Wallets and cryptocurrencies storage - #05

Blockchain and Distributed Ledger technologies

SAPIENZA
UNIVERSITÀ DI ROMA

Massimo La Morgia
massimo.lamorgia@uniroma1.it

Kind of storage

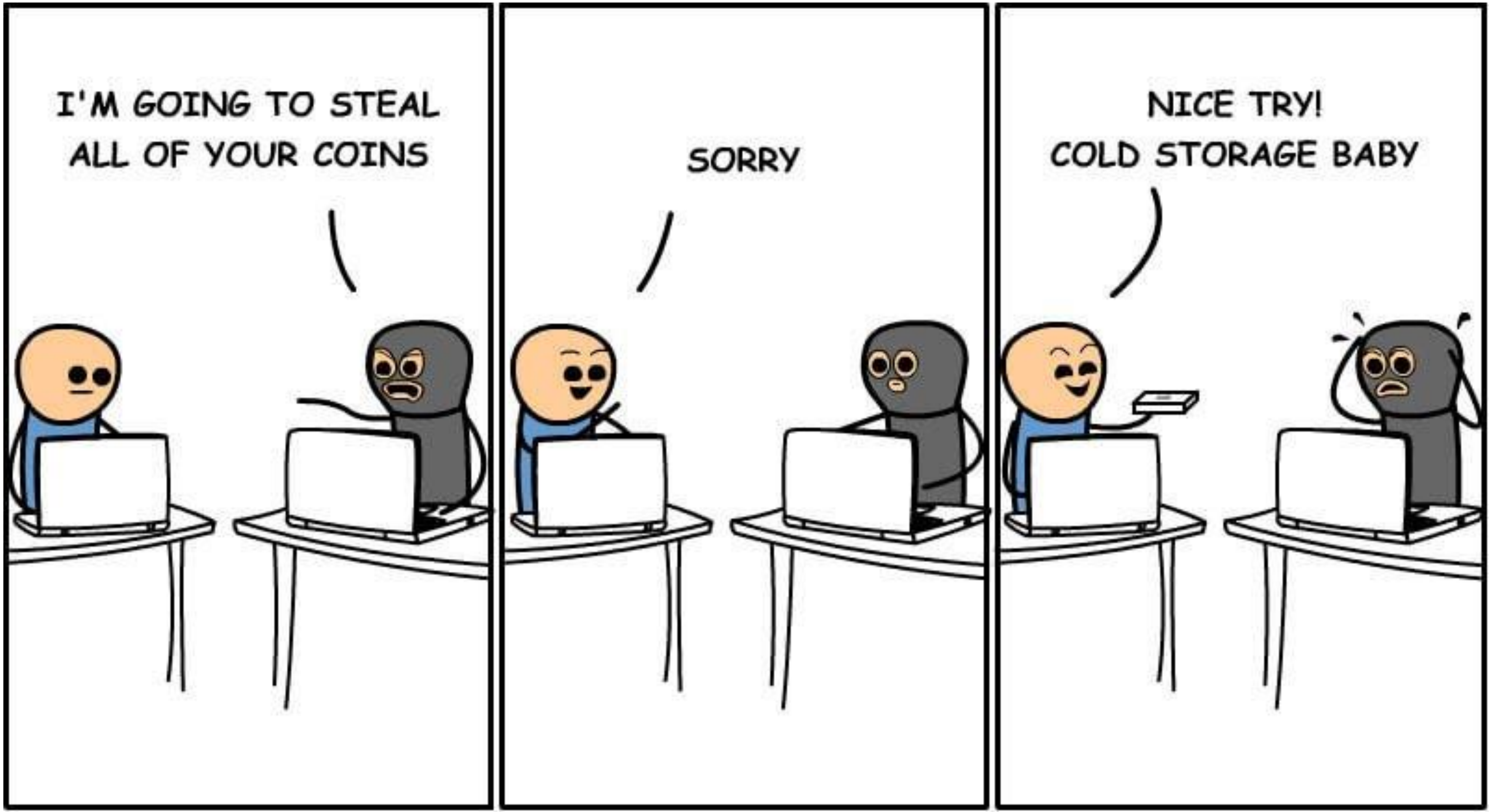
Storing bitcoins is really all about storing and managing Bitcoin secret keys.

Kind of storage

Wallet: it is software that keeps track of all your coins, manages all the details of your keys, and makes things convenient with a nice user interface. Wallet software gives you a simple interface that tells you how much is in your wallet. When you want to spend bitcoins, it handles the details of which keys to use and how to generate new addresses and so on.

