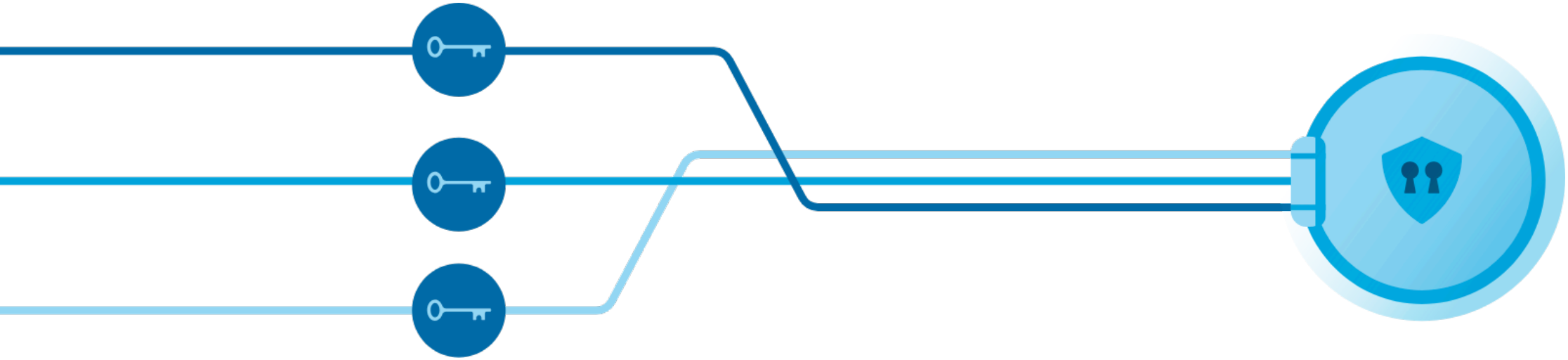
multi-sig

from mystery to mastery



BITSAGA

WHOAMI

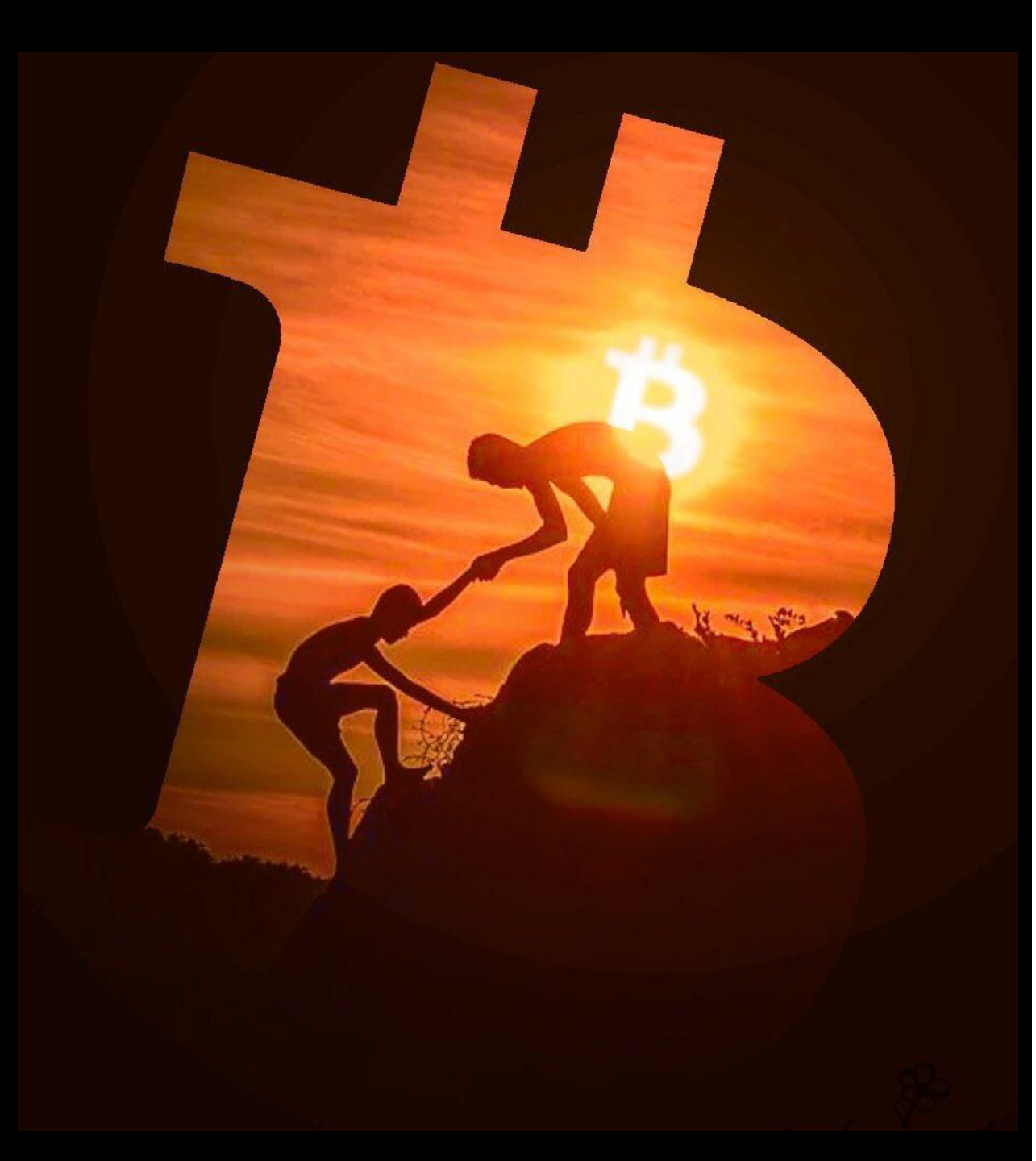
www.bitsaga.be

@BitsagaRob

@Bitsaga

Rob Segers

- Software engineer
- >10 year in bitcoin
- Fintech startup founder



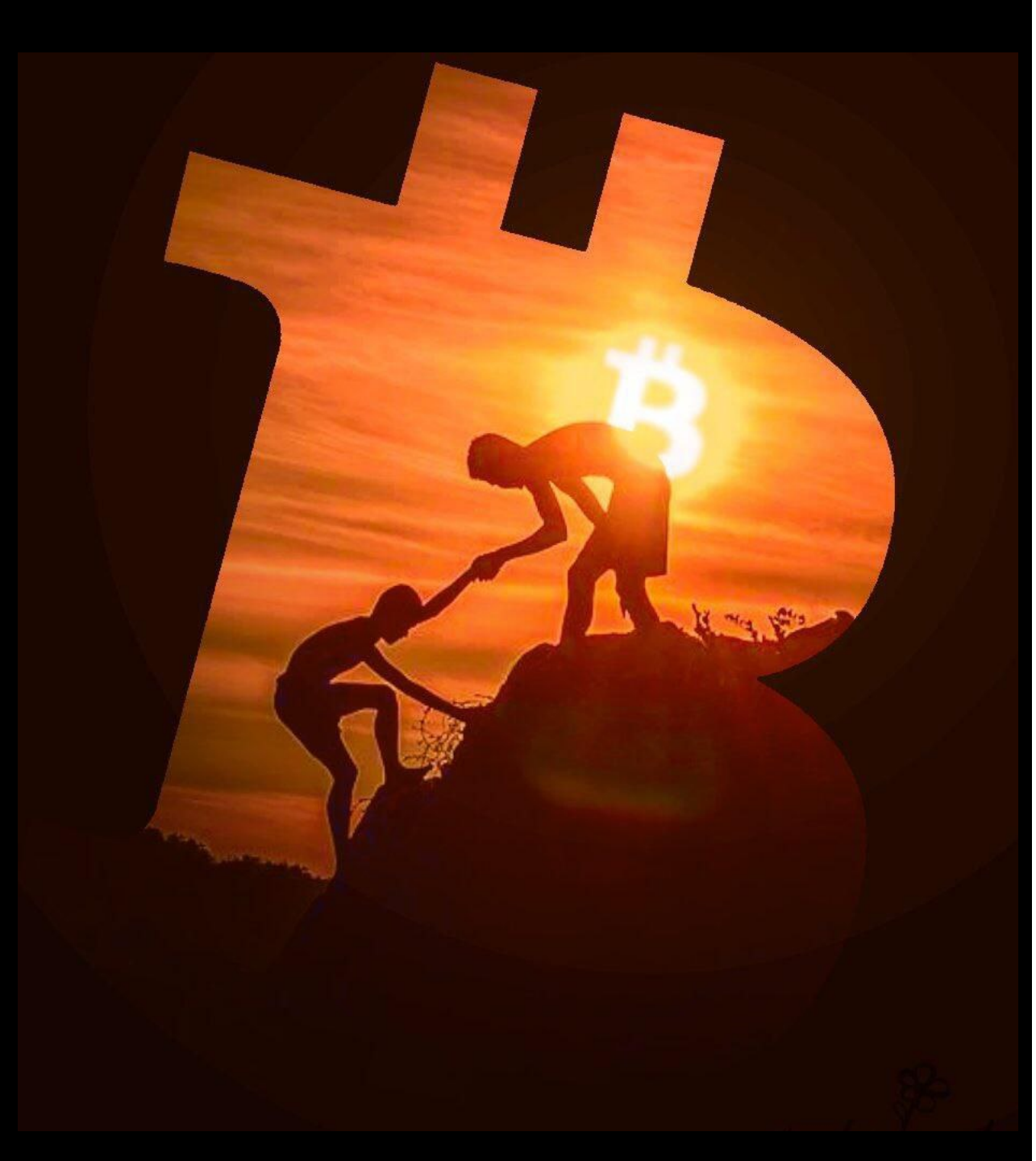
Multi-sig: mystery to mastery agenda

Disclaimer:

- Not here to convince
- Not here to sell

INFORM

BITSAGA



Multi-sig: mystery to mastery agenda

- Theoretical background
- Practical action
- Tools

Pierce through the perceived complexity of multi-sig to increase peace of mind

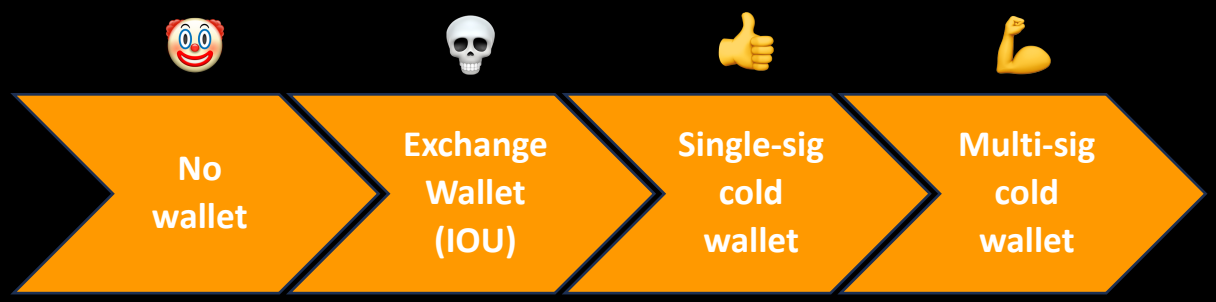
BITSAGA

Inspired by Michael Flaxman - btcguide.github.io

People worry about their bitcoin

- **Value**
- FUD
  - External (hacks, bankruptcies, seizures)
  - Internal (loss, mistakes, intrusion)

