Babylon上线 BTCFi赛道再思考

作者：Revc，本站

Babylon 平台宣布其比特币质押主网已正式启动。在首个阶段，平台设置了 1000 个比特币的质押上限，目前这一上限已全部达成。根据平台数据显示，已有超过 1.27 万名用户参与了质押，总质押价值超过了 1000 个比特币。

## Babylon是什么

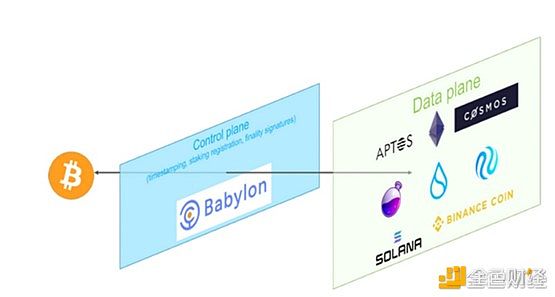
Babylon是一个旨在利用比特币的安全性来为其他PoS链提供安全保障的协议。Babylon可以为包括BTC layer2等PoS链提供安全、免跨链、免托管的原生质押解决方案，并促进跨链互操作性。通常被类比为以太坊生态的Eigenlayer。

### Babylon的工作核心原理

远程质押： 利用比特币的UTXO模型和脚本系统，实现对比特币的质押、罚没和奖励。

时间戳服务器： 通过在比特币区块链上记录PoS链的事件，为这些事件提供不可篡改的时间戳。

三层架构： 比特币作为底层，Babylon作为中间层，PoS链作为上层。Babylon负责将PoS链的检查点记录到比特币上。



### Babylon的优势

增强PoS链安全性： 利用比特币的安全性，提高PoS链的抗攻击能力。

缩短质押周期： 通过比特币的时间戳机制，缩短PoS链的质押周期。

促进跨链互操作性： 实现不同区块链之间的无缝通信和数据共享。

为比特币生态系统带来新的活力： 激活休眠的比特币，为比特币生态系统带来新的应用场景。

## BTCFi生态概览

目前比特币生态已经进入了大基建的阶段，各方争相涌入BTCFi赛道，毕竟该赛道有着价值近1.5万亿美元的资产待激活。以下是头部BTCFi项目的盘点：

### BounceBit

BounceBit 融合了 CeFi 和 DeFi，为比特币提供更灵活的收益方式。通过流动性托管和再质押，用户可以在多个链上获取收益。

核心功能：

CeFi+DeFi 结合： 将比特币存入 CeFi 平台，同时参与 DeFi 协议，获取双重收益。

流动性托管： 提供流动托管服务，让用户可以随时赎回资产。

再质押： 允许用户将质押的比特币再次质押到其他协议中，获取更多收益。

技术设计：BounceBit 通过验证者共识、Mainnet Digital 的托管服务以及 Ceffu 的 MirrorX 技术的多重安全机制，确保跨链资产的安全，降低了黑客攻击的风险。

### Solv Protocol

Solv Protocol创建了一种全链收益比特币资产 SolvBTC，将比特币的流动性引入各种 DeFi 协议。

核心功能：

SolvBTC： 一种代表质押比特币的衍生资产，可以在多个链上使用。

去中心化资产管理： 通过智能合约和多重签名，确保资产安全。

跨链互操作性： 支持在多个区块链上使用 SolvBTC。

技术设计：将各种流动性资源和投资机会集中到一个平台上，用户可以通过设置交易策略Vault，实现自动化投资。

### Yala

Yala 旨在打造一个多链稳定币生态系统，利用比特币的流动性。

核心功能：

多链稳定币： 提供基于比特币的稳定币，可在多个链上使用。

DeFi 生态： 提供借贷、质押等 DeFi 服务。

模块化架构： 灵活可扩展，支持自定义模块。

目前各方协议在安全方案上，较多采用了中心化的方式，即CeFi和多签，试图最大限度激活比特币链上的价值流动，因为UTXO等链上验证方式尽管是以去中心化保证安全，但是由于比特币上缺乏完善的智能合约系统，难以激发价值流动，而链上验证多用于再质押赛道。