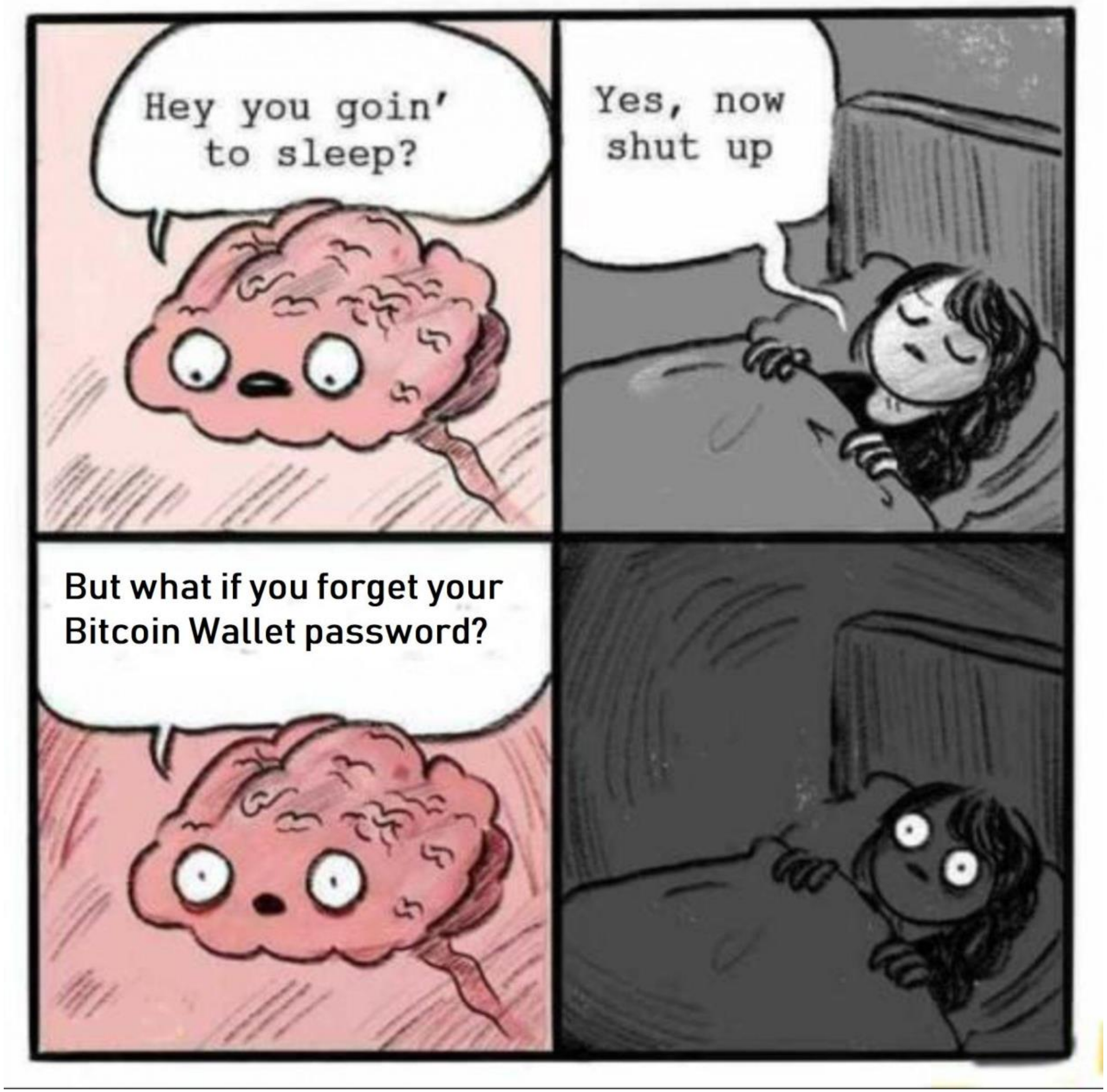
Kind of storage

Cold storage: means storing private keys completely offline This method greatly reduces the risk of theft or unauthorized access, making it ideal for long-term holdings, though it is less convenient for frequent transactions.


I'M GOING TO STEAL ALL OF YOUR COINS
SORRY
NICE TRY! COLD STORAGE BABY

Brain wallet

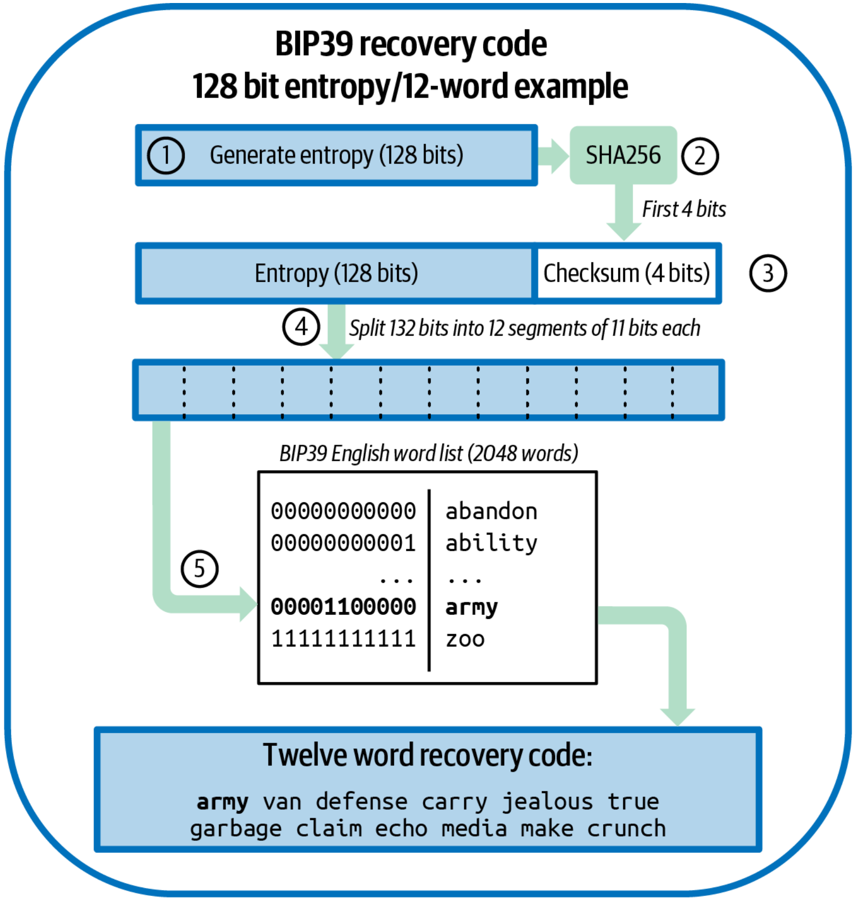
Brain wallet



Seed as English words

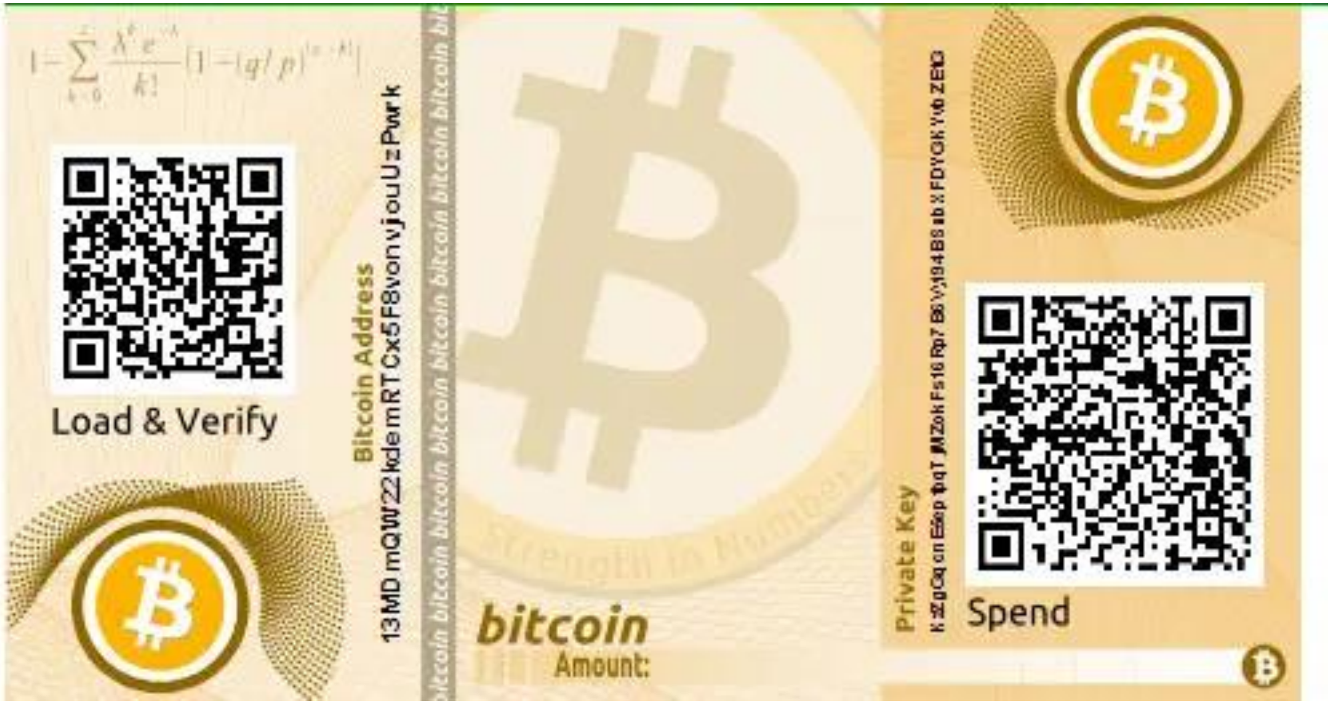
Hex-encoded:
0C1E 24E5 9177 79D2 97E1 4D45 F14E 1A1A

