Post-Merge Wallet

Chang-Wu Chen
Head of imToken Labs
Q1: What is your ideal crypto wallet?
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.
Present
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  ↓
With cheaper tx fee, we can do more things.

- 2015
  - Token
  - ICO

- 2020
  - DeFi
  - NFT

- 2022
  - 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
  - ...

24
Solutions

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

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

Transaction

Threshold signature
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
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

Smart contract wallet
AA wallet

Smart contract wallet (Account = 0xd8da6bf2..)

Entry point:
1. Signature verification
2. Execute a call

Signer = 0x782cf6b6..

account != signer
<table>
<thead>
<tr>
<th>Feature</th>
<th>MPC wallet</th>
<th>AA wallet</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(DKLs18; GG18; GG20; CMP, Alice)</td>
<td>(EIP-2938; EIP-4337)</td>
</tr>
<tr>
<td>Multisig-similar</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>Changeable signer</td>
<td></td>
<td>✅</td>
</tr>
<tr>
<td>Self &amp; social recovery</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>Risk control</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>Multichain</td>
<td>✅</td>
<td></td>
</tr>
<tr>
<td>Relayer-friendly</td>
<td></td>
<td>✅</td>
</tr>
<tr>
<td>DeFi-friendly (EIP-1271)</td>
<td>✅</td>
<td></td>
</tr>
</tbody>
</table>
Q2: Can we do better?
MPC wallet

AA wallet

MPC + AA wallet

Future wallet
(MPC + AA) wallet

Entry point:
1. Signature verification
2. Execute a call
(MPC + AA) wallet

Signer = 0x782cf6b6..

Entry point:
1. Signature verification
2. Execute a call

Account = 0xd8da6bf2..

Off-Chain

On-Chain
(MPC + AA) wallet

1. Signature verification
2. Execute a call

Account = 0xd8da6bf2..

Entry point:
1. Signature verification
2. Execute a call

Signer = 0x782cf6b6..

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