

What's the most secure cryptocurrency wallet?

10/25/2024 12:29 am EDT

It is safer to store cryptocurrency on a cold wallet (usually a hardware wallet device), whereby the private keys are not stored on any internet-connected device, as opposed to storing cryptocurrency on a hot wallet, whereby the private keys are stored on internet-connected devices, albeit usually in an encrypted form.

The reason for this is because having physical possession of the hardware device is required to be able to execute transactions from the wallet, unless the seed phrase is used to subvert this process, whether for legitimate or illegitimate reasons.

Reputable hardware wallet providers include Trezor, Ledger, Ellipal, Safepal and NGRIVE.

However, any wallet is only as secure as the operational security practices of the person using it. If the seed phrase isn't safely stored, such as if it is stored on the cloud, then you have effectively made your cold wallet a hot wallet -- or worse since the seed phrase containing the private keys may not be encrypted. Additionally, a hardware wallet won't prevent a user from inadvertently authorizing malicious smart contracts that can steal funds.

For these reasons, the the operational security practices and procedures are actually more important for the security of a users' cryptocurrency wallet than the specific type of cryptocurrency wallet utilized. Even the best hardware wallet won't keep a users' cryptocurrency wallet secure if the user doesn't employ adequate security practices.
