NO FF ONE 2022

Corporate Cryptocurrency Wallet Management

Valery Tyukhmenev

Exness

Moscow, August 25, 2022

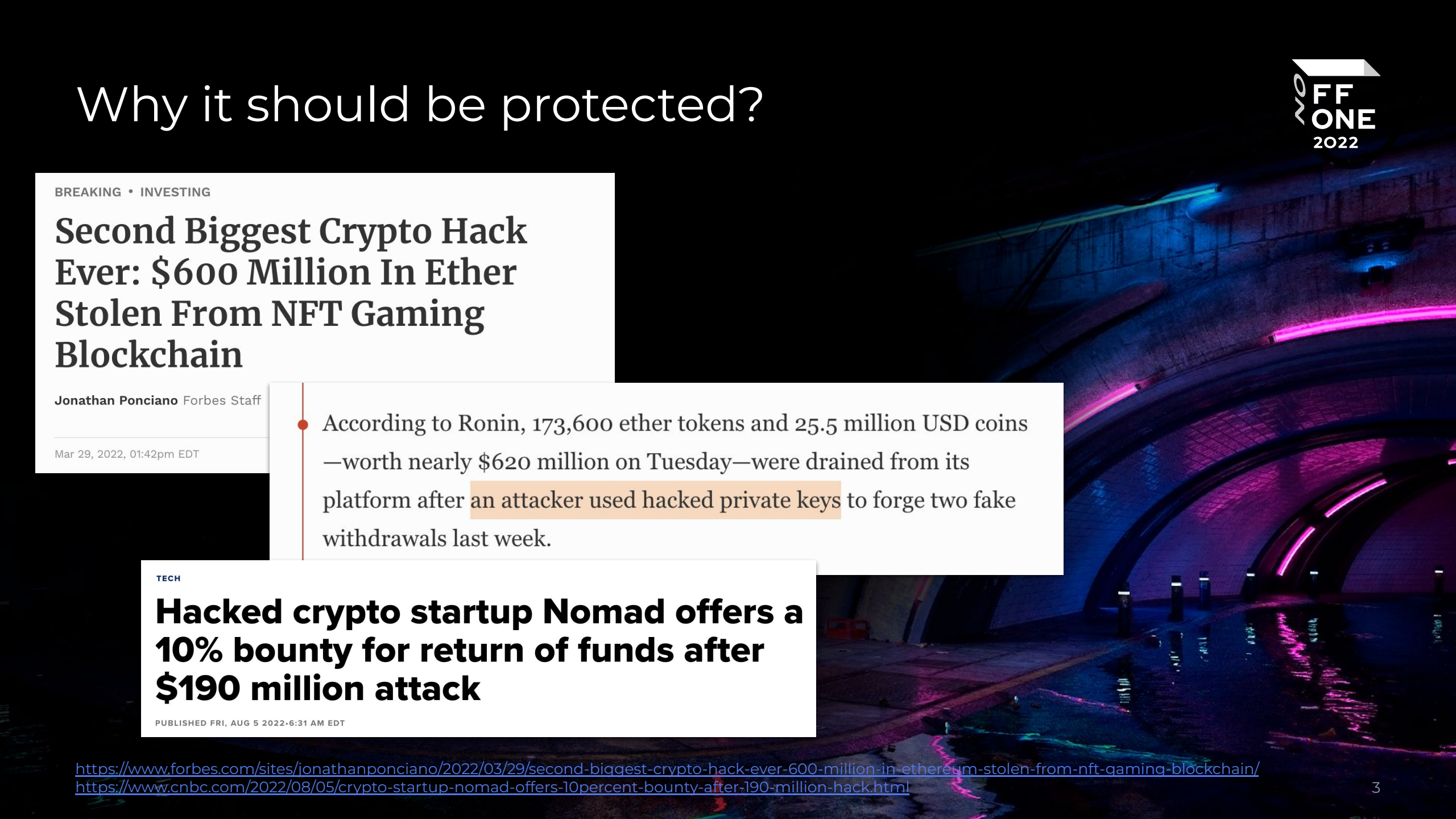
What is cryptocurrency

Cryptocurrency is decentralized digital money that's based on blockchain technology.

A blockchain is an open, distributed ledger that records transactions in code. In practice, it's a little like a checkbook that's distributed across countless computers around the world. Transactions are recorded in "blocks" that are then linked together on a "chain" of previous cryptocurrency transactions.

https://www.forbes.com/advisor/investing/cryptocurrency/what-is-cryptocurrency/
https://marketing.exness.com/crypto/

Why it should be protected?



BREAKING • INVESTING

Second Biggest Crypto Hack Ever: $600 Million In Ether Stolen From NFT Gaming Blockchain

Jonathan Ponciano Forbes Staff

Mar 29, 2022, 01:42pm EDT

According to Ronin, 173,600 ether tokens and 25.5 million USD coins —worth nearly $620 million on Tuesday—were drained from its platform after an attacker used hacked private keys to forge two fake withdrawals last week.

TECH

Hacked crypto startup Nomad offers a 10% bounty for return of funds after $190 million attack

PUBLISHED FRI, AUG 5 2022•6:31 AM EDT

https://www.forbes.com/sites/jonathanponciano/2022/03/29/second-biggest-crypto-hack-ever-600-million-in-ethereum-stolen-from-nft-gaming-blockchain/
https://www.cnbc.com/2022/08/05/crypto-startup-nomad-offers-10percent-bounty-after-190-million-hack.html

Why it should be protected?

