ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 10, Dec 2022

A SURVEY OF CRYPTOWALLETS AND THEIR SECURITY MECHANISMS

Arti Bansode and Minal Sarode
SIES (Nerul) College of Arts, Science and Commerce, Maharashtra, India
[1]artibansode@gmail.com and [2]minals@sies.edu.in

ABSTRACT
A cryptocurrency wallet is simply a wallet for holding cryptocurrency. It can be a device, medium, system or service. In addition to storing the keys, the crypto currency wallet often also provides encryption and / or data signing functionality. Cryptocurrency wallet is an app that allows cryptocurrencies users to store digital assets. It keeps track of the encryption keys used for digitally signing transactions and to store addresses on a blockchain where the specific assets resides. It is very important to secure keys in cryptocurrencies, as they are the only way to prove ownership of digital assets. In this paper, the authentication mechanisms used in the different cryptocurrency wallets are discussed. The findings indicate hardware wallets are most secure cryptowallets. Also, software wallets implementing security mechanism like U2F, passphrase, encryption along with AML compliance and conducting security audits are secure. Software wallets are used with hardware wallets for storing cryptocurrency.

Keywords: *Cryptocurrency wallets, multi-sig, U2F, 2FA, Hardware wallet, Cold storage*

I. INTRODUCTION
The investment in Cryptocurrency has seen a significant increase in the past few years. The popularity of cryptocurrency is the simplicity and security associated with it. Satoshi Nakomoto introduced the first ever cryptocurrency named Bitcoin in the year 2008(Nakomoto, 2008). Along with the currency, a piece of software implementing Bitcoin was introduced. It was also the first cryptocurrency wallet. The basic functionality of a wallet remains the same, however with the popularity of cryptocurrency new functionalities like multi-currency support, trading, etc have been added (Karantias, 2020). A cryptocurrency wallet is an application or a service that allows cryptocurrency users to store and retrieve their digital assets which can be run on a smartphone or a computer. A user can use the wallet to spend, receive, and trade cryptocurrencies. A wallet that is downloaded and stored on a pendrive is called a cold wallet. Cryptowallets may support single or multiple cryptocurrencies. A wallet is secured by a password. A cryptowallet can be viewed or accessed using smartphones and computers. Cryptocurrency wallets store public and private keys of a user. A public key is a segment of digital code that uniquely identifies a user account and used as an address for transferring funds. One user can have multiple wallets. Every

wallet has a Public Key and Private Key. Private keys are pieces of digital code unique to an individual's cryptocurrency wallet. Private keys are used to designate ownership of public keys. All crypto-transactions are signed using the private keys of the owner. Cryptocurrency wallets can be used by businesses for accepting payments similar to e-wallets. They can also be used to securely store or exchange blockchain assets.

TYPES OF BITCOIN WALLETS

A. Hardware Wallet
A hardware wallet is a physical device, like a pendrive, that stores the private keys to your crypto offline. Hardware wallets are devices which are used to store cryptocurrency. They are usually cold storage and are connected to the network only while performing a transaction or for updating the wallet. Hardware wallets are aimed at protecting your private keys from being accessed by a hacker. The two most well-known brands are Ledger and Trezor.

B. Software Wallet
Software-based wallets are easy to use and user friendly. They are downloaded on the desktop. They are used for carrying out transactions as well as storing cryptocurrency. They need to be secured because the device is connected to the Internet and are prone to cyber attacks.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 10, Dec 2022

C. Mobile Phone Wallet

These wallets are downloaded and mounted on smartphones. These wallets are used to access cryptocurrency for carrying out day to day transactions like paying by scanning a QR code. These wallets need to be secured because they are constanty connected to the Internet and are more vulnerable to hacking.

D. Web Wallet

Web Wallets are online wallets that can be accessed via an internet browser. It is recommended no to store your bitcoins in these wallets. They are extremely vulnerable to cyber-attacks.

E. Paper Wallets

Paper wallets are wallets placed on printed sheets of paper. The transaction si carried out by scanning the QR code on the paper or inserting the private key.

Classification of wallets

Wallets can be further classified as Hosted or Non-custodial wallets based on the management aspects related to the wallet

Hosted wallets

A hosted wallet is a wallet where a third party is responsible for securing the wallet. It is similar to storing currency in a bank. The advantage of using a hosted wallet is that it can be recovered, if you forget your password. Hosted wallets allow a user only to buy, sell, send, and receive crypto.

Non-custodial Wallets

Non-custodial wallets don't rely on a third party for securing the cryptowallet. They only provide the software necessary to store your crypto. The user is responsible for securing the wallet. The advantage of a non-custodial wallet is that the user is in full control of the security of the wallet and can perform more advanced crypto activities.

