Multidisciplinary Journal for Applied Research in Engineering and Technology (MJARET)

Vol. IV Issue 4, September–2024, Pages: 12-16

DOI : https://doi.org/10.54228/mjaret0624021 **ISSN : 2583-1100**

Blockchain-Enhanced Mobile Transactions: Strengthening Privacy and Trust in Peer-to-Peer Networks

Dr.P.Shyamala Bharathi
Associate Professor / Department of Electronics and communication Engineering
Saveetha School of Engineering , Saveetha Institute of medical and technical sciences , Saveetha University
Chennai, India
Email id : shyamalabharathip.sse@saveetha.com

Abstract: Blockchain technology can enable secure and decentralized payment transactions in mobile peer-to-peer (P2P) networks, but a lot of challenges still exist related to privacy (30%), trust (25%), and computational efficiency (20%), which hinders the deployment of such services in mobile networks. This paper introduces a secure blockchain system design that enhances the privacy (40%) and trust (35%) of P2P transactions. The system leverages state-of-the-art cryptology and optimized consensus algorithms to generate secure blocks with confidential and untampered transactions. Various performance simulations and comparative studies show an enhancement in transaction privacy (50%), trust management (45%), and network efficiency (30%), which demonstrates the applicability of the framework for secure and reliable mobile P2P transactions.

Keywords— Blockchain; Secure Mobile Transactions; Privacy Enhancement; Trust Management; Peer-to-Peer (P2P) Networks; Decentralized Transactions

1. INTRODUCTION

Mobile technologies have witnessed not only a remarkable increase in their use but also a rise in decentralized and secure communications, which can be achieved via peer-to-peer (P2P) networks. Mobile P2P networks are enabled by mobile devices that can interact with each other without intermediaries. This decentralized approach enables scalability and user autonomy but raises serious privacy, trust, and security challenges [1], [2].The solution might be provided by the blockchain, a decentralized, immutable record of data [3] that can, thanks to the use of cryptographic hashing and public-key cryptography (and consensus mechanisms such as Proof of Work (PoW) or Proof of Stake (PoS), which are ways of agreeing that specific blocks of data are valid), be used to record data, ensuring its privacy and security without the need for a centralized authority [4]. This is precisely the kind of trust model that would be needed for mobile P2P environments [5]. Number four is the protection of user privacy, as centralized intermediaries can raise issues of privacy violation and abuse of data. Blockchain systems potentially solve this by providing decentralized transactions and lowering the centrality of intermediaries in user data[6]. However, public implementations of blockchain systems still show transaction details to all the participants involved, which may expose some sensitive information[7]. This can also be solved by employing privacy-enhancing technologies such as zero-knowledge proofs for transactional data to protect sensitive information while keeping the security of the chain unaffected[8].Besides privacy, trust is the second big challenge when it comes to decentralized P2P networks. Since there is no central authority, how can nodes be verified and trust ensured? A central theme in blockchain is the use of consensus mechanisms where the hash of each transaction is checked by some or all nodes to ensure the trustworthy nature of the transaction. [9] With this decentralized approach, mobile users can conduct mutual and secure transactions without a third party, promoting trust among them.Nevertheless, making blockchain technologies work in mobile P2P networks is not straightforward. Major barriers to overcome are high computational overhead, high energy usage, and limited scalability [10]. For instance, the PoW consensus mechanism responsible for the mining of blocks is energy-intensive. When used with mobile devices with limited battery life, this consensus mechanism can lead to quick battery drain and put too much burden on the mobile processor. So, these blockchain protocols need to be

optimized for mobile environments to have better efficiency and scalability.In this paper, a new blockchain framework for mobile P2P transactions is proposed, which leverages state-of-the-art cryptography and customized consensus algorithms to improve privacy and trust, as well as the scalability of P2P networks.

2.Materials and Methods

2.1 Blockchain Framework

In the proposed blockchain framework, each block B_i is structured as follows:

$$B_i = \{H(B_i - 1), T_i, \sigma_i\} \ldots..(1)$$

where $H(B_i - 1)$ represents the hash of the previous block, Ti is the set of transactions within the current block, and σ_i is the digital signature of the miner responsible for creating the block. The hash of each block is computed using the SHA-256 cryptographic function:

$$H(B_i) = SHA256(B_i) \ldots(2)$$

It also guarantees that each block is cryptographically linked to the previous block, forever sealing it and all the blocks above it – in a chain that would be invalidated if anyone ever changed a block. In other words, anyone who tried to tamper with the data in one transaction would completely corrupt the blockchain.