## 比特币再质押赛道的思考

回到Babylon所处的再质押赛道本身，首先区块链主要通过模块化方式共享安全共识，模块化区块链通过“出租”比特币和以太坊等优质公链的安全性、去中心化特性和价值共识，为其他区块链提供基础设施，从而提高区块链的性能和效率。目前主要分为三类方案：

以太坊为基础的方案：

优点： 安全性高，合法性强，可直接利用以太坊生态资源。

缺点： 吞吐量和成本可能较低，不适合所有类型的应用链。

全新DA层方案（如Celestia）：

优点： 性能好，成本低，旨在提供与以太坊相当的安全性和去中心化特性。

缺点： 安全性和去中心化特性仍需时间验证，缺乏合法性，可能受到以太坊社区的排斥。

权益证明（POS）共享安全方案（如Babylon、EigenLayer）：

优点： 继承了比特币或以太坊的合法性和安全性，为其资产提供了更多实用价值，灵活性高。

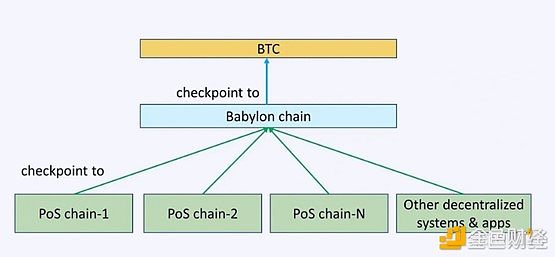
缺点： 相对较新，长期表现仍需观察。

Babylon采用的权益证明（POS）核心概念，利用比特币或以太坊的资产价值来创建共享安全服务。优势在于在继承合法性和安全性的同时还为主链资产提供了更多的实用价值，并且提供了更高的灵活性。但也由此引发了一系列的思考：

在以太坊网络中，一般质押者的安全责任要大于非质押者，因为质押中的ETH参与共识维护，而流通中的ETH其实是网络安全受益方，同时他们也付出了质押的机会成本。所以从共享安全性的角度来讲，权益证明共享方案目前低于以太坊的基础方案，除非权益证明方案的资产是stETH等资产，因为stETH对应以太坊网络中的参与验证的ETH，粗略的理解为，以太坊网络安全，其他采用stETH质押的PoS网络也是安全的。

而Babylon的PoW+PoS的方案，安全性共享逻辑不够完善，首先比特币网络的安全维护系统主要人员是矿工，虽然矿工也是受BTC代币价值本身利益驱动的，但是质押在Babylon协议中的比特币持有人没有直接主动的维护比特币网络安全，也就没有直接将比特币网络的安全性传导给联通Babylon网络的Pos网络。在这里我们可以思考一下，是否安全的受益人也可以将安全保障传递给他人。也就是说整个PoS网络的安全性与比特币网络低相关，与比特币质押者强相关，所以我们要思考共享安全性是在资产层面的共享（更像是一种担保），还是网络层面的共享。

BTC质押者或者持有人没有主动的维护比特币和PoS网络安全，从Babylon第一阶段的设计上来看，比特币网络更像是被动的接收来自PoS网络的数据，实际上整体安全性更多的取决于Babylon的PoS网络本身。



而从数量上来看，第一阶段1000枚比特币所占比特币现有流通量极少的份额，在经济上，目前PoS链也没有共享比特币网络的安全性，而共享资产的安全性与共享资产所在网络的安全性是两个概念，这个还值得更深一步探讨。

此外在技术上，PoS的时间戳如何与比特币网络区块的时间戳协同，比特币网络出块时间是分钟级的，出块时间和交易确认有一定不确定性，而PoS网络确认交易的最终性是秒级的，随即产生了一个PoS与PoW的区块协同性问题。

## 小结

比特币网络是价值最大的去中心化网络，包括Babylon在内的BTCFi众多赛道项目，有潜力使得比特币网络成为整个加密行业的基石底座，为比特币生态系统带来新的可能性。

在发展的过程中，除了重点关注去中心化属性的继承外，因BTCFi项目涉及资金体量巨大，也需要高度重视协议和智能合约的安全性。