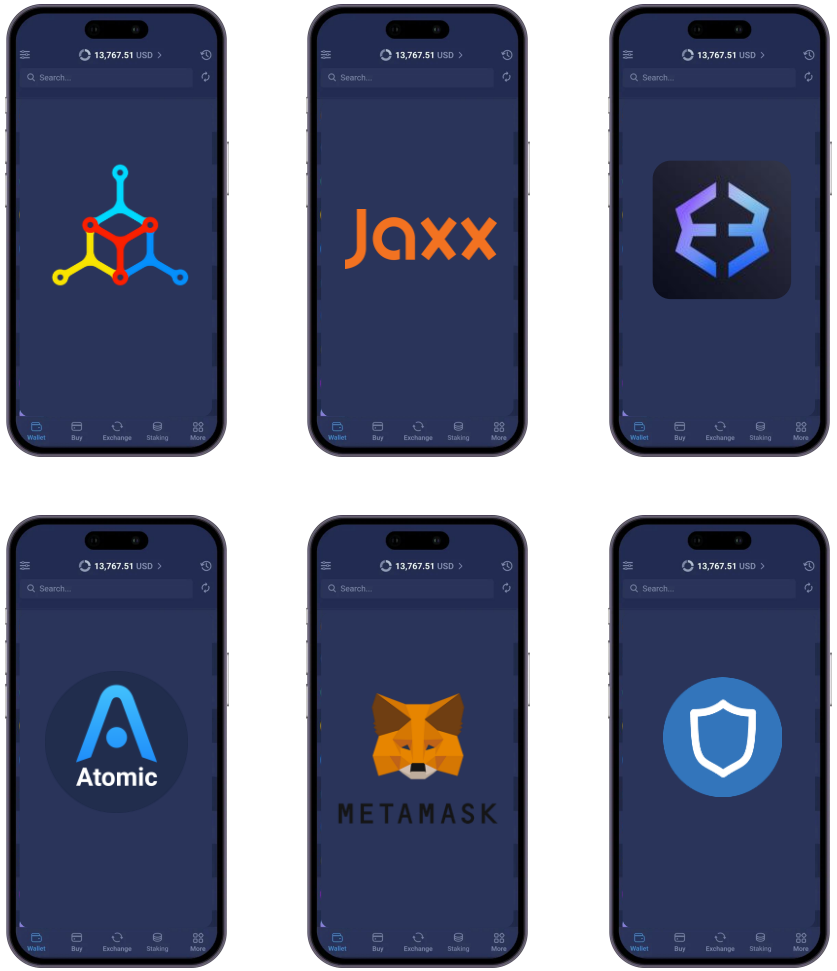
BitcoinBadger.net

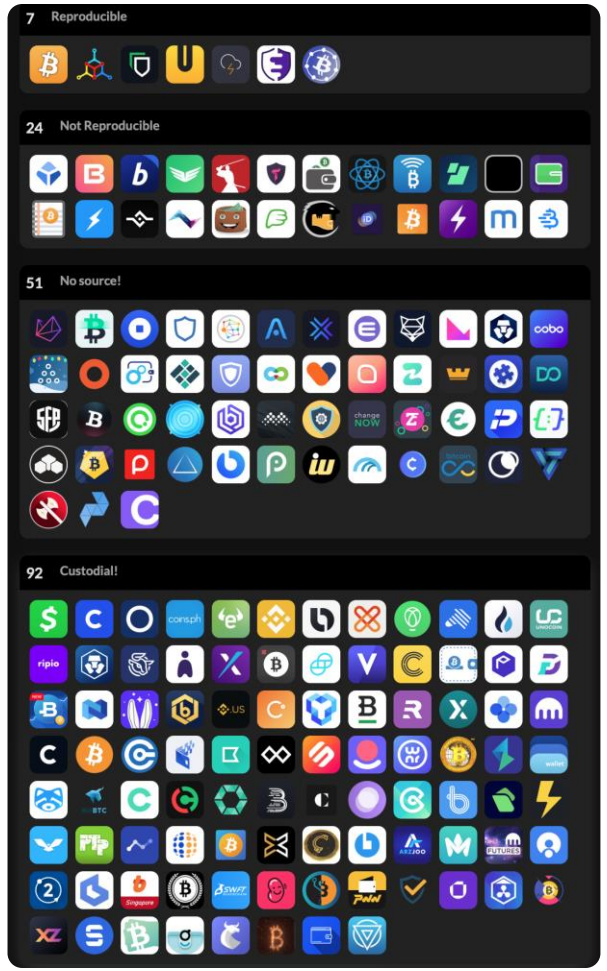
6: Wallet derivation path


Bitcoin (BTC)
1.3478 BTC
51,220.06 USD
Your transactions
+ 0.0031671 BTC
23:21
05.02.21
Confirmed
+ 0.0025704 BTC
21:05
05.02.21
Confirmed
+ 0.0071143 BTC
13:25
03.02.21
Confirmed
+ 0.0000392 BTC
21:05
02.02.21
Confirmed
RECEIVE
SEND

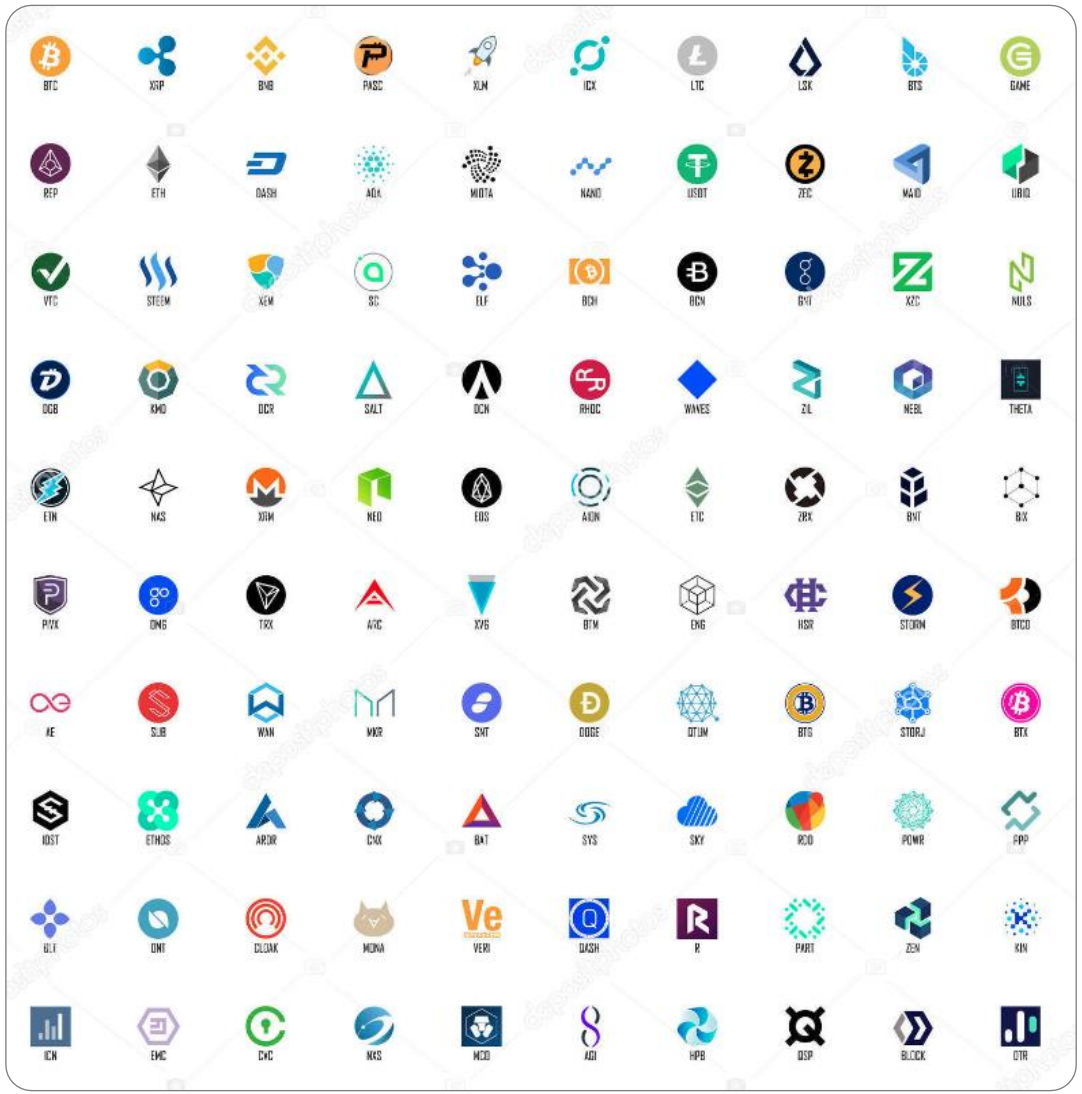

Bitcoin (BTC)
1.3478 BTC
51,220.06 USD
Your transactions
+ 0.0031671 BTC
23:21
05.02.21
Confirmed
+ 0.0025704 BTC
21:05
05.02.21
Confirmed
+ 0.0071143 BTC
13:25
03.02.21
Confirmed
+ 0.0000392 BTC
21:05
02.02.21
Confirmed
RECEIVE
SEND


13,767.51 USD
Search...
BTC
$22,740.17 (-0.75%)
0.06244358
$1440.83
ETH
$1,633.32 (0.13%)
0.45800341
$738.34
USDT
$1 (0.001%)
536.37
$536
BNB
$334.95 (0.16%)
1.343
$449.83
USDC
$1 (-0.006%)
276
$276
XRP
$0.4623 (-0.05%)
2.434
$137.82
ADA
$0.385 (0.03%)
692.96
$266.73
DOGE
$0.078 (1.06%)
1966
$153.82
MATIC
$0.9771 (-0.93%)
74.32
$72.7
SOL
4.026
Wallet
Buy
Exchange
Staking
More


Jaxx
Atomic
METAMASK


7 Reproducible
24 Not Reproducible
51 No source!
92 Custodial!


13,767.51 USD
Search...
BTC
$22,740.17 (-0.75%)
0.06244358
$1440.83
ETH
$1,633.32 (0.13%)
0.45800341
$738.34
USDT
$1 (0.001%)
536.37
$536
BNB
$334.95 (0.16%)
1.343
$449.83
USDC
$1 (-0.006%)
276
$276
XRP
$0.4623 (-0.05%)
2.434
$137.82
ADA
$0.385 (0.03%)
692.96
$266.73
DOGE
$0.078 (1.06%)
1966
$153.82
MATIC
$0.9771 (-0.93%)
74.32
$72.7
SOL
4.026
Wallet
Buy
Exchange
Staking
More




13,767.51 USD
Search...
BTC
$22,740.17 (-0.75%)
0.06244358
$1440.83
ETH
$1,633.32 (0.13%)
0.45800341
$738.34
USDT
$1 (0.001%)
536.37
$536
BNB
$334.95 (0.16%)
1.343
$449.83
USDC
$1 (-0.006%)
276
$276
XRP
$0.4623 (-0.05%)
2.434
$137.82
ADA
$0.385 (0.03%)
692.96
$266.73
DOGE
$0.078 (1.06%)
1966
$153.82
MATIC
$0.9771 (-0.93%)
74.32
$72.7
SOL
4.026
Wallet
Buy
Exchange
Staking
More

1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy

bc1qar0srrr7xfkvy5l643lydnw9re59gtzzwf8k3y

bc1p5d7rjq7g6rdk2yhzks9smlaqtedr4dekq08ge8ztwac72sfr9rusxg3297

0x742d35Cc6634C0532925a3b844Bc454e4438f44e

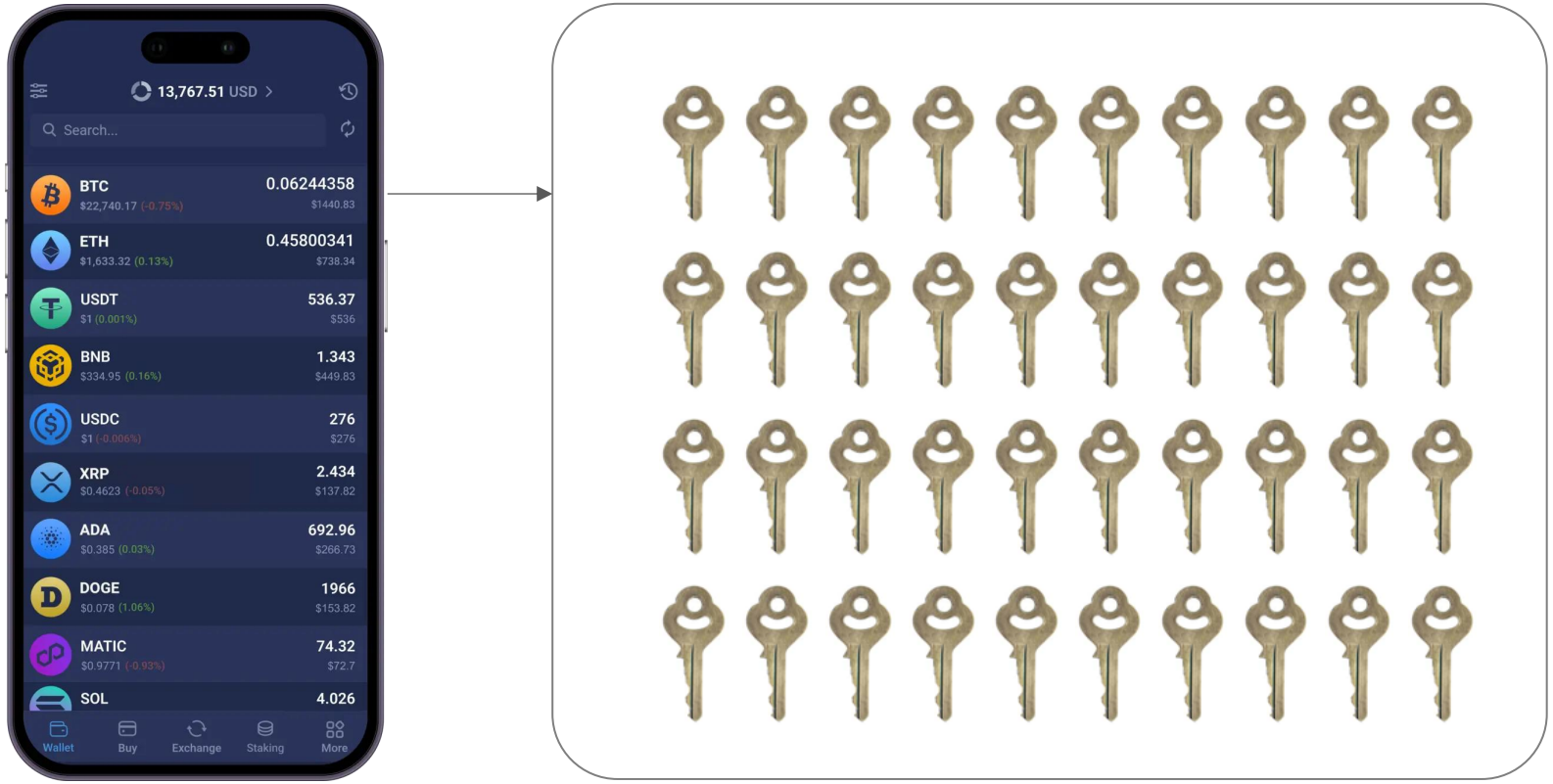
0x71C7656EC7ab88b098defB751B7401B5f6d8976F

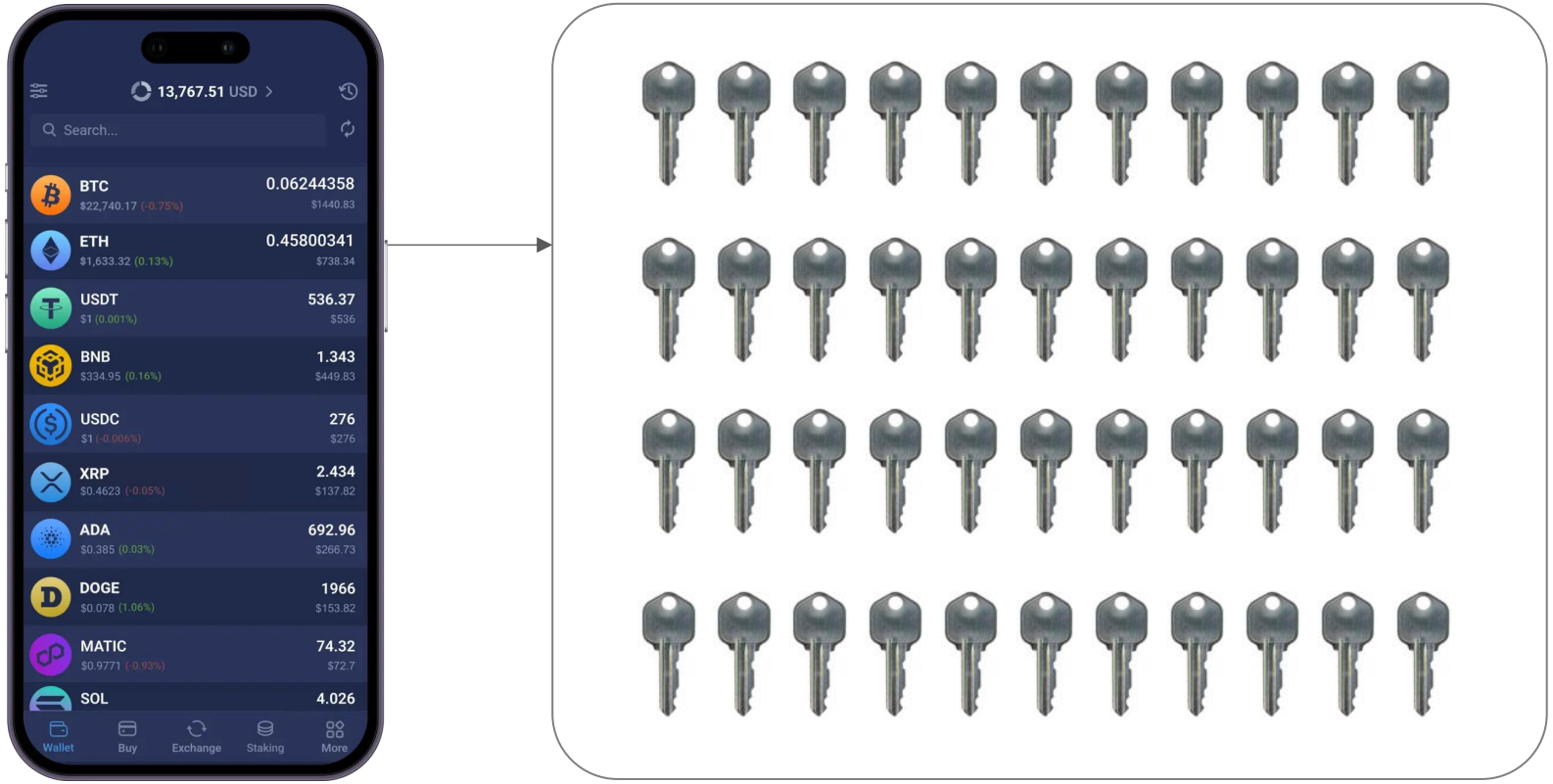
0xb794f5ea0ba39494ce839613fffba74279579268

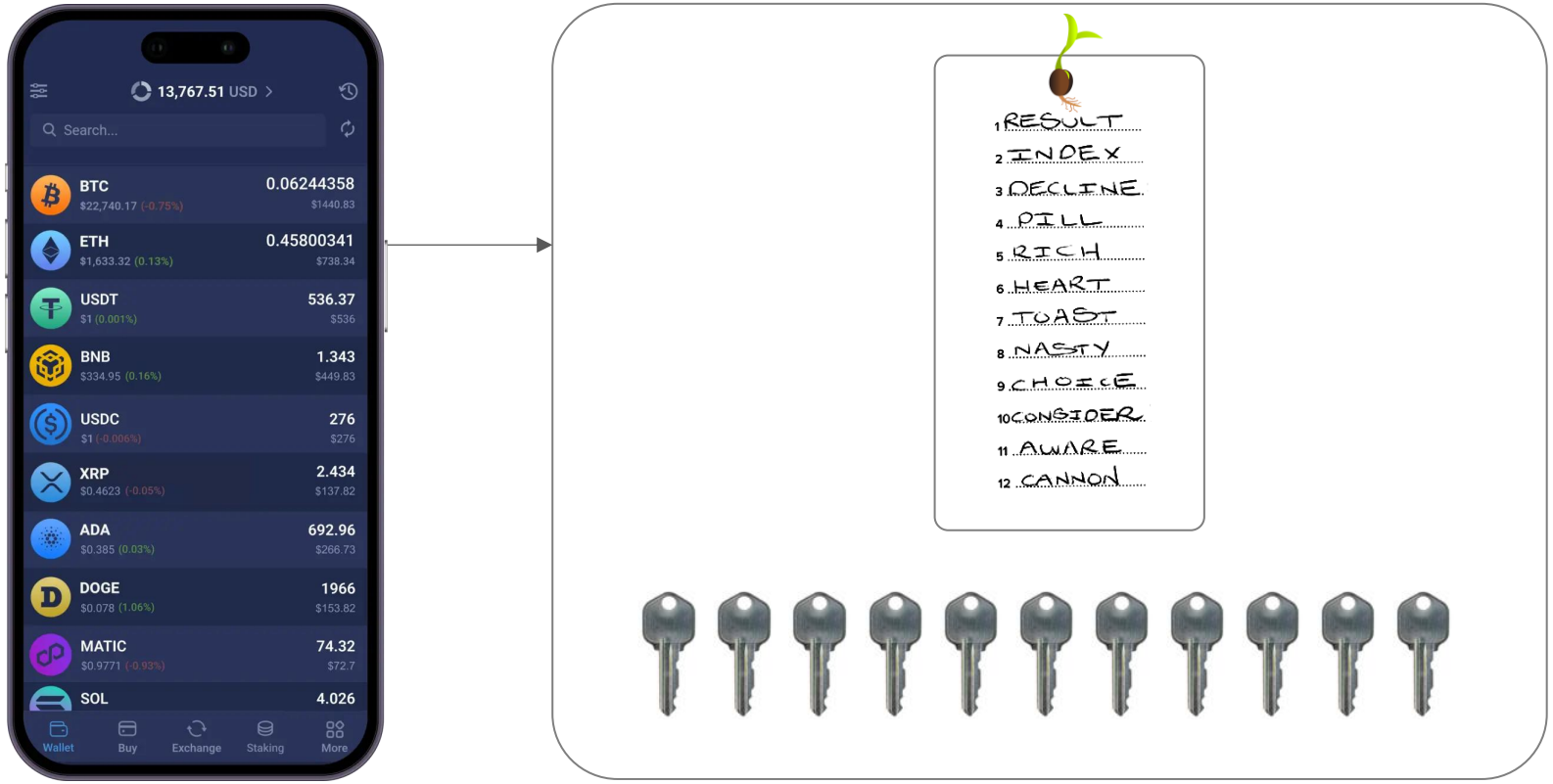
45GjcbHh1fvEyXEA6mDAKqNDMmy1Gon6CNHrdhp9hghfLXQNQj4J76TLtwYGoooKApWLM7kaZwdAxLycceHmuVcELCSFPHq

84EgZVjXKF4d1JkEhZSxm4LQQEx64AvqQEwkvWPtHEb5JMrB1Y86y1vCPSCiXsKzbfS9x8vCpx3gVgPaHCpobPYqQzANTnC

8FKZ5LYDj98gmRH9ex4GCUi7SCpBeckyX5vi97A2YSN9a5wHYGXKfMfZXHXZGJn87X6NDHAB2jZWWRnnysWoeHTw6XGSCDXRo

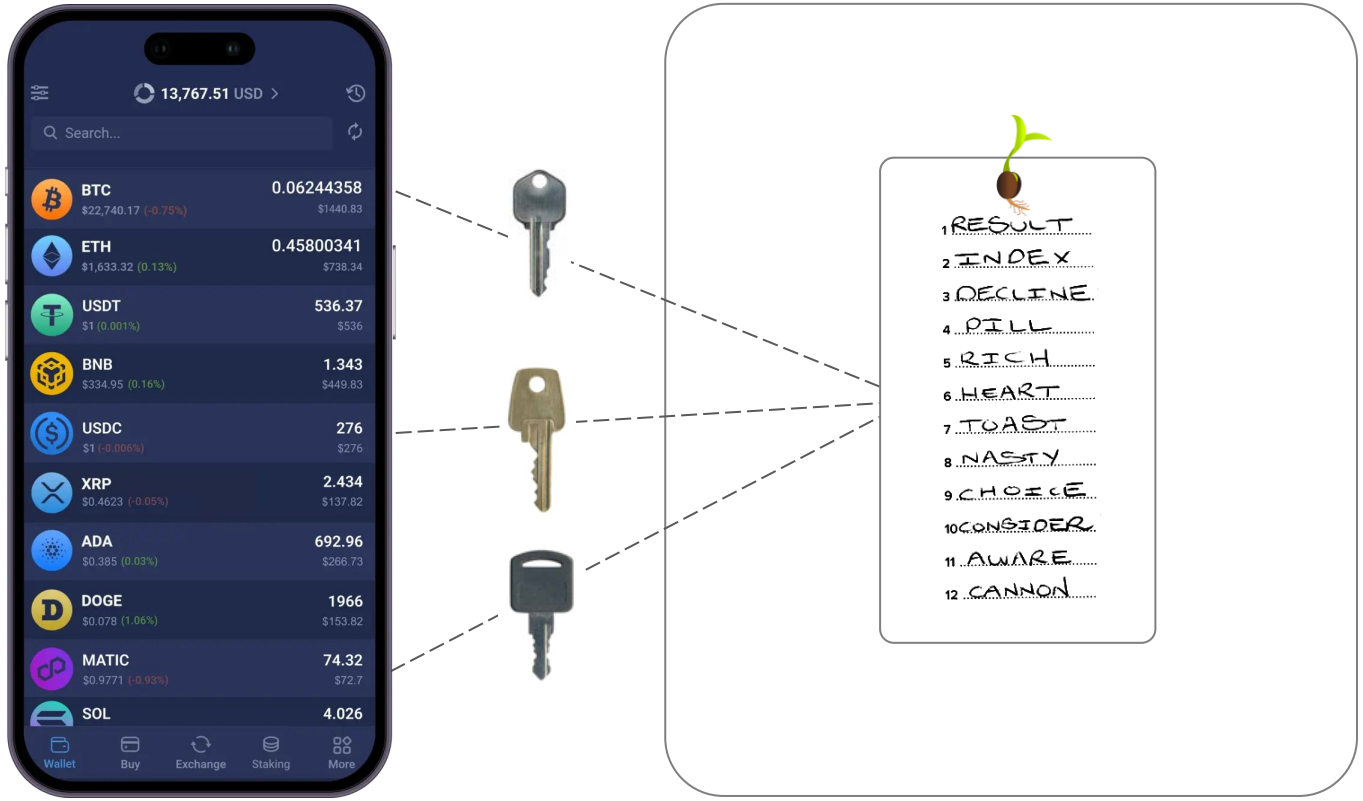

13,767.51 USD
Search...
BTC
$22,740.17 (-0.75%)
0.06244358
$1440.83
ETH
$1,633.32 (0.13%)
0.45800341
$738.34
USDT
$1 (0.001%)
536.37
$536
BNB
$334.95 (0.16%)
1.343
$449.83
USDC
$1 (-0.006%)
276
$276
XRP
$0.4623 (-0.05%)
2.434
$137.82
ADA
$0.385 (0.03%)
692.96
$266.73
DOGE
$0.078 (1.06%)
1966
$153.82
MATIC
$0.9771 (-0.93%)
74.32
$72.7
SOL
4.026
Wallet
Buy
Exchange
Staking
More

