Introduction to Crypto Wallets

What are crypto wallets?

As the name suggests, a wallet is a type of purse that stores your access keys to crypto coins and tokens. Such an application works like an online bank account for cryptocurrencies and tokens with the significant difference that there are no intermediaries. Everyone can create and use a wallet ("bank the unbanked") without signing up or authenticating.

Background

Many blockchains operate with their native cryptocurrency, like Ether for Ethereum. Transactions of these cryptocurrencies are managed through keys and are securely stored in a decentralized ledger. For usability and security purposes the keys can be used and stored within a wallet. Each wallet has two keys: a public key, similar to a bank account number, that is publicly visible, and a private key, similar to a password and signature, usually consisting of letters and numbers. The password opens the virtual vault to the blockchain where the coins and tokens are stored.

Since these private keys are long and difficult to remember, wallets usually link them to a seed or recovery phrase. This phrase consists of a sequence of 12 or 24 words used as the master password. Wallets store the keys and work as a frontend application allowing easy transaction handling and a good overview of one's cryptocurrencies and digital assets.

Not your keys, not your coins

There are different types of wallets, which differ mainly in usability and security. Software wallets – desktop or mobile – are the most user-friendly and fall into the category of "hot wallets" (because they are online). On the other hand, the so-called "cold wallets" – hard and paper wallets – have lower usability but are highly secure because they are offline and storable with utmost security.

A third wallet type is the so-called "custodial wallet." In such a scenario, third parties, i.e., exchanges or CeFi providers, look after and store the private keys. This is often the easiest and most user-friendly way to handle a wallet, do transactions or to generate yield with the tokens in the wallet.

QUICK TAKEAWAYS

A crypto wallet stores your access keys to your cryptocurrencies and allows you to send or receive payment. Each wallet has a public key, similar to a bank account number, and a private key comparable to a password. It is crucial never to lose control over the private key.

Wallets are classified as "custodial," meaning a third party manages your private key, or "non-custodial," meaning you're the only one who possesses the private key. Custodial wallets require trusting a third party, but they also reduce the risk of losing your private key and being permanently locked out of your wallet.

A solid wallet strategy and thought-through governance are necessary if a business considers using cryptocurrency.

ENTERPRISE ETHEREUM ALLIANCE®

However, it represents the lowest security level because one does not control the private key, and therefore – like keeping money in banks – the owner loses access to his tokens in the event of the counterparty's bankruptcy, for example.

Secure enough for business purposes?

A solid wallet strategy and thought-through governance are necessary if businesses consider investing in cryptocurrencies, run crypto transactions and payments on a regular basis, or buy and hold NFTs.

One of the first questions a company needs to answer is whether they intend to hold and secure tokens in a wallet by themselves or transfer them to a professional, regulated custody provider. If tokens are not needed regularly and have a high value, a custody provider might be the right choice. However, if tokens are transferred regularly and may be needed on short notice, then self-custody within the company is the way to go.

In a self-custody scenario, a company needs to implement a governance approach in which not only one employee but different employees with different roles and responsibilities are involved in approving transactions through a multi-signature wallet. In this case, transactions can only be executed if, for example, three out of four responsible employees sign and confirm a transaction. Additionally, handling the private key or seed phrase is critical if only one person is responsible for storing it securely.

The location determines the regulation

Investors know what to expect when trading stocks since this sector is heavily regulated, protecting investors from fraud or other risks. On the contrary, there is still an international regulatory patchwork with cryptocurrencies or NFTs. You should be aware of the regulatory differences between markets as a business. Especially if you decide to work with a custodial service, you should check the regulations at the domicile of the service. It is strongly advised to consult the expertise of lawyers specializing in this service.

HOW DO I FIND OUT MORE?

Read: Lost Passwords Lock Millionaires Out of Their Bitcoin Fortunes, from the New York Times

Watch: Cryptocurrencies: How Regulators Lost Control, from The Financial Times

Peruse: Cryptocurrency Regulations Around the World, from Comply Advantage

View file on web page

About the EEA

The Enterprise Ethereum Alliance (EEA) enables organizations to adopt and use Ethereum technology in their daily business operations. The EEA empowers the Ethereum ecosystem to develop new business opportunities, drive industry adoption, and learn and collaborate.

To learn more about joining the EEA, reach out to james.harsh@entethalliance.org or visit https://entethalliance.org/become-a-member/.

Follow the EEA on Facebook, Twitter, LinkedIn, and YouTube.

ENTERPRISE ETHEREUM ALLIANCE®