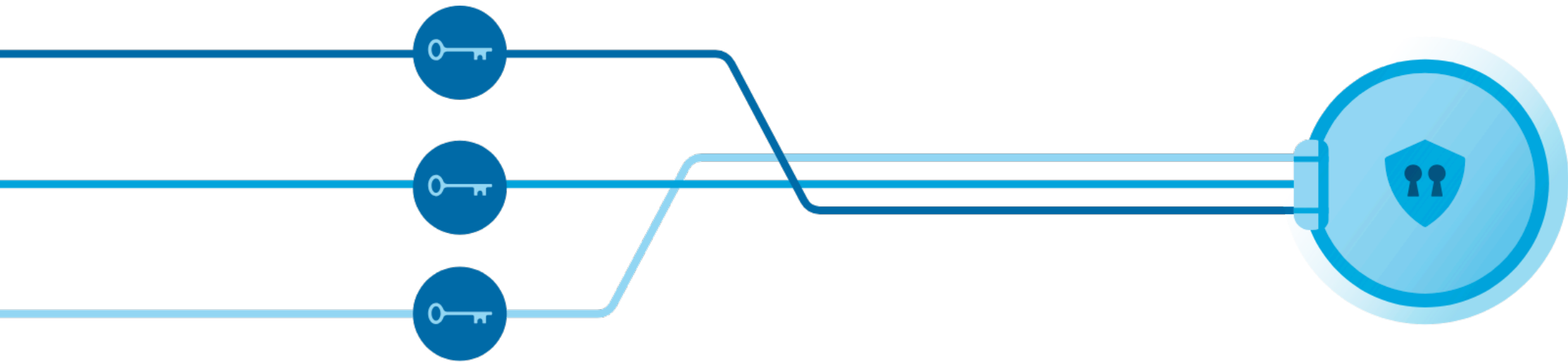


🔑 multi-sig

from mystery to mastery





www.bitsaga.be



@BitsagaRob



@Bitsaga

WHOAMI

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



Multi-sig: mystery to mastery agenda

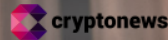
- ▶ Theoretical background
- ▶ Practical action
- ▶ Tools



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

*"Your keys, your Bitcoin.
Not your keys, not your Bitcoin."*

- Andreas M. Antonopoulos



No
wallet



Exchange
Wallet
(IOU)



Single-sig
cold
wallet

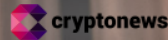
Inspired by Michael Flaxman - [btcguide.github.io](https://github.com/btcguide)

People worry about their bitcoin

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

**"Your keys, your Bitcoin.
Not your keys, not your Bitcoin."**

- Andreas M. Antonopoulos



No
wallet



Exchange
Wallet
(IOU)



Single-sig
cold
wallet



Multi-sig
cold
wallet

Inspired by Michael Flaxman - [btcguide.github.io](https://github.com/btcguide)

