Bank-Guard Fusion System

Prof. Nikita Gosavi
Department of Computer Engineering
JSPM's JSCOE
nikitagosavi1113@gmail.com

Ms. Taniya Jagtap
Department of Computer Engineering
JSPM's JSCOE
taniyajagtap8861@gmail.com

Ms. Sanika Solapure
Department of Computer Engineering
JSPM's JSCOE
sanikasolapure@gmail.com

Mr. Atharv Nikude
Department of Computer Engineering
JSPM's JSCOE
atharvanikude761@gmail.com

Mr. Akash Sulgekar
Department of Computer Engineering
JSPM's JSCOE
akashsulgekar@gmail.com

Abstract - This paper introduces Bank-Guard Fusion System, a decentralized blockchain wallet system designed for secure cryptocurrency management. Utilizing blockchain's decentralized, cryptographic strengths, the platform enables wallet creation, balance checks, and transactions in a user-friendly, secure environment. Built with React.js, Flask, and MongoDB, it provides a seamless interface and decentralized data handling. Integrating Proof of Work (PoW) and Proof of Stake (PoS) for transaction validation, this solution enhances trust, transparency, and security, bridging users and blockchain technology to facilitate sustainable, scalable, and robust digital transactions.

Keywords – Blockchain, Cryptocurrency, Flask, MongoDB, React.js, Decentralized Application, Wallet, Secure Transactions, PoW, PoS, XMSS, Hybrid Security

I. INTRODUCTION

(Bank-Guard Fusion System)

Blockchain technology, originally developed to support cryptocurrency transactions, has evolved into a transformative tool across many sectors, including finance, healthcare, and supply chain management. Its decentralized architecture eliminates the need for intermediaries, making it highly suitable for secure and transparent transactions. Blockchain's key attributes—decentralization, immutability, and cryptographic security—offer numerous benefits for industries dealing with sensitive data or transactions, such as the banking sector. In traditional banking, security and trust are managed through central authorities and intermediaries, leading to issues like high transaction fees, slow processing times, and vulnerability to cyberattacks. Blockchain disrupts this model by allowing peer-to-peer transactions that are recorded in an immutable ledger, which reduces the risks of tampering, fraud, and unauthorized access. However, blockchain technology faces challenges in terms of user accessibility, transaction efficiency, and scalability. This paper, titled the Bank-Guard Fusion System, proposes a decentralized wallet application that harnesses blockchain to provide a secure, transparent, and user-friendly solution for digital asset management. The system is designed to allow users to create wallets, check balances, and conduct transactions within a robust and scalable framework. It utilizes a hybrid consensus model combining Proof of Work (PoW) and Proof of Stake (PoS), ensuring security and energy efficiency. Additionally, it incorporates the ExtendedMerkle Signature Scheme (XMSS) for quantum resistance, making the system future-proof against emerging quantum threats. The Bank- Guard Fusion System employs modern development tools: React.js for the frontend interface, Flask for backend processing, and MongoDB for decentralized data storage. By integrating these technologies, the project addresses several limitations in current financial systems, such as limited accessibility to secure digital asset management and reliance on centralized authorities. This blockchain- based wallet system aims to bridge the gap between users and blockchain, offering a solution that is as accessible and secure as it is technologically advanced.

Overview: The Bank-Guard Fusion System is a decentralized blockchain wallet application that enhances digital asset management security and accessibility. Using React.js for the frontend, Flask for backend processing, and MongoDB for decentralized storage, it offers users a secure platform for wallet creation, balance checks, and transactions. With a hybrid PoW and PoS consensus model, combined with XMSS for quantum resistance, Bank-Guard Fusion System ensures robust security, efficiency, and scalability, bridging the gap between users and blockchain for a more secure, transparent financial experience.

II. LITERATURE SURVEY

The paper highlights blockchain's transformative impact on financial systems by enabling decentralized, peer-to-peer transactions that eliminate intermediaries. This shift not only lowers transaction costs but also enhances overall security. In paper [1] the integration of quantum-resistant algorithms into Ethereum's blockchain, highlighting performance and memory usage. It identifies the Dilithium2 algorithm as a viable alternative, with minimal impact on blockchain efficiency. This paper discusses the role of blockchain in reshaping financial systems worldwide. The paper elaborates on how decentralized systems remove the need for intermediaries, thus reducing transaction costs and increasing security. Despite the performance trade-offs, the results indicate that a blockchain using quantum-resistant algorithms can maintain high performance with minimal increases in resource consumption (0.029% increase in block processing time and 0.2% memory savings). The paper concludes that the integration of quantum-resistant algorithms into blockchains is feasible without significantly degrading performance, and the findings support the viability of quantum-safe blockchain systems.

