Bitcoin Multisignature

and its applications

Quick review of a Bitcoin transaction

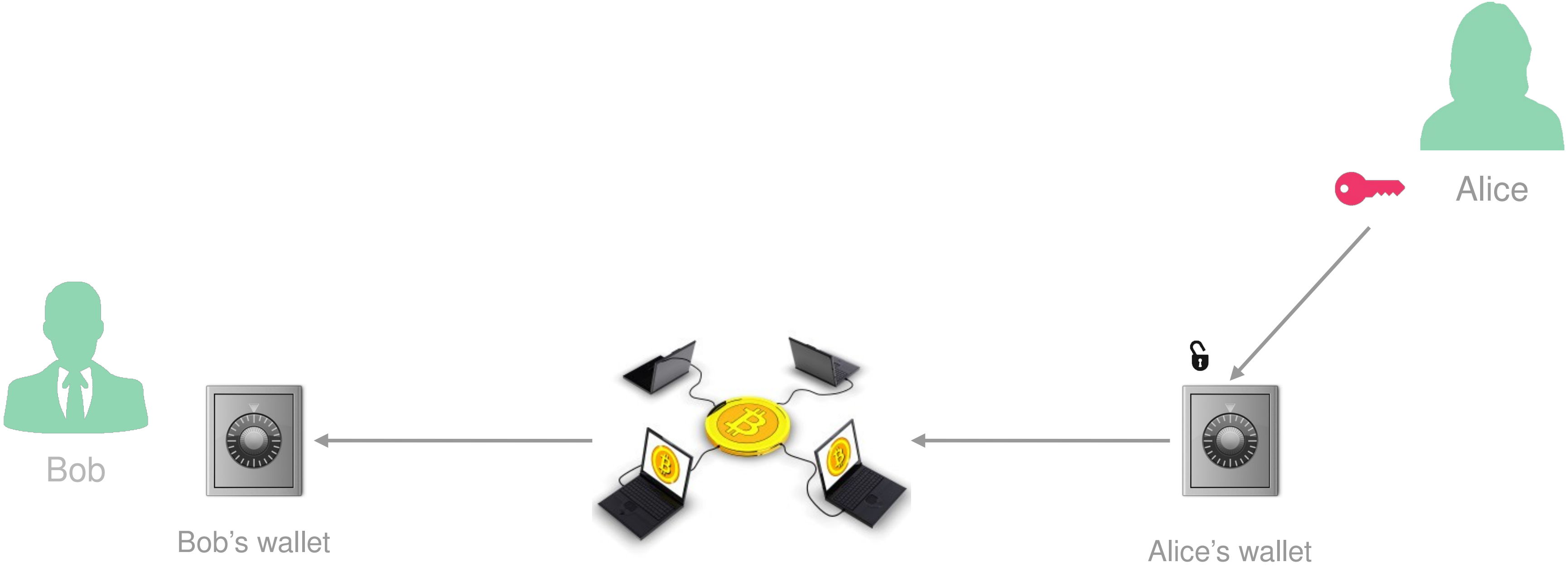
No multisig

Transaction: send 1 Bitcoin

Alice

Bob

Alice unlocks her coins with her single pair of keys



Alice

Bob

Bob’s wallet

Alice’s wallet

Bitcoin network validates transaction

Using a simple Bitcoin transaction Alice can:

Make a transaction in a ***trustless*** network
(no government, company or bank)

Transaction is ***fast***

Cheap as fees are very low

BUT she can lose access to her coins

Losing her “single” pair of keys

Losing her wallet (if the wallet is stored on her laptop)

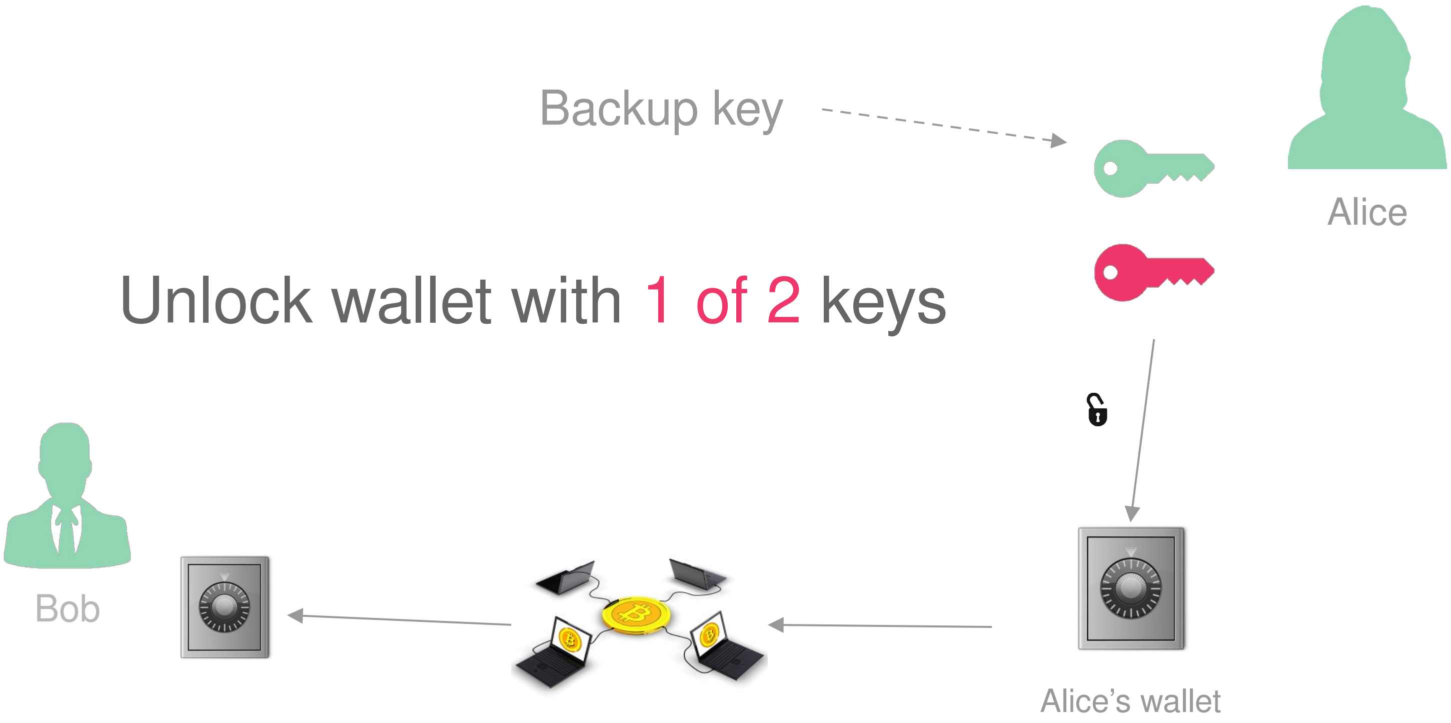
Her online wallet server gets hacked and her coins stolen

