10.48047/jocaaa.2024.32.02.48

A Research based on Enhancing Block chain Scalability through Application-Specific Optimizations

Ms. Manu Sharma
Assistant Professor, Department of Computer Science & Engineering, Dronacharya Group of Institutions, Greater Noida, Uttar Pradesh
manu.sharma@gnindia.dronacharya.info

Ms. Preeti Kumari Singh
Assistant Professor, Department of Computer Science and Engineering, Dronacharya Group of Institutions, Greater Noida, Uttar Pradesh
preeti.kumari@gnindia.dronacharya.info

Abstract

Crypto currencies like bitcoin, litecoin, dogecoin, and peercoin have gained popularity over the past decade due to their potential for securely transporting vast amounts of data through a peer-to-peer network. Blockchains, a complex topic involving economics, law, cryptography, and software engineering, are the foundation of these currencies. However, blockchains still face scalability issues, which can be resolved through a study that explores the scalability problem with blockchains. The study proposes a novel approach called blockchain-based designing of secured examination systems, using Ethereum blockchain for its decentralized nature and smart contract functionalities. The study also suggests using a unique Shard technology with PBFT Blockchain to reduce latency and increase throughput. The Black Hole Optimization (BHO) technique is used to decrease the trade-off between scalability and delay while increasing throughput per second.

Keywords: AI, Blockchain, Internet of Things (IoT),Machine Learning (ML), Security

Introduction

The latest generation of computers offers an opportunity to enhance patient care and therapeutic outcomes in the medical field by using blockchain systems to enhance information security, confidentiality, and independence. The paper explores the development of a blockchain-based decentralized education database platform, addressing issues like information tampering and concerns about confidentiality. The study also highlights the improvement of smart contracts technology due to decentralized blockchain adoption. Secure authentication for users is provided through smart agreements, ensuring accountability, accountability, and data quality [1].

Blockchain scalability is analyzed using AI models, machine learning concepts, and deep learning concepts. Various approaches have been proposed to enhance blockchain scalability, including PBFT-based Blockchain scalability improvement, Artificial Neural Network (ANN)-based Blockchain scalability improvement, and Metaheuristic algorithm-based Blockchain scalability improvement. Deep learning frameworks have been developed to protect privacy threat intelligence and secure sensitive data in the context of IIoT. The distributed DL architecture has been analyzed to enable blockchain learning, addressing safety and scaling issues while enhancing accuracy and convergence speed. Blockchain and Federated Learning

10.48047/jocaaa.2024.32.02.48

(FL) technology has been introduced to protect privacy in IoT healthcare data, providing data contextualization in intelligent cities [2-5].

