***Atomic Cross-Chain Swaps***

**需求**

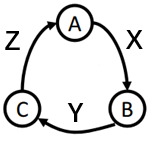
每种区块链都是一个独立的账本，不同的区块链是互不相关的。由于目前流通的数字货币已有超过2000种，区块链的用户对于“将一种区块链上的资产转移到另一种区块链上”的功能的需求正变得越来越迫切。而跨链技术的目的就是实现链间的互通互联。

**主要技术**

1. 公证人机制：Ripple的Interledger协议；
2. 侧链/中继：BTC Relay；
3. 分布式私钥控制：Wanchain、Fusion；
4. **哈希锁定**：闪电网络。双方HTLC的原子性已借由强连通图得到了证明。

HTLC（Hashed Time Lock Contract）：哈希时间锁定合约，包含“时间限制”和“强制执行交易”的机制，保证交易各方无法在合约签订后私自中断合约交易。

**一种不具备原子性的交易方案**

假设有三个希望进行交易的主体，每个交易方均有愿意卖出的资产Asset1和希望购进的资产Asset2，但A的潜在买家和B的卖家不是同一个，交易关系（或次序）呈环状，如右图，可视为强连通图。

记该图为G=（V，E），包含三个参数，**点的个数|V|=3**，**时间锁定值TL=6Δ**，以及三个交易方中**随机的某一个参与者**。假设它们的交易遵循以下规则：

1. A定义一个随机数s，计算其哈希值h=Hash(s)，然后根据哈希值h和时间锁定值TL=6Δ在自己的区块链上发布一份交易合约，用来将自己的资产X发送给B；
2. 当B确认A已经发布交易合约后，将用从A处接收到的哈希值h建立并发布一份自己的交易合约，其中TL=5Δ，合约用来将Y发送给C；
3. 当C确认B已经发布交易合约后，重复B的操作，但TL=4Δ；
4. 当A确认C已经发布交易合约后，将原始的随机数s发往C发布的合约处，要求获得资产Z，然后把s的值告知C；
5. C在得知s的值后，重复A的行为，获取需要的资产Y；随后B也重复C的行为，获取资产X，资产交换结束。

假如有一个交易方（比方说，C）试图在交易完成前**提前退出**交易，那么：

1. 在交易合约的部署期间（步骤1~3）退出，最终所有的合约都会因为TL超时而失效，资产X、Y、Z将原路退回；
2. 在某个交易合约被触发后（步骤4~6）退出，之前触发的合约（Z→A）仍旧有效，本应在之后触发的交易合约（Y→C，X→B）将因为收不到原始随机数s而超时，资产X、Y原路退回。最终B不受影响，C因中途退出而遭到“惩罚”。

合约的**发布顺序**和**时间锁定值**的设定也很重要。前者关系到交易链能够按顺序逐步完成；后者的恰当设定可以保证交易方有时间向下一个结点请求应得的资产，并传递随机数s，不至于因为时间不够导致交易链意外中断，造成资产损失。另外，假如A在步骤4确认前意外泄漏了s的值，它将遭受资产损失且无法获得想要的Z。

**一种原子交换协议**

1. **哈希锁（hashlock）与哈希解（hashkey）**

一种合格的原子交换协议应当满足：

1. 所有交易方都遵守协议时，资产交换将发生；
2. 当有参与者试图违反协议时，遵守协议的交易方不会有资产损失；
3. 不应该存在鼓励结盟并集体违背协议的内容。

能够证明，当且仅当图D是强连通图时，作用于图D上的统一交换协议是原子性的。

*统一/一致性（uniform）：称一个协议是统一的，假如它同时满足：a）所有交易方都遵守协议时交易正常执行并结束；b）有参与者串通违背协议时，守法交易者不会遭受损失。*

在简单的**两方交换**中，就如同上述交易方案规定的那样，每一方发布一份可以临时控制自己的资产的交易合约，其中包含两个值：哈希值h和时间锁定值t。假如在时间t内收到满足h=Hash(s)的正确的s时，合约被触发，其控制的资产将被不可逆地转移给对方；否则，资产将退还给原主人。

对于**多方交换**的情况，需要从数个方面扩展这些概念。

前面提到，每个结点（交易方）对应的入边（预计得到的资产）的时间锁定值TL与其出边（即将付出的资产）的TL的差至少为 Δ，确保在出边上的合约被触发后，结点有足够的时间触发对应的所有入边上的合约。

