iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** V **Month of publication:** May 2024

DOI: https://doi.org/10.22214/ijraset.2024.62095

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue V May 2024- Available at www.ijraset.com

Blockchian Based Hybrid Consensus Algorithm for Data Security in Edge Computing

Amit Saxena[1], Dr. Mohit Gupta[2]
[1]*PhD Research Scholar*[2]*Associate Professor, Department of CSE, University of Technology, Jaipur*

Abstract: ***Edge computing has emerged as a paradigm to process data closer to its source, enabling low-latency and real-time applications. However, the distributed and heterogeneous nature of edge environments poses significant challenges for ensuring data security and integrity. Blockchain technology offers a promising solution by providing a decentralized and immutable ledger for recording transactions. This abstract proposes a consensus algorithm tailored for securing data in edge computing environments using blockchain technology.***

The proposed consensus algorithm leverages a hybrid approach combining Proof of Authority (PoA) and Practical Byzantine Fault Tolerance (PBFT). PoA ensures that only trusted nodes within the edge network are eligible to participate in the consensus process, mitigating the risk of malicious attacks. PBFT enhances the efficiency and scalability of the consensus algorithm by allowing fast decision-making among a subset of nodes, thereby reducing latency in data validation and verification.

Furthermore, smart contracts are employed to enforce data access control and execute predefined rules for data processing and sharing. These smart contracts facilitate secure and transparent interactions among edge devices, ensuring that only authorized parties can access and manipulate sensitive data.

The integration of blockchain technology with edge computing offers several benefits, including enhanced data security, traceability, and accountability. By employing a tailored consensus algorithm, edge computing environments can effectively mitigate security threats while maintaining low-latency data processing capabilities. Future research directions may explore optimization techniques to further improve the performance and scalability of the proposed solution in large-scale edge networks.

Keywords: Blockchain, Edge Computing, Data Security, Consensus Algorithms

I. INTRODUCTION

In the digital age, where data is ubiquitous and computing is increasingly decentralized, the convergence of edge computing and blockchain technology emerges as a formidable solution to address the escalating concerns surrounding data security. Edge computing, characterized by distributed data processing at the edge of the network, offers unparalleled efficiency and reduced latency for a myriad of applications spanning from smart cities to autonomous vehicles. However, the dispersed nature of edge devices introduces inherent vulnerabilities, necessitating robust mechanisms to safeguard sensitive data.

Blockchain, renowned for its immutable ledger and decentralized consensus protocol, has revolutionized trust and transparency in various domains, ranging from finance to supply chain management. By integrating blockchain technology into edge computing environments, organizations can enhance data security through cryptographic primitives, decentralized governance, and immutable transaction records.

This paper delves into the synergy between edge computing and blockchain technology, elucidating how their integration augments data security in distributed computing environments. We explore the fundamental principles underpinning both paradigms and examine real-world applications where blockchain fortifies data integrity, confidentiality, and authenticity at the edge.

At the core of blockchain's contribution to edge computing security lies its immutable ledger, which ensures the tamper-resistant storage of data transactions. By leveraging cryptographic hashing and consensus mechanisms, blockchain mitigates the risk of unauthorized tampering or alteration of data, thereby instilling trust in the integrity of information processed at the edge.

Furthermore, blockchain's decentralized architecture enhances resilience against single points of failure, minimizing the susceptibility to attacks and ensuring continuous operation even in the face of network disruptions or malicious activities. Through distributed consensus protocols such as Proof of Work (PoW) or Proof of Stake (PoS), blockchain fosters a trustless environment where data transactions are validated by a network of nodes, eliminating the need for intermediaries and central authorities.

Moreover, blockchain technology facilitates secure data sharing and access control in edge computing ecosystems. Smart contracts, programmable self-executing agreements deployed on blockchain networks, enable the enforcement of predefined rules and access policies, thereby mitigating the risk of unauthorized data access or leakage.

In addition to enhancing data integrity and confidentiality, blockchain enhances auditability and compliance in edge computing environments. By maintaining a transparent and immutable record of data transactions, blockchain facilitates regulatory adherence and enables stakeholders to trace the lineage of information, thereby fostering accountability and transparency.

