imToken

2023 Crypto Wallet Report:

Top 3 Trends to Look Out For

In collaboration with Matter Labs NEAR STARKWARE

Contents

A note from the author

Let's begin this year with an outlook on what we know best: wallets.

In this report, we show current wallet developments and trends to expect in 2023. We do this by digging into the wallet industry and interviewing crypto-end users as well as teams that are actively innovating on wallets.

Now, let's start by defining wallets. A mobile app wallet - for example - looks and feels very different from a hardware wallet, as does a smart contract wallet.

All of those tools do however share a common feature. They all help users manage their keys, and with that enabling self custody: Digital ownership. Just like cash, but online.

After each exchange hack, Twitter users are reminded of the main selling point of self-custody: "Not your keys, not your crypto". A strong statement, with which you might think a majority of users agree. However, we found that that's not the case. A majority of users are still afraid of losing funds held in self-custody while longing for solutions like multi-factor authentication.

Let's use this report to dig deeper into those notions and shine light on possible solutions being actively developed in 2023.

We want to thank for their contribution: Omar Azhar, Head of Enterprise Business Development at Matter Labs, Tom Brand, Product Lead at StarkWare, Illia Polosukhin, Co-Founder of NEAR, Denys Kovalenko at NEARWEEK, and Chang-Wu Chen, Head of Research at imToken.

One note regarding us, at imToken. We do research on innovations. But for this report we should focus on the industry as a whole.

Philipp Seifert (Business Development Director) and the imToken team.

Wallets saw steady developments in 2022

Before we look into the future, let's see where we stand today. In terms of new developments in the wallet space 2022 was not that usual. For 2023, however, we see important developments gathering pace. We identify three main areas of interest:

Self-custodial wallets
smart wallets specifically

Multi-party computation (MPC)

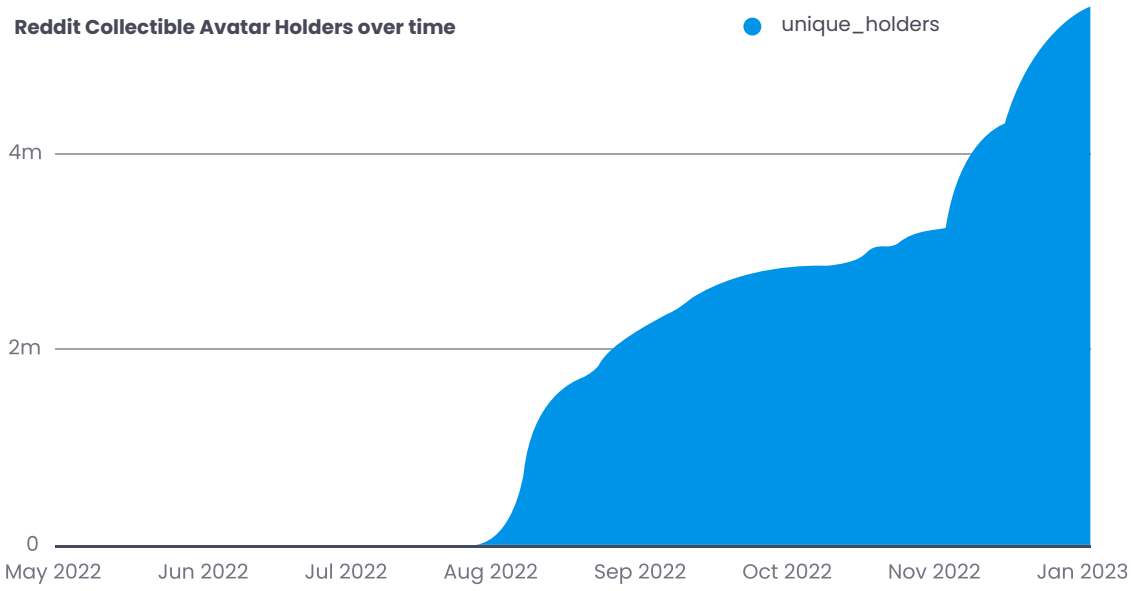
Account Abstraction (AA)

The first main area is the ongoing fight between self-custody vs custody. Wallets like Metamask, imToken and Ledger promise security as well as easy access to DeFi. Exchanges, on the other hand, stand for convenience, easy access to traditional trading and lending products.

