Let’s learn about *bitcoin*

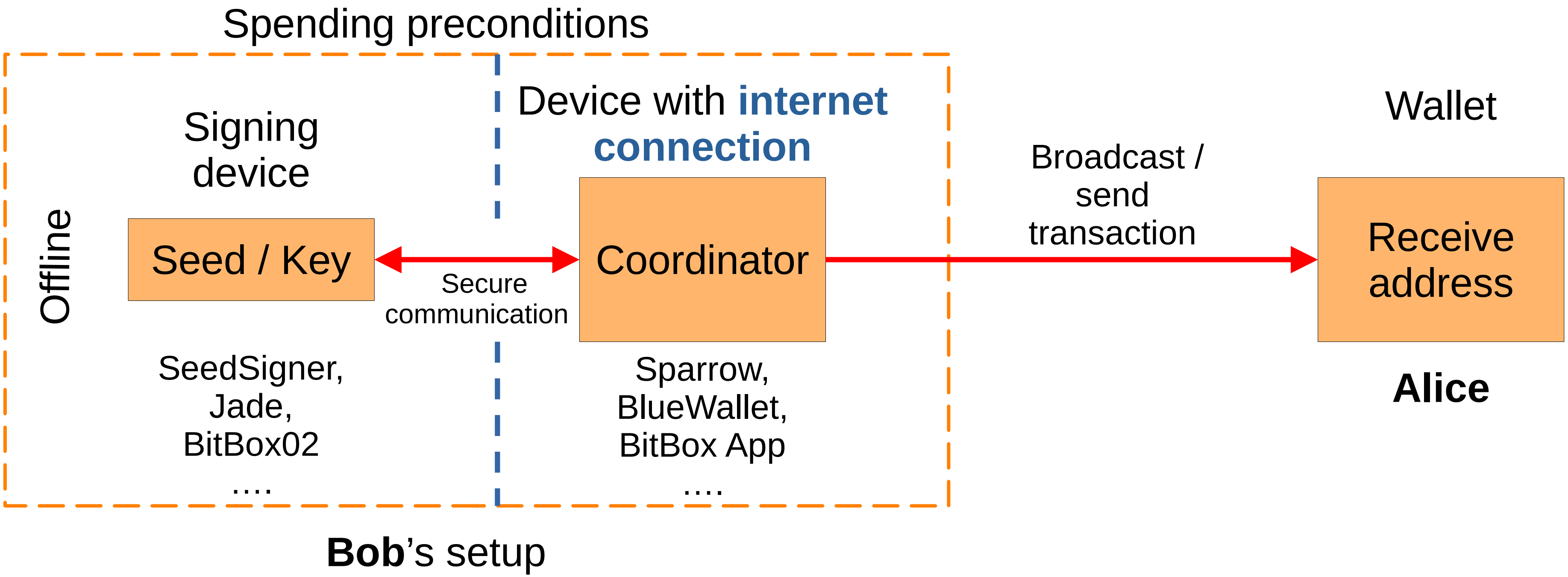
Multisig basics

bitcoin beach
TRAVEMÜNDE

Introduction

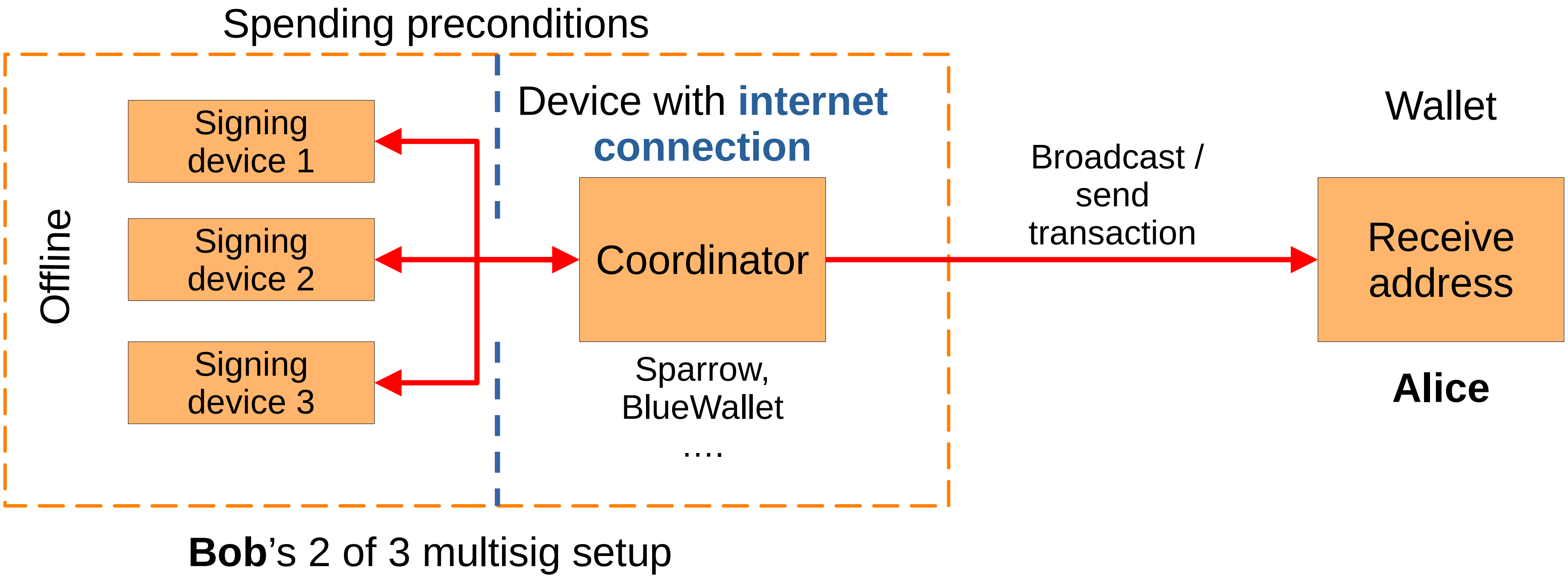
- Not an expert
- Have fun
- Ask questions
- Share your knowledge
- **Don’t trust, verify!**

