钱包是加密货币世界中的重要基础设施。所有与加密货币相关的操作，包括买卖加密货币，持有加密货币，转账，甚至质押跑马圈地，都或多或少与钱包有关。。正如网络浏览器是网络的入口一样，钱包也是网络的入口。因为它的重要性，人们已经在加密货币钱包行业投资了大约4亿美元。其中，莱杰(8800万美元)、区块链(7000万美元)、BRD(5400万美元)和凯西(3550万美元)筹集的资金最多。目前为

大量的人力物力都集中在设计更好的钱包用户体验上。本文将向读者简要介绍加密货币钱包的生态系统，重点介绍钱包用户界面或用户体验的最新进展。这些进步包括：钱包SDK、智能合约钱包和元交易。

在比特币发展的早期，最早的用户是熟悉公钥和私钥密码学的cryptopunk。因此一开始，人们管理资金的方式(也称为&quot私钥管理&quot)写下私钥和助记词(也称为&quot种子短语&quot)放在一张纸上，妥善保管。换句话说私钥是资金的所有权和使用权)。

4136FB984d0a8650c6DDC54698CB9365479a607402120e0b7527B2a1f5d8903女巫崩练馈羞开对溪路再冰留(译者&#039；s注意：这里是私钥和助记符的例子。。私钥是随机字符串，助记符与私钥一一对应。所以掌握了助记符就等于掌握了私钥。显然，大多数人不会&#039；我不想为了转账而记住这一串又长又臭的随机字母和数字。另一个担心是随身携带私钥的风险太高。于是有人提出了&quot大脑钱包&quot:用户可以选择一组容易记忆的助记符。，然后使用某种哈希函数(如SHA-256)将这组单词转换成私钥。大脑钱包这个名字也表明了——允许用户写下助记符而不是写出来的想法。如果用户忘记了助记符，或者用户死亡。然后ta&#039s比特币一去不复返了。

此外，大脑钱包模式还意味着用户&#039；他的财产安全依赖于他自己破坏助记短语的能力(译者&#039；s注：如果用户选择的助记词不够乱，这些助记词会被猜到。，从而揭示用户&#039；的私钥)。而人类并不善于选择足够混乱的助记短语，所以他们选择的助记词往往是可预测的。正如这次黑客大会所显示的，黑客可以从选择不当的大脑钱包中窃取数百个比特币。

。这些大脑钱包现在价值数百万美元。

然后就出现了我们现在常说的钱包(软件)。有了钱包软件，用户不再需要直接触摸私钥，而是可以通过简单的用户界面进行转账和接受加密货币；备份钱包的时候记下私钥就好了，保管好。软件只是帮你使用私钥，那个私钥才是资金的真正归属)。最早的钱包是基于客户端的，用户必须下载电脑软件才能使用。桌面钱包要么在本地运行轻型客户端，要么连接到另一个节点。。每次打开钱包，都要花几分钟同步到最新区块。

对于用户来说，花很长时间下载的体验显然不好，所以下一代钱包会发展成web钱包和手机钱包。

所有这些钱包都具有安全保管加密货币和收发交易的基本功能。大多数钱包是用户控制的钱包，这意味着这些钱包的供应商只提供软件来帮助用户使用私钥，但他们无权访问用户&#039；私钥。所以没有挪用用户的能力&#039；资金。这样钱包供应商就把留住用户的责任还回来了&#039；用户自己的私钥。

现在有很多基于客户端的钱包，web钱包，移动钱包。两者差别不大(在保管资金和收发交易方面)。这些钱包的差异化体现在：——中的部分钱包通过Wyre或Simplex等支付服务商帮助用户直接用法币购买加密货币；部分钱包支持Shapeshift或Changelly等货币兑换服务；一些钱包也使用混合货币服务(如Bitocin上的CoinJoin)来保护用户&#039；隐私。。支持更多种类的加密货币，甚至在线收藏，也是差异化的一部分。

但是中国的钱包软件往往选择了另一条路。这些钱包模仿微信支付，希望用户尽可能停留在自己的软件中，不要使用其他钱包软件，所以也包含了尽可能多的功能。例如，imToken允许用户关闭钱包中MakerDAO(以太网工作坊上的一个应用)中的抵押债务仓库。国内其他比较受欢迎的钱包还有Bitpie，RenrenBit，Cobo钱包。

