

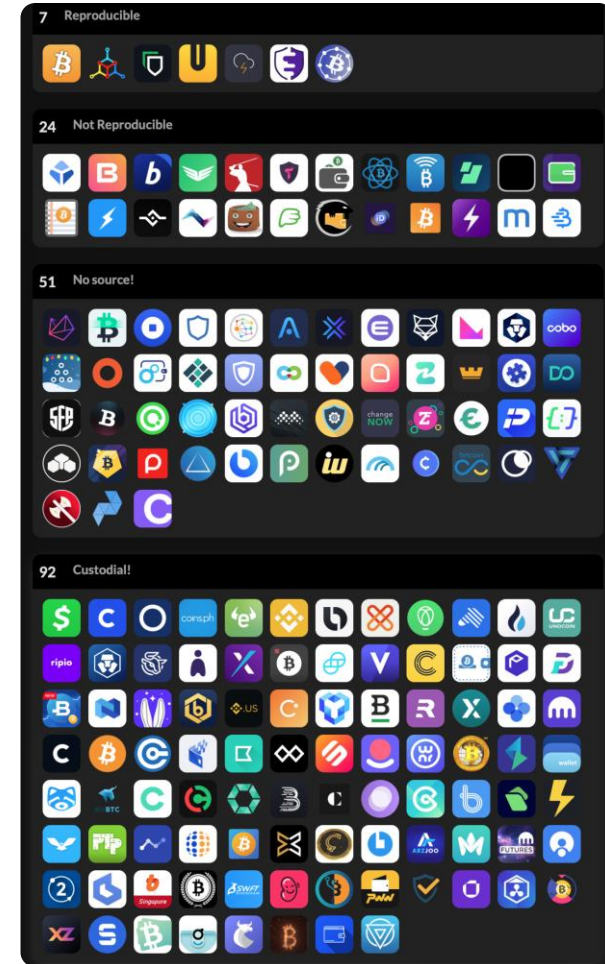
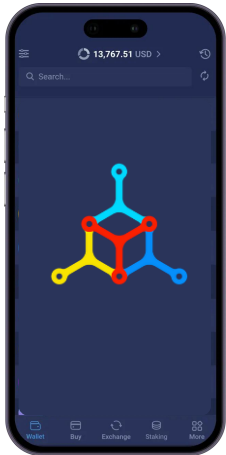


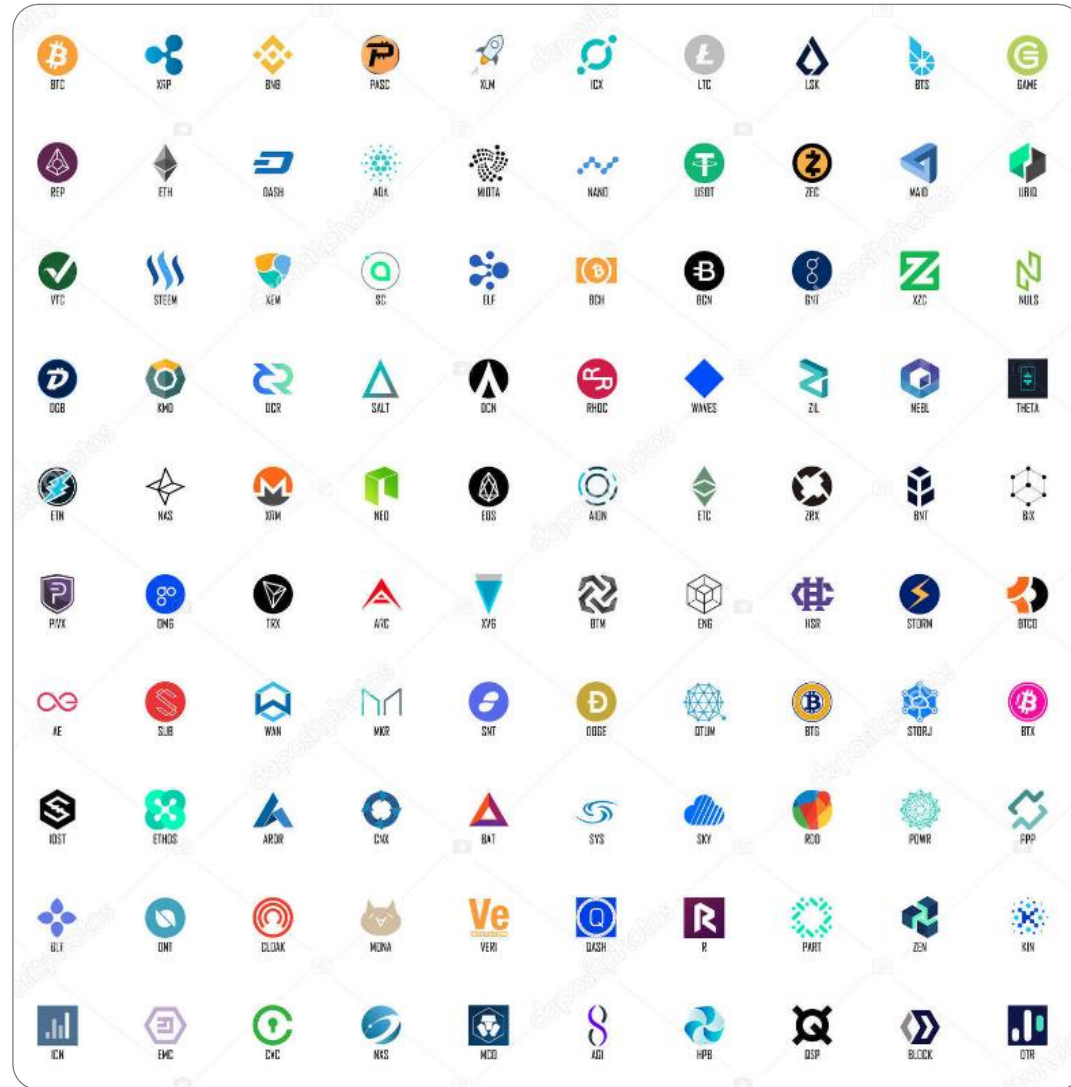
BitcoinBadger.net

## 6: Wallet derivation path













**1**A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

**3**J98t1WpEZ73CNmQviecnyiWrnqRhWNLy

**bc1**qar0srrr7xfkvy5l643lydnw9re59gtzwwf8k3y

**bc1p**5d7rjq7g6rdk2yhzks9smlaqtedr4dekq08ge8ztwac72sfr9rusxg3297



**0x**742d35Cc6634C0532925a3b844Bc454e4438f44e

**0x**71C7656EC7ab88b098defB751B7401B5f6d8976F

**0x**b794f5ea0ba39494ce839613fffba74279579268



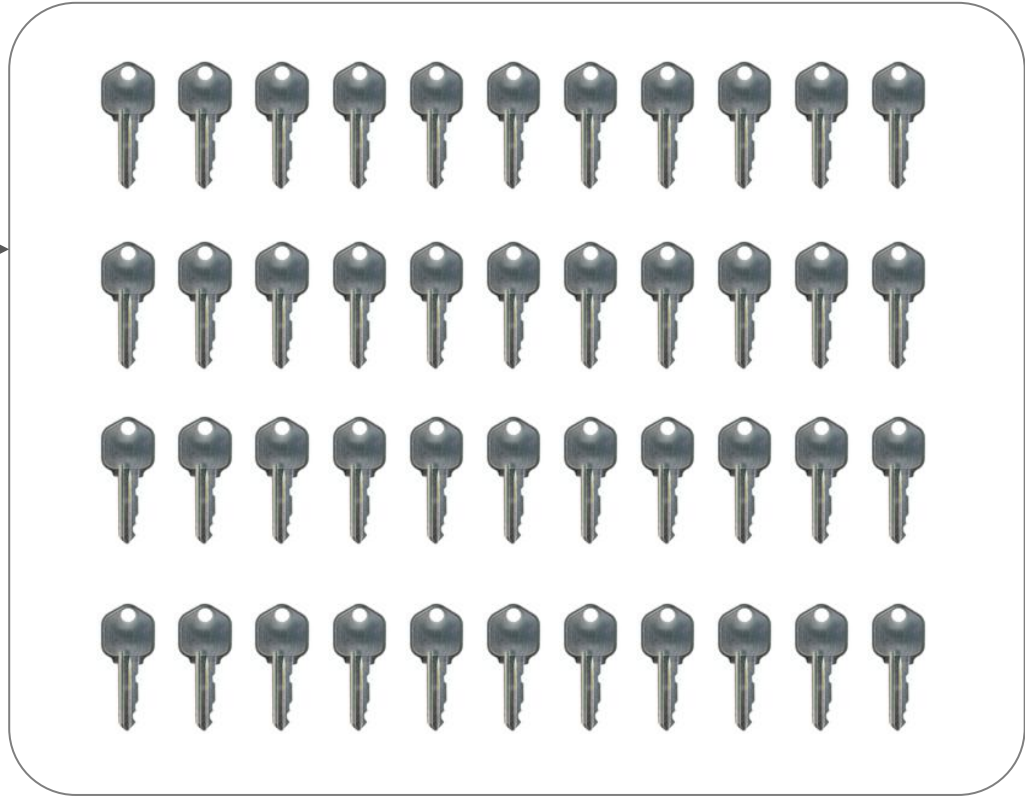


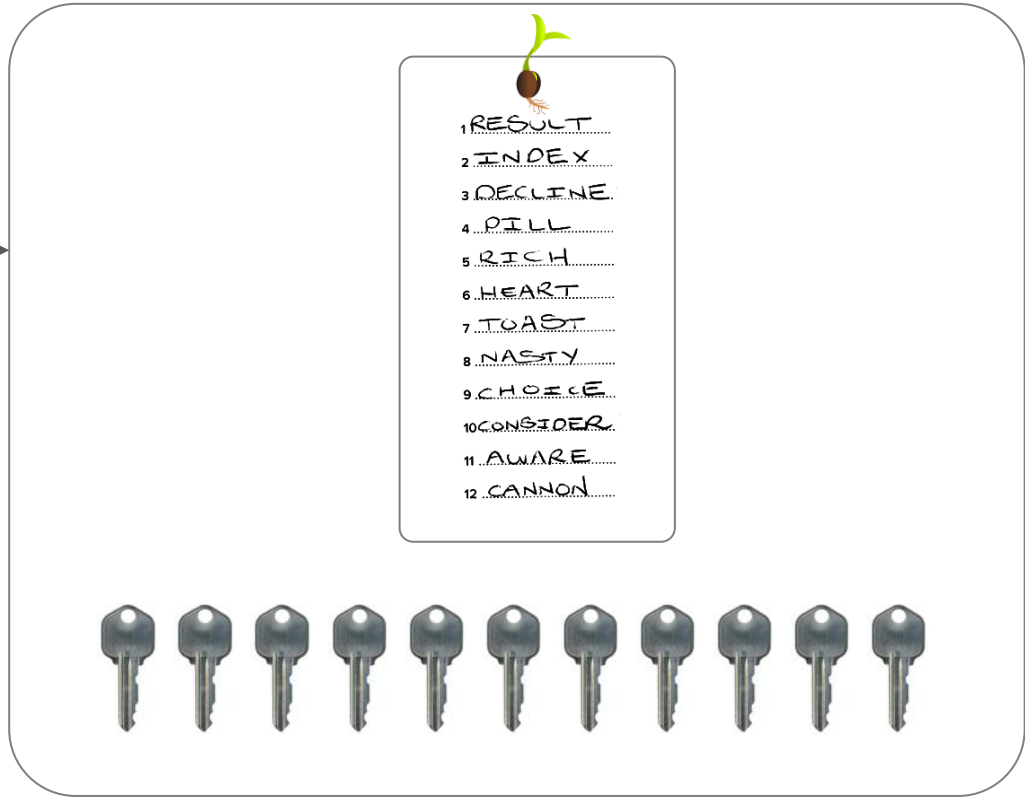
**4**5GjcbHh1fvEyXEA6mDAKqNDMmy1Gon6CNHrdhp9hghfLXQnQj4J76TLtwYGoooKApWLM7kaZwdAxLycceHmuVcELCSFPHQ

**8**4EgZVjXKF4d1JkEhZSxm4LQQEx64AvqQEwkvWptHEb5JMrB1Y86y1vCPSCiXsKzbfS9x8vCpx3gVgPaHCpobPYqQzANTnC

**8**FKZ5LYDj98gmRH9ex4GCUi7SCpBeckyX5vi97A2YSN9a5wHYGXXkfMfZXHXZGJn87X6NDHAB2jZWWRnnysWoeHTw6XGSCDXRo

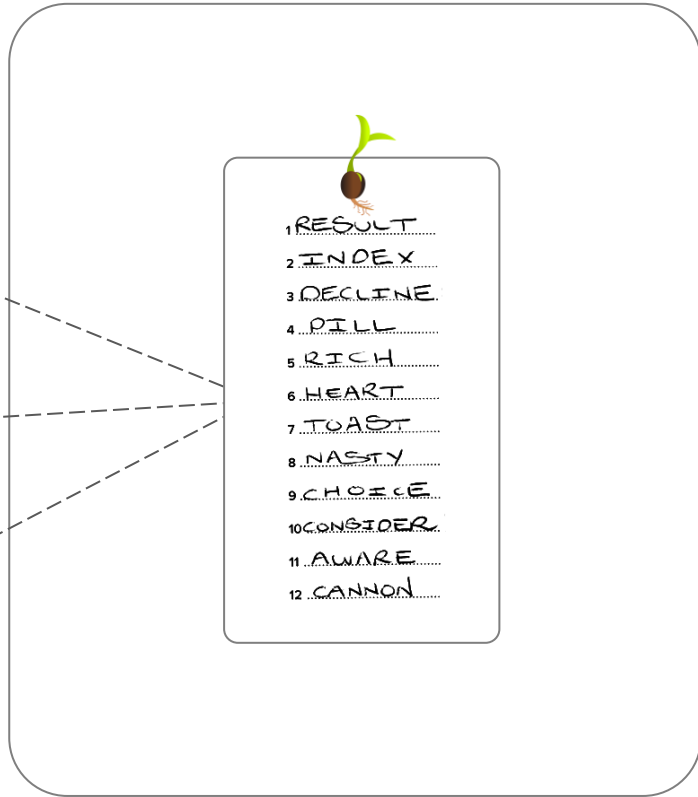






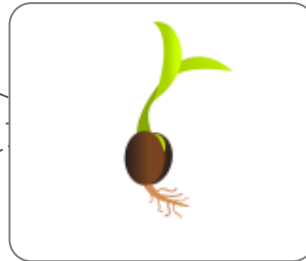




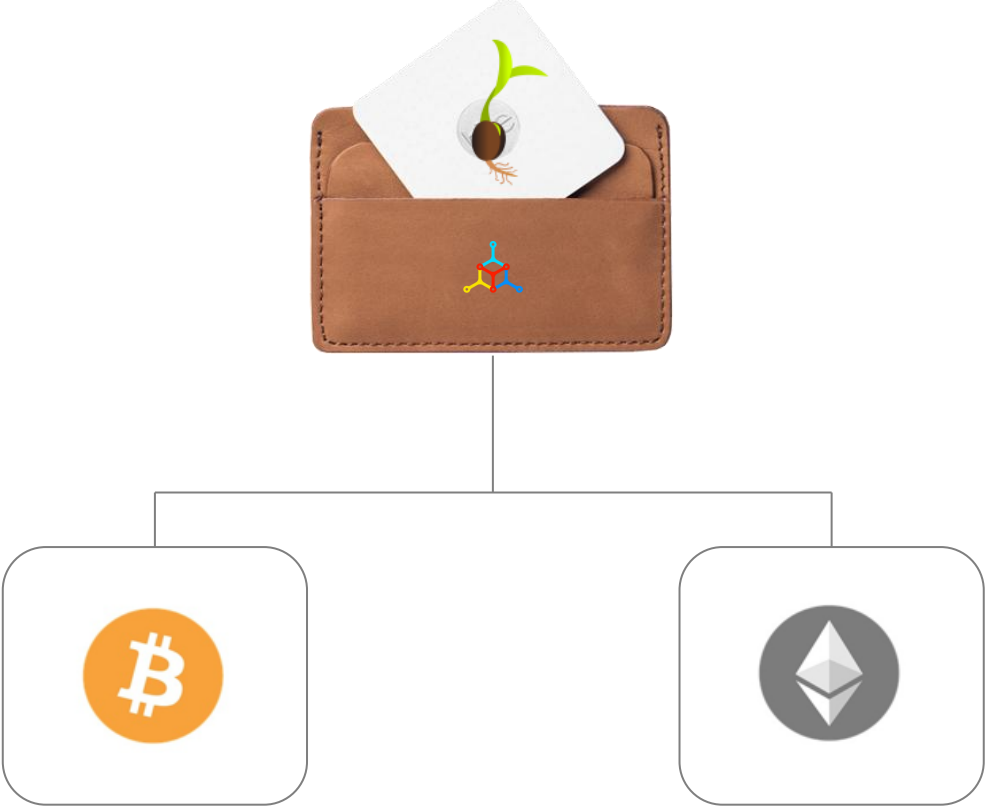




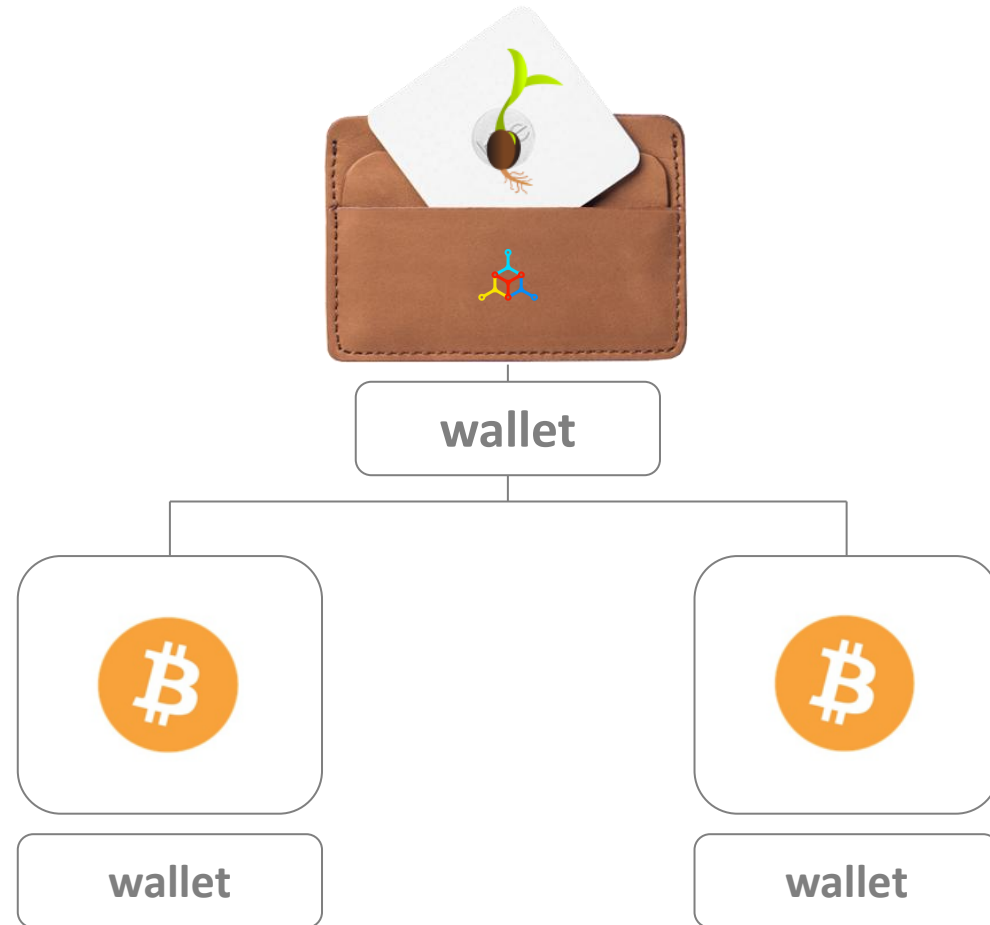
HD wallets:





