加密货币钱包产品现状及发展趋势

钱包是加密货币的关键基础设施。每一种加密领域的行为，无论是购买还是出售加密币、长期持有加密币、发送加密币、抵押加密币等等，都以某种方式仰仗钱包进行。

钱包也是 Web3 的门户，就像网络浏览器是 Web2 互联网的门户一样。因为加密钱包如此重要，迄今已有近 4 亿美元资金流向加密钱包业务，其中以 **Ledger***（8,800 万美元）、***Blockchain***（7,000 万美元）、***BRD***（5,400 万美元）*和**Abra***（3,550 万美元）*筹集的资金最多。

为设计出更好的钱包用户体验，目前已有大量的研究和工作投入其中。在这篇文章里，我将对加密币钱包的生态系统进行概述，并着重介绍最近在钱包的用户界面 / 用户体验 *(UI/UX)* 方面的一些改进，包括钱包 SDK、智能合约钱包和元交易 *（meta transactions）*。

加密币钱包的兴起

在比特币的早期，第一批用户是加密朋克，他们熟悉公钥和私钥的概念。因此，起初对加密币进行密钥管理的做法是，在一张纸上写下一个私钥或一个助记短语 *（又称种子短语）*，并好好保管这张纸。比如下面这样：

4136fb984d0a8650c6ddc54698cb9365479a607402120e0b7527b2aa1f5d8903

显然，普通人不会为了给别人寄钱而记住一串随机的字母数字字符，而且随身携带私钥非常危险。**Brainwallet** 项目试图让用户生成他们自己定义的种子短语，然后通过 SHA-256 之类的哈希算法将其转换为一个私钥。Brainwallet 这个名字来自于这样一个事实：种子短语只存储在用户自己的大脑中，而不是记在什么地方。如果用户忘了种子短语或者不幸去世，这份比特币也将永远消失。

用户靠自己选择一个好的种子期短语的能力，以承受失去一笔财富的风险。但是人类在生成无序种子短语方面一直很差劲，他们想出的种子短语往往会形成容易预测的规律。正如在一个 DEFCON 演讲中所展示的那样，黑客们已从拙劣生成的 Brainwallet 中窃取了数百个比特币，而这些比特币如今价值数百万美元。

于是，钱包诞生了。钱包把私钥抽离出来，允许用户通过一个简单的 UI 发送和接收加密币。除了备份钱包，用户无需直接与自己的私钥进行交互。各个钱包的第一版都是基于客户端的，要求用户下载桌面软件。这些桌面钱包要么在本地运行轻量级客户端，要么连接到一个节点，每次钱包打开时都需要几分钟来同步到最新的区块。

加载时间太长，可不是一种很好的用户体验。于是，下一版的钱包大多基于网络或是移动钱包。

所有这些钱包都具有安全存储加密币、发送和接收交易的基本功能。几乎所有这些钱包都是由用户控制的，这意味着钱包提供商只能创建钱包软件，而不能触及用户的资金。钱包提供商不负责存储用户的私钥，他们将这一负担转交到用户身上。

如今，有很多基于客户端、基于网络和移动端的钱包，它们大体上没有什么区别，只有细节上的差异。比如有的钱包允许用户直接在钱包里用法币购买加密币，通过 **Waye** 或 **Simplex** 之类的支付处理方，也有的通过 **Shapeshift** 或 **Changelly** 支持用户进行加密币互换，也有的使用像 **CoinJoin** 这样的比特币混币服务来支持私密交易，还有的支持各种加密币和加密收藏品。

