Cryptocurrency Wallet: A Review

Saurabh Suratkar
Department of Computer Engineering,
Veermata Jijabai Technological Institute,
Matunga, Mumbai, India
suratkarsaurabh@gmail.com

Mahesh Shirole
Department of Information Technology,
Veermata Jijabai Technological Institute,
Matunga, Mumbai, India
mrshirole@it.vjti.ac.in

Sunil Bhirud
Department of Computer Engineering,
Veermata Jijabai Technological Institute,
Matunga, Mumbai, India
sgbhirud@ce.vjti.ac.in

2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP) | 978-1-7281-6509-7/20/$31.00 ©2020 IEEE | DOI: 10.1109/ICCCSP49186.2020.9315193

***Abstract*—A blockchain is a growing list of records, called blocks, that are linked using cryptography. Blockchain private and public keys are stored in a cryptocurrency wallet, but not the actual currency values. Wallets provide customers with the ability to send and receive virtual currency / tokens and tune their balance through interaction with blockchains. Multi-currency wallets may be broken down into 3 categories: software, hardware, and paper. Software wallets are web, mobile and desktop. Growing penetration of blockchain in many industries makes one to understand wallets in detail. There are a variety of wallet kinds to pick out from. This paper focuses on multi-currency wallets review exploring on features like supported currencies, anonymity, cost, platform support, key management, wallet recovery methods and fiat currencies supported.**

***Index Terms*—Blockchain, Multi-currency wallet, software and hardware wallets, wallet features.**

I. INTRODUCTION

Blockchain software is an immutable database with secured access by design. It is an open, distributed ledger that can record transactions, which are verifiable, between parties effi-ciently. A blockchain is commonly managed through a peer-to-peer network forming a disbursed ledger, all peers together ad-here to a protocol for inter-node communication and vali-dation of new blocks. A valid data is recorded on blockchain with consensus of network and linked with hash of previous blocks thus it becomes immutable record. Hence, a recorded block can't be altered retroactively without alteration of all next blocks. Although blockchain statistics are unalterable, blockchains could also be taken into consideration steady by layout and exemplify a disbursed computer gadget with high Byzantine fault tolerance [26].

Cryptocurrency wallets (crypto-wallets) are key to use blockchain. Every user, who intend to use blockchain platform for any transaction, has to use crypto-wallet. Unlike traditional pocket wallets, cryptocurrencies are not stored in crypto-wallets. In fact, cryptocurrencies are neither stored in any single area nor exist anywhere in any bodily form, but it exists as data of transactions stored on blockchain. Wallets facilitate user to create an account, i.e., a pair of private key and public key and store it in a wallet software. To make any transaction on the blockchain, a user has to sign off his possession of the coins to his wallet's address. User can spend coins by unlocking the funds in the wallet using keys stored in the wallet. There is no real exchange of actual coins, but the exchange of transaction data values is created at the blockchain. Thereby, a trade of balance in customers crypto-wallet [27], [28]. Cryptocurrency wallet is much more secure than the exchanging. A long string, which is referred to as the key represents the address of your portfolio and generated through sophisticated cryptography techniques.

Wallets are commonly known as software or hardware wallets. Soft wallets are downloadable software programs for your PC or phone, while hardware wallets are physical vaults that store cryptocurrency data on a specially designed hard drive contained in the device. Soft wallets are typically hot or cold. Hot wallet: A wallet is hot when it's connected to the Internet. Nothing on the Internet is 100% secure, so funds kept in a hot wallet are always at a slight risk of theft or loss from software bugs. Cold wallet: A wallet is cold when it's safely offline and can't be deliberately or accidentally compromised over the Internet. All the popular hardware wallets are designed to be as secure as possible and can be backed up in different ways.

Cryptocurrencies are handled using different type of crypto-wallets as listed below.

Desktop wallet: It is a software that can be downloaded and installed on a PC or a laptop [39]–[41]. It is easy to use from a single computer in which it is installed. Desktop wallets offer one of the maximum tiers of security. However, if computer is hacked or receives a virus, there is possibility of loosing keys and thereby funds.

Online wallet: It is a software that runs on the cloud and is theoretically easy to use from any location [29]–

[1] Although it is handy to access, such wallets save your private and public keys on-line and are controlled by a third party. It subjects to on-line risk of hacking or compromising third party.

Mobile wallet: It is a software that runs as a mobile ap-plication on your phone [35]–[38]. It is more convenient and user friendly to use for transactions and payments like retail stores. Mobile wallet software has a simple user interface than desktop wallets.