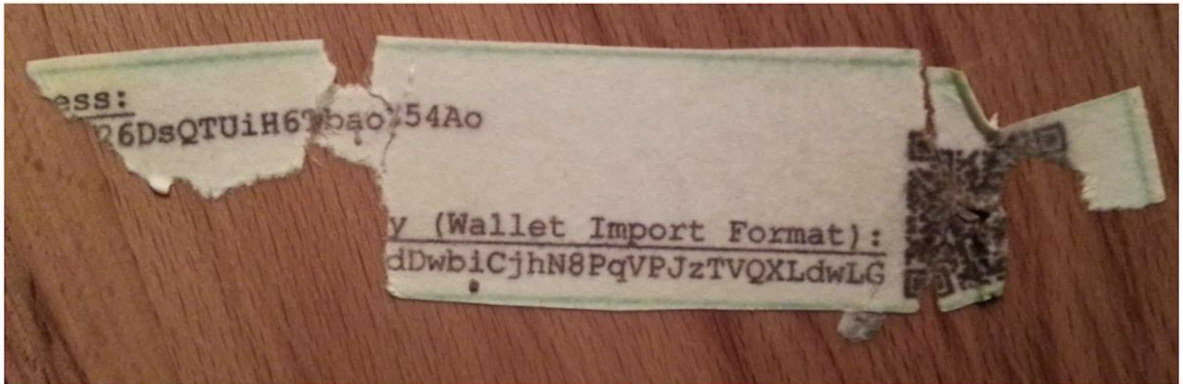
Word-encoded:
army van defense carry jealous true garbage claim echo media make crunch


BIP39 recovery code
128 bit entropy/12-word example
1 Generate entropy (128 bits)
SHA256 2
First 4 bits
Entropy (128 bits)
Checksum (4 bits) 3
4 Split 132 bits into 12 segments of 11 bits each
BIP39 English word list (2048 words)
5
Twelve word recovery code:
army van defense carry jealous true
garbage claim echo media make crunch

00000000000	abandon
00000000001	ability
...	...
00001100000	**army**
11111111111	zoo

Paper wallet

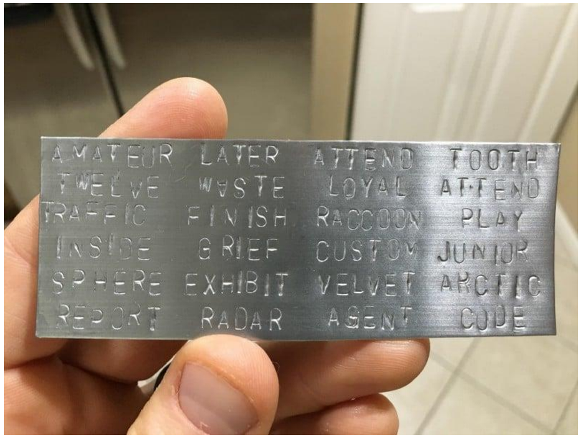


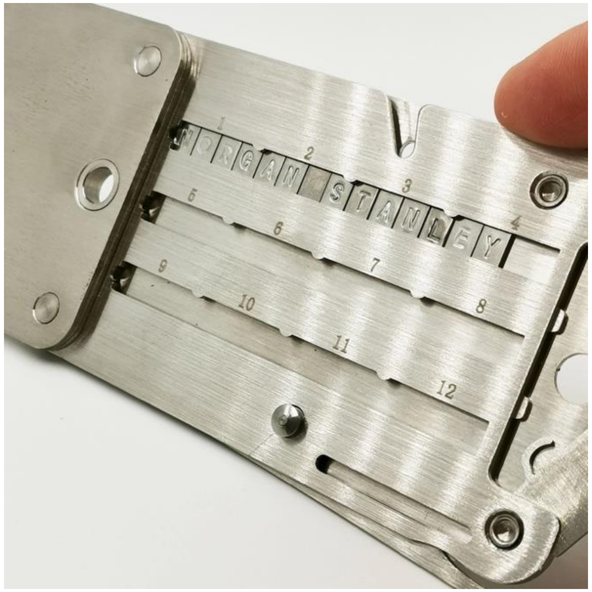


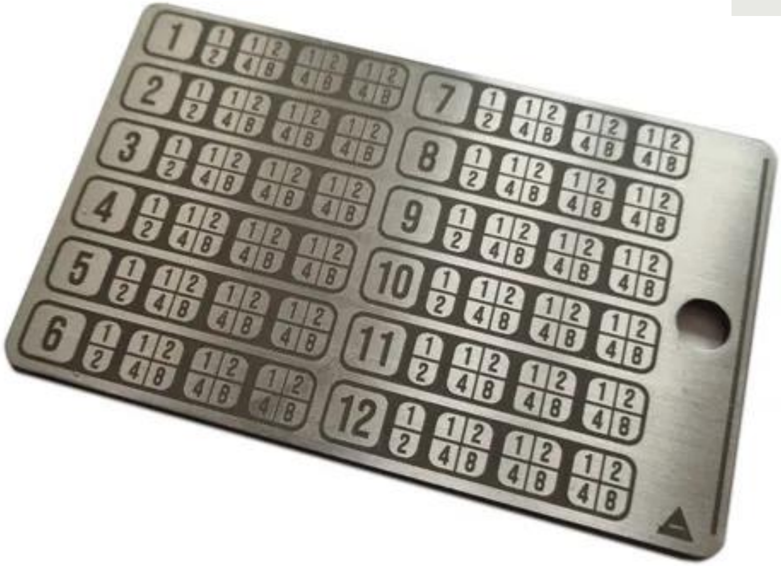
ess:
26DsQTUiH6?bao?54Ao

y (Wallet Import Format):
dDwbiCjhN8PqVPJzTVQXLdwLG

Steel wallet


AMATEUR LATER ATTEND TOOTH
TWELVE WASTE LOYAL ATTEND
TRAFFIC FINISH RACCOON PLAY
INSIDE GRIEF CUSTOM JUNIOR
SPHERE EXHIBIT VELVET ARCTIC
REPORT RADAR AGENT CODE





Tamper proof wallet

Air-Gapped wallet wallet

- Key Generation: Private keys are generated within the device in a secure and offline environment.
- Transaction Signing: When you want to make a transaction, the details are transferred to the air-gapped device through secure methods such as QR codes or microSD cards.
- Confirmation and Authorization: The user verifies the transaction details on the device's display and physically authorizes it.
- Secure Transmission: The signed transaction is then transferred back to the connected device (such as a smartphone or computer) to be broadcast to the blockchain network.

https://www.hardwarewallet.it/en/guides-en/air-gapped-hardware-wallet-no-pc-connection-and-secure/

Kind of storage

Hot storage: refers to keeping Bitcoin private keys on devices connected to the internet. It allows fast and convenient access for transactions but exposes the keys to higher security risks like hacking or malware.