Through a synthesis of theoretical insights and practical case studies, this paper showcases the transformative potential of integrating blockchain technology into edge computing architectures to fortify data security. From securing IoT devices and edge networks to enabling trusted data sharing in decentralized edge ecosystems, blockchain emerges as a cornerstone in the quest for resilient and trustworthy computing paradigms at the edge.

II. THE ARCHITECTURE

IoT architecture can be divided into three layers: an IoT device layer, edge layer and a cloud layer. Blockchain can be integrated at each of these layers.

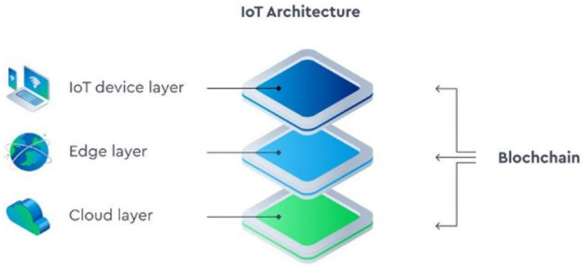


Fig: 1

A. *The IoT Device Layer*

Each edge server at this layer, together with the devices connected to it, form their own local network. The local edge server manages and registers an IoT device after the device trusts the CA (certificate authority) certificate presented to it. Communication between IoT devices, between devices and the edge server, or between edge servers are recorded as transactions and stored on the edge server blockchain. Each edge server is a blockchain manager responsible for the creation, verification and storage of transactions.

Interdevice communication at this layer can be divided into two categories. Device-to-device communication in the same local network and device-to-device communication in different local networks. In the first case, IoT devices forward source requests to their manager, the edge server. The manager authenticates the request, then broadcasts it to the whole network. In the second case, transactions between IoT devices are authenticated by their respective edge manager.

All transactions are mined and stored in blocks on the edge servers. Edge servers process real-time requests and store data in their blockchain. Data that is not time-sensitive and that needs further aggregation or analysis is sent to the cloud layer.

B. *The Edge Layer*

Edge servers that maintain the edge blockchain reside at this layer. IoT devices lack the computational power, memory and storage required for the mining and consensus process. The edge layer offloads this computational overhead from IoT devices and stores all transactions between IoT devices, and between IoT devices and the edge servers on the blockchain.

Blockchain's cryptography services secure the transactions made by IoT devices by encrypting them and attaching their digital signatures to each transaction. Edge servers working as blockchain managers use consensus algorithms like proof of work or proof of storage to validate and write transactions into a block, after which they broadcast the block to other edge servers for verification.

C. The Cloud Layer

The layer consists of cloud servers that have their own decentralized blockchain. It stores data that is not latency-sensitive and that might require further in-depth analysis. For example, sensor data can be combined with data from other sources for more detailed insights.

III. A REAL-LIFE APPLICATION OF BLOCKCHAIN AND EDGE COMPUTING

Though blockchain is most commonly associated with Bitcoin and Ethereum, it can be used for much more than cryptocurrency applications. Other industries that benefit from blockchain's security features and decentralized nature include healthcare, industrial IoT, smart cities and smart home automation.

Let's take a quick look at how edge computing and blockchain enhance the security of patient medical records in a hospital setting. Wearables retrieve health data from a patient and store it in an electronic medical card. This data can then be encrypted and sent to edge servers. Edge servers store this data on the edge blockchain for improved data security and confidentiality.

Patients and authorized hospital staff can access the data from the edge much faster than if they were to access the data from the cloud. Edge servers send any data that is not required for real-time analysis to the cloud.

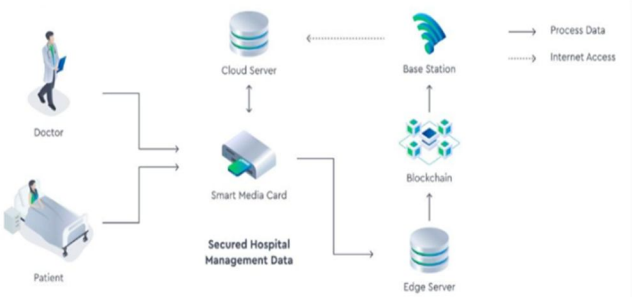


Fig: 2

Edge computing, integrated with blockchain, helps allow us to build a distributed and secure edge computing architecture that can promote the safety and integrity of IoT data throughout its lifetime.