Hardware wallet: These wallets are differ from software wallets in terms of key storage and management as Keys are saved on a device like a USB [42]–[48]. Although hardware wallets make transactions online, public and private keys are saved offline. Hence, it delivers immoderate security. allet: It

978-1-7281-6509-7/20/$31.00 ©2020 IEEE

is absolutely a physical copy or printout of user's public and private keys [28], [51], [54]. It also refers to a bit of software that is used to securely generate multiple keys which is then subsequently printed on paper. Use of a paper wallet is relatively trustworthy and it provides the highest stage of security as compared to above wallets. But, compromising or loss of paper wallet is still risky.

Digital wallets are not registered under the law of any country, so it is important to cautiously choose the cryptocurrency wallet for digitized transactions. It is always better to choose a universal cryptocurrency wallet that supports more than one cryptocurrency. Therefore, in this article we have considered only multicurrency wallets.

The organization of this paper is as follows. Section II presents operating principle, features and security factors of wallets. The details of Web and Mobile wallets are discussed in Section III. Subsequently, discussion on Desktop and Hard-ware wallets is presented in Section IV. Finally, conclusions are presented in Section V.

II BASIC THEORY

Wallets are software applications which can be used to view cryptocurrency balances and make transactions. Each wallet type is a piece of different software, which provides access to blockchain data and operate on blockchain data. In general, any given wallet can work with one or more cryptocurrencies and features. Public addresses are like cryptocurrency precise account numbers, they are used to acquire a particular kind of cryptocurrency and can be shared publicly. For example, to access Bitcoin blockchain one needs Bitcoin address, similarly to access Ethereum blockchain one needs Ethereum address. Wallet helps to access all transactions associated with that address on respective blockchain. In general, a wallet allows you to view balances associated with an address and lets you move funds around on the blockchain till you are the owner of the address [3], [4]. One cannot make blockchain transactions without a cryptocurrency wallet. In this section, we discuss the working principle of wallets, the features we used to compare different wallets, and the security parameters.

A. Working Principle

Wallets are software packages which are used to make transactions on given blockchain. Wallets store one or more cryptocurrency-unique public addresses. A public address is a hexadecimal string with a combination of numbers and letters, using both upper case and lower case. It needs to be shared publicly to receive cryptocurrency. The software within the cryptocurrency wallet is connected directly to the blockchain. The connected wallet allows user to read transactions and to submit transactions to the blockchain. More specifically, wallet is client software to blockchain platform to facilitate operations on the blockchain.

A secret key associated with a public address known as privet key is also stored in the wallet. A private address is also a hexadecimal string. It is difficult to remember by the human beings, therefore it is store in wallet software or with third party vendors in case of online wallets. A user need to know a pin associated with each private key to access the wallet. A pin is easy to remember small string similar to ATM pin. In general, a wallet is like your online bank account platform, your public address is similar to your account number, the blockchain is like the bank's ledger, and with custodial wallets, the custodian is a bit like a banker. Most wallets are Hierarchical Deterministic(HD) wallets as they facilitate users to restore balance and full transaction history using a single mnemonic code when anything bad happens to their device.

In nutshell, wallet interacts with the blockchain with stored public address. Transactions on blockchain are signed with the private key associated with the public key.

B. Features

Almost all wallets allow to check balance of account and make transactions. With this basic features one need to understand the other features that wallet offers for ease of business. As we know there are different types of wallets as discussed in Section I. All these wallets offer some or all of the features like authorization of user, key generation, key management, anonymity of users, multicurrency support, coin or token conversion rates, cryprto-exchange, QR code scan to transact cryptocurrency, push notifications, and backup and restoration facility of keys. Managing multiple wallets for multiple assets is hard, where multicurrency wallets make life easy. However some of the features we found relevant to compare different wallet types are as follows.

Supported Currencies: In supported currencies we consider both coins and tokens. Inherently every currency coin is associated with its own unique Blockchain. Coins, tokens are used to perform monetary transactions using digital currencies rather than fiat currencies. Bitcoin and Ether are paragons of cryptocurrencies and have their own blockchain platform. Tokens (fungible tokens) pos-sess currency-like properties, which are interchangeable, uniform across platforms and are divisible into smaller units. Tokens are provided by businesses, the holder of the token gets access to different functions provided by businesses for trading tokens. All fungible tokens are based on ERC20 standard [55]. One should purchase a token with a base currency coin. Coin operates independently, while token capabilities a specific use within the project's ecosystem. Coins are native to their own blockchain. While tokens are built on top of blockchain, like Ethereum, NEO, or Waves [50], [52], [53].

