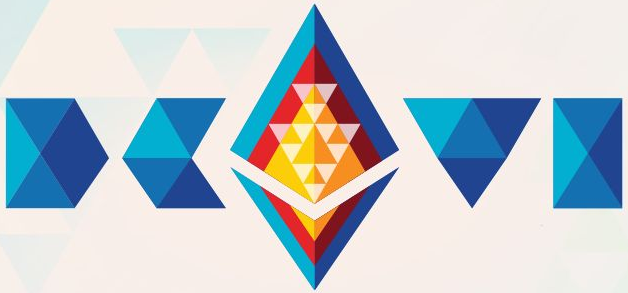


Post-Merge Wallet

Chang-Wu Chen
Head of imToken Labs

imToken

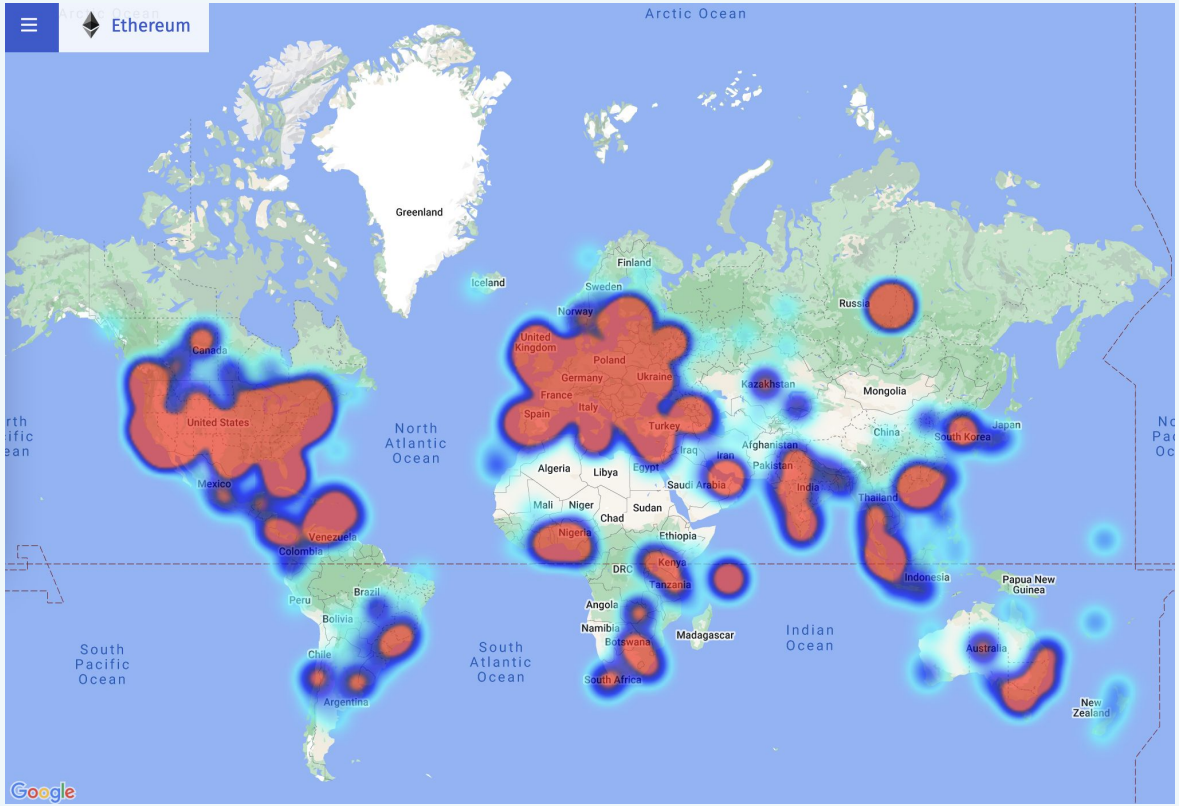
Q1: What is your ideal crypto wallet?

Past

Present

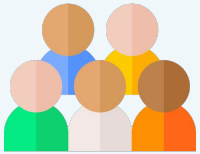
Future

Ethereum Adoption Map



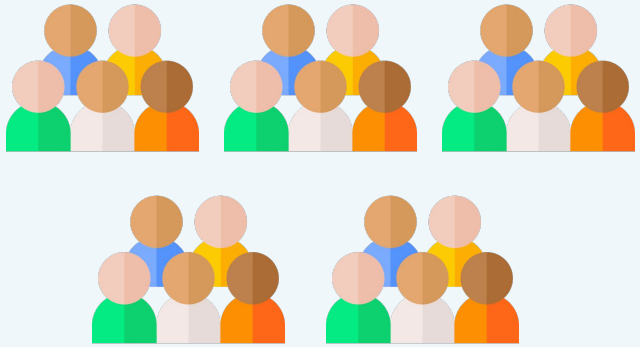
Source: https://cryptwerk.com/coinmap/eth/2/44.33485164/75.67382813/

There are over **221** million cryptocurrency users worldwide.