IV. BENEFITS OF BLOCKCHAIN IN EDGE COMPUTING

Blockchain integration into edge computing environments offers a plethora of benefits, revolutionizing data security, trust, and transparency in distributed computing ecosystems. Here are some key advantages:

1) *Enhanced Data Security:* Blockchain's immutable ledger ensures tamper-resistant storage of data transactions at the edge. This prevents unauthorized tampering or alteration of data, enhancing the integrity and reliability of information processed by edge devices.
2) *Decentralized Trust:* By leveraging decentralized consensus mechanisms, such as Proof of Work (PoW) or Proof of Stake (PoS), blockchain eliminates the need for centralized authorities or intermediaries in verifying data transactions. This fosters trust in the integrity of data processed at the edge without relying on single points of failure.
3) *Resilience Against Attacks:* Blockchain's distributed architecture enhances resilience against various cyber threats, including DDoS attacks and data breaches. Even in the event of network disruptions or malicious activities, blockchain ensures continuous operation and data availability at the edge.
4) *Transparent and Auditable Transactions:* Blockchain maintains a transparent and immutable record of data transactions, enabling stakeholders to trace the lineage of information and verify its authenticity. This fosters transparency, accountability, and regulatory compliance in edge computing environments.
5) *Efficient Data Sharing and Access Control:* Smart contracts deployed on blockchain networks enable programmable and automated enforcement of access policies and data sharing agreements at the edge. This ensures secure and efficient data exchange between edge devices while mitigating the risk of unauthorized access or leakage.
6) *Reduced Latency and Improved Efficiency:* Blockchain integration optimizes data processing and communication at the edge, reducing latency and improving overall system efficiency. This is particularly crucial for latency-sensitive applications, such as autonomous vehicles and industrial automation, where real-time data processing is paramount.

7) *Scalability and Interoperability:* Blockchain's modular architecture and interoperability standards facilitate seamless integration with existing edge computing infrastructures and diverse IoT devices. This scalability enables edge ecosystems to accommodate the growing volume of data transactions while maintaining interoperability across heterogeneous environments.
8) *Economic Incentives and Tokenization:* Blockchain-based incentive mechanisms, such as tokenization and smart contracts, incentivize active participation and contribution from edge devices in data processing and validation tasks. This creates economic value within edge ecosystems and encourages collaborative efforts towards maintaining network security and reliability.

V. CONSENSUS ALGORITHMS

Consensus algorithms are of the highest relevance to blockchain technology since the purpose of Bitcoin was to transfer value in an unregulated, distrusting environment, where a sure way of validating transactions was needed. The goal of the consensus algorithm is to ensure a single history of transactions exists and that that history does not contain invalid or contradictory transactions. For example, that no account is attempting to spend more than the account contains, or to spend the same token twice, so-called double-spending. In Table 5.1, different important consensus algorithms are compared to each other. Below, a brief introduction to a few of them is given, but for more details, the reader is referred to (Back, 1997), (Nakamoto, 2008), (Fischer, 1983), (Tendermint, 2017).

Bitcoin solved the consensus problem by, for each new block announcing a target, which the hash of the previous block, the current block and a variable nonce has to equal less than. Since the output of the hashing function is evenly distributed, it's impossible to create a block such that it with certainty will be easy to reach the target. Therefore, there is a race between the mining computers in the network to find the right nonce. Once a target is reached, the mining computer broadcasts that block to the network and other participants validate the transactions. If enough validating nodes find the transactions to add up, they agree upon that block being added to the chain. This procedure is called proof-of-work (PoW). Since the goal is, not to give too much power to a single person or organization, a limited resource has to be chosen which will be spent upon voting for the validity of a block. In PoW, that resource is computing power.(Cynthia Dwork, 1992). Since computing power is getting cheaper and more available with Moore's Law and cloud computing, the difficulty of the hashing problem is regulated according to the frequency with which the previous problems were solved. A common critique of PoW is however, that the "waste" of computing power also means a large waste of energy. There are miners who only mine in winter, and use the exhaust heat from the mining farm
to warm up their house. ("Hotmine Inc." 2016). What this essentially means is that miners are forced to pool resources into what can ultimately be a handful of giant Bitcoin farms, thus having centralised the decentralised network. Additionally, Bitcoin does not have a very high throughput of transactions since the block time stays constant at about 10 minutes and block size as well (about 1 MB). The energy waste and throughput are two reasons why alternatives have emerged. The most relevant for this thesis are Proof-of-Stake (PoS) and Tendermint which are very similar.