978-1-7281-6509-7/20/$31.00 ©2020 IEEE

Key Management: It is often categorized into hosted managed by the third party and non-hosted managed by the user wallets. With a non-hosted wallet, the creator of account only knows the private keys. Alternatively, with hosted wallets, a third party knows your private keys and does not screen them to you, however the organisation will send, receive, and store bitcoins on your behalf. Some hosted wallet software program do not store the personal keys. Users can log in, send and receive coins, and monitor coin transactions using their own private keys.

Anonymity: Anonymity of wallets refer to send and receive funds anonymously by users of the the blockchain. There are three levels for a wallet anonymity: full, half or less. In general, financial institutions need user to register with all of user's personal information. A fully anonymous wallet does not ask for user details. The users do no longer proportion their statistics with anyone, no records goes to be stored via the provider. Hence, despite the fact that the servers get hacked, the funds are secure. Wallet does not reveal any identity of the user. A wallet is considered as half anonymous if only mail id is required for creation of a wallet or password recovery. A much less anonymous wallets collect loads of information about its customers, including photograph ID.

Crypto exchanges: Exchanges allow users the direct conversion of fiat currencies like US Dollars, Euros, and most government-backed currencies into cryptocurrency. Users sign up for an exchange, deposit fiat currency or wire transfer and get required cryptocurrency. Cryp-tocurrency exchanges are websites where you can buy, sell or exchange cryptocurrencies. Wallets also allow exchange of one crypto for another crypto. Similarly, one can withdraw funds and get fiat currency or other cryptocurrency. Thus, user to begin with blockchain need to buy an intermediary cryptocurrency like Bitcoin or Ethereum that does accept fiat.

Wallet recovery: Users forget password or problems with storage then user coins are lost forever. In case of lost keys or restoring a wallet, seed phrase method is widely used. A seed phrase is a set of 12-24 random words that is used to access your crypto currency wallet.

C. *SECURITY*

Cryptocurrency wallets are trustworthy, secure and conve-nient, help user to keep his/her cryptocurrency safe. As we know every wallet consists of a public address and a private key. The private key must be kept safe without sharing with no one. In contrast, public address (public key) should be shared with everyone to whom user wish to send/receive money. So security of the wallet is of paramount importance.

Wallets security relies on the type of wallet used like desktop, mobile, online, paper, and hardware. Online wallets are prone to more security threats compared to offline wallets. Online wallets can make customers exploitable to viable vulnerabilities inside the wallet platform that may be exploited by means of hackers to steal credentials. Offline wallets can not be hacked due to the fact that they are not connected to the internet and do not rely on third party for security [1], [2], [5]. Although online wallets are prone to vulnerable attacks, tight protection precautions against vulnerabilities by the vendor make wallet secure and safe. Precautions should be taken and be very careful [6]–[10].

Although hardware wallets are secure, loosing private key will lead to loss of all the balance of account. Therefore, regular backup and safe storage of private keys is important for hardware wallets. In case of the desktop and mobile wallets client side encryption of the keys and data is of importance to avoid the leak of information and thereby hack of wallet.

Multiple wallets are also good option for secure operation of assets. One can use web-based wallet for the small transactions and hardware wallet for the large amount transactions. Where most of the crypto balance is associated with the hardware wallet address. Wallet software needs to be updated for the new updates and security patches to avoid risk of hacking the data stored in the wallet. Most of the wallets use pin to start the software that need to be chosen carefully and for every transaction private key need to be unlocked with more secure second level pin. With these precautions, cryptocurrency wallets will be more trustworthy and secure to use.

III. WEB AND MOBILE WALLETS

A. *Web Wallets*

Web (online) wallets are usually cryptocurrency wallets that you simply access through any web browser. User use web wallets via a browser interface without having to download or install anything. Online wallets are the least secure wallet as they are owned by third parties, that store user's private keys. One good thing about an online wallet is that user can access it from anywhere, from any device via the internet. In most cases, user creates a new pocket (wallet account) and set a non-public password to get right of entry to it. However, some providers hold and manipulate the private keys to user's behalf. Although this is handy for new users, it is a risky practice. Many web wallets allow user to manage keys, either absolutely or through shared control, i.e. via multi-signatures.