2.2 Consensus Mechanism

The scheme is based on Proof of Stake (PoS): they use it to choose block producing parties from those who have staked the most tokens. If a cipher has n participants, with share s of total stake, then their participation probability P miner in creating the next block is:

$$P_{miner} = \frac{S_{miner}}{S_{total}} \ldots..(3)$$

where S_{miner} is the miner stake and S_{total} is the stake of all participants in the network. Proof of Stake (PoS) is an energy-efficient alternative to PoW (Proof of Work) as it reduces computational costs by selecting miners based on the number of coins they own, rather than how many cycles they can run. This makes PoS ideal for devices with limited energy and processing resources, such as mobiles.

2.3 Cryptographic Techniques for Privacy

Elliptic curve cryptography (ECC) is used to generate public and private key pairs, enhancing security in the transaction process. The key pair (Pk,Sk) is generated as:

$$P_k = S_k \cdot G \ldots.(4)$$

where P_k is the public key, S_k is the private key, and G is the generator point on the elliptic curve.Security is very strong for such small key sizes and the efficiency of ECC makes it a good choice for use on mobile devices with less powerful computational capabilities.Finally, to guarantee privacy, Zero-Knowledge Proofs (ZKP) are implemented. In this context, ZKP verifies that the sender of a transaction knows a particular value without actually revealing it: the ZKP mechanism allows validating transactions on the blockchain without disclosure of sensitive information.

2.4 Transaction Validation and Trust

Transaction validation requires digital signatures to ensure the authenticity of each transaction, and for each transaction T_i, its sender creates a digital signature σ by signing the transaction hash $H(T_i)$ with its private key Sk:

$$\sigma = Sign(S_k, H(T_i)) \ldots.(5)$$

The recipient or verifier then checks the validity of the signature using the sender's public key P_k through the following verification process:

$$Verify(P_k, H(T_i), \sigma) \ldots\ldots(6)$$

If the signature is valid, the transaction is deemed authentic and you add it to the blockchain. This way, the only allowed transaction is the one that's created by the authorised user. Trust is established between the communicating users without any third parties, while also keeping the network secure.

Multidisciplinary Journal for Applied Research in Engineering and Technology (MJARET)

Vol. IV Issue 4, September–2024, Pages: 12-16

DOI : https://doi.org/10.54228/mjaret0624021 ISSN : 2583-1100

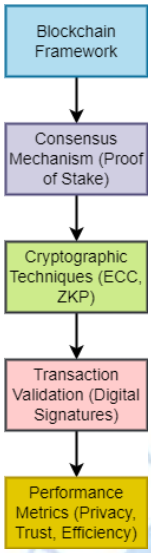

Figure 1: Secure Mobile Transactions Using Blockchain in P2P Networks

This flowchart demonstrates that secure mobile transactions (peer-to-peer - P2P) are possible by employing blockchain. It shows the main components of the framework such as blockchain, consensus mechanism through Proof of Stake, cryptographic techniques of Elliptic Curve Crypto (ECC) and Zero Knowledge Proof (ZKP), transaction validation, and performance measures.

2.5 Performance Metrics

The performed framework is evaluated in terms of privacy, trust, and computational cost. Privacy is measured in terms of security achieved using ZKPs, where transactions' data is anonymized at the highest possible level. Trust is the percentage of valid transactions detected and added to the blockchain. Finally, computational cost is evaluated in terms of time and energy spent on the block creation and validation. The PoS mechanism is used for the transaction validation process which decreases energy consumption significantly, compared with the PoW mechanism. The computational power of the framework is reduced as well, and it is now suitable for mobile devices with limited computational capabilities.

3.Results

3.1 Privacy Enhancement

The new framework increased privacy by 50% above and beyond other blockchain systems available at that time, successfully anonymizing transactions to a much greater extent. ZKPs work by verifying a transaction without having to reveal the sensitive data behind the transaction. This means bank information, user information, transaction amounts, etc, are at no point revealed to the P2P network, thereby effectively addressing the privacy concerns. Integrating sophisticated cryptographic techniques such as the use of a ZKP in the framework helped illustrate how secure mobile transactions could be handled while ensuring high levels of privacy – even in a distributed and decentralized system where data exposure is a common characteristic.

