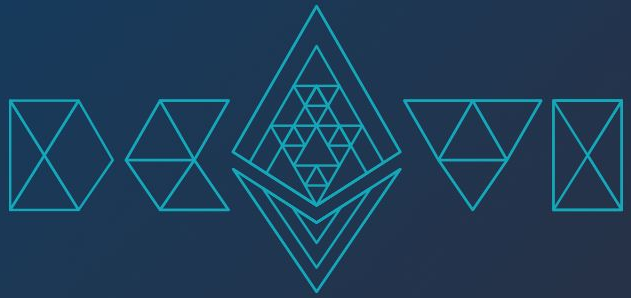


The future of Ethereum Wallets

MPC vs Smart Contract Wallets

Ivo Georgiev

CEO, Ambire Wallet

AMBIRE

Can self-custody be the future for the next billion users?

Myth: “most people are not ready for self-custody”
Reality: most self-custodial wallets are not ready for users

AMBIRE

Current issues with self-custody

- Seed phrases, backup techniques
- Compromised keys, software wallets vulnerable to malware & supply chain attacks
- Social engineering attacks, see BAYC

How do we prevent this? The solution lies in multi-factor authentication, aka **multisigs**

AMBIRE

Why are multisigs *(kind of)* a silver bullet?

- Seedless onboarding: for example, you're onboarded with 2 devices; or separate time-locked recovery key
- Account recovery (eg social recovery)
- Multi-factor authentication
- Resistance to hacks and compromised keys

AMBIRE

MPC vs smart wallets/account abstractions

Which technology is the future?

AMBIRE

What is MPC and what is a smart wallet

MPC refers to multi-party computation. In the context of wallets, in **MPC wallets** the signatures must be produced by 2 or more separate parties.

In other words, a multisig.

With **smart wallets**, each user account is a smart contract, allowing for any custom authentication or execution logic.

Including multisigs.

AMBIRE

Smart wallet mythbusting

- **Myth**: smart wallets can't sign messages
  - **Reality**: smart wallets can sign messages via EIP 1271
- **Myth**: smart wallets produce a different address on each chain, and require setup
  - **Reality**: thanks to CREATE2, smart wallets can be counterfactually deployed on any EVM chain
- **Myth**: smart wallets have huge gas overhead
  - **Reality**: thanks to minimal proxies, the permanent gas overhead is ~3k gas (delegatecall)

AMBIRE

The case for smart wallets

- Much more than just multisigs: **timelocks, spending limits**
  - This also enables recovery mechanisms such as **Argent's social recovery**, or safe seedless onboarding and recovery such as **Ambire's email/pass authentication**
- **Mutable**: you can change the authentication scheme, rotate keys, add/remove signers, etc. - without changing the address
- **Gas abstractions**: paying transaction fees in ERC20 tokens
- **Batching**: multiple operations in one transaction, safely hiding ERC20 approvals; saves the 21k gas base

AMBIRE

The case for smart wallets: advanced use cases

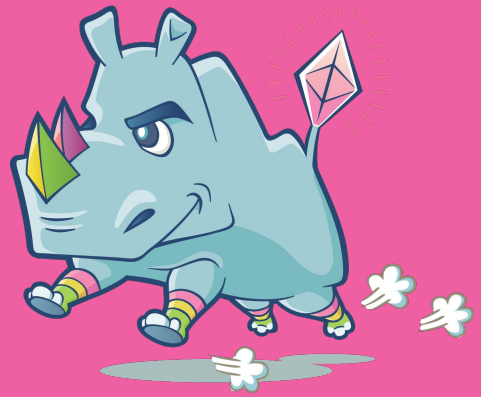
- **Automations**: eg Instadapp, DeFi Saver - for example auto-harvesting rewards
- **Flash loans**: eg Furucombo
- **Alternative cryptography**: eg the NIST curve (Ed25519), paving the way to using WebAuthn, and iOS biometrics

Drawbacks of smart wallets and adoption challenges

- Gas overhead: 30-40k gas on first transaction, 2k gas afterwards
- EIP 1271 still largely unadopted, especially on front-ends
- Developer education: some devs intentionally block smart contracts, they don’t realize contracts can be wallets; “bot protection”

AMBIRE

When would you want to use MPC?



MPC wallets have some distinct advantages

- Off-chain recovery, which is cheaper and easier, but not as flexible
- Truly cross-chain, no dependence on smart contracts - Bitcoin support
- No gas overhead
- No need for any changes in dApps (signatures just work)

AMBIRE

….but it comes at a cost

Problems with MPC wallets

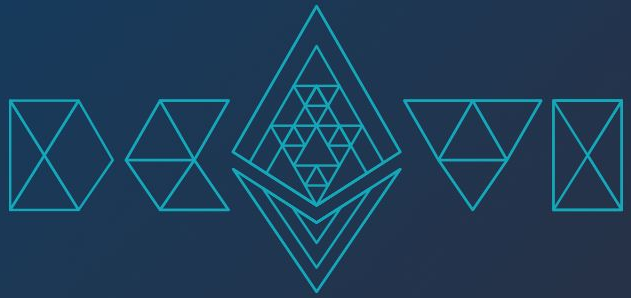
- Custom cryptography required - not great from a security perspective
- Immutable authentication rules, no timelocks, limited to multisig (TSS)
- Cannot be used currently with Trezor/Ledger until they implement it

AMBIRE

Conclusion

- Smart wallets/AAs are more flexible and future proof
- MPC can be a fantastic transitory solution for specific use cases

AMBIRE



Thank you!

Ivo Georgiev

CEO, Ambire Wallet

ivo@ambire.com

@lvshti

AMBIRE