Completely Secured Crypto Wallet with Blockchain Technologies

Abhishek Yadav[1], Shiv Pathak[2], Shailja Shakya[3], Arpita Pandey[4]
[1,2,3,4]AITM

Abstract: A big challenge in E-Transaction is to get the secured platform and an anonymous environment. If someone is having there on decentralized banking system then securing a private key from potential hacker is really a Big-Deal. No-One can rollback the transaction's done by the stolen keys, when the receiver acknowledges it. If somehow, we can manage the secured platform and anonymous environment then biggest climax is to get the taxation free and Untraceable transactions. So, for getting the technical solution of these incredible issues is the cryptocurrency wallet, hardware or a combination to manage the keys. by evaluating several wallets and transaction modules by different services there is the most common issue among them is lack of a secure and convenient backup and recovery process. To Overcome these issues, we have purposed one brand new cryptographical scheme to safely back up a hardware wallet relying on besides channel by human visual verification on the wallet. So not only the verification part but also, we have introduced a practical mechanism to protect the funds is splitting the money between two wallets with small and large transactions. Specifically, we have created a hierarchical wallet that we call deterministic sub-wallet to achieve this goal. Simply we have introduced a multi-layered architecture for cryptocurrency wallets based on a Secured-and-Safety strategy to protect private keys with a balance between convenience and security. The private keys can be protected by any of the users in three restricted layers with different protection mechanisms. That make the e-transactions end-to-end secured. Getting a Secured transaction from hackers is not really a big deal. But to get the transaction taxation free is the really the one. Several countries imposed taxation up to 30% to 40% taxation on crypto transaction's. So, for that we have also created a secondary scheme for that and that is called tokenized transactions. In a tokenized transaction, the asset owner would first create digital tokens representing the underlying asset and then offer them for sale on a blockchain-based platform. Investors can then purchase the tokens using cryptocurrency or other forms of payment. The ownership of the tokens represents ownership of the underlying asset, and the tokens can be can be freely traded on the market.

Keywords: Crypto Wallet, Block Chain Wallet, UPI Transactions, Tokenization, NFT Tokens, Personal Wallet.

I.INTRODUCTION

Blockchain, is the technology which can transform the foundation of all other crypto currencies, has been considered as innovative potentials can transform most industries. But it's unable to do so, main reason behind this is because several domains of blockchains are untouched.

A blockchain's peer-to-peer connection system provides verifiable ledger maintenance without a centralized authority. It considers not only a single point-of-failure but also a single point-of-trust. One of the main fields where the blockchain deals with is Crypto transactions or can be say that e-transactions. These types of transaction are not favourable by techies (technophiles), because it have some of the loop wholes in that and one of the most common loop whole is Security and to keep manage the public and private keys. If these things are manageable then the most common issues faced by the users or miners(mining) are high taxation on transaction by the government or by the service providing companies.

There are several types of Crypto Wallets present in the market some of them are Software wallets: These are wallets that can be downloaded and installed on a computer or mobile device. Examples include Exodus, Atomic Wallet, and Trust Wallet. Hardware wallets: These are physical devices that store your private keys and can be connected to a computer or mobile device when you need to send or receive cryptocurrency.[4] Examples include Ledger Nano S, Trezor, and KeepKey. Paper wallets: These are physical documents that contain your public and private keys, which you can print out and store securely. Examples include Bit Address and WalletGenerator. Web wallets: These are wallets that are accessed through a web browser and hosted by a third party. Examples include MyEtherWallet, MetaMask, and Coinbase Wallet. Mobile wallets: These are wallets

that are specifically designed to be used on a mobile device, allowing you to send and receive cryptocurrency on the go. Examples include Edge, Jaxx, and BRD. It's important to note that each type of wallet has its own pros and cons. But one of the most common issues which all kind of wallets are facing is security and taxation charged by authorities. So, By finding the solution of these things we have created a Smart, Safe and Taxation free Crypto Wallet.

