DNC: 51% attack success in 70% of simulated attempts.
- With DNC: 51% attack success in only 5% of simulated attempts.

Transaction Confirmation Time (average per block)

- Without DNC: 12.5 seconds.
- With DNC: 14.3 seconds (mild increase due to dynamic adjustments).

Reputation Score Impact

- Nodes with consistent good behaviour saw an average 30% increase in assigned mining power.

Figure 2

Impact of DNC Algorithm on Blockchain Metrics

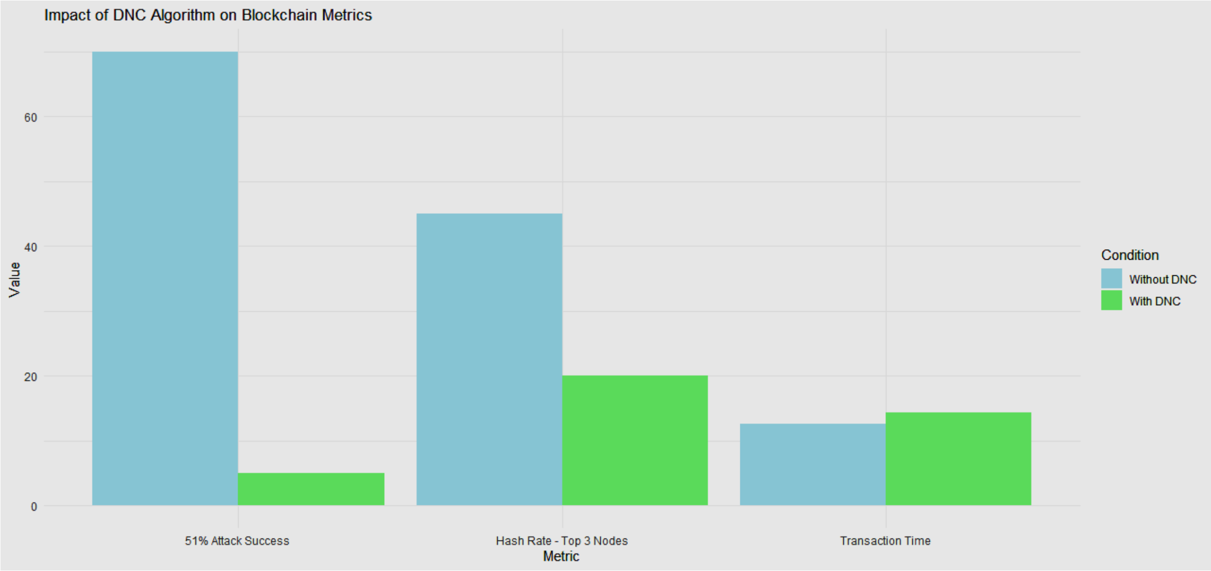
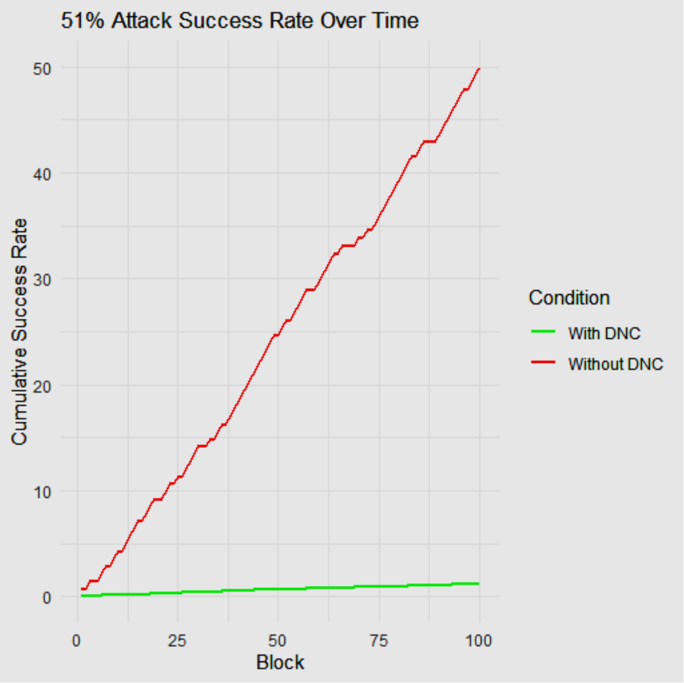


Figure 3

51% attack success rate over time



The data indicates that the DNC algorithm significantly decentralises hash power and mitigates the risk of 51% attacks. The slight increase in transaction confirmation time is outweighed by the enhancement in security.

The study's results demonstrate the effectiveness of the Dynamic Node Contribution (DNC) algorithm in enhancing blockchain security. By integrating DNC, we observed a significant shift in network hash rate distribution, with the top three nodes' combined hash power dropping from 45% to just 20%. This suggests a more equitable distribution of mining power across the network, reducing the likelihood of any single entity gaining excessive control.