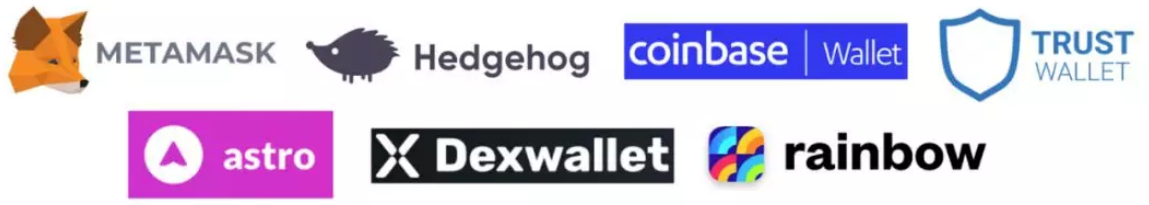
唯一的例外是中国的钱包，他们试图复制微信的玩法，往里面塞进尽可能多的功能，好让用户无需逃离。例如，**imToken** 允许用户从钱包中获得一个原生的 **MakerDAO** 抵押债仓。其他在中国流行的钱包还有**比特派** *(Bitpie)*、**RenrenBit** 和 **Cobo 钱包**。

除了这些软件钱包，还有硬件钱包。硬件钱包提供冷储存，即与互联网在物理上隔离，它们通常存放在银行的保险箱里。如果想要储存大量资金，硬件钱包非常合适，因为黑客若要窃取这笔资金，唯一的方法是物理入侵银行才能拿到这些硬件钱包。

Web3 钱包

如果你只想安全地存储加密币、发送和接收交易以及买卖加密币，那么上面列出的钱包是很好的选择。不过，如果要与 Web3 应用程序交互，它们就不那么有用了。

从用户的角度来看，Web2 和 Web3 应用程序的主要区别在于， Web3 应用程序需要在浏览器中有一个钱包。在进入 Web3 应用时，网站会检查是否有支持 Web3 .js 库的钱包扩展，如果没有，它会告知用户，在使用该 DApp 前应该先去下载一个 **MetaMask**。像 **BRD** 钱包和**Edge** 钱包这样的非 Web3 钱包不支持 Web3 .js 库，因此，从一个非 Web3 钱包中是无法在 **Compound** 或 **Uniswap** 这样的 DApp 上使用 ETH 的。



Me*taMask** *显然是 Web3 钱包的主要玩家。截至 4 月份，预计 MetaMask 有 26.4 万月活跃用户和 9 万个周活跃用户。考虑到几乎每个 DApp 都要求用户在使用网站之前下载 MetaMask 扩展，MetaMask 指标也代表了当前 DApp 可寻址的总体市场规模。在某种程度上，MetaMask 目前扮演着 Web3 看门人的角色，也有极强的「产品市场契合」*（产品和市场达到最佳的契合点）*，尽管它在用户体验上还有很多可改进的空间。当然，Web3 的任务本就是要减少个别中心化的看门人对网络入口的控制，因此有许许多多的团队正在构建 MetaMask 的替代方案。

Hedgehog 是 MetaMask 之外的另一个选择，这个桌面 Web3 钱包由 **Audius** 团队开发。该钱包用一个用户生成的密码给私钥加密，也不强制用户多次确认交易弹出窗口，这样就降低了钱包的复杂性。但这个方案的缺点在于，无法恢复账户，并且主要是为小金额的财务用例而构建的。

Coinbase 钱包和 **Trust 钱包**是两个活跃的移动端 Web3 钱包，而 MetaMask Mobile 和**Astro** 钱包目前都是 Beta 版。一个移动版 Web3 钱包，实际上只是一个添加了普通移动钱包的浏览器，便于用户在各种网站上使用其移动端钱包的资金。移动版的 Web3 钱包也可以通过扫描二维码在电脑上接入，使用 **WalletConnect** 或 **WalletLink** 来将两个设备连接。有些移动版钱包，如 **DexWallet** 和 **Rainbow** 则是定制的，主要服务于去中心化金融 *(DeFi)* 的用例。