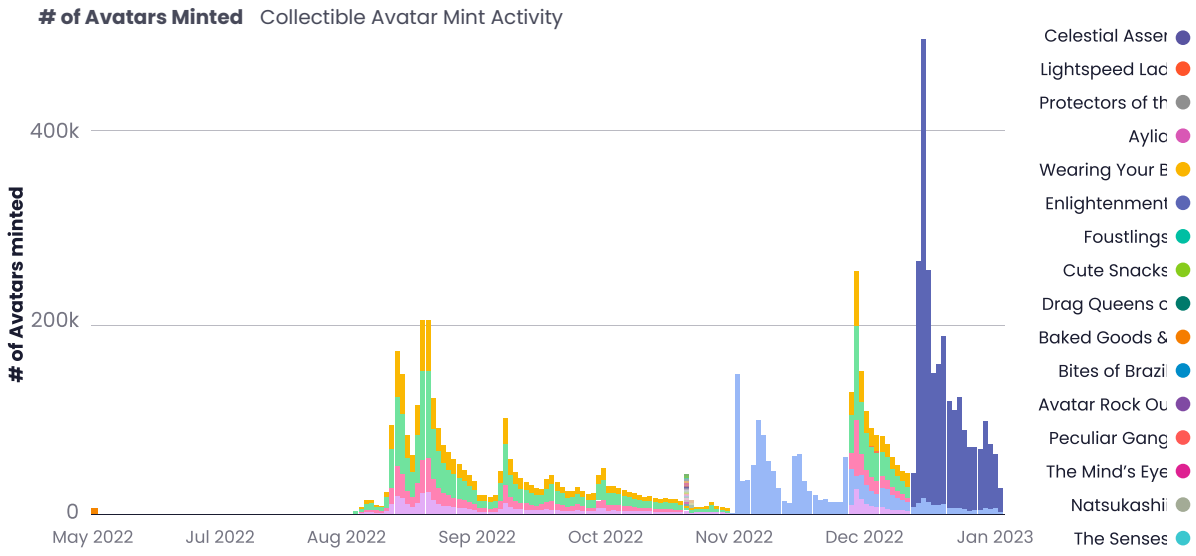
In 2022, we saw old narratives continue like Apple insisting on their fee on any crypto payments and stopping Coinbase Wallet from supporting NFTs. At the same time we saw DeFi projects - like dYdX, ParaSwap - release their own mobile wallets.

On top, PayPal released a custodial wallet feature, and Web2 companies like Reddit - the 6th most popular website of the world - added a wallet functionality to their app.

Curiously, Reddit calls their wallet feature a “vault” and somewhat hides private keys from the user. By hiding this complexity that traditional crypto wallets usually present to the user, Reddit was able to onboard millions of users to the blockchain. Most of their users might not even know the blockchain that guarantees integrity of their “Reddit Collectible Avatars”, Polygon.



Millions of people started using crypto wallets, thanks to Reddit[1]



Reddit NFTs are popular as shown by the increasing number of mints[2]

Users feel pain around self-custody

Curious about their motivation, we surveyed 180 crypto users about self-custody and wallets.

We learned that nearly two thirds (63%) of users found trading on exchanges to be more convenient or cheaper than trading on wallets.

More shocking though, 38% of users found wallets less secure than exchanges. Security being one of the key differentiators in the favor of wallets does not seem to convince end users who fear being hacked (29%) or by their own mistake (18%).

63%

of users found trading on exchanges to be more convenient or cheaper than trading on wallets.

38%

of users found wallets less secure than exchanges.

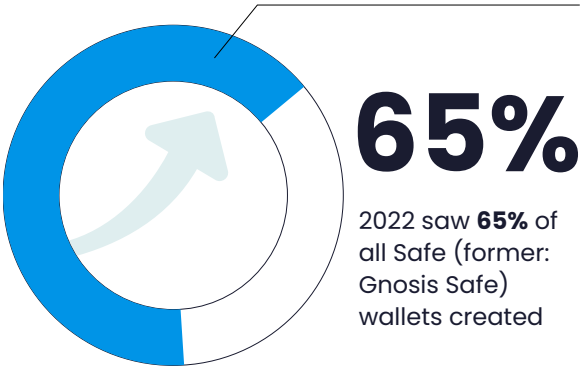
And those pain points are real. Crypto enthusiasts told us they would pay up to US$100 for a wallet that would solve all of those issues that exist with the wallet they use today. However, they are not optimistic. A big part of users (over 25%) think that most people will only start switching to self-custody - the fundamental paradigm of crypto - in 5 years or more. And a similar number of interviewed users (25%) believe that a majority of crypto users will stay with custodial solutions, even 10 years from now.