BITSAGA



Inspired by Michael Flaxman - btcguide.github.io

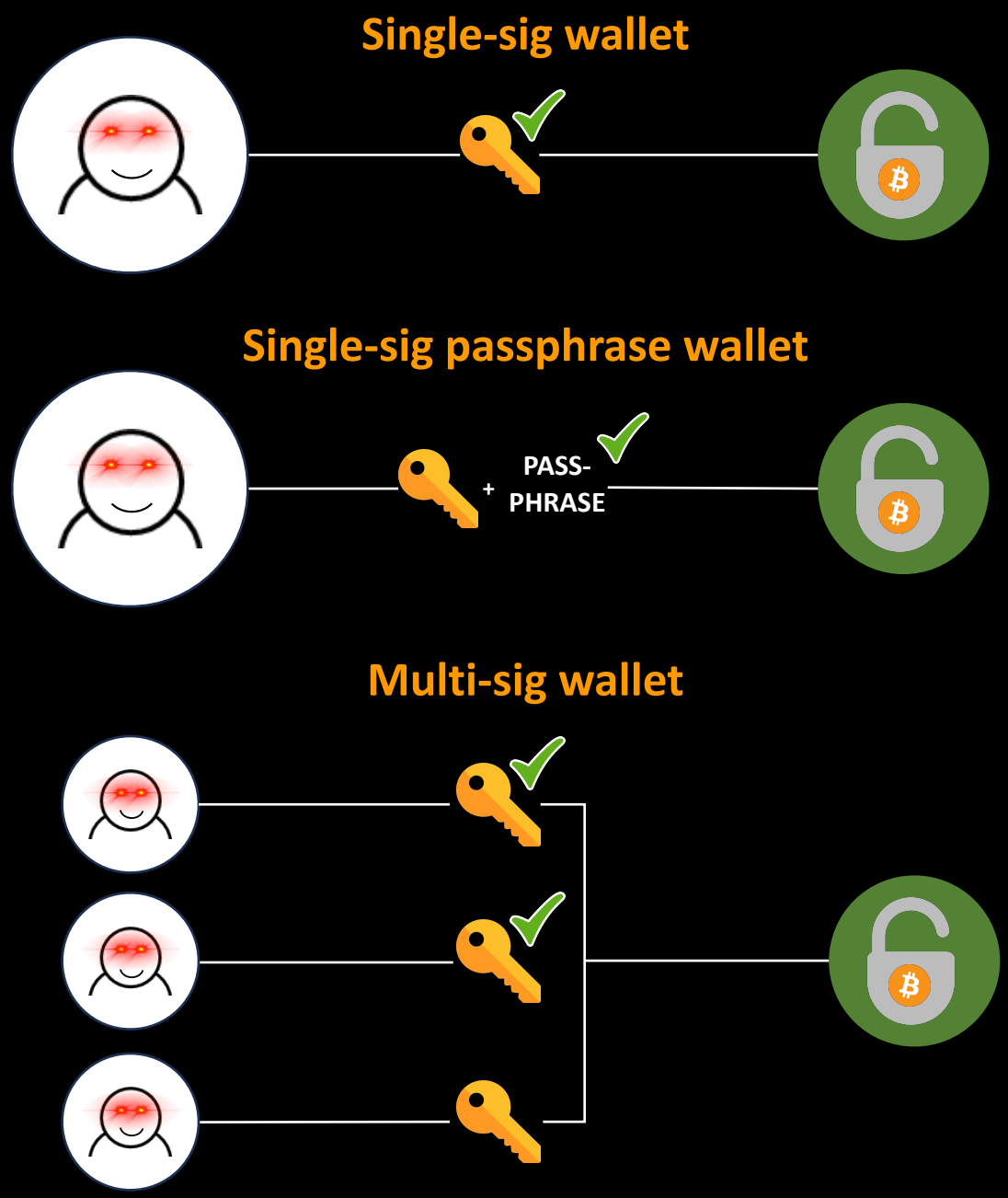
People worry about their bitcoin

- **Value**
- FUD
  - External (hacks, bankruptcies, seizures)
  - Internal (loss, mistakes, intrusion)

Single-sig

- **Does protect against external**
- **Does NOT protect against internal**

BITSAGA



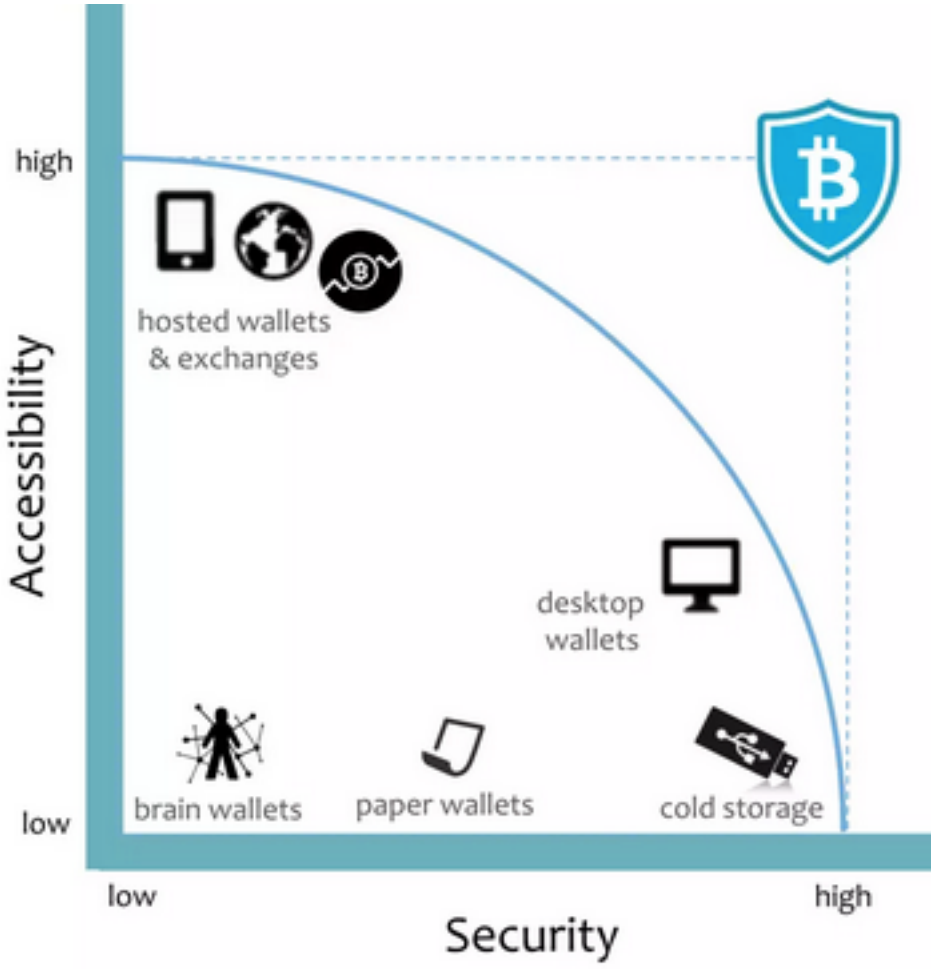
Bitcoin wallet types

Generally, 3 types of wallets

- Single signature
- Passphrase
- Multi signature

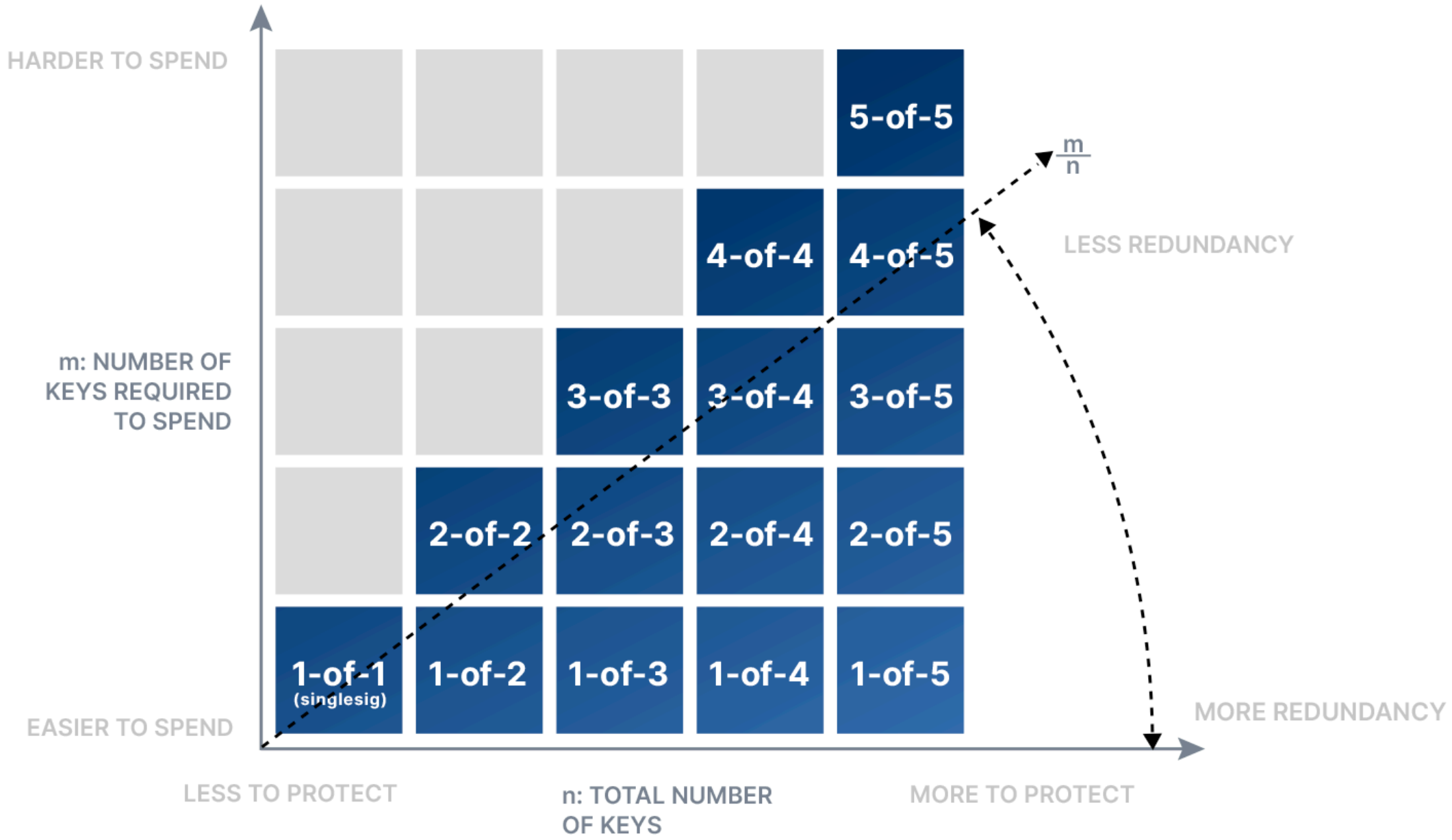
BITSAGA

single-sig


high
low
Accessibility
hosted wallets
& exchanges
desktop
wallets
brain wallets
paper wallets
cold storage
low
high
Security

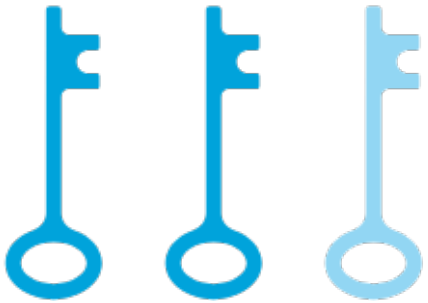
multi-sig


m
THE NUMBER OF KEYS
REQUIRED TO SIGN
n
THE TOTAL NUMBER
OF KEYS

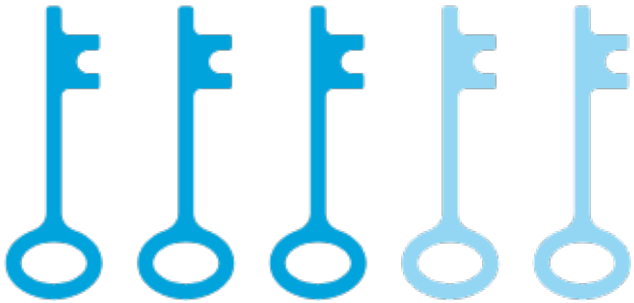

HARDER TO SPEND
m: NUMBER OF KEYS REQUIRED TO SPEND
EASIER TO SPEND
5-of-5
4-of-4
4-of-5
3-of-3
3-of-4
3-of-5
2-of-2
2-of-3
2-of-4
2-of-5
1-of-1 (singlesig)
1-of-2
1-of-3
1-of-4
1-of-5
m/n
LESS REDUNDANCY
MORE REDUNDANCY
LESS TO PROTECT
n: TOTAL NUMBER OF KEYS
MORE TO PROTECT

