imToken

2023 年
加密钱包报告：

值得关注的三大趋势

联合发布 Matter Labs NEAR STARKWARE

目录

前言

新的一年，我们准备了一份加密钱包赛道报告，和大家分享。

在这份报告中，我们通过数据分析、采访加密货币用户及钱包领域的创新团队，总结和探讨了钱包的发展现状及其在 2023 年的趋势。

首先，什么是钱包？我们熟悉的钱包形态有移动端钱包、硬件钱包、智能合约钱包等，它们形态和使用方式各不相同，但却有一个共同点：帮助用户管理自己的密钥，以此实现自我托管资产及数据所有权。

我们原以为「Not your keys, not your crypto」已是加密货币持有者的共识，但本次研究显示事实并非如此：大多数用户害怕丢失自我托管的资产，并期待多因素身份验证等资产管理解决方案。

继续阅读！和我们一起深入挖掘这些概念，并探讨 2023 年值得期待的最新方案。

感谢 Matter Labs 企业业务发展主管 Omar Azhar、StarkWare 产品主管 Tom Brand、NEAR 联合创始人 Illia Polosukhin、NEARWEEK 的 Denys Kovalenko 和 imToken Labs 负责人 Chang-Wu Chen 为本报告作出的贡献。

注：imToken 是钱包服务商，但在这份报告中，我们聚焦于整个行业。
Philipp Seifert（业务发展总监）和 imToken 团队

2022 年，钱包稳步发展

基于对 2022 年的观察总结，我们看到了钱包赛道上的三个主要创新方向：

自托管钱包

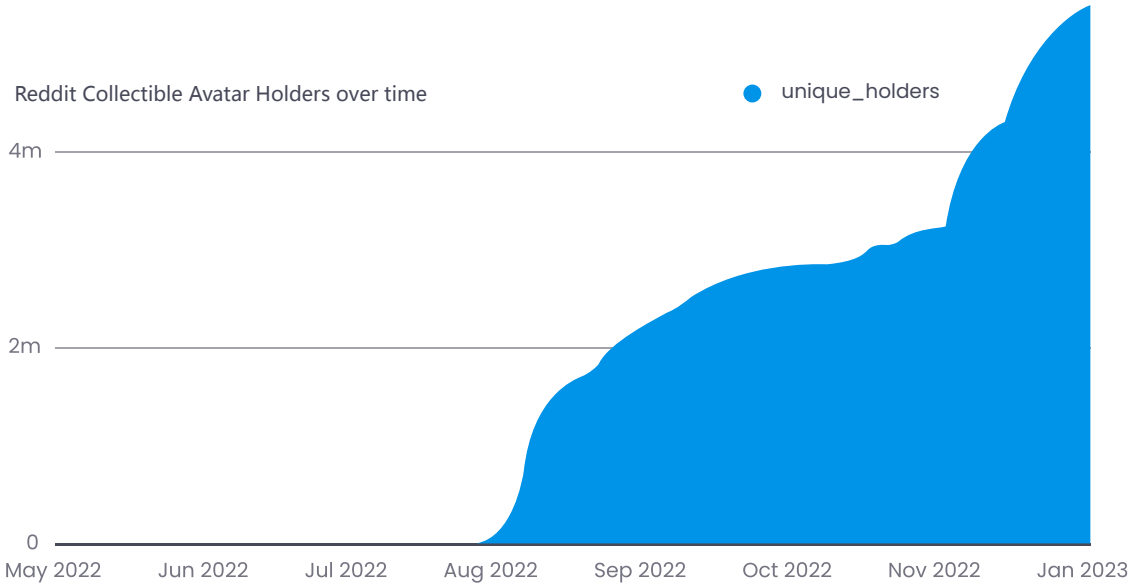
多方计算
(MPC)

抽象账户
(AA)

