International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Secure Crypto currency Transaction using Elliptic Curve Digital Signature Algorithm for Storing Wallets

Dr. Dhilipkumar.S[1*], Mr. Francis Jasper Terence Rex.[2], Ms. Jerlin A[3], Ms. Viji Charles.[4]

Submitted: 25/01/2024 **Revised**: 03/03/2024 **Accepted**: 11/03/2024

Abstract: Crypto currency has become a universal currency. Though certain countries restrict its usage and plans to create their own crypto currency, the prevalence of the existing crypto currencies such as Bitcoin and their values are remarkable. Crypto currencies along with blockchain technology enables the anonymity of users, decentralization but with security and reliability. The security of encrypted wallets is becoming increasingly important as the overall value of digital currency increases. The hardware only wallets are secure somehow but it is not likely to have convenience of software-based wallets. Similarly, the software wallets are handy but have cyber vulnerabilities. In this paper, a hardware based crypto wallet for storage and transaction purposes is proposed by using encryption techniques. The main objective is to build a safe, secure, and durable wallet for storing the crypto currency and to maintain a ledger of the transactions which in turn increases the wallet's security and the convenience of using it for an average consumer. The remote access will be available when the wallet is online. Hence for authentication, we are using Elliptic Curve Digital Signature Algorithm (ECDSA). The authenticity of the data and credibility of user's credential can be proved with this technique.

Keywords: *Hardware Crypto wallets; Crypto currency; Bitcoins; Block chain technology; Elliptic Curve DSA; SHA 256; Crypto attacks.*

1. Introduction

Bitcoin is a decentralized digital currency contemplated by a group of anonymous programmers under the pseudonym 'Satoshi Nakamoto', which could be the alternative for traditional currency with all the potential. Afteryears traverses after the development, bitcoin has grown in popularity in the financial field of research and technology [1]. As of December 13 2023, the price of bitcoin is $42,067.21[2]. Some researchers have proposed a distributed e-cash system that uses cryptographic techniques to sever the connection between individual Bitcoin transactions without the addition of trusted intermediaries. Using conventional cryptographic methods, this system enables entirely anonymous currency transactions that do not involve any additional trusted parties or third parties. It highlights zero coin's cryptographic construction and its performance both in terms of computation and effect on Bitcoin protocol [3]. The block body includes the counter for transaction and details of transactions. The number of transactions in a block depends on the size of the block and transaction size.

[1*] *Assistant Professor, Department of Electronics and Communication Engineering, Loyola-ICAM college of Engineering and Technology, Chennai-600034,Tamil Nadu,India.*
[2] *Student, Department of Electronics and Communication Engineering, Loyola-ICAM college of Engineering and Technology,Tamil Nadu, India.*
[3] *Assistant Professor, Department of Electronics and Communication Engineering, Loyola-ICAM college of Engineering and Technology Chennai-600034, Tamil Nadu, India.*
[4] *Assistant Professor, Department of Electronics and Communication Engineering, Loyola-ICAM college of Engineering and Technology, Chennai-600034,Tamil Nadu, India.*
** Corresponding Author Email: dhilip2711@gmaill.com*

Digital signatures based on asymmetric cryptography- are utilized in an unreliable setting. A pair of public and private keys are assigned to each user. The secret private key is used to sign the transactions. The details are decentralised as it is distributed throughout the network while transmission. There are two phases, signing phase and verification phase in the digital signature. The user who initiates transaction encrypts the information private key and the intended user receives the data and validates the result with public key. In that way, it can be easily checked whether the data is tampered or not [4].

Peer-to-peer (P2P) technology, used by Bitcoin, runs devoid of any centralized services like banks or notaries or other trusted third parties. Unlike traditional regional currencies, the owner has full control over the digital currencies and can use it ubiquitously without any centralised entities authority. Though it is decentralised, the transactions are secured cryptographically by the electronic payment system involving tokens called bitcoins [5]. The network of bitcoins and similar digital currencies can be interacted by users with an interface software client called wallets. Wallet maintains a ledger of all the transactions. The bitcoin holders can restore the digital currency in the wallet with a private key which is nothing but the bitcoin address of the transaction stored in wallets [6].

The two most significant security and privacy concerns that are currently faced by crypto currencies are those related to authentication and wallet key management. In digital signature algorithms, threshold secret sharing is

used. In which the secret value is split and given to different users with properties of information unaltered. The multiple device usage in the threshold secret sharing in turn harms the usability of the system.

Wallets are categorized into hot and cold. In cold wallets, it holds user deposits whereas in hot wallets, it is responsible for addressing withdrawal requests. The disadvantages of this strategy include 1) the existence of private keys on at least one cold device and 2) the exposure of all private keys to a single, trusted cold wallet administrator. Users' withdrawal requests are handled through the hot wallet. Users individually manage the destination addresses in hot wallet transactions, which are typically users' local wallets or accounts on other exchanges [7].

The existing crypto wallets are mostly cloud based as they are always connected to the internet and are prone to internet threats like malwares. In this paper, a secure wallet is proposed to store the crypto currency and to develop a Safe, Secure and Durable Wallet. Even though many products are present in the market similar to the design, they miss out on the convenience part of the wallet, nullifying the purpose of a crypto wallet.