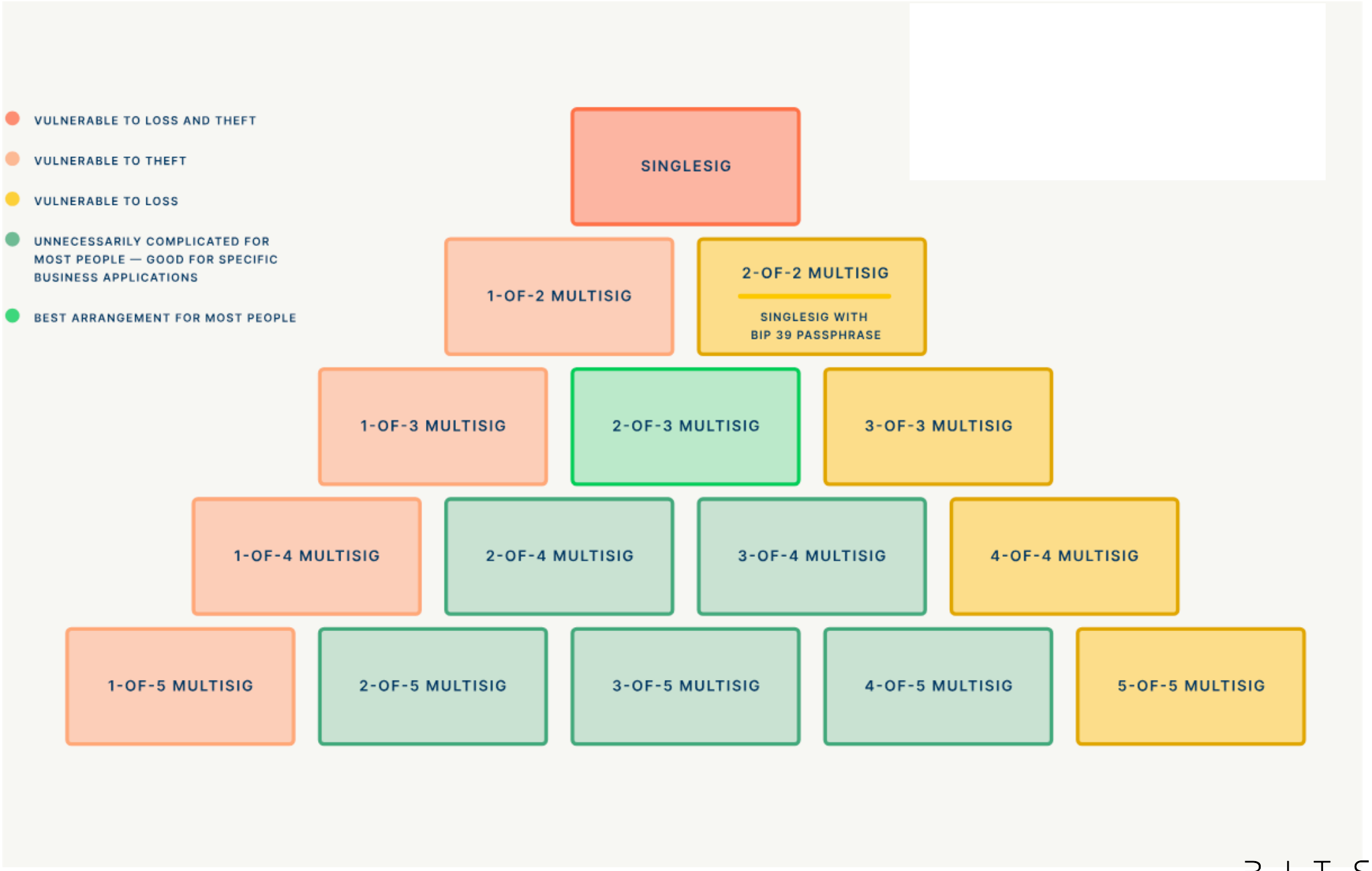
BITSAGA

2 KEYS REQUIRED / 3 TOTAL KEYS

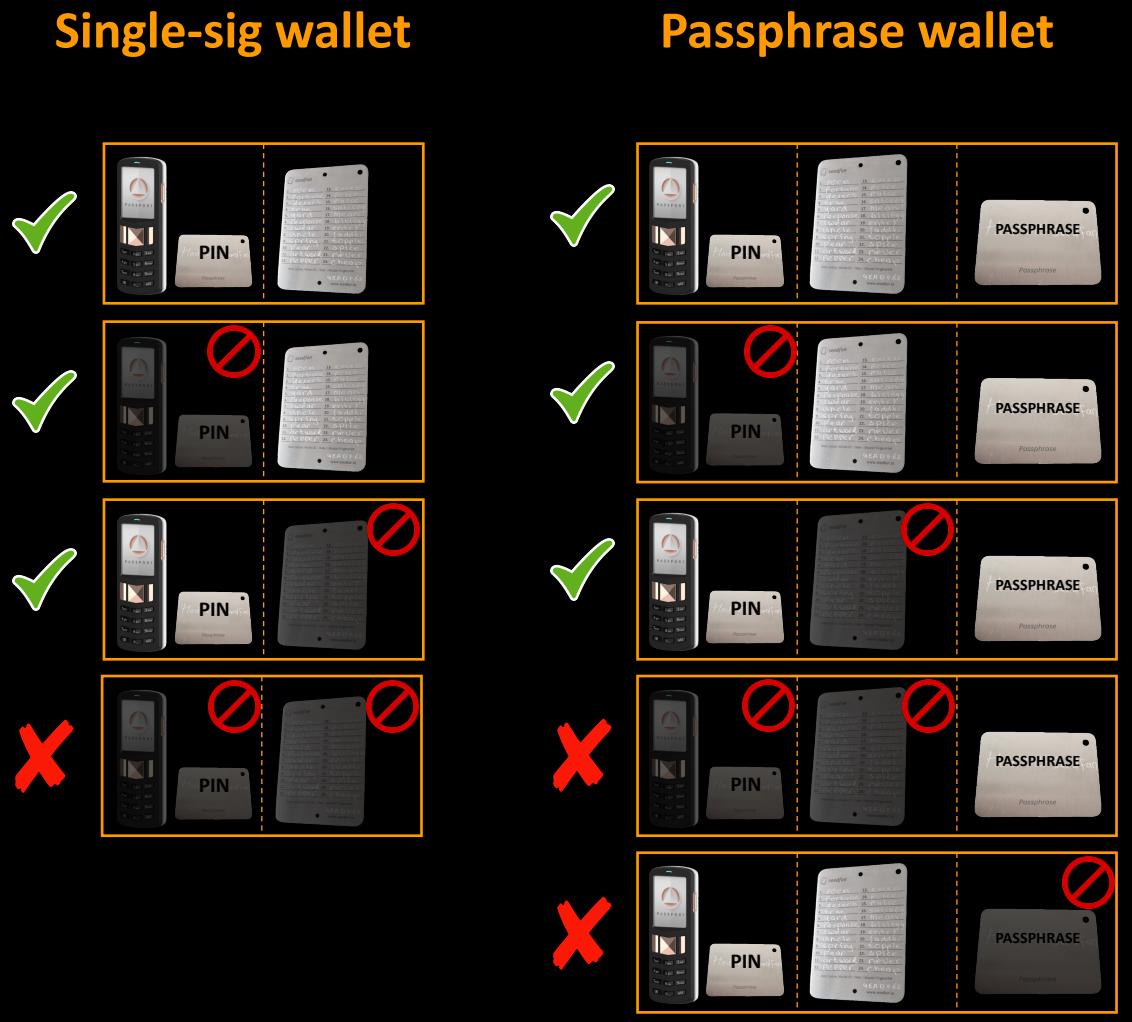


3 KEYS REQUIRED / 5 TOTAL KEYS




VULNERABLE TO LOSS AND THEFT
VULNERABLE TO THEFT
VULNERABLE TO LOSS
UNNECESSARILY COMPLICATED FOR MOST PEOPLE — GOOD FOR SPECIFIC BUSINESS APPLICATIONS
BEST ARRANGEMENT FOR MOST PEOPLE
SINGLESIG
1-OF-2 MULTISIG
2-OF-2 MULTISIG
SINGLESIG WITH BIP 39 PASSPHRASE
1-OF-3 MULTISIG
2-OF-3 MULTISIG
3-OF-3 MULTISIG
1-OF-4 MULTISIG
2-OF-4 MULTISIG
3-OF-4 MULTISIG
4-OF-4 MULTISIG
1-OF-5 MULTISIG
2-OF-5 MULTISIG
3-OF-5 MULTISIG
4-OF-5 MULTISIG
5-OF-5 MULTISIG

Fault tolerance



Fault tolerance

Single sig & passphrase

Single sig wallet

- Single key
- Single point of failure

Passphrase wallet (BIP-39)

- Key + passphrase
- Single point of failure (key)
- Single point of failure (passphrase)

Passphrase

- adds security
- adds a single point of failure (2/2)

BITSAGA

Fault tolerance
Multi-sig

Multi-sig wallet

- Multiple private keys AND descriptor!
- No single point of failure

Output descriptor

- Public wallet information (xpubs)
- Leaking output descriptor = privacy risk
- **Critical** to back-up, often misunderstood

Multi-sig mitigates

- **Single point of failure**
- **Physical & software risks**

Hardware & software risks

Single-sig hardware risks

Risk	Best practice
Loss	Back-up
Fault	Reset and recover
Damage	Back-up in steel
Exposure	Secure location
Tampering	Secure element
Inheritance	?

Single signature wallet

- Single points of failure
- Ways to mitigate

Mitigating single-sig hardware risks can be a challenge

BITSAGA

Risk	Best practice
Compromised seed generator	Manual entropy
Mismatch seed / private key	Check on 2nd device
Malicious receive address	Check on 2nd device
Malicious send address	Visual check input/output
Compromised software	Verify software

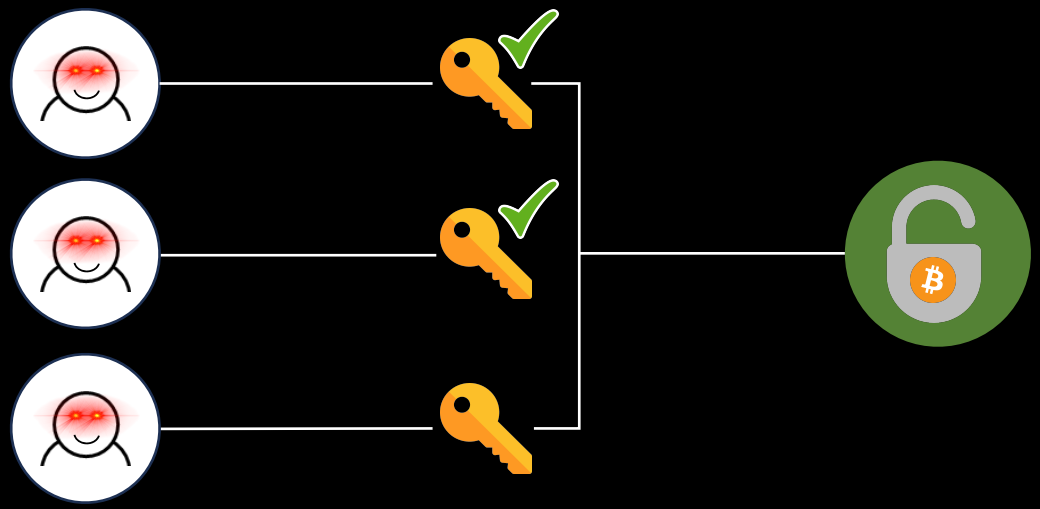
Single-sig software risks

Single signature wallet

- Trust the code
- Supply chain attacks
- Retirement attacks
- Software attacks
- …
- Ways to mitigate

Mitigating single-sig software risks can be a challenge

BITSAGA



Multi-sig mitigates risks by design

Physical risk protection

- Lost & stolen private key
- Fault, damage, exposure, tampering
- Inheritance planning opportunities

Software risk protection

- Don’t trust: decentralised code (multi-vendor)
- Built-in address verification

Multi-signature exponentially adds security while adding only a little complexity

