Decentralized Payment System

Vaibhav Bhaliya ,

B.E INFT

*St Francis Institute of Technology*Mumbai, India

vaibhavbhaliya@student.sfit.ac.in

Rahul Biya

B.E INFT

*St Francis Institute of Technology*Mumbai, India

rahulbiya@student.sfit.ac.in

Sasank Paria

B.E INFT

*St Francis Institute of Technology*Mumbai, India

sasankparia@student.sfit.ac.in

Gauresh Wadekar

B.E INFT

*St Francis Institute of Technology*Mumbai, India

gaureshwadekar92@sfit.ac.in

Balaraju Vijayalakshmi

Assistant Professor in Information Technology

*St Francis Institute of Technology*Mumbai, India

balarajulakshmi@sfit.ac.in

**ABSTRACT**

Blockchain technology, based on Ethereum, has revolutionized financial transactions. However, challenges related to speed and data protection persist. While numerous technologies have been developed in the blockchain field, they often lack innovation, and there is no perfect system that incorporates new features to enhance the overall speed of cryptocurrency transactions. This project introduces a groundbreaking solution by integrating a scan-to-pay feature and using the SHA-512 hashing algorithm to boost efficiency. The scan-to-pay feature simplifies transactions through QR codes, reducing complexity and errors and optimizing the user experience. Its versatility allows for easy integration into existing systems without requiring extensive modifications. Simultaneously, the SHA-512 algorithm strengthens security, protecting sensitive payment data and mitigating risks. By seamlessly combining user-centric features and advanced security measures, our project contributes to the evolution of Ethereum's blockchain technology, addressing critical issues and propelling decentralized payment systems into a new era of usability and protection.

Keywords: Ethereum Blockchain, Scan-to-Pay, SHA-512, QR codes, smart contracts

**1.INTRODUCTION**

Blockchain is a revolutionary technology that serves as a decentralized and distributed ledger, enabling secure and transparent record-keeping of transactions across a network of computers [1]. It operates on a consensus mechanism, ensuring that all participants agree on the validity of the recorded information without the need for a central authority. Ethereum blockchain is a decentralized and distributed ledger technology that operates on a network of computers worldwide. Unlike traditional centralized systems, Ethereum does not rely on a single authority to validate and record transactions [3]. Instead, it employs a consensus mechanism where nodes in the network agree on the state of the blockchain. The uniqueness of Ethereum lies in its ability to execute smart contracts. Smart contracts are self-executing agreements with the terms directly encoded into computer programming, allowing for trustless and automated transactions without intermediaries [4].

The decision to use Ethereum stems from its versatility and the capability it offers to build decentralized applications (DApps) and smart contracts. Ethereum serves as a platform for developers to create a wide range of applications, from decentralized finance (DeFi) systems to token issuance and more. Its decentralized nature ensures security and transparency, providing users with control over their data and transactions.

Using Ethereum involves interacting with its blockchain through a cryptocurrency wallet. Users can create accounts on the Ethereum network, each identified by a unique address. Transactions are initiated by sending cryptocurrency, such as Ether (ETH), from one account to another. Smart contracts can be deployed on the Ethereum network, and users can interact with these contracts by sending transactions that execute specific functions encoded in the contract's code

II.LITERATURE REVIEW

Blockchain is a tamper-evident and tamper-resistant digital ledger system, operating in a distributed and decentralized manner. Originally introduced in 2008 with Bitcoin, it facilitates a community of users to record irreversible transactions in a shared ledger. Users employ cryptographic mechanisms, utilizing public and private keys, to digitally sign and securely transact within the system. The blockchain's decentralized nature, maintained collaboratively by a distributed group, ensures resilience against attempts to modify the ledger.[1]

The paper underscores the significance of secure transactions and challenges associated with third-party involvement in transactional security. Emphasizing blockchain as a tamper-proof solution for transaction tracking, the paper discusses various consensus protocols like Hyperledger Fabric and Ethereum. The potential applications of blockchain across diverse domains, including healthcare, science, literacy, publishing, economic growth, and art and culture, are highlighted. Additionally, the paper introduces Hyperledger as an open-source collaboration aimed at enhancing the efficiency and reliability of blockchain systems.[3]