Some widely used multicurrency web wallets are compared in Table I. As shown in the Table I, supported cryptocur-rencies are high for Jaxx, Guarda, and Coinbase,

978-1-7281-6509-7/20/$31.00 ©2020 IEEE

medium for Cryptonator, and low for Gatehub and Blockchain wallet. Higher the cryptocurrencies supported better the wallet for use. Cryptonator, Guarda, Jaxx, and blockchain wallets support key management by the user, which is better compared to others where key management is done by third party. As we know more the fiat currency support better the wallet. For the Web wallets, Jaxx, coinbase, blockchain wallets support good number of fiat currency exchange support compared to other. Anonymity is high in case of Jaxx and Guarda as they do not require any information of the user to start the wallet and transaction on blockchain. Whereas, all other wallets are less anonymous as they need to provide either email or user id information. All listed wallets are portable on all exiting OS and browser platforms. In conclusion, Jaxx and Guarda are the better choices for the web based cryptocurrency wallets based on the data.

TABLE I
COMPARISON OF MULTICURRENCY WEB WALLETS BASED ON SOME UNIQUE FEATURES

Features	**Coinbase [29]**	**Cryptonator [30]**	**GateHub [31]**	**Guarda [32]**	**Jaxx [33]**	**Blockchain Wallet [34]**
Supported Currencies(Coins and tokens)	ALGO,ATOM, BAT, BTC, BCH, BSV, CVC, DAI, DASH,DNT, EOS, ETH,ETC, REP,USDC, XLM, XRP, XTZ, ZEC, ZIL, GNT,LINK, LOOM,LTC, MANA, MKR, OXT, ZRX	BTC, BCH, BLK, BCN, XMR, EMC, VTC, PPC, XPM, ETH, DOGE, DASH, EMC, LTC, RDD, XRP, XPY, ZEC	XRP, BTC, ETC, BCH, ETH, DASH, QAU, REP, XAU	AYA , BTCB, BSV, BTH, CLO, KMD, LSK, LTC, XMR, XEM, ADA, ATOM, DASH, DCR, DGB, BNB, BTC, BCH, BTG, RDD, XRP, XLM, TRX, XVG, VTC, WAVES, YEC, DOGE, EOS, ERC20, ELA, USDT, XTZ, UBQ, VET, ETH, ETC, EXP, GRS, NLG, ZEN, KIN, NEO, ONT, QTUM, XZC, ZEC, JOYS, ROPSTEN	BTC, ETH, STX, POE, MCI, QTUM, CFI, ART, BCH, REP, LTC, ZEC, PAY, DASH, ETC, RSK, DGE, ICN, GNO, GNT, DGD, BCAP, CVC and 55+ more	BTC, BCH, ETH
Key Management	Hosted or third party.	Non-hosted or user.	Hosted or third party.	Non-hosted or user.	Non-hosted or user.	Non-hosted or user.
Fiat Currencies	USD, EUR and many more(32 countries)	USD, EUR, RUB and UAH	EUR(Euro), USD(US Dollar)	Euro (EUR), Dollar (USD), British Pound (GBP), Ruble (RUB) and Danish Krone (DKK)	USD , EURO and many more	USD , EURO and many more.
Anonymity	User ID required	Only Email required	Only Email required.	No need of user details.	No need of user details.	User ID required.
Platform Support	Google Chrome, Mozilla Firefox, Microsoft Edge, Opera and blockchain-based decentralized browser Brave.	Chrome. Firefox Android. Windows. iOS. OSX.	Chrome, Firefox, etc	Chrome, Mozilla Firefox or Opera, Windows, Linux, MAC, Android, IOS	Chrome, Firefox, Windows, Linux, MAC, Android, IOS	Chrome, Firefox, Android, IOS
Wallet recovery method	Seed phrase	Email support	32 character recovery key	Seed phrase	Seed phrase	Seed phrase

