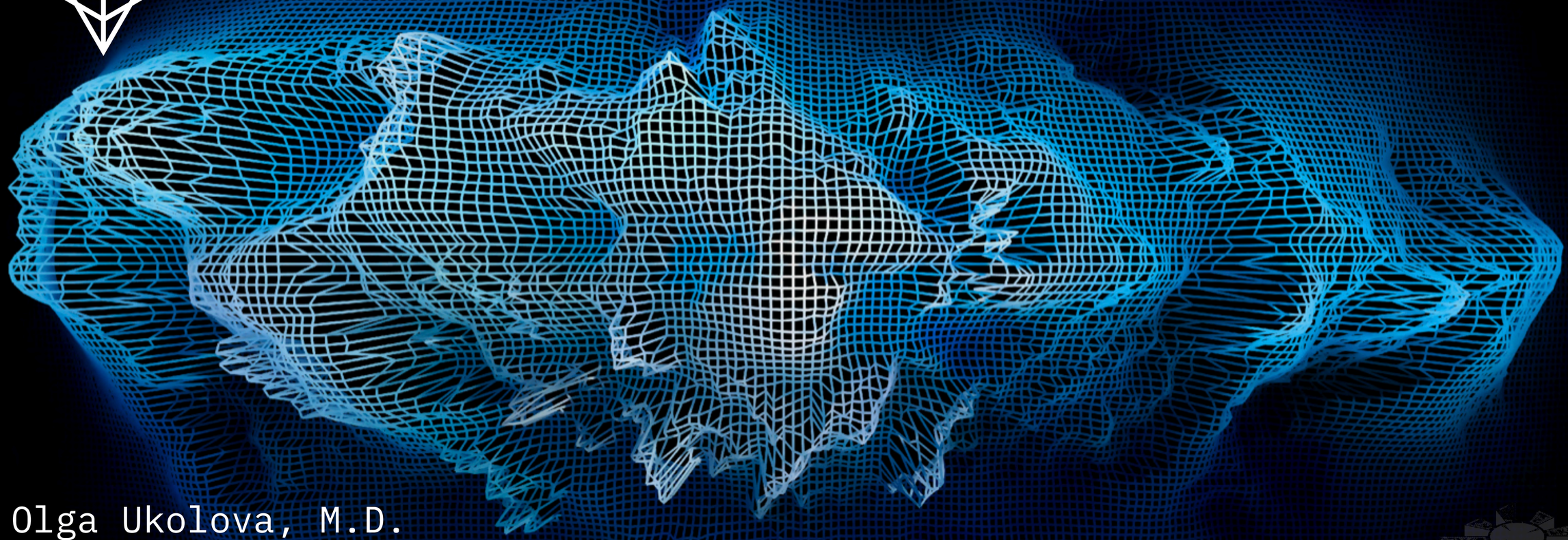
Pandora Prime

The #BiFi (Bitcoin Finance) company



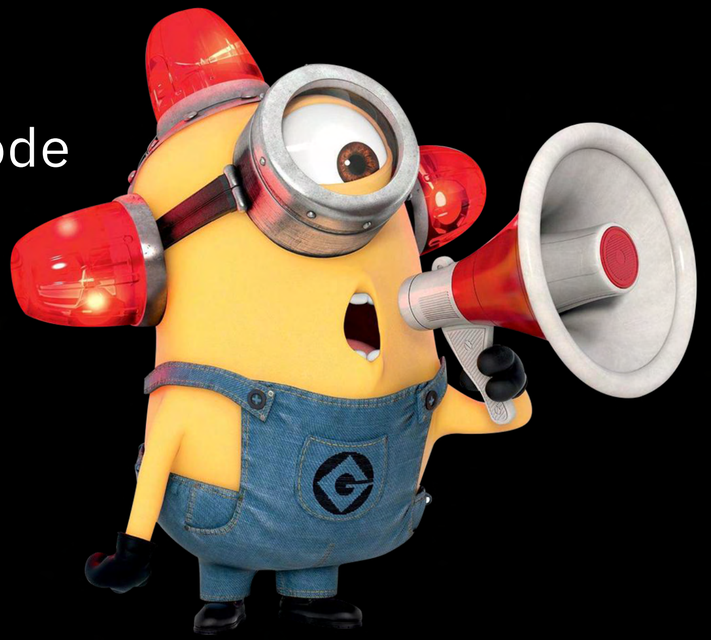
Olga Ukolova, M.D.

Board member of LNP/BP Standards Association

Co-Founder of Pandora Prime SA

DISCLAIMER!

- High toxicity content
- Cypherporn, cryptonudity
- 1984+
- Not suitable for pregnant children
- May contain traces of black magic code

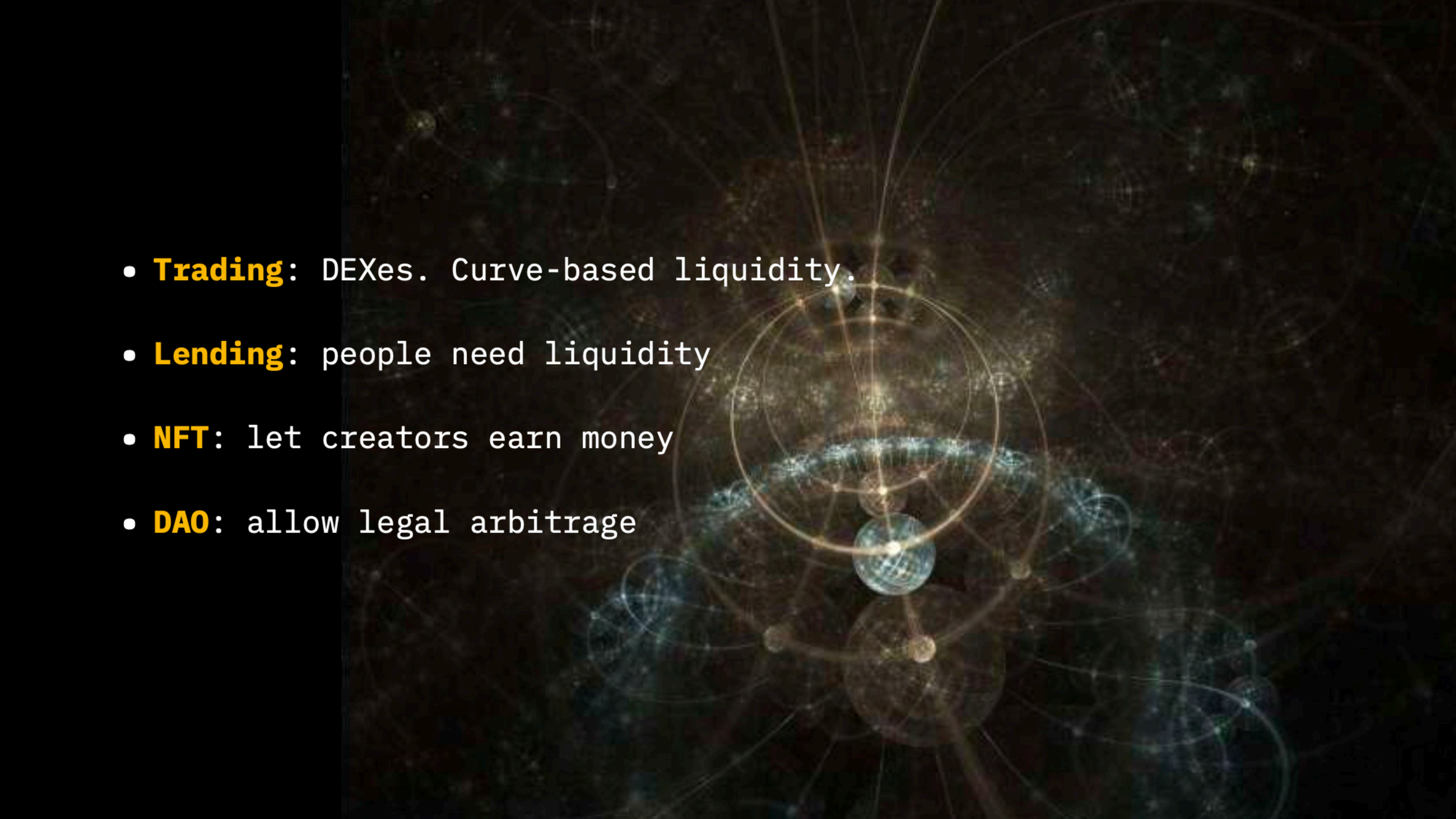


We have it all

We have it all

…don’t we?


There is a need for DeFi



- **Trading**: DEXes. Curve-based liquidity.
- **Lending**: people need liquidity
- **NFT**: let creators earn money
- **DAO**: allow legal arbitrage