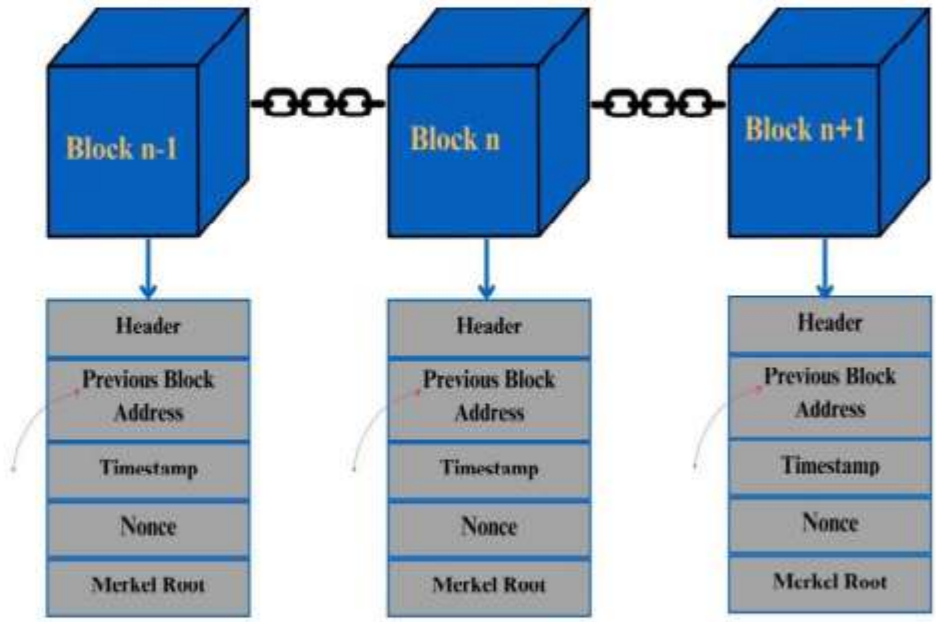

Fig.-1 Framework of Blockchain

Shahbazi et al. (2020) proposed fuzzy logic and machine learning models for perishable food-oriented blockchain, which incorporates distributed ledger systems and fuzzy logic traceability strategies to address supply chain issues. Zerka et al. (2020) proposed trustworthy distributed ML for privacy preservation, using publicly accessible information to forecast mortality from lung cancer over two years [6-8].

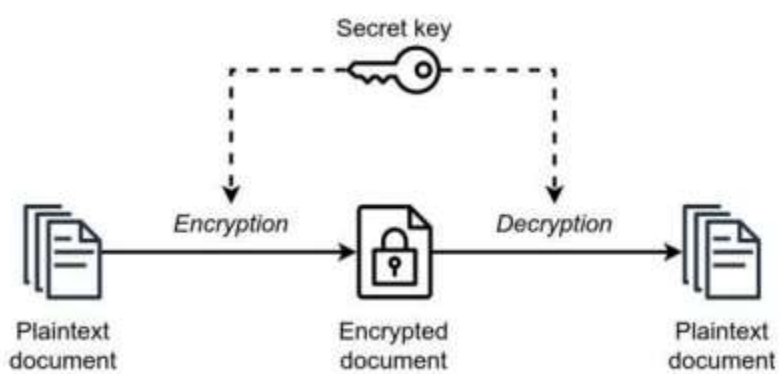

Fig.-2 Symmetric Key Cryptography model

Wu et al. (2020) introduced edge computing and blockchain convergence to scalable and secure IIoT critical infrastructures. They discussed the importance of infrastructure for the fourth

10.48047/jocaaa.2024.32.02.48

industrial revolution, the use of side chains, and the development of context-aware side chains. Balani et al. (2023) improved the blockchain-based sidechain configuration by designing heuristic models, optimizing time taken for mining blockchain data using random modelling [9-10].

Bhandari et al. (2023) suggested the integration of blockchain and machine learning for security applications. They highlighted the potential benefits of ML and Bitcoin in identifying anomalies in Bitcoin systems and highlighted new advances incorporating the two methods. Jain et al. (2022) proposed ML to increase accuracy in blockchain-based transactions, focusing on decentralized ledgers for enhancing QoS and creating affordable intelligent contracts for distributed applications [11-14].

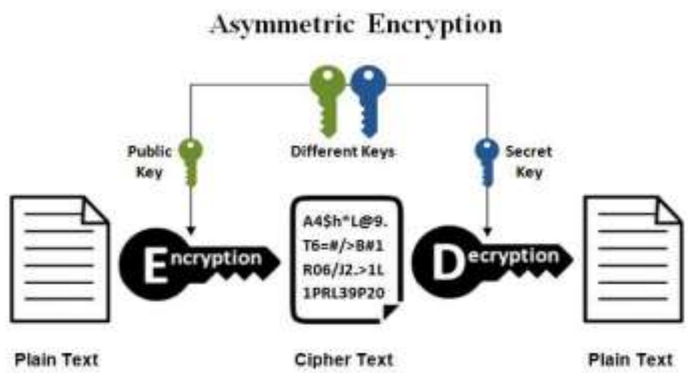

Fig.-3 Asymmetric Key Cryptography

Sami (2022) suggested extreme ML to enhance latency and scalability of blockchain, while EDGE computing addresses challenges in managing distributed systems and maintaining privacy. The integration of computational edge technology and blockchain is discussed, with a focus on common notions and challenges in integrating these technologies [15-16].