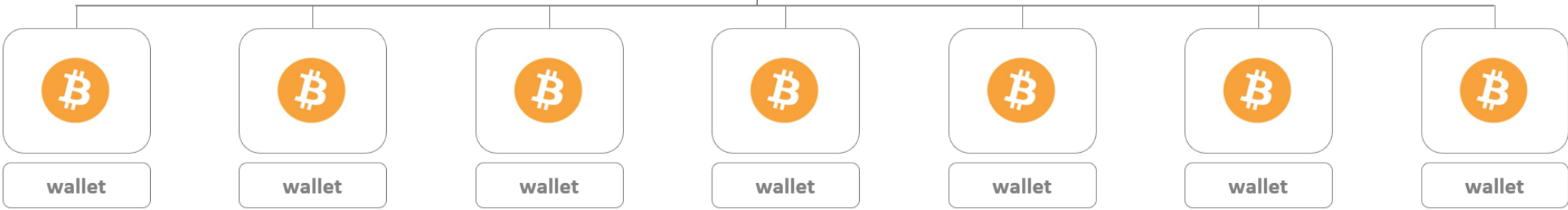


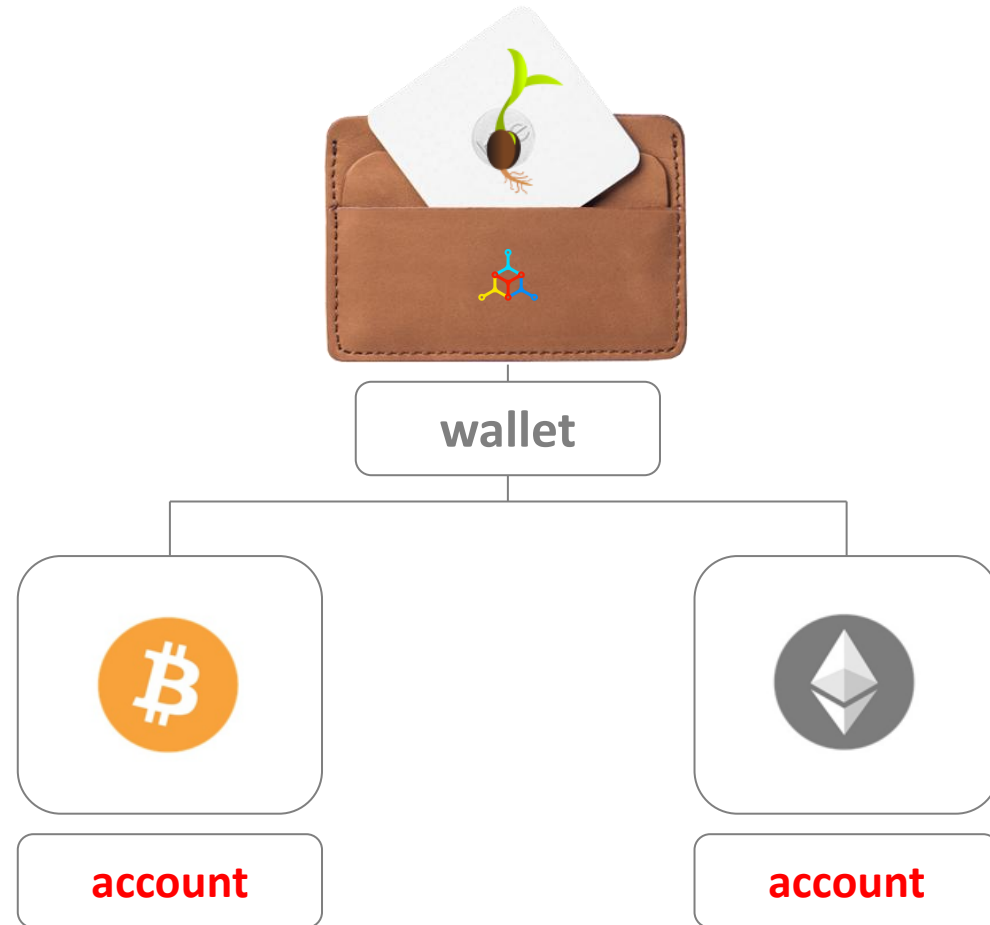


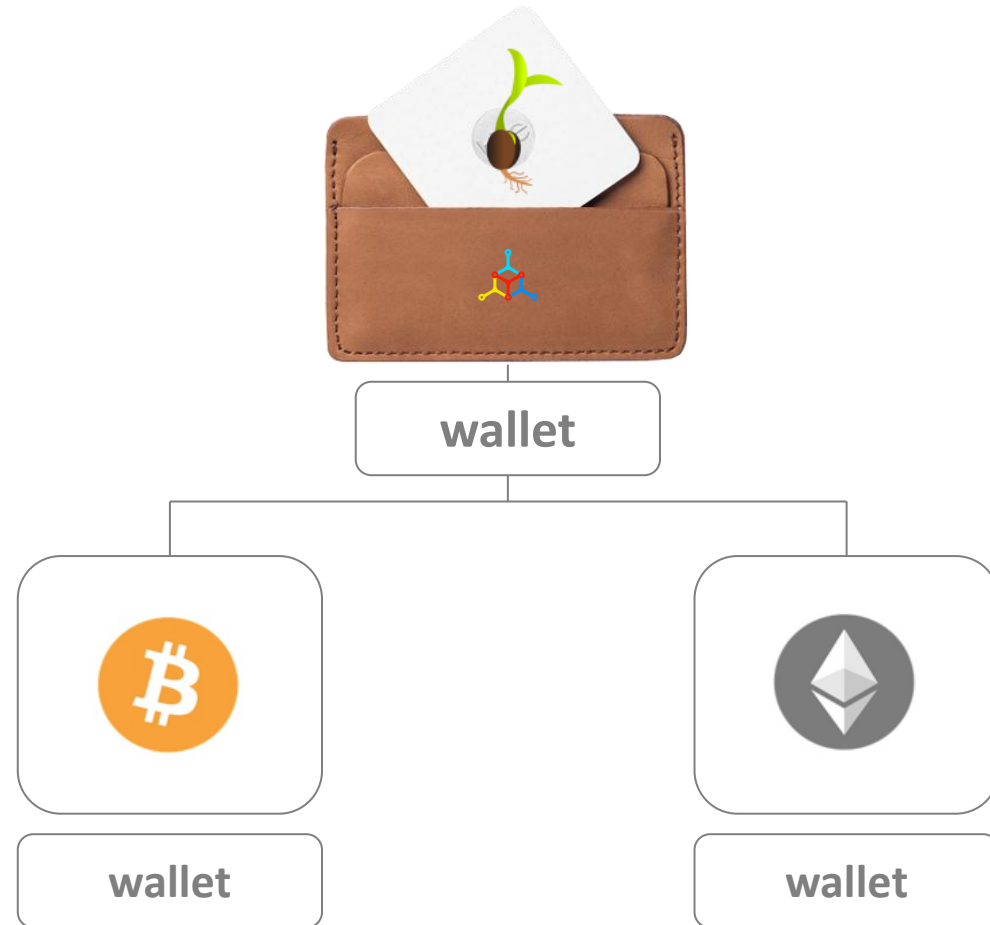




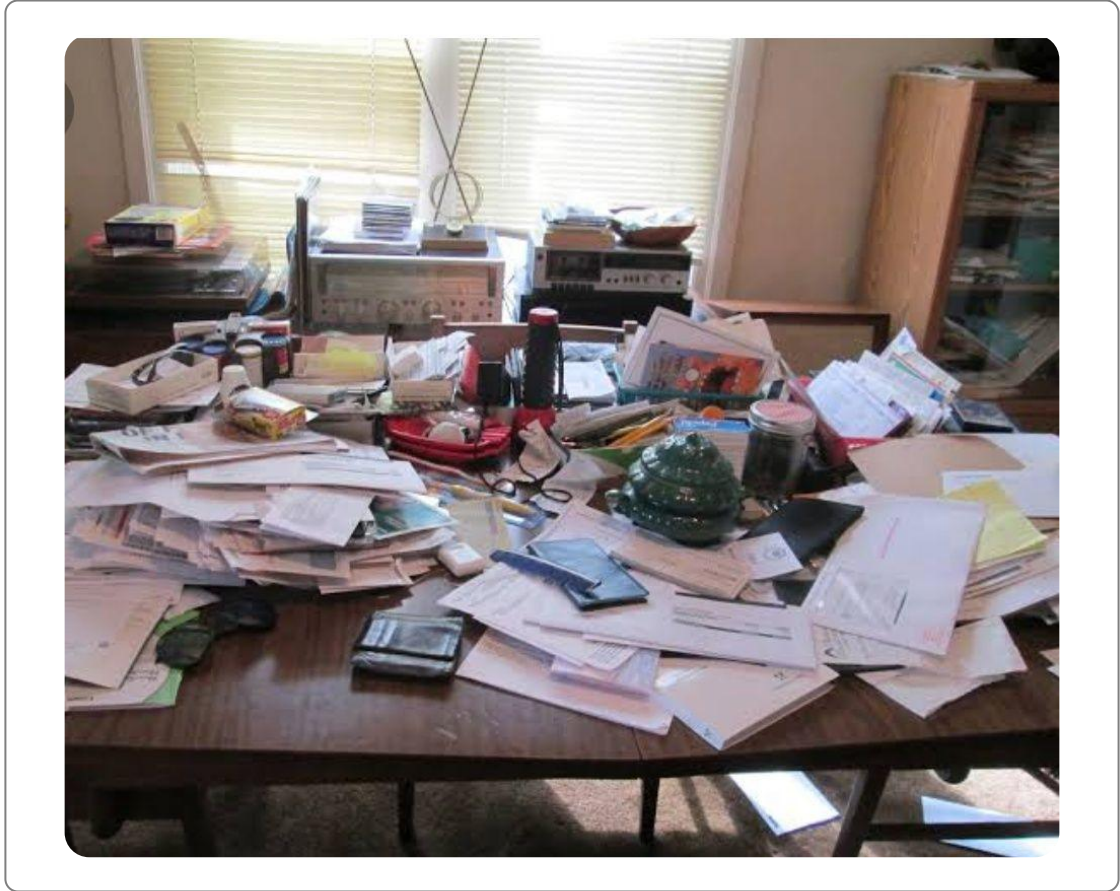
wallet







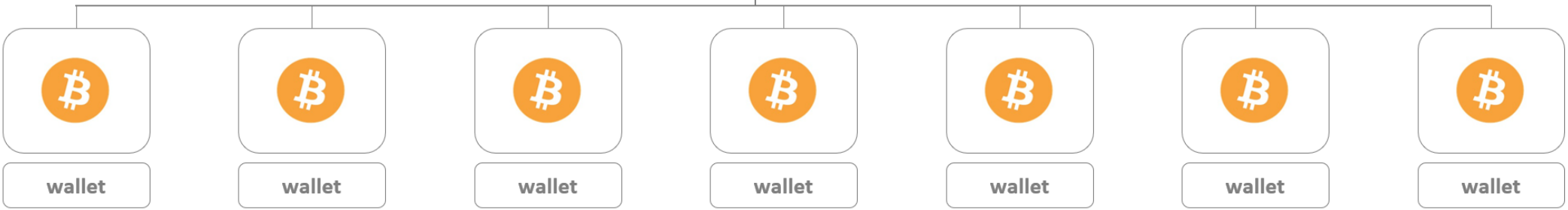








wallet



passphrase1

passphrase2

passphrase3

passphrase4

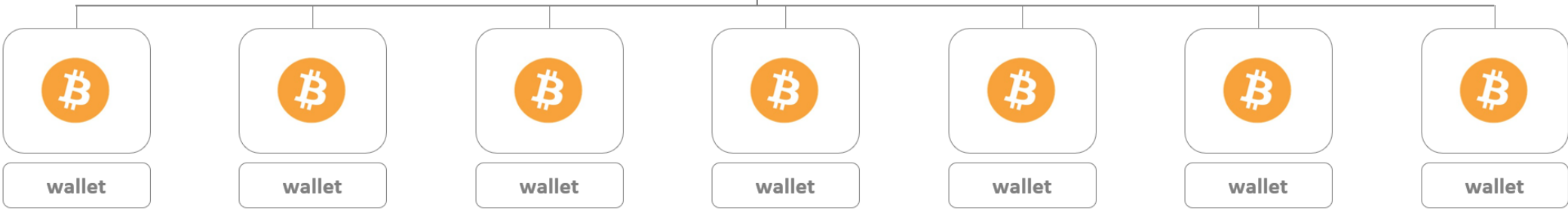
passphrase5

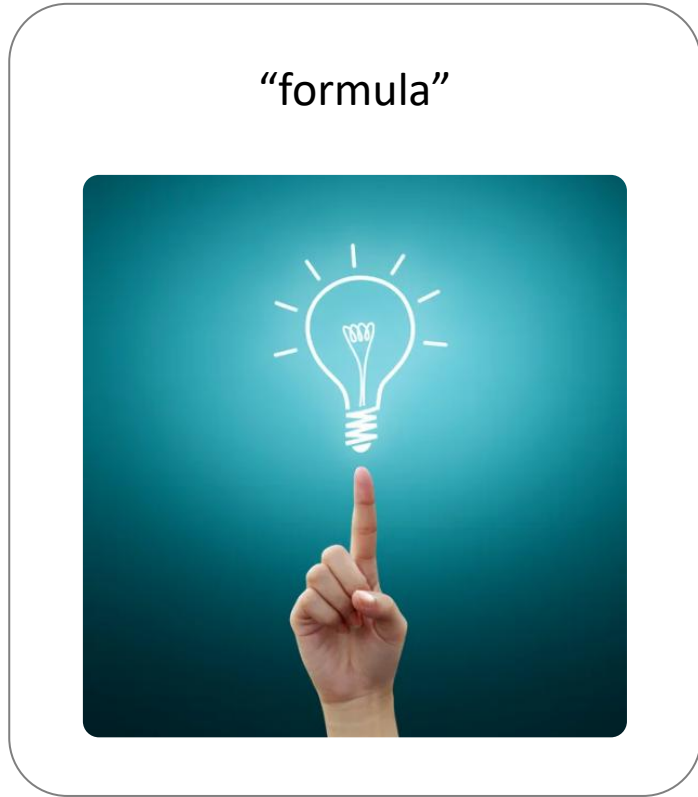
passphrase6

passphrase7



wallet







## “Derivation path”







## Wallet (2009)

Random number	★ ★ ★
Private Key	₿ ₿ ₿

## Wallet (2009)

Random number	
Private Key	

## HD wallet (BIP32)

Random number	
Master private key	
XPRIV	
Private Keys	


## Wallet (2009)

Random number	
Private Key	

## HD wallet (BIP32)

Random number	
Master private key	
XPRIV	
Private Keys	

## HD wallet (BIP38)

Random number	
Passphrase	@!?
Master private key	
XPRIV	
Private Keys	

### Wallet (2009)

Random number	
Private Key	






### HD wallet (BIP32)

Random number	
Master private key	
XPRIV	
Private Keys	

### HD wallet (BIP38)

Random number	
Passphrase	
Master private key	
XPRIV	
Private Keys	

### HD wallet (BIP39)

Seed words	
Random number	
Passphrase	@!?
Master private key	
XPRIV	
Private Keys	



Wallet (2009)

Random number	
Private Key	






HD wallet (BIP32)

Random number	
Master private key	
XPRIV	
Private Keys	

HD wallet (BIP38)

Random number	
Passphrase	
Master private key	
XPRIV	
Private Keys	

HD wallet(BIP39)

Seed words	
Random number	
Passphrase	@!?
Master private key	
XPRIV	
Private Keys	

### Wallet (2009)

Random number	
Private Key	






### HD wallet (BIP32)

Random number	
BIP44	
Master private key	
XPRIV	
Private Keys	

### HD wallet (BIP38)

Random number	
Passphrase	
BIP44	
Master private key	
XPRIV	
Private Keys	

### HD wallet(BIP39)

Seed words	
Random number	
Passphrase	@!?
BIP44	
Master private key	
XPRIV	
Private Keys	

## Wallet (2009)

Random number	
Private Key	






## HD wallet (BIP32)

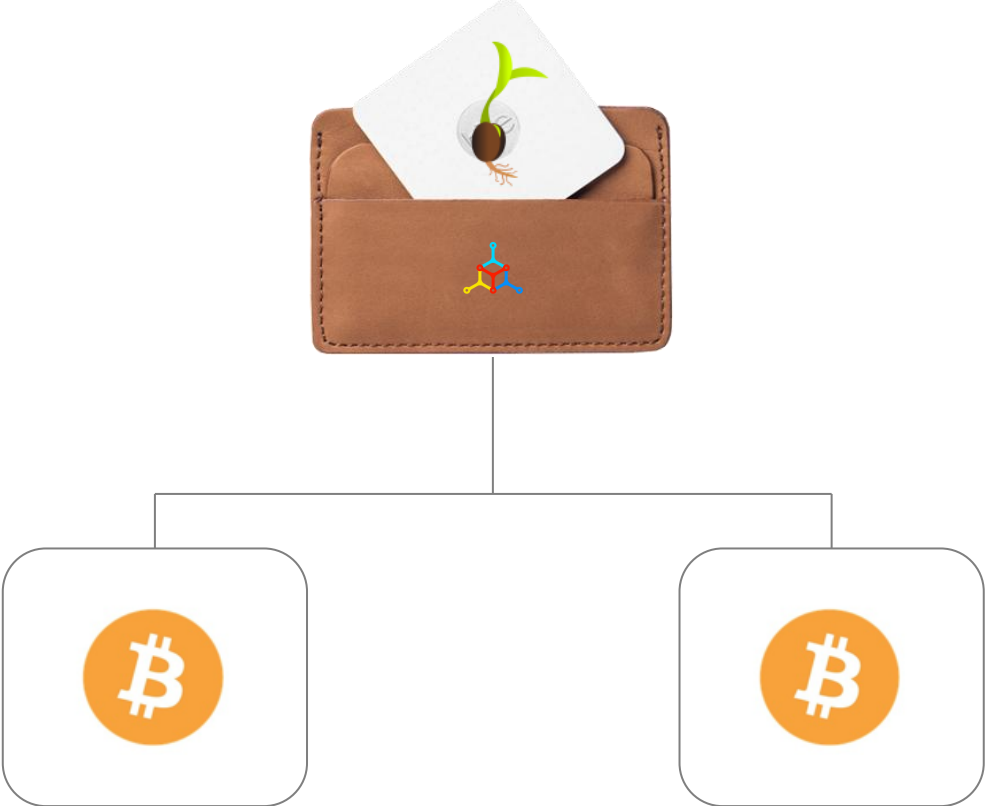
Random number	
<b>Derivation path</b>	
Master private key	
XPRIV	
Private Keys	

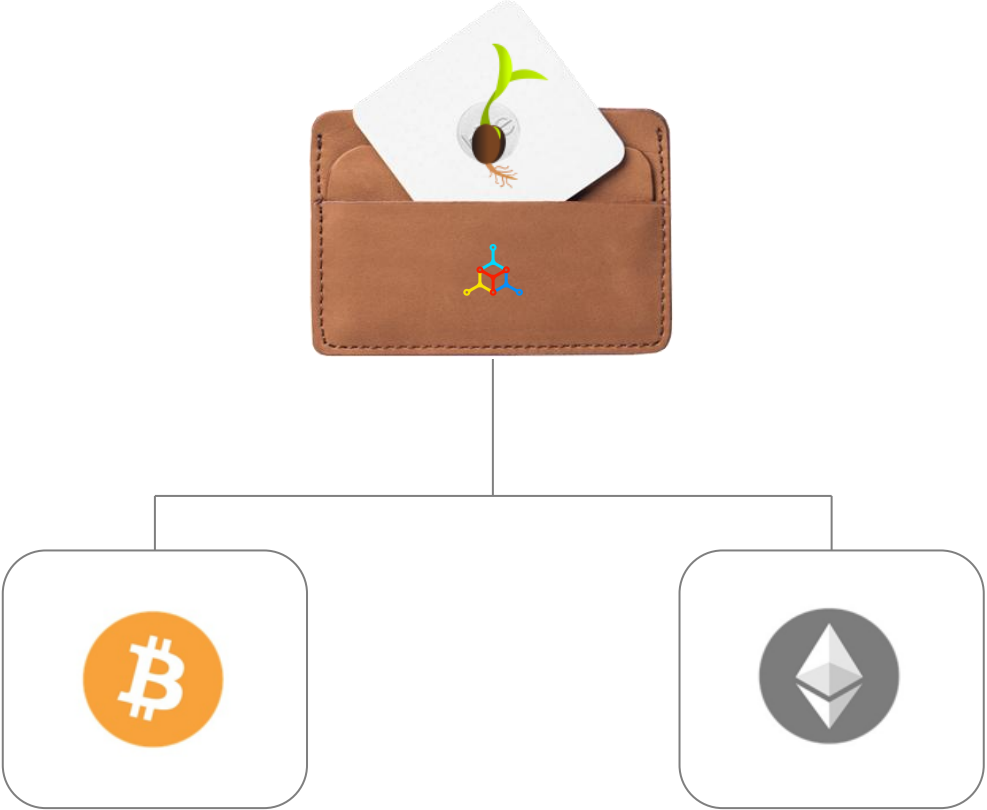
## HD wallet (BIP38)

Random number	
Passphrase	
<b>Derivation path</b>	
Master private key	
XPRIV	
Private Keys	