Total Volume of Funds Reportedly Stolen Per Country 2011-2022

Search

No. of Incidents	Total Amount	No. of Countries
364	$14.6b	45

Incident ↓	Type ↓	Date ↓	Amount ↑	Currencies	Country ↓
Plus Token Ponzi	Fraud	16/12/2019	$2.9b	BTC, ETH	
Thodex	Fraud	22/04/2021	$2b	UNKNOWN	Turkey
Wotoken	Fraud	14/05/2020	$1b	BCH, BTC, ...	China
Ronin	DeFi Breach	29/03/2022	$650m	ETH, ERC20	
Mt. Gox	Breach	07/02/2014	$615m	BTC	Japan
PolyNetwork	DeFi Breach	10/08/2021	$614m	ETH, BSC, ...	
Coincheck	Breach	26/01/2018	$535m	NEM	Japan
MyCoin	Fraud	09/02/2015	$387m		Hong Kong
Wormhole	DeFi Breach	02/02/2022	$326m	SOL	
Kucoin	Breach	26/09/2020	$281m	BTC, ETH	Seychelles

https://crystalblockchain.com/security-breaches-and-fraud-involving-crypto/

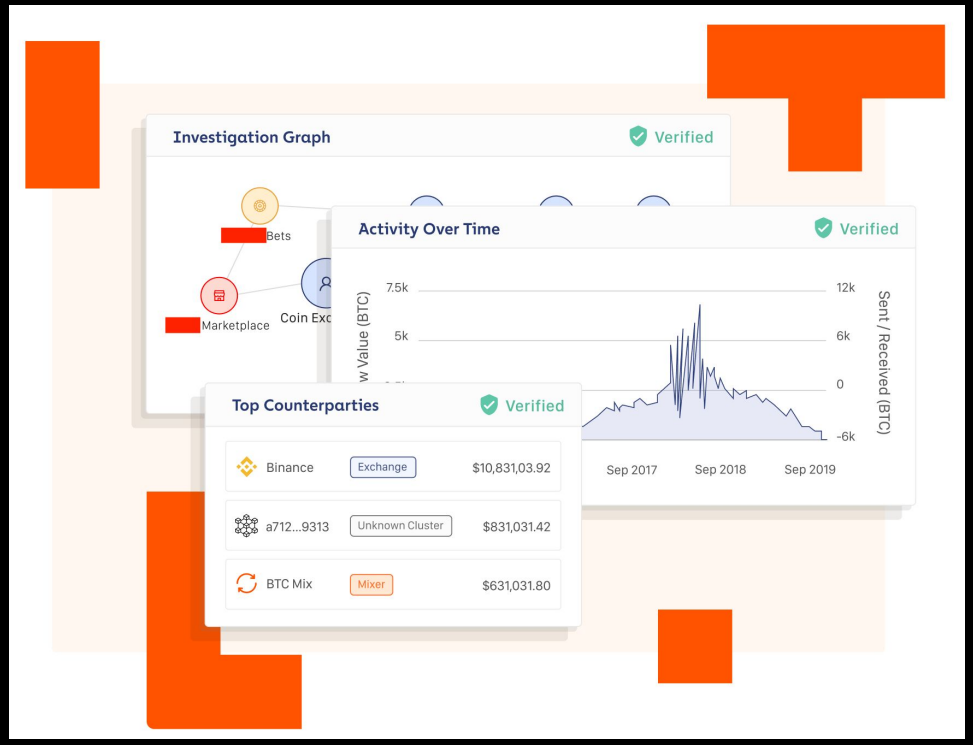
Cryptocurrency

https://www.coinparticle.com/market/all

KYT (Know Your Transaction)

Addition to KYC / AML

Know Your Transaction or KYT is a commonly used financial industry term that refers to the process of examining financial transactions for fraudulent or suspicious activities including money laundering. As cryptocurrency adoption continues to grow, it has been important for institutions to have the ability to drill down into crypto transactions for evidence of financial crimes.



https://crystalblockchain.com/articles/the-importance-of-knowing-your-cryptocurrency-transaction-kyt/
https://www.chainalysis.com/chainalysis-kyt/

Wallet Types

Hot Wallet

- Easiest to start using crypto
- Keys are being generated and stored online
- Transactions (TXs) are being signed by provider
- Lowest security level

Warm Wallet

- Uses proprietary software to generate and store wallets
- Keys stored offline on device (eg smartphone)
- TXs are being signed on user's device
- Balanced approach for everyday usage

Cold Wallet

- Private key is being stored on special hardware device with no internet access
- Requires manual actions for signing
- Usually signed TX is being broadcasted on separate device
- Best overall security