Singlesig

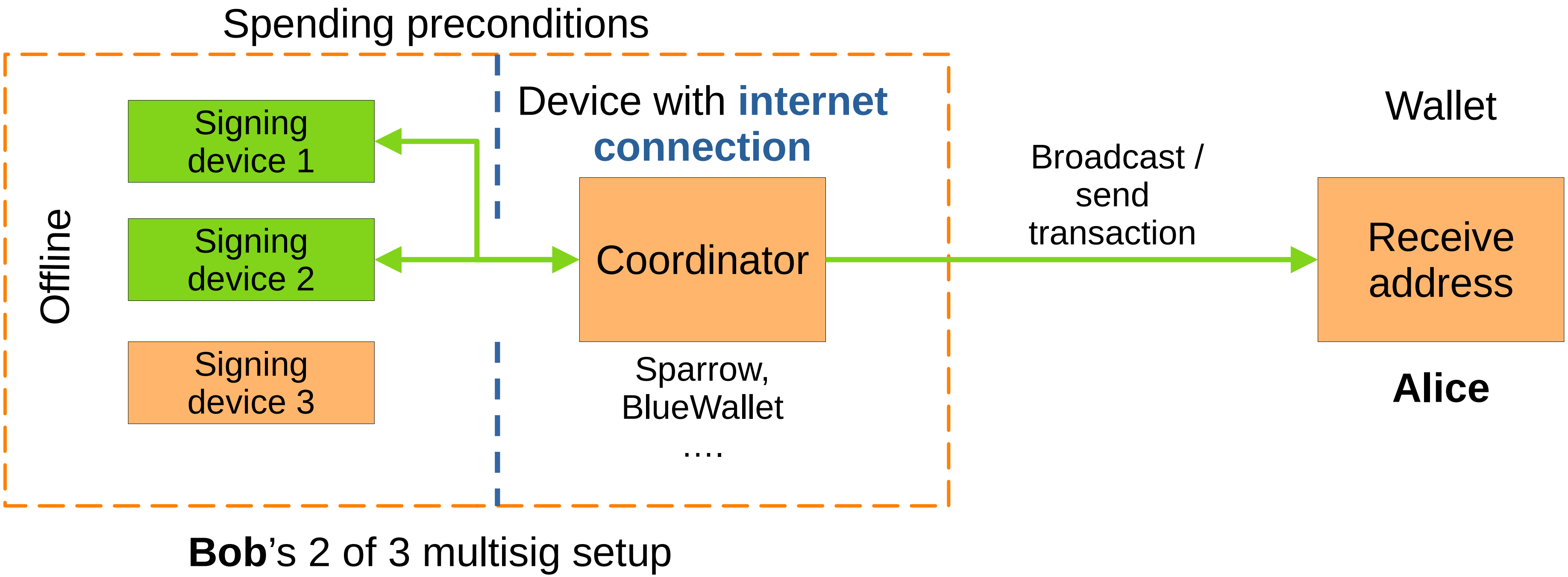


Spending preconditions
Signing device
Offline
Seed / Key
Secure communication
SeedSigner, Jade, BitBox02 ....
Device with **internet connection**