The paper [2] evaluates the complexity of different consensus algorithms in blockchain, focusing on Proof-of-Work (PoW), Proof-of-Stake (PoS), and hybrid protocols. Using Crutchfield's Statistical Complexity measure, the study shows that PoS protocols (like Nxt and Qtum) have much higher complexity compared to PoW. The paper highlights that while PoW is less complex, PoS introduces unnecessary computational complexity, which may affect scalability and efficiency. It suggests that this increased complexity could lead to chaotic system behavior. The paper also calls for further exploration of next-gen consensus algorithms like DAG, IOTA, and HashGraph. In this paper, researchers introduced a hybrid consensus algorithm that combines Proof of Work (PoW) and Proof of Stake (PoS) mechanisms. This combination enhances the overall security and reduces energy consumption while maintaining the decentralized nature of blockchain. Hybrid Algorithm: Limited analysis of hybrid PoW-PoS protocols, lacking a detailed examination of impacts on real-world scalability, network security, or specific attack vectors like 51% attacks. PoW: While PoW is discussed in terms of low complexity, the paper does not analyze its energy efficiency or more sophisticated hybrid mechanisms and their potential for security or performance optimization. PoS: The paper identifies PoS protocols as overly complex but does not delve into how PoS complexity impacts potential vulnerabilities in depth, particularly under conditions of increasing network load. The paper [3] titled Hybrid Double-Spending Attack by Akbar, Muneer, El Hakim, and Fati (2021) explores vulnerabilities in blockchain systems, specifically focusing on double-spending attacks. It introduces a hybrid model combining elements from existing attack vectors to assess the effectiveness of such threats in decentralized networks. The study evaluates the impact on both PoW and PoS systems, addressing the challenges posed by malicious actors attempting to manipulate transactions through double-spending tactics. The paper [4] shows the success and popularity of Bitcoin mainly focuses the underlying blockchain technology which is totally immutable distributed ledger, highly secured by its P2P network consensus named Proof of Work (PoW). One of the worst threats to a Proof-of-Work based cryptocurrency is 51% attack. If one or more dishonest network peer gains more than 50% of resource such as processing power, then they will become the majority decision maker in the network. It is already proved that mixing of two or more existing protocol that is called hybrid protocol can make the network enough resistive to this attack. The recent implementations of hybrid protocols have other limitations and problems that they are facing and striving to resolve. But their main weakness is in distribution of block mining reward to the investors. From the perspective of an investor, an investor invests his hard-earned money in a cryptocurrency for making proper profit from his investment. The main source of this profit is the block reward which is generated and given to the miner on successful mining of a block. So, to ensure this profit is given to proper user on proper time interval, the consistency of block generation time interval is a vital factor.

III. PROPOSED SYSTEM

A. PROBLEM STATEMENT

The problem statement of the Bank-Guard Fusion systemaddresses the need for a secure, user-friendly, and decentralized platform for managing digital assets. In traditional banking and financial systems, centralization introduces issues like high transaction fees, slow processing times, security vulnerabilities, and reliance on intermediaries. As cryptocurrency and digital assets become more widespread, users face challenges in managing these assets securely and efficiently due to the complexity of blockchain technology and the risk of cyberattacks. This paper seeks to overcome these challenges by developing a blockchain wallet system that combines advanced security features, such as Proof of Work (PoW) and Proof of Stake (PoS) for transaction validation, and quantum-resistant algorithms to protect against emerging threats. The goal is to create a decentralized, scalable, and accessible platform that allows users to manage digital assets seamlessly, bridging the gap between users and blockchain technology while providing a robust alternative to traditional financial systems.