Convenience VS Security

Most users use online wallets

Trade trust and security for convenience

Multi Signature Transaction



Backup key

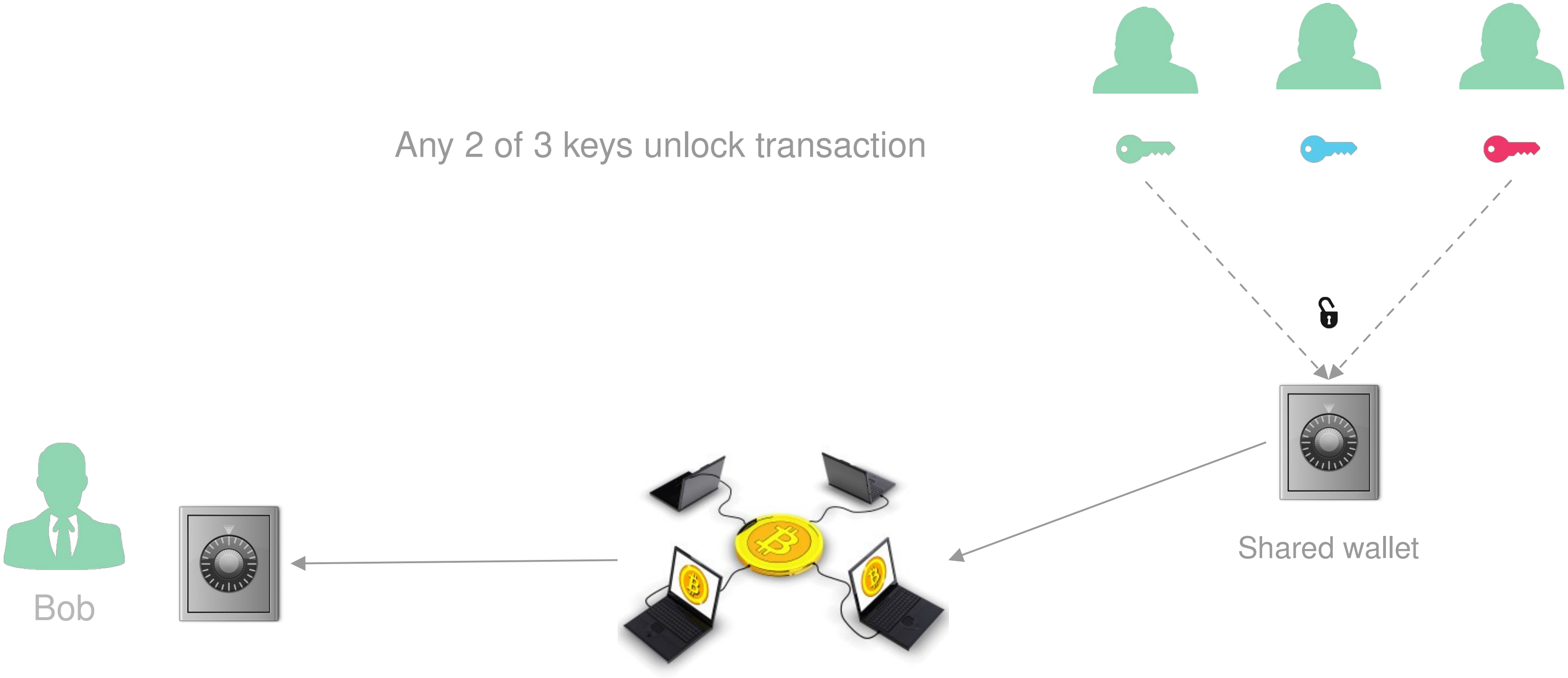
Alice

Unlock wallet with 1 of 2 keys

Bob

Alice’s wallet

Multi Signature Transaction

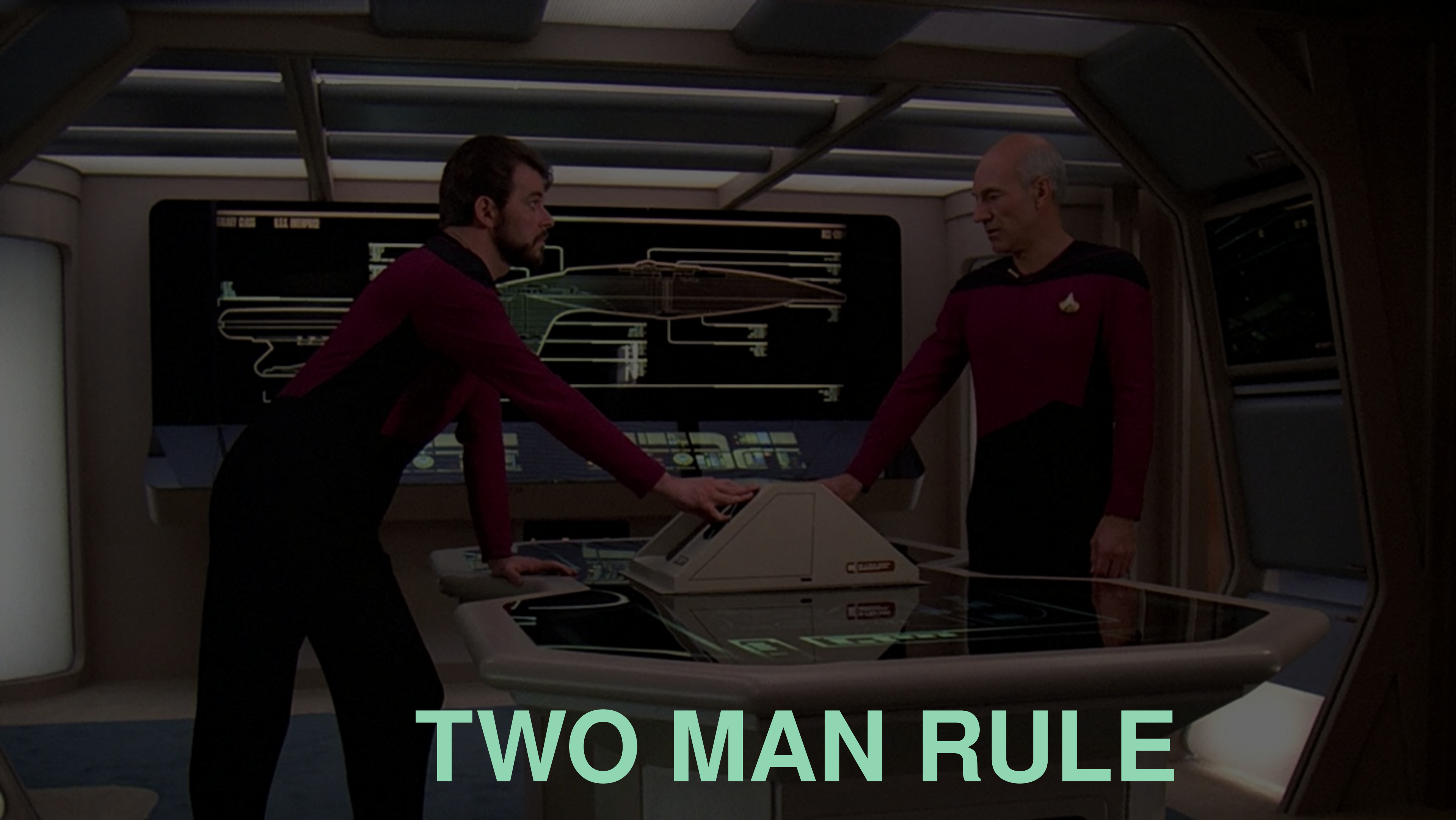


Any 2 of 3 keys unlock transaction

Shared wallet

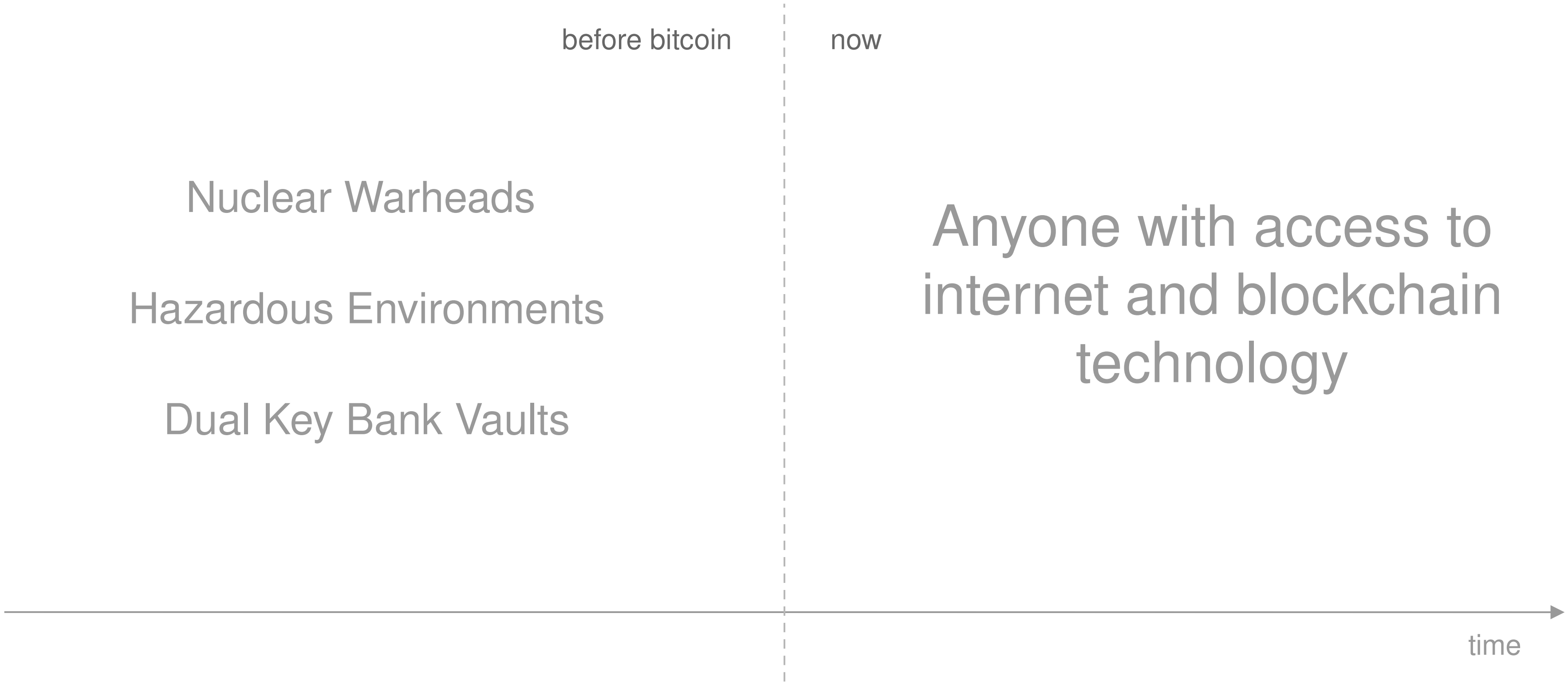
Bob

Bitcoin network validates transaction



TWO MAN RULE

High security for critical operations



