对话Bool网络及其生态项目：如何为BTCFi提供安全的资产托管

受访者：Jeffrey，Bool Network

Kai，Bool Network

Witter，Hibit

水牛，ChainSwift

自2023年铭文之夏以来，比特币生态始终都是人们关注的焦点，而BTC Layer2在短暂繁荣后再度陷入谷底，让部分人对BTC二层叙事的合理性产生了怀疑；此外，绝大多数BTC托管方案无法摆脱多签/MPC的模式，毫无疑问这成为了限制BTC生态发展的重大瓶颈。

对此，极客web3邀请了Bool Network及其生态内的CEX应用链Hibit及BTCFi项目ChainSwift，就比特币生态及Layer2体系的现状、比特币资产托管的问题、Bool Network在托管方案上的独特设计、Hibit和ChainSwift的原理及其与Bool的结合点展开了讨论。期间Bool的Jeffery指出，大多数比特币二层是伪概念，大家真正该做的是拓宽BTC的应用场景，尤其是BTCFi。

以下为此次对话的文字版记录，欢迎大家阅读！



1. Faust：最近从很多渠道听闻，不少VC和项目方认为比特币二层的叙事到了谷底，热度远不及几个月前，甚至有人认为EVM系比特币二层不能证明自己的存在价值。现在有不少人把目光转向了BTCFi概念上，对此各位怎么看？

Jeffrey：就我个人的见闻而言，有不少人对比特币二层没了信心，有几个项目之前还在比特币生态里积极推广，现在却连推特都不更新了。其实归根结底，绝大多数比特币二层没有跳出“WBTC-以太坊”的模式，尤其是EVM系Layer2，无非是“源链上锁定资产，目标链mint映射资产”，这跟把比特币通过WBTC的方式跨到以太坊上去有什么区别呢？而且大多数二层的跨链桥部分，甚至都不及WBTC安全可靠。

对于比特币而言，单纯的“扩容”是一种伪概念和伪需求，真正的刚需是拓展其应用场景，这不是说你搞一条独立公链搭个桥搞个WBTC这类东西就行了。像Babylon就是一个释放比特币潜能的优质案例，它可以让比特币赋能POS公链的经济安全，在功能性上对比特币进行拓展。

至于BTCFi，更多是拓展比特币的金融场景，这要比BTC Layer2的叙事更细化，聚焦的点也更集中。比特币链上常年有那么多BTC处于休眠状态，很多老OG宁愿把比特币放在冷钱包里也不愿意拿出来参与金融活动，究其根源，1是大多数平台无法真正保障资产安全，2是缺乏有吸引力的东西。如果BTCFi的发展成熟了，我相信会改变比特币生态的很多问题。

对于Bool Network而言，我们是认同BTCFi和比特币本身的巨大潜力的，现在我们的主要立足点在于，通过尽可能Trustless的方式解锁BTC的资产潜力。Babylon的案例已经说明Web3的许多地方都需要比特币资产的参与，这块的的想象空间还是很大的。

2. Faust：其实Bitlayer的联创Kevin之前也表达过，很多BTC大户有资产生息的需求，但前提是要放到足够安全的地方。现在比特币生态很多项目都存在风险。对于资产安全这个话题，你们怎么看？

Jeffrey：其实资产安全是一个说来话长的问题。很多人认为“用户不关心xx项目是不是安全的”，但事实是抱有这种想法的“用户”都不是高净值的，很多大户或大机构都很重视资产安全，甚至是如履薄冰，他们是否愿意把资产放置在某个平台，必要条件就是安全性。

这里拿Babylon举一个例子，其实Babylon有一个瑕疵，会阻碍它吸引BTC大户，因为它的罚没机制。在Babylon的机制模型中，我的BTC通过Staking的形式，为某个PoS应用链提供了经济安全，对应地，我会获得该应用链的Token作为质押奖励。

