外部所有帐户（EOAs）——由私钥控制

产品名称	外部所有帐户（EOAs）——由私钥控制
公司名称	东莞市数云网络科技有限公司
价格	.00/件
规格参数	
公司地址	东莞市
联系电话	18665158422 18665158422

产品详情

自我托管一直被誉为管理加密资产的实践。*近的FTX和Celsius事件再一次提醒业内人士“ notyourkeys,notyourcoin ”，人们纷纷转向非托管钱包，而类似这样的事件过去发生了很多很多。在FTX事件曝光后，Safe获得了8亿美元以上的净流入，Ledger在短时间内连续创下多个销售额历史新高，Trezor销售额飙升300%，ZenGo在一夜之间实现了三位数增长，存款达到了历史水平，所有这些都发生在同一周内。 然而，大量用户仍然甘冒托管风险，以换取低成本和易用性。Memes和很多痛苦的教训只能让我们把自我托管当成默认选项，在非托管钱包基础设施成为阻力的资产保护和管理的方式之前，我们还有很长的路要走。 幸运的是，现在蓬勃发展的钱包生态系统，为个人、DAO和机构提供了更多的选择。加密货币不再只关注安全存储，还关心在新经济中的资产使用。随着攻击面和漏洞的增加，钱包功能也越来越丰富，不仅要能抵御攻击，同时还要支持日常业务和个人使用。 与所有的设计决策一样，这是一个经多方权衡后的化过程，考虑了特定用例和钱包解决方案及密钥管理实践能力等各维度，切实平衡其目标用户的各种需求：
个人用户希望获得无缝顺畅的用户体验、低成本以及能够与dapp灵活交互。
DAO想要财库管理透明，能够参与生态系统治理。
*机构希望将无关性、可审计性和机构级安全性等责任外包。 有两类密钥管理解决方案取得了很大进展：智能合约钱包（包括多重签名钱包）和多方计算（MPC）协议。
（上图显示的三类钱包分别为：传统钱包、智能合约钱包、MPC钱包） 本文内容包括：
钱包需要考虑的属性。 传统、MPC和智能合约钱包概述。
钱包生态系统面临的持续挑战。
总结当前钱包解决方案的优缺点，展望钱包基础设施前景。 钱包需要考虑的属性 安全。针对从简单攻击到复杂攻击的相应保护程度。在今天，“ 良好的密钥管理 ”往往意味着选择由多个解决方案构成的组合方案，其启用和运营成本与上活动性质和相关资产金额相一致。
成本。创建帐户、管理访问和执行交易的成本有多高。
用户体验和灵活性。访问控制管理、开销策略、限制和权限的粒度。
可恢复性。在受攻击或发生故障的情况下，有能力回收资产恢复访问权。
可扩展性。可为核心产品带来新功能和集成的产品和服务生态系统。
隐私。地址与个人相关联的难易程度，以及钱包在多大程度上揭示了组织的操作程序。
传统（HD）钱包 传统钱包使用助记词和分层确定性（HD）结构来派生私钥、对应公钥和上地址。这些钱包允许用户生成用于签署交易的私钥，并使用助记词恢复所有密钥。 到目前为止，传统钱包一直是用户选择自我托管资产及与区块应用程序交互的主要入口。像MetaMask这样的浏览器扩展和