(译者&#039；注：MakerDAO是一个运行在以太坊区块链上的系统，用户可以通过抵押资产贷出与美元软锚定的稳定货币DAI。)

除了上述所说的软件钱包之外还有硬件钱包。硬件钱包侧重于冷藏，这意味着它们与互联网隔离，可以放在银行&#039；安全了。五金钱包适合存放大额存款。黑客想偷这笔钱，只能先偷实体的硬件钱包。

(译者&#039；s注：冷存储是指正常情况下不联网的设备。)

如果你只关注钱包保管、收发交易和买卖加密货币的安全性，那么以上钱包对你来说足够了。但是如果你仍然想使用Web3应用程序，这些钱包在易用性方面有很大不同。

来自用户&#039；的观点来看，Web2和Web3应用程序之间的主要区别是使用Web3应用程序需要用户在浏览器中安装钱包，而Web2则不需要。进入Web3应用后，网站会检查用户是否支持web3.js库的wallet扩展。如果发现它不受支持，用户将

被告知在使用dApp之前下载Metamask(一种浏览器插件钱包)。。BRD钱包和Edge钱包等非Web3钱包不会&#039；不支持web3.js库，所以即使你钱包里有ETH，，你可以&#039；不要使用dApp(如复合或Uniswap)。

(译者&#039；注：Compound是以太坊上的一个借贷市场，用户可以在这里存入资金并赚取利息。也可以借代币；你需要；Uniswap是以太坊上的分散式交换，可用于令牌的交换)

Metamask是Web3中最著名的钱包。截至4月，Metamask估计有264，000名月活跃用户和90，000名周活跃用户。。考虑到大部分dApp需要用户下载Metamask插件才能使用该功能，Metamask的指标也代表了目前dApp所能触及的所有市场。可以说Metamask是Web3的看门人。其产品的市场适应能力可能也是最强的，虽然在用户体验上还有很多不足。但Web3本身的愿景是削弱网络上的集中式看门人的控制，因此我们可以看到许多团队正在构建更好的替代方案。

Hedgehog是Audius团队开发的一款桌面Web3钱包，用来替代Metamask。此钱包支持用户使用自定义密码加密和保存私钥。并且用户不会被迫手动确认交易信息，从而隐藏钱包的复杂性。这种方案的缺点是没有账户回收功能，主要针对涉及金额较小的用例。

币基钱包和信托钱包是已经推出的两种手机Web3钱包，而MetamaskMobile和Astro钱包还在测试阶段。直言不讳移动Web3钱包是一个浏览器加上一个普通的移动钱包，允许用户在访问网站时使用自己的资金。使用WalletConnect或WalletLink，您还可以在电脑上操作mobileWeb3钱包。只需扫描二维码，将两个设备关联起来。像DexWallet和Rainbow这样的钱包是专门为DeFi用户定制的。

更好的用户体验是每个dApp(如MakerDAO和Augur)都有专门的手机App，用户可以直接从AppStore或PlayStore下载。。它&#039；就好像大多数用户通过脸书应用程序在他们的移动设备上使用脸书，而不是使用移动浏览器来访问facebook.com。为了改善移动设备上dApps的用户体验Tasit正在为各种流行的以太坊dApps开发移动应用SDK。

(译者&#039；s注：Augur是以太坊上的一个预测市场平台，用户可以在这里预测未来事件或者参与预测。。

metamask虽然长期以来备受关注，但在用户界面和用户体验上仍有很大的提升空间，可以有针对性地推动dApp的普及。。使用Metamask的用户体验主要瓶颈是3354用户要单独下载浏览器插件(虽然Metamask最近发布了新的网站整合插件)。在

与专门跟踪用户转化的dApp开发者交谈后，我们知道——中超过90%的dApp用户在发现需要下载Metamask才能使用dApp时会放弃。

如果我们真的想让主流用户使用以太坊，那么登录Web3应用程序和登录Web2应用程序应该没有区别。

Web3walletSDK类似于Web2用户名和密码登录。用户不&#039；使用该应用程序时，不需要下载额外的插件，它们不会&#039；他们不需要每次发送交易时都点击弹出窗口。而且钱包和网站是一体的。，所有设备和浏览器都可用。缺点是——只能在集成了相关钱包代码的dApp上正常使用这种钱包。