Smart(er) wallets are niche, but growing

How are wallets solving those pain points in 2023? How far is development, and how will 2023 see big changes?

Let's take a look at our second and third focus areas, smart contract wallets as well as new developments such as MPC, AA. Both areas are still relatively young, but promising and supported by major industry players.

In its entire history, 2022 was the industry's year where most smart contract wallets were created, although arguably a bad year for crypto. For example, 2022 saw 65% of all Safe (former: Gnosis Safe) wallets created. More than double the previous year.

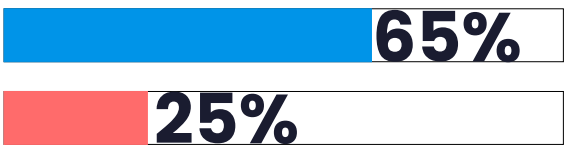


65%

2022 saw **65%** of all Safe (former: Gnosis Safe) wallets created

At the same time Argent, another smart wallet, saw declining numbers[3]. And the industry consolidated with OpenSea acquiring Dharma, a smart wallet pioneer team.

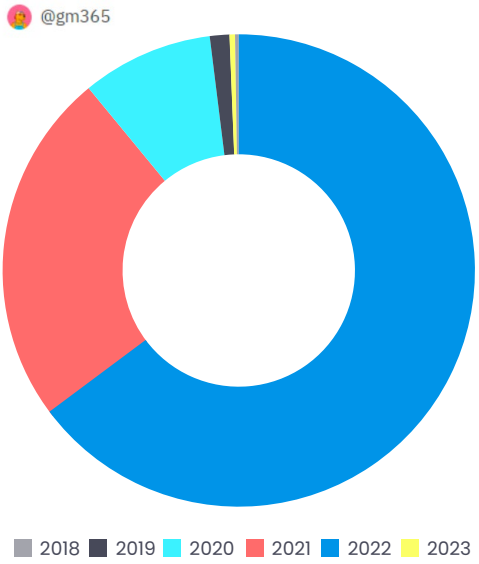
In our survey, 65% of users stated that they heard of smart wallets and know what they are. Not so with the newer concepts of MPC or AA, which respectively only 25% of users know.



Users know about smart wallets
User approval MPC or AA

Explained

Smart contract wallets (like Safe, Argent) look like other wallet apps, but are based on smart contracts instead of end user accounts. Therefore, they can have some additional features built into them, like multi-sigs and time-locks.



Gnosis Safe's Creation Year[4]

A big part of wallets are not 'smart' though. Let's assume the number of crypto wallet users peaks at around 30 million MAU (i.e. MetaMask's MAU[5]). And Safe user numbers peak around 30k - 60k[6]. **Then smart wallet users make for only one in a thousand crypto wallet users.**

0.1%

of wallets are smart

In the area of new developments we saw Coinbase release the first mainstream MPC wallet, after having acquired Unbound Security in 2021[7]. And crypto infrastructure provider Blockdaemon acquired Sepior[8]. Both acquired companies are top tier MPC companies.

Explained

Multi-party computation (MPC) wallets (like the Coinbase app or Zengo) replace the traditional private key with a "secret" shared between your device and one or more others. This also gives additional features like easier account recovery.

Explained

Account Abstraction (AA) basically makes smart contracts work the same way ordinary end-user accounts work today; either by improving smart contracts or actually changing the underlying blockchain's code. This helps building smart contract wallets with even more features.

Wallets will be able to solve pain points in 2023

We started this report with a definition of a wallet being about managing key pairs. When it comes to new solutions it is not surprising that most new features change some way of handling keys. The approaches mentioned before simply use different technical solutions to help users add, delete, restrict or change keys to an account, or add custom logic to the account itself.