## HD wallet (BIP39)

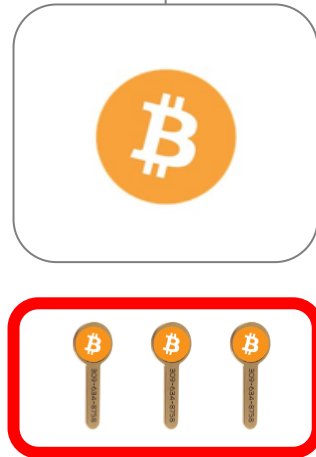
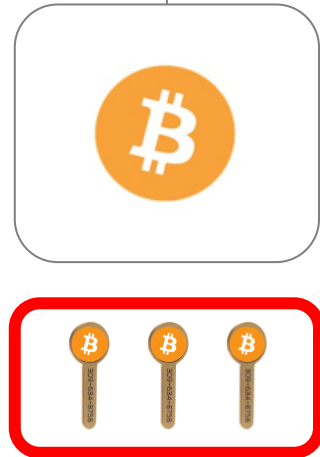
Seed words	
Random number	
Passphrase	@!?
<b>Derivation path</b>	
Master private key	
XPRIV	
Private Keys	







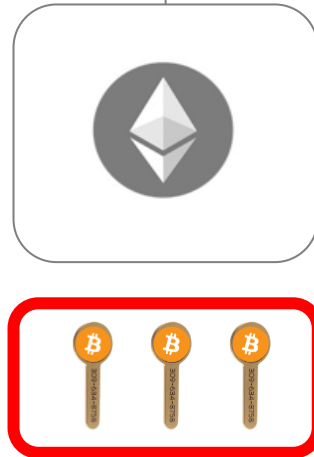
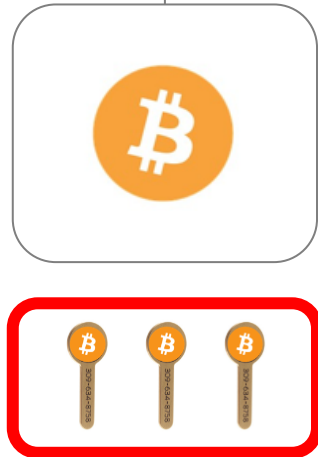
Seed	
Master private key	
XPRIV	
Private Keys	



Seed	
Master private key	
XPRIV	
Private Keys	



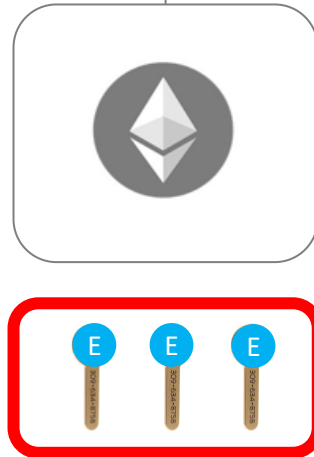
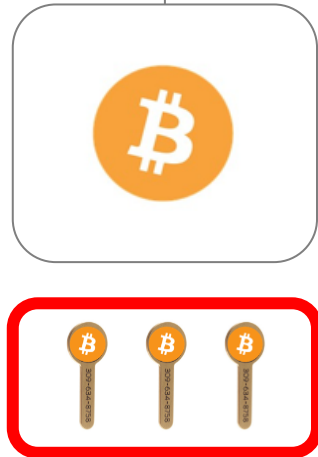
Seed	
Master private key	
XPRIV	
Private Keys	



Seed	
Master private key	
XPRIV	
Private Keys	



Seed	
Master private key	
XPRIV	
Private Keys	



Seed	
Master private key	
XPRIV	
Private Keys	



## HD wallet(BIP39)

Seed words	
Random number	
Passphrase	
<b>Derivation path</b>	
Master private key	
XPRIV	
Private Keys	

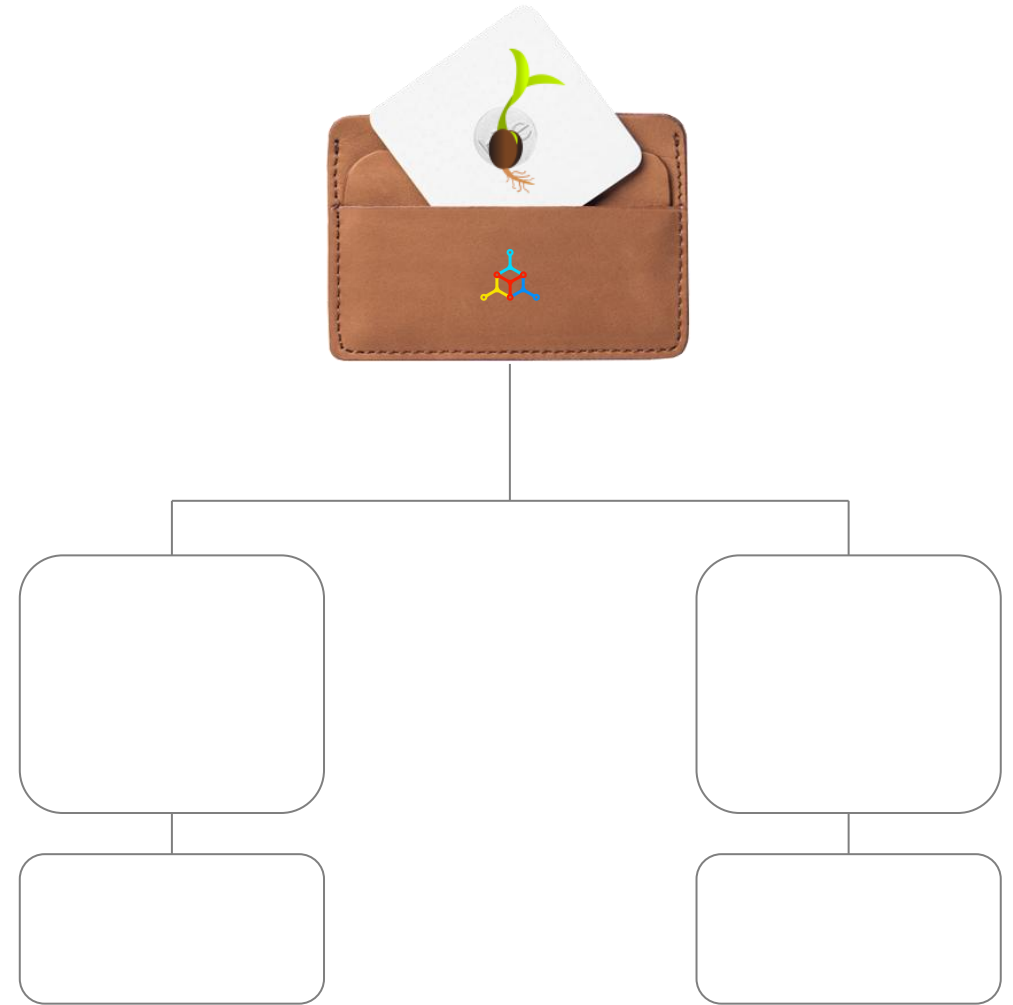
## HD wallet(BIP39)

Seed words	
Random number	
Passphrase	
<b>Derivation path</b>	<b>m/44'/0'/0'</b>
Master private key	
XPRIV	
Private Keys	

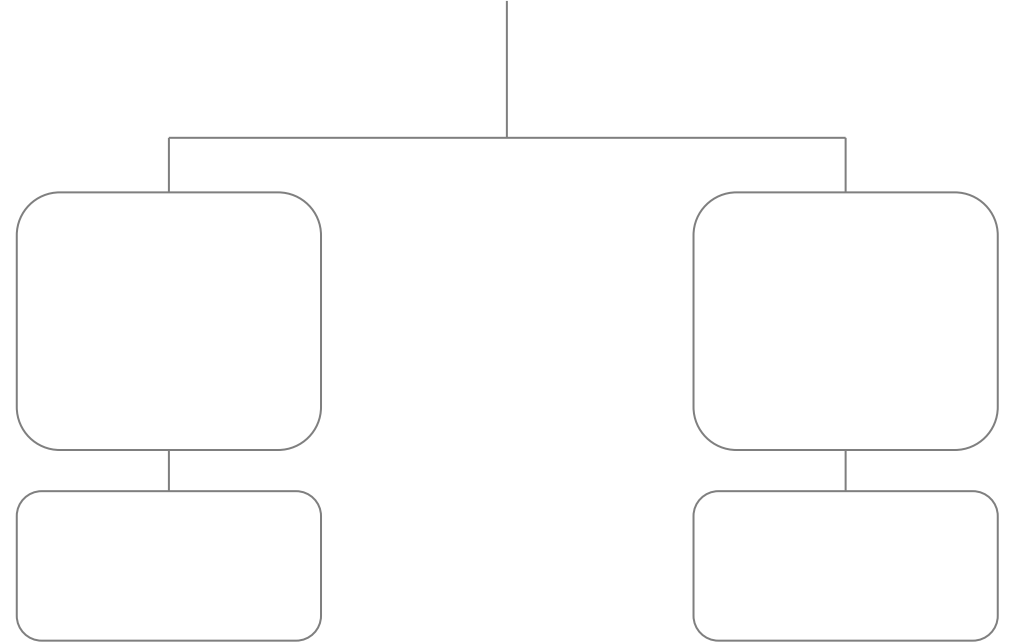
## HD wallet(BIP39)

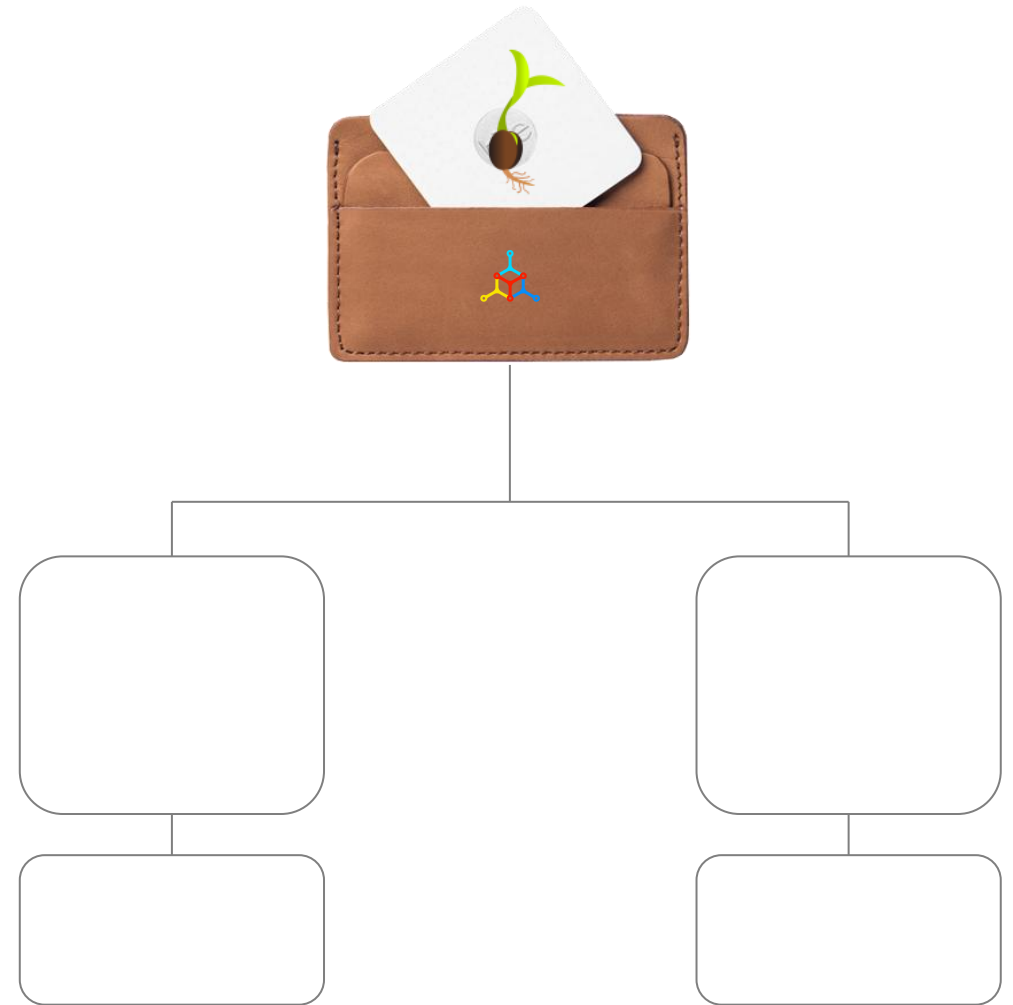
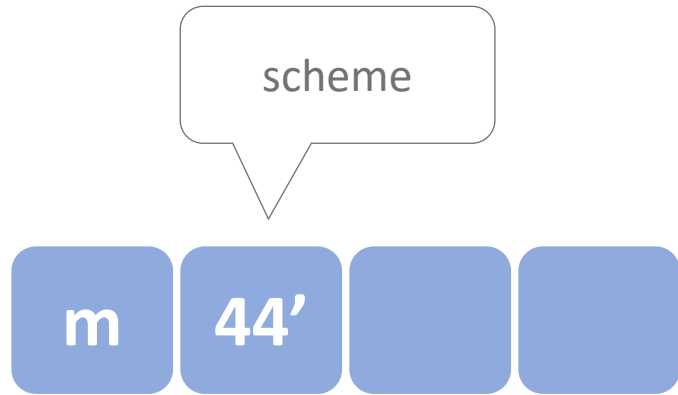
Seed words	
Random number	
Passphrase	
<b>Derivation path</b>	<b>m/44'/0'/0'</b>
Master private key	
XPRIV	
Private Keys	



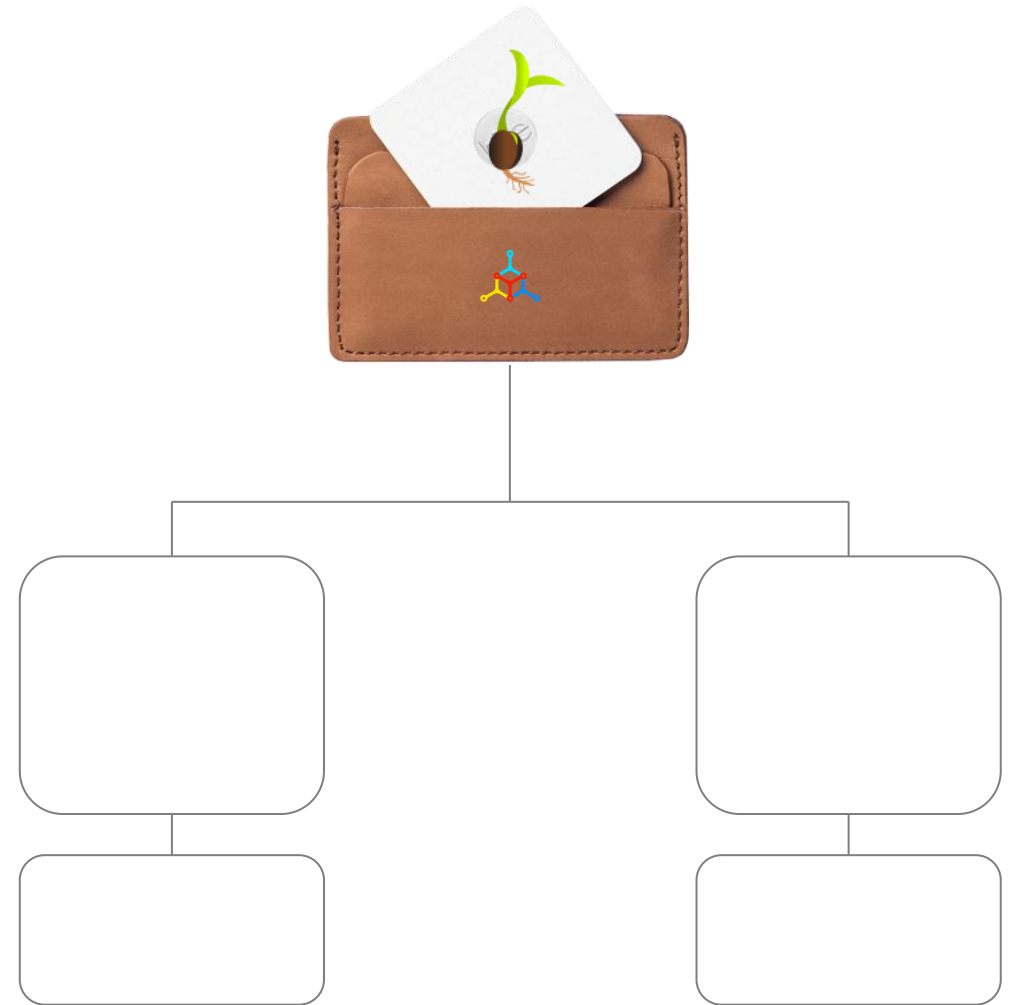


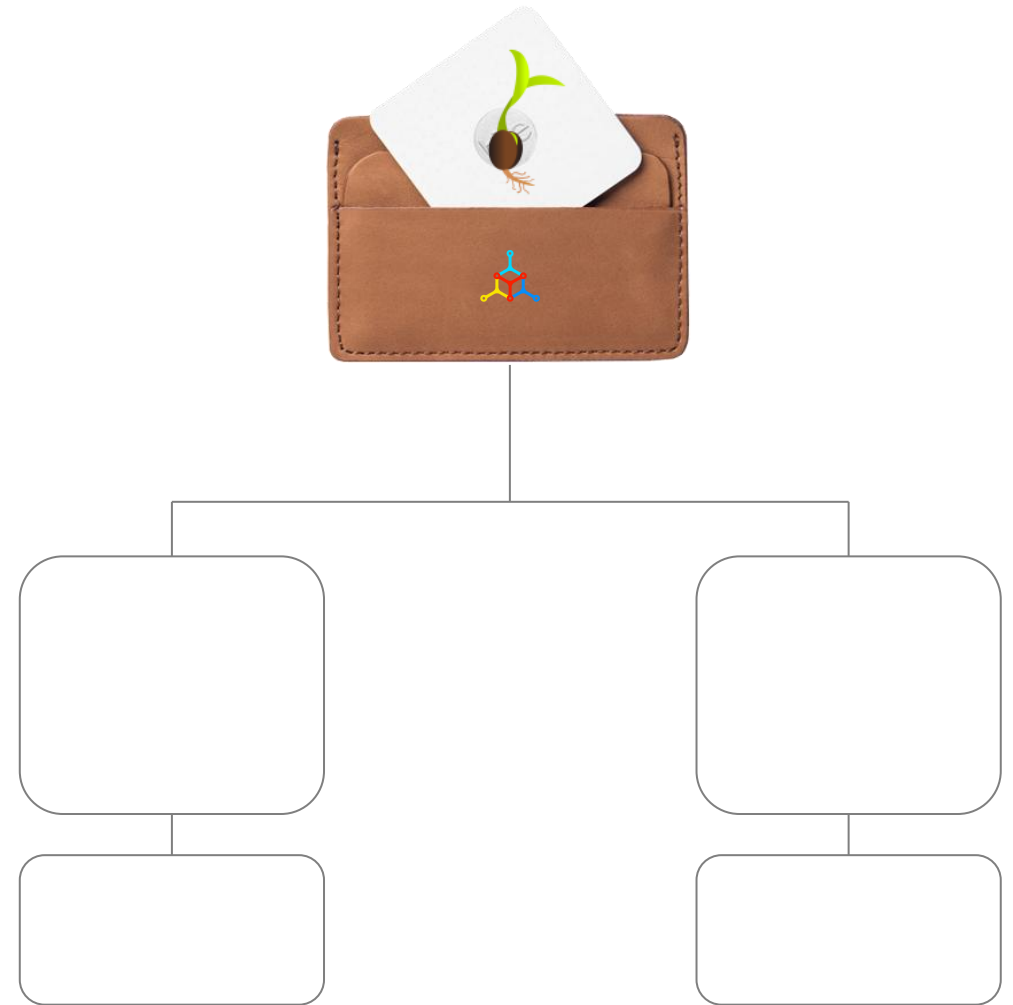
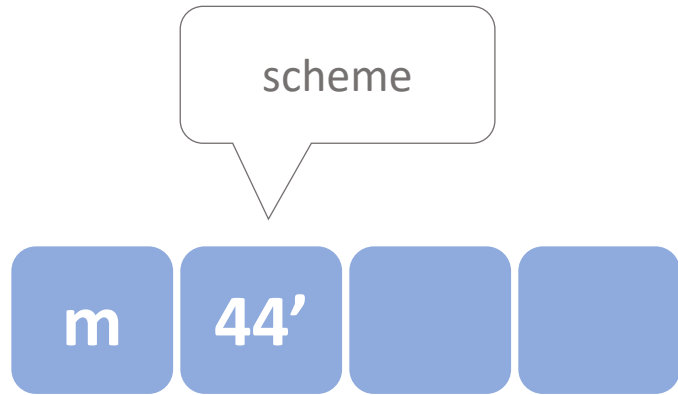
master



