GNOSIS SAFE 2019

Recovery & dapp interaction

GNOSIS

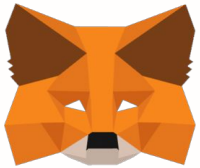
https://safe.gnosis.io

@gnosisSafe

Tobias Schubotz | @tschubotz








Why yet another wallet?





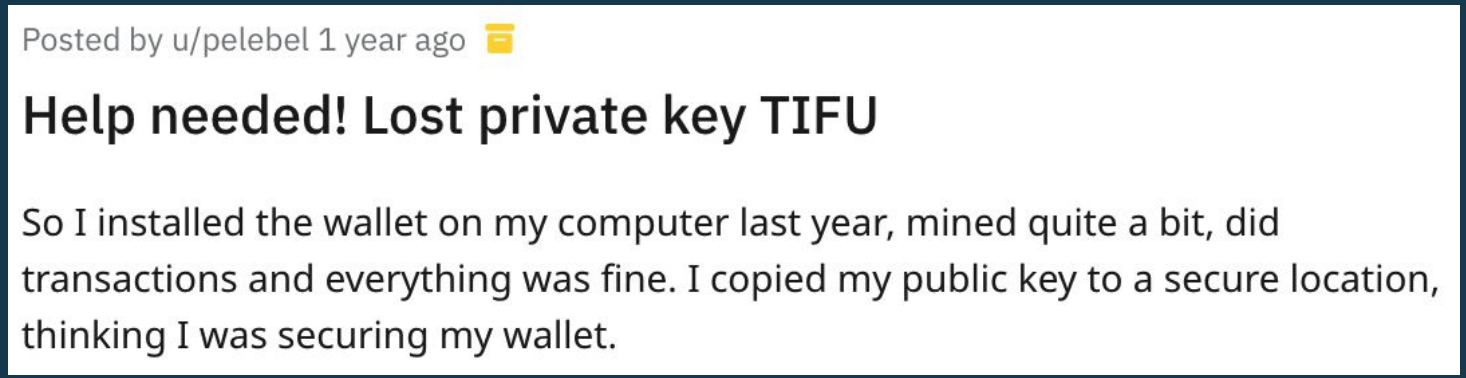

Gnosis Safe is a **smart contract** based wallet for **mobile**.

Today: **Externally owned accounts** (EOA)

Backups of seed phrase **required**!

No access control: Access all or nothing.

Users are **not** ready for it

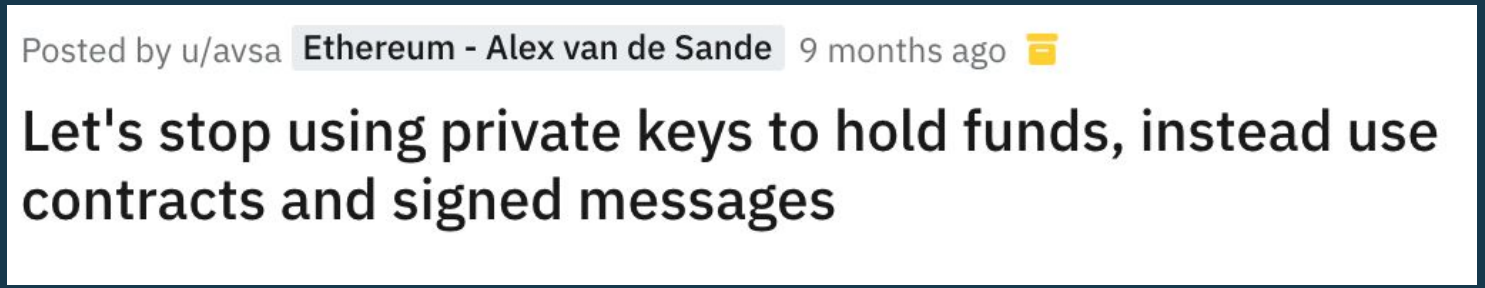


Posted by u/pelebel 1 year ago

Help needed! Lost private key TIFU

So I installed the wallet on my computer last year, mined quite a bit, did transactions and everything was fine. I copied my public key to a secure location, thinking I was securing my wallet.