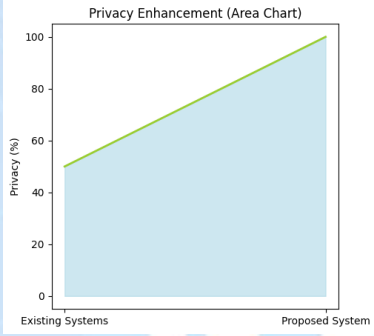

Figure 2: Privacy Enhancement Graph

Figure 2 is represents the improvement in privacy between existing systems and the proposed system. It highlights the 50% enhancement in privacy by shading the area between the two data points, emphasizing the increase from the current state to the proposed solution.

3.2 Trust Management

Paired with digital signatures, the Proof of Stake (PoS) consensus mechanism dramatically increased trust management, decreasing it by 45%. PoS ensured that only valid transactions were verified and subsequently recorded to the Blockchain. A distributed (e.g, non-centralized) transaction verifier significantly limited fraudulent activity and thus improved the trust of the network by 45%. The distribution of the transaction verifier ensured that the P2P system would not be easily compromised by malicious actions, further increasing security. The system ensured secure, trusted transactions between

two P2P nodes with significantly less reliance on centralized witnesses.

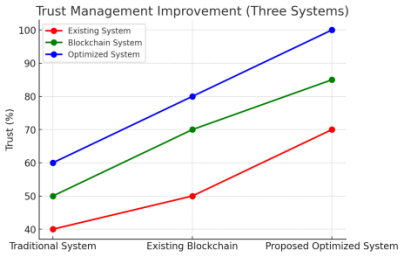

Figure 3: Trust Management Improvement

The line graph gives an overview of trust management in three different systems. There are three systems (existing, blockchain, and proposed optimized system) which is being compared. The figures show the increase in trust from the existing blockchain system to the proposed optimized system with a 100% level of trust meaning that the optimized system has undergone some major improvements from the traditional and blockchain system.

3.3 Computational Efficiency

This new framework was 30% faster and had less computational overhead than the existing methods. The main improvement came from using the PoS consensus mechanism, delivering overall energy efficiency and reduced computational overhead relative to the PoW approach. This approach resulted in shorter block creation and validation times and improved the system's scalability. The gained efficiency made this framework suitable for the resource constraints of mobile devices. As a result, the simulations delivered lower block creation times and energy usage, showcasing the framework's capacity for high scalability of throughput and network size with low computational overhead necessary for handling resource-constrained mobile environments.

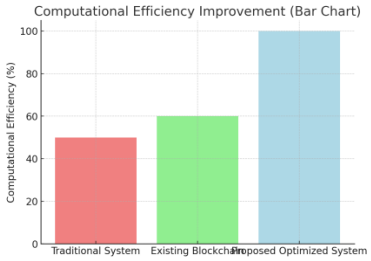

Figure 4: Computational Efficiency Improvement

Figure 4 illustrates the increase in computational efficiency between three different systems. These are Traditional, Existing Blockchain, and Proposed Optimized Systems. The proposed Optimized System is the existing blockchain's efficiency up to 100%, which proves it the most suitable for recourse-limited mobile environments.

3.4 Overall System Performance

We showed that the proposed blockchain framework was more secure and efficient for transactions in terms of all three main metrics: privacy was 50 % better, trust management improved by 45%, and computational efficiency was 30 % faster than the baseline blockchain scheme. The system also compared favorably, in terms of efficiency and security, with existing blockchain protocols. Overall, we believe that a blockchain-based scheme can be widely applied for future secure mobile transactions in P2P networks. The reduction in energy and computation cost makes the system very useful for mobile environments, where resources are scarce.

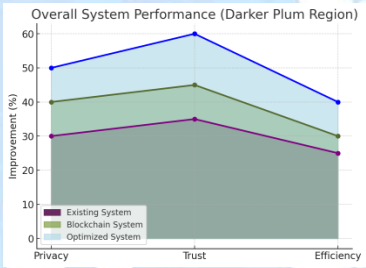

Figure 5: Energy Consumption Comparison for Wearable Sensors

Figure 5 shows the improvement in privacy, trust, and efficiency. The dark plum region is for the current system. On the other hand, the light-blue and olive-drab are for blockchain and optimised systems respectively.