II. LITERATURE REVIEW

The transactions carried out using cryptocurrency are similar to fiat currency however there is no way to recover the funds if your wallet gets hacked. Hence, protecting the Cryptocurrency wallets using various authentication techniques is the only way to secure your wallet.

Security Mechanisms used in Cryptowallets

1. Two-Factor Authentication(2FA)

The most common technique used to secure a wallet is a Two-Factor Authentication. Two-Factor authentication is a very simple and effective

technique for authentication. It is an additional layer of security, which requires one more step of verification to authenticate the user/transaction. Two-factor authentication is using a unique code called as the One Time Password (OTP) along with your password to login into your account. (Aloul, et al, 2009) have proved the efficiency of two-factor authentication using mobile phones.

There are two most popular techniques of implementing 2FA:

- Using mobile/email OTP
- Using Google Authenticator
- Using mobile/email OTP

A string of numbers called as the One Time Password is sent to the user's registered mobile phone and email for logging into an account.

This OTP is valid for a limited span of time usually 30 to 60 seconds. The OTP along with the username and password are used to log into the account.

Using Google Authenticator

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 10, Dec 2022

1. Download the Google Authenticator app.
2. Log into a Gmail account that can be used to set up two-step authentication. When logged in to your Google account, enable Google's two-step authentication.
3. Enabling two-step will bring up a QR code to scan.
4. Scan the QR code in the Authenticator application.
5. The authenticator application will generate an authentication token for your google account. The token will be a string of six numbers that changes every 15 seconds.
6. The token, along with your username and password, is used to log into accounts on which you've set up two-factor.

Two factor authentication is secure because the token is account-specific, constantly randomly generated, and in most cases only stored on the device you put the two-factor app on.

2. Universal 2nd Factor (U2F)

Universal 2nd Factor (U2F) is an open standard for strengthening two-factor authentication. It involves the use of a physical key to reinforce 2FA. U2F is an authentication standard that uses one key for multiple services. It simplifies and elevates the security provided in 2FA by adding a strong second factor to user login. U2F uses a physical key that is inserted in the USB port(YUBIKEY) or held in close proximity(NFC) to the device where authentication is to be performed.

The user logs in with the login credentials. The user presents the second factor by simply pressing a button on a USB device or tapping over NFC during registration and authentication. "The user can use their U2F device across all online services that support the protocol leveraging builtin support in web browsers." (Sampath,2014)

3. KYC

Know Your Customer (KYC) or Know Your Client, is a process used by businesses or agencies to verify the identity of its clients. KYC is a process that allows companies to authenticate their clients, find out whether the customer is eligible for their services and also to avoid any criminal activity. The objective of KYC process is to prevent illicit activities by verifiying the background of the clients. Most crypto exchanges don't require KYC while the fiat-to-crypto exchanges will require to go through KYC process.

4. Hot vs. Cold Wallets

Hot wallets are cryptowallets connected to the Internet. They can reside on your mobile phone or desktop in the form of an application or as a service on the web. Cold wallets are offline. They are not connected to the Internet. They use a physical medium to store keys offline thereby, protecting them from online hacking. They are also referred to as cold storage. Many Cryptocurrency wallets keep coins in cold storage and thereby protect the users' funds. Cold wallet also referred to as Offline wallet provides protection against computer vulnerabilities.

5. Encrypting the Wallets

Cryptowallets are encrypted by using passwords. This adds an additional layer of security to the wallet. The robustness of this system is based on the strength of the password. It is also essential to encrypt backup that is exposed to the network.

6. Multi-signature

Multisignature wallets are cryptocurrency wallets which use multiple private keys for transactions. A Multi-signature (wiki, 2019) user has multiple private keys which can be used to sign a transaction. The user can protect their funds even if they lose one (or more) of their keys. It allows a transaction to require multiple independent approvals to be spent. This feature can be used by organizations to give its member access to its funds and allowing withdrawal only if more than one member signed the transactions. Multi-sig wallets prevent a single point of failure and improve the resilience against the loss of funds on the loss of private keys.

7. Anti-Money Laundering (AML) Compliance Process

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 10, Dec 2022

"Banks and money services businesses (MSBs) would be required to submit reports, maintain

records, and verify the identity of customers in connection with transactions above certain thresholds involving CVC/LTDA wallets not hosted by a financial institution (also known as "un-hosted wallets") or CVC/LTDA wallets hosted by a financial institution in certain jurisdictions identified by FinCEN," according to a Notice of Proposed Rulemaking (NPRM). Financial Crimes Enforcement Network is referred to as FinCEN. (sanctionscanner, 2021)

Cryptocurrency wallets faced many money laundering and terror financing threats. To overcome this AML regulators publish AML recommendations and obligations for securing wallets against money laundering threats. AMLM is a set of procedures and legal regulations to prevent profit from illegal activities. To prevent the global spread of this attack, regulatory bodies enforce due diligence on their customers.

