Kanpur Philosophers
ISSN 2348-8301
International Journal of humanities, Law and Social Sciences
Published biannually by New Archaeological & Genological Society
Kanpur India

Vol. X, Issue I(K) : 2023

SAFETY HAZARDS WITH CRYPTOGRAPHIC WALLETS

Ms. Bhakti Choudhari, Asst. Professor, Department of BSc.IT and CS, Nirmala Memorial Foundation College of Commerce and Science
Ms. Hiral Vishal Sojitra, Asst. Professor, Department of BSc.IT and CS, Nirmala Memorial Foundation College of Commerce and Science

Abstract:
Bitcoin overtook every other digital currency as the most popular one with the development of blockchain technologies. A key aspect of using bitcoin through its wallet is investing in cryptocurrencies and Initial Coin Offerings. Bitcoin's use is escalating rapidly as a result of its many advantages, including easy payment and transfer, conversion to legal cash, low fees for sending and receiving money, and others. However, as the price of bitcoin rises, concerns over security breaches are also flourishing. We lend an in-depth evaluation of the privacy and safety precautions of Bitcoin wallets. These flaws enable the execution of numerous security attacks against Bitcoin's standard operation. Recent research, mostly focused on the Bitcoin protocol, indicates that the cryptocurrency is not completely secure against user alliances that conspire to defraud the "Honest" Bitcoin miners using various attacks.

Keywords: Bitcoin, Blockchain, Vulnerabilities, Wallet.

1. Introduction

1.1 Blockchain

A peer-to-peer network's entire transactions are captured in a blockchain, which is a decentralized ledger. Participants can confirm transactions using this technology without the requirement for a central clearing organization. Applications might involve paying bills, concluding business deals, casting ballots, and a host of other things. Data structures developed using blockchaintechnology include built-in security features. It is founded on cryptographic, decentralized, and consensus concepts that guarantee the accuracy of transactions. The data is organized into blocks in the vast majority of blockchains or distributed ledger technology (DLT), and each block contains a transaction or accumulation of transactions. In a cryptographic chain, each new block is connected to all the blocks that came before it in a way that makes manipulating with it nearly impossible. A consensus mechanism verifies and accepts each transaction contained within the blocks, ensuring that each transaction is accurate and true.[1] Decentralization is made possible by blockchain technology by allowing members of a dispersed network to contribute to it. No single point of failure exists, and a single user cannot alter the transaction record. However, there are some significant security distinctions among blockchain technologies.

The block header comprises chain and block management information. The block body, meanwhile, contains a list of transactions. Since blockchain is a decentralised system, every single node has a digital signature that can be used to verify transactions and communicate with the other nodes

directly through a peer-to-peer network. A ledger made up of a series of blocks that some nodes have also agreed upon is available [1]. Proof of Work (PoW) and Proof of Stake (PoS) are two consensus algorithms that are frequently used in blockchain technology to ensure that the data on the ledger remains updated [1].

1.2 Cryptocurrency

Money acts as a store of value by enabling us to save the benefits of our work or business in a handy object. From the time of barter to the advent of commodity money like metal and coins like gold and silver, current monetary systems and checks, and finally most recent developments in the world of money like the introduction of cryptocurrencies like Bitcoin and Ethereum. Cryptocurrencies can be classified into digital currencies, alternative currencies, and virtual currencies. The currency is used more extensively. Bitcoin, an increasingly popular cryptocurrency, creates additional contemporary digital money. These sites do not allow third parties to handle their transactions.The purpose of cryptocurrency is to operate as a medium of exchange. Over 1600 cryptocurrencies are currently accessible online, and the count is rising. Any time a new cryptocurrency is invented. Bitcoin, followed by Ripple, Ethereum, and the Litecoin is now the largest blockchain network in terms of market capitalization.[1] Cryptocurrencies can be separated into digital currencies, alternative currencies, and virtual currencies. Bitcoin, a well-known cryptocurrency, creates additional contemporary digital money.

