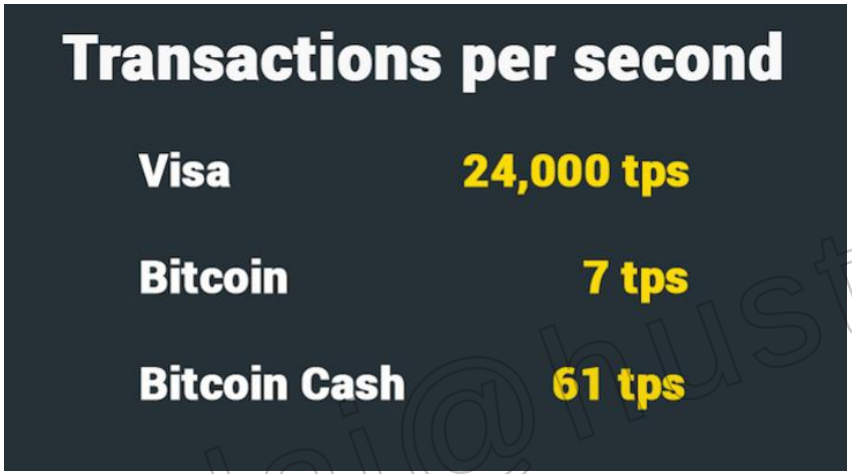
闪电网络

代炜琦

wqdai@hust.edu.cn
华中科技大学
Huazhong University of Science and Technology

比特币闪电网络（Lighting Network）



- 比特币的交易网络最为人诟病的一点便是交易性能：全网每秒 7 笔的交易速度，远低于传统的金融交易系统；同时，等待 6 个块的可信确认导致约 1 个小时的最终确认时间。
- 闪电网络的主要思路十分简单 -- 将大量交易放到比特币区块链之外进行。该设计最早是 2015 年 2 月在论文《The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments》中提出。

什么是闪电网络？

在历史的某个时刻，发送电报是最快捷，最有效的长途通信方式。为此，你必须前往当地邮局，填写表格并根据其中包含的信件支付费用。然后，该消息将被发送到最近的电报局，以便传送到远端。邮差然后将电报发送到目的地。

什么是闪电网络？

基本上，有很多人参与发送一条简短的短信，你必须付出相当多的钱。这几乎是比特币网络的当前状态。在这个类比中，闪电网络基本上像如果有一个你想要快速拨号交谈的人：只需要按“1”就可以让你朋友的电话响了。

什么是闪电网络？

简而言之，比特币闪电网络背后的想法可能听起来像这样：我们真的不需要每一笔交易都记录在区块链上。

相反，Lightning Network为比特币的区块链增加了另一层，使用户能够在该额外层上的任何两方之间创建支付渠道。这些渠道可以根据需要存在，并且由于它们是在两个人之间建立的，交易几乎是即时的，费用将极低甚至不存在。

闪电网络是如何工作的?

输入Danny和Jon。他们需要经常，快速且以最低费用向对方汇款。因此，他们在闪电网络上建立了一个频道。

闪电网络是如何工作的?

首先，Danny和Jon需要创建一个多功能钱包，这是一个钱包，他们可以用他们各自的私钥访问。
然后，他们都将一定数量的比特币（比如每个3比特币）存入该钱包。

闪电网络是如何工作的?

从这时开始，他们可以在两者之间进行无限制的交易。而且这些交易是存储在共享钱包中的资金的重新分配。

闪电网络是如何工作的?

例如，如果Danny想要向Jon发送1BTC，她需要将该金额的所有权转让给他。然后他们两个使用他们的私钥签署更新的资产负债表。

资金的实际分配发生在渠道关闭时。算法使用最近签署的资产负债表来确定谁获得了什么。如果Danny和Jon决定在一次交易后关闭频道，Danny将获得2BTC，而Jon将获得4BTC。

闪电网络是如何工作的?

只有在频道关闭后，有关其初始和最终余额的信息才会广播到比特币区块。因此Lighting Network的工作方式是它允许用户在主区块链之外进行大量交易，然后将它们记录为单个交易。

闪电网络安全吗?