B. OBJECTIVE

The objective of the Bank-Guard fusion system is to develop a secure, decentralized blockchain wallet system that addresses key challenges in digital asset management. The system aims to enhance security by utilizing a hybrid approach of Proof of Work (PoW) and Proof of Stake (PoS) consensus mechanisms for reliable transaction validation. Additionally, it incorporates quantum-resistant algorithms, such as the Extended Merkle Signature Scheme (XMSS), to safeguard against potential quantum computing threats, ensuring long-term resilience. The project also focuses on user accessibility by providing a simplified interface through React.js, enabling both technical and non-technical users to interact with blockchain securely. By leveraging MongoDB for decentralized and scalable data storage, the system maintains reliable transaction records while supporting platform growth. To promote energy efficiency, the project combines PoW and PoS to reduce energy consumption without compromising security. Furthermore, by enabling peer-to-peer transactions, the platform minimizes the need for intermediaries, lowering transaction costs and increasing financial inclusivity. Ultimately, this project bridges the gap between users and blockchain technology by offering a secure, accessible, and scalable wallet system designed for the evolving needs of the digital financial ecosystem.

C. METHODOLOGY

The methodology of the paper focuses on creating a secure, decentralized blockchain wallet system by integrating front-end, back-end, and data management technologies with advanced consensus and cryptographic methods. The front end of the system is developed using React.js, providing an intuitive interface for users to manage wallets, check balances, and conduct transactions seamlessly. Flask is employed for the backend, handling API requests and enabling communication between the user interface and the blockchain network, while MongoDB serves as the primary decentralized data storage solution to ensure scalability and efficient transaction handling.

To secure the network, the project uses a hybrid consensus

model combining Proof of Work (PoW) and Proof of Stake (PoS). PoW ensures robust transaction validation, while PoS enhances energy efficiency and network stability. For quantum-resistant security, the Extended Merkle Signature Scheme (XMSS) is integrated to protect against future quantum threats, ensuring that user data and transactions remain secure. Together, these elements provide a system architecture that balances security, accessibility, and scalability. The methodology also includes iterative testing and refinement, ensuring each component functions efficiently and meets security standards. The testing phase involves validating wallet creation, balance checks, and transactions to confirm accuracy and security. By combining blockchain's decentralized architecture with a user-friendly interface and advanced security protocols, the methodology aims to deliver a reliable, scalable blockchain wallet system that addresses the needs of modern digital asset management.

D. ARCHITECTURE DIAGRAM

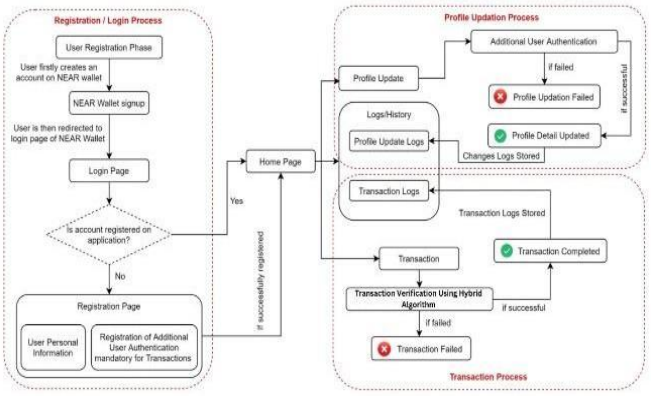

Fig. 3.1 Architecture Diagram

This design diagram shows the architecture of the Bank-Guard Fusion system,

1. Registration/Login Process
   User Registration Phase: User creates an account on the NEAR wallet. User is redirected to the login page.
   Login Page: The system checks if the user's account is registered on the application. If not, the user is directed to the registration page. If yes, the user is logged in.
   Registration Page: User provides personal information. Additional user authentication is mandatory for transactions.

2. Profile Update Process
   Profile Update: The user can update their profile information. The system logs the changes.
   Additional User Authentication: The user is required to authenticate themselves before making changes to their profile.
   Profile Update Logs: The system stores logs of profile updates.
   Transaction Logs: The system stores logs of transactions.

3. Transaction Process
   Transaction: The user initiates a transaction. The system verifies the transaction using a hybrid algorithm.
   Transaction Verification Using Hybrid Algorithm: The system verifies the transaction using a combination of different verification methods.
   Transaction Logs: The system stores logs of transactions.

4. Key Terms and Explanations
   NEAR Wallet: This is likely a digital wallet used for storing and managing cryptocurrency.
   Hybrid Algorithm: This refers to a combination of different algorithms used for transaction verification.
   Additional User Authentication: This is an extra security measure to ensure that only authorized users can make changes to their profile or initiate transactions.

