# Enhancement of digital signature algorithm in bitcoin wallet

**Farah Maath Jasem[1], Ali Makki Sagheer[2], Abdullah M. Awad[3]**
[1,3]College of Computer Science and Information Technology, University of Anbar, Iraq
[2]Al-Qalam University College, Kirkuk, Iraq

**Article Info**

***Article history:***

Received Apr 24, 2020
Revised Jun 4, 2020
Accepted Jul 31, 2020

***Keywords:***

Bitcoin
ECDSA
Key management
Privacy
Wallets

## ABSTRACT

Bitcoin is a peer-to-peer electronic cash system largely used for online financial transactions. It gained popularity due to its anonymity, privacy, and comparatively low transaction cost. Its wallet heavily relies on elliptic curve digital signature algorithm (ECDSA). Weaknesses in such algorithms can significantly affect the safety and the security of bitcoin wallets. In this paper, a secure key management wallet was designed based on several changes in the wallet parts. In the cold wallet, we employed an image-based passphrase to achieve a strong entropy source of master seed. The hot wallet, the proposed Key_Gen algorithm is modifying to the key generation step of the ECDSA that it is to generate a fresh key pair at each transaction. The final part ensures recovering all keys on both hot and cold wallets without daily backups in case of losing the wallet. The findings prove that the proposed cold wallet is resisting against a dictionary attack and overcoming the memorizing problem. The proposed hot wallet model acquires good anonymity and privacy for bitcoin users by eliminating transaction likability without additional cost. The execution time for signing a transaction of the proposed model is~70 millisecond, which is then important in the bitcoin domain.

***Corresponding Author:***

Farah Maath Jasem,
College of Computer Science and Information Technology,
University of Anbar, Ramadi, Iraq.
Email: farahmaath86@uoanbar.edu.iq

## 1. INTRODUCTION

The emergence of the internet and technology during the last decade largely contributed to the growth of the economy worldwide, from management of finance to how businesses abroad operate [1]. Recently, technology had yet changed the financial world with a proposition of electronic currency which is becoming a more attractive system for banks, investors, and even developers [2, 3]. Such progress in methods of payments potentially decreased transaction costs, effort, and time, and further, laid the foundation for new forms of currencies, namely digital currency such as bitcoin cryptocurrencies. In turn, the term cryptocurrency stands for digital currency based on the principle of cryptography; it is the combination of two words; currency with cryptography. The general public may confuse cryptocurrency with Bitcoin since many cryptocurrencies exist nowadays [4, 5]. However, all cryptocurrencies share the same underlining principles of being decentralized digital currency [6, 7].

Bitcoin created as an alternative to fiat currencies by an unknown computer scientist called the pseudonym Satoshi Nakamoto. Currently, it occupies the largest market share among other digital currencies and is “mined” using computing power in a distributed peer-to-peer global network of volunteers. At its core, Bitcoin is nothing more than a digital file lists every transaction that has ever happened over the network, a public ledger called the “Blockchain” [8, 9]. The main components of the bitcoin system are wallets, peer to peer (P2P) bitcoin network, miners, and blockchain [10, 11]. However, a bitcoin wallet relies on public keys cryptography for user authentication, which allows the user to spend any bitcoin associated with those keys. Loss of the private keys effectively means loss of funds and exposure of the public keys conveys. Moreover, bitcoin provides a limited form of transaction unlikability [12, 13]. An attacker can use blockchain to recursively link the history of the user's transactions to a valid bitcoin address [14-16] hence, user privacy. Moreover, the security of ECDSA and the bitcoin wallet keys management are the most important security and privacy issues at present in the cryptocurrency. This paper aims to study the bitcoin system design and analyze its strengths and weaknesses with attention given to key management issues, enhancing the security of ECDSA through increasing the security space of key bits. In order to avoid the weaknesses of the conventional passphrases and solving the challenge of remembering password used in brain wallets through using a new image-based approach, enhancing anonymity and privacy of the user in the bitcoin payment system by eliminating internal likability of bitcoin transactions. Finally, the recovery of cold and hot wallet keys is without the requirement of a cold wallet. The rest of the paper is organized as follows: section 1 is the introduction and section 2 cover the related work. Section 3 presents the details of the design and implementation of the proposed. Section 4 presents the results that are obtained, and section 5 presents the conclusions of this paper.