Neither uses computing power as a scarce resource, but rather the ownership of the inherent tokens of the blockchain. The principle is that owners of tokens put a certain amount of tokens at "stake" by betting on the version of the blockchain that they believe is the correct one. This will increasingly incentivise validators to behave according to the rules depending on how much they possess. Validators in the Tendermint consensus algorithm are nodes who take turns proposing blocks of transactions and then vote on them. If a block fails to get enough votes, the protocol moves to the next validator to propose a block. To successfully commit a block, there are two stages that need to be passed: pre-commit and pre-vote. A block is committed when more than 2/3 of validators pre-commit for the same block on the same round. As long as no more than 1/3 of validators are byzantine, it is impossible for conflicting blocks to be committed at the same height of the blockchain. Tendermint can be modified to act as a Proof-of-Stake algorithm by assigning different "weights" to the votes of different validators. In PoS, there is an attack, or a problem, called the nothing-at-stake-attack. The core of it is that there is no reason why a validator couldn't bet on all different proposed versions, thus being certain to win.

The Ethereum wiki-page explains it as: an attacker may be able to send a transaction in exchange for some digital good (usually another cryptocurrency), receive the good, then start a fork of the blockchain from one block behind the transaction and send the money to themselves instead, and even with 1% of the total stake the attacker's fork would win because everyone else is mining on both. ("Ethereum GitHub Wiki - Proof of Stake FAQ," 2017)

Consensus algorithm	Resource being used	Benefits	Drawbacks	Examples
Proof-of-Work	Computing power	Trustless, immutable, highly decentralised	Energy consumption, transaction throughput.	Bitcoin, Litecoin.
Proof-of-Stake (PoS)	Ownership of fixed amount of tokens	Efficient in energy and throughput, scalable	Nothing-at-Stake problem. I.e. voting for different forks at the same time	NXT
Delegated PoS	Ownership of scarce tokens + peer reputation (elections for delegates)	Allegedly more efficient than PoS	Voter apathy in elections can lead to excessive centralisation and reduced robustness	BitShares
Tendermint (Proof-of-Validation) (Tendermint, 2017)	Security deposit of scarce tokens subject to burn if voting dishonestly	Gives the benefits of proof-of-stake without almost any of its drawbacks	Nothing-at-stake problem still persists over long periods of time	Eris-Db ("Monax - Blockchain explainer," 2016)
Proof-of-Authority (PoA)	Selected authorities are randomly selected to validate transactions	Efficient, doesn't require any inherent tokens or economic value	The corruption of authorities is a large possibility, relies on authorities being well-selected and controlling eachother	Parity PoA

Table 5.1: Consensus algorithms for usage in blockchains. Adapted from source: (Mattila, 2016) with addition of Proof-of-Authority

VI. COMBINED MECHANISM OF PROOF OF AUTHORITY (POA) AND PRACTICAL BYZANTINE FAULT TOLERANCE (PBFT)

A consensus algorithm that combines Proof of Authority (PoA) and Practical Byzantine Fault Tolerance (PBFT) is indeed an interesting hybrid approach. Let's break down how this might work:

1) *Proof of Authority (PoA):* PoA is a consensus mechanism where transactions and blocks are validated by approved accounts, known as validators or authorities. These validators are typically known and trusted entities, reducing the risk of malicious behavior. PoA provides fast transaction speeds and low computational requirements, making it suitable for private or consortium blockchains.
2) *Practical Byzantine Fault Tolerance (PBFT):* PBFT is another consensus algorithm designed to tolerate Byzantine faults, where nodes in a network may act arbitrarily or maliciously. PBFT ensures consensus by having a predetermined set of nodes (replicas) reach agreement on the validity of transactions through a multi-round voting process. It's highly efficient in terms of throughput and can tolerate a certain number of malicious nodes based on its fault tolerance threshold. Combining these two mechanisms can leverage the benefits of both:
3) *Performance:* PoA provides fast block confirmation times and low latency, while PBFT ensures high throughput and fault tolerance.