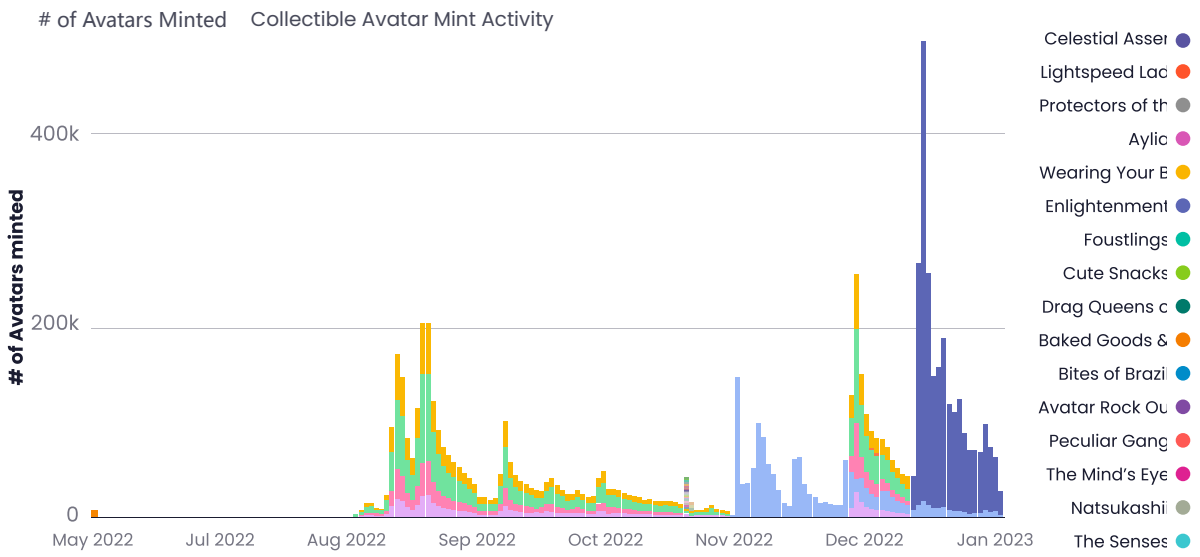
第一个创新方向关于第三方托管和自托管。自托管服务如 MetaMask、imToken 和 Ledger 等钱包承诺安全并支持轻松访问 DeFi。第三方托管服务如中心化交易所往往以便捷为卖点，支持传统交易模式并允许用户轻松使用借贷产品。

2022 年，我们观察到此类中心化和去中心化的对抗仍在持续。比如 Apple 坚持对其生态中的任何加密支付收取费用，并禁止 Coinbase 钱包的 NFT 功能；我们也看到 DeFi 项目如 dYdX、ParaSwap 发布了自己的移动端钱包应用；PayPal 发布了托管钱包功能；世界第六大最受欢迎的网站 Reddit 也在其应用程序中添加了钱包功能。

值得一提的是 Reddit 的钱包功能被命名为「valut」，意为保险库，而非常见的「wallet（钱包）」，并在一定程度上隐藏了私钥的概念。通过隐藏传统加密钱包在用户体验上的复杂性，Reddit 顺利让数百万用户触及区块链，即便其中大多数用户甚至可能不知道自己的 Reddit 收藏头像是基于 Polygon 区块链发行的 NFT。



感谢 Reddit，数百万人开始使用加密钱包 [1]



铸币数量的增加，表明 Reddit 上的 NFT 很受欢迎 [2]

用户仍对「自托管」模式缺乏信心

出于对加密用户动机的好奇，我们设计了一个关于自托管和钱包的问卷，并收集了 180 份用户反馈。

统计数据表明，近三分之二（63%）的受访者认为在交易所交易比在钱包内交易更方便或更便宜。

更令人震惊的是，38% 的受访者认为钱包不如交易所安全。自托管所赋予的安全性是钱包的基础和关键优势，但这似乎仍无法打消他们对被黑客攻击 (29%) 或害怕自己犯错 (18%) 导致资产丢失的担心。

63%

的受访者认为在交易所交易比在钱包内交易更方便或更便宜。

38%

的受访者认为钱包不如交易所安全。

这些痛点是真实存在的。加密货币的忠实用户告诉我们，他们愿意支付 100 美元，以解决他们目前所使用钱包存在的所有问题，换取一份安心。然而，他们对钱包普及并不乐观。25% 的受访者认为至少需要 5 年时间，自托管钱包才会被大多数人所接受。另 25% 的受访者认为，即便再过十年，大多数加密货币用户仍会选择第三方托管方案。