Lightning Network的概念意味着系统将在区块链之上工作，但实际上并不具备其安全性。因此，它很可能主要用于小微交易。需要去中心化安全性的较大转账很可能仍将在原始层上完成。

最后，目前正在测试的Lightning Network的另一个有趣特征是交叉链原子交换，它是不同区块链之间的代币转移。简而言之，它是一种在不使用加密货币交换的情况下将任何给定的加密货币交换到另一种加密货币的方式。
最终，这项技术可能会使不安全的集中式加密货币交换以及与交易相关的麻烦都过时。比特币和莱特币测试区块链之间交换代币的第一个测试已经证明是成功的。

跨链

代炜琦

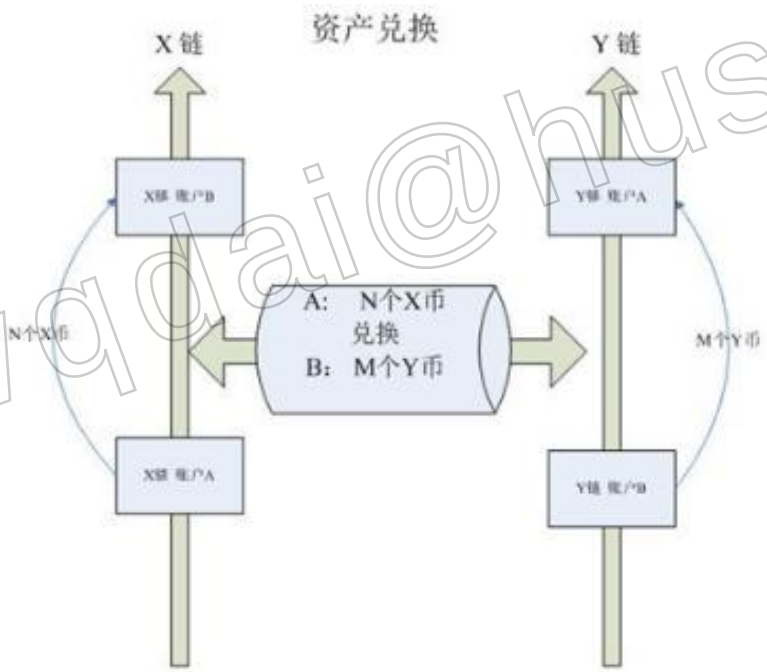
wqdai@hust.edu.cn
华中科技大学
Huazhong University of Science and Technology

跨链技术背景

区块链属于分布式账本技术的一种，每一条链都相当于一个独立的账本，通常情况下不同账本之间是无法实现价值转移的。随着技术以及市场的发展，加密货币的种类越来越多，与此同时也涌现出来大量不同的区块链。不同链之间的协同从操作以及价值流通成为了用户们的新需求，因此区块链的“跨链技术”应运而生。

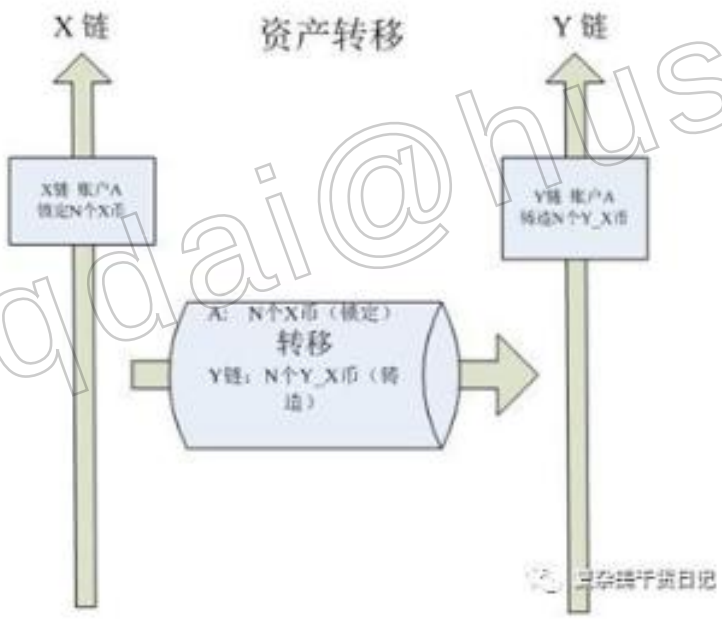
跨链基础需求-资产兑换

资产兑换：A想用X链的币（Token）兑换Y链的币（token），B想用Y链的币兑换X链的币，经系统撮合，两者互相兑换成功；



