JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

BUILDING A DECENTRALIZED CRYPTO WALLET AND EXCHANGE PLATFORM ON ETHEREUM LEDGER

[1]Harshad Joshi, [2]Dinesh Pamu, [3]Tejas Kadam, [4]Tejas Birari, [5]Namdeo Kedare
[1]Student, [2] Student, [3] Student, [4] Student, [5]Professor
[1]Department of Information Technology,
[1]Dhole Patil College of Engineering, Pune, India

Abstract: This paper introduces a decentralized cryptocurrency wallet web application built on the Ethereum ledger. With the increasing significance of securely managing digital assets in the realm of cryptocurrencies, the application aims to offer users a reliable and user-friendly solution for organizing, storing, and transacting with various cryptocurrencies. By leveraging the decentralized nature of the Ethereum blockchain, users can maintain complete control over their private keys and digital assets, mitigating risks associated with centralized exchanges or custodial wallets. The web application encompasses key features such as account creation, key management, transaction processing, and integration with external services. Its intuitive interfaces, efficient transaction processing, and real-time updates ensure a seamless user experience, powered by Ethereum's robust infrastructure.

Keywords - Monitoring funds, Crypto Wallet, Blockchain, Trading funds, Ethereum, Private Key, Transactions, Smart Contracts

I. INTRODUCTION

Researchers and industrial interest in blockchain has recently increased. In 2008, Satoshi Nakamoto initially described the idea of a blockchain. The first industry to use blockchain was lash currency. Blockchain applications are currently being used in various industries with the implementation of smart contracts. Ethereum is now the blockchain system that is used the most. Ethereum DApps work in conjunction with smart contracts. The goal of Ethereum is to create a new protocol to build decentralised apps. It is alleged to have the benefit of rapid code manufacturing along with safety precautions.

Decentralized applications and smart contracts are rising the agenda as more businesses and developers strive to use the blockchain infrastructure to find new business models. The use of DApp generated a significant amount of data. Making an application based on the Blockchain platform has certain challenges as well. On the internet, a variety of development environment solutions are given individually.

We all understand that the current payment and money transfer systems are centralized because they involve third parties like banks and other governmental organizations like the Reserve Bank of India and Federal Deposit Insurance Corporation. However, they make use of their peer-to-peer networks to make their online payment technologies, such as Unified Payments Interface, Society for Worldwide Interbank Financial Telecom, etc. more frictionless for users. The primary concern is that a single point of failure in the databases of big financial institutions might cause enormous losses for the nation's financial resources. Blockchain is an infrastructure that is resistant to hackers and has no one point of failure since each node gets a copy of every transaction recorded in the ledger. Building a fund transfer system on top of this technology will yield the best outcomes. In bitcoin wallets, which might be hardware or software, you may maintain your digital currency. The address of the wallet you use to accept payments from others is the public key for these wallets, and the private key is the most important key that you should never share since it may be utilized for manipulating all the coins that are held in the wallet Since a transaction is always recorded on the ledger and cannot be modified after it has been completed, a transaction performed using a cryptocurrency wallet is more secure than one done using a conventional wallet.

II. LITERATURE REVIEW

The author of Cryptocurrency Wallet: A Review 2020 [4], is a continuously expanding list of records known as blocks that are connected by cryptography. Each block in the blockchain contains data, a hash, and the hash from the preceding block, increasing its security. By interacting with the blockchain to transfer, receive, and reconcile virtual currency/token balances, crypto wallets give users the chance to do this. The Ethereum ledger is offered as a tool for keeping wallet contracts in a highly effective manner by Monika di Angelo, Gernot Slazer's author of "Wallet Contracts on Ethereum, 2020" [1]. They suggested that a wallet be (partially) realized as a smart contract with features like daily limitations, permissions, multi-signatures, and recovery procedures in order to boost security and trust. The most well-known platform for tokens and smart contracts, also known as wallet contracts, is Ethereum.

The author discusses how traditional wallets differ from cryptocurrency wallets in terms of security and dependability in "Comparative Analysis of Cryptocurrency Wallets vs Traditional Wallets" [5]. This essay discusses the condition of digital wallets as they stand on the market today, better ways to buy and use them, digital wallet security, and potential future developments. The author of the paper "Building a Decentralised Application on the Ethereum blockchain" [7] described how programmers can begin building their first decentralised application using the Ethereum ledger using ganache and solidity with a potential tool combination needed to quickly develop applications with the Ethereum infrastructure.