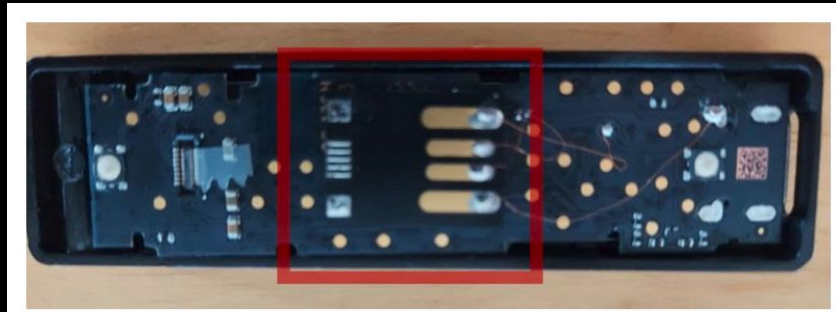
https://glacierprotocol.org/

Wallet Types

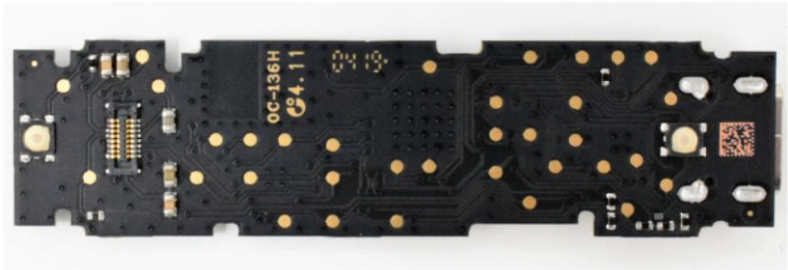
Hardware Wallets is not a panacea

The enclosed instructions tell the person to connect the Ledger to their computer, open a drive that appears, and run the enclosed application.

The instructions then tell the person to enter their Ledger recovery phrase to import their wallet to the new device.



Back of fake Ledger hardware wallet
Source: Reddit



Back of real Ledger hardware wallet
Source: Ledger

https://www.bleepingcomputer.com/news/cryptocurrency/criminals-are-mailing-altered-ledger-devices-to-steal-cryptocurrency/

Crypto Custody Types

Third-party custody

- \+ Custodian handles any problems
- \+ Easier for small business
- \+ Usually have insurance

- – Custodian controls crypto liquidity (can be frozen etc)
- – Custodian may be hacked (or any other 3rd-party risk)
- – Fees can be applied

Self-Custody

- \+ Full control of crypto liquidity
- \+ No 3rd party risks

- – Have to handle the management of keys
- – Also can be hacked

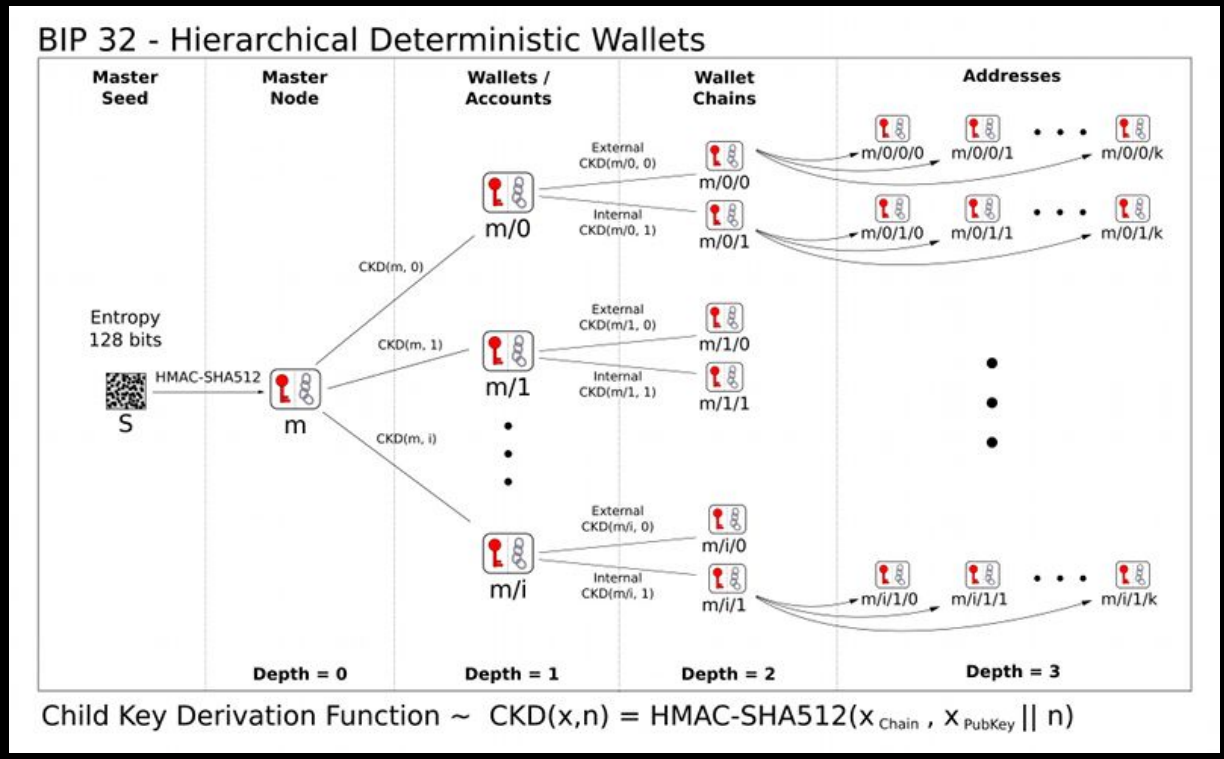
Hierarchical Deterministic Wallets (BIP-0032)

This standard defines how to derive private and public keys of a wallet from a binary **master seed (m)** and an ordered set of indices (called **path**) usually provided by values separated by slash:

```
m / purpose' / coin_type' / account' / change / address_index
```