Future: **Smart contract wallets**



Contracts are **first class citizens!**

What makes the Gnosis Safe *different?*

- 2-factor authentication
- Token payment
- Seedless recovery

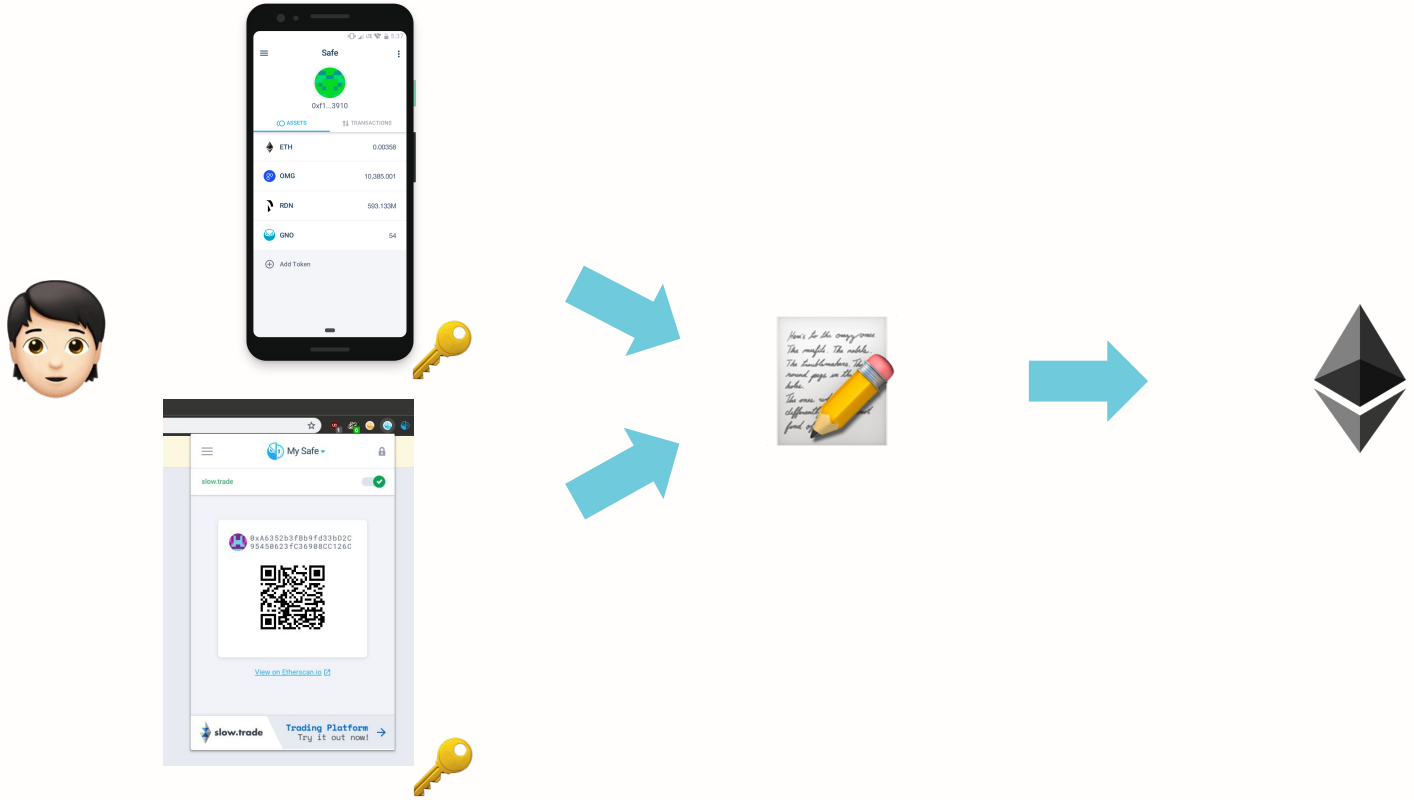
2-factor authentication*

* available right now

Transactions with EOAs

2FA transactions with smart contract wallets

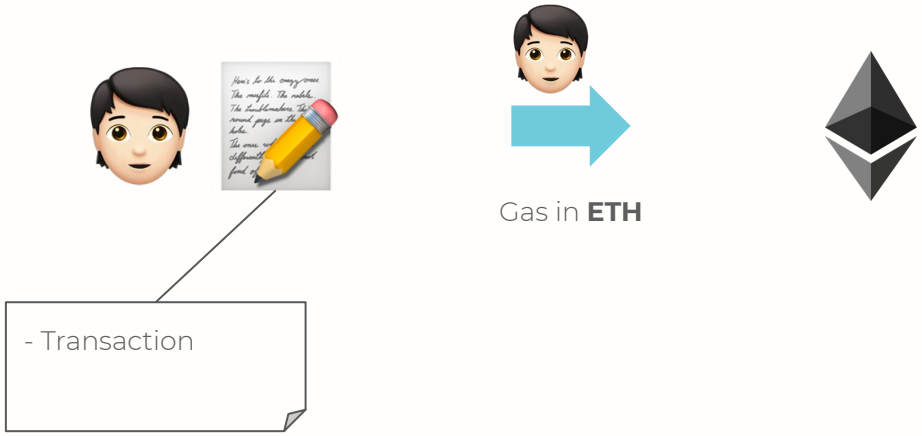
2FA transactions with the Gnosis Safe



