



Blockchain and Cryptocurrency

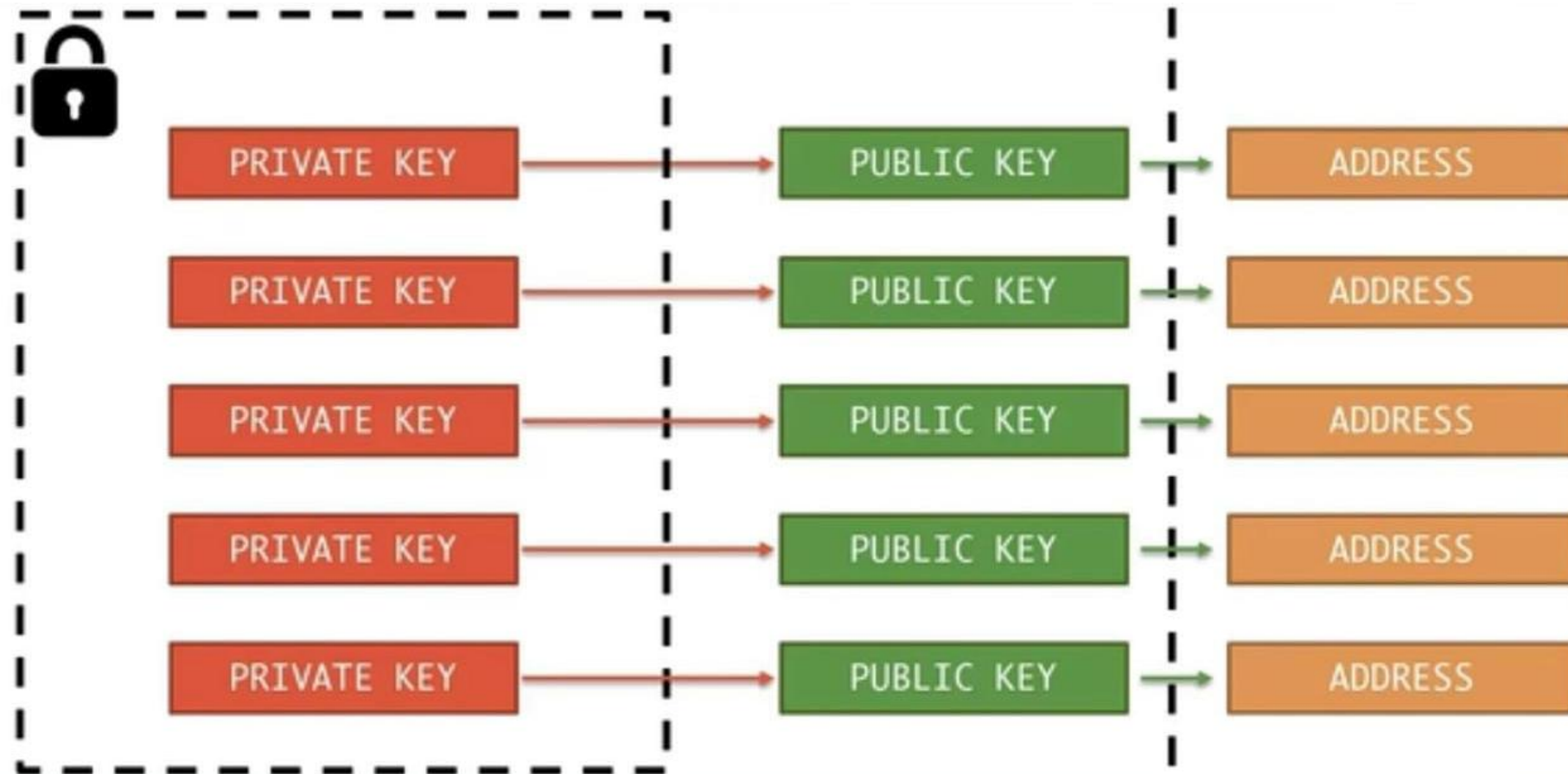
By: Syeda Tayyaba Bukhari



HD(Hierarchically Deterministic) Wallets



Multiple private-public keys for security purpose





MASTER PRIV KEY

PRIVATE KEY

PUBLIC KEY

ADDRESS

+1

PRIVATE KEY

PUBLIC KEY

ADDRESS

+2

PRIVATE KEY

PUBLIC KEY

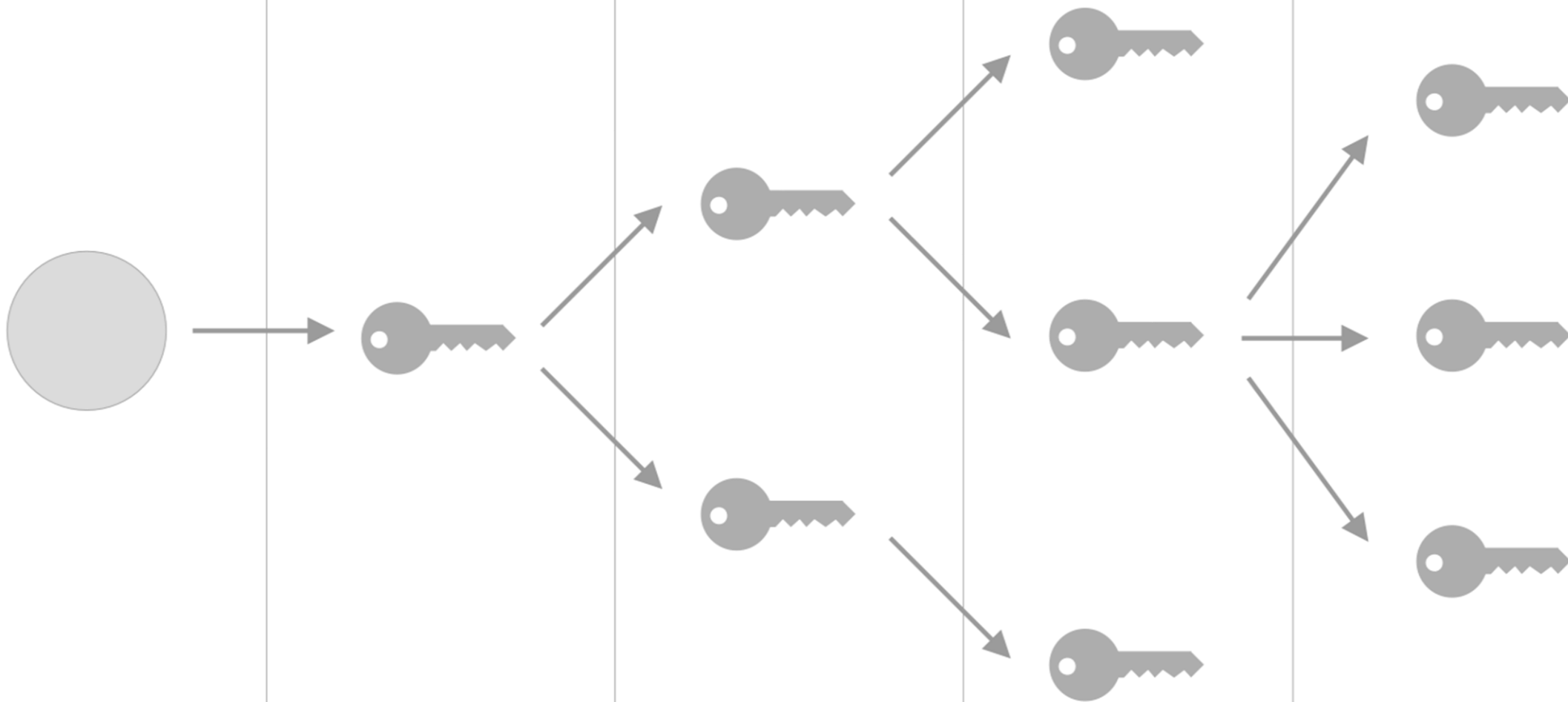
ADDRESS

+3

PRIVATE KEY

PUBLIC KEY

ADDRESS



Additional Reading



DETERMINISTIC WALLETS, THEIR ADVANTAGES AND THEIR UNDERSTATED FLAWS

<https://bitcoinmagazine.com/technical/deterministic-wallets-advantages-flaw-1385450276>



Crypto Wallets



Crypto Wallet

Cryptocurrency Wallet is nothing but a software codings used to store,send and receive cryptocurrency. Crypto wallet is a place that stores private and public keys safely and allows you to interact with various blockchain network which enables users to send and receive virtual currency.

What is a Cryptocurrency Wallet?