before bitcoin

now

Nuclear Warheads

Hazardous Environments

Dual Key Bank Vaults

Anyone with access to internet and blockchain technology

time

Applications

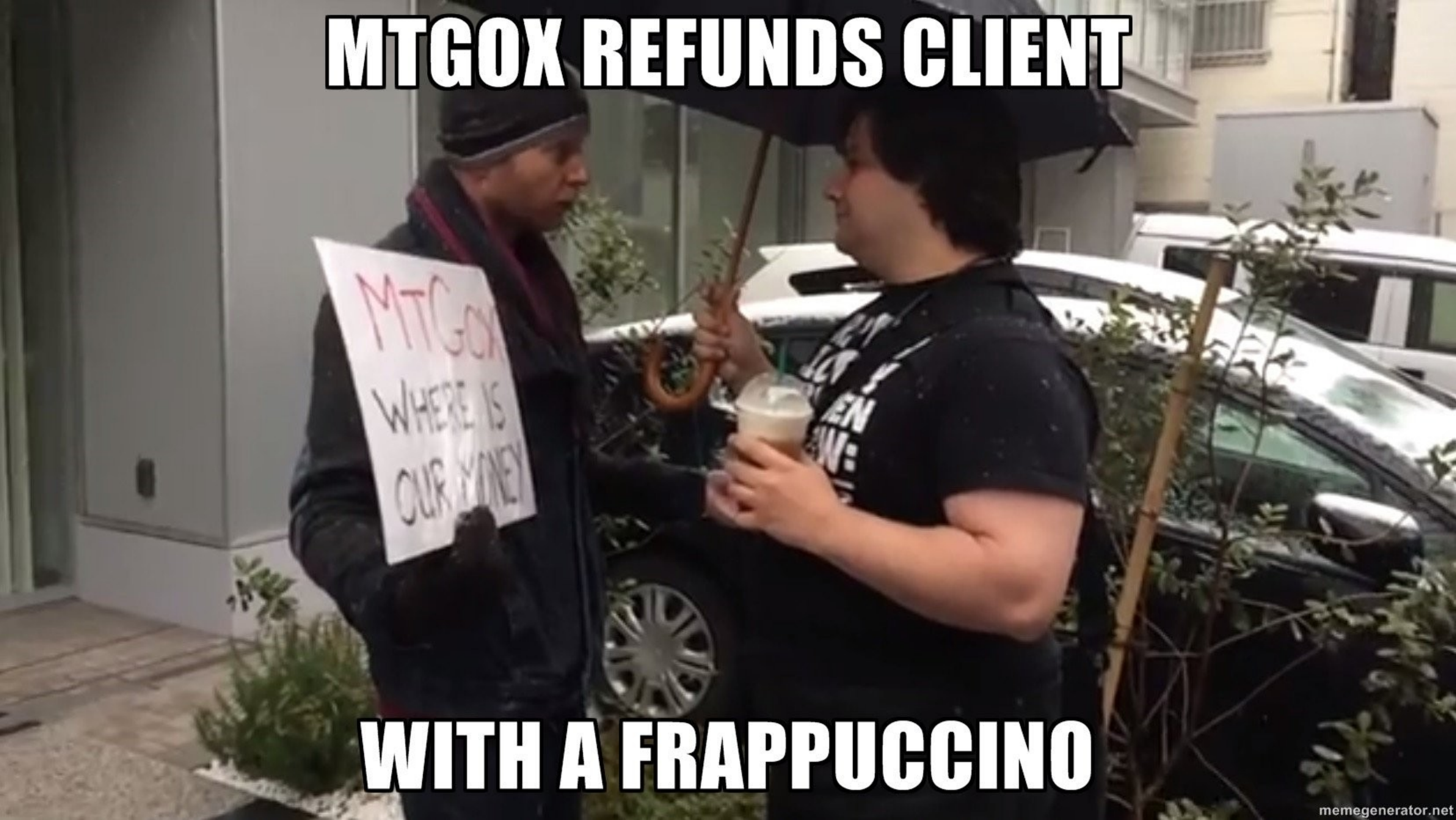
Improved Security: Exchanges, Oracles, Wallets …

Escrow and arbitration

Crowdfunding

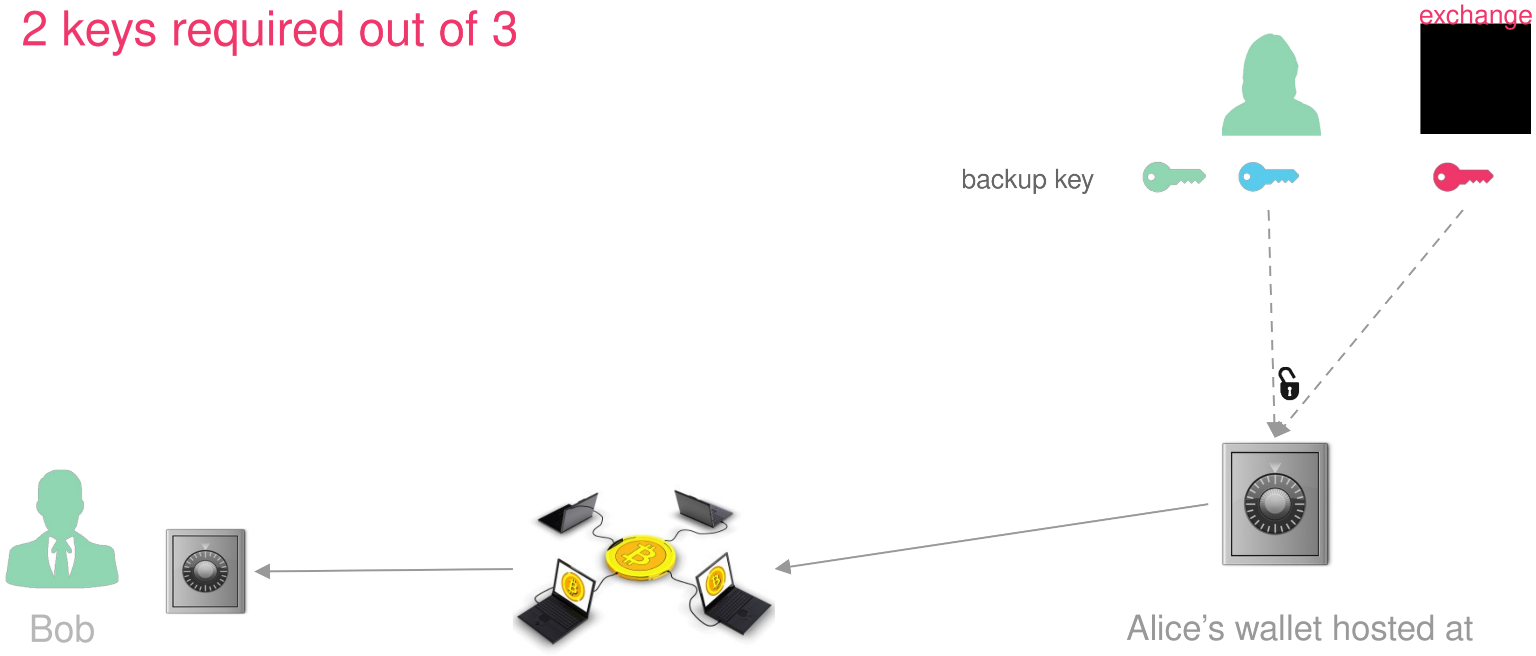
Co-Spending

…


MTGOX REFUNDS CLIENT
MtGox
WHERE IS
OUR MONEY
WITH A FRAPPUCCINO
memegenerator.net

Multi Signature with Exchanges

2 keys required out of 3



exchange

[redacted]