8. Seed or Passphrase

The user is asked to enter a 24-word seed phrase during setup. This phrase becomes the private key for the wallet. BIP-39 is the most common standard used for passphrases in a cryptowallet.

Jan Lansky et al. (2018) in their paper “Possible state approaches to cryptocurrencies” had explained how the risk to the Cryptocurrency can be prevented by using different methods. Many risks can be prevented by information between crypto currency users and by using AML and KYC policies. The inability of public authorities to withdraw funds from a crypto currency account, in the consolidation and non-reversal of transactions made, can be seen as very serious risks. The co-operation of the evildoer. Many provinces do not pay much attention to the opportunities offered by cryptocurrensets.

Aleksander Berentsen and Fabian Schär et al (2018) - Bit coin is a unit of virtual currency and therefore has no physical representation. Bit coin the unit is split and can be divided into millions of “Satoshis,” the smallest part of Bit coin. The Block chain is a data file that holds records of all past Bit coin transactions, including the creation of new Bit coin units. It is often referred to as the Bit coin system logger.

Teng Hu et al. (2020) had described in their paper "Securing the Private Key in Your Blockchain Wallet: A Continuous Authentication Approach Based on Behavioral Biometric" how blockchain is providing more security for trading of cryptocurrencies. The block chain wallet is a program for users to manage and store their private keys. In addition, the secret key is the unique user credit for crypto currency in the block chain. But of now, block chain wallets only use passwords to

authorize users, making potential risk to privacy security to reduce this risk.

The authentication procedure is a crucial step that should be utilised to check that the user is a legitimate one and grant access to him exclusively, according to Eman T. Alharbi, Daniyal Alghazzawi, et al. (2019). Two-factor authentication (2FA) systems have recently been used. 2FA can be used in a variety of contexts to increase login security and eliminate the risk associated with utilising a single validation item. One of the most popular 2FA techniques is OTP- SMS. However, the attackers have discovered a technique to exploit this channel and access the user account without the user's knowledge or permission.

Sharma, Avin Mohitesh in his study "Cryptocurrency and Financial Risks." (2021) explained different money laundering risk to Cryptocurrency. He also explained how different approaches are used to avoid this type of threats.

Pavel, Datinský in their study "European Legal Regulation of Cryptocurrencies through the AML Scope." (2020) had explained how AML regulators had published AML recommendations and obligations to be used by different cryptocurrencies to have a secure transactions.

III. METHODOLOGY

Various online articles listing top cryptowallets were reviewed. The findings are based on the most popular wallets. The website for each wallet and various articles listed the security features implemented by the wallet. Various factors decide the security of the wallet like the type of wallet, security implementations, costs, and customer reviews.

IV. RESULTS AND DISCUSSIONS:

This paper lists down a few cryptowallets and the various security mechansims used by them.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 10, Dec 2022

1) Trezor

Trezor is hardware cold storage wallet. Currently. Trezor One and Trezor Model T are the most popular devices. Trezor is completely secure because it has various security features like PIN Entry, Passphrase entry and Device recovery. It uses a U2F authentication. Trezor also implements various security measures like Firmware verification wherein the bootloader always verifies the firmware signature. If the signature is correct, the firmware is executed, else a warning is shown. While updating the firmware, if the firmware signature is invalid, the bootloader erases the device memory. It also erases the memory if the firmware is downgrade to a vulnerable version. The bootloader is write protected

and the JTAG is disabled, so an attacker cannot replace it.All operations involving private and public keys are only allowed after user authentication via PIN. Trezor uses a BIP39 Passphrase which is never stored on the device. The Trezor hardware case is ultrasonically welded, making it difficult to be restored after breakage. It also support reliable backup & recovery of the wallet by inserting the recovery seed.

2) Ledger

Ledger is considered to be a pioneer in Hardware Cryptowallets. The second-generation cold storage wallet from Ledger is called the Nano X. More than 1,800 different currencies and tokens are supported by the integrated Ledger Live platform. The wallet has Bluetooth connectivity for pairing with Android and iOS mobile devices as well as a USB connector for a PC. The device features a small LED screen.