Keeping my cryptocurrency on an exchange
"It's fine, it's totally safe there!"
Exchange gets hacked; me: 😭

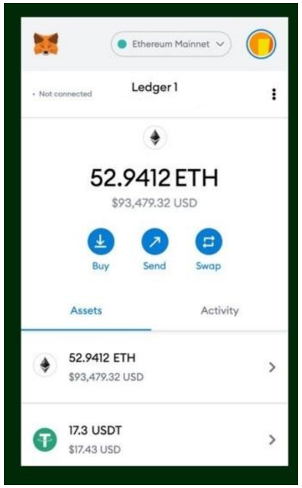
made with AI on imgflip.com based on prefix "Not your Keys not your coins - coins auf Börse lassen"

Hot storage

Non custodial wallet

A non-custodial wallet is a wallet in which you are responsible for storing and managing your private keys. Instead of third parties like crypto exchanges having custodial access, you have full control over your digital assets.

MetaMask is a cryptocurrency wallet and browser extension that allows users to store, send, and receive digital assets, primarily on the Ethereum blockchain and compatible networks. It also acts as a gateway to decentralized applications (dApps), enabling users to interact with smart contracts directly from their browser while maintaining control of their private keys.



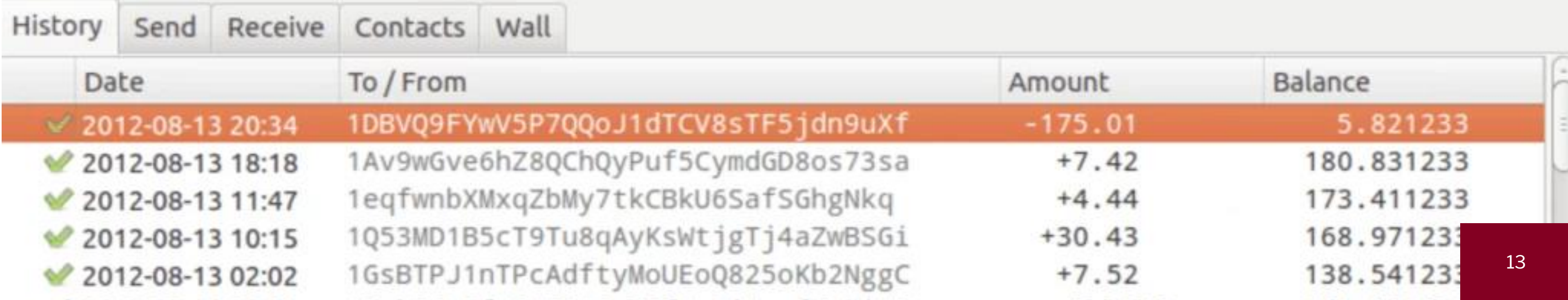
52.9412 ETH
$93,479.32 USD

52.9412 ETH
$93,479.32 USD

17.3 USDT
$17.43 USD

Trust Wallet is a mobile wallet that supports a wide range of cryptocurrencies and blockchains. It gives users full control of their private keys and integrates directly with decentralized exchanges (DEXs) and dApps.

Electrum is one of the oldest Bitcoin wallets, focused on speed, security, and flexibility. It's non-custodial and allows advanced features like hardware wallet integration and custom transaction fees.



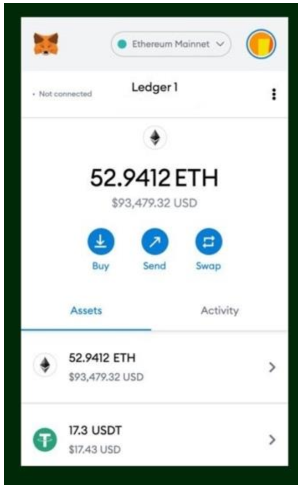
	Date	To / From	Amount	Balance
✓	2012-08-13 20:34	1DBVQ9FYwV5P7QQoJ1dTCV8sTF5jdn9uXf	-175.01	5.821233
✓	2012-08-13 18:18	1Av9wGve6hZ8QChQyPuf5CymdGD8os73sa	+7.42	180.831233
✓	2012-08-13 11:47	1eqfwnbXMxqZbMy7tkCBkU6SafSGhgNkq	+4.44	173.411233
✓	2012-08-13 10:15	1Q53MD1B5cT9Tu8qAyKsWtjgTj4aZwBSGi	+30.43	168.97123
✓	2012-08-13 02:02	1GsBTPJ1nTPcAdftyMoUEoQ825oKb2NggC	+7.52	138.54123

Hot storage

Non custodial wallet

A non-custodial wallet is a wallet in which you are responsible for storing and managing your private keys. Instead of third parties like crypto exchanges having custodial access, you have full control over your digital assets.

MetaMask is a cryptocurrency wallet and browser extension that allows users to store, send, and receive digital assets, primarily on the Ethereum blockchain and compatible networks. It also acts as a gateway to decentralized applications (dApps), enabling users to interact with smart contracts directly from their browser while maintaining control of their private keys.



Ethereum Mainnet

Not connected

Ledger 1

52.9412 ETH

$93,479.32 USD

52.9412 ETH

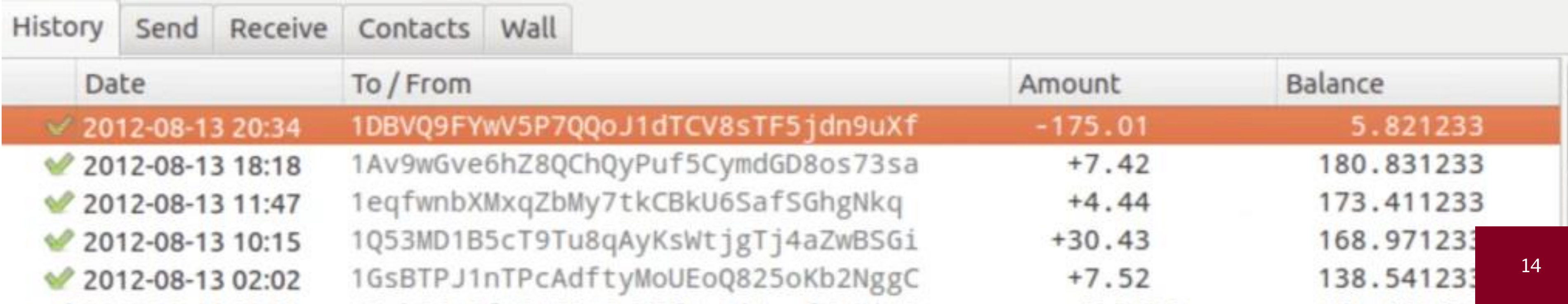
$93,479.32 USD

17.3 USDT

$17.43 USD

Trust Wallet is a mobile wallet that supports a wide range of cryptocurrencies and blockchains. It gives users full control of their private keys and integrates directly with decentralized exchanges (DEXs) and dApps.