智能合约钱包：小众，但在增长

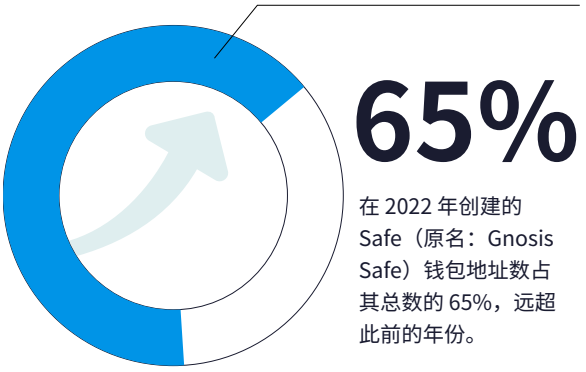
钱包如何在 2023 年解决这些痛点？发展现状如何，2023 有哪些值得期待？

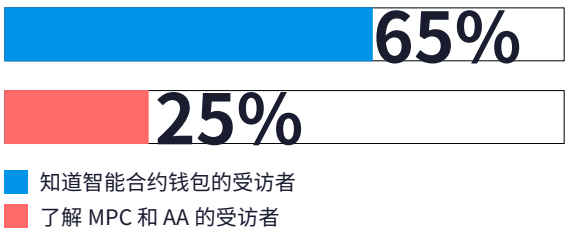
来看第二和第三个创新方向，分别是 MPC 和 AA，两者共同为智能合约钱包的基础。这两个方向都还相对早期，但前景广阔，并得到了主要行业参与者的支持。

尽管 2022 年是加密寒冬，但从整个加密发展史来看，它却是智能合约钱包地址快速增长的一年。例如，在 2022 年创建的 Safe（原名：Gnosis Safe）钱包地址数占其总数的 65%，远超此前的年份。

与此同时，智能合约钱包 Argent 的地址创建数在 2022 年有所下滑[3]。此外，OpenSea 收购了 Dharma Labs - 另一个智能合约钱包团队。

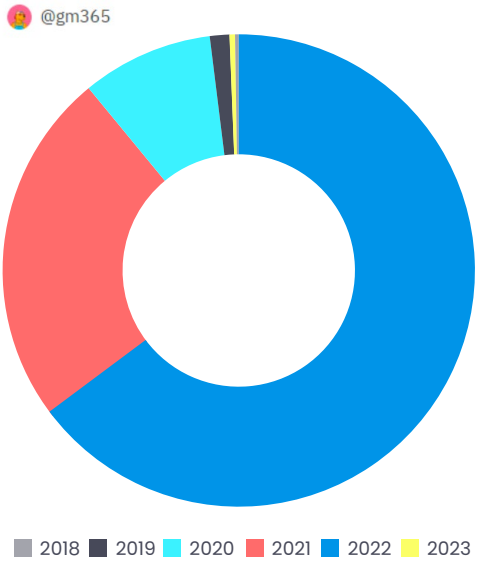
在我们的调查中，65% 的受访者表示听说过智能合约钱包并知道它们是什么。但对于 MPC 和 AA 这两个新概念，受访者中分别只有 25% 表示了解。





名词解释

智能合约钱包（如 Safe、Argent）：不同于其他钱包应用，通过它创建的钱包地址账户类型属于合约账户（基于智能合约），而非 EOA 账户（即目前多数钱包支持的账户类型）。因此，它们可以内置一些附加功能，如多重签名和时间锁。



Gnosis Safe's Creation Year[4]

当下，大多数钱包并非智能合约钱包。我们假定加密钱包用户的数量为 3000 万（即 MetaMask 的 MAU[5]）。Safe 钱包用户数量在 30k - 60k[6]。由此算得**智能合约钱包用户约仅占加密钱包用户的千分之一。**

0.1%

的智能合约钱包

关于这方面的发展现状，我们观察到 Coinbase 在 2021 年收购 Unbound Security 之后[7]，发布了第一个主流 MPC 钱包。加密基础设施提供商 Blockdaemon 收购了 Sepior[8]。这两家被收购的公司都是第一梯队的 MPC 团队。

名词解释

多方计算（MPC）钱包（如 Coinbase 应用、ZenGo）：用你的设备与一个或多个其他设备共享的「秘密」取代传统的私钥。基于该特性还有更多衍生功能，如更轻松的账户恢复。