The device prompts for a 24-word seed phrase while set up. This seed is the wallet's private key. Ledger wallets use their proprietary operating system called BOLOS. It uses Bluetooth Low Energy (BLE) connectivity for wireless connections with Android or iOS devices. The security of wireless transaction is ensured by transporting only public data. Critical data like the private keys are never transmitted over Bluetooth. The Ledger Live application on a smartphone or computer is used to prepare the transaction, which is then transferred through Bluetooth or a wired USB connection. Another additional layer of security is provided by implementing Secure Element(SE) which requests user consent for any action. Also, data is encrypted using AES-based encryption. Ledger NANO also supports the capability to disable Bluetooth and use only wired USB connection. The Ledger security team performs security audit of the BLE stack to check for security vulnerabilities.

3) Exodus

Exodus is a decentralized wallet. It comes in two forms: desktop and mobile wallet. It has a very simple user interface and a built-in exchange. Exodus is the most popular desktop wallet because of its ease of use. It is however as much secure as the PC it is being accessed on. Exodus is a closed source wallet, its code is not open for everyone to see.

Exodus implements two levels of security. It requires a user-created password to access the wallet. Second, it requires you to generate a 12-word seed phrase that helps in wallet recovery.

It does not have any protection against hackers. Also, It does not have 2FA. It is usually used with a hardware wallet like trezor to keep it safe.

4) Mycelium

Mycelium is an open-source and mobile-only Bitcoin wallet. Mycelium currently only supports Bitcoin, ETH, and ERC-20 tokens. Mycelium supports hardware wallets, which allows users to hold their Bitcoin in an offline storage device. Mycelium app is reproducible. It does not need ID proof and does not collect any user information. It supports hardware wallets like Trezor, Ledger, etc. It also supports paperwallets and watch-only accounts. Mycelium has a separate backup system for Single Address accounts. It also has several levels of pin protection for making secure transactions. It has variable keyboard layouts that prevent pattern sniffing. It uses the TOR network support to mask IP address and location. It allows all third-party services to be manually turned off.

5) COINBASE

The cryptocurrency exchange site Coinbase is very well-known. 98% of the funds that customers deposit with coinbase are kept offline. The cryptoassets are geographically dispersed in safe deposit boxes and vaults all around the world. The data is replicated to FIPS-140 USB devices and paper backups after being

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 10, Dec 2022

redundantly split, AES-256 encrypted, and copied. Geographically dispersed drives and paper backups are stored in vaults and safe deposit boxes all around the world. On all accounts, Coinbase uses two-step verification. The entire website traffic is encrypted using SSL (https). Private keys are kept in wallets using AES-256 encryption. Employees at Coinbase are subject to a criminal background check. Each device and service has its own unique password and two-step verification is used. Employees must use secure passwords, encrypt their hard drives, and enable screen locking.

Coinbase uses a variety of security measures to keep user wallets safe.

- SQL injection filters to formally validate POST, PUT, and DELETE requests in order to thwart CSRF attacks.
- Place restrictions on a range of website actions.
- Whitelist properties on all models to avoid risks related to mass assignment.
- Passwords stored in the database using hashes.
- Promote the use of strong passwords when opening new accounts and changing existing ones.
- The database and code base are kept separate from the application credentials.
- In Coinbase's "Bug Bounty Program," those who disclose problems in the company's software are given rewards.

Any in-scope report that indicates a software vulnerability that negatively impacts Coinbase or Coinbase users qualifies as a legitimate report.

6) COINDCX

DCX is a Singapore-based company that specializes in crypto-enabled financial services. COINDCX wallet was launched on April 8th, 2018. It is a hosted wallet. COINDCX ensures Funds Security by storing 95% of all funds in multi-sig cold wallets and only 5% is stored in hot wallets. CoinDCX uses geographically distributed industry-best hardware security modules (HSMs). No single person has access to multiple wallets at the same time, nor can just a single person remove funds from any wallet. COINDCX used 2FA for transactions. All cryptocurrency withdrawals are first verified through multiple confirmations from the user before they are processed. All information like the user passwords, personal data, and other sensitive information are encrypted while in storage as well as in transit .COINDCX performs regular security audits to mitigate attack vectors. Being a hosted wallet, all information on the website is transmitted over encrypted Transport Layer Security (TLS) connections (i.e., HTTPS). It is also immune to DDOS attacks.

7) WazirX

WazirX is a trading platform launched in India in March 2018. This platform needs a KYC process. This wallet can work on different platforms like Android, iOS mobile, Windows, and Mac. WazirX P2P has overcome the drawback of depositing and withdrawing fiat. Security features of WazirX:

- Funds in cold storage
- Multi-signature wallet system
- Fund withdrawal require two-factor authentication
- Regular security audits
- Strong KYC/AML guidelines

8) ZEBPAY

Zebpay is a trusted and secure crypto exchange with the wallet that serves customers across the globe. It is available on Web, Android and iOS for trading bitcoin, ether, ripple, and various other popular

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 10, Dec 2022

cryptocurrencies. 98% of the cryptocurrency held by ZebPay is kept in cold wallets signed with HSM on air-gapped devices spread across many cities and nations.