Coordinator
Sparrow, BlueWallet, BitBox App ....
Bob’s setup
Broadcast / send transaction
Wallet
Receive address
Alice

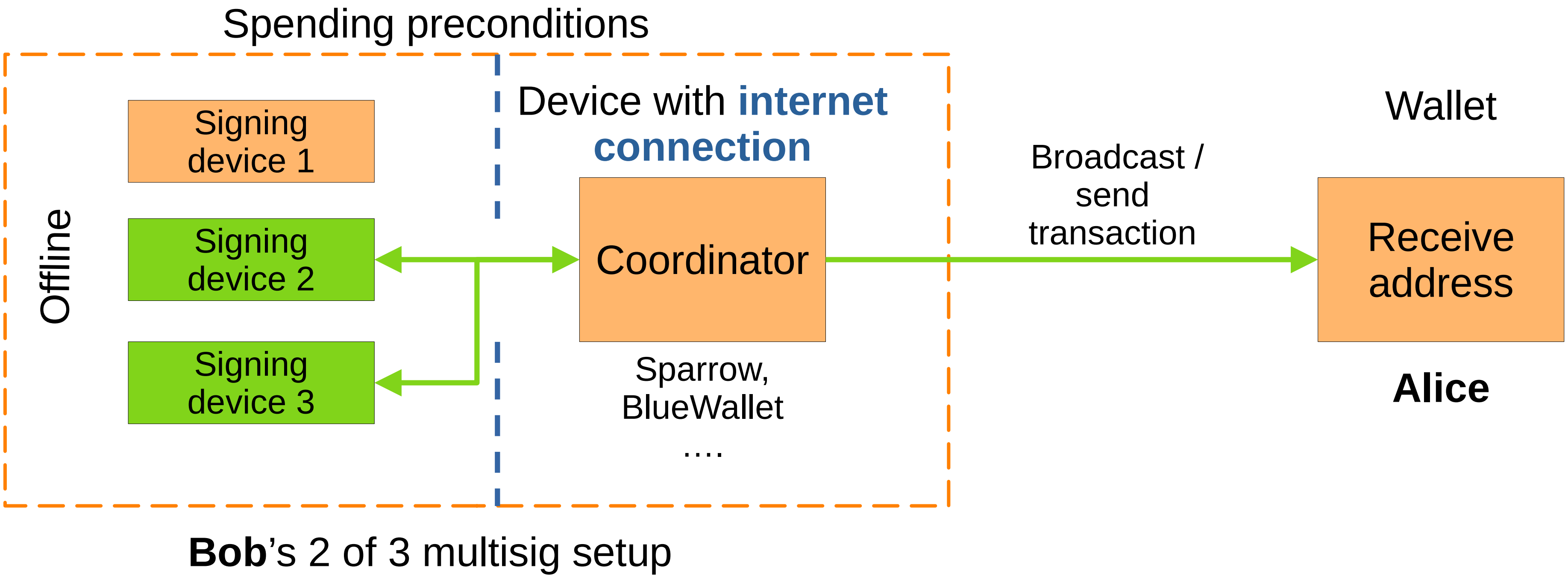
Multisig (m of n)