Rainbow这样的移动应用程序已经为该生态系统吸引了数百万用户。存在更大利益风险的用户可以选择Ledger和Trezor等硬件钱包，它们能提供更高安全性，因为硬件钱包可以离线保护私钥。 虽然业界已经共同做出了巨大努力来教育用户确保助记词和密钥安全的重要性，但这类单点故障仍然是阻碍广泛采用的一个重要因素。如果私钥丢失，除了失去所有资产外，用户还必须手动跟踪多个地址和代授权，还要为gas提供新地址，牺牲隐私。 应用层的创新速度意味着，今天，不可撤销的字符串不仅可以让一个人的毕生积蓄获得全部访问权，而且与促进他们线上身份认证的上历史联系越来越紧密。获得私钥访问权的动机太大了，以至于从业余到资助的全部投入无尽的资源，进行花样百出的攻击。所以，现在单纯依靠用户的安全操作已经不够了——我们需要完全消除这类单点故障。 多方计算（MPC）钱包和智能合约钱包能帮助我们实现这个目标，并且已经出现了一个由这两类产品和服务组成的生态系统，已被机构、加密原生个人用户和DAO等采用。虽然这两种类型的钱包都消除了单点故障，但它们存在一些基本的技术差异，导致不同的利弊权衡。下面我们来对两者进行概述。 MPC钱包 广义上讲，多方计算（MPC）使一组互不信任的各方能够联合计算输入函数，同时保护这些输入的隐私。在学中，这对于保管用于解密数据或生成数字签名的私钥特别有用。 MPC钱包通过使用门限签名方案（TSS）消除了单点故障。在这个范式下，我们创建并分发私钥分片，这样就没有哪个人或机器能够完全控制私钥——这个过程被称为分布式密钥生成（DKG）。然后，我们可以通过在不暴露各方密钥分片的情况下合并密钥分片，从而共同生成公钥。 想要对消息和交易进行签名，各方要将其密钥分片连同公共输入（要签名的消息）一起输入，生成数字签名。此后，任何知道公钥的人（即验证者节点）都应能够验证签名。由于各密钥是组合在一起的，并且签名是在下生成的，因此从MPC钱包生成的交易与传统的私钥钱包的交易没有什么区别。 这为MPC钱包用户提供了一定程度的隐私保障。对于那些希望将其签名方案和签名者活动置于公众视线之外的组织来说，这个功能是开箱即用的，因为一系列过程是在下进行的。这样，组织可以保留关于参与签名者的内部日志，而不会对开。 私钥轮换是另一种MPC协议，它输入各密钥分片，然后输出一组新的密钥分片。旧的密钥分片可以被删除并替换为新的密钥分片，新的密钥分片可以以相同的方式使用，而无需更改相应的公钥和地址。

MPC钱包的优点

无单点故障。一个完整的私钥在任何时候都不会集中在一台设备上。也没有助记词。 可调整的签名方案。授权的法定人数可以随着个人和组织需求的变化而变化，同时不改变地址。组织可以动态调整签名方案，而不必每次都通知交易对手一个新的地址。 细粒度访问控制。机构用户可以为一个策略分配无限数量的交易审批者，并委派能够准确反映组织角色和安全措施（时间锁、MFA多因素验证、欺诈监控）的权限。个人可以通过MPC钱包即服务（wallet-as-a-service）选择半托管方式，由第三方持有其中部分密钥分片。 更低的交易成本和密钥恢复成本。MPC钱包在区块上表示为单个地址，其gas费与常规私钥地址相同。这对于每天进行数百笔交易的用户（例如在B2C用例中）来说非常重要。丢失的密钥分片也可以在下恢复。 区块无关性。密钥生成和签名依赖于下纯学。与新的区块兼容很容易，因为钱包只需要能够使用该可识别的算法生成签名就可以了。 MPC钱包的缺点 下问责制。签名授权策略和授权法定人数是在下管理的，因此这些自定义规则仍然容易出现中心化故障。密钥分片仍然是加密秘密，应该拥有与完整私钥相同的处理方式。下规则和签名阻碍了透明度，需要更严格的运营审计。 与多数用户采用的大多数传统钱包不兼容（没有助记词，没有完整的私钥存储在单个设备上）。MPC算法并没有标准化，也没有得到机构级安全设备（如iPhoneSEP和HSMs）的原生支持。 大多是单独定制产品。许多MPC库和解决方案都不是开源的，因此，如果出现问题，生态系统很难对它们进行独立审计和集成，很难进行事故分析。