钱包SDK的供应商将存储加密的用户密码。该密码与私钥匹配。——比如Fortmatic和Bitski这两个SDK会选择将私钥存储在HSM(硬件安全模块)上，而Torus会将其切片，单独存储。。因为密码和私钥之间的映射存储在walletSDK上，所以更新映射可以重置密码。这对于徘徊在Web2应用周围的用户来说非常重要，因为他们的假设是——总有办法找回密码。但是如果用户丢失了其传统钱包的私钥，则私钥对应的资金将永远找不回来。以太坊上的智能合约可以为DeFi提供可编程货币。那我们能不能智能承包给程序钱包，提供额外的功能？

首先介绍一些以太坊账户模型的背景知识。在以太坊上，有两种不同类型的账户：外部所有者账户(EOA)和合约账户。传统的以太坊钱包使用所有外部账户。资金的安全性完全取决于私钥(通常转换成一个十二字&quot助记符&quot对于用户)。最终用户的责任是保管好这些助记符。如果失去了他们，账户里的资金就会石沉大海。与之相对的

合约账户是永久保存在以太坊区块链的代码。这些帐户没有私钥，所以它们不&#039；使用合同账户中的资金不需要私钥。

因此，智能合约钱包摒弃了完全让用户管理私钥的方法。甚至于智能合约钱包可以写入与传统银行相同的安全保障，如账户恢复、欺诈保护和取款限额。

在传统的钱包中如果用户没有&#039；不备份他的记忆法，丢了手机，钱就没了。然而，使用智能合约钱包，用户可以将他们信任的家人或朋友指定为&quot备份&quot(名为&quot卫报&quot银色)。。如果大多数备份同意，用户可以启动社会恢复计划。应该注意的是，备份永远不会偷走用户&#039；资金，他们只有特殊的许可来完成帐户恢复程序。

为了防止欺诈GnosisSafe也使用2FA(双因素认证)。这是最重要的在线账户服务将会做的。Dapper还可以监控异常行为，例如帐户是否在异常区域启动。是否有大笔资金被转移到可疑账户；此外，在确认交易之前，将检查异常情况。

在传统的银行系统中，取款金额是一个极其常见的安全功能。使用智能合约，用户可以为所有交易设置最大交易限额。。如果发起的交易超过最大金额，交易将被暂停，直到经过预定的时间段(交易可以继续发送)。在此期间，用户可以随时取消交易。

虽然智能合约钱包可以提供比传统钱包更多的安全功能。但智能合约钱包的风险在于，它不是冷库；另外，编程钱包会增加被攻击的区域数量。智能合约不像普通钱包。它可以&#039；通过保护私钥，不能保证钱包永远不会被黑。只要代码有漏洞就可能被黑。。NexusMutual提供智能合约钱包保险，当钱包被黑客攻击，用户损失金钱时，将向用户赔付。目前Argent和InstaDapp的保险费分别为24000美元和15000美元。

元交易是AustinGriffth提出的一种新模型，可以大大降低人们使用dApp的障碍。现在围绕这个概念形成了一个社区，这在很大程度上归功于开创性的工作MetaCartel。。

元交易是不需要用户支付燃气费用的交易。用户不需要安装浏览器插件，也不需要购买加密货币，使用元交易就可以直接使用dApp。元事务的概念是3354用户首先用私钥对事务进行签名。，然后将交易数据传递给中继，中继会将数据打包成以太坊交易，然后付Gas发送到网络。需要再次提醒大家的是，——元交易不是钱包，所以用户如何存储私钥取决于你用来执行元交易的钱包。

元事务最早的实现是只通过一个中继来广播事务，非常集中。理论上，这个中继可以审查用户&#039；交易；但实际上，因为钱包和dApp本身经常充当继电器，所以审查自己是没有意义的。然而，齐柏林飞艇和泰布克的成员们。的团队巧妙地通过分散化解决了这个问题，并正在努力开发加油站网络。