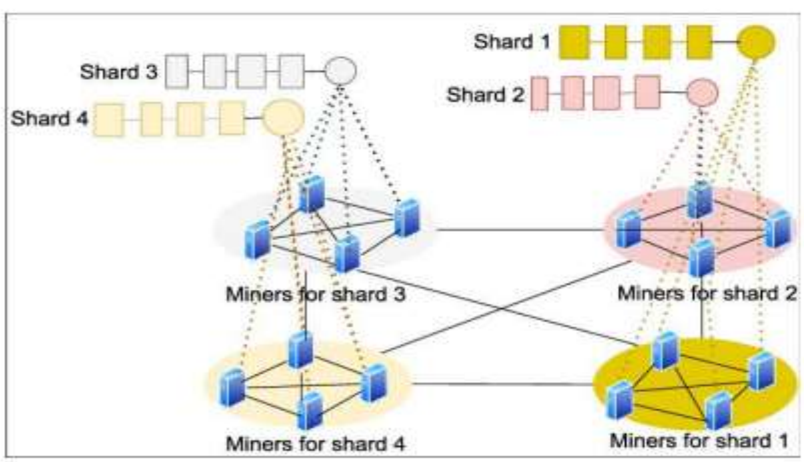

Fig.-4 Service based sharding

10.48047/jocaaa.2024.32.02.48

Akrasi-Mensah et al. (2022) introduced machine learning (ML) to improve storage efficiency in blockchain-based IIoT applications. The increasing demand for storage for bitcoin peer makes it difficult to integrate into IIoT due to the rapid generation of large quantities of information. This article examines the issue of inefficient storing in current blockchain technologies, its impact on scaling, and the difficulties it creates for how they interact into IIoT.

Ogundokun et al. (2022) suggested an ML-based blockchain model to enhance process management application security. They used big-data methods to create and analyze acquired information, and their prediction ML strategy was tested for error diagnostics prediction. Ma et al. (2023) suggested a collaborative model and blockchain-escorted distributed DL model for 6G networks. They compared the proposed design to P2P and cloud, finding that the proposed model performed better in terms of correctness and latencies.

Dong et al. (2023) introduced federated learning (FL) re-identification for blockchain-combined keen distribution systems. They used individual's ReID use for smart transport systems and incorporated the Distributed process of re Agreement mechanism to address the stability issue in better transportation systems. Measurements on confirmation time, energy efficiency, and performance were used to demonstrate the effectiveness of their suggested methodology.

The research provides useful information and potential options for navigating data privacy and security issues in the rapidly expanding field of electronic vehicle delivery platforms. Blockchain scalability improvement has been explored using Proof-of-Work (PoW)-based blockchain systems. Li et al. (2020) proposed a scalable multi-layer PBFT-based consensus mechanism, reducing communication complexity and enabling PBFT in large systems like Internet of Things ecosystems and blockchain. Lao et al. (2020) introduced G-PBFT, a new scalable and geographically based consensus technique for non-financial blockchain applications. Wu et al. (2020) proposed a hybrid blockchain consensus method with two stages: sortition and witness, combining the benefits of POS and PBFT algorithms. Li et al. (2023) proposed a model using a mesh-and-spoke network and an H-PBFT consensus called MANDALA, which reduces communication complexity and enhances fault tolerance. Tang et al. (2022) proposed an enhanced version of the trust-based practical Byzantine algorithm, suitable for consortium chains' high-frequency trading settings. Li et al. (2022) examined the security of sharding in blockchain systems using PBFT consensus for both non-cross and cross-sharding transactions. The study found that the security of a sharding is influenced by both the number of nodes in a sharding and the number of harmful nodes. Overall, these studies aim to improve blockchain scalability and security in various blockchain applications.

Li et al. (2022) proposed an enhanced Raft-based PBFT consensus method based on network fragmentation, which is more scalable than PBFT and Raft in large-scale networks. Fairness

10.48047/jocaaa.2024.32.02.48

packing method was suggested for keeping transactions in blockchain systems to enhance user experience and TPS. Suliyanti et al. (2023) suggested a multi-layer BFT to decrease communication complexity but increased latency. Double-Layer Byzantine Fault Tolerance (DLBFT) was suggested to enhance BIM communication on blockchains and their scalability.