## 2. RELATED WORK

Researchers in this domain effort focused either on the security or privacy of the bitcoin wallet. Enhancing digital signatures was studied by [16]. They designed implemented and evaluated a two-factor based secure bitcoin wallet, using digital signature algorithm (DSA) and elliptic curve digital signature algorithm (ECDSA). Threshold secret sharing is the method of splitting a secret value which can be given to different participants while preserving the following two properties: (i) any subset of shares can reconstruct the secret, as long as the size of the subset equals or exceeds a specified threshold (ii) any subset of shares smaller than this threshold together yields no information about the secret. Using two-factor authentication can also help in backing up and later recover any lost key(s). Moreover, the proposed solution store backups of each share independently to minimize the chances of both being stolen. The main drawback of threshold schema is the use of multiple devices which in return harms the usability of the system since coins can no longer be spent without operating multiple devices.

Further, the additional operational complexity is required for signing transactions, especially for fast payment transactions. An approach and proposed an improved weight threshold ECDSA to secure bitcoin wallets. The algorithm distributes a portion of the private key over a group of individuals/users which guarantees no complete access given to any user within the group. While individuals can be arranged into separate groups with different weights, individuals within the same group have the same weight and those having greater than or equal to a threshold value of that group only are authorized to reconstruct the secret key [17]. Weights and keys management of each group and its participant is the main drawback of this schema. Dikshit and Singh enhanced the weighted threshold ECDSA scheme by suggesting that all players should get a single share, thus, to accomplish the requirements of weight. However, the enhanced schema is only feasible for players within the same group. In other words, it does not support collaboration among players from different groups to reconstruct the key [18].

On the other hand, and since the proposal of brain wallet, it became the subject of several academic studies with much focus given to newly added features, Mnemonic words. Volety *et al.* examined and studied the security of two publicly available bitcoin wallets (multi-bit HD and electrum). It was carried through implementing a software package to perform a dictionary attack to crack the master seed of both selected wallets. Moreover, steps in the proposed system were: (i) extract the dictionary, (ii) create the combinations for a dictionary file, and (iii) check for the correct MS. Thus, they succeeded in restoring and crack several user wallets, which were able to identify more than one combination of a given 12 words (Seed) successfully in a short time, However, the findings of this research are only limited to these two bitcoin wallets [19].

O. Hsama proposed a steganography technique to embed the MS bits stream into steganography fractals. The mnemonic bitstream is hidden by discretizing the angles and lengths of the tree branches. Which each tree node can hold a single ASCII character (1 byte). The tree can then be printed without the fear of being lost or stolen [20]. However, the researcher in this paper focuses on solving the memorizing problem of the MS only. The advantage of this approach is that it is a little cost. After a seed is generated in an offline computer as part of the wallet setup, it will need a bit more of typing/writing to do on the backup paper. However, the main drawbacks of the proposed approach are: (i) it needs a tree of five levels to represent MS of 50 bytes on contrast the research results prove lower accuracy, whereas the tree grows up three levels; and (ii) the proposed approach does not solve the salt problem. Besides, it is just a piece of paper that would be hence susceptible to be damaged or lost.

## 3. THE PROPOSED KEY MANAGEMENT MODEL

The proposed key management schema is illustrated. Several proposed changes are aspired to increase the security of the bitcoin wallet against several known attacks. Moreover, overcoming the drawbacks of the standard model in the hot wallet, the cold wallet, and MS memorization. The proposed schema consists of three main correlated parts: cold wallet, hot wallet, and recovery wallet. The sending coins from Alice to Bob are achieved with respect to the following steps. Firstly, when the payee (Alice) needs to pay some bitcoins to any vendor (Bob), the payee is required to set up the proposed cold wallet in which the user must specify the number of keys (passwords). The second step is the setup of the hot wallet to send and receive bitcoins. The proposed hot wallet generates a new pair of keys for every bitcoin transaction using the selected imported keys from the cold wallet (paper wallet) and address book. Then the newly computed private key is used to sign the transaction. Moreover, the signature's public key is attached in the transaction token before it is announced to the bitcoin P2P network. The public key is used to verify the transaction by the vendor. Therefore, the proposed hot wallet address book contains all vendors bitcoin addresses that wallet owner had sent coin(s) to with a special counter attached to each address to denote the total number of exchanges occurred. Finally, the proposed recovery wallet needs to use stego image and address book to recover cold wallet passwords and then the complete hot wallet keys' hierarchical. Figure 1 show the proposed key management model.

