IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 3, March 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303028 |

Building a Crypto Wallet with Solidity Smart Contracts and Meta Mask

Naveen Kumar V, Nireesh J, Sundheep S, Yokesh S, Dr.V.Prasanna Srinivasan

UG Students, Dept. of Information Technology, R.M.D. Engineering College, Tiruvallur, TamilNadu, India

Professor, Dept. of Information Technology, R.M.D. Engineering College, Tiruvallur, TamilNadu, India

ABSTRACT: Cryptocurrencies have revolutionized the concept of finance by introducing decentralized digital currencies that enable peer-to-peer transactions without the need for intermediaries. With the increasing adoption of cryptocurrencies, the need for secure and user-friendly wallets to store and manage digital assets has become paramount. This project aims to address this need by developing a cryptocurrency wallet smart contract using Solidity, the programming language for writing smart contracts on the Ethereum blockchain. The cryptocurrency wallet smart contract will provide users with a secure and decentralized solution for storing, sending, and receiving Ethereum-based tokens. The smart contract will implement essential wallet functionalities, including account creation, private key management, token transfers, balance tracking, and transaction verification.

KEYWORDS: Decentralized Finance (DeFi), Crypto Wallet, Solidity Smart Contracts, MetaMask, Ethereum Blockchain, Cryptocurrency Management, Trustless Transactions, Smart Contract Development, User Interface Integration, Security Best Practices

I. INTRODUCTION

Blockchain technology is a distributed ledger technology that allows for the creation of a secure and tamper-proof digital ledger that records every transaction that occurs between participants in the supply chain. This technology provides a transparent and efficient way to manage the supply chain, reducing the risk of fraud, counterfeiting, and other issues that can compromise the integrity of the supply chain.

A web-based blockchain wallet provides users with a convenient way to manage their cryptocurrency assets directly from their web browser. It offers accessibility across various devices with internet connectivity, enabling users to securely access their funds and conduct transactions from anywhere.

Additionally, these wallets often provide users with real-time updates on their account balance and transaction history, ensuring transparency and accountability. Overall, web-based blockchain wallets offer a user-friendly interface and seamless integration with the broader blockchain ecosystem, empowering individuals to participate in decentralized finance with ease.

Scalability and gas efficiency will be optimized to minimize transaction costs and enhance performance. Compatibility and interoperability with other Ethereum-based smart contracts and DeFi protocols will be prioritized, adhering to Ethereum's token standards. User authentication and authorization mechanisms will ensure that only authorized users can access and manage their funds, potentially incorporating multi-factor authentication and role-based access control. With the increasing adoption of cryptocurrencies, the need for secure and user-friendly wallets to store and manage digital assets has become paramount. The smart contract will implement essential wallet functionalities, including account creation, private key management, token transfers, balance tracking, and transaction verification.

II. RELATED WORK

First, anonymity is one of the reasons why people use cryptocurrencies like Bitcoin. However, there are some known techniques to reveal the identity of a user. Nevertheless, there exist also practical ways to make these attacks more difficult, for example, by using a new address for each new transaction. Our review of the literature has shown that only a few of the available applications use such methods.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303028 |

Our analysis is based both on the growing academic literature on the topic, on the participation to Internet blogs and discussion forums about Ethereum, and on our practical experience on programming smart contracts.Password based authentication mechanisms are inadequate for the protection of currencies within digital wallets. We present an efficient method to deanonymize Bitcoin users, which allows to link user pseudonyms to the IP addresses where the transactions are generated. Our techniques work for the most common and the most challenging scenario when users are behind NATs or firewalls of their ISPs.Cryptocurrencies are gaining prominence among individuals and companies alike, resulting in the growing adoption of so-called cryptocurrency wallet applications, as these simplify transactions.We have developed a novel probability theory for calculating a finitetime attack probability.This can be used to size up attack resources needed to obtain the profit. The results enable us to derive a sufficient and necessary condition on the value of a transaction targeted by a DS attack. Our result is quite surprising: we theoretically show how a DS attack at any proportion of computing power can be made profitable.