In a Proof of Authority (PoA) consensus mechanism augmented with Practical Byzantine Fault Tolerance (PBFT), the performance characteristics would be influenced by several factors:

- Transaction Throughput: PBFT is known for its high throughput compared to some other consensus mechanisms like Proof of Work (PoW). By leveraging PBFT alongside PoA, the blockchain network could achieve even higher transaction throughput. This is because PBFT allows for parallel processing of transactions by a predetermined set of nodes, reducing the time it takes to reach consensus on each block.
- Latency: PoA typically provides low-latency confirmation of transactions since the block creation process is controlled by a predefined set of authorities. When combined with PBFT, which also aims for low-latency block finalization through a multi-round voting process, the overall latency of the system could be further reduced.

- Scalability: Scalability is a crucial aspect of blockchain performance. By combining PoA and PBFT, the blockchain network can potentially scale to handle a larger number of transactions per second compared to using either consensus mechanism alone. PBFT's parallel processing of transactions and PoA's efficient block creation can contribute to improved scalability.
- Fault Tolerance: PBFT provides Byzantine fault tolerance, meaning the system can tolerate a certain number of malicious nodes or arbitrary behavior. When integrated with PoA, which relies on trusted authorities to validate transactions and create blocks, the hybrid consensus mechanism can offer robust fault tolerance properties, enhancing the overall security of the blockchain network.
- Node Requirements: Both PoA and PBFT have specific node requirements. PoA requires a set of trusted authorities to validate transactions, while PBFT requires a predetermined set of nodes to participate in the consensus process. Integrating these two mechanisms would necessitate ensuring that the nodes meet the requirements of both consensus algorithms, which may involve careful selection and management of node operators.

Overall, a PoA consensus mechanism augmented with PBFT can potentially offer high performance, low latency, scalability, and robust fault tolerance, making it suitable for various blockchain applications where speed, security, and efficiency are essential considerations. However, the actual performance would depend on the specific implementation details, network configuration, and the characteristics of the underlying blockchain platform.

4) Security: PoA establishes a trusted set of validators, reducing the risk of malicious behavior, while PBFT provides Byzantine fault tolerance, ensuring the system can tolerate malicious nodes.

The security of a blockchain network utilizing a hybrid consensus mechanism combining Proof of Authority (PoA) with Practical Byzantine Fault Tolerance (PBFT) is influenced by several factors:

- Validator Selection: In a PoA system, validators are typically known and trusted entities. These validators are responsible for creating and validating blocks. By carefully selecting reputable and reliable validators, the network can maintain a high level of security. However, the selection process must be transparent and fair to prevent centralization or collusion among validators.
- Byzantine Fault Tolerance: PBFT provides Byzantine fault tolerance, meaning the network can tolerate a certain number of malicious or faulty nodes without compromising the integrity of the system. This ensures that even if some validators behave maliciously or experience failures, the network can still reach a consensus on the validity of transactions.
- Multi-round Consensus: PBFT achieves consensus through a multi-round voting process where a predetermined set of nodes (validators) exchange messages to agree on the order and validity of transactions. This process helps in detecting and isolating malicious behavior, enhancing the security of the system.
- Resilience to Attacks: The combination of PoA and PBFT can make the blockchain network resilient to various attacks, including Sybil attacks, where an adversary controls multiple identities, and Byzantine attacks, where malicious nodes attempt to disrupt the consensus process. PoA's reliance on trusted validators and PBFT's fault tolerance mechanisms help mitigate the impact of such attacks.
- Immutability and Tamper Resistance: One of the fundamental aspects of blockchain security is immutability and tamper resistance. Once transactions are confirmed and added to a block, they are cryptographically linked and cannot be altered without consensus from the network. The combination of PoA and PBFT ensures that the blockchain maintains its integrity and remains resistant to tampering or unauthorized modifications.
- Regular Audits and Monitoring: Continuous monitoring of the network and regular audits of validator activities can help detect and mitigate security threats. Validators should be held accountable for their actions, and mechanisms for reporting suspicious behavior should be in place to maintain the integrity of the network.

