Highly Secure Cryptocurrency Hardware Wallet

Srinivas Vedula, Abdul Sameer, Vaishali K, Varun VP, Radha Prajapath, Ms. Shaleen Bhatnagar

Student, Student, Student, Student, Student, Professor,
Department of Computer Science and Engineering, School of Engineering,
Presidency University, Bengaluru, India.

Abstract: With the increasing popularity of Bitcoin, decentralized digital currency, and payment systems, the number of malicious third parties trying to steal Bitcoin has greatly increased. An attacker can steal bitcoins worth millions of dollars from victims by using simple malware code to gain access to the system that contains the information about the user's private key, these systems can be a computer or smartphone. To prevent the attackers from stealing the user's Bitcoin private key, We propose the use of a hardware wallet for the authentication of every payment, this will provide security from the hackers because the private key would be on an offline device built using raspberry pi zero. This allows the users private key to be separately stored in a hardware device that is not vulnerable to online malware attacks, hence providing security and ensuring a reliable transaction.

IndexTerms - Blockchain, Cryptocurrency, Raspberry Pi, Trezor, SHA-256, PBKDF-2.

I. INTRODUCTION

Internet is all over the world and has reached a level where it merges with one's life, data security holds a lot of importance and it is a concern for everyone connected to the web. The era of information and communication has given many excellent opportunities in several areas. One such field that is benefitted is the financial and business sector, many transactions are activated virtually thus creating a new business phenomenon of trading and new transactions and currencies have been arising. One such remarkable financial form that emerged is cryptocurrency a medium of exchange. Bitcoin is the most successful cryptocurrency, as this turned to be the future there were many attacks on this and as a part of securing this, we produced the advancement of protecting the private key of the bitcoins in a highly secured cryptocurrency wallet. The industry state of the art for protecting cryptocurrency is a hardware wallet, the problem with this existing system is the private key is stored in the website and we must be more cautious about this account.[16] Bitcoin is going to be the future of transactions and our vision is to protect provide high security and authorization.

II. BLOCKCHAIN

Blockchain, the building block of Bitcoin, has gotten expansive contemplations lately. Blockchain is an innovation that permits information to be put away and traded on a peer-to-peer (P2P) premise. Primarily, blockchain information can be counselled, shared and tied down on account of agreement based algorithms. It is utilized in a decentralized way and eliminates the requirement for mediators, or on the other hand "confided in outsiders".

The blockchain is open-ended and works in a decentralized, progressing way on account of the movement of its clients who can store data, and to agreement calculations (strikingly "confirmation of-work" and "verification of-stake") which guarantee the data per block (unit). Clients running these calculations are known as diggers. At the instance when a block has been approved, it is connected to the blockchain and shared with the organization. Blocks are associated with one another in such a manner that if clients wish to transform one square, the whole blockchain should likewise be changed[1].

A blockchain is typically a disseminated information base of records or public record, everything being equal, or leading-edge occasions that have been executed and divided between partaking parties. Each trade-off in the public record is checked by the consent of the majority of the partaker in the network, data can never be eradicated. The blockchain contains a definite and undeniable record of every single exchange at any point made. To utilize a fundamental similarity, it is not difficult to take a treat from a treat container, kept in a segregated spot than taking the treat from a treat container kept in a commercial centre, being seen by a huge number of individuals.

III. CRYPTOCURRENCY

A peer-to-peer digital exchange system that uses cryptographic techniques to generate and consign currency units is called cryptocurrency. This process involves a transaction of distributed verification without a central prerogative. The amount and the currency that the payer owns and their transactions are verified by ensuring the currency units are not reused, this process of verification is called mining[1]. Cryptocurrency targets and ensures restriction on the no of transactions done per unit time.

Cryptocurrencies are the trending financial software systems. which depend on consigned ledger data structure and is secured, mining is an indispensable part of software systems. Mining reconsolidates records of past transactions to the distributed register known as the Blockchain, which allows users to reach secure, robust, and concord for each transaction. This also introduces new units of currency named "bitcoins". Cryptocurrencies were designed as peer-to-peer end sub-systems that lack authority to mediate the transaction. To validate and scrutinize the transactions they rely on miners. Cryptocurrencies require secure and strong mining algorithms. Cryptocurrencies will replace transaction intermediaries with cryptographic methods.