在加油站网络上，用户从由独立中继组成的网络中随机选择中继代表自己提交交易。接力赛由dApps支付。如果接力者有不良企图，其预存的保证金将被没收。。这样dApp承担了直放站和燃气的成本(也就是TA的获客成本)，可以为用户提供一站式的体验。DApp未来可以根据自己的商业模式，通过其他渠道收取用户费用(如订阅费)。

元交易也可以在智能合约钱包中执行。Argent和Astro使用元交易，因此用户可以

发送交易而无需支付汽油。但更重要的是，元事务支持将多个事务绑定到一个事务中。这很重要。因为像Uniswap这样的dApp，用户需要使用额外的交易来解锁所有想要兑换的令牌的相关权限，然后用户才能兑换令牌。元事务消除了所有这些不必要的准备步骤。

，让用户可以直接和dApp进行交易。

由ETHDener推出的BurnerWallet支持黑客马拉松的参与者为小吃摊付款。此后，又出现了多次布瑞纳钱包的类似事件——[XY002]。另一个利用元交易引导新用户的著名例子是burnerwallet。它的用户体验非常简单，就是一个可以快速发送小额款项的web钱包。。当用户通过手机或电脑浏览器访问xdai.io时，会自动生成一个一次性钱包，无需下载任何软件，也无需记忆任何助记符。私钥将存储在用户的本地存储器中&#039；的浏览器。。burner钱包之间发送交易类似于用微信支付，扫描二维码就可以互相交易。

一次性钱包就像现金。你不&#039；Idon’我不想带太多东西，要么是怕被小偷记住，要么是因为你太粗心。但是现金的流动性真的很强。因为用户&#039；的私钥存储在浏览器中&#039；的本地存储空间，BurnerWallet为用户提供了良好的开机体验，虽然不适合长时间保存资金。来解决这个问题。BurnerWallet和Gnosis Safe协同工作，在用户存够一定金额后，自动将钱转移到更安全的钱包。具有知识安全的安全性和广泛的功能。再加上Burner钱包极强的适用性，两者强强联手，大大提升了以太坊钱包的水平。

很多人认为加密货币和dApp的用户体验一时半会儿还成不了气候，但是近几年来，，它在用户体验上实现了很多很大的突破，但是现在需要嫁接到这些钱包上。我相信，一旦像元交易这样的用户体验被dApp开发者更好地理解并广泛实现，dApp的爆发就会到来。

我也注意到加密货币的新老用户是有区别的。老用户似乎对Metamask普遍满意(至少已经适应了他们的用户体验问题)，也没有换钱包的动力。除非新功能真的能带来什么立竿见影的好处，比如以太坊气价暴涨的时候不用交气费。

相反，新用户不会&#039；我不太明白&quotWeb3的应用需要Web3&quot。一旦助教发现他们可以&#039；不要用没有钱包的网站，他们会扭头就走。钱包领域几乎所有正在开发的UI/UX改进都是为了满足新用户的需求。所以钱包项目也是一场赌博。用户体验差(而不是缺少杀手级软件)是dApps被广泛使用的最大瓶颈。这个问题一旦解决，下一波加密货币普及指日可待。

为了弥合新老用户之间的鸿沟。我认为理想的解决方案是——提供两种登录方式。

一是利用Matamask照顾成熟用户对自主性的需求，二是用新钱包俘获新用户(但代价是审查和隐私)。或者也许在将来现在这些网络浏览器，比如Chrome和Firefox，都会在浏览器中为所有用户推出预装钱包。这时候，你就可以真正使用HTTP402错误代码(translator&#039s注：HTTP在设计时特意留了一个支付请求的错误码，是402。但HTTP问世后，没有可以嵌入浏览器的支付服务。，所以这个代码从来没用过)。到那一天，我们将实现互联网货币的神奇梦想。

以上是区块链科普的详细介绍：加密货币钱包全景概览。更多关于加密货币钱包的全景概览，请关注www.dadaqq.coMDadaqq.Com的其他相关文章！

本站提醒投资有风险，入市需谨慎。此内容不作为投资理财建议。