From MPC Wallets to Smart Contract Accounts

Phuc Thai

Head Researcher, Sky Mavis

Issues of EOAs

- **Complexity for Non-Technical Users:** Managing EOAs requires a level of technical understanding that most average users do not possess. Without intuitive interfaces or educational resources, many struggle to grasp key management concepts.
- **Inaccessible Recovery Mechanisms:** For most people, the process of securely storing and retrieving seed phrases feels burdensome and impractical, creating barriers for mainstream users.
- **High Stakes of Mismanagement:** A single mistake in handling an EOA can lead to the irreversible loss of assets, heightening user anxiety and deterring wider adoption.

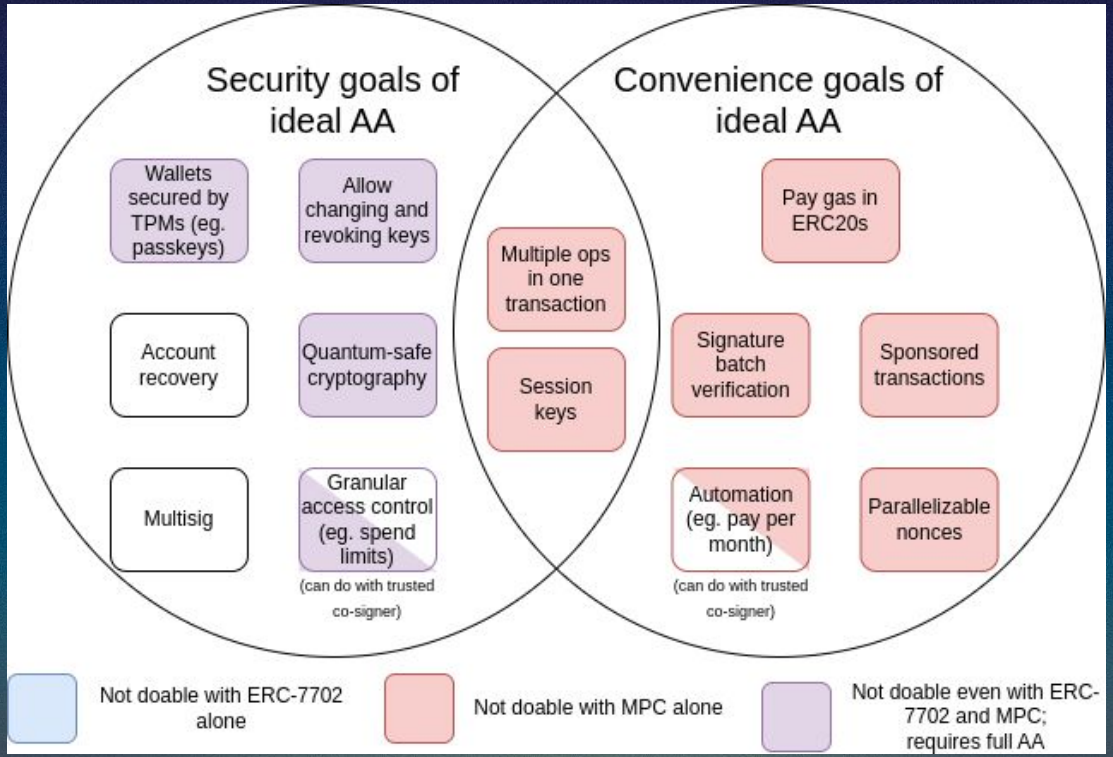
MPC wallets

- Social login, off-chain key recovery
- Off-chain, private transaction policies
- 40+ year old technology, ready to use

Account Abstraction

- Social login on-chain key recovery
- On-chain, transparent transaction policies
- Relatively new and still under development, but flexible, and more future-proof