In the cryptocurrency system, there is a double-spending problem: once a transaction is done. A cryptocurrency system is defined by two parameters: money growth rate $\mu \geq 0$ and transaction fee charge at a rate $\tau \geq 0$ [16]. They have attracted several types of users and many invest in this for a huge return. characteristics of cryptocurrencies are decentralization, their inheritor pseudo-anonymous. They are one out of many constructs called crypto assets, they are global characters, they are intriguing and attractive[18].

IV. CRYPTOGRAPHY

Confidentiality of messages can be obtained through the technique of Cryptography; this provides privacy of individual and organization in a secured way. Cryptography is used on daily basis across the globe, it is highly brittle. As crackers are trying to hack network systems, we came up with legal changes concerned cryptography, reliability, and technologies used in privacy enhancement. It will play a major role in the protection of data and information as of now and in the future. In this the concealed information is known as plain text and encryption is the process of disguising this plain text[2].

The invention of public-key encryption is considered a cryptography evolution and through this, it spread across areas and played a vital role in achieving security goals, confidentiality, and authentication. To achieve these goals algorithms are developed. This provides a reliable, robust network, strong data security. In cryptography, an ingenious human-readable message, mentioned as plaintext, is modified using an algorithm, or series of mathematical operations, into something that to an uninformed observer would appear as if gibberish; this gibberish is named ciphertext.

4.1 Advantages of Cryptography

4.1.1 Keep the substance of information classified.
4.1.2 Authenticate the identification of the sender and receiver of a message.
4.1.3 Guarantee the trustworthiness of the information, showing that it hasn't been changed.
4.1.4 Demonstrate that the supposed sender sent this message, a principle referred to as non-repudiation[2][3].

4.2 Types of Cryptography

4.2.1 Secret Key Cryptography

The secret key cryptography is utilized to scramble the plaintext message utilizing a progression of pieces called the secret key. The secret key in cryptography is additionally an input for the encryption algorithm as this is often the initial intelligible message or data that's fed into the algorithm as input.[3] the most is an algorithm value independent from the plaintext. counting on the actual key used the algorithm outputs a special result. The ciphertext is an almost random stream of knowledge which because it stands.

4.2.2 Public Key Cryptography

Public-key cryptography, or asymmetric cryptography, is an encryption scheme that uses two mathematically related, but not identical, keys - a public key and a personal key. Unlike symmetric key algorithms that believe one key to both encrypt and decrypt, each key performs a singular function. the general public key's wont to encrypt and therefore the private key's wont to decrypt.

Since public keys got to be shared but are too big to be easily remembered, they're stored on digital certificates for secure transport and sharing. Since private keys aren't shared, they're simply stored within the software or OS you employ, or on hardware (e.g., USB token, hardware security module) containing drivers that allow it to be used together with your software or OS[3].

4.2.3 Hash Functions

A cryptographic hash function takes an arbitrary amount of data input—a credential—and produces a fixed-size output of enciphered text called a hash value, or just “hash.” That enciphered text can then be stored rather than the password itself, and later wont to verify the user.

This makes hashing algorithms an excellent tool for ensuring data integrity. as an example, a message is often sent alongside its own hash. Upon receiving the message, you'll run an equivalent hashing algorithm on the message text; if the hash you produce is different from the one accompanying the message, you recognize the message has been modified in transit[4].

4.3 Need of Public-key and Private-key

Blockchain utilizes a few distinct types of cryptography. Among these is: Public Key Cryptography Public key cryptography utilizes a couple of a public key and a private key to perform various assignments. Public keys are generally distributed, while private keys are kept in mystery.

Utilizing an individual's public key, it is feasible to encode a message so just the individual with the private key can decode and understand it. Utilizing a private key, a digital signature can be made so anybody with the relating public key can check that the message was made by the proprietor of the private key and was not altered since. The algorithms utilize a simple numerical issue to create a message, yet we make it difficult for that message to be decoded by somebody who shouldn't unscramble it, and public and private keys assume a major part in the blockchain.

4.4 Generation of Public-key and Private-key in Trezor

Trezor's engineering is with the end goal that it keeps hidden keys inside the device and never disclose them. Trezor utilizes an idea called "deterministic" public keys. From the private key, the alone expert public key is determined. From that solitary expert public key, quite a few broadened public key can be determined. Each all-encompassing public key relates to a Trezor "account". For each all-inclusive public key, quite a few real open keys (for example bitcoin address) can be determined.