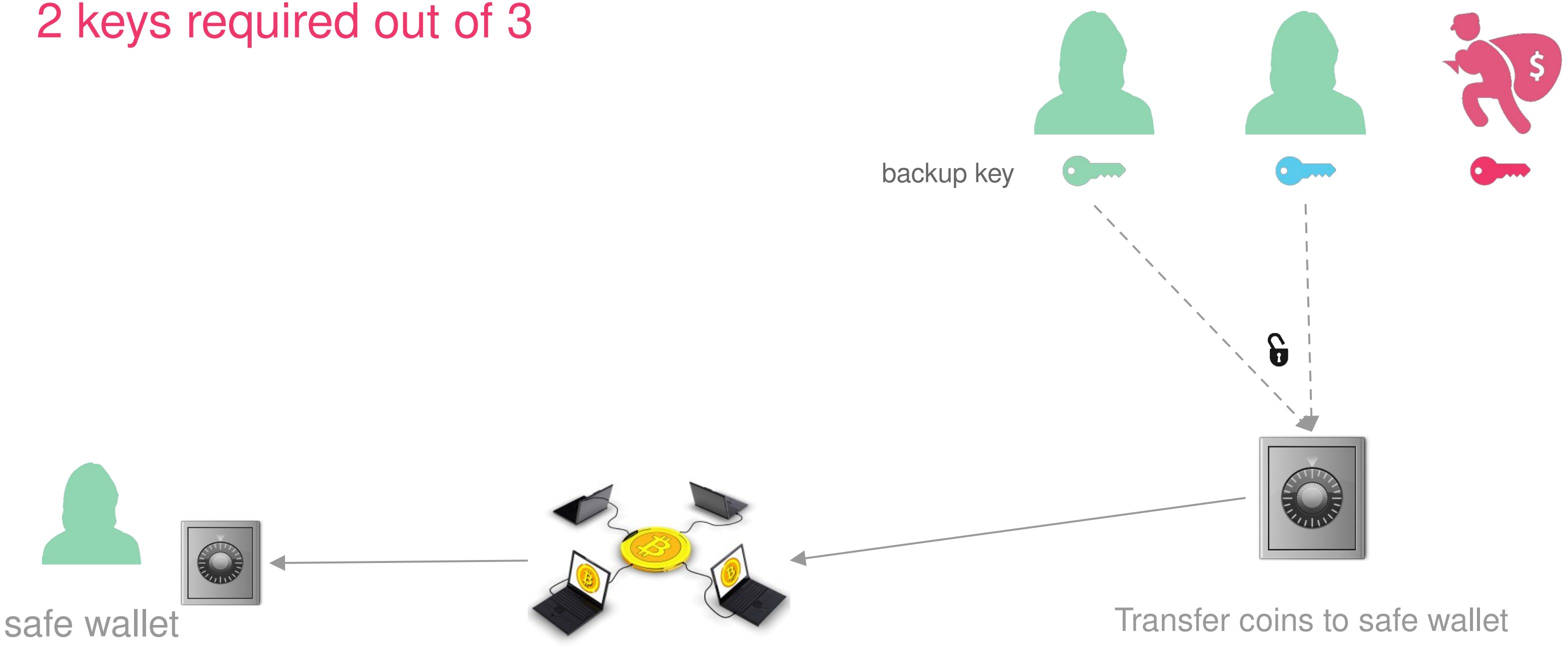
backup key

Bob

Alice’s wallet hosted at
exchange service

Multi Signature with Exchanges

2 keys required out of 3

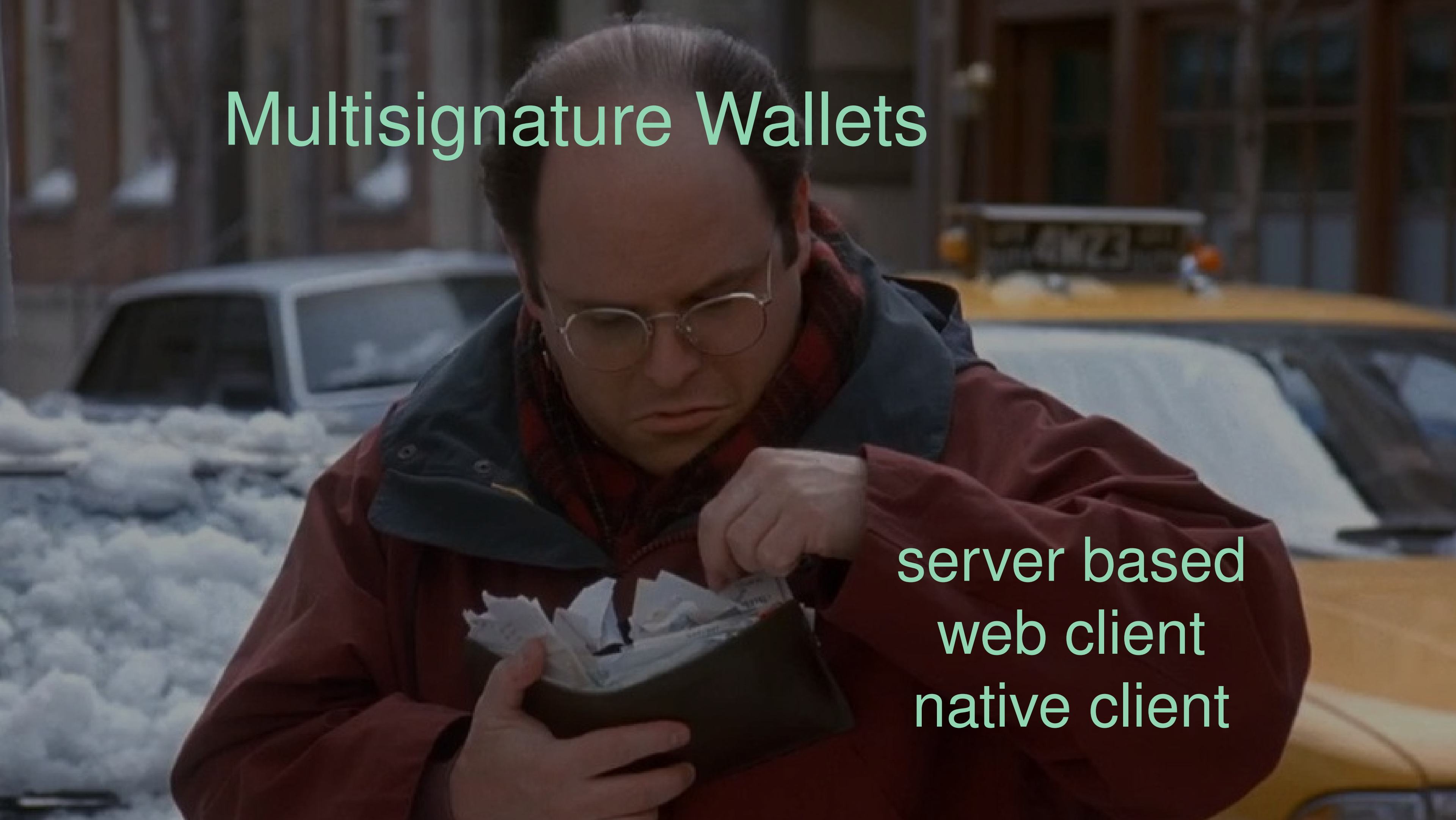


backup key

safe wallet

Transfer coins to safe wallet

Multisignature Wallets



server based
web client
native client

Where are your wallet keys stored ?

On a remote server

exchanges
coinbase

On your device
Offline

Bitcoin Core
Electrum
Armory

Where are your wallet keys stored ?

On a remote server	On your browser (aka web wallets)	On your device Offline
exchanges coinbase	blockchain dark wallet * web wallets	Bitcoin Core Electrum Armory

Armory

ARMORY

Native client with multisig

Lockboxes feature with M of N transactions

Total freedom and flexibility

Simulfunding: Simultaneous wallet funding (private crowdfunding)

Most secure Bitcoin and multisig wallet.

Not the most convenient

Armory

ARMORY

Native client with multisig

1-of-2: Husband-wife joint account (either can spend)

2-of-2: Husband-wife savings account (requires both signatures)

2-of-3: Buyer-seller escrow with trusted third-party (use simulfunding)

2-of-3: Personal savings using two hot wallets and one cold backup

3-of-5: Board of directors of a company managing company funds

3-of-6: Board of five directors, but CEO has two keys (only two required if CEO is involved; else three)

4-of-7: Ultra high-security storage using 7 offline devices in vaults around the world

M-of-N: Use your imagination! (up to 7-of-7)

https://bitcoinarmory.com/about/using-lockboxes/

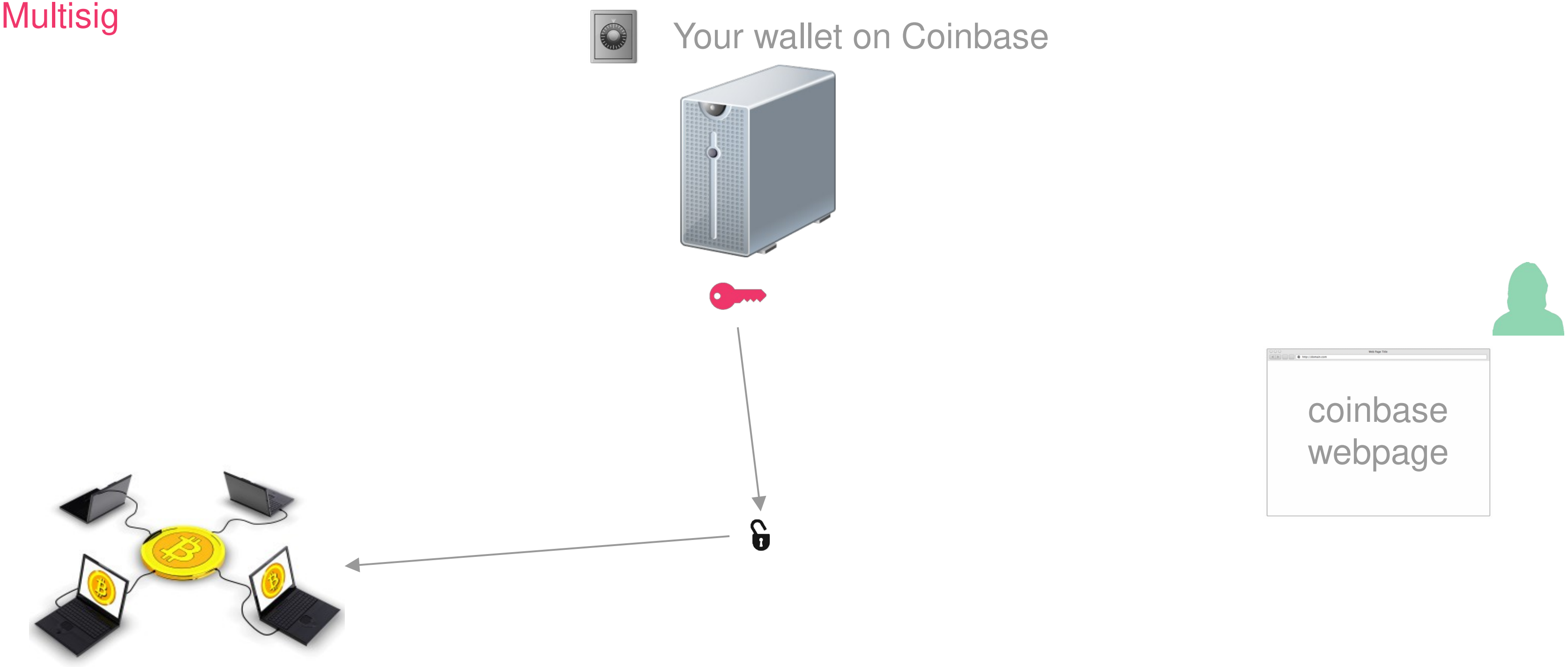
Server Based Wallets

Coinbase Vault: Offline storage

Multi sig coming soon

Server Based

No Multisig



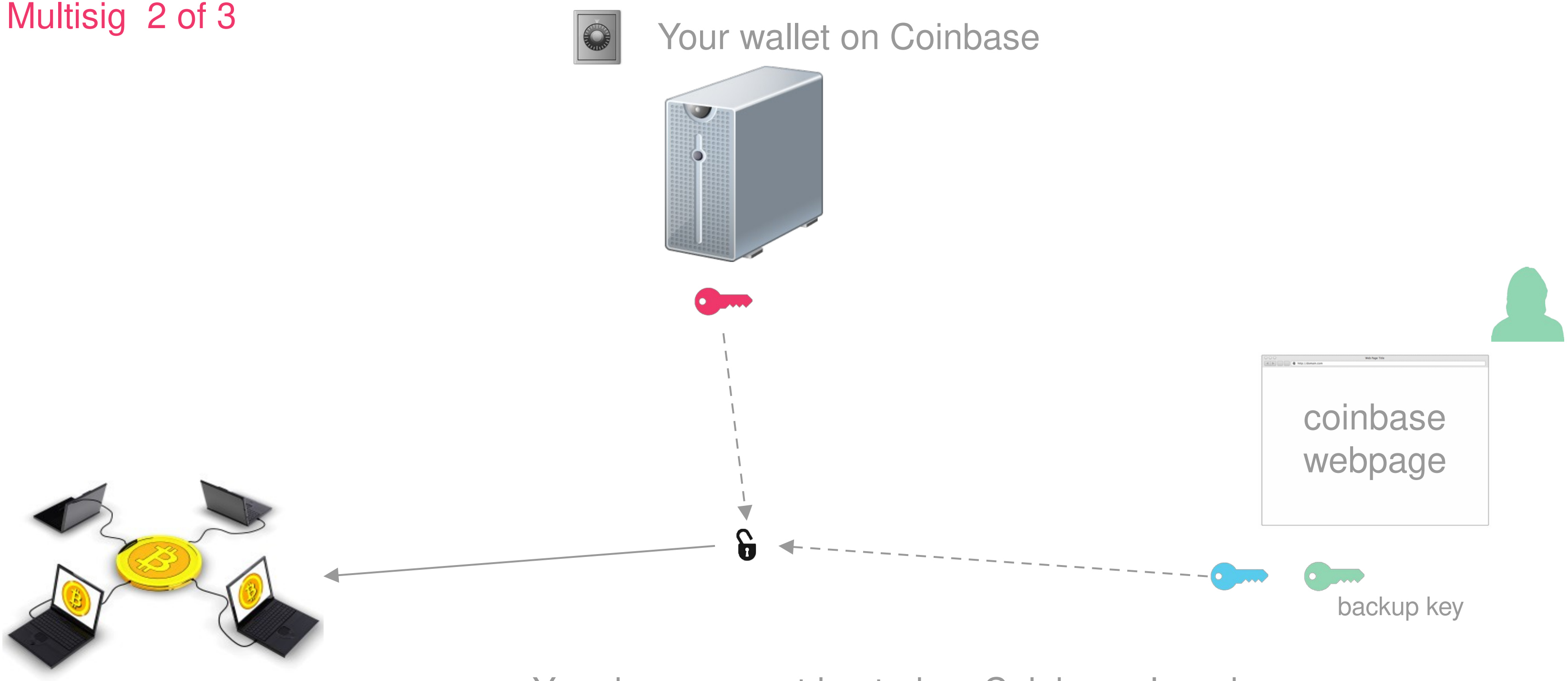
Your wallet on Coinbase

coinbase webpage

Your key is hosted on Coinbase’s server

Server Based

With Multisig 2 of 3



Your wallet on Coinbase

coinbase webpage

backup key

Your keys are not hosted on Coinbases's webpage
You need to somehow sign the transaction (out of web page)