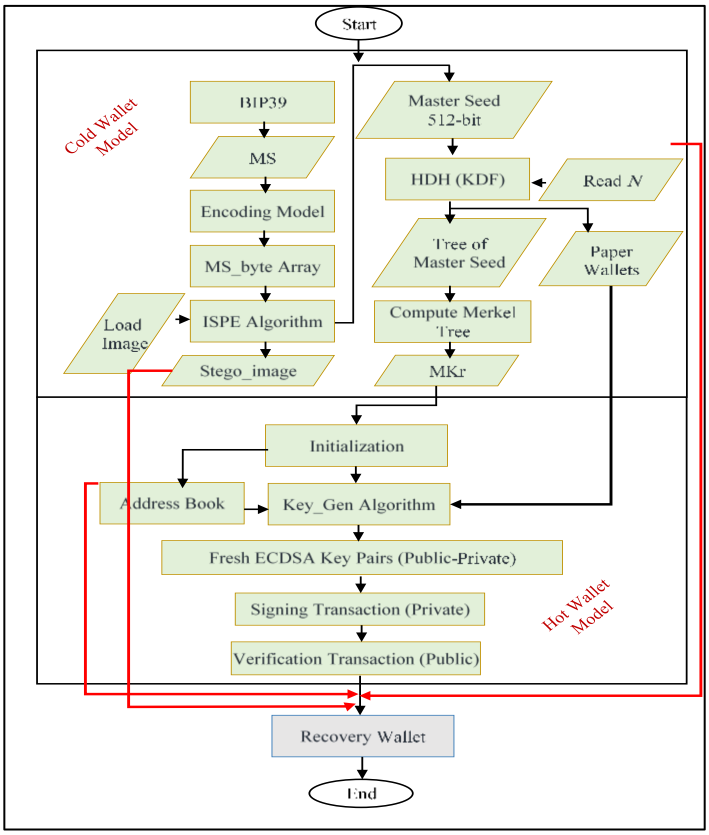

Figure 1. The proposed key management model

### 3.1. Proposed cold wallet model

Cold wallet model is encompassed of five main steps, in which, several updates were made to the original model to overcome the drawbacks of the cold wallet original model. In the first step, MS_byte is generated by a modified BIP39 that it supported the Arabic language with the new encoding system [21]. The second step, Master seed generation is one of the important factors to realize a secure bitcoin wallet is to generate the master seed of high entropy, ISPE algorithm is proposed to steganography the encoded bytes in an image selected by the user. ISPE uses the LSB algorithm to hide the encoded bytes of MS. Then, the master seed is generated using HMAC512, which accepts two inputs, *Key* and *Data*. The proposed schema suggests that *Key* is SHA256 string computed from the stego image while *Data* is the SHA256 string of encoded bytes of the generated mnemonic words. Algorithm 1 summarizes the proposed schema.

```
Algorithm 1: ISPE
Input: passphrase encoded bytes, select Color image ($img$).
Output: master seed sequence of 512-bit hex characters.
Start
Step 1. $\boldsymbol{img}$ = load the cover image
Step 2. $\boldsymbol{Data} = SHA256\ (\boldsymbol{MS\_byte})$.
Step 3. Embedded (Bitmap $\boldsymbol{img}$, $\boldsymbol{X}$) and return Bitmap stego image ($\boldsymbol{Stego\_img}$).
Step 4. Save the steog image (($\boldsymbol{Stego\_img}$) as .BMP which must be kept in secure cold
    storage.
Step 5. $\boldsymbol{Key} = SHA256\ (\boldsymbol{Stego\_img})$.
Step 6. $\boldsymbol{Master\ seed} = HMAC512\ (\boldsymbol{key}.\boldsymbol{Data})$
End
```

Note, LSB algorithm calls embedding function is to hide 3 bits from MS byte per one pixel of the select image. However, if MS is encrypted with a weak key (salt), the dictionary attacker who has all the wordlists ' combinations and the weak salts will perform a simple matching process to get the master seed. Hence, the entire wallet is cracked. Moreover, the user is likely to forget MS, salt or both resulting from losing his/her wallet in its recovery status. So, the researchers used an image-based approach to produce salt with high entropy bit and achieved an effective solution to challenges the security of the brain wallet. The main reason regarding the use of LSB to hide MS is to ensure salt uniqueness. In case any user has the same image in the bitcoin network would never be generating the same salt. The third step, HDH child key derivation, proposes merging the concept of secret passphrase from a deterministic wallet to ensure seeds with high entropy with the hierarchy property of HD wallet to ensure ease of recovery. Due to deterministic wallet uses a secret passphrase defined by the wallet owner every time a new pair of keys is derived. In contrast, the HD wallet favors the hierarchy derivation of keys.