III. RESEARCH METHODOLOGY

3.1 Decentralization

Decentralization is fundamentally about transferring control and decision-making from a single central authority or body to a network of people or organizations. Decentralization has become a crucial idea in the creation of many cutting-edge systems and applications in the world of technology. Decentralized systems are intended to function without the need for a central authority, such as a government or company, and rely on a network of computers and users to keep the system's integrity.

Increased security is one of the main advantages of decentralization. Decentralization can lessen the chance of a single point of failure or attack by doing away with the necessity for centralized authority. Decentralized systems can also offer more resilience against network disruptions since they can keep running even if a sizable piece of the network is down.

A small number of people or organizations frequently make decisions in a centralized system behind closed doors. Decisions are instead reached by a network of users through a process of consensus in a decentralized system. Greater transparency and accountability may result from this.

3.2 Decentralization in Crypto Wallet

The principle of decentralization in Bitcoin wallets has fundamentally altered how consumers controls their digital assets. Decentralized wallets give consumers direct control over their digital assets, in contrast to traditional financial institutions, which rely on middlemen like banks to keep and handle cash. By relying on a network of computers and users to preserve the integrity of the system, this direct control allows users to avoid many of the hazards connected with conventional financial institutions, such as hacking and theft. Enhanced security is one of the main advantages of a decentralized wallet. Users can avoid many of the hazards connected with conventional financial institutions by doing away with the requirement for a centralized intermediary. Users have total ownership over their digital assets in a decentralized wallet, and no third party is able to access their money without their consent. Users may feel more secure and at ease because of this.

3.3 Smart Contracts in Crypto Wallet

In order to offer consumers a variety of automated financial services, smart contracts, a crucial part of the decentralized finance (DeFi) ecosystem, are increasingly being deployed in cryptocurrency wallets. A self-executing program with the terms of the agreement encoded directly into the code is what makes up a smart contract. They can be used to automate a variety of transactions, from straightforward payments to intricate financial instruments, and are built to run without the assistance of intermediaries like banks or financial institutions.

The fact that smart contracts offer higher efficiency and security than conventional techniques is one of the main advantages of employing them in cryptocurrency wallets. Smart contracts allow for the automatic execution of transactions without the use of middlemen.

Decentralized applications (DApps) in cryptocurrency wallets can also be made using smart contracts. Peer-to-peer lending, decentralized exchanges, and other financial services can all be offered to users by these DApps. Without the use of middlemen, these services can be automatically and securely carried out utilizing smart contracts.

3.4 Proposed System

A distributed ledger would be used to store the cryptocurrencies, and transactions involving those currencies would take place on the ledger. This would make up the system architecture for a blockchain-based cryptocurrency wallet on the Ethereum ledger. The user would first establish a connection with the application through its meta mask wallet, and the authentication details could then be saved in a database. At that point, the user would be prepared to use the app's many functionalities, such as sending, receiving, and trading money. Each transaction would be handled by the Ethereum ledger's RPC network, and the database would be used to store the transaction data. The accompanying etherscan link for each transaction can be used to verify the legitimacy of each one. The most well-known platform for tokens and smart contracts, also known as wallet contracts, is Ethereum. The author discusses how traditional wallets differ from cryptocurrency wallets in terms of security and dependability in "Comparative Analysis of Cryptocurrency Wallets vs Traditional Wallets" [1]. This essay discusses the condition of digital wallets as they stand on the market today, better ways to buy and use them, digital wallet security, and potential future developments. The author of the paper "Building a Decentralised Application on the Ethereum blockchain" [2] described how programmers can begin building their first decentralised application using the Ethereum ledger using ganache and solidity with a potential tool combination needed to quickly develop applications with the Ethereum infrastructure.