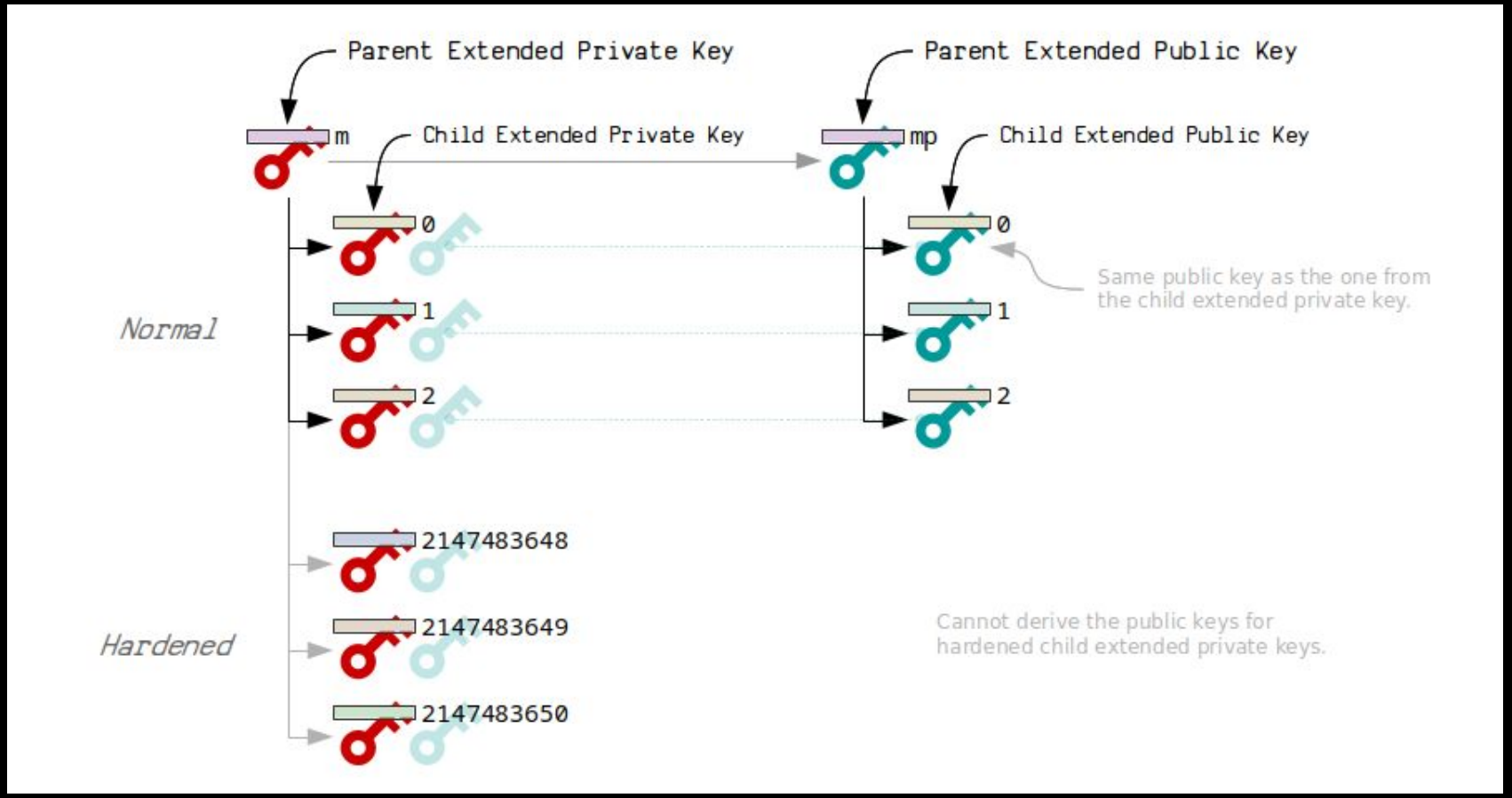
```
m / 44' / 0' / 1' / 3 / 37
```

There are two possible types of BIP32 derivation: **hardened** or **non-hardened**



https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki
https://github.com/bitcoin/bips/blob/master/bip-0044.mediawiki

