MobileCoin

一种能为区块链应用带来优质用户体验的虚拟代币

2017年11月13日

研发初衷

目前，结合了加密货币和区块链技术的应用程序往往都很难调配，尤其是在移动环境下。这类应用程序的系统，正面临着设备资源限制、交易时间、密钥管理三方面巨大的调配挑战，而这些都会带来糟糕的用户体验。移动应用目前并不具备同步整条千兆字节区块链的能力，用户也无法接受确认一笔交易，需要等待数分钟之久。此外，大多用户也并不能真正做到长期、可靠地保管密钥。

很多原本想创造优秀用户体验的应用，大多却依托于了第三方服务，让第三方来管理密钥和确认交易。结果，大大牺牲了加密货币的主要优势。

MobileCoin正致力于开发一种快捷、私密、易于使用的加密货币，即使在设备资源受限的环境下，也可调配给那些无法长期妥善保管密钥的用户，而且资金控制权始终都在用户手中，不会被转交给第三方支付服务商。

用户体验

MobileCoin的设计初衷是为了提升加密货币在WhatsApp或Signal等移动通讯应用中的用户体验。用户需要下载安装app并输入4位PIN码，然后通过电话号码或用户ID就可以向其他用户发送 / 接收资金。每笔交易的确认时长不到一秒，资金到账就能立即使用，任何信息服务商或其他第三方都无法获取用户的资料（如，账户收支、交易历史、放款 / 收款人地址等）。无论何时何地，重装系统也好，更换手机也好，只要用户能够确保收到4位PIN码，那么就可以重新获得资金的安全访问权限。而支付也将能够在各种app和网络之间自由进行。

代币设计

MobileCoin的设计源于其最初意识到了“并非所有用户都有能力参与到P2P网络中”，并就此提出了一种联盟化的解决方案。

MobileCoin网络由众多节点组成，且每个节点都将被用以服务用户。

由节点负责完成那些客户端无法处理的任务，例如，维护一个庞大的账本和处理高吞吐、低延迟的交易，但被这样设计出的节点运行者却既不能访问用户资金，也无法知晓用户的余额和交易历史。

这是通过分层途径完成的，结合了多层次的多层防御和前向安全性。

1. Intel软件保护扩展（Intel Software Guard Extension, SGX）

所有的MobileCoin节点都在SGX安全区域中运行。而SGX安全区域在硬件加密的内存中，与操作系统分离，这样有效防止了节点运行者“窥探”安全区域中的内容。即便是这样，通过访问内存导致信息泄露也是需要小心避免的。SGX还支持一种称为“远程认证”的特性，这个特性使用户能够通过网络连接，远程判断出服务器正在SGX安全区域内运行哪些特定软件。在节点间建立加密连接之前进行远程认证，使得整个MobileCoin账本在全网的SGX安全区域中都是始终保持着封闭的。而这意味着，该账本在“公开”和分配给所有MobileCoin节点时，都是不能人为访问或查看的（即使是MobileCoin节点运行者），从而保证了SGX和MobileCoin的安全性。

2. 交易隐私

MobileCoin不会仅仅依靠SGX维护交易隐私。交易使用CryptoNote[1]一次性地址和一次性环签名。因此，即使攻击者能够攻破SGX并在网络上查看交易，MobileCoin也仍然能通过无法链接到的地址保护交易隐私。

3. 共识机制

MobileCoin节点利用具有联合特性的恒星共识协议（Stellar Consensus Protocol[2]）来同步分类账本，这不仅能使其在正常情况下的交易速度达到次秒级别，加以去中心化的控制和灵活的信任机制；还能避免节点存储交易历史的完整区块链，因为只需要维护地址账簿映射，和使用过的镜像钥列表（防止重复消费）就够了。

而这就为前向保密[3]提供了一定措施。即使一次性环签名将交易源隐藏在了大量可能的备选项中，使用SCP也意味着，信息可以在交易完成后全部丢弃，并不需要永久保存在区块链中。

4. 密钥管理

在SGX区域中运行MobileCoin能够使节点为用户安全地管理密钥。客户端可以通过远程认证，在将其密钥传输远程安全区域之前，连同简短恢复PIN码一起，将密钥传输到MobileCoin节点。之后，MobileCoin节点就可以对密钥的“已认证”访问进行限制，而安全区域也将保护节点免受其运行者或任何危害节点的人绕过软件并试图直接暴力访问密钥。通过这种方式，用户密钥便可以安全地驻留在节点中，并能在应用程序重新安装或丢失时得以保留，无需信任节点操作者或节点计算机的安全性，更不必记住或安全存储极长的恢复助记词。

---

1 https://cryptonote.org/whitepaper.pdf

2 https://www.stellar.org/papers/stellar-consensus-protocol.pdf

3 https://en.wikipedia.org/wiki/Forward_secrecy

交易流程

- 安装时，Alice的客户端生成了一个MobileCoin钥匙对和一个PIN简短恢复码。
- 安装时，Alice的客户端通过MobileCoin节点执行远程认证，在SGX安全区域内建立安全通信信道，然后连同MobileCoin钥匙对一起发送PIN简短恢复码
- 为了向Bob付款，Alice的客户端查找Bob的公钥
- Alice的客户端为Bob生成一次性CryptoNote公钥
- Alice的客户端为交易生成一次性CryptoNote环签名
- Alice的客户端将待传输交易上传至MobileCoin节点
- 节点经恒星共识协议（Stellar Consensus Protocol）将交易同步到网络。MobileCoin账本被更新以反映交易输出值，同时生成镜像钥，作为一次性环签名的一部分以防止双重消费。其他全部丢弃。
- Bob的MobileCoin节点用Bob的CryptoNote跟踪密钥来识别其一次性公钥
- Bob的MobileCoin节点向Bob的客户端发出消息，并通过该消息计算出与该一次性公钥对应的私钥。
- Bob成功收到了付款。