Electrum is one of the oldest Bitcoin wallets, focused on speed, security, and flexibility. It’s non-custodial and allows advanced features like hardware wallet integration and custom transaction fees.



	Date	To / From	Amount	Balance
✓	2012-08-13 20:34	1DBVQ9FYwV5P7QQoJ1dTCV8sTF5jdn9uXf	-175.01	5.821233
✓	2012-08-13 18:18	1Av9wGve6hZ8QChQyPuf5CymdGD8os73sa	+7.42	180.831233
✓	2012-08-13 11:47	1eqfwnbXMxqZbMy7tkCBkU6SafSGhgNkq	+4.44	173.411233
✓	2012-08-13 10:15	1Q53MD1B5cT9Tu8qAyKsWtjgTj4aZwBSGi	+30.43	168.97123
✓	2012-08-13 02:02	1GsBTPJ1nTPcAdftyMoUEoQ825oKb2NggC	+7.52	138.54123

Hot storage

Custodial wallet

A non-custodial wallets is that custodial wallets give a third party the permission to hold your private keys, whereas non-custodial wallets give you sovereign control of your private keys.

Third party are usually exchanges.

With a custodial wallet, every transaction requires approval from the central exchange.

The transaction history is also not recorded on the underlying blockchain.

Transaction costs are typically higher due to the involvement of custodians and other intermediaries.

Account creation for custodial wallets may be a lengthier process. Users need to complete Know Your Customer (KYC) and Anti Money Laundering (AML) forms for security and regulatory compliance. This can be a lengthy and time-consuming process.

Custodial wallet users can rely on the custodian to retrieve their password in the case of loss.

Risks of exchanges

Bank run

A bank run is what happens when a bunch of people show up all at once and want their money back. Since the bank maintains only fractional reserves, it might be unable to cope with the simultaneous withdrawals.

https://www.coindesk.com/business/2025/02/22/bybit-sees-over-usd4-billion-bank-run-after-crypto-s-biggest-hack

Fall prey to a frauds

The owner of the exchange is arranging a Ponzi schema or have a bad asset management or simply wants to stole your money (see FTX, Celsius or QuadrigaCX).

Hack

It is the risk that someone, perhaps even an employee of the exchange, will manage to penetrate the security of the exchange. If something goes wrong, your money could get stolen from the exchange (see MTGox, Bybit).

Proof of reserve

The goal is to prove to customers they have the money they deposited or at least a fraction of the money.

First part: prove the amount of reserve the exchange is holding.

The company simply publishes a valid payment-to-self transaction of the claimed reserve amount. Then they sign a challenge string — a random string of bits generated by some impartial party — with the same private key that was used to sign the payment-to-self transaction.
This proves that someone who knew that private key participated in the proof of reserve.

Caveats:

- The exchange can underclaims its reserves.
- It may not actually really owning the given amount of money (e.g. they can be landed money.).

Proof of liabilities

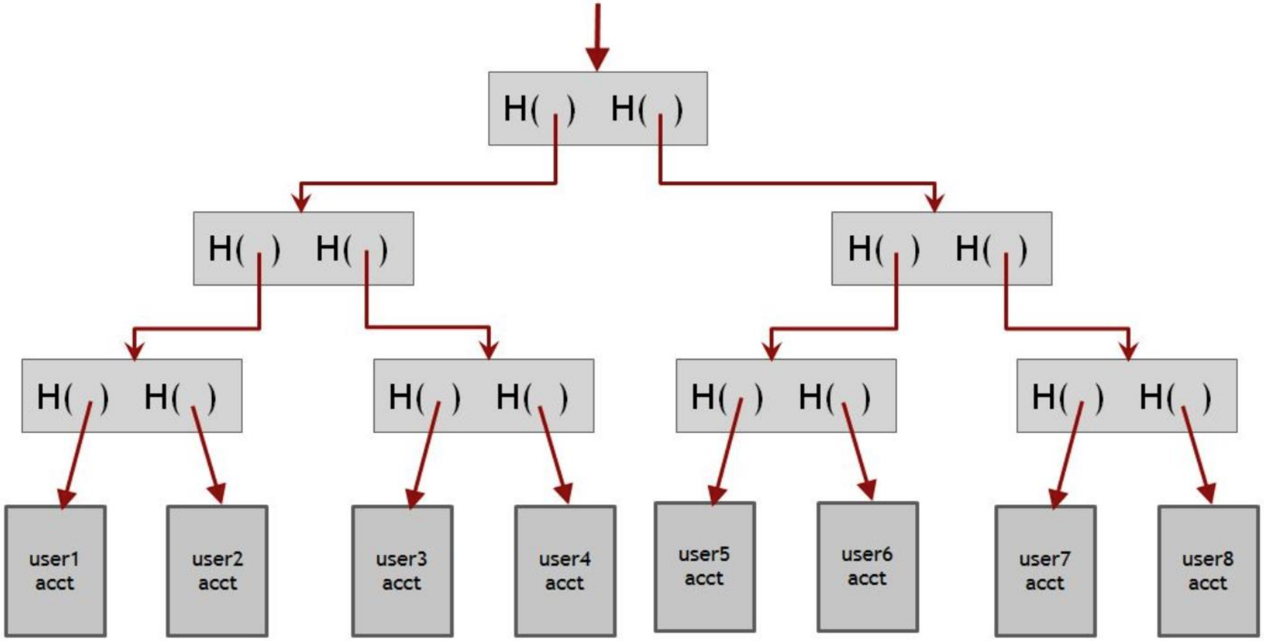
The goal is to to prove how many demand deposits you hold.

Simple way: publish the amount of assets deposited by each users and their username. Anyone can calculate the total liabilities

Caveat:

- Privacy

The crypto way: the exchange build a Merkle-tree in which each leaf correspond to a user and contains the deposited amounts. Each node contains the hash-pointer and the sum of the value of the sub-tree and publish the root of the Merkle-tree.