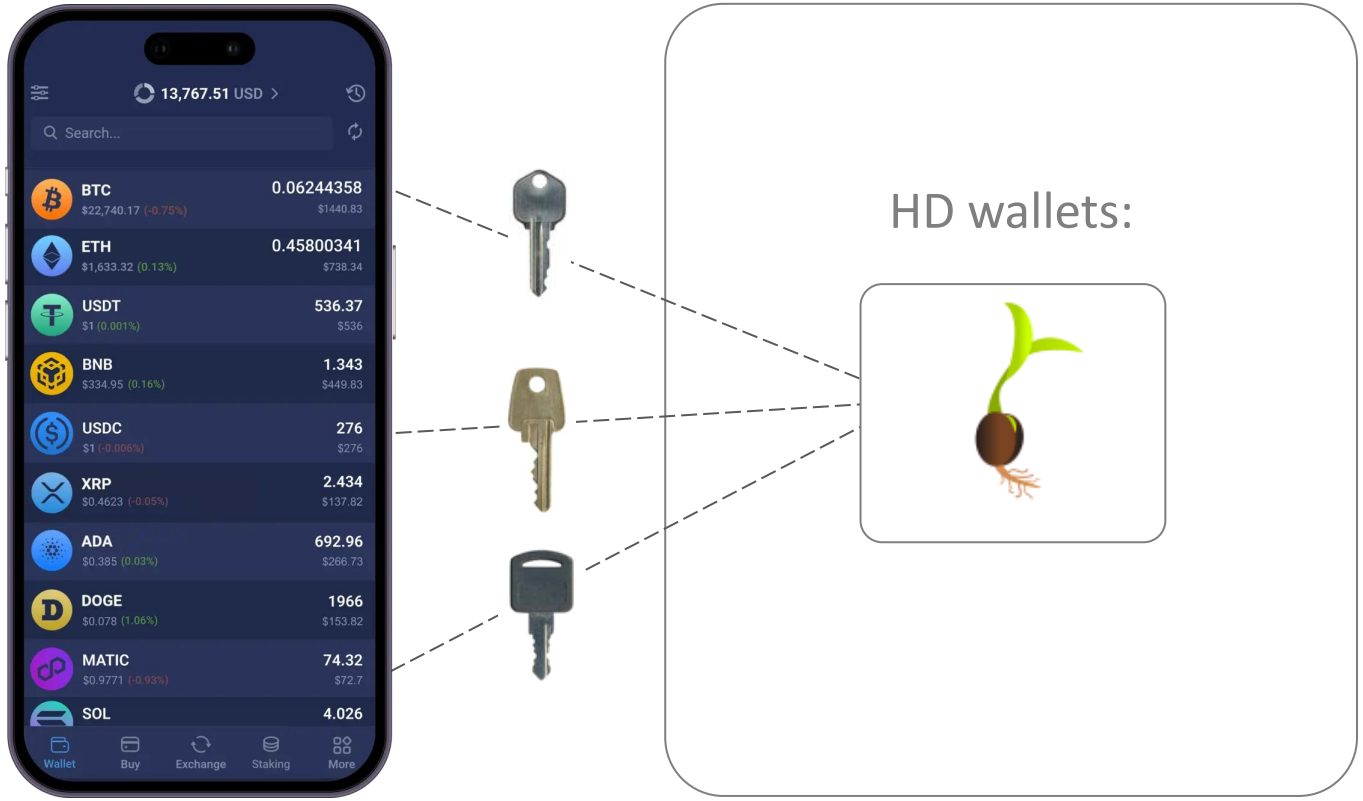

13,767.51 USD
Search...
BTC
$22,740.17 (-0.75%)
0.06244358
$1440.83
ETH
$1,633.32 (0.13%)
0.45800341
$738.34
USDT
$1 (0.001%)
536.37
$536
BNB
$334.95 (0.16%)
1.343
$449.83
USDC
$1 (-0.006%)
276
$276
XRP
$0.4623 (-0.05%)
2.434
$137.82
ADA
$0.385 (0.03%)
692.96
$266.73
DOGE
$0.078 (1.06%)
1966
$153.82
MATIC
$0.9771 (-0.93%)
74.32
$72.7
SOL
4.026
Wallet
Buy
Exchange
Staking
More

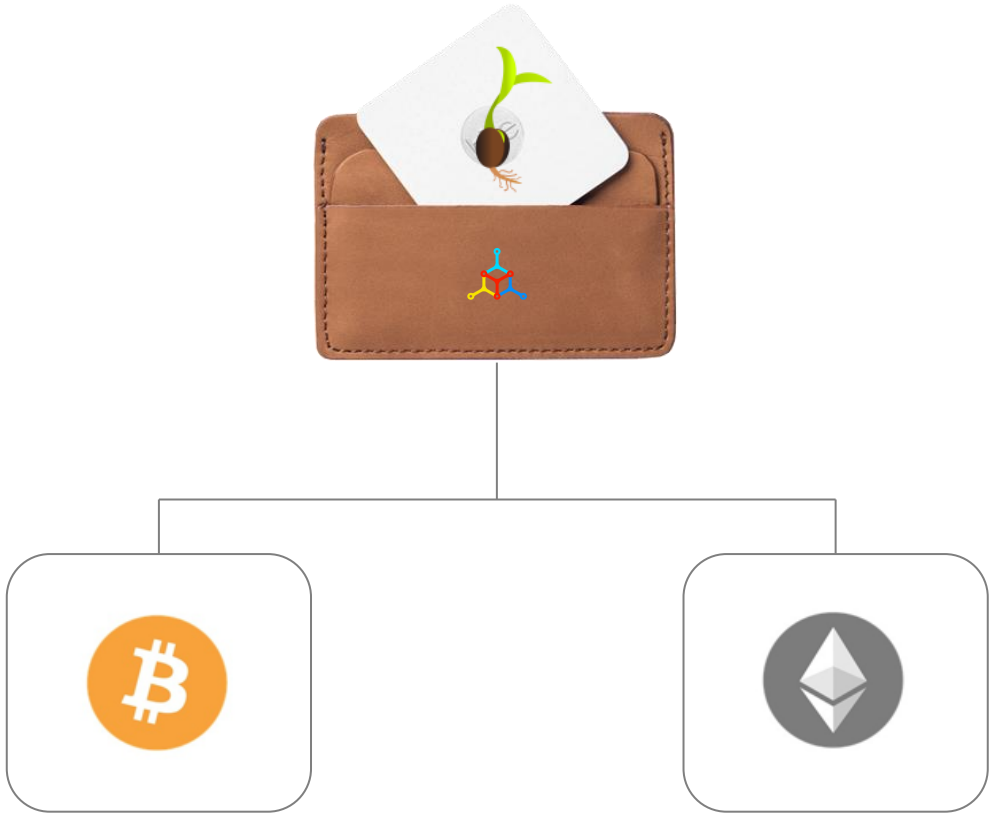

13,767.51 USD
Search...
BTC
$22,740.17 (-0.75%)
0.06244358
$1440.83
ETH
$1,633.32 (0.13%)
0.45800341
$738.34
USDT
$1 (0.001%)
536.37
$536
BNB
$334.95 (0.16%)
1.343
$449.83
USDC
$1 (-0.006%)
276
$276
XRP
$0.4623 (-0.05%)
2.434
$137.82
ADA
$0.385 (0.03%)
692.96
$266.73
DOGE
$0.078 (1.06%)
1966
$153.82
MATIC
$0.9771 (-0.93%)
74.32
$72.7
SOL
4.026
Wallet
Buy
Exchange
Staking
More
1 RESULT
2 INDEX
3 DECLINE
4 PILL
5 RICH
6 HEART
7 TOAST
8 NASTY
9 CHOICE
10 CONSIDER
11 AWARE
12 CANNON

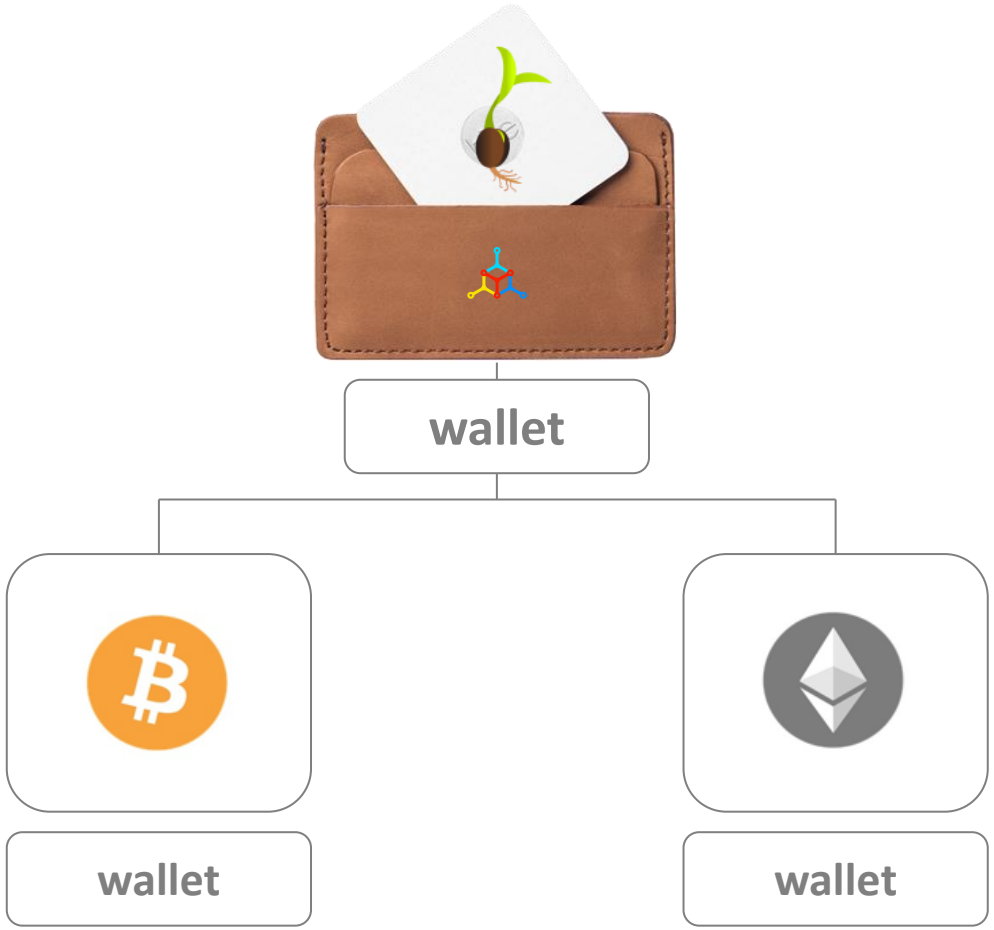

13,767.51 USD
Search...
BTC
$22,740.17 (-0.75%)
0.06244358
$1440.83
ETH
$1,633.32 (0.13%)
0.45800341
$738.34
USDT
$1 (0.001%)
536.37
$536
BNB
$334.95 (0.16%)
1.343
$449.83
USDC
$1 (-0.006%)
276
$276
XRP
$0.4623 (-0.05%)
2.434
$137.82
ADA
$0.385 (0.03%)
692.96
$266.73
DOGE
$0.078 (1.06%)
1966
$153.82
MATIC
$0.9771 (-0.93%)
74.32
$72.7
SOL
4.026
Wallet
Buy
Exchange
Staking
More

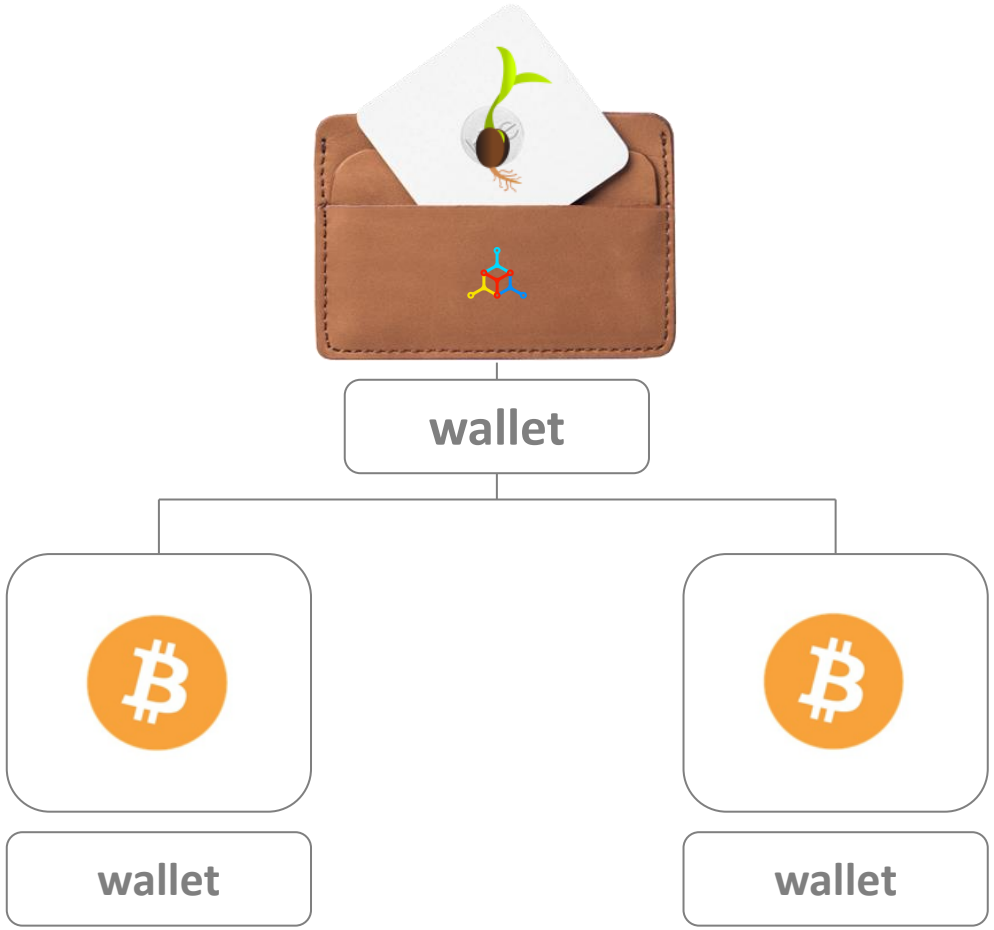

13,767.51 USD
Search...
BTC
$22,740.17 (-0.75%)
0.06244358
$1440.83
ETH
$1,633.32 (0.13%)
0.45800341
$738.34
USDT
$1 (0.001%)
536.37
$536
BNB
$334.95 (0.16%)
1.343
$449.83
USDC
$1 (-0.006%)
276
$276
XRP
$0.4623 (-0.05%)
2.434
$137.82
ADA
$0.385 (0.03%)
692.96
$266.73
DOGE
$0.078 (1.06%)
1966
$153.82
MATIC
$0.9771 (-0.93%)
74.32
$72.7
SOL
4.026
Wallet
Buy
Exchange
Staking
More

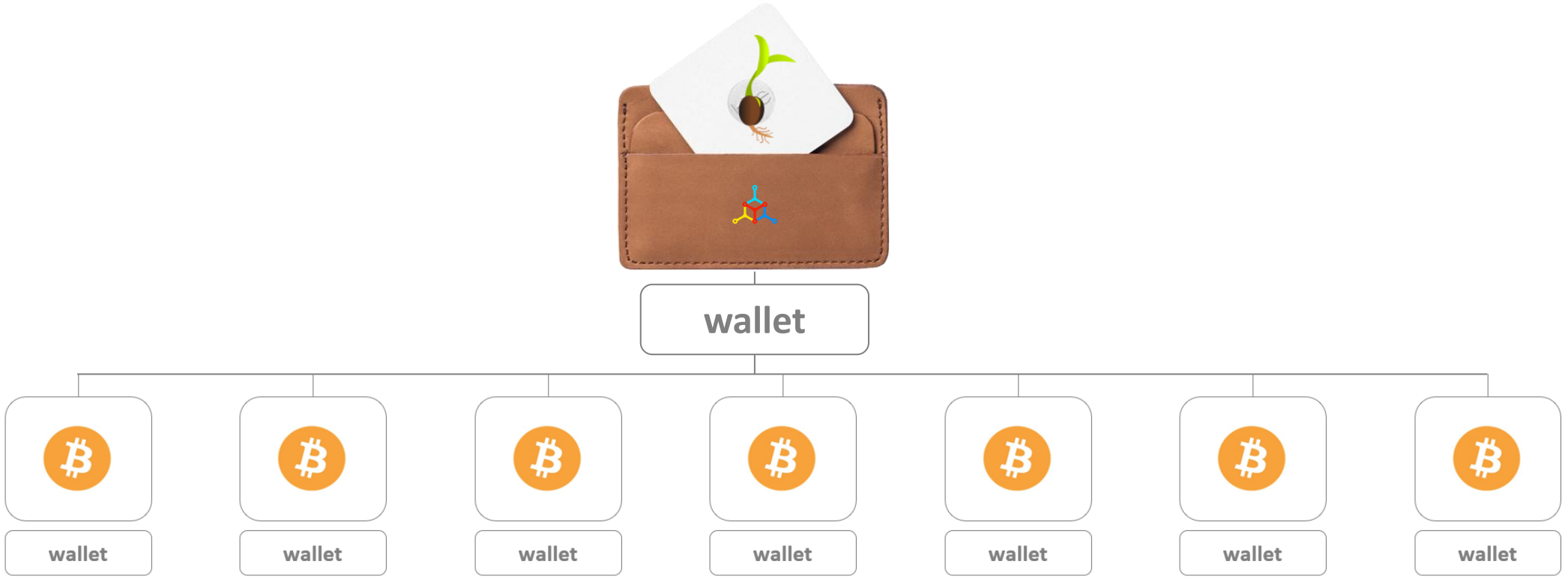

13,767.51 USD
Search...
BTC
$22,740.17 (-0.75%)
0.06244358
$1440.83
ETH
$1,633.32 (0.13%)
0.45800341
$738.34
USDT
$1 (0.001%)
536.37
$536
BNB
$334.95 (0.16%)
1.343
$449.83
USDC
$1 (-0.006%)
276
$276
XRP
$0.4623 (-0.05%)
2.434
$137.82
ADA
$0.385 (0.03%)
692.96
$266.73
DOGE
$0.078 (1.06%)
1966
$153.82
MATIC
$0.9771 (-0.93%)
74.32
$72.7
SOL
4.026
Wallet
Buy
Exchange
Staking
More
1 RESULT
2 INDEX
3 DECLINE
4 PILL
5 RICH
6 HEART
7 TOAST
8 NASTY
9 CHOICE
10 CONSIDER
11 AWARE
12 CANNON

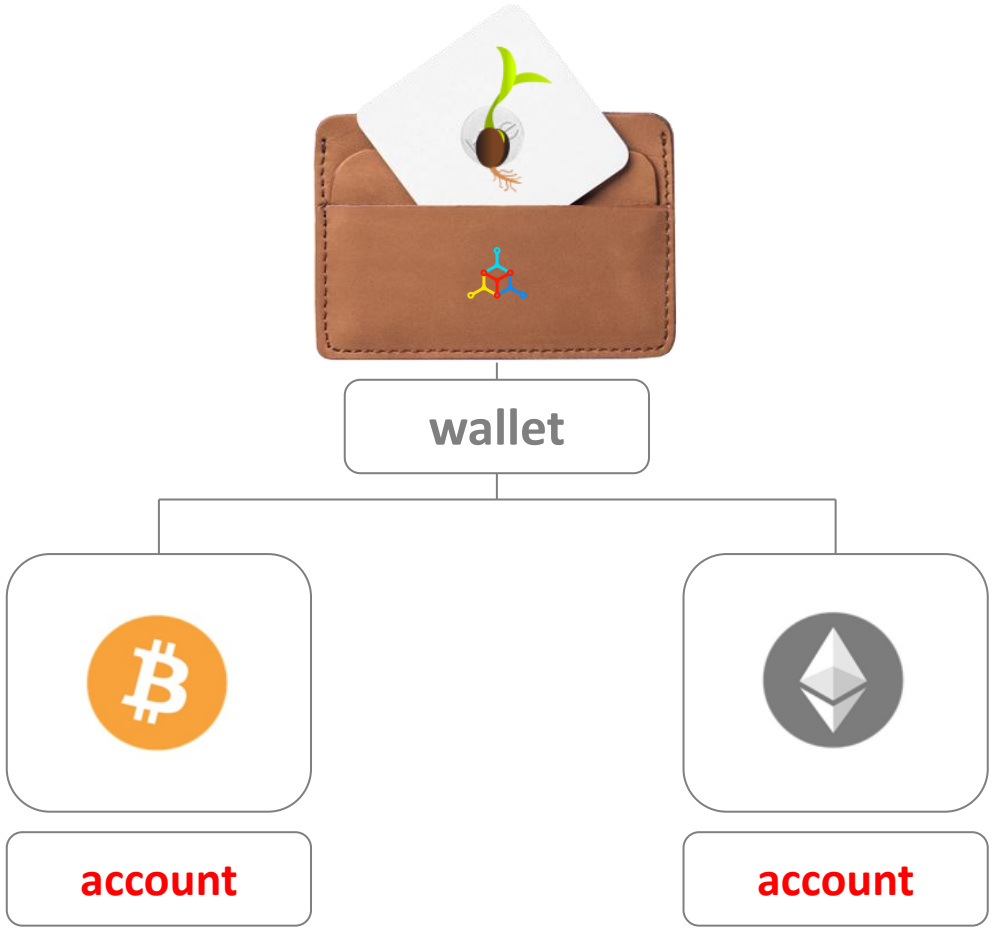

13,767.51 USD
Search...
BTC
$22,740.17 (-0.75%)
0.06244358
$1440.83
ETH
$1,633.32 (0.13%)
0.45800341
$738.34
USDT
$1 (0.001%)
536.37
$536
BNB
$334.95 (0.16%)
1.343
$449.83
USDC
$1 (-0.006%)
276
$276
XRP
$0.4623 (-0.05%)
2.434
$137.82
ADA
$0.385 (0.03%)
692.96
$266.73
DOGE
$0.078 (1.06%)
1966
$153.82
MATIC
$0.9771 (-0.93%)
74.32
$72.7
SOL
4.026
Wallet
Buy
Exchange
Staking
More
HD wallets:

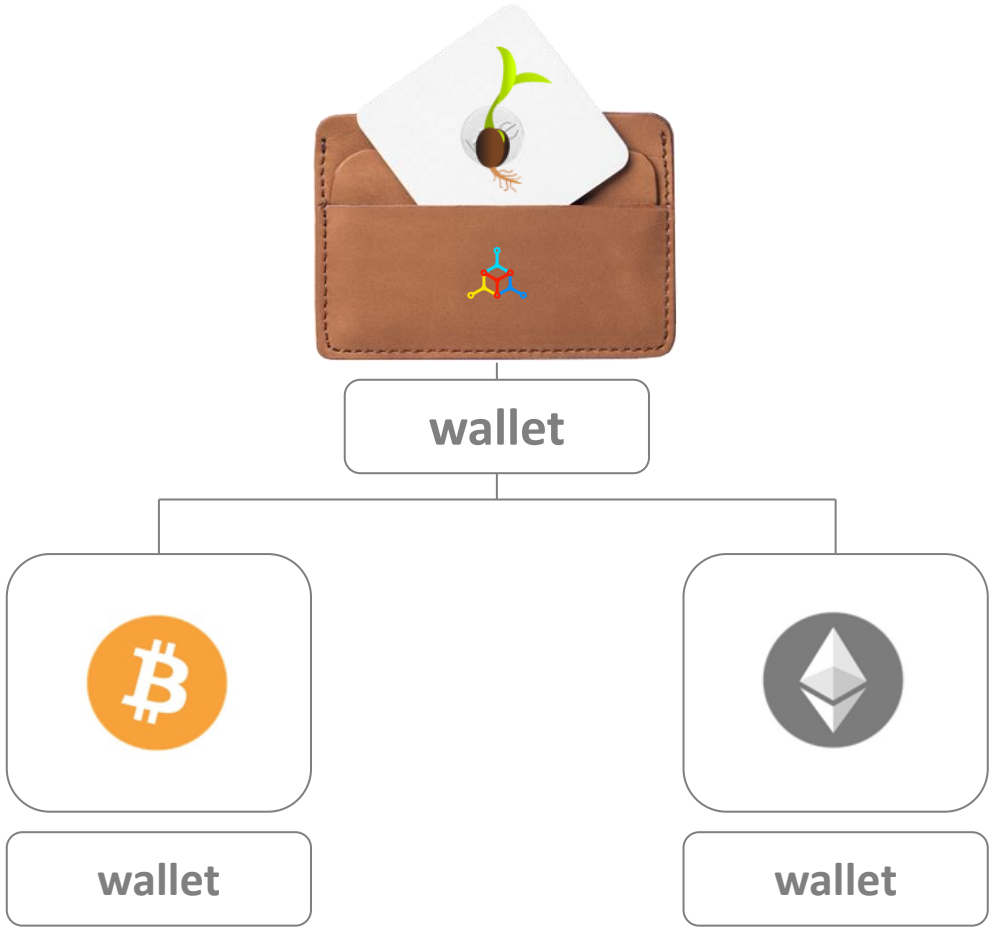



wallet
wallet
wallet


wallet
wallet
wallet

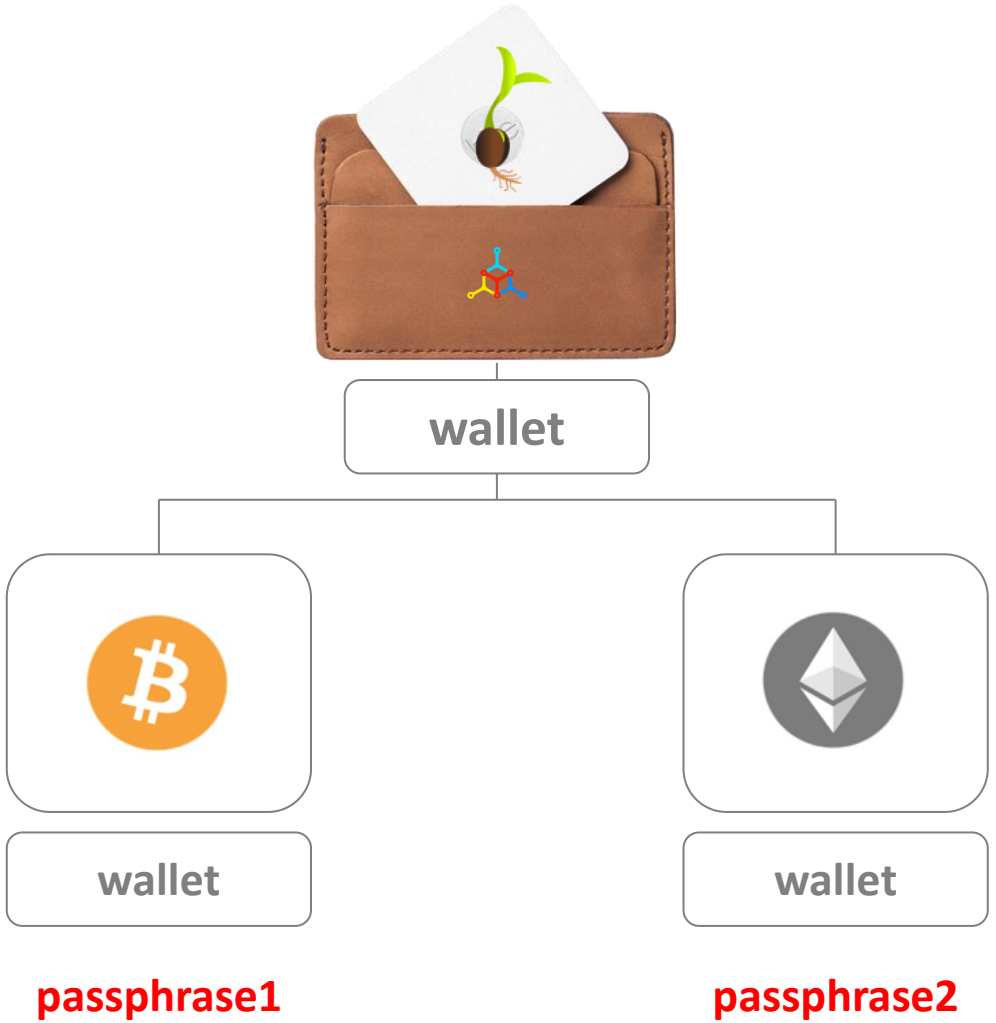

wallet
wallet
wallet
wallet
wallet
wallet
wallet
wallet


wallet
account
account


wallet
wallet
wallet


wallet
wallet
wallet
wallet
wallet
wallet
wallet
wallet


wallet
wallet
wallet
wallet
wallet
wallet
wallet
wallet
passphrase1
passphrase2
passphrase3
passphrase4
passphrase5
passphrase6
passphrase7


wallet
wallet
wallet
passphrase1
passphrase2


13,767.51 USD
Search...
BTC
$22,740.17 (-0.75%)
0.06244358
$1440.83
ETH
$1,633.32 (0.13%)
0.45800341
$738.34
USDT
$1 (0.001%)
536.37
$536
BNB
$334.95 (0.16%)
1.343
$449.83
USDC
$1 (-0.006%)
276
$276
XRP
$0.4623 (-0.05%)
2.434
$137.82
ADA
$0.385 (0.03%)
692.96
$266.73
DOGE
$0.078 (1.06%)
1966
$153.82
MATIC
$0.9771 (-0.93%)
74.32
$72.7
SOL
4.026
Wallet
Buy
Exchange
Staking
More

“formula”

“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)

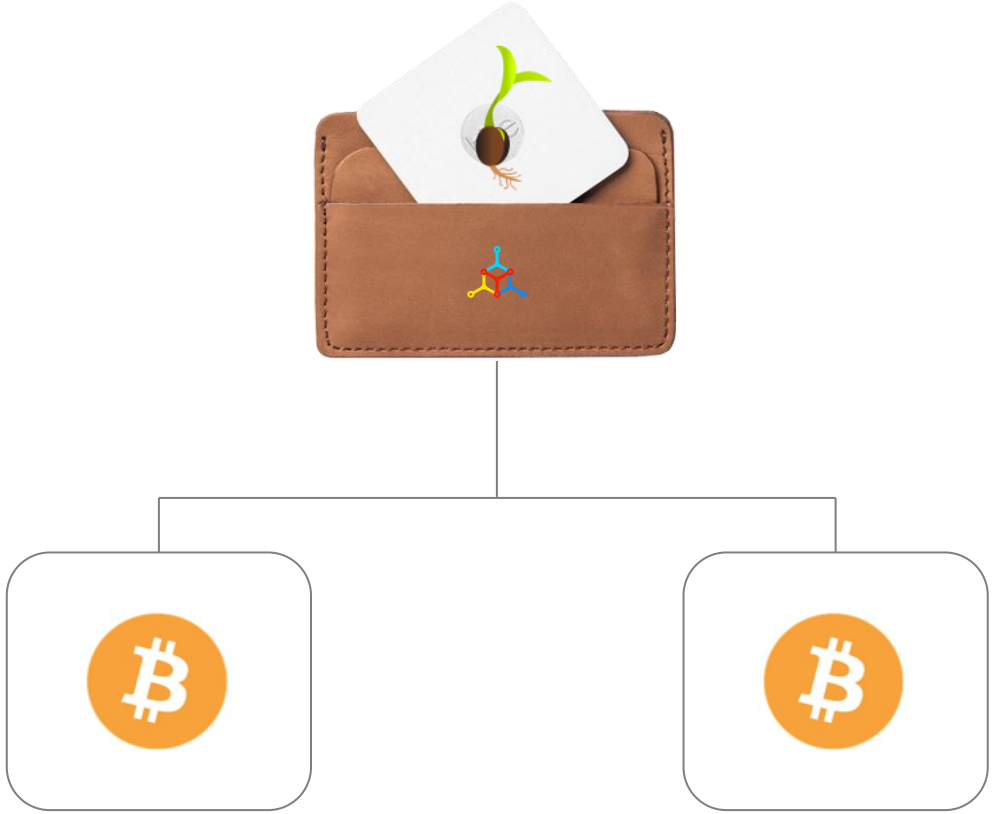
Random number	
Derivation path	
Master private key	
XPRIV	
Private Keys	

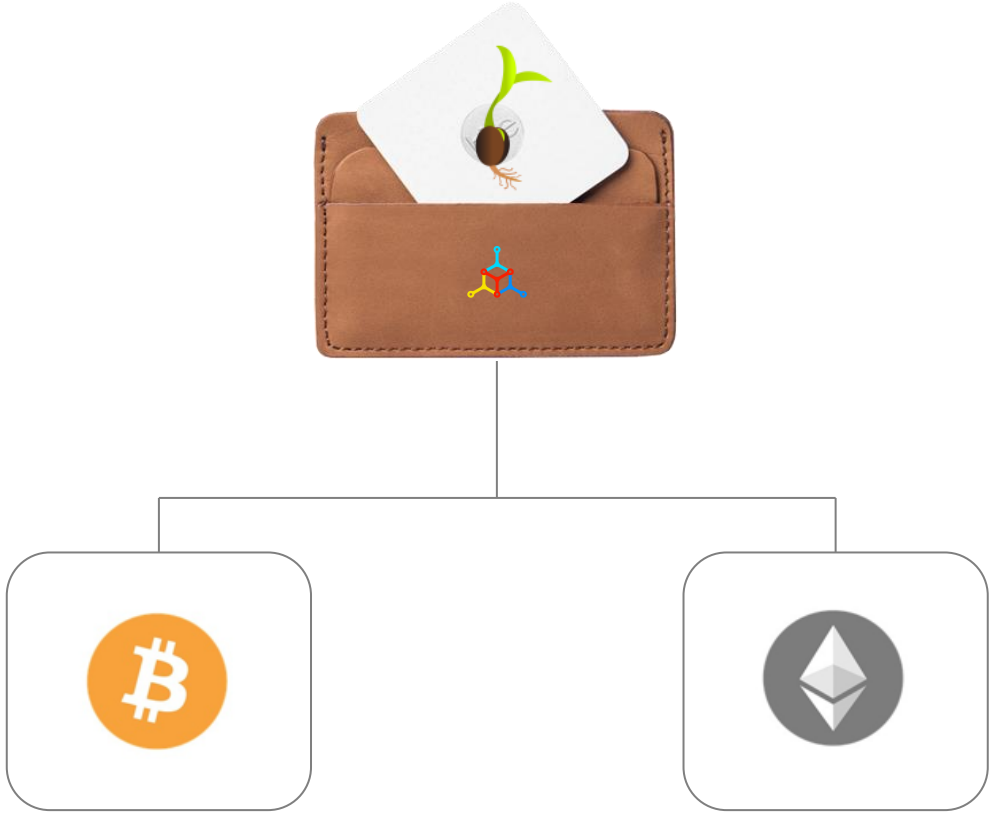
HD wallet (BIP38)

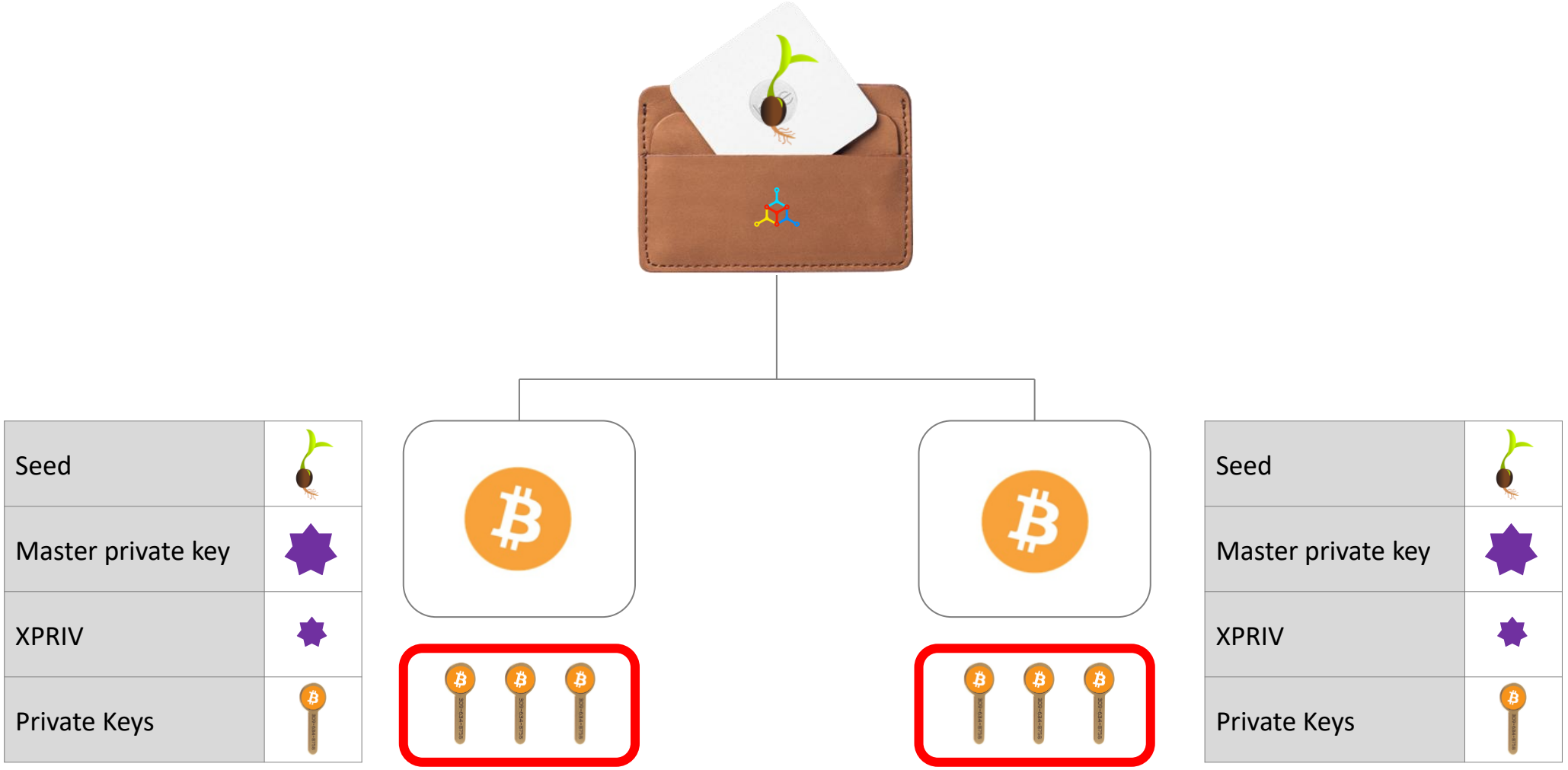
Random number	
Passphrase	
Derivation path	
Master private key	
XPRIV	
Private Keys	

HD wallet(BIP39)

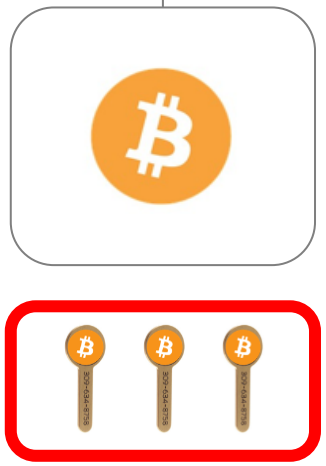
Seed words	
Random number	
Passphrase	@!?
Derivation path	
Master private key	
XPRIV	
Private Keys	

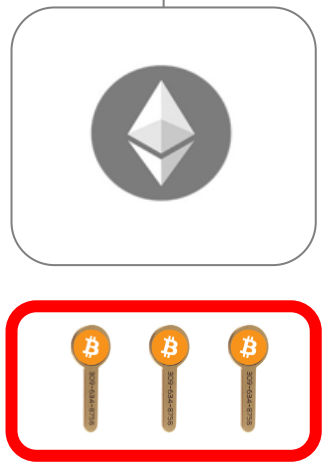




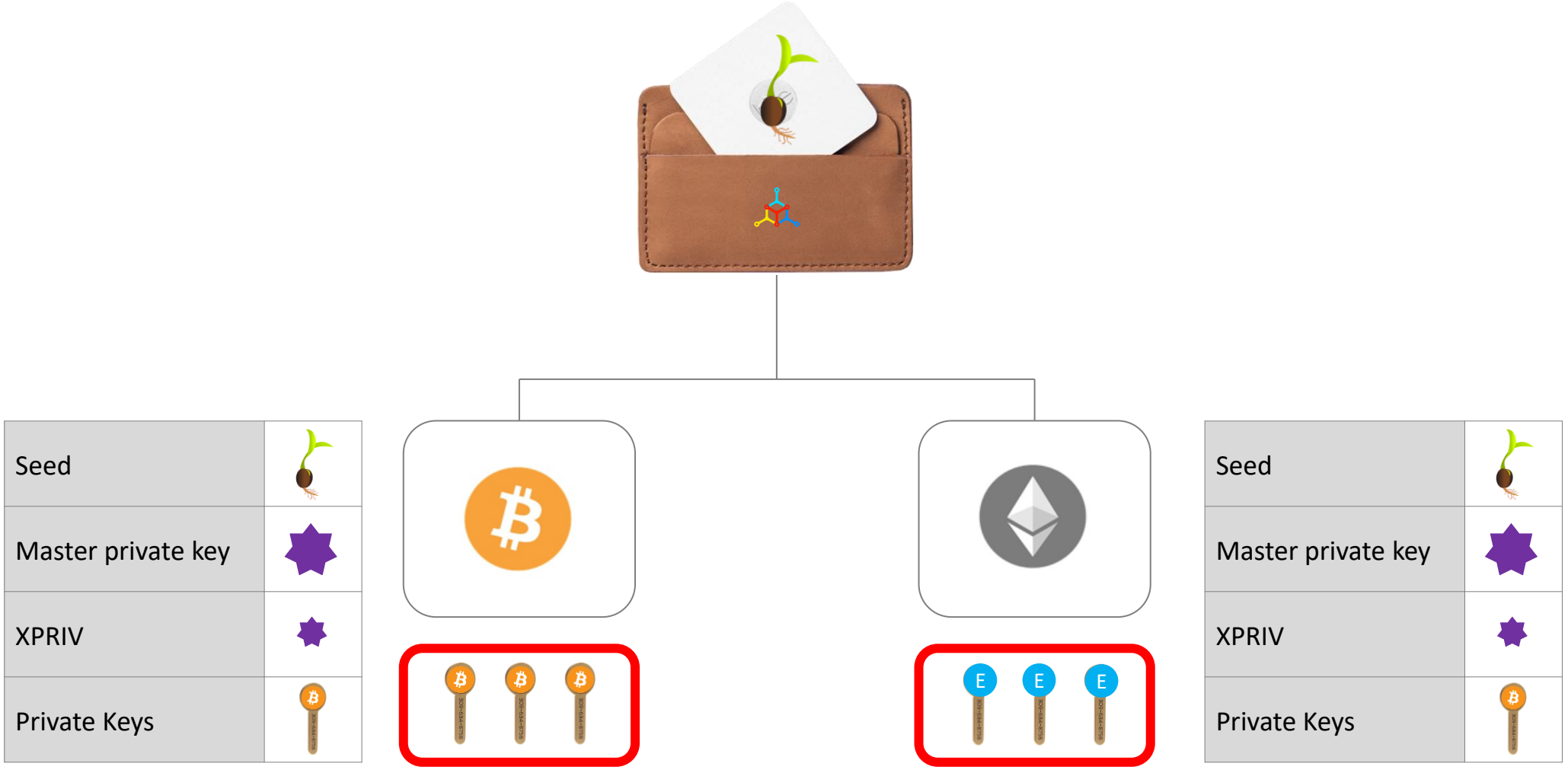

Seed
Master private key
XPRIV
Private Keys
Seed
Master private key
XPRIV
Private Keys

Seed	
Master private key	
XPRIV	
Private Keys	





Seed	
Master private key	
XPRIV	
Private Keys	

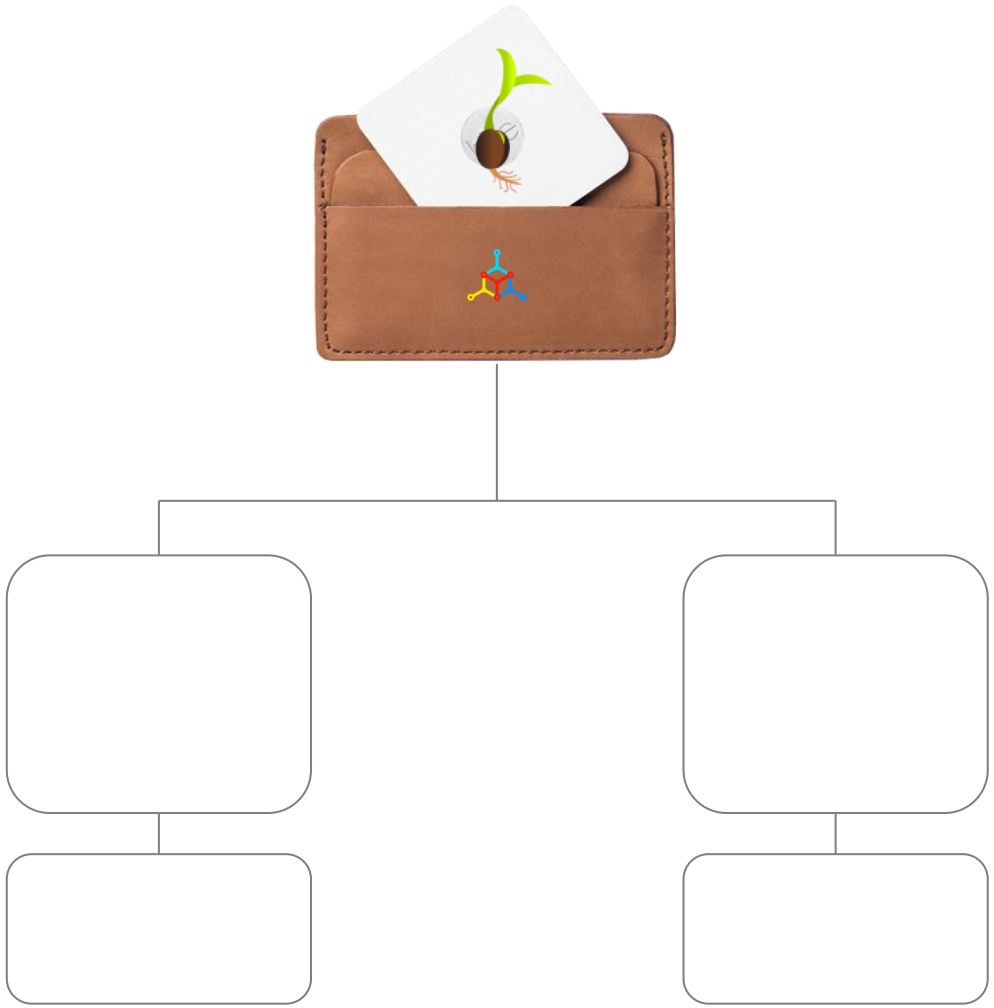

Seed
Master private key
XPRIV
Private Keys
Seed
Master private key
XPRIV
Private Keys

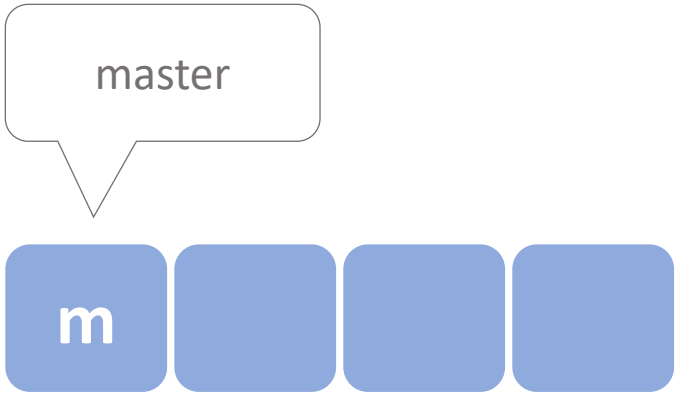
HD wallet(BIP39)

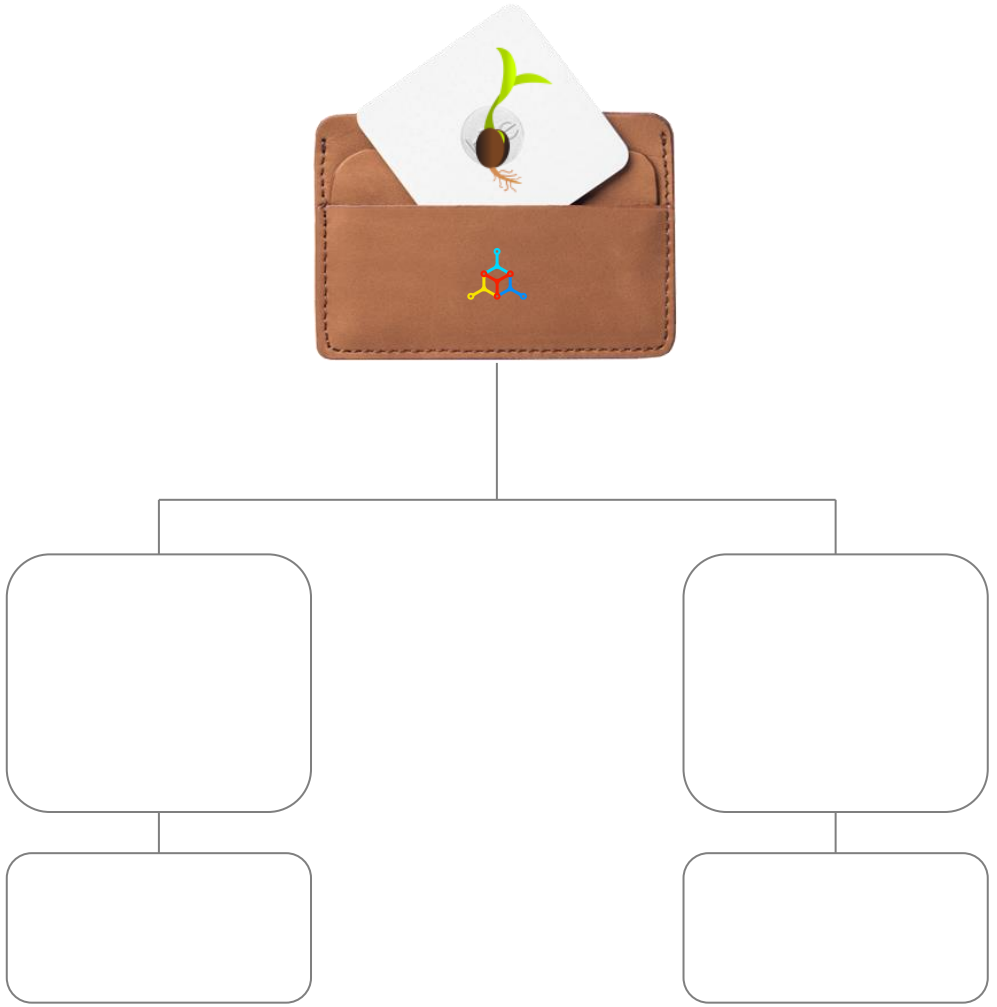
Seed words	
Random number	
Passphrase	
Derivation path	
Master private key	
XPRIV	
Private Keys	

