10.7251/ZRSNG1801102J

Analysis and security of crypto currency wallets

Stevo Jokić, Sinergija University

A digital wallet is an electrical device or application trough which users can preform different types of transactions. They are divided into two categories of cold and hot digital wallets. The first category includes digital wallets that require an internet connection and the second category includes digital wallets that do not require internet connection. When selecting a wallet, it is necessary to determine the purpose of using a wallet and then make a purchase. The use of digital wallets is reflected in various characteristics. The convenience of using the ability to execute a mobile phone transaction in matter of seconds. Efficiency is reflected in the speed of transaction execution. Data organization is one of the key features of digital wallets. The cost of using digital wallets is far less than the traditional way to carry out transactions, which includes different commissions and payments. Security of digital wallets is at high level. Every day there is a growing need for their use because of security, speed, transactions between two users without third party assistance. This paper describes the current state of digital wallets on the market, the choices of a better solution for purchasing and using digital wallets, security of digital wallets and future trends in their development.

Keywords **– Digital wallet; Cryptowallet; Cryptocurrencies; Security; Transactions**

I. TYPES OF DIGITAL WALLETS

A digital wallet for cryptocurrencies is a software program that holds public and private keys and successufully works on different blockchains which allows users to exchange currencies between each other and to keep track of the balance of their currency. A digital wallet can store, send and receive different currencies. Crypto currencies are not stored as physical (fiat) money within the wallet. Every transaction is recorded and stored in the blockchain. Sending a bitcoin or some other currency to a user would mean sending out your own public key. If the user should receive the payment his private key must be in accordance with the sender's public key. There is no real exchange of coins. The transaction was conculded with a record in the blockchain and a change in user digital wallet. [1]

These keys are part of the science called cryptography. There are two basic models for security symmetric and asymmetric model. The symmetric model usually comes with secret key and asymmetric model comes with public and private key. The focus will be on asymmetric model, because this model is commonly used in completing cryptocurrency transactions. Asymmetric encryption is an encryption model that uses different encryption and decryption algorithms as well as two keys that are linked with each other (private and public key). The sender should have a copy of the public key of the recipient., but in that case it must be considered that the attacker has the same copy. In this case, the sender encrypt the message with the proper algorithm for encryption, and the recipient has the ability to decrypt the message with his private key. So the purpose of this asymmetric model is that the attacker can not decrypt a message which is encrypted by the public key. [2]

Cryptocurrency wallets can be divided in two major categories and they are: cold wallets and hot wallets. The difference between two of them is that for hot wallets is necessary an internet connection and for cold wallets not. Hot wallet users usually use to buy something on the internet and hold a small amount of money for that purpose, while cold wallet is just like vault in the bank to store different kind of digital values. The best thing is to have both wallets mainly for security reasons.

Hot and cold wallets can be divided into several categories. Online wallets, hardware wallets, mobile wallets, paper wallets and desktop wallets. Online, mobile, desktop and multisignature wallets belongs to a hot wallet category and hardware, paper belongs to a cold wallet category. Depending on the choice of digital wallet, each has its own level of security to ensure to protect the private key.

Multisignature wallets: In order access funds after completing a transaction trough multisignature wallet it will need two or three private keys depending on the level of security. This practice is good for companies to give a reponsibility to a differenet employees which means they all need to give their private key to gain access to funds. Example of multisignature wallet is BitGo where user store one key, second key is stored by a person of trust and the third key is kept by company itself. [3]

Online wallets: Access to this type of wallets can be a via web browser. These wallets are vulnerable, so it is not recommended to store a larger amount of crypto token to this wallet.
Advantages:

- Transactions are completed in short amount of time
- Recommended to store a small amount of cryptocurrency
- Some of these digital wallets are suitable for storing several different cryptocurrencies and making transfer beetwen them
- Possibility of using TOR network for more privacy

Disadvantages:

- The full control of digital wallet is in hand of third party or central authority
- To use a digital wallet is recommended to use a personal computer and it is neccesary instaling security software
- Lack of knowledge in information technologies leads users to the risk of various online frauds

Mobile wallets: With the use of mobile wallets user have an access at every place with internet connection.
Advantages:

- More useful and easier to use than other types of crypto wallets
- Possibility of using the TOR network for more privacy
- A great feature is using QR code for scanning

Disadvantages:

- Mobile phones are insecure devices. A user can lose his crypto tokens if the phone becomes compromised.
- They are susceptible to malware, key logger and viruses

Desktop wallets: is considered safer than the previous two wallets, but that can depend in the field of security for securing online crypto wallets.
Advantages:

- Very easy to use this type of wallet
- Private keys are stored on the user's computer

Disadvantages:

- If a computer has a connection to the internet it becomes vulnerable and requires more security
- Regular backup is necessary because in some point system may break down and all data can be lost

Higher level of security for desktop wallets can be possession of an older laptop with clean operating system. This kind of laptops can implement a cold storage method. The concept of cold storage in cryptocurrency is for users who want to store their digital assets in a very long time. There are several types of laptops that can be used as a cold storage for crypto currencies. That laptop's only purpose should be for storing digital assets or a lightweight crypto mining rig. It should have a safe operating system such as MacOs, Ubuntu or ChromeOs (Chromebook). The first convenient crypto laptop is Xiaomi Air with a fingerprint sensor as an extra layer of security. Price range for this laptop start's at 900$ and represent a good investment. Second best investment in crypto laptop would be buying Huawei MateBookX13 with starting price range at 800$. At this moment Huawei company is making these laptops only with the windows operating system. The third and the cheapest laptop is Asus Chromebook Flip with the highest price range of 500$. This is the best-selling lapotp with a ChromeOS which is very secure. It has an ability to work with other USB crypto wallets.