但这个应用链的Token，跟我手中真金白银的BTC比起来，实际上就是空气币。而参与POS Staking的过程中，我的BTC是可能被罚没的，也就是说，我获得的奖励可能是一堆空气币，代价却是失去真金白银的BTC，这对大户来说是很难接受的。

类似的道理，因为大多数BTCFi项目给参与者提供的激励基本都是Alt Coin，如果要让这些人愿意理你，最好还是让自己做的东西足够安全，这就是资产安全的价值所在。

3.雾月：我们把话题回到Bool Network本身。你们的自我定位是什么？从技术上来讲，Bool怎么保证资产安全？我记得你们说，Bool网络里参与门限签名的节点不知道具体计算内容，这个怎么实现？

Jeffrey：Bool做的事情其实是为BTC做去信任的资产托管，并且为用户提供强制提款、逃生舱等机制，使BTC安全的参与到BTCFi等场景中。我们为跨链桥、Restaking、基于BTC的稳定币、预言机、链上交易平台等提供BTC托管设施，但这些场景中要提供的功能，不只是把BTC跨走跨回那么简单。

要更通俗的概括，因为BTCFi几乎都要依赖于链下的组件，当你的BTC尝试和链下的东西产生交互关系时，我怎么保证BTC仍然安全？这就涉及到资产托管的方式。大多数跨链桥和交易平台以及Defi平台，核心业务就是资产托管，你要把自己的资产交给第三方去保管，在需要的时候拿回来，但怎么能保证资金不被托管方卷走或是扣留，我怎么无需许可的把比特币强制提回到BTC链上，都是要考虑的。

对此我们基于预签名、Taproot和时间锁等技术，在BTC链上搭建了类似于强制提款/逃生舱的功能，用户可以对自己的BTC掌握主动权，关键时刻可以免信任的把资产强制撤回。

此外，我们还基于ZK和TEE提出了“动态隐藏委员会”的概念，简称“DHC"。这里我说一下动态隐藏委员会DHC是怎么生回事。首先，Bool Network是基于资产质押的无需准入网络，只要买了特定硬件，再加上一定的资产质押，就可以参与成为Bool网络中的节点。

假如现在有1000个节点分布在全球各地，那我如何去创建DHC呢？假如说，现在某个资管平台用了Bool的服务，需要让Bool为它创建一个有效期为10分钟的MPC/TSS委员会，阈值为7/10（简单理解为安全性更高的多签），也就是说从1000个节点里临时选10个，组成一个委员会做门限签名，过10分钟就解散换一批节点。

我们为此原创了Ring VRF算法，结合ZK做了隐私保护，在每届委员会的任期内，10个被选中者的身份是无法获知的，包括被选中者自己都不知道（这块用了TEE）。

这种设计有两个好处，首先由于DHC是动态、临时、保密的，想要作恶的话，你要在有限的时间内黑掉或者贿赂10个人中的7个，但因为有隐私保护，你都不知道这10个人是谁；其次，由于DHC成员之间彼此隐藏，串谋作恶的问题可以被规避，因为互相之间的身份都无从知晓，自然无法串谋。反串谋这个事很关键，因为大多数中心化多签很难解决串谋作恶问题，而我们的方案可以反串谋。

这种情况下，除非你把整个Bool网络大部分节点都黑了才行，或者是破解Bool的机制设计。也就是说，基于DHC的资产托管，其安全性与整个网络的安全基本等同。

雾月：关于用到TEE（可信执行环境）这块，可以展开多讲讲吗？

Jeffrey：TEE其实就是个黑匣子，程序和数据可以加密存储后跑在黑匣子里，连设备运行者都不知道TEE里跑的是什么。

我们刚才说Bool用到了TEE，如果不用TEE，节点运行者能通过一定方式，观察得知当前DHC参与者的账号，甚至可以对选举程序本身进行攻击。加上TEE后，相当于把程序和数据放在黑匣子里运行，节点运行者无法得知TEE里封存着的账号、密钥等信息。