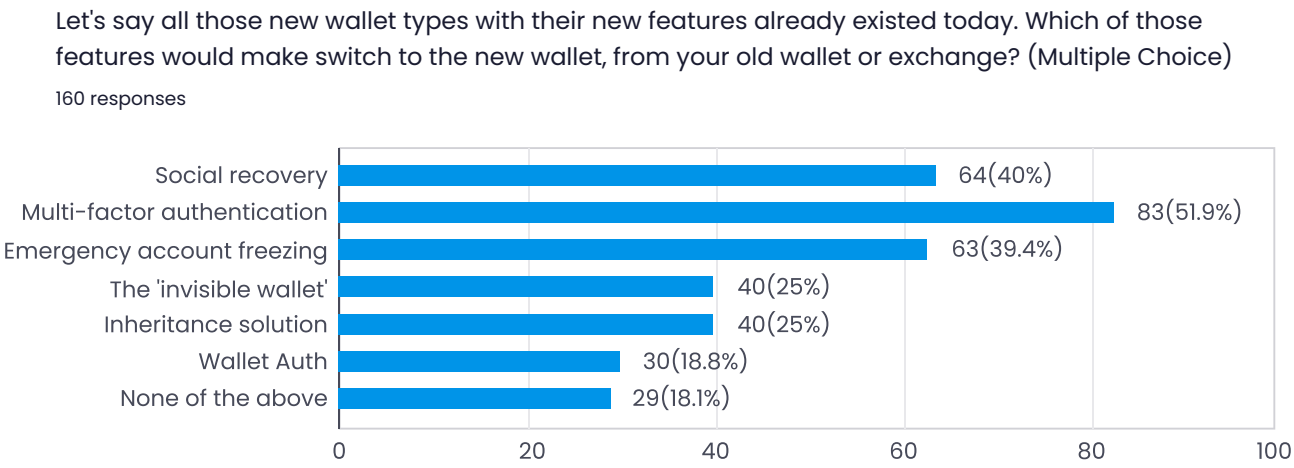
Let us take theft as an example. Restricting access helps to minimize damage, after which taking away a thief's key and changing access to another key pair owned by the user helps to recover access. Providing keys to a third-party helps reduce workload for the user.

1. Security

Security. In case of a third-party gaining access or the user losing access, new kinds of wallets limit, restrict access to third-parties and finally help to regain access.

51%

We asked crypto users which benefits they expect from future wallets. **Over half of participants (51%) told us they would take improved security in the form of multi-factor authentication as a reason to choose a new wallet.**



We identified three areas where wallets promise improved security. First, wallets can help users to control risks before funds are stolen or access is lost. Second, should anything happen to an account, users can stop unwanted access. And last, users can regain access after the security incident happened.

1 Risk control

- Daily transaction amount limit. A transaction amount limit can be set to help reduce the chance of an expensive user error and to help prevent an attacker from emptying a wallet in one transaction.

- Other conditions for transactions such as time limits.

2 Stop access

- Emergency account freezing. In the event of a lost or stolen device, an account can be locked, or access to the account from the compromised device can be deactivated.
- Multi-factor authentication. Smart wallets can provide an extra layer of security via authenticator apps and/or native wallet solutions.
- Whitelisting. Users can specify that transfers be made only to known addresses.

3 Regain access

- Multi-signature authorization. Two or more users can approve a transaction for improved security. Smart wallets can also enable multisig transactions to be authorized offline to save users time.
- Self & social recovery. Smart wallets like Argent might use the term “Guardians”, and other wallets simply call them multi-signature signers. But what they help you to do is the same: "Seedless" account recovery. You or your friends can unlock frozen accounts or approve new devices.
- Key rotation. Retire and replace a compromised key.

2. Convenience

A whooping 76% of interviewed users found custodial solutions more convenient than wallets, while only few looked for convenience in wallets. We think that users will only realize convenience once use cases - such as inheritance solutions - exist. Before then, users might be happy with custodial solutions.

76%

of interviewed users found custodial solutions more convenient than wallets

1. The "Invisible Wallet": Being able to use an email login as well as batching transactions creates a Web2-like experience.

Bundled transactions and session keys. Smart contract wallets can approve an amount of tokens to use with a dapp and execute all transactions in “bundled” transactions.

Paid gas fees. Smart contract wallets can pay gas fees for users, preventing users from having to maintain an ETH balance and greatly improving the transaction experience.