II. LITERATURE REVIEW

Taxation on cryptocurrency varies depending on the country and jurisdiction in which an individual resides. Different countries have different approaches and regulations when it comes to taxing cryptocurrencies. It is essential to understand the specific tax laws and guidelines in one's own country. In general, cryptocurrency is treated as property for tax purposes, which means that the tax rules that apply to property transactions also apply to transactions involving cryptocurrency. For example, if we live in the United States, the Internal Revenue Service (IRS) considers cryptocurrency to be property, and therefore subject to capital gains tax. This means that if we buy cryptocurrency and later sell it for a profit, we will owe taxes on the difference between the purchase price and the sale price. In other countries, the tax treatment of cryptocurrency may be different. Some countries may treat cryptocurrency as a form of currency, while others may consider it to be a commodity or security.[6] The Indian government has clearly formulated a clear regulatory framework for the 30% of taxation in cryptocurrency, although it has signalled its intention to be incremented in future. The Reserve Bank of India (RBI) has prohibited banks from dealing with or providing services to any individual or business dealing in cryptocurrencies. The positive domain is that Indian government has not yet explicitly banned cryptocurrency trading, buying or selling. But the percentage of imposing on taxation duties is really a big deal. In the absence of clear regulatory guidance, it is likely that the tax treatment of cryptocurrency transactions in India will follow the general principles of taxation on property transactions. [8] This means that cryptocurrency will be treated as a capital asset, and any gains or losses from cryptocurrency transactions will be subject to capital gains tax.

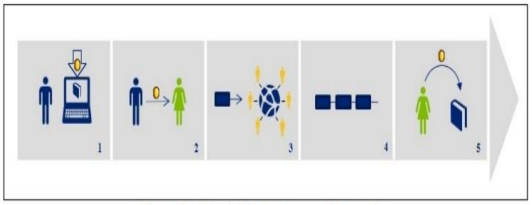
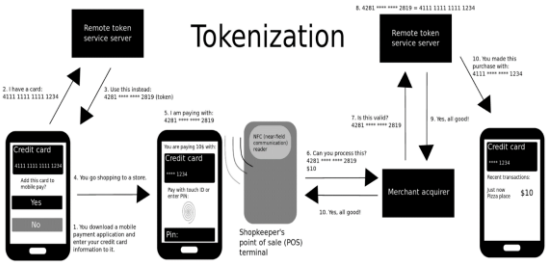


Figure 1. A Basic Cryptocurrency Transaction

III. MOTIVATION

Increasing of hacking culture in the current market and the of taxation on the crypto assets and on crypto transactions is the greatest motivation for creating these types of wallets. The Indian government has clearly formulated a clear regulatory framework for the 30% of taxation in cryptocurrencies although it has signalled its intention to be incremented in future. So the main perspective is to overcome the taxation plus to get the fully secured environment.

IV. PROPOSED SYSTEM

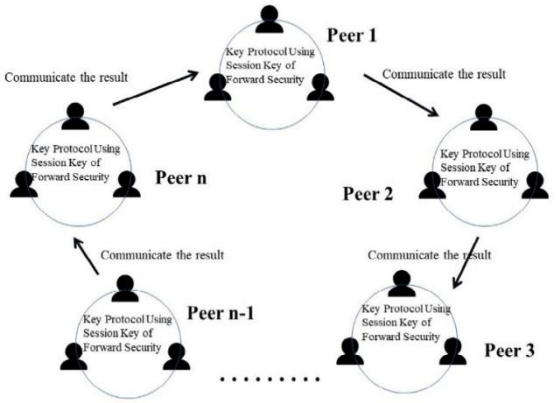


So, getting off from the taxation prices on cryptocurrencies we founded a great solution and we called it Token – Transactions. Specifically in which we are just creating transferring the the amount in the form of Token's. So in more clear manner we are occupying that much amount tokens which we want to transfer from one user to another.

Tokenization:

Tokenization is the process of breaking down a text document into smaller units called tokens. In natural language processing (NLP), tokenization is a crucial step in the pre-processing stage of text analysis. Tokenization involves splitting the text into individual words, phrases, or symbols, depending on the level of granularity required for the specific NLP task. For example, in a basic word-level tokenization, the sentence "The quick brown fox jumped over the lazy dog" would be tokenized into individual words as follows: ["The", "quick", "brown", "fox", "jumped", "over", "the", "lazy", "dog"]

Tokenization can also involve splitting the text into larger chunks, such as phrases or sentences. This is often useful in tasks such as sentiment analysis or machine translation. Tokenization can be performed using various techniques such as whitespace tokenization, punctuation-based tokenization, and regular expression-based tokenization. The selection of a tokenization technique relies on the particular demands of the NLP task at hand and the attributes of the text being analysed. We can also se how the tokenization works. Block Diagram Clearly shows about how it works.