TABLE II
COMPARISON OF MULTICURRENCY MOBILE WALLETS BASED ON SOME UNIQUE FEATURES

Features	Edge [35]	Coinomi [36]	Enjin [37]	Abra [38]
Supported Currencies(Coins and tokens)	BTC, XRP, DASH, ETH, REP, BCH, LTC, XMR, WINGS, IND, XZC, FTC	BTC, ETH, DGB, DGC, BTA, ABN, NEOS, XVG, VTC, ETC, BTG, DOGE, LTC, LCC, BCH, DASH, NBT, PPC, RDD, MONA, and 100+ more	ENJ, BTC, ETH, ERC721, LTC, ERC20, ERC1155	BTC, BCH, DOGE, GNT, LSK, XMR, SNT, STRAT, XEM, NEO, OMG, QTUM, TRX, XVG, ETH, XLM, ADA, BTG, XRP, ETC, LTC, TRX, REP, BAT, DASH, DGB, VTC, ZEC, ZRX
Key Management	Non-hosted or user.	Non-hosted or user.	Non-hosted or user.	Non-hosted or user.
Fiat Currencies	USD, EUR	No	USD, GBP, CAD, EUR, CNY, RUB and many more.	USD, EUR, AUD, GBP and many more.
Anonymity	No need of user details.	No need of user details.	No need of user details.	User ID required.
Platform Support	Android, IOS	Android, IOS	Android, IOS	Android, IOS
Wallet recovery method	Email support	Seed phrase	Seed phrase	Seed phrase

B. Mobile Wallets

Mobile wallets are telephone applications on Android and iOS mobile operating system. All you would like to strive is to put in an app on your telephone and open an account. Generally, mobile wallets are taken into consideration to be more secure than cloud wallets. Mobile breakdown or breach of security is risky for mobile wallets, therefore regular backup of data is important.

Commonly used mobile wallets are compared in Table II. From Table II, multicurrency support is high for Coinomi, medium for Abra and low for Edge and Enjin. In case of all wallets, key management is done by the user. Though Coinomi doesn't have direct support for fiat currency, it uses third party to do it. Abra is less anonymous as compared to all. Platforms like Android and iOS are supported by all. So, we can conclude that Coinomi is the best mobile wallet.

IV. DESKTOP AND HARDWARE WALLETS

978-1-7281-6509-7/20/$31.00 ©2020 IEEE

A. Desktop Wallets

Desktop wallets are downloaded and installed on your computer. Unlike some web based versions, desktop wallets offer you full control over keys and funds. Post installation of wallet data is stored in \pockets:dat" file. This file consists of the private key records used to get entry to your cryptocurrency addresses. Generally it is encrypted with a non-public secret password, which need to be stored secretly and safely by the user. Loss of secret password, presumably lose the access to cryptocurrency addresses and thereby the digital assets. Therefore, it is crucial to backup your pockets:dat document and preserve it some place safe. Alternatively, user has to export the corresponding personal key or seed phrase. Thereby, user will be ready to get entry to digital assets on different devices.

TABLE III
COMPARISON OF MULTICURRENCY DESKTOP WALLETS BASED ON SOME UNIQUE FEATURES

Features	Exodus [39]	Eidoo [40]	Atomic Wallet [41]
Supported Currencies(Coins and tokens)	BTC, LTC, ETH, VTC, FUN, DASH, ETC, DCR, EOS, OMG, ANT, GNO, BCH, BTG, BAT and 15+ more.	BTC, FUN, OMG, ERC20 tokens, VET, REP, ERC223 tokens, ETH, EOS, TRX,	BTC, DGB, ZEC, XRP, QTUM, XLM, BCH, ETC, DASH, AWC, BTG, DOGE, TPAY, VET, LTC, ETH, VTHO, DCR, TRX, XMR and 280+ more.
Key Management	Non-hosted or user.	Non-hosted or user.	Non-hosted or user.
Fiat Currencies	No	USD, CHF,EUR,GBP	USD, CHF,EUR,GBP
Anonymity	No need of user details.	User ID required.	No need of user details.
Platform Support	Windows, Mac, Linux	Windows, Mac, Linux, Android, IOS	Windows, Linux, MAC
Wallet recovery method	Seed phrase	Seed phrase	Seed phrase