Zheng et al. (2021) analyzed the enhancements of the Practical Byzantine Fault-Tolerant (PBFT) consensus algorithm and compared them to the original PBFT algorithm. Seo et al. (2020) created a consensus coordinator that categorizes transactions and performs a conditionally BFT-based consensus process. The authors conducted three experiments, achieving 4.75 times greater performance using their method than with only PBFT and a 61.81% boost in performance with Hyperledger Besu's IBFT.

Blockchain networks focus on consensus among peers and fraudulent spending, but they lack efficiency and scalability due to communication overhead. Navaroj et al. (2022) proposed an adaptive practical Byzantine fault tolerance mechanism in permission blockchains, which splits nodes into 38 trust nodes and defective nodes. This method offers long-term periodicity, enhanced scalability, and reduced total transmission costs.

Shen et al. (2023) provided a node trustworthy shard architecture based on guarantee tree, addressing these issues while retaining some degree of decentralization and security. They designed a trustworthy node choosing strategy based on the guarantee procedure, which assesses node guarantee results and consensus behavior. They also suggested a Dual-Leaders supervision system to ensure the deputy feels the leader's pulse while the actions of the delegate are picked up by consensus nodes. The proposed algorithm's throughput increases by 48% over Raft and is noticeably higher than PBFT, resulting in better throughput but shorter consensus latency. The literature review of PBFT-based blockchain scalability enhancement works lists their merits and demerits. Cui et al. (2023) proposed a many-objective optimized sharding model to improve blockchain performance, reducing agreement delay, sharding failure likelihood, and increasing sharding productivity. Gedam et al. (2023) proposed a novel bacterial foraging optimization (BFO) model to improve blockchain QoS model, focusing on temporally miner efficiency and processing lag time. Xu et al. (2023) suggested network optimization techniques to optimize speed and scalability of blockchain transactions. Saqibet al. (2023) introduced particle swarm optimization work proof for blockchain-based financial transactions, addressing issues with bitcoin scaling. Zhang et al. (2023) suggested an optimized blockchain sharding scheme, assigning nodes with different levels of confidence to appropriate shards to increase shard dependability and reduce the likelihood of distributed ledger collapse. The study took into account communication latencies and shard node counts to reduce communication time between shards. Simulation findings showed that the proposed technique significantly improved partition reliability and digital currency sharding speed. Cryptocurrencies have experienced significant growth, but blockchain-based ones have also raised concerns about scalability. One promising

10.48047/jocaaa.2024.32.02.48

method to increase scalability is the payment channel network (PCN), which allows off-chain processing of transactions with minimal participation of expensive blockchain activities. Zhang et al. (2019) proposed the CheaPay distributed method as the best solution to reduce transaction charges while meeting timeliness and feasibility requirements. Semi-distributed P2P network architectures are increasingly used in blockchain applications, but the original gossip method is not well-suited for real-world networks. He et at. (2019) offered an enhanced HNA-Gossip method that can lessen the likelihood of choosing duplicate nodes to relay communications by constantly storing historical node data. Thakkar et al. (2018) conducted a thorough empirical analysis to characterize the performance of Hyperledger Fabric and identify possible performance bottlenecks. Samuel et al. (2022) suggested ant colony optimization with artificial intelligence for sustainable smart cities, while Azzaoui et al. (2021) proposed a quantum approximate optimization algorithm for secure and scalable smart logistics blockchain systems. Singh et al. (2021) introduced a multiobjective optimization model based on CPU network and power bandwidth, finding that choosing a block dimension of 3.8 MB improves transaction choice and block construction time on different operating systems with CPU speeds ranging from 1.1 GHz to 3.0 GHz. Li et al. (2021) proposed an optimized byzantine fault tolerance model for consortium blockchain, addressing the drawbacks of PBFT. Wu et al. (2020) suggested hybrid consensus algorithm optimization for application in blockchain, combining PBFT and POS methods in a hypothetical bitcoin hybrid consensus method [17-20].