E. MATHEMATICAL MODEL

Transaction: A transaction ti is validated by checking the sender's signature: ti = { S ,R ,A , σi }
Where σi is the valid cryptographic signature that ensures the transaction's authenticity.

Reward Distribution

Rewards are distributed to miners (PoW) or validators (PoS) as an incentive for participation:
Reward=f(Mining Effort or Stake)
This function f varies based on the system's consensus mechanism, encouraging participation while securing the network.

Block Creation
Each new block Bi is defined as a combination of the previous block's hash, the transactions Ti, the nonce n, and the cryptographic signature σ:
Bi=H(Bprev‖Ti‖n‖σ)
where:

- Bprev: Hash of the previous block.
- Ti: Transactions in the current block.
- n: Nonce (in PoW).
- σ : Signature ensuring data integrity.

PoW Validation: To validate the block, miners must solve the PoW puzzle: H(Bprev ‖T‖ n) < target

If true, the block is accepted as valid.

Where:Bprev is the previous block's hash.

- T is the current transaction data (e.g., ti).
- n is a nonce (a number used once) that miners adjust to find a valid hash.
- H is the cryptographic hash function (e.g., SHA-256).
- target is a predefined difficulty level for the puzzle, determining the required number of leading zeros in the hash output.

PoS Validation: The validator selection is based on the proportion of cryptocurrency held:

Validator Selection Probability= Pvalidator / Ptotal

Where:

- Pvalidator is the amount of cryptocurrency held by the validator.
- Ptotal is the total cryptocurrency supply in the network.

Quantum-Resistant Security:

Transactions are signed using XMSS: σi = XMSSSign(mi,k)

Where mi is the transaction data and k is the private key.

F. ALGORITHM

The Algorithms used are :

[1] Proof of Work (PoW)
[2] Proof of Stake (PoS)
[3] XMSS (Quantum-Resistant Signature)

The combined algorithm leverages Proof of Work (PoW), Proof of Stake (PoS), and XMSS (Quantum-Resistant Signature) to create a robust and secure blockchain system that balances security, energy efficiency, and future-proofing. In PoW, transactions are validated through a cryptographic puzzle, where miners compete to find a valid hash by solving complex computational challenges. This process requires substantial computational resources, ensuring the integrity of the blockchain and securing it against malicious actors. However, PoW can be energy-intensive due to the computational power required. In contrast, PoS offers a more energy-efficient alternative by selecting validators to propose the next block based on the amount of cryptocurrency they hold, with a higher stake increasing the probability of being chosen. This method eliminates the need for resource-heavy mining, offering a more sustainable way to validate transactions. The XMSS (eXtended Merkle Signature Scheme) is employed to provide quantum-resistant cryptographic signatures. Unlike traditional elliptic curve cryptography, XMSS relies on hash-based cryptography, which is resistant to potential quantum computing threats. This is crucial for securing the blockchain in the face of advancements in quantum technology. The algorithm works in a coordinated flow: users create and sign transactions using XMSS, ensuring the transaction's authenticity and quantum resistance. These transactions are then validated using either PoW or PoS. In PoW, miners solve the cryptographic puzzle to add the transaction block to the blockchain, while in PoS, validators are selected based on their cryptocurrency stake. Once validated, the block is added to the blockchain, and rewards, such as transaction fees or new cryptocurrency, are distributed to the miner or validator. This hybrid approach combines the strengths of PoW and PoS, ensuring that the blockchain is not only secure and resistant to attacks but also energy-efficient and prepared for future threats like quantum computing. This algorithm offers a comprehensive solution to the challenges of scalability

RESULTS AND ANALYSIS

The expected result of the system is the development of a decentralized, secure, and user-friendly wallet for managing cryptocurrency. This wallet is designed to provide users with a seamless and safe experience in handling their digital assets while ensuring the integrity and privacy of their transaction. By integrating advanced blockchain technologies such as Proof of Work (PoW) and Proof of Stake (PoS) for consensus, along with XMSS for quantum-resistant security, the system aims to deliver a robust platform for cryptocurrency. In terms of performance, the system is expected to provide fast transaction validation and a smooth user experience, with PoS reducing energy consumption and increasing efficiency, while PoW ensures strong security through cryptographic challenges. Overall, the wallet system will empower users with a secure, efficient, and user-friendly tool for managing their cryptocurrency assets.

