MiXin白皮书中文翻译

钟晓宏 简书作者

2018.01.02 19:57 打开App

一、动机

人们接触到的区块链和加密货币的新闻越来越多，但是即使是软件开发者，也很难进入这些奇特的事物。

大部分的区块链项目着重于分布式因素和安全秘钥管理。然而所有这些导致了低交易速度、私钥丢失，难以理解。基本不可能将这些分布式节点部署在移动设备上（最受欢迎的计算设备）。

虽然他们在分布式的梦想中努力，但是我们注意到一个事实：即使最去中心化的区块链共识算法，也造成了几大矿池的控制，想想BCH从BTC分叉出来就知道了。

一些热门的区块链项目已经，或者计划选择一些不那么分布式的共识算法的设计，比如以太坊正在向权益证明算法迁移，EOS正在使用DPOS。这些努力可能会提高交易吞吐量，但是仅仅而已。

人们仍然需要管理奇特的私钥，面对私钥丢失，矿池和大的节点不花吹灰之力，就可以无数次分叉网络。开发者尽最大的努力开发一些新的代币，人们没有合适的方法使用在移动设备上的节点。

二、设计

Mixin致力于找到分布式网络和传统服务器群集之间的平衡，通过权衡，结合两者的优点。

1、受限且可信任的全节点，保证数据透明和一致

2、零知识证明和免交易费，高吞吐量和低延迟性

3、通过区块链跨链协议连接所有热门的区块链网络

4、未确认的交易，直接和外部信任源交互

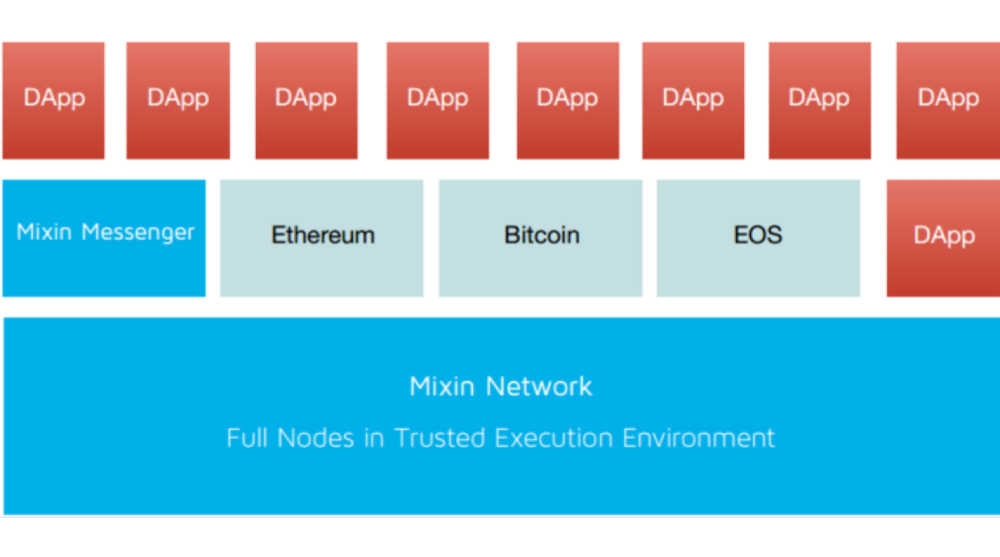
5、基于手机号码和PIN码账户模型，易于手机使用

6、安全和端对端加密信息通道，发送消息到每个会话的参与者

6、对开发者友好，方便使用所有的linux库和编程语言

7、最大的移动区块链区块链网络效应应该防止分叉

为了实现这些目标，我们设计了一个独一无二的区块链模型，这个模型依赖于可信任的执行环境技术和关系。共识算法主要用于保证数据的复制。移动设备节点主要用于全节点运行时的验证。