名词解释

抽象账户（AA）：通过改进智能合约或更改底层区块链代码，使智能合约的使用体验和 EOA 账户（即目前多数钱包支持的账户类型）的使用体验基本相同，有助于构建具有更多功能的智能合约钱包。

2023 年，有望解决钱包痛点

我们在这份报告开篇定义了钱包：一种帮助用户管理自己的密钥，以此实现自我托管资产及数据所有权的工具。因此新的解决方案也基本围绕如何处理密钥而展开。上文提到的方法归纳起来即为通过使用不同的技术方案来帮助用户添加、删除、限制或更改账户的密钥，或者为账户本身提供自定义逻辑。

以盗币案件为例。取消攻击者盗取的密钥权限并将访问权更改为用户拥有的另一对密钥，从而帮助用户恢复账户，将损失降至最低；向第三方提供部分密钥也有助于分担用户自托管的责任。

1. 安全

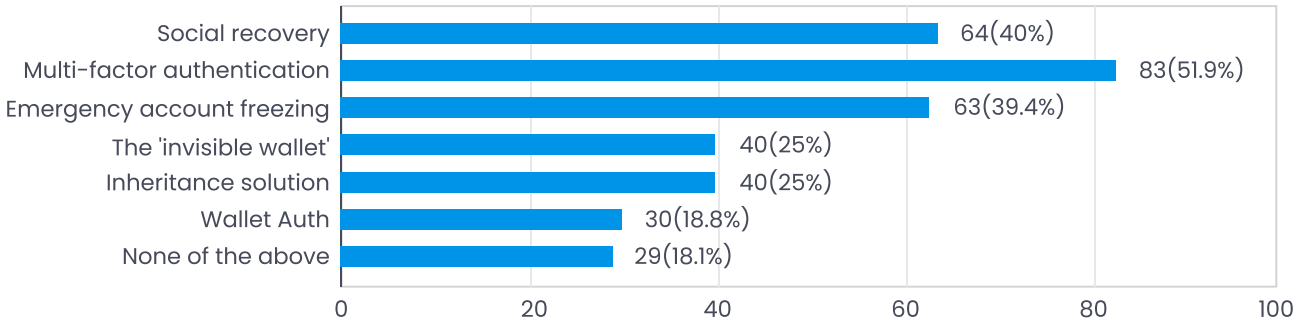
在攻击者获得访问权限或用户失去访问权限的情况下，下一代钱包将可限制攻击者的权限并帮助用户重新获得访问权限。

51%

通过统计受访者关于「在下一代钱包的诸多功能中，最期待哪一个」的回答，我们看到**超过一半的受访者（51%）愿意以「支持多因素身份验证提高安全性」为由选择新钱包。**

Let's say all those new wallet types with their new features already existed today. Which of those features would make switch to the new wallet, from your old wallet or exchange? (Multiple Choice)

160 responses



我们将钱包安全性分为三方面。首先，钱包可以帮助用户在资金被盗或访问权限丢失之前控制风险。其次，如果账户出现任何异常，用户可以终止未经许可的访问。最后，用户可以在安全事件发生后重新获得访问权限。

1 风险控制

- 每日交易金额限制。通过设置交易金额限制，帮助用户降低误操作的可能性，并防止攻击者在一次交易中清空钱包。
- 其他交易风险控制，例如时间限制。

2 停止访问

- 紧急账户冻结。在设备丢失或被盗的情况下，可以锁定账户，或者可以解除受感染设备对账户的访问权限。
- 多因素身份验证。智能合约钱包可以通过身份验证器应用程序和 / 或本地钱包解决方案提供额外的安全保护。
- 白名单。用户可以指定只向已知地址进行转账。

3 重新获得访问权限

- 多重签名授权。通过要求两个及以上用户共同授权以批准交易来提高安全性。智能合约钱包还可支持离线授权多重签名交易，以节省用户时间。
- 自我恢复、社交恢复。如智能合约钱包 Argent 的「Guardians」，其他钱包的「多签签名者」，它们的作用相同：帮助用户无需助记词或私钥即可完成账户恢复。你或你的朋友可以解锁冻结的账户或授权新设备。
- 密钥轮换。停用并更换受损密钥。

