MPC钱包 VS 智能合约钱包开发

产品名称	MPC钱包 VS 智能合约钱包开发
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:MPC钱包 VS 智能合约钱包开发
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

在波哥大举办的Devcon6大会中，TomaszTunguz提到了Web3.0的一些统计数据：各主流公链DAU累计约为250万，而传统互联网的DAU为50亿，前者勉强够上后者的0.05%。从供给侧来看，约有1.6万名kaifa者在Web3.0kaifa，而世界上kaifa者总数达到了2700万，Web3kaifa者占卜不足0.06%。因此，Web3.0离massadoption还有很远的距离。

钱包，作为Web3.0的入口，其用户体验直接影响到加密行业何时能迎来大规模化采用。尽管各大钱包在这方面卯足了劲，可在普通用户的眼里，钱包使用体验依旧不尽人意。托管钱包虽然易用，但是安全性是一个很大的隐患，钱包被盗事件层出不穷。自托管钱包虽然相对安全，但保管长长的助记词和私钥的方式与传统互联网的用户名-密码体系相比复杂了很多。据Chainalysis的研究报告显示，截止2021年约有20%流通中的bitebi，因所有者不记得私钥而丢失。很多人可能会有疑问，为什么我们不能将传统的验证方式应用到Web3.0来呢？

为什么我们只能通过私钥的方式进行验证？为了回答这个问题，我们需要了一些背景知识和概念。首先是以太坊上的账户类型。以太坊一共有两种账户：外部账户和合约账户。合约账户就是智能合约，其代码由以太坊虚拟机来运行。而外部账户就是我们平常用来发起交易的钱包账户，它之所以被称为“ 外部“ 是因为这种账户本身是没有代码的，因此独立于以太坊虚拟机之外，由用户通过私钥进行控制。

合约账户虽然有自定义逻辑，但它是无法主动发起事务的。因此任何合约状态的改变都依赖外部账户来发起，并由外部账户支付Ether。那如何验证事务的合法性呢？以太坊上的验证方式为检查事务的发起人和资产(Ether)的所有人，也就是这个外部账户的拥有者是一致的。因此用户需要通过钱包对交易进行签署。而以太坊默认的验证逻辑是中本聪设计的，也正是通过此算法生了密钥对。签名的正确性可以通过验证该签名是否出自跟某个共钥对应的私钥检验，因此用户必须掌握这个私钥。这就是为什么无论如何优化钱包的用户体验也无法绕开私钥的问题。

MPC，全称为Multi-PartyComputation，是一种重要的加密安全措施。其包含了很多种技术方案，在本文的语境下主要指MPC-TSS。而MPC钱包，是通过对私钥进行多方计算在链下实现“ 多签“ 、”跨链“ 等等更复杂的验证方式。简单来说，就是将一个私钥打碎成多片，将私钥碎片交与一个去中心化的网络进行计算和加密。当需要私钥签名时，则将碎片再拼接起来形成一个完整的私钥。MPC的核心

思路为分散控制权以达到分散风险或提高备灾的目的，有效避免了单点失败等安全问题。

MPC钱包“ 多方参与 ”的概念与“ 多签钱包 ”有些类似，但实际上，虽然都可以实现“ 多签 ”的功能，二者的实现途径是不一样的。之前我们所熟知的多签钱包，比如GnosisSafe等等，是建立在智能合约上的钱包，合约中定义了验证逻辑，比如如果需要验证一笔交易，需要一个以上的私钥，或者五个中至少三个私钥进行验证。这类钱包属于后文即将提到的智能钱包的一种。而MPC钱包，则是将一个私钥分解成多个片段，验证过程只涉及到一个私钥。并且计算网络是链下的，与智能合约并无联系。