While PoA with PBFT offers robust security properties, it's essential to consider potential vulnerabilities and continuously improve the network's security measures through ongoing research, testing, and collaboration within the blockchain community.

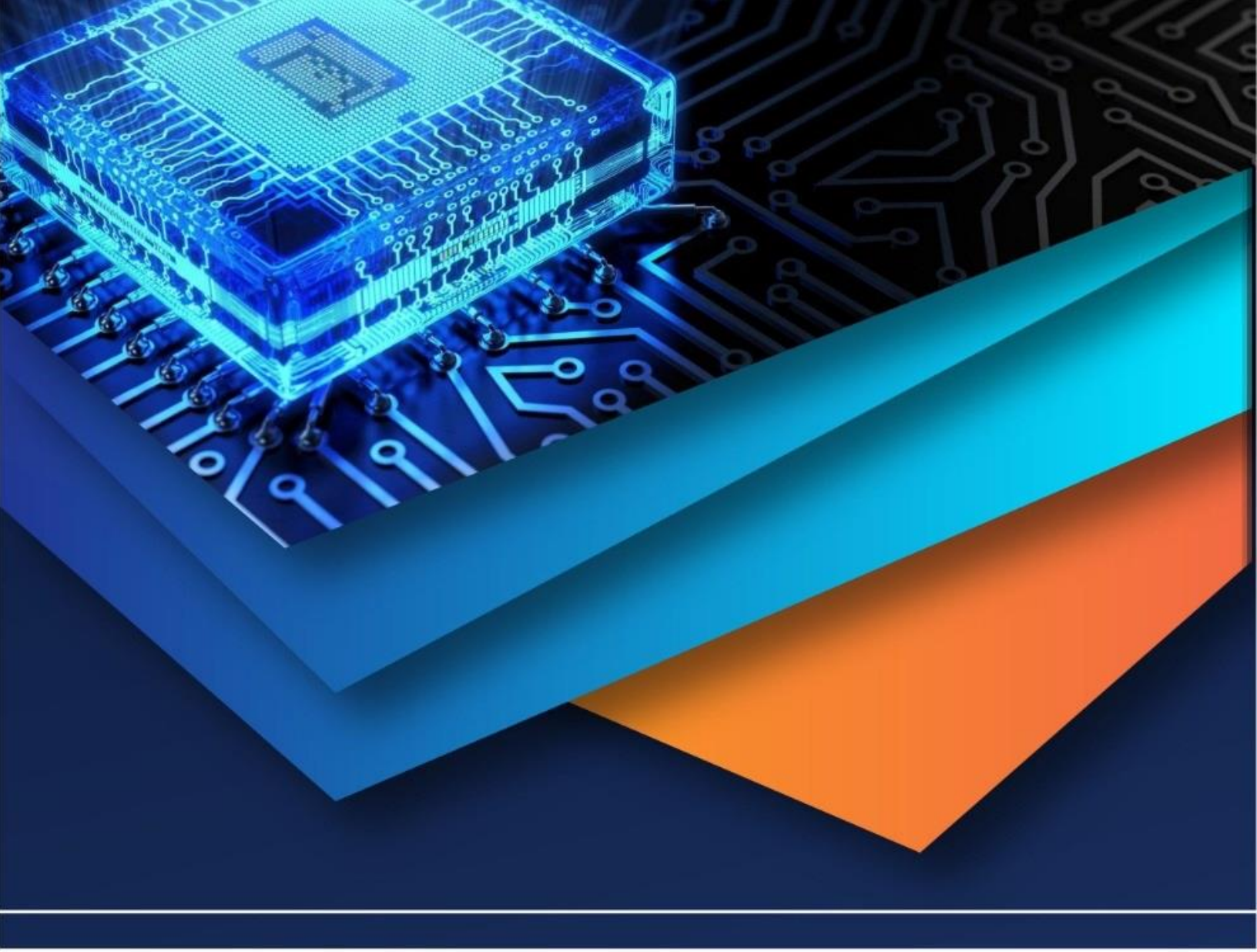
VII. CONCLUSION

In this hybrid approach, the PoA mechanism could serve as an initial filter to validate transactions quickly, while the PBFT mechanism could be used for finalizing the blocks and ensuring consensus among a larger set of nodes, providing additional security guarantees. That means the hybrid approach combining PoA and PBFT offers a balanced solution that addresses the key challenges of security, performance, scalability, and fault tolerance in blockchain networks. By integrating the strengths of both consensus mechanisms, this approach provides a solid foundation for building secure and efficient blockchain systems capable of meeting the demands of real-world applications.