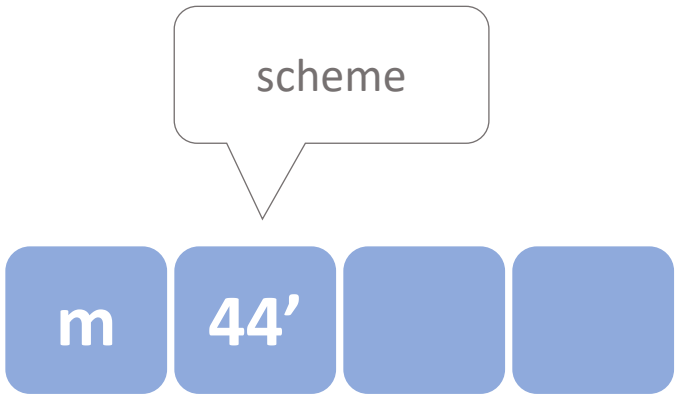
HD wallet(BIP39)

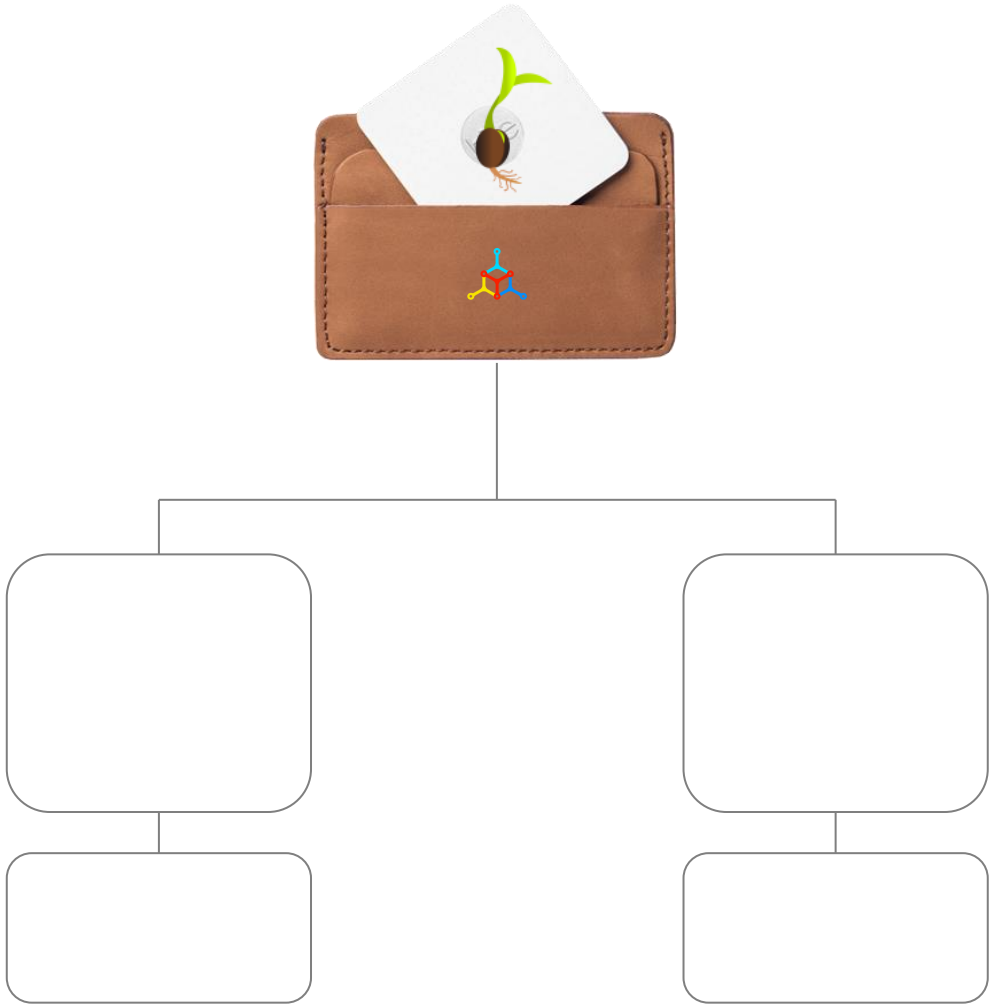
Seed words	
Random number	
Passphrase	
Derivation path	**m/44’/0’/0’**
Master private key	
XPRIV	
Private Keys	



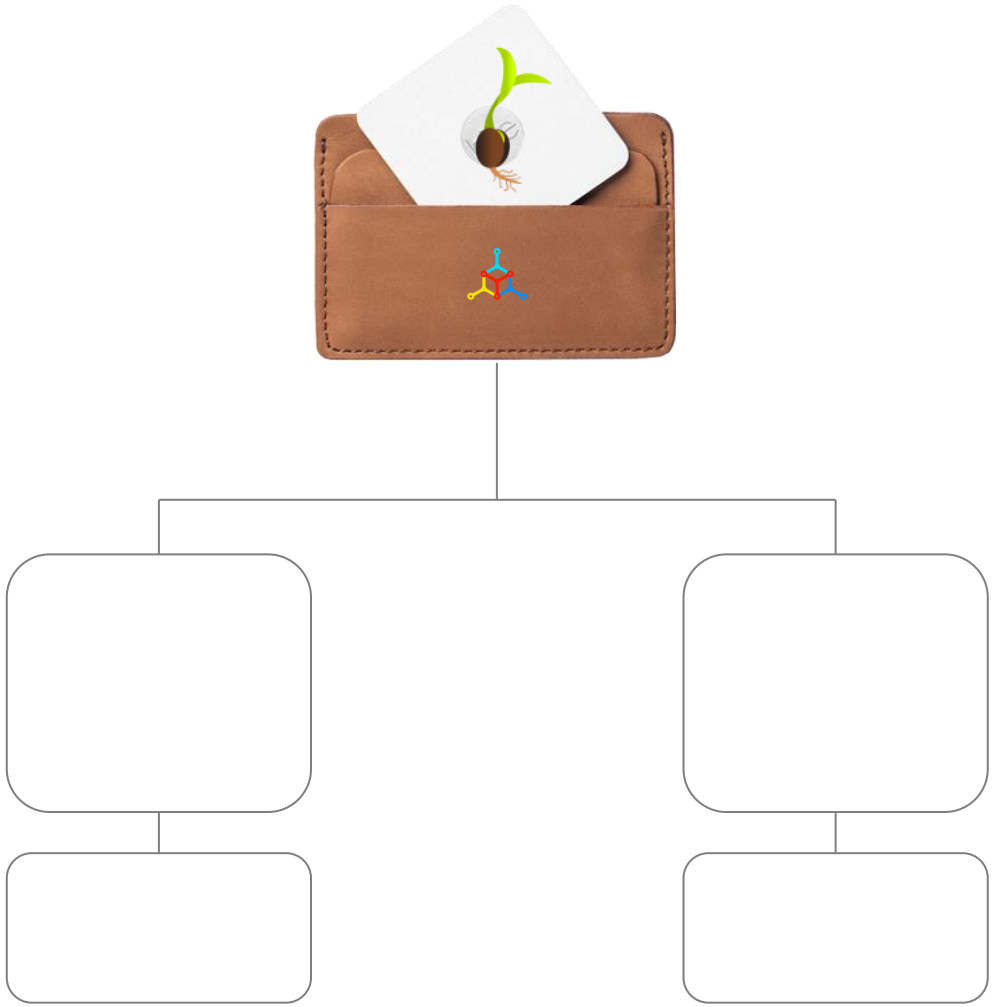

master
m

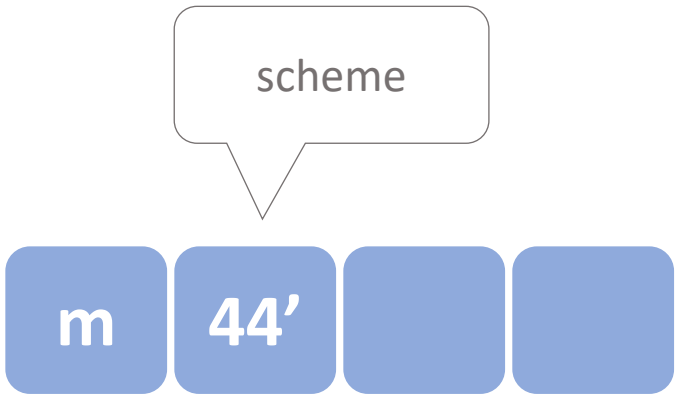


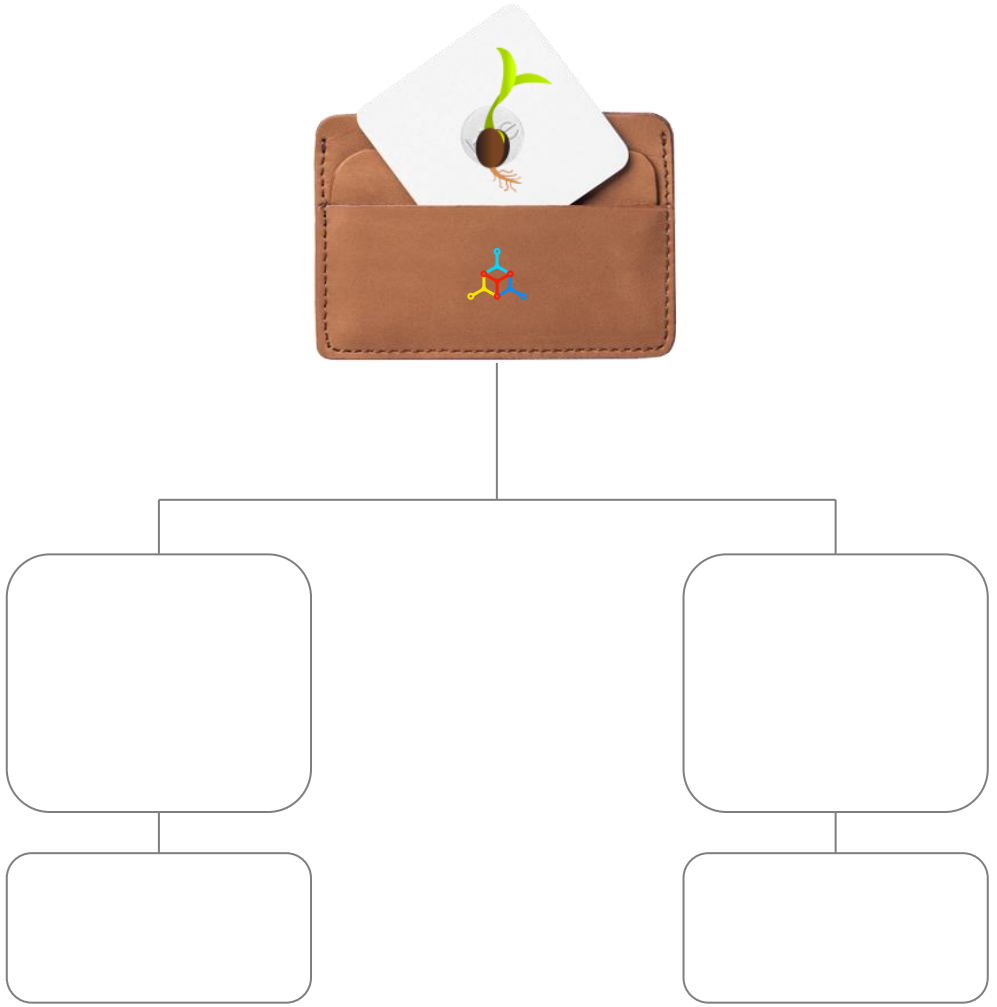

scheme
m
44’

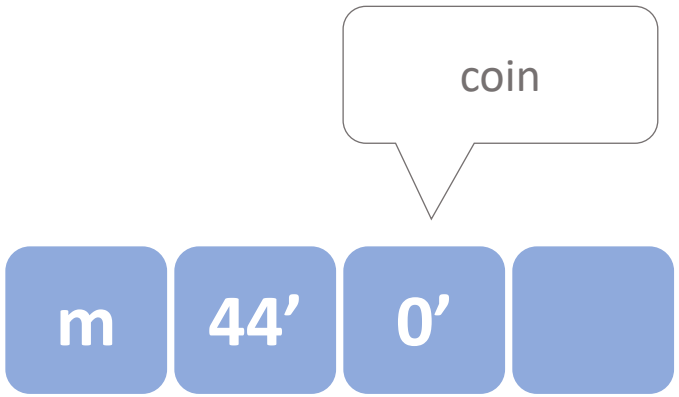


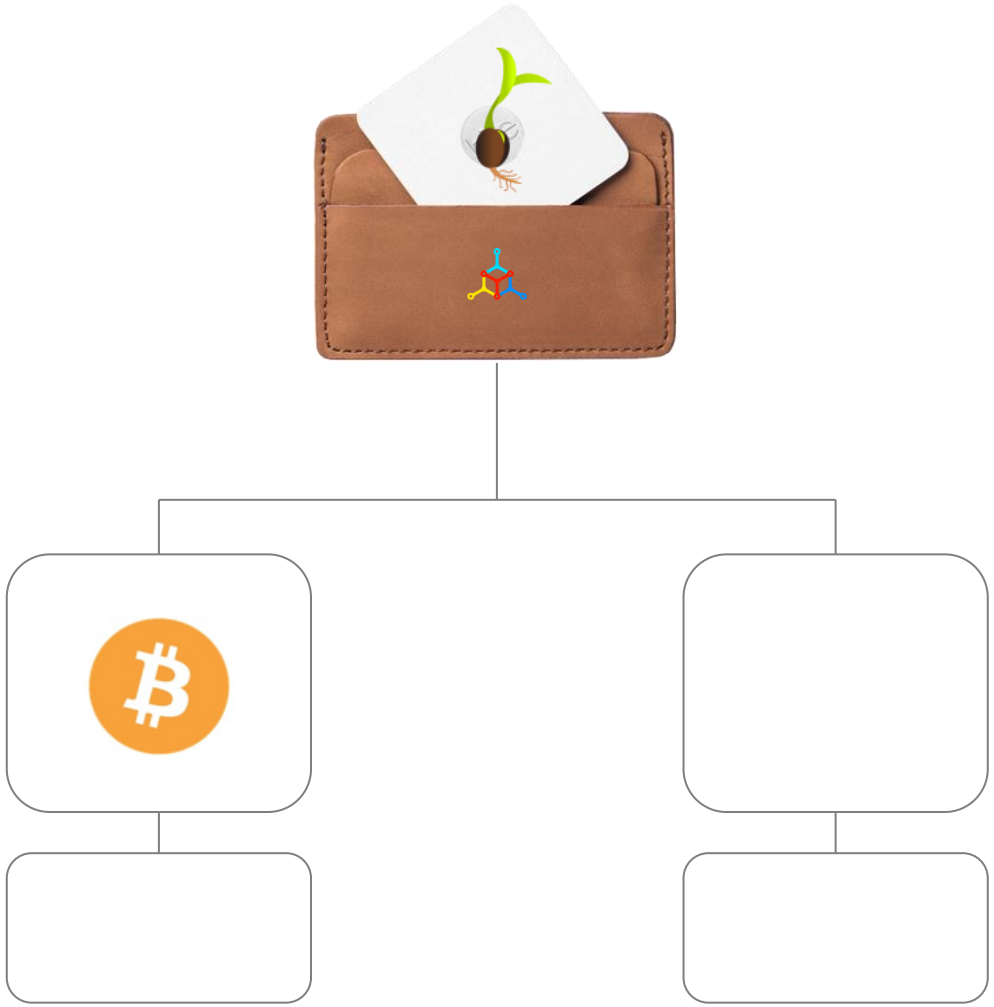
m	44’	legacy (1)
	49’	w-segwit (3)
	84’	n-segwit (bc1)
	86’	taproot (bc1p)

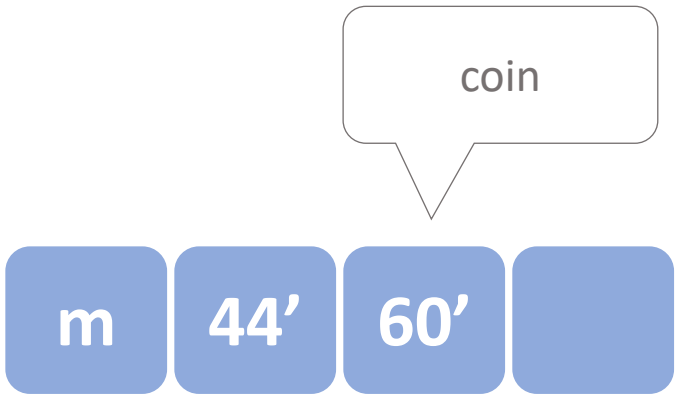


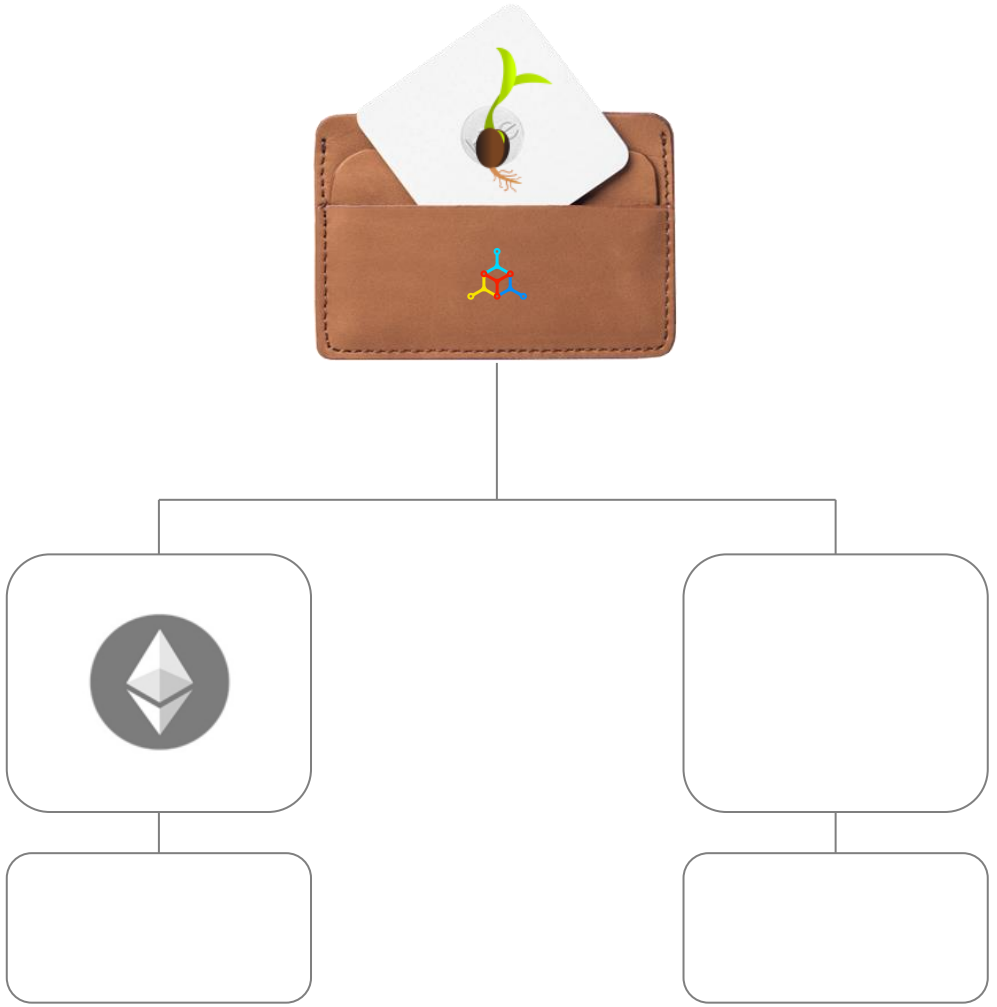

scheme
m
44’

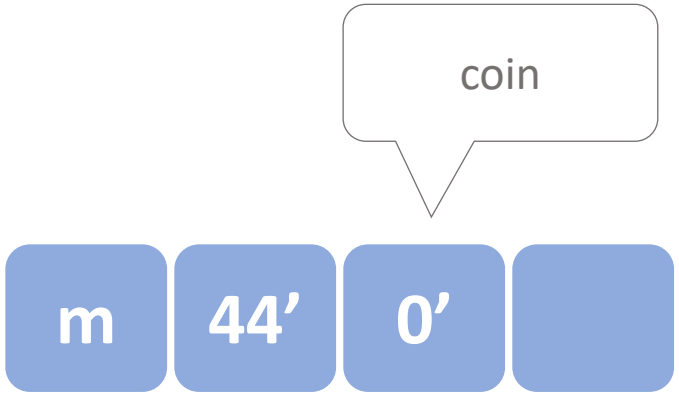



coin
m
44’
0’




coin
m
44’
60’





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

wallet number

m | 44’ | 0’ | 0’

Keystore

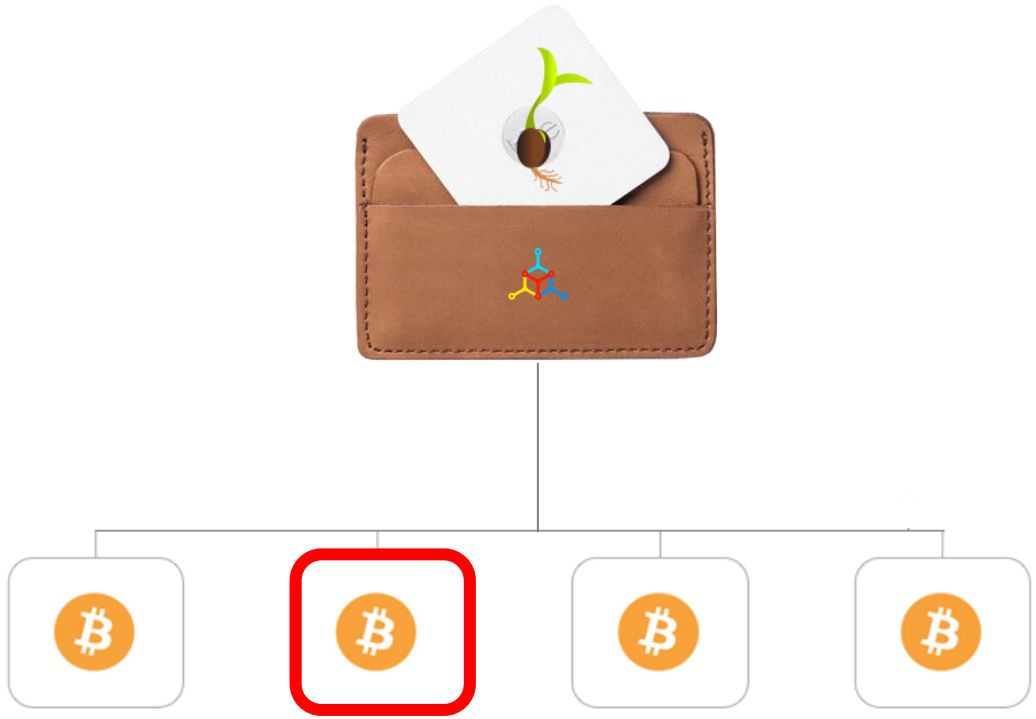
m | 44’ | 0’ | 0’

wallet number

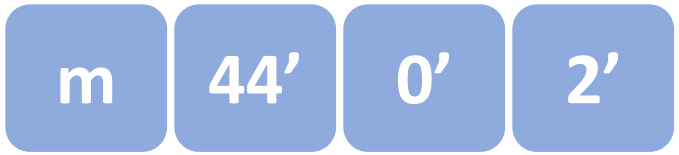
m | 44’ | 0’ | 0’

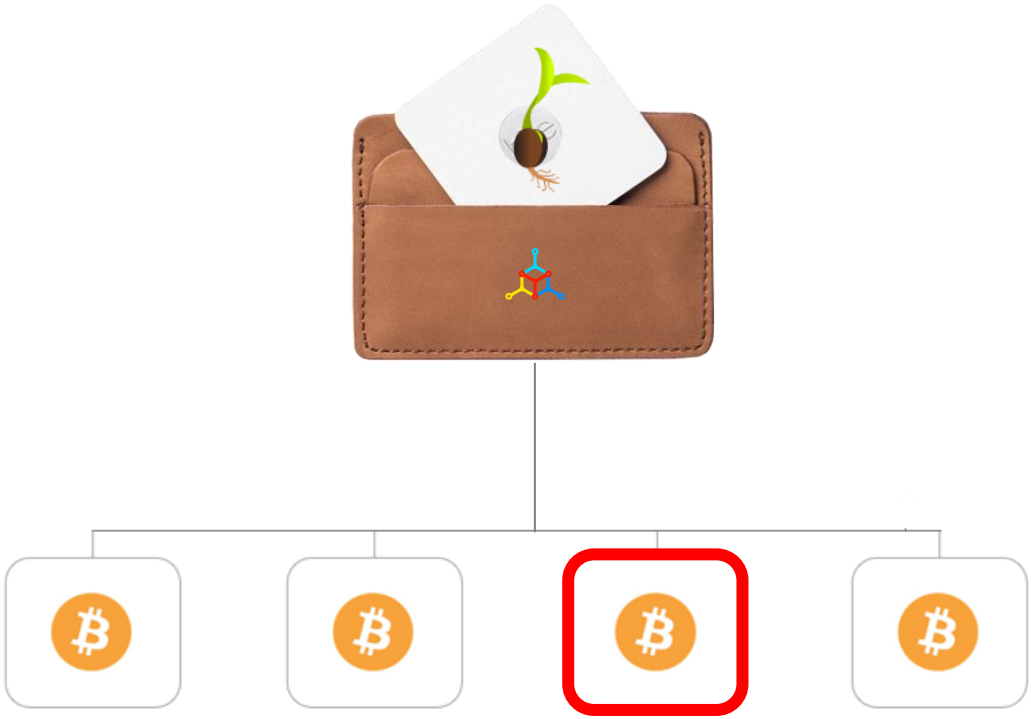
wallet number

m | 44’ | 0’ | 1’



wallet number



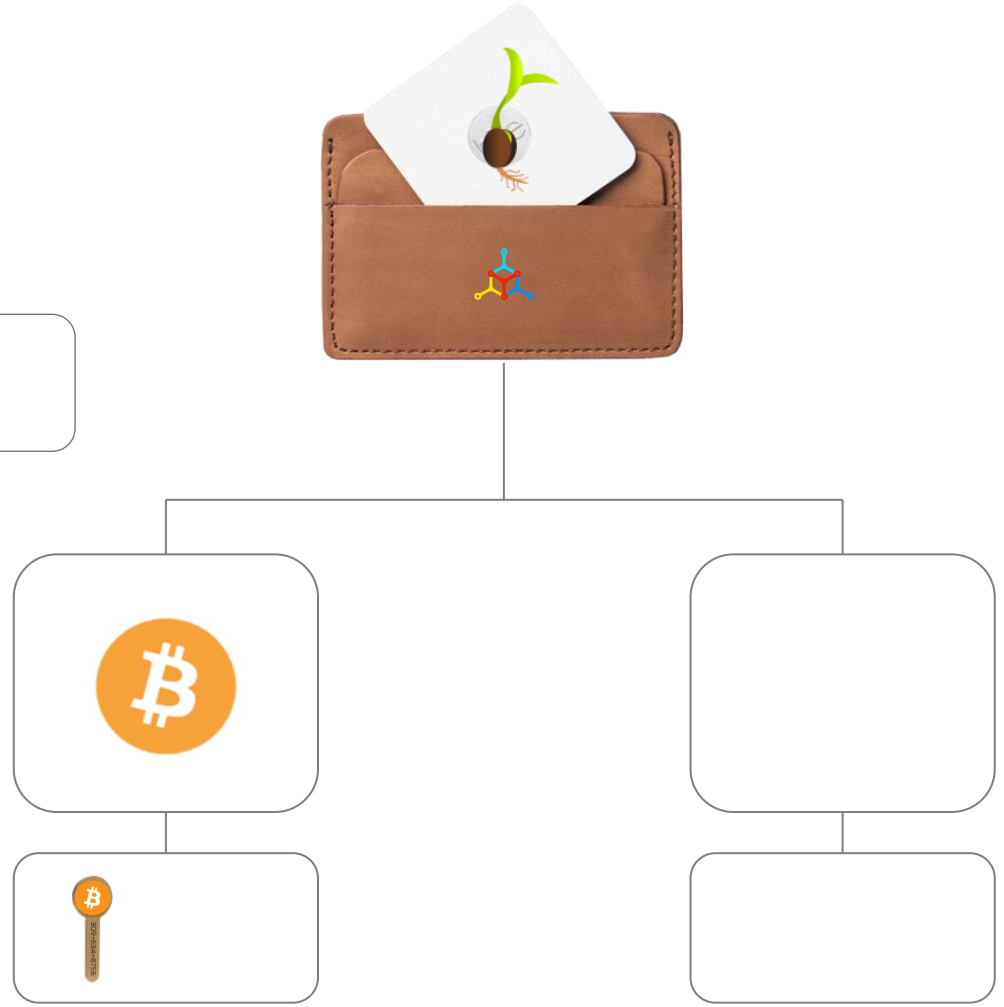


wallet number

m | 44’ | 0’ | 3’

