构建zkBridge跨链桥：B² Network如何用BitVM挑战机制落地双向管道？

和一些以中心化托管机构信用背书的BTC跨链解决方案不太一样，以“模块化B² Hub”、“BitVM挑战者模式”等为核心构建的BSquare似乎倾向于更Technical的方式。B² Buzz目前也已累计了超6亿美元BTC资产。那么 @BSquaredNetwork 如何基于zkBridge实现资产跨BTC到layer2的双向安全桥接？基于技术理解剖析下：

通常情况下，要实现两条链之间的资产安全跨链，最简单就是中心化托管机构撮合并统一管帐，但若要执着一种Technical的方案，就需要根据链原生特性做一些特别的设计：

-同构链跨链桥

“同构链”指代双边都支持智能合约的链，比如B² 和其他EVM- Compatible链之间的跨链，双边链可以基于统一的可交互操作通信标准，由智能合约控制资金的双向流动。存在两种资金管理模型：

1）智能合约管理流动性资金：可在链A和链B之上都建立一个开放透明的流动性池，两边池保持Mirro镜像管理模式，假定A链上有用户存入资产，资产会被锁在A链流动性池内，而B链上的流动性池则立即向用户释放镜像流动性资产。两边流动性池始终保持总量一致，有个中心化的服务器会监听两条链上的资金进出情况，并实时进行资产调度管理。

此种方案，需要双边链都存在一个跨链流动性池，这样才能保证资金的正常流动，如果A链流动性不足则该链上的用户就会停止跨链。不足之处是需要设计有效管理机制来防止双花和恶意攻击。

比如用户在A链和B链都有资产，且同时在A、B链都发起交易请求，万一监听出错，A、B链的资产池没做到状态同步，就有可能让两笔交易同时发生，用户等于多花费了池子内的非所属资产。

2）基于ZK技术底层管理智能合约状态：在A链和B链分别部署智能合约，再搞一条zkBridge跨链桥来负责跨链通信管理，当A链用户向B链发送交易时，A链智能合约会Burn掉一笔资产，然后生成ZK Proof证明传递给B链合约，B链合约在验证过信息无误后，在B链新Mint一笔资产。通过ZK技术在跨链环境下的信任机制来实现资产的跨链流通。

刚刚以10亿估值融资的 @PolyhedraZK 采用的就是此种方案，依靠智能合约和ZK技术，实现了多zkBridge主体的去中心化跨链解决方案。但此类方案仅适用于同构EVM链之间，若遇到BTC这种无法支持智能合约的链环境，就无法有效实施。

-异构跨链桥（BTC和EVM- Compatible链）

异构链通常又有BTC和EVM- Compatible链，以及EVM和非EVM链之间（SUI、Aptos等支持智能合约但标准和数据结构不统一的链），非EVM但支持智能合约的链，在此就不赘述了。难点是如何把zkBridge应用到和BTC主网的跨链桥上。B² 在处理资产流入和流出双向Channel跨链问题时，正面临这样的技术挑战；

1）从Bitcoin到B2资产流入时，B² 采用了Ployhedra提供的zkBridge跨链桥方案，具体而言：B² 公开了一个MPC+TSS可信安全多钱地址用来存入BTC资产，当zkOracle节点监控并记录到该资产的流入后，会将存入状态生成ZK Proof证明，比如交易金额、收款地址等信息，该证明会传递给部署在B² 上的AA智能合约，经合约校验ZK证明信息无误后，向用户在B² 链的地址Mint释放资产。

2）从B² 向Bitcoin 流出Withdraw资产时，B² 则联合Polyhedra特别定制了跨链桥。简单来说，当用户在B² 发起资产Withdraw请求时，合约会先把用户的交易请求在B² Hub中发起一个Proposal，经由其他Validators验证是否准予通过。

此前我在文章中分析了，B² Hub的Validators其实是二层链的共识管理者，当大多数选择了Approve投票等同于该资产提现请求是合法的，然后该投票结果会以ZK Proof形式传递到MPC+TSS多签地址上，由该地址直接向用户释放资产。

若用户提出了提币请求，还被Validator非法拒绝了，怎么办呢？由于B² Hub的节点之间都受BitVM挑战机制的约束，用户可以向B² Hub发起挑战，证明自己是一笔合法提币请求，此时验证节点会因执行了错误的决策而遭到惩罚。所谓特别定制，其实就是在zkBridge的基础上加上了B² 特有的BitVM挑战者机制，以此来确保资产向非智能合约平台流入时的状态处理安全。

以上

不难看出，模块化设计+特有的BitVM挑战者机制给了B² 诸多技术实践落地的可能性，对BTC layer2后续开发者处理类似资金跨链方面也有较大的参考意义。