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

Bitcoin wallet types

Generally, 3 types of wallets

- ▶ Single signature
- ▶ Passphrase
- ▶ Multi signature

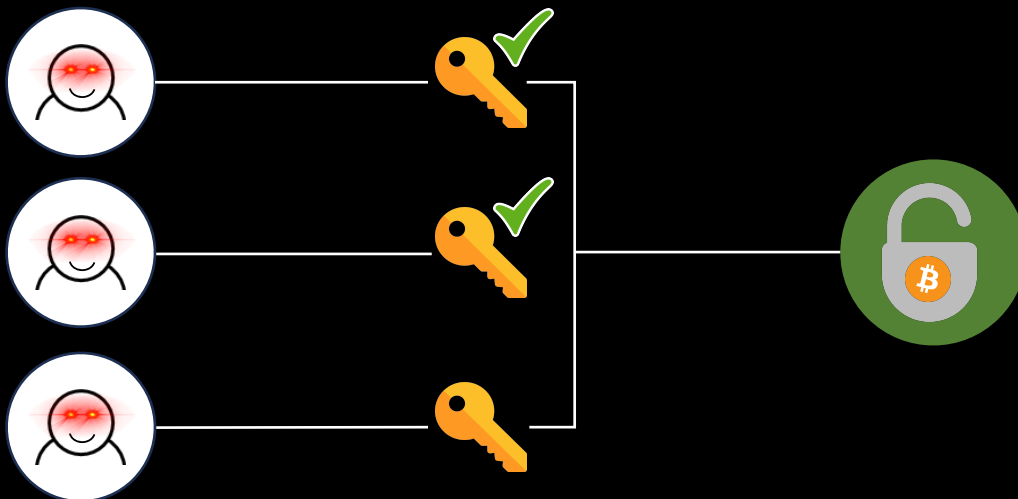
Single-sig wallet



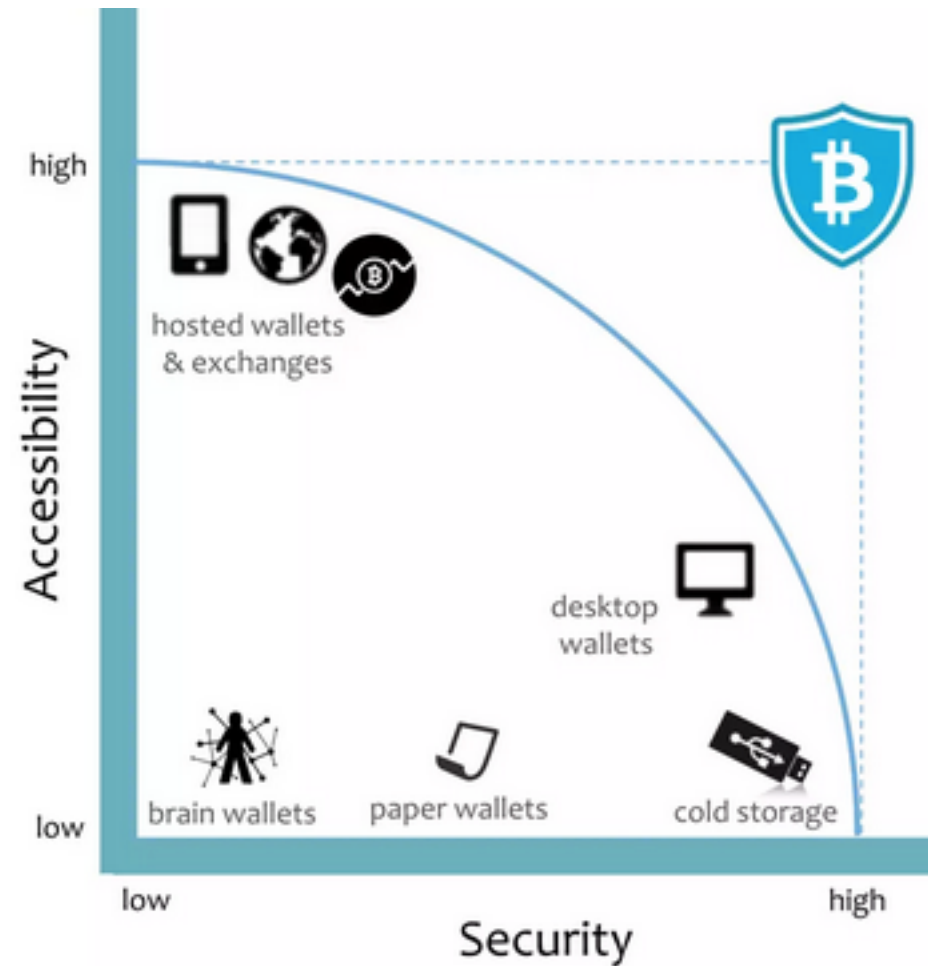
Single-sig passphrase wallet



Multi-sig wallet



single-sig



multi-sig

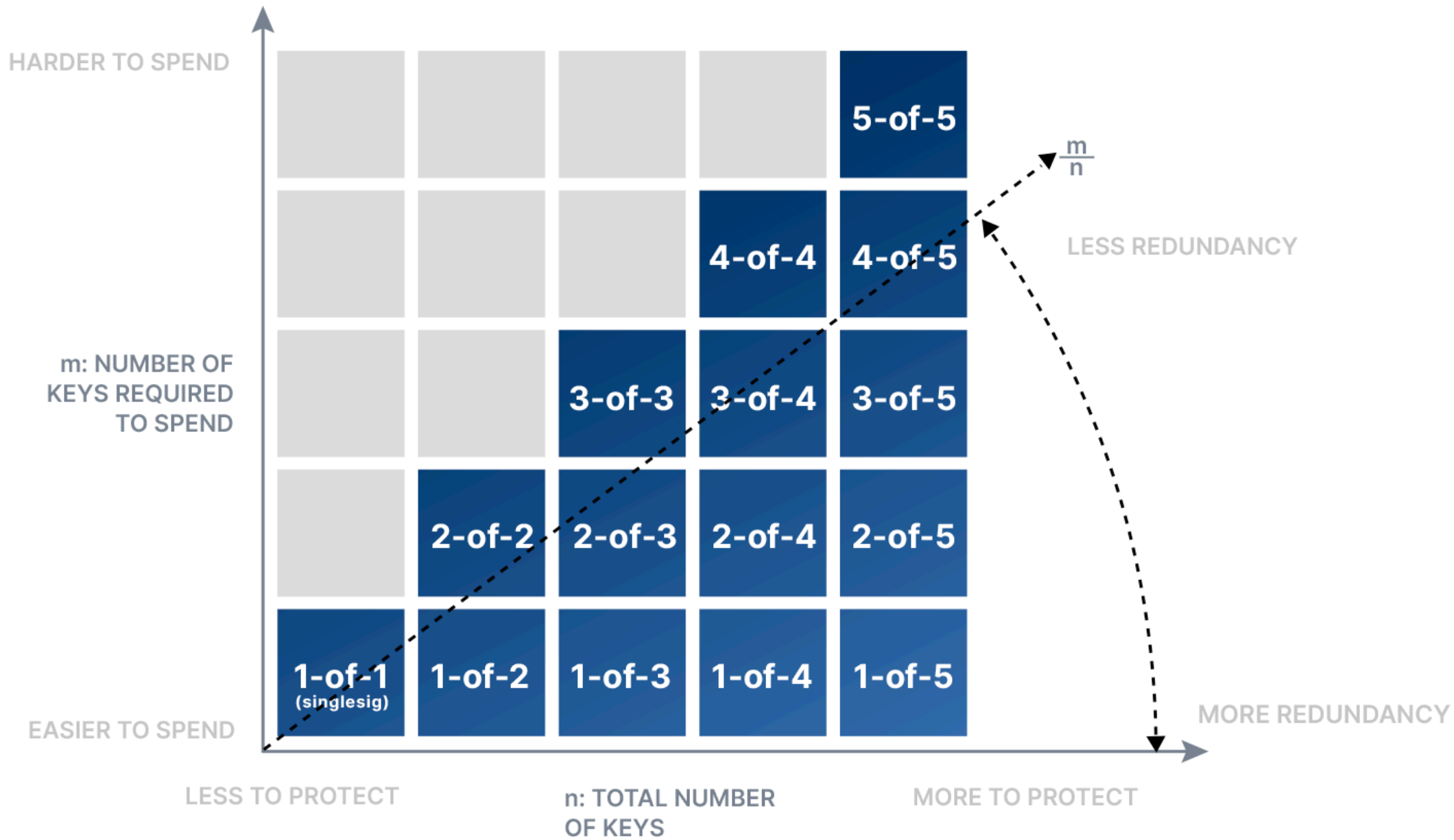
m

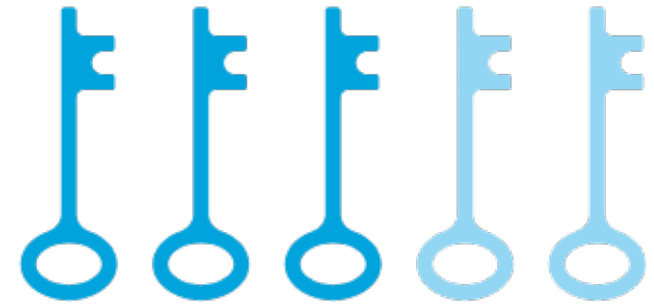
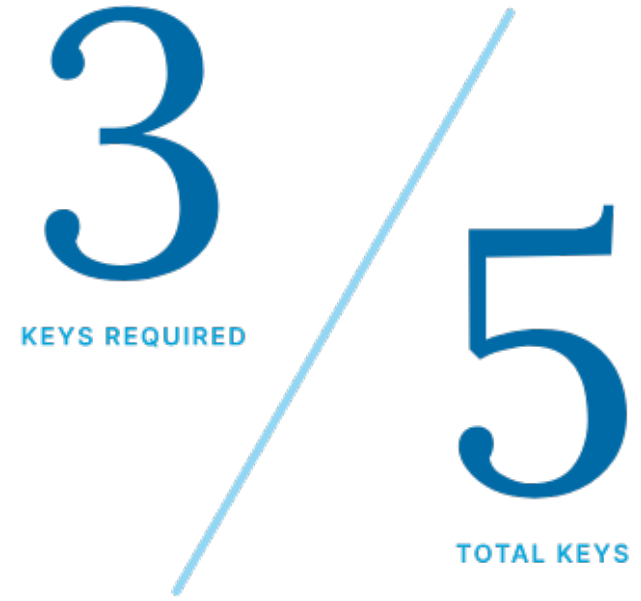
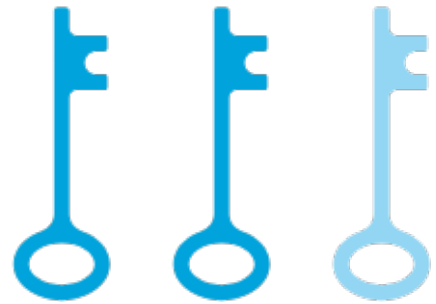
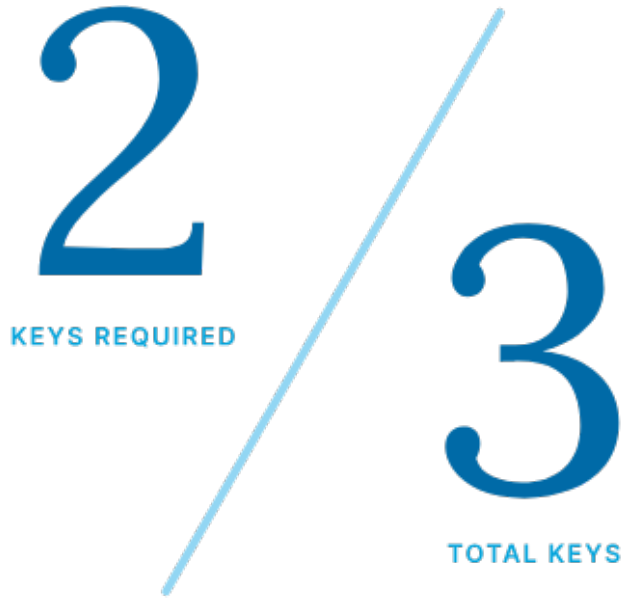
THE NUMBER OF KEYS
REQUIRED TO SIGN