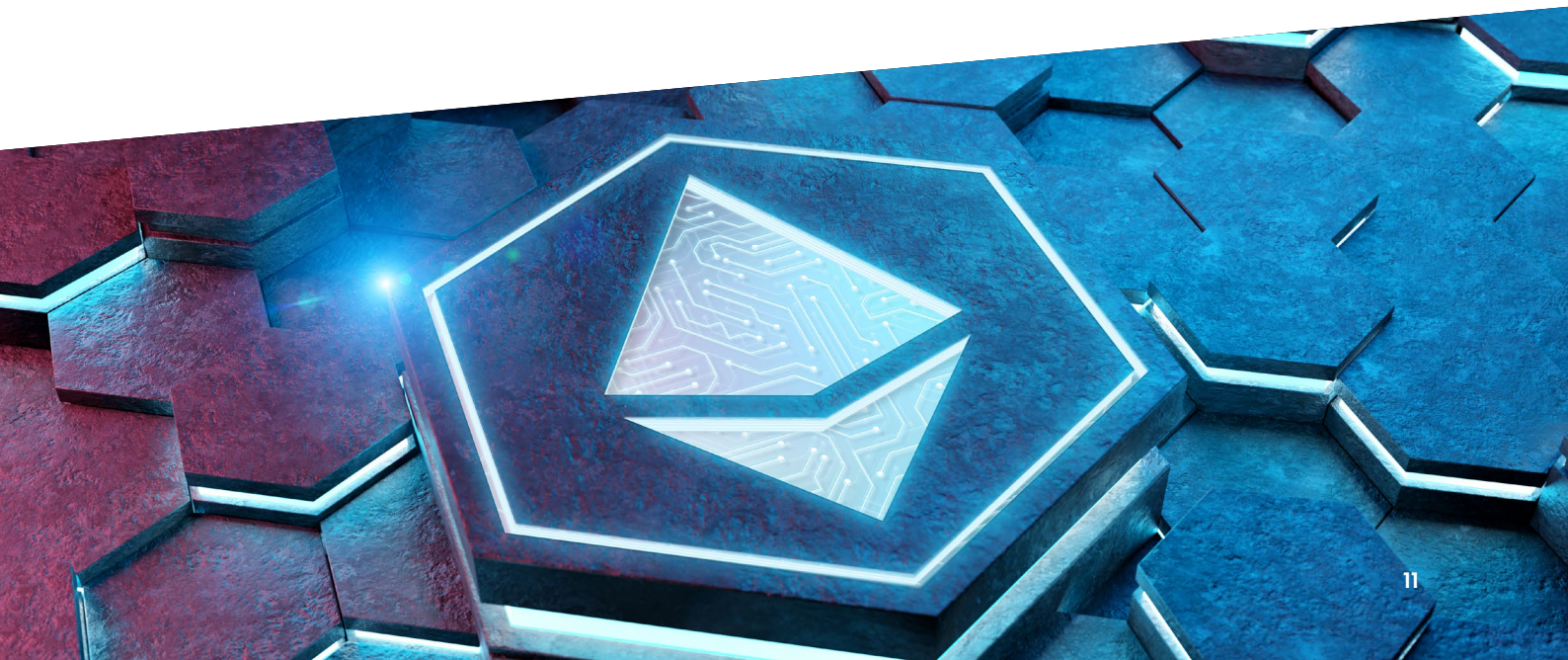
Automatic and recurring payments like your utility company or your mortgage lender.

2 "Custom business logic" being built directly into smart wallets thanks to Account Abstraction.

Identity and KYC can be linked with the accounts so that users can automatically authenticate against an authority like an exchange asking for KYC.

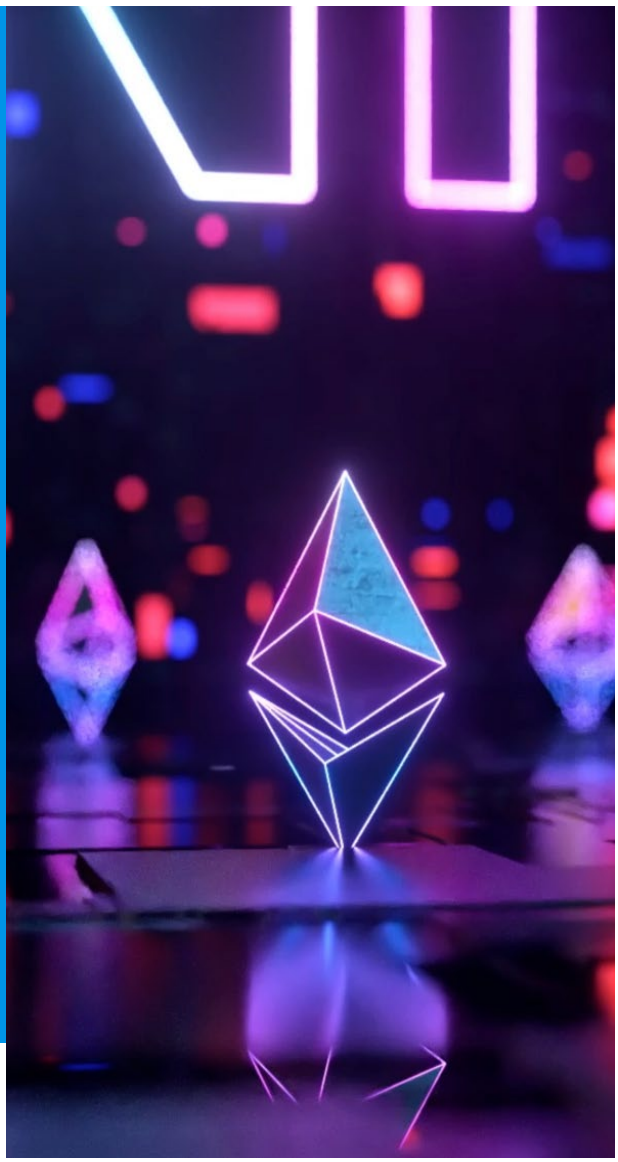
Different wallet types allow for different, specific functions and capabilities like checking account wallets or retirement accounts.