HDH starts with a single master seed, which is the output of the previous phase of the cold wallet. Then generating several enumerated child keys as multi passphrase but in HD derivation. The derivation based on BIP32 except for the index number. An index is a $2^{32}$ + N, where N begins from zero to the number of private keys that the user required. The ability to manipulate the index allows the extension and creation of sequent child keys from a single parent, e.g., Child 0, Child 1, Child n. To generate the tree of keys, it needs extended master private ($Ext_k$), and then the HMAC algorithm is applied with the following inputs: Hash function: SHA512; Key: chain code; Message: $Ext_k\ +\ I\ where\ I{=}2^{32} + i\,, i = 0 \leq n$. The fourth step, Merkle tree root hashed (MKr) value for a list of private keys from HDH to be used as the second input seed to generate any key in the hot wallet. The final step is Importing private Keys Passphrases are then selected and assigned to be used as the master private key to generate different keys for any payment type in the hot wallet.

```
Algorithm 2: HDH function
Input: Master _seed (512 bit), entered number of keys N
Output: Tree of deterministic private keys.
Start
Step 1. Read N
Step 2. New_master = master_ seed;
Step 3. index = $2^{32}$
Step 4. For  I = 0 to N
    $private\_left = New\_master(0,31)$ - The first 32 byte from master seed.
    $codechain\_right = New\_master(32,63)$ - The last 32 byte.
                      $Hash\_message = HMAC512(codechain\_right).(private\_left||Index)$
    $Increment\ Index\ by\ one$ ;
    $New\_master = Hash\_message$
    Print the ($private\_left$) as private key for level I
        End For
End
```

## 3.2. The proposed hot wallet model

In the hot wallet, the first part is the wallet initialization, which includes all the steps above such as the selection of language and number of mnemonic words, generate and save the secure image, and the number of passwords in a cold wallet, Merkel root, and creation of empty address book. In the second step, the user should select and export change and fast payment keys to the user hot wallet. Users with already configured wallets can immediately start sending and receiving bitcoins logging in and synchronizing their address book. Moreover, The address book is among the changes proposed in this work for the hot wallet. It is composed of a list of entries, each of which describes the information of the individual vendor. An address book entry is composed of three fields, the receiver bitcoin address, special counter, and type of payments; $fast$ type means fast payment whereas $slow$ means slow payment. At every transaction, the receiving address is checked first in the address book, if it is found, the counter is increased by one. Otherwise, an entry is added, holding the new address with a counter value set to zero. Changes made to address books are immediately synchronized.

The second part is the key generation algorithm in the proposed wallet is redesigned to eliminate internal likability for users in the P2P bitcoin network such that new fresh keys are generated and used for every bitcoin transaction (sending and one for receiving change). The proposed Keygen takes four unique seeds: (i) The secret passphrase from user HDH wallet as seed1 (paper wallet), (ii) $MKr$: Merkle root as seed2, (iii) Receiver bitcoin address stored under $R\_Add$ in the address book as seed3, (iv) The counter associated with $R\_Add$ in the address book. Use of counter to ensure that seed 1, seed 2, and seed 3 are always hashed to a unique value called seed 4. Seed 1 defines the type of use for the newly generated key, whether to send bitcoin (slow or fast payment) or to receive change from the already sent coins. Algorithm 3 summarizes the proposed Key_Gen method. As illustrated, this step is generated by two private keys. The first key will be used to sign the transaction for the sending process. Moreover, the second key is used to sign the change transaction that returns by the p2p network.

```
Algorithm 3:- The proposed key_ Gen Method
 Input: MKr, secret passphrase, Receiver address ($R\_Add$), and counter ($C$).
Output: Two private key in Base58 format
Start
 Step 1. $seed1s$ = scan the secret passphrase from fast paper wallet.
 Step 2. $seed1c$ = scan the secret passphrase from change paper wallet.
 Step 3. $seed2$ = get  $MKr$.
 Step 4. $seed3$ = get $R\_Add$ from address book.
 Step 5. $seed4$ = get the corresponding counter $C$ from address book.
 Step 6.   $S1 = combine\ (seed1s||seed2||seed3||seed4)$
 Step 7.   $S2 = combine\ (seed1c||seed2||seed3||seed4)$
 Step 8. $S\_byte1 = convert\ (S1)\ to\ array\ of\ byte$
 Step 9. $S\_byte2 = convert\ (S2)\ to\ array\ of\ byte$
 Step 10. $d1 = (SHA256(S\_byte1))$ mod n
 Step 11. $d2 = (SHA256(S\_byte2))$ mod n
 Step 12. Return $(d1, d2)$
End
```