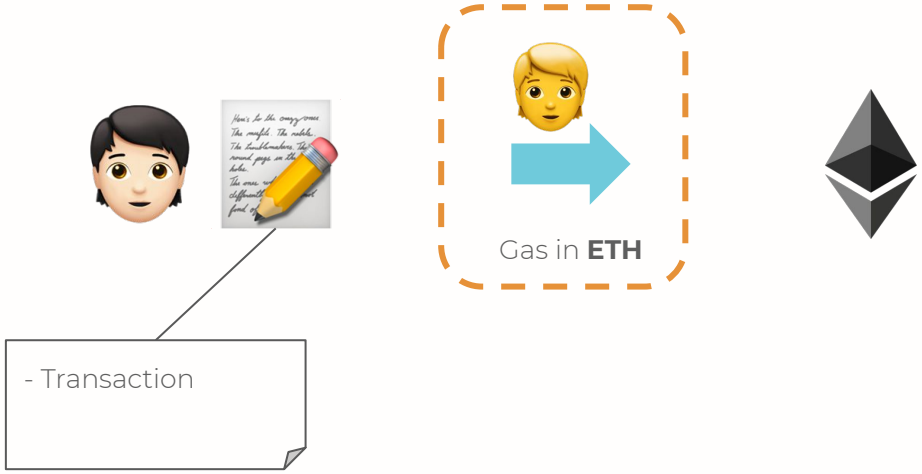
Token payment *

* prototype available in Android app

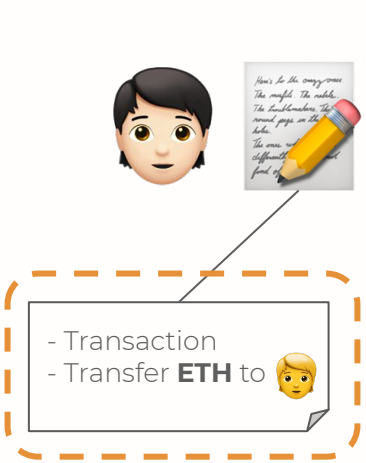
Regular Ethereum transactions

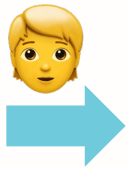


Meta transactions



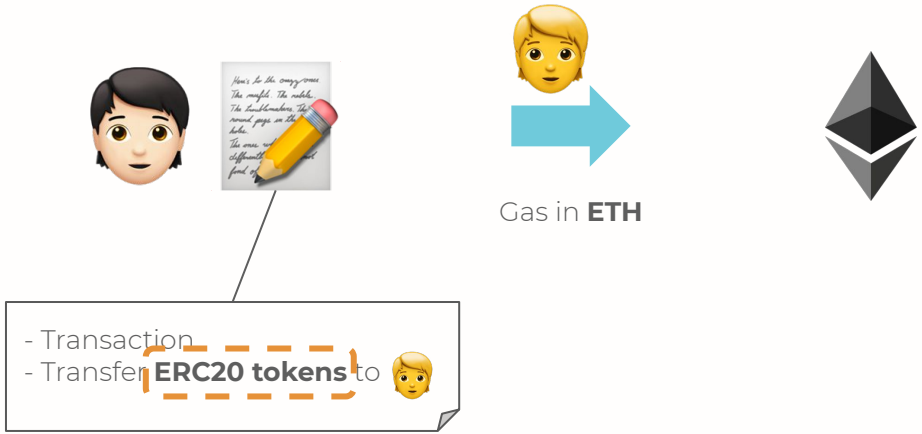
Meta transactions with refund





Gas in **ETH**

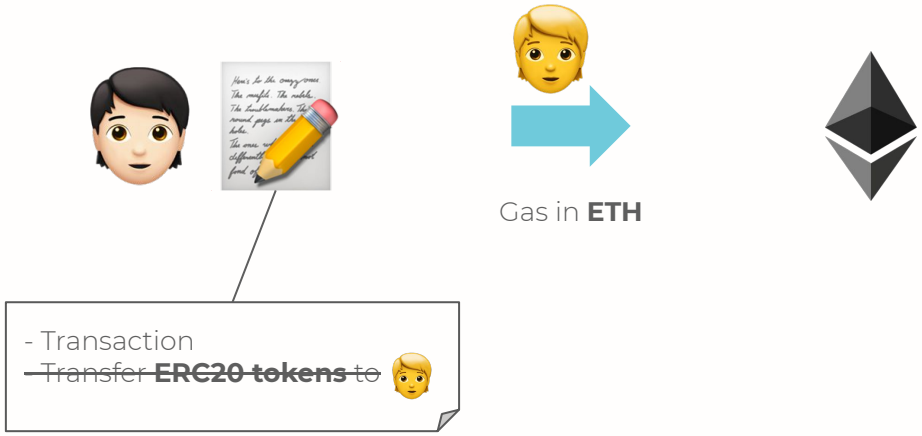
Meta transactions with refund in ERC20 tokens



Why meta transactions?