Methodology

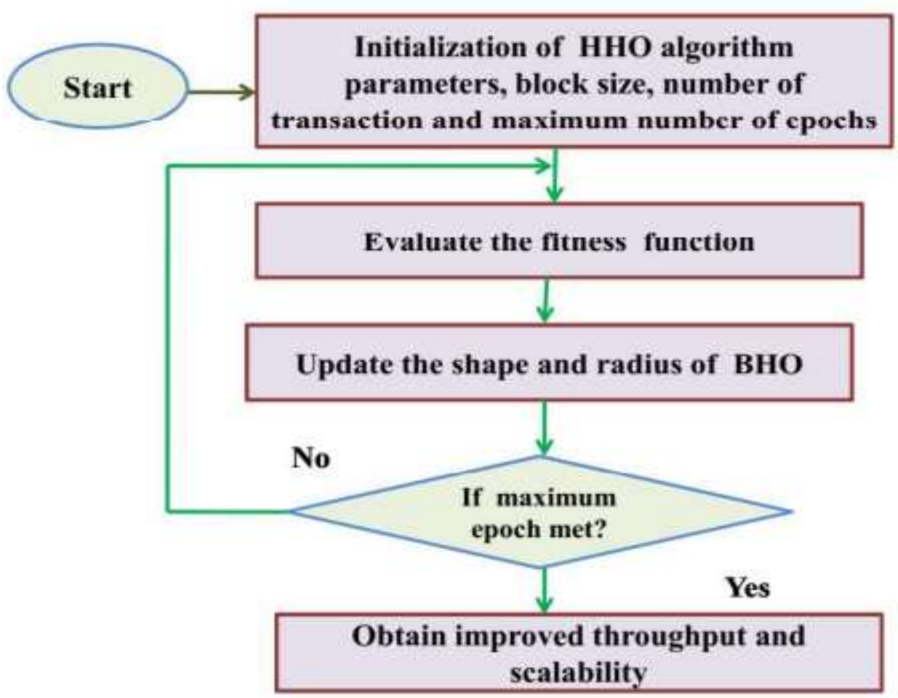

Fig.-5 The BHO algorithm for scalability improvement

10.48047/jocaaa.2024.32.02.48

This study focuses on the scalability improvement of blockchain technology for decentralized services, specifically addressing the issue of latency and transaction rate per second. The authors propose a revolutionary Shard technology in addition to PBFT Blockchain to reduce latency and increase throughput. They also use IPFS to create a decentralized student database to assess transaction time and compare results to the implementation of Sharding and PBFT techniques. The study aims to minimize the trade-off between scalability and delay by using the Black Hole Optimization (BHO) algorithm. The IPFS is used to create a decentralized student database to calculate transaction time. The proposed methodology outlines a sharded blockchain structure backed by a network, which is used in various fields such as smart houses, smart grids, and smart watches. Blockchain technology is the most emerging distributed storage technology, improving privacy and security through a decentralized consensus mechanism. It has applications in security trust, privacy protection, identity authentication, and data storage in vehicular networks. However, previous studies have faced shortcomings in privacy enhancement and detection accuracy.

The proposed shard blockchain network is used to handle massive amounts of data from the IoT network in parallel. Blockchain validators are grouped together in several shard groupings, and the validity of the blocks is verified via intra-shard consensus. The Black Hole Optimization (BHO) algorithm is a technique that improves scalability by adjusting the block size and number of shards. It was developed to minimize the trade-off between scalability and latency while increasing throughput per second. The Schwarzschild black hole radius and form are calculated using equations, which determine the distance between processes or transactions. The algorithm updates the black hole's new position, causing star motion, and selects the most potent appearance to serve as the new black hole.

The experimental analysis of the proposed study uses 1026 pupils' data stored in decentralized IPFS (Inter Planetary File System). The results show that the PBFT model performed better than the blockchain and PBFT in terms of minimal transaction time for each transaction size. The BHO method is compared to the Cuckoo Search method (CSA), Ant Colony Optimization (ACO), and other algorithms used in the field. The pace of convergence is quicker than that of earlier techniques like ACO and CSA. The study found that the PBFT model had a lower minimum transaction time for each transaction size than the blockchain and PBFT. In comparison to earlier techniques like ACO and CSA, the suggested BHO method has a higher throughput. This suggests that the PBFT algorithm can be used to reduce latency and increase throughput in blockchain systems.