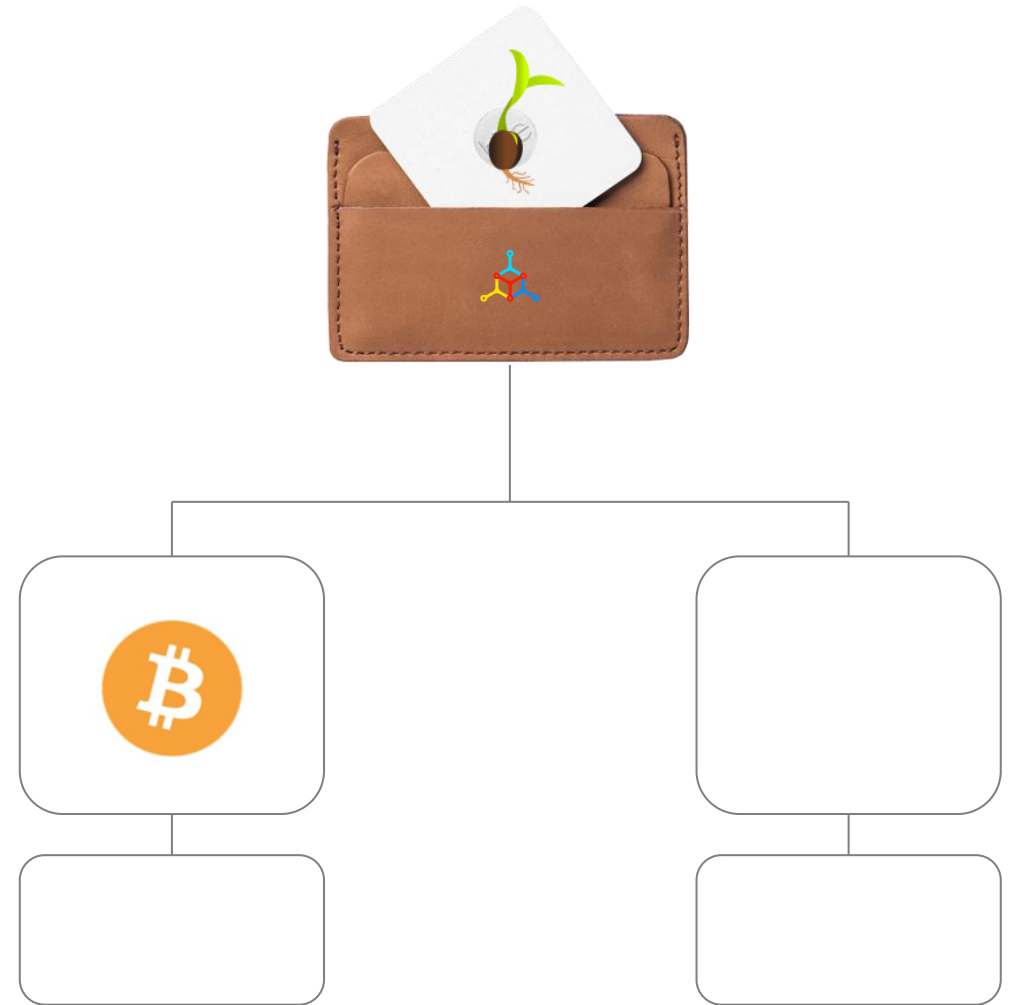
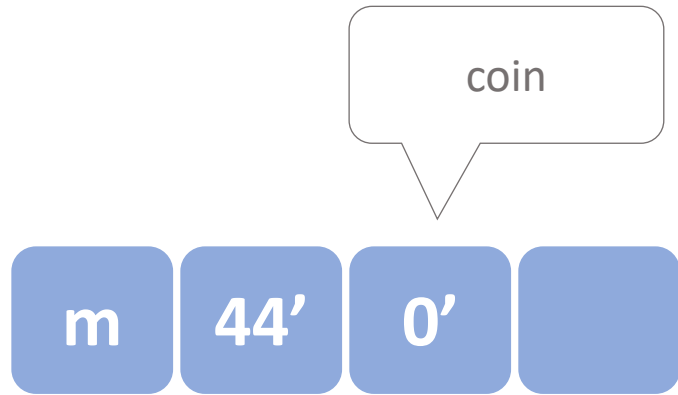


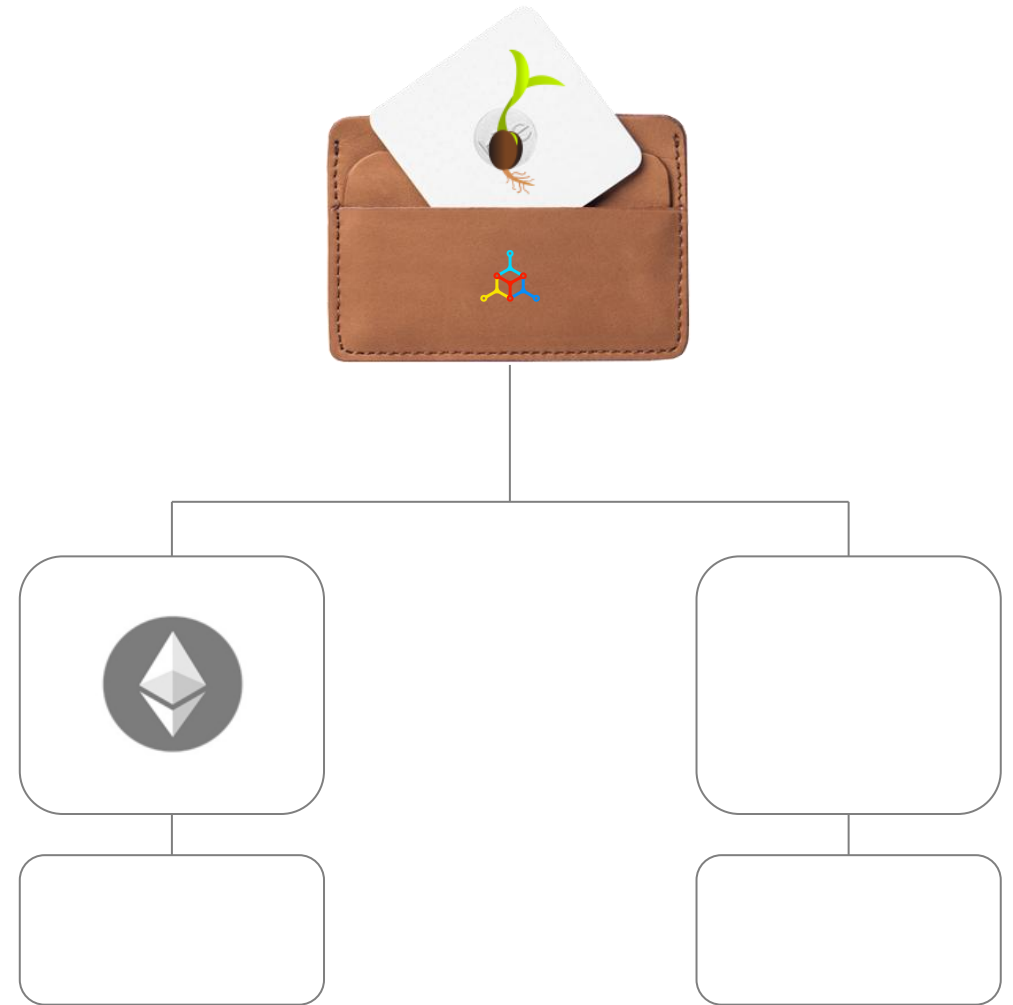
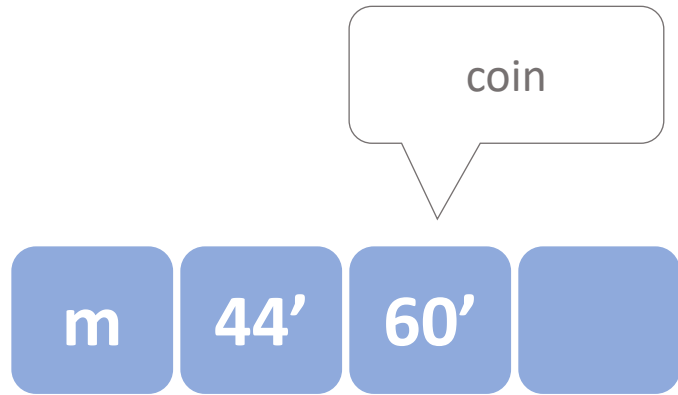
m	44'	legacy (1)
	49'	w-segwit (3)
	84'	n-segwit (bc1)
	86'	taproot (bc1p)

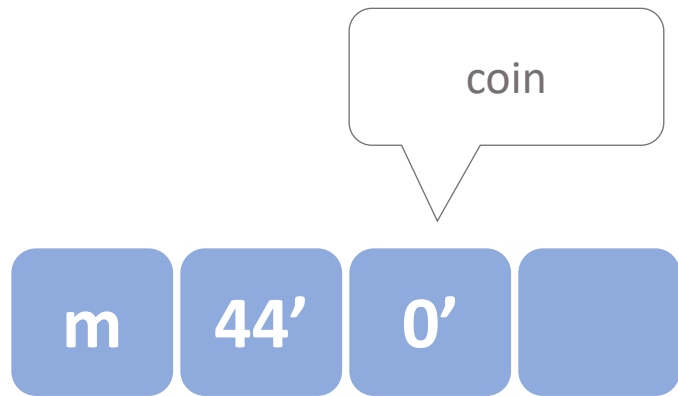




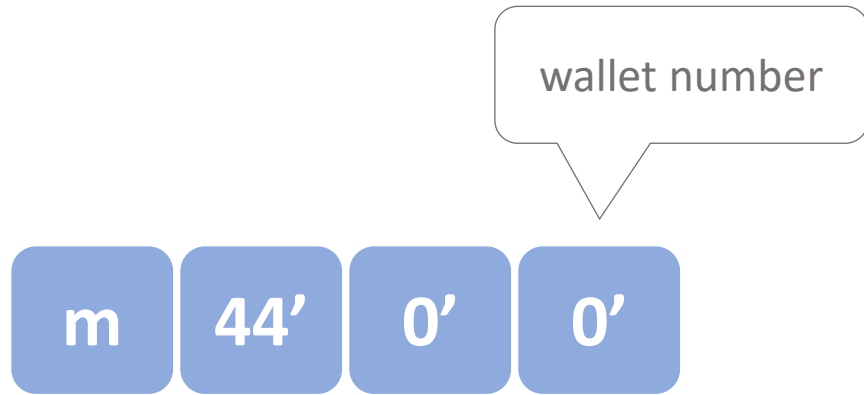


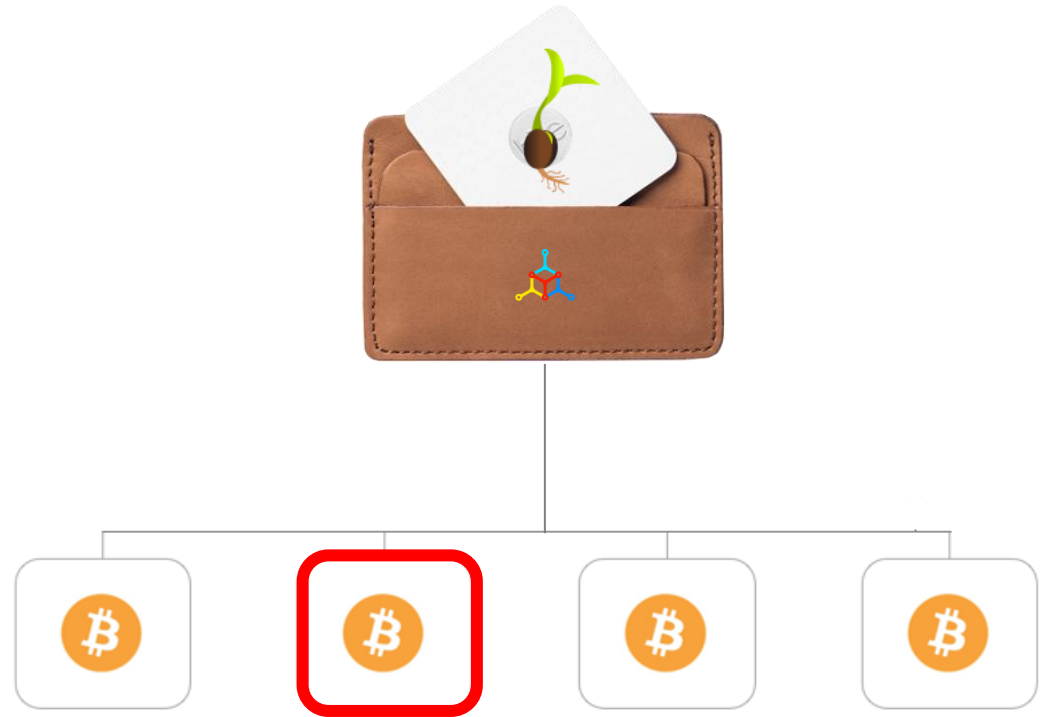
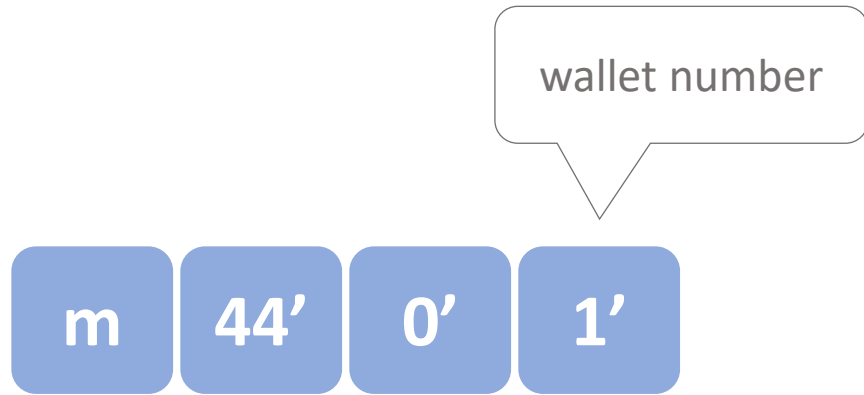


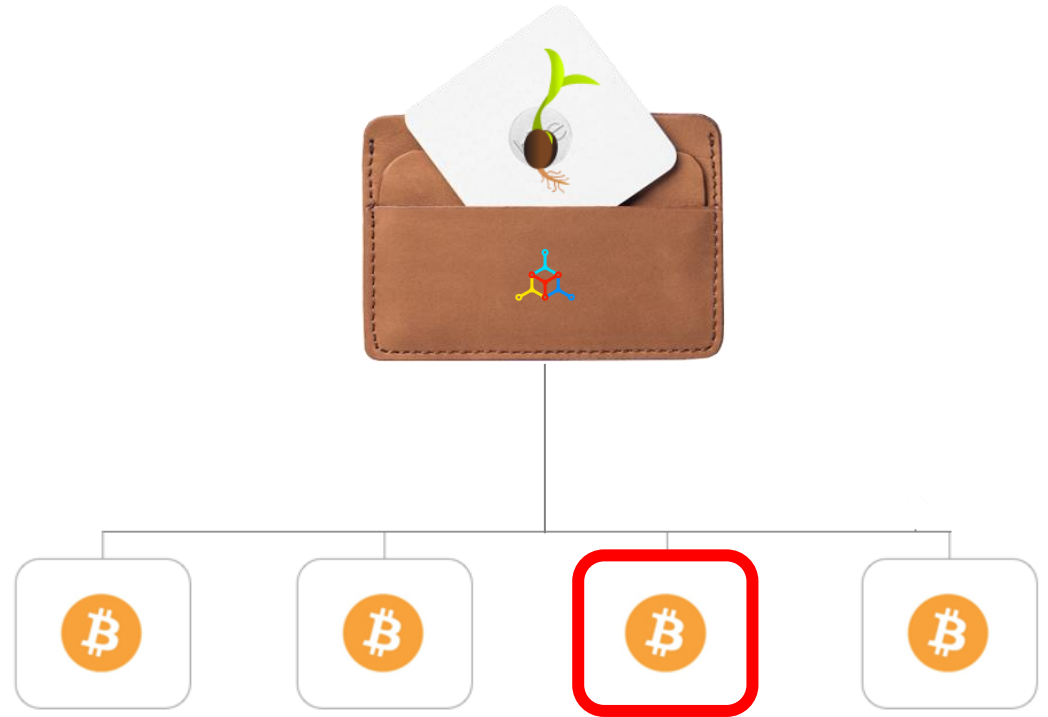
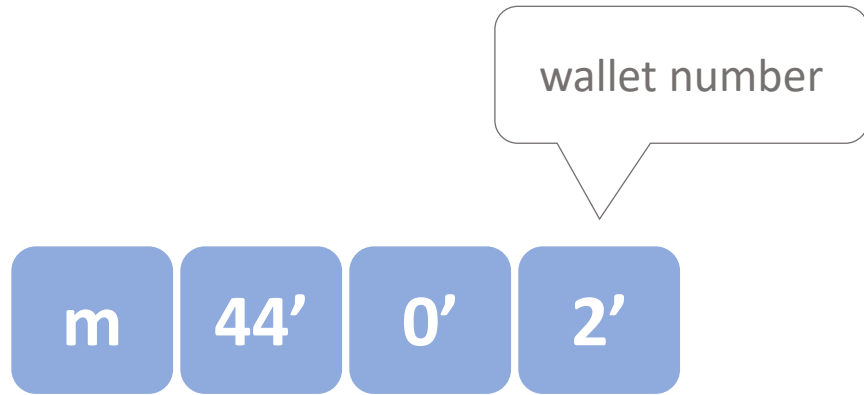


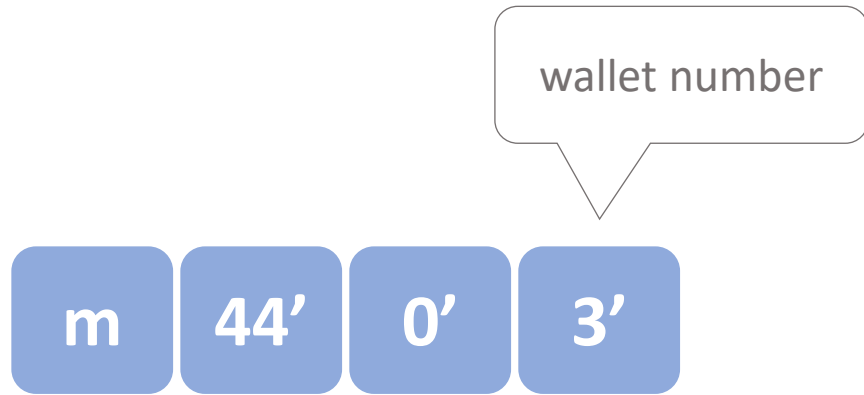


<b>Bitcoin</b>	<b>BTC</b>	<b>0</b>
Ethereum	ETH	60
Litecoin	LTC	2
Dash	DASH	5
Ripple	XRP	144
Cardano	ADA	1815
Neo	NEO	888
Zcash	ZEC	133



