Who are you?

Ramón Martínez rampa@dlthub.eu
BAES blockchain labs
Nov 15th 2018

The Wallet

All blockchain technologies rely on a wallet. A wallet sores the public and private keys of the user. Each pair of keys is called an identity.

The Wallet

Private key: The private key is a SECRET that only the user can know. When the private keys is stored on a file, if the file (and the backups) are lost then the cryptocurrency, tokens and digital assets stored in blockchain are lost forever.

The Wallet

Public key: The public key Public key is the key part that can be shared with all the parties in the network. is used as a method of assuring the confidentiality, authenticity and non repudiation of electronic communications and data storage.

Brain Wallet

When someone remembers the information to regenerate the private and public key pair(, (like a mnemonic sentence, or a password) it is called a brain wallet.

Brain Wallet

Brain wallets should be a good solution to the problem, but then we have a challenge. The mnemonic or password must be strong enough to secure the data and very easy of remember to the user (if he loses it, all assets are gone again)

Multi-factor Authentication

is a method of confirming a user's claimed identity in which a user is granted access only after successfully presenting two or more pieces of evidence (or factors).

Multi-factor Authentication

- Possession: Something the user has
- Knowledge: Something the user knows
- Inherent: Usually biometric data
- Location: Where the user is

Multi-factor Authentication

Possible possession elements:

- A bank card
- An electronic ID CARD
- an electronic certificate
- etc

Multi-factor Authentication

Possible knowledge elements:

- Pin code
- Password
- A memorable sentence
- etc

Multi-factor Authentication

Possible Inherent elements:

- Voice biometrics
- Face biometrics
- Fingerprint
- etc

Multi-factor Authentication

Possible location elements:

- GPS
- Mobile network
- IP address geolocation
- etc

Multi-factor Wallet

The goal is to construct a “multifactor wallet” using at least two of the previous factors (The gps location is not valid for the wallet generator, but very interesting at the exact moment of the transaction (is he at the payment place?, is he in the country he says?) In this way, the user will be able to reconstruct his identity at any time without having to keep his data stored.