DeFi

Expectation

- I am sovereign
- My data - my Citadel
- My peers = my tribe = my fam

Reality

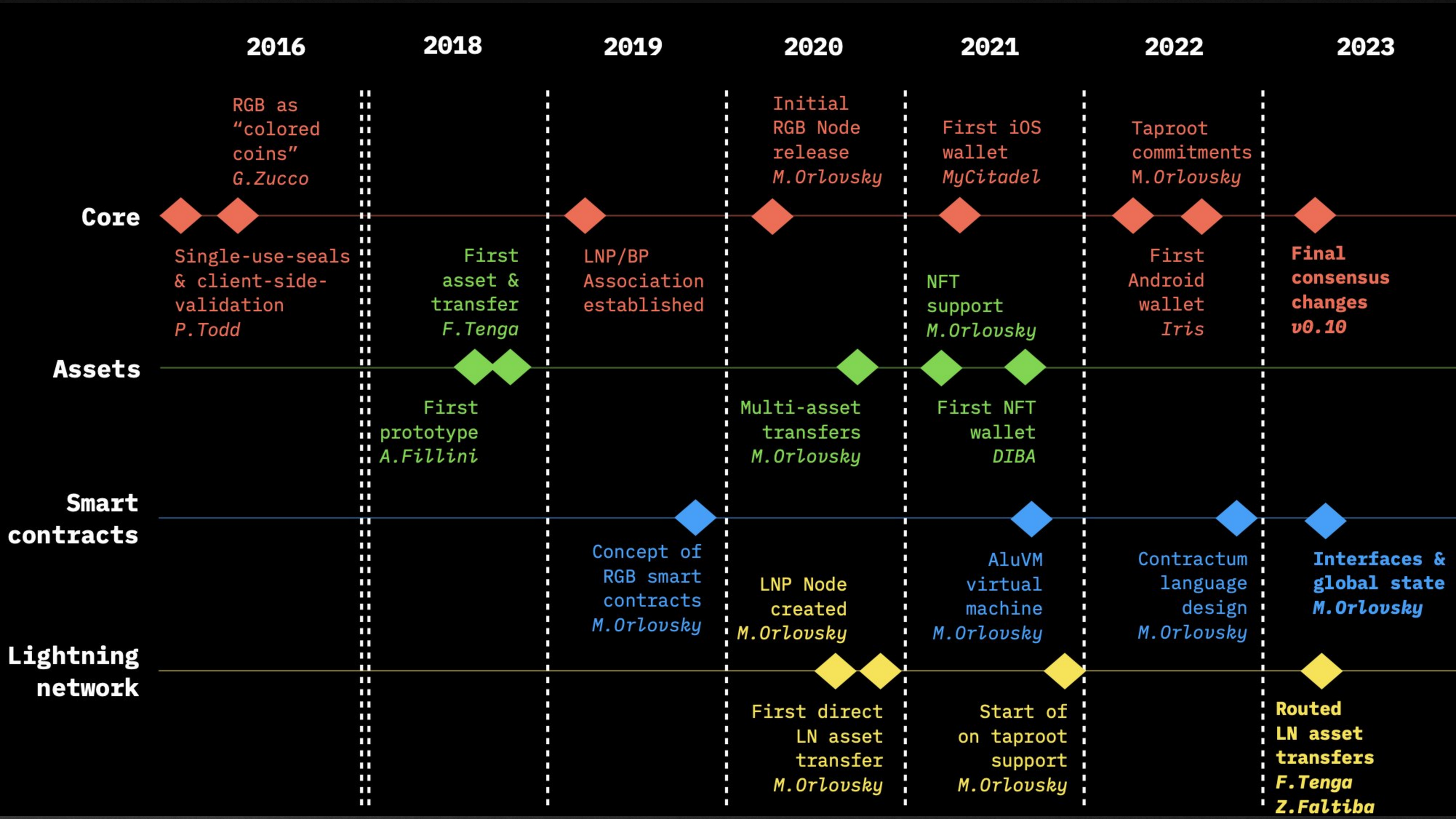
- Govern me harder Daddy
- We got HREKT (Hacked and REKT)
- Chainanalysis is my best friend

What is needed?

- Smart-contract system
- Private but verifiable
- Resistant to censorship but open for fair participation
- Scalable but without bloating the blockchain
- Fast but able to process big massives of data

RGB

RGB is scalable Turing-complete smart contracts for Bitcoin,
able to run on Lightning Network
zk-based, with strong privacy


2016
2018
2019
2020
2021
2022
2023
Core
Assets
Smart contracts
Lightning network
RGB as "colored coins" G.Zucco
Single-use-seals & client-side-validation P.Todd
First asset & transfer F.Tenga
First prototype A.Fillini
LNP/BP Association established
Concept of RGB smart contracts M.Orlovsky
Initial RGB Node release M.Orlovsky
Multi-asset transfers M.Orlovsky
LNP Node created M.Orlovsky
First direct LN asset transfer M.Orlovsky
First iOS wallet MyCitadel
NFT support M.Orlovsky
First NFT wallet DIBA
AluVM virtual machine M.Orlovsky
Start of on taproot support M.Orlovsky
Taproot commitments M.Orlovsky
First Android wallet Iris
Contractum language design M.Orlovsky
Final consensus changes v0.10
Interfaces & global state M.Orlovsky
Routed LN asset transfers F.Tenga Z.Faltiba

RGB IS:

- smart-contract system*
- DAG
- No native token
- Private
- The only tech that works over Lightning Network
- Blockchain agnostic

**Smart contract* - *is the way to enforce the fulfillment of a certain agreement between humans without an external centralized agency (military, government, court etc)*

RGB paradigms:

- **Client-side validation** - all the data is kept outside of the bitcoin transactions, i.e. bitcoin blockchain or lightning channel state
- **Single-use seals** - abstract mechanism to prevent double-spends
- **Cryptographic commitments**
- **Strict encoding**

https://github.com/LNP-BP/rust-lnpbp/tree/refactor-structure/src/paradigms

	AluVM	Bitcoin script	EVM, kEVM, IELE	WASM	JVM, CLR	LLVM
Type	Register	Stack	Stack	Stack	Stack	Stack
Random memory access	No	No	No	Yes	Yes	Yes
Dynamic memory allocations	No	Yes	Yes	Yes	Yes	Yes
I/O operations	No	No	No	Via extensions	Yes	Yes
Turing completeness	Yes (bounded)	No	Yes (bounded)	Yes	Yes	Yes
Static analysis	Simple	Simple	Complex	Hard	Hard	Hard
Sandboxing	Always	Always	Always	Poor	No native	No native
Runtime environment	Any sandboxed	UTXO blockchain	Account-based blockchain	Internet	OS	Compiler
Library code immutability	Yes	No libraries	Yes	No	No	No
Undefined behavior (UB)	Impossible	Possible	Possible	Possible	Possible	Possible

Info-resources

LNP/BP Standards Association

- www.rgbfaq.com
- www.rgb.tech

- LNP/BP Standards Association
  https://twitter.com/lnp_bp
- RGB Community
  https://twitter.com/i/communities/1585365616743022595

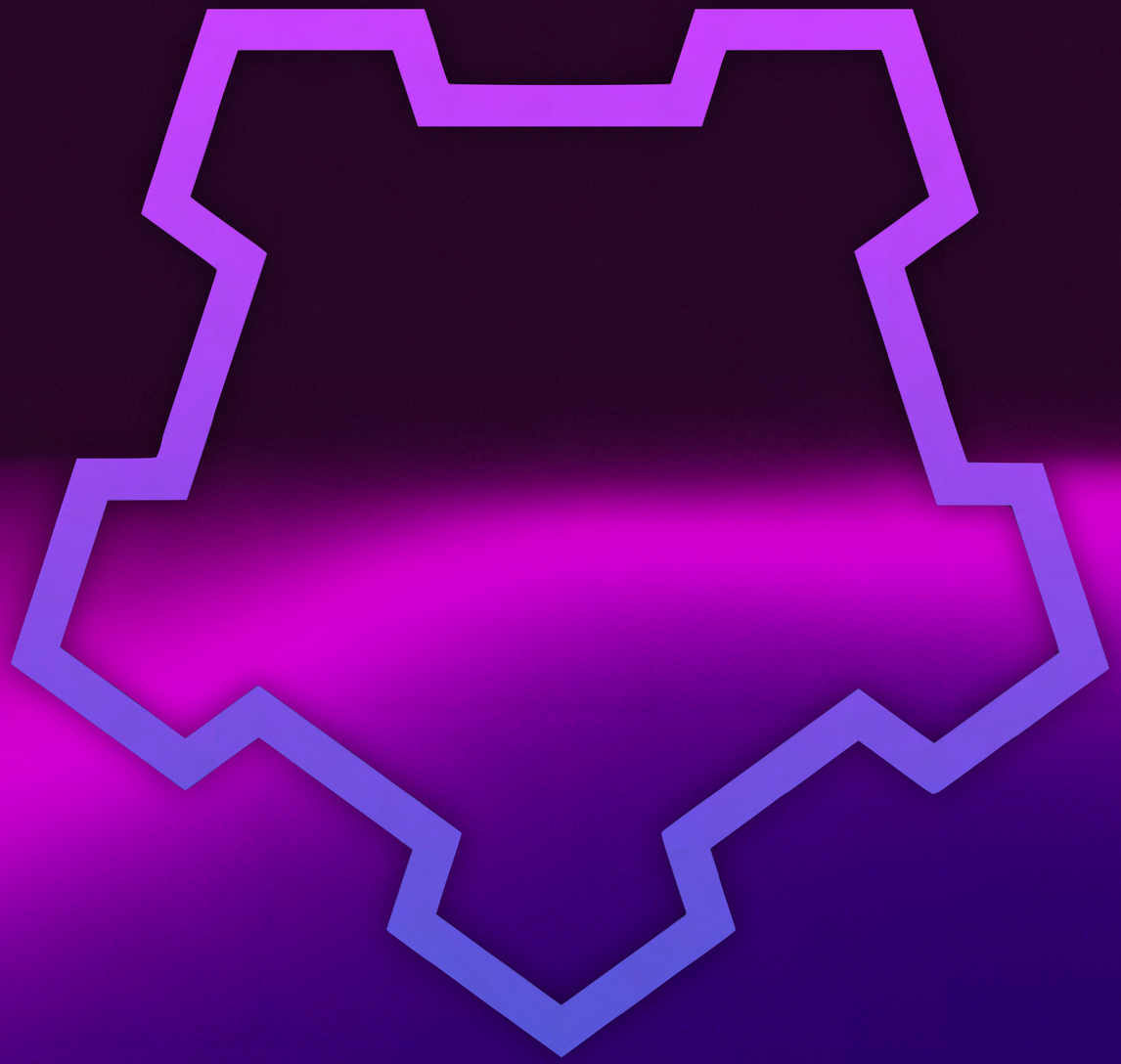
- LNP/BP Standards YouTube channel
  http://youtube.com/c/LNPBP

- RGB Telegram chat
  https://t.me/rgbtelegram
- LNP/BP Telegram channel
  https://t.me/lnp_bp

But how to custody and manage assets in the safest way?