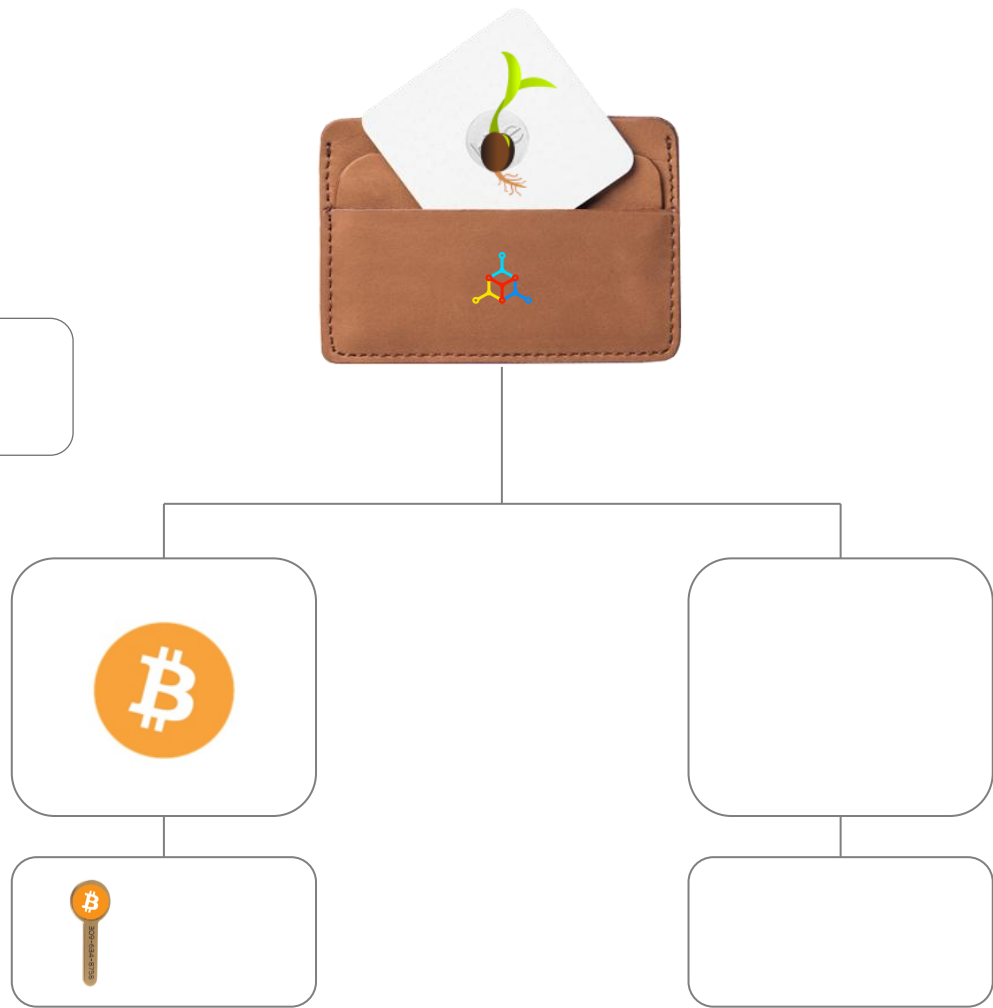




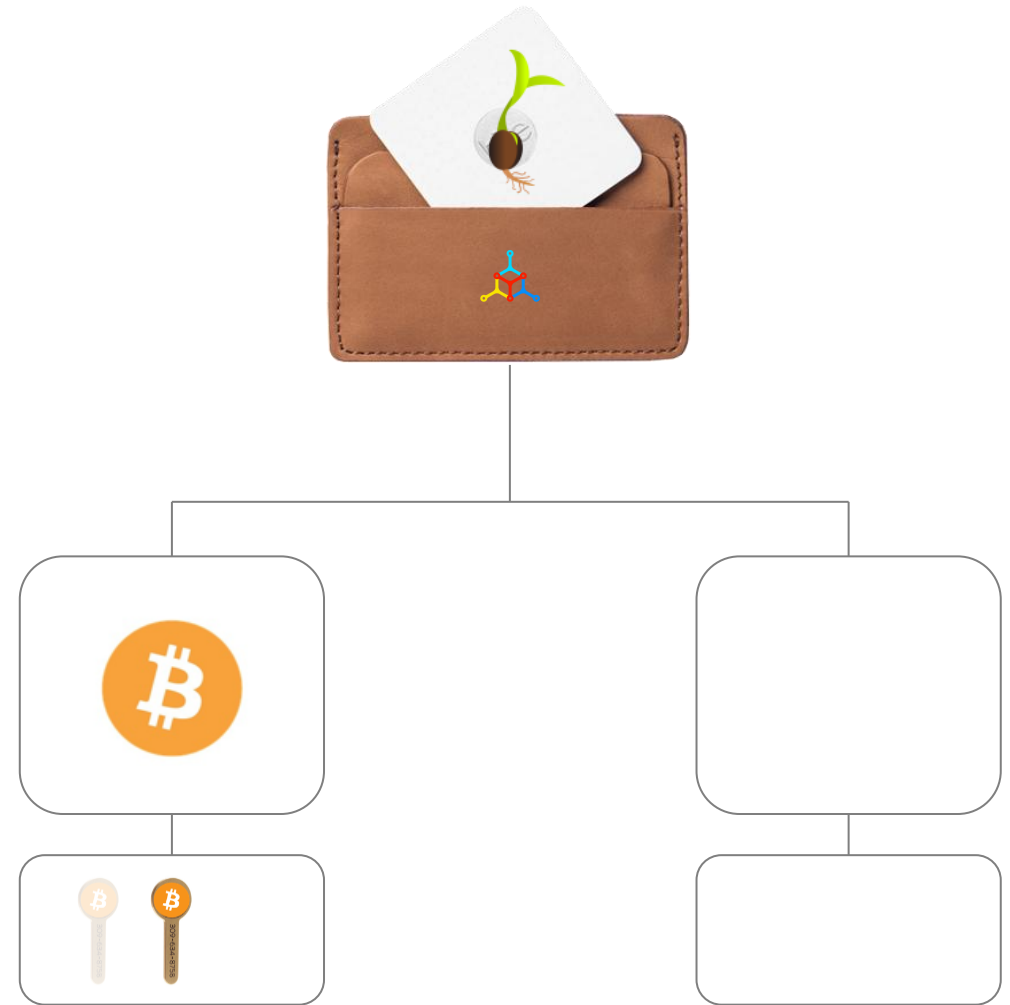
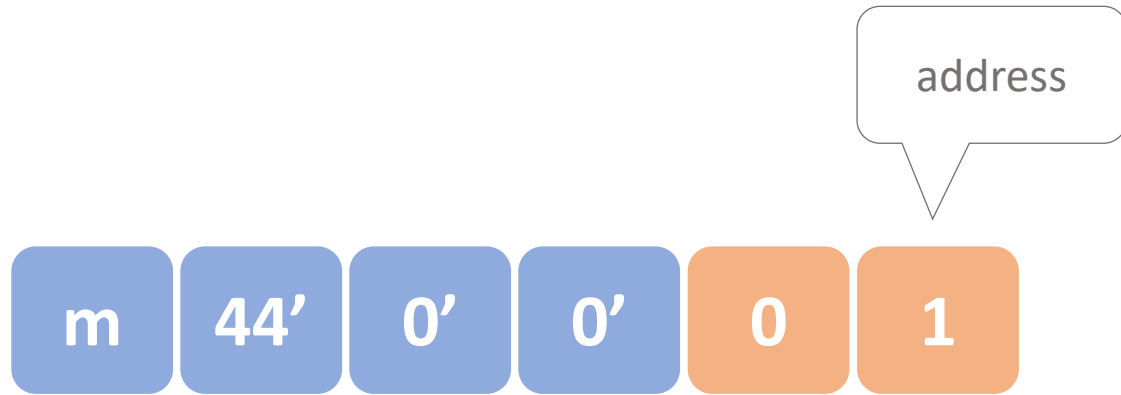


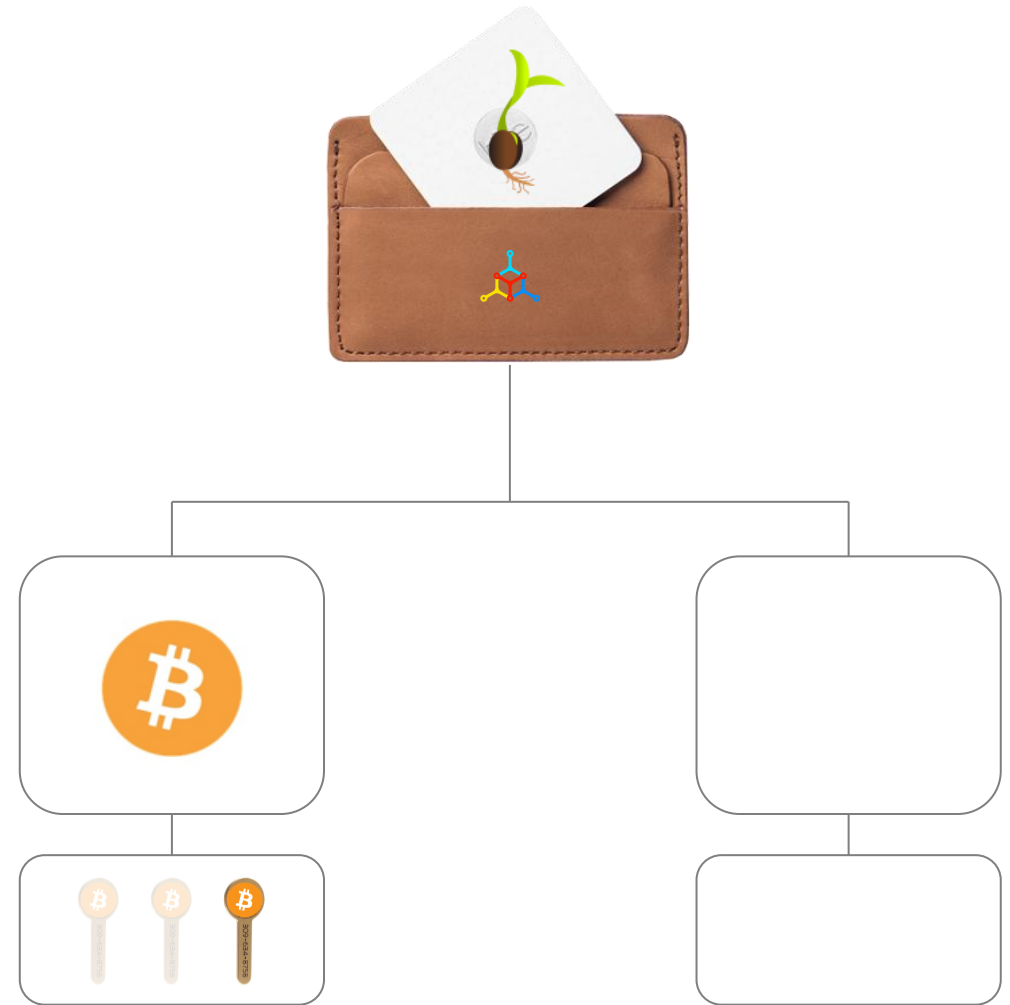
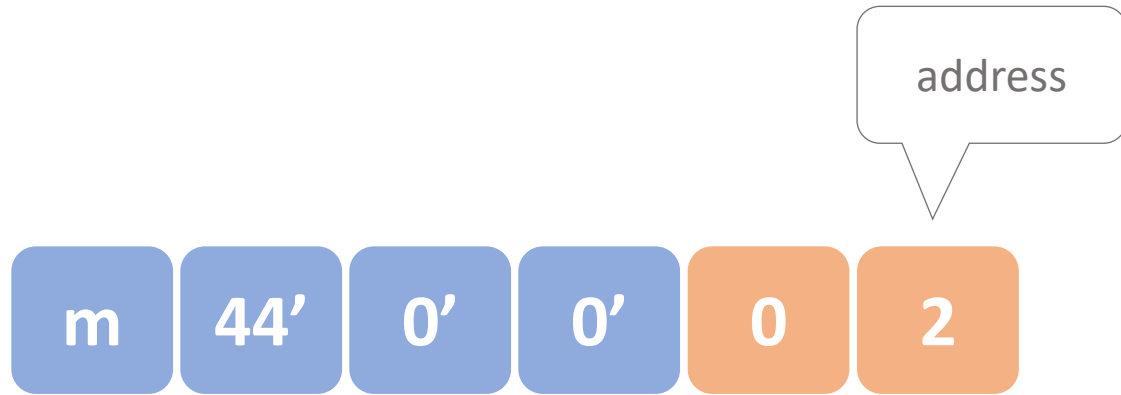
m 44' 0' 0' 0

receive(0) or change(1)

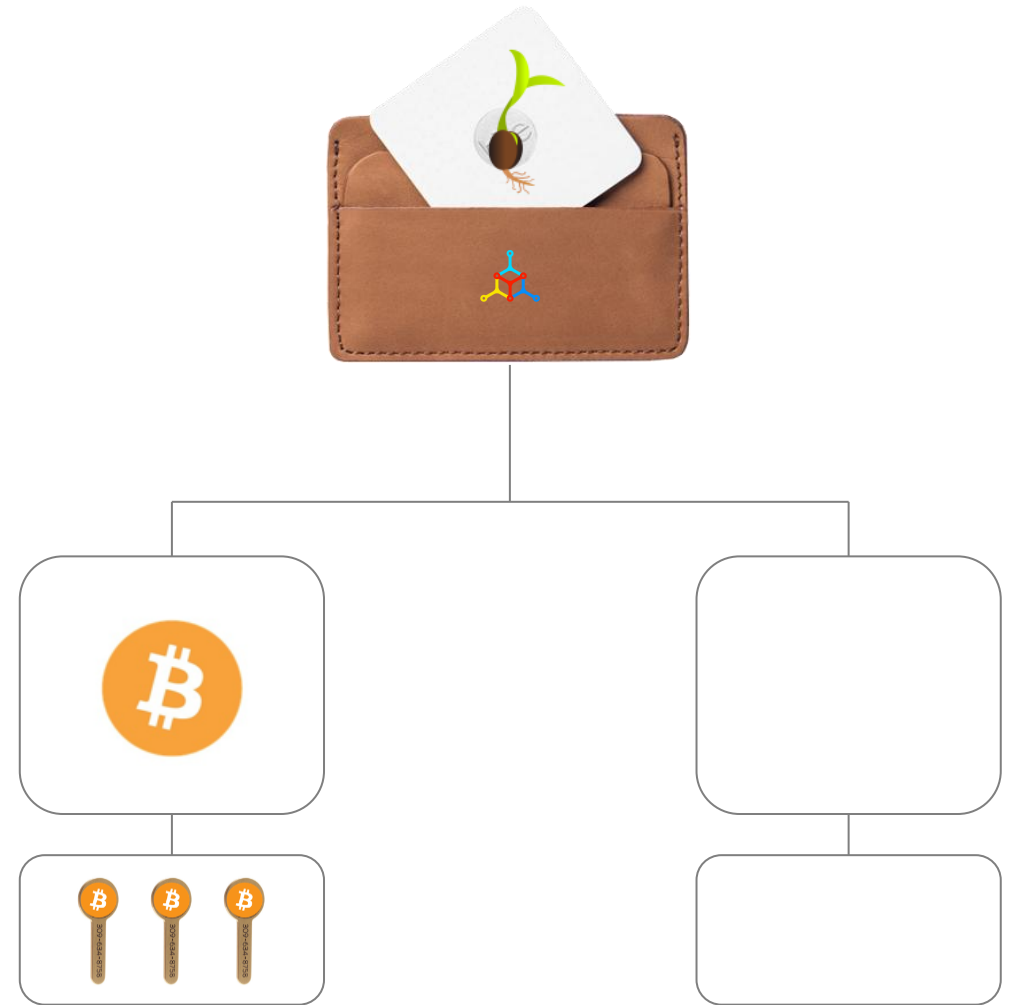


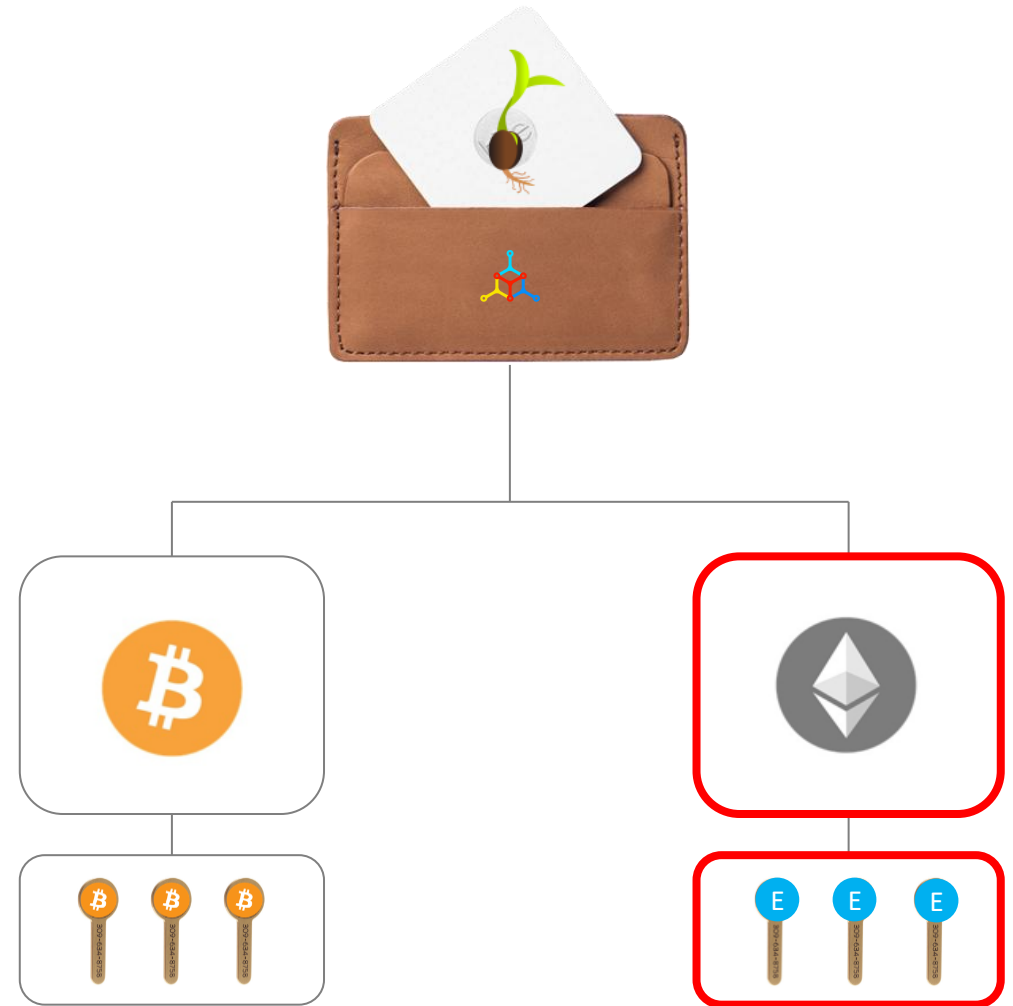
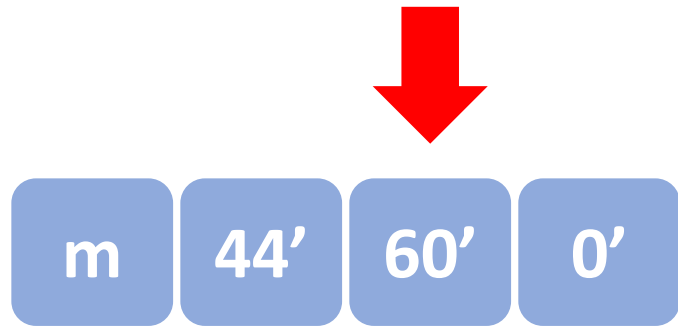


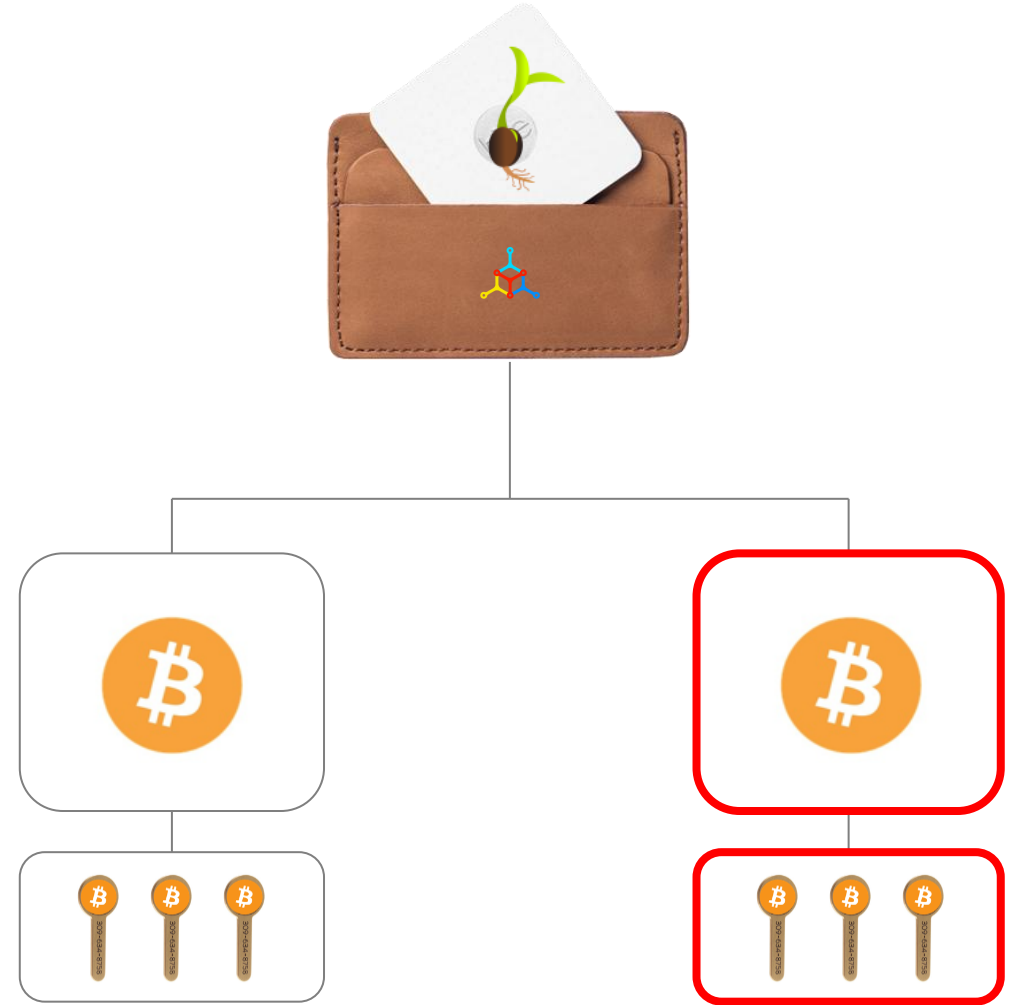
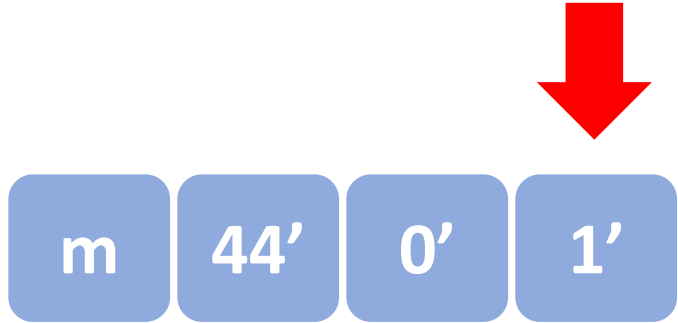




m 44' 0' 0'







m 86' 0' 0'



m 44' 0' 0'

Settings

Policy Type: Single Signature ?