TABLE IV
COMPARISON OF MULTICURRENCY HARDWARE WALLETS BASED ON SOME UNIQUE FEATURES

Features	Keepkey [42]	Ledger Nano S [44]	Ledger Nano X [43]	Trezor [45]	Corazon [46]	CoolWalletS [47]	Sugi [48]
Supported Currencies(Coins and tokens)	BTC, DOGE, NMC, ETH, LTC, BCH , DASH,	BTC, EOS, XLM, LTC, XRP, TRX, ADA, MIOTA, ETH, BCH, and 1,300+ more	BTC, XRP, ETH, ZEC, VET ,BCH, XTZ, WAVES, DOGEEOS, XLM, LTC, TRX, BNB, XMR, ADA, MIOTA, DASH, NEO, ETC and 1,000+ more	BTC, BCH, ETH, ERC20, DOGE, ETC, NEM, NMC, UBQ , BTG, LTC, DASH, ZEC, EXP	BTC, DASH, DOGE, NMC, ZEC, ETC, ETH, ERC20, NEM, EXP, UBQ ,BCH, BTG, LTC	BTC, BCH, ETC, XRP, LTC, ICX, ERC20 Tokens	BTC, ETH, ERC20, LTC, XRP, BCH
Key Management	Non-hosted or user.	Non-hosted or user.	Non-hosted or user.	Non-hosted or user.	Non-hosted or user.	Non-hosted or user.	Non-hosted or user.
Cost	$79	$59	$119	$59	$700-$1500	$99	$133.33
Anonymity	No need of user details.	No need of user details.	No need of user details.	No need of user de-tails.	No need of user details.	No need of user details.	No need of user details.
Platform Support	Mac, Windows, Linux, IOS, Android	Mac, Windows, Linux, IOS, Android	Mac, Windows, Linux, IOS, Android	Mac, Windows, Linux, Android	Mac, Windows, Linux, Android	Android, IOS	Mac, Windows, Linux, IOS, Android
Wallet recovery method	Seed phrase	Seed phrase	Seed phrase	Seed phrase	Seed phrase	Seed phrase	Seed phrase

The widely used desktop wallets are described in Table III. From Table III, support for multicurrency is high for Atomic Wallet, medium for Exodus and low for Eidoo. In case of all wallets, key management is done by the user. Exodus doesn't have support for fiat currency. Eidoo is less anonymous as compared to all but support all mobile and desktop platforms. From the available data, we can conclude that Atomic Wallet is the best desktop wallet.

B. Hardware Wallets

Hardware wallets are secure, offline devices, typically an USB drive. They store your private keys offline so they can't be hacked. They're prepared to make online transactions. Various producers make hardware wallets compatible with different internet interfaces. Therefore, complete characteristics depend on wallets integration. Hardware storage is additionally con-venient due to its potential to send and receive currencies by means of merely plugging them into the internet enabled tool and authorizing yourself. Therefore, hardware wallet is that the costliest, at the same time it has safest options.

The widely used Hardware wallets are described in Table IV. From Table IV, multicurrency support is high for Ledger Nano S and X, medium for Trezor, Corazon and low for Keepkey, CoolWalletS and Sugi. In case of all wallets, key management is done by the user. When it comes to cost, Ledger Nano S and Trezor are at the best. All hardware wallets are fully anonymous. CoolWalletS have only mobile support, the rest have both desktop as well as mobile. So, we can conclude that Ledger Nano S is the best hardware wallet.

It is recommended to follow standard security best practices when using a wallet:

Always use strong usernames and passwords. Only use verified and trusted wallets.

Access only secure online wallet with https protocol.

Update your wallet software frequently.

978-1-7281-6509-7/20/$31.00 ©2020 IEEE

Avoid access of online wallets from public Wi-Fi.

Install antivirus and anti-malware software and keep them up-to-date.

V. CONCLUSIONS

There are plenty of wallets that are available for use. We have selected a few sample wallets from different categories. Most probably, all wallets use SHA256, ECDSA key generation algorithms as they are built for existing blockchains. Wallets such as Guarda, Jaxx supports web, mobile and desk-top platforms. If protection is the concern, choose a hardware wallet. If comfort is the concern, choose an internet or cell wallet.

When choosing the best cryptocurrency wallets, we recommend you to make use of 2 types of wallets, a web-based wallet and a hardware wallet. On the web-based wallet, you store your petty cash, and on the hardware wallet, you store all your other cryptos. Via the web-based wallet, you'll be trading to and fro other exchange based wallets, and then transferring trading profits from your web-wallet onto your hardware wallet for long term safekeeping.

From our limited set of sampling of wallets, i) Jaxx and Guarda are the better choices for the web based cryptocurrency wallets, ii) Coinomi is the best mobile wallet, iii) Atomic Wallet is the best desktop wallet, and iv) Ledger Nano S is the best hardware wallet. Before choosing a cryptocurrency mobile wallet, one needs to take into account the OS it supports, level of security as well as supported coins. And keep in mind not to hold all your assets in one place. It should be noted that there's -no one size fits all- wallet.

REFERENCES

[1] Corina Sas, Irni Eliana Khairuddin, Exploring Trust in Bitcoin Technol-ogy: A Framework for HCI Research, ACM 2015.