- The Gnosis Safe is a smart contract wallet
- User does not need ETH on EOA
- Free choice on who pays for gas

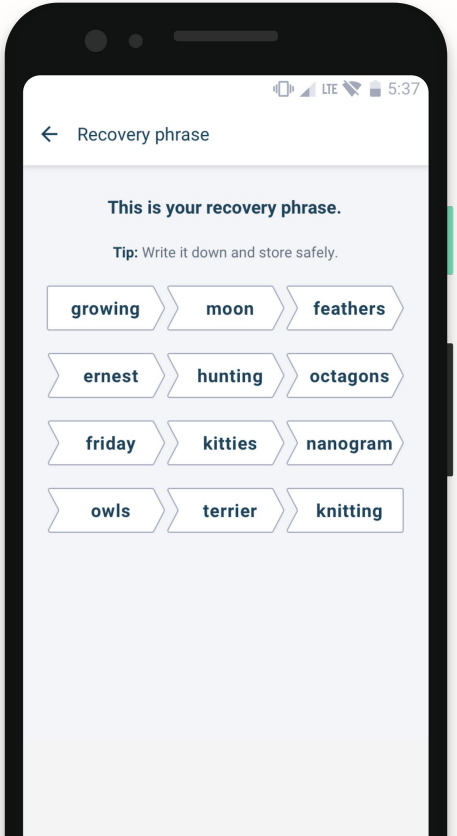
Why not pay all transaction fees for the user?