Digital wallet

Stores public and private keys

The keys are used to send and receive cryptocurrency

Does not store currency

Cryptocurrency Wallet Terms

Public Key

- Your wallet's public address – used to receive coins to your wallet

Private Key

- A digital signature that proves you own the coins

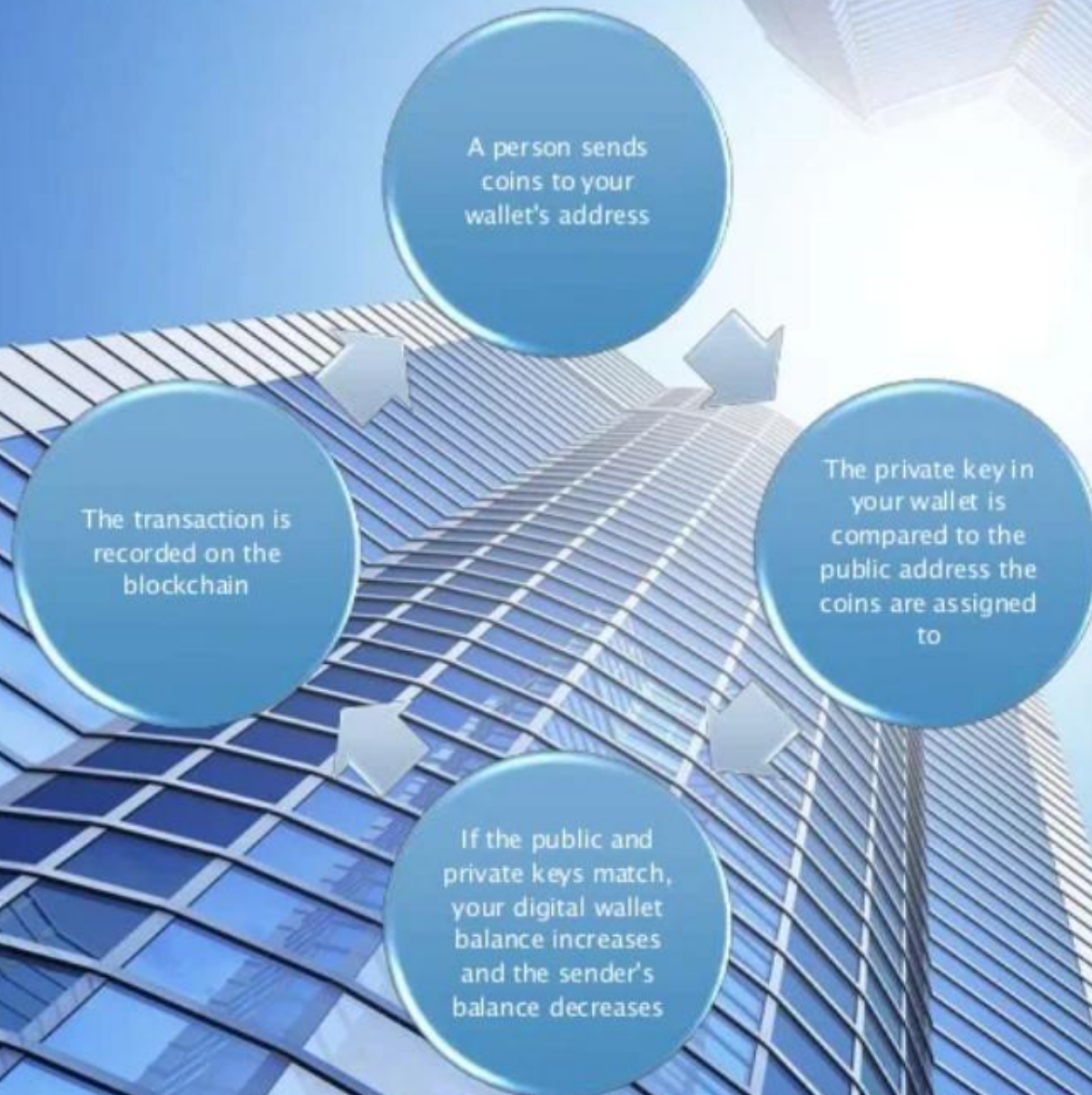
Keystore File

- An encrypted version of your private keys

Mnemonic Phrase (Seed)

- List of words which store all the information needed to recover funds in a wallet

How does it work?



Types of Crypto Wallet

Here are the different types of crypto wallet available.

1. Software Wallet
2. Hardware Wallet
3. Paper Wallet

Types of Crypto Wallet

Software Wallet

Software wallet can again be divided into

1. Desktop Wallet
2. Mobile Wallet
3. Online Wallet

Desktop Wallet

Desktop wallet is one which is downloaded and installed on desktop or laptop. It can be only accessed in the system in which it is downloaded. Desktop Wallet also offers high end security until the system is hacked .When the system gets a virus there is the possibility that you may lose your crypto assets.

Online Wallet

Online Wallet runs on cloud storage and is accessible from any device conveniently. Online Wallet stores private and public key online which is controlled by third party. This makes it more harmful and easily available for hackings and theft.

Mobile Wallet

Mobile wallet is an app that runs on mobile phone , which is more useful that they can be used anytime anywhere. Mobile wallets are usually much smaller and simple as only limited space is available on the mobile.

Software Wallets



How to setup a Software Wallet ex. Coinbase?