V. STEPS AND OBSERVATION

Managing security in crypto wallets is essential to keep your cryptocurrencies safe from unauthorized access, theft, or loss. Here are some best practices to consider it is. Hardware wallets provide a secure method for storing cryptocurrencies by keeping private keys offline. This feature makes them less susceptible to hacking attempts, making hardware wallets one of the most secure options available for cryptocurrency storage. Choose a strong password: Use a strong and unique password for your wallet, preferably a combination of upper- and lower-case letters, numbers, and special characters.

To enhance the security of your wallet, it is recommended to avoid using common words or easily guessable passwords. Additionally, enabling two-factor authentication (2FA) can provide an extra layer of protection. By implementing 2FA, you add an additional step to the login process, typically involving a unique code sent to your mobile device or generated by an authentication app. This authentication method adds an extra layer of security by requiring both something you know (your password) and something you have (your mobile device or authentication app) to access your wallet. Keep your private keys secure: Your private keys are what allow you to access and manage your cryptocurrencies.

Never share your private keys with anyone and store them in a secure place. Keep your software up to date: Make sure to update your wallet software regularly to protect against vulnerabilities and bugs. Be cautious of phishing scams: Always verify the authenticity of any messages or emails you receive related to your wallet. Scammers may attempt to trick you into giving them your private keys or login credentials. Use reputable wallets: Stick to well-known and reputable wallets to minimize the risk of fraud or security breaches. [13]

By following these best practices, you can help to ensure the security of your crypto wallet and the cryptocurrencies stored within it. [14] This key protocol is a protocol to protect a cryptocurrency wallet key. The overall protocol mechanism is shown in Fig. 3. A peer typically consists of multiple parties, where each party comprises a minimum of three individuals. Within this framework, each peer is required to execute the key protocol utilizing a session key that is established to ensure forward security for authorized users. The protocol includes a session key protocol test, which verifies the effectiveness and reliability of the session key protocol.

In Fig. 3, Peer 1 proceeds with the key protocol with the session key of the forward security and Peer 2 proceeds with the key protocol with the session key of the forward security. The communication process involves Peer 1 interacting with the protocol, which is linked to Peer 2. Then, Peer 2 engages with the protocol, which is sequentially connected to Peer 3, and so on for Peer n. Throughout this process, the protocol automatically terminates if an unauthorized user is detected. This ensures that only legitimate individuals capable of conducting cryptocurrency transactions can participate. To ensure fault tolerance, the peer engages with multiple parties using the Federated Byzantine Agreement (FBA) mechanism. This approach helps mitigate potential faults or failures within the network Fig. 2. The proposed key protocol mechanism.[15]

VI. CONCLUSION

The following paper presents a new type of blockchain key that is designed to withstand Byzantine faults,

making it suitable for use in asynchronous systems like the internet. Many cryptocurrency hacking incidents occur when a wallet's information is stolen, as the key that provides access to the account is stored in the wallet.

To prevent this theft, the paper proposes a key protocol that uses session key agreement instead of key storage in a wallet. This multilateral protocol utilizes session key authentication and cluster key in a peer, which work together to perform multiparty computations using FBA based on blockchain technology. The key protocol ensures that the blockchain remains secure by preventing collusion between miners and data receivers.

It also protects users' privacy through key agreement and does not violate forward security. This proposal could help address concerns about cryptocurrency security and enable a robust cryptocurrency market without the need for decentralized exchange. The key protocol could be applied to other areas that require secure distributed networks, making it scalable. Not only regarding security purpose but also it helps us to manage then taxation prices are imposed by authorities. By the help of tokenization wallet we can easily by pass 30% taxation on crypto currencies. One-on-One or Peer-to-Peer transaction gives us end to end encryption and it will help all the community to get the speedy transaction recovery. And go free on crypto currencies transactions. For our proposed mechanisms, we implemented a prototype as a proof-of-concept on a smart card, which is a secure but resource constraint option to build a hardware wallet. We also provided performance evaluation and security analysis for these mechanisms.

VII.ACKNOWLEDGMENT

We would like to thank the Department of Computer Science and Engineering for providing the right environment to learn and guidance with continuous support for project and research work.