The Fig. 4 .1 Shows the results of task user can perform

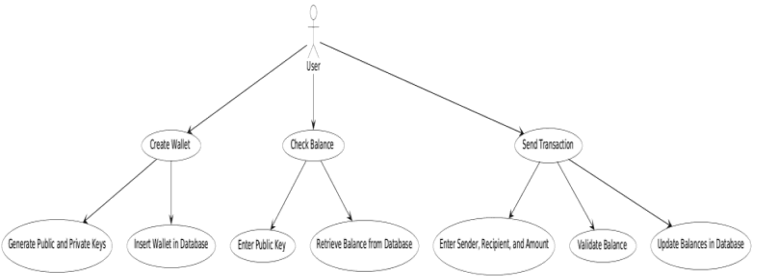

Fig. 4.1. Task User can Perform

The diagram illustrates the user flow within a cryptocurrency wallet. It shows the steps involved in creating a wallet, checking the balance, and sending transactions. The user starts by creating a wallet, which involves generating a public and private key pair and storing the public key in the wallet. The user can then check their balance by entering their public key and retrieving the balance from the database. To send a transaction, the user enters the sender's and recipient's addresses, the amount to be sent, and validates the balance. The system then updates the balances in the database accordingly.

The Fig.4.2. Shows the Frontend of Bank-Guard Fusion System, (React.js)

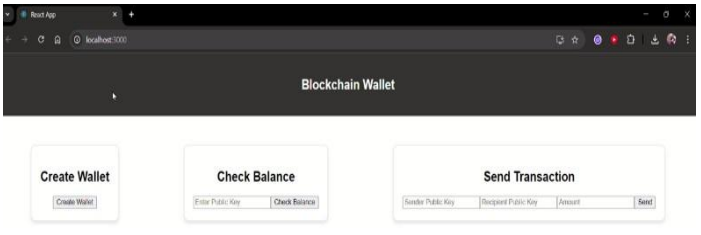

Fig .4.2 The Frontend of the Bank-Guard Fusion System.

The provided image showcases a React-based frontend for a blockchain wallet application. The user interface is composed of distinct cards, each dedicated to a specific functionality: creating a new wallet, checking an existing wallet's balance, and initiating a transaction. The presence of input fields for public keys and amounts, coupled with interactive buttons, further solidifies the interactive nature of the application. This design, leveraging the component-based structure of React, enables efficient development and maintenance of the user interface.

The Fig. 4 .3 Shows the Backend Output of the Bank-Guard Fusion System, (MongoDB)

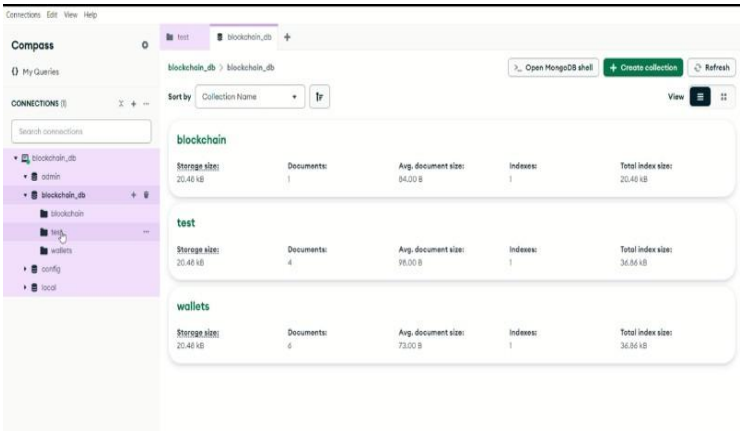

Fig.4.3 Output of the Bank-Guard Fusion System, (MongoDB)

This is the representation of MongoDB database management interface, likely using Compass. The hierarchical structure of databases and collections, along with the document-oriented nature of the data, confirms the use of MongoDB as the underlying database technology. This backend choice is ideal for applications demanding flexible data modeling and scalability.