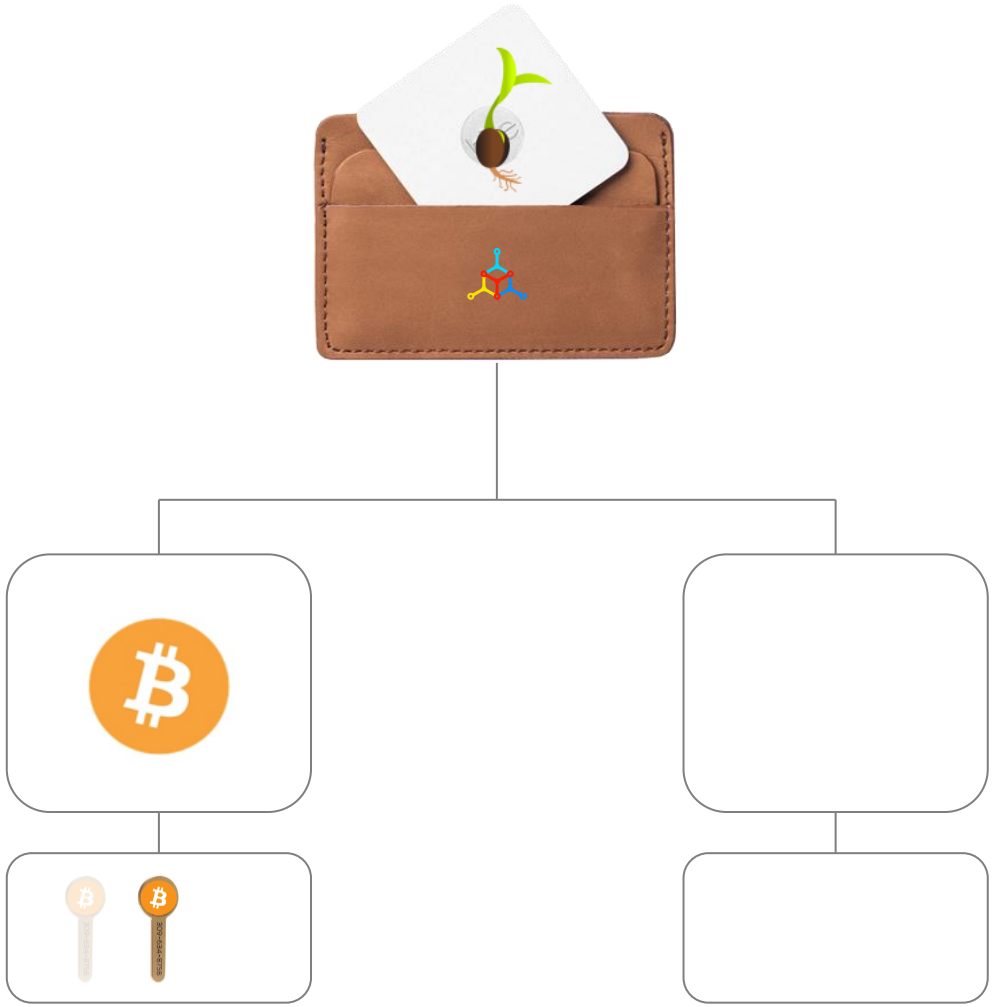
receive(0) or change(1)

m	44’	0’	0’	0



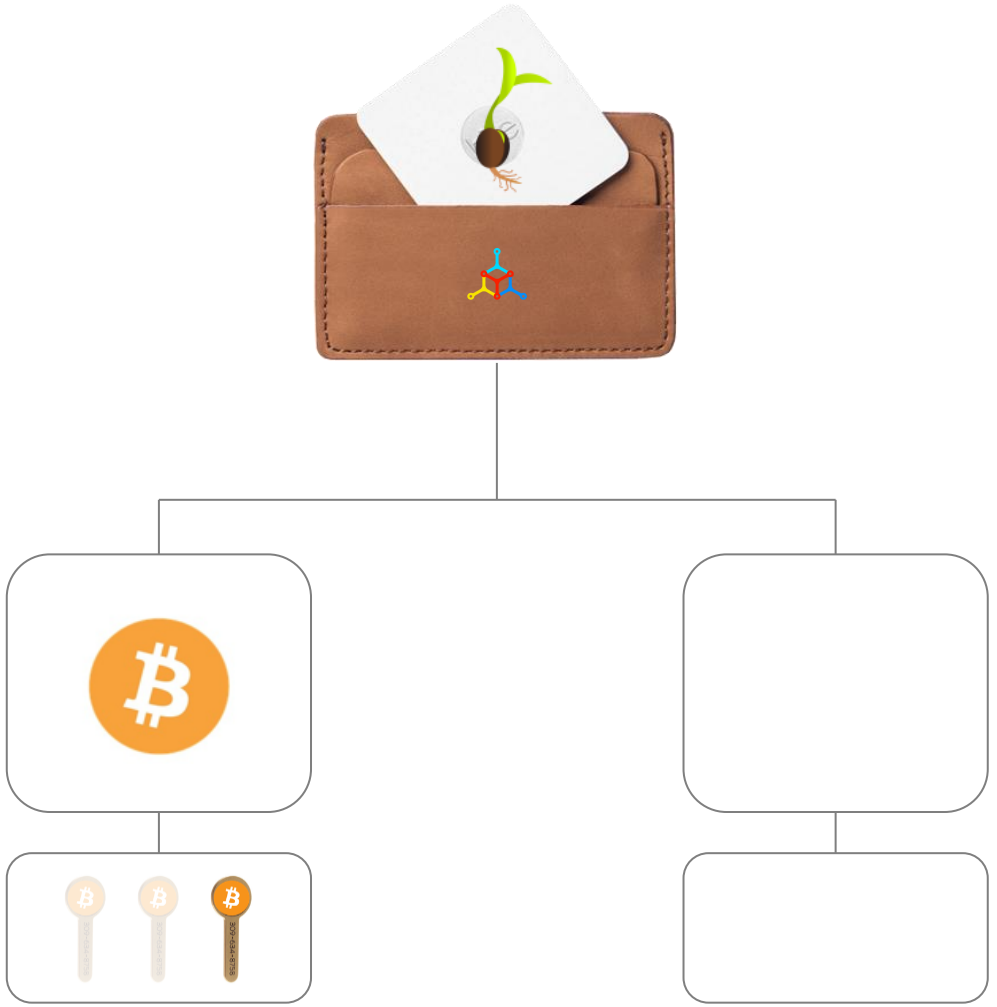
address

m	44’	0’	0’	0	1

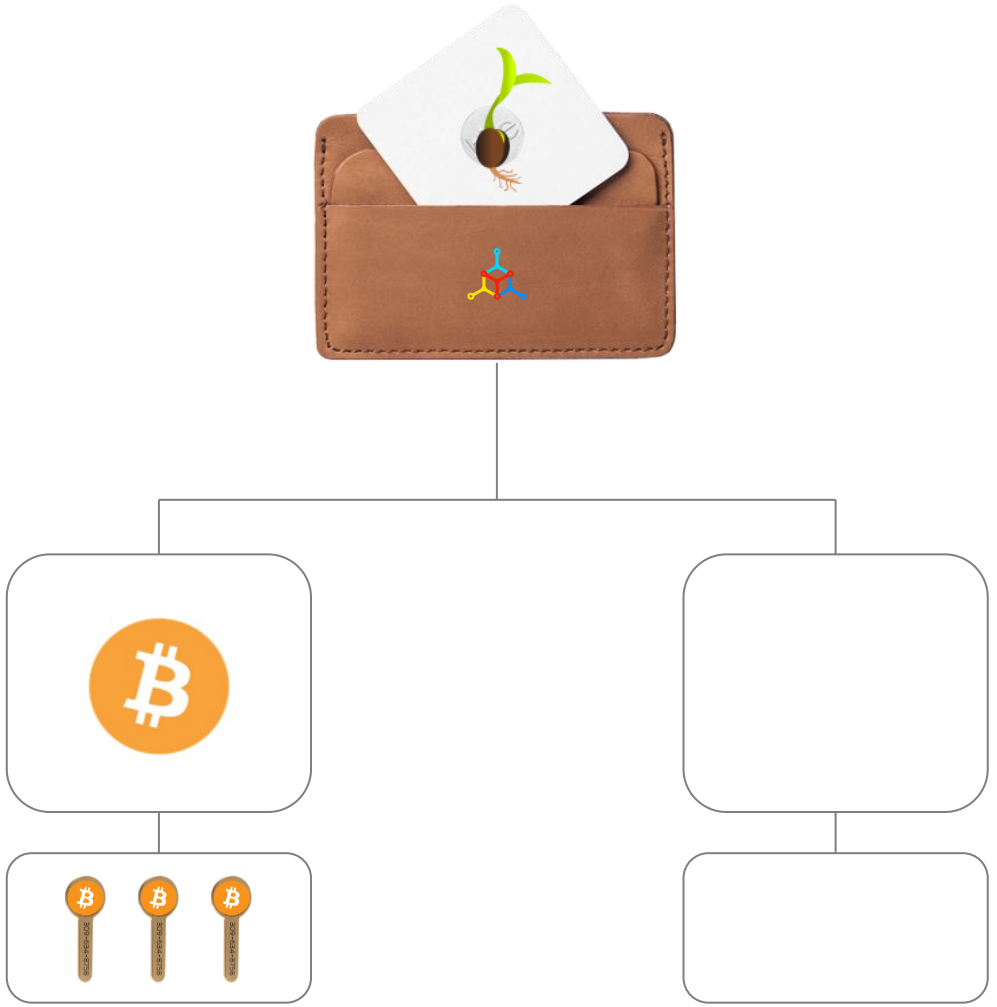


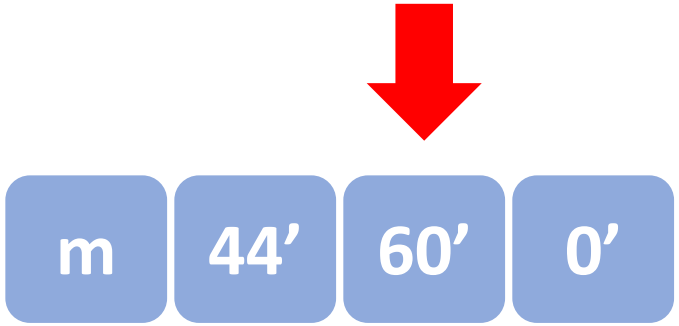
address

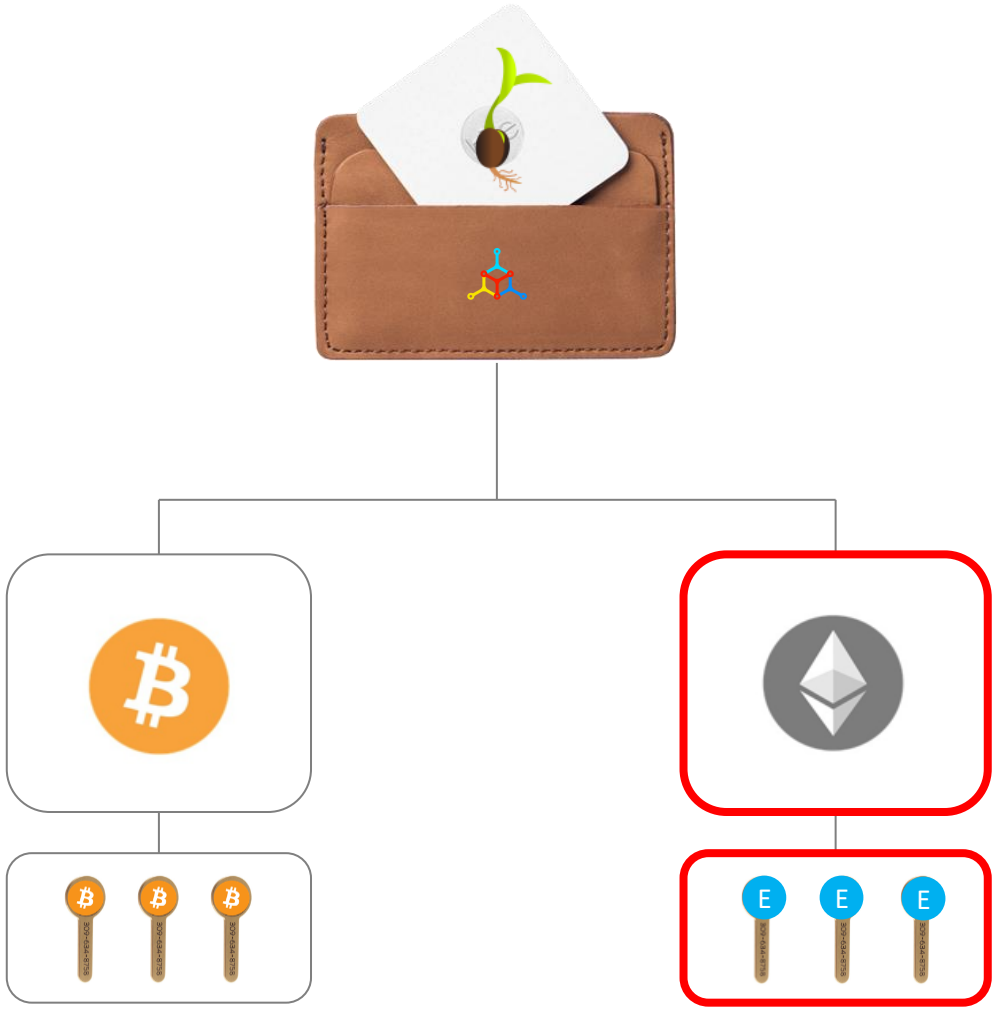
m	44’	0’	0’	0	2

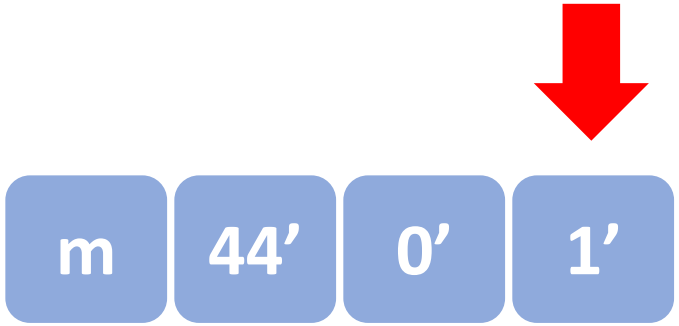


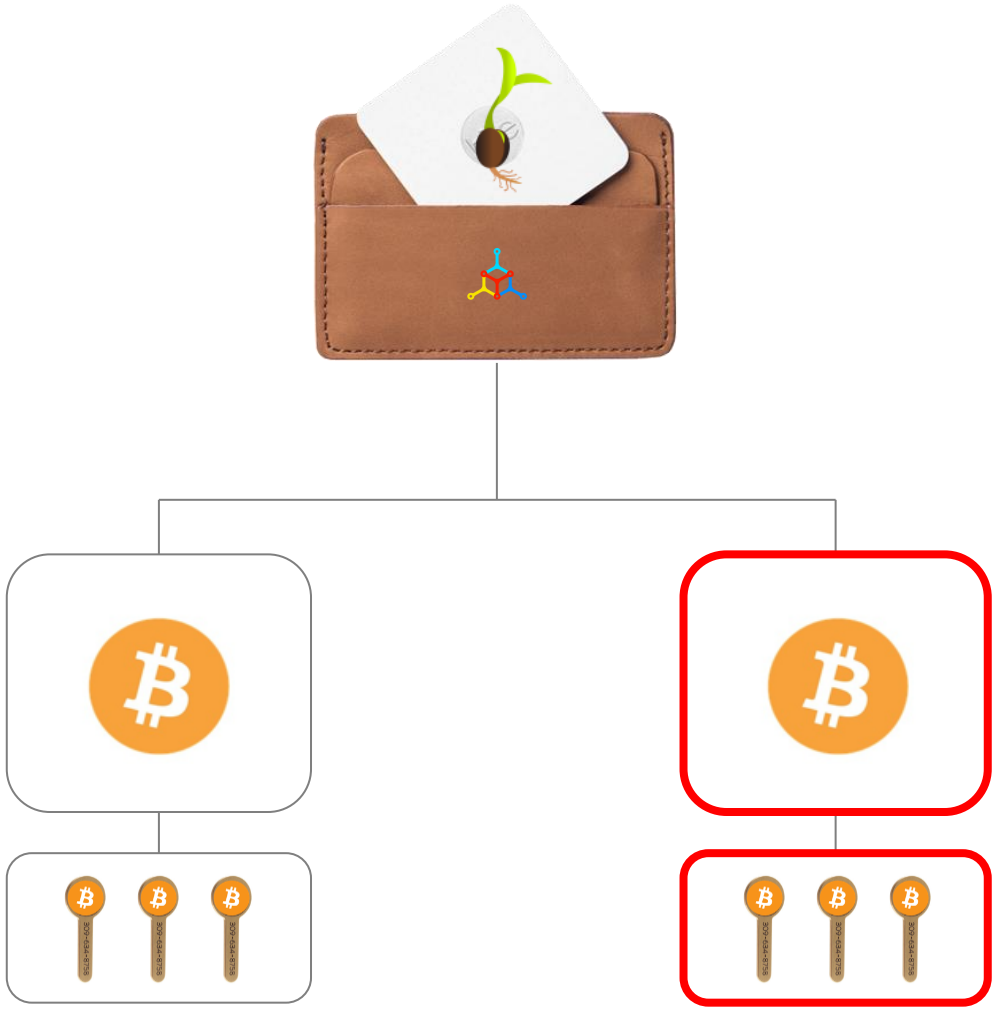
m	44’	0’	0’



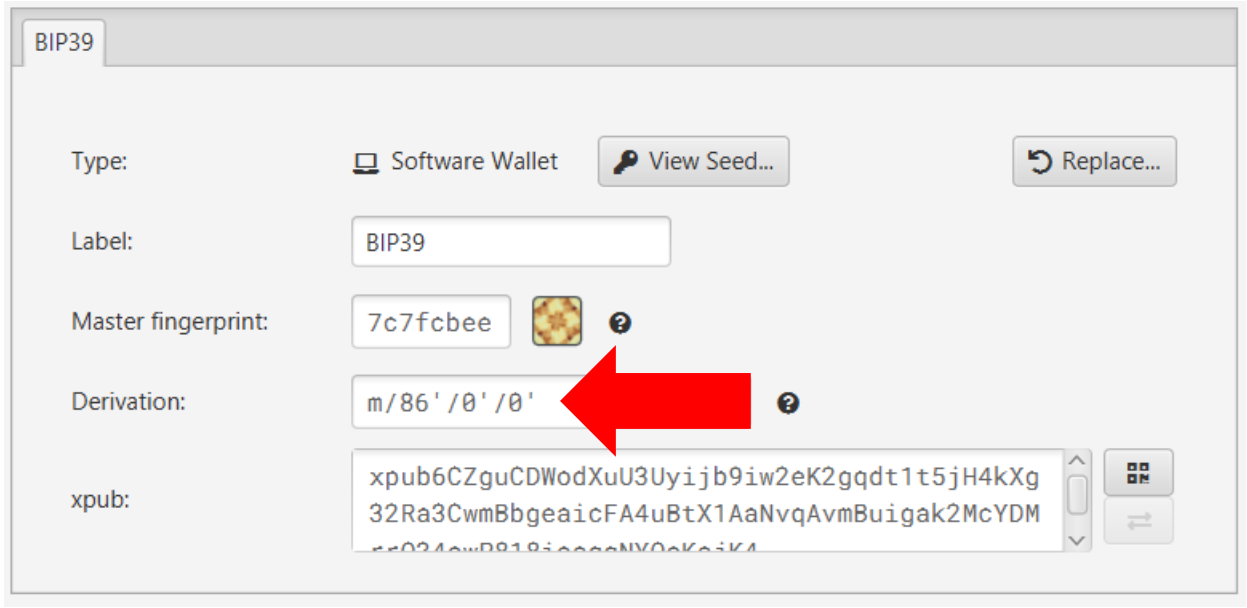

m
44’
60’
0’



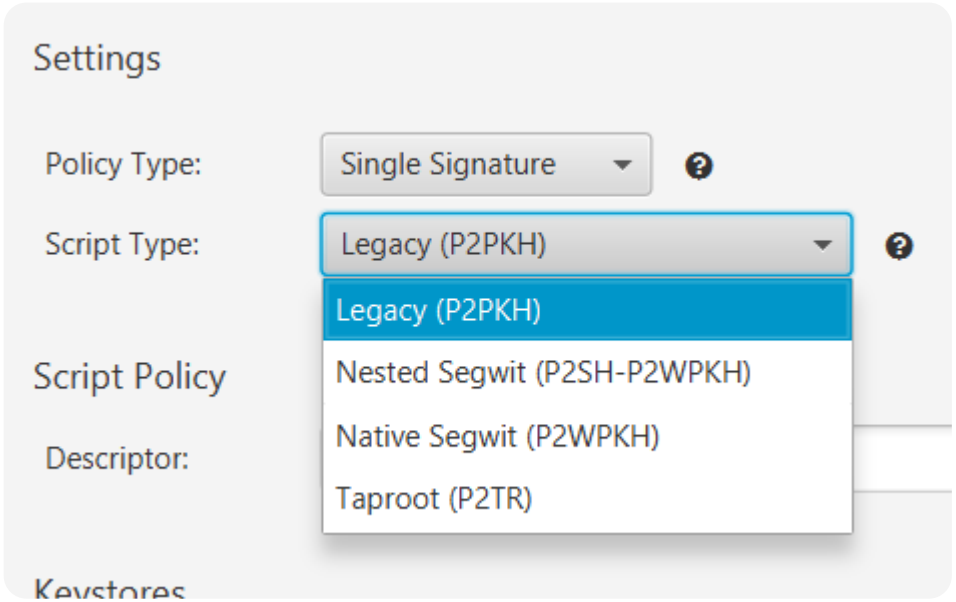

m
44’
0’
1’