如果交易的强连通图**只有一个**leader，，那么由剩下的followers组成的子有向图是无环的，且每条边的时间锁定值 。

*leader：生成并传递随机数s的结点；follower：接收随机数s及其哈希值h的结点；*

*：图D中任意两个结点的路径长度的最大值；：两个结点的路径长度。*

如果存在**多个**leader，比如 ，每个leader 生成一个随机数 和对应的哈希值 ，并赋值给相应的边。每条边 上的 的解是一个三元组 ，其中 是原始随机数的值， 是结点 到leader的路径， 表示路径 中的每个结点都依次对 进行签名最后得到的结果。这个解将在交换协议启动后的 时间内有效。当一条边上的所有哈希锁 都在有效时限内解锁时，这条边上的合约才会被触发；当某个哈希锁的解全部超时，这个哈希锁才被视为超时。

*：表示结点 用自己的私钥对某个值 进行签名之后得到的加密的结果。*

1. **市场出清**

*市场出清（market clearing）：指商品价格具有充分的灵活性，能使需求和供给迅速达到均衡的市场。如果市场未出清，则一定存在短缺或过剩。*

为方便起见，假定交易有向图（swap digraph）由一个（可能中心化的）市场出清服务构建。每个交易方生成一个随机密钥 ，并把对应的哈希锁 以及希望进行交易的内容发送给这个清算服务。清算服务将合并所有的交易清单，构造并发布一个交易有向图，开始时间为 T。当所有交易方都确认并遵守协议时，全部的交易合约将在 前触发，否则将执行资产回退。

1. **合约**

涉及到的智能合约类似于面向对象编程语言中的类对象，它包含长期有效的状态属性，初始化这些属性的构造函数，一个或多个管理这些属性的函数。

这些状态属性记录了：a）等待被转移或退回的资产；b）有向图D；c）有向图中leaders的集合；d）准备转移资产的交易方；e）对应的资产接收方；f）一组时间锁TLs；g）一组哈希锁；h）一组记录对应的哈希锁是否已解锁的布尔变量。

管理函数中的unlock()将在有效时限未过，且三元组 全部正确时解锁对应的哈希锁 ；refund()和claim()分别由资产的发出方和接收方调用，用于资产回退或转移。

1. **Pebble Games**

*Pebble games：一种游戏。首先按一定的规则将卵石放在有向无环图G的顶点上。游戏的每一步，或者在G的一个空顶点上放置一个卵石，或者从前一个被覆盖的顶点上移除一个卵石。一个顶点只有在它的前驱结点都有卵石的情况下才视为被卵石覆盖。目标是以任意顺序依次覆盖G的每个顶点，并最小化同时出现在图上的卵石的数量。*

对于一个强连通图D和leaders集合L，pebble game有两种情况：

1. lazy：开始时，在leaders的所有出边上放置一块卵石。随后，假如某个结点的**所有**入边上都有卵石，则在其出边上也放置卵石；
2. eager：开始时，在结点z的所有出边上放置一个卵石。随后，假如某个结点的**任意**入边上有卵石，则在其出边上也放置卵石。