BITSAGA

Output descriptor

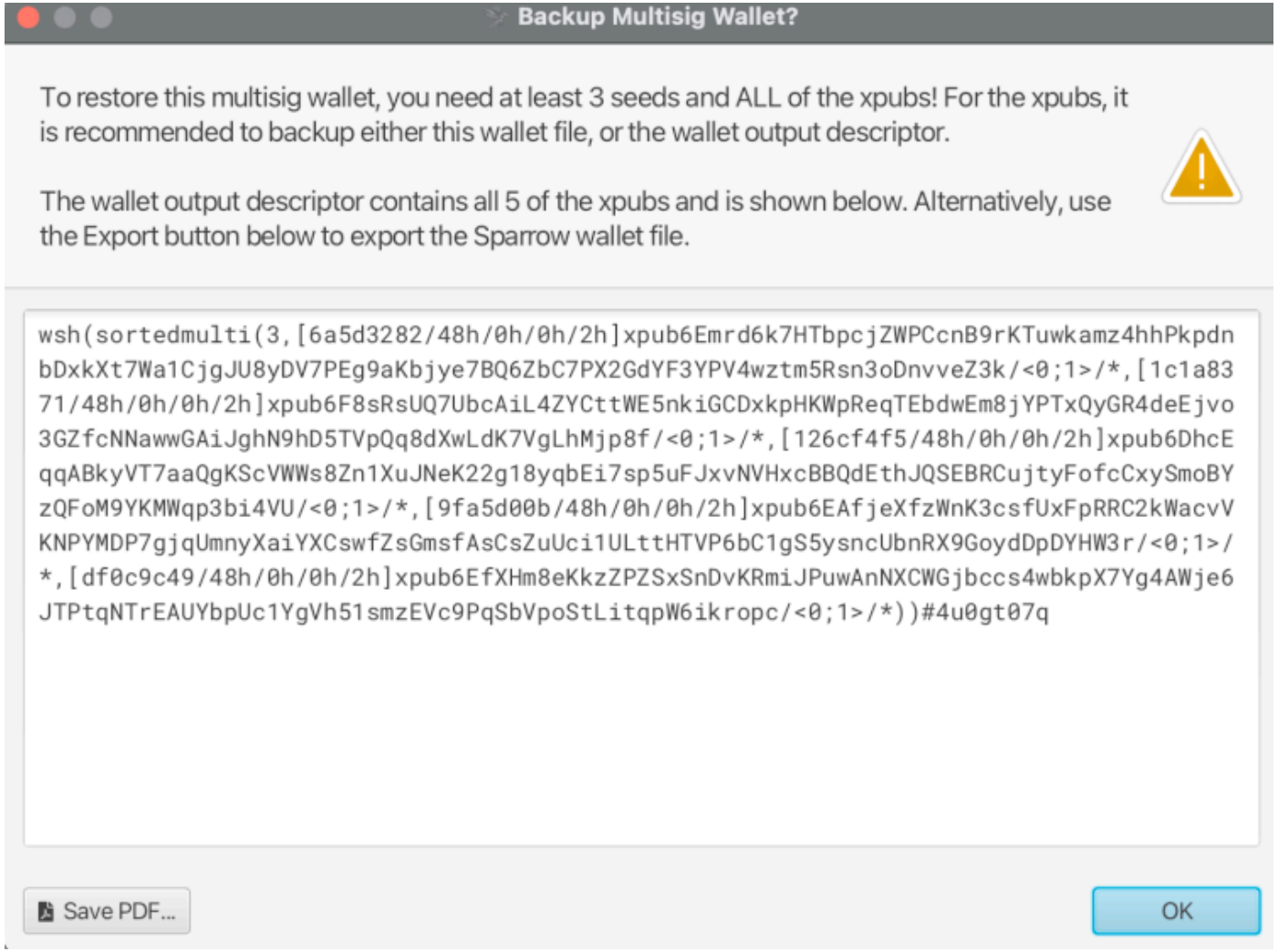
Under the hood

Creating a 2-of-3 P2SH multisig address

```
bitcoin-cli -testnet createmultisig 2 '"
  [
    'mjbLRSidW1MY8oubvs4SMEnHNFXxCcoehQ",
    "02ecd2d250a76d204011de6bc365a56033b9b3a149f679bc17205555d3c2b2854f",
    "mt17cV37fBqZsnMmrHnGCm9pM28R1kQdMG"
  ]'"

Result
{
  "address" : "2MyVxxgNBk5zHRPRY2iVjGRJHYZEp1pMCSq"
  "redeemScript" :
"522103ede722780d27b05f0b1169efc90fa15a601a32fc6c3295114500c586831b6aaf2102e
cd2d250a76d204011de6bc365a56033b9b3a149f679bc17205555d3c2b2854f21022d609d2f
0d359e5bc0e5d0ea20ff9f5d3396cb5b1906aa9c56a0e7b5edc0c5d553ae"
}
```

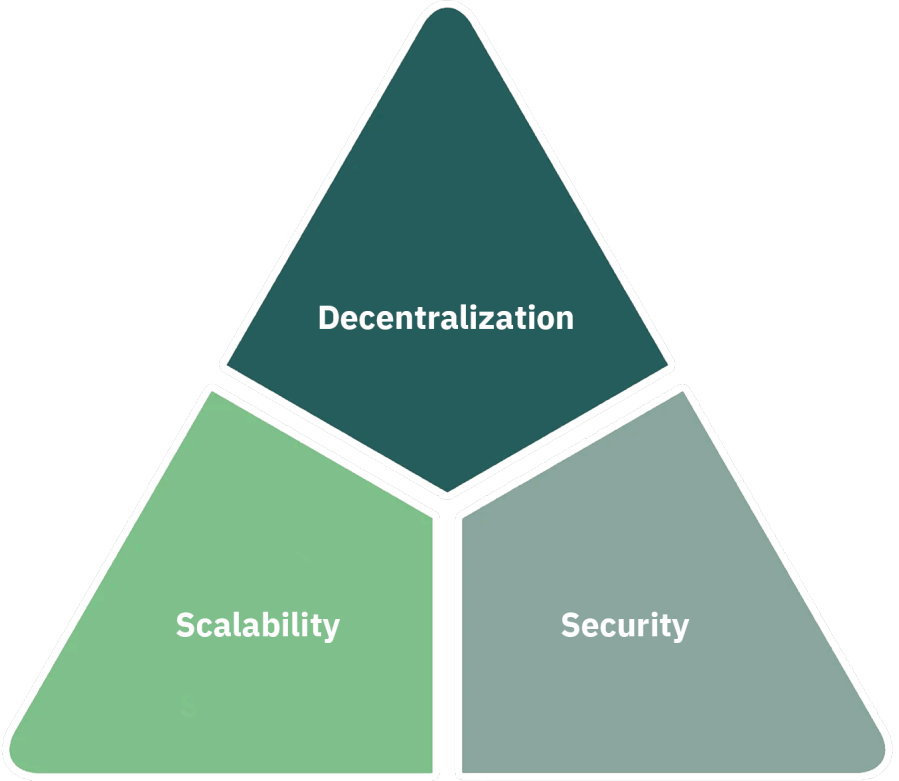
```
bitcoin-cli -testnet decodescript 522103ede722780d27b05f0b1169ef\
c90fa15a601a32fc6c3295114500c586831b6aaf2102ecd2d250a76d204011de\
6bc365a56033b9b3a149f679bc17205555d3c2b2854f21022d609d2f0d359e5b\
c0e5d0ea20ff9f5d3396cb5b1906aa9c56a0e7b5edc0c5d553ae

{OP_CHECKMULTISIG",
   "reqSigs" : 2,
   "type" : "multisig",
   "addresses" : [
      "mjbLRSidW1MY8oubvs4SMEnHNFXxCcoehQ",
      "mo1vzGwCzWqteip29vGWWW6MsEBREuzW94",
      "mt17cV37fBqZsnMmrHnGCm9pM28R1kQdMG"
   ],
   "p2sh" : "2MyVxxgNBk5zHRPRY2iVjGRJHYZEp1pMCSq"
}
```

Output descriptor



BITSAGA

The bitcoin way



Storing bitcoin on exchanges is un-bitcoin

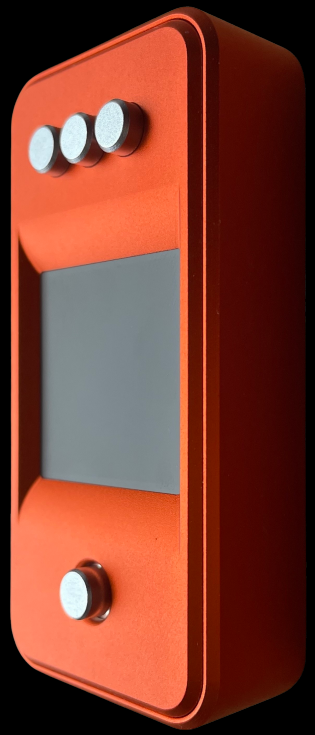
Storing bitcoin in single sig is un-bitcoin

Multi-sig: software

- Mobile & desktop
- Guided setups
- Collaborative custody
- Young tools

New software has simplified multi-sig

BITSAGA



Multi-sig: hardware

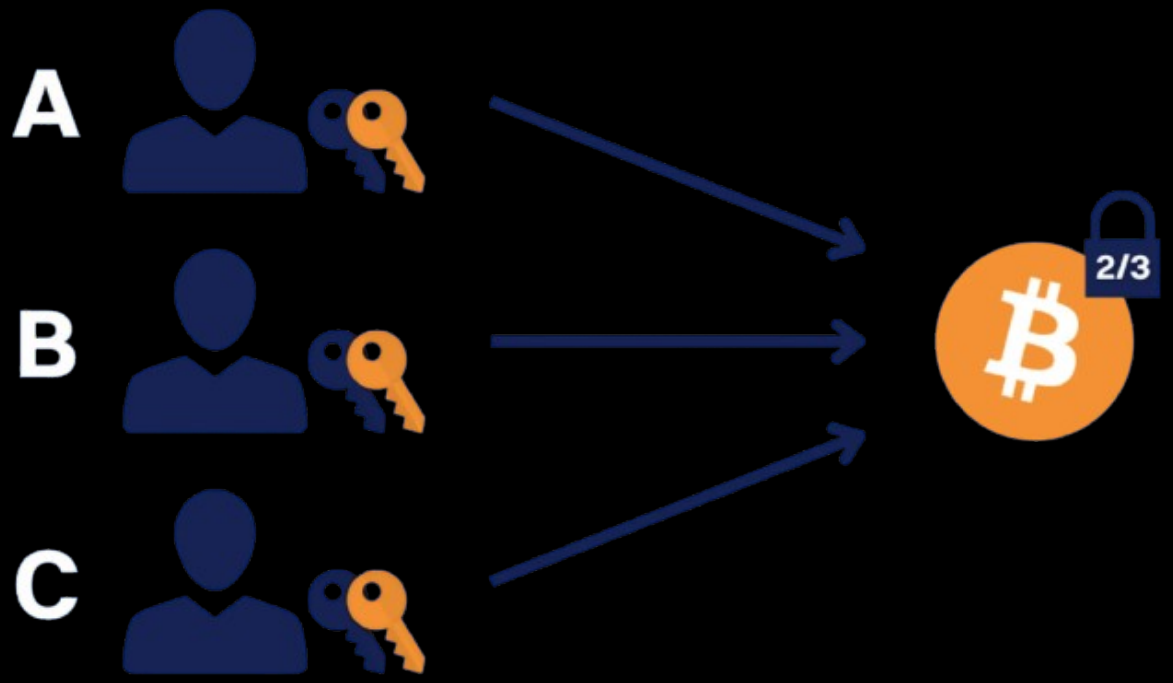
- Airgapped devices
- QRs = game changer
  - Transaction (PSBT - BIP174)
  - Adress
  - Seed