Analysis

PBFT is a consensus algorithm designed to enhance the scalability of a blockchain network. It is designed to work in asynchronous networks, where nodes can operate at varying speeds. PBFT can improve blockchain scalability by reducing the number of validators, allowing for faster consensus, lower latency, parallel processing, improved network efficiency, and dynamic validator sets. It can also be combined with other scalability solutions like sharding or layer-2 solutions. To leverage PBFT, one must understand the consensus algorithm, integrate it into the blockchain platform, select a suitable node set, tune configuration parameters, optimize network communication, parallel transaction processing, consider sharding, implement optimistic execution, monitor and optimize performance, and maintain security and resilience. However,

10.48047/jocaaa.2024.32.02.48

PBFT may not be suitable for all types of blockchain applications, so it is essential to consider factors like decentralization level, participant number, and trust model before implementing it.

In summary, PBFT can significantly improve scalability in blockchain networks by reducing the number of validators, reducing latency, allowing parallel processing, dividing the network into smaller shards, implementing optimistic execution, monitoring and optimizing performance, and maintaining security and resilience. The PBFT consensus model is a distributed consensus method used in many blockchain systems, including EOS. It consists of three processes: Commit, construct, and Pre-prepare. In the pre-prepare stage, a transaction is gathered from the transaction pool, and blocks are produced and disseminated to other nodes. The node failure ratio is set to one across all nodes participating in the consensus process.

The two-step consensus process involves shard clustering, where shard numbers are distributed to each validator in a decentralized manner. After reaching intra-shard consensus, local blocks are validated based on the final consensus. The PBFT executes all consensus procedures using basic PoW. The consensus process involves determining a node's involvement in the network from its ID, using a simple PoW algorithm. The node ID is calculated using nonce, IP, and KP (public key), and the assignment of the shard number is determined by the last L-bits. The final consensus is achieved by exchanging local blocks from every shard with a directory committee node. The consensus trust, transmission hash, data size, timestamp, and block producer are determined by the variance of consensus views among nodes. The block consensus process is verified and message exchanges are verified.