### 3.3. The proposed wallet recovery model

The proposed HDH connect cold and hot wallets where the deterministically derived passphrases in the cold wallet are further used to generate keys in the hot wallet. Therefore, the recovery of a user wallet is two steps process. Each step and show how the recovery is simplified due to the proposed image-based approach. The proposed cold wallet recovery model requires the stego image used by the wallet owner. The recovery is a straightforward process and it can be followed as:

a. Load $stego\_image$.
b. Call image steganography passphrase decryption (ISPD) function ($Extraction(Stego\_image)$). This function applies the LSB extraction method to return a string of bytes of the MS that was encoded. The encoding.
c. If the language of MS was Arabic, then "$Encoding.Unicode$" the function is called lead to obtain Arabic words equivalent to message bytes. Otherwise, "$Encoding.UTF8$" is called.
d. Generating master seed of cold wallet is the next step after MS recovery. It follows the same procedure explained previously in Algoritm 1. Then, the proposed model uses the passphrase key for the HMAC512 algorithm which form ally is an optional choice for the user.
e. To derive the tree of the primary secret keys, HDH is called. However, the number of keys $N$ in the tree will be requested from the user. The computation of MKr should conclude the cold wallet recovery.

Recovery of hot wallet consists of recovering all slow, fast, and change keys. After the recovery of the cold wallet keys' tree and Merkel root value is recomputed. The user is prompted to sync the user address book and reselect the keys used previously for the hot wallet.

## 4. RESULTS AND DISCUSSION

This section is divided into three main parts; the first part deals with the proposed cold wallet model. The second part presents the results of the proposed hot wallet model. Moreover, discussing the security criteria of the proposed key management models along with the standard bitcoin key management. Finally, the comparisons of the proposed key management models with the key management introduced in the literature were obtained. In order to evaluate the performance and the quality of the ISPE algorithm. The obtained stego images are used in different languages. Three widely used standard images are selected to test the proposed model. Namely Lena 400x400, airplane 512x512, and frog 1118x1105. There are many of the well-known objective measures for the image quality after the embedding process was used as mean square error (MES), peak signal to noise ratio (PSNR) [22].

$$MSE = \frac{1}{M*N} \Sigma_{i=1}^{M} \Sigma_{j=1}^{N} [I\ (i,j) - I^*\ (i,j)]^2 \qquad (1)\ [23],$$

where M and N are the size of the image. I (i, j) is the value of the pixel located at (i ,j) position in the original image and I*(i ,j) is the corresponding pixel in the stego image.

PSNR in (2) is a numerical measure that is used to calculate the ratio of noise occurred in the encrypted image and it is caused by the implementation of the encryption technique on the source image. The acceptable value must be greater than 28.

$$\text{PSNR}=10 * Log_{10} \left|\frac{Max}{MSE}\right|^2 \qquad (2)$$

where $MAX$ is the maximum pixel value of the image, and MSE is from (1)

Table 1 shows the MSE and PSNR value measured between the original and the stego, which are computed by applying (1) and (2) respectively, encryption/decryption time of the selected images with different data sizes. According to PSNR, measures show that ISPE algorithm preserved image quality after encryption, all above 45dB for both languages. It is also shown that the accumulative square error values are acceptable and stable even when choosing different $n$ of words. Generally, when the payload is increased, MSE will be increased and consequently decreased PSNR, and vice versa.

Table 1. ISPE algorithm results

| Image/Language | Data size | PSNR | MSE | Encryption time | Decryption time |
|---|---|---|---|---|---|
| Lena | 153 | 45.1839 | 0.1546 | 80 | 90 |
| Airplane | 112 | 45.1826 | 0.1472 | 109 | 107 |
| Frog | 234 | 45.2887 | 0.2269 | 189 | 190 |

Moreover, estimating or measuring password strength (resistance to guess, and key randomize) is essential to many security specialists to protect against malicious theft and attacks on user's accounts. The results of the measuring salt strength by using two significant tests, the NIST test measures the salt randomization [12], and the Zxcvbn test (measures the salt cracking time [24]. Since the NIST entropy formula was maybe poor predictors of actual cracking time, therefore Zxcvbn will be used. After embedding different lengths of MS from Arabic and English dictionary using proposed ISPE, salt in 64 hex format passphrases (256 bit) is then generated respectively. In the NIST test, if the p-value$\geq$ 0.01, then the test sequence is considered to be pseudo-random. The nature of all salt is a short sequence. Therefore, the tests that examine the sequences longer than 100,000 bits are excluded and hence one is left with the frequency test; the frequency test within a block; runs test; test for the longest run of ones in a block; serial test, this test produces two P-values called serial-1 and serial-2; approximate entropy test; and cumulative sums test this test produces two P-values called FORWARD and REVERS. The test was performed using the salt bits as parameter inputs, where the salt size was 256 bits. The results in Table 2 indicating that the tests meet the requirements of NIST test randomness, and all p-value is also in an acceptable range. Moreover, it was noted from the experiments that high entropy images always generate a high entropy salt and vice versa.