最终可以得到**结论**：两种情况下，图D中的每条边上最终都会有一块卵石，且这个过程将在游戏开始后的 时间内完成。

1. **协议**

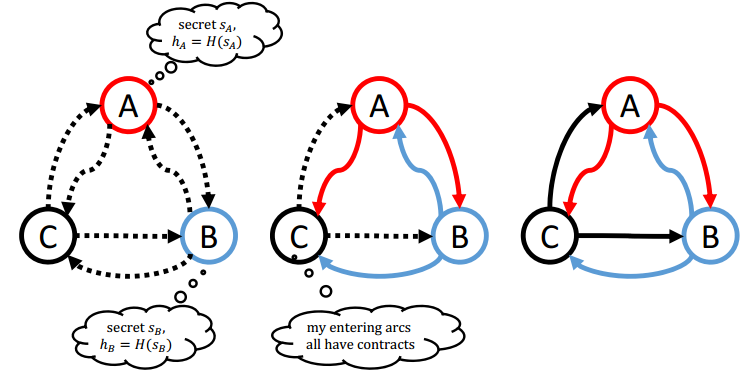
协议包含两个阶段。

**阶段1**：交换合约从leaders开始，通过图D进行传播。每个交易方监视入边上的合约状态，验证已发布的合约是否合法，非法合约将被丢弃。具体过程如下图所示。

协议——阶段1——对于leaders：

1. 在每条出边上发布合约；
2. 等待入边上的合约均被合法地建立。

协议——阶段1——对于followers：

1. 等待入边上的合约均被合法地建立；
2. 在每条出边上发布合约。

**阶段2**：交易方通过哈希解传播密钥s，其传播方向/顺序是资产接收方到发出方，与合约的建立相反。

在本阶段的开始，leader结点 对每条入边上的合约调用unlock()函数进行解锁，函数参数为 ，分别是哈希解、回退路径和签名结果。当其它交易方观察到自己的某条出边上的合约的哈希锁被解除时，该交易方 将在自己的所有入边上调用unlock()函数，函数参数为 。当哈希锁 超时或在全部边上被解锁，密钥 的传播过程即告结束。

一个简单的优化：使用一条共享区块链（比如清算服务所在的那条）作为广播中介。每个leader 将自己的密钥（即随机数） 发布到共享链上；followers监听这条共享链，用发现的密钥解锁入边上的合约。这样，我们就在follower到leader之间构造了一条逻辑通路，可以将协议的时间复杂度控制在 。但鉴于leaders未必会遵守这个规定，因此该优化不能完全替代原始设计。

我们可得到这样的**结论**：

1. 如果所有交易方都遵守协议，那么图D中的每条边都会在时间 内拥有一份合约，且每份合约都会在时间 内被触发。
2. 如果遵守协议的交易方 的某条入边上的哈希锁 超时，那么 的所有出边上的哈希锁 必定在此之前已经超时失效。因此守法的交易方不会遭受损失。
3. 对于图 和leaders集合 ，其空间复杂度为 ，其中 是图中合约的数量。
4. 在任何统一的基于哈希锁定的交换协议中：在入边上的合约全部建立完成之前，followers不能在出边上发布自己的合约。
5. leaders集合是图D中的一个反馈点集。

*反馈点集（feedback vertex set）：图D的点集V的一个子集，当从图中删去这个子集中的结点时，图D将变为有向无环图。*

1. **单leader有向图**

交易有向图中**只有一个leader**是上述内容的一种常见的特殊情况。

我们可以用普通的超时设定代替哈希解，减小传播信号的长度，并去除对数字签名的需求。令D指代一个交易有向图，它有一个leader 和哈希锁 。

我们可以得出结论：

1. 对于每个守法交易方 ，如果每条入边有时限 ，那么这个时限一定被设置得比出边的时限设定晚/多 Δ。
2. 对于使用超时设定的单leader有向图，如果某守法交易方 的入边的哈希锁超时，那么它的出边上的哈希锁一定也超时。
3. **问题**