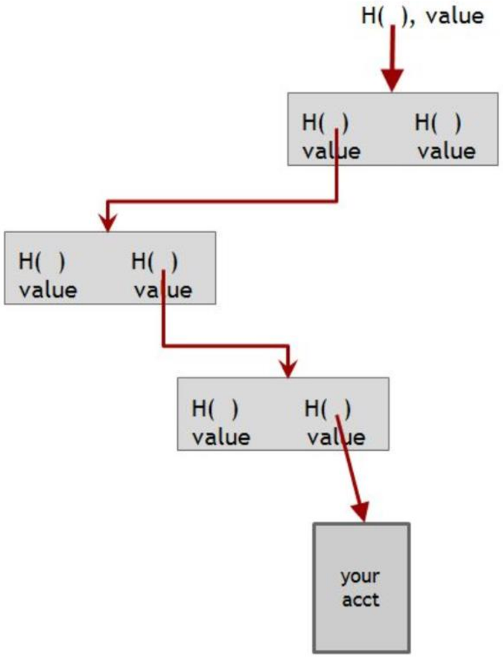
Proof of inclusion

The goal is to prove the customers that their liabilities are included in the Merkle-tree

The exchange shows the customer the partial tree from the customer's leaf up to the root

The customer verifies that:

1. The root hash pointer and root value are the same as what the exchange signed and published.
2. The hash pointers are consistent all the way down, that is, each hash value is indeed the cryptographic hash of the node it points to.
3. The leaf contains the correct user account info (say, username/user ID, and deposit amount).
4. Each value is the sum of the values of the two values beneath it.
5. Neither of the values is a negative number.

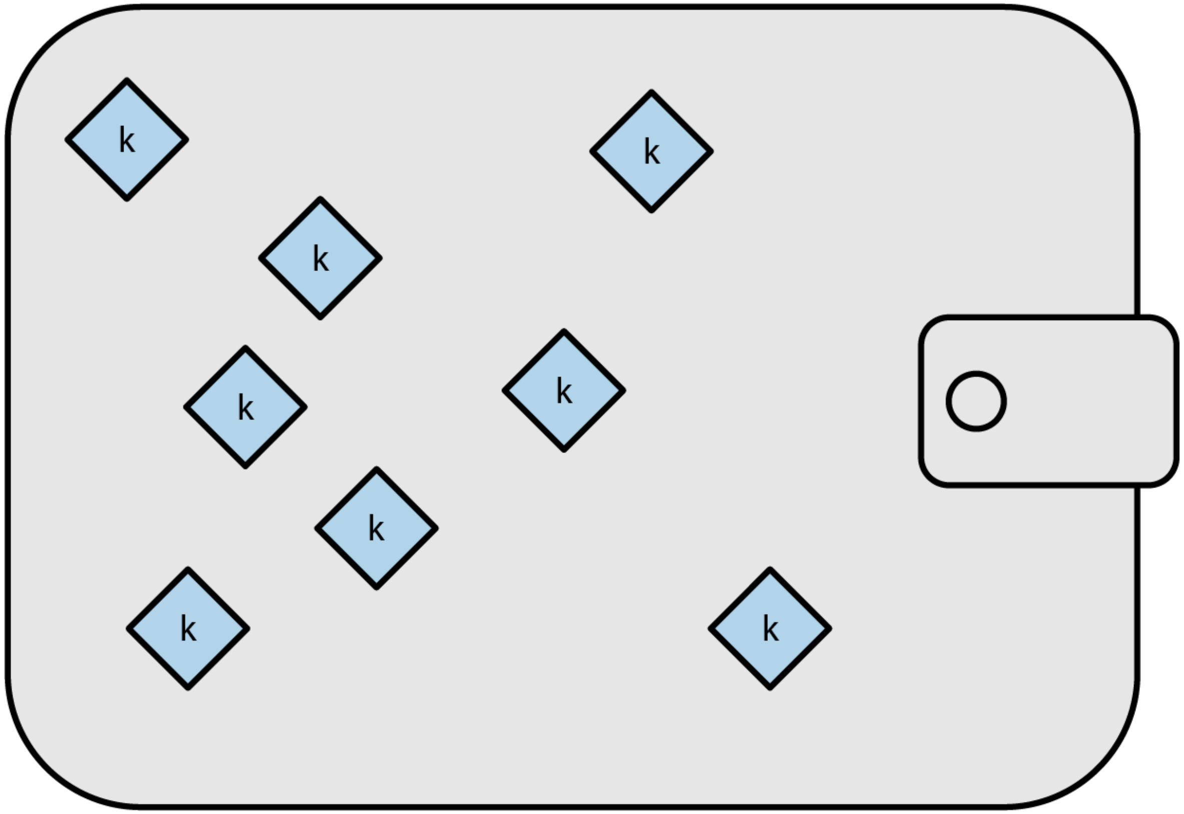


Private key generation

In ECDSA the private key is a large, randomly generated number x.
The public key is g^x, while g is the generator point of the elliptic curve (secp256k1 for bitcoin).

Nondeterministic key generation

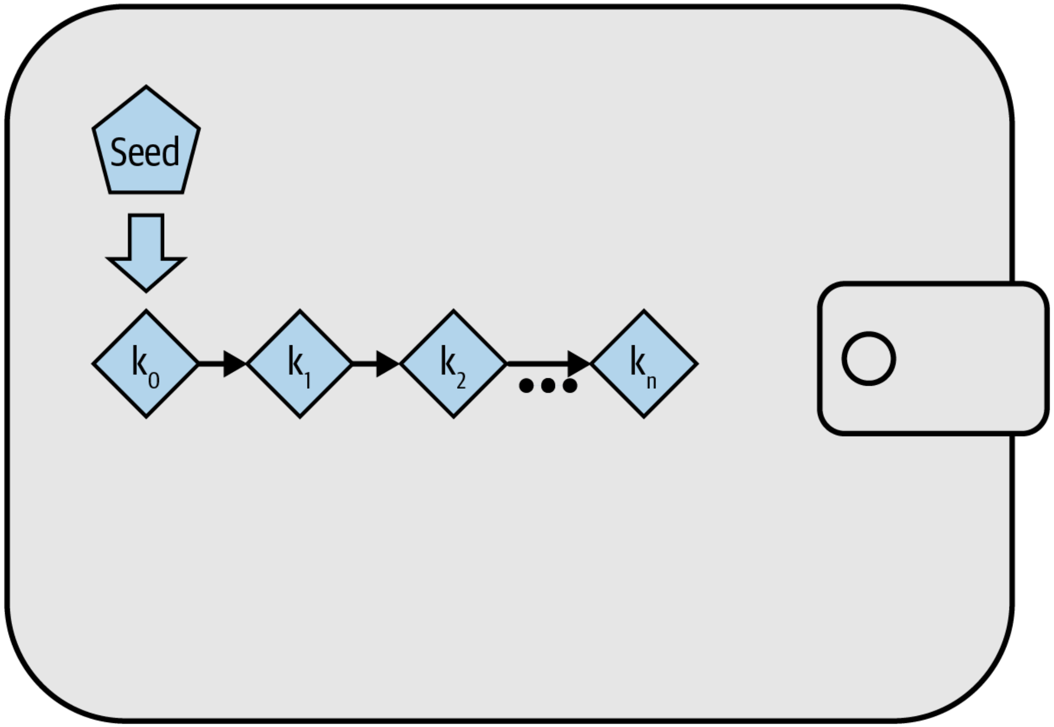
A wallet application can independently generate each of the wallet keys it later plans to use.
It required users to back up the wallet database.
For each independently generated key, the user would need to back up about 32 bytes.



