Private key storage

cryptorecords

www.cryptorecords.ca

Recovery phrase vs private key

- Recovery phrase: Commonly 12 or 24 words. When inputted into a wallet it will provide access to all wallets that were created with that recovery phrase, even across various blockchains.
- Private key: A long string of characters that will provide access to only one specific wallet, often to only one blockchain, except for those that are compatible such as EVM wallets.

Managing the security of your private keys is critical in the world of cryptocurrency. Private keys are what give you access to your crypto assets, and if you lose access to them, you lose access to your funds. Storing your keys in a single location increases the risk of losing them, while spreading them across multiple locations can expose them to potential security breaches.

Q: What is the backup plan if you lose access to your keys?

A: There is no backup plan. If you have lost access to your keys you have lost your crypto.

Storage options

There is no single "right" solution for safeguarding your private keys. Each method comes with its own risks, and only you can determine what works best for you. Below is a list of options to consider for securely storing your keys:

- **Paper**: Writing down your keys.
- **Metal imprints**: Storing your keys on durable metal sheets.
- **Encrypted files**: Digital files secured by encryption.
- **Electronic vault**: Files stored in a secure digital vault.
- **External storage**: Using external drives to store encrypted files.
- **Device storage**: A data vault on your personal device.
- **Fire safe**: Physical storage in a fireproof safe.
- **Bank vault**: Storing your keys securely in a bank vault.
- **Third-party storage**: Using trusted third-party storage providers.
- **Split key storage**: Storing part of your key on one device and the other part on a separate device.
- **Cloud options:** Cloud storage is often not recommended. However if you use any cloud options it would be advisable to: 1) ensure your password is complex, 2) ensure you have set the requirement for a second step login (2FA, OTP), 3) ensure the file that your keys are stored in is password protected and is stored inside an encrypted vault file.
    - **Cloud storage drive**
    - **Password manager**

You can combine these methods for added security, such as:

1. ***Encrypt a password-protected document***
2. ***Store the document in an encrypted electronic vault***
3. ***Place that encrypted vault on encrypted external drives***
4. ***Store the drives in a bank vault, a fire safe, or both, and / or store the encrypted vault in a secure cloud or password manager***

Tips

1. People often use the term “private keys” as a catch-all. The term in the literal sense does not mean “recovery phrase” but in common use individuals use that term to refer to either or both “recovery phrase” and “private keys”'.
2. Being paranoid about your security is better than being lazy. Laziness often leads to loss. Be diligent with your private keys, using aggressive methods to keep them safe and accessible to only you.
3. Consider a “dead man’s switch” - a method to provide access to your crypto to your loved ones. Feel free to contact us to discuss this option.

What we bring to the table:

- Extensive experience in crypto, business, and taxation strategies.
- A team comprised 100% of crypto enthusiasts who are personally familiar with crypto platforms, products, and taxation.

How we can help you:

- Get us working for you to generate your annual tax reports, to implement a tax-smart crypto plan, and to collaborate with your tax advisor.
- Get in touch for a host of free resources and to join one of our private crypto communities so you can learn from others, participate in routine webinars, AMAs, and round table events.
- Initial consultations are always free.

www.cryptorecords.ca