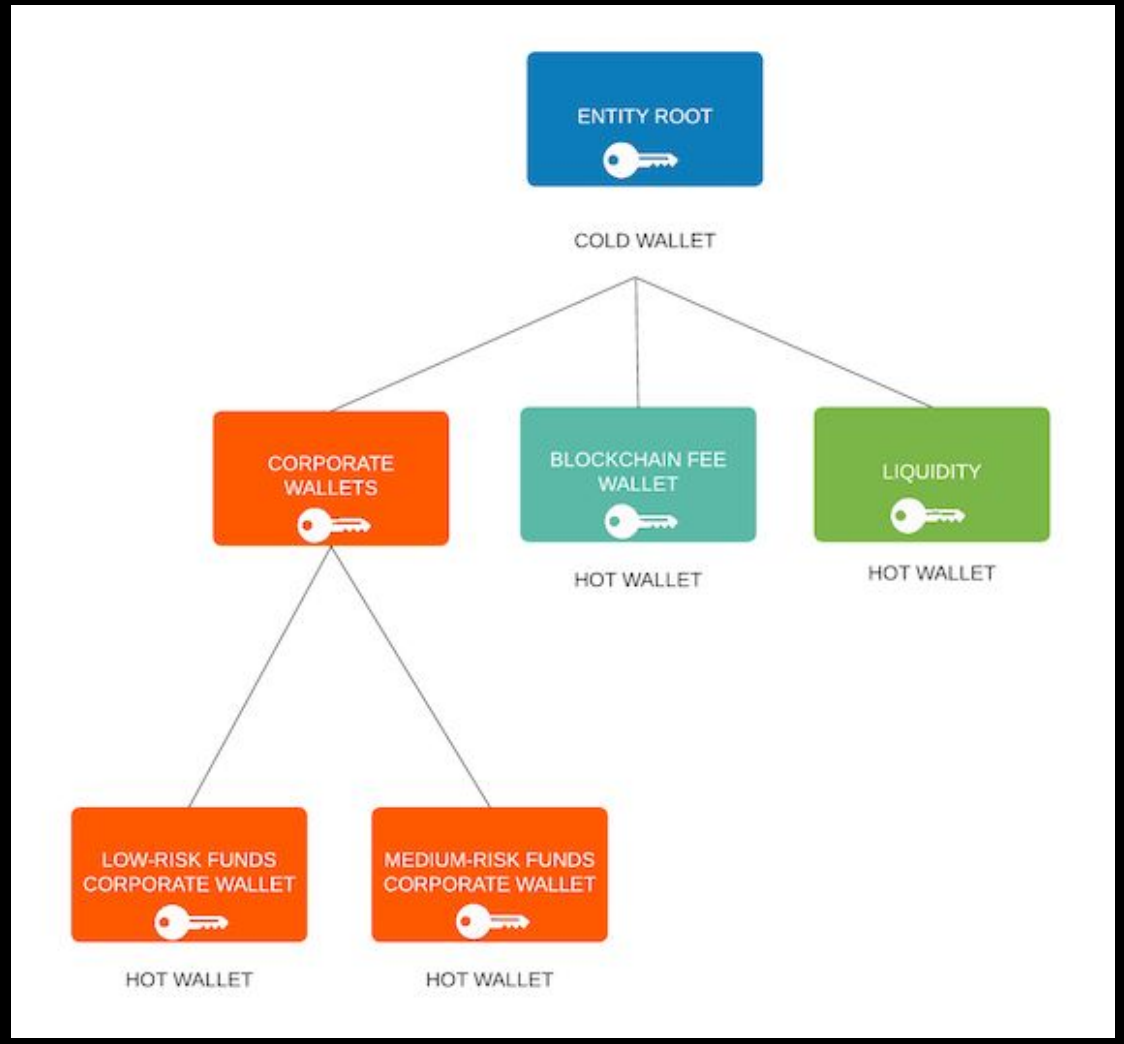
Hierarchical Deterministic Wallets

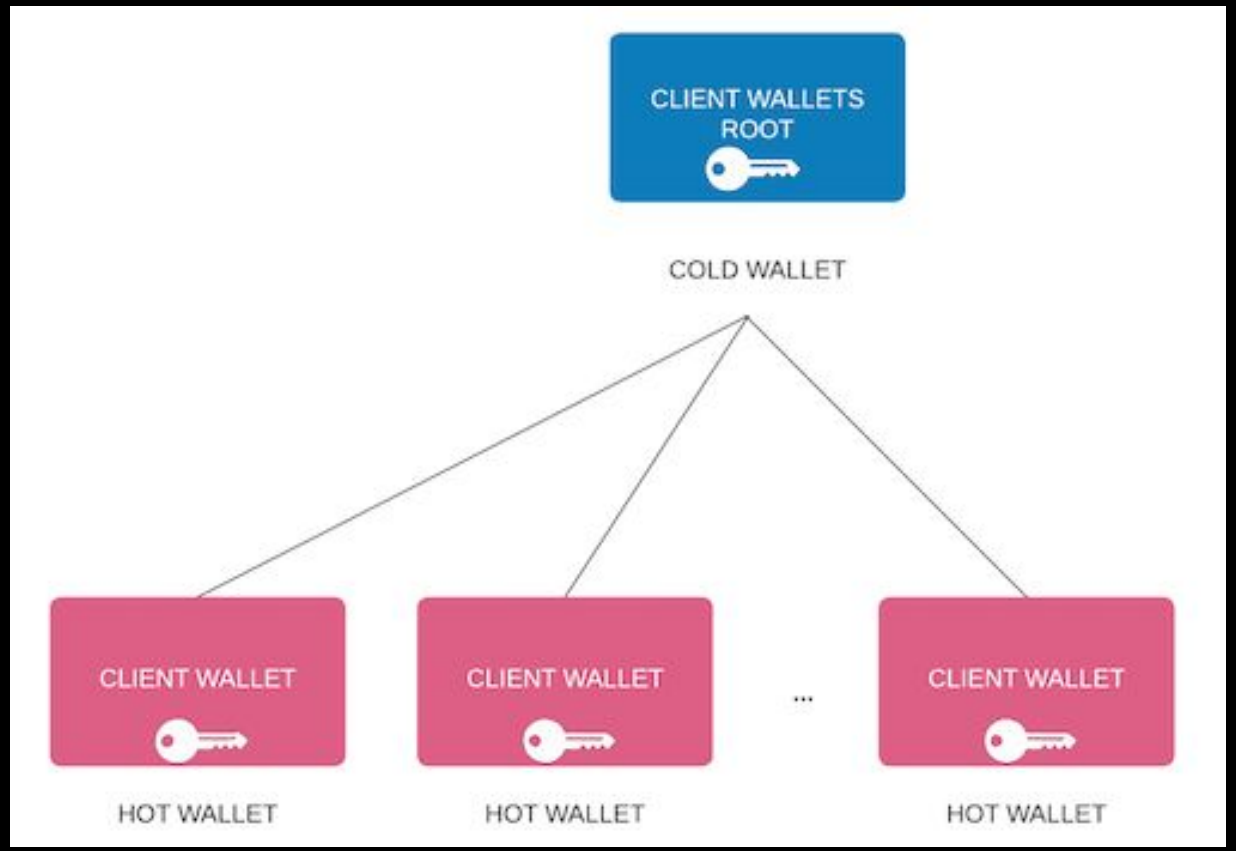


A **parent extended public key** together with a non-hardened **child private key** can expose the **parent private key**

https://medium.com/@blainemalone01/hd-wallets-why-hardened-derivation-matters-89efcdc71671
https://learnmeabitcoin.com/technical/extended-keys