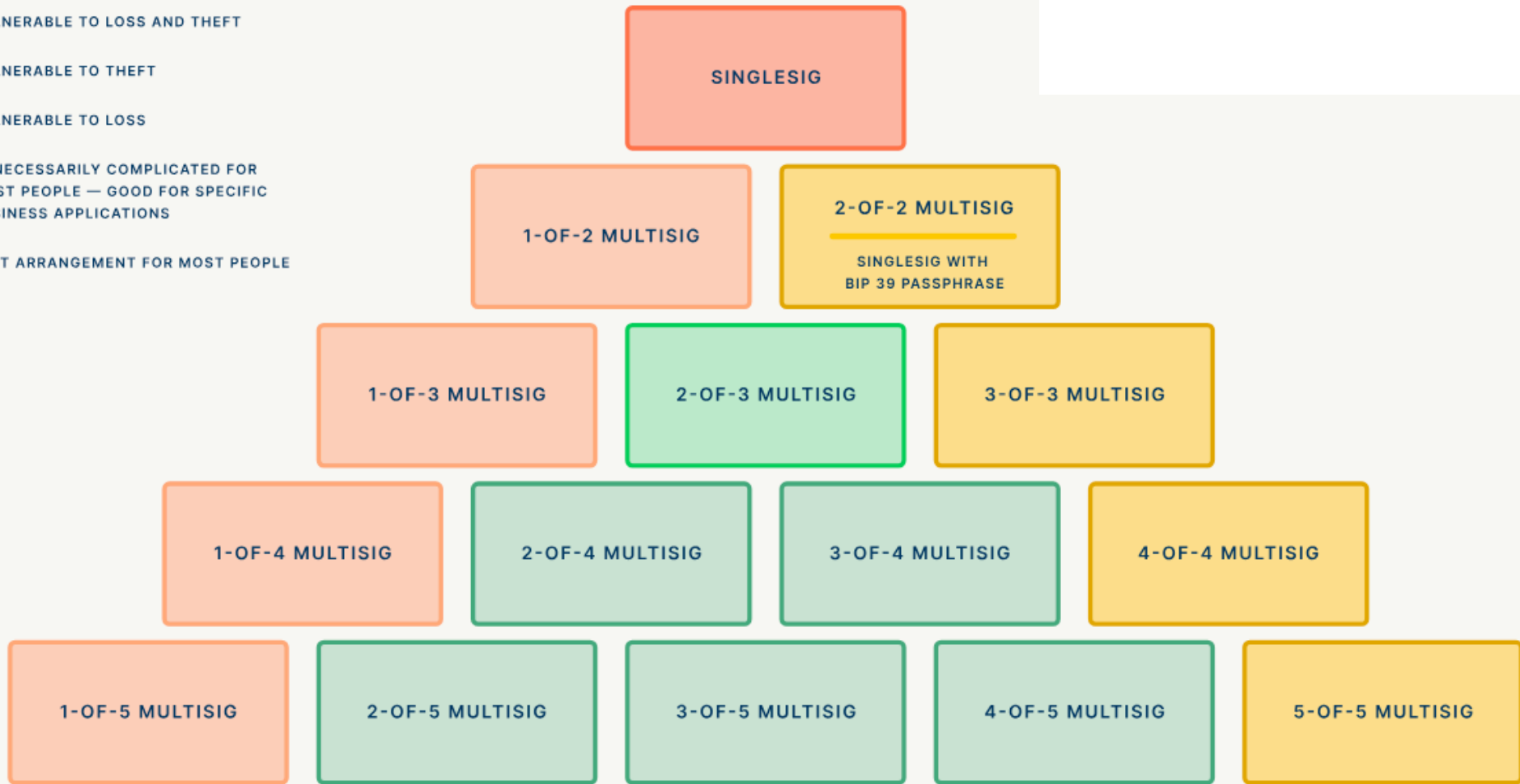
n

THE TOTAL NUMBER
OF 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



Fault tolerance

Single-sig wallet



Passphrase wallet



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)

Multi-sig wallet (2/3)



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

Single signature wallet

- ▶ Single points of failure
- ▶ Ways to mitigate

**Mitigating single-sig hardware risks
can be a challenge**

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

Single-sig software risks

```
clickHandler = function() {
  $this = $(this)
  $target = $($this.attr('data-target')) // st
  href.replace(/.*(?:#[^\s]+$)/, '') // st
  if ($target.hasClass('carousel')) return
  options = $.extend({}, $target.data(), {
    slideIndex: $this.attr('data-slide-to')
  })
  (slideIndex) options.interval = false
  Plugin.call($target, options)
  (slideIndex) {
    $target.data('bs.carousel')
  }
}
```

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

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

Multi-sig mitigates risks by design

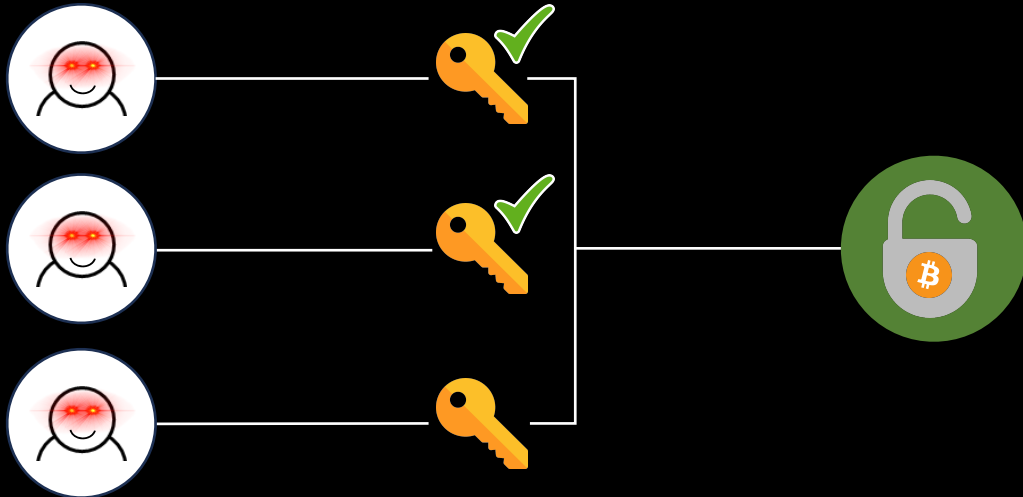
Physical risk protection

- ▶ 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



Output descriptor

Under the hood

Creating a 2-of-3 [P2SH multisig address](#)

```
bitcoin-cli -testnet createmultisig 2 ""
```

```
[  
  "mjbLRSidW1MY8oubvs4SMEnHNFxXCcoehQ",  
  "02ecd2d250a76d204011de6bc365a56033b9b3a149f679bc1720555d3c2b2854f",  
  "mt17cV37fBqZsnMmrHnGCm9pM28R1kQdMG"  
]"
```