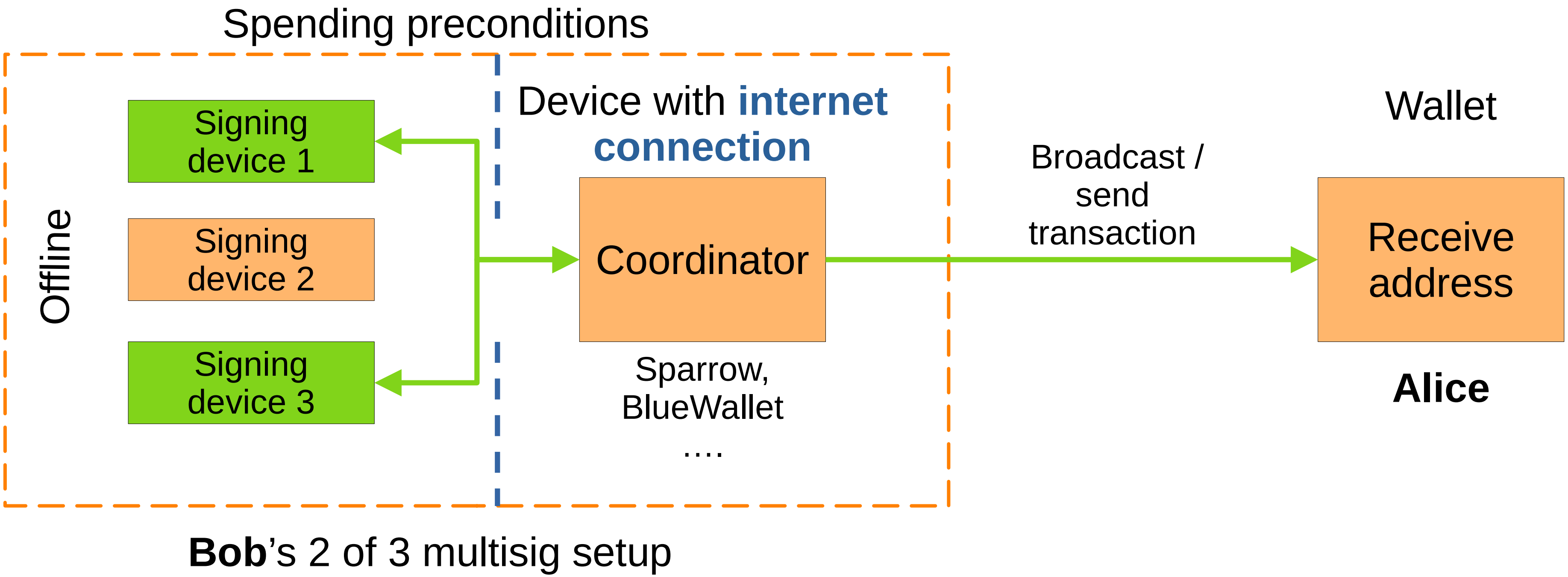
Multisig (m of n)



Multisig (m of n)



Multisig (m of n)



Multisig risks

- More backups

  A backup of all public keys (store the “wallet descriptor” with each backup)

- More devices
- More complicated – can your kids operate a 2 of 3 multisig?

Multisig benefits

- “No single point of failure”
- If one seed is compromised, the others are still usable
- Multiple people (m of n) can manage one wallet
- Use of several different hardware wallets

Hardware signing devices

- SeedSigner
- Jade
- Passport
- BitBox02
- Coldcard

Software

- Sparrow Wallet
- Specter Wallet
- BlueWallet (mobile only) - not for all multisig setups

Backup (m of n)

- Store every seed phrase + wallet descriptor
- Learn how to recover your wallet (signers and coordinator)
- think of your **family** and keep things **simple**

Partially Signed Bitcoin Transactions (PSBTs)