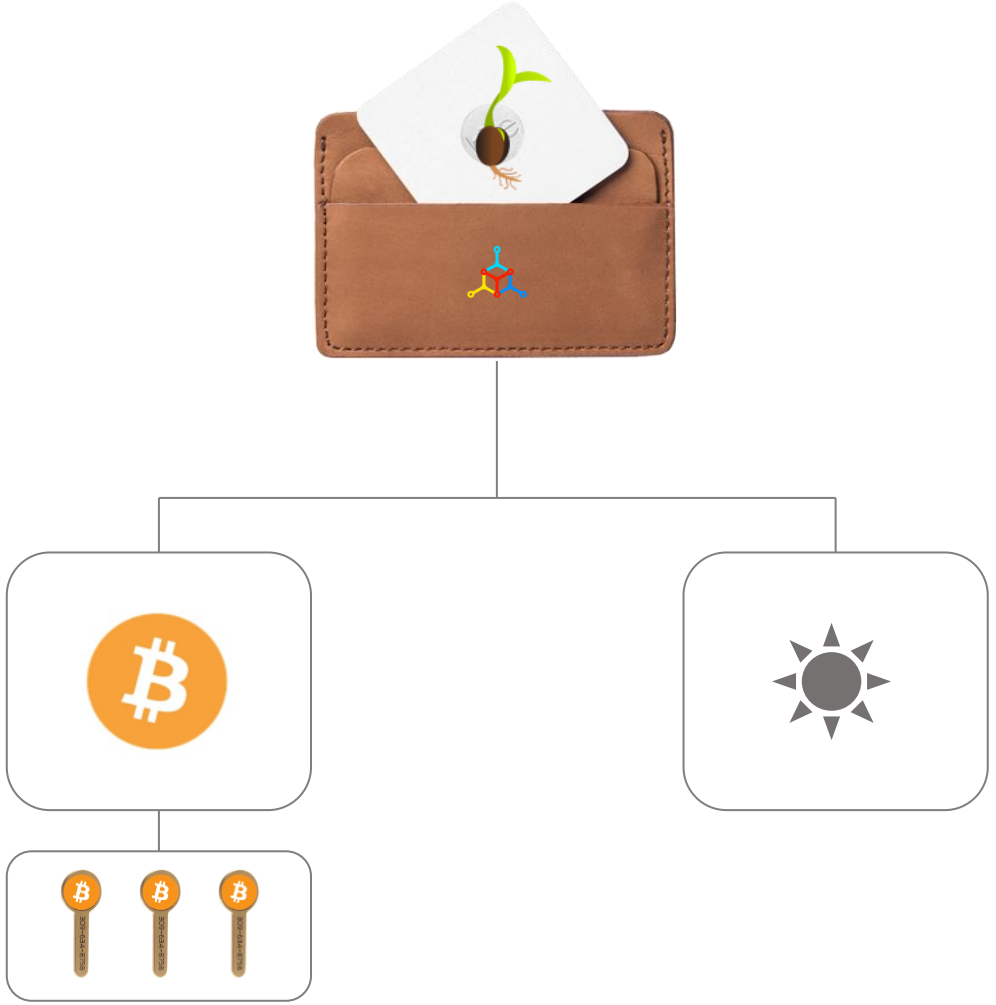


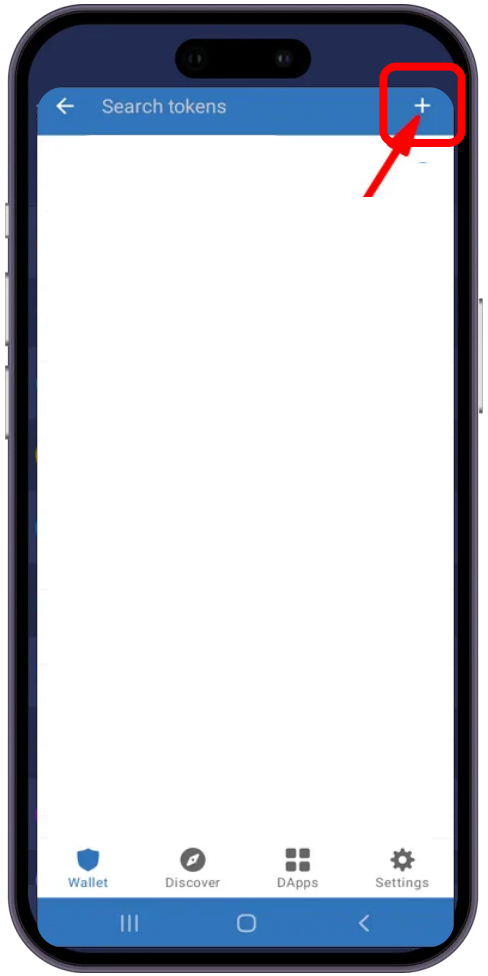
m | 86’ | 0’ | 0’

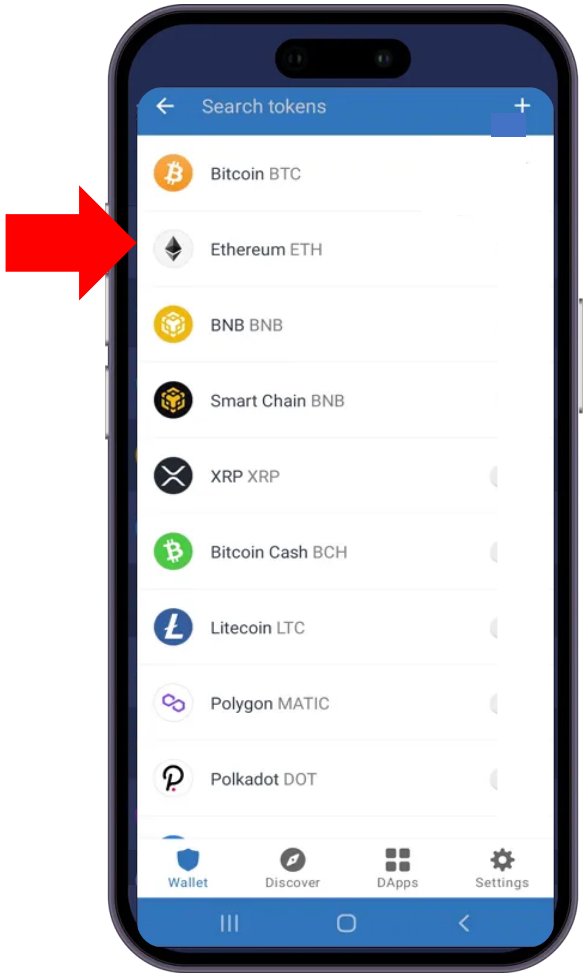

BIP39
Type:
Software Wallet
View Seed...
Replace...
Label:
BIP39
Master fingerprint:
7c7fcbee
Derivation:
m/86'/0'/0'
xpub:
xpub6CZguCDWodXuU3Uyijb9iw2eK2gqdt1t5jH4kXg
32Ra3CwmBbgeaicFA4uBtX1AaNvqAvmBuigak2McYDM

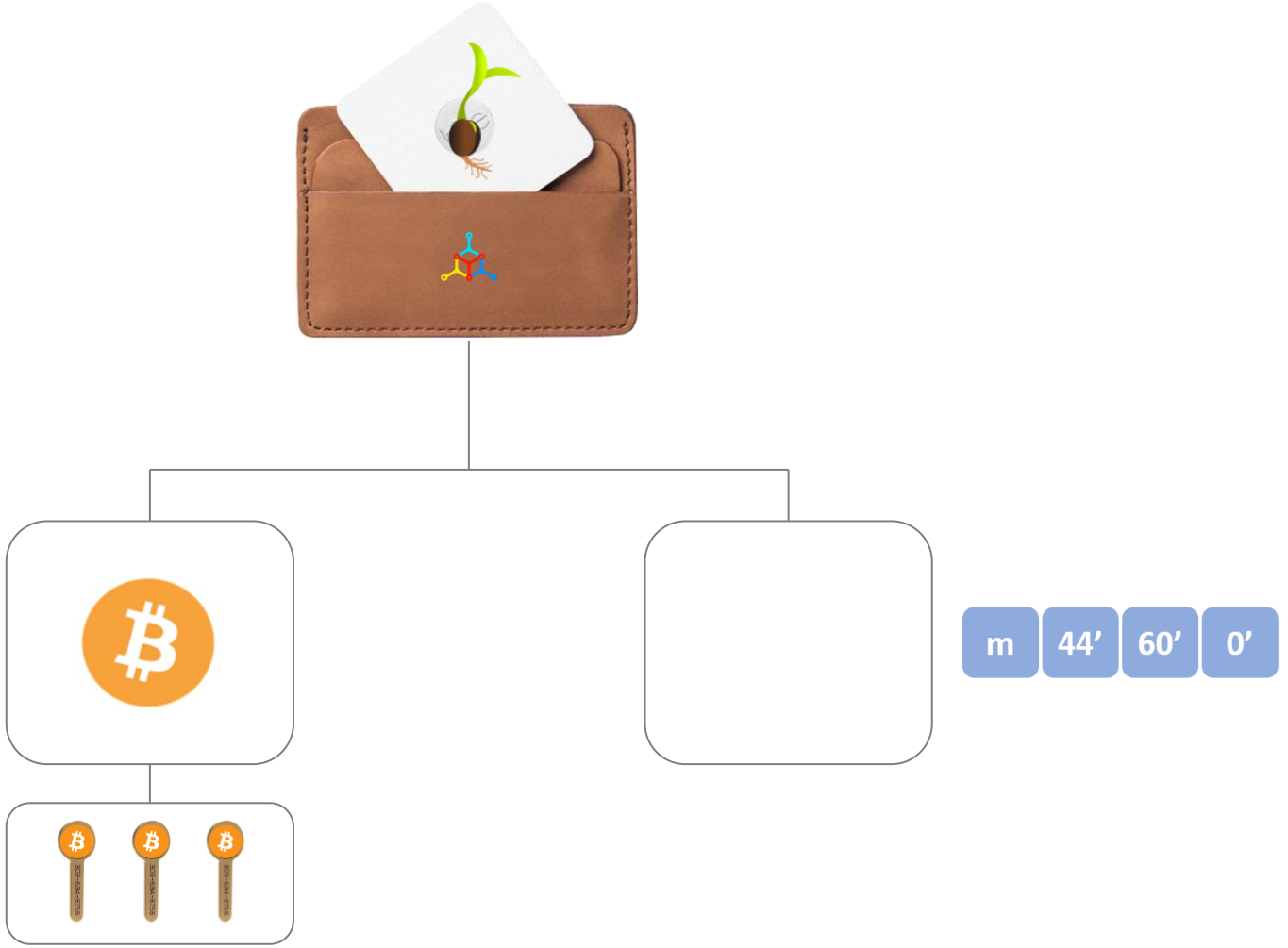
m | 44’ | 0’ | 0’

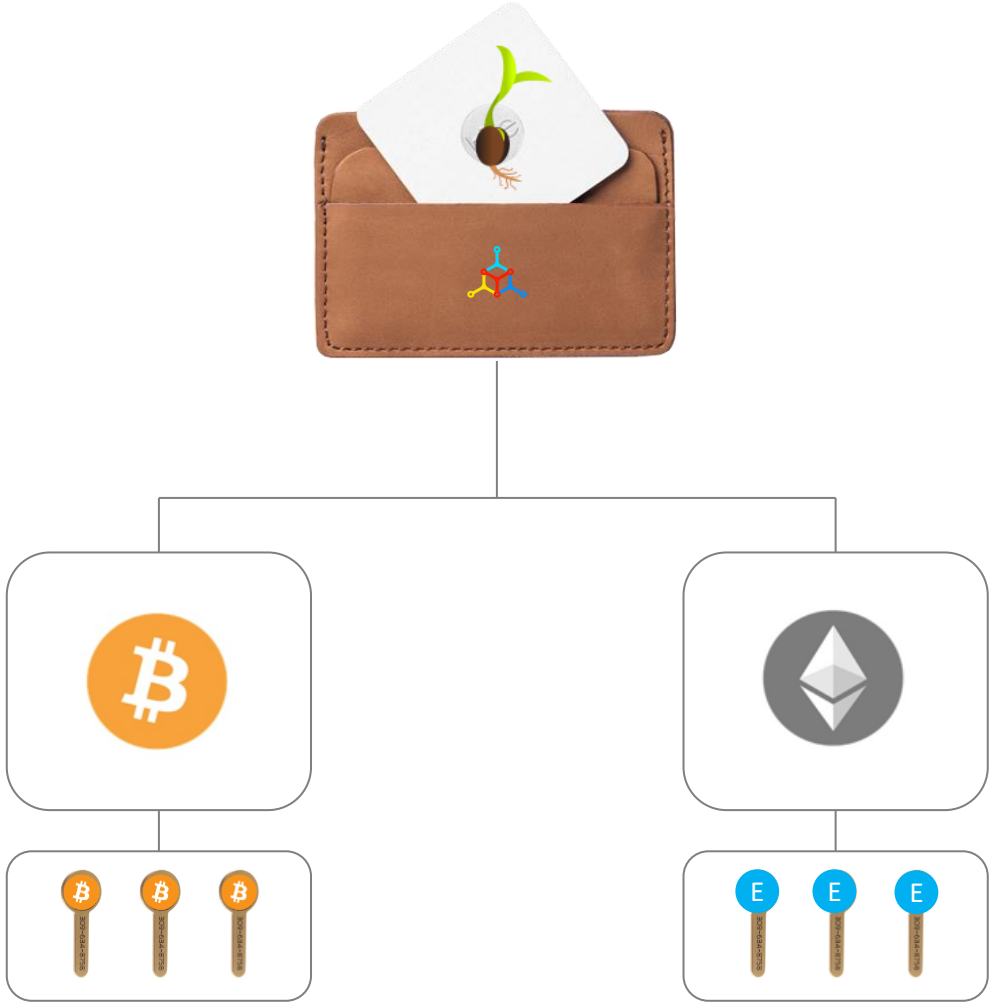

Settings
Policy Type:
Single Signature
Script Type:
Legacy (P2PKH)
Legacy (P2PKH)
Nested Segwit (P2SH-P2WPKH)
Native Segwit (P2WPKH)
Taproot (P2TR)
Script Policy
Descriptor:
Keystores

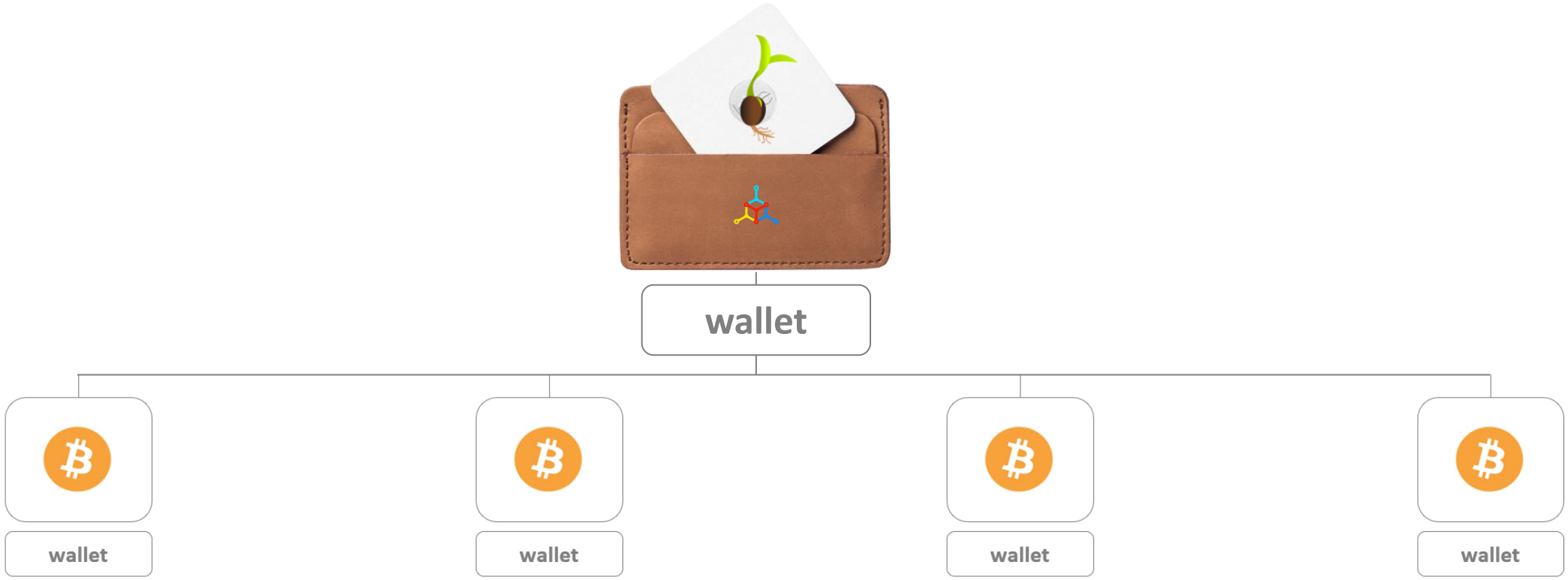


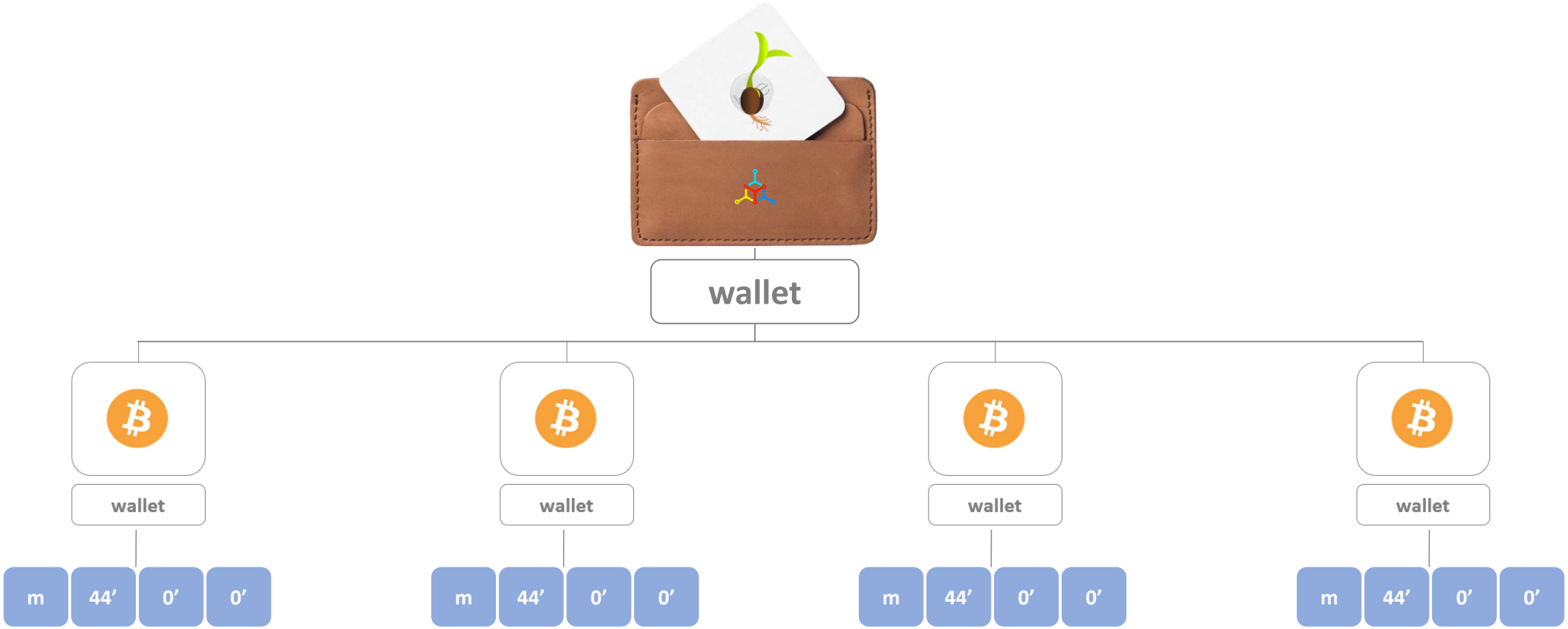

Search tokens
+
Wallet
Discover
DApps
Settings

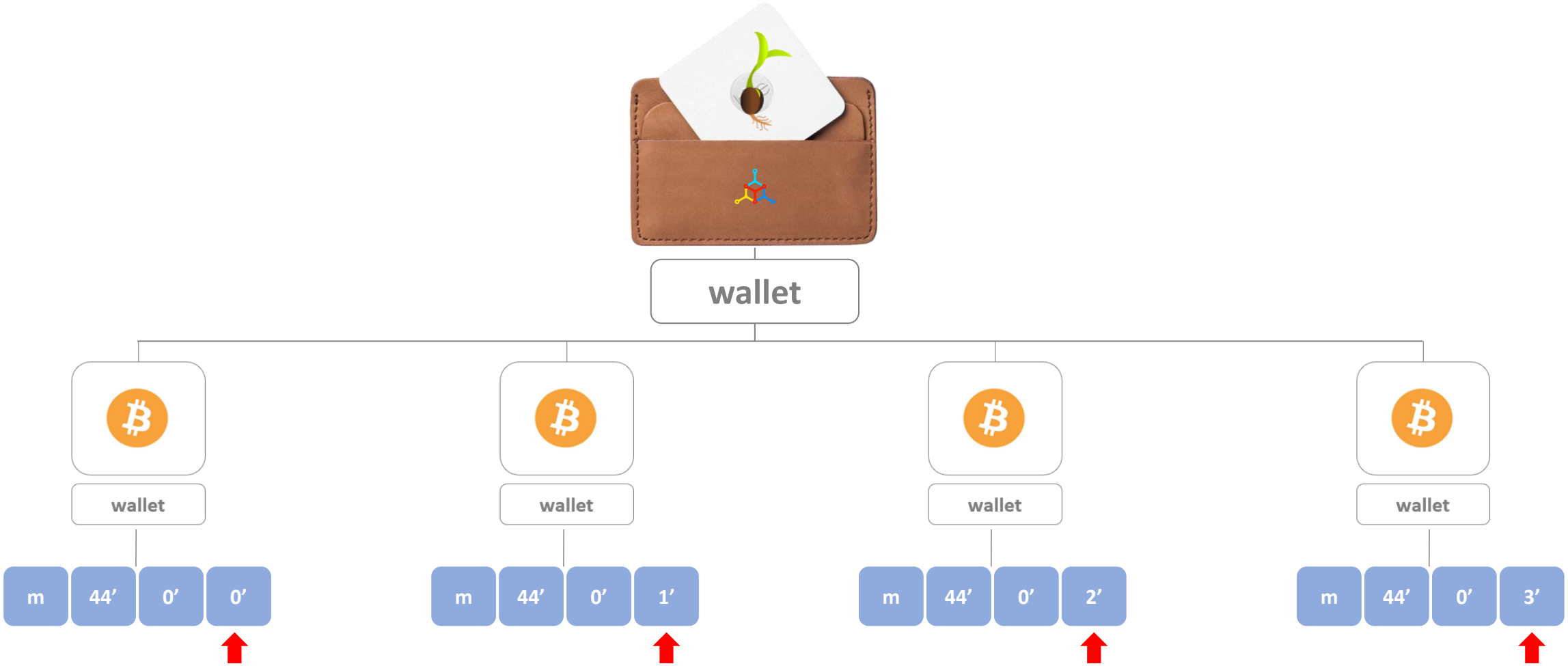

Search tokens
Bitcoin BTC
Ethereum ETH
BNB BNB
Smart Chain BNB
XRP XRP
Bitcoin Cash BCH
Litecoin LTC
Polygon MATIC
Polkadot DOT
Wallet
Discover
DApps
Settings

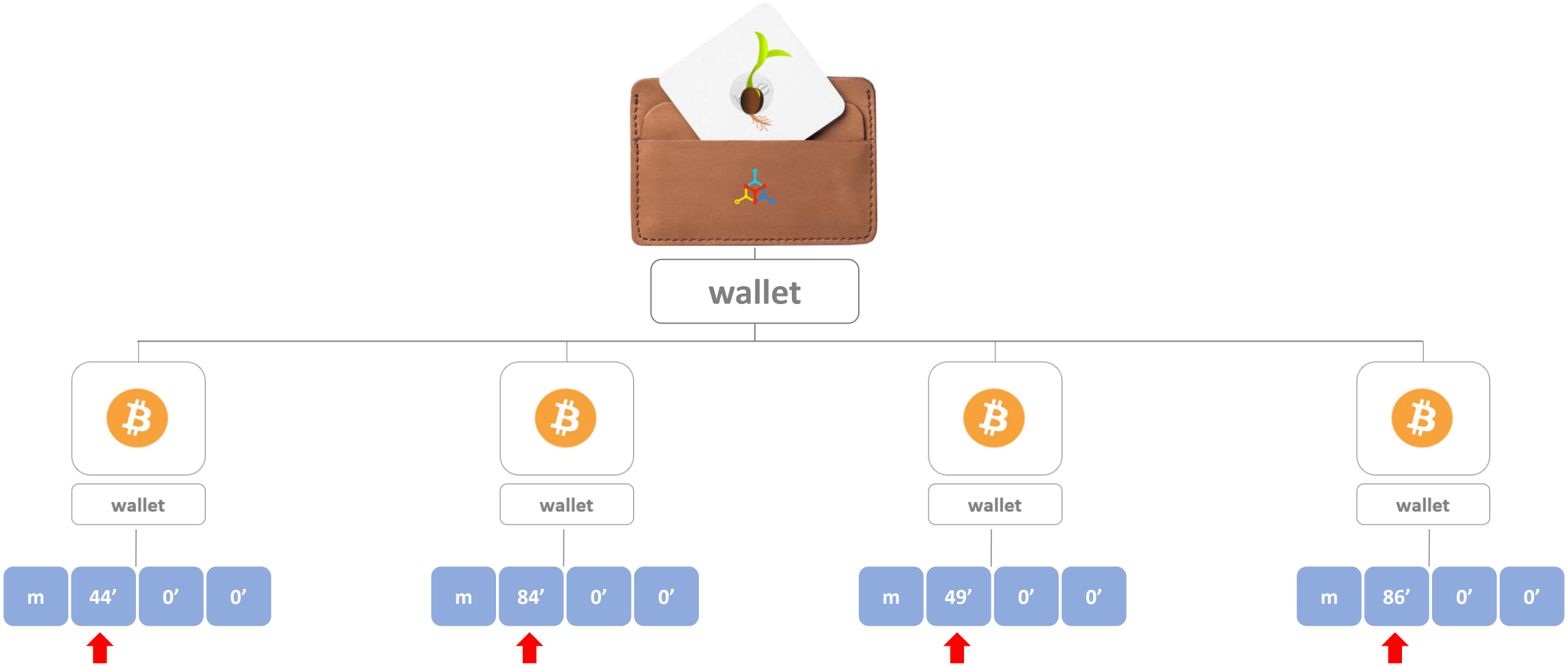

m
44’
60’
0’