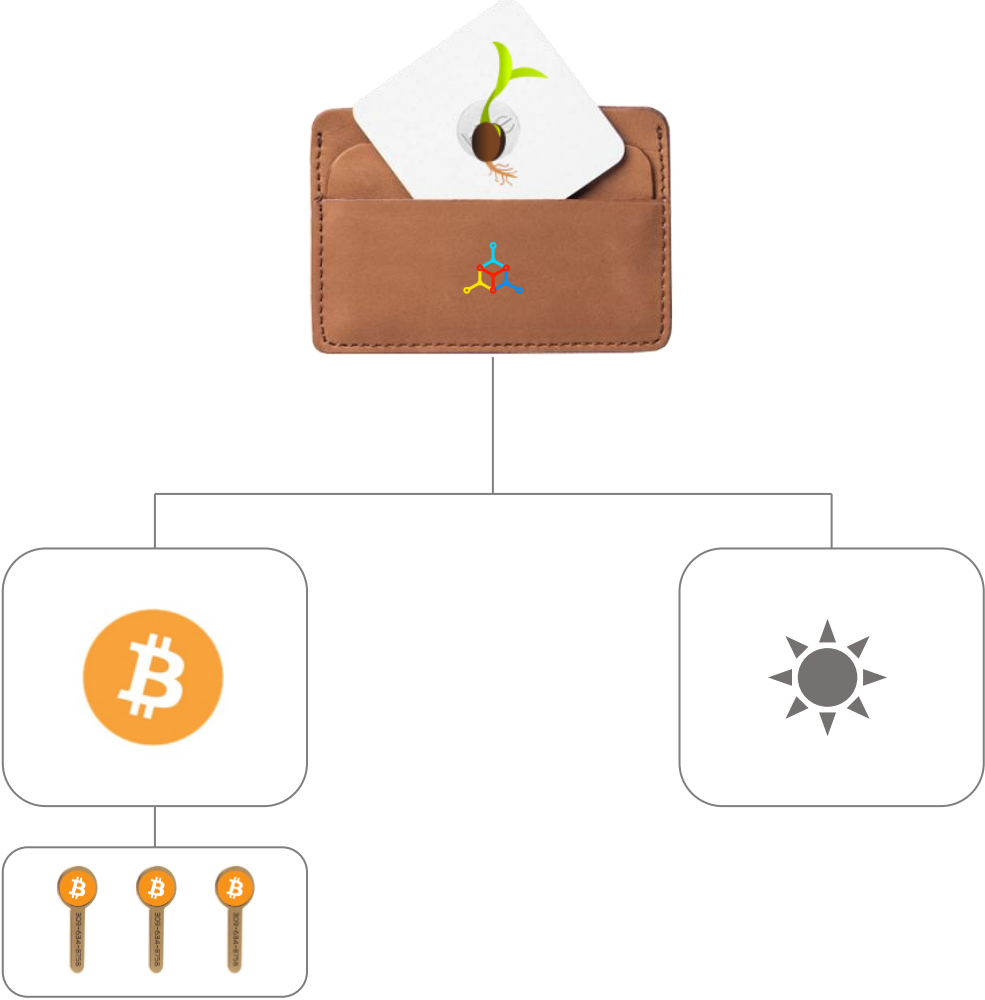
Script Type: Legacy (P2PKH) ?

Script Policy

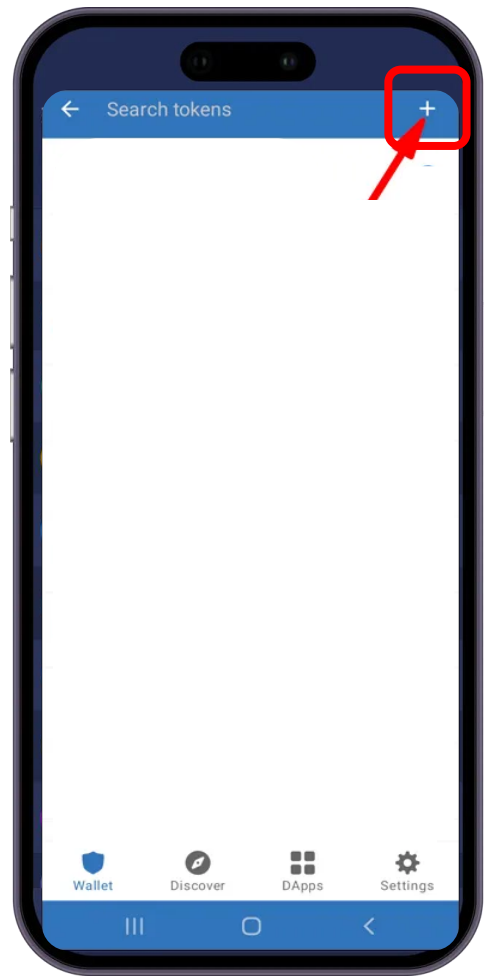
Descriptor:

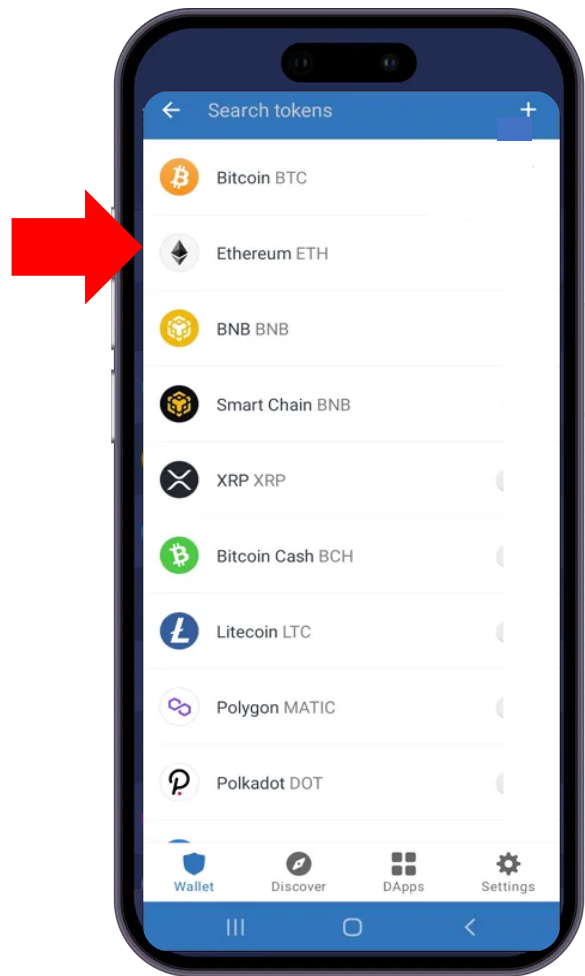
- Legacy (P2PKH)
- Nested Segwit (P2SH-P2WPKH)
- Native Segwit (P2WPKH)
- Taproot (P2TR)