Moreover, Zxcvbn is a password strength estimation tool used by many due to its speed and accurate measures. A rank of five levels plus estimation information is the nature of the output of the Zxcvbn tool for a given tested password. Last, several passphrases from the simple questionnaire and generated passphrases tested with the Zxcvbn tool. The test shows that users' selected passphrases are very weak to normal with 95% and 90% pass ratio against unthrottled online and offline attacks. However, they perform poorly with only a 20% pass rate against offline fast hash attack. Besides the NIST and Zxbncv tests results for the proposed cold wallet, it is important to add the following factors: First, in the ISPE, a stego image is considered a good pseudo-random number generator (PRNG) for the hash function to generate a stable salt, and it ensures the user uniqueness. If the salt length is at least 16 bytes and was generated with a cryptographically secure PRNG which is what is wanted for a salt. Since every generated salt is some number of $2^{256}$, which technically requires atomically fast computing power capable of generating trillions of possibilities to be able to circulate through an approximately of $10^{77}$ possible instance. Second, the proposed ISPE prevents standard dictionary attacks against weak salt. Due to the number of possible attempts to break the master seed for any language are huge: Number of possible $=2^{256} * 2048^{n_{word}}$, where $n\_word$ equal to (12, 15, 18, 21, 24) word sequences. Third, the proposed HDH schema adds an extra level of security to the bitcoin wallet that collectively disrupts the steps required for an attacker to succeed. In that, instead of a single point of attack to prevent the attacker. The adversary has to compromise multiple aspects of the wallet in order to gain full access, such as paper wallet, MKr cold wallet value, an address book that is located in the cloud. Finally, the proposed model eliminates the daily storage processes, which could be in danger as well as the consumption of storage space. On the other word, assumes that the user has been purchasing ten times a day, the user will need ten keys. So it should all are stored and daily backup, which is considered storage concerns.

Table 2. NIST test function result of the ISPE salts (Lena)

| Test | | 12 | 18 | 24 |
|---|---|---|---|---|
| Name | | English | English | English |
| Apn | | 0.904400 | 0.983586 | 0.948018 |
| Freq_b | | 0.825761 | 0.568090 | 0.267422 |
| Cum | Cum-F | 0.745642 | 0.803522 | 0.906386 |
| | Cum-R | 0.857965 | 0.857965 | 0.974204 |
| Freq | | 0.500524 | 0.617075 | 0.600524 |
| longest | | 1.000000 | 1.000000 | 1.000000 |
| Run | | 0.060643 | 0.695792 | 0.616366 |
| Serial | Serial_1 | 0.257573 | 0.316603 | 0.807037 |
| | Serial_2 | 0.327285 | 0.853253 | 0.529713 |

### 4.1. Evaluation criteria based on key management framework

The key management evaluation framework proposed by Eskandari [25], is a multi-criteria-based framework used to evaluate the security and usability of bitcoin key management approaches. The framework contains ten criteria; namely (a) malware resistant, (b) key stored offline, (c) no trusted third party, (d) resistant to physical theft, (e) resistant to physical observation, (f) resilient to password loss, (g) resilient to key churn, (h) immediate access, (i) no new user software, (j) cross-device portability. The proposed model evaluated according to those factors and compared with the currently important bitcoin wallet. Black dot (•) in Table 3 means that the schema satisfies the denoted property, while the circle (°) means partial satisfaction of the corresponding property. However, a blank means that the system does not satisfy this property.

According to the definition of malware resistant (the first criteria), the proposed HDH schema fully satisfies this factor since the cold wallet is not stored on any internet-connected device and it is only used once it used to compute the hot wallet’s keys. The infrequently used hot wallet keys are not archived to the offline storage. Therefore, the proposed schema of the hot wallet partially satisfies the second criterion. The third criterion, the proposed hot wallet, does not depend on a trusted third party to maintain signing authority over the user’s bitcoin; all signatures are dependent on enhanced multi-factor based ECDSA algorithm. The fourth criterion, since the stego image and wallet address book, will be safely stored in a cloud-based location and are only accessed during wallet recovery. The physical theft of media or devices that hold cryptographic wallet keys is nearly impossible. Besides, and for the same reason, the wallet is resistant to physical observation, where the attacker can perceive the cold wallet keystrokes or QR code, which may result in access to the user’s bitcoin wallet.