更好的用户体验最好是像 MakerDao 和 Auger 这样的 DApp，它们各自提供了专门的移动应用程序，用户可以从 App Store 或 Play Store 下载，这就跟大多数用户是通过手机应用访问 Facebook，而不是在移动端浏览器上访问 facebook.com 一样。为了改善 DApp 在移动设备上的 UI/UX，**Tasit** 正在构建一个开发移动应用的 SDK，服务于各种流行的以太坊DApp。

钱包 SDK

尽管 MetaMask 有先发优势，但在 UI/UX 方面仍有很多容易实现的改进可以吸引主流用户对DApp 的采用。使用 MetaMask 的主要 UX 瓶颈在于，用户需要下载一个单独的浏览器扩展 *（不过最近 MetaMask 发布了一个用于网站集成的新插件）*。追踪用户转化率的 DApp 开发人员告诉我，试图尝试 DApp 的用户中，有超过 90% 的人在被告知需要下载 MetaMask 时会选择放弃。

如果我们想让主流用户试着用一下以太坊，那么，登录到 Web3 应用程序，应该与登录到 Web2 应用程序没有任何差异。

一个 Web3 钱包 SDK，如同 Web2 的用户名和密码登录。用户不需要为了使用这个应用程序而专门下载一个单独的扩展，也不必在每次发送一个交易时点击一个弹出窗口。而且，这个钱包原生地集成到该网站，可以在所有设备和浏览器上得到支持。而缺点则是，这种钱包只适用于为该钱包集成了几行代码的 DApp。

钱包 SDK 提供商存储了被加密的用户密码，该密码映射对应的私钥，在 **Fortmatic** 和**Bitski** 的案例中存储在 HSM 上，在 **Torus** 案例中则被分片。因为钱包 SDK 提供商存储了密码和私钥之间的映射，所以，更新映射就可以重置密码。这一点很重要，因为用户已经在 Web2 应用程序中习惯了重置，他们会认为无论如何都有用于密码恢复的后门。而在传统钱包里，如果用户丢了他们的私钥，那么里面的资金就永远丢失了。

智能合约钱包

以太坊上的智能合约可以为 DeFi 这样的用例提供可编程货币。如果我们可以利用智能合约为可编程钱包添加额外的功能，那就太有想象力了。

首先，我要说说**以太坊账户模型**的一些背景知识。在以太坊中有两种不同类型的账户：从外部拥有的账户和合约账户。传统的以太坊钱包使用从外部拥有的账户，这些账户用私钥实现安全保障，通常为用户转换成 12 个单词的「种子短语」。所以担子压在最终用户肩上，他们得确保不丢失这个短语，万一丢了，账户中的资金也就永远丢失了。

相反，合约账户是只在以太坊区块链上才能存活的代码，不存在可以接触该账户内资金的私钥。利用合约账户，智能合约钱包完全撇开了为用户管理私钥这种概念。而且，智能合约钱包可以被编程为拥有与传统银行相同的安全保障，比如账户恢复、欺诈保护和取款限制。