Corporate Key Structure





HSM & TPM

Hardware Security Modules (HSMs) are hardware devices that can reside on a computer motherboard, but the more advanced models are contained in their own chassis as an **external device** and can be accessed via the network

Trusted Platform Modules (TPMs) are small hardware devices that are usually **embedded into computer motherboards** and are available as external devices

Both contains secret key(s) inside and can perform **cryptographic operations** with it **without exposing it to the outside**

Bitcoin Multisig (BIP-0011)

Mechanism that moves multiple signatures verification on the blockchain side.

scriptPubKey:

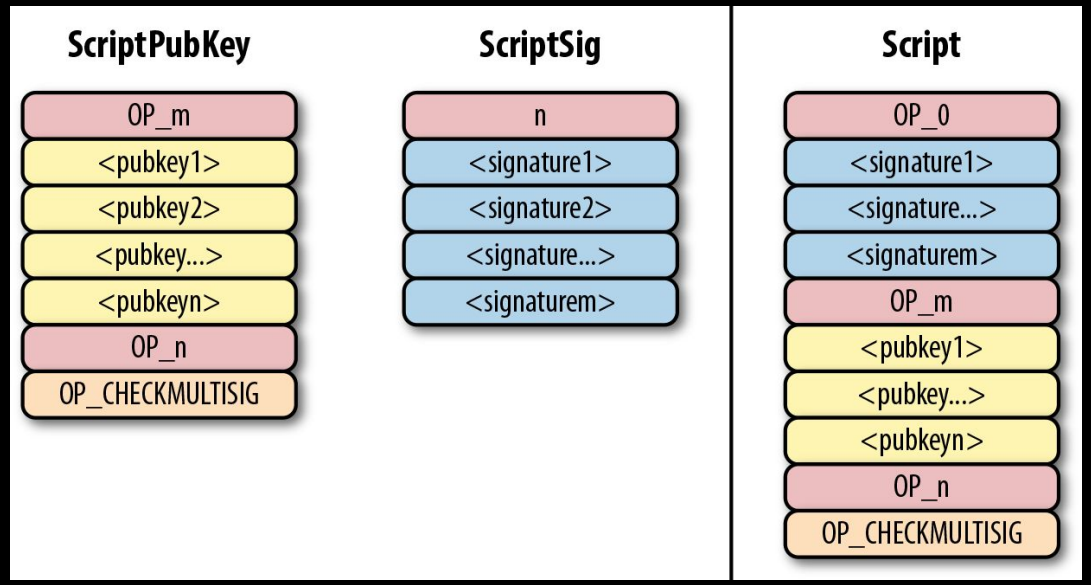
```
m {pubkey}...{pubkey} n OP_CHECKMULTISIG
```

scriptSig:

```
OP_0 ...signatures...
```

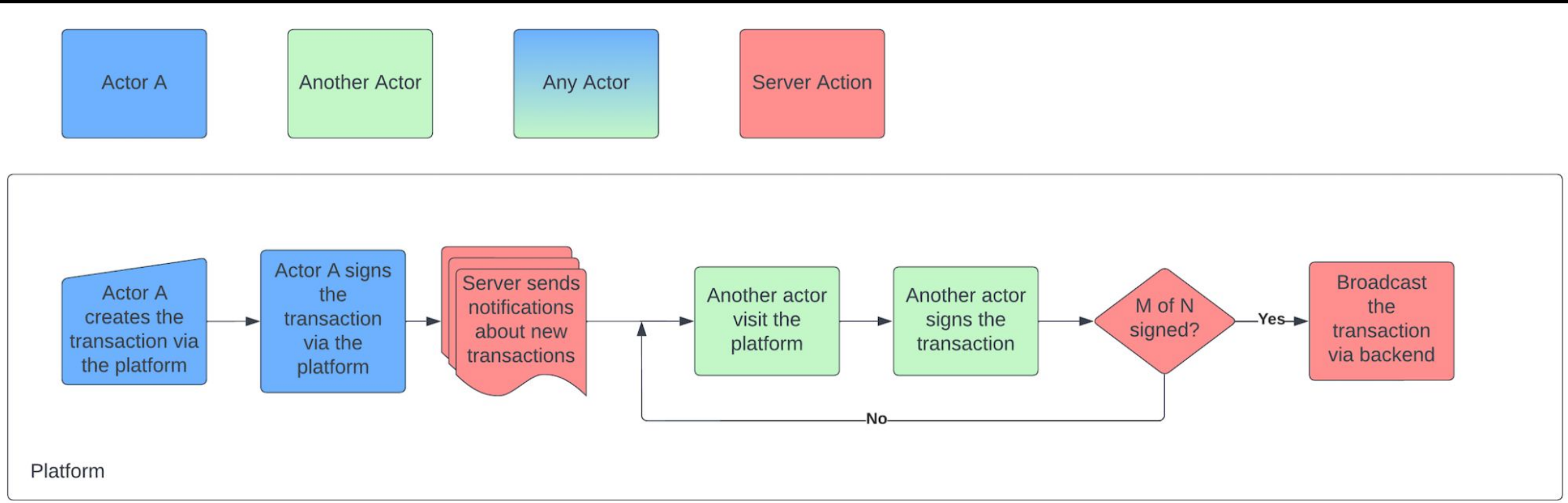
Order matters!

```
OP_0 sigB sigA OP_2 pubA pubB pubC OP_3
OP_CHECKMULTISIG -> fail
```