Wallet resilience to password loss (the sixth factor) is an important criterion that should be satisfied by all wallets. Losing a password may result in some bitcoin becoming unrecoverable. When a client sends bitcoin change to a newly-created change address, a wallet is key churn resilient. If and only if it can maintain access to the funds even after exhausting the initial key pool. In other words, all previously and newly created change addresses must always be kept accessible to the wallet. Although many of the reviewed wallets by Eskandari *et al.* satisfy this criterion, it is challenged by the cost of storage. The proposed hot wallet is not only resilient to key churn but it also storage effective. Due to the enhanced Keygen function, the wallet can virtually access all previously created change addresses via direct local-computation of designated change address without accessing any local or remote storage. Further, it enables direct access of key management to the bitcoin wallet, which helps bitcoin transactions to be performed immediately. Moreover, the proposed wallet is software and hardware-independent, which means any of the currently used wallets can adopt the proposed schema with no platform dependency nor specialized hardware required. Therefore, the proposed approach is fully satisfying "No New User Software" and "cross-device portability criteria," the ninth and tenth criteria in Table 3.

Table 3. Comparison of bitcoin key management techniques contrasted with proposed key management

| Category | Example | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Mix | Proposed | • | ○ | • | • | • | • | • | • | • | • |
| Local storage | Bitcoin core |  |  | • |  | • | • | • | • |  |  |
| Offline storage | Bitaddress | ○ | • | • |  |  | • |  |  |  | • |
| Password-derived keys | Brainwallet |  | • | • | ○ |  |  | • | • | • | • |
| Hosted wallet | Blockchain.info | ○ | ○ |  |  | • | • | • | • | • |  |

## 5. CONCLUSION

This paper concludes that is by improving the key management schema. The ECDSA will be enhanced. There is no doubt that the strength of any algorithm is heavily dependent on the security strength of the key management. Thus, a secure key management model to the bitcoin wallet was designed. After simulating and implementation of the proposed work. A modified multi-factor Key_Gen algorithm enhances the wallet security by increasing the keyspace against the bad K ECDSA Known attacks. Moreover, the proposed model eliminates internal likability through the generation of new hot change and hot fast and slow payment keys for each transaction, so this leads to increase privacy and anonymity. A proper storage and recovery for bitcoin hot wallet by the proposed hot Key_Gen function was designed to keep a fixed number of keys in the hot wallet. Meaning, previously used hotkeys can be directly recalculated when needed without the need to store them in the hot wallet. Thus, there is no backup required. During wallet restoration, stego image and wallet address book are used, and all passwords are recalculated through HDH schema, then hot wallet keys are derived. Overall evaluation is done; it was found that the proposed ISPE does not affect the quality of the image. Moreover, this proposal leads to open a new research area to apply different image steganography techniques in this domain. Key management achieves nine out of the ten security evaluation criteria when compared with existing bitcoin key management techniques. In conclusion, the proposed wallet in this work does not require additional fees, mixing services, and it is hardware and software independent.

## REFERENCES

[1] S. Nakamoto, "Bitcoin : A Peer-to-Peer Electronic Cash System," *Satoshi Nakamoto Institute*, pp. 1-9, 2008.

[2] H. Abdullah and A. H. Ibrahim, "Blockchain technology opportunities in kurdistan, applications and challenges," Indonesian Journal of Electrical Engineering and Computer Science, vol. 18, no. 1, pp. 405-411, April 2019.

[3] E. P. E. Deepika and E. R. Kaur, "Cryptocurrency: Trends, Perspectives and Challenges," *International Journal of Trend in Research and Development,* vol. 4, no. 4, pp. 4-6, 2017.

[4] A. Biryukov and S. Tikhomirov, 'Security and privacy of mobile wallet users in Bitcoin, Dash, Monero, and Zcash', *Pervasive Mob. Comput.*, vol. 59, 2019.

[5] D. I. Wang, "Secure Implementation of ECDSA Signatures in Bitcoin," *MSc in Information Security,* pp. 1-78, 2014.

[6] S. Alani, Z. Zakaria, and M. M. Hamdi, "A Study Review on Mobile Ad-Hoc Network : Characteristics , Applications , Challenges and Routing Protocols Classification," *International Journal of Advanced Science and Technology*, vol. 28, no. 1, pp. 394-405, 2019.

[7] H. L. H. S. Warnars, Y. Lanita, A. Prasetyo, and R. Randriatoamanana, "Smart integrated payment system for public transportation in jakarta," *Buletin of Electrical Engineering and Informatic,* vol. 6, no. 3, pp. 241-249, 2017.

[8] J. Bucko, D. Pal'ová, and M. Vejacka, "Security and Trust in Cryptocurrencies," in *Central European Conference in Finance and Economics*, pp. 14-24, 2015.

[9] S. Goswami, "Scalability Analysis of Blockchains Through Blockchain Simulation," *Bachelor of Technology-Computer Science*, University of Nevada, Las Vegas, pp. 1-58, 2017.

[10] S. Alani, Z. Zakaria, and H. Lago, "A new energy consumption technique for mobile Ad-Hoc networks," *International Journal of Electrical & Computer Engineering,* vol. 9, no. 5, pp. 4147-4153, Oct 2019.