之前有人问过，既然你们用了TEE，为什么还要用到ZK和MPC/TSS这样的技术？其实主要是为了增强系统的整体安全，如果我运行了基于TEE的节点，然后如果这个节点挂掉了，由于MPC/TSS本身就有很好的容错，网络依然可以正常运行，即MPC和TSS可以在TEE基础上增强容错属性，而有了ZK，可以保护DHC与者的隐私，防止串谋。综合下来，我们选用了TEE+MPC+ZK这样的复合技术，最大程度保证系统的安全。

之前很多人诟病，说TEE会用到较为中心化的远程认证方法，比方说如果我们用到SGX，会涉及到英特尔这样的中心化公司的影响。但我们把远程认证的程序以智能合约的形式实现了，认证方式可以变得去中心化（Scroll和Taiko也用到了类似的思路）。即使哪天英特尔出现了变故，我们这套程序仍然可以运行。

Kai：我对这一部分做个补充。Bool节点运行的程序是高度自动化的，TEE的主要功能，是把Bool客户端里需要保密的程序和数据，跟平时人机交互的那部分程序隔离开，但它会保留一些基础的，比如登录、交互等界面。只要将节点启动，后面它做验证也好，还是向链上提交SGX Proof也罢，整个程序都是自动化且关在TEE黑箱里面的。

TEE硬件会给Bool节点向外提交的任何信息打一个标识，方便外界去验证这个Bool节点是不是跑在TEE里的。如果他不是运行在TEE里，Bool布置在链上的智能合约会对该节点的质押资产进行Slash。

4. Faust：今天正好Bool生态内的项目也在，比如Hibit要做一个去中心化订单簿交易平台，选用Bool Network和ICP作为基础设施，解决资产托管与数据验证和资产快照的问题。

对此，有一个叫做Degate的交易平台，把自己做成了以太坊Layer2的形态，类似于路印协议。如果将你们与Degate和路印协议相比，相似点和差异点在哪里？

Witter：其实这个问题关系到信息透明和资产可撤回。CEX具有很多缺点，比如说可以挪用用户资产、可以操纵所内的流动性并砸盘，DEX虽然很大程度解决了这些问题，但也面临着TPS受限、多链流动性割裂的麻烦。

一个理想化的交易平台模型，是拥有中心化的性能体验，同时拥有去中心化的可信、数据可验证，并能够连通全链，包括全链资产和全链钱包。我们的目标就是成为这样的一个平台。

那么该如何实现这些？首先我们拥有自己的类似于Layer2和应用链混合的架构，Hibit网络内有固定的排序器节点，然后有上百台Validator，但这些节点之间没有直接的共识，是自顾自的从排序器那接收最新的交易数据，然后执行交易，再打包生成区块。

那么该如何保证不同节点的数据更新具有一致性？我们在ICP、Solana等高性能公链上部署了Verifier智能合约，直接让Hibit节点把本地生成的区块头发送到Verifier合约，只要大多数节点提交的区块头一致，就认为达成了共识。我们之所以这么做，主要是为了降低不同Validator节点之间频繁通讯产生的开销，最大程度提升TPS。

值得一提的是，我们会把区块头或者说Block Hash同步到比特币链上，通过OP\_Return操作码之类的方式，这其实相当于把Hibit的区块和比特币区块锚定起来，防止回滚。

Faust：这里我要问一下，Degate和路印协议都是有强制提款/逃生舱功能的，可以让用户绕开平台方的许可把资产强制撤出交易平台。你们对此有类似的机制设计吗？

Witter：如果对应到交易平台这个场景下，我们就要考虑一些极端情况，比如某个人被审查攻击，平台拒绝处理某个人的请求，这个时候用户就需要把资产强制撤出，逃生舱功能就是如此。