[2] Stanislaw Jarecki, Aggelos Kiayias, Hugo Krawczyk and Jiayu Xu, Highly Efficient and Composable Password-Protected Secret Sharing (Or: How to Protect Your Bitcoin Wallet Online) IEEE 2016.

[3] Nelisiwe Peaceness DLAMINI , Mfundo Shakes SCOTT, Kishor Krish-nan NAIR, Development of an SMS System Used to Access Bitcoin Wallets, IST Africa 2017.

[4] Miraje Gentilal, Paulo Martins, Leonel Sousa, TrustZone-backed Bitcoin Wallet, ACM 2017.

[5] Puneet Kumar Kaushal, Dr. Amandeep Bagga, Dr. Rajeev Sobti, Evolu-tion of Bitcoin and Security Risk in Bitcoin Wallets, IEEE 2017.

[6] Yi Liu, Ruilin Li, Xingtong Liu , Jian Wang , Lei Zhang , Chaojing Tang and Hongyan Kang, An Efficient Method to Enhance Bitcoin Wallet Security, IEEE 2017.

[7] Yi Liu, Xingtong Liu, Lei Zhang, Chaojing Tang and Hongyan Kang, An Efficient Strategy to Eliminate Malleability of Bitcoin Transaction, IEEE 2017.

[8] Obinna Stanley Okpara, Girish Bekaroo, Cam-Wallet: Fingerprint-Based Authentication in M-Wallets using Embedded Cameras, IEEE 2017.

[9] Po-Wei Chen, Bo-Sian Jiang, Chia-Hui Wang, Blockchain-based Payment Collection Supervision System using Pervasive Bitcoin Digital Wallet, IEEE 2017.

[10] Pratyush Dikshit, Kunwar Singh, Efficient Weighted Threshold ECDSA for Securing Bitcoin Wallet, IEEE 2017.

[11] Fangdong Zhu, Wen Chen, Yunpeng Wang, Ping Lin , Tao Li, Xiaochun Cao and Long Yuan, Trust Your Wallet: A New Online Wallet Architec-ture for Bitcoin, IEEE 2017.

[12] Arunmozhi Manimuthu, Raja Sreedharan V , Rejikumar G and Drishti Marwaha, A literature review on Bitcoin: Transformation of crypto currency into a global phenomenon, IEEE 2018.

[13] Yi-Hui Chen, Shih-Hsin Chen, Iuon-Chang Lin, Blockchain based Smart Contract for Bidding System, IEEE 2018.

[14] Mordechai Guri, BeatCoin: Leaking Private Keys from Air-Gapped Cryptocurrency Wallets, IEEE 2018.

[15] Shuangyu HE 1 , Qianhong WU 1 , Xizhao Luo 2 , Zhi Liang 1 , Dawei LI 1 , Hanwen Feng 1 , Haibin Zheng 1 and Yanan LI ,A Social-Network-based Cryptocurrency Wallet Management Scheme, IEEE 2018.

[16] Pallavi Maindola, Neetu Singhal, Akash D Dubey, Sentiment Analysis of Digital Wallets and UPI Systems in India Post Demonetization Using IBM Watson, IEEE 2018.

[17] Karan Singh, Nikita Singh, Dharmender Singh Kushwaha, An Inter-operable and Secure E-Wallet Architecture based on Digital Ledger Technology using Blockchain, IEEE 2018.

[18] Priyesh Ranjan , Sumit Soman , Amit Kumar Ateria and Praveen K Srivastava, Streamlining Payment Workflows using a Patient Wallet for Hospital Information Systems, IEEE 2018.

[19] Yuxiao Wang and Juntao Gao, A Regulation Scheme Based on the Ciphertext- Policy Hierarchical Attribute-Based Encryption in Bitcoin System, IEEE 2018.

[20] Kazi Abu Taher, Tahmin Nahar, Syed Akhter Hossain, Enhanced Cryp-tocurrency Security by Time-Based Token Multi-Factor Authentication Algorithm, IEEE 2019.

[21] Hyochang Baek, Junhyoung Oh, Chang Yeon Kim, Kyungho Lee, A Model for Detecting Cryptocurrency Transactions with Discernible Purpose, IEEE 2019.

[22] Ashish Rajendra Sai, Jim Buckley, Andrew Le Gear, Privacy and Security analysis of cryptocurrency mobile applications, IEEE 2019.

[23] Seongho Hong, Heeyoul Kim, Analysis of Bitcoin Exchange Using Relationship of Transactions and Addresses, ICACT 2019.