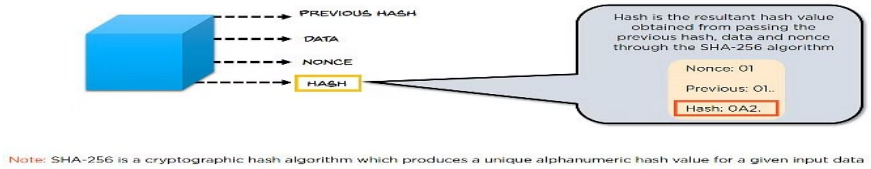
1. 3 Bitcoin

The popularity of Bitcoin, the most famous and well-known cryptocurrency in the world, has been rising. About 2 million bitcoins (BTC) will still need to be mined as of June 2022, making the total number in circulation close to 19 million. Due to its distinctive design and underlying technology, Bitcoin has recently become more popular as an investment. In contrast, Bitcoin is an opt-in currency that is controlled by user consensus or will. It consists of an expanding network of users who voluntarily comply with the Bitcoin protocol's principles. They employ decentralized technology to carry out peer-to-peer transactions and hold value apart from any enterprise, government, or financial institution. When utilizing Bitcoin, there is no requirement to request authorization and no chance of being disconnected from the network.

1.3.1PoW - Proof of Work :

The original consensus algorithm in a blockchain network is referred to as Proof of Work (PoW). The algorithm contributes a new block to the chain and verifies the transaction. Bitcoin is the most renowned Proof of Work (PoW) application. The Hashcash proof of work technology allows for the implementation of proof of work in a blockchain.

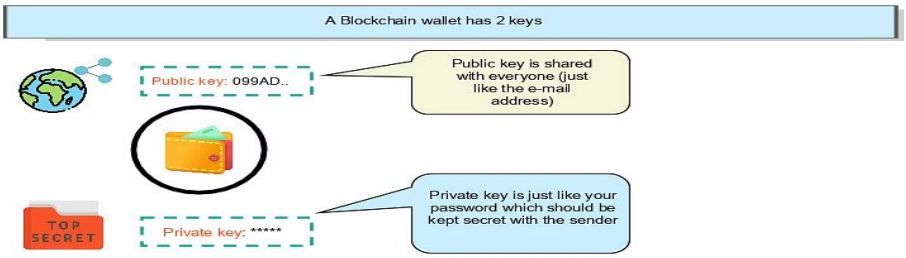
- Nonce: The nonce, which is employed in bitcoin's "proof of work" consensus mechanism, is a random number that changes the output of the hash value. The nonce is the parameter that is used to generate the hash value that each block is intended to provide. The blockchain's transaction verification procedure is the proof of work.
- Hash: This is the result of running the data, the nonce, and the previous hash value through the SHA-256 algorithm; it serves as the block's digital signature.[11]



- SHA-256: Blockchain guarantees that the blocks are kept safe by using a hash function called SHA-256 to prevent unauthorised access. They have a digital signature. Once produced, their hash value cannot be changed.
- Proof of work: In blockchain mining, miners verify transactions by figuring out a challenging math problem known as proof of work.

1.4 Wallet

As a result, the private key controls all cryptocurrencyfunds, hence safeguarding the user's private keys is of the utmost significance. It is a crucial obstacle for cryptocurrencies [4]. The private keys must be stored and transactions must be signed using a special piece of hardware or software called a crypto wallet in existing systems. Cryptocurrency wallets range from online to cold wallets, but many experts agree that the hardware wallet is the best safe option. Typically, it takes the form of a smart card, USB stick, or Bluetooth device that is specifically designed for cryptography. The hardware wallet is secure in many ways, but there are certain crucial problems that need to be resolved. The word "crypto wallet" refers to cryptographic software that controls a user's private addresses, keys, and seeds in blockchain and cryptocurrency. This programme may be located on a laptop, smartphone, web server, or even specific hardware. The keys would be securely generated, kept, and some method of backup and restoration would be provided.