Hot wallets

Pros

- Highly accessible
- Available on any internet-enabled device
- Often free of cost

Cons

- Vulnerable to hacking
- Technical issues

Hardware Wallet

Hardware Wallet is more different from Software wallet in the way that they store a user's private and public key on the hardware devices like USB. Even hardware wallet do transaction online, they store cryptos offline which is highly secured.

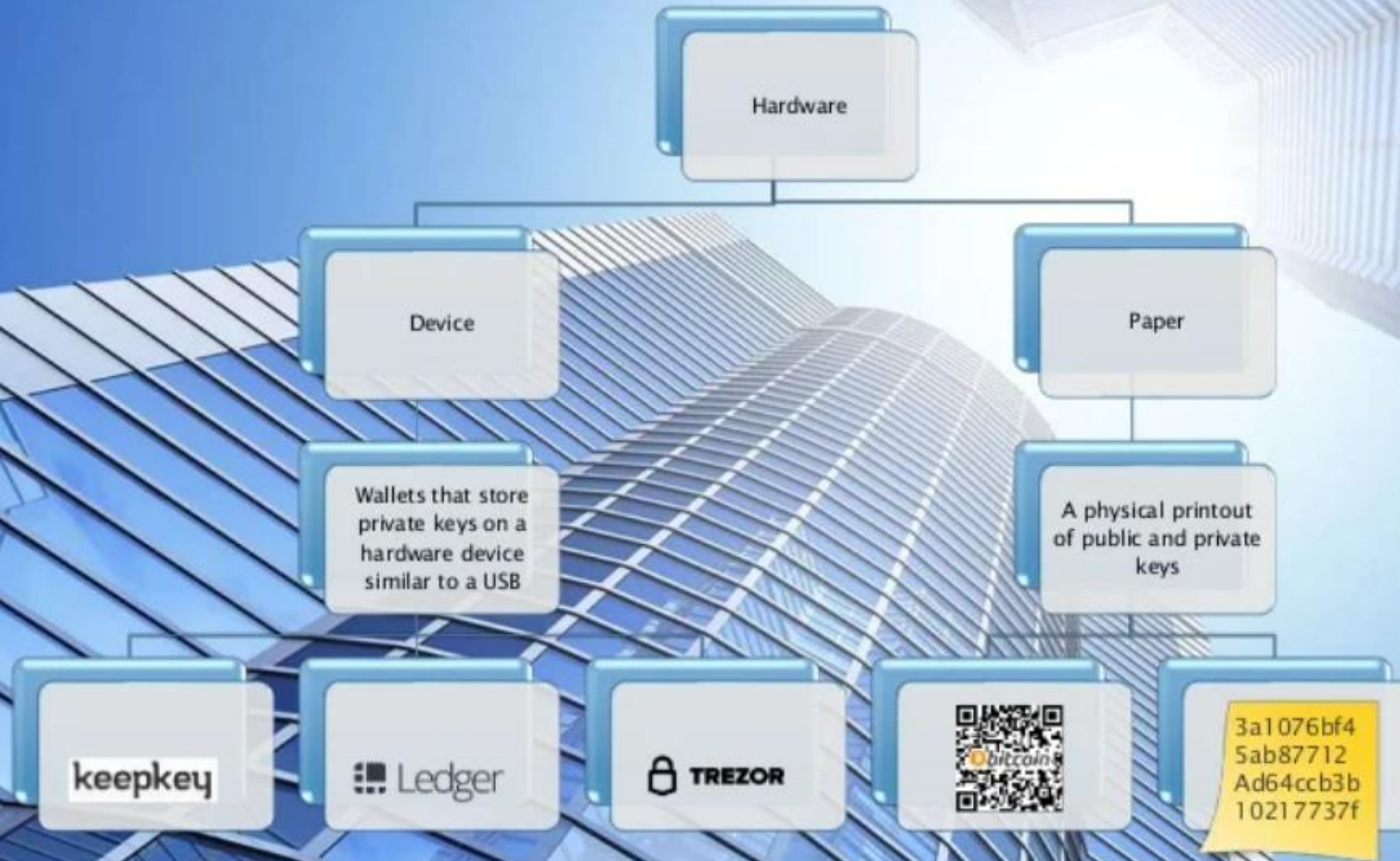
Hardware Wallets



Paper Wallet

Paper wallet is one which provides high level of security to store cryptocurrency. This refer to a physical copy or printout of the public and private keys. Paper wallet can be piece of software that is used to securely generate a pair of keys which are then printed.

Hardware Wallets (“Cold Storage”)



How to setup a Hardware Wallet ex. KeepKey?





Cold wallets

Pros

- Extremely secure
- No issues involving internet

Cons

- Not easily accessible
 - Expensive

To develop your own crypto wallet , contact

Bitdeal - Cryptocurrency Wallet Development Company, which offers complete crypto wallet development services all over the world.