3.5 Technology

1. Software Specification
    - Operating System: Windows 10(64-bit)
    - Programming Language: JavaScript, Solidity
    - UI/UX: Figma
    - Front-end: NEXT JS
    - Back-end: Node JS, Rapid API

- Database: MongoDB
- Ethereum- Test Network: Goerli Test Network
- Deployment: Netlify

2. Hardware Specification
   - Processor: Intel Core i3 or Higher
   - RAM: 4GB or above
   - Hard Drive: 100GB (min)

3.6 Working of Crypto Wallet

Here is a high-level, step-by-step explanation of how a common cryptocurrency wallet programme operates:

- **User registration:** The user starts by setting up an account on the application for their digital currency wallet. They generate a special username and password in addition to providing their basic information.
- **Wallet Creation:** After a user register successfully, a cryptographic wallet is created for them. A public key and a private key are the two cryptographic keys that make up this wallet.
- **Public Key Sharing:** The network receives the public key from the user's wallet application. The user's address for receiving cryptocurrency is represented by the public key.
- **Account Funding:** To begin utilising the wallet, the user must first fund their account by moving cryptocurrency from another wallet or an exchange. Initiating a transaction requires the user to supply the recipient's public key.
- **Transaction Verification:** A transaction is broadcast to the decentralised network of nodes or miners after it has been started. The network verifies the transaction to make sure it's legitimate and that the sender has enough money.
- **Cryptographic Signing:** The transaction is signed using the sender's private key after being verified. The transaction's integrity and authenticity are guaranteed by the cryptographic signature.
- **Transaction Broadcasting:** After the transaction has been signed, it is broadcast to the network and spread to other nodes. The transaction is included in the block that the miner is presently mining.
- **Block Mining:** For a new block to be added to the blockchain, miners must compete to solve a challenging mathematical challenge. Mining is the process of solving puzzles, and it needs a lot of processing power.
- **Block Validation:** A miner who has figured out the riddle broadcasts the fresh block to the network. The block is validated by other nodes, who check that the transactions included therein are legitimate and that the miner complied with the consensus guidelines.
- **Block Confirmation:** A block is deemed confirmed when it has been verified by the majority of the network. The block's transactions have now been added to the blockchain, and the user's wallet balance has been adjusted as a result.
- **Balance Update:** After receiving the confirmation of the transaction, the user's wallet application changes the user's balance. The successful transfer of funds is reflected in the updated balance.

3.7 Consensus Mechanism Used

A decision that is unanimously accepted by all members of a network is what is meant by the term consensus. For instance, there is no argument when a bunch of friends decide to play cricket. Here we are in a state of unanimity or mutual consent to play cricket together. "The major goal is to provide a collection of various nodes. However, a group of players will update in a secure manner while adhering to several defined norms. In the case of Blockchain, the impending change requires the support of at least 51% of nodes or network users. The network is updated with the new change if this occurs. Otherwise, he mutually agrees to reject the adjustment.

1. Proof of Work (PoW)

The Bitcoin and Ethereum networks both use the well-known PoW consensus mechanism. Here, by changing the block's nonce, miners (or block adders) have to carry out difficult mathematical operations to obtain the right hash. The miner who finds the hash below the necessary level of difficulty gets the opportunity to add his block to the network. So accepts the prize. It achieves a consensus in a puzzle-friendly manner using strong computation. Then, users of the already-existing network who performed authorized transactions in the block that the miner added. Blockchains that use the PoW algorithm include those for Bitcoin, Ethereum, Dogecoin, Litecoin, Zcash, and Horizon

2. Proof of Stack (PoS)

PoW's high energy need is eliminated by PoS consensus. In a proof-of-stake (PoS) network, validators (also known as miners) must stake some of their earned money in order to be selected for adding a block.
A network's first consensus algorithm is not it. It can only be used in a network after there are enough members (or nodes) for it to function.
Polkadot, EOSIO, Cardano, Ethereum 2.0, and numerous more blockchains use the PoS consensus algorithm.

3.8 Crypto Wallet Algorithm

Here is a high-level explanation of the algorithm that a crypto wallet follows to store, send, and receive cryptocurrency:

A. Key Generation: When you create a crypto wallet, you are given a one-of-a-kind private key. This private key is necessary for accessing and managing your cryptocurrency. In addition, your wallet generates a public key, which is used to receive cryptocurrency.
```
# Key Creation
generate_private_key () = private key
generate_public_key(private_key) = public key
```

B. Transaction Signing: When you want to send cryptocurrency, you use your private key to sign the transaction. This confirms that you are the owner of the funds and that you want to send them to another address.
```
#makefile
# Transaction Signing
signed_transaction = sign_transaction(private_key, transaction)
```

C. Broadcast to the Network: After the transaction is signed, it is broadcast to the network, where it is verified by other nodes on the network.
```
#python
# Broadcast to the Network
broadcast_transaction(signed_transaction)
```

D. Confirmation: Once the transaction is confirmed by other nodes, it is added to the blockchain, and the funds are transferred from your wallet to the recipient's wallet.
```
# Confirmation
if transaction_confirmed(signed_transaction):
update_balance(public_key, transaction)
```

This is a simplified explanation of the algorithm that a crypto wallet follows. In reality, crypto wallets use complex cryptography and blockchain technology to ensure the security and privacy of your cryptocurrency. The specific algorithm may vary depending on the type of cryptocurrency and the wallet you are using.