- A more secure lightweight wallet is designed. It can be more conveniently carried everywhere and secure compared to the conventional hardware wallet and software-based wallet. The private is kept in secret devoid of attackers.
- The crypto wallet design constraints must be safe even in crucial environments thus an extra layer of protection is added to the device. This system will encrypt and secure the crypto wallet and to maintain a ledger of the transactions. It enables blockchain features in transmitting cryptocurrency.

2. Background of the research

A crypto wallet is a software program that allows users to store, manage, and transfer digital assets such as Bitcoin, Ethereum, and other cryptocurrencies. The wallet keeps the private keys that give users access to their digital assets on the blockchain network. These private keys function as passwords for the funds stored on the blockchain. A public address is also provided by a cryptocurrency wallet, and this address can be used to accept cryptocurrency from other users [8].

2.1 Types of Wallets

Hot wallets [9] are often more convenient and easier to use than cold wallets since they provide instant access to digital assets from any location with an internet connection. They are available via a web browser, a mobile app, or other applications. Yet, because they are connected to the internet, they are vulnerable to hackers and theft [10]. Desktop wallet is a crypto wallet installed on a desktop. It is considered more secure since it gives users total control over their private keys and does not rely on third party servers. Instead of requiring the user to download the complete blockchain, lightweight wallets rely on a remote server to give access to the blockchain. The well-known desktop wallets include Exodus, Bitcoin Core, and Electrum. Mobile wallets are similar to desktop wallets comes under the crypto hot wallets. They are easy to use and handy for sending and receiving cryptocurrencies, checking balances, and making transactions with enabled merchants. They are classified into two types: custodial and non -custodial wallet[11]. A few well-known mobile wallets are Mycelium Wallet, Trust Wallet, and Coinbase Wallet. Cold wallets are cryptocurrency wallets that keep private keys offline, making them less susceptible to hacking and theft. They are more secure than "hot" wallets, which are internet-connected and more prone to hacking and theft. A paper wallet is a physical printout that contains private and public keys that are used in transactions. The key generator creates random QR codes and alphanumeric strings. Paper wallets are the safest alternative for storing cryptocurrencies, but they are fragile and prone to wear and tear, fire, water damage and environmental factors [12]. A brain wallet [13] enables users to keep their private keys in their memory as opposed to a tangible object. The private key should be regularly backed up and kept in a secure place in case the passphrase is forgotten. Hardware wallets are a sort of cold wallet that employs a physical device to hold the private keys, such as a USB stick or a tiny hardware device. They offer an extra degree of protection by requiring a physical button push to validate transactions, and they frequently include advanced security features like two-factor authentication and PIN numbers [13]. Trezor, Ledger Nano S, and KeepKey[14] are examples of popular hardware wallets.

2.2 Attacks on Crypto Wallets

Since there is more demand for cryptocurrencies, particularly bitcoins, there are more security issues and attacks. Many nations and enormously large organizations have begun conducting business on the blockchain utilizing bitcoin to pay for their goods and services. People trust cryptocurrencies because it is challenging to introduce any security flaws into the blockchain [15]. Attacker tries to deceive users into disclose confidential information in a phishing attack. It entails making false phone calls or text messages appear to be from a trustworthy source, as well as sending fraudulent emails or messages that look to be from them. It is crucial to exercise caution when opening unwanted emails or messages, confirm the legitimacy of the sender and the website, enable two-factor authentication, and use different, strong passwords for each

account in order to safeguard against phishing attacks [16]. A type of attack known as "double-spending" on a network of digital currencies enables users to spend the same digital asset twice [17]. A 51% attack, a race attack, or a Finney attack are a few strategies that can be used to commit double-spending.

In a 51% attack, the attacker seizes the majority of the network's computing power, giving them the ability to undo transactions and possibly spend the same virtual asset twice [18]. When a group of hackers or a hacker holds more than half of the hash rate, the block chain network is subject to a 51% attack. By doing so, the attacker can forge a different chain that disregards earlier blocks and potentially bring down the entire network. A race attack involves the attacker starting two transactions to two different network nodes at the same time. The blockchain only stores the first confirmed transaction; all others are ignored. In order to spend the same cryptocurrency twice, the attacker wants to get one of the transactions confirmed while the other is rejected [19,20]. A sort of double-spending attack known as a Finney attack uses a flaw in the blockchain network to spend the same cryptocurrency twice. In a Finney attack, the attacker generates a second transaction spending the same cryptocurrency to themself after mining a block that contains a transaction sending money to an authorized recipient. The attacker broadcasts the second transaction to the network after the first transaction has been verified and put to the blockchain. A brute force attack in cryptocurrency is an effort to guess a user's private key by methodically attempting different combinations until the correct one is found. This is a time-consuming operation, but it is possible provided the attacker has sufficient processing power and time [21].

3. Sentinel- a secure wallet design

When the sentinel hardware crypto wallet device is injected into a computer, it will request for the biometric authentication from the user. As an additional security, it requires a 24-word recovery phrase as a password credential which is also known as a mnemonic or seed phrase. Even if someone could acquire the passphrase from human carelessness, one cannot bypass unique biometric authentication. So, no one could gain access to the hardware wallet, which possesses an extra layer of security. The device uses blue wallet, a watch only wallet which allows us to monitor our cold storage without having access to our private key. The process starts by plugging in the hardware wallet and the user is subjected to a two-step authentication process consisting of a biometric fingerprint scanner and a personal password. On confirmation, the wallet is directed to its interface wallet to access your coins present in the account which can be further sold or brought in through the application. The block diagram and inside view of developed sentinel wallet is shown in Figure 1 and Figure 2. The display acts as an interface to the processor by displaying various messages regarding the transaction or security of the wallet and the user's data. The schematic flow of encryption process in the proposed hardware wallet is shown in Figure 3.

