跨链技术调研报告

1 跨链交易已有方案研究

1.1 Interledger

Interledger 是 Ripple 于 2015 年提出的跨链交易协议，简称 ILP。它提出的目标是作为所有账本的仲裁器，无论是分布式账本还是中心化账本，目前代码开发已经基本完全。Interledger 提供了两种交易的方式，atomic mode 和 universal mode。在 atomic mode 下，节点先选定公证人（notaries），然后发送者将资金发送到可信第三方的账户（escrow），然后 connector 将资金发入接收者所在链的可信第三方账户，之后公证人获取到接收者的 commit 后，通过 PBFT 达成共识，通知两条链上的可信第三方，由两条链上的可信第三方再将资金分别转到 connector 和接收者的账户；如果节点无法选定公证人，则进入 universal mode，在这一模式下，不再由公证人决定交易进行状态，而是假设参与者均为理性的，由利益驱使整个交易的完成。Interledger 的设计上有如下的问题：

- 需要选取公证人，且公证人无 membership change，无 weighting
- 资金的接收者必须在线才能完成交易
- 需要可信第三方 escrow
- 无跨链交易历史明细纪录

1.2 COSMOS

COSMOS 是今年 4 月份刚有的项目，由于是新兴项目，修正了不少 Interledger 的缺陷，同时 COSMOS 的技术文档对其机制描述并不清晰。根据有限资料的理解，它提供了一套通信接口 IBCP（inter blockchain communication protocol），能够完成原链上资金的锁定，并且再 Hub 链上能够完整跨链资产的交易。但是这个交易并不影响原链，只是维护 Hub 链上的多资产账户。

2 跨链交易方案的硬性技术指标

跨链交易能力对于区块链而言具有重要意义，它能够将传统的单独运行、机制各异的区块链项目连结起来，形成一张区块链的网络（a network of

blockchain）,达到互联互通、数字资产无障碍转移的效果。根据对跨链交易作用的认识，结合区块链去中心的特点和其应用场景的考虑，初步认为跨链交易方案应当达到一下五个技术指标：

- **对于 ad-hoc 网络的强适应性**

区块链是由通过 P2P 协议连接在一起的节点组成，每个节点地位平等，无中心节点，并且可以自由加入和退出。整个节点网络没有固定拓扑结构，是典型的 ad-hoc 网络。因此，跨链交易方案必须对应这样的网络环境具有强适应性，即在一定界限下，任意节点的加入和退出，都不会影响整个方案的正确性和完成度。某种程度上，要求这个方案有足够的“容错性”和“稳定性”。

- **无需可信第三方或者 trust setup 过程**

区块链的一个重要特点是去中心化，它之所以应用广泛，本质上就去将传统场景中的中心化节点去掉，降低了价值传输的成本。跨链交易方案是要将区块链连结起来的，因此它也必须遵守这一准则，无需可信第三方或者 trust setup 过程，否则系统建立的成本和跨链交易的成本都会大大增加，降低其实用性和适用性。

- **支持离线交易以及交易历史查询**

支持离线交易是一个高效交易方案的基本要求，可以为交易提供更多的灵活性。同时，作为跨链交易方案，也需要一套机制去纪录链与链之间的交易历史，并且保证是安全可信、不可篡改的。

- **通用性强，接入壁垒低，不会导致硬分叉**

高效的跨链交易方案应该保证任意的区块链，即使运行机制差异巨大，也应当能够在不改变原链技术指标情况下，完成跨链交易。因为改变原链技术指标会导致硬分叉问题，这无疑是很致命的，也会降低跨链交易的参与度。

- **完善的激励准则**

跨链交易可以认为是一个区块链服务，任意区块链加入跨链交易都可以认为是定制这样一个服务。参与跨链交易的主体需要提供必需的交易费，用以支付为

跨链交易提供算力贡献的主体。因此需要有一个完整而科学的激励体系去支持整个系统安全稳定运行，提高系统的鲁棒性。