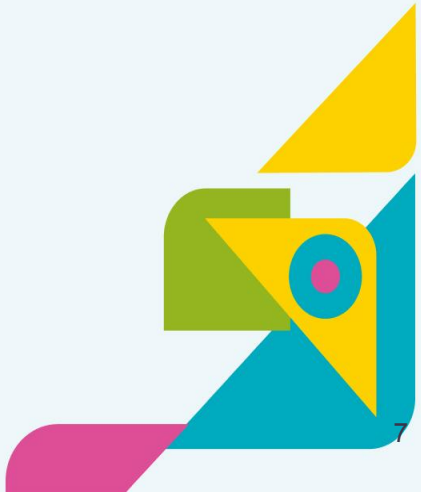


Source: https://explodingtopics.com/blog/cryptocurrency-stats

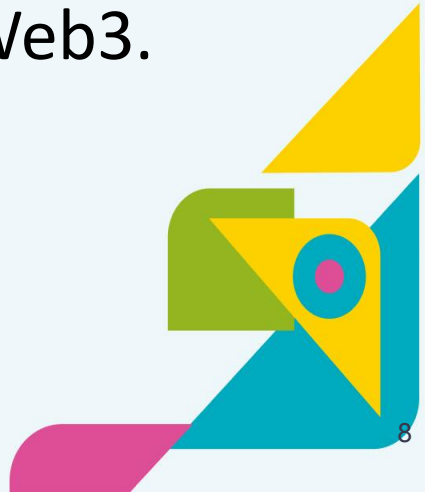
Still **97%** users who doesn’t know crypto and doesn’t have any crypto assets



- Don’t know what is seed phrase
- Don’t know how to switch between networks
- Don’t know how to speed up the stuck transaction
- Can’t protect their private key pretty well
- Can’t recover the account as the key gets lost
- Can’t read the signing message
- Can't identify which token is legit
- Can’t understand how to revoke token approval
- Hard to remember the address
- …



For mass adoption to happen, crypto wallet is critical and is an entry point to onboard users to Web3.



- Don’t know what is seed phrase
- Don’t know how to switch between networks
- Don’t know how to speed up the stuck transaction
- Can’t protect their private key pretty well
- Can’t recover the account as the key gets lost
- Can’t read the signing message
- Can't identify which token is legit
- Can’t understand how to revoke token approval
- Hard to remember the address
- …

Recap

- If we want to rebuild a wallet, then we need to know what the future wallet looks like.

- That is the reason why the topic is called **Post-Merge** wallet.

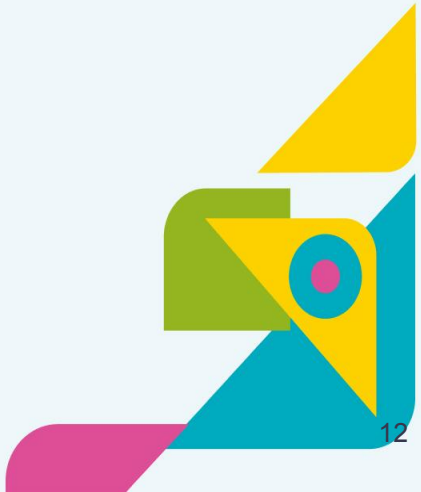
Past

Present

Future

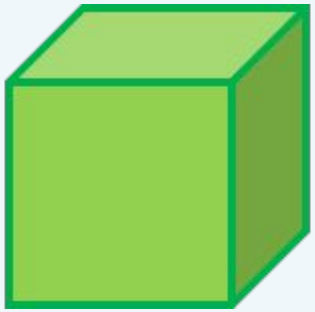
Endgame

(Scaling Ethereum for billion users)