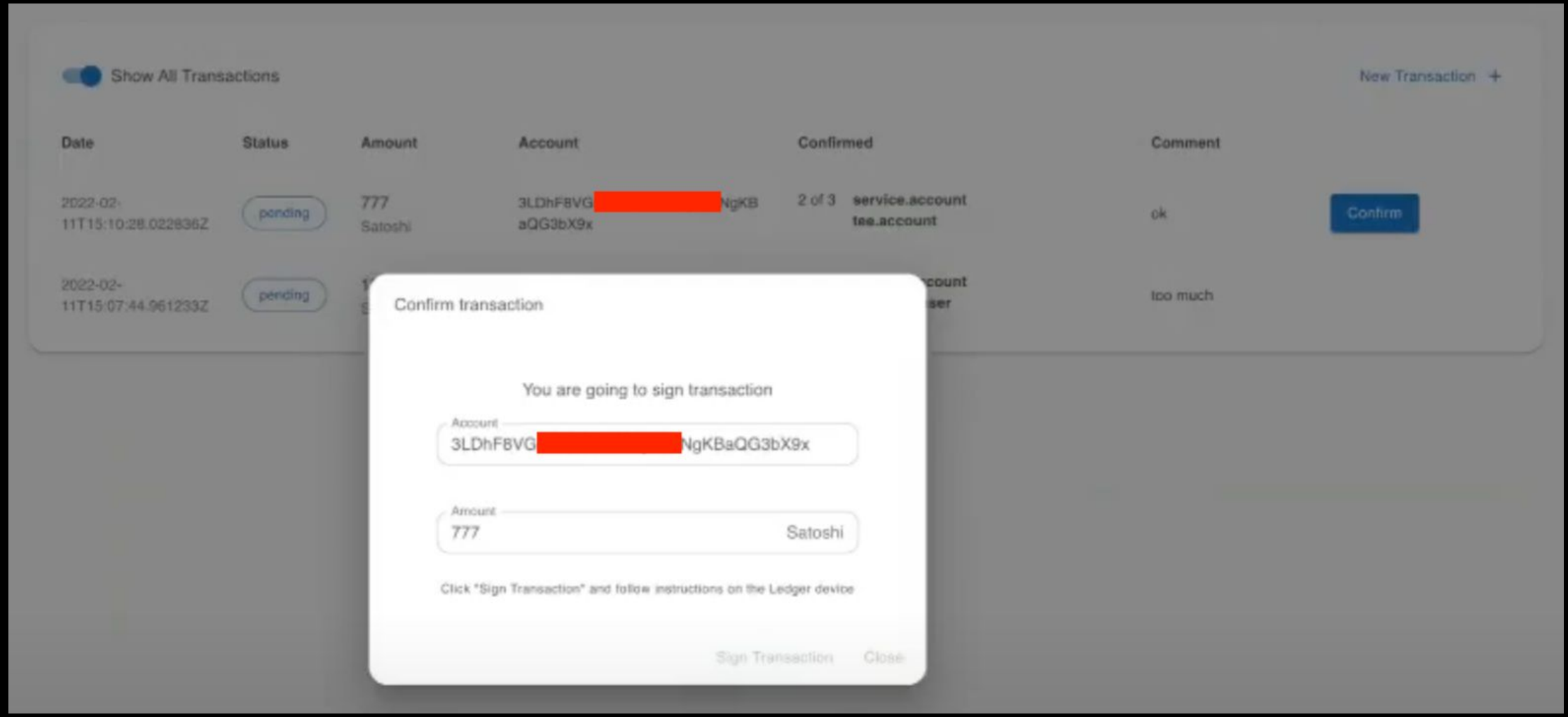


https://github.com/bitcoin/bips/blob/master/bip-0011.mediawiki

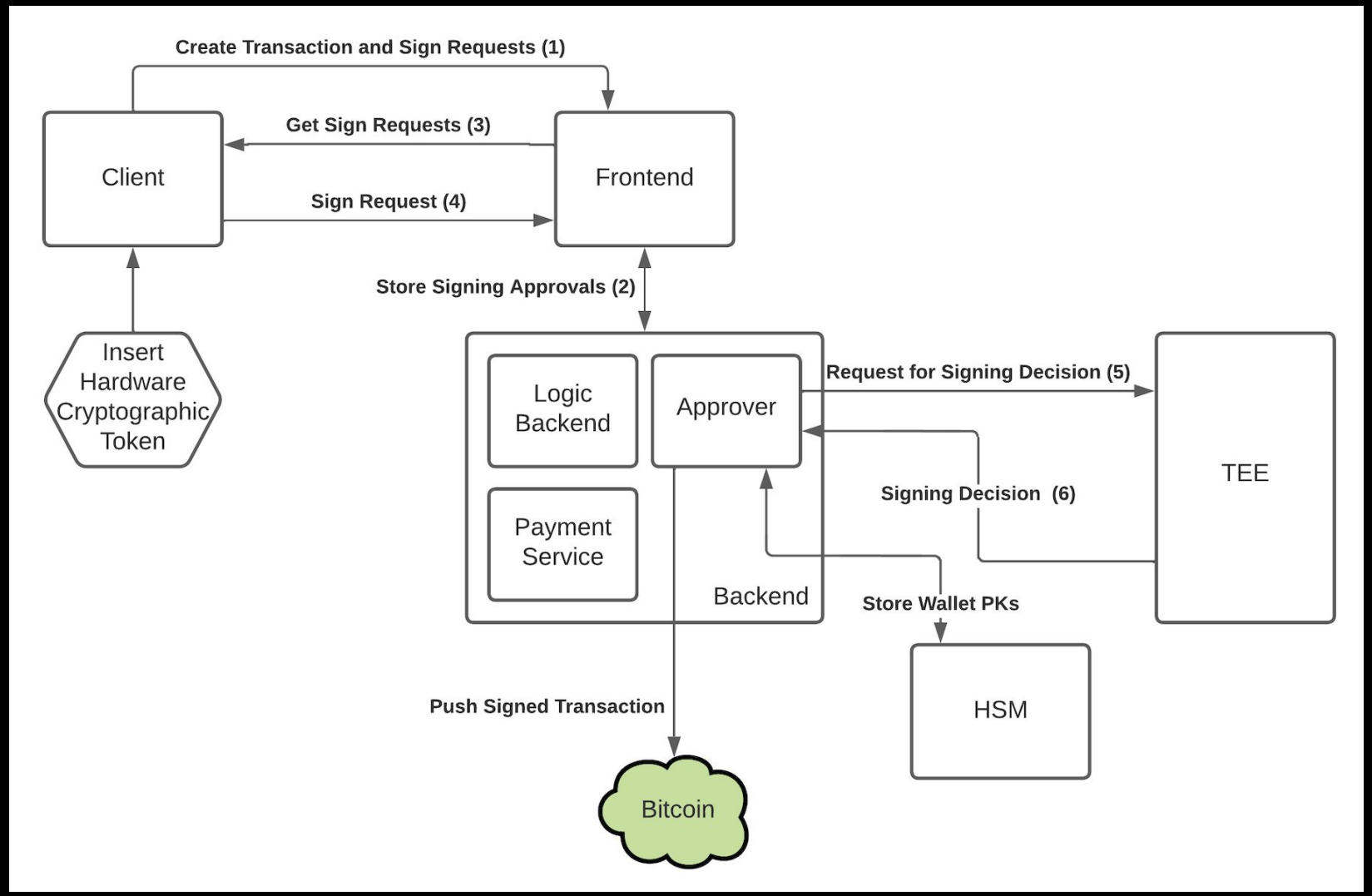
Real-World Bitcoin Multisig Implementation



Real-World Bitcoin Multisig Implementation



Real-World Bitcoin Multisig Implementation



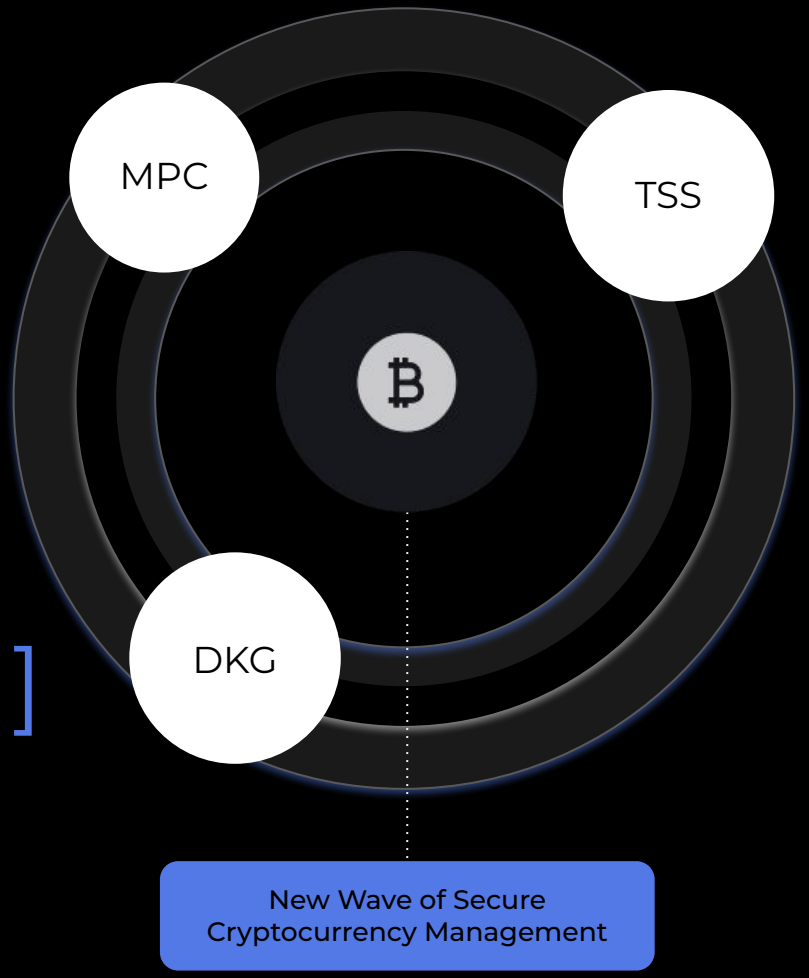
MPC, DKG, TSS

Multi-party computation

Allows to make the signature and derive the keys without having the private key in the same place

Distributed key generation

Allows to generate the private key parts without having the original one



Threshold signature scheme

Allows to make a signature of transaction having M of N required secret parts

- Can be combined with approaches like multisig & hd wallets
- Universal solution for multiple blockchains
- Requires more research for enterprise usage

https://github.com/ZenGo-X/awesome-tss
Multiple Bugs in Multi-Party Computation: https://www.youtube.com/watch?v=0Okqvm4lBQI


ON
FF
ONE
2022