Wallet Types

- **Hot Wallet** Online wallets called "hot wallets" allow for quick cryptocurrency transfers. (For instance, the Coinbase wallet [5]), the user saves the keys on a password- or two-factor-protected online cloud server similar to exchanges. On the desktop, laptop, and smartphone, it is practical and widely available, but if hackers attack a cloud server, all users' keys will be exposed. In the actual world, it happens frequently [6][7] since these servers serve as a haven for hackers. They can be encountered online. Coinbase and Blockchain.info are two examples.

- **Cold Wallet** Digital offline wallets known as "cold wallets" sign transactions offline before disclosing them online. To preserve strong security, they are maintained offline rather than in the cloud on the internet. The Trezor and Ledger are two types of cold wallets.

In cold wallets, private keys are kept on a paper document or in separate hardware that is not linked to the internet or the cloud. This device has no Internet connection and transfers keys and transactions with a USB stick. This type of wallet is still vulnerable to advanced attacks. For example, the author of transfers the secret keys via ultrasound from an offline wallet to an adjacent online computer.[8]

- **Brain Wallet** The simplest one is the brain wallet. All secret keys and addresses are derived from the passphrase the user selects. As a result, the user does not need to keep track of a wallet made of paper, software, or hardware. He creates the secret keys and enters the passphrase into a wallet programme each time he needs to perform a transaction. The wallet programme deletes the password and all generated keys from memory after signing a transaction. There are a lot of problems with the brain wallet. First of all, the user forfeits all funds if he forgets the passphrase. Second, the wallet program's malware is capable of sniffing the user's passphrase and stealing his money.

- **Paper Wallet** A paper wallet is an approach to offline cryptocurrency storage. Your private key and public key are both contained on this printed piece of paper wallet, which can be accessed by scanning a QR code. Two popular paper wallets are Bitcoin Paper Wallet and MyEtherWallet. Funds can be transferred from your software wallet to the public address listed on your paper wallet. You park your money in a software wallet first, then transfer it to the paper wallet's public address using your software wallet's public address.

1.5 Attacks on the Wallet Softwares :

The client-side applications known as 'wallets' are basically used to manage the Bitcoins owned by the client as well as the transaction of the Bitcoins from/to the client. The client can either go for the online wallet services or he can choose to have wallet applications downloaded in his node. Generally, the online wallets are more vulnerable to the attacks and thus need to be encrypted and backed off-line. Existing backup facilities allows the user to retrieve old wallet files and contents. The coin history is traceable that leads to linking the user identity with the Bitcoin address. Distributed denials of service (DDoS) attacks are potential threats for the online wallet application.

1. Copy & Paste aka "Clipboard Hijackers"

In case we need to transact currency from a wallet, and if we copy and paste the address, then there are programs that can replace the address that is copied for another address, to get you to send your funds to the wrong wallet. So, you must always double, triple check the address you are sending to. Cryptoshuffler is a program used to hijack crypto addresses has been used to steal 140,000 in Bitcoins. [9]

2. Factor Authentication by SMS or TEXT

SMS and messages are poor choices for 2-factor authentication (2FA) setup since they can be easily hacked. This kind of hacking is rapidly expanding, particularly in the US where mobile phone operators are gullible and have frequently been tricked into disclosing information that provides hackers access to accounts connected to the hacked cell phone (who would've guessed!). The names, last names, and phone numbers of crypto holders are all that the hackers require.

3. Hacked Coinbase Wallet (a successful experiment story):

A Coinbase account that was linked to a Gmail account has been found to be two-factor secured. The organisation was able to intercept all text messages received to the phone for a predetermined amount of time by taking advantage of well-known bugs in the cell network. That was sufficient to change the Gmail account's password, after which the Coinbase wallet was taken over. The organisation only need the target Bitcoin user's name, last name, and phone number. Despite the fact that it would have been simple to do so, since these individuals were security researchers rather than criminals, no one's bitcoin was really stolen.