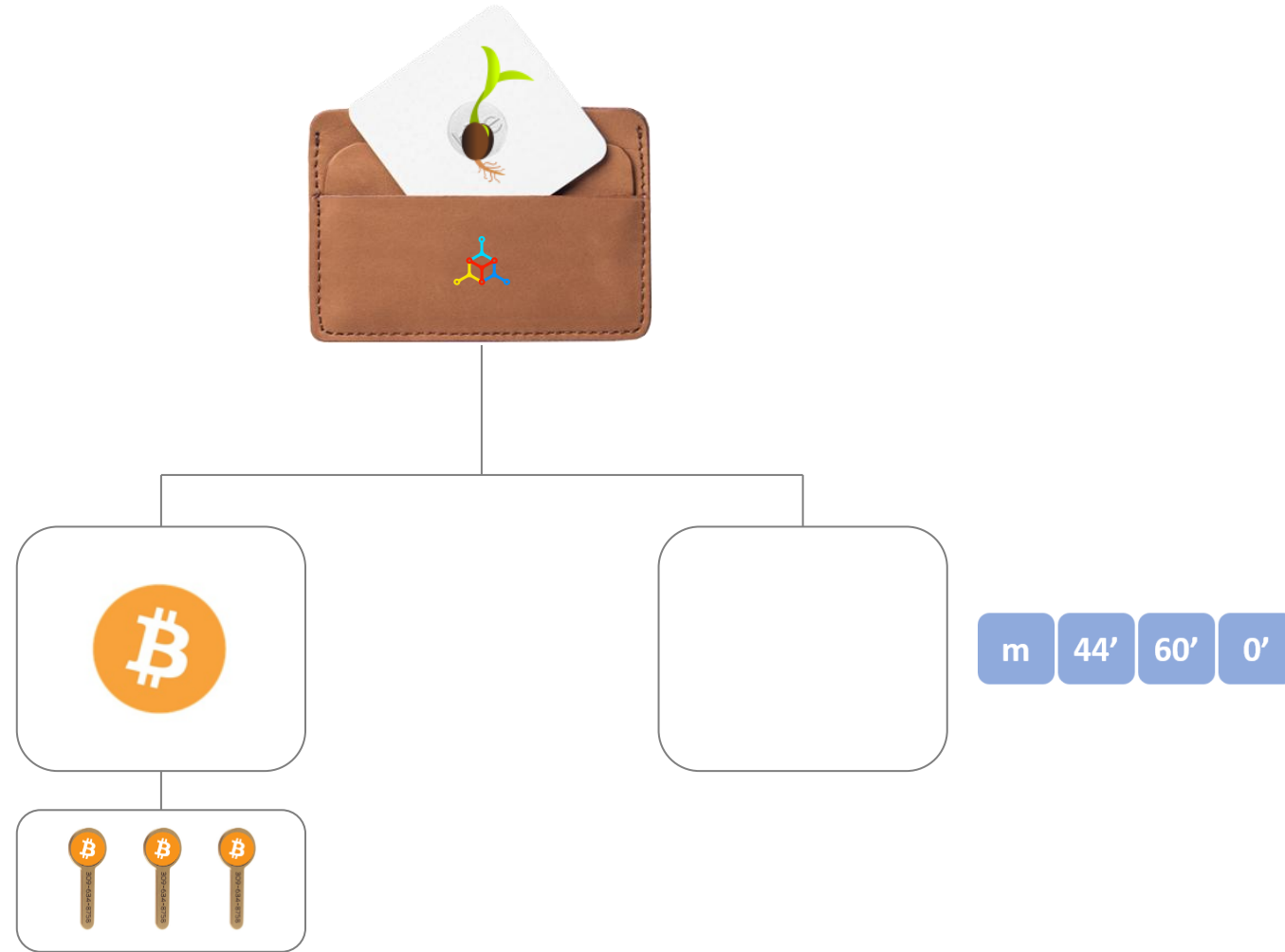
Keystores

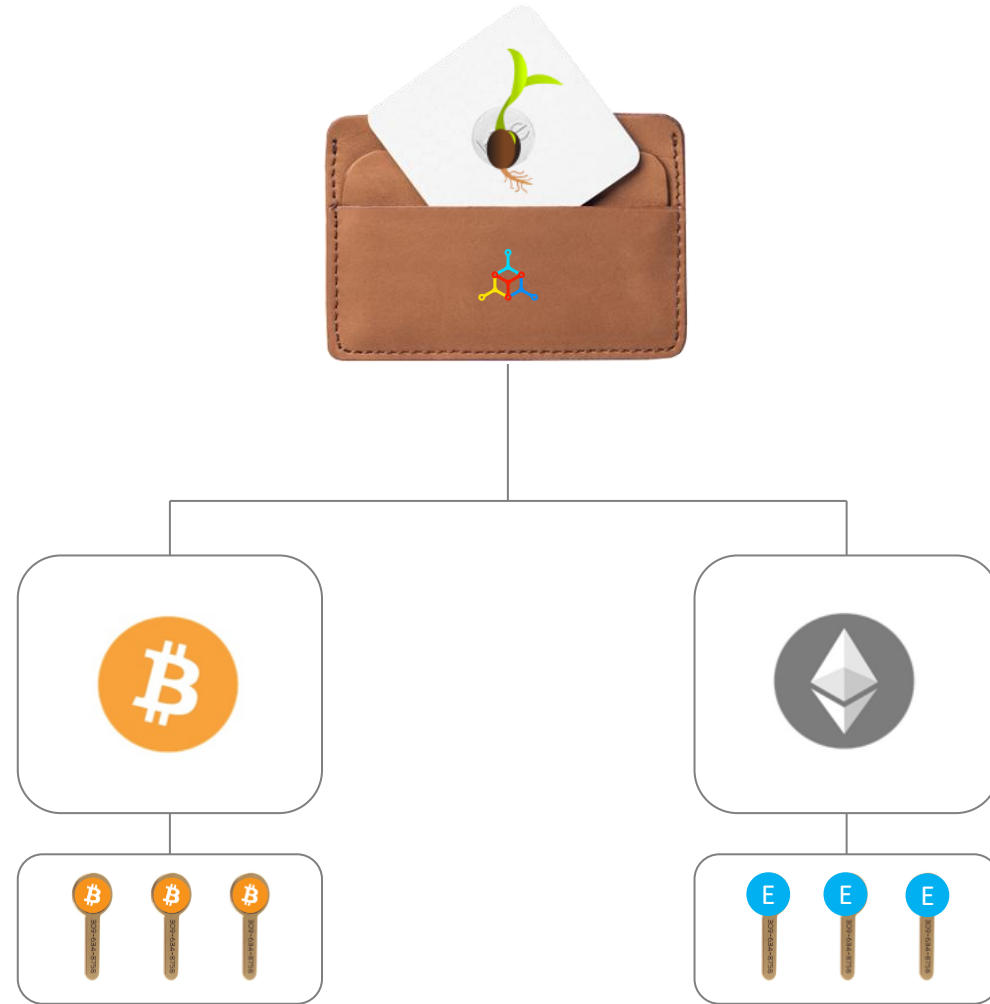












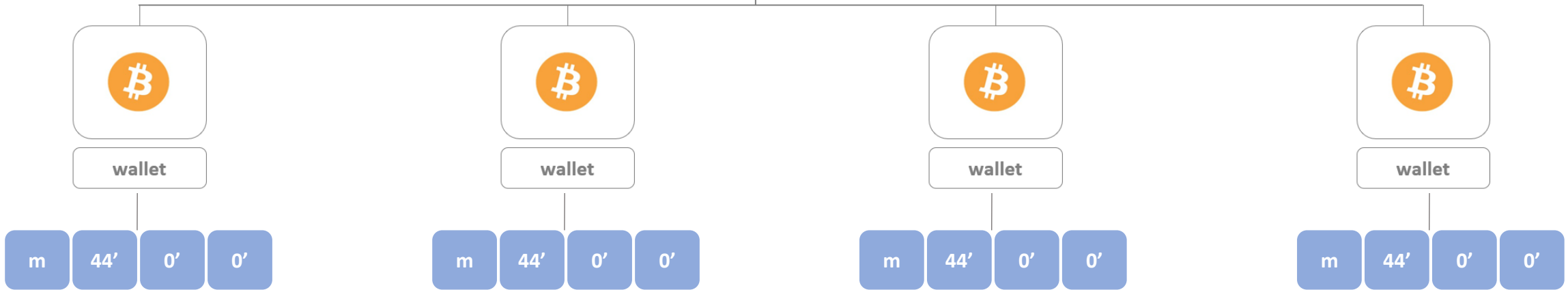


wallet



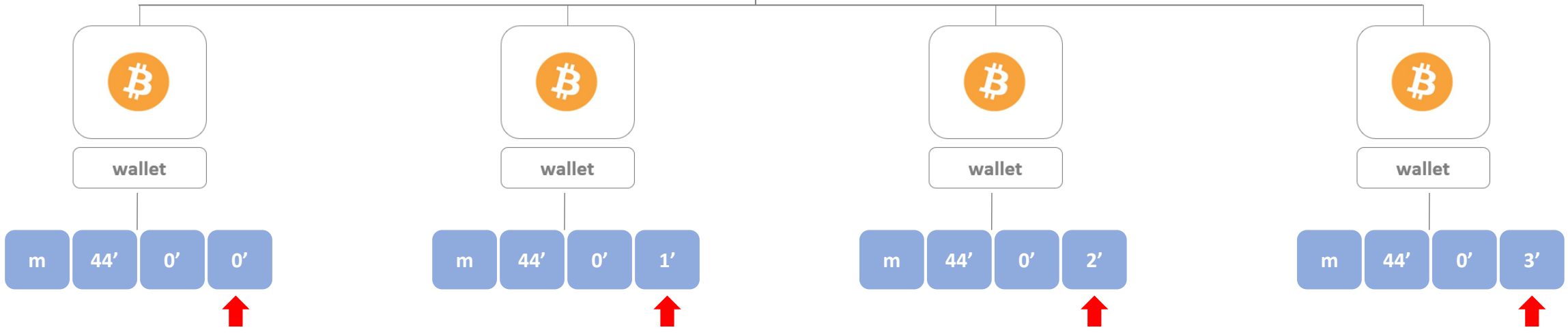


wallet



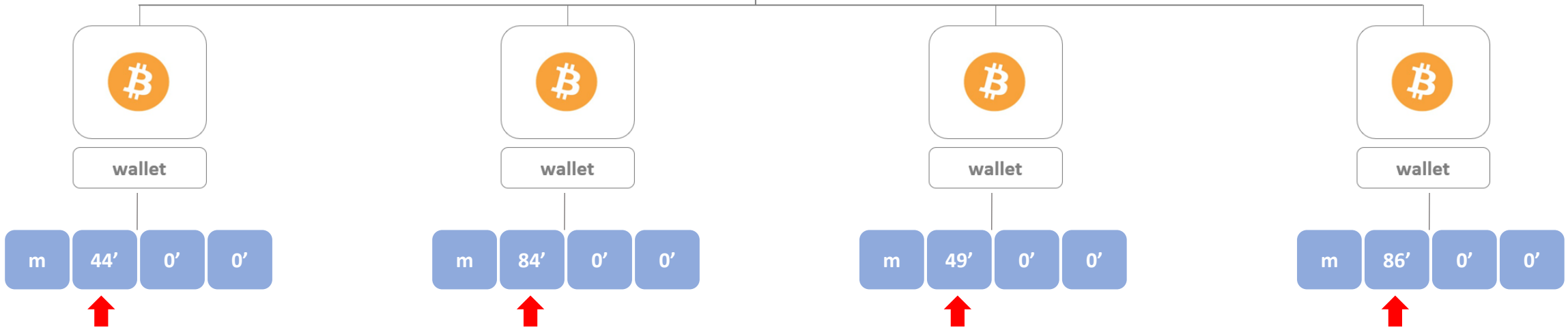


wallet





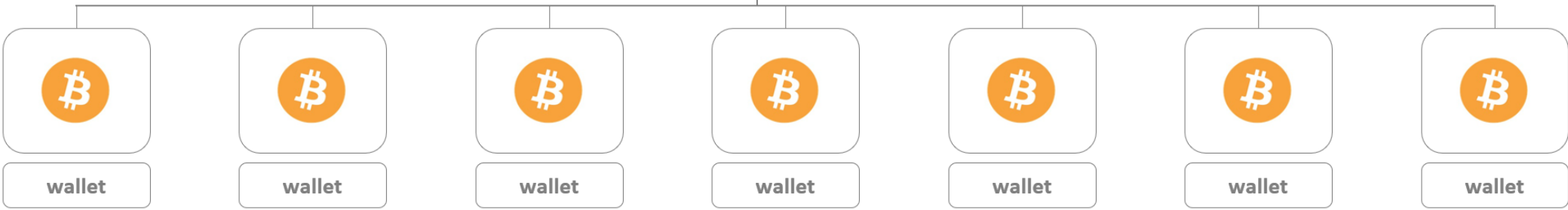
wallet





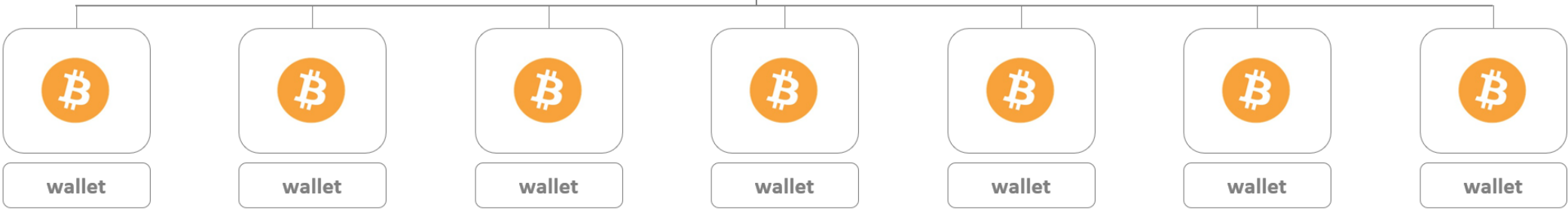


wallet



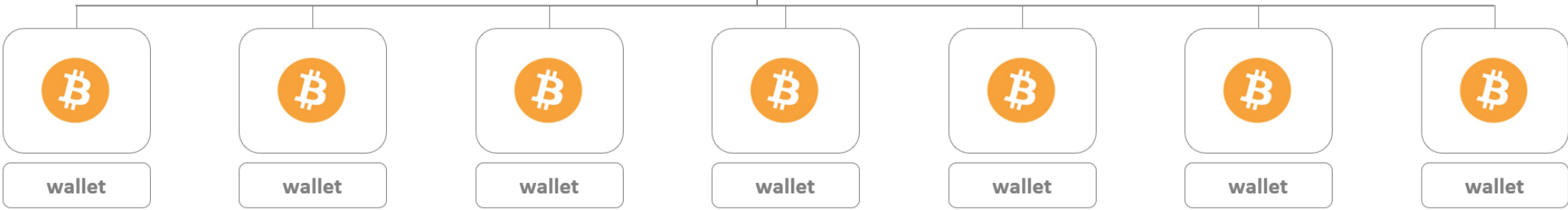


wallet



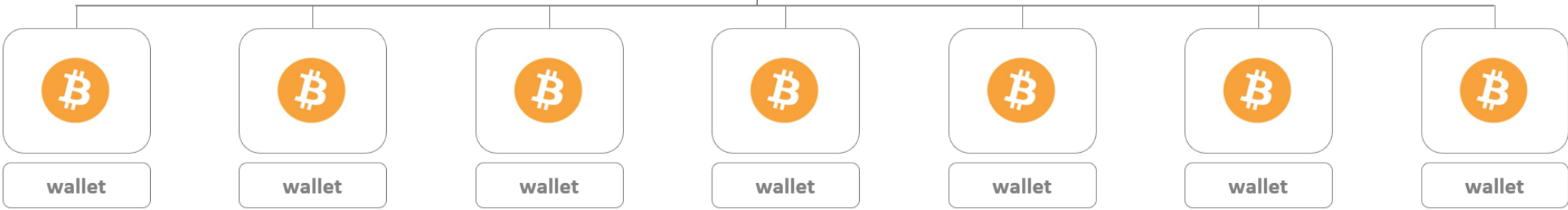


wallet



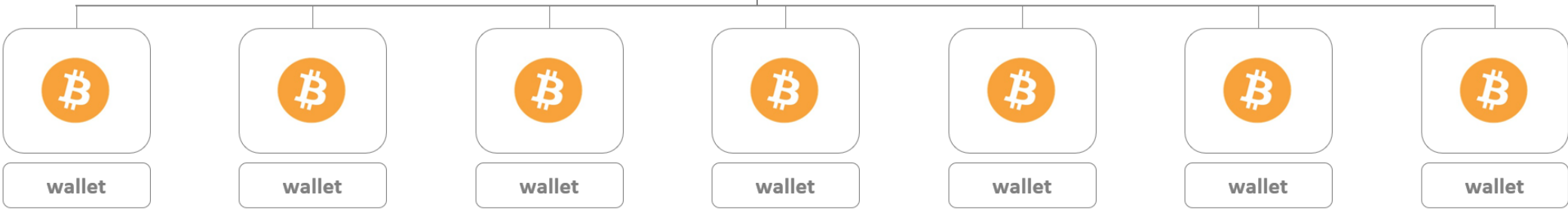


wallet





wallet

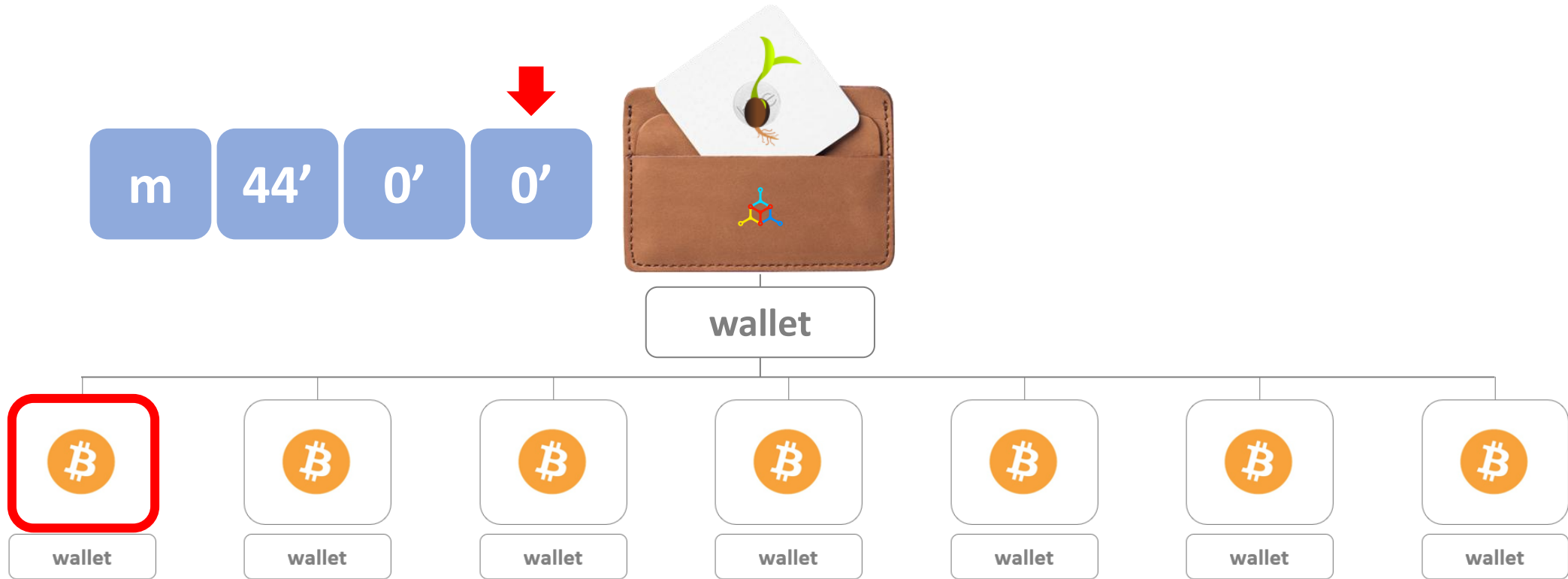




- 1 RESULT.....
- 2 INDEX.....
- 3 DECLINE.....
- 4 PILL.....
- 5 RICH.....
- 6 HEART.....
- 7 TOAST.....
- 8 NASTY.....
- 9 CHOICE.....
- 10 CONSIDER.....
- 11 AWARE.....
- 12 CANNON.....

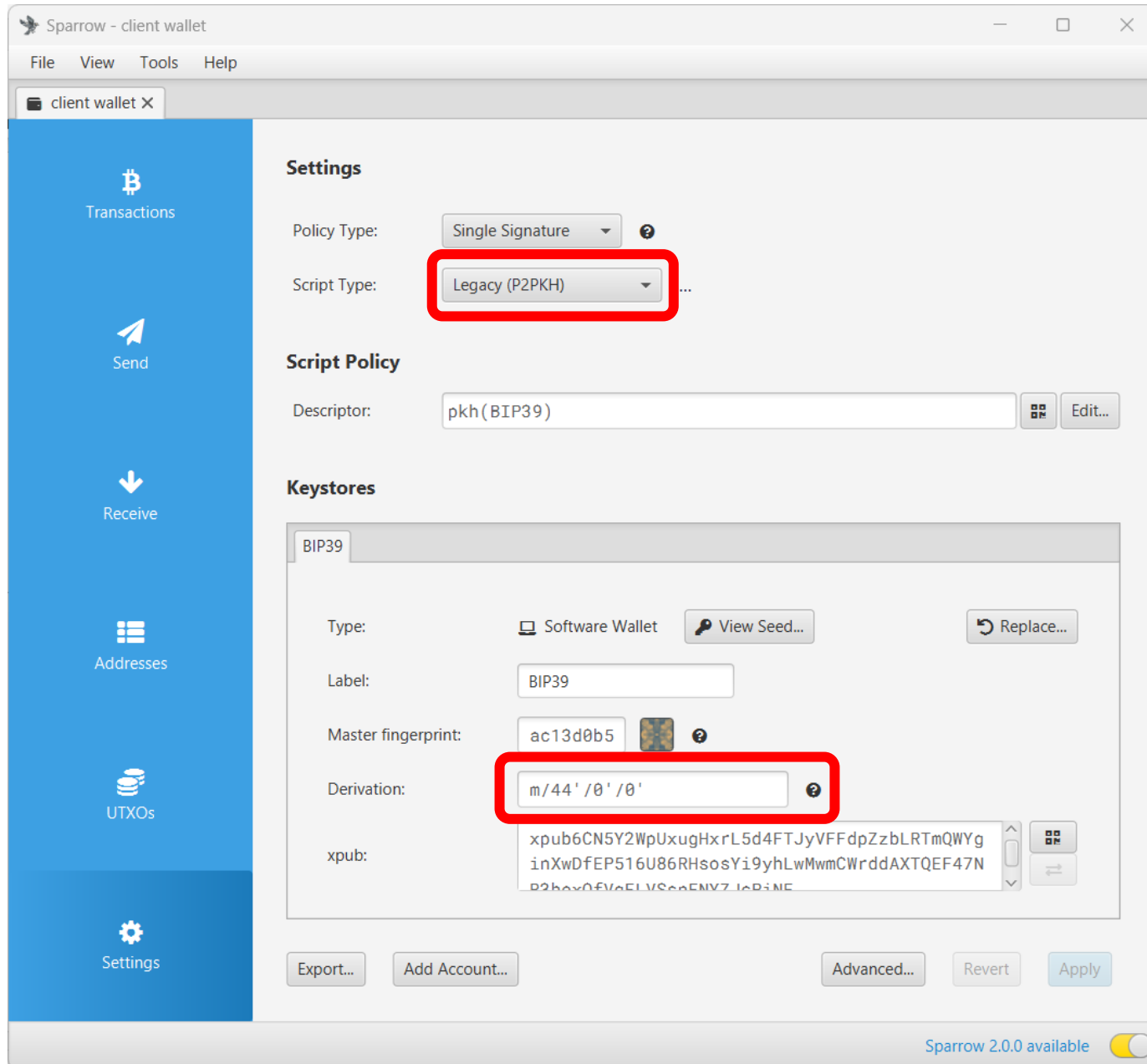
wallet

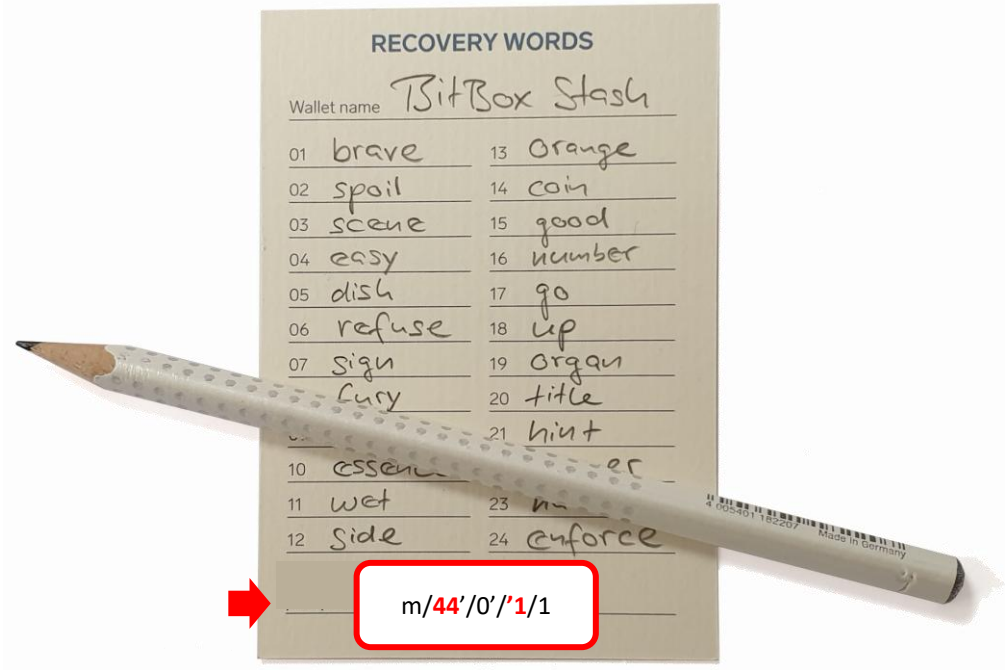


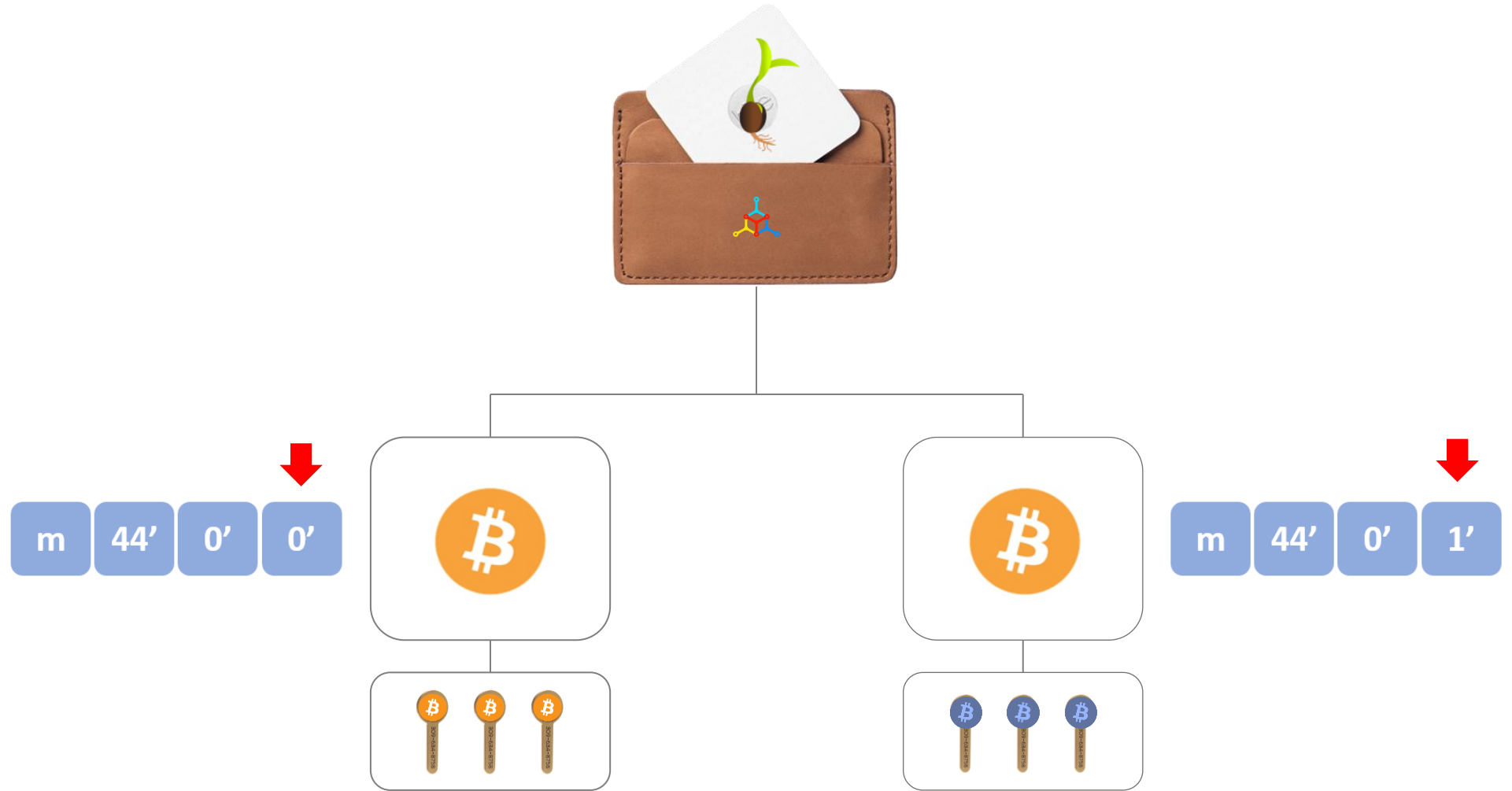


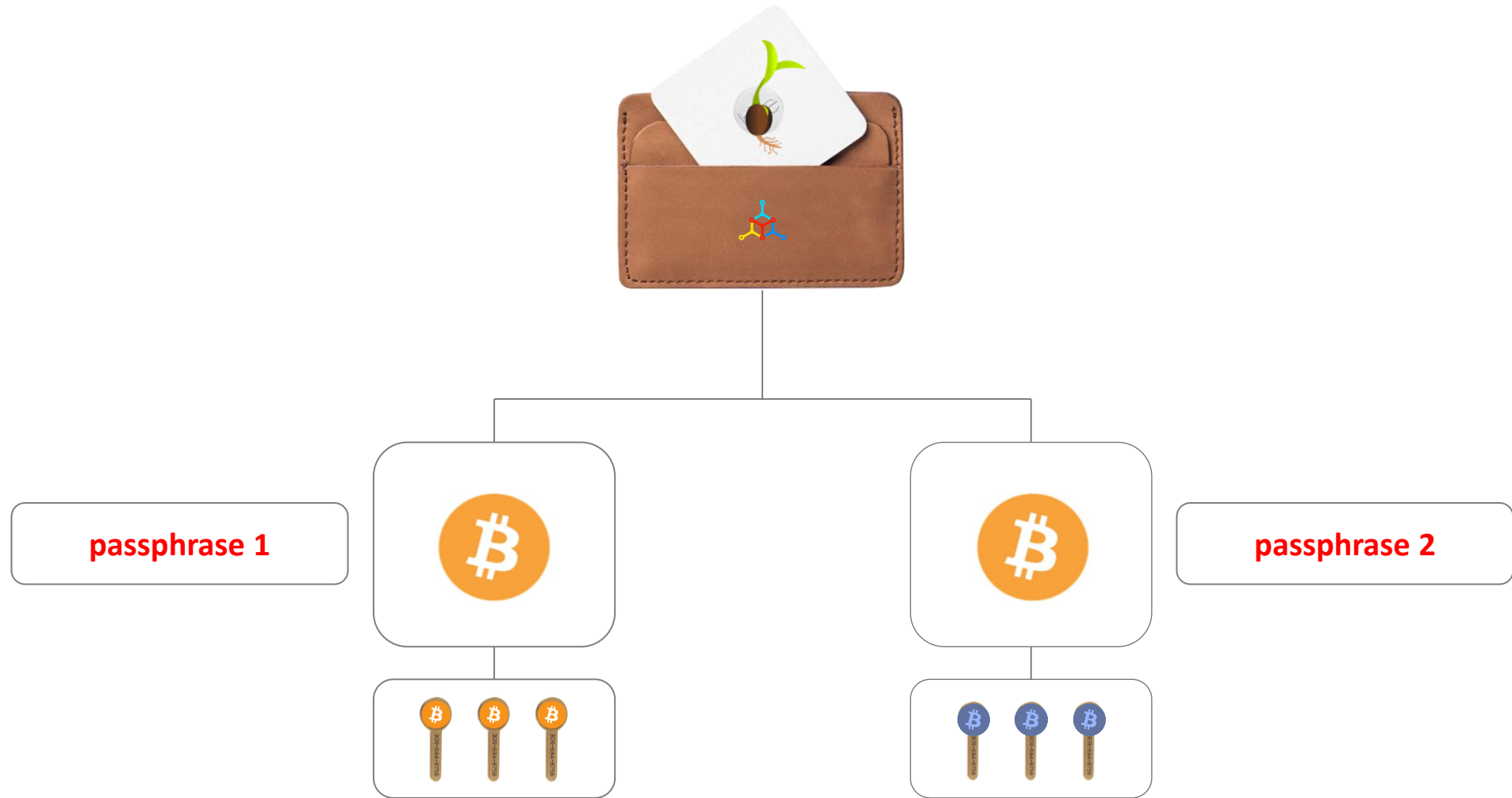













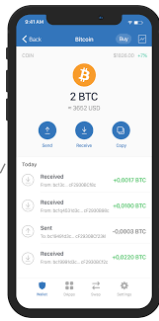




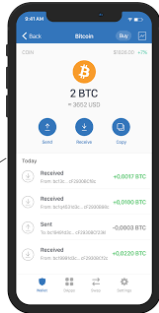
Seed words	
Random number	
Passphrase	@!?
Derivation path	44'0'
Master private key	
XPRIV	
Private Keys	