2. 便捷

高达 76% 的受访者认为第三方托管方案比钱包更方便。对此，我们认为，只有当用例（例如资产继承）存在时，用户才可能切实体会到自托管的便利。否则，用户可能会更倾向于第三方托管方案。

76%

的受访者认为第三方托管方案比钱包更方便。

1 **隐形钱包：能够使用邮箱登录以及批处理交易，创建类似 Web2 的体验。**

捆绑交易和会话密钥。智能合约钱包可以批准一定数量的代币与 DApp 一起使用，并在捆绑交易中执行所有交易，以降低操作复杂度。

代付交易费用。智能合约钱包可以替用户支付交易费用，避免用户由于没有预留 ETH 而无法发起交易，优化交易体验。

自动和定期付款。如公司的定期支出、个人的抵押还款等。

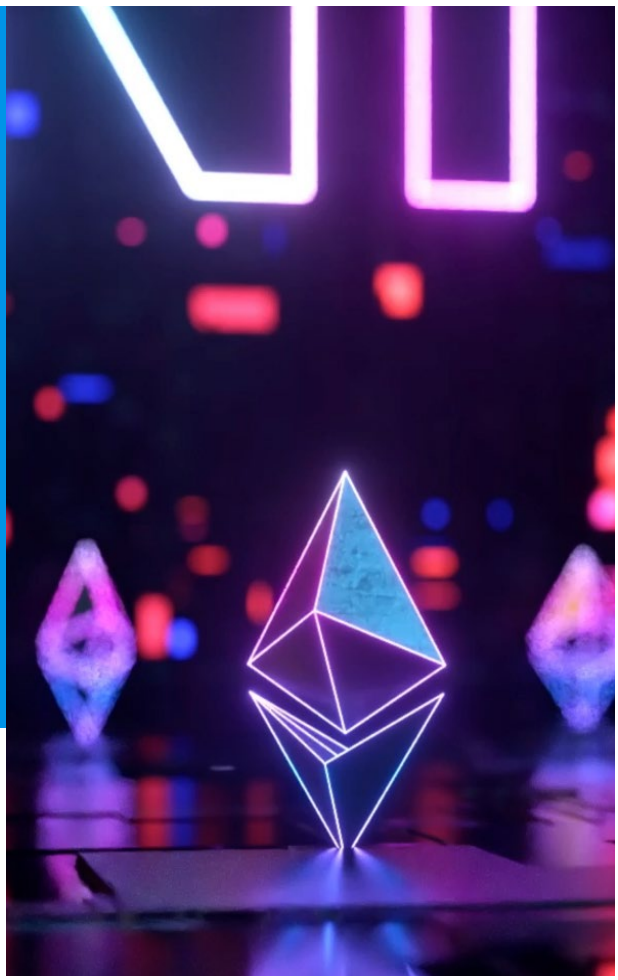
2 **基于抽象账户，内置「自定义业务逻辑」的智能合约钱包。**

身份和 KYC 可以与账户相关联，以便用户进行身份验证，例如要求 KYC 的交易所。

更灵活的钱包设置。不同的钱包类型可支持特定的功能，例如支票账户或退休账户。

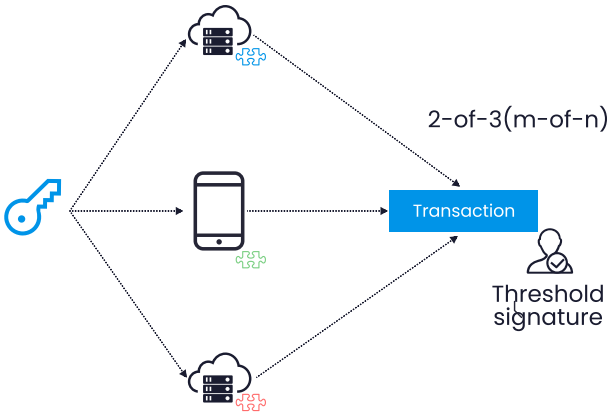
3 **社交登录或应用程序登录。使自托管钱包能够在所有 DApp 上使用谷歌登录。**