以太坊ZK Rollup的逃生舱是依赖于状态快照的，就是说我要把自己的资产从Layer2强制撤回到以太坊链上，要先出示资产余额的快照，证明自己在XX时刻有多少多少资产，那么这些资产快照数据存储在哪里就是个问题。

对此，Hibit采用了一种模块化资管的方案，我们把用户资产的余额快照存储在ICP、IPFS或是Arweave这类低成本的存储平台，在你需要的时候，你可以去这些平台上读取数据。前面我曾提到，Hibit会把Block Hash记录在比特币链上，根据这些Block Hash，你可以核对自己在Arweave等地方获取的状态快照是否有问题。

至于强制提款功能，我们将这部分模块搭建在Bool Network之上，可以在多条公链上通过智能合约来验证资产快照，确定你的确有xx数额的钱存放在Hibit平台，然后你可以把属于自己的钱从Hibit的托管钱包中强制抽离。更深层次的细节，涉及到负责快照验证的合约与Hibit的托管钱包如何交互，这块其实让Bool Network的人去说比较合适，我在这里就不展开了。

Faust：这里我有个问题，如何保证Hibit节点一定会往ICP和Arweave上发状态快照而不偷懒？

Witter：提交快照数据的事情有选定的节点来负责，只要这些节点去提交数据就行。这里要注意，Hibit验证节点们要先提交区块头，让ICP、Solana链上的Verifier合约确认一致，通过验证，然后专属节点再去往ICP、Arweave这些地方提交区块头对应的状态快照。如果经过很长时间都未提交，或是提交的快照和区块头不能对应，就会被Slash。

5. Faust：接下来请Chainswift介绍一下自己的项目？你们似乎做的是基于BTC的稳定币协议？你们的机制设计大体如何？

水牛：Chainswift做的事情其实就是让用户抵押BTC借出稳定币，类似于MakerDAO。但这种平台本质还是有资管属性，BTC需要质押到一个安全的地址，这是关键。Bool Network刚好可以提供这块的安全性，我们可以直接让Bool网络提供MPC/TSS服务，把BTC资产存放到由Bool网络托管的比特币Taproot地址。用户把BTC打到这个Taproot地址后，可以将这笔钱跨到其他平台，参与铸造稳定币等。这就是Chianswift大致的框架。

Faust：协议用到的预言机你们如何选择？

水牛：预言机说白了就是如何为指定平台提供BTC报价。一方面，我们可以去参考链上流动性比较强的DEX中WBTC的报价；另一方面，我们还要选出十几个节点，这些节点可以从链外的数据源取得报价。最后，我们通过中位数算法取得一个合理的值，其实和Chainlink的原理差不多。

但因为是链上报价，价格曲线肯定无法像CEX中那样精确到秒，大概可以精确到小时级别。如果价格出现了短时间内扎针，这种中位数算法会自动帮助抹平，这不会使清算机制出现问题。至于清算机制，其实和MakerDAO差不多。

6. Faust：最后还是聊聊Bool Network本身吧。据我所知，Bool Network分为两部分，主要部分是前面说的DHC备选网络，另一部分是类似于信标链的Bool Chian，专门为DHC备选节点做登记等偏管理的事宜。Bool Chain和DHC备选节点的准入门槛现分别是怎样的？

Jeffrey：Bool Chain是基于波卡Substrate框架搭建的普通POS公链。至于为何用Substrate，这是因为在POS链的共识算法里（单纯说共识算法），波卡的共识算法最去中心化，能够支持上千个节点；此外，基于Substrate可以直接复用波卡的很多成果，比如其比较完备的链上治理体系，这便于我们后续落地为DAO的模式。

Bool的DHC节点目前也只是基于资产质押的，只需购置一台带TEE硬件的设备即可，而且这个机器也是通用性的，成本也不高。虽然两种节点都需要资产质押，但为了保证去中心化，我们会让质押门槛尽量低一些。