[24] Shervin Erfani, Majid Ahmadi, Bitcoin Security Reference Model: An Implementation Platform, IEEE 2019.

[25] 'How to generate a bitcoin address- Step by Step ', 2018.

[29] Coinbase Exchange Review',2018. https://www.finder.com/in/coinbase-exchange-review. [Accessed: 22-Jan- 2020].

[30] 'Cryptonator Review', 2020. https://www.7binaryoptions.com/crypto/cryptonator-review/. [Accessed: 22- Jan- 2020].

[31] 'Gatehub', 2019. https://en.bitcoinwiki.org/wiki/GateHub. [Accessed: 22- Jan- 2020].

[32] 'Guarda Wallet', 2017. https://www.cryptowisser.com/wallet/guarda-wallet/. [Accessed: 22- Jan- 2020].

[33] 'Jaxx', 2020. https://www.fxempire.com/crypto/wallets/jaxx. [Accessed: 22- Jan- 2020].

[34] Blockchain Wallet Review,2020.https://www.bestbitcoinexchange.io/wallets/ blockchain/. [Accessed: 22- Jan- 2020].

[35] 'Edge Wallet Review', 2018. https://www.finder.com/edge-wallet-review. [Accessed: 28- Jan- 2020].

[36] 'Coinomi Wallet Review', 2018. https://www.finder.com/in/coinomi-wallet-review. [Accessed: 28- Jan- 2020].

[37] 'Enjin Smart Wallet', 2020. https://www.finder.com/enjin-smart-wallet. [Accessed: 28- Jan- 2020].

[38] 'Abra Cryptocurrency Wallet', 2019. https://www.finder.com/abra-cryptocurrency-app. [Accessed: 28- Jan- 2020].

[39] 'Exodus', 2020. https://www.fxempire.com/crypto/wallets/exodus. [Ac-cessed: 27- Jan- 2020].

[40] 'Eidoo', 2017. https://www.cryptowisser.com/wallet/eidoo/. [Accessed: 27- Jan- 2020].

[41] 'Atomic Wallet Review', 2019. https://www.finder.com/in/atomic-wallet-review. [Accessed: 28- Jan- 2020].

[42] 'Keepkey Wallet Review', 2018. https://www.finder.com/in/keepkey-wallet-review. [Accessed: 28- Jan- 2020].

[43] Ledger Nano X', 2019. https://www.finder.com/ledger-nano-x. [Accessed: 28- Jan- 2020].

[44] Ledger Nano S', 2018. https://www.finder.com/in/ledger-nano-s-wallet-review. [Accessed: 28- Jan- 2020].

978-1-7281-6509-7/20/$31.00 ©2020 IEEE

[45] Trezor', 2020. https://www.fxempire.com/crypto/wallets/trezor. [Accessed: 28- Jan- 2020].

[46] 'Corazon Review', 2019. https://www.finder.com.au/corazon-model-t-wallet-review. [Accessed: 28- Jan- 2020].

[47] 'CoolWalletS', 2020. https://www.finder.com/in/coolwallet-s-wallet-review. [Accessed: 28- Jan- 2020].

[48] 'Sugi Review', 2018. https://www.finder.com/sugi-wallet-review. [Ac-cessed: 28- Jan- 2020].

[49] 'Mining Algorithms' 2020. https://en.bitcoinwiki.org/wiki/Mining algorithms. [Accessed: 17- Feb- 2020].

[50] List of Cryptocurrencies', 2017. http://cryptomining24.net/list-of-cryptocurrencies/. [Accessed: 17- Feb- 2020].

[51] Cryptocurrency Wallet Types,2017. https://www.binance.vision/blockchain/ crypto-wallet-types-explained. [Accessed: 18- Feb- 2020].

[52] 'All Cryptocurrencies', 2020. https://coinmarketcap.com/all/views/all/. [Accessed: 19- Feb- 2020].

[53] 'All tokens', 2020. https://coinmarketcap.com/tokens/views/all/. [Accessed: 19- Feb- 2020].

[54] 'Cryptocurrency Wallets', 2020. https://www.finder.com/in/cryptocurrency/wallets. [Accessed: 19-Feb- 2020].

[55] Mahesh Shirole, Maneesh Darisi, Sunil Bhirud, Cryptocurrency Token:An Overview, In proceedings of IC-BCT 2019 SpringerInternational Conference on Blockchain Technology, Springer 2019.

978-1-7281-6509-7/20/$31.00 ©2020 IEEE