Matrix跨链

## 跨链简介

我们可以把跨链也理解为一种协议，解决两个或多个不同链上的资产以及功能状态可以互相传递、转移、交换的难题。也就是说，跨链的存在，不仅是增加了区块链的可拓展性，还可以解决不同公链之间交易困难产生的“数据孤岛”问题。

**跨链的本质是在两条链上产生原子性的对等交易**

## 跨链技术的核心问题

1. 一个基本的跨链行为
   1. 有两条链，ChainA 和 ChainB，ChainA上的原生币为TokenA，ChainB上的原生币为TokenB
   2. Alice在ChainA上的账户为A[A]，在ChainB上的账户为B[A]，Bob在ChainA上的账户为A[B]，在ChainB上的账户为B[B]。
   3. Alice和Bob达成一致性协议，Alice要用10个TokenA换Bob的50个TokenB
   4. 跨链的结果要实现
      1. ChainA上：Alice的账户A[A]转10个TokenA给Bob的账户A[B]
      2. ChainB上：Bob的账户B[B]转50个TokenB给Alice的账户B[A]
2. 所以，在一个跨链行为中：
   1. 涉及两个角色，Alice和Bob
   2. 涉及两条链：ChainA和ChainB
   3. 涉及4个账户：A[A],A[B],B[A],B[B]，分别属于两个人和两条链
   4. 涉及两个方向的交易，在两条链上
3. 同时，跨链行为有以下特性：
   1. 任何一个链上的币种不会凭空消失，只是账户之间的转移
   2. 两个币种之间的交换价值是事先约定的
   3. 两个链上的交易要满足原子性，要么都成功，要么都失败
4. 所以，跨链的核心问题是原子性：
   1. 首先，要有互相信任的两个链的交易证明，保证交易的真实发生
   2. 其次，要有合理的确认时间，保证区块链的数据不会回滚
   3. 最重要的，要保证双方的交易确实原子性，要么都成功，要么都失败
   4. 最后，用户可以查询交易，钱包要有交易验证功能

## 跨链技术的两大核心问题

### 跨链交易证明

跨链交易证明基本分为两种：

1. 在A链上存储B链的跨链交易证明，目前网上有侧链、中继等方法
2. 公证人机制(Notary Schemas)：用一个或多个公证人来证明B链上的交易是合法的

一般来说，大多数链都是混合机制。交易证明也需要公证人进行公证

### 跨链交易原子性

跨链原子性也基本分为两种

1. 跨链原子性最有名的就是hash锁定。
2. 其次，就是中心化背书机制.

很多公链也是两种的混合机制。

## Matrix的跨链方案设计

### 跨链交易证明

Matrix有天然的validator集合可作为公证人，所以用公证人机制是首选，为了扩展灵活，我们也做混合验证机制，侧链+公证人机制

1. 首先，起一条侧链，来进行链间通信
2. 侧链要做的事情是：
   1. 首先，收集两条链上的关于跨链的交易，所以跨链交易要有唯一的标识
   2. 其次，完成与主链的交易验证通信，满足验证者的bft共识
   3. 再次，拥有辅助功能、发送交易等功能，辅助完成跨链
3. 侧链的运转需要有一定的安全性：
   1. 可以使用目前Matrix的验证机制，可以直接使用Matrix的出块流程及出块节点
   2. 可以产生新的公证人，公证人有押金

### 跨链原子性

可以根据实际情况使用hash锁定，或者背书方式。

参考内容：

https://blog.csdn.net/qq\_42204339/article/details/80506517