公链开发技术应用实战:多签名钱包的构建

产品名称	公链开发技术应用实战:多签名钱包的构建
公司名称	河南漫云科技有限公司
价格	1000.00/件
规格参数	漫云科技:公链开发技术应用实战:多签名钱包的构建
公司地址	郑东新区升龙广场3号楼A座3202
联系电话	13103827627 13103827627

产品详情

我们平常都是使用单签钱包与qukuailian进行一系列的操作，如在进行转账时，我们需要使用钱包（metamask）去approve一个签名，然后交易才会执行并且进行转账。那么多签钱包（MultisigWallet）就是要多个人去签名执行某个交互操作的钱包。

使用多签钱包进行转账，往往需要>=1个人去签名发送交易之后，转账操作才能完成。使用多签钱包时，我们可以指定m/n的签名模式，就是n个人里面有m个人签名即可完成操作。可以根据自己的需求设置多签规则，例如：

1/2多签模式：两个互相信任的朋友或自己的两个钱包，可以凭各自的私钥独立发起交易（类似于合伙账户）。

2/2多签模式：金库中的资金需要2个管理员均同意才能动用这笔资金（需要两个私钥才能转移资金）。

2/3多签模式：三个合伙人共同管理资金，为了规避私钥丢失的风险，其中两个私钥签名就可以转移资金。

当然，还有1/3多签、2/4多签、5/8多签不同规则的多签方案，规则是按需的。虽然麻烦了一点，都是它保证安全是非常可靠的。

多签钱包的应用

1.保证个人资金安全

在单签钱包中，一旦私钥丢失或持有者遗忘钱包助记词，那就意味着持有者失去了对该钱包地址的控制权，与其相关联的加密资产将完全丢失。而多签钱包的存在，大程度降低了单个私钥丢失时的资产损失风险。以2/3模式为例，在全部3个私钥中，只要有2个私钥完成了签名授权操作就能进行相关加密货

币的交易。即使有1个私钥丢失，还能通过剩下的2个私钥完成对资产的转移，避免资产损失。这种情况下，个人可以创建一个多签钱包，再创建多个钱包地址，分布在多个地方，比如metamask一个，手机上一个，冷钱包一个，把这几个地址都加入多签钱包中，动用里面资产需要用其中一个钱包签名，为了方便，使用1/3模式签名也可以，这样，如果一个设备丢了，可以立马把该设备的钱包地址从多签钱包移出，保证资产安全。

2.资产共管

很多DeFi协议/DAO组织/qukuailian团队其实都有自己的金库，金库里的钱是不能由任何一个人直接动用的，每次动用都要经过多数人的同意或社区投票。这时使用多签钱包来保存金库资产是再合适不过了。

3.多签操作

在目前这个发展阶段，很多去中心化协议其实都是有个管理员权限的，这个管理员权限往往可以更改协议的某些关键参数。行业普遍做法是把这个管理员权限交给一个多签钱包或时间锁，当需要更改参数时，需要多个人共同签署相关操作。