专访TBC：基于UTXO的比特币二层扩容 为何可行性越来越高？

基于比特币UTXO账户模型的扩容方案，被行业认为是“最清真”的二层方案。这个方案试图基于比特币 UTXO 进行链下账本计算，并通过客户端验证来确保账本的真实性，由此既保留了比特币原有的特性，又实现了二层账本共享和安全。

一直以来，行业公认该方案实施起来十分困难。通过该方案构建起的知名的项目和协议有RGB、RGB++、BitVM等。虽然知名，但方案的进展其实都比较缓慢，如RGB涉及的多个技术要点具有较高实现难度，又比如BitVM虽然提供了一种在比特币网络上实现复杂合约的方法，但是在一些技术细节上仍然存在争议。

这样一个相对困难的技术路线，为何仍有大量项目方愿意实践？与其它模式相比， BTC 同构的 UTXO 模型二层方案，无疑是既安全又优雅的。我们回望依托于UTXO的二层扩容方案发展历程发现，铭文这种写入UTXO的“资产发行”模式的火爆，为这种UTXO模式的二层扩容方案注入许多关注和资源，让开发者和项目方们认真审视这一路径实现二层方案的可能性。

和以太坊二层扩容方案有着明确方案不同，比特币的二层方案百花齐放，再伴随着比特币协议本身的一些升级，比特币的二层其实有着很多可能性，好玩且创新也足。

目前项目方们依托于UTXO的技术做了哪些比特币二层的改进和创新？为了探寻这些问题的答案，本站专访了TBC的CMO，以技术为基点探寻UTXO模式比特币二层的实现路径。

本站：请您介绍一下基于UTXO模式的比特币二层在技术上是如何实现的？

TBC：这种技术是将数据封装到比特币的每一个UTXO上，然后通过客户端验证来确保资产安全。

举几个例子，如RGB的思路，就是将链外的RGB交易与比特币交易的UTXO绑定在一起。而RGB++协议是受到了RGB协议的启发，主要思路与RGB类似，通过链下的计算，然后执行和验证交易，最后在比特币链上进行结算。RGB和RGB++两者不同的在于，RGB++在交易和资产验证环节，采取了不太一样的思路。

TBC又和以上两种方案不同，我们采用的是大区块加数据剪裁，再加智能合约的方案。我们的定位是比特币的一个智能合约层，为比特币系统引入智能合约方案，并带来海量应用。TBC也是比特币虚拟机BVM的开创者。

目前，比特币生态崛起，越来越多的开发者涌入，新的应用层出不穷。但是比特币的主网区块仍限制在一兆，而在每十分钟网络传播的必要数据包越来越大的情况下，主网就不太能满足这一需求。比特币小区块的设计，每分钟100兆以上就吃不消了。

而TBC这种大区块加数据剪裁加UTXO智能合约模式能够帮助BTC解决拥堵和区块限制问题。TBC最初选择这一路径也是发现了UTXO模块就是这样一个底层模型就是天然适合高并发和高性能。

本站：TBC的这一路径在实现过程中遇到了哪些困难，又是如何解决的？

TBC：最主要的问题其实是BTC的可扩展性较差。一直到了2017年隔离见证升级激活，解决了比特币链上一些交易可塑性问题。到了2018年，开发者们开始逐渐部署一些节点。更重要的则是2012年参数的升级为比特币带来了比较高效、灵活、私密的传输方式。这个升级的核心是使用了施诺尔签名和模块抽象语法树合约。

以上这些升级给BTC的进一步扩展带来了比较好基础，我们之前所说的一些开发难点，在升级后都得到了一定缓解。因为比特币本身技术的发展，类似修改签名，其实增加了一个连接一层和二层的桥接的作用，并不是直接拓展了一层。

本站：目前比特币二层的路线和项目都繁多，你怎么看？

TBC：在我看来，以BTC作为资产结算层，然后构建本地的共识和计算验证能力来实现的二层扩展方案都是可行的。比特币生态和以太坊生态的一个很大不同是，它不遵守什么统一的规范和正统性，所以能够百花齐放。

本站：行业内的共识还是觉得UTXO的二层模式落地太困难了？这个难点怎么解决？

TBC：目前行业内对于UTXO这种模式其实存在一个误解，他们认为UTXO模式没有办法维护全均状态，或者无法实现循环调用，所以无法实现智能合约。这个观点现在看是片面且过时的，TBC已经证明了UTXO模式的区块链是完全可以实现智能合约的，只是实现的方式和其它的二层方案不同。当然，目前基于UTXO模型实现智能合约的基础工具在不断成熟，大家都在不断尝试。

对于TBC来说，发展的关键节点其实是TBC 20标准协议即将上线，这意味着项目方来TBC上做应用和协议会变得容易，这能推动TBC链上生态的繁荣，乃至整个比特币生态的繁荣。

本站：TBC对比其它的二层方案，有何优势和创新？

TBC：我们相当于一个创新型的路线，这套BVM的方案目前看只有TBC在做。简单说，该方案是基于比特币的脚本系统的恢复和功能扩展的一种虚拟机，也是TBC智能合约的一个执行引擎。

它包括输入和输出栈那类语言栈，这样在进行任意操作的时候，能实现更高层次的逻辑。目前编程语言的执行结构，很大程度上都是依赖执行栈的。从原理上讲，只要通过栈式结构，就可以实现任意复杂程序。当然，同时需要保证内存资源足够多。栈式结构也可以不作为编程语言的基础，但由于比特币对于脚本系统的一些限制，导致只能进行一些简单的逻辑判断，可以使用的操作码是相对来说比较有限的，所以说无法实现一些复杂的智能合约。

这就需要BTC的核心开发者不断去做一些提案，比如说最近比较火的OP\_CAT的提案，简单来说，OP\_CAT可以实现多个UTXO解锁脚本字节串的组合连接处理，来提升BTC主网的可编程特性。

本站：比特币生态目前发展到了哪个阶段，目前发展的难点在哪里？

TBC：目前比特币生态肯定还处于早期，目前的难点其实在于开发者太少，一些刚刚投身比特币生态的开发者需要重新学习开发语言，周期大概是一两个月。随着开发者的增加，开发的应用就会增加，从而实现量变到质变，才能实现类似以太坊生态的繁荣状况。目前比特币生态的开发，还是亚太的团队更多。

本站：对于散户来说，如何抓住比特币生的一些机会？

TBC：能够帮助比特币做好小额支付的协议，或者大额抵押借贷协议都是值得关注的。以及基于UTXO架构的智能合约层，也能跑出一些比较优秀的项目。