In this way, the private keys are just on the gadget, however, either the expert public key or any of the xpub keys are sent from the gadget to both your internet browser and to mytrezor.com workers. Thus, the private keys are not planned or proposed to leave the gadget, and they are not needed to create new addresses securely.
A public key is a cryptographic code that permits a client to get digital forms of money into their record. The public key combined with the private key is huge instruments needed to guarantee the security of the crypto economy.

XPUB is an expert public key used to create all locations for a record in a various levelled deterministic wallet (both effectively utilized and unused). As the XPUB key is a public key, it doesn't permit individuals to spend reserves, however, it makes it conceivable to tune in on every one of the exchanges and equilibriums associated with it.
To process the expert private key, a calculation called PBKDF-2 is executed. During this period, the force utilization of the processor is higher than when the calculation stops to revive the presentation (which it completes multiple times). After the last revival, the public key of the TREZOR is processed. When zooming close into the various parts, one can recognize the PBKDF-2 calculation from the part where the public key is processed.

V. ALGORITHM

We will be using SHA-256 as a hashing algorithm, BIP39 for mnemonic code generation and PBKDF-2 for hash-based message authentication code (HMAC) or public key and private key derivation.

5.1 SHA-256

Hashing algorithms take in transaction input and these inputs are run through an algorithm like SHA-256 which gives us an output of fixed length variables. SHA-256 is a cryptographic hash function that is mostly used in bitcoin, the abbreviation of SHA is Secure Hash Algorithm it was a technology developed by the NSA(National Security Agency), the basic function of SHA-256 is to take an input of any variable size and return an output that is almost-unique 256-bit (32-byte) signature for a text, SHA-256 is used in several different parts of the Bitcoin network, SHA-256 is an algorithm that is also used in Bitcoin mining.SHA-256 is used in the creation of bitcoin addresses to improve security and privacy[8].

5.2 BIP-39

BIP39 is used to generate deterministic keys and it is also a type of mnemonic code, BIP is used as an algorithm in the recovery seed and is related to BIP32 binary master seed. It consists of two parts, generating the recovery seed and then converting it into a binary master seed, and it also includes an optional application that passphrase it during the conversion.
Generating the recovery seed/Generate Entropy, The process starts with entropy generation. With the higher number of entropy, security is improved but the sentence length increases. The length is supposed to be in the range of 128–256 bits to generate 12–24 phrases[5].

5.3 PBKDF-2

The abbreviation of PBKDF2 stands for Password-Based Key Derivation Function 2, is a key derivation function with highly varying computational cost, PBKDF2 is used to reduce chances of brute-force attacks and rainbow table attacks. PBKDF2 is part of RSA Laboratories' Public-Key Cryptography Standards (PKCS), PBKDF2 takes several input parameters and produces the derived key as key = pbkdf2(password, salt, iterations-count, hash-function, derived-key-len)[5]

VI. PROPOSED WORK

We have designed a highly secured multi-currency wallet that allows the user to store different cryptocurrency it is designed to protect your private keys from online/offline attacks. To do this it keeps the private key away from the internet and signs the required transactions.

The hardware wallet is built using raspberry pi zero w as a major component, we have configured the device to run the Terzor operating system on the pi zero device, we have also provided visual feedback to the user for every bitcoin transaction on an OLED display mounted to the pi device, for the interaction with the device we have provided two push buttons. The pushbuttons allow the user to accept or reject the payments.

The Trezor OS provides the functionality that permits the user to store his private key on the SD card installed within the raspberry pi zero whence making it a highly secured hardware wallet, Trezor features a feature that permits the users to use seed words (using seed you'll recover the wallet if it's lost or broken) for backup, the main function of Trezor API is used to send/receive cryptocurrency from other cryptocurrency wallets to your highly secure hardware wallet. Trezor uses SHA-256 for encryption and decryption and also uses BIP-39 for deterministic keys which are used for enhanced security