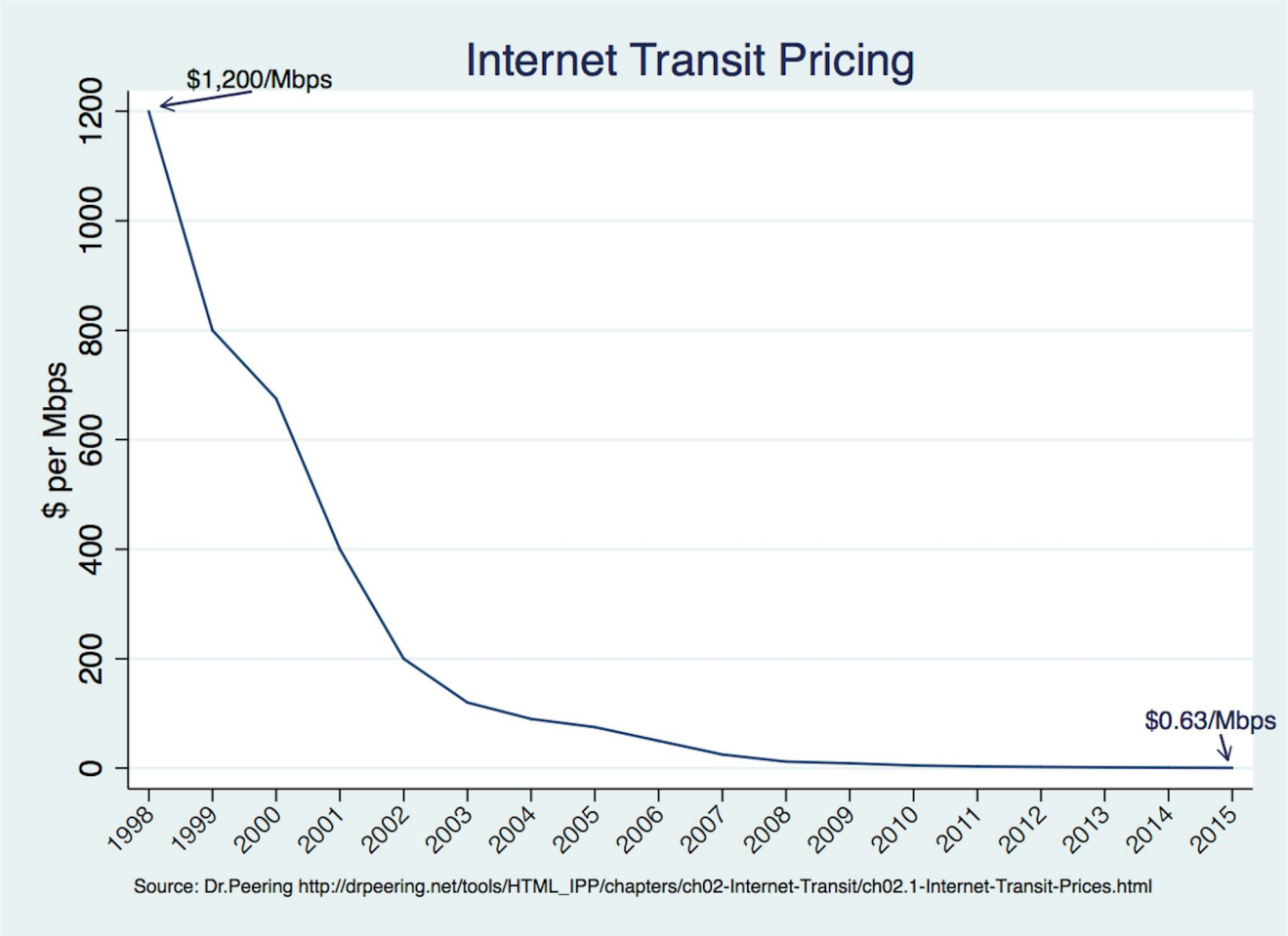
Source: https://vitalik.ca/general/2021/12/06/endgame.html

- Ethereum is pivoting to a rollup-centric roadmap
- Danksharding provides more data space per block
- Data compression improvement for rollup transaction



TPS 

Fee 



Source: https://techpolicyinstitute.org/publications/miscellaneous/cloud-computing-co-invention-for-the-masses/

With cheaper tx fee, we can do more things.

- Token
- ICO

- DeFi
- NFT

- Payment
- NFT
- Social applications
- Gaming
- …

So, we need to have a wallet which fits L2 roadmap after the post-merge and is user-friendly.

Short summary

- Difficult for general users to understand and manage their keys 

Short summary

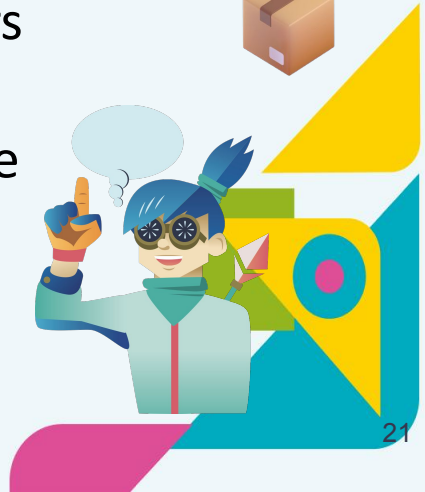
- Difficult for general users to understand and manage their keys 
- Bad user experience for wallet users now 