如今，基于MPC的解决方案主要面向基金、家庭办公室、和托管人等机构客户。Fireblocks和Qredo等MPC技术提供商使客户能够为不同类型的交易定义自己的工作流程，并且能够让他们保持合规和安全。然而，散户投资者仍然依赖独立研究和私人密钥钱包。Web3Auth*近发布了一个MPCSDK，允许任何钱包或dapp借此成为用户的 ” web3原生多因素验证 ”，让用户可以使用自己的iCloud或电子邮件进行备份。去中心化托管协议（如Entropy）正在为消费者和DAO开发开源工具，以在线存储资产，并通过MPC设计交易的安全预防措施。 MPC的持续显著发展：可编程密钥对 Lit是一个去中心化协议，它将密钥分片存储在Lit网络节点上。在这里，公钥/私钥对由PKP（可编程密钥对）NFT表示，其所有者是密钥对的控制者。然后，PKP所有者可以触发网络聚合秘钥分片，以解密文件或在满足任意定义的条件时代表密钥分片签名消息。 这对去中心化访问控制、资产管理和上自动化交互具有深远意义。通过向LitAction（部署到IPFS的不可变代码）授予签名特权，PKP可以用作MPC或去中心化云钱包，使用任何可用jascript表示的认证方法。 铸造一个PKPNFT是基于MPC的分布式密钥生成过程，它使NFT所有者成为PKP的root所有者。因此，转让这个NFT相当于交易私钥，这实际上打破了“ 灵魂绑定 ”代（

