Survey Paper on Decentralized Crypto Wallet Application using Ethereum Ledger

Dinesh Pamu[1], Harshad[2], Tejas Birari[3], Tejas Kadam[4], Namdeo Kedare[5]

[1] *Student, Information technology, Dhole Patil College of Engineering - Pune, Maharashtra, India*
[2] *Student, Information technology, Dhole Patil College of Engineering - Pune, Maharashtra, India*
[3] *Student, Information technology, Dhole Patil College of Engineering - Pune, Maharashtra, India*
[4] *Student, Information technology, Dhole Patil College of Engineering - Pune, Maharashtra, India*
[5] *Professor, Information technology, Dhole Patil College of Engineering - Pune, Maharashtra, India*

ABSTRACT

In today's era where the internet is at the fingertips of almost every person the digital data of the users are saved by big MNCs in their large data warehouses and we can't trust anyone who is using our data for what purpose and reason also we are not sure whether our data is secure or not, as the current system is centralized all the companies have access to our data and they can change it in the manner they want, despite this many times hackers attack their databases and breach the data, and the solution to this is blockchain technology. "Blockchain" refers to a growing collection of data known as blocks that are connected through encryption. Each node in the blockchain has three main things which are data, its own unique hash, and the hash of the previous node this design of node makes the blockchain database more secure and robust than other databases. A Crypto wallet is a software that contains private and public keys and uses blockchain to send and receive currency. Crypto wallet provides main features as (a) sending, receiving, monitoring & trading coins using a wallet. (b) Ensures the privacy of the user by using a hexadecimal address of the wallet. (c) No third-party involvement during transferring and receiving of funds as the entire system is decentralized. So our idea is to build a robust Digital coin wallet application that does not involve any third-party authorization and is completely decentralized also it is more secure as it works on the Ethereum Distributed ledger. It involves all the functionalities that a wallet contains like storing, transferring, and getting digital currency.

Keywords: - *Blockchain, Ethereum, Crypto Wallet, Transactions, Trading funds, Monitoring funds, Private key, Public Key*

1. INTRODUCTION

As we know the current payment or money transfer mechanisms whole over the world is centralized because third parties such as banks and other government institutions eg - RBI, FDIC are involved in this process of transferring and receiving funds yet they are using their peer-to-peer network to give a smoothless experience to the user via their online payment technologies such as UPI, SWIFT, IMPS, etc... But the main thing is that a single point of failure of the databases of these financial institutions can lead to heavy losses to the countries funds. Now Blockchain is a technology that is non-hackable and does not have a single point of failure because each node has saved a replica of all the transactions within the ledger and if we develop a fund transferring tool on top of this technology will give us the best results. Crypto wallets are software or hardware tools in which you can store your cryptocurrencies. These wallets contain a public and a private key where the public key is the wallet address that you will use to receive funds from others and the private key is the most important key which you should not share with others because all the coins stored inside the wallet can be manipulated using this key. A transaction through a crypto wallet is more secure than traditional wallets because whenever a transaction happens it is written on the ledger and can't be modified once done.

1.1 Comparing Hardware and Software Wallets

Parameter	Software wallet	Hardware wallet
Cost of purchasing	These wallets are free to use any user can download their app or can go to their website to create their crypto wallet.	These wallets costs up to 25 to 200 usd as they require an external tool.
Suitability	These wallets are frequently used for trading as they are convenient to use and they are go to wallets.	These wallets are suitable when you need to store your funds for long term in safe place
Max no. of assets they can store	These wallets can store many funds as one to ten thousands as of user requirements.	These wallets can store as many from thousand to ten thousands crypto coins.
Security	These are secure but not more than hardware wallets as they are live on internet so are vulnerable to some extent	They are highly secure but they need to be safely kept so they didn't get damaged or stolen
Data Recovery	These wallets are good in data recovery and most of them can be accessed through multiple devices.	These are not so great in data recovery if you have lost your wallet.
Ease of Transferring crypto currency	These wallets are already connected to internet so transferring crypto currencies and receiving them is easy and continent in these wallets.	These wallets need an extra step to connect them through Wi-Fi or USB internet to transfer funds.