Hardware wallets: are in most cases safer wallets. It's usually a USB device with a software in it. Some of them have a screen which means the user doesn't need a computer to complete a transaction. This type of wallet offers more control over the user's criptocurrency and represent a proper solution for storing digital assets for a long time.
Advantages:

- The most secure USB wallets are with the screen on it
- Safer than all the other types of wallets

Disadvantages:

- Very difficult to buy
- It's not recomened for beginners

Paper wallets: This is the safest wallets that exist. They belong to cold storage wallets. As the name says, paper wallet is a piece of printed paper with public and private keys. The paper has a QR code which represents the user keys and can be used for any transactions. The only concern of the user should be to keep that peace of paper and that is why is this type of wallet the safest.
Advantages:

- Stored in the user pocket or physical wallet without any connection to the computer

Disadvantages:

- It takes more time to complete the transaction

Multi-currency wallets can be a good investment for users who want to trade with various currencies. Bitcoin is the first currency, but there are hundreds of different currencies in the market and every one of them has a different infrastructure network. [4]

II. THE BEST DIGITAL WALLETS ON THE MARKET

Before choosing a cryptocurrency wallet important thing to know is that the digital currency is in some countries banned or restriced and some countries allows its use and trade. It could happen to choose a wrong wallet for certain digital currency and to lose the money. Recommended thing for users is to take some time in researching of how different types of crypto currency wallet works. Here is a list of a few popular different wallets: Ledger Nano S (hardware wallet), Ledger Blue (hardware wallet), Coinpayments (online wallet), Exodus (online wallet), Jaxx (mobile wallet).

Ledger Nano S is a hardware digital USB wallet made for crypto currencies. Although hardware wallets are more expensive than the other type of wallets it is a cost-effective investment with a lot of different features. Special attetion is devoted to a security and the backup of the private key. To start this device computer is unnecessary. It has a small screen in the front of the device so the user can manage without any difficulties. Various functions are available such as exchanging digital currencies, transferring money from account to account etc. Figuer 1. shows Ledger Nano S digital wallet.

[1]

Figure 1. Ledger Nano S

Ledger Nano S have two sizes. 98 mm is the bigger device and the smaller device is 60mm. The main features of this hardware wallets are:

- Multi-currency wallet – This wallet has an ability to store many different popular crypto currencies in the same wallet
- Small screen – User can watch on-going transactions and use the button to verify them.
- User-friendly – No matter the device is small, user can still operate comfortably
- Safety measure – For this purpose there is plenty options for security as well as option to lock the wallet using a pin code
- Backup and recovery – In case of losing crypto currency money restoration process is very fast

Ledger Blue is also the hardware wallet made by the same company. It is much more superior than Ledger Nano S with a lot of new options. By reason of these features this wallet is among the most expensive wallets on the market. Figure 2. shows Ledger Blue digital wallet.

[2]

Figure 2. Ledger Blue

The most important security features are shown below:

- Security – Ledger blue wallet is based on dual chip technology and has an integrated firmware for protection of digital currencies
- Resistant to malicious software – this wallet can not be hacked which means that it is 100% resistant to malicious software
- Pin code – user can set 4 to 6 digits code to limit outside access

Coinpayments is an online digital wallet. They reached the level of popularity when they achieved that their wallet can store more than 300 different crypto currencies. The only fee they got is when user completes the transaction through their wallet. Based on so many different currencies as this wallet is accepted in many online stores, so it is possible to use this wallet to purchase online. Coinpayments has a greate security features:

- BitGo services is integrated into this wallet to ensure a high level of security and to make transactions a lot faster.
- Safe – this feature is included with the purpose to protect user's money from thieves
- Multi-currency wallet – An ability to store different currencies in the same wallet
- Common – Often used in thousands of online stores for online purchasing

Exodus is another web-based digital wallet with amazing design, reporting system and it is easy to use. The great thing about Exodus when compare it to other web wallets it has the similar features and maybe some better than others. Figure 3. Shows Exouds interface wallet.