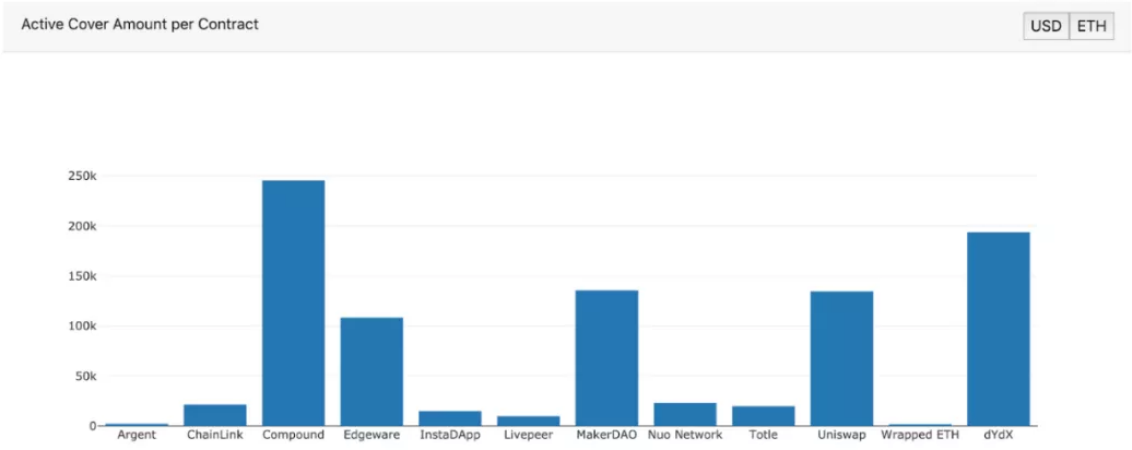
在传统的钱包中，如果用户没有备份他们的种子短语，又弄丢了手机，那么他们所有的资金都将消失。然而，有了智能合约钱包，用户可以指定可靠的家人和朋友作为「备份者」（*在 Argent 中称为守护人*）。如果大多数备份者同意，用户能够触发一个社交恢复过程以取回他们的资金。需要注意的是，备份者永远无法窃取用户的资金；他们的权限是，只有他们能参与完成恢复过程。

为了防止欺诈，**Gnosis Safe** 目前实施了两步验证，大多数人都在使用自己重要的在线账户时都会采用两步验证。**Dapper** 还可以监控异常行为，比如向可疑地址发送大额资金，或者在异常区域活动，以及在交易确认前进行检查。

取款限额是传统银行系统中极为常见的安全特性。有了智能合约钱包，用户可以为任何给定的交易设置最大转账限额。如果触发的交易超过这个数额，交易将暂定一段时间，直到某一指定的时间点。在此期间，用户可以取消这个交易。

虽然相较传统钱包，智能合约钱包可以提供更多的安全功能，但智能合约钱包也有它自身的风险：它不是冷储存，给钱包编程会增加其攻击面的向量。如果是普通的钱包，只要私钥安全，钱包则永远不会被黑，而智能合约钱包则可能因代码有 bug 而被黑。

Nexus Mutual 为智能合约钱包提供保险，以应对钱包被黑或用户丢失资金的意外情况。目前，**Argent** 和 **InstaDapp** 上的保额分别为 2,400 美元和 15,000 美元。



欲知详情，请登陆 NexusTracker.io

元交易

元交易（Meta transactions）是由 **Austin Griffth** 开创的一种新兴设计模式，它极大地降低了 DApp 被大规模采用的门槛。围绕着这一想法，一个充满激情的社区已经形成，牵头的主要是 **MetaCartel**。

元交易是一种无 gas 的交易，它让用户无需安装浏览器扩展或购买加密币，就能即刻使用 DApp。元交易的概念是，用户用自己的私钥给一个交易签名，然后将其传送给一个接收该交易数据的中继器（*replayer*），中继器将其打包到一个实际的以太坊交易中，然后支付 gas 费用以将该交易提交给以太坊区块链。

需要注意的是，元交易不是钱包，所以，用户的私钥存储在何处，取决于实施元交易的钱包如何设计。

元交易的第一版依赖于单个中继器来广播交易，这使得系统非常中心化。理论上，中继器可以审查用户的交易，但由于钱包提供商或 DApp 通常就是中继器，所以在实践中他们审查自己的用户毫无意义。尽管如此，**Zeppelin** 和 **TabooKey** 团队的成员非常机智地解决了这个问题，他们以去中心化的方式中继所有元交易，正在发布 Gas Station 网络。

在 **Gas Station** 网络中，用户从由多个独立中继器组成的网络中随机选择一个，代表自己向区块链提交自己的交易。DApp 向中继器支付报酬，同时后者要提交一笔押金，万一有恶意行为，押金就得被没收。通过这种方式，DApp 承担了中继器和 gas 成本，就当作客户获取成本吧。而用户则可享受无缝的使用体验。基于 DApp 的商业模式，它们可以通过收取订阅费等方式向用户收费。