不同技术方案及其权衡

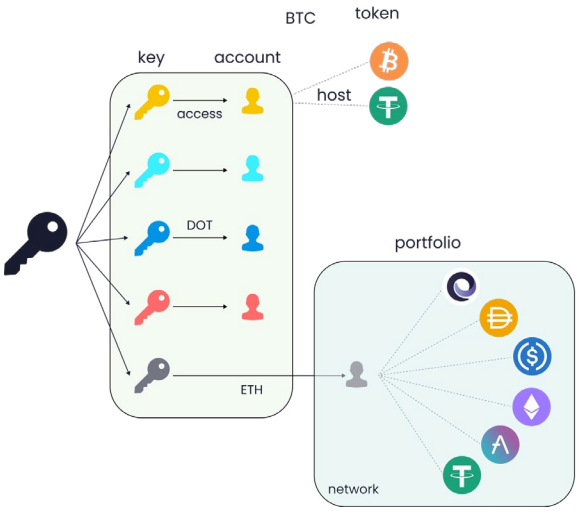


1. 多方计算（MPC）

多方计算（MPC）[9]钱包（如 Coinbase 应用、ZenGo）用你的设备与一个或多个其他设备共享的「秘密」取代传统的私钥。基于该特性还有更多衍生功能，如更轻松的账户恢复。



因此，MPC 钱包账户类似一个带有隐形私钥的 EOA 账户。此外，它还支持阈值设置，如 ⅔ 阈值设置，即每笔交易至少需要三方中的两方共同生成签名才可生效。



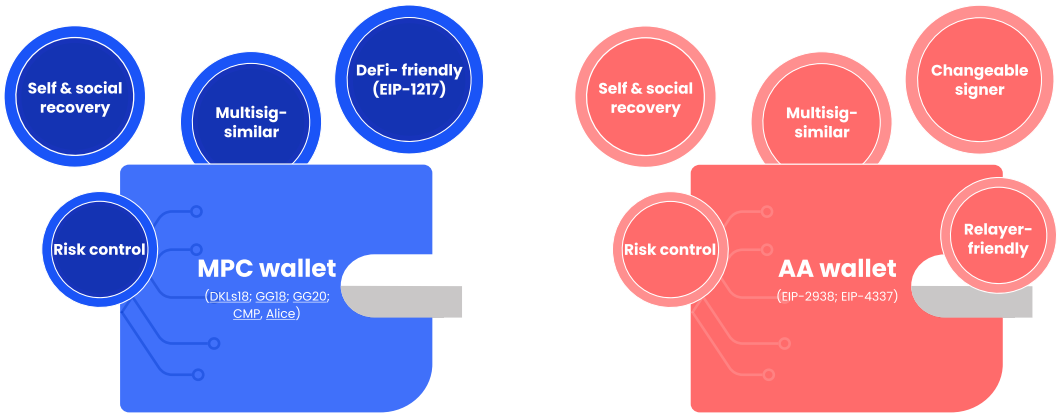
imToken Labs 负责人 Chang-Wu Chen：“MPC 钱包像带有隐形私钥的 EOA 账户。因此它可以原生支持多链，如 BTC 和其他任意公链，只要对应公链的签名算法支持 MPC。唯一的限制是，MPC 技术需要一个在线计算单元来协同执行。”