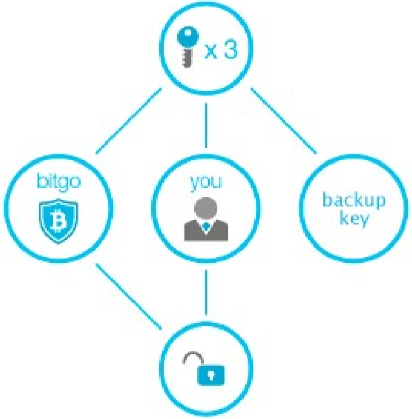
Web Wallets

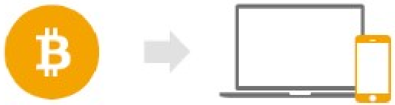
BitGo™

Bank Grade Security

2 of 3 MultiSig

Offline Storage





Web Wallets

Greenaddress.it

HD wallet

Multi Signature (2 of 3)

Presigned transactions: pay in the future :)

Web Wallets

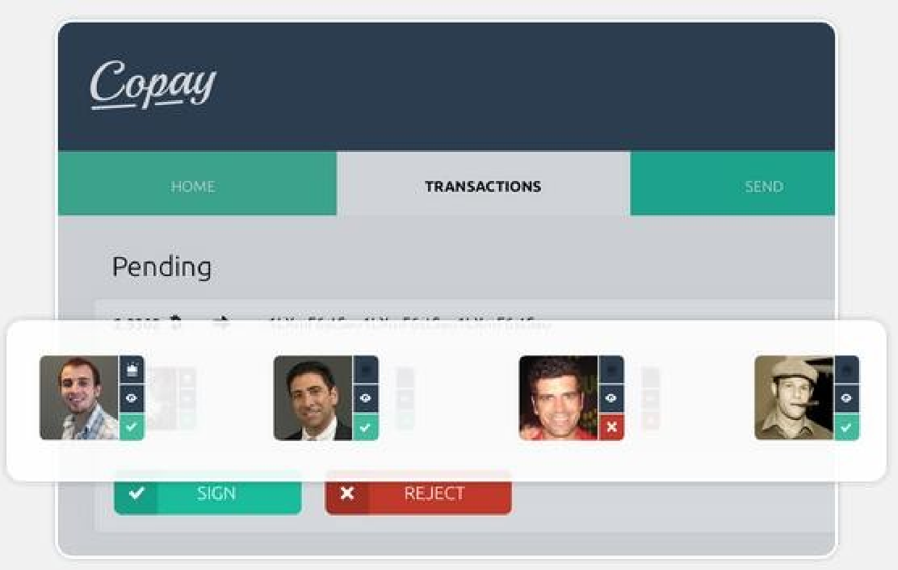
CoPay BitPay

still in beta

HD wallet

Multi Signature (M of N)

Real time multi signature



Web Wallets

Onchain.io

HD wallet

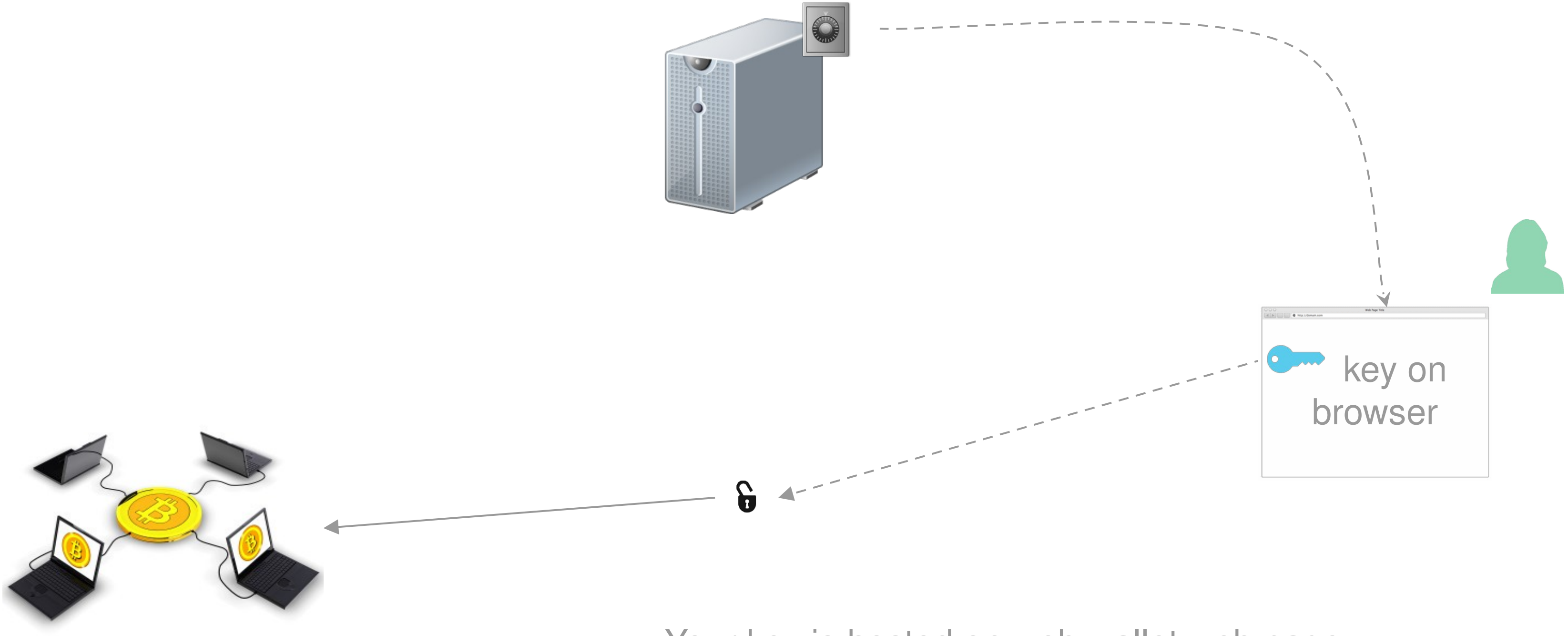
Multi Signature (M of N)

Out Of Band (Phone app as extra signing key)

Beware of “Security Theater”

Web Wallet: Web App

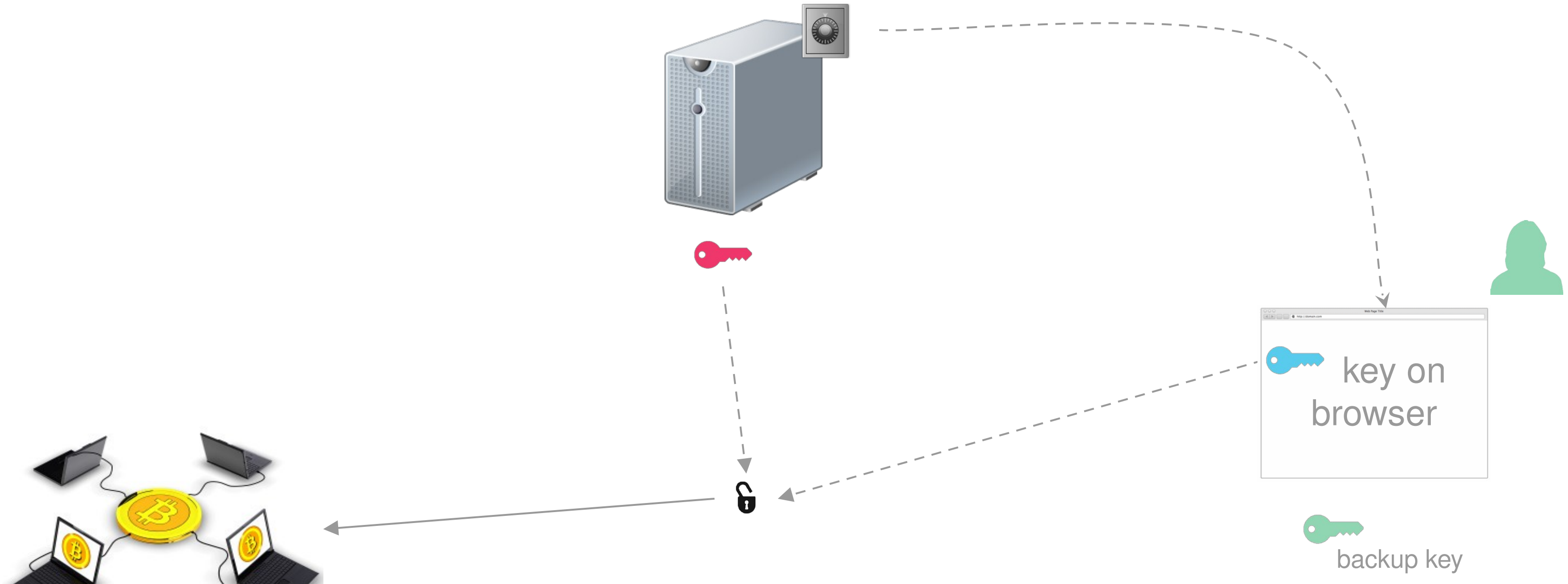
Without Multisig



Your key is hosted on web wallet web page
You sign the transaction on the web page