- 1 RESULT
- 2 INDEX
- 3 DECLINE
- 4 PILL
- 5 RICH
- 6 HEART
- 7 TOAST
- 8 NASTY
- 9 CHOICE
- 10 CONSIDER
- 11 AWARE
- 12 CANNON



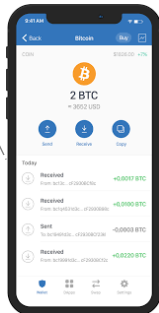
passphrase dad



passphrase mom

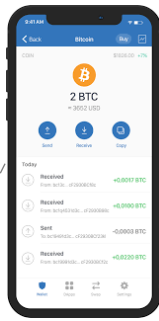


passphrase sally

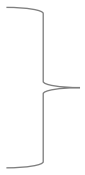
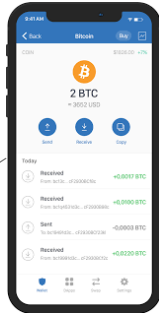


passphrase jack

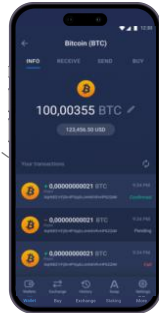
- 1 RESULT
- 2 INDEX
- 3 DECLINE
- 4 PILL
- 5 RICH
- 6 HEART
- 7 TOAST
- 8 NASTY
- 9 CHOICE
- 10 CONSIDER
- 11 AWARE
- 12 CANNON



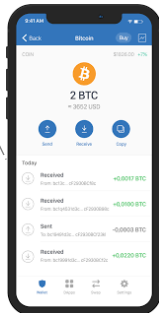
m 44' 0' 0'



m 44' 0' 1'



m 44' 0' 2'



m 44' 0' 3'



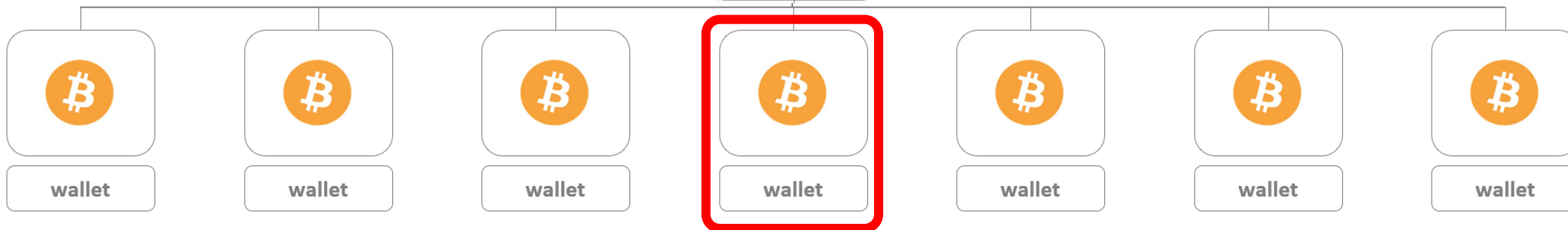
**BitcoinBadger.net**





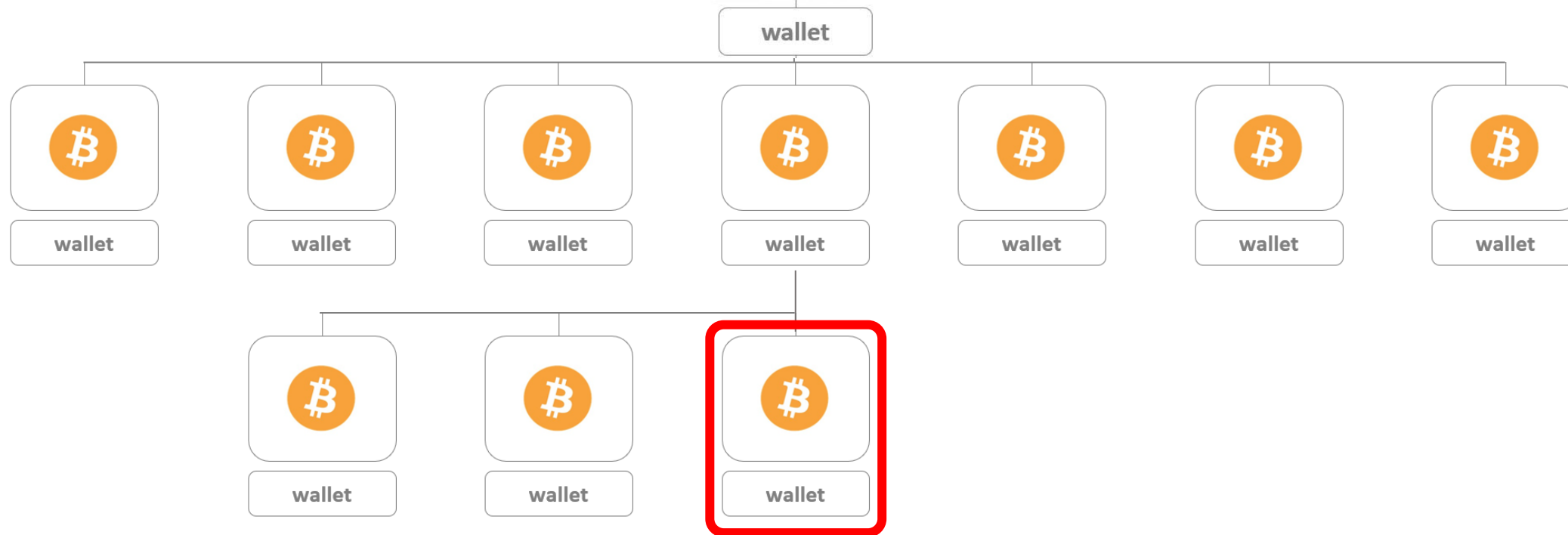
m 44' 0' 3'

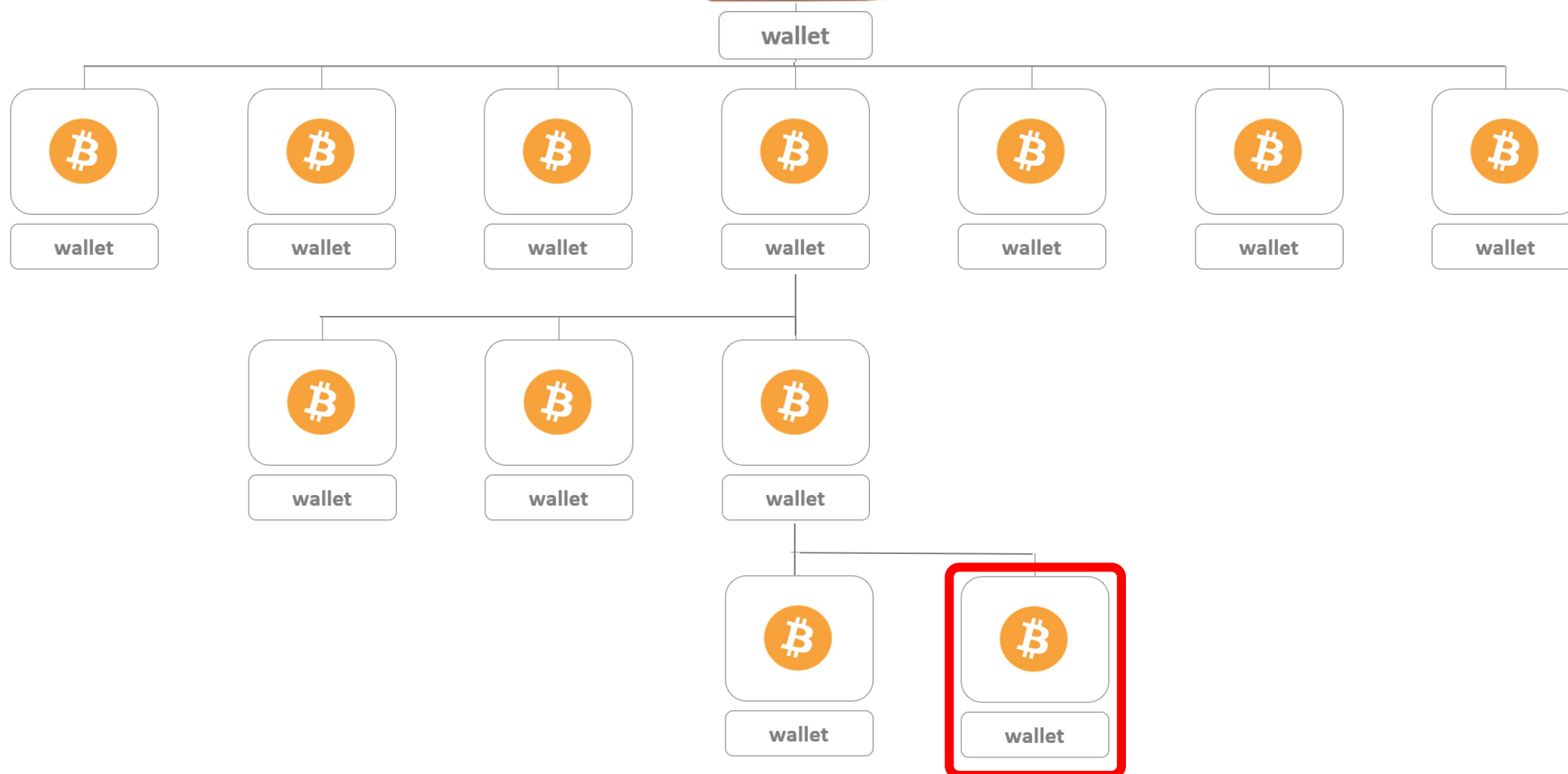
wallet





m 44' 0' 3' 2'







wallet

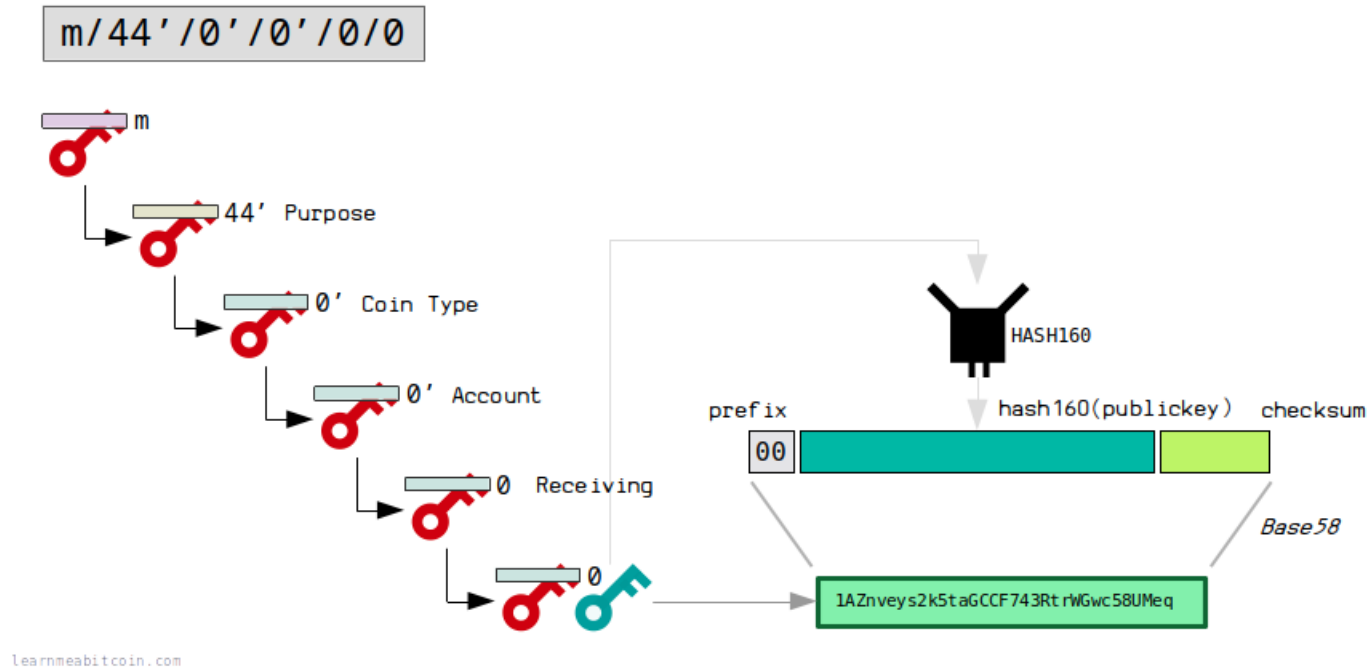
m 44' 0' 3' 2' 1' 0' 3' 2' 1'



wallet

m 44' 0' 3' 2' 1' 0' 3' 2' 1' 23

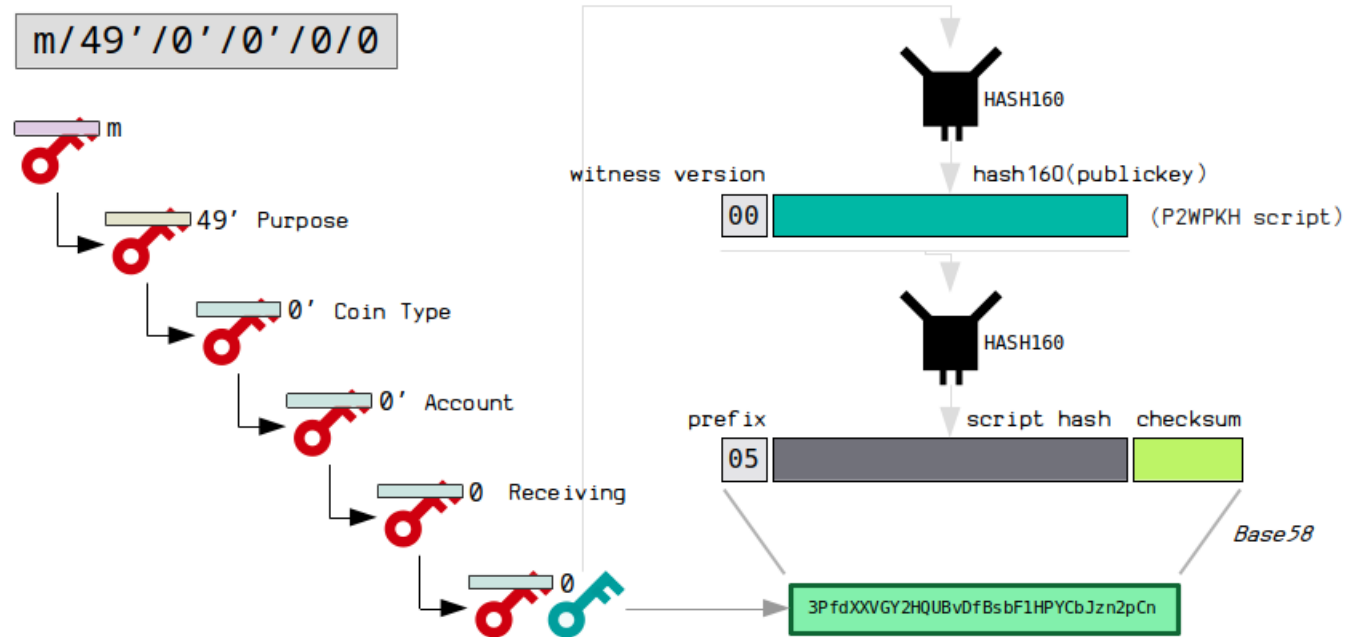
## BIP 44: `m/44'/0'/0'/0/0`



[BIP 44](#) builds upon the original BIP 32 scheme to include a [purpose](#) (which is like a version number to identify the upcoming scheme), as well as a **coin type** so that the same seed can be used to generate keys for different cryptocurrencies.

The first level of `44'` indicates that the wallet uses `1addresses` ([P2PKH](#)).

## BIP 49: `m/49'/0'/0'/0/0`

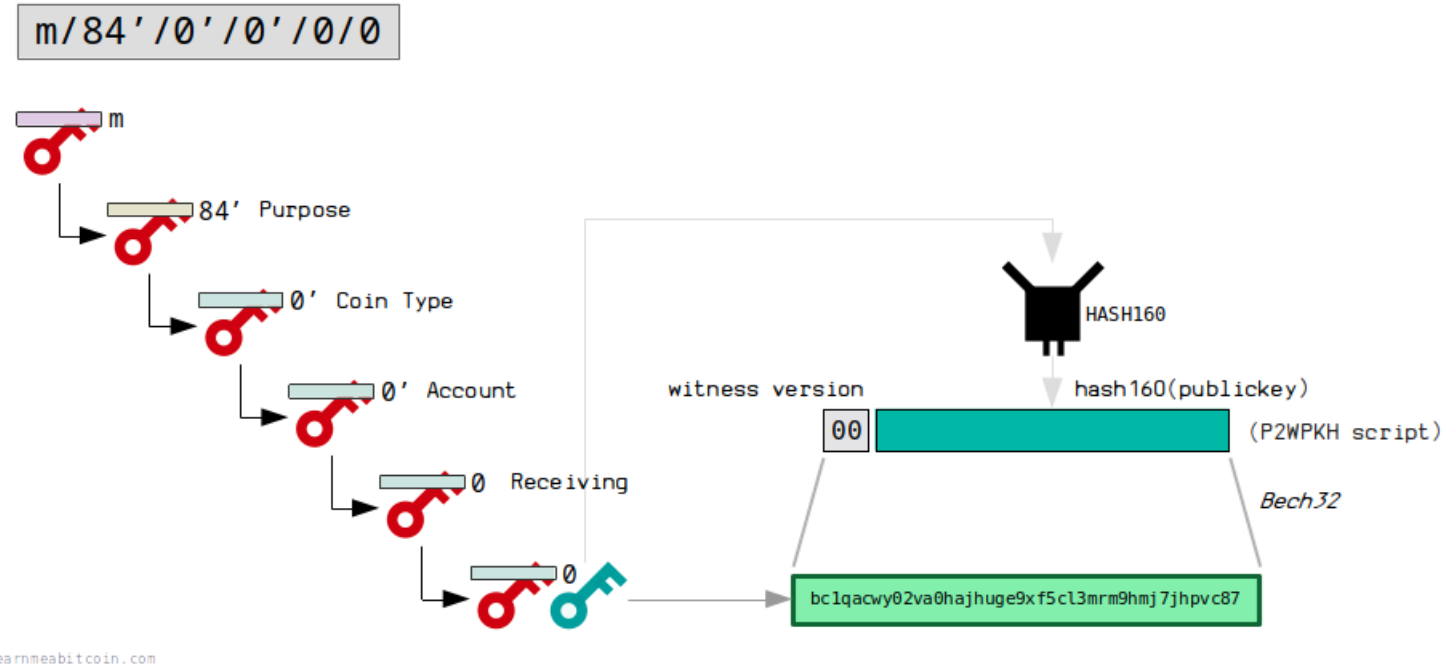


learnmeabitcoin.com

[BIP 49](#) uses the same structure as BIP 44.

The first level of `49'` indicates that the wallet uses `3addresses` (P2WPKH wrapped in P2SH).

## BIP 84: `m/84'/0'/0'/0/0`



[BIP 84](#) uses the same structure as BIP 44.

The first level of `84'` indicates that the wallet uses `bc1addresses` (P2WPKH).





**BitcoinBadger.net**