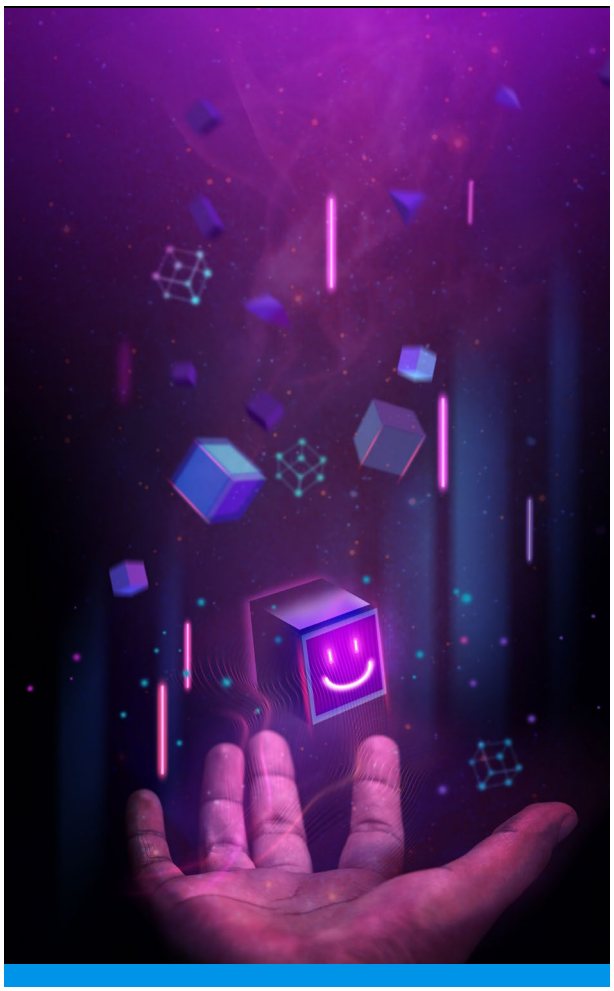
2. 抽象账户（AA）

以太坊上的账户类型有两种：EOA 账户和合约账户。抽象账户 是合约账户的一种，相较于 MPC，具有合约设计灵活、便于自定义逻辑和始终在线的优势。抽象账户钱包（AA 钱包）会在入口点（EntryPoint）的合约先进行交易验证，通过验证后则进入到执行交易阶段。而在当前的以太坊上，交易只能通过 ECDSA 签名验证，并检查余额和随机数，然后执行转账或调用函数。

抽象账户支持自定义规则，所以在签名算法的选择上，除了 ECDSA，我们还可以选择其他签名算法，如 BLS、EdDSA，以更好满足特定应用场景下的需求。此外，我们还可以根据自己的喜好设置每日提款限额或其他规则。

imToken Labs 负责人 Chang-Wu Chen 表示对他而言：“最重要和有趣的是，通过 AA 我们可以将账户与授权分离。由此，我们可以有一个与账户分开的签名（授权）者。以前，丢失私钥等同于丢失身份。但现在，AA 钱包可以做到权限和身份分离，而且具备可恢复的特性，这为未来 DID（去中心化身份）的设计带来更好的基础。这是非常值得期待的。”





3. 底层账户创新

除上述 MPC 和 AA 技术方案，还有一些项目方提出了可以实现类似功能的解决方案。我们采访了其中的三个区块链项目：

Layer2 项目方

Matter Labs (zkSync)

StarkWare (StarkNet)

公链项目

NEAR

NEAR

NEAR 团队于 2020 年启动了其主网[11]。NEAR 区块链的账户模型不同于以太坊，其上所有账户都是可由多个密钥对管理的合约[12]。

这使 NEAR 区块链天然具备一些特性。NEAR 用户可以为每个密钥设置不同的权限、添加和删除设备、支持社交恢复等以太坊社区正在努力添加到以太坊主网上的功能。

NEAR 联合创始人 Illia Polosukhin 表示，账户模型的“安全确实至关重要”，到目前为止，估计有 “50 万至 100 万个账户” 使用了多个密钥。

关于和以太坊的竞争，Illia 提到 “（以太坊的）模型非常不同，现在改变难度很大，因为这将涉及 EVM 改造和许多其他方面的调整来适配。”

NEARWEEK 的 Denys Kovalenko 补充说：“越来越多公链将会意识到 NEAR 一开始便采用的账户系统是一个重要特性，它是未来 Web3 被大规模采用的关键，我们将看到更多 Web2 世界中的概念出现在区块链上，例如域名、基于域名的邮箱地址等。”

Matter Labs 和 StarkWare

和 NEAR 一样，StarkWare 和 Matter Labs 同样致力于为用户带来便捷、安全和灵活的体验。

不同之处在于，Layer2 项目在底层创新方面，由于要兼顾现有的 EVM 范式，确实存在更大的挑战。对此，我们采访了 Matter Labs（zkSync 的开发团队）和 StarkWare（StarkNet 的开发团队）。