REFERENCES

[1] Zhou X, Yang X, Ma J, Kevin I, Wang K (2021) Energy-efficient smart routing based on link correlation mining for wireless edge computing in IoT. IEEE Internet Things J 9(16):14988–14997
[2] Hu C, Fan W, Zeng E, Hang Z, Wang F, Qi L, Bhuiyan MZA (2021) Digital twin-assisted real-time traffic data prediction method for 5g-enabled internet of vehicles. IEEE Trans Ind Inf 18(4):2811–2819
[3] Zhou X, Xu X, Liang W, Zeng Z, Yan Z (2021) Deep-learning-enhanced multitarget detection for end–edge–cloud surveillance in smart IoT. IEEE Internet Things J 8(16):12588–12596
[4] Qi L, Chi X, Zhou X, Liu Q, Dai F, Xu X, Zhang X (2022) Privacy-aware data fusion and prediction for smart city services in edge computing environment. In: 2022 IEEE International Conferences on Internet of Things (iThings) and IEEE Green Computing & Communications (GreenCom) and IEEE Cyber, Physical & Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics), IEEE, pp 9–16
[5] Qi L, Hu C, Zhang X, Khosravi MR, Sharma S, Pang S, Wang T (2021) Privacy-aware data fusion and prediction with spatial-temporal context for smart city industrial environment. IEEE Trans Ind Inform 17(6):4159–4167
[6] Zhang T, Li Y, Chen CP (2021) Edge computing and its role in industrial internet: Methodologies, applications, and future directions. Inf Sci 557:34–65
[7] Li X, Li D, Wan J, Liu C, Imran M (2018) Adaptive transmission optimization in sdn-based industrial internet of things with edge computing. IEEE Internet Things J 5(3):1351–1360
[8] Dai X, Xiao Z, Jiang H, Alazab M, Lui JC, Dustdar S, Liu J (2022) Task co-folding for d2d-assisted mobile edge computing in industrial internet of things. IEEE Trans Ind Inf 19(1):480–490
[9] Ranaweera P, Jurcut AD, Liyanage M (2021) Survey on multi-access edge computing security and privacy. IEEE Commun Surv Tutor 23(2):1078–1124
[10] Wang R, Lai J, Zhang Z, Li X, Vijayakumar P, Karuppiah M (2022) Privacy preserving federated learning for internet of medical things under edge computing. IEEE J Biomed Health Inform 27(2):854–865.
[11] Zhou X, Liang W, Yan K, Li W, Kevin I, Wang K, Ma J, Jin Q (2022) Edge enabled two-stage scheduling based on deep reinforcement learning for internet of everything. IEEE Internet Things J 10(4):3295–3304
[12] Yuan L, He Q, Chen F, Zhang J, Qi L, Xu X, Xiang Y, Yang Y (2022) Csedge: Enabling collaborative edge storage for multi-access edge computing based on blockchain. IEEE Trans Parallel Distrib Syst 33(8):1873–1887
[13] Xu G, Dong J, Ma C, Liu J, Clif UGO (2022) A certifcateless signcryption mechanism based on blockchain for edge computing. IEEE Internet Things J https://doi.org/10.1109/JIOT.2022.3151359
[14] Qi L, Liu Y, Zhang Y, Xu X, Bilal M, Song H (2022) Privacy-aware point-ofinterest category recommendation in internet of things. IEEE Internet Things J 9(21):21398–21408
[15] Liang W, Hu Y, Zhou X, Pan Y, Kevin I, Wang K (2021) Variational few-shot learning for microservice-oriented intrusion detection in distributed industrial IoT. IEEE Trans Ind Inform 18(8):5087–5095
[16] Wang G, Li C, Huang Y, Wang X, Luo Y (2022) Smart contract-based caching and data transaction optimization in mobile edge computing. Knowl-Based Syst 252(109):344
[17] Boo E, Kim J, Ko J (2021) Litezkp: Lightening zero-knowledge proof-based blockchains for IoT and edge platforms. IEEE Syst J 16(1):112–123
[18] Nawaz A, Peña Queralta J, Guan J, Awais M, Gia TN, Bashir AK, Kan H, Westerlund T (2020) Edge computing to secure IoT data ownership and trade with the Ethereum blockchain. Sensors 20(14):3965