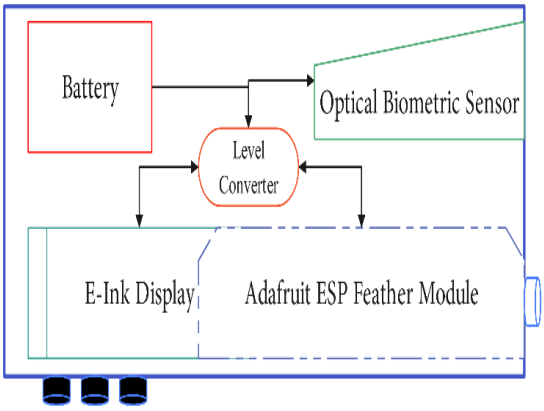

Figure 1: Block diagram of the Sentinel HyperPay wallet

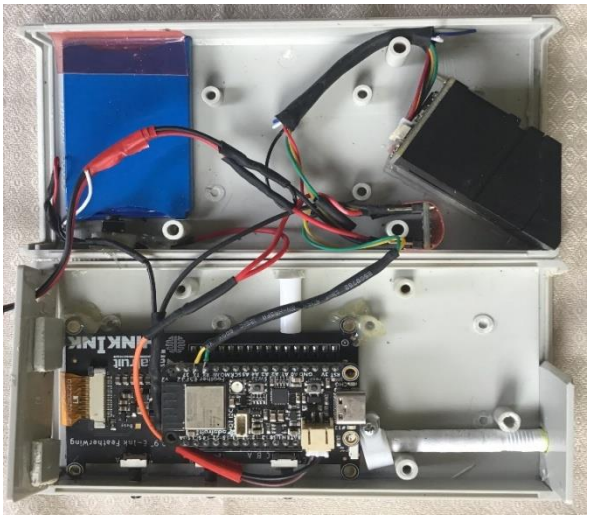

Figure 2: Inside view of the Sentinel HyperPay Wallet

4. Bluewallet

BlueWallet is the ledger management system used by Bitcoin traders [22]. BlueWallet is one of the crypto community's preferred solutions for storing their bitcoin because it allows for the management of various cryptocurrency wallets via an easy-to-use user interface and is compatible with the Lightning Network. It lacks educational resources and does not provide two-factor authentication. However, biometric verification measures are included to make it even more secure.

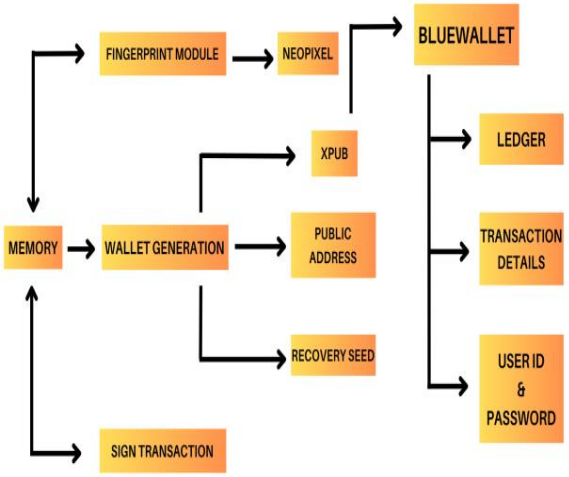

Figure 3: Flow diagram of Encryption process

BlueWallet's primary function is to sign Bitcoin transactions, and bitcoin owners can contribute the signatures required to approve a transaction. BlueWallet is not required to be linked to the Bitcoin network because another organization will oversee creating the unsigned transaction. This enables us to create a gadget with little memory and minimal power consumption. On BlueWallet, the user's private key that is required to sign a transaction is securely kept. The user can only unlock the private key if they input the PIN properly, and it never leaves BlueWallet. The user's private key, which is required to sign a transaction, is securely kept on BlueWallet and can only be opened by properly entering the user's PIN.

4.1 bluewallet registration

When a user selects the "Add now" button, they are given the choice to choose between the Lightning or Bitcoin wallet and to create a wallet name. The user can proceed to build the wallet after providing a wallet name and choosing a wallet type. The 24-recovery seed-words for the new wallet will then be required to be written down. Users who already have a bitcoin wallet and want to recover it should note that they can do so by selecting "import wallet" and inputting the 24 recovery seed words of that wallet. BlueWallet chose a traditional strategy. The user is only asked to jot down the 24 words on the screen. The seed-word count begins at zero instead of one, so it will be 0-23 seed-word. To avoid this poor security practice, the software blocks you from capturing a snapshot of the seed words.