寻找图D的最小反馈点集是一个NP-完全问题。

交换协议易受拒绝服务攻击。

要求交易有向图、leaders和哈希锁属于全体交易方的常识。

**跨链-概述**

**原理**

1. **嵌入式**

嵌入式解决方案需要把区块链互操作性逻辑集成到底层协议中。

时间和成本开销少。

存在安全隐患，可能会在区块链网络中引入新的攻击载体或安全缺陷。

1. **非嵌入式**

**难点**

1. **跨链交易验证**

区块链系统之间的信任机制，使得一个区块链可以接收并验证另一个区块链上的交易。

包含的问题：确认交易已经发生并且写入区块链账本

验证交易已经获得了系统中足够多区块的确认

常见验证机制：公证人机制、侧链/中继技术、Hash锁定技术、分布式密钥控制技术。

1. **跨链事务管理**

一个完整的跨链交易可以拆分成若干个子交易，每个子交易在各自所属的区块链系统中进行处理。这些子交易构成一个事务，需要跨链事务管理。

包含的问题：交易的最终确定性问题

交易的原子性问题

确定性问题：等待足够多的确认数：简单粗暴；事务处理的时间变长。

区块纠缠：令两个链之间的区块存有依赖关系，当一个链上的某个区块被撤销时，自动撤销其他链上的相关区块。

使用DPoS/xBFT等共识算法。

1. **锁定资产管理**

双向锚定是主链与侧链上的资产按照1:1兑换比例双向转移的过程。

包含的问题：由谁来管理锁定账户并执行锁定和解锁等操作

如何保证锁定资产被安全地释放

如何保证两条链的资产总量不变

常见方案：单一托管人模式、联盟托管模式和智能合约模式。

1. **多链协议适配**

多链互联互通蕴含着两层含义，一是已经存在的区块链系统如何实现互联互通 ；二是对于要开发的区块链，如何为其互联互通做好铺垫和准备。

多链跨链方案：主动兼容型方案：自上而下进行，主要针对已有的区块链系统。

被动兼容型方案：自下而上进行，主要针对尚未开发的区块链系统。

1. **跨链安全保障**

当两个系统发生交互时，难免会对彼此产生影响，若是链间安全无法隔离，那么如果一条链遭受攻击，将影响整个跨链网络。

解决的方向：适度隔离、检测安全事件和保障跨链交易正确性。

**主流跨链技术**

1. **公证人机制**

寻找双方都信任的中介。通过选举一个或一组可信节点作为公证人，对区块链Y上是否发生了特定事件进行验证，并向区块链X上的节点进行证明。

公证人机制分为中心化公证人机制和多重签名公证人机制，采用公证人机制的典型项目有R3推出的Corda和Ripple实验室提出的The Interledger Protocol (ILP)。

1. **侧链/中继**

侧链是验证来自其他区块链数据的区块链。通常将链X称为主链，将链Y称为侧链。当主链性能出现瓶颈或者某些功能无法扩展时，把资产转移到侧链上，相关交易就可以在侧链上执行，从而达到分担主链压力、扩展主链性能和功能的目的。

比特币在主链和侧链上的资产双向转移称为资产的双向锚定。双向锚定是侧链实现的核心原理。双向锚定实施的安全性取决于区块链中的激励机制，以使参与双向锚定的关键方能够真正执行双向锚定所应实现的功能。双向锚定技术可通过以下模式实现：单一托管模式、联盟模式、 SPV模式、驱动链模式和混合式设计。

中继模式适用于链接两个异构或同构区块链，是实现区块链互操作性的更为直接的方式。该模式不完全依赖于可信第三方的验证判断，仅通过中间人收集两条链的数据状态进行自我验证，其验证方式依据自身结构不同而存在显著差异。

侧链和中继的最基本需求就是采集原链信息。它们的区别在于 ：1）在从属关系上，侧链从属于主链，是主链与侧链之间去信任交互方案，且交易被限定在主链与侧链之间，更多地着眼于可拓展性而非可伸缩性 ；中继采用了中心辐射设计，不从属于某条主链，中继链更像是“调度中心”，只负责数据传递，不负责链维护。2）从执行过程看，侧链需要同步所有的区块头，验证区块链网络是否认可该项交易 ；中继不需要下载所有的区块头，因此拥有更优越的速度。3）在安全性方面，侧链的安全性建立在侧链能有效激励矿工进行交易一致性验证的基础上，主链的安全性无法在侧链上起作用 ；中继是由主链自行验证，安全性有一定保证。

比特币侧链：闪电网络、BTC Relay和Rootstock；非比特币侧链：Lisk、Asch和Loom Network；中继：Polkadot和Cosmos。

1. **哈希锁定**

通过资产锁定并设置相应的时间和解锁条件来实现公平交易。哈希锁定是系统之间进行原子交易的基本框架，能保障跨链交易的原子性，可拓展应用于中心化账本或去中心化账本的系统之间。

哈希锁定只能实现跨链的资产兑换，即各链资产总量保持不变的情况下，资产的持有人变化，无法真正将资产转移至另一条链上。对于资产转移，还需要配合其他跨链技术方可实现。哈希锁定项目如闪电网络。

1. **分布式私钥控制**

分布式私钥控制通过分布式节点控制各种资产的私钥，并将原链资产映射至跨链中，确保各种资产在区块链系统中实现互联互通。分布式私钥控制的核心在于分布式控制权管理，即资产的所有权和使用权的分离。类似于公证人机制，但用户始终拥有对资产的控制权，只是在存储数字资产的密钥上采用了分布式存储的方式。

适用范围广，易于实现。但由于不改变原链特性，跨链需要根据原链的特性适配开发，开发难度较大，且等待原链确认时间较长，致使运行效率偏低。分布式私钥控制项目有Wanchain、Fusion及EKT等。

1. **通信协议簇？**

指该跨链技术主要通过规定一系列通信数据格式与协议规范等实现区块链接入。