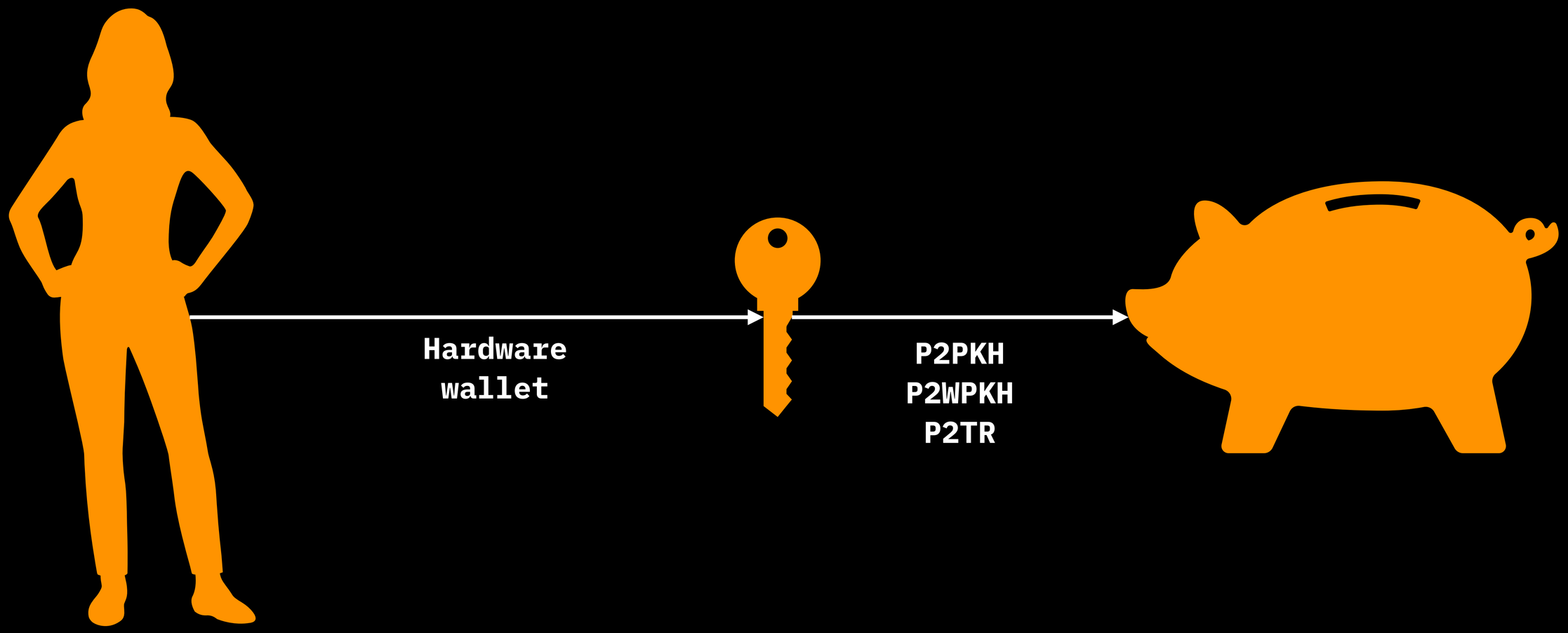
Self-sovereignty is hard

MyCitadel was created to make it reachable



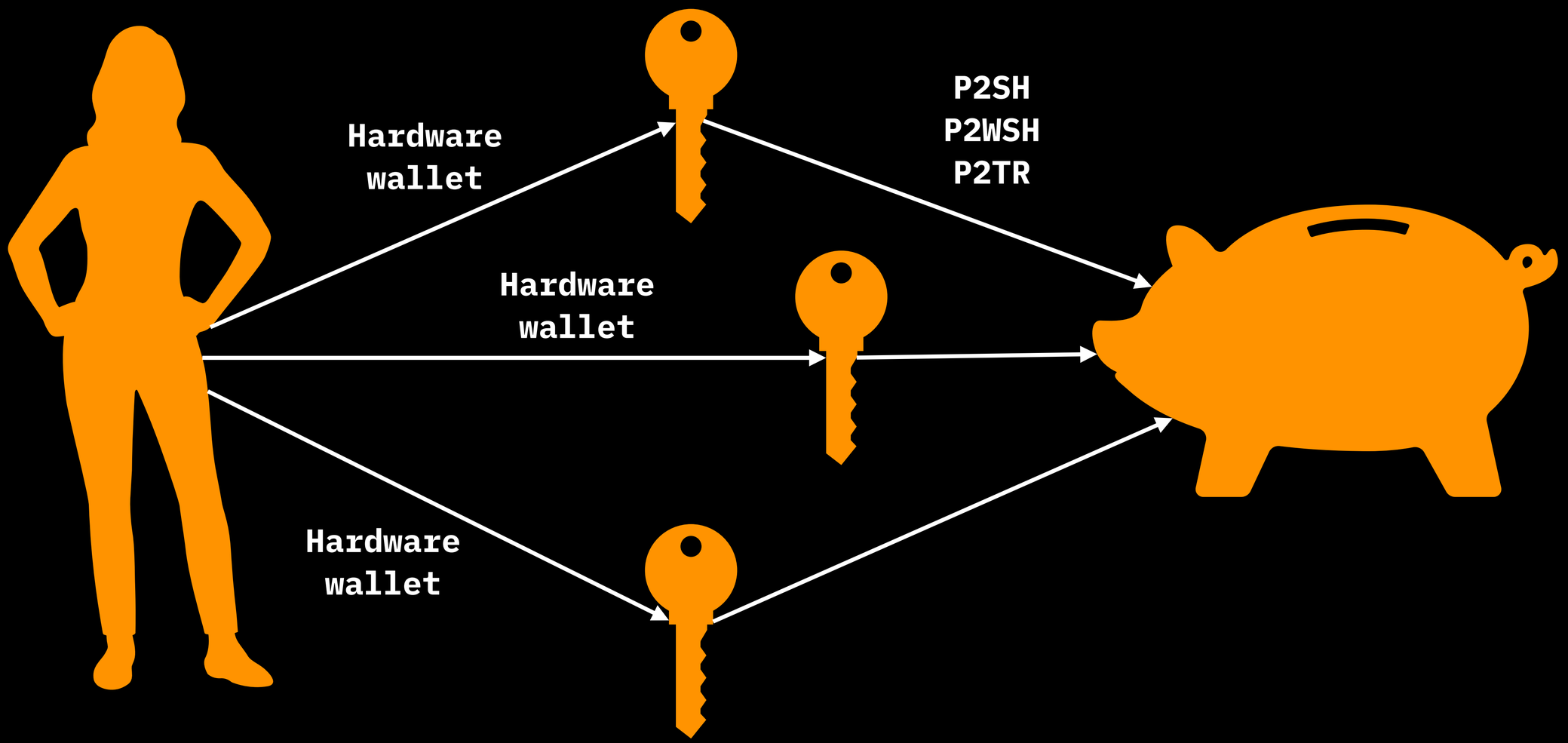
Hardware wallets

Own your key

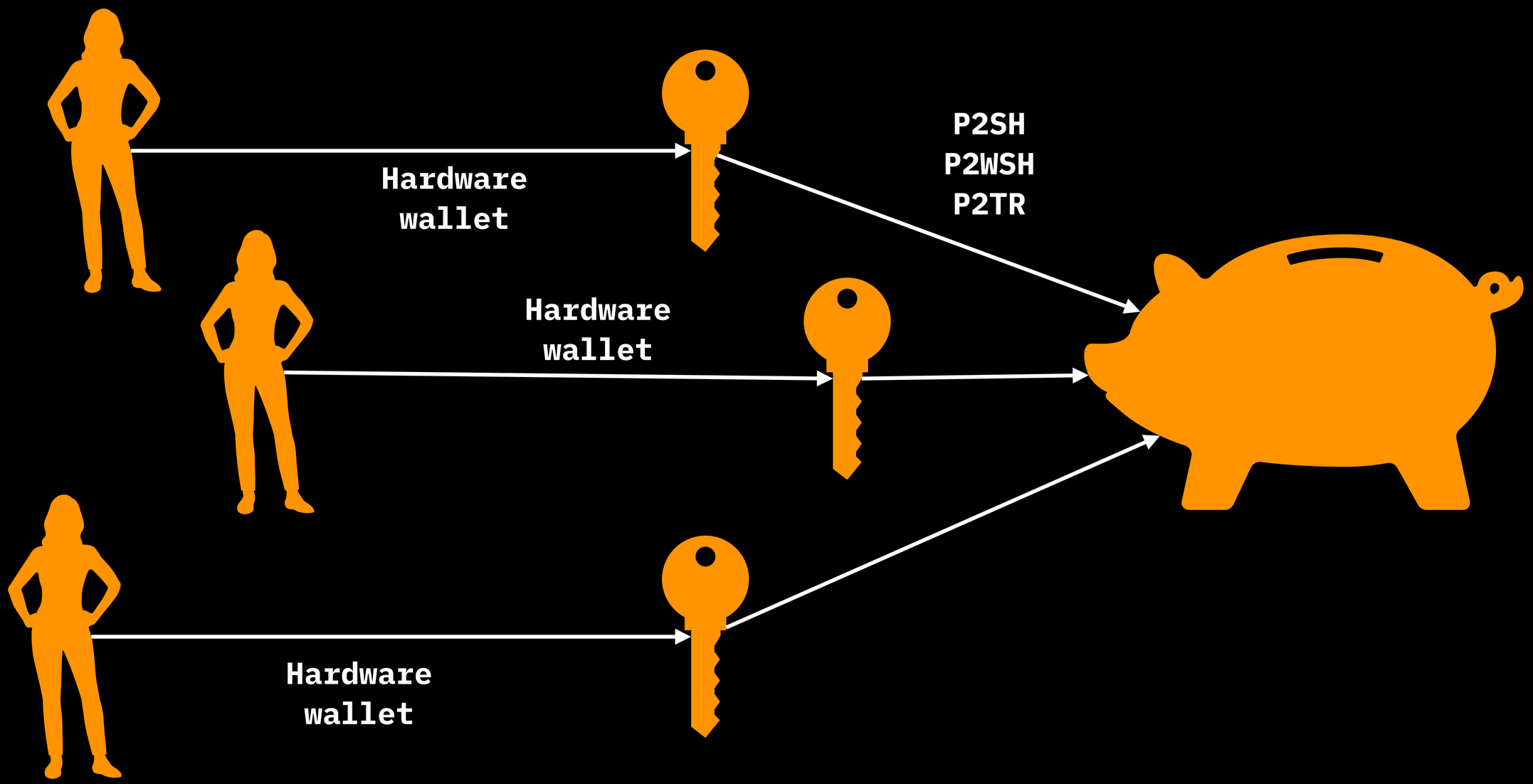


- Seed leak
- Not applicable to orgs
- Not applicable to shared accounts
- No inheritance plan

Make keys multiple!