4.2 Security

The private key of each unique public address the wallet creates will not ever need to be saved, so one does not have to. The private keys are really encrypted on your device and are only accessed when signing a transaction. If you misplace your wallet PIN or lose your phone, all that is required to restore your cash is the mnemonic recovery seed.Users of the wallet may use biometrics to unlock, erase, and export their wallets, as well as sign transactions. The ability to encrypt your wallets with an extra password is another feature of BlueWallet. It should be emphasized that if the wallet is encrypted with a password, biometrics will not be enough to decode it because they are regarded to be less secure than the password. Users of Blue wallet can choose a different password to decode a false wallet. In this manner, one can quickly input the password for the fictitious account if they were forced to release their wallet (wrench attack). You may imagine it as a fake wallet that you might carry around in your pocket and have $20 cash in. Only when wallet encryption has been set is this function available.

5. Cryptographies of bitcoin

Bitcoin cryptography is the core of the Bitcoin network's security and anonymity. It employs powerful cryptographic algorithms to assure transaction security and confidentiality. Bitcoin cryptography is built on public-key cryptography, which secures transactions with public and private key pairs. Public-key cryptography is used in Bitcoin to generate digital signatures that prove ownership of Bitcoins and authorize transactions. A public key and a private keypair are used to encode and decode the information by every Bitcoin user. Using complicated mathematical methods, the public key is obtained from the private key. Public key is used to produce a unique identifier called Bitcoin address for receiving payments.

When a Bitcoin user delivers Bitcoins to another user, they utilize their private key to establish a digital key. The digital signature and hashing involved is depicted in Figure 4. This digital signature includes transaction data as well as the public key. The digital signature canbe broadcasted to the Bitcoin network, where other users may verify it. Cryptography of bitcoin is a safe and anonymous method of transferring money over the internet. The bitcoin users can use the public key to decode and validate the digital signature.

The Hash generation in Figure 5 implies the complexity involved in generating the unique hash key which cannot be generated in reverse. The transaction gets uploaded to the blockchain [23], which is a decentralized public ledger, if the signature is legitimate. The transactions are validated by the proof-of-work and updated in the blockchain, guaranteeing that each block is distinct and cannot be changed without redoing the proof-of-work.

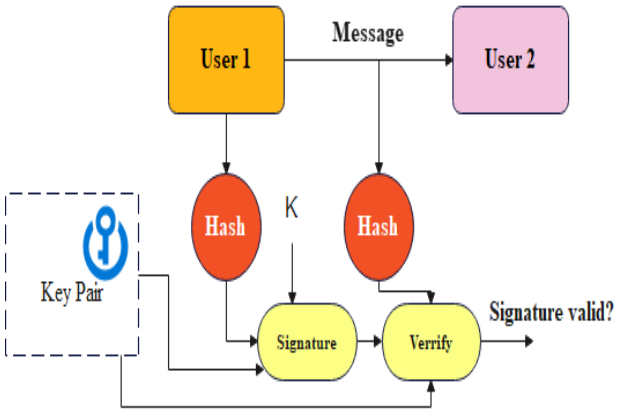

Figure 4: Digital Signature and Hashing

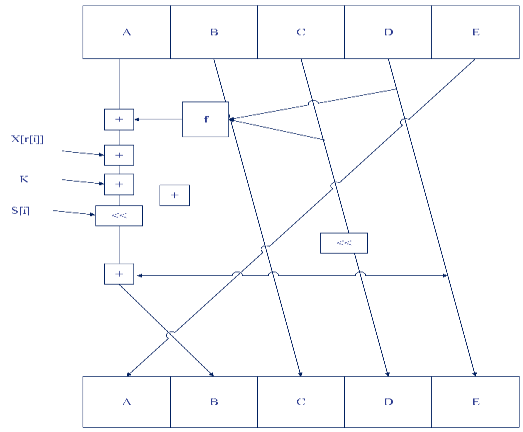

Figure 5: Hash Generation

6. Elliptic curve dsa

ECDSA (Elliptic Curve Digital Signature Algorithm) isenabled to safeguard transactions in the Bitcoin network. When one Bitcoin user wishes to send Bitcoin to another, they produce a transaction message that comprises the unique address, the number of bitcoins being delivered, and the sender's identity for authentication. ECDSA is used to generate the digital signature, which shows that the user is authorized for the transaction.

The user's private key is used to construct a unique key signature that is attached to the data to establish a digital signature using ECDSA [24]. ECDSA is based on elliptic curve cryptography, which generates public and private keys using mathematical curves. This approach is faster and more secure than typical public-key cryptography techniques. ECDSA is an important part of Bitcoin cryptography since it protects the integrity and security of Bitcoin transactions. Users may trust that their transactions are safe and authorized by the sender by employing ECDSA digital signatures.

7. Hash generation

When a user establishes a new Bitcoin wallet, the BIP39 standard is used to produce a 24-word seed phrase. Using the SHA-256 hash method [25,26], this seed phrase is utilized to produce a master private key. Using the BIP32 standard, the master private key is then utilized to build a hierarchical deterministicwallet. The HD wallet is used to generate numerous Bitcoin addresses and secret private keys for Bitcoin transactions. The SHA-256 and RIPEMD-160 (RACE Integrity Primitives Evaluation Message Digest) hash algorithms are used to produce each Bitcoin address, ensuring that the addresses are unique and safe. The RIPEMD-160 hashing algorithm is widely used in the cryptocurrency sector for creating addresses in Bitcoin and other cryptocurrencies. It is also supported by the BIP32 and BIP39 standards, which are commonly used in the building of bitcoin wallets.