Result

```
{  
  "address" : "2MyVxxgNBk5zHRPRY2iVjGRJHYZE1pMCSq"  
  "redeemScript" :  
  "522103ede722780d27b05f0b1169efc90fa15a601a32fc6c3295114500c586831b6aaf2102e  
cd2d250a76d204011de6bc365a56033b9b3a149f679bc1720555d3c2b2854f21022d609d2f  
0d359e5bc0e5d0ea20ff9f5d3396cb5b1906aa9c56a0e7b5edc0c5d553ae"  
}
```

```
bitcoin-cli -testnet decodescript 522103ede722780d27b05f0b1169ef  
c90fa15a601a32fc6c3295114500c586831b6aaf2102ecd2d250a76d204011de\  
6bc365a56033b9b3a149f679bc1720555d3c2b2854f21022d609d2f0d359e5b\  
c0e5d0ea20ff9f5d3396cb5b1906aa9c56a0e7b5edc0c5d553ae
```

```
{OP_CHECKMULTISIG,  
  "reqSigs" : 2,  
  "type" : "multisig",  
  "addresses" : [  
    "mjbLRSidW1MY8oubvs4SMEnHNFxXCcoehQ",  
    "mo1vzGwCzWqteip29vGWWW6MsEBREuzW94",  
    "mt17cV37fBqZsnMmrHnGCm9pM28R1kQdMG"  
  ],  
  "p2sh" : "2MyVxxgNBk5zHRPRY2iVjGRJHYZE1pMCSq"  
}
```


Output descriptor


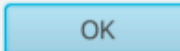
Backup Multisig Wallet?

To restore this multisig wallet, you need at least 3 seeds and ALL of the xpubs! For the xpubs, it is recommended to backup either this wallet file, or the wallet output descriptor.

The wallet output descriptor contains all 5 of the xpubs and is shown below. Alternatively, use the Export button below to export the Sparrow wallet file.

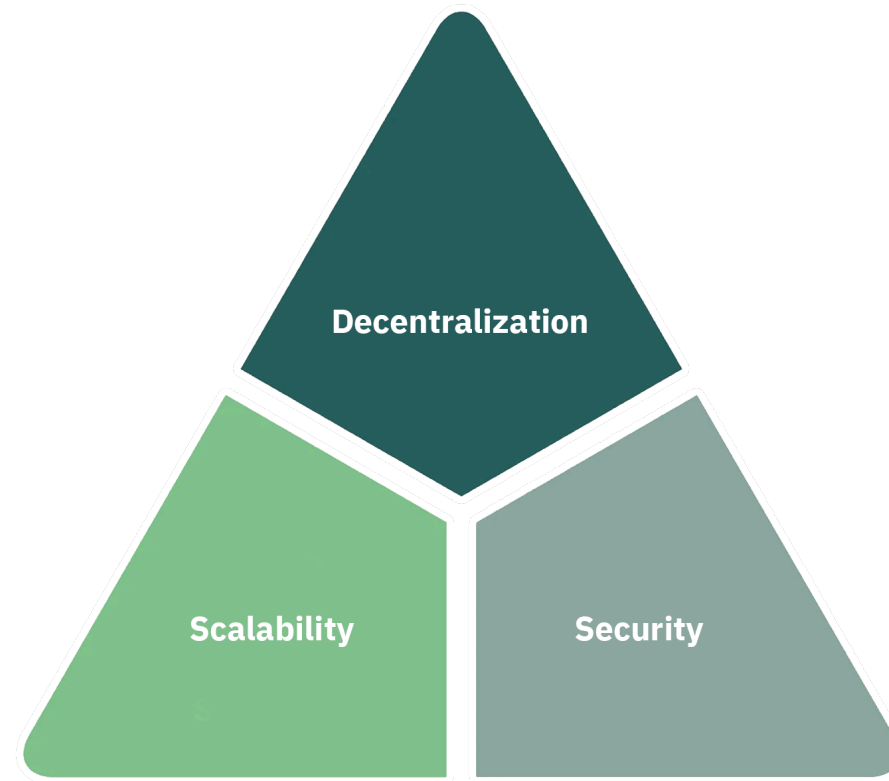
```
wsh(sortedmulti(3, [6a5d3282/48h/0h/0h/2h]xpub6Emrd6k7HTbpcjZWPCcnB9rKTuwkamz4hhPkpdn
bDxkXt7Wa1CjgJU8yDV7PEg9aKbjye7BQ6Zbc7PX2GdYF3YPV4wztm5Rsn3oDnvveZ3k/<0;1>/*, [1c1a83
71/48h/0h/0h/2h]xpub6F8sRsUQ7UbcAiL4ZYCttWE5nkiGCDxkpHKWpReqTEbdwEm8jYPTxQyGR4deEjvo
3GZfcNNawwGaiJghN9hD5TVpQq8dXwLdK7VgLhMjp8f/<0;1>/*, [126cf4f5/48h/0h/0h/2h]xpub6DhcE
qqABkyVT7aaQgKScVWws8Zn1XuJNeK22g18yqbEi7sp5uFJxvNVHxcBBQdEthJQSEBRcuJtyFofcCxySmoBY
zQFoM9YKMWqp3bi4VU/<0;1>/*, [9fa5d00b/48h/0h/0h/2h]xpub6EafjeXfzWnK3csfUxFpRRC2kWacvV
KNPYMDP7gjqUmnyXaiYXCswfZsGmsfAsCsZuUci1ULttHTVP6bC1gS5ysncUbnRX9GoydDpDYHW3r/<0;1>/
*, [df0c9c49/48h/0h/0h/2h]xpub6EfXHm8eKkzPZSxSnDvKRmiJPuwanNXCWgjbccs4wbkpX7Yg4AWje6
JTPtqNtrEAUybpUc1YgVh51smzEVc9PqSbVpoStLitqPW6ikropc/<0;1>/*))#4u0gt07q
```



 Save PDF...  OK



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



Multi-sig: hardware

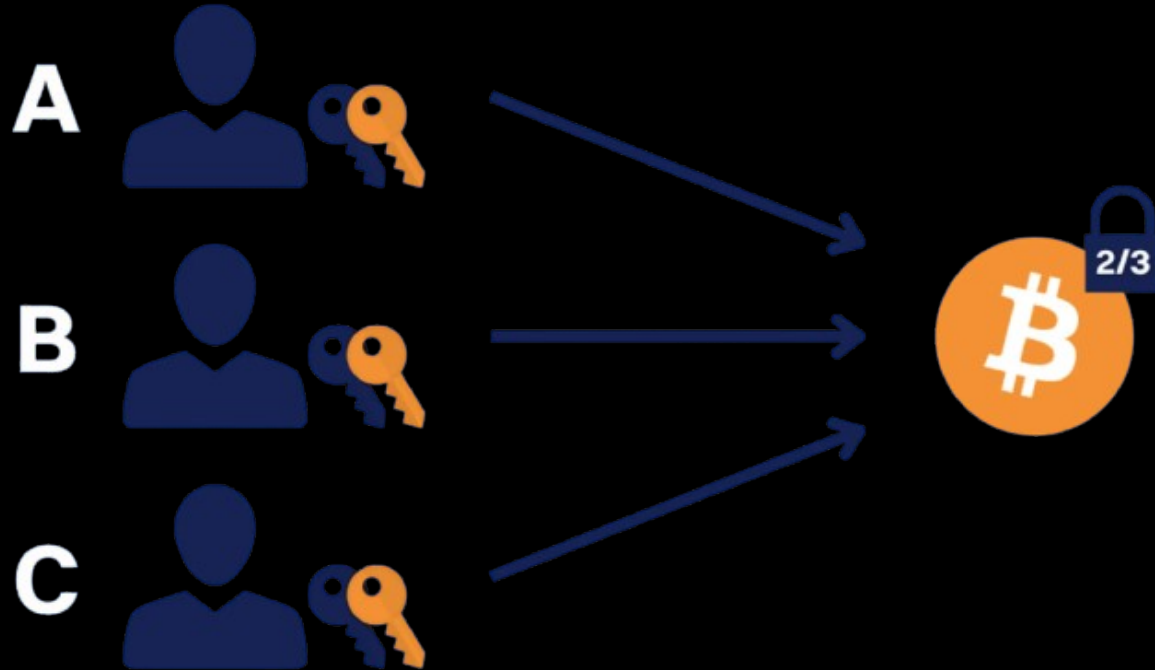
- ▶ Airgapped devices
- ▶ QRs = game changer
 - Transaction (PSBT - BIP174)
 - Address
 - Seed