Deterministic key generation

In ECDSA the private key is a large, randomly generated number *x*.
The public key is g^x, while g is the generator point of the elliptic curve (secp256k1 for bitcoin).

Private key generation info: x
i^{th} *private key*: $x_i = \mathrm{x} + \mathrm{i}$
Address generation info: g^{x}
i^{th} *public key*: $g^{\mathrm{x+i}}$
i^{th} *address*: *H*($g^{\mathrm{x+i}}$)



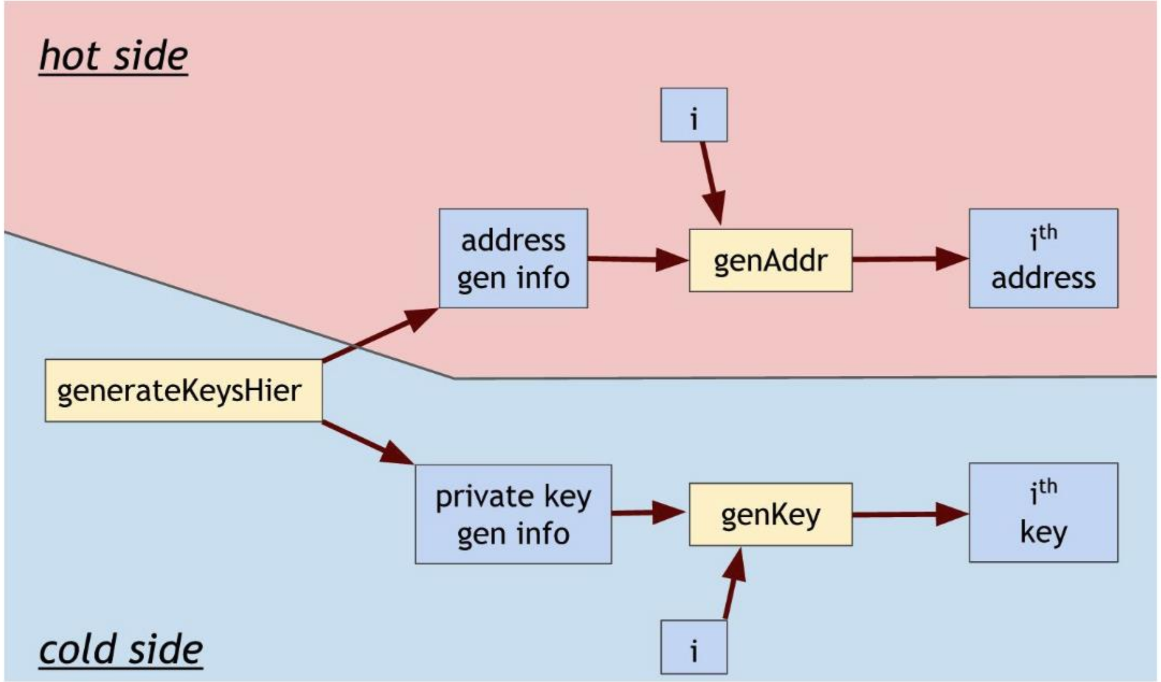
Hierarchical-Deterministic key generation

Private key generation info: k , x , y

It is used x as seed to generate other two random numbers *k* and *y*.
i^{th} *private key:* $x_i = y + H(k||i)$

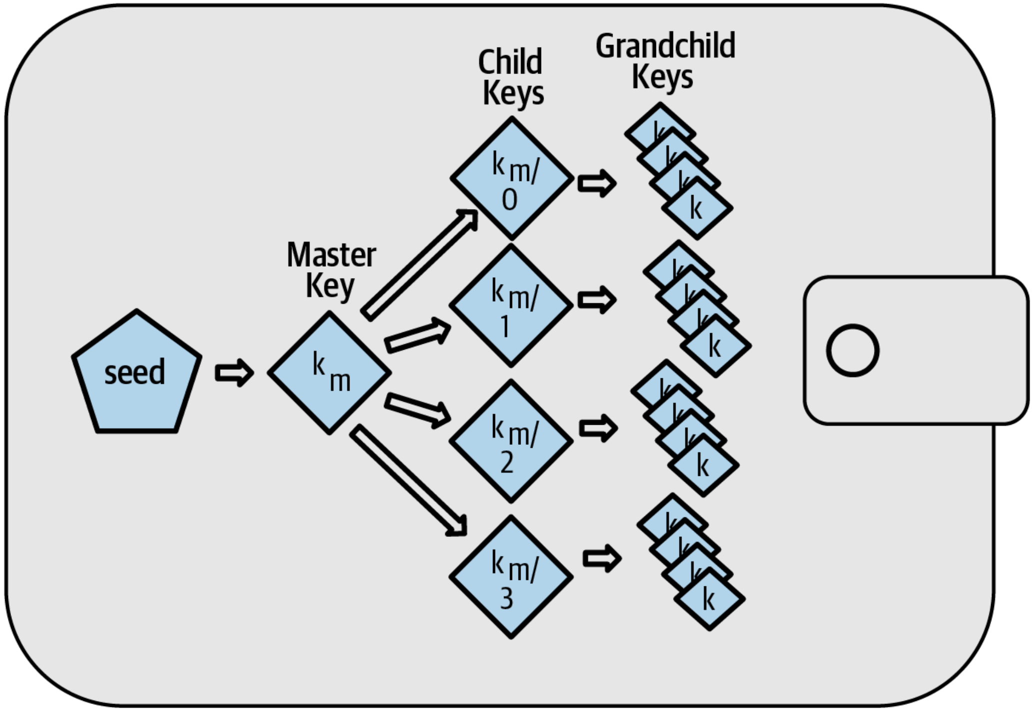
Address generation info: k , g^y
i^{th} *public key:* $g^{x_i} = g^{H(k||i)} + g^y$
i^{th} *address:* H(g^{x_i})

A user of deterministic key generation can back up every key in their wallet by simply recording their seed and a reference to the deterministic algorithm they used.