这样的交易在几秒间完成，且所有的交易和账户信息都妥善保存在全网SGX安全区域内，使交易本身永不可见，交易隐私也能在攻击者伪造SGX远程认证，以便通过修改后的软件连接到网络时，得到CryptoNote一次性地址和一次性环签名的进一步保护。节点运行者或攻击过节点的人永久不能访问用户密钥或用户数据，但用户可以通过输入4~6位PIN码简单地在更换手机或重新下载app时保持他们的资金访问权限。

MobileCoin钱包

MobileCoin的设计为如Whatsapp和Signal一类的移动通讯应用程序提供了MobileCoin钱包服务。通讯应用程序可以安全地恢复所需信息，既有利于在安装或重新安装时从MobileCoin节点上创建和确认交易，又有利于从MobileCoin节

点上接收更新－即使是在网络连接并不持续的情况下。被集成到如Whatsapp和Signal一类的移动通讯应用程序的MobileCoin钱包还可以根据用户名查阅到收款终端的公钥地址，并向收款方发送拥有可拒信号的加密信息，以证明该交易的发起。

团队成员

Joshua Goldbard - CEO

Joshua虽高中辍学，却深入学习了叙事和信息系统。成年时期大部分时间从事于电信行业，Joshua曾开发、管理、执行了非常复杂的通信网络。他对于移动系统的专业性和对加密货币作为信息网络价值调节系统的热情帮助他领到了这个项目。

Moxie Marlinspike - CTO

Moxie 是一位对安全通信充满热情的密码学家。除了身为Open Whisper System的首席开发人员，Moxie还是Signal（约有1000万用户）的整体负责人、负责调配WhatsApp（超过13亿用户）的加密协议，而以上两家都是当今世界领先的加密信息系统。此外，Moxie还负责开发SSL认证固定（SSL certificate pinning）技术及帮助主管Twitter的安全性。Moxie喜欢探险和旅游，通过海、陆、空任意方式探索这个世界。

Shane Glynn - 法律总顾问

Shane是一位对寻求肾上腺素的快感和逻辑一致性有着强烈热情的律师。在Google就职期间，Shane曾帮助众多团队实现了产品上线，其中包括Android。Shane喜欢了解与法律有关的新奇问题，对吸收现有的加密货币法规也有着强

烈热忱。身为一名成功的跳伞运动员，Shane享受从天空掉落的感觉，就像阅读美国证监会（SEC）案例法一样。

顾问

李笑来

EOS，Sia，ZCash和yunbi.com早期投资者。

Eric Meltzer

INB合伙人，Basecoin和Stream顾问。

Dax Hansen

Perkins Coie合伙人。全球最早关注加密行业的律师之一。

Todd Huffman

3scan创始人及CEO，BIL联盟联合创始人。

私募预售FAQ

MOB代币的发行总量是多少?

2亿5千万枚。代币的供应和发行是定量的，且永远都不会增发。

预售阶段会出售多少枚代币呢?

3750万枚代币。

募资目标是多少?

3千万美元。

预售阶段代币价格是多少?

1 MOB ＝ 0.8美元。

有任何批量折扣或特殊折扣吗?

没有，1 MOB＝0.8美元是MOB代币现提供的固定和唯一价格。

预售阶段何时结束?

软性承诺将于12月18日截止。

有锁定期吗?

对用户来说没有，团队的代币会锁定一年，然后后续4年逐步解锁。

代币什么时候上交易所?

MOB在12月底会登陆一个交易所（硬性承诺），然后很可能会于2018年第一到第二季度间登陆其他交易所。

ERC20代币什么时候能被转换成我们上线的网络代币?

团队计划在预售完成6个月内将MobileCoin上线。通常而言，使用到新技术的软件项目研发是很难的，我们将始终优先考虑传输安全而非传输速度。

为何要在MOB网络运行之前拥有ERC20代币呢?

ERC20代币转换为活跃代币这一过程是一个极其难得的机会，迫使100%的用户经历“绊倒”过程，让大家感受MOB网络代币分发的匿名特性。其他匿名加密货币遭受着一种能够轻易被“破”匿名化的初始交易集合，而这正是我们想要通

过技术避免的东西。此外，允许一段时间的交易可以增加账本中的地址数量，可以增强CryptoNote的私密特性。

什么是Enclave安全区域?

Secure Enclaves（安全区域）是现代计算机内部存在的强化安全系统。通过正确的技术实现，这些安全区域将能够提供0知识运行环境，允许节点在不知道当前运行内容的情况下运行程序。

什么是安全密钥管理系统?

通过使用包含安全区域的简单技术系统，用户即使在新设备上也可以通过输入4~6位PIN码找回其加密资产。这样的PIN码还运用于与其他身份启发式技术结合，以授权交易。

如何分配代币的销售收益?

全部收益都将用于开发开源软件、工具、MobileCoin协议和生态系统的基础结构。

- 私募咨询: MOB顾问Eric (微信wheatpond), Mixin-Iris (微信835661681)；
- MobileCoin Telegram社群(复制下方链接到浏览器后可加入群聊)：
  https://t.me/joinchat/GA07XBL9Jn0Nub8ZythAWA