The paper delves into the pivotal role of hash functions in network security and cryptography, offering insights into well-known algorithms such as SHA-1, SHA-2, SHA-3, MD4, MD5, and Whirlpool. Conducting a comparative analysis, it evaluates the varying levels of security provided by these hash algorithms. The paper underscores the use of hash functions in ensuring the integrity, authenticity, and digital signature of transmitted data, fostering secure communication between sender and receiver. The crucial role of hash functions in key generation for both symmetric and asymmetric key cryptosystems is highlighted as well.[9]

Xiaofei Luor proposes a decentralized payment routing scheme and a Markov Chain-based routing algorithm to improve the efficiency of payment channel networks (PCNs). The proposed routing algorithm achieves higher throughput and shorter payment times compared to other routing schemes, ensuring efficient payments in PCNs. The multi-branch routing scheme improves payment success ratio and reduces collateral requirements in PCNs. But this results in increased transaction time compared to non-routing methods. Since routing requires more machines, it may results in more maintenance and lead to potential issues.[10]

Yuhui Zhang discusses the routing challenges in Payment Channel Networks (PCNs) and highlights the distinct features of PCNs that differentiate them from conventional ad-hoc networks. It proposes an (i, j)-MTFM algorithm for routing in PCNs, which involves splitting nodes and constructing payment paths. It aims to optimize the routing process by considering the feasibility and timeliness constraints specific to PCNs.[11].

Decentralized payment systems leverage distributed ledgers for transaction recording, but early implementations face privacy challenges. Privacy-enhanced solutions like Monero and Zerocash address these concerns. While completely decentralized anonymous payment systems resist effective regulation, striking a balance between privacy and regulation is crucial. A proposed system integrates SPK for knowledge arguments, an extractor for rewinding, and a register procedure for managers and users. Employing on-chain (TX) and off-chain (TLS) communication methods, the system aims to achieve the delicate equilibrium of privacy and regulation.[12].

Kim-Kwang Raymond Choo utilizes zero-knowledge Succinct Non-interactive ARguments of Knowledge (zk-SNARKs) to construct a decentralized anonymous payment scheme (DAP scheme) called Zerocash. It leverages recent advances in zk-SNARKs to formulate and construct the DAP scheme, which enables users to make private payments with hidden origin, destination, and amount. The transactions in Zerocash are less than 1 kB and take under 6 ms to verify. The paper presents a full-fledged ledger-based digital currency, Zerocash, that offers strong privacy guarantees for decentralized anonymous payments by hiding the payment's origin, destination, and transferred amount.[13]

**A. CHALLENGES**

The literature survey reveals notable observations and identifies gaps in existing research. The implementation of routing in transactions has been found to potentially impact speed. The involvement of third parties poses risks to user privacy and security. Notably no innovative approaches have been implemented to enhance transaction speed. Addressing these concerns presents an opportunity for future research to explore novel solutions, ensuring efficient and secure transactions without sacrificing speed or compromising user privacy.

**III. PROPOSED SYSTEM**

Addressing the imperative for innovation in blockchain-based payment systems, our focus is on crafting an advanced decentralized payment ecosystem for Ethereum. While current blockchain technologies have transformed digital transactions, issues persist regarding user accessibility and transaction speed. The objective is to overcome these challenges by introducing novel features, including seamless QR code scanning for payments and robust security through SHA-512 encryption. Striking a balance between user-friendliness and data protection, our approach builds upon existing blockchain foundations.

The proposed blockchain payment system integrates QR code scanning for streamlined transactions while prioritizing security with SHA-512 encryption. SHA-512, part of the SHA-2 family, provides robust 512-bit output, enhancing data protection against potential threats. Each user is assigned a unique QR code linked to their wallet address, facilitating speedy cryptocurrency transfers. SHA-512 encrypts transaction details, bolstering privacy for both senders and receivers. Its fixed-length 512-bit output ensures resistance to collision and preimage attacks, making it suitable for digital signatures and secure data storage. Implemented through a user-friendly website, the system enables wallet connection and manual entry or QR code scanning of receiver addresses, ensuring secure and private transactions.