4. Fake Mobile Apps

Some hackers have the skills necessary to break into legitimate mobile applications and create phoney real mobile applications to trick users into trading on phoney platforms. The "trading" will involve traders delivering their money and all of their personal information to the hackers' wallets. This occurred with the well-known exchange Poloniex, which used phishing applications spread throughout Google to trick users into trading on a Fake Poloniex platform. As a result, we must take precautions to protect mobile devices with Touch ID, PINs, and anything else you have access to in order to safeguard the gadgets you use to access your wallet and keys. Asking you to keep your phone locked may seem straightforward, yet the majority of phone hijackings occur as a result of our disregard for the slightest aspects.

5. Phishing Emails
Probably the most common of all attacks, where hackers send you an email as if they were from your wallets service (for example), with a URL that looks legitimate but will redirect you to a FAKE URL to have you enter your information trying to enter your wallet. You can always hoover over the link (which may look genuine) to see if you are being directed to the link you are seeing. Hackers search for simple human "deficiencies", the disclosure of personal data on social media, passwords, etc. So never leave any of this sort of information lying in your mail.

6. Stealing Keys and Passphrases
Key encryption at the application level is a need. Hackers will be able to steal keys if they are left unencrypted in preference regions, the programme sandbox, the SD card, or in external locations like the clipboard. They can do whatever they want with the money in the wallet once they get the keys. Even if the device is compromised, the keys will still be secure if the data is encrypted at the application level.

7. Dynamic Attacks on Private Keys
The keys and pass phrases to a crypto wallet can also be dynamically stolen, meaning that they are somehow intercepted as the wallet owner types the key or passphrase characters into the crypto wallet mobile app. Hackers typically use one of three methods to do this:

- Over-the-shoulder attack: Historically, this refers to a hacker who is physically and surreptitiously close enough to a user to see them enter the passphrase into the crypto wallet. But today, there's no need to be there in the flesh. Screenshots and screen recording can be abused to this end.
- Keylogging malware: Here, malware runs in the background on the app to capture every keystroke and send them to cybercriminals. Rooting (Android) and jailbreaking (iOS) the smartphone makes keylogging even easier to accomplish.
- Overlay attack: In this case, malware places a screen, which could look genuine or could be transparent, that tricks the crypto wallet's owner into entering credentials either into a field inside the wallet app or a malicious screen. The malware either transmits the information directly to cybercriminals or takes over the wallet directly to transfer the funds in the wallet to hackers.

Defending against these threats requires the app to detect keylogging, overlays and recording, so it can take direct action by warning the wallet's owner or even shutting down the app entirely.

8. Malicious Instrumenting
The security of a mobile wallet depends on the integrity of the platform that runs it, because if the device is rooted or jailbroken, or if hackers abuse development tools like Frida, they can gain access to the blockchain address of the client app. They can even impersonate the app to make transactions on their own. Mobile crypto wallet apps must be able to tell when they are working within a rooted or jailbroken environment so they can, if called for, shut down to protect the user. They must also be able to block Magisk, Frida and other dynamic analysis and instrumentation tools that can be abused to compromise critical functions' integrity. Just as important, developers should obfuscate the app's code so that hackers will have a much more difficult time reverse-engineering the app's inner workings and logic.