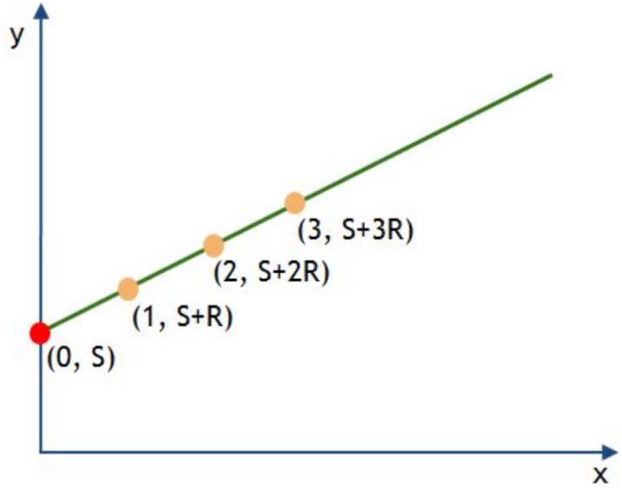
Tree Hierarchical-Deterministic key generation

It is possible to use a combination of HD and deterministic keys to produce a tree of keys. Branches of keys can also be used in corporate settings, allocating different branches to departments, subsidiaries, specific functions, or accounting categories.



Secret sharing

We want to divide our secret key into some number N of pieces. We want to do it in such a way that if we're given any K of those pieces then we'll be able to reconstruct the original secret, but if we're given fewer than K pieces then we won't be able to learn anything about the original secret.



Equation	Degree	Shape	Random parameters	Number of points (K) needed to recover S
(S + RX) mod P	1	Line	R	2
$(S + R_1X + R_2X^2)$ mod P	2	Parabola	R_1, R_2	3
$(S + R_1X + R_2X^2 + R_3X^3)$ mod P	3	Cubic	R_1, R_2, R_3	4

Multi-signature

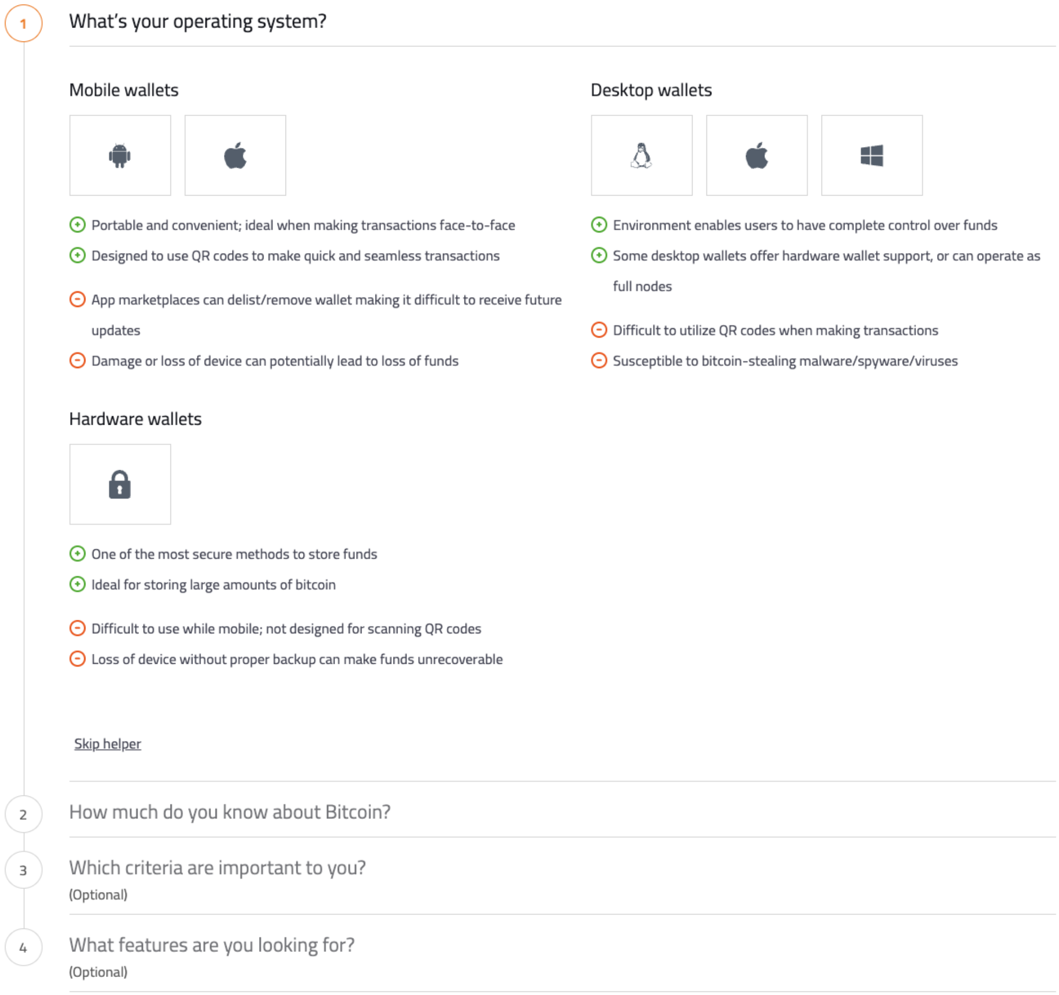
Bitcoin script directly allows you to stipulate that control over an address be split between different keys. These keys can then be stored in different locations and the signatures produced separately.

A multisig is composed of one or more addresses and a threshold. The threshold defines how many signatories (participating addresses) need to agree on submitting an extrinsic for the call to be successful.

For example, Alice, Bob, and Charlie set up a multisig with a threshold of 2. This means Alice and Bob can execute any call even if Charlie disagrees with it. Likewise, Charlie and Bob can execute any call without Alice. A threshold is typically a number smaller than the total number of members but can also be equal to it, which means they all have to agree.

Pick your wallet

https://bitcoin.org/en/choose-your-wallet



1 What's your operating system?

Mobile wallets

- ⊕ Portable and convenient; ideal when making transactions face-to-face
- ⊕ Designed to use QR codes to make quick and seamless transactions
- ⊖ App marketplaces can delist/remove wallet making it difficult to receive future updates
- ⊖ Damage or loss of device can potentially lead to loss of funds

Desktop wallets

- ⊕ Environment enables users to have complete control over funds
- ⊕ Some desktop wallets offer hardware wallet support, or can operate as full nodes
- ⊖ Difficult to utilize QR codes when making transactions
- ⊖ Susceptible to bitcoin-stealing malware/spyware/viruses

Hardware wallets

- ⊕ One of the most secure methods to store funds
- ⊕ Ideal for storing large amounts of bitcoin
- ⊖ Difficult to use while mobile; not designed for scanning QR codes
- ⊖ Loss of device without proper backup can make funds unrecoverable

2 How much do you know about Bitcoin?

3 Which criteria are important to you?
(Optional)

4 What features are you looking for?
(Optional)