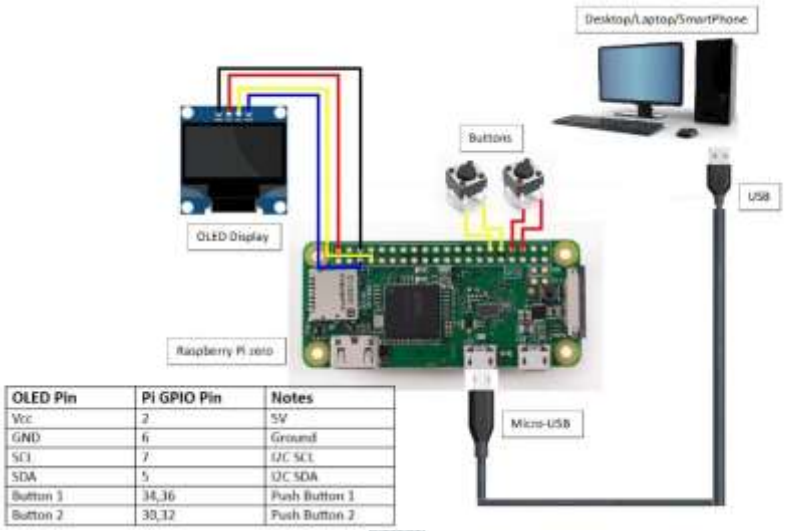
VII. IMPLEMENTATION

For the implementation we need a Raspberry Pi zero w, 0.96 Inch(128x64) 4pi I2C OLED Display alternatively we can use ADAFRUIT OLED display 128x64, 2 pushbuttons, jumper wires, micro-USB, SD-Card, Heat sink.

6.1 Connections

Our display has four pins GND, VCC, SCL, SDA. Connect pin GND to GND(6 or 9) of Rasberry pi zero w, connect OLED VCC to 3.3v VCC of Raspberry pi zero w(Pin: 1), connect SCL to pin number 5 and connect SDA to pin number 3. Now we have to connect two push-button for the following option YES and NO or NEXT and PREVIOUS, for connection select two

terminals of the button on the same side and place one terminal to pin 34 and another to pin 36, and for button NO connect one terminal to pin 30 and another to 32.



OLED Pin	Pi GPIO Pin	Notes
Vcc	2	5V
GND	6	Ground
SCL	7	I2C SCL
SDA	5	I2C SDA
Button 1	34,36	Push Button 1
Button 2	30,32	Push Button 2

Fig. 1: Connection diagram

After connecting all the components we will flash the SD card with the Pi-Trezor image file(.img). for flashing the .img file we will use BalenaEtcher.After successfully flashing the .img file we have to open the .config file and make the following changes to it. export TREZOR_OLED_TYPE=5, export TREZOR_OLED_FLIP=1, export TREZOR_GPIO_YES=16, export TREZOR_GPIO_NO=12. After making the following changes to the .config file insert the SD card in Rasberry Pi zero w, and connect the micro-USB port of Rasberry pi zero w to the USB port of your laptop/Desktop/smartphone. As shown below.

VIII. WORKING

8.1 Receive Cryptocurrency:

Connect the configured hardware wallet containing your private key to your desktop or laptop go to the trezor.io website, enter the pin the pin layout is also displayed on the device. Go to the receive tab in the trezor.io main page and click on show full address ,user will receive address on the website screen as well as on the device for confirmation the user can cross check the address on the website with the address on the device, the address provided can be used to receive bitcoin payment, once the user has confirmed the address on the device matches the address on the website the user can press continue to receive a qr code which will help the user make payments easily, since the address can be copy pasting process can have errors user can use this method to make a more reliable transaction, the user can choose bitcoin platform form where you he wants to receive a payment the go into the withdrawal section of the bitcoin platform, this section will contain a input box by the name Destination BTC Address, the address that has been received from the terzor.io website has to be copy pasted on to this input box, user has to check the address one more time to make a secure transaction, then click on continue now the transaction is in process this transaction will take some amount of time to process, once the transaction is confirmed the terzor.io website will be updated and the transaction will be visible under the transaction tab

8.2 Send Cryptocurrency:

Connect the configured hardware wallet containing your private key to your desktop or laptop go to the trezor.io website, enter the pin, the pin layout is also displayed on the device, go to the Send tab on terzor.io website, in the Address column enter the address of the receiver, next entre the Amount of bitcoin to be sent, the fee column is for the system the mines and makes the transactions from your account to the receivers account lower the fee, the transaction will require more time to be processed, higher the fee, the transaction will be processed in less amount of time, once all the details are entered, the user can click on Send. You will be again prompted to enter the pin before proceeding with the transaction, the hardware wallet will be signing the transaction, then the user will be prompted to confirm the transaction on the hardware wallet, the address and the amount will be displayed on the Hardware wallet, the user can click on the accept push-button on the Hardware wallet to confirm the transaction, once the push button is pressed the website would require 10 seconds to refresh and display the details. Now the transaction has been completed