元交易可以在智能合约钱包中实现。**Argent** 和 **Astro** 钱包使用了元交易，这样用户不用支付 gas 费就可以发送交易。但更重要的是，元交易允许多个交易捆绑到一个交易中。这一点很重要，因为像 Uniswap 这样的 DApp 需要额外的交易来解锁用户想要兑换的每个代币，然后用户才能进行单笔兑换。元交易消除了所有这些不必要的初始步骤，用户可以直接与 DApp 进行交易。

在 ETHDenver 上， ***Burner Wallet*** *发布了，让参加黑客马拉松的人们可以支付餐车费用。**从那以后，在其他活动中出现了很多不同版本的 Burner Wallet。*

另一个在实践中使用元交易来吸引新加密用户试用的好例子是 **Burner Wallet**。它是一个网络钱包，以简单的界面用于小额加密币的快速支付。当你从网络或移动浏览器访问 xdai.io 时，会自动生成一个 Burner Wallet，无需下载任何应用程序或种子短语，私钥存储在浏览器的本地存储中。在 Burner Wallet 之间发送交易，就跟微信支付一样——扫一扫二维码，即可在用户之间交换加密币。

Burner Wallet 类似于现金——你不会随身带大把钞票，因为很容易弄丢，而钞票兑换又很方便。由于用户的私钥存储在他们的浏览器的本地存储中，所以 Burner Wallet 为用户提供了一个很好的试用体验，但这并不是一个永久存储资金的办法。为了解决这个问题，Burner Wallet 与 Gnosis Safe 合作，一旦用户在他们的 Burner Wallet 中积累了足够的款项，就会自动将资金转移到一个更安全的钱包中。将 Gnosis Safe 的安全性和扩展功能与 Burner Wallet 的易访问性相结合，这是以太坊钱包基础设施上的一个重大改进。

钱包事业将走向何方

大多数人认为，加密货币和 DApp 的用户体验，距离主流人群的可用性尚有好几年时间，但在过去的一年里，用户体验其实已经有了很多重大突破，只需要在现有的钱包中实现即可。我相信，只要像元交易这类更出色的用户体验能向 DApp 开发者推广，并得到更广泛的实施，我们将看到 DApp 使用的爆发点到来。

我还注意到，在钱包使用行为中，现有加密货币原生用户和加密货币新手之间存在鸿沟。现有的加密货币原生用户似乎都能很好地使用 MetaMask *（或者至少已经适应了它的 UX 问题）*，没有切换到其他钱包的强烈动机。当然，在以太坊 gas 价格飙升时，他们还是会想利用不支付 gas 费这类功能的。

然而，加密货币新手并不明白， Web3 应用程序需要一个 Web3 钱包，一旦碰到某个网站说它与 Web3 不兼容时，他们就会感觉无路可走。钱包领域中目前完成的几乎所有 UI/UX 工作，其实都是针对后一类用户的。同样，各类钱包项目也确信，是用户体验，而不是缺少杀手级应用，才是 DApp 大规模采用的最大瓶颈。解决了这个瓶颈，就将促成加密货币普及的下一个热潮。

为了解决这种分裂的情形，在我看来，理想的解决方案是提供两种登录选项：一种是使用 MetaMask，为在意自主性的现有加密原生用户服务，另一种是使用一种新的钱包基础设施，它迎合新用户，会在抗审查和隐私等方面做出权衡。

或者还存在这种可能：在未来，像 Chrome 和 Firefox 这样的 Web 浏览器，将有一个预装的钱包供所有用户使用，到那时候，HTTP 402 错误代码就真的能够派上用场了*（译者注：HTTP 402 为将来使用而预留。**原计划此状态码可能用于电子现金或者网上小额交易，但一直未实现）*。在这种情况下，我们将实现神奇的互联网货币的梦想。