Figure 3. Exodus wallet interface

[3]

There are many features that this wallet gives but here is the list of the best security features:

- Multi-currency wallet – storing multiple different crypto currencies in the same wallet along with other digital assets without additional fee
- Security – Even though this is an online wallet, at the same time is an offline wallet because when wallet is created the information are stored on the user's computer
- Free registration – Everyone can fill out the form and become an owner of this type of cryptowallet

Jaxx is mobile digital wallet, but also can be called as a desktop wallet because it also works on Windows operating system as same as on mobile devices. Jaxx is created for all digital assets make them secure from hackers. Todays' mobile wallets offer many security features in case the user losese his phone. In that case they allow you to switch to another account. Features of Jaxx wallet are:

- Full control – When a private key is being created it's been stored at the user's comptuer, so even Jaxx company can't see the user's digital funds.
- Easily operated – Usually the online wallets demand a lot of steps to make the transaction. Jaxx model is

[1] https://www.ledgerwallet.com/products/ledger-nano-s
[2] https://www.ledgerwallet.com/products/ledger-blue
[3] https://www.exodus.io/#

based on Nada privacy model. This model protects confidentiality and privacy.

- Acceptable – Jaxx can be implemented on every major operating system

III. DIGITAL WALLETS SECURITY

The crypto wallet as well as the real plastic wallet can be secured. In the case of the most popular crypto currency Bitcoin there are different data transfer functionalities. These thigns can be security issue but Bitcoin includes very high level of security which implies their proper use. When it comes to placing money on onlline platforms attention should be focused on their security. In case of buying wallet for this crypto currency, it is recommended to use two-factor authentication. Smart way of storing money in the wallet can compare with physical wallet. This means that the digital crypto wallet should contain a small amount of money for everyday use.

Backup wallet is just another expression for storing money to some other place or making a copy. Backup wallet can prevent problems that arise form a computer errors or data theft, but this request can be fulfilled if the data is encrypted.

Data stored on the network is not one hundred percent secure. Any computer connected to the neetwork can be affected by malicious software. An important safety practice is that data should be encrypted to avoid any chance to be compromissed. Data should be stored in several different locations. When it comes to different locations, it's not just about online storage, but also on hardver devices such as usb, cd, external hard drive etc. Regular backups or daily backups ensures that you always keep your data fresh.

Encryption is a very important for digital wallets. Encrypting digital wallet is one of the best ways to secure your funds which are stored inside the digital wallet. In this way, a password is set if someone tries to accces the digital wallet. Password must not be lost because if that happens the funds will be lost. The difference between the crypto currency and the real money is that if a loss password occurs, user can make a request to get a new password. In blockchain and crypto currency user has full responsibility. It is very important to create a strong password which includes letters, characters, numbers.

Another way of storing and securing data is to use cold wallets. These wallets are hardware wallets which do not have a connection to the internet. Offline transaction signing involves two computers sharing parts of the same digital wallet. The first computer should be disconected from any network and only this computer contains a complete digital wallet and have an authoriztation to sign the transaction. The second computer has connection to the network and and contains the digital wallet only for watching and can create unsigned transactions. The transaction can be done in a few steps:

1. Create a new transaction on the computer that is connected to the network and store it on a usb drive.
2. Sign a transaction with the computer that is not connected to the network.
3. Send the signed transaction with computer that is connected to the network.

The digital wallet software version should always be updated because every time when software is updated user will receive an important security updates. Updates can include some new features for digital wallet, it can prevent different problems various severity and many other things.

Crypto wallets can use a mulitple signature feature where multiple approvals are required for transaction to be spent. This type of protection can be used in bigger organizations such as banks where employees have access to it's treasury. Web wallets also include multi signature feature. [5]

CONCLUSION

For the current year 2018 it is predicted that the use of digital wallets for crypto currencies will increase and that the use of physical wallets will be reduced. The most popular crypto currency Bitcoin reaches the highest record profits and slowly gets a reputation as legitimate currency. Based on the research so far it can be concluded that these wallets are very safe as well as suitable for use as the additional costs are minimal in relation to the costs when paying with physical money. Payment in crypto currencies provides these minimum costs because two nodes that execute a transaction operate directly where there is no inclusion of a third party. The only cost is payment to the network in which the transaction is exectued for example bitcoin network. Depending on the speed of transaction execution, there are different fees (in dollars per transaction) but they are much lesser than the payment in the standard way.
According to Wallet Investor investing in Bitcoin would be a smart 1-year investmen decision. 1 BTC worth is 6,656 dollars at 15/10/2018. Future forecasts for bitcoin are good. By 2023, it is expected that the value of one bitcoin will be 18,585 dollars. By investing $100 for 1BTC you could by 0,156BTC, and a long-term forecast for that same amount of money by 2023. would be $279,2. Current price for 1BTC is $6,411.120.

REFERENCES

IV. References

[1] BlockGeeks, „BlockGeeks," [Na mreži]. Available: https://blockgeeks.com/guides/cryptocurrency-wallet-guide/.

[2] S. A. Mladen Veinović, Kriptologija 1, Beograd: Univerzitet Singidunum, 2013.

[3] Coti. [Na mreži]. Available: https://medium.com/cotinetwork/the-difference-between-hot-and-cold-wallets-in-the-digital-currency-world-1aa6f957ddd1 .

[4] H. laptop. [Na mreži]. Available: https://hobowithalaptop.com/crypto-wallets .

[5] [Na mreži]. Available: https://bitcoin.org/en/secure-your-wallet#update .