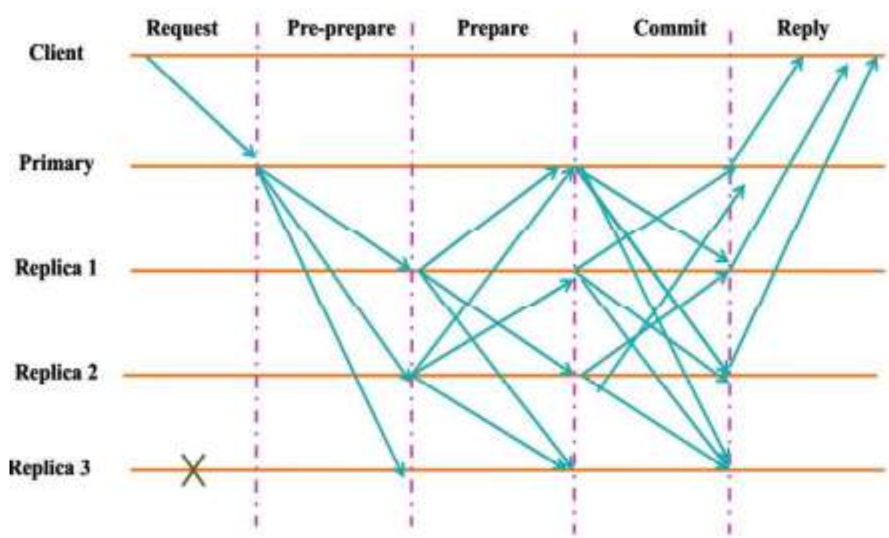

Fig.-6 Analysis-I

10.48047/jocaaa.2024.32.02.48

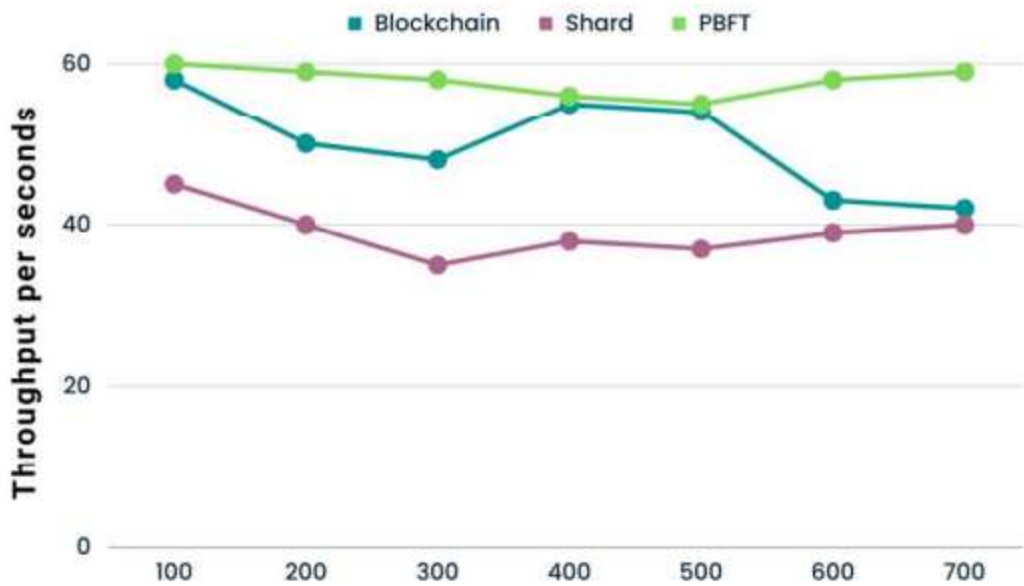

Fig.-7 Analysis-II

Conclusion

This papers discusses the research work and future enhancements for a decentralized database. It includes the design and implementation of a DAPP for student data storage, improvements in scalability using blackhole optimization, proof of stake consensus, and PBFT improvements for identifying faulty nodes in the blockchain network. These findings could be applied to educational institutions and financial transactions. Crypto currencies like bitcoin, litecoin, dogecoin, and peercoin have gained popularity for securely transporting data through peer-to-peer networks. However, blockchains, the foundation of these currencies, face scalability issues. A study proposes a novel approach using Ethereum blockchain for secure examination systems, Shard technology with PBFT Blockchain to reduce latency and increase throughput, and the Black Hole Optimization technique to balance scalability and delay. The study also explores the development of a blockchain-based decentralized education database platform to address issues like information tampering and confidentiality. Various approaches to enhance blockchain scalability are proposed, including PBFT-based, Artificial Neural Network, and Metaheuristic algorithm-based improvements. Blockchain research has advanced in various areas, including fuzzy logic and machine learning models for perishable food-oriented blockchain, symmetric key cryptography models, service-based sharding, and Proof-of-Work (PoW)-based blockchain systems. Network optimization techniques have been proposed to optimize speed and scalability of blockchain transactions.