IV. CONCLUSION

In conclusion, this blockchain wallet project offers a comprehensive solution for managing digital assets in a secure, scalable, and user-friendly manner within a decentralized framework. By leveraging cutting-edge web development technologies such as Flask, React.js, and MongoDB, in combination with blockchain consensus algorithms like Proof of Work (PoW) and Proof of Stake (PoS), we have created a platform that enables users to securely create wallets, check balances, and perform transactions. This system not only addresses key concerns in the cryptocurrency space, including trust, transparency, and security, but also empowers users to have greater control over their digital assets in a decentralized environment. The integration of PoW and PoS ensures both security and energy efficiency in the transaction validation process, while the use of XMSS offers quantum-resistant signatures, future-proofing the system against emerging threats from quantum computing. This combination of innovative technologies makes the platform resilient, fast, and scalable, providing users with a seamless experience in handling their cryptocurrency holdings. Furthermore, this paper highlights the transformative potential of decentralized applications (dApps) in reshaping traditional financial systems.ACKNOWLEDGEMENT

We would like to express our deepest gratitude to our guide, Prof. Nikita Gosavi, for her incredible support and mentorship throughout this project. Her insights, patience, and encouragement have been invaluable in guiding us through challenges and helping us grow. We are also very thankful to Dr. Poonam Lambhate , Head of the Computer Department, for her constant support and belief in our work, and to our Principal, Mr. R.D. Kanphade, for providing the resources and environment needed to bring this project to life. Our appreciation also goes out to the dedicated faculty and staff members whose assistance has been crucial at every step.

V. REFERENCES

[1] Karim Schierbauer, BSc (2024); Performance Measurement of Quantum-Resistant Algorithms in Blockchain Network.

[2] Renato P. Dos Santos (2022); PoW, PoS, & Hybrid Protocols: A Matter of Complexity.

[3] Akbar, N.A.; Muneer, A., ElHakim, N.; Fati, S.M. (2021); Hybrid Double-Spending Attack.

[4] Kishor Datta Gupta, Abdur Rahman, Subash Poudyal (2022); A Hybrid POW-POS Implementation Against 51 percent Attack in Cryptocurrency System.

[5] Singh, B. A. McGlynn, and J. Chen A Comprehensive Analysis of DeFi Protocol Vulnerabilities.

[6] Saleh, F. Block-chain Without Waste: Proof-of-Stake (2020). The Review of Financial Studies, 34(3), 1156-1190. doi:10.1093/rfs/hhaa075.

[7] Kim, H., & Laskowski, M. Toward an Ontology-Driven Block-chain Design for Supply-Chain Provenance (2018). Int. J. of E-Business Research (IJEBR),14(2),20-45.doi:10.4018/IJEBR.2018040102.

[8] Xie, H., Li, Z., & Wang, F. Practical Byzantine Fault Tolerance: A Comparative Analysis (2019). 2019 IEEE International Conference on Block-chain.

[9] Kiayias, A., & Panagiotakos, G. (2015). Speed-Security Tradeoffs in Block-chain Protocols. Cryptology ePrint Archive, Report 2015/1019.

[10] Buterin, V. (2014). A Next-Generation Smart Contract and Decentralized Application Platform. Ethereum Whitepaper.

[11] Larimer, D. (2014). Delegated Proof-of-Stake (DPoS). Steemit Article.

[12] Duong, T. X., Tran, T. A., & Bui, T. D. (2020). A Hybrid Consensus Algorithm Combining PoW and PoS for Block-chain Networks. IEEE Access, 8, 90685-90696. doi:10.1109/ACCESS.2020.2993845.

[13] Nakamoto, S. (2008). Bit-coin: A Peer-to-Peer Electronic Cash System. Bit-coin Whitepaper.

[14] Popper, N. (2015). Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money. Harper Business.

[15] Bonneau, J., Narayanan, A., Bonneau, J., Miller, A., & Clark, J. (2015). SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. In 2015 IEEE Symposium on Security and Privacy (pp. 104-121).

[16] Paillier, P. (1999). Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. In Proceedings of Eurocrypt 1999 (pp. 223-238). Springer.

[17] Chaum, D., & van Heyst, E. (1991). Group Signatures. In Proceedings of the 10th Annual International Conference on Theory and Application of Cryptographic Techniques (pp. 257-265). Springer.

[18] Rivest, R. L., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 21(2), 120-126.

[19] Dwork, C., & Naor, M. (1993). Pricing via Processing or Combatting Junk Mail. In Proceedings of the 12th Annual ACM Symposium on Principles of Distributed Computing (pp. 139-147). ACM

[20] Wood, G. (2014). Ethereum: A Secure Decentralized Generalized Transaction Ledger. Ethereum Whitepaper