Short summary

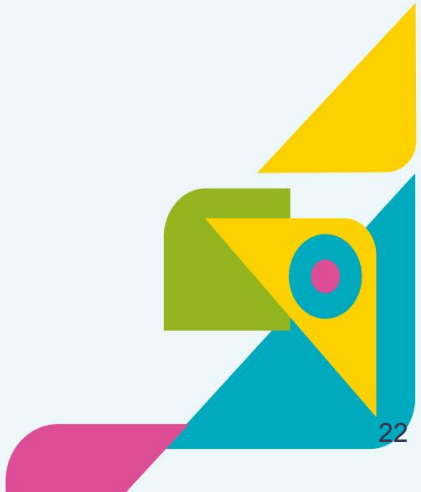
- Difficult for general users to understand and manage their keys
- Bad user experience for wallet users now
- Need a user friendly wallet to onboard non-crypto users

Short summary

- Difficult for general users to understand and manage their keys
- Bad user experience for wallet users now
- Need a user friendly wallet to onboard non-crypto users
- Need a L2-ready wallet, which is designed for the future



Following is the requirement that we think an ideal wallet should have.



Challenges

- Don’t know what is seed phrase
- Don’t know how to switch between networks
- Don’t know how to speed up the stuck transaction
- Can’t protect their private key pretty well
- Can’t recover the account as the key gets lost
- Can’t read the signing message
- Can't identify which token is legit
- Can’t understand how to revoke token approval
- Hard to remember the address
- …

Requirements

- Non-Custodial wallet
  - No need seed phrase
  - Multichain supports
  - Fee management
  - Key management
  - Self/Social recovery
  - Decoding messages
  - Risk control/Simulation
  - Approval/Permit management
  - Name service
  - …

Challenges

- Don’t know what is seed phrase
- Don’t know how to switch between networks
- Don’t know how to speed up the stuck transaction
- Can’t protect their private key pretty well
- Can’t recover the account as the key gets lost
- Can’t read the signing message
- Can't identify which token is legit
- Can’t understand how to revoke token approval
- Hard to remember the address
- …

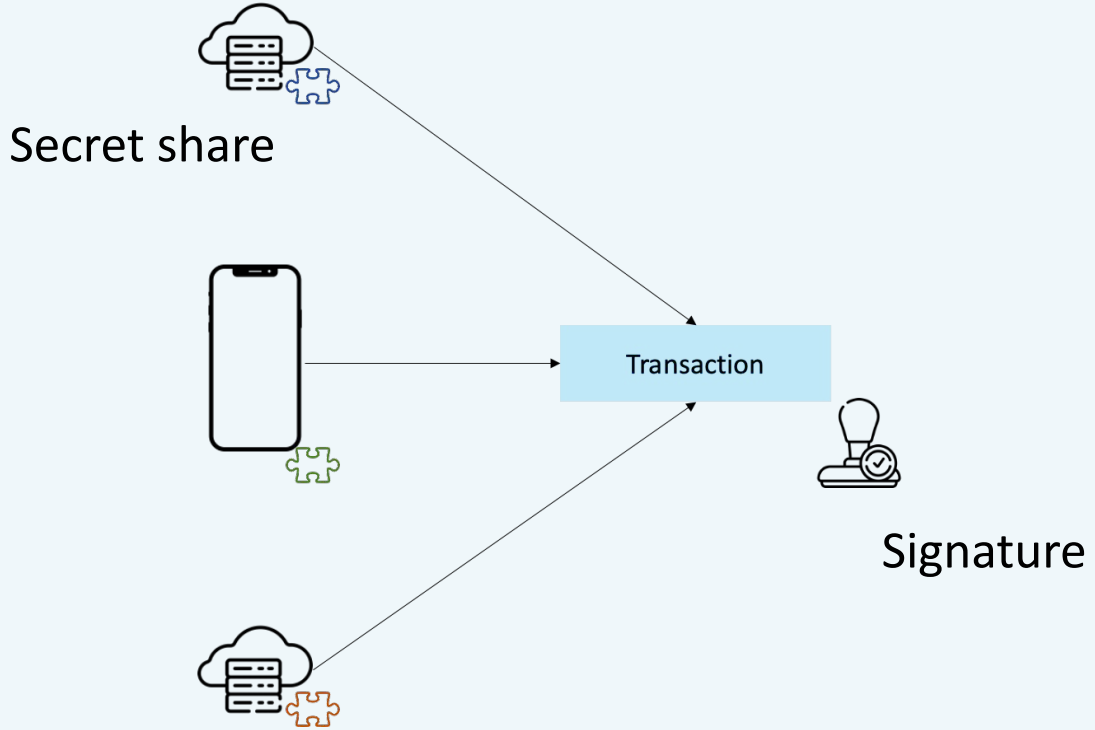
Requirements

- Non-Custodial wallet
  - No need seed phrase
  - Multichain supports
  - Fee management
  - Key management
  - Self/Social recovery
  - Decoding messages
  - Risk control/Simulation
  - Approval/Permit management
  - Name service
  - …

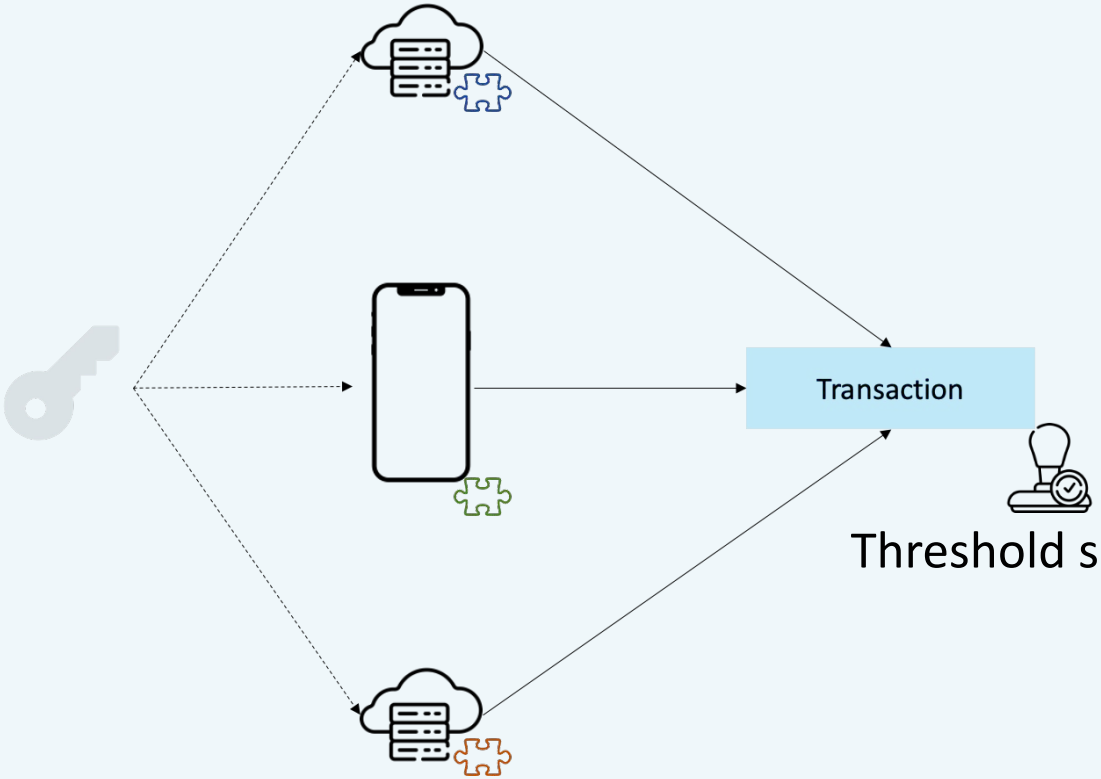
Solutions

1. MPC (Multi-party computation)
2. AA (Abstract account)

MPC wallet

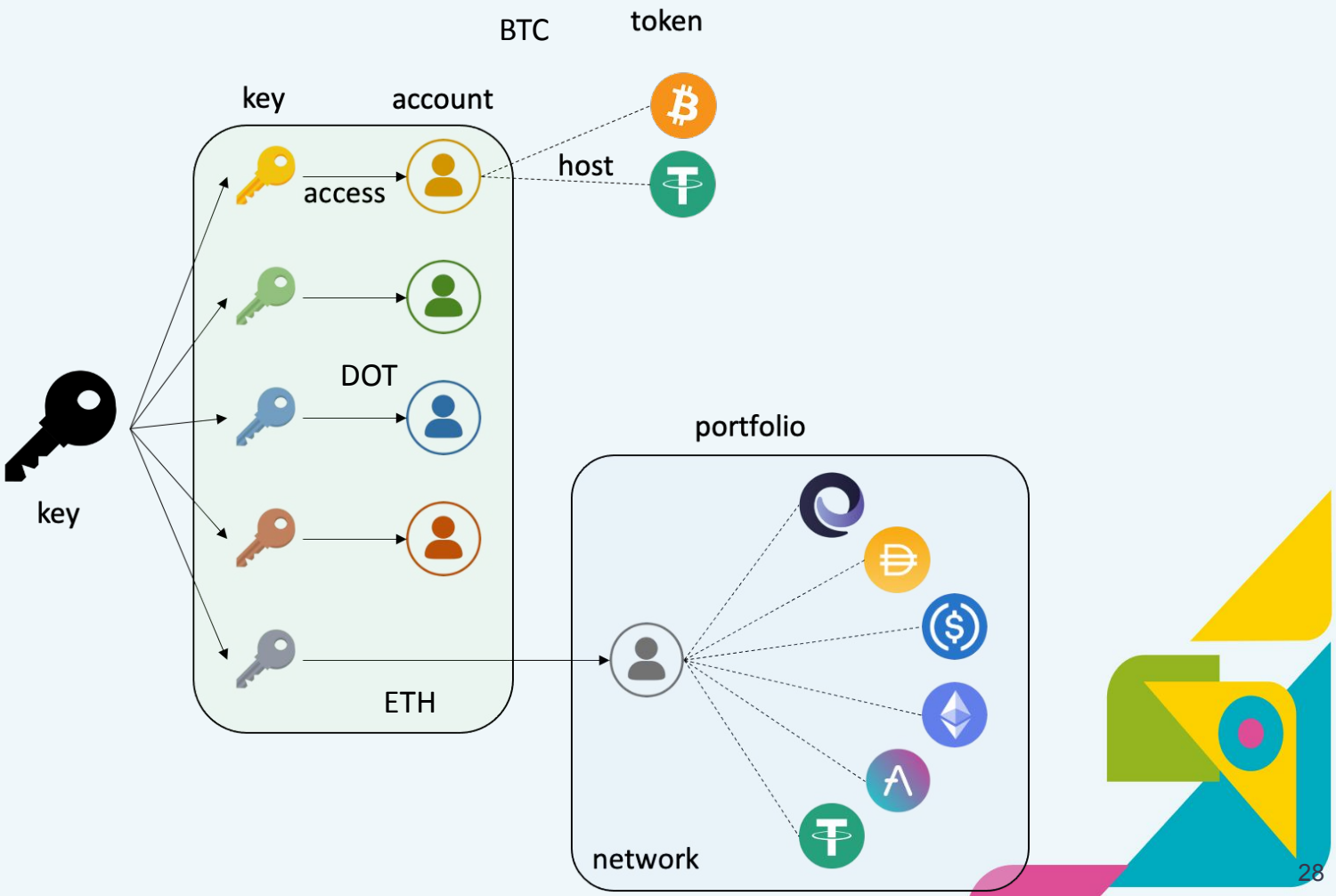


MPC wallet



2-of-3 (m-of-n)

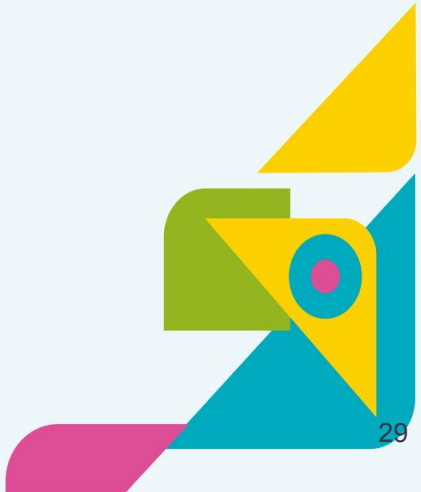
Threshold signature


BTC
token
key
account
host
access
DOT
key
portfolio
ETH
network

Accounts

There are two types of accounts:

1. External owned account, EOA
2. Contract account



AA wallet

Smart contract wallet

Entry point:

1. Signature verification
2. Execute a call

AA wallet

Smart contract wallet

Entry point:

1. Signature verification
2. Execute a call

Customized verification rule

- BLS, Schnoor, EdDSA etc.
- Multisig
- Off-chain signing message
- Change signer

AA wallet

account != signer

Smart contract wallet (**Account = 0xd8da6bf2..**)

Entry point:

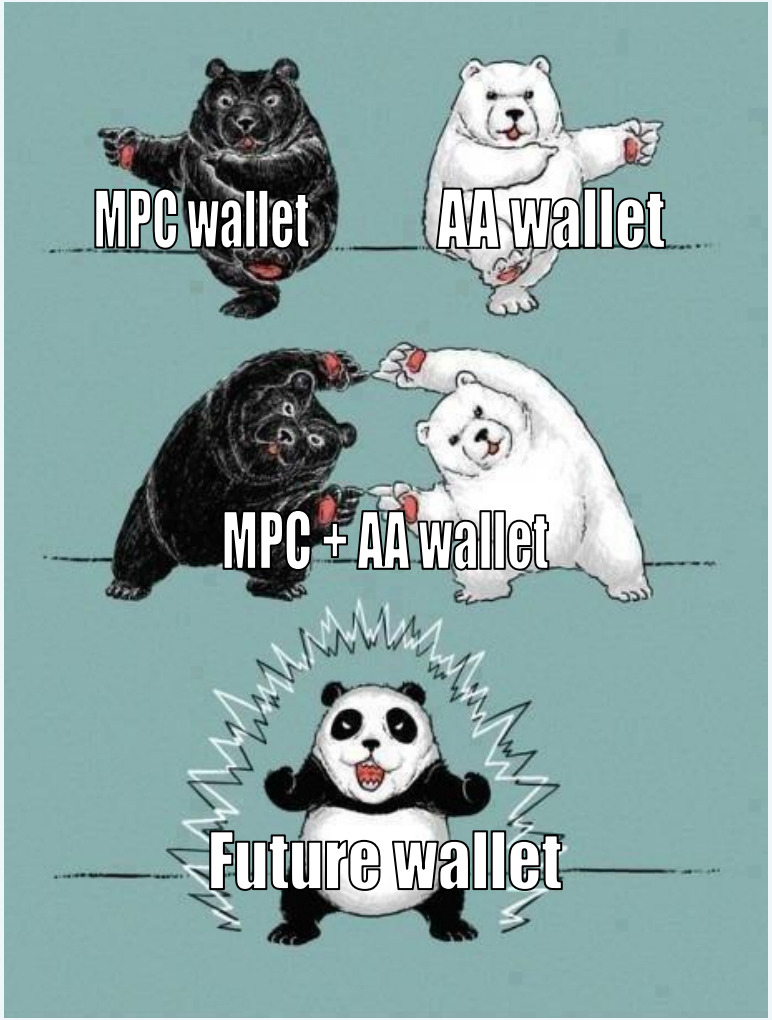
1. Signature verification
2. Execute a call

Signer = 0x782cf6b6..

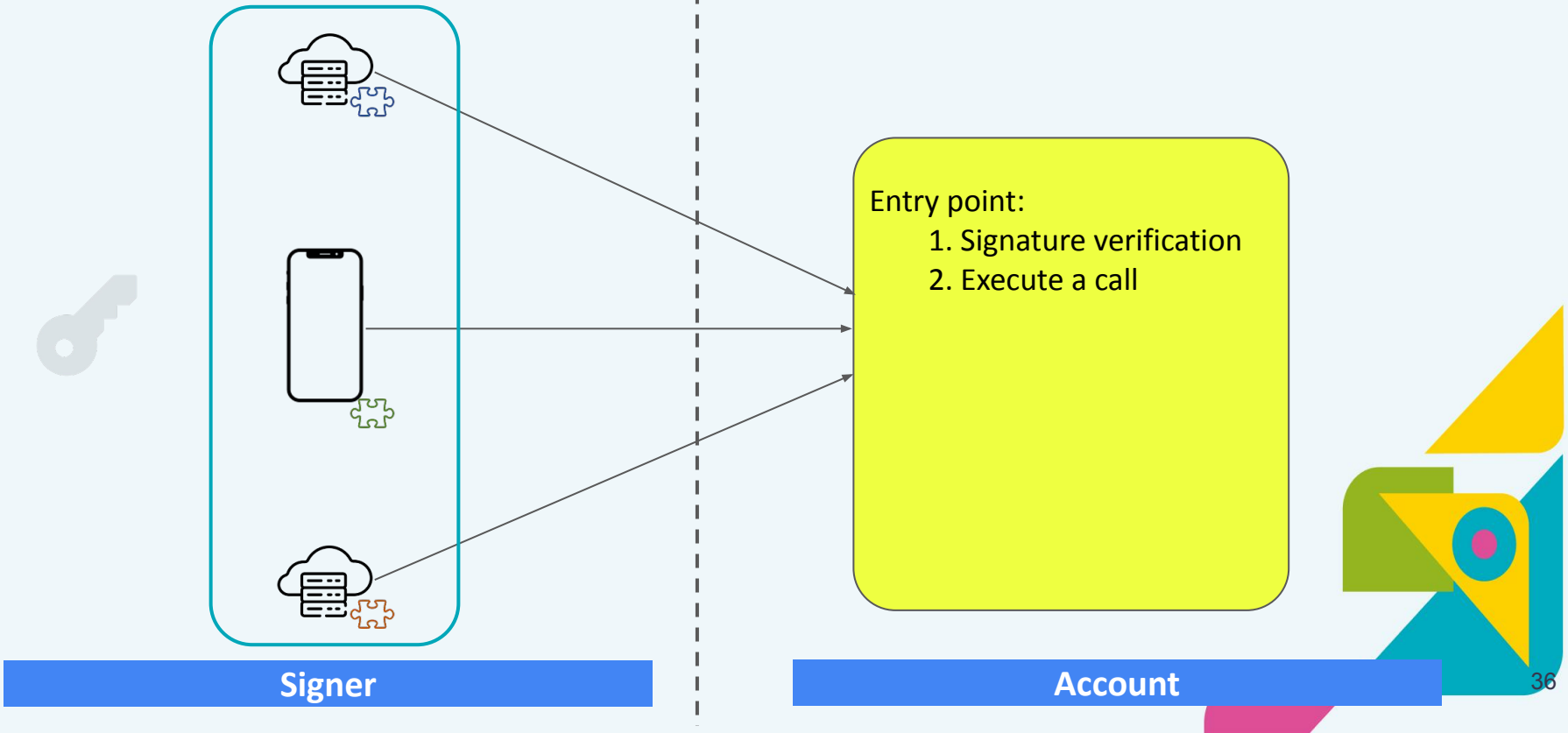
	MPC wallet (DKLs18; GG18; GG20; CMP, Alice)	**AA wallet** (EIP-2938; EIP-4337)
Multisig-similar	✅	✅
Changeable signer		✅
Self & social recovery	✅	✅
Risk control	✅	✅
Multichain	✅	
Relayer-friendly		✅
DeFi-friendly (EIP-1271)	✅	

imToken

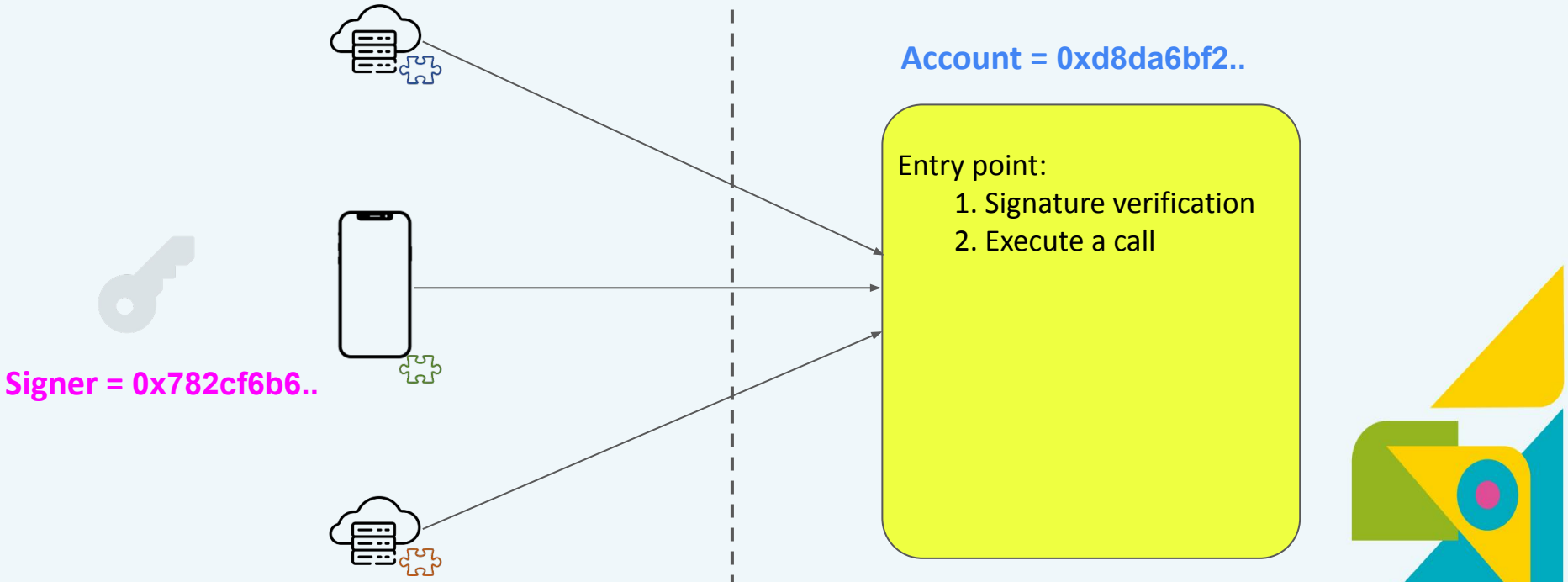
Q2: Can we do better?


MPC wallet
AA wallet
MPC + AA wallet
Future wallet

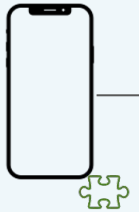
(MPC + AA) wallet



(MPC + AA) wallet



(MPC + AA) wallet



Signer = 0x782cf6b6..

Account = 0xd8da6bf2..

Entry point:

1. Signature verification
2. Execute a call

Synchronous

Asynchronous

Benefits

- Payment
- DID (Soulbound token)
- Gaming
- Paymaster (meta-tx)
- Self/Social recovery

Thank you!

Chang-Wu Chen

Head of imToken Labs

changwu@token.im

imToken