New hardware has simplified multi-sig



Let's walk the talk

Multi-sig: mastery



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

Multi-sig: Blue



20:29

45



Wallets

Add a wallet

It's free, and you can create as many as you like.

Add now

Transactions

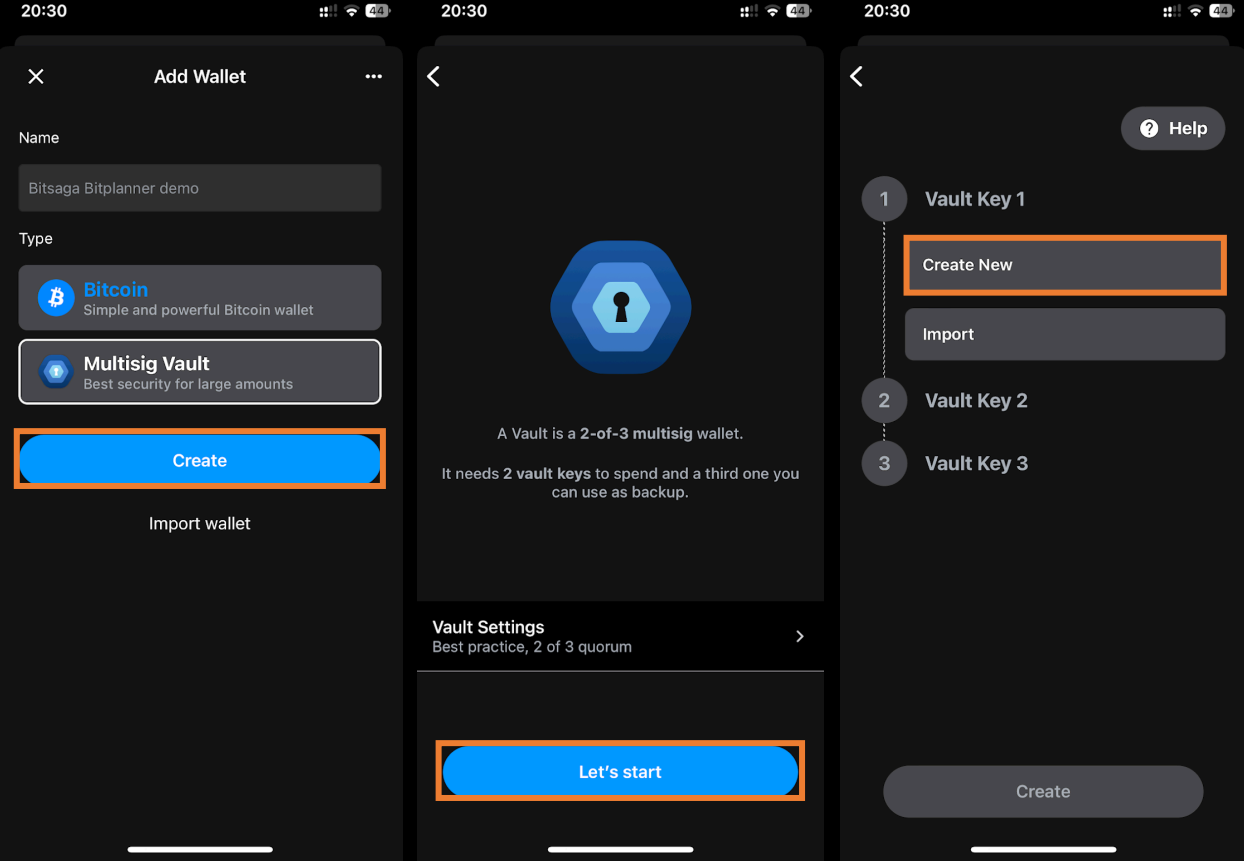
Your transactions will appear here.
Start with your wallet.

Scan

Multi-sig: Blue



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



Add multi-sig wallet key 2 (cold)



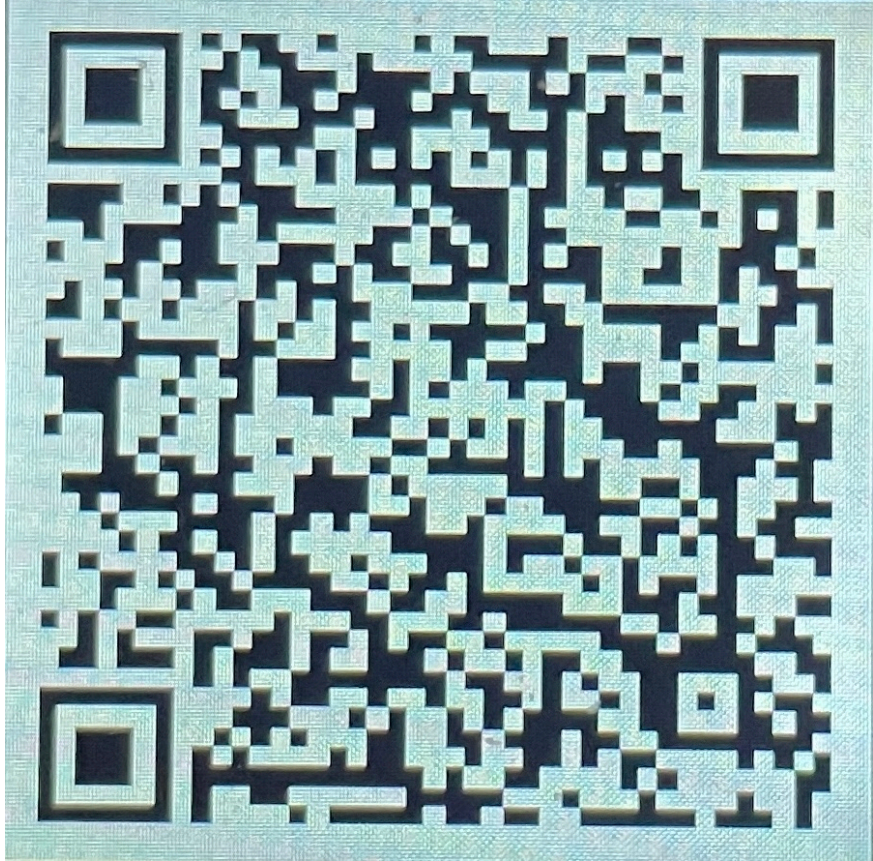
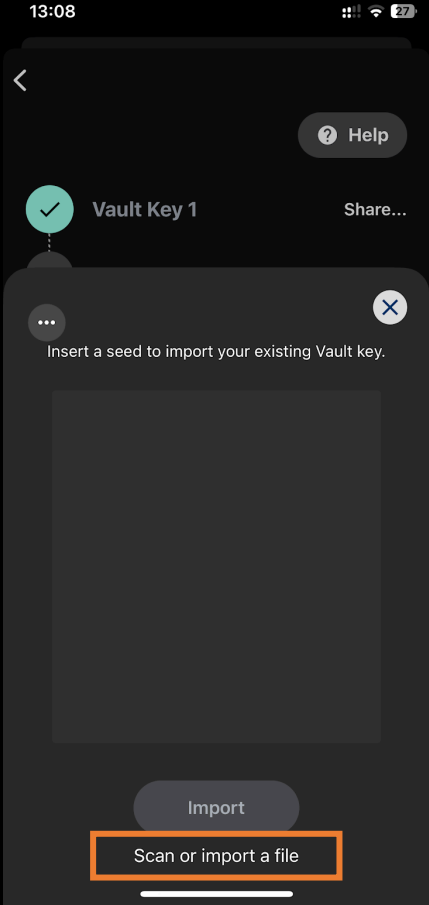
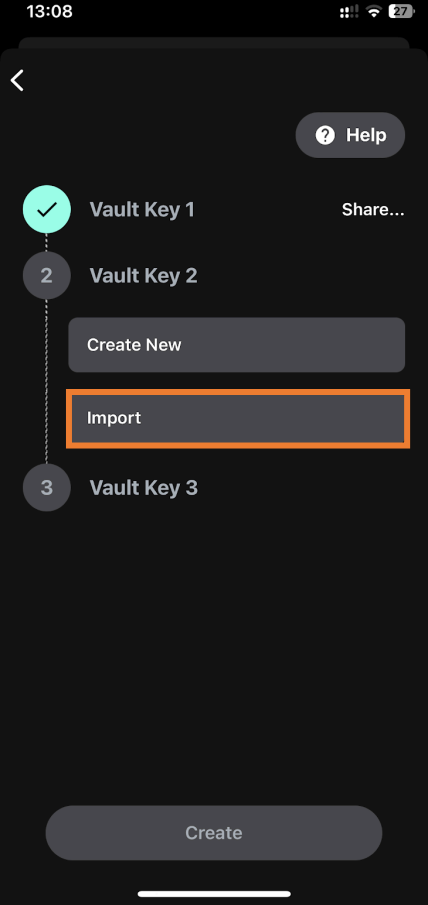
Add multi-sig wallet key 2 (cold)



Add multi-sig wallet key 2 (cold)



Scan Xpub QR to add key 2



Add multi-sig wallet key 3 (cold)



Add multi-sig wallet key 3 (cold)



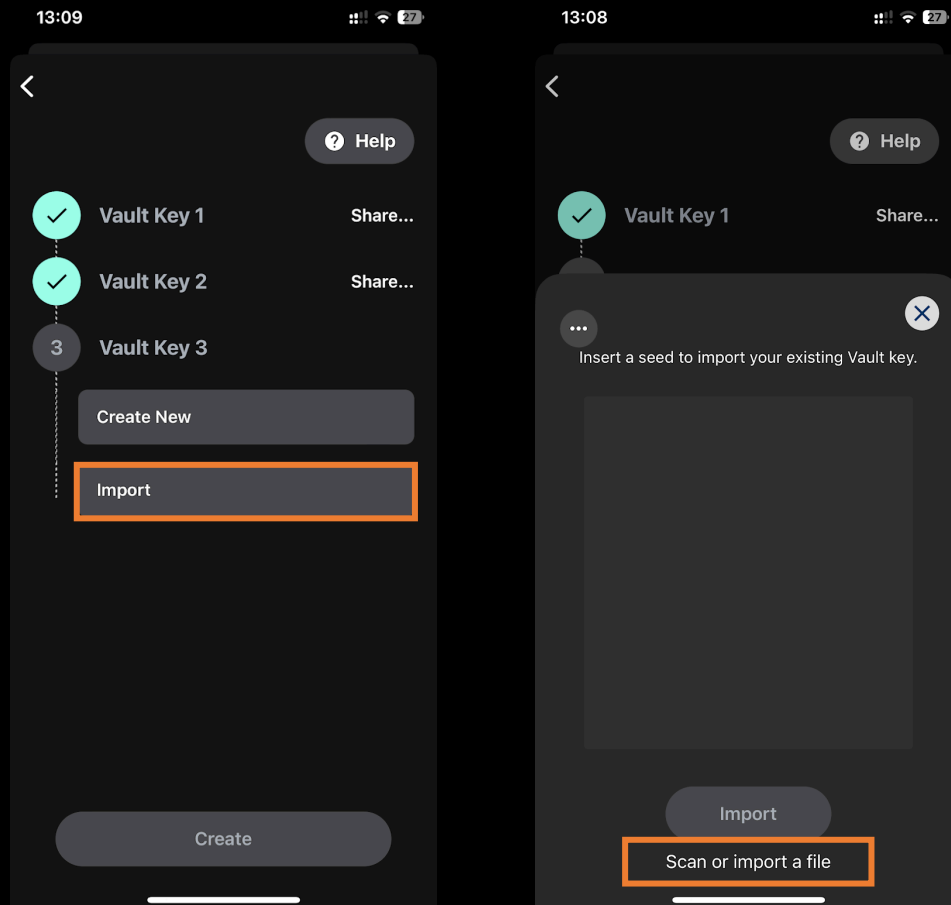
Add multi-sig wallet key 3 (cold)



Add multi-sig wallet key 3 (cold)



Scan Xpub QR to add key 3





Help



Vault Key 1

Share...



Vault Key 2

Share...



Vault Key 3

Share...

Create

Multi-sig wallet keys added

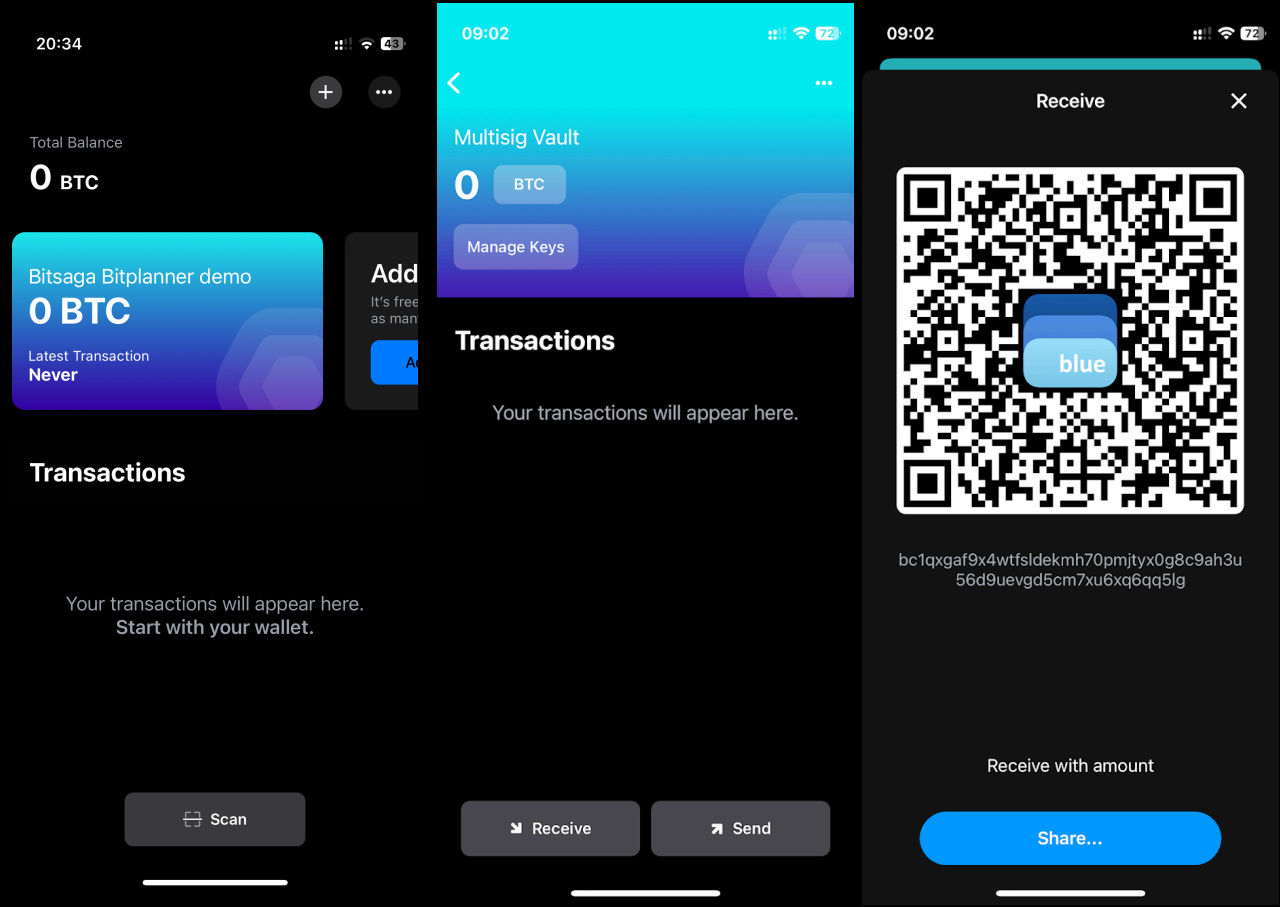


Let's walk the talk

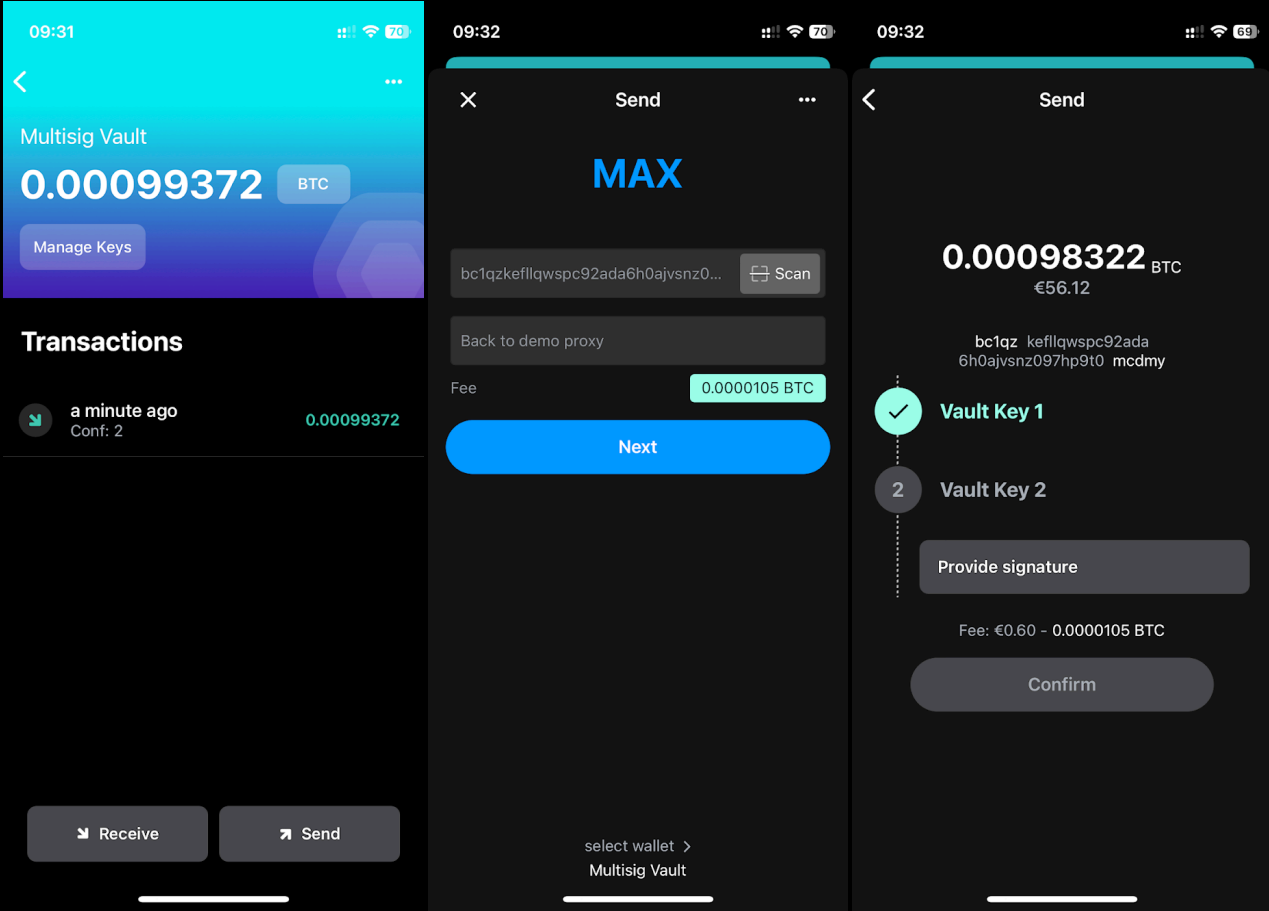
- ▶ Create MS wallet
- ▶ Add keys
- ▶ Send and receive
- ▶ Backup and restore



Multi-sig wallet receive



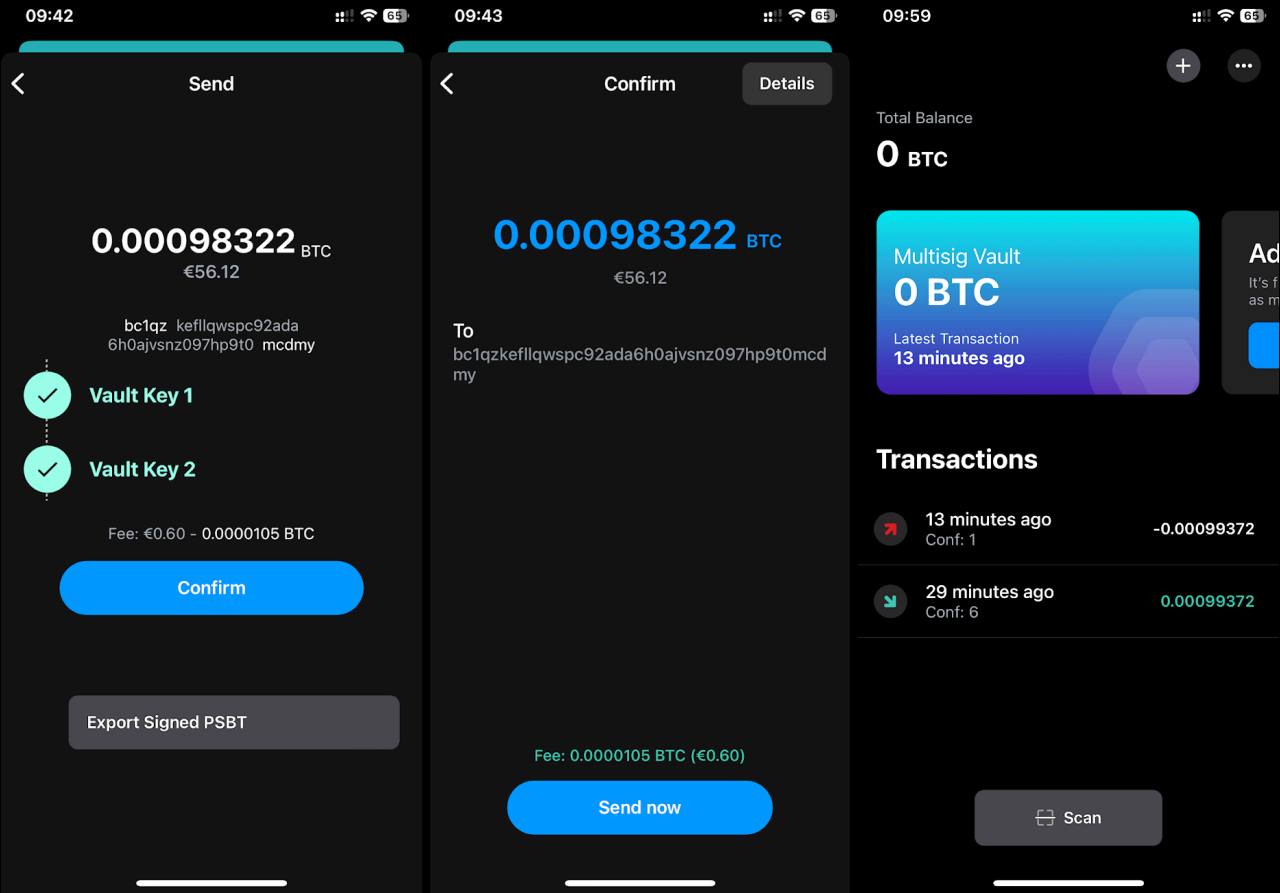
Multi-sig wallet send: sign with hot key



Multi-sig wallet send: sign with cold key



Multi-sig wallet confirm send

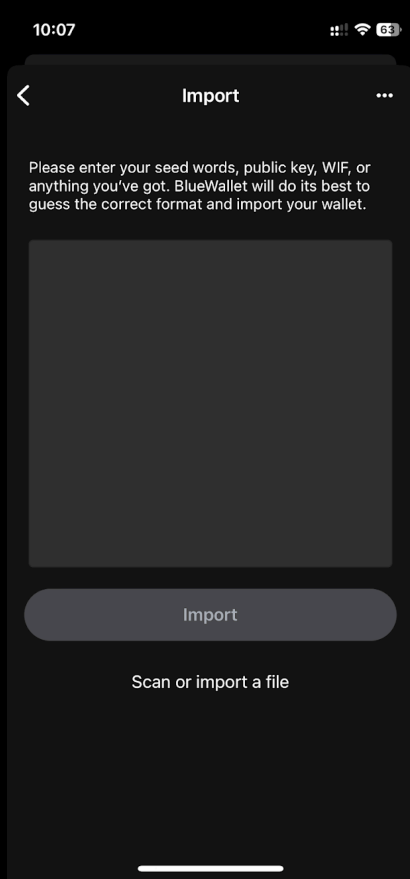
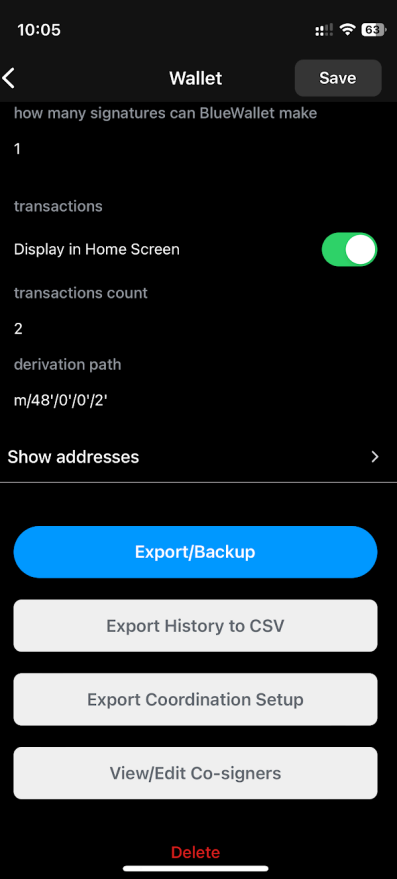


Let's walk the talk

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



Multi-sig wallet backup

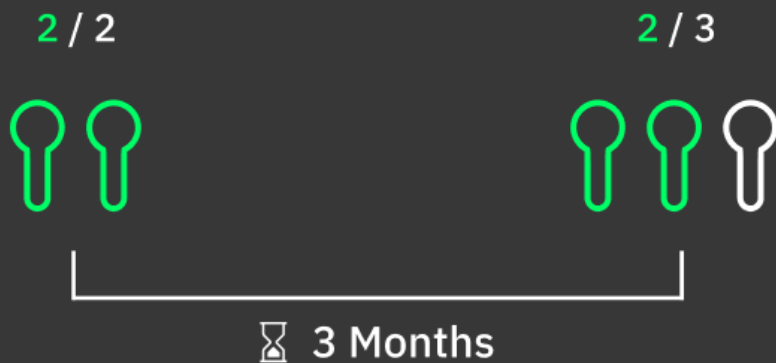
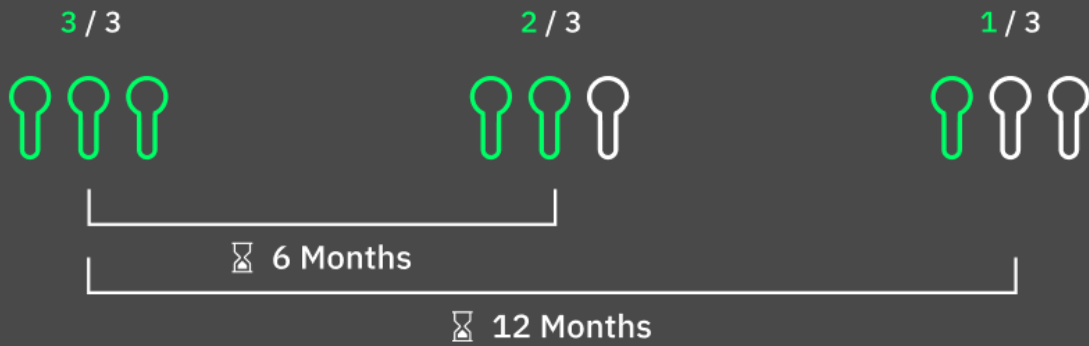




- ▶ Many changes in multi-sig past years
- ▶ Still advanced but way more accessible
- ▶ Learn, practice & start small



Advanced multi-sig



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

Thank you for your attention!

Questions?

rob@bitsaga.be