- Increases interoperability between different software and hardware wallets
- Portable - a transaction can be signed by multiple parties

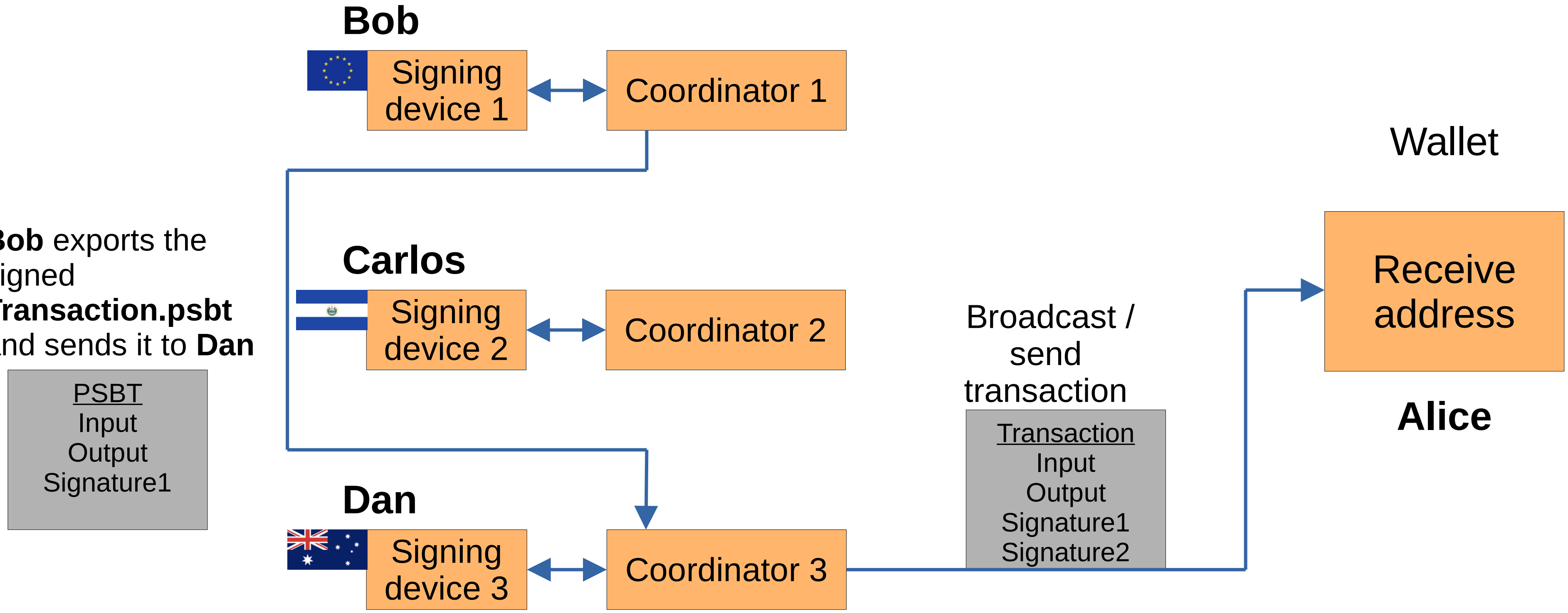
PSBT

Input

Output

Signatures (m of n)

Partially Signed Bitcoin Transactions (PSBTs)