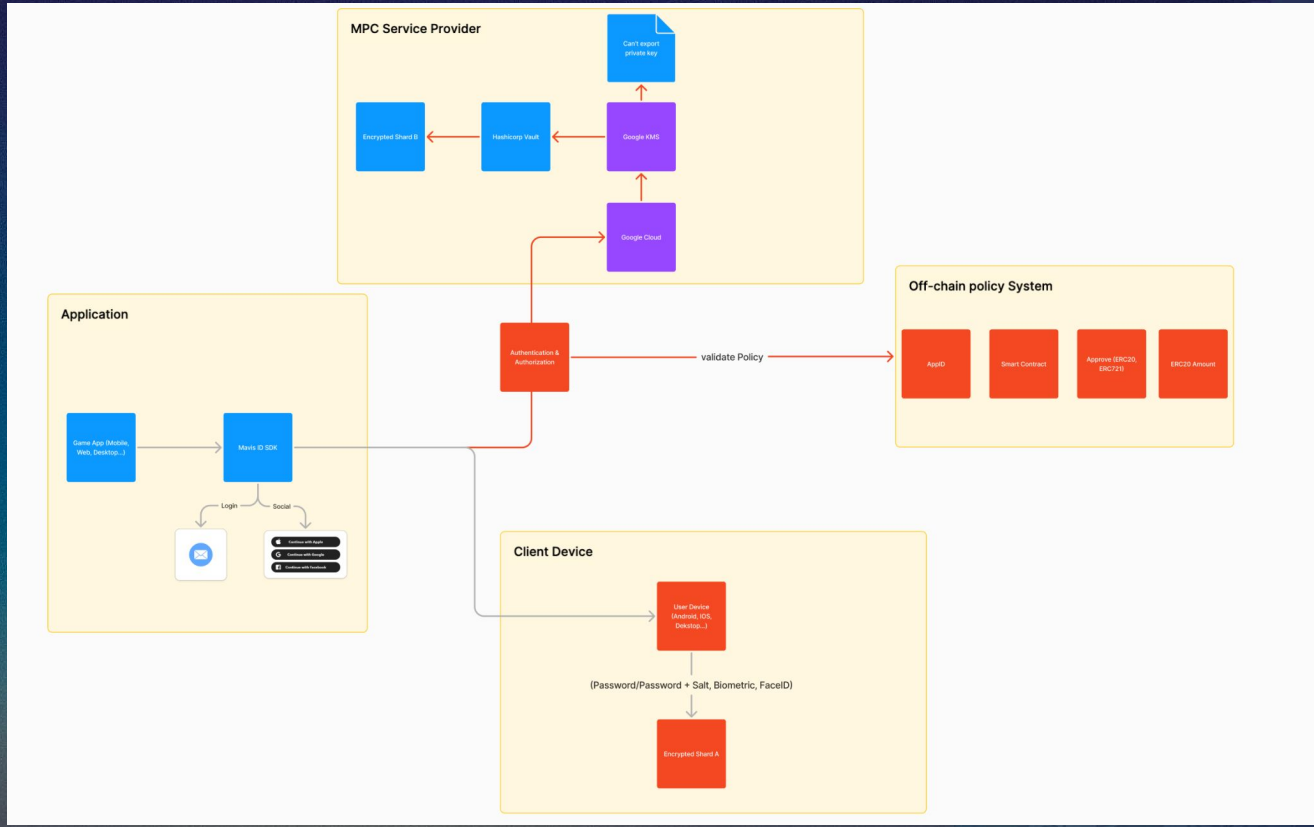
Combine MPC and EIP-7702



Source: https://vitalik.eth.limo/general/2024/10/29/futures6.html

Privilege de-escalation

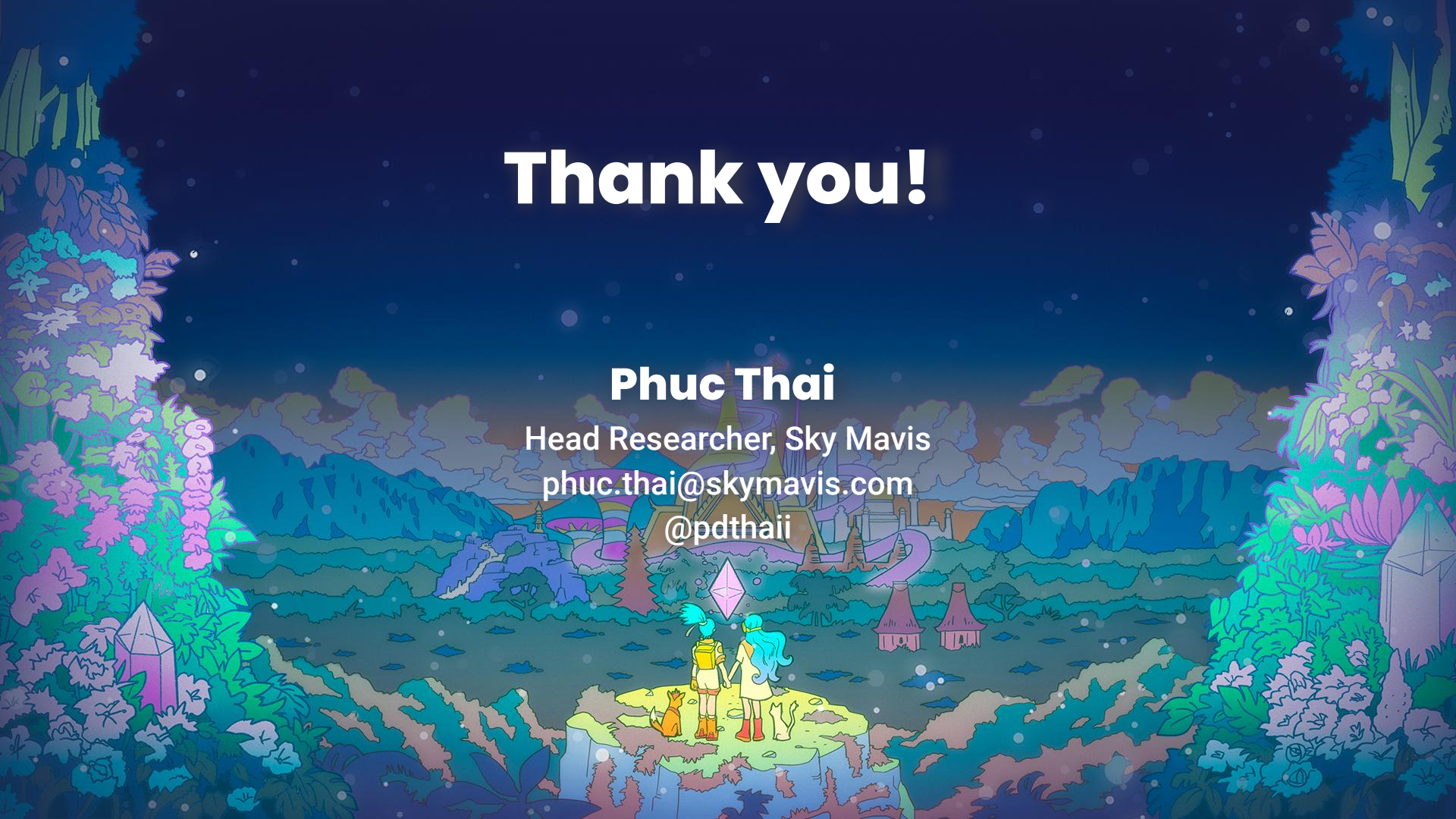
Users can grant access to the key shards within the MPC system, which includes a ready-to-use management solution for handling these key shards.



Time-lock on-chain key recovery

- Selecting an MPC threshold involves trade-offs
  - 2/3 threshold: transactions can be signed without user knowing
  - 2/2 threshold: key cannot be recovered if user loss their key shard
- 2/2 threshold with time-lock on-chain key recovery
  - Allow either shard to gain wallet access if the other shard does not challenge within 30 days

Thank you!



Phuc Thai

Head Researcher, Sky Mavis

phuc.thai@skymavis.com

@pdthaii