[19] Dasgupta D, Shrein JM, Gupta KD (2019) A survey of blockchain from security perspective. J Bank Financ Technol 3:1–17
[20] Berdik D, Otoum S, Schmidt N, Porter D, Jararweh Y (2021) A survey on blockchain for information systems management and security. Inf Process Manag 58(1):102397
[21] Feng J, Yang LT, Gati NJ, Xie X, Gavuna BS (2020) Privacy-preserving computation in cyber-physical-social systems: A survey of the state-ofthe-art and perspectives. Inf Sci 527:341–355
[22] Liu Z, Yang D, Wang Y, Lu M, Li R (2023) Egnn: graph structure learning based on evolutionary computation helps more in graph neural networks. Appl Soft Comput 135:110040
[23] Zhou X, Liang W, Li W, Yan K, Shimizu S, Kevin I, Wang K (2021) Hierarchical adversarial attacks against graph-neural-network-based IoT network intrusion detection system. IEEE Internet Things J 9(12):9310–9319
[24] Khan A (2022) Graph analysis of the ethereum blockchain data: A survey of datasets, methods, and future work. In: 2022 IEEE International Conference on Blockchain (Blockchain), IEEE, pp 250–257
[25] Farrugia S, Ellul J, Azzopardi G (2020) Detection of illicit accounts over the Ethereum blockchain. Expert Syst Appl 150:1–11
[26] Poursafaei F, Hamad GB, Zilic Z (2020) Detecting malicious ethereum entities via application of machine learning classifcation. In: Proceedings 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS). IEEE, pp 120–127
[27] Zhang Y, Yu W, Li Z, Raza S, Cao H (2022) Detecting Ethereum Ponzi schemes based on improved lightGBM algorithm. IEEE Trans Compute Soc Syst 9(2):624–637
[28] Chen W, Guo X, Chen Z, Zheng Z, Lu Y (2020) Phishing scam detection on ethereum: Towards fnancial security for blockchain ecosystem. In: Proceedings 29th International Joint Conference on Artifcial Intelligence, Morgan Kaufmann, pp 4506–4512
[29] Wu Z, Pan S, Chen F, Long G, Zhang C, Philip SY (2020) A comprehensive survey on graph neural networks. IEEE Trans Neural Netw Learn Syst 32(1):4–24
[30] Liu M, Gao H, Ji S (2020) Towards deeper graph neural networks. In:Proceedings of the 26th ACM SIGKDD international conference on knowledge discovery and data mining. ACM, pp 338–348
[31] Liu X, Tang Z, Li P, Guo S, Fan X, Zhang J (2022) A graph learning based approach for identity inference in dapp platform blockchain. IEEE Trans Emerg Top Comput 10(1):438–449
[32] Weber M, Domeniconi G, Chen J, Weidele DKI, Bellei C, Robinson T, Leiserson CE Anti-money laundering in bitcoin: Experimenting with graph convolutional networks for fnancial forensics. 2019. arXiv:1908. 02591
[33] Cai H, Zheng VW, Chang KCC (2018) A comprehensive survey of graph embedding: Problems, techniques, and applications. IEEE Trans Knowledge Data Eng 30(9):1616–1637

[34] Wang X, Bo D, Shi C, Fan S, Ye Y, Yu PS (2023) A survey on heterogeneous graph embedding: Methods, techniques, applications and sources. IEEE Trans Big Data 9(2):415–436
[35] Yuan Q, Huang B, Zhang J, Wu J, Zhang H, Zhang X (2020) Detecting phishing scams on ethereum based on transaction records. In: Proceedings 2020 IEEE International Symposium on Circuits and Systems. IEEE, pp 1–5
[36] Wu J, Yuan Q, Lin D, You W, Chen W, Chen C, Zheng Z (2022) Who are the phishers? phishing scam detection on Ethereum via network embedding. IEEE Trans Syst Man Cybern: Syst 52(2):1156–1166



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY