VAULTAVO

CRYPTOCURRENCY WALLETS

VAULTAVO

ABSTRACT

Cryptocurrency wallets are the technologies by which people and institutions interface with, secure and store their digital assets. In this paper we consider the two primary technologies in this regard: hot and cold wallets. We assess the features of each wallet and discuss which is most suitable for various kinds of actors in the space, be they retail or institutional investors. We furthermore provide direction on the most salient features to consider when choosing your cryptocurrency wallet.

INTRODUCTION

Digital assets are still a relatively new phenomenon and the dangers and best practices when storing and securing these assets are often overlooked by newcomers and casual investors. There is a misconception that has propagated regarding the inherent security properties of blockchain technologies. Many believe that the immutability, or, the inability to change, the ledger of a blockchain automatically ensures a high level of security. However, the blockchain technology provides us with high assurance regarding its veracity and verifiability of transactions, but a great deal of caution and personal responsibility still applies to crypto ownership.

> **IN THE PHYSICAL WORLD, YOUR BANK MAY HAVE A HIGH DEGREE OF SECURITY AND VERACITY BUT THAT DOES NOT MEAN YOUR LEATHER WALLET IS NOT STILL AT RISK.**

In the physical world, your bank may have a high degree of security and veracity but that does not mean your leather wallet is not still at risk of being stolen if left unattended. Similarly, crypto wallets can still be exploited if insufficient precautionary measures are taken. Therefore, it is essential that all investors, retail and institutional alike, understand and appreciate the nuances of cryptocurrency wallets so they can choose one that satisfies their bespoke needs. In this paper, we will explain how these wallets work, the differences between the primary categories of crypto wallets and what to look out for when choosing your crypto wallet.

CRYPTOCURRENCIES AND BLOCKCHAIN TECHNOLOGY

In order to understand cryptocurrency wallets it is important to first establish a high level understanding of cryptocurrency and blockchain technology. Cryptocurrencies, or crypto, are a form of digital money that is secured using cryptography on distributed ledger technology (DLT); the most common form of DLT utilized by cryptocurrencies is called a blockchain. While substantial differences between crypto exist, for the purpose of this paper it is important to note that the accounting mechanisms that keep track of who owns what on these protocols is (are) recorded on a distributed ledger. What this means is that multiple parties are responsible for recording transactions and verifying the true version of the ledger at all times. These parties are financially incentivized to keep the ledger updated and accurate. The more parties involved, the more decentralized the protocol is with regard to block propagation.

Decentralization is naturally a desirable characteristic in this context, it is what distinguishes cryptocurrencies from fiat currencies which depend on centralized institutions that could hypothetically deny service to individuals or groups. Cryptocurrencies that are decentralized push power to edges in this regard as blockchains are uncensorable, permissionless, borderless, peer-to-peer systems. It is these aspects that make cryptocurrencies and other digital assets such desirable investment vehicles.

"IN ORDER TO UNDERSTAND CRYPTOCURRENCY WALLETS IT IS IMPORTANT TO FIRST ESTABLISH A HIGH LEVEL UNDERSTANDING OF CRYPTOCURRENCY AND BLOCKCHAIN TECHNOLOGY."

The aforementioned ledger that is stored on the blockchain is immutable. It therefore cannot be altered once parties have agreed on the true record of the ledger. This is important to note when considering the purpose of cryptocurrency wallets. The distributed ledger is like a continuous database, constantly updating the change of ownership of assets on the blockchain.

No value ever leaves the blockchain. Cryptocurrency wallets are unique in this regard as value is not subtracted from the blockchain and transferred to your wallet, instead, crypto wallets are merely tools that point to the records on the ledger to prove or change ownership of the assets. Now that we have established a high level understanding of crypto wallets, let us dive a bit deeper into the mechanics and discuss public and private keys.

HOW DO CRYPTO WALLETS WORK?

So far we have established that crypto wallets do not actually hold your crypto assets, instead they are tools for interacting with the blockchain but how do they achieve this? Let's use Alice as our subject and a Bitcoin crypto wallet as an example. When Alice downloads a Bitcoin wallet application on her smartphone it enables her to create a digital Bitcoin wallet which in turn generates multiple pairs of public and private keys. Public and private keys are an integral part of crypto wallets so we should take the time to expand on each.

> **CRYPTO WALLETS DO NOT ACTUALLY HOLD YOUR CRYPTO ASSETS, INSTEAD THEY ARE TOOLS FOR INTERACTING WITH THE BLOCKCHAIN.**

Private keys

The private key enables Alice to access her crypto funds and is furthermore used to sign and thereby approve outgoing transactions. The private key can be represented in various ways depending on the device you are using. Some private keys are represented by a string of digits and characters, other more sophisticated technologies secure your keys using biometric data such as a fingerprint. The most common private key type is a seed phrase; a sequence of twelve or twenty-four randomly generated words. As the name suggests, private keys should be kept private. Anyone Alice shares her private key with will be able to access her funds and make transactions on her behalf. This is a major security risk as that person has the means to void her account and Alice will have virtually no recourse to retrieve the stolen funds. Securing one's private key is thus a crucially important responsibility for any crypto holder.

One of the great features of a private key is that in the event that Alice's smartphone, laptop or hardware device which hosts the wallet is lost or stolen, her wallet can be regenerated using the same private key. Therefore, the theft of the device on which your crypto is stored does not mean the thief can access your wallet, for that, they would require your private key. Alice may also choose to use a single private key on multiple devices or multiple wallets. This practice is more convenient but is naturally a higher security risk as one key effectively opens numerous safes. Now that we have a sufficient understanding of the inner workings of crypto wallets, let us look at the various kinds of wallets available and which are best suited for different users.