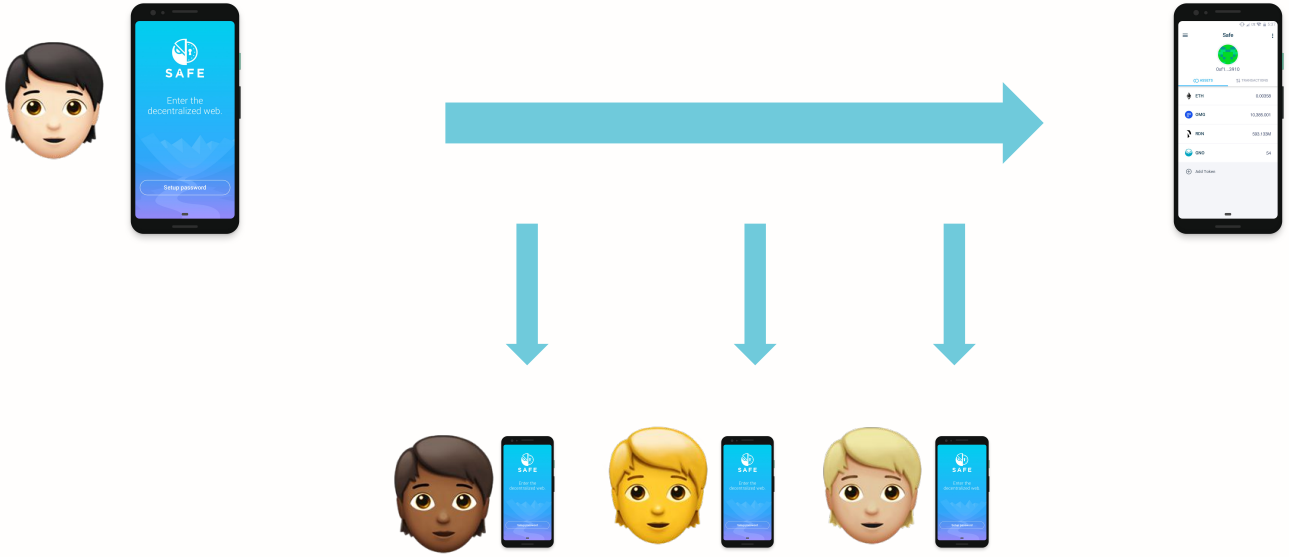
Seedless recovery *

* in development

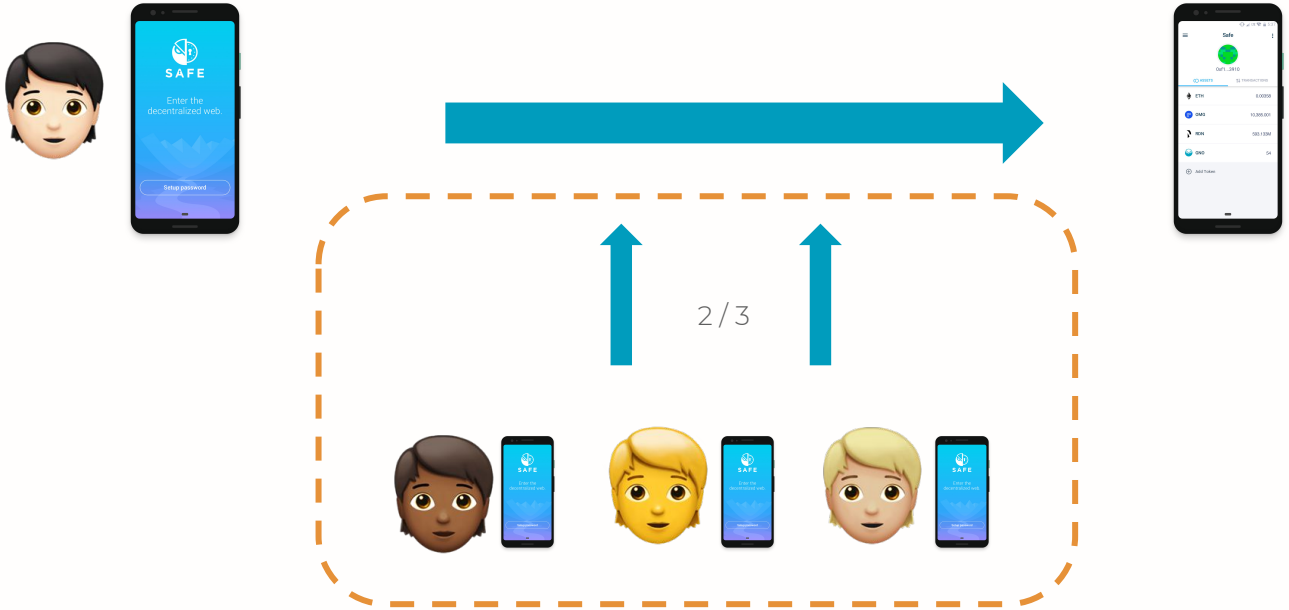
Recovery phrases



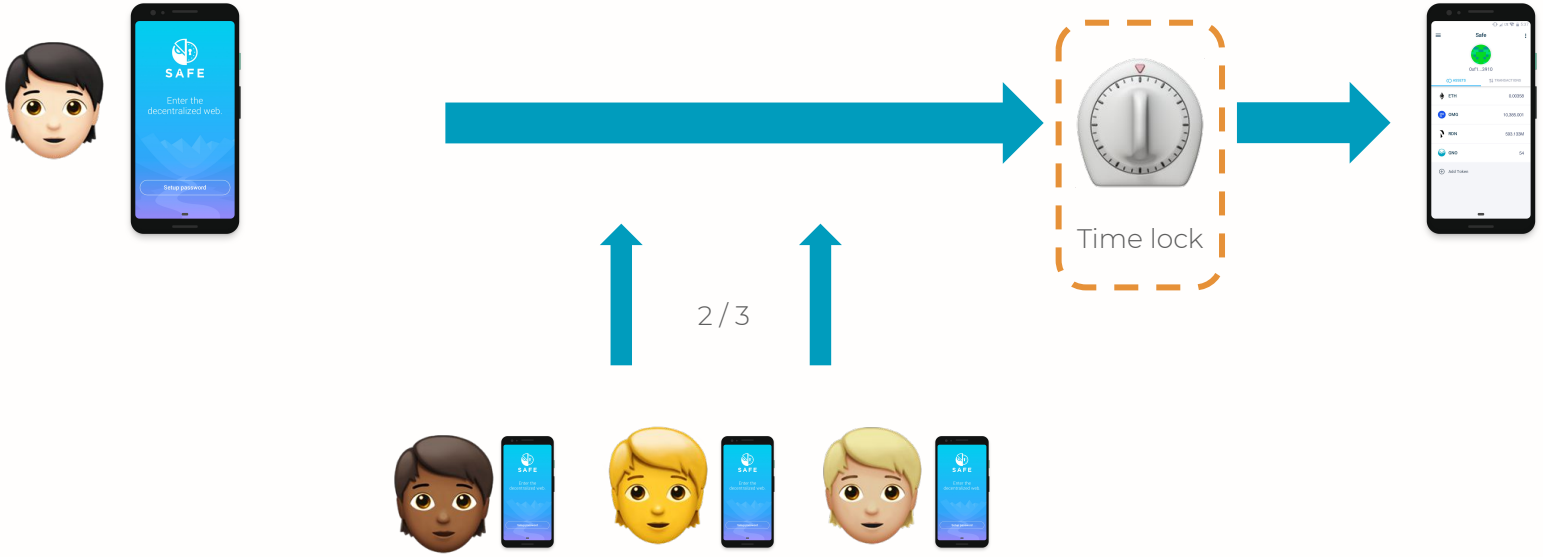
Social recovery - Setup flow



Social recovery - **Recovery flow**



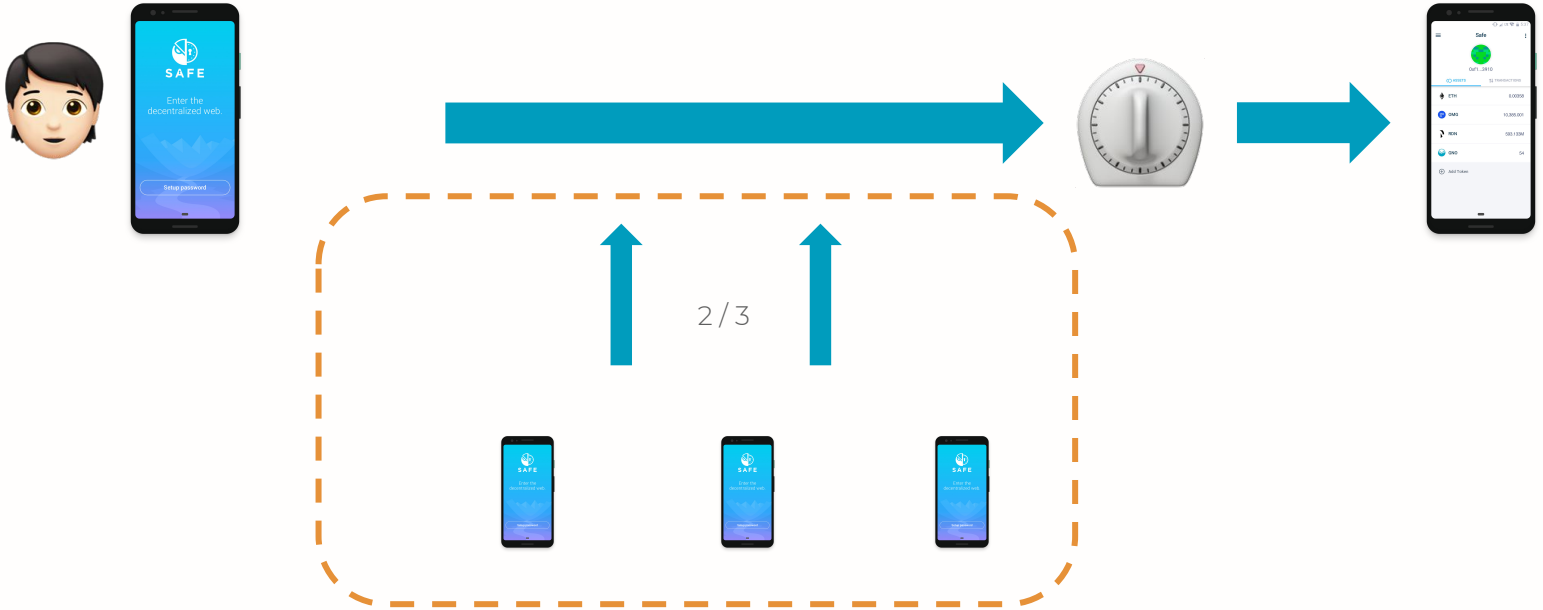
Social recovery - Recovery flow



Time lock / challenge period

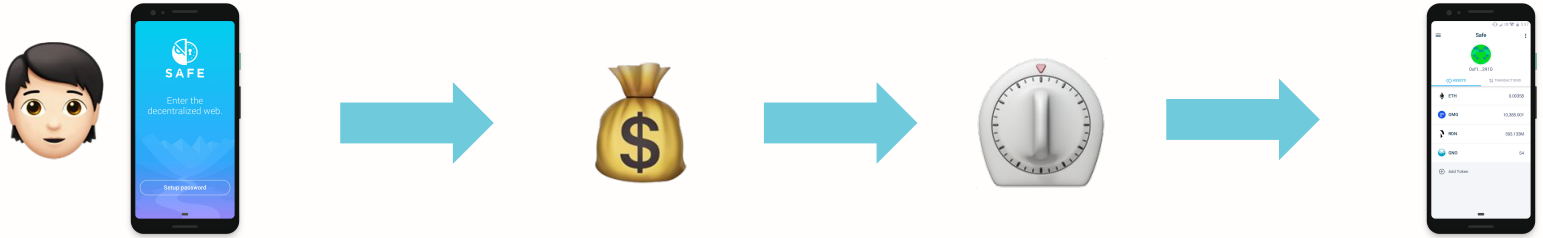
- How does the user notice?
- How long should the time lock last?
- Is there an option to accelerate?

Social recovery - Recovery flow



What if there is *recovery phrase is lost & social recovery fails?*

Paralysis proof



Other features

- Contract signatures
- WalletConnect integration

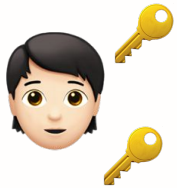
Contract signatures *

* in development

Off-chain signatures

Who?

Contract signatures



Who?