3 Social login or application specific login, enables self-custody wallet to use google sign-in on all DApps.



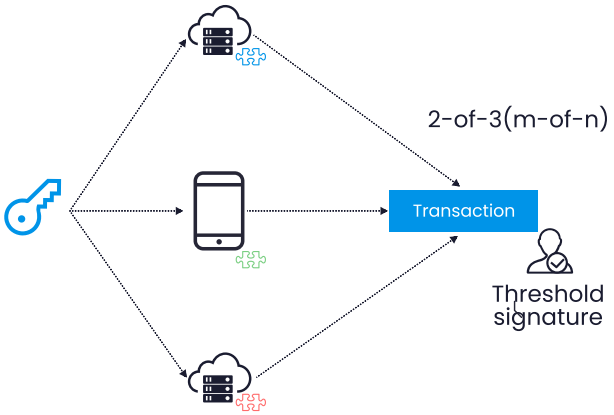
Different technical solutions and their trade-offs

Smart contract wallets (like Safe, Argent) look like other wallet apps, but are based on smart contracts instead of ordinary accounts. Therefore, they can have some additional features built into them, like multi-sigs and time-locks.

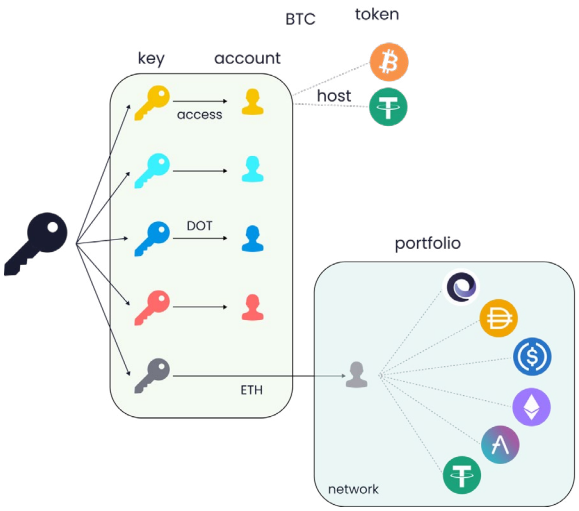


1. Multi-party computation (MPC)

Multi-party computation (MPC)[9] wallets (like the Coinbase app or Zengo) replace the traditional private key with a "secret" shared between your device and one or more others. This also gives additional features like easier account recovery.



The MPC wallet looks like an EOA with an invisible private key. Besides, it could be designed with the threshold setting. For a 2-of-3 threshold wallet, the user requires another party to co-generate the signature. The party could be designed in a centralized or decentralized way.



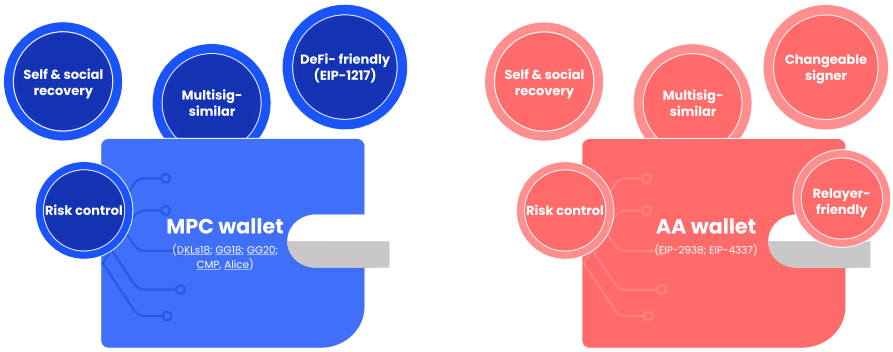
imToken Head of Research, Chang-Wu Chen, noted: "A MPC wallet looks like an EOA with an invisible private key. So it can natively support multichain, like BTC, or whatever public blockchain, only if their signature scheme is MPC-friendly. Sounds perfect, right? But for the MPC solution, it requires having an online computing unit to co-work with."