Web Wallet: Web App

With Multisig 2 of 3



key on browser

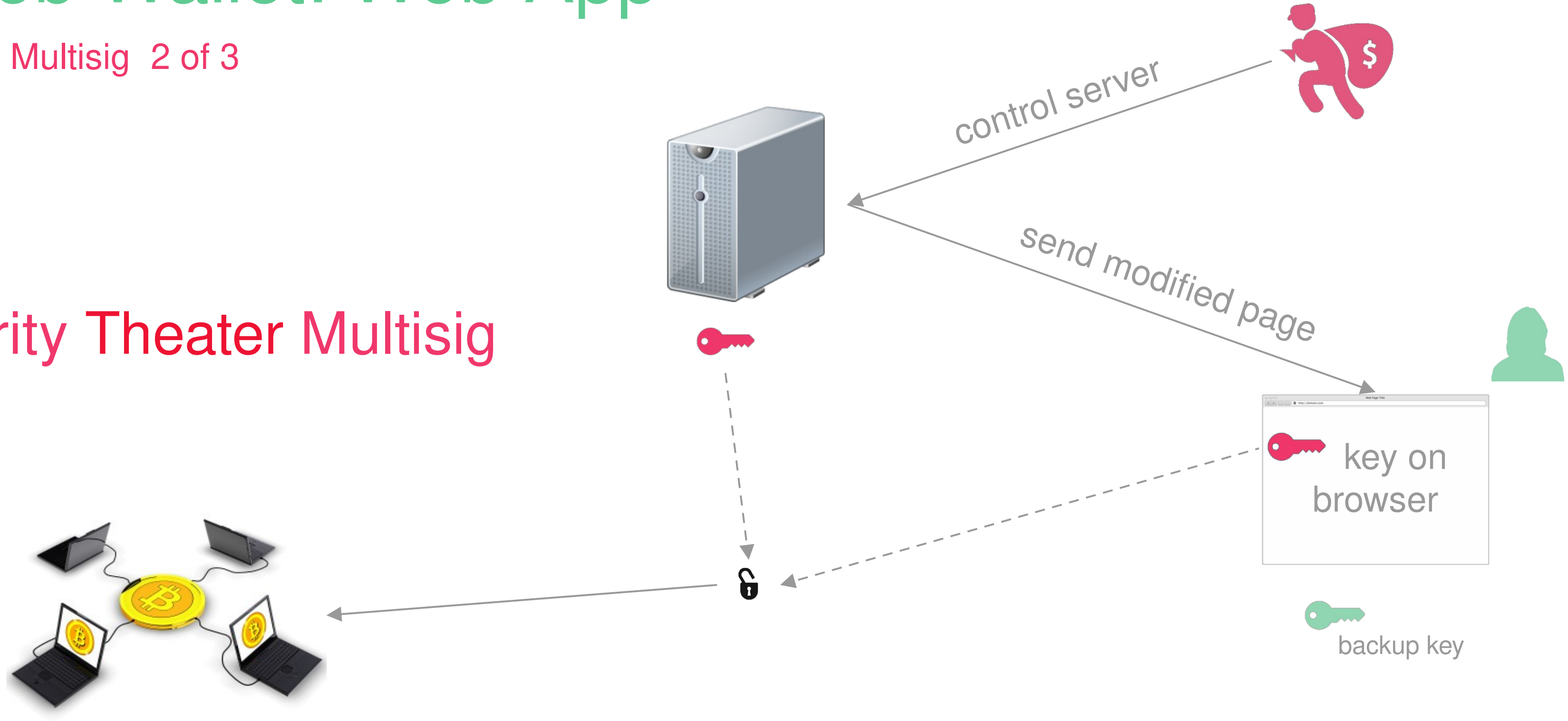
backup key

Your key is hosted on web wallet web page
You multisign the transaction on the web page

Web Wallet: Web App

With Multisig 2 of 3

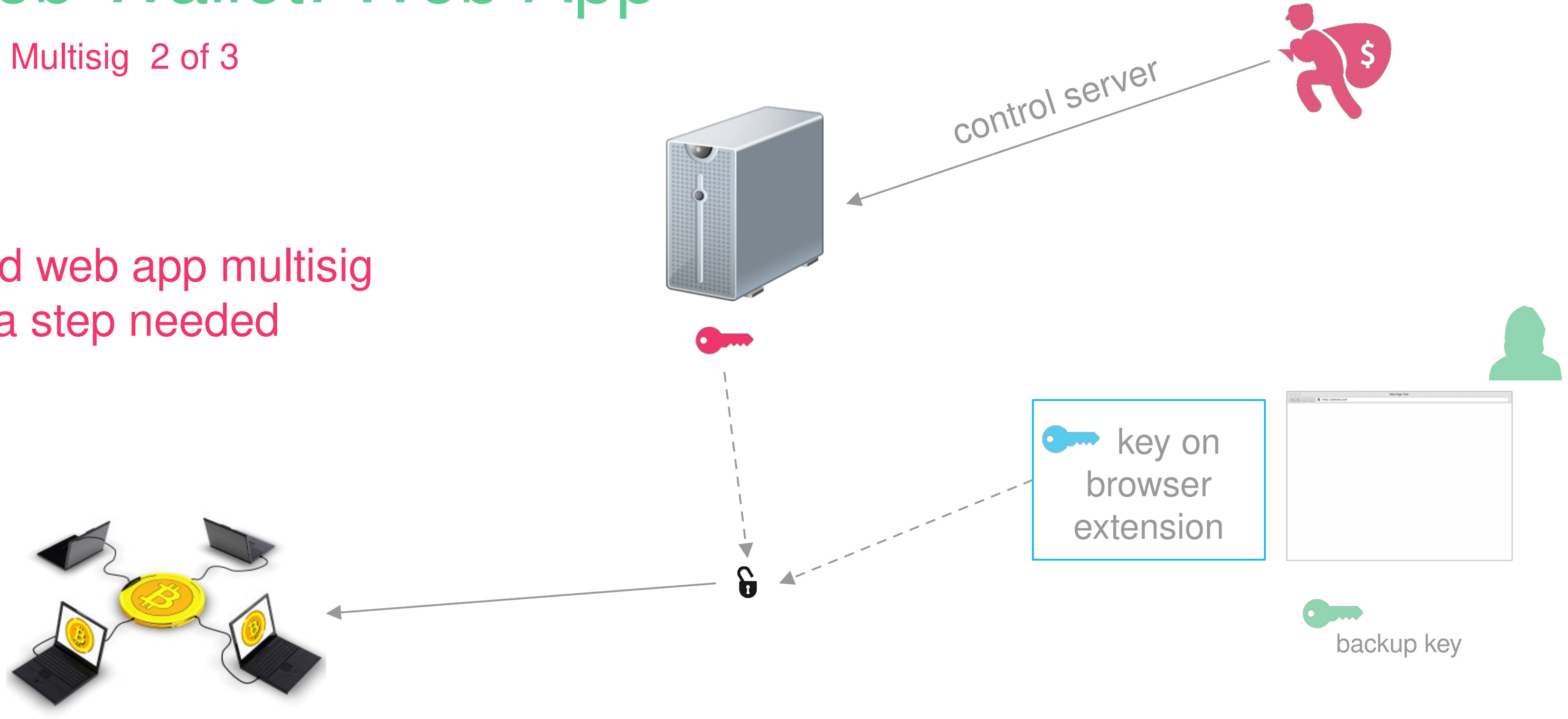
Security Theater Multisig



Web Wallet: Web App

With Multisig 2 of 3

Good web app multisig
Extra step needed



Oracles

CryptoCorp third party oracle

API Integrates with Wallets and Services

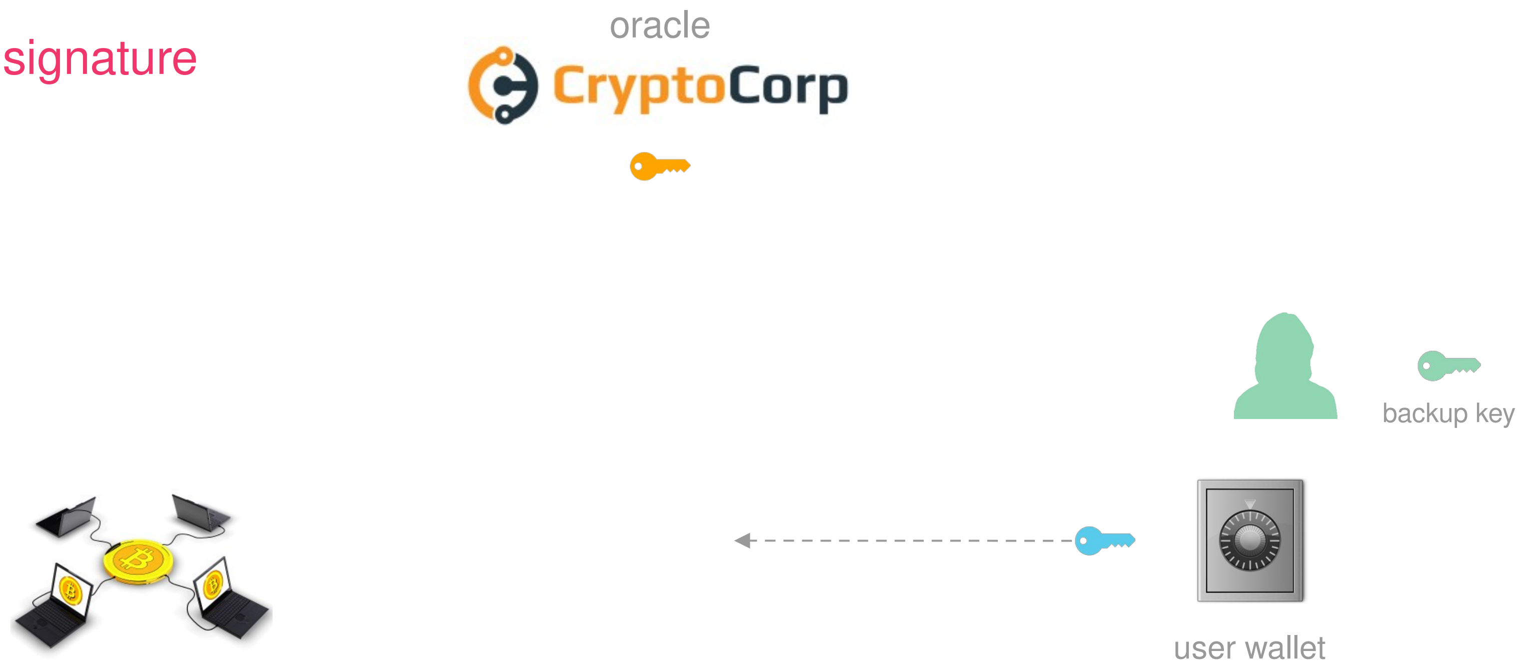
Theft prevention

Fraud risk detection

Organisations can protect shared wallet

(NeoBee fiasco)