**III. A SYSTEM DESIGN**



Fig. 1 System Design

Users will first need to connect their MetaMask wallet to their account on our website. Then, they can send Ethereum to anyone by entering necessary details like the receiver's address. Every transaction will take place through a smart contract, which provides encryption, security, and privacy to the sender and receiver. User sends the payment to another user using XCrypt and can also receive a payment. Users can also see the transaction details. Additional information about the user, like wallet address and wallet balance, can also be displayed. Wallets are used for the storage of users' cryptocurrencies. Information about the user, such as wallet address and wallet balance, can be displayed.

**IV. METHODOLOGIES**

Transactions undergo hashing using the SHA-512 hashing algorithm. Subsequently, all transactions contribute to the creation of a Merkle tree, with its root node being appended to the blockchain. Proof of Stake is employed to validate transactions within the blockchain.

SHA-512 is considered to have better security than SHA-1 due to its larger hash value and resistance to various attacks. Here are some key differences between the two algorithms: SHA-1 generates a 160-bit (20-byte) hash value, while SHA-512 generates a 512-bit (64-byte) hash value. A large hash value makes SHA-512 more resistant to attacks and less prone to hash collisions. It has not been compromised and will remain secure for at least the next few years. In contrast, it is generally slower than SHA-1 but is still faster than SHA-256 for processing larger strings. However, for small strings, SHA-256 is faster. SHA-512 provides better security than SHA-1 due to its large hash value and more secure algorithm structure. It is more suitable for applications that require high security, such as password hashing and digital signatures.

Proof of Stake (PoS) is a consensus mechanism used in blockchain networks to validate and confirm transactions and secure the network. Unlike Proof of Work (PoW), where miners compete to solve complex mathematical puzzles to validate transactions and create new blocks, PoS relies on validators who to create new blocks and validate transactions based on the number of cryptocurrency tokens they hold and are willing to "stake" or lock up as collateral. In a PoS system, validators are choosed to create new blocks and validate transactions based on multiple factors like the number of tokens they hold and how long they have been staking them. The probability of being chosen as a validator is directly proportional to the amount of cryptocurrency tokens they have staked. The likelihood of being selected as a validator increases in direct proportion to the quantity of cryptocurrency tokens they have staked.

PoS is more energy efficient than PoW because it does not require the massive computational power to solve complex puzzles. Additionally, PoS is to be more resistant to centralization since it isnt heavily influenced by mining power concentration. Overall, PoS is a consensus mechanism that aims to provide security and validate transactions in a decentralized manner by leveraging participants' stake in the network.

**V. RESULTS AND DISCUSSIONS**



Fig 2. Connect with Wallet



Fig3. Ethers transfer thru QR code



Fig 4. Crypto Price Tracker

**VI. CONCLUSION**

In this study, we delved into decentralized payment systems, focusing on Ethereum-based solutions to enhance user experience. Blockchain adoption has freed transactions from centralized constraints, providing decentralization, scalability, and security. We identified concerns like scalability, slow speeds, high fees, wallet intricacies, security vulnerabilities, user errors, regulatory challenges, and environmental impacts. Our solutions include QR payment integration for faster transactions and SHA-512 encryption for heightened security. Results demonstrate improved efficiency, addressing concerns and positioning Ethereum-based systems as user-friendly and eco-conscious. These advancements signify progress in decentralized payment adoption amid the evolving digital transaction landscape.

Future enhancements for our decentralized payment system include the incorporation of a chat feature for user communication, the development of a mobile application to expedite cryptocurrency transfers, updates to the hashing algorithm for heightened security, and the potential addition of support for various cryptocurrencies beyond Ethereum, ensuring adaptability and sustained innovation.