由上图可知，Mixin网络的基础是运行在可信任执行环境的全节点。

所有Mixin全节点被完全信任，这是因为它们可以证明其它全节点的ID和运行时可信任执行环境下运行的code。

MiXin节点处理交易，参与共识算法。

由于可以验证code，为了高吞吐量和低延迟，只有一个节点跑DAPP。

为了保障安全和隐私，保持数据的透明和一致，网络中所有敏感的组件应该在可信任执行环境下运行。

三、端对端消息加密

Mixin使用Signal协议管理所有会话，不管私信和群聊。

这个协议是基于客户端，服务端只是一个消息代理。因为端对端加密特性，没有人能够查看被代理的消息，即使Mixin全节点。

一旦消息被会话的所有成员读取，服务器上的所有消息将会被永久删除。

在上传到我们的云存储之前，图片、视频和其它附件 也用随机AES秘钥加密，然后客户端将传输所有元数据，比如缩略图、作为Signal发送者秘钥加密的容器的AES秘钥

由于Mixin使用成熟的Signal协议和开源的库作为消息协议，我们不打算深挖白皮书中特性的技术细节。

四、手机和PIN验证码

阻碍人们使用区块链的不是性能，是账号管理程序。

所有流行的区块链网络需要人们获取和管理至少一个私钥。这太复杂了，不是一点点，而是比用户名和密码方案复杂数百倍。

所有现存的区块链数据是透明的，在使用用户名和密码之外，为了保证账户安全，用户还需要管理一个复杂的密码，例如BTS和EOS。

多亏有零知识和Mixin网络中的安全执行环境，使得我们能够设计一个基于手机验证码和PIN码，简单得多的ID方案。

人们只需要一个电话号码，记住6位数PIN码，比用户名密码方案更简单，没有复杂的私钥，但是安全水平不相上下。

使用手机号码校验来传输私钥，保证了简单的手机迁移，6位PIN码可以被手机上的Touch ID或者Face ID替换，大大提高了用户体验。

典型的比特币交易需要花费1个小时才能确认，对于小微支付来说，交易费用太高，且区块链数据的公开性使得交易不可能有隐私。

为了克服比特币的这个问题，使用上面的ID处理程序，我们设计了一个跨链的交易网络，类似于比特币的闪电网络，或者以太坊的雷电网络。

Mixin PIN码的底层技术仍然是私钥管理，但是Mixin零知识可信任的执行网络，保证了安全和简单。所以可以把这种当做像管理比特币，或者其它区块链资产的闪电网络的智能合约。

其它区块链资产进入Mixin网络后，当一个Mixin用户向另外一个Mixin用户发起比特币交易。服务器不会在比特币区块链上发起真正的交易，只是他们在Mixin区块链上的余额数字变了，交易速度速度堪比通用的数据库操作。

五、XIN 代币

XIN是Mixin上许多服务使用的代币，特别是全节点抵押，DAPP创建和API调用。

想要成为网络中的全节点，需要抵押至少1万个XIN代币，以建立初始的信任。

所有DAPP创建，每次都需要花费一些XIN，消耗的数量由DAPP claim消耗的资源而定。

DAPP调用Minxin API也需要花费一些XIN，消耗的数量由调用的类型和数量而定。

平台获得的XIN都将被销毁，以增加现存XIN的价值。

1百万XIN代币一次性发布，为了计算的方便，Mixin Messager主要使用MIX作为主要货币符号，MIX是milliXIN的缩写，等价于千分之一XIN。

六、总结

Mixin网络无限吞吐量，简单和熟悉的账户模型，连接和使用现存区块链网络的所有数字货币。

除了底层的Mixin网络，我们正在开发第一款DAPP和Mixin网络的入口：Mixin Messenger。Mixin Messager所有代码是开源的，开发者可以概览如何在Mixin网络中开发。

如果**将Mixin网络看成开源的安卓生态系统**，所有现存的区块链网络看成不同的手机制造商和国家，那么**Mixin Messenger就如同Google Play**，是用户和开发者的DAPP商店。

Minxin网络拥有将近1百万预注册用户，欢迎所有的开发者，在熟悉的开发环境下，开发或者适配他们当前app到平台上。

值得一提的是，Mixin App安卓版已经上线，读者可以下载体验一下。

注册网址： https://mixin.one/enroll/681441

app下载地址：https://mixin.one/

请注意：本文不构成投资建议

以上，如果翻译有错，或者表达不够准确，请不吝指出！

如果觉得本翻译有价值，也可以打赏QYB（区研币），区研币是中国最大的区块链知识服务社区：区块链研习社发行的，全世界第一个知识社区币。

以下是我的QYB地址：

QXH6xff9CM6GgNtcs4fu9otbducnWfGH2n

小礼物走一走，来简书关注我

赞赏支持

简书作者

钟晓宏

写了 9552 字，获得了 24 个喜欢

＋ 关注

作者个人主页 ›