[11] A. Houria, B. M. Abdelkader, and G. Abderezzak, "A comparison between the secp256r1 and the koblitz secp256k1 bitcoin curves," *Indonesian Journal of Electrical Engineering and Computer Science,* vol. 13, no. 3, pp. 910-918, 2019.

[12] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid, "Recommendation for key management part 1: General (revision 3)," *NIST Special Publication*, vol. 800, Part 1, no. 57, pp. 1-147, 2012.

[13] H. Hosseinian, H. Shahinzadeh, G. B. Gharehpetian, Z. Azani, and M. Shaneh, "Blockchain outlook for deployment of IoT in distribution networks and smart homes," International Journal of Electrical and Computer Engineering, vol. 10, no. 3, pp. 2787-2796, June 2020.

[14] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, "Bitcoin and Cryptocurrency Technologies," *Princeton University Press*, 2016.

[15] A. M. Fahad, A. A. Ahmed, A. H. Alghushami, and S. Alani, "Detection of Black Hole Attacks in Mobile Ad Hoc Networks via HSA-CBDS Method," in *Springer Nature Switzerland*, Springer International Publishing, vol. 866, pp. 46-55, 2019.

[16] S. Goldfeder *et al.*, "Securing Bitcoin wallets via a new DSA/ECDSA threshold signature scheme," pp. 1-26, 2015.

[17] P. Dikshit and K. Singh, 'Weighted threshold ECDSA for securing bitcoin wallet', *Accent. Trans. Inf. Secur.*,

vol. 2, pp. 43-51, 2016.

[18] P. Dikshit and K. Singh, ‘Efficient weighted threshold ECDSA for securing bitcoin wallet’, in *2017 ISEA Asia Security and Privacy (ISEASP)*, pp. 1-9, 2017.

[19] T. Volety, S. Saini, T. McGhin, C. Z. Liu, and K.-K. R. Choo, “Cracking Bitcoin wallets: I want what you have in the wallets,” *Future Generation Computer Systems,* vol. 91, pp. 136-143, Feb 2019.

[20] O. Hosam, “Hiding Bitcoins in Steganographic Fractals,” *2018 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT)*, Louisville, KY, USA, pp. 512-519, 2018.

[21] A. M. A. Farah Maath Jasim Ali Makki Sagheer, “Enhancing The Security Of The Bitcoin Wallet Master Seed,” *College of Computer Science and Information Technology,University of Anbar*, Ramadi, Iraq, pp. 609-615, 2019.

[22] S. Eskandari, D. Barrera, E. Stobert, and J. Clark, “A First Look at the Usability of Bitcoin Key Management,” in *arXiv*, vol. 8, no. 7, pp. 1-10, 2015.

[23] A. M. Odat and M. A. Otair, “Image Steganography using Modified Least Significant Bit,” *Indian Journal of Science and Technology*, vol. 9, no. 39, pp. 1-5, 2016.

[24] D. Wheeler, “zxcvbn Realistic password strength estimation,” *Dropbox Tech Blog,* April, 2012.

[25] S. Eskandari, J. Clark, D. Barrera, and E. Stobert, “A first look at the usability of bitcoin key management,” *arXiv*, pp. 1-10, 2018.

## BIOGRAPHIES OF AUTHORS

**Farah Maath Jasem** was born in Iraq-Anbar in 1986. She received her B.Sc. of Artificial Intelligence in Computer Science Department at the University of Technology (2008)-Iraq, M.Sc. in Data Security from the University of Anbar (2019)-Iraq. she is interested in Cryptology, Information Security, and Image Processing.

**Ali Makki Sagheer** was born in Iraq-Basrah in 1979. He got on B.Sc. of Information System in Computer Science Department at the University of Technology (2001)-Iraq, M.Sc. in Data Security from the University of Technology (2004)-Iraq and Ph.D. in Computer Science from the University of Technology (2007)-Iraq. He is interested in Cryptology, Information Security, Cyber Security Number Theory, Multimedia Compression, Image Processing, Coding Systems and Artificial Intelligence. He published more than seventy papers in different scientific journals and conferences twenty-four of them are published in Scopus. Finally, he obtained Professor's scientific degree in Cryptography and Information Security since 18 Jul 2015.

**Abdullah Mohammed Awad** was born in Iraq-Ramadi 1955. He got on B.Sc. of Electrical Engineering Department at the University of Technology (1977)-Iraq, M.Sc. in Image Processing from the University of Anbar (2005)-Iraq and Ph.D. in Computer Science from the University of Technology (2016)-Iraq. He is interested in Cryptology, Information Security, and Image Processing.