2. LITERATURE REVIEW

The author of Cryptocurrency Wallet: A Review 2020 [3], states that the blockchain is an ever-growing list of records so-called blocks linked by cryptography. Each block in the blockchain has data, hash, and the previous hash which makes it more secure. Crypto wallets offer customers the opportunity to do this by sending, receiving, and reconciling virtual currencies/tokens balance through interaction with the blockchain. Monika di Angelo, Gernot Slazer author of "Wallet Contracts on Ethereum, 2020 [4], suggested how the Ethereum ledger helps in maintaining the wallet contracts in a highly efficient manner. They proposed that a wallet is (partially) realized as a smart contract aimed at increasing trust and security by being transparent and offering features such as daily limits, permissions, multi-signatures, and recovery mechanisms. Ethereum is the most famous platform for both tokens and smart contracts, i.e., wallet contracts. In "Comparative Analysis of Cryptocurrency Wallets vs Traditional Wallets" [1], the author explains how traditional wallets are different from crypto wallets in terms of safety and reliability. This paper describes the current state of digital wallets in the market, how to choose better solutions for purchasing and using digital wallets, digital wallet security, and future development trends. In "Building A Decentralized Application on the Ethereum blockchain" [2], paper the author specified how developers can get started with their

first decentralized application using the Ethereum ledger using ganache and solidity with a possible combination of tools required to easily develop applications with the Ethereum infrastructure.

3. PROPOSED SYSTEM ARCHITECTURE

The system architecture for a blockchain based crypto wallet on the Ethereum ledger would consist of a distributed ledger that would be used to store the cryptocurrencies and their transactions happened on the ledger. The user firstly would get connected with the application through its meta mask wallet and the authentication information can be stored in a database after which user is ready to use the different features of the application such as transferring, receiving, and trading their funds each transaction would be processed through the RPC network of the Ethereum ledger, and the transaction information would be stored in the database. The authenticity of each transaction can be checked with the corresponding etherscan link of the particular transaction.