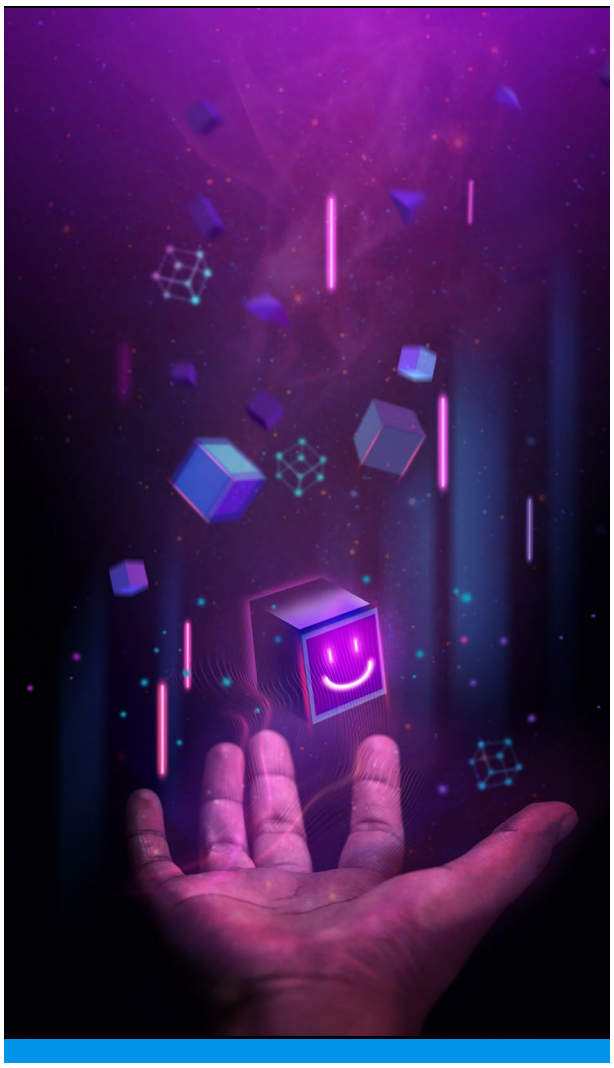
2. Account Abstraction

On Ethereum, there are two types of accounts, EOA and smart contract account. An abstract account[10] wallet is a kind of smart contract wallet. The nice thing - compared to MPC - is that the smart contract is flexible and easier to have customized logic and it's always online. For an AA wallet, there is an entrypoint for two phases, verification and execution. On current Ethereum, transactions are verified by ECDSA signature, with balance and nonce check, then execute the transfer or the call function.

Abstract account allows you to define your own rule, so we don't really have to use ECDSA. You can have other signatures, like BLS, EdDSA. Also, you can define the withdrawal daily limit or other rules on whatever you like.

Head of Research at imToken, Chang-Wu Chen, told us that to him "the most important and interesting thing is that we can abstract accounts from the EOA. Thus, we can have a signer, separate from the account. This is really perfect for the future because we can have a DID. If we can guarantee the signer could be changed or recovered, then we can have the same account just like our ID number. "





3. Baselayer account innovation

Some blockchains already offer solutions that offer benefits similar to the ones from MPC and AA wallet solutions. We interviewed three blockchain projects in that area:

The Layer 2 projects

Matter Labs (zkSync)

StarkWare (StarkNet)

The blockchain project

NEAR

NEAR

The NEAR team launched its mainnet in 2020[11] with an account model unlike its 5 year older sibling, Ethereum. On the NEAR blockchain all accounts are contracts[12], all of which can be controlled by multiple key pairs.

This brings a couple of smart features to NEAR users by default. They can set different permissions per key, add and remove devices, create social recovery and more - all features that the Ethereum community is working to add on top of its base layer blockchain.

NEAR's co-founder, Illia Polosukhin, told us that "security is indeed a big part" of the benefit of the account model, with an estimated "500k-1m accounts" having used multiple keys per account so far.

Regarding the competition Illia mentioned that Ethereum's "model is very

different and changing now is really hard, it would involve changing EVM and lots of other stuff to properly support it or it will be just a hack on top which nobody wants".