When a user sends Bitcoin from their Wallet, the wallet software generates a transaction message that includes the recipient's address, the number of Bitcoin sent, and a digital signature created with the ECDSAand SHA-256 hash algorithm. The digital signature verifies and protects the transaction's integrity and security. Blue Wallet generates a unique hash key of the transaction data using the SHA-256hash algorithm [27]. The transaction data comprises the sender's and recipient's addresses, the amount of Bitcoin transmitted, and any other information such as transaction fees. The SHA-256 method is then used to combine and hash this data. The SHA-256 algorithm accepts any length message as input and returns a fixed-size 256-bit output. The input message is first padded to make it a multiple of 512 bits long. The appended message is then divided into 512-bit blocks, with each block undergoing a sequence of procedures to yield a final 256-bit output. The SHA-256 algorithm has numerous qualities that make it appropriate for use in cryptography. First, it is a one-way function, which means that determining the input message from the output hash is computationally impossible. Second, even little changes to the input message result in significantly different output hashes, making it impossible to counterfeit or edit the transaction data. Finally, the technique can enable transactions to withstand collision attackswhen two distinct inputs yield the same hash key as output. After hashing the transaction data using the SHA-256 technique, the resultant hash is signed with the ECDSA (Elliptic Curve Digital Signature technique) signature mechanism in Blue Wallet. The ECDSA technique generates a unique digital signature for the transaction private key, which can be verified using the public key. This guarantees the authorized transaction. and avoids manipulation or double-spending. Blue Wallet provides a strong and secure means to transmit, receive, and store Bitcoin by leveraging the SHA-256 algorithm to produce unique hashes of transaction data and the ECDSA signature technique to sign and validate transactions.

8. Sentinel work flow

The Processor (Adafruit ESP32 Feather V2) [28] shown in Figure 7a,band an EPD (Adafruit 2.9 E-ink Feather Wing

Display) [29, 30] shown in Figure 6a,b are the two primary components of the Wallet. A UART Biometric Fingerprint module is added for Wallet security, where the Biometric images are kept in encrypted form, protecting the system from data access. By circumventing the Fingerprint module, the user is presented to numerous quotes of notable inventors that are circulated one at a time every few minutes and set as a screensaver to save battery use and keep the machine at rest rather than going off after a few minutes of inactivity. The Adafruit ESP32 Feather V2 features an embedded Neo Pixel LED module on the processor board, which we used as a flashlight in case of faulty fingerprint identification, and the LED is also used as an indication in different tasks.

Figure 6a: Thin Ink E-paper display a)Front b)Back

Figure 6b: Thin Ink E-paper display a)Front b)Back

To begin with the Wallet Functions, a new wallet is created by following the instructions in the EPD, and this wallet may be used as a Burner Wallet since we can reset the system at any moment, and all this data is written on an SD card (optional). As soon as the wallet is created, 24 random phrases are produced, which serve as the wallet's recovery words. For security reasons, these phrases are not stored on the SD card and must be kept with user in secret. This is the most important phase in the wallet production process since anybody with these 24 words may access the wallet without even possessing the actual wallet. As a result, it is deemed necessary to safeguard the wallet recovery words.

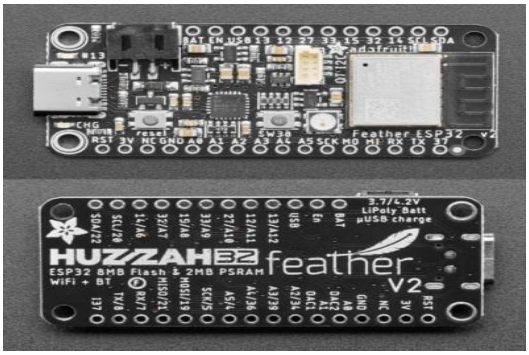

Figure 7: Adafruit ESP32 Feather V2a)top b)bottom

The XPUB (Public Key) of the newly produced wallet is kept when the wallet is generated and may also be presented as input into a watch-only wallet like BlueWallet in the future to access or see the wallet through the application's UI. Now that the wallet has been created, the user can view his blockchain address and verify it by logging in to the watch-only wallet, in this case BlueWallet. The user's Ledger can be saved on an SD card optionally. During a transaction, the user's address is converted into a QR code so that others can scan the QR code rather than entering the user's entire address manually. This QR code can be shown in the EPD or printed on an Optical Thermal Printer. Finally, during the final stages of the transaction, the user can physically sign the transaction on the wallet, avoiding all types of threats, even if the device containing the user's data in Watch-Only Wallet is hacked.

8.1. Xpub

The XPUB key functions like the master key, in that it can produce child public keys for each new cryptographic transaction [31]. A private key, and a public address are all required components of a cryptocurrency wallet. These components are just random strings of numbers and letters. The private key functions similarly to a password used to access information and resources in your wallet. Because having access to the private key enables a user to transmit money to other cryptocurrency wallets, the wallet owner must never divulge it to anyone. To use your cryptocurrency funds for transactions, on the other hand, you must share the public key with other users. A public key can be compared to an account number. Encrypted information can only be decrypted using your private key. When crypto is sent to a public key, only the wallet's owner with secret private key has access to it. The public address is a condensed version of your private key, consisting of fewer digits and characters. It defines where your bitcoin wallet is on the blockchain. Custodial wallets, mobile wallets, desktop wallets, and hardware wallets are all common types of bitcoin wallets. Each of them has a unique use case and safety profile. They each have a distinct use case and safety profile. The xPub (or Extended Public Key) of your wallet is the source of every public

address the wallet creates. Your wallet will use the xPub to create a new receiving address each time you receive money.