2 of 3 multisignature



oracle

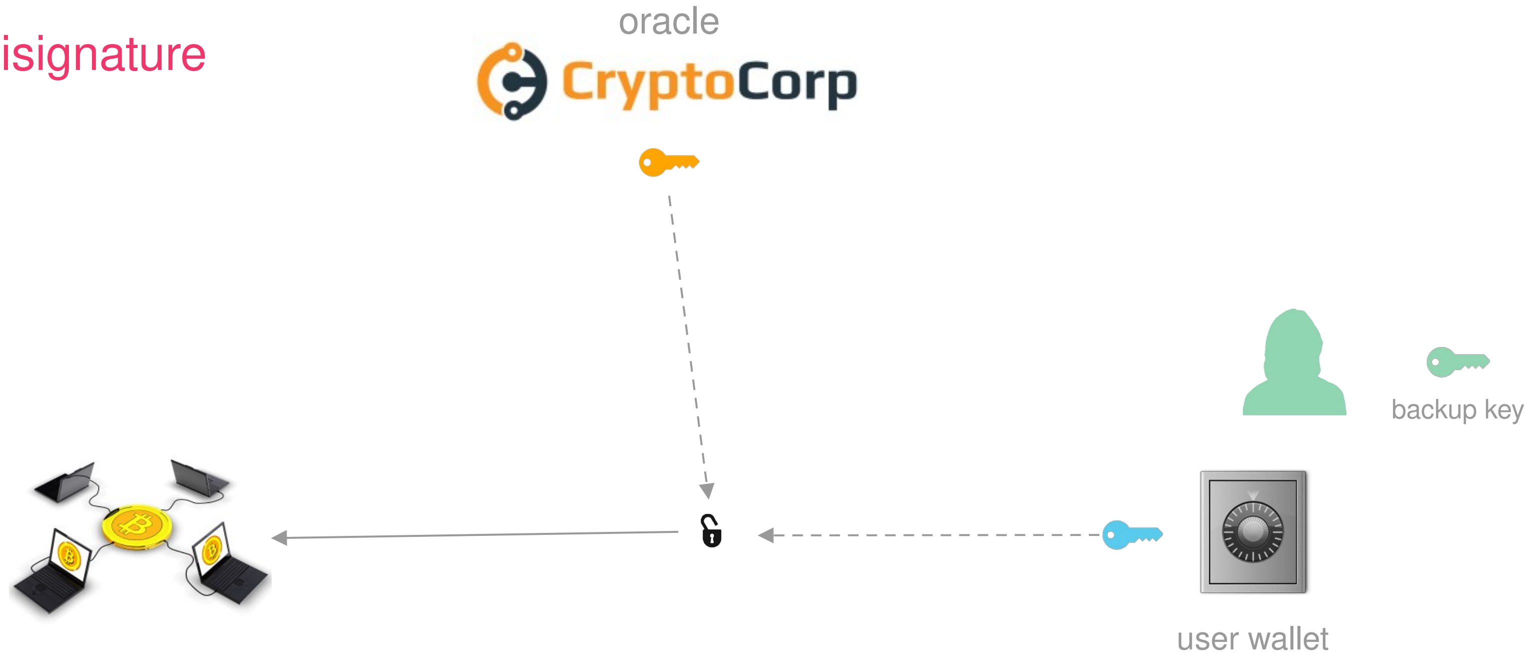
CryptoCorp

backup key

user wallet

Alice orders a transaction from her wallet

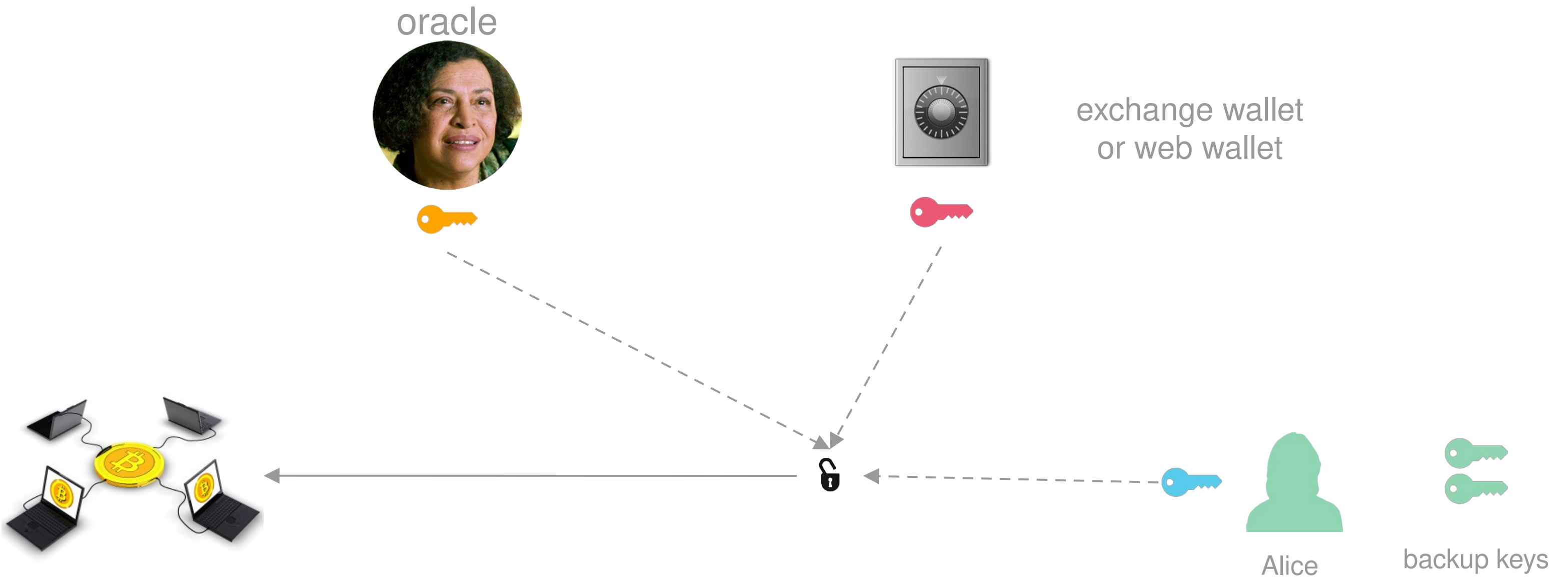
2 of 3 multisignature



Oracle applies third party verifications
then signs transaction

We can go further

3 of 5 multisignature



oracle

exchange wallet
or web wallet

Alice

backup keys

Arbitration and Escrow

OpenBazaar

Open Source p2p decentralized marketplace

No fees, no censorship

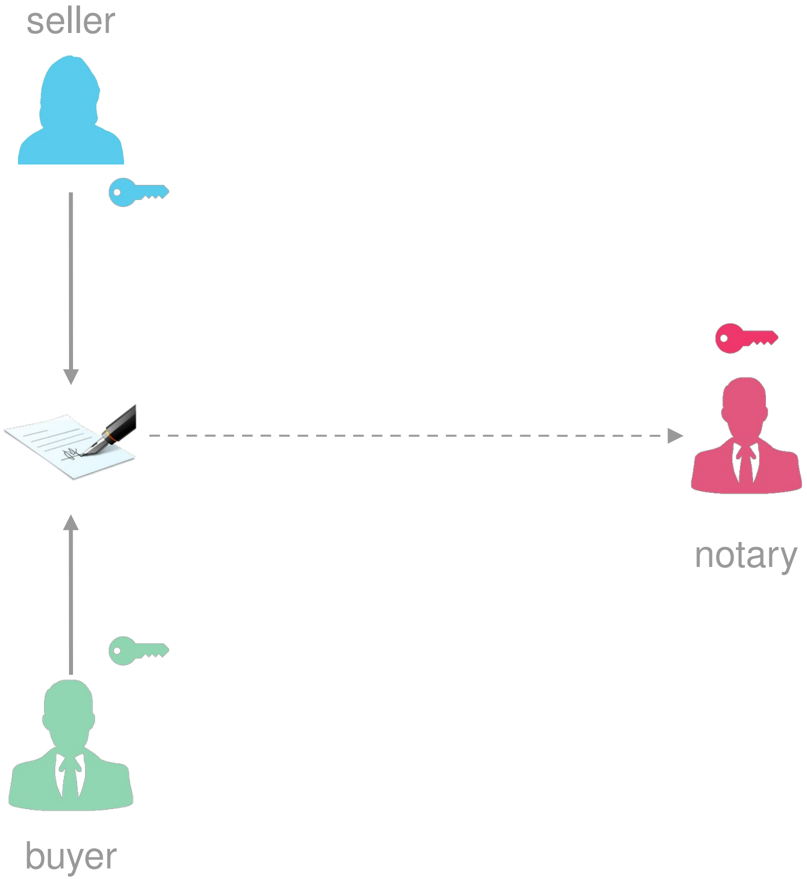
Ricardian contracts: trade and arbitration