StarkNet 和 zkSync都在各自的 Layer2 区块链上原生集成了 AA 特性，使用户账户均以可发起交易的智能合约形式存在。

StarkWare 的产品主管 Tom Brand 将达成 “Web2 用户体验” 作为目标，并提到 Visa（金融服务公司）如何在 StarkWare 的网络上构建产品[13]。其支付原型设计表明 AA 技术可帮助用户在现有 Visa 账户和 StarkNet 自托管账户之间定期付款的体验中感受到和传统支付相同的便捷。

Matter Labs 企业业务发展主管 Omar Azhar 同样赞成 “许多公司有兴趣了解如何在其应用中为自托管钱包提供无缝的 Web2 体验”的观点，并补充说，“能够使用邮箱登录，同时借助支付工具和 AA 技术来实现批量交易” 将有助于在用户和应用之间建立信任 —— 这是加密产品的重要基础。另一方面，“借助 AA 技术，我们可以把 ‘自定义业务’ 逻辑直接内置到智能合约钱包中”，例如嵌入式身份和 KYC。

Tom Brand 补充说：“AA 将有助于提高用户账户的安全性”。Azhar 也提到了“借助 AA，我们可以创建高度自定义的钱包类型——如支票账户钱包、退休账户”。

参考文献

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. 要深入了解 MPC，请参阅： DKLs18; GG18; GG20; CMP, Alice
10. 要深入了解 AA，请参阅： 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

结语

2022 年，加密钱包行业整体稳步发展：

- 越来越多区块链项目方和传统公司加入钱包赛道，并以不同方式促进了区块链的普及。
- 智能合约钱包仍然小众，但在快速增长。

对加密用户的问卷调研显示：

38% 的受访者认为钱包不如交易所安全

65% 的受访者表示了解智能合约钱包概念

51% 的受访者愿意以「支持多因素身份验证提高安全性」为由选择新钱包

76% 的受访者认为第三方托管方案比钱包更方便

以上统计数据表明，自托管钱包发展任重道远，仍有很多痛点亟待解决。

痛点

安全：如何在自托管的基础上进一步提供安全保障

解决方案

- 风险控制：每日交易金额限制；时间限制
- 停止访问：紧急账户冻结；多因素身份验证；白名单
- 重新获得访问权限：多重签名授权；自我恢复、社交恢复；密钥轮换

痛点

便捷：如何提升自托管钱包的使用体验

解决方案

- 隐形钱包：捆绑交易和会话密钥；代付交易费用；自动和定期付款
- 基于抽象账户，内置「自定义业务逻辑」的智能合约钱包：身份管理；KYC 关联；灵活的钱包设置
- 社交登录或应用程序登录

2023 年，新的解决方案将围绕如何处理密钥继续展开，通过使用不同的技术方案来帮助用户添加、删除、限制或更改账户的密钥，或者为账户本身提供自定义逻辑以解决当前痛点。主要技术路线有：多方计算（MPC）、抽象账户（AA）、底层账户创新。

关于 imToken

imToken 是一款去中心化的数字钱包，用于承载加密数字世界的资产、身份和数据，成立于 2016 年，imToken 已在全球 150 余个国家和地区，累计为超过 1500 万用户提供了安全可信赖的数字资产管理服务。

关于 StarkWare

StarkWare 致力于基于 STARK 的 ZK Rollup 解决方案，为业界提供了安全、无需信任和可拓展的技术方案。

已开发产品：

- StarkEx：基于 Validity Rollup；支持抽象账户
- StarkNet：基于无需许可的去中心化 ZK Rollup；支持抽象账户

关于 Matter Labs

Matter Labs 致力于通过零知识证明技术扩展以太坊，并坚信这是使区块链被大规模采用的最可行方案。其使命是加速区块链金融革命。

其主要产品 zkSync 在 2020 年夏季上线，并仍在快速发展中，同时，该团队还在抽象帐户方面进行了创新。

关于 NEAR

NEAR 协议是类似于以太坊的公共区块链，采用权益证明机制，并通过分片技术实现可拓展性。

该团队专注于面向开发人员和用户友好，创造性地开发了向智能合约开发者自动分摊交易费用等功能，并在 NEAR 区块链的底层账户模型中支持智能合约钱包功能。

imToken

想了解更多信息，请点击以下社交媒体平台。

Linkedin Twitter Youtube Instagram Discord