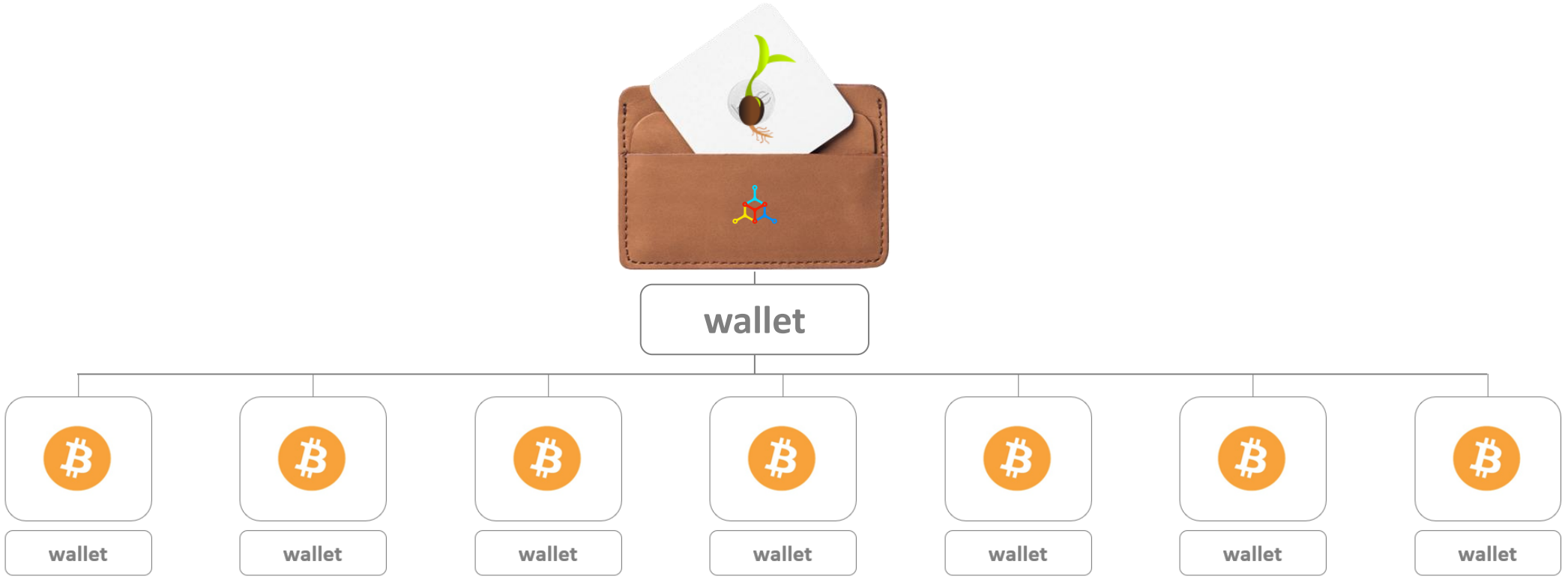


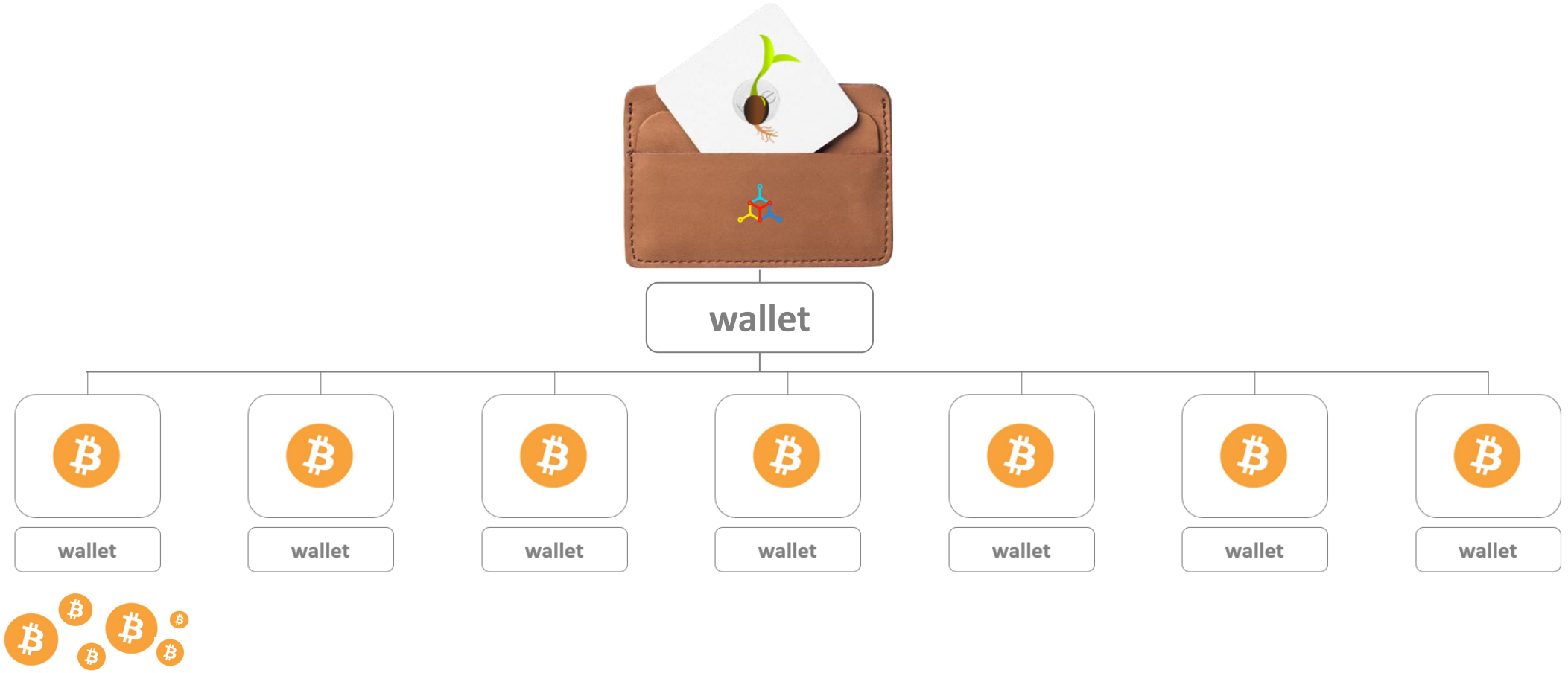

wallet
wallet
wallet
wallet
wallet

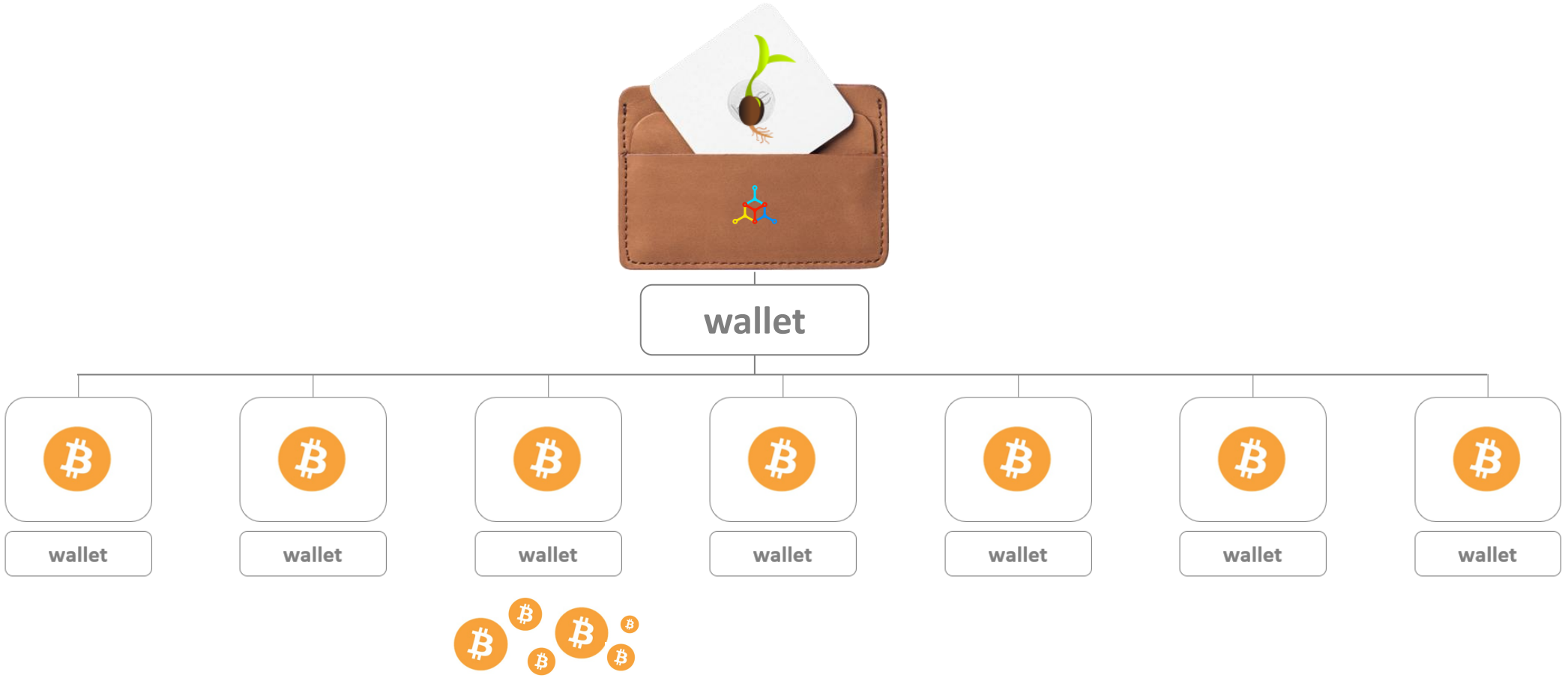

wallet
wallet
wallet
wallet
wallet
m
44’
0’
0’
m
44’
0’
0’
m
44’
0’
0’
m
44’
0’
0’

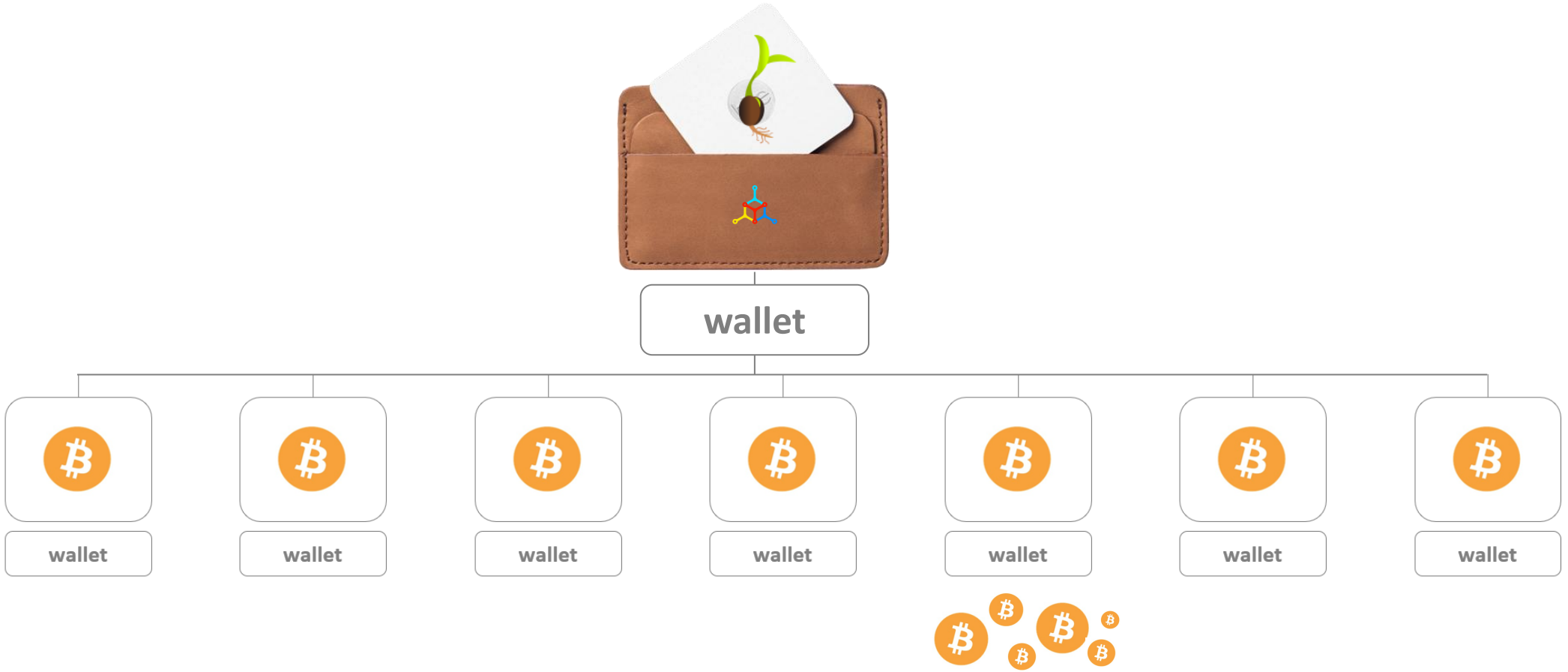

wallet
wallet
wallet
wallet
wallet
m
44’
0’
0’
m
44’
0’
1’
m
44’
0’
2’
m
44’
0’
3’


wallet
wallet
wallet
wallet
wallet
m
44’
0’
0’
m
84’
0’
0’
m
49’
0’
0’
m
86’
0’
0’


wallet
wallet
wallet
wallet
wallet
wallet
wallet
wallet

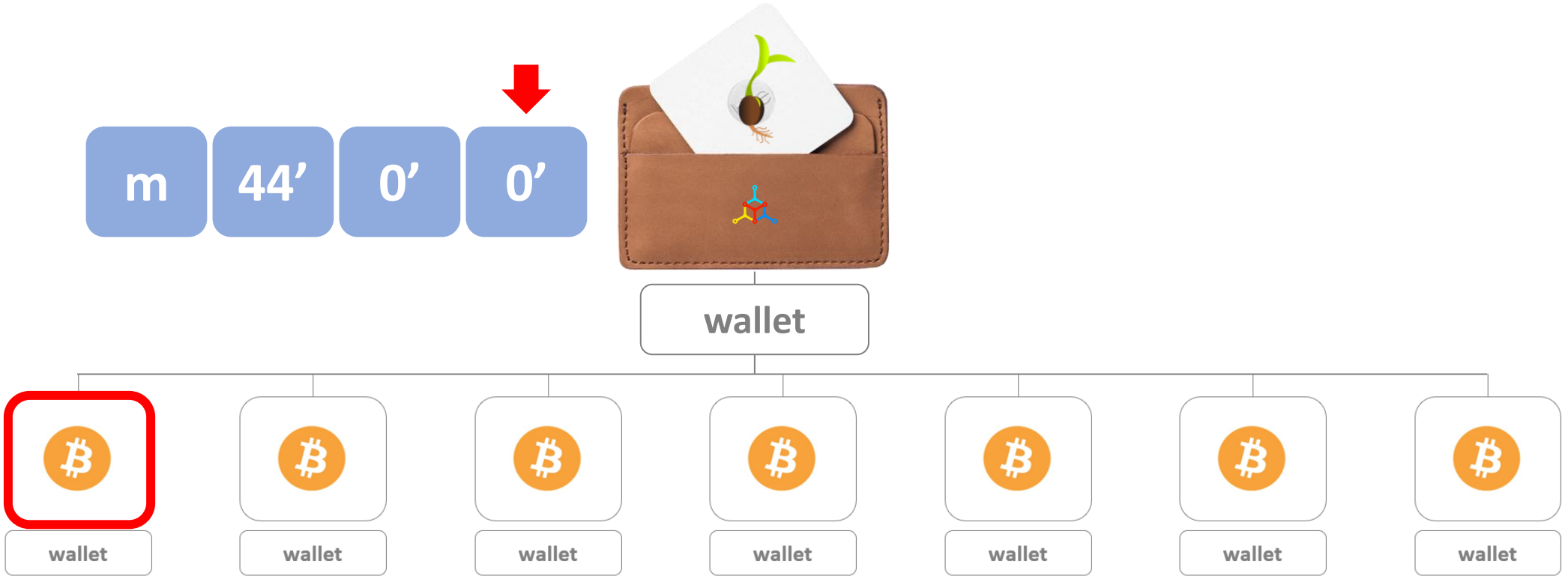

wallet
wallet
wallet
wallet
wallet
wallet
wallet
wallet

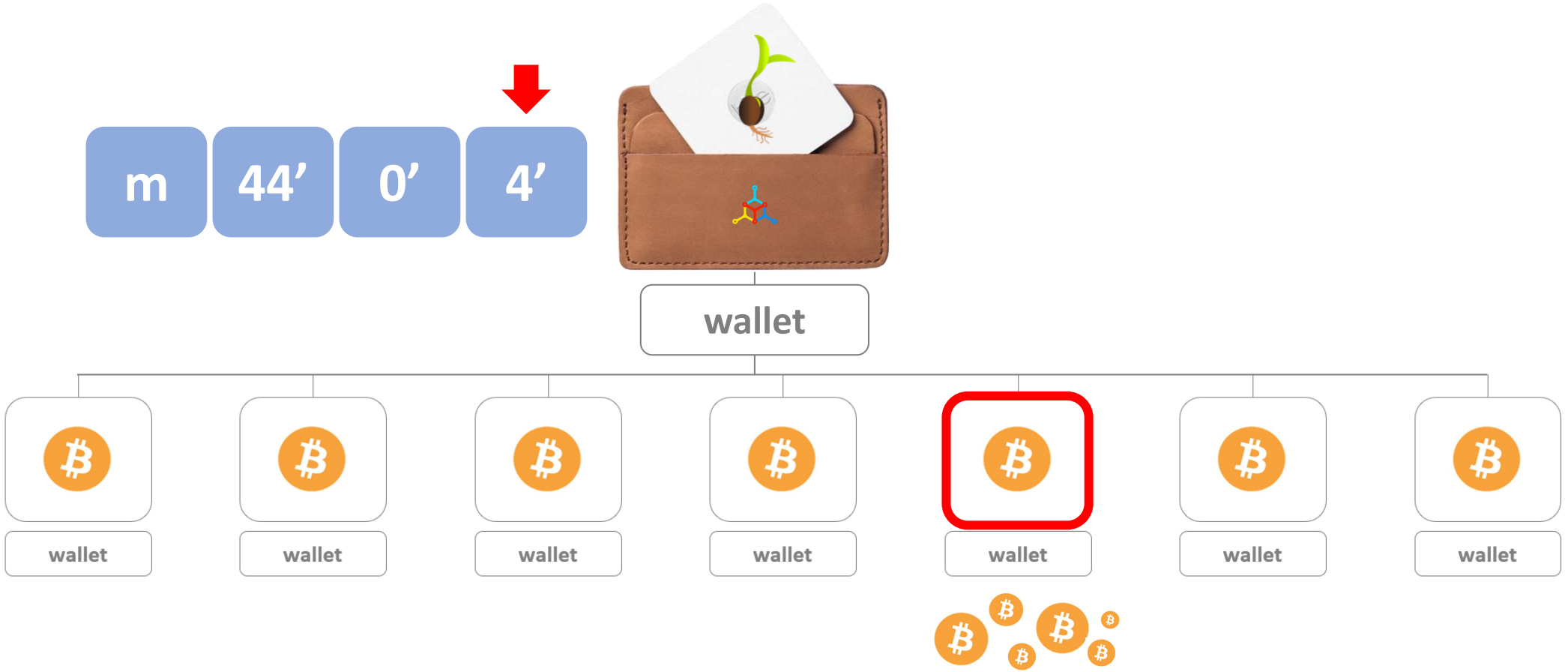

wallet
wallet
wallet
wallet
wallet
wallet
wallet
wallet

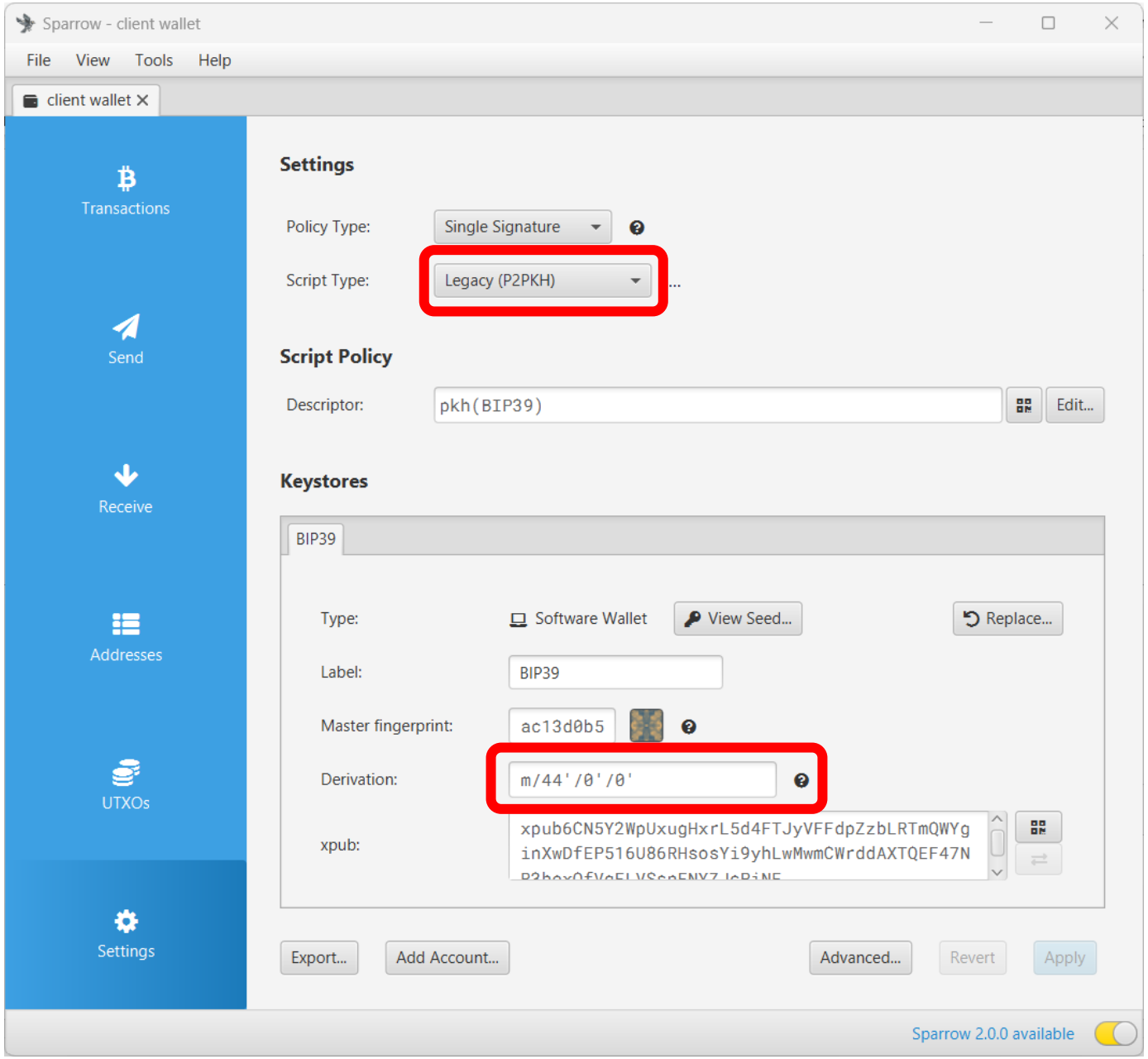

wallet
wallet
wallet
wallet
wallet
wallet
wallet
wallet

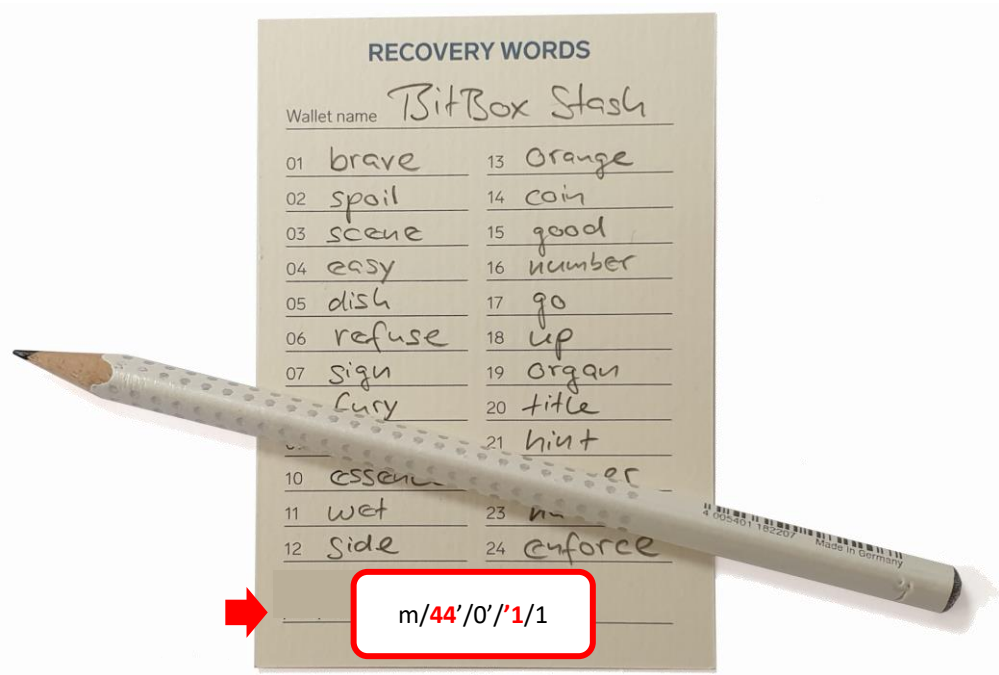

wallet
wallet
wallet
wallet
wallet
wallet
wallet
wallet

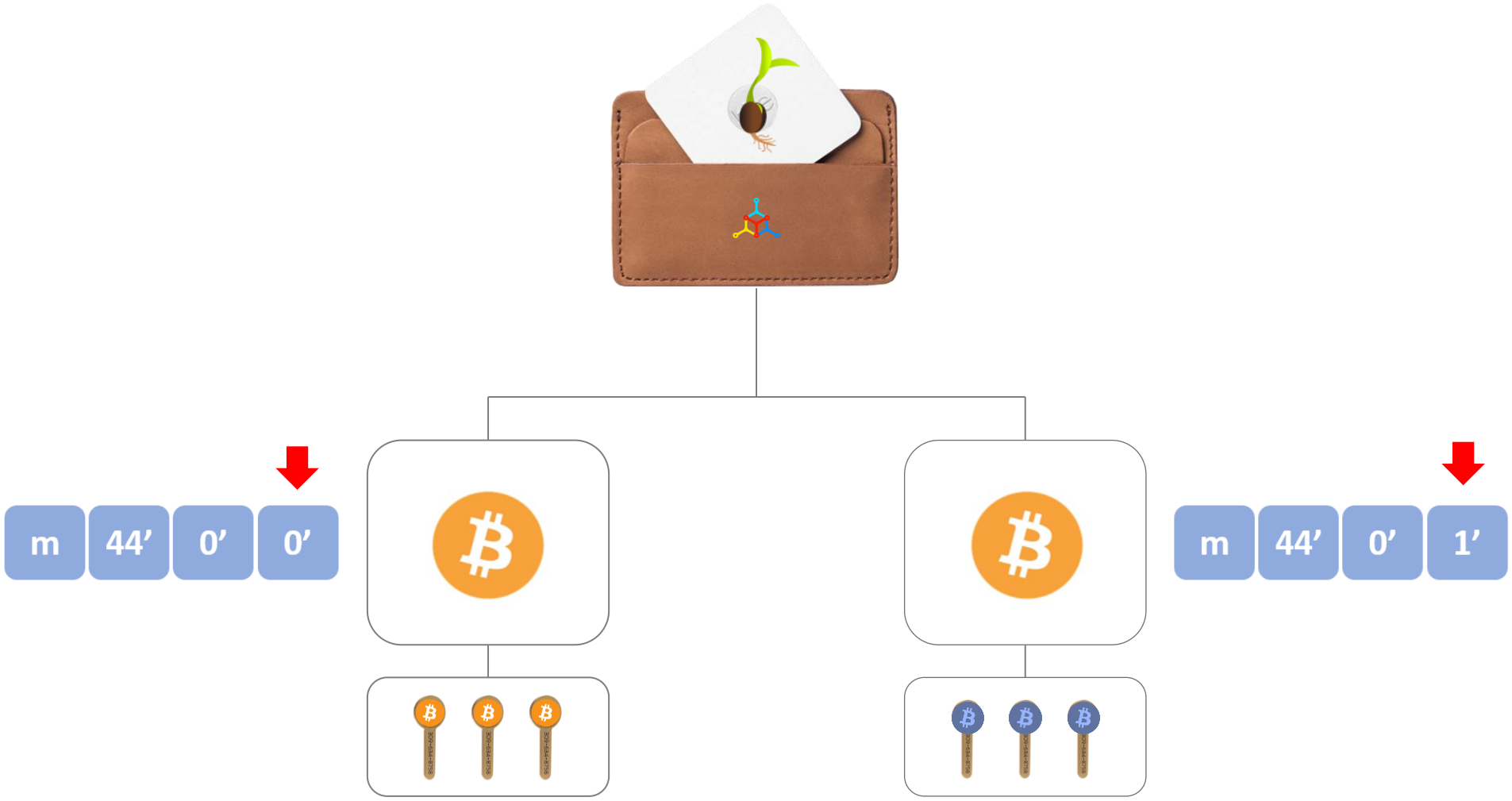

1 RESULT
2 INDEX
3 DECLINE
4 PILL
5 RICH
6 HEART
7 TOAST
8 NASTY
9 CHOICE
10 CONSIDER
11 AWARE
12 CANNON
wallet
wallet
wallet
wallet
wallet
wallet
wallet
wallet