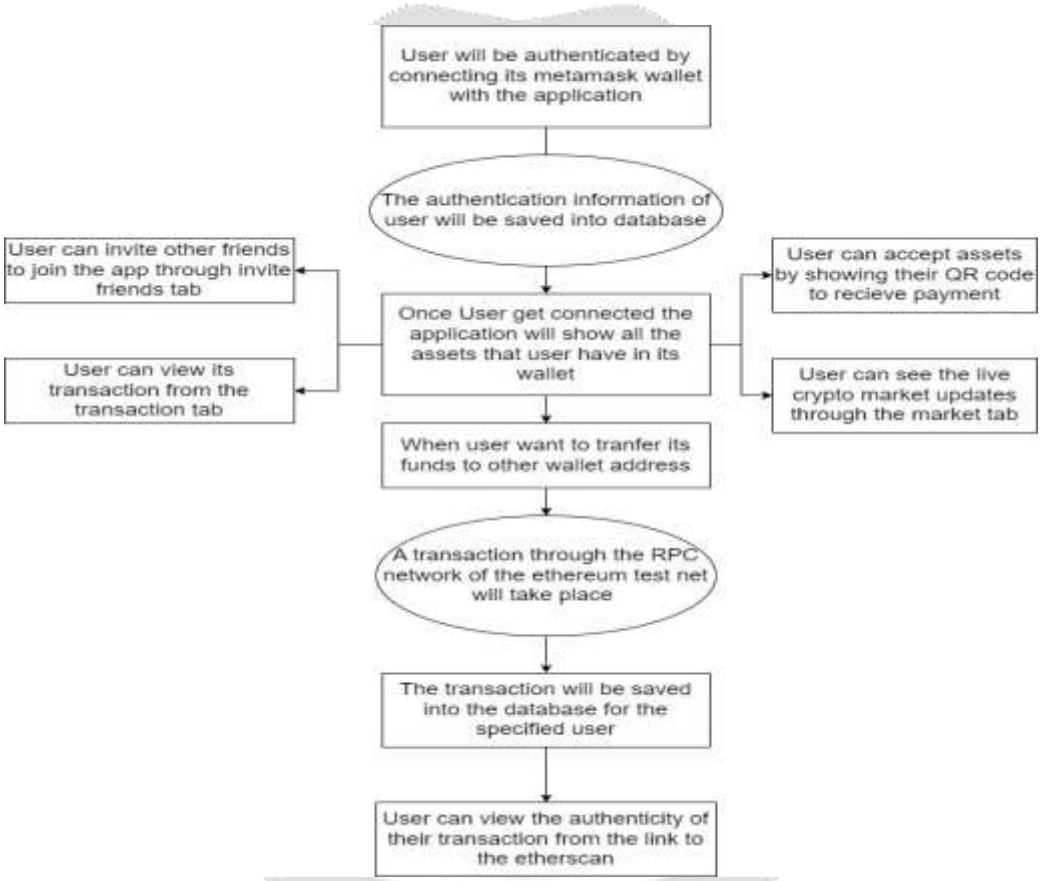

Figure 2: Blockchain-based Crypto wallet system architecture

Wallets also have inbuilt integrated QR codes and near-field scanner technology which permits the user to scan a code, select an amount, enter the user's key, select the transaction charges, and hit send.

Receiving is even simpler- the receiving user enters the sender's address and follows the same path. The sender accepts the payment, and the transaction is done.

4. CHALLENGES

It is also commonly known that bitcoin wallets have slow transaction speeds. The network is currently getting close to being oversaturated, which significantly slows down the transaction rate. Because there are currently no blocks larger than 1MB, transaction confirmation is quite unreliable. The development of a crypto wallet with a lightning-fast network, sidechain, and batch processing has drastically slowed down Oodles' ability to execute transactions. Security flaws and attacks frequently occur on cryptocurrency exchanges and wallets. The proper encryption and

decryption techniques can be used if you use white label crypto wallet creation. This might greatly lower the chance of hacking. Users also require private keys, which are 12-word mnemonic phrases, in order to access their wallets. Like other financial products, the price of cryptocurrencies is likewise influenced by supply and demand as well as perceived worth. Additionally, compared to other financial markets like stock exchanges, the rivalry and price differences are increased by the ever-growing quantity of cryptocurrencies and the lack of regulation. There is no way to keep an account open without being subject to potential losses in the future. Additionally, it makes sure that the wallet is completely compromised whenever the private key is lost.

5. CONCLUSION

With its recent improvements spurred not just by technological but also by social expectations, distributed ledger technology has the potential to revolutionize numerous industries. Decentralized applications can now be created thanks to blockchain technology, but the process is still difficult because there are so many brand-new, immature technological solutions that can be used to solve many DLT problems and provide new prospects for implementation. Since blockchain technology is still in its infancy, it is necessary to analyze recent developments in architecture, design, and implementation in order to increase understanding and facilitate the creation of new applications. Recently, Ethereum infrastructure has caught the attention of developers who are considering building applications on blockchain platforms in many industries. We have outlined the advantageous traits of DApps. Currently, research is being done to determine how the blockchain might be utilized to decentralize established systems like financial sector as well as to develop new decentralized applications. Future research will focus on addressing scalability issues and ensuring that the proposed application complies with generally accepted security standards for the cryptocurrency industry

6. REFERENCES

[1] Stevo Jokić , Aleksandar Sandro Cvetković , Saša Adamović , Nenad Ristić , Petar Spalević5 \ Comparative Analysis of Cryptocurrency Wallets vs Traditional Wallets 2019.

[2] Ruhi Taş, Ömer Özgür Tanrıöver \ Building A Decentralized Application on the Ethereum Blockchain, 2020

[3] Saurabh Suratkar Mahesh Shirole Sunil Bhirud \ Cryptocurrency Wallet: A Review 2020

[4] Monika di Angelo, Gernot Slazer \Wallet Contracts on Ethereum, 2020

[5] Vitalik Buterin “Ethereum White Paper” 2014 Ethereum Docs

[6] Wood G. Ethereum: A secure decentralised generalized transaction ledger[J]. Ethereum project yellow paper, 2014

[7] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[R]. Manubot, 2019.