New hardware has simplified multi-sig

BITSAGA

Let’s walk the talk

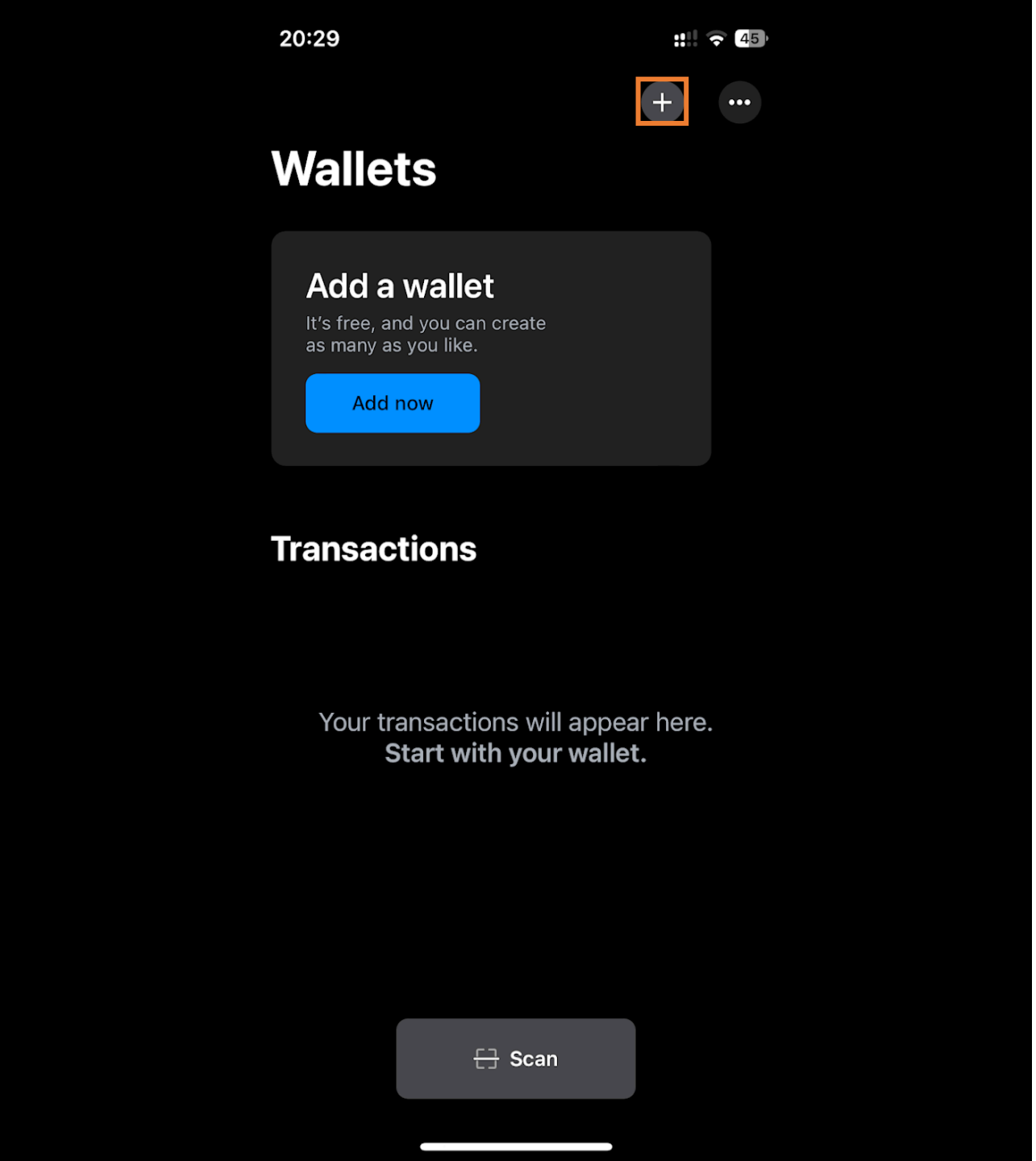
BITSAGA



Multi-sig: mastery

- Create 2/3 multi-sig wallet
- Add 3 keys
- Receive and send
- Backup and restore

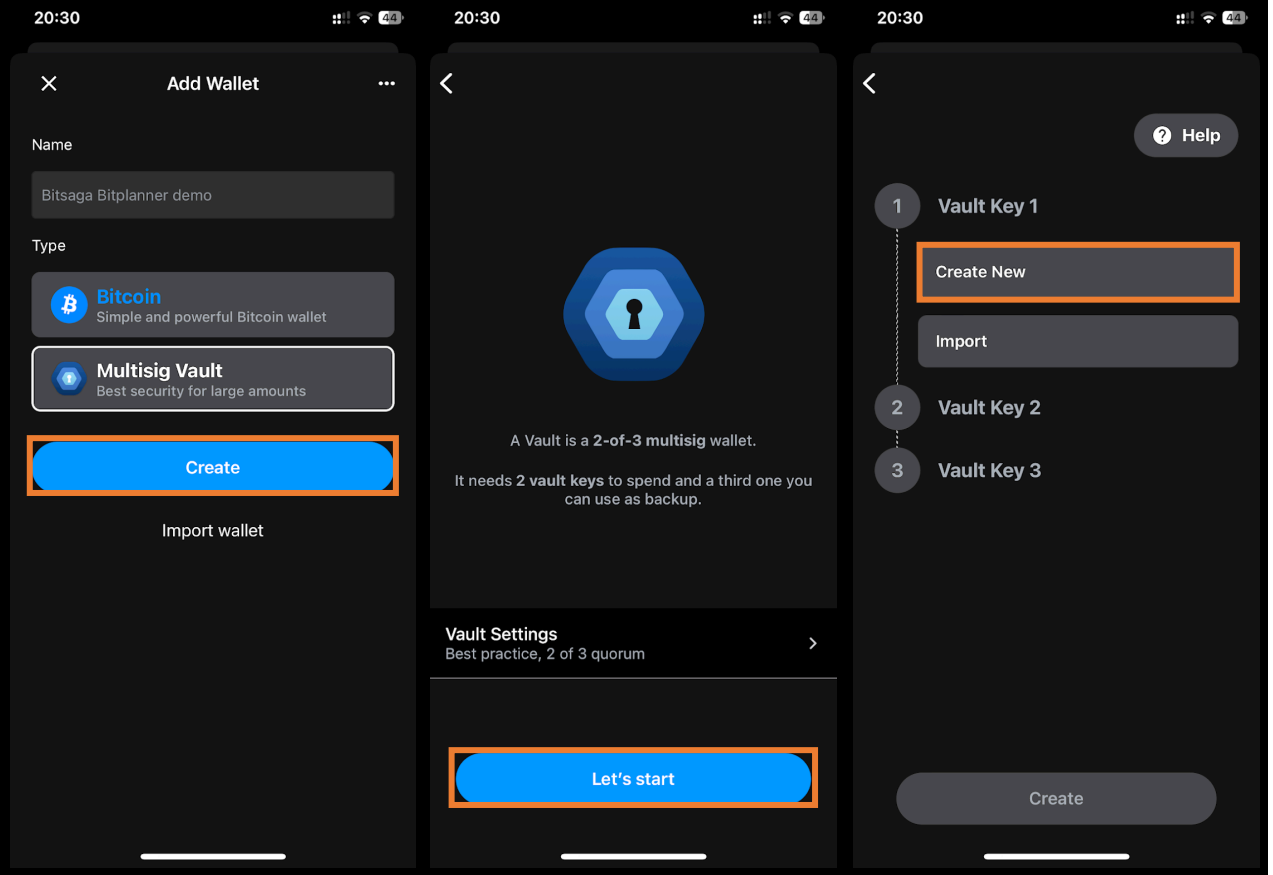
Multi-sig: Blue



Multi-sig: Blue

BITSAGA

Create multi-sig wallet & add key 1 (hot)



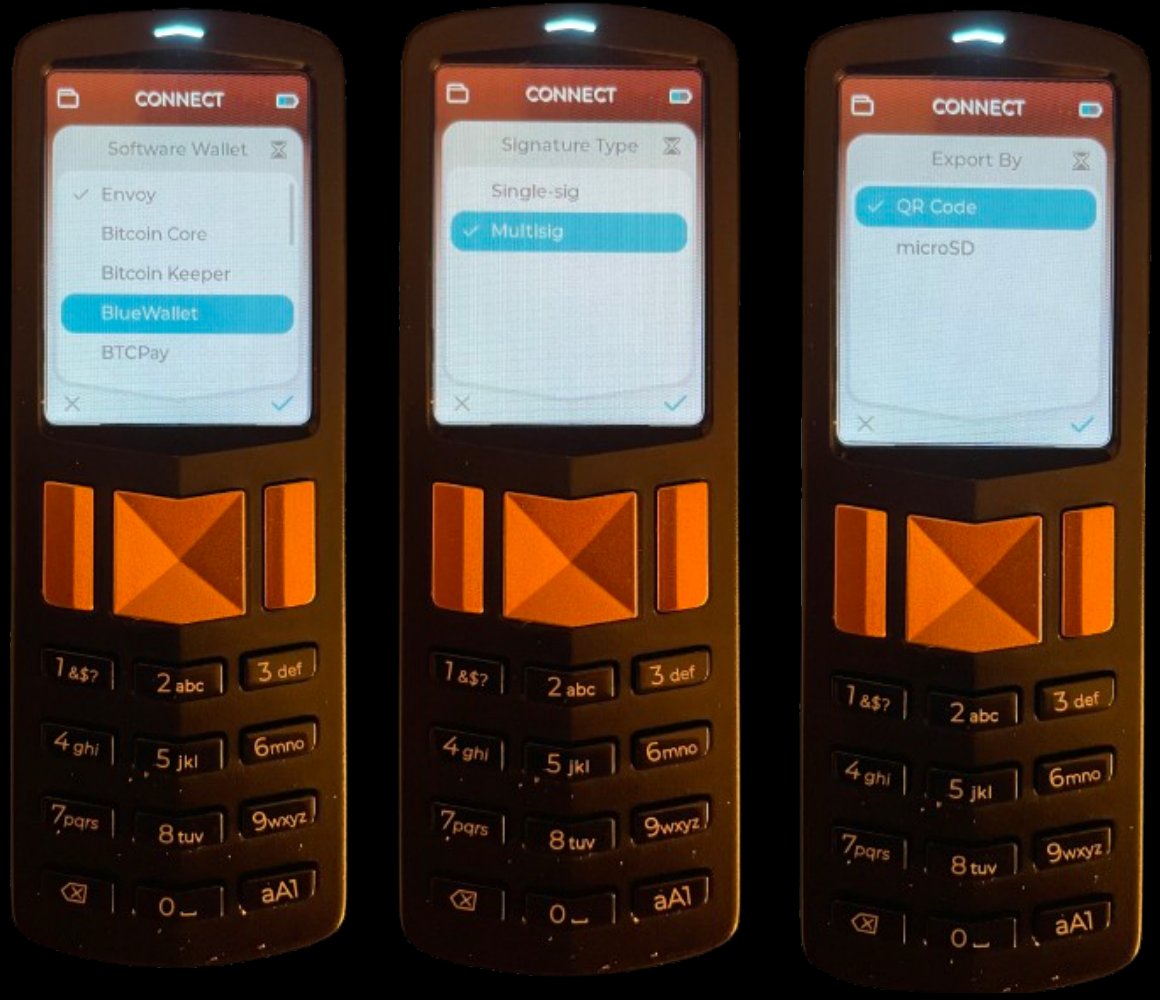
BITSAGA

Add multi-sig wallet key 2 (cold)

BITSAGA

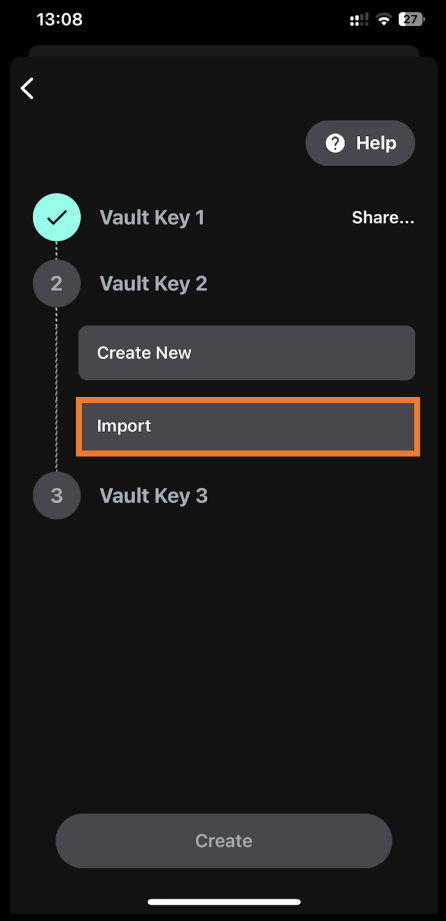
Add multi-sig wallet key 2 (cold)