III. PROPOSED ALGORITHM

Our proposed system is a decentralized application that utilizes blockchain technology to manage and monitor crypto transfer in a transparent and secure manner. This system is designed to address some of the challenges faced by traditional wallets, such as limited transparency, traceability, and security. By leveraging blockchain technology, our system can provide a more efficient, transparent, and secure solution for managing crypto transfers.Our proposed system utilizes a decentralized architecture that is based on blockchain technology. The system consists of three main components:

1.Smart contracts: Implement the cryptocurrency wallet smart contract using Solidity, adhering to the designed architecture and security requirements. Test the smart contract functionality using automated unit tests and integration tests.

2.User Interface Development: Develop user-friendly interfaces for interacting with the cryptocurrency wallet across web, mobile, and browser platforms. Implement features for account creation, transaction management, and authentication.

3.Deployment and Launch: Deploy the cryptocurrency wallet smart contract on the Ethereum blockchain, making it accessible to users. Launch the wallet application across web, mobile, and browser platforms, and promote it to the cryptocurrency community.

4.Enhanced Transparency: Blockchain technology enables enhanced transparency in the transaction by providing a secure, tamper-proof record of all transactions. This can help to reduce the risk of fraud and other malicious activities and increase trust among stakeholders.

5.Improved Efficiency: A transparent integrated transaction network using blockchain technology can help to streamline processes and reduce the need for intermediaries, which can lead to improved efficiency and lower costs.

6.User Privacy: The proposed system prioritizes user privacy by minimizing the collection and storage of personal data, implementing privacy-enhancing technologies, and adhering to strict privacy policies.

7.Reduced Costs: The use of blockchain technology can reduce costs by eliminating the need for intermediaries and streamlining processes. This can help to reduce the cost of goods and services and make them more affordable for consumers.

IV. PSEUDO CODE

Step 1: Import hardhat from console.sol.
Step 2: Create contract for transactions.
Step 3: Declare transactionCount as uint256.
Step 4: Create structure for transfer of address of sender, receiver, amount, message, timestamp, keyword.
Step 5: Create function addtoBlockChain to add transaction.
Step 6: Add a function getAllTransacations that returns all transaction
Step 7: End.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303028 |

V. SIMULATION RESULTS

The development journey begins with a comprehensive understanding of the requirements, where the fundamental functionalities of the crypto wallet are outlined. These functionalities encompass the creation of wallets, secure storage of cryptocurrencies, transaction management, and interaction with the Ethereum blockchain. Leveraging Solidity, a statically-typed programming language for writing smart contracts on the Ethereum platform, the project proceeds to implement these functionalities in a series of modular smart contracts. These contracts are meticulously tested to ensure reliability and security, utilizing tools like Truffle framework for automated testing.

Integration with MetaMask serves as the bridge between the blockchain and the user interface, enabling seamless interaction with the deployed smart contracts. By leveraging MetaMask's robust API, the frontend interface allows users to effortlessly manage their crypto assets while retaining control over their private keys. The result is a decentralized crypto wallet that empowers users with full sovereignty over their digital assets, while adhering to the principles of security, transparency, and user-friendliness. Through this project, we showcase the potential of combining Solidity smart contracts and MetaMask to revolutionize the landscape of decentralized finance, offering users a reliable and intuitive solution for managing their crypto portfolios.