8.3 Firmware Update:

Before doing any transaction check if the device is updated by clicking on the show details button on the main page. User will be redirected to a new page showing the firmware Update status of the Hardware wallet, if your Hardware wallet is up to date there will be no warnings telling you to update the firmware, if there is a warning on the screen telling you to update the firmware of the device unplugs the Hardware wallet from your system. And then plug it back in while holding two push buttons on the Hardware wallet, now the device will enter boot mode and you will see the Update button on the website, you can click on it to start updating the firmware once the device is updated unplug the device and plug it back in enter the pin

IX. RESULT

Once you connect the device to the system you will have to enter the pin, and got to the sent tab on the trezor.io website. Enter the Address(3LGQZU1tvWThcWK3ofcUZzWF7ZfJPKSj2v) of the receiver and all payment details. And click on the send button. To proceed with the transaction.

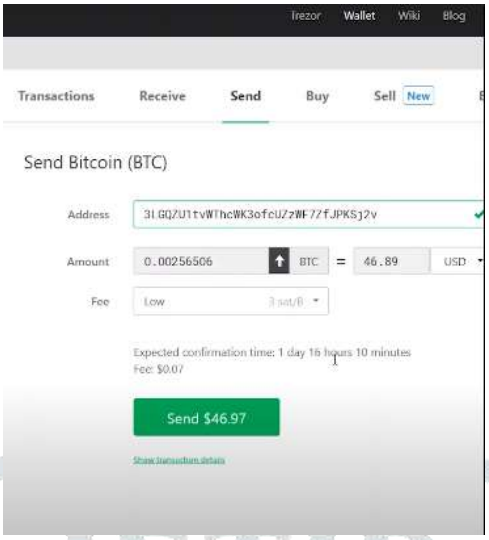


Fig. 2 Sending Cryptocurrency

When prompted to confirm the transaction on the device check the address and click confirm on the hardware wallet, the secure transaction has been completed with the Hardware wallet now.

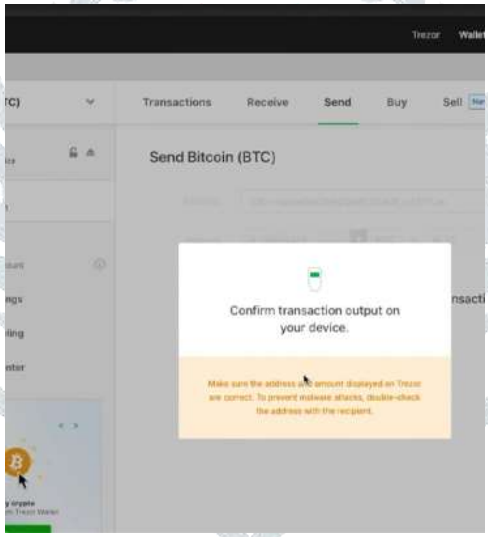


Fig. 3 Waiting for confirmation from our wallet

X. CONCLUSION

Overall, the highly secured hardware wallet is a solid project, with functional software, it stores the private keys inside itself and does signing in device with user interaction enforced between the highly secured hardware wallet and the machine running the client. Since the keys are never exposed, this reduces the chances that a hacker who gains access to a computer (or phone) can steal bitcoins. Signing Bitcoin transactions with a highly secured hardware wallet is secure and fast. A user can simply pay with Bitcoin by reviewing the transaction information on the screen of a highly secured hardware wallet and entering her PIN code. This makes our e-wallet a viable option for credit card and cash payment methods.

REFERENCES

[1] H. Rezaeighaleh and C. C. Zou, "New Secure Approach to Backup Cryptocurrency Wallets," 2019 IEEE Global Communications Conference (GLOBECOM), 2019, pp. 1-6, doi: 10.1109/GLOBECOM38437.2019.9014007.