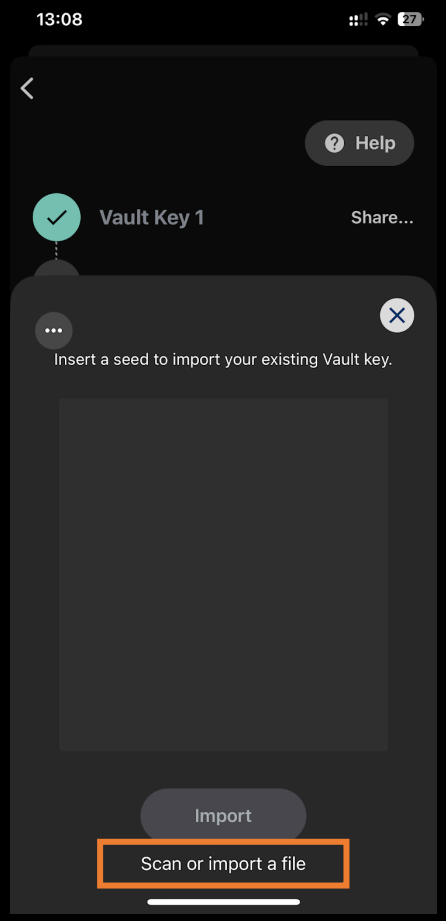
BITSAGA



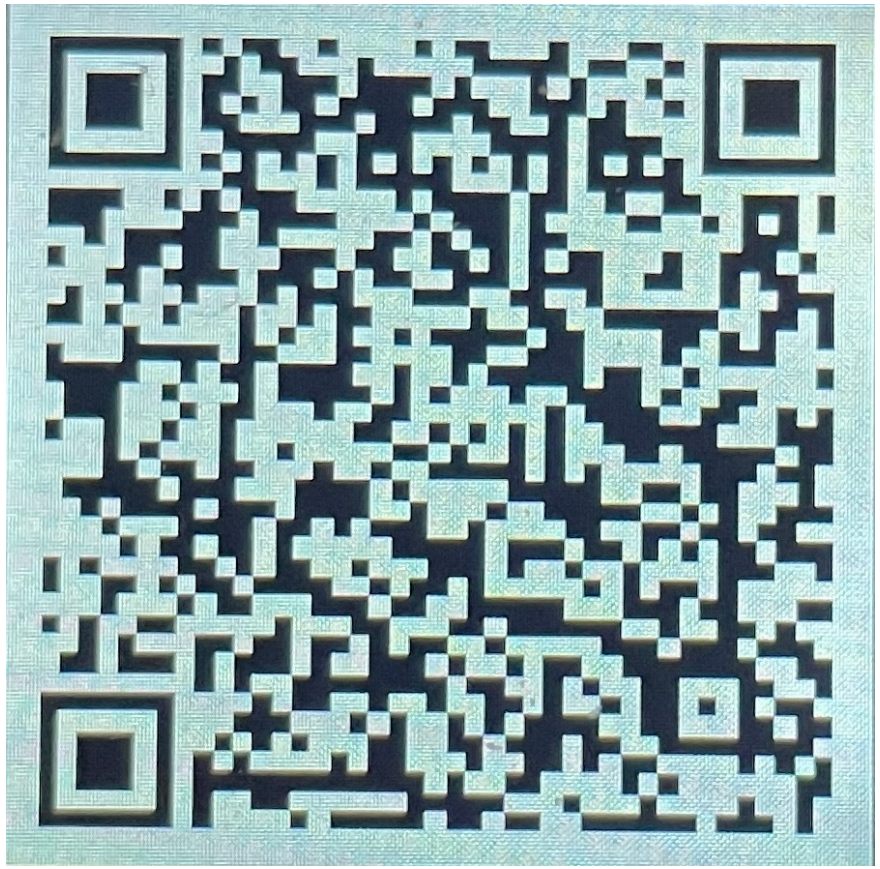
Add multi-sig wallet key 2 (cold)

BITSAGA





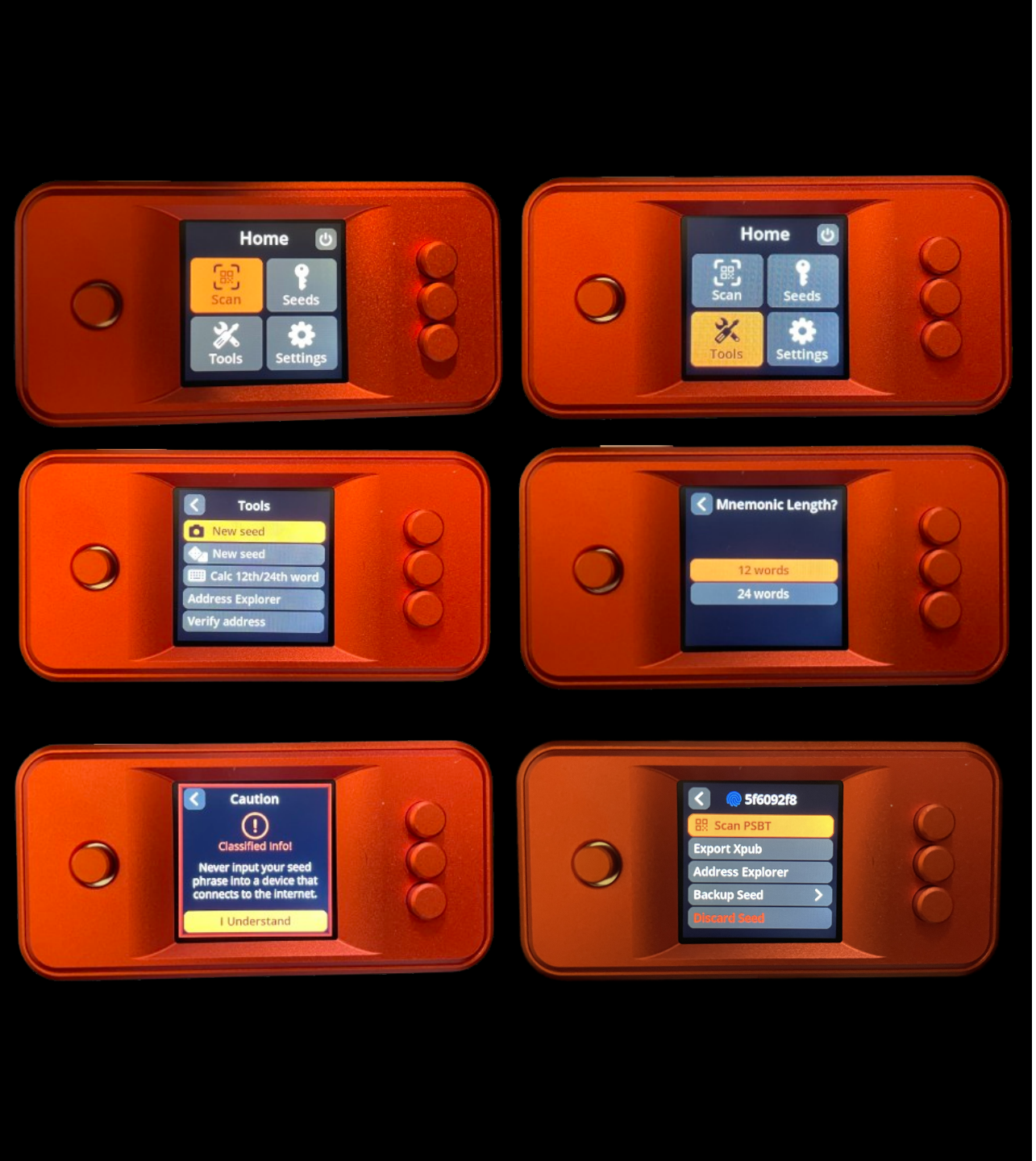
Scan Xpub QR to add key 2



BITSAGA

Add multi-sig wallet key 3 (cold)

BITSAGA



Add multi-sig wallet key 3 (cold)

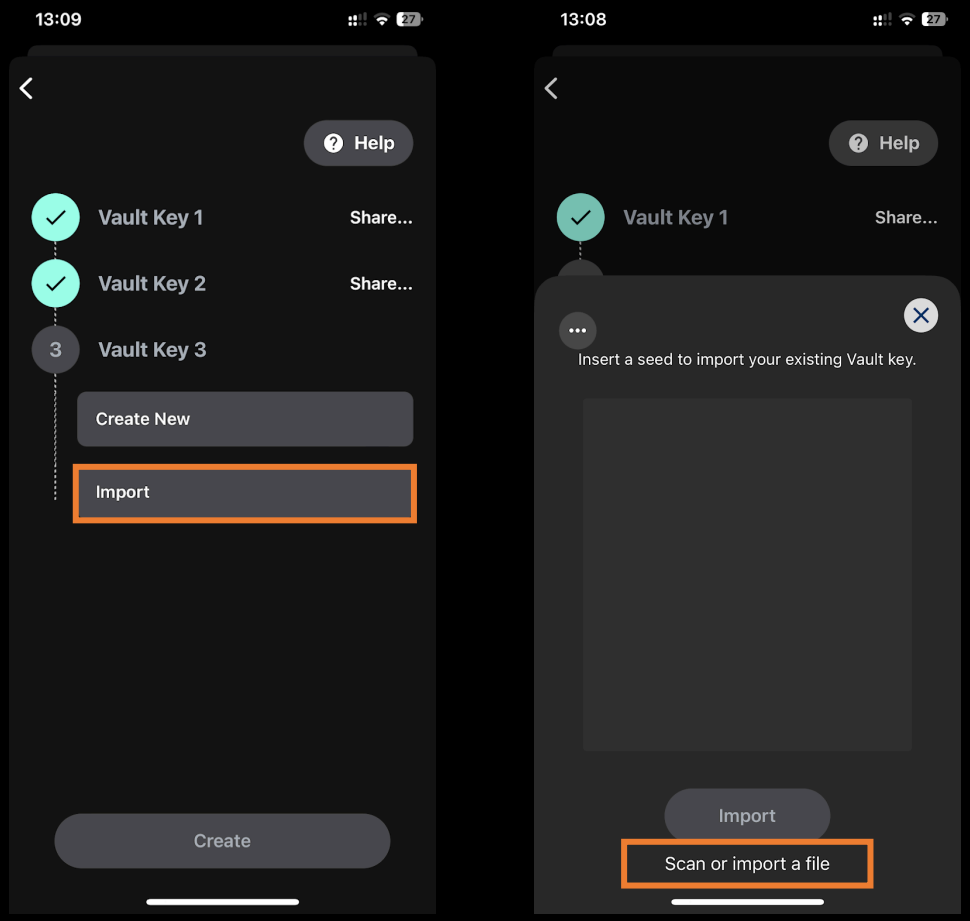
BITSAGA

Add multi-sig wallet key 3 (cold)

BITSAGA

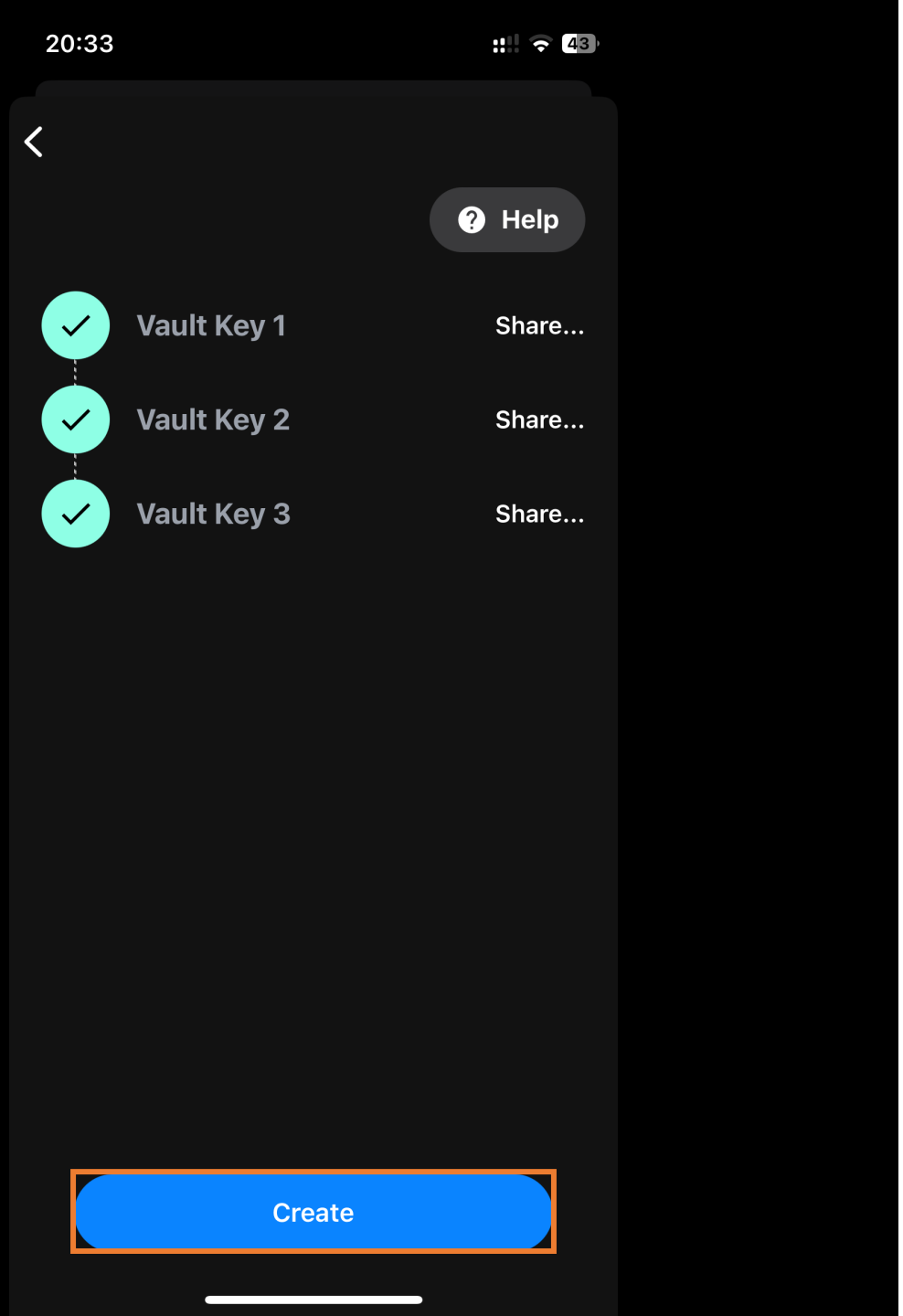
Add multi-sig wallet key 3 (cold)