Fig.1.Home Page of the wallet

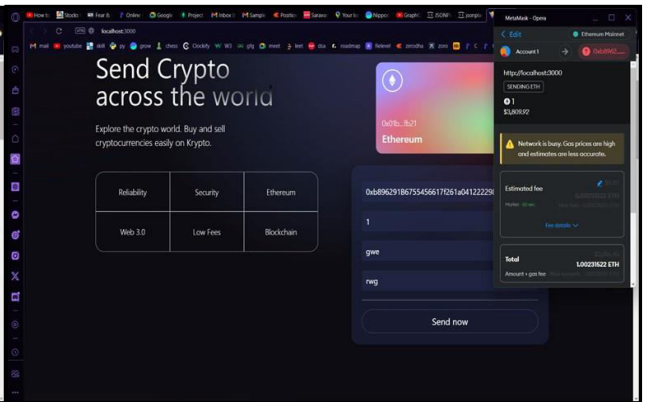

Fig. 2. Linking with MetaMask

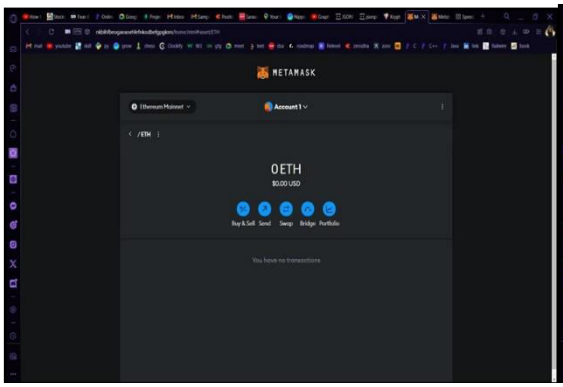

Fig. 3. Our account in MetaMask

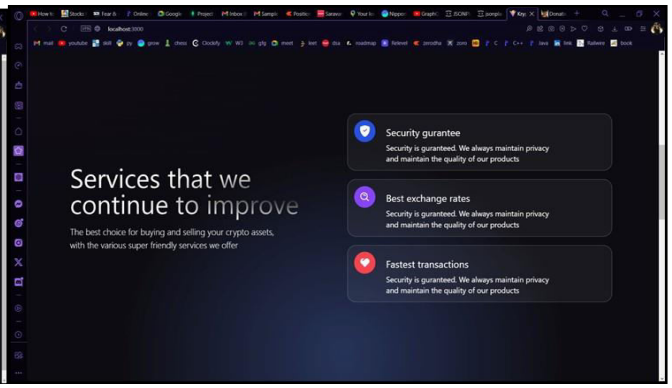

Fig 4. Services that we provide

VI. CONCLUSION AND FUTURE WORK

In conclusion, building a decentralized app using Ethereum blockchain for transaction has the potential to revolutionize the industry by providing a **transparent, secure,** and **efficient** platform for tracking goods and products as they move through the supply chain.stakeholders can gain access to **tamper-proof records** of each transaction, ensuring that every step of the process is verifiable, auditable, and secure. This can help **reduce the risk of fraud, counterfeiting, and other forms of malfeasance** that are common in traditional supply chains. Smart contracts, which are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303028 |

of code, can be used to automate and streamline transaction processes, reducing the time, cost, and complexity of managing the transaction.

REFERENCES

1. A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in Internet of Things: Challenges and Solutions," in Proceedings of the IEEE, vol. 107, no. 7, pp. 1291-1297, July 2019.
2. A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management," in Proceedings of the 2nd International Conference on Open and Big Data, Vienna, Austria, August 2016, pp. 25-30.
3. R. Zhang, L. Wen, and Y. Hu, "An IoT Electric Business System Based on Blockchain Technology," in Journal of Physics: Conference Series, vol. 1019, no. 1, p. 012063, 2018.
4. M. Li, X. Li, S. Chen, X. Liu, and Y. Cai, "A Blockchain-based Framework for Supply Chain Management," in Proceedings of the 2017 IEEE International Conference on Industrial Engineering and Engineering Management, Singapore, December 2017, pp. 174-178.
5. J. H. Park, J. Kim, Y. Lee, and H. Kim, "A Blockchain-Based Framework for Secure and Efficient Supply Chain Management," in Journal of Business Research, vol. 98, pp. 365-380, September 2019.
6. Y. Zheng, W. Sun, W. Yan, J. Li, and X. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in Proceedings of the 2018 IEEE International Congress on Big Data, San Francisco, CA, USA, June 2018, pp. 557-564.
7. M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain Technology: Beyond Bitcoin," in Applied Innovation, vol. 2, no. 6-10, pp. 71-81, December 2016.
8. A. M. A. Razak, R. Hassan, and N. A. Rahman, "Blockchain Technology in Supply Chain Management: A Review," in Proceedings of the 2nd International Conference on Intelligent Computing and Optimization, Pattaya, Thailand, February 2020, pp. 28-36.
9. Y. Zhao, J. Feng, J. Qian, and C. Chen, "A Blockchain-based System for Supply Chain Traceability and Quality Management," in Proceedings of the 2018 International Conference on Smart Computing and Electronic Enterprise, Shanghai, China, August 2018, pp. 245-252.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details