S）的概念，因为S是与特定的所有者绑定在一起的。现在，钱包自身可以安全地进行交易（因此，“ 钱
包绑定代 ”在这里可能对不可转让的NFT来说是个更合适的名字）。　智能合约钱包
以太坊目前有两种账户类型：　外部所有帐户（EOAs）——由私钥控制外部所有帐户（EOAs）—
—由私钥控制外部所有帐户（EOAs）——由私钥控制外部所有帐户（EOAs）——由私钥控制外部所有
帐户（EOAs）——由私钥控制外部所有帐户（EOAs）——由私钥控制外部所有帐户（EOAs）——由私
钥控制外部所有帐户（EOAs）——由私钥控制外部所有帐户（EOAs）——由私钥控制外部所有帐户（E
OAs）——由私钥控制外部所有帐户（EOAs）——由私钥控制外部所有帐户（EOAs）——由私钥控制外
部所有帐户（EOAs）——由私钥控制外部所有帐户（EOAs）——由私钥控制外部所有帐户（EOAs）—
—由私钥控制外部所有帐户（EOAs）——由私钥控制外部所有帐户（EOAs）——由私钥控制外部所有
帐户（EOAs）——由私钥控制外部所有帐户（EOAs）——由私钥控制外部所有帐户（EOAs）——由私
钥控制外部所有帐户（EOAs）——由私钥控制外部所有帐户（EOAs）——由私钥控制　与不可升
级的合约不兼容。尽管EIP-1271允许应用程序代表合约钱包进行签名，但仍然没有得到普遍支持，并且
不能整合到不可升级的合约中。　智能合约钱包的持续显著发展：帐户抽象　智能钱包在整个
生态系统完全摆脱EOA和私钥的努力中发挥着必不可少的作用，也就是帐户抽象。在这种范式下，所有
账户都是智能合约，它们有自己的逻辑来规定什么是有效的交易，允许用户根据自己的特定需求自定义
账户。　自2016年以来大家一直在讨论帐户抽象这一话题，但生态系统在解决方案上的协调进度一
直很慢。L2已经极大加快了账户抽象意识及其采用，例如Starkware的所有Starknet账户已成为原生智能钱
包，即将发布的zkSync2.0也将是账户抽象的。
在以太坊上，已存在多个EIP致力于完成账户抽象路线图上的一个个里程碑。　ERC-4337将签名验
证、gas支付和重放保护从核心协议移出到EVM，使用户能够使用包含任意验证逻辑的智能钱包，将其作
为主要账户而非EOA，同时不需要任何的共识层更改。这个EIP引入了一个UserOperations内存池，与现
有的内存池并行存在。捆绑器（验证器、MEV搜索器或应用程序本身）从UserOperations池获取交易，将
它们转发给区块并支付。Paymasters是代付交易的可选步骤。在这里，启动钱包本身不支付gas费，但应用
程序可以通过收费订阅模式为用户聚合和代付gas费。
EIP-3074允许EOA将控制权委托给合约，让现有的EOA发送由第三方支付的交易任务。
EIP-5003将现有的EOA升级为合约，并允许从ECDSA迁移到更或抗签名方案。
钱包生态系统发展面临的持续挑战　技术漏洞　ParityMultisig攻击和*近的RabbySwap漏洞表明
，如果在实现中存在缺陷，那么即使是的资金存储概念和方法也没有什么意义。使用开源软件和生态系
统方法添加功能，漏洞将比黑盒代码更容易被发现，可以更快得到解决。我们可以预见，智能合约账户
标准将会出现，比如OpenZeppelin对ERC-20和ERC-721的实现，随着生态系统的成熟，林迪效应发展壮大
，开发者可以更有信心地进行开发构建。　社交攻击　任何一个技术解决方案的优点都不能消
除社交层的风险。6亿美元的RoninBridge漏洞并不是由于技术缺陷，而是针对SkyMis员工的社会工程攻击
，让攻击者能够访问验证者密钥。除了对使用哪个钱包来管理资产做出负责任的决定之外，组织还需要
确保这个关键系统的每个组件在社交层和技术层都是真正独立的。　*安全和迁移成本　从一
个帐户迁移到另一个帐户既不有趣也不便宜。尽管目前市场上有强大的钱包替代方案，但用户迁移现有
的EOA成本很高：交易、平仓/持仓DeFi头寸、税收影响、用户错误、时间和精力等等。
操作安全　自我托管对今天的大多数用户来说都是一个可怕的前景，因为提高个人的操作安全需要
有意识的努力和付出，可能是一项艰巨的任务。大多数交易数据对于人类来说是不可读的（尽管这一点
正在改变），一旦发生错误就是不可逆转的。许多钱包网站会提醒用户“ 你完全拥有自己的加密货，如
果你弄丢了助记词，那我们也无能为力 ”，这让很大一部分潜在用户打了退堂鼓。混合设置（例如，像
Casa这样的多签服务供应商）提供了一种追索和支持路径，可妥善管理用户资金。就像加密教育一样，
这个问题不能靠某个团队单打独斗解决，需要整个生态系统开发与安全实践相结合的工具和用户体验模
式。　结论　尽管MPC和智能钱包有着这样那样的不同，但从长远来看它们并不是竞争关系，
而是互补关系。MPC在密钥生成和管理级别提供了共享安全性，而智能合约则为功能和应用程序开发带
来了可扩展性和生态系统方法。例如：　MPC可以通过将一个或多个私钥进行多片分割来增强现有
的多重签名方案。如果有三个人来负责一个多签2/3的安全，这三个用户中的任何一个人都可以使用MPC
细分他们的个人私钥，并将他们的MPC密钥分片存储在独立的机器上，也就是让MPC帐户成为箱的所有
者。　社区或DAO可以是持有PKPNFT的多签签名者，该NFT管理去中心化云钱包，可用于自动投
资或DEX交互。　今年，中心化实体许多不计后果的行为从很多方面削弱了加密货的发展，它们侵
蚀了行业信任，引来了监管审查，*重要的是，还损失了用户的资金，其中很多是用户的毕生储蓄。文中
重点提及的技术和项目为未来铺平了道路，每个人都可以参与到去中心化经济中，不再把自己的命运交

到少数人手中。