BITSAGA



Scan Xpub QR to add key 3

BITSAGA



Multi-sig wallet keys added

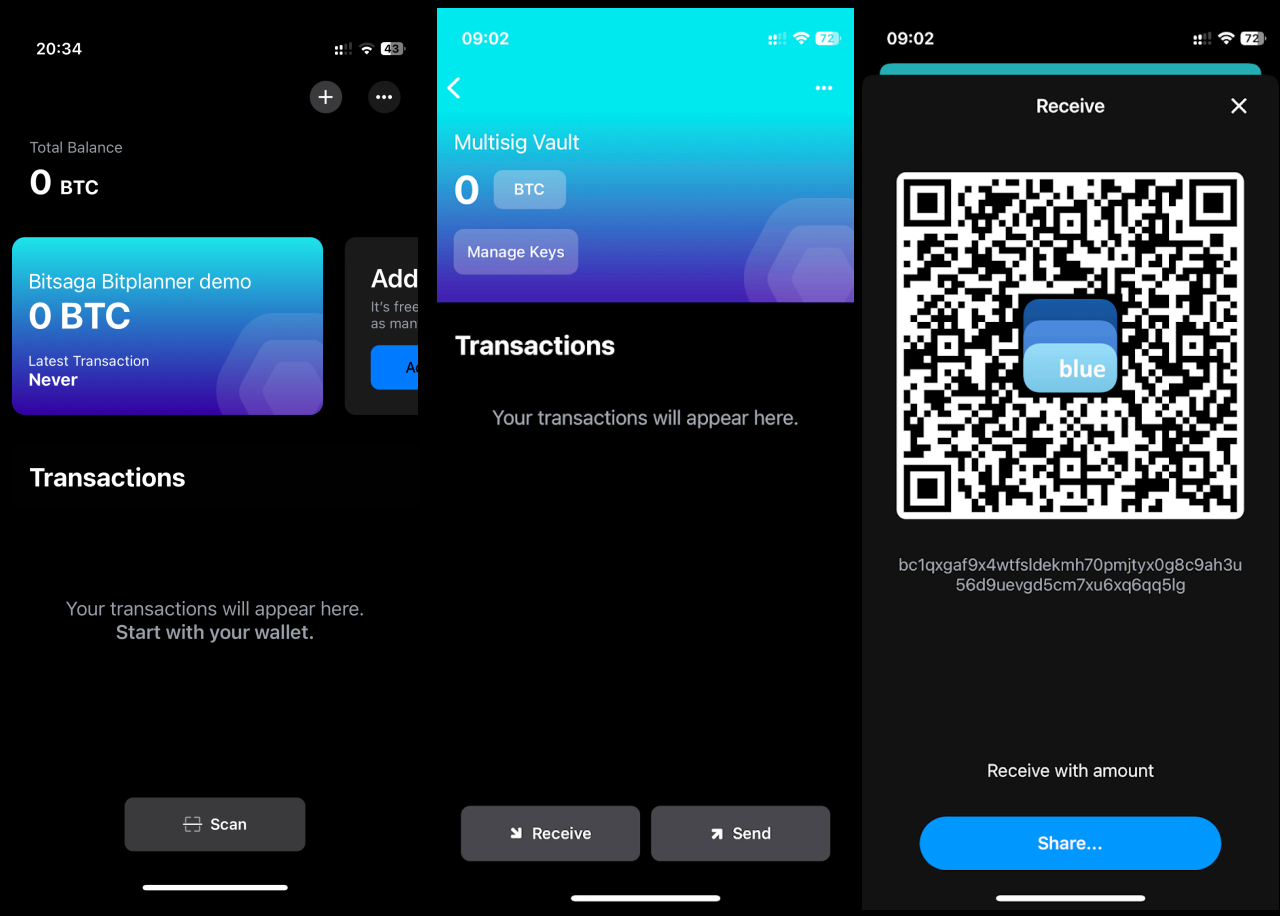
BITSAGA

Let’s walk the talk

- Create MS wallet ✓
- Add keys ✓
- Send and receive
- Backup and restore

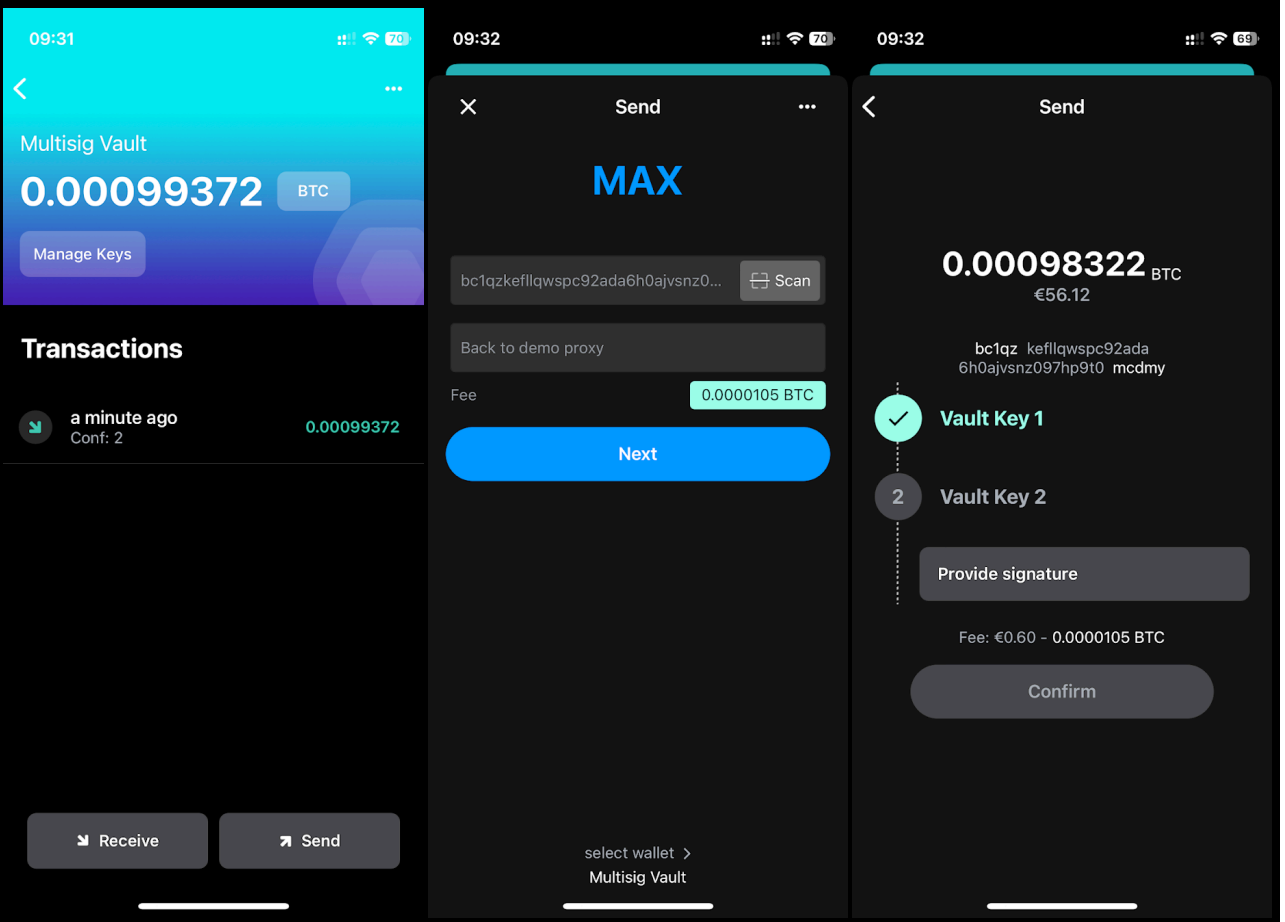
BITSAGA

Multi-sig wallet receive



BITSAGA

Multi-sig wallet send: sign with hot key

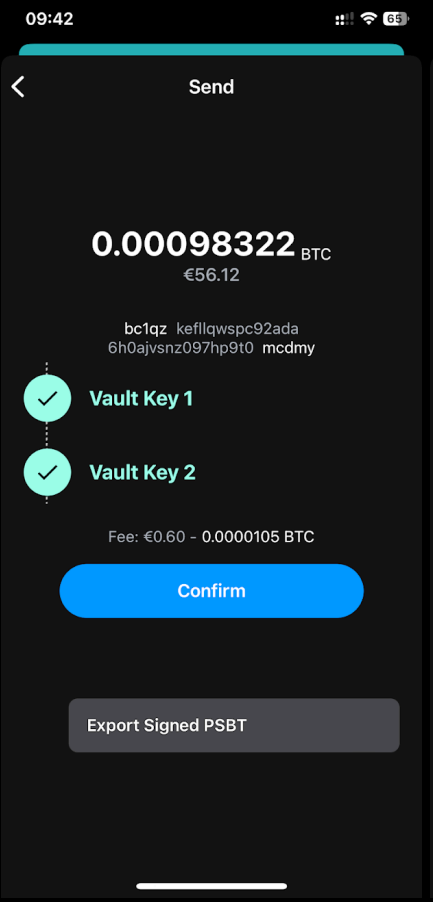


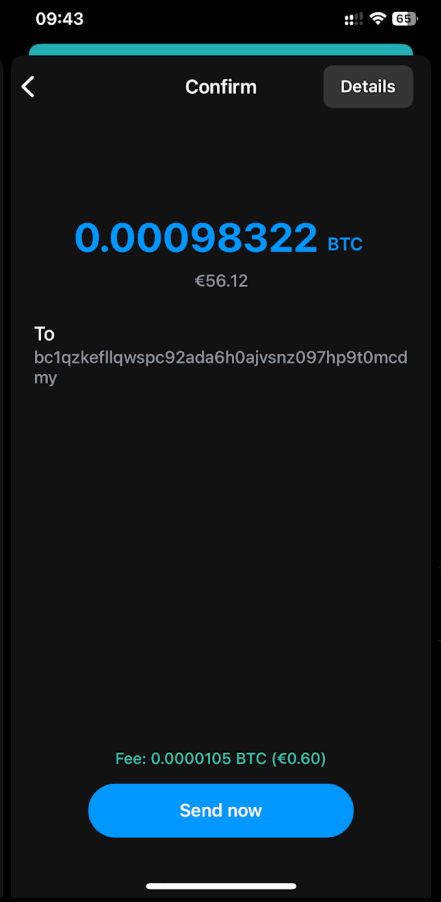
BITSAGA

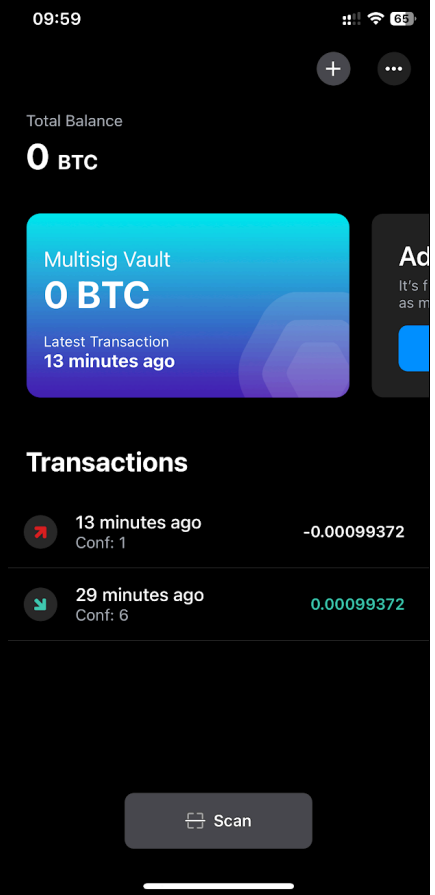
Multi-sig wallet send: sign with cold key