Bob

Signing device 1

Coordinator 1

Carlos

Signing device 2

Coordinator 2

Dan

Signing device 3

Coordinator 3

Bob exports the signed **Transaction.psbt** and sends it to **Dan**

PSBT
Input
Output
Signature1

Broadcast / send transaction

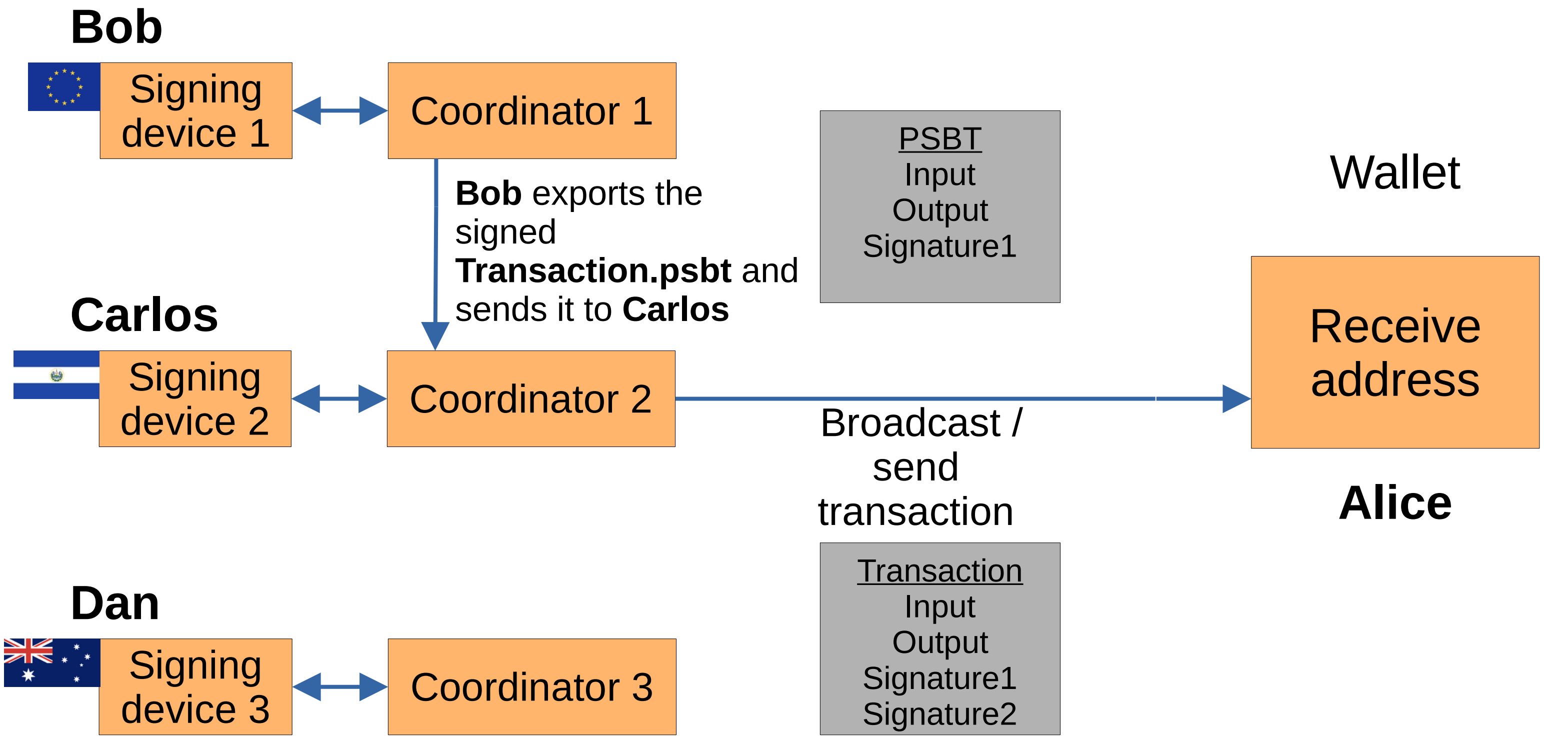
Transaction
Input
Output
Signature1
Signature2

Wallet

Receive address

Alice

Partially Signed Bitcoin Transactions (PSBTs)



Bob

Signing device 1

Coordinator 1

Bob exports the signed **Transaction.psbt** and sends it to **Carlos**

PSBT
Input
Output
Signature1

Wallet

Carlos

Signing device 2

Coordinator 2

Broadcast / send transaction

Receive address

Alice

Dan

Signing device 3

Coordinator 3

Transaction
Input
Output
Signature1
Signature2

Is multisig necessary for me?

- It depends on your “requirements” of self custody
- think of your **family** and keep things **simple**

END

Github:
https://github.com/marc3linho

Nostr:
https://nostriches.net/s/marcelinho