9. Results and Outputs

The proposed work presents the design and implementation of a hardware crypto wallet that utilizes a 2.9" grayscale e-ink display from Adafruit to provide a clear ad easy-to-read user interface. The crypto wallet is designed to be user-friendly and intuitive allowing seamless navigation and operation.

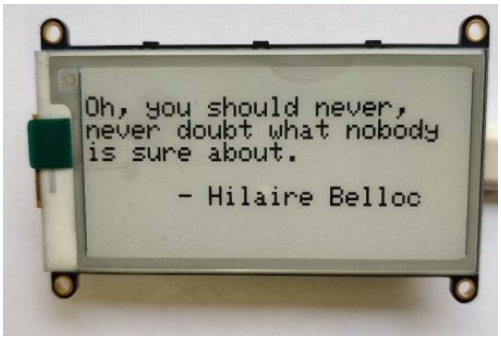

Figure 8a: Random quotes in display

The display in Figure 8a shows the numerous quotes of notable inventors that are displayed cyclically one at a time every few minutes and set as screensaver to save battery use and keep the machine at rest rather than going off after a few minutes of inactivity.

Figure 8b:User Menu

Figure 8c: Sentinel- Cased Wallet with Biometric

Figure 8b shows the user menu and Figure 8c shows the fully built wallet enclosed with switched case. A new wallet can be created by following the instructions in the Electronic Paper Display (EPD), and this wallet may be used as a Burner Wallet since we can reset the system at any moment, and all this data is written on an SD card (optional). To access the menu, the user must simultaneously press the three buttons located at the top of the device. Once the menu is displayed, the user can choose from a variety of options. Pressing the top left button allows the user to sign a transaction, while pressing the middle top button generates a new wallet. Finally, the top right button can be used to activate a flashlight, providing a useful feature for users who may need to access their crypto wallet in low-light conditions. The user interface of the sentinel is designed and developed to be simple usage with ease, making it accessible to both beginners and pro users. The grayscale e-ink display provides clear and easy-to-read text and graphics, while the three buttons on the top of the device allow for easy navigation and operation.

Figure 8d: Wallet Menu Accessing

Figure 8e: Public Address

Figure 8d shows the wallet menu and Figure 8e shows the public address generated. Upon pressing the top left button on the device by the user, the public address of the wallet will be displayed, providing the user with the information they need to receive cryptocurrency payments or transfers.

This feature is both easy to use and informative, allowing users to access important wallet information quickly and easily.

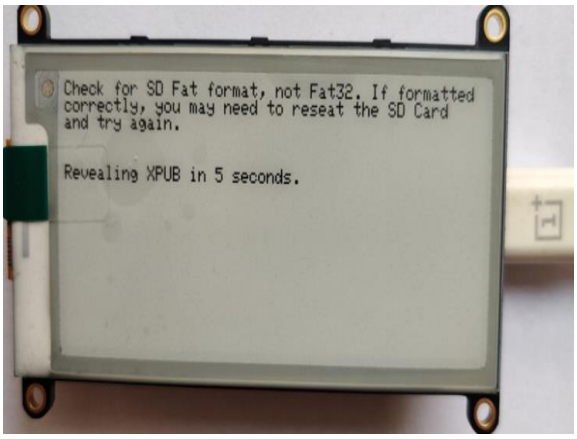

Figure 8f: Extended Public key generation

An instruction has been included that allows the user to display the extended public key of the wallet as shown in Figure 8e and Figure 8f, which can be used to access the BlueWallet application and view transactions. To do this, the user simply needs to press the top middle button on the device. Upon pressing the button, the extended public key of the wallet will be displayed on the screen. The user can then use this extended public key to access the BlueWallet application on their mobile device or computer. In the BlueWallet application, the user can view their transaction history and manage their cryptocurrency assets. Figure 8g shows that the String of Extended Public Address.

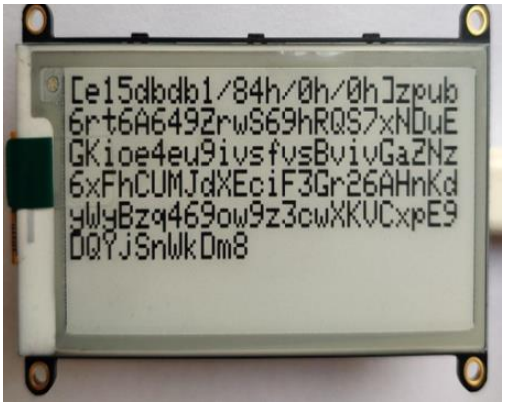

Figure 8g: String of Extended Public Address

By pressing the top right button in Wallet, it shows the private recovery phrase which is the wallet's recovery words as shown in Figure 8h.