NEARWEEK's Denys Kovalenko added that "more blockchains will realize the accounting system NEAR adopted from the beginning is a feature as it's a flagman for Web3 mass adoption, we will see more similarities from Web2 world like: domain names, email address based on domain names, etc"

Matter Labs and StarkWare

Just like NEAR's Polosukhin, both representatives of StarkWare and Matter Labs told us to be excited about bringing benefits in convenience, security and flexibility to users.

Unlike NEAR, Layer 2s do have the challenge to work with existing EVM paradigm while trying to offer smartness at the baselayer. We asked Matter Labs - the developer of zkSync - and StarkWare - the developer of StarkNet - about their approach.

StarkNet and zkSync both natively add AA to their Layer 2 blockchain. User accounts are represented by smart contracts which can initiate transactions.

Tom Brand, Product Lead at StarkWare, liked the result to "a Web2 user experience", and mentioned how Visa (the financial services company) recently built on StarkWare's network[13]. The payment prototype shows that Account Abstraction allows users to have the same user experience for recurring payments in between existing Visa users and StarkNet self-custodial users as with traditional payments.

Omar Azhar, Head of Enterprise Business Development at Matter Labs, agreed that "many companies are interested in seeing how they can enable a seamless Web2 experience for self-custody wallets within their applications". Azhar added "being

able to use an email login, using paymaster and AA to batch transactions" would help applications to build trust with users - an invaluable asset for crypto products. Fittingly he called this the "Invisible Wallet".

Azhar added that another benefit was "'custom business' logic being built directly into smart wallets thanks to Account Abstraction", like embedded identity and KYC.

Tom Brand added that users could "even use plug-ins to access new functionalities and technologies" and "block scam addresses, which can help improve the security of their digital accounts and transactions". Which Azhar addressed as well, saying that Account Abstraction could create "different wallet types with specific functions and capabilities - checking account wallet, retirement account".

Reference

1. https://dune.com/polygon_analytics/reddit-collectible-avatars
2. https://dune.com/polygon_analytics/reddit-collectible-avatars
3. https://dune.com/queries/1846106
4. https://dune.com/gm365/gnosis-safe
5. https://consensys.net/blog/press-release/metamask-celebrates-its-6th-anniversary-with-6-digit-growth-strategic-update-to-the-market/
6. https://dune.com/queries/1841765
7. https://www.coinbase.com/blog/coinbase-to-acquire-leading-cryptographic-security-company-unbound-security
8. https://techcrunch.com/2022/07/20/crypto-startup-blockdaemon-continues-acquisition-spree-buying-sepior
9. To dive deeper into MPC see: DKLs18; GG18; GG20; CMP, Alice
10. To dive deeper into AA see: EIP-2938, EIP-4337
11. https://near.org/blog/near-mainnet-is-now-community-operated/
12. https://docs.near.org/concepts/basics/accounts/access-keys
13. https://usa.visa.com/solutions/crypto/auto-payments-for-self-custodial-wallets.html

About imToken

imToken is a decentralized digital wallet used to manage and safeguard a wide range of blockchain- and token-based assets, identities and data. Since its founding in 2016, it has helped its users transact and exchange billions of dollars in value across more than 150 countries around the world.

About StarkWare

StarkWare develops ZK-Rollups, STARK-based solutions for the blockchain industry. Its products facilitate secure, trustless, and scalable blockchain applications.

StarkWare develops StarkEx, a standalone permissioned Validity-Rollup, and StarkNet, a permissionless decentralized ZK-Rollup, while also implementing account abstraction to improve user experience.

About Matter Labs

Matter Labs is scaling Ethereum with zero-knowledge proofs, which they identify as “most viable technology to enable the mainstream adoption of public blockchains”. Their mission is to accelerate this ongoing financial revolution.

Its main product, zkSync, has been in production since Summer 2020. While growing in usage, making crypto payments cheaper, the team also innovates on Account Abstraction.

About NEAR

NEAR Protocol is a general purpose blockchain similar to Ethereum. NEAR is a Proof-of-Stake blockchain that uses sharding technology to achieve scalability, similar to the future plan for Ethereum.

The team focuses on developer and user-friendliness, innovating on features like automatic transaction fee sharing to smart contract developers. The blockchain’s account model adds smart wallet features at a base layer level.

imToken

For more information, please click the following social media platforms.

Linkedin Twitter Youtube Instagram Discord