IV. MODELS

4.1 ER-Diagram

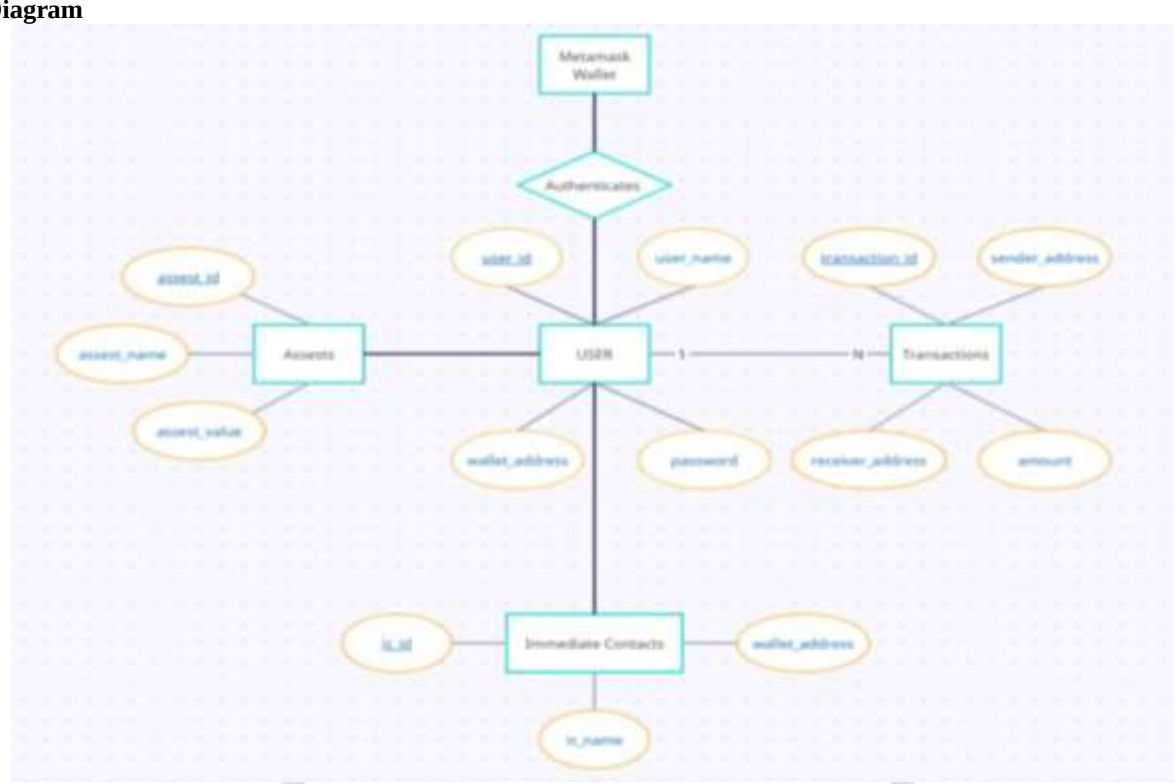

Fig 1. ER-Diagram of Crypto Wallet

4.2 UML-Diagram

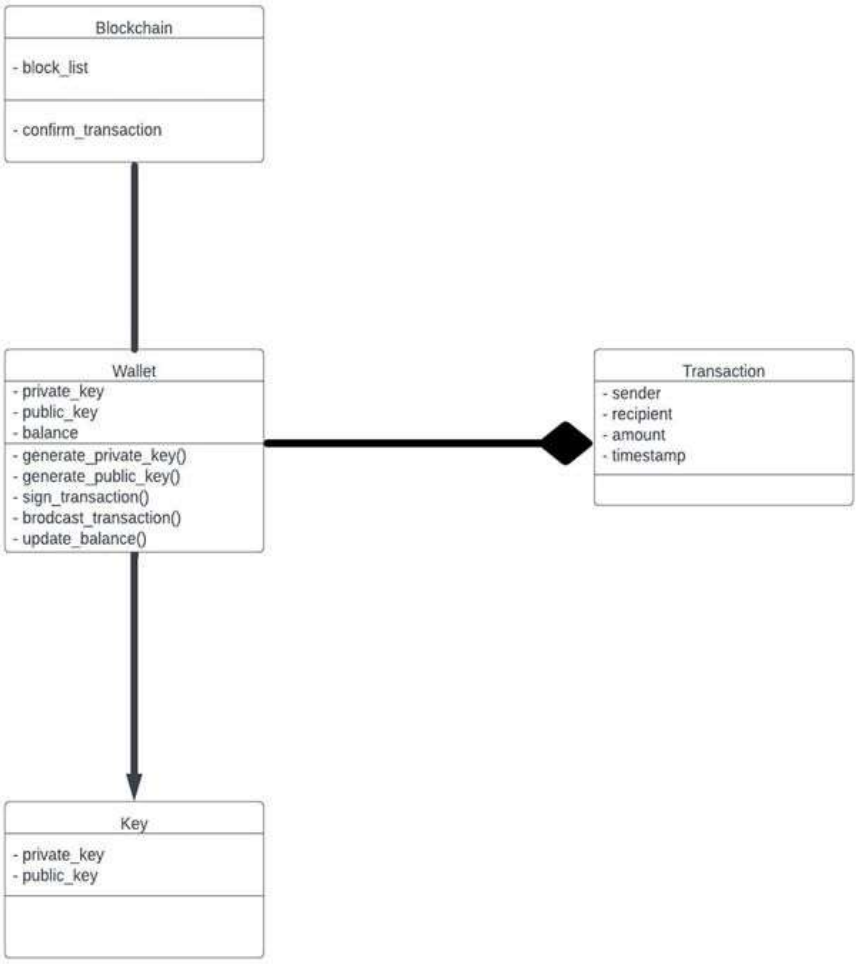

Fig 2. UML-Diagram of Crypto Wallet

V. RESULTS AND DISCUSSION

5.1 Results

According to the study, decentralised crypto wallets are more secure than their centralized equivalents. Decentralization lowers the possibility of hacking and unauthorized access by removing the reliance on a single entity or server. Decentralised cryptocurrency wallets have shown to be successful in protecting user privacy and upholding anonymity. The study's conclusions highlighted the value of user empowerment and control in decentralised cryptocurrency wallets. Users completely own and control their digital assets, doing away with the need for middlemen. By enabling users to access and manage numerous cryptocurrencies via a single interface, decentralised wallets increase interoperability.

5.2 Discussion

Decentralised crypto wallets have many benefits, but the investigation also revealed some drawbacks. Decentralised wallets can also be difficult for non-technical consumers to use; therefore usability and user-friendly interfaces need to be improved. Cryptocurrency wallets that operate decentralised from established regulatory structures are common. Smart contract-compatible decentralised wallets provide additional dangers. According to the report, smart contracts may have weaknesses due to coding mistakes or criminal intent that could cost customers money. Widespread acceptance and awareness-raising are essential for decentralised crypto wallets to fully realize their advantages.