Escrow payment with multi signatures

OpenBazaar

Buyer and Seller review and sign contract

Notary signs final contract

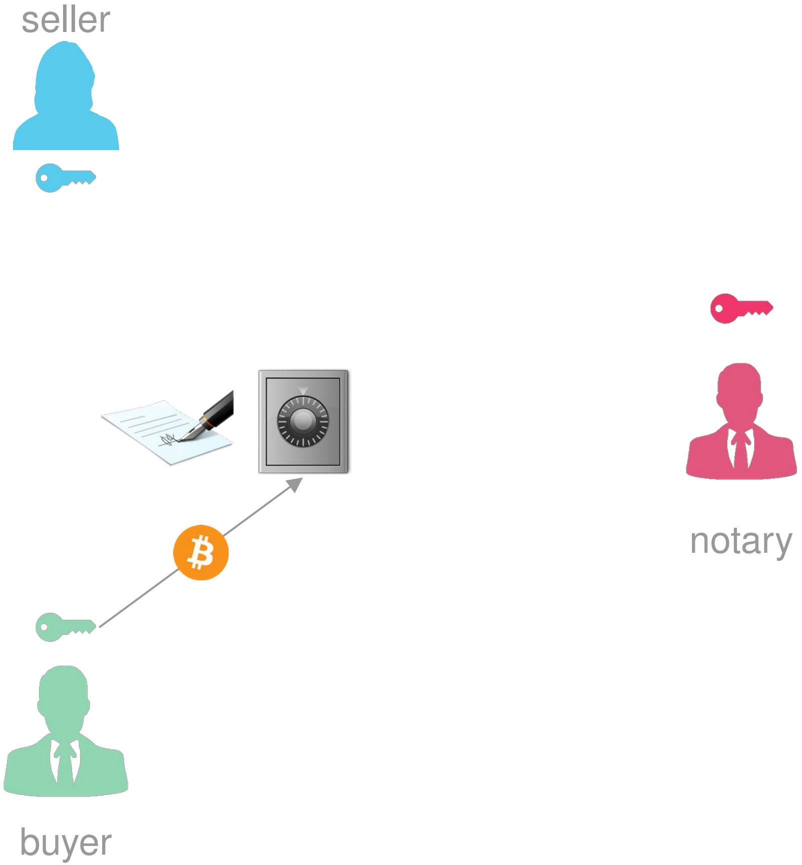


OpenBazaar

Notary creates multisig bitcoin address

Buyer send money to address

2 of 3 keys to unlock payment

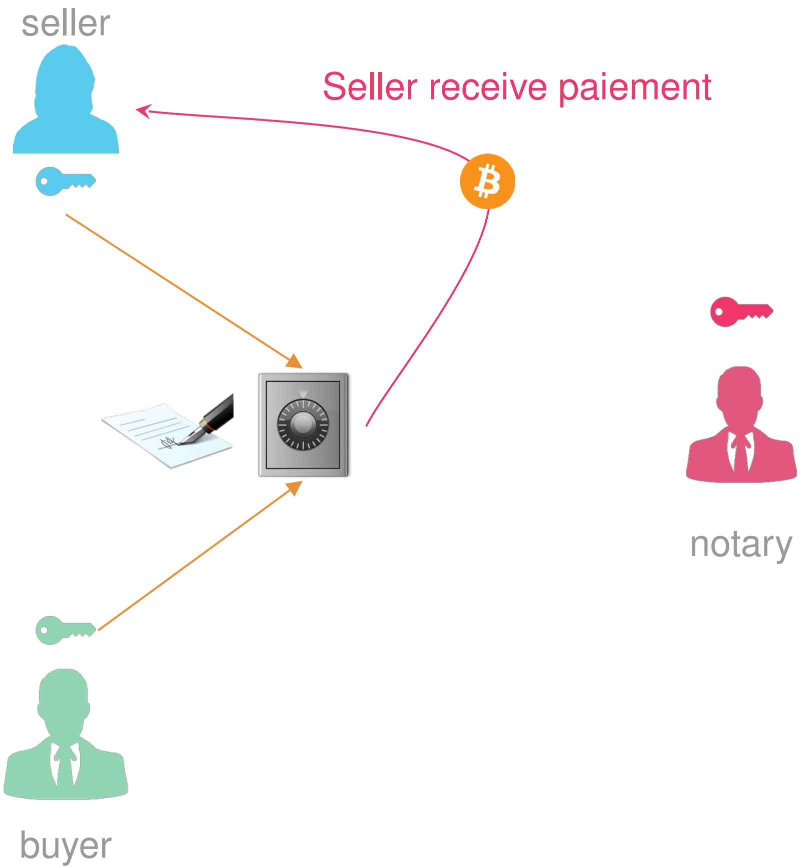


OpenBazaar

Buyer and Seller settle transaction

Funds unlocked with both their keys

Notary receives fee



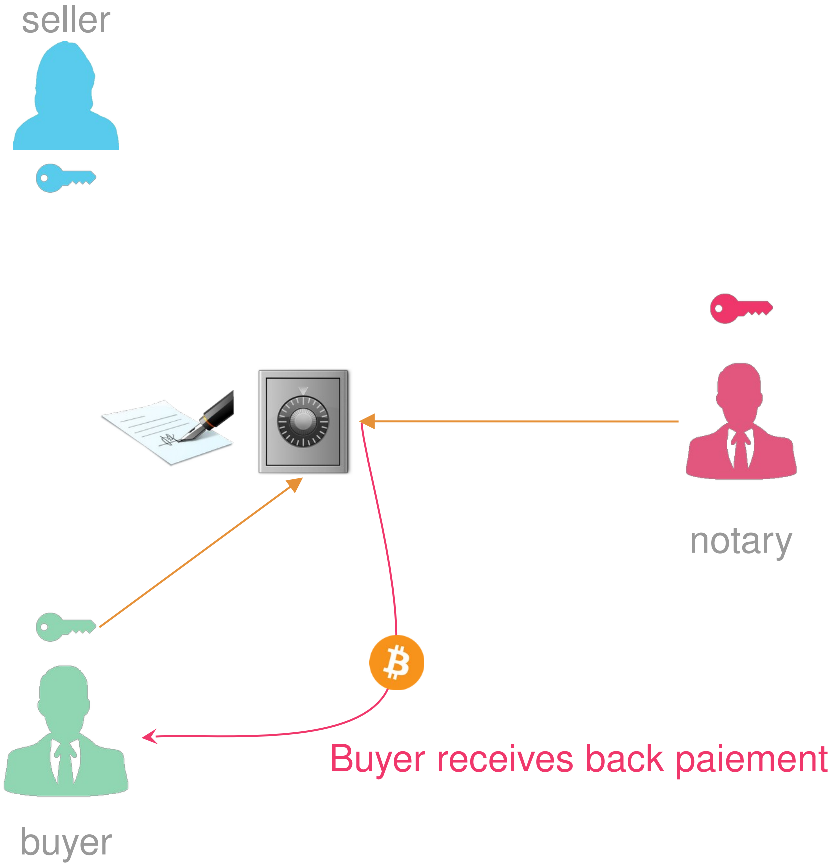
OpenBazaar

Buyer and Seller disagree

Notary makes arbitration

Seller is bad

Notary receives fee



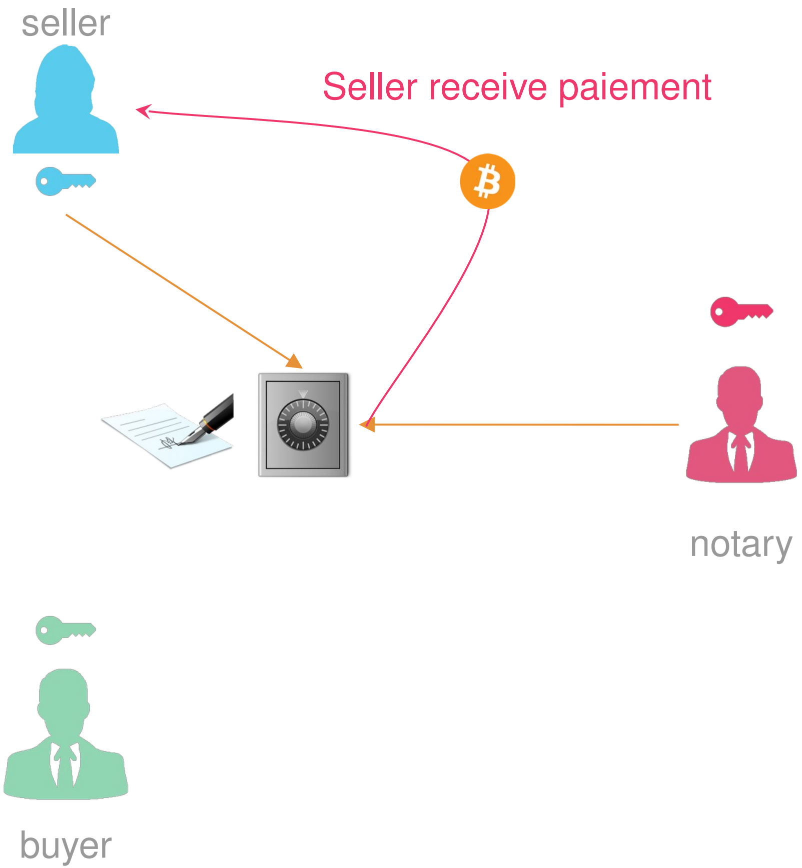
OpenBazaar

Buyer and Seller disagree

Notary makes arbitration

Buyer is bad

Notary receives fee



Final Thaughts

With multisig we can reach unmatched levels of security

No need for regulations to protect users ;)

Give some time to infrastructure to mature

You can start using multisig Today

Thanks for listening

send your love to

19DavSZz6vopuYyER3S2Jnd2jzoEQa4Ww8

OR

chakib.benz@gmail.com