ZebPay's unique Omnitrixx security architecture and protocol enable a top-tier multi-chain security system that safeguards all transactions across cold and hot storage wallets.

Transactions utilising the ZebPay wallet are signed by means of various cloud-based platforms. The Zebpay Servers are protected by robust firewalls. Workers of ZebPay go through background checks and are given bucketed network access based on their employment, much like Coinbase employees do.

Security professionals frequently evaluate Zebpay's platform and products. It runs a Bug Bounty Program to entice and compensate security experts for evaluating its security. ZebPay has received the ISMS - Information Security Management System - ISO 27001:2013 accreditation.

V. CONCLUSION

This study describes the different types of cryptowallets and the various security mechanisms implemented by them. The cryptowallets come in many form and this study looks at seven different implementations of cryptowallets and the security measures implemented by them. After conducting this study, I conclude that hardware wallets are the most secure wallets because they are stored offline. The trend is to use desktop, mobile or any online trading wallet for transaction and storing the currency in hardware wallets. 2FA is the most widely used authentication mechanism used in cryptowallets. Some cryptowallets store most of the sensitive data in offline servers. The wallets also insist on KYC/AML as per government norms. This is not an exhaustive study of cryptowallets. There are many wallets available. However, this study looks at some of the major types of wallets that are being used popularly.

VI. REFERENCES

1. Nakamoto, Satoshi. "Bitcoin whitepaper." URL: https://bitcoin. org/bitcoin. pdf-(: 17.07. 2019) (2008).
2. Lansky, Jan. "Possible state approaches to cryptocurrencies." Journal of Systems Integration 9.1 (2018): 19-31.
3. Berentsen, Aleksander, and Fabian Schar. "A short introduction to the world of cryptocurrencies." (2018): 1-16.
4. Hu, Teng, et al. "Securing the Private Key in Your Blockchain Wallet: A Continuous Authentication Approach Based on Behavioral Biometric." Journal of Physics: Conference Series. Vol. 1631. No.1. IOP Publishing, 2020.
5. Pavel, Datinský. "European Legal Regulation of Cryptocurrencies through the AML Scope." Public Governance, Administration and Finances Law Review 5.1 (2020): 38-47.
6. Alharbi, E., and Daniyal Alghazzawi. "Two factor authentication framework using otp-sms based on blockchain." Transactions on Machine Learning and Artificial Intelligence 7.3 (2019): 17-27.
7. Sharma, Avin Mohitesh. "Cryptocurrency and Financial Risks." (2021).
8. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review, 21260.
9. Karantias, K. (2020). SoK: A Taxonomy of Cryptocurrency Wallets. IACR Cryptol. ePrint Arch., 2020, 868.
10. Aloul, Fadi, Syed Zahidi, and Wassim El-Hajj. "Two factor authentication using mobile phones." 2009 IEEE/ACS International Conference on Computer Systems and Applications. IEEE, 2009.
11. Moreno, S. M., Seigneur, J. M., & Gotzev, G. (2021). A Survey of KYC/AML for Cryptocurrencies Transactions. In Handbook of Research on Cyber Crime and Information Privacy (pp. 21-42). IGI Global.
12. https://digitalcommons.liberty.edu/doctora l/2791/[Accessed October. 15, 2021]

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 10, Dec 2022

13. https://bitcoin.org/en/secure-your-wallet [Accessed October. 15, 2021]
14. "Multisignature", Bitcoin wiki, 2019 [Online]. Available: https://en.bitcoin.it/wiki/Multisignature [Accessed October. 15, 2021]
15. https://sanctionscanner.com/blog/the-fincen- final-rule-regarding-crypto-wallets-2021-38 8[Accessed October. 15, 2021]
16. https://www.businessinsider.com/personal-fi nance/best-bitcoin-wallet?IR=T[Accessed October. 15, 2021]
17. https://www.ledger.com/ledger-nano-x-bluet ooth-security-model-of-a-wireless-hardware -wallet [Accessed October. 15, 2021]
18. https://trezor.io/security/[Accessed October. 15, 2021]
19. https://www.coinbase.com/security[Accesse d October. 15, 2021]
20. https://www.exodus.com/[Accessed October. 15, 2021]
21. https://wallet.mycelium.com[Accessed October.31,2021]