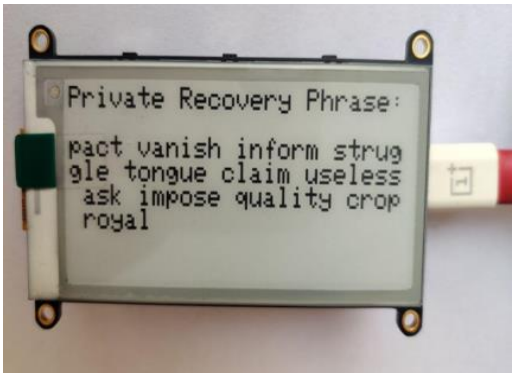

Figure 8h: Private Recovery Phrase

A fingerprint module has been attached to enhance the security of the wallet as an additional layer of protection as shown in Figure 8i, making it more difficult for unauthorized users to access the contents of the wallet. To use the fingerprint module, the user simply needs to place their finger on the sensor. The module will then scan the fingerprint and compare it to previously stored fingerprints to authenticate the user. If the fingerprint matches, the user will be granted access to the wallet. If the fingerprint does not match, the user will be denied access. This feature provides several benefits. Firstly, it ensures the authorized access of the wallet. This is important because cryptocurrency assets can be very valuable, and unauthorized access could result in significant losses. Secondly, the fingerprint module is easy to use, which encourages users to implement strong security measures. Finally, the module adds an additional layer of security that is difficult to bypass, making it an ideal choice for those who prioritize security. The front view of cased Sentinel HyperPay wallet is shown in Figure 9.

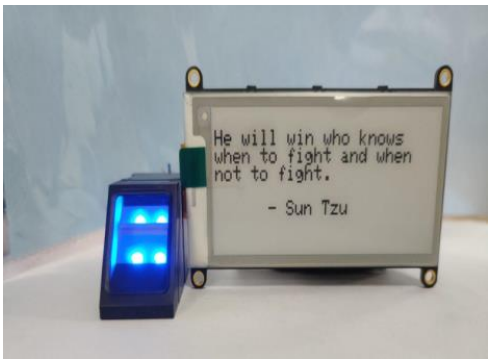

Figure 8i: Hardware Wallet with Finger Print Module

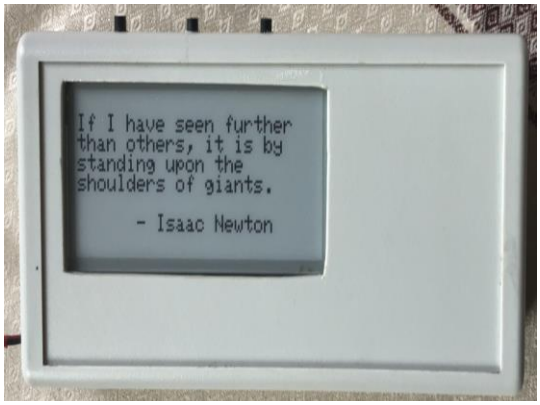

Figure 9: Cased Hardware Wallet- Sentinel-Front view

10. Conclusion

The use of hardware wallets is increasingly becoming popular in securing cryptocurrency assets. This paper focused on the development of a hardware cryptocurrency wallet that features a secure mechanism to protect users' digital assets from unauthorized access, hacking, and other security threats. The proposed solution utilized an Adafruit 2.9" Grayscale eInk, ePaper Display FeatherWing [29, 30] and Adafruit ESP32 Feather V2 [28] microcontroller, and a fingerprint sensor to ensure top-notch security. The hardware wallet developed in the work addresses the vulnerabilities and threats associated with traditional software wallets by providing a high level of security, convenience, and ease of use overcoming the shortcomings of previous wallets. By incorporating a secure element chip and utilizing BIP39 for seed recovery, the wallet ensures that users' private keys are well-protected and can be easily recovered in case of any unforeseen events. Additionally, the use of a fingerprint sensor enhances the security of the wallet, as only authorized users can access it. The combination of the fingerprint sensor, secure element chip, and BIP39 ensures that users' digital assets are well-protected against hacking, theft, and other forms of cyberattacks. Overall, the proposed hardware wallet solution demonstrates the importance of incorporating security mechanisms in cryptocurrency wallets to protect users' digital assets from security threats. The use of secure element chips, fingerprint sensors, and BIP39 for seed recovery are some of the ways that can be utilized to improve the security of cryptocurrency wallets. Sentinel provides a foundation for further research and development of secure hardware wallets for cryptocurrency storage and management.

References

[1] S. Nakamoto, 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. *Decentralized business review* pp.1-9,

[2] *Coindesk Bitcoin price website*https://www.coindesk.com/price/bitcoin/[Last Accessed 13th December 2023].

[3] I. Miers, C. Garman, M. Green and A. D. Rubin, 2013. Zerocoin: Anonymous Distributed E-Cash from Bitcoin. *In 2013 IEEE Symposium on Security and Privacy, Berkeley, CA, USA*, pp. 397-411.

[4] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, 2017. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *In 2017 IEEE International Congress on Big Data (BigData Congress)*, Honolulu, HI, USA, pp. 557-564.

[5] M. Conti, E. Sandeep Kumar, C. Lal and S. Ruj, 2018. A Survey on Security and Privacy Issues of Bitcoin. *IEEE Communications Surveys & Tutorials*, 20(4), pp. 3416-3452, Fourthquarter doi: 10.1109/COMST.2018.2842460.