Furthermore, the success rate of 51% of attacks decreased dramatically from 70% to a mere 5% when using the DNC algorithm. This highlights the algorithm's capability to mitigate the risk of such attacks, thereby enhancing overall network robustness. However, there was a slight increase in transaction confirmation time, averaging 14.3 seconds compared to 12.5 seconds without DNC. This moderate rise is attributed to the dynamic adjustments made by the algorithm to improve security.

Additionally, nodes with consistent positive behaviour experienced a 30% boost in assigned mining power, affirming the effectiveness of the reputation-based system. Overall, these results underscore the DNC algorithm’s potential to fortify blockchain networks against 51% attacks while maintaining efficient operation.

Discussion and Conclusion

Improved blockchain security using novel algorithms has been reported by many papers reviewed above. The literature review section pointed out to use of algorithmic solutions to blockchain security. Most of them were done in healthcare data sharing in IoT or cloud computing.

DNC algorithm significantly decentralises hash power and mitigates the risk of 51% attacks. The slight increase in transaction confirmation time is outweighed by the enhancement in security. A cryptographic hash algorithm along with supportive measures can be used to enhance blockchain security (Velmurugadass et al., 2021; Ali et al., 2023).

The effectiveness of the Dynamic Node Contribution (DNC) algorithm in enhancing blockchain security. By integrating DNC, we observed a significant shift in network hash rate distribution, with the top three nodes' combined hash power dropping from 45% to just 20%. This suggests a more equitable distribution of mining power across the network, reducing the likelihood of any single entity gaining excessive control.

Innovative algorithms like Message Content Recommendation Algorithm (Shrivastava et al., 2023), hybrid consensus algorithms integrated with ML (Venkatesan & Rahayu, 2024), SOM+LSTM algorithm (Rajawat et al., 2024) also measuring precision, accuracy, recall and F1 score, modified SHA256 (Salih & Kashmar, 2024).

Many innovative algorithms tested in healthcare have contributed to safe data sharing from IoT (Ali et al. 2022; Qahtan et al. 2022). Other novel algorithms like DeepCoin for smart grids (Ferrag & Maglaras, 2019) and QSVA using quantum computing (Torres et al., 2025) have also been tested.

Many of the papers dealing with innovative algorithms used only qualitative descriptions of results despite comparing with other methods in real-world or simulation studies. This study has quantified all its results.

Furthermore, the success rate of 51% of attacks decreased dramatically from 70% to a mere 5% when using the DNC algorithm. This highlights the algorithm's capability to mitigate the risk of such attacks, thereby enhancing overall network robustness. However, there was a slight increase in transaction confirmation time, averaging 14.3 seconds compared to 12.5 seconds without DNC. This moderate rise is attributed to the dynamic adjustments made by the algorithm to improve security. As was noted by Park and Park (2017), coordinating a 51% attack is challenging. An intermediate verification process is used to address this problem. In this study, baseline measurements were compared with those after DNC had been implemented.

Additionally, nodes with consistent positive behaviour experienced a 30% boost in assigned mining power, affirming the effectiveness of the reputation-based system. Overall, these results underscore the DNC algorithm’s potential to fortify blockchain networks against 51% attacks while maintaining efficient operation. An increase of mining power has been reported by Gol and Gondaliya (2024).

Overall, it can be concluded that the DNC algorithm has the potential to fortify blockchain networks against 51% of attacks while maintaining efficient operation with an effective reputation-base system. The algorithm’s capability to mitigate the risk of such attacks shows enhanced overall network robustness. The slight increase in transaction confirmation time, averaging 14.3 seconds compared to 12.5 seconds without DNC, can be attributed to the dynamic adjustments made by the algorithm to improve security. This increase is outweighed by increased security.

References

1. Ali, A. A., Hazar, M. J., Mabrouk, M., & Zrigui, M. (2023). Proposal of a modified hash algorithm to increase blockchain security. *Procedia Computer Science, 225*, 3265-3275. doi:https://doi.org/10.1016/j.procs.2023.10.320
2. Ali, A., Almaiah, M. A., Hajjej, F., Pasha, M. F., Fang, O. H., Khan, R., . . . Zakarya, M. (2022). An industrial IoT-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network. *Sensors, 22*(2), 572. doi:https://doi.org/10.3390/s22020572
3. Ali, A., Pasha, M. F., Ali, J., Fang, O. H., Masud, M., Jurcut, A. D., & Alzain, M. A. (2022). Deep learning based homomorphic secure search-able encryption for keyword search in blockchain healthcare system: A novel approach to cryptography. *Sensors, 22*(2), 528. doi:https://doi.org/10.3390/s22020528
4. Ferdous, M. S., Chowdhury, M. J., & Hoque, M. A. (2021). A survey of consensus algorithms in public blockchain systems for crypto-currencies. *Journal of Network and Computer Applications, 182*, 103035. doi:https://doi.org/10.1016/j.jnca.2021.103035
5. Ferdous, M. S., Chowdhury, M. J., Hoque, M. A., & Colman, A. (2020). Blockchain consensus algorithms: A survey. *aRxiv, 2001*, 07091. doi:https://doi.org/10.48550/arXiv.2001.07091