VI. CONCLUSION

It may be inferred from extensive research that blockchain technology can offer a dependable and secure solution for the storage and transfer of digital assets. The problem of centralized systems and the security of digital data is addressed by the proposed development of a decentralised digital coin wallet application using Ethereum's distributed ledger. The programme represents a significant advancement in the realm of digital transactions since it can provide privacy protection and security while also removing the need for third-party involvement. The app's capabilities, such as the capacity to store, send, and receive digital currency, make it a useful addition to the ecosystem of blockchain technology.

REFERENCES

[1] Monika di Angelo, Gernot Slazer \Wallet Contracts on Ethereum, 2020
[2] Wood G. Ethereum: A secure decentralised generalized transaction ledger [J]. Ethereum project yellow paper, 2014
[3] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[R]. Manubot, 2019
[4] Saurabh Suratkar Mahesh Shirole Sunil Bhirud \ Cryptocurrency Wallet: A Review 2020
[5] Stevo Jokić , Aleksandar Sandro Cvetković , Saša Adamović , Nenad Ristić , Petar Spalević5 \ Comparative Analysis of Cryptocurrency Wallets vs Traditional Wallets 2019
[6] Vitalik Buterin "Ethereum White Paper" 2014 Ethereum Docs
[7] Ruhi Taş, Ömer Özgür Tanrıöver \ Building a Decentralized Application on the Ethereum Blockchain, 2020