BITSAGA

Multi-sig wallet confirm send







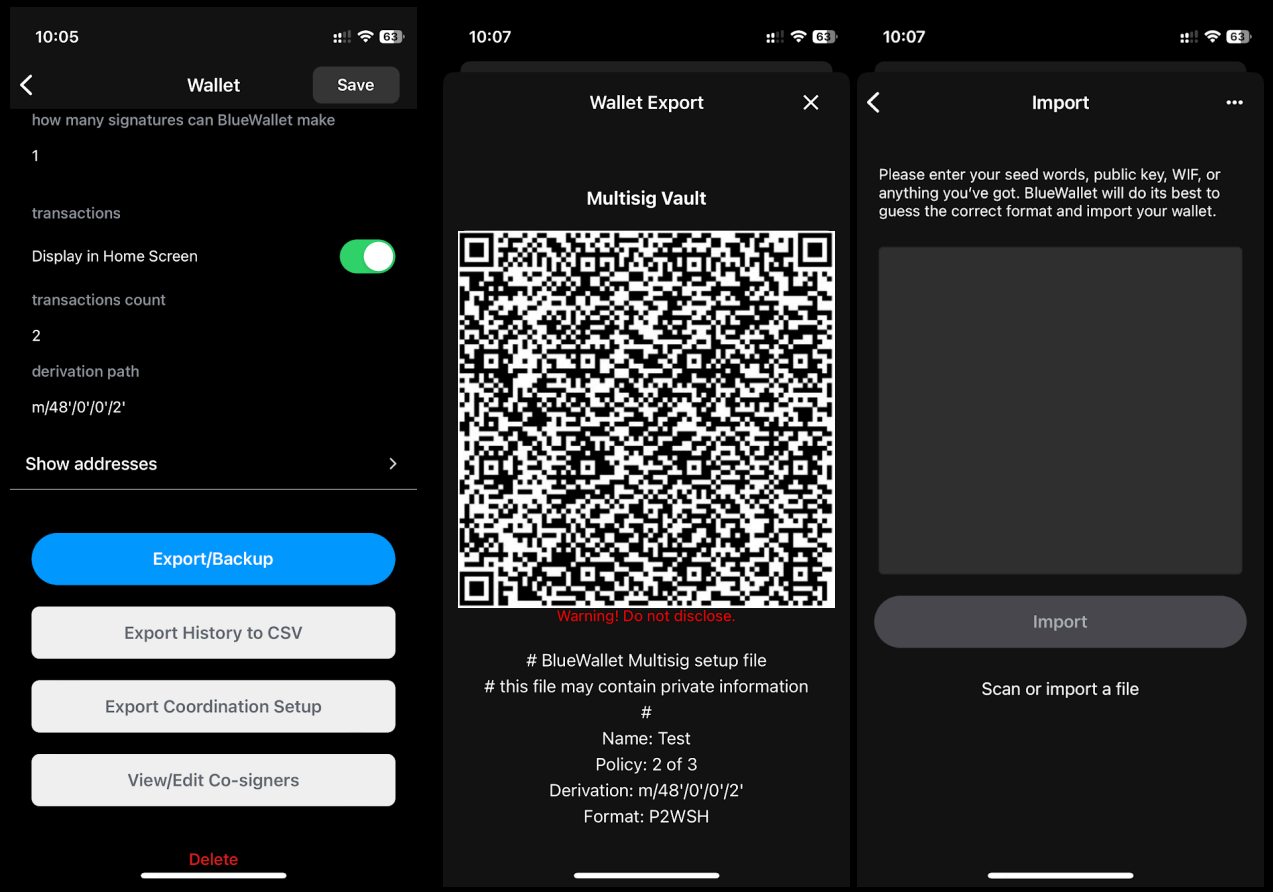
BITSAGA

Let’s walk the talk

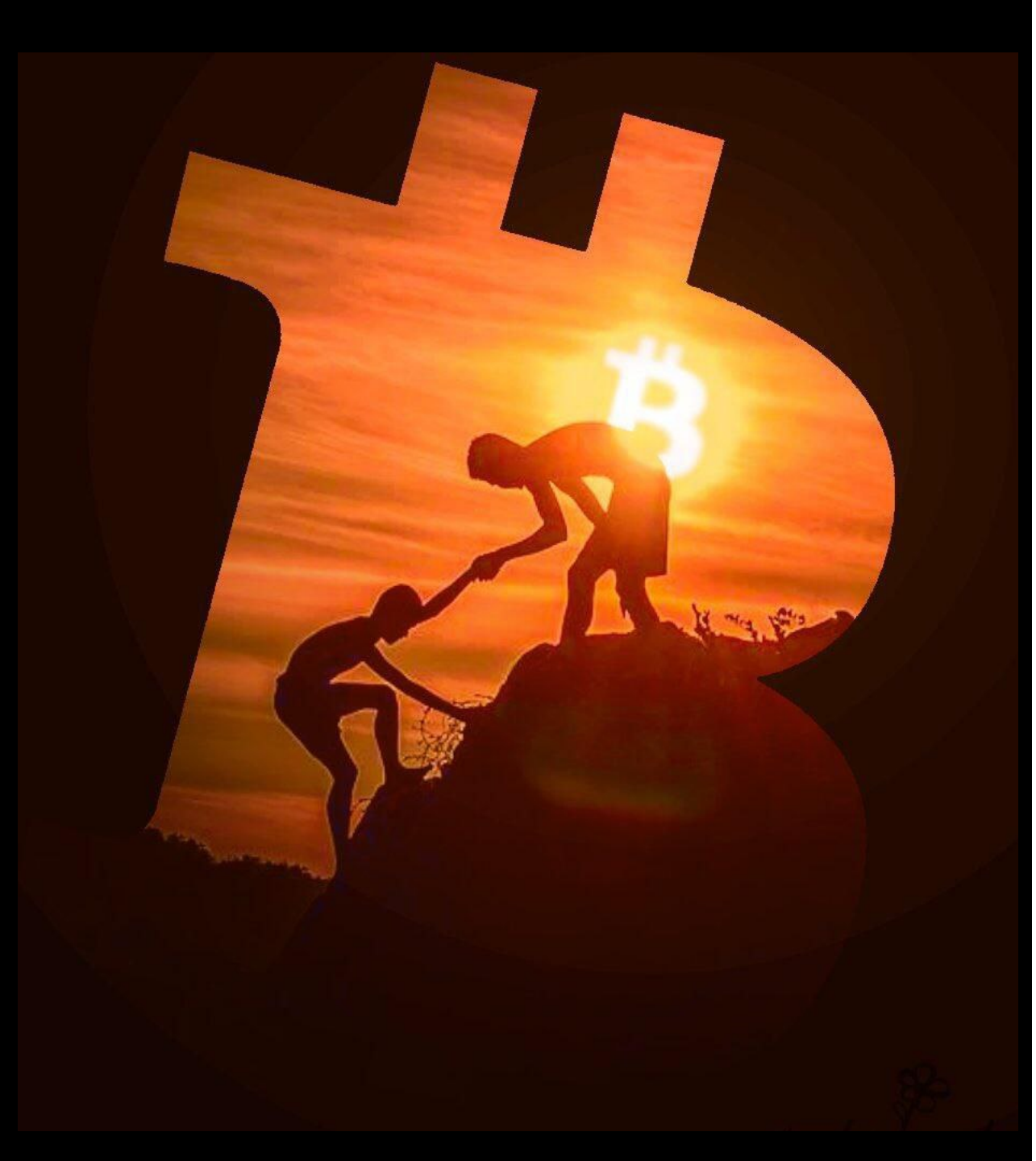
- Create MS wallet ✓
- Add keys ✓
- Send and receive ✓
- Backup and restore

BITSAGA

Multi-sig wallet backup



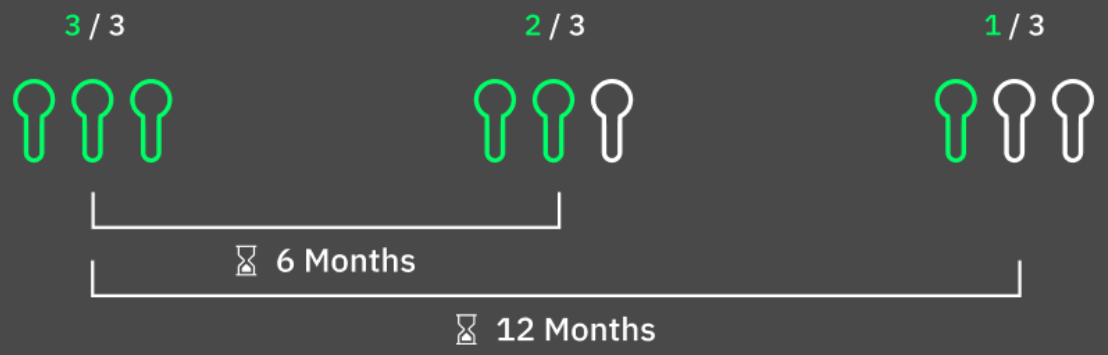
BITSAGA



- Many changes in multi-sig past years
- Still advanced but way more accessible
- Learn, practice & start small

BITSAGA

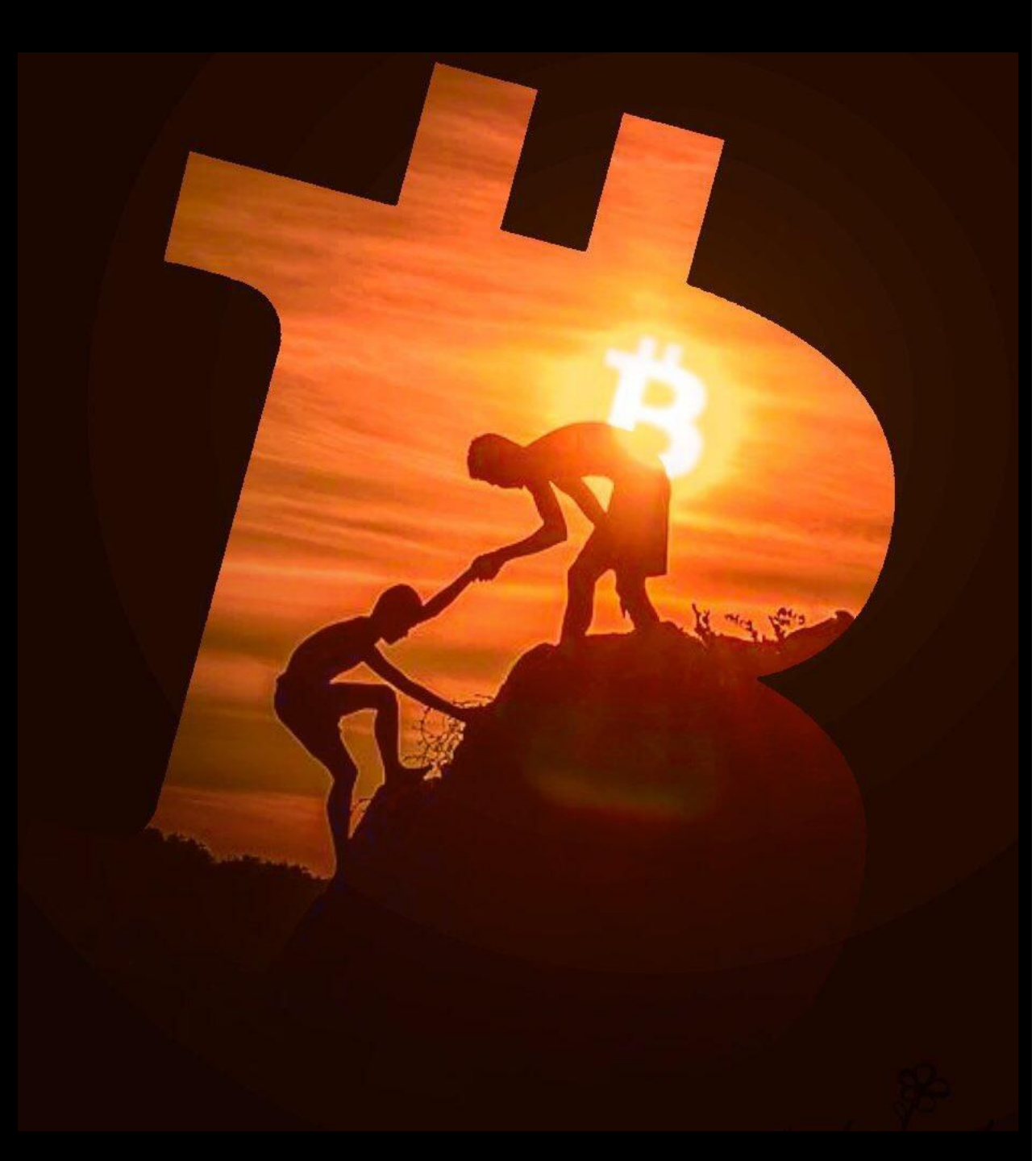
Liana



Advanced multi-sig

- Expanding multi-sig
- Decaying multi-sig
- Timelocked keys

BITSAGA



Thank you for your attention!

Questions?

rob@bitsaga.be

BITSAGA