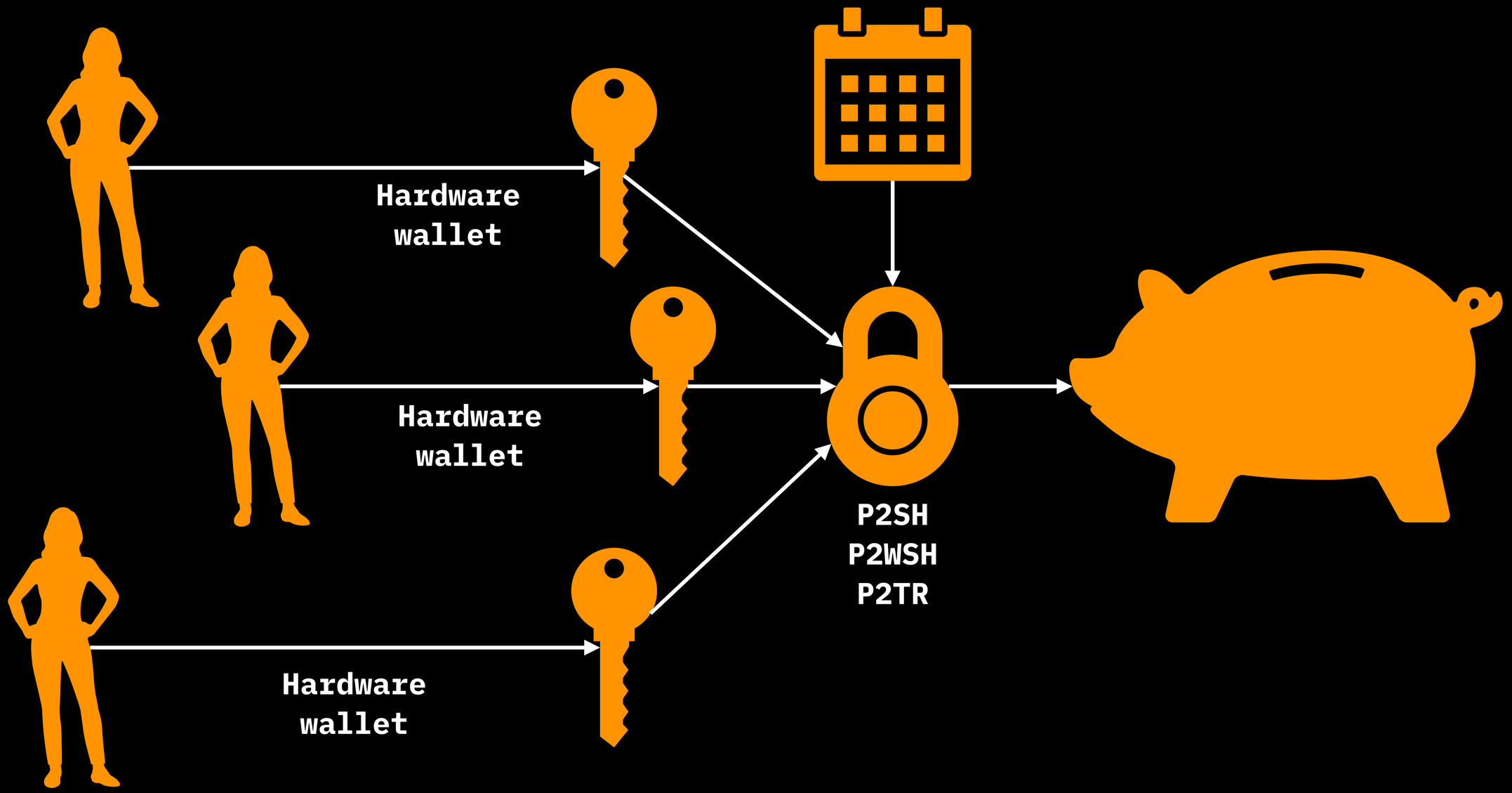


Make keys multiple!

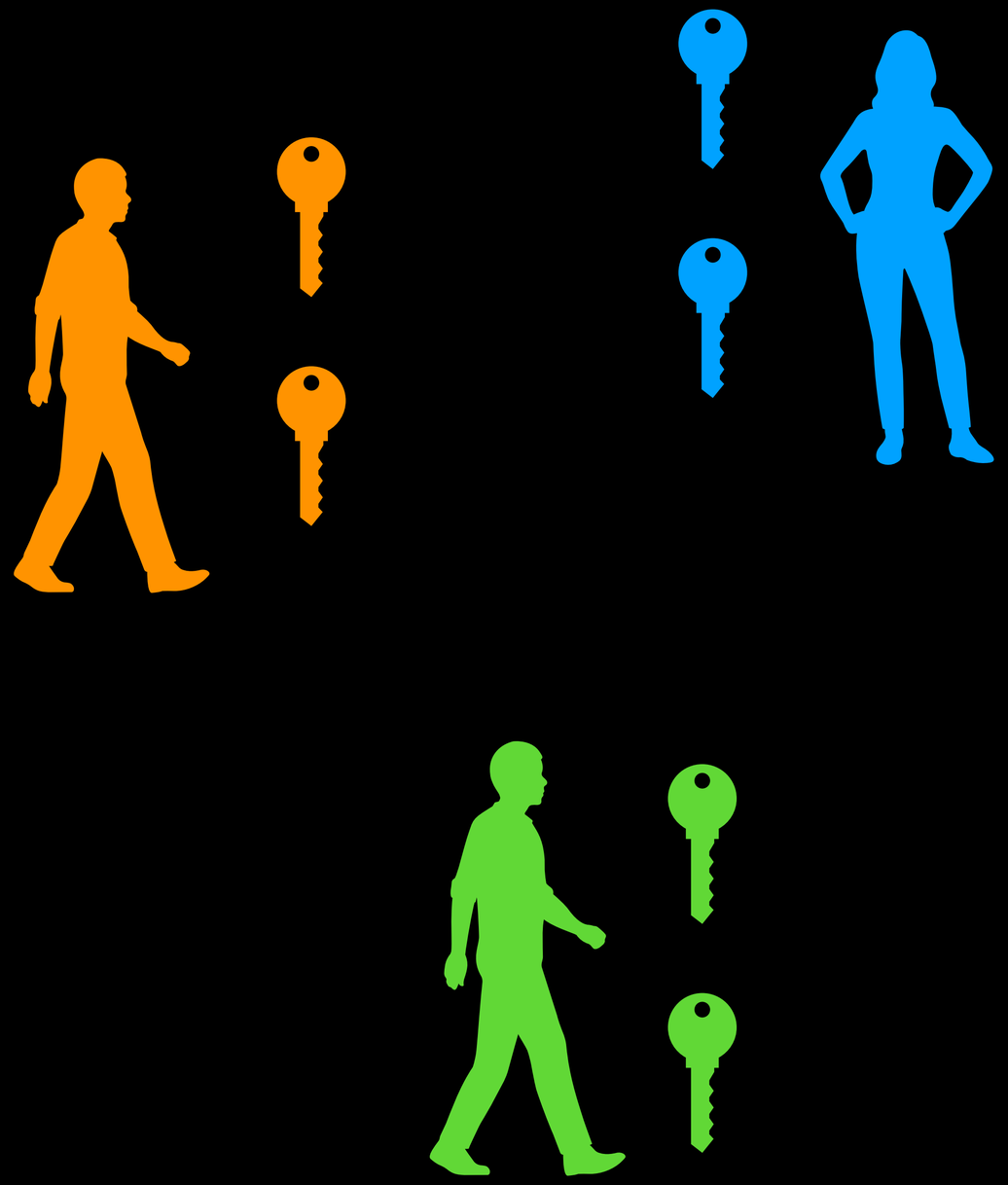


- Seed leak
- Not applicable to orgs (firing people etc)
- No inheritance plan

Different spending conditions

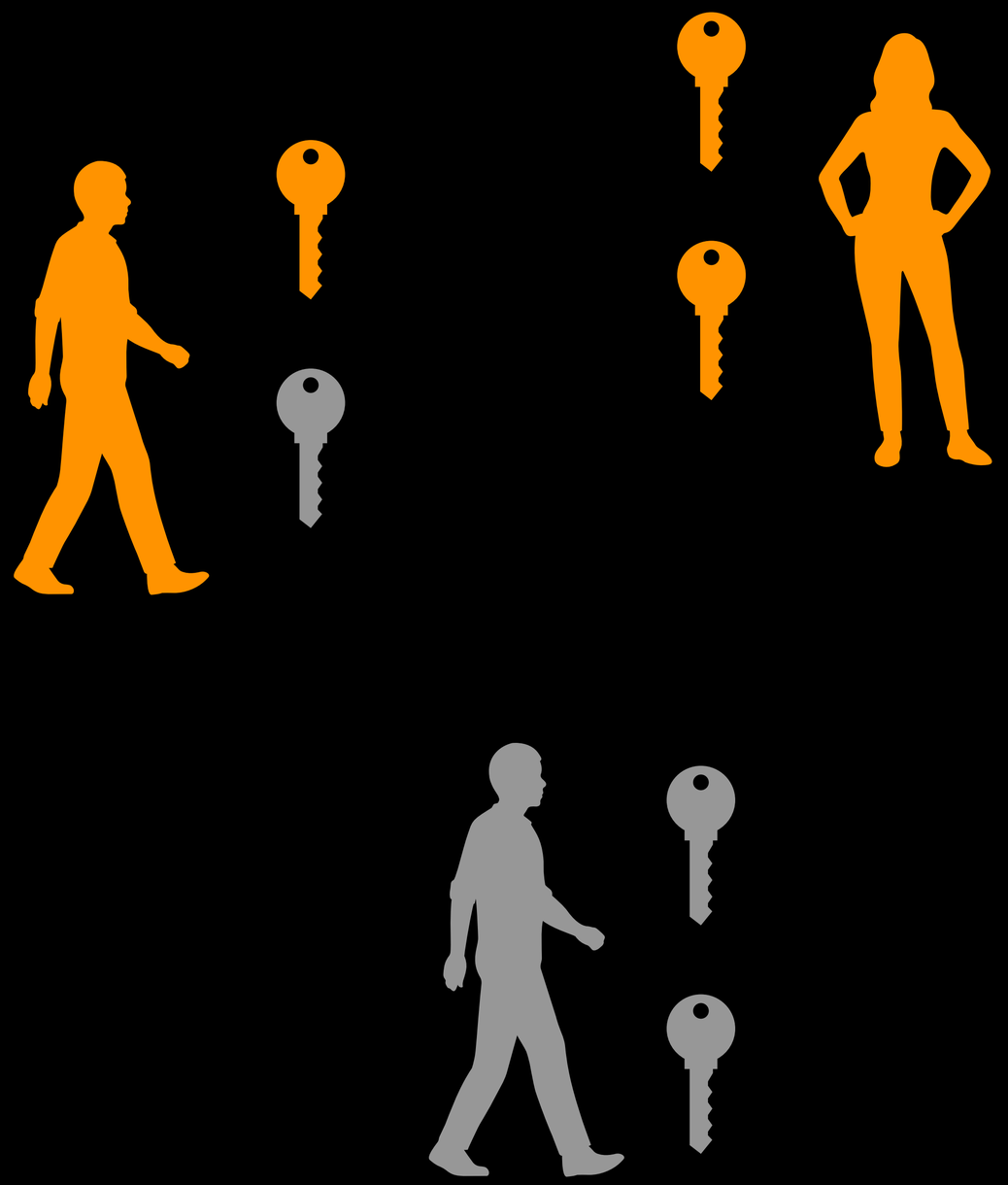


Example org



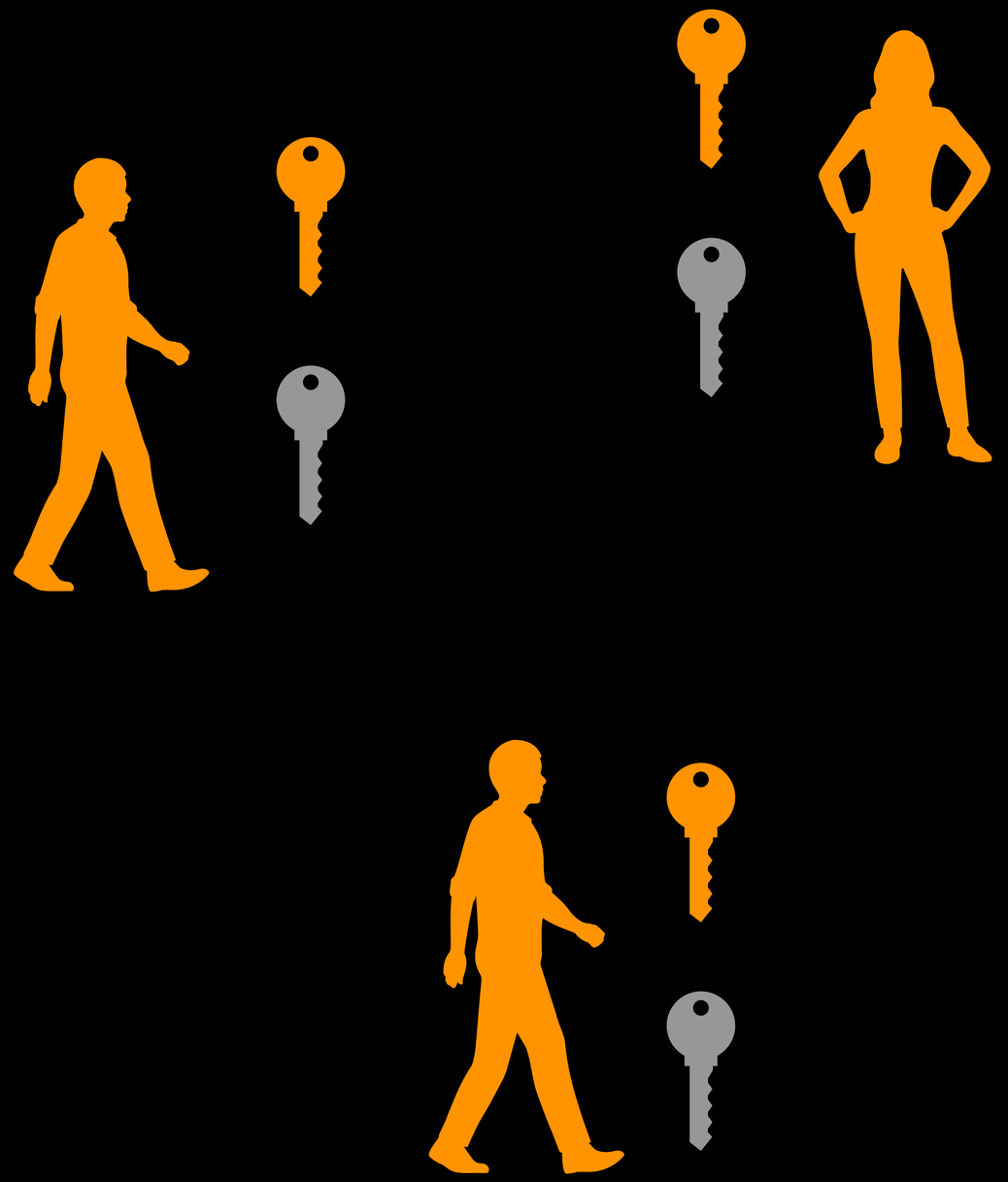
Example org

- 3-of-6 multisig at any moment of time



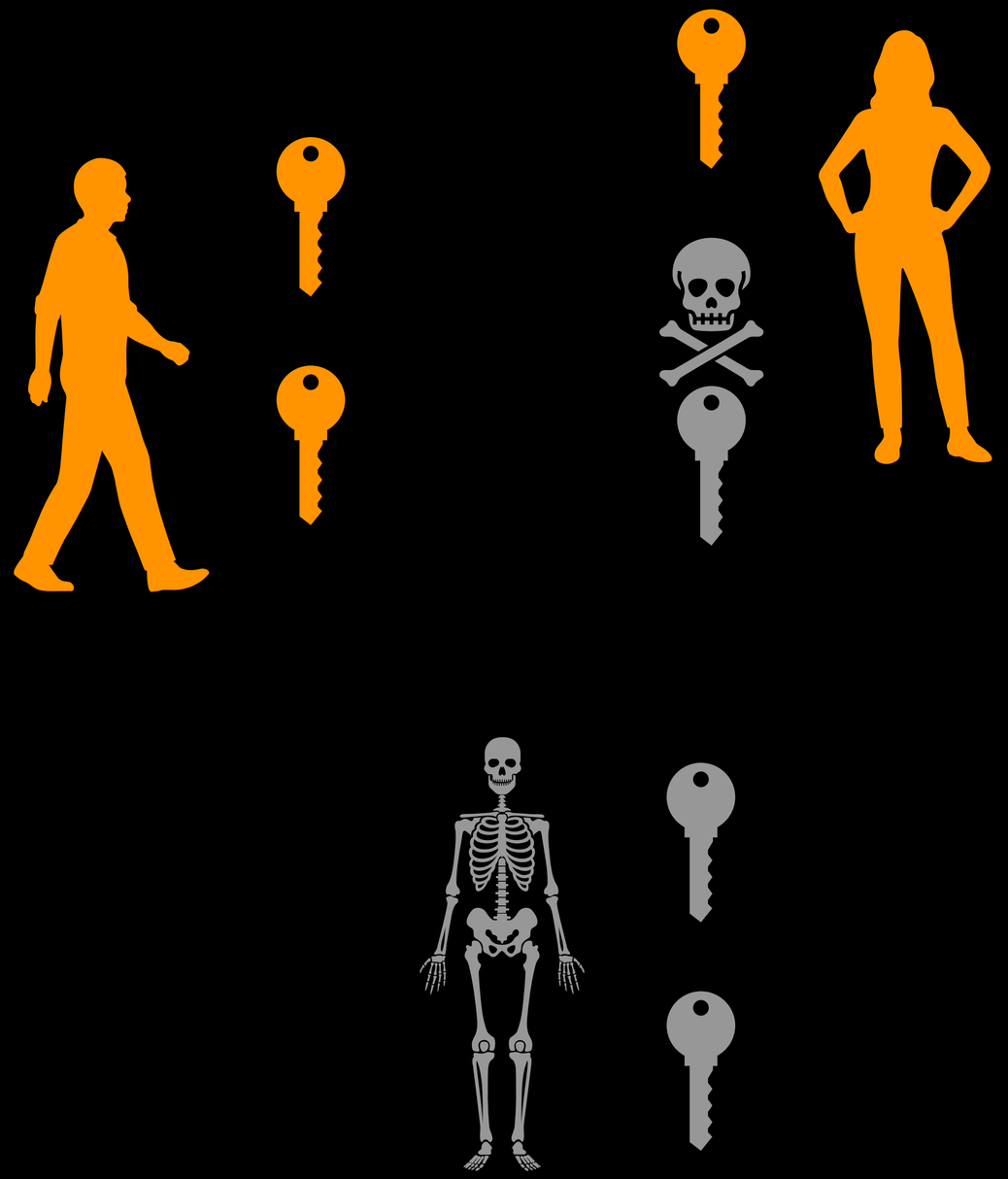
Example org

- 3-of-6 multisig at any moment of time



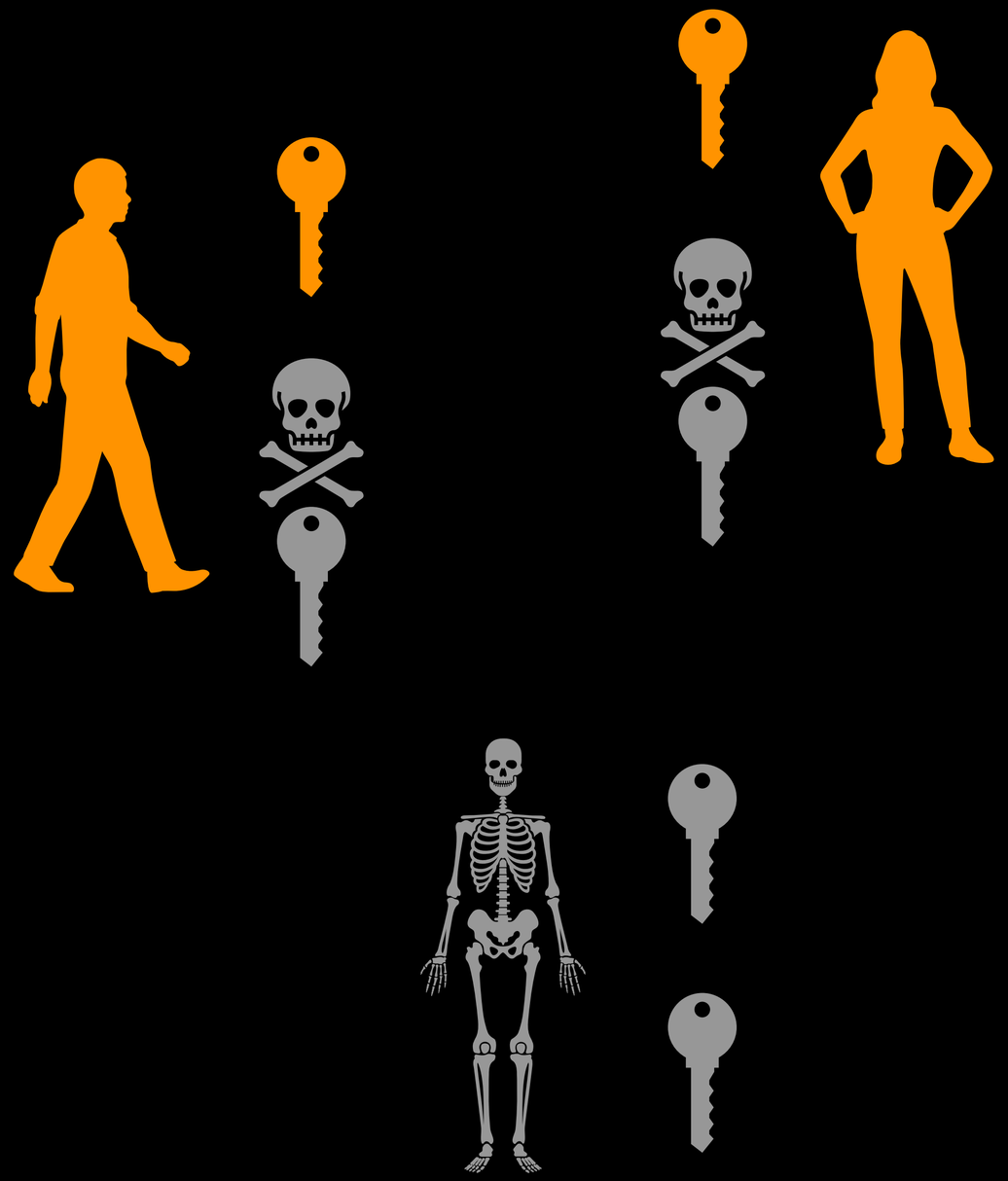
Example org

- 3-of-6 multisig at any moment of time



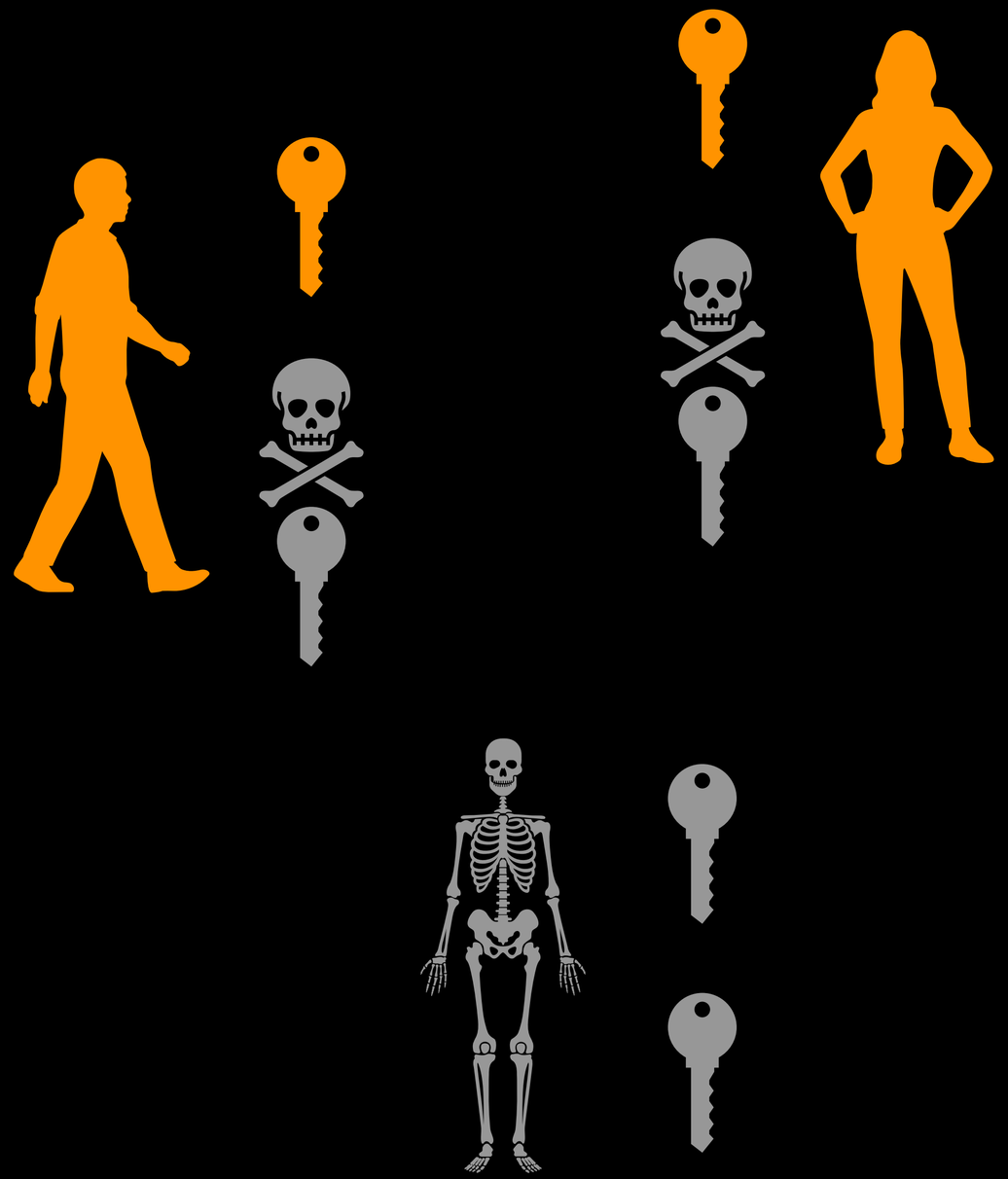
Example org

- 3-of-6 multisig at any moment of time



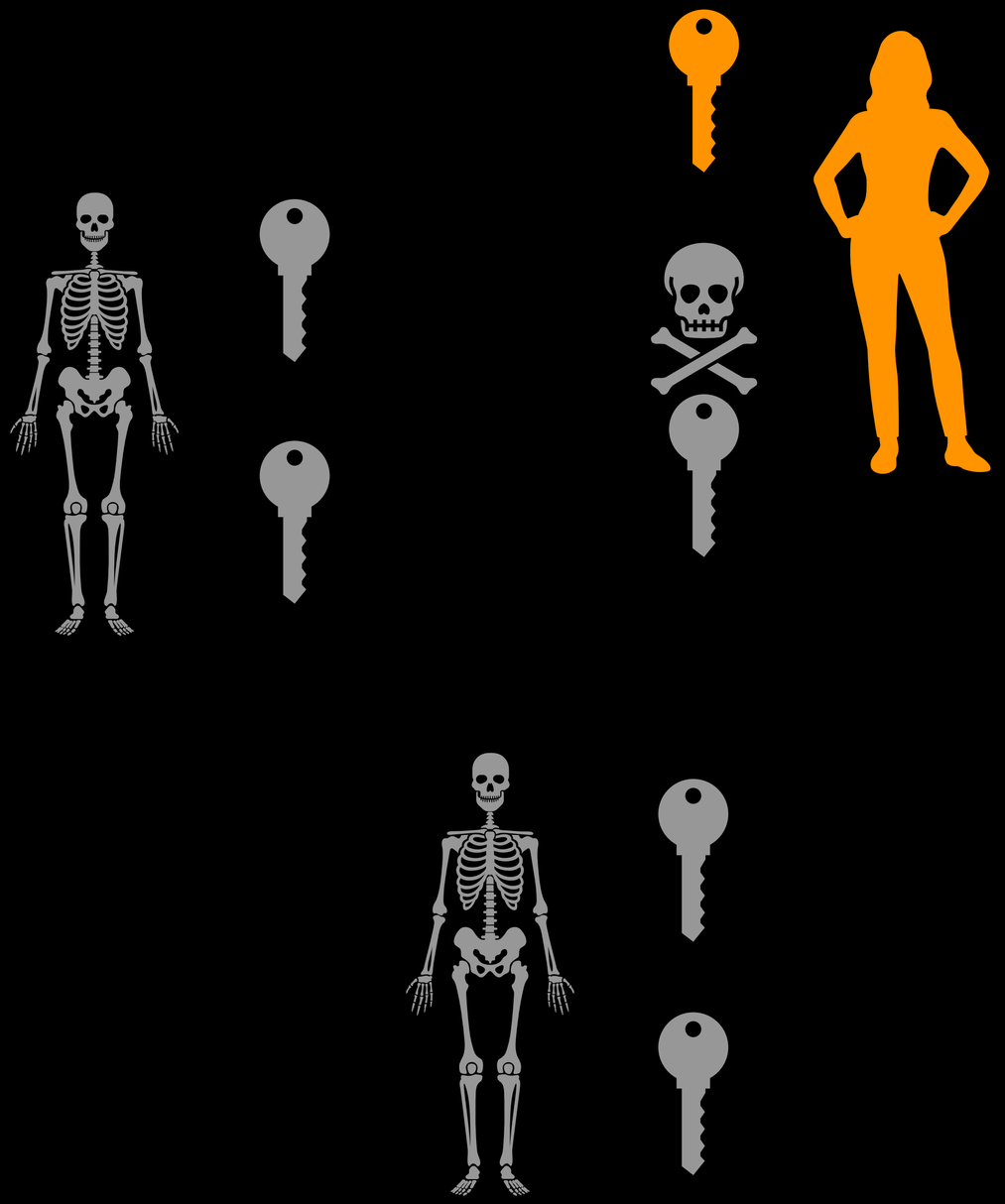
Example org

- 3-of-6 multisig at any moment of time
- 2-of-6 in 2 years



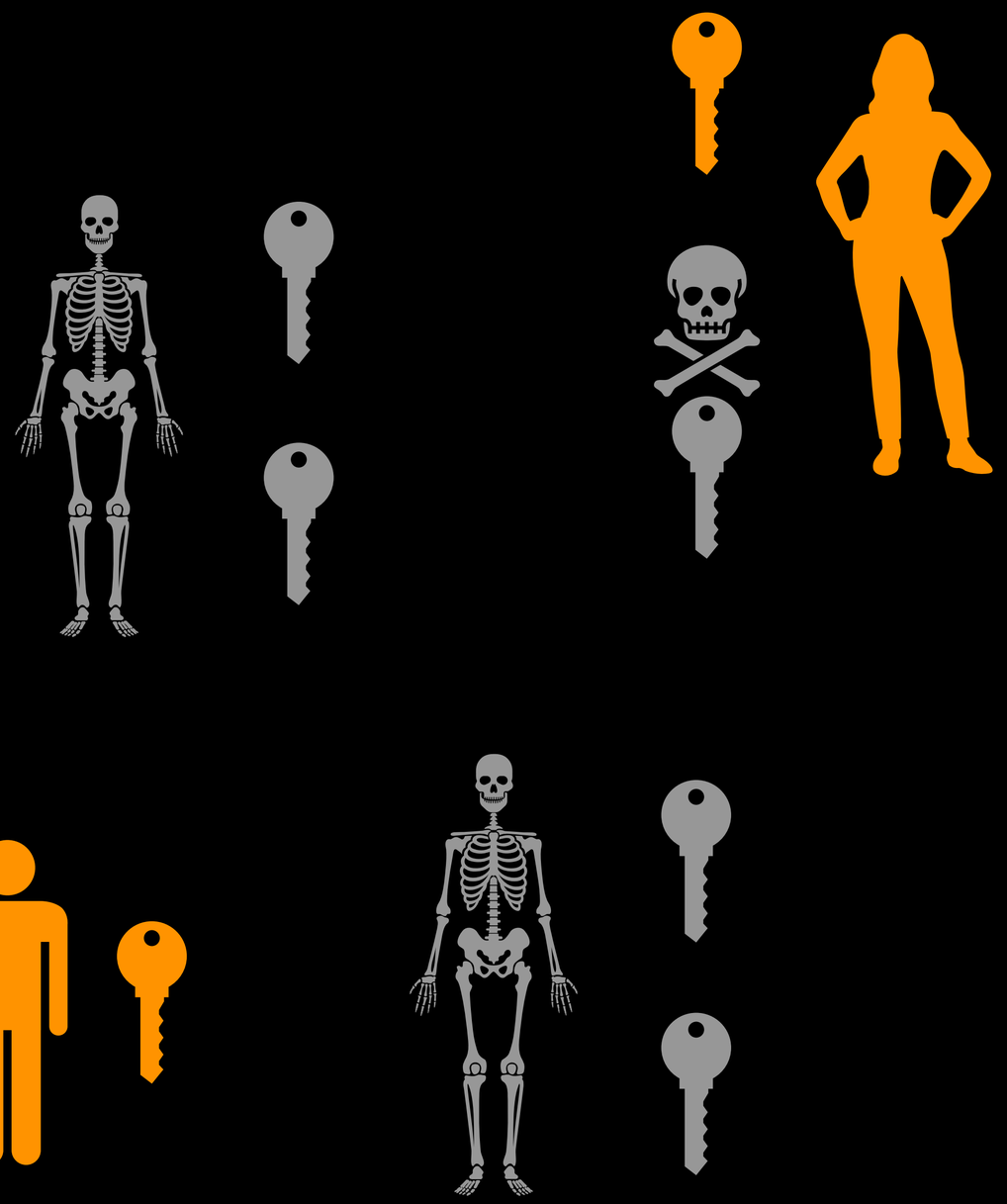
Example org

- 3-of-6 multisig at any moment of time
- 2-of-6 in 2 years
- any single key in 3 years



Example org

- 3-of-6 multisig at any moment of time
- 2-of-6 in 2 years
- lawyer’s key + any other key in 3 years



- Inheritance & families
- Corporations
- DAOs

Can we do it today?

- Yes, with Taproot!
  — **wait, no**: hardware wallets don’t support any taproot scripting

Can we do it today?

- Yes, with Taproot!
  — **wait, no**: hardware wallets don’t support any taproot scripting

- Yes, with SegWit & miniscript!
  — **wait, no**: miniscript prohibits re-use of the same keys in different conditions

Can we do it today?

- Yes, with Taproot!
  – **wait, no**: hardware wallets don’t support any taproot scripting
- Yes, with SegWit & miniscript!
  – **wait, no**: miniscript prohibits re-use of the same keys in different conditions
- Just use SegWit with multiple devices per user
  – **wait, no**: very hard to manage, and quite expensive

Can we do it today?

- Yes, with Taproot!
  — **wait, no**: hardware wallets don’t support any taproot scripting

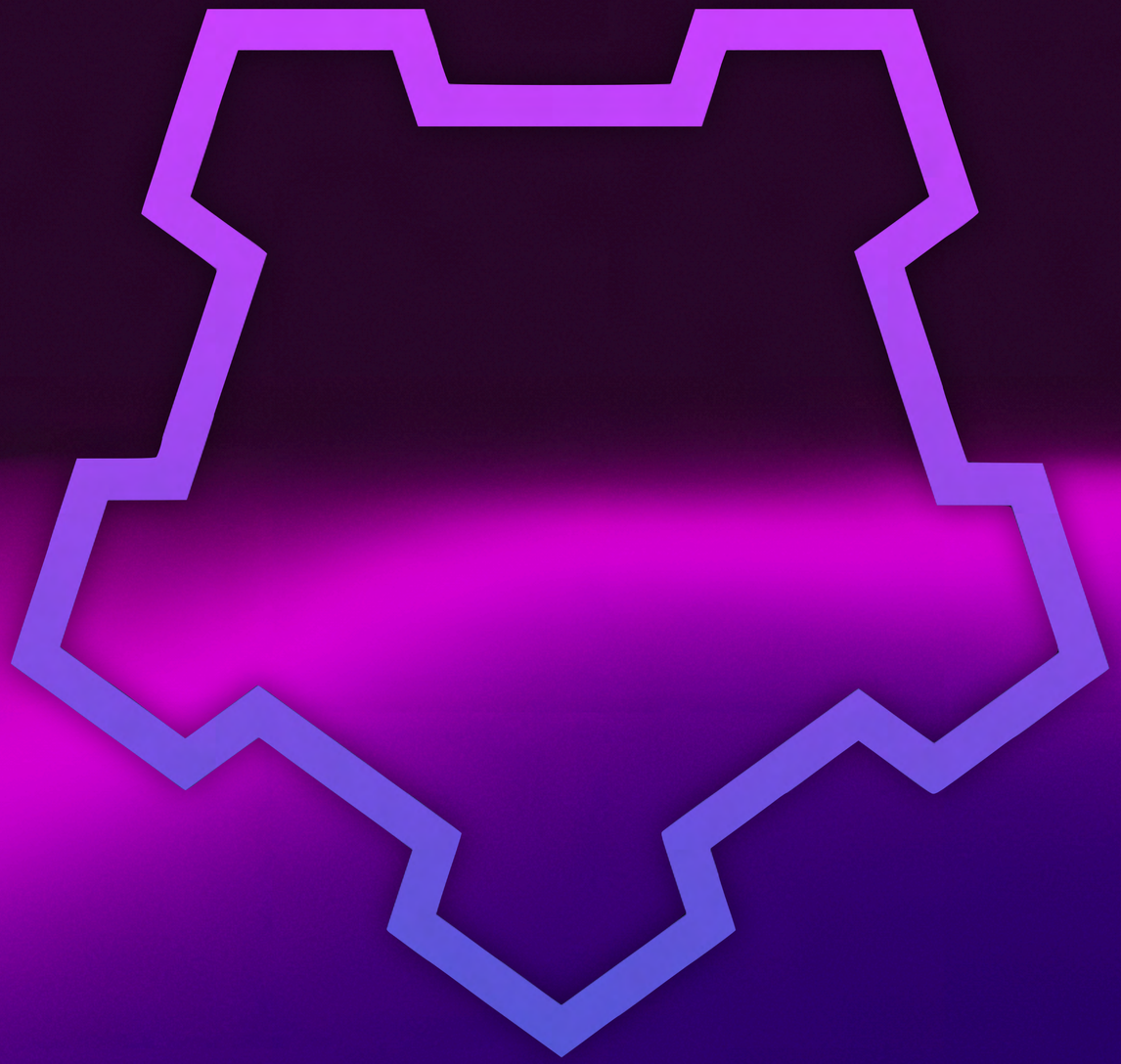
- Yes, with SegWit & miniscript!
  — **wait, no**: miniscript prohibits re-use of the same keys in different conditions

- Just use SegWit with multiple devices per user
  — **wait, no**: very hard to manage, and quite expensive

- **Yes, with MyCitadel!**
  — use account-bases keys for different spending conditions

Self-sovereignty is hard

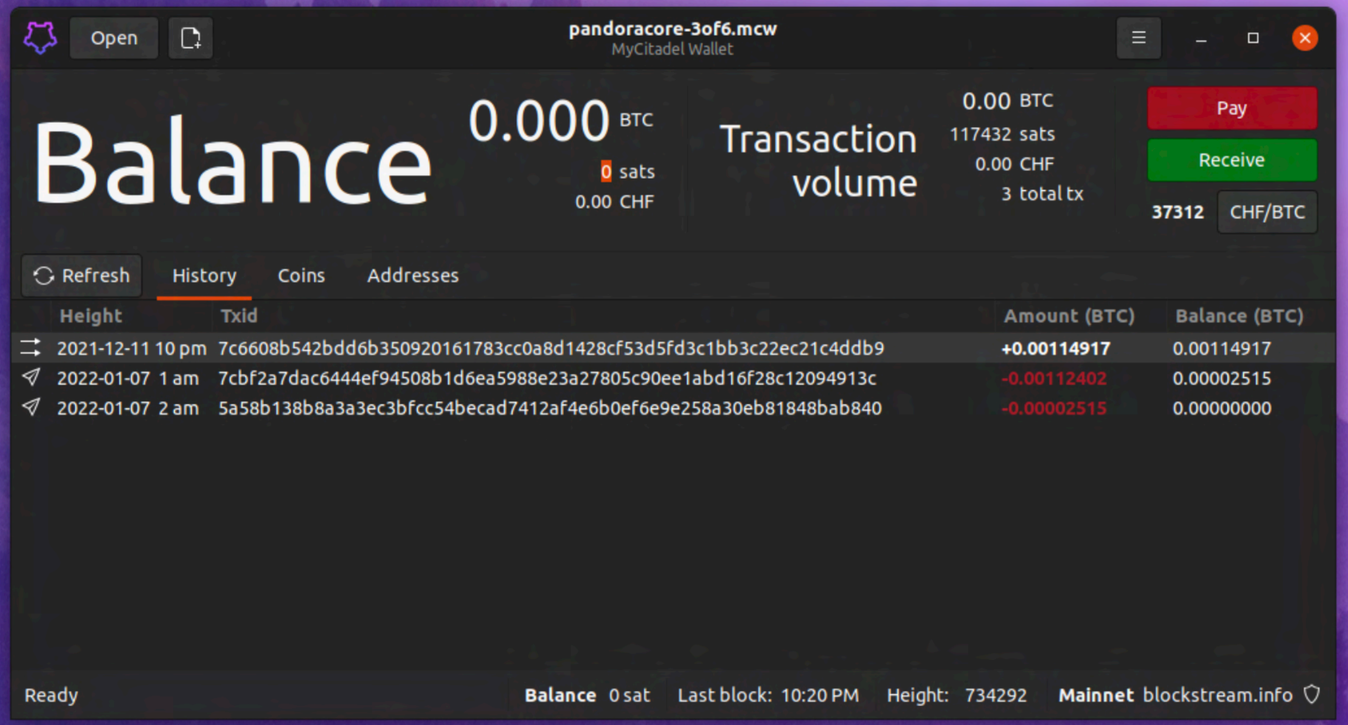
MyCitadel was created to make it reachable



MyCitadel: Ultimate digital sovereignty

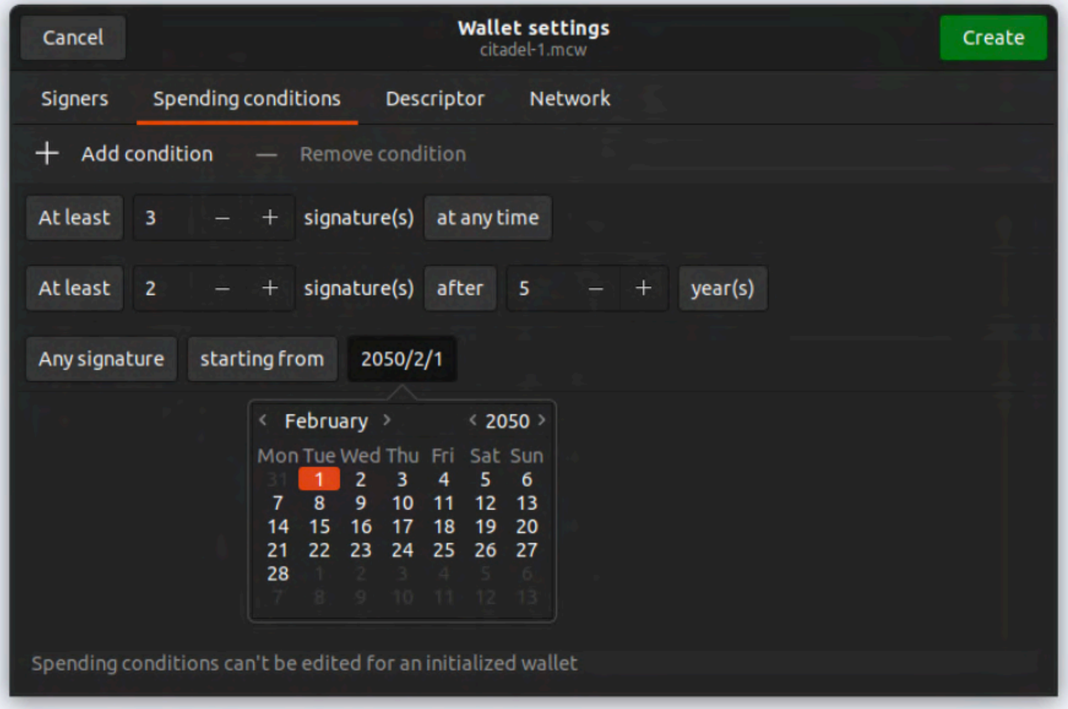
Do a reliable hodling, organizational, & current accounts – or instant Lightning payments. Work with single- and multisigs using hardware & air-gaped keys; arbitrary complex time-lock scripts and wallet descriptors.

DOWNLOAD



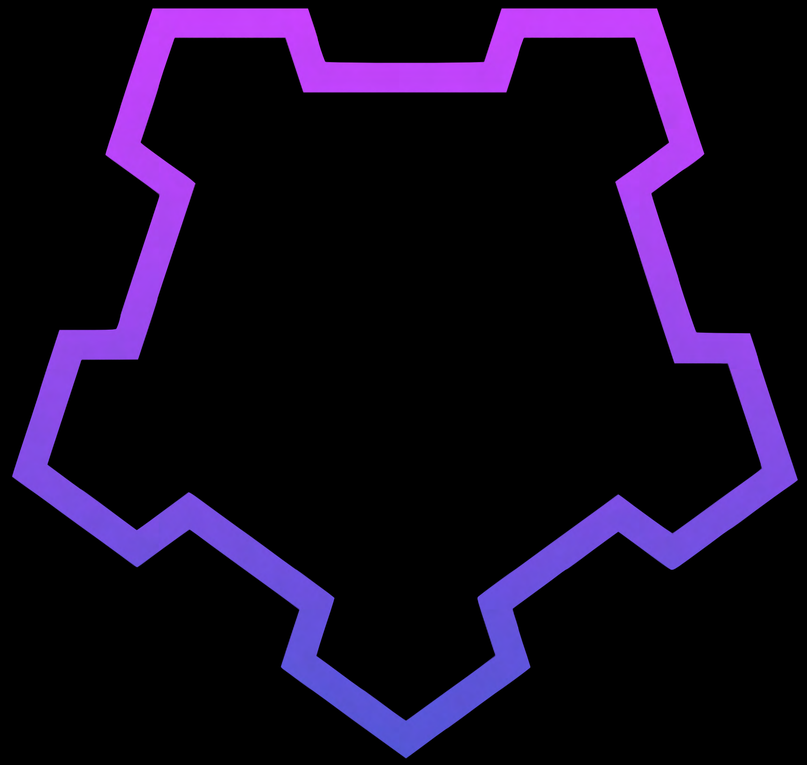
Time-locked spending conditions

MyCitadel is a wallet for **bitcoin, digital assets and bitcoin finance (#BiFi) smart contracts**. It is blazingly fast, secure, cross-platform and technically most advanced wallet on the market, being the first wallet allowing taproot multisig and locktime-based spending conditions.



Release v1.3

Debian



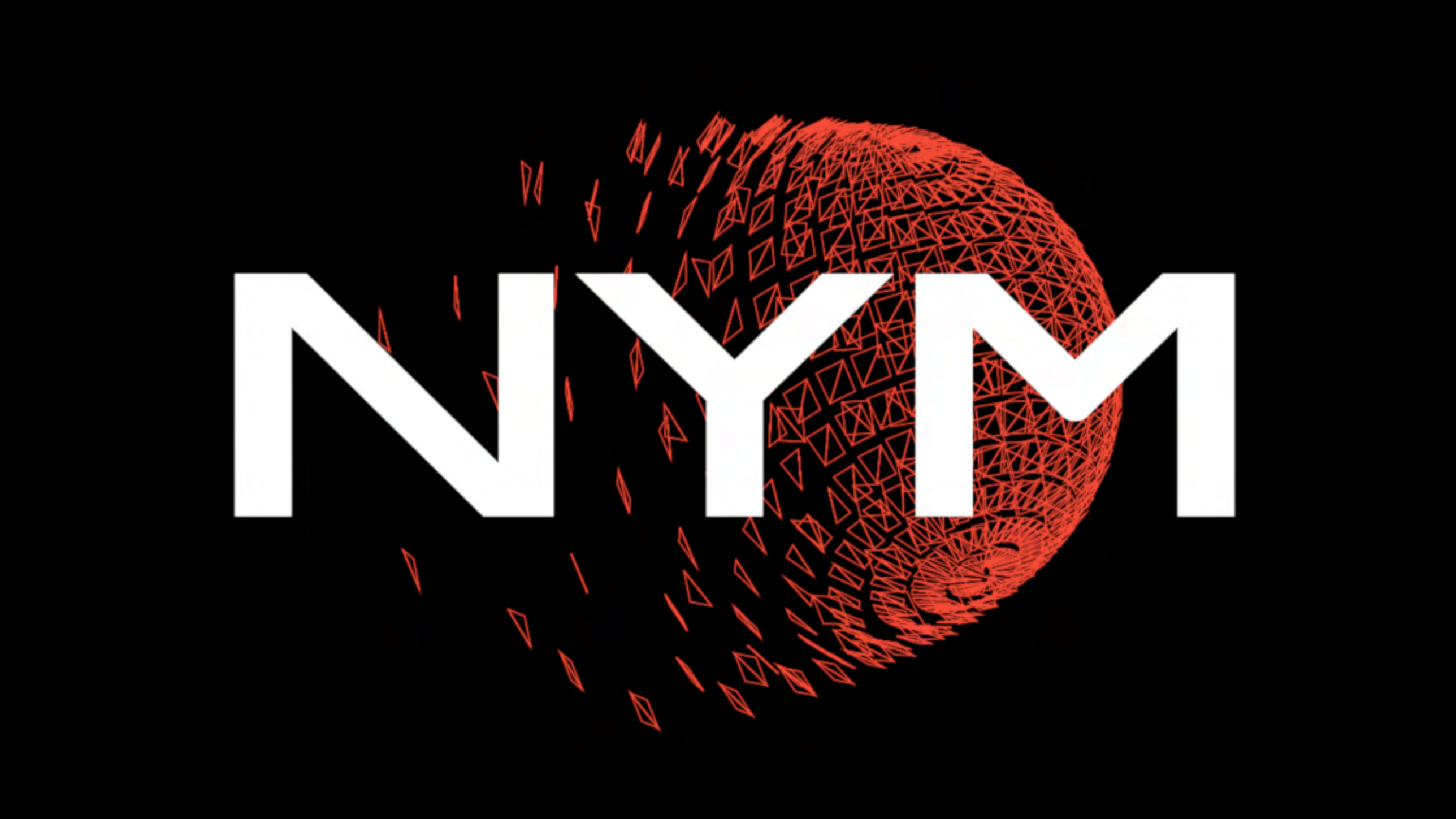
Windows Installer

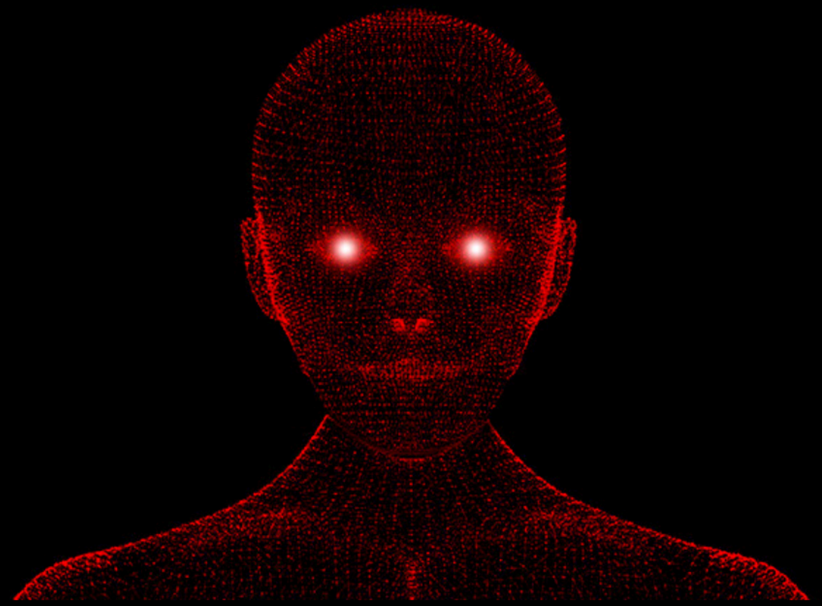
Flatpak


ONE MORE
THING

More to come in v2

- RGB assets & contracts
- Nostr integration & relays in MyCitadel private cloud for:
  - Multisig setup
  - Signing transactions by multiple signers
  - Sync tx annotations across devices
- Export for accounting software
- Home/org server assembled by Nodl


NYM



Olga Ukolova*

Twitter @dr_ukolova

- Co-author of #FreeAI Manifesto
- Board member at LNP/BP Standards Association
- Founder @Pandora Prime

**I identify as Dolores the Queen of Geeks*