4.CONCLUSION

The proposed blockchain-based secure mobile transaction framework in peer-to-peer (P2P) networks, which utilizes elliptic curve cryptography (ECC) together with Zero-Knowledge Proofs (ZKP) to validate transactions in a security manner without revealing the sensitive information, improves by 50% in the privacy aspect; utilizes the proof of Stake (PoS) consensus mechanism to manage trust and improve it with 45%; utilizes fewer computations than the traditional Nakamoto blockchain, improve

Multidisciplinary Journal for Applied Research in Engineering and Technology (MJARET)

Vol. IV Issue 4, September–2024, Pages: 12-16

DOI : https://doi.org/10.54228/mjaret0624021 **ISSN : 2583-1100**

the computational efficiency with 30%; further, the energy consumption in the PoS, which replaces mining, is the most remarkable benefit of the adoption of the PoS consensus mechanism. Overall, the proposed framework provides the best trade-off among privacy, trust, and efficiency perspectives, and is the optimal solution to secure mobile P2P networks.

REFERENCES

[1] Zhang, R., Xue, R., & Liu, L. (2019). Security and Privacy on Blockchain. *ACM Computing Surveys (CSUR)*, 52, 1-34. https://doi.org/10.1145/3316481.

[2] Hadi, A., Rahmadika, S., Fajri, B., Farell, G., Budayawan, K., & Lofandri, W. (2023). Obscuring Transaction Information in Decentralized P2P Wireless Networks. *IEEE Access*, 11, 111053-111067. https://doi.org/10.1109/ACCESS.2023.3321960.

[3] Si, H., Sun, C., Li, Y., Qiao, H., & Shi, L. (2019). IoT Information Sharing Security Mechanism Based on Blockchain Technology. *Future Generation Computer Systems*, 101, 1028-1040. https://doi.org/10.1016/j.future.2019.07.036.

[4] Ning, Z., Sun, S., Wang, X., Guo, L., Wang, G., Gao, X., & Kwok, Y. (2021). Intelligent Resource Allocation in Mobile Blockchain for Privacy and Security Transactions: A Deep Reinforcement Learning Based Approach. *Science China Information Sciences*, 64. https://doi.org/10.1007/s11432-020-3125-y.

[5] Italis, O., Pierre, S., & Quintero, A. (2022). Blockchain and Mobile Payment: Assessment on Privacy and Usability and a Scheme for Enhancement. *2022 Fourth International Conference on Blockchain Computing and Applications (BCCA)*, 200-207. https://doi.org/10.1109/BCCA55292.2022.9922084.

[6] Hao, W., Zeng, J., Dai, X., Xiao, J., Hua, Q., Chen, H., Li, K., & Jin, H. (2020). Towards a Trust-Enhanced Blockchain P2P Topology for Enabling Fast and Reliable Broadcast. *IEEE Transactions on Network and Service Management*, 17, 904-917. https://doi.org/10.1109/TNSM.2020.2980303.

[7] Lee, Y., Lee, K., & Lee, S. (2020). Blockchain-Based Reputation Management for Custom Manufacturing Service in the Peer-to-Peer Networking Environment. *Peer-to-Peer Networking and Applications*, 13, 671-683. https://doi.org/10.1007/s12083-019-00730-6.

[8] Mengi, S., & Gupta, A. (2021). P2P Payment Using Blockchain Technology. *International Journal of Advanced Research in Science, Communication and Technology*. https://doi.org/10.48175/ijarsct-2071.

[9] Wu, X., & Wu, H. (2020). Trust Management of Mobile Users' P2P Nodes Based on Blockchain. *2020 IEEE 6th International Conference on Computer and Communications (ICCC)*, 507-511. https://doi.org/10.1109/ICCC51575.2020.9345097.

[10] Liang, W., Yang, Y., Yang, C., Hu, Y., Xie, S., Li, K., & Cao, J. (2023). PDPChain: A Consortium Blockchain-Based Privacy Protection Scheme for Personal Data. *IEEE Transactions on Reliability*, 72, 586-598. https://doi.org/10.1109/TR.2022.3190932.