**References**

[1] Yaga, D. , Mell, P. , Roby, N. and Scarfone, K. (2018), Blockchain Technology Overview, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.IR.8202 (Accessed January 22, 2024)

[2] A. Averin and O. Averina, "Review of Blockchain Technology Vulnerabilities and Blockchain-System Attacks," 2019 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon), Vladivostok, Russia, 2019, pp. 1-6, doi: 10.1109/FarEastCon.2019.8934243.

[3] K. Huang, J. Ma and X. Wang, "A Comparative Analysis of Bitcoin and Ethereum Blockchain," 2021 2nd International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT), Shanghai, China, 2021, pp. 678-682, doi: 10.1109/AINIT54228.2021.00137.

[4] Khan, Shafaq & Loukil, Faiza & Ghedira, Chirine & Benkhelifa, Elhadj & Bani-Hani, Anoud. (2021). “Blockchain Smart Contracts: Applications, Challenges, and Future Trends”, September 2021 Peer-to-Peer Networking and Applications. DOI:10.1007/s12083-021-01127-0

[5] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han and F. -Y. Wang, "Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 49, no. 11, pp. 2266-2277, Nov. 2019, doi: 10.1109/TSMC.2019.2895123

[6] Bartoletti M., Pompianu L. (2017), “An Empirical Analysis of Smart Contracts: Platforms, Applications, and Design Patterns” In: Brenner, M., et al. Financial Cryptography and Data Security. FC 2017. Lecture Notes in Computer Science(), vol 10323. Springer, Cham. https://doi.org/10.1007/978-3-319-70278-0\_31

[7] S. Yan, "Analysis on Blockchain Consensus Mechanism Based on Proof of Work and Proof of Stake," 2022 International Conference on Data Analytics, Computing and Artificial Intelligence (ICDACAI), Zakopane, Poland, 2022, pp. 464-467, doi: 10.1109/ICDACAI57211.2022.00098.

[8] Sumagita, Meiliana and Imam Riadi. “Analysis of Secure Hash Algorithm (SHA) 512 for Encryption Process on Web Based Application.” International Journal of Cyber-Security and Digital Forensics 7 (2018): 373-381.

[9] Prashant P. Pittalia, "A Comparative Study of Hash Algorithms in Cryptography," International Journal of Computer Science and Mobile Computing, Vol.8 Issue.6, June- 2019, pg. 147-152, S. P. University, India, 2019, pp. 788-792.

[10] X. Luo and P. Li, "LEAF: Let’s Efficiently Make Adaptive Forwarding in Payment Channel Networks," in IEEE Access, vol. 11, pp. 4194-4206, 2023, doi: 10.1109/ACCESS.2023.3235828.

[11] Y. Zhang and D. Yang, "RobustPay+: Robust Payment Routing With Approximation Guarantee in Blockchain-Based Payment Channel Networks," in IEEE/ACM Transactions on Networking, vol. 29, no. 4, pp. 1676-1686, Aug. 2021, doi: 10.1109/TNET.2021.3069725

[12] C. Lin, D. He, X. Huang, M. K. Khan and K. -K. R. Choo, "DCAP: A Secure and Efficient Decentralized Conditional Anonymous Payment System Based on Blockchain," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 2440-2452, 2020, doi: 10.1109/TIFS.2020.2969565

[13] E. Ben Sasson et al., "Zerocash: Decentralized Anonymous Payments from Bitcoin," 2014 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 2014, pp. 459-474, doi: 10.1109/SP.2014.36

[14] Jani, Shailak. (2018). The Growth of Cryptocurrency in India: Its Challenges & Potential Impacts on Legislation. 10.13140/RG.2.2.14220.36486.

[15] Raoul722, “Is double SHA-256 the best choice for Bitcoin?,” Cryptography Stack Exchange, https://crypto.stackexchange.com/questions/87434/is-double-sha-256-the-best-choice-for-bitcoin (accessed Oct. 22, 2023).

[16] Paul, “Ethereum Tutorial – A Deeper Look Into Ethereum!”, Edureka!, https://www.edureka.co/blog/ethereum-tutorial-with-smart-contracts (accessed Oct. 22, 2023)