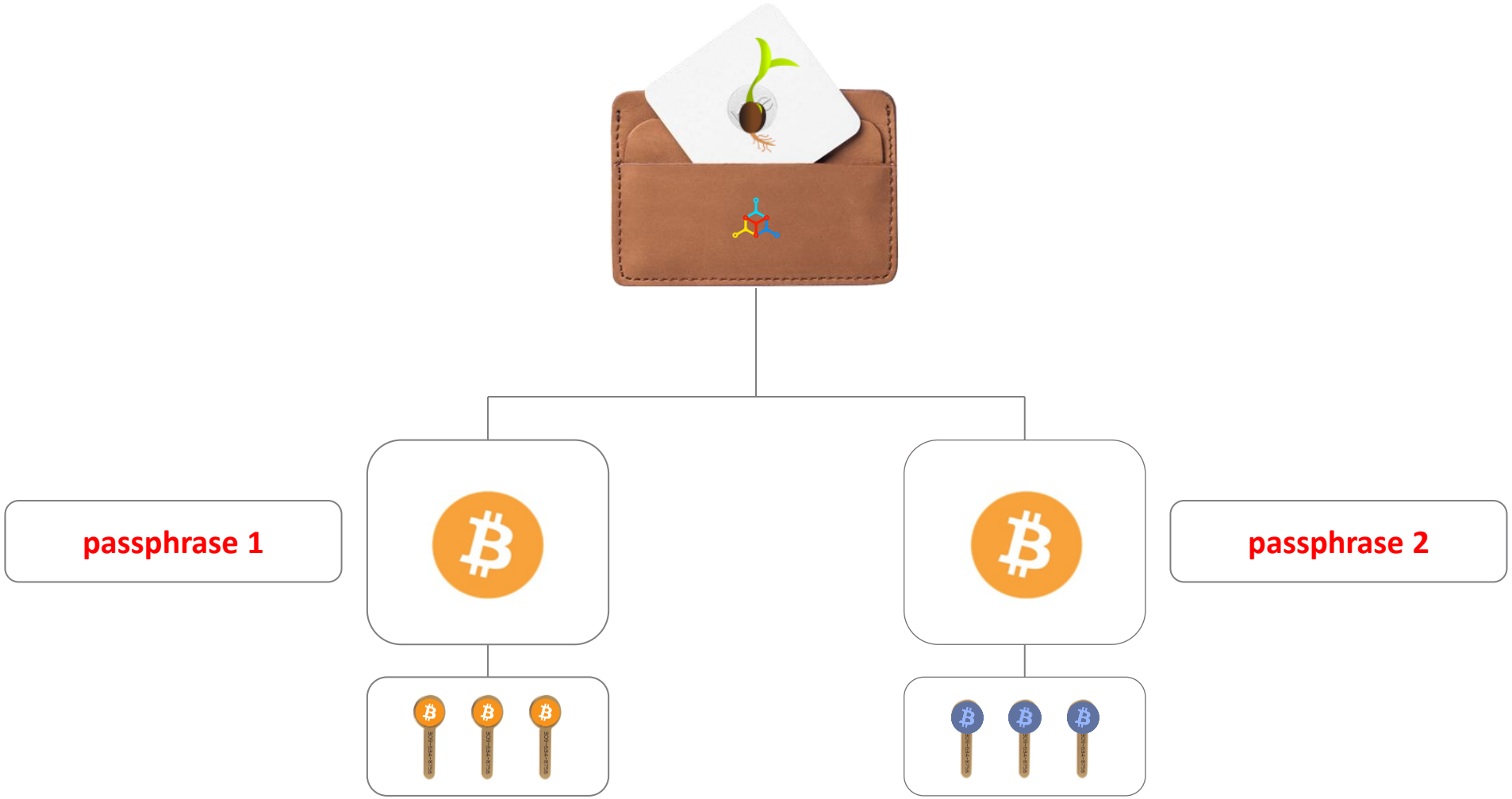

m
44’
0’
0’
wallet
wallet
wallet
wallet
wallet
wallet
wallet
wallet


m
44’
0’
4’
wallet
wallet
wallet
wallet
wallet
wallet
wallet
wallet


Sparrow - client wallet
File
View
Tools
Help
client wallet
Transactions
Send
Receive
Addresses
UTXOs
Settings
Settings
Policy Type:
Single Signature
Script Type:
Legacy (P2PKH)
Script Policy
Descriptor:
pkh(BIP39)
Edit...
Keystores
BIP39
Type:
Software Wallet
View Seed...
Replace...
Label:
BIP39
Master fingerprint:
ac13d0b5
Derivation:
m/44'/0'/0'
xpub:
xpub6CN5Y2WpUxugHxrL5d4FTJyVFFdpZzbLRTmQWYg
inXwDfEP516U86RHsosYi9yhLwMwmCWrddAXTQEF47N
Export...
Add Account...
Advanced...
Revert
Apply
Sparrow 2.0.0 available

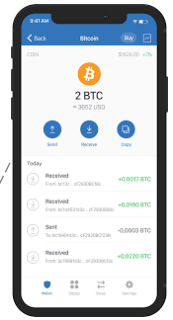

RECOVERY WORDS
Wallet name BitBox Stash
01 brave
02 spoil
03 scene
04 easy
05 dish
06 refuse
07 sign
fury
10 essen
11 wet
12 side
13 orange
14 coin
15 good
16 number
17 go
18 up
19 organ
20 title
21 hint
er
23
24 enforce
m/44'/0'/'1/1

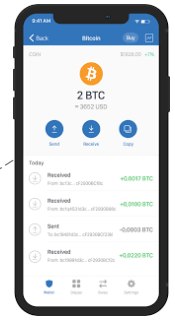

m
44’
0’
0’
m
44’
0’
1’

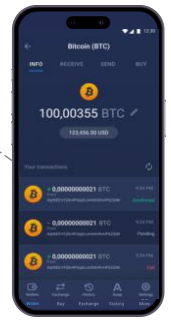

passphrase 1
passphrase 2

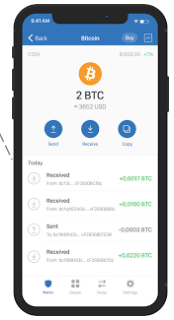
Seed words	
Random number	
Passphrase	@!?
Derivation path	44’0’
Master private key	
XPRIV	
Private Keys	

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









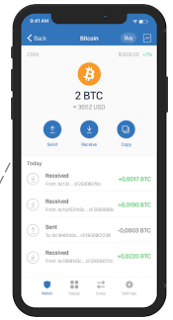
passphrase dad

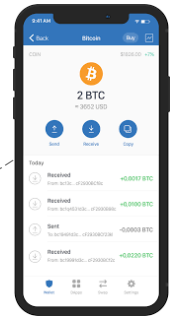
passphrase mom

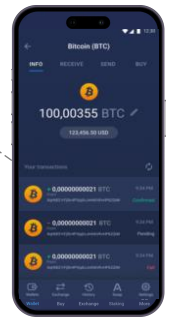
passphrase sally

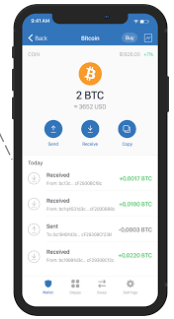
passphrase jack

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’

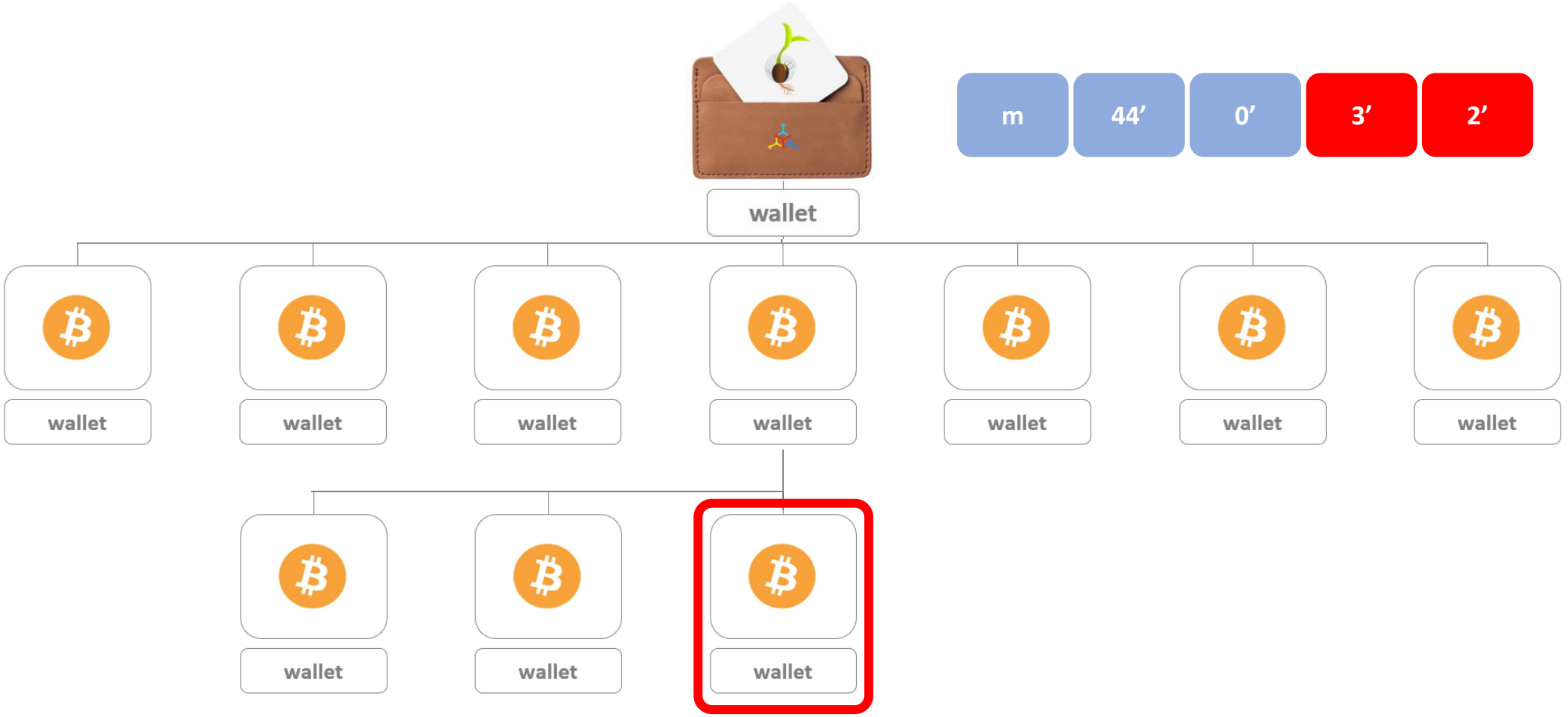
m 44’ 0’ 1’

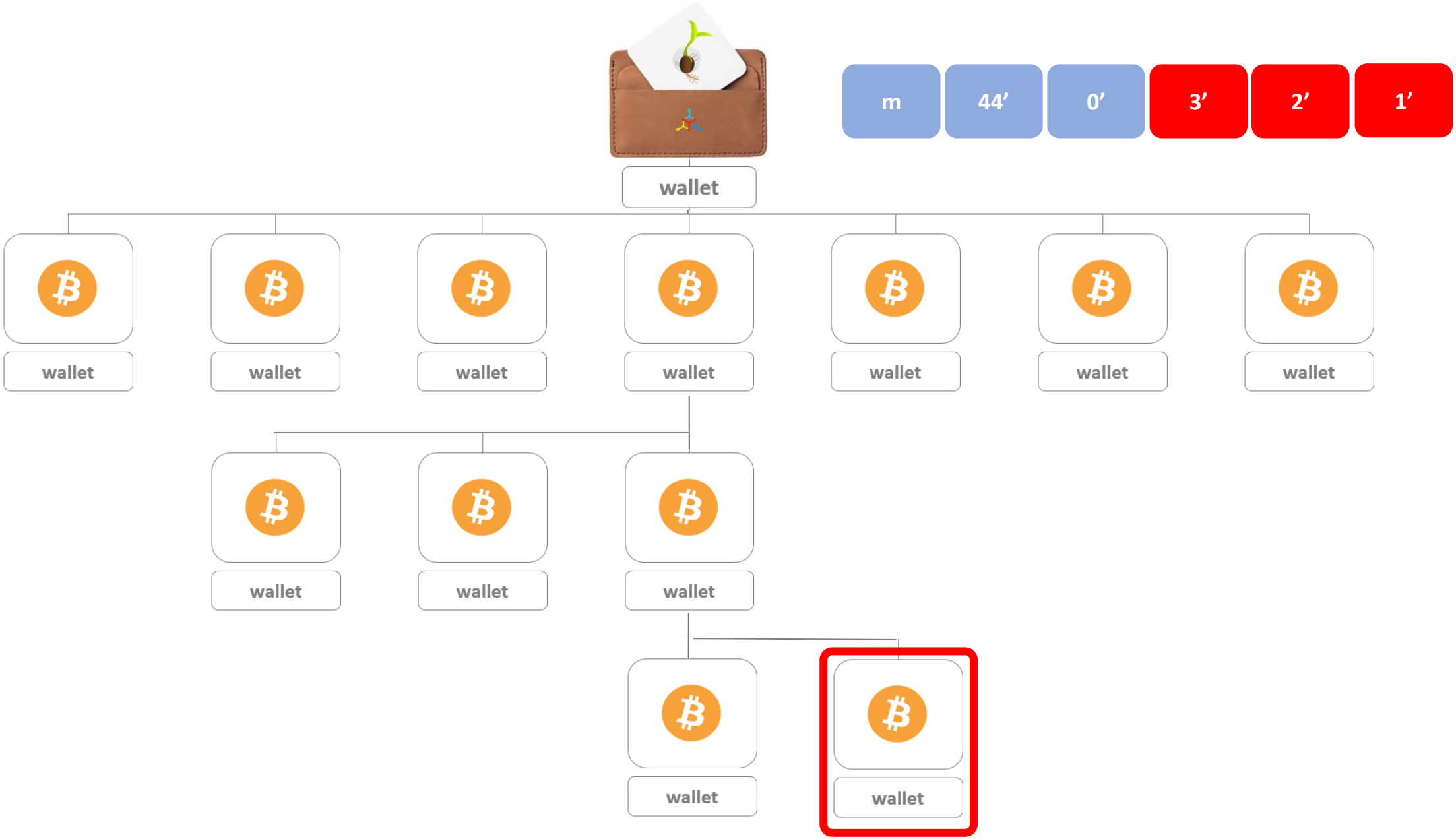
m 44’ 0’ 2’

m 44’ 0’ 3’

BitcoinBadger.net


m
44’
0’
3’
wallet
wallet
wallet
wallet
wallet
wallet
wallet
wallet

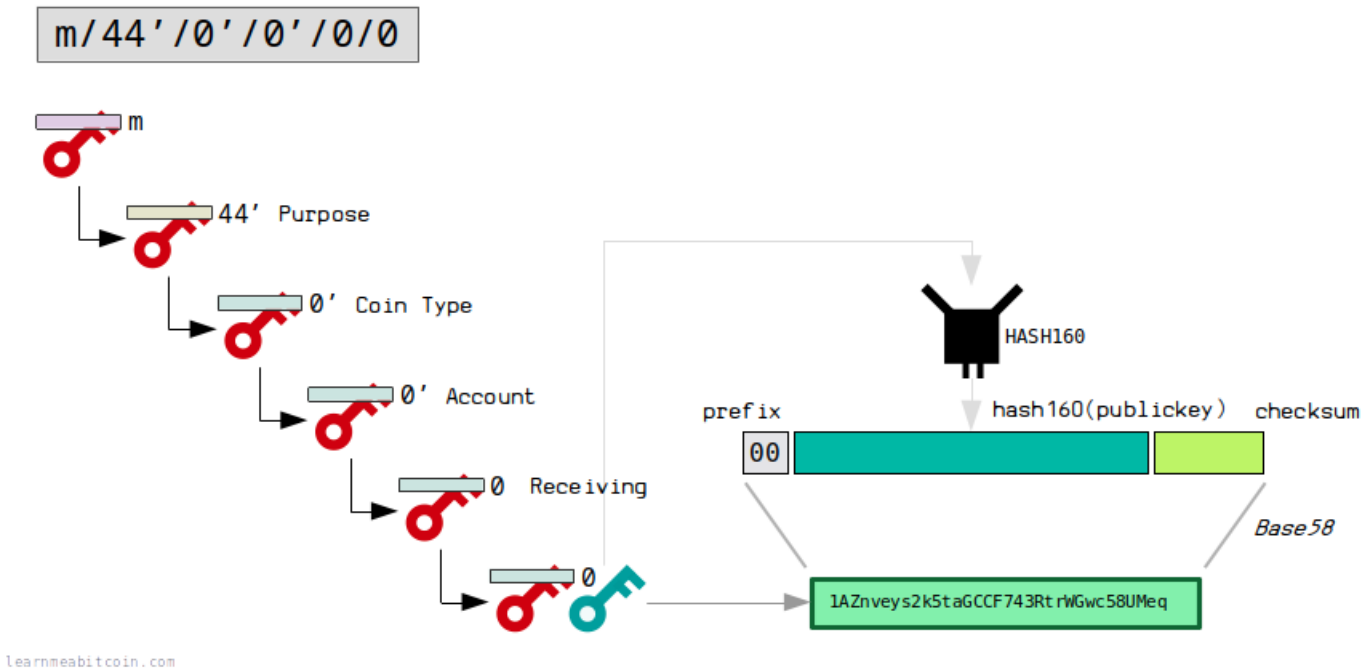

m
44’
0’
3’
2’
wallet
wallet
wallet
wallet
wallet
wallet
wallet
wallet
wallet
wallet
wallet


m
44’
0’
3’
2’
1’
wallet
wallet
wallet
wallet
wallet
wallet
wallet
wallet
wallet
wallet
wallet
wallet
wallet
wallet

m	44’	0’	3’	2’	1’	0’	3’	2’	1’

m	44’	0’	3’	2’	1’	0’	3’	2’	1’	23

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

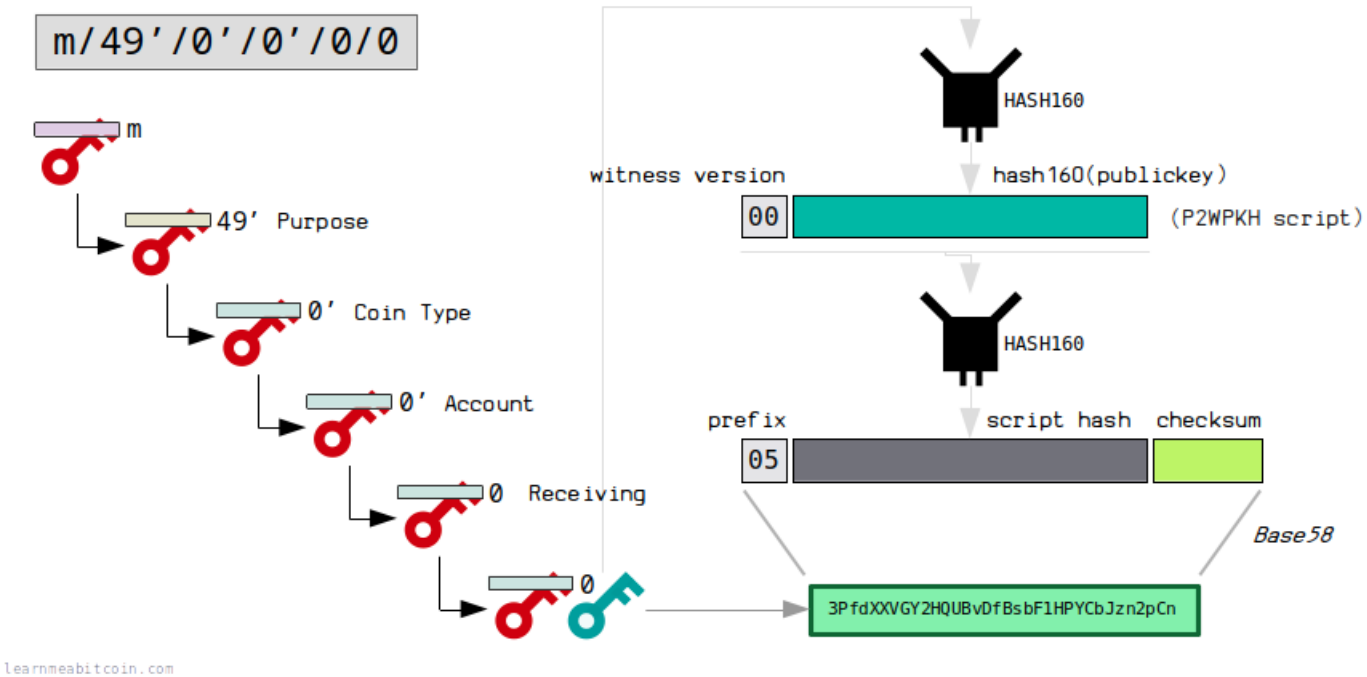


BIP 44 ↗ builds upon the original BIP 32 scheme to include a **purpose ↗** (which is like a version number to identify the upcoming scheme), as well as a **coin type** so that the same seed can be used to generate keys for different cryptocurrencies.

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

BIP 44 Extended Key Addresses [show]

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

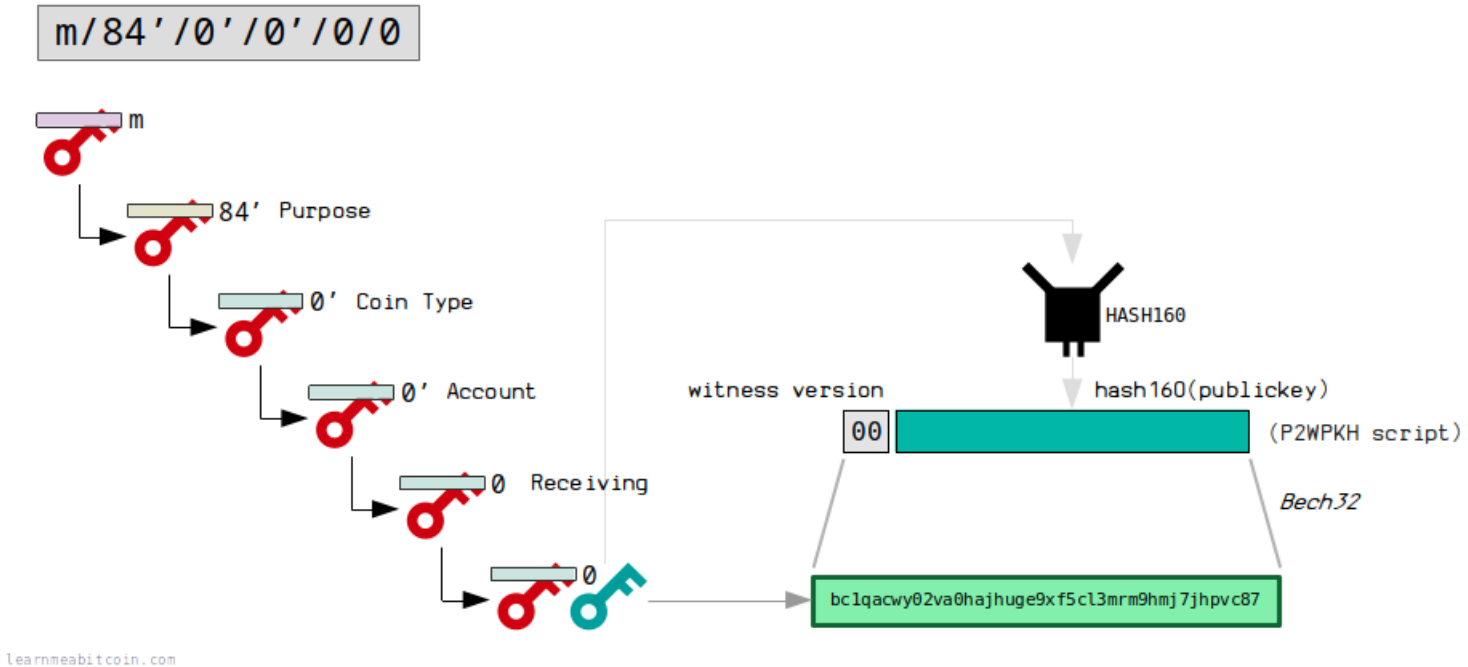


BIP 49 ↗ uses the same structure as BIP 44.

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

BIP 49 Extended Key Addresses [show]

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).

BIP 84 Extended Key Addresses [show]

BitcoinBadger.net