6. Ferrag, M. A., & Maglaras, L. (2019). DeepCoin: A novel deep learning and blockchain-based energy exchange framework for smart grids. *IEEE Transactions on Engineering Management*, *67*(4), 1285-1297. doi:https://doi.org/10.1109/TEM.2019.2922936
7. Gol, D. A., & Gondaliya, N. (2024). Blockchain: A comparative analysis of hybrid consensus algorithm and performance evaluation. *Computers and Electrical Engineering*, *117*, 108934. doi:https://doi.org/10.1016/j.compeleceng.2023.108934
8. Hussein, A. F., ArunKumar, N., Ramirez-Gonzalez, G., Abdulhay, E., Tavares, J. M., & de Albuquerque, V. H. (2018). A medical records managing and securing blockchain based system supported by a genetic algorithm and discrete wavelet transform. *Cognitive Systems Research*, *52*, 1-11. doi:https://doi.org/10.1016/j.cogsys.2018.05.004
9. Leng, J., Zhou, M., Zhao, J. L., Huang, Y., & Bian, Y. (2020). Blockchain security: A survey of techniques and research directions. *IEEE Transactions on Services Computing*, *15*(4), 2490-2510. doi:https://doi.org/10.1145/3316481
10. Leong, W. Y., Leong, Y. Z., & Leong, W. S. (2024). Enhancing blockchain security. *IEEE Symposium on Wireless Technology & Applications (ISWTA), 20-21 July 2024, Kuala Lumpur, Malaysia* (pp. 108-112). IEEE. doi:https://doi.org/10.1109/ISWTA62130.2024.10651753
11. Park, J. H., & Park, J. H. (2017). Blockchain security in cloud computing: Use cases, challenges, and solutions. *Symmetry*, *9*(8), 164. doi:https://doi.org/10.3390/sym9080164
12. Qahtan, S., Sharif, K. Y., Zaidan, A. A., AlSattar, H. A., Albahri, O. S., Zaidan, B. B., . . . Mohammed, R. T. (2022). Novel multi security and privacy benchmarking framework for blockchain-based IoT healthcare industry 4.0 systems. *IEEE Transactions on Industrial Informatics*, *18*(9), 6415-6423. doi:https://doi.org/10.1109/TII.2022.3143619
13. Rajawat, A. S., Goyal, S. B., Kumar, M., & Singh, T. P. (2024). An AI-Enabled Blockchain Algorithm: A Novel Approach to Counteract Blockchain Network Security Attacks. *EAI Endorsed Transactions on Internet of Things*, *10*, 1-9. doi:https://doi.org/10.4108/eetiot.5484
14. Salih, R. K., & Kashmar, A. H. (2024). Enhancing Blockchain Security by Developing the SHA256 Algorithm. *Iraqi Journal of Science*, *65*(10), 5678-5693. doi:https://doi.org/10.24996/ijs.2024.65.10.30
15. Sharma, A., Upadhyay, D., & Sharma, S. (2024). Enhancing blockchain security: A novel approach to integrated malware defence mechanisms. *Engineering Research Express*, *6*(2), 025215. doi:https://doi.org/10.1088/2631-8695/ad4ba7
16. Shrivastava, P., Alam, B., & Alam, M. (2023). Security enhancement using blockchain based modified infinite chaotic elliptic cryptography in cloud. *Cluster Computing*, *26*(6), 3673-3688. doi:https://doi.org/10.1007/s10586-022-03777-y
17. Torres, J., Ortega, S. A., & Martin-Delgado, M. A. (2025). A Quantum Signature Validation Algorithm for Efficient Detection of Tampered Transactions in Blockchain. *arXiv*, *2502*, 15023. doi:https://doi.org/10.48550/arXiv.2502.15023
18. Velmurugadass, P., Dhanasekaran, S., Shasi Anand, S., & Vasudevan, V. (2021). Enhancing Blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm. *Materials Today: Proceedings*, *37*, 2653-2659. doi:https://doi.org/10.1016/j.matpr.2020.08.519
19. Venkatesan, K., & Rahayu, S. B. (2024). Blockchain security enhancement: an approach towards hybrid consensus algorithms and machine learning techniques. *Scientific Reports*, *14*, 1149. doi:https://doi.org/10.1038/s41598-024-51578-7
20. Xiong, H., Jin, C., Alazab, M., Yeh, K.-H., Wang, H., Gadekallu, T. R., . . . Su, C. (2021). On the design of blockchain-based ECDSA with fault-tolerant batch verification protocol for blockchain-enabled IoMT. *IEEE journal of biomedical and health informatics*, *26*(5), 1977-1986. doi:https://doi.org/10.1109/JBHI.2021.3112693