Summary :
Users are placing a sizable portion of their tokens (i.e., money) in crypto wallets. They anticipate security at least as good as what they receive from other banking and financial apps. Some teams, who developed extremely well-liked wallets, lack the security and cryptography knowledge necessary to recognise that their implementation exposes users to risks. Security for digital wallets is a tough creature. All of the interesting faults we've discovered—input validation, input

authentication, access to local storage, cryptography—come together to create possible problems and vulnerabilities. Although they are all fairly small, when combined, they open up unexpected attack vectors. Therefore, it makes sense to consider not just individual flaws but also their interactions. A large portion of the customers' tokens (or money) are put in crypto wallets. They anticipate a degree of security that is at least as good as that offered by other banking and financial apps. After creating really well-liked wallets, some teams fail to comprehend how their implementation exposes consumers to issues since they lack security and cryptography knowledge. Security for digital wallets can be challenging. The junction of several faults, including those in input validation, authentication, access to local storage, and cryptography, results in all the interesting vulnerabilities and possible problems we've discovered. Despite being fairly small individually, together they create unexpected attack vectors. It becomes sense to consider not only individual defects but also how they interact. Secure coding and appropriate testing are two ways to prevent security issues.

References :

[1] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, "Bitcoin and cryptocurrency technologies: A comprehensive introduction," Princeton University Press, 2016.

[2] Z. Zheng, S. Xie, H. N. Dai, and H. Wang, "Blockchain challenges and opportunities: A survey," in International Journal of Web and Grid Services, 2016.

[3]https://www.researchgate.net/publication/316656878_An_Analysis_of_Cryptocurrency_Bitcoin_and_the_Future/link/590a0af90f7e9b1d0823c253/download

[4] https://stars.library.ucf.edu/cgi/viewcontent.cgi?article=1402&context=etd2020

[5] Open Source JavaScript Client-Side Bitcoin Wallet Generator, Online: https://www.bitaddress.org [18] Coinbase home page, https://www.coinbase.com/

[6] P. Rizzo, "Mt. Gox allegedly loses $350 million in Bitcoin (744,400 BTC), rumoured to be insolvent", CoinDesk, Feb. 25, 2014 [Online]. Available: https://www.coindesk.com/mt-gox-loses-340-million-bitcoin-rumoured-insolvent [Accessed Oct. 8, 2018].

[7] Y. Nakamura, A. Tan, and Y. Hagiwara, "Coincheck Says It Lost Crypto Coins Valued at About $400 Million", Bloomberg, Jan. 26, 2018 [Online]. Available: https://www.bloomberg.com/news/articles/2018-01-26/cryptocurrencies-drop-afterjapanese-exchange-halts-withdrawals [Accessed Oct. 8, 2018].

[8] M. Guri, "BeatCoin: Leaking Private Keys from Air-Gapped Cryptocurrency Wallets", arXiv.org, 2018 [Online]. Available: https://arxiv.org/pdf/1804.08714.pdf [Accessed Oct. 8, 2018].

[9] https://www.digitalshadows.com/blog-and-research/cryptocurrency-attacks-to-be-aware-of-2021/

[10] https://d1wqtxts1xzle7.cloudfront.net/93545860/4081-libre.pdf?1667411111=&response-content-disposition=inline%3B+filename%3DIntroduction_to_Cryptocurrency_An_Overvi.pdf&Expires=1683186602&Signature=AFX4X0TbHW4ROoxIspP9mMg9zgwbURFKKCp~Mwzj64ytqVa6e4vg~ECyzKzzkLVeql1aJvSa3UpzbGYE3Npybkv0RtBr5l~IK7lBGXYi1BgKXJ46NdbC6Cn2Kl4h3bRbA1olyVc1vVCVOixGgPRmlfNmEONMN9uXc1jeKZpvhEEQzWfbK9I8nwsG6X4iEiuXGJrUJ5aapRtCMelP6uOsYjqiQvp9QsmiK5Nq1U5Hhf5P2JK6iqEr1iq2ZM546MEt3SQXdWO8DMezkMGC4EAf4ujTfaKpzsuIiNP44VTmYg1AosNBTUdsfebtbsSFqaEBZ1Pt2iTKhjcFMrFFA__&Key-PairId=APKAJLOHF5GGSLRBV4ZA

[11] https://www.simplilearn.com/bitcoin-mining-explained-article