[6] D. Rai, M.P. Shetty, G.L. Alva, A. Hedge and M. Shiran, 2018. Wallet for Bitcoin Cryptocurrency. *International Research Journal of Engineering and Technology*, 05(07), pp.2465-2467.

[7] S. Ebrahimi, P. Hasanizadeh, S.M. Aghamirmohammadali and A. Akbari, 2021. Enhancing Cold Wallet Security with Native Multi-Signature schemes in Centralized Exchanges. 23, pp.1-13.16.

[8] S. Suratkar, M. Shirole and S. Bhirud, 2020. Cryptocurrency Wallet: A Review. *In 2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP)*, Chennai, India, pp. 1-7.

[9] H. Rezaeighaleh, 2020. Improving Security of Crypto Wallets in Blockchain Technologies. *Electronic Theses and Dissertations*.

[10] M. Azman and K. Sharma, 2020. HCH DEX: A Secure Cryptocurrency e-Wallet & Exchange System with Two-way Authentication. *In 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)*, Tirunelveli, India, pp. 305-310.

[11] Diego Geroni, 2021 Different Types Of Crypto Wallets – Explained https://101blockchains.com/types-of-crypto-wallets/[Last Accessed 13th December 2023].

[12] "Paper Wallet: A Crypto Relic or Still ─ Relevant?" 2022 Available: https://learn.bybit.com/crypto/crypto-paper-wallet/ [Last Accessed 13th December 2023].

[13] M. Vasek, J. Bonneau, R. Castellucci, C. Keith, and T. Moor, 2017. The Bitcoin Brain Drain: Examining the Use and Abuse of Bitcoin Brain Wallets. *Lecture Notes in Computer Science*, 10, pp.609-618.

[14] Trezor, 2020. https://www.fxempire.com/crypto/wallets/trezor. [Last Accessed 13th December 2023].

[15] M.S. Pedro, V. Servant, C. Guillemet, 2019. Practical side-channel attack on a security device, https://ieeexplore.ieee.org/document/9021685

[16] V. Bhavsar, A. Kadlak and S. Sharma, 2018. Study on Phishing Attacks, *International Journal of Computer Applications*, 182, pp. 27-29. 10.5120/ijca2018918286.

[17] G. Karame, E. Androulaki and S. Capkun, 2012. Double-spending fast payments in Bitcoin. *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 906-917.

[18] F. A. Aponte-Novoa, A. L. S. Orozco, R. Villanueva-Polanco and P. Wightman, 2021. The 51% Attack on Blockchains: A Mining Behavior Study. *IEEE Access*, 9, pp. 140549-140564, 2021, doi: 10.1109/ACCESS.2021.3119291.

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

[20] S. Aggarwal and N. Kumar, 2021. Chapter Twenty-Attacks on blockchain. *Advances in Computers, Elsevier,* 121, pp:399-410.

[21] H. Rezaeighaleh and C. C. Zou, 2019. New Secure Approach to Backup Cryptocurrency Wallets. *In 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA*, pp. 1-6.

[22] "BlueWallet Crypto Wallet" Marco Monroy Robles, 2023 Available: https://money.com/bluewallet-crypto-wallet-review/ [Last Accessed 13th December 2023].

[23] S. P. Gupta, K. Gupta and B. R. Chandavarkar, 2021. The Role of Cryptography in Cryptocurrency. *In 2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC*), Jalandhar, India, pp. 273-278.

[24] B.K. Kikwai, 2017. Elliptic Curve Digital Signatures and their application in the Bitcoin Crypt-currency transactions. *International Journal of Scientific and Research Publications*, 7(11).

[25] SHA-2 Standard, National Institute of Standards and Technology (NIST), Secure Hash Standard, FIPS PUB 180-2, www.itl.nist.gov/fipspuhs/fip180-2.htm

[26] N. Sklavos and O. Koufopavlou, 2003. On the hardware implementations of the SHA-2 (256, 384, 512) hash functions. *Proceedings of the 2003 International Symposium on Circuits and Systems,* 2003. ISCAS '03., Bangkok, Thailand, pp. V-V, doi: 10.1109/ISCAS.2003.1206214.

[27] M. Parmar, and H.J. Kaur, 2021. Comparative Analysis of Secured Hash Algorithms for Blockchain Technology and Internet of Things. *International Journal of Advanced Computer Science and Applications*. 12. 10.14569/IJACSA.2021.0120335.

[28] KattniRembor, Adafruit ESP32 Feather V2, https://www.adafruit.com/product/3405 [Last Accessed 13th December 2023].

[29] M. LeBlanc-Williams, Adafruit 2.9" eInk Display Breakouts and FeatherWings: Easy E-paper with built in memory. https://learn.adafruit.com/adafruit-2-9-eink-display-breakouts-and-featherwings [last updated on Sep 22, 2021].

[30] Lady ada, (2022, Dec, 01), Adafruit eInk Display Breakouts and FeatherWings [Web]. Available: https://cdn-learn.adafruit.com/downloads/pdf/adafruit-eink-display-breakouts.pdf [Last Accessed 13th December 2023].

[31] Understanding the xPub and address generation https://support.blockchain.com/hc/en-us/articles/4417077967508-Your-Wallet-Its-Master-Seed-How-do-they-work-[Last Accessed 13th December 2023].