Public keys

The public key is a feature of crypto wallets that allows for the generation of numerous BTC wallet addresses. These addresses can be shared by Alice with anyone who wants to deposit BTC into her wallet. Sharing an address is so safe that many users on Twitter even post a BTC address on their profile so that people who enjoy the content they create can tip them in crypto. These transactions are public however, as are all transactions on a blockchain. Blockchains are a tool for transparency after all.

Numerous addresses can be generated by the public key, and consistently using various addresses and not displaying the addresses publicly will afford Alice greater degree of privacy. It is safe to share public addresses in the sense that this information cannot be reverse engineered in order to access private keys which control funds but publicly sharing BTC addresses will allow people to view transactions made to and from those public keys.

TYPES OF CRYPTO WALLETS

There are various kinds of users in the crypto space and each have different risk models and tolerance for complexity. There is no perfect product to satisfy everyone's crypto storage and security needs, however we believe that Vaultavo's biometric card solution comes close and we will explain why in a later section. In this section we explore the three kinds of crypto wallets that users are likely to encounter and what type of investor will find them most suitable. We will look at three specific types of wallets: hardware, software and paper wallets.

"THERE IS NO PERFECT PRODUCT TO SATISFY EVERYONE'S CRYPTO STORAGE AND SECURITY NEEDS, HOWEVER WE BELIEVE THAT VAULTAVO'S BIOMETRIC CARD SOLUTION COMES CLOSE."

Hardware Wallets

Crypto hardware wallets are technological devices that have been specifically designed for the purpose of storing and securing crypto assets. The most common form factor is that of a small plug-in device resembling a usb style flash drive. Hardware wallets are often simply referred to as 'hard wallets' or in some instances 'cold wallets'. Hard wallets are also referred to as cold wallets because they do not have an active connection to the internet, this decreases the device's attack surface and provides an additional layer of security compared to software wallets. The lack of connection to the internet prevents users from exposing their crypto assets to phishing sites, malware and cyber attacks.

The extra layer of security that a hardware wallet offers is its primary benefit. The device itself is often stored in a safe or third party vault, this is known as deep storage. Making transactions on the device requires connecting the device to the computer which again exposes one's funds to additional risks. Using hardware wallets tend to be somewhat more technically demanding than software wallets. Hardware wallets are thus more relevant for those who are serious about protecting their assets and do not need to make frequent transactions.

Software Wallets

Software Wallets are applications on a smartphone or web-based extensions that store and secure crypto assets. Software wallets are often considered to be less secure due to the fact that they have an active connection to the internet whenever in-use, thus greatly increasing its attack surface which leaves room for phishing, malware and cyber attacks. It is for this reason that software or 'soft wallets' are also called 'hot wallets', due to their active connection to the internet. Not all wallets are created equal and some have greater security profiles than others. Be sure to conduct extensive research before settling on a software wallet. Software wallets are admittedly very simple and convenient, making them the ideal choice for users who need to frequently access their funds and make transactions. It is still advisable to keep larger funds in cold storage so that in the event of an exploit that not all funds are lost.

There is also a major difference between custodial and non-custodial wallets. Most exchanges will have default wallets that seemingly protect your coins, but because you are not in possession of the seed phrase, or private keys, this means you do not truly have ownership over assets you hold on the exchange until you remove them. Many exchanges have clauses in their terms of service that stipulate that in the event of a bankruptcy your crypto assets may be used to cover their losses. Therefore if you do choose to use software wallets make sure that they are custodial.

Paper Wallets

Paper wallets are likely the least popular type of crypto wallet we discuss in this paper but important nonetheless. Paper wallets are another physical-form, cold wallet that is unconnected to the internet enabling users to take their crypto offline. In its simplest form it is just the public and private keys printed out on a piece of paper, others print barcodes which serve the same purpose. Paper wallets need not be on paper, some engrave their keys into wood or stone tablets for greater durability. Those who opt for paper wallets tend to distrust hardware wallet manufacturers and believe that paper wallets cannot be exploited and carry even less risk. This may be the simplest wallet type but just be sure to save it in a safe place that no-one else can access.

VAULTAVO

CONCLUSION

Cryptocurrency wallets are merely tools for people to interact with the blockchain. Cryptocurrencies never truly leave the blockchain or enter crypto wallets. Instead crypto wallets generate public and private key-pairs that allow users to prove ownership and sign transactions of assets on the blockchain. There are three primary kinds of wallets: hardware, software and paper. Hardware and paper wallets are offline and thus reduce their attack surface by removing the possibility of phishing, malware or cyber attacks -making hard wallets ideal for long term storage. Software wallets or hot wallets are exposed to these risks, but they are simple and convenient which makes them valuable for smaller daily transactions.

> **"CRYPTO WALLETS GENERATE PUBLIC AND PRIVATE KEYPAIRS THAT ALLOW USERS TO PROVE OWNERSHIP AND SIGN TRANSACTIONS OF ASSETS ON THE BLOCKCHAIN."**

TO LEARN MORE VISIT
www.vaultavo.com

FOLLOW US ON TWITTER
@vaultavo

FOR GENERAL ENQUIRIES CONTACT
hello@vaultavo.com