[2] M. Conti, E. Sandeep Kumar, C. Lal and S. Ruj, "A Survey on Security and Privacy Issues of Bitcoin," in IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3416-3452, Fourthquarter 2018, doi: 10.1109/COMST.2018.2842460.

[3] Jokić, Stevo & Cvetković, Aleksandar Sandro & Adamović, Saša & Ristić, Nenad & Spalević, Petar. (2019). Comparative analysis of cryptocurrency wallets vs traditional wallets. Ekonomika. 65. 10.5937/ekonomika1903065J.

[4] G. Khan, A. H. Zahid, M. Hussain and U. Riaz, "Security of Cryptocurrency Using Hardware Wallet and QR Code," 2019 International Conference on Innovative Computing (ICIC), 2019, pp. 1-10, doi: 10.1109/ICIC48496.2019.8966739.

[5] Bamert, Tobias & Decker, Christian & Wattenhofer, Roger & Welten, Samuel. (2014). BlueWallet: The Secure Bitcoin Wallet. 8743. 65-80. 10.1007/978-3-319-11851-2_5.

[6] Barber, Simon & Boyen, Xavier & Shi, Elaine & Uzun, Ersin. (2012). Bitter to Better — How to Make Bitcoin a Better Currency. Advances in Water Resources - ADV WATER RESOUR. 7397. 10.1007/978-3-642-32946-3_29.

[7] Heilman E., Kendler A., Zohar A., and Goldberg S., "Eclipse attacks on Bitcoin's peer-to-peer network," in Proc. 24th USENIX Conf. Security Symp. (SEC), Washington, DC, USA: USENIX Assoc., 2015, pp. 129–144.

[8] Eastlake D., and Hansen T.. (2011). U.S. Secure Hash Algorithms (SHA and SHA-Based HMAC and HKDF). [Online]. Available: http://www.ietf.org/rfc/rfc6234.txt

[9] McCorry P., Möser M., Shahandasti S. F., and Hao F., "Towards Bitcoin payment networks," in Proc. 21st Aust. Conf. Inf. Security Privacy, Springer-Verlag, 2016, pp. 57–76

[10] Nakamoto, Satoshi. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. Cryptography Mailing list at https://metzdowd.com.

[11] Rezaeighaleh, Hossein, "Improving Security of Crypto Wallets in Blockchain Technologies" (2020). Electronic Theses and Dissertations, 2020-. 403. https://stars.library.ucf.edu/etd2020/403

[12] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in 2015 IEEE Security and Privacy Workshops, May 2015, pp. 180–184.

[13] Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract] y," SIGMETRICS Perform. Eval. Rev., vol. 42, no. 3, pp. 34–37, Dec. 2014.

[14] S. Jarecki, A. Kiayias, H. Krawczyk, and J. Xu, "Highly-efficient and composable password-protected secret sharing (or: How to protect your bitcoin wallet online)," in 2016 IEEE European Symposium on Security and Privacy (EuroS P), March 2016, pp. 276–291.

[15] M. Gentilal, P. Martins, and L. Sousa, "Trustzone-backed bitcoin wallet," in Proceedings of the Fourth Workshop on Cryptography and Security in Computing Systems, ser. CS2 '17. New York, NY, USA: ACM, 2017, pp. 25–28.

[16] M. H. u. Rehman, K. Salah, E. Damiani and D. Svetinovic, "Trust in Blockchain Cryptocurrency Ecosystem," in IEEE Transactions on Engineering Management, vol. 67, no. 4, pp. 1196-1212, Nov. 2020, doi: 10.1109/TEM.2019.2948861.

[17] Mohammed, Abdalbasit & Varol, Nurhayat. (2019). A Review Paper on Cryptography. 1-6. 10.1109/ISDFS.2019.8757514.

[18] Arapinis, Myrto & Gkaniatsou, Andriana & Karakostas, Dimitris. (2019). A Formal Treatment of Hardware Wallets.

[19] . Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J.A., Felten, E.W.: Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In: Security and Privacy (SP), 2015 IEEE Symposium on. pp. 104–121. IEEE (2015).

[20] . Hsiao, H.C., Lin, Y.H., Studer, A., Studer, C., Wang, K.H., Kikuchi, H., Perrig, A., Sun, H.M., Yang, B.Y.: A study of user-friendly hash comparison schemes. In: Computer Security Applications Conference, 2009. ACSAC'09. Annual. pp. 105– 114. IEEE (2009)