ORION INVESTIGATIONS

KEEPING YOUR CRYPTOCURRENCIES SAFE

Author – Andrew Smith - Director of Computer Forensics Services

18 May 2021

Keeping your Cryptocurrencies Safe

With cryptocurrencies such as Bitcoin, Ethereum and various alt coins having reached all-time highs recently, this has resulted in a flood of new investors opening trading accounts with crypto exchanges around the world. Many of these investors blinded by the potential for large profits may only have a basic level of knowledge of the crypto markets and how the underlying technology works. This results in many people falling prey to scammers, losing their investment on exchanges that perform exit scams or making mistakes that result in them losing access to their crypto forever.

With the renewed interest in cryptocurrencies, now seems like an appropriate time to discuss the steps you need to take to keep your cryptocurrencies safe. There is a popular saying in the crypto world, "***Not Your Keys, Not Your Coins***". The saying refers to the need to owning the private keys associated with your crypto. Whoever controls the private keys ultimately controls the crypto. When someone sends you some cryptocurrency such as Bitcoin you will provide them with a receiving address. The exact format of the receiving address will vary from cryptocurrency to cryptocurrency. The receiving address is your public key. It is called a public key because you can send it to anyone without compromising your cryptocurrency. Associated with the public key is a private key. The private key is what allows you to access and control your cryptocurrency. The private key identifies you as the owner of the crypto and allows you to transfer or sell your crypto asset.

When you store your cryptocurrencies on an exchange, the exchange is in control of the private keys and as a result while you may have access to your crypto assets you do not have control of them. With this is mind the following points should be considered when using a crypto exchange:

- Only use well known reputable exchanges
- Only use exchanges that offer security features such as:
  - Two-factor authentication (2FA), such as Google Authenticator
  - Complex captchas
  - Additional verification via email or SMS when logging in from new devices or IP addresses
- Only use exchanges that are insured in the event that they suffer a major hack.
- Use exchanges that store the majority of the crypto assets in cold wallets. A cold wallet is a wallet that is not connected to the Internet.
- Only use exchanges that undertake yearly security assessments by independent cyber-security firms.
- Only store on the exchange the crypto that you are actively trading.
- Do not use the exchange for long term storage of your crypto assets.

When not storing your cryptocurrency on an exchange, what options do you have to safely store your crypto? There are basically two category of wallets that you can use, hot wallets and cold wallets. A hot wallet is any wallet that is connected to the internet while a cold wallet remains disconnected from the Internet for the majority of the time.

Before I discuss the different types of wallets in more detail there is one misconception that needs to be cleared up. People often mistakenly think that their cryptocurrencies is stored in the wallet. This is not the case. The cryptocurrency remains located on the public blockchain while the wallet stores the information required to access the blockchain thereby allowing the user to conduct transactions. Information held on the wallet includes the public and private keys.

So how are the private keys generated? When you create a wallet where you have control of the keys, private keys will need to be created. This will generally be done by using something called a recovery seed. The seed will often consist of a list of either 12 or 24 random words which is used to generate the private keys. You will then create a password for access to the wallet. It is vital that you retain a copy of the recovery seed and keep the copy somewhere secure. If you ever forget your password the recovery seed can be used to regain access to your crypto. If someone else gains access to your recovery seed, they will also be able to gain access to your crypto and will be able to transfer it to a wallet under their control. It is recommended to write down your recovery seed on paper and keep it somewhere safe so it cannot be accessed via the Internet. Remember if you forget your password and lose your recovery seed it will be impossible to recover your cryptocurrency.

Hot Wallets

Hot wallets offer convenience and include exchange wallets, web wallets or software wallets installed on the computer or on mobile devices.

Web Wallets – A web wallet allows you to access your cryptocurrency via a web browser interface. You would create a wallet and a password to secure the wallet. However, it is important to understand that depending on the provider, they may still control the public and private key. Many web wallets do allow you to control the keys and the safest way to do this is to store your private keys on a hardware wallet (*see further details on hardware wallet under cold wallets section*). This option would give you full control over your keys in the most secure way. Therefore, it is important that you do your research before entrusting your cryptocurrency to a web wallet provider.

Software Wallets – Using a software wallet allows you to download and install the wallet to your computer or mobile devices. The advantage of a software wallet is that it gives you complete control of your private keys. The private keys will be stored in a file on your computer. With this in mind the following points should be considered:

- Encrypt the file that contains the private keys with a password. This option can usually be done through the wallet software.
- Make a backup of the file and store it somewhere secure.
- Make a backup of the recovery seed and store it somewhere offline.
- Make sure you have security software such as anti-virus installed on your system and it is kept up to date. If your computer is hacked or becomes infected with malware such as a keylogger a malicious person may gain access to your password and your wallet.

Cold Wallets

Hardware Wallets – hardware wallets are USB hardware devices that are used to generate public and private keys which are stored on the device itself. The hardware wallet is considered one of the most secure options for protecting your private keys. The device itself is protected by a password which you create and must enter in order to access the device. When you set up the device you will be provided with a recovery seed which as discussed before you must record and keep secure. The private keys for your web wallets and software wallets can be stored on the device. This means that when you wish to access your wallets the device must be plugged into your computer or connected

via Bluetooth. A question commonly asked by people is *"What happens if my hardware wallet breaks or is lost or stolen?"* As long as you still retain possession of your recovery seed then there is no issue in regaining access to your crypto. It is simply a matter of obtaining a new hardware wallet and set it up using your recovery seed. You will then have full access to your cryptocurrency again. Several important points to remember when purchasing a hardware wallet:

- Do not purchase second hand hardware wallets as they may have been tampered with or are fake.
- Only purchase from reputable sellers.
- Only purchase reputable brand name hardware devices. Reputable brands include Ledger, Trezor, KeepKey and CoolWallet.
- When purchasing a new hardware device, the box it comes in should be sealed with some kind of security seal. If this is broken return the device back to the store.
- Record your recovery seed and keep it secure.

Summary

The cryptocurrency market is highly volatile. Some crypto coins/tokens you currently own that are only worth a few cents each, may be worth thousands of dollars in a few years' time. It is not uncommon to hear stories of people who forgot that they were storing cryptocurrency on their computer and as a result either reinstalled the operating system, sold the computer or simply forgot their password and as a result can no longer get access to their cryptocurrency that would have made them a millionaire. To avoid finding yourself in a similar situation remember the following key points:

- Remember **"Not Your Keys, Not Your Coins"**. Only store on a trusted fully insured exchange the crypto you are actively trading.
- For long term storage, store your crypto in a wallet where you have complete control of the private keys.
- Hardware wallets are considered the most secure option for storing your private keys.
- Only buy trusted brand name hardware wallets from trusted sellers.
- **Remember to record your recovery seed and keep it offline**. If you forget your password and do not have a copy of your recovery seed, you have lost your crypto forever.

The final point to remember is that no customer service agent from a legitimate crypto exchange or wallet provider will ask you to provide them with your wallet password or recovery seed. If someone asks you for this information, they are trying to scam you.

If you find yourself in the unfortunate position of having lost access to your cryptocurrency, either as a result of having forgotten your password or accidently deleting your wallet, then contact Orion to discuss how we may be able to assist.

About the Author – Andrew has completed the CSITech Ltd Cryptocurrencies for Investigators course and is an active trader of various cryptocurrencies. He is not associated with any product brands mentioned in this article.