10.48047/jocaaa.2024.32.02.48

References

1. Singh, A., Click, K., Parizi, R.M., Zhang, Q., Dehghantanha, A. and Choo, K.K.R., 2020. Sidechain technologies in blockchain networks: An examination and state-of-the-art review. Journal of Network and Computer Applications, 149, p.102471.
2. Xie, J., Yu, F.R., Huang, T., Xie, R., Liu, J. and Liu, Y., 2019. A survey on the scalability of blockchain systems. IEEE network, 33(5), pp.166-173.
3. Sivaganesan, D. "A hybrid architecture combining artificial intelligence and blockchain for IOT Applications." IRO Journal on Sustainable Wireless Systems 2, no. 3 (2021): 138-142.
4. Zhao, G., Liu, S., Lopez, C., Lu, H., Elgueta, S., Chen, H. and Boshkoska, B.M., 2019. Blockchain technology in agri-food value chain management: A synpapers of applications, challenges and future research directions. Computers in industry, 109, pp.83-99.
5. Guruprakash, J., and SrinivasKoppu. "EC-ElGamal and Genetic algorithm-based enhancement for lightweight scalable blockchain in IoT domain." IEEE Access 8 (2020): 141269-141281.
6. Singh, Amritraj, Kelly Click, Reza M. Parizi, Qi Zhang, Ali Dehghantanha, and KimKwang Raymond Choo. "Sidechain technologies in blockchain networks: An examination and state-of-the-art review." Journal of Network and Computer Applications 149 (2020): 102471.
7. Patil, Pradnya, M. Sangeetha, and VidhyacharanBhaskar. "Blockchain for IoT access control, security and privacy: a review." Wireless Personal Communications 117 (2021): 1815-1834.
8. Vu, Nam, AbhijeetGhadge, and Michael Bourlakis. "Blockchain adoption in food supply chains: A review and implementation framework." Production Planning & Control 34, no. 6 (2023): 506-523.
9. Abed, S.E., Jaffal, R. and Mohd, B.J., 2023. A review on blockchain and iot integration from energy, security and hardware perspectives. Wireless Personal Communications, 129(3), pp.2079-2122.
10. Kudva, Sowmya, ShahriarBadsha, ShamikSengupta, Hung La, Ibrahim Khalil, and Mohammed Atiquzzaman. "A scalable blockchain based trust management in VANET routing protocol." Journal of Parallel and Distributed Computing 152 (2021): 144-156.
11. Han, Hongdan, Radha K. Shiwakoti, Robin Jarvis, ChimaMordi, and David Botchie. "Accounting and auditing with blockchain technology and artificial Intelligence: A literature review." International Journal of Accounting Information Systems 48 (2023): 100598.
12. Singh, S., Rathore, S., Alfarraj, O., Tolba, A. and Yoon, B., 2022. A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology. Future Generation Computer Systems, 129, pp.380-388.
13. Balani, N. and Chavan, P., 2023. Design of heuristic model to improve blockchainbased sidechain configuration. International journal of computational science and engineering, 26(4), pp.372-384.
14. Sami, F., 2022. Integration Of Blockchain and Edge Computing to Improve The Scalability and Latency. International Journal of Advanced Sciences and Computing, 1(1), pp.27-36.
15. Cui, Z., Xue, Z., Ma, Y., Cai, X. and Chen, J., 2023. A Many-objective Optimized Sharding Scheme for Blockchain Performance Improvement in End-Edge Enabled Internet of Things. IEEE Internet of Things Journal.
16. Li, Xinling, HaoxiangLuo, and JingshanDuan. "Security Analysis of Sharding in Blockchain with PBFT Consensus." In The 2022 4th International Conference on Blockchain Technology, pp. 9-14. 2022.

10.48047/jocaaa.2024.32.02.48

17. Suliyanti, Widya Nita, and RiriFitri Sari. "Blockchain-Based Double-Layer Byzantine Fault Tolerance for Scalability Enhancement for Building Information Modeling Information Exchange." Big Data and Cognitive Computing 7, no. 2 (2023): 90.
18. Seo, Jungwon, DeokyoonKo, Suntae Kim, and Sooyong Park. "A coordination technique for improving scalability of byzantine fault-tolerant consensus." Applied Sciences 10, no. 21 (2020): 7609.
19. Rani, K.L.F.C. and Anuradha, M.P., 2023. Fuzzy-Enhanced Optimization Algorithm for Blockchain Mining Check for updates. Futuristic Communication and Network Technologies: Select Proceedings of VICFCNT 2021, Volume 2, 995, p.77.
20. Xu, Zhiyong. "Blockchain for the metaverse: optimize blockchain transaction speed and scalability." (2023).
21. Li, Y., Qiao, L. and Lv, Z., 2021. An optimized byzantine fault tolerance algorithm for consortium blockchain. Peer-to-Peer Networking and Applications, 14, pp.2826-2839.