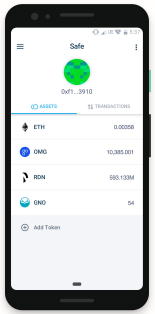
Contract signatures

Who?

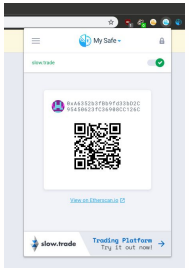
WallectConnect integration *

* in development

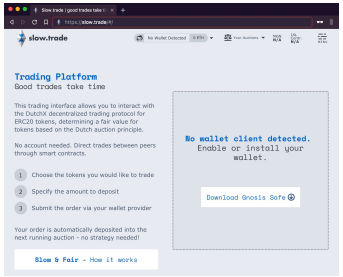
Dapp interaction via Gnosis Safe browser extension



Gnosis Safe
mobile app

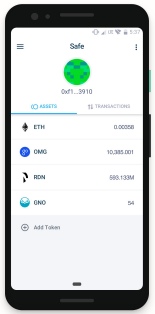


Gnosis Safe
Chrome extension



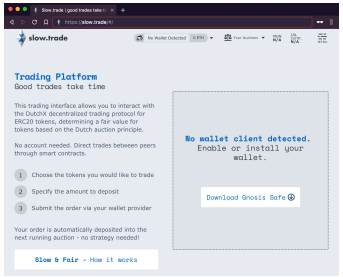
Dapp

Dapp interaction via WalletConnect



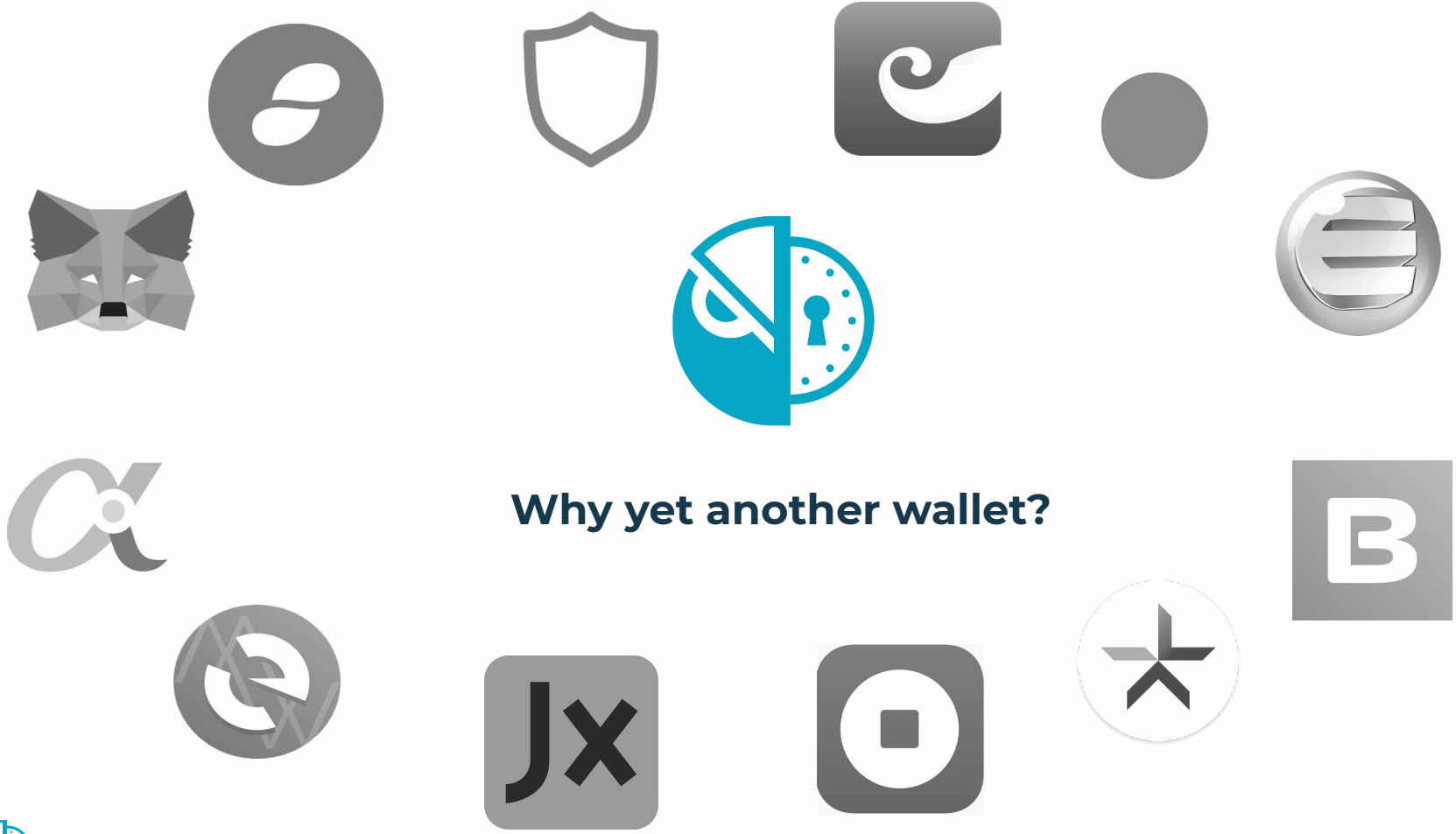
Gnosis Safe
mobile app

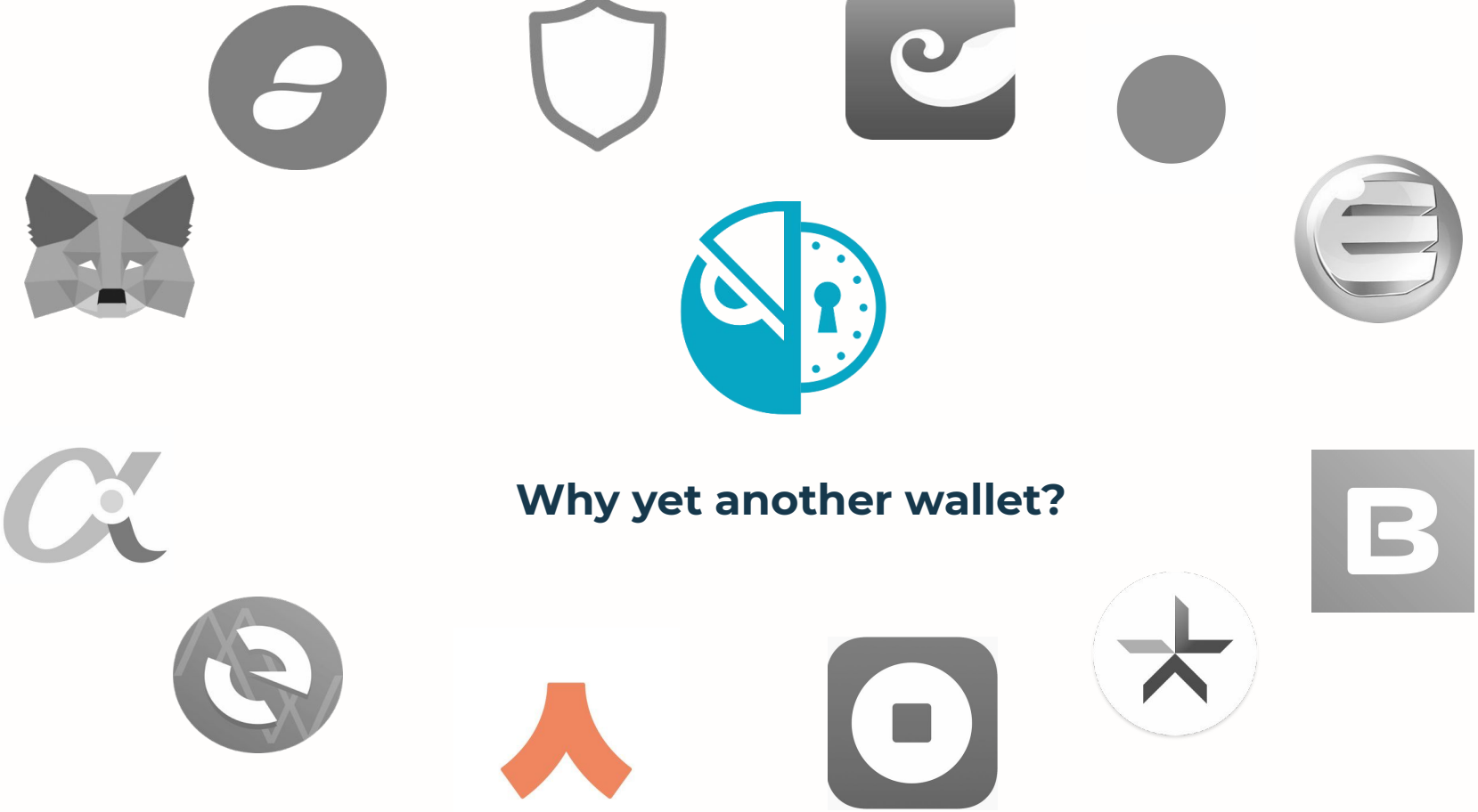
WalletConnect



Dapp

- Formal verification
  - Formalize smart contracts as mathematical specification
  - Verify that EVM bytecode satisfies contract's specification
  - https://github.com/runtimeverification/verified-smart-contracts/blob/master/gnosis/GnosisSafe_RuntimeVerification.pdf


Why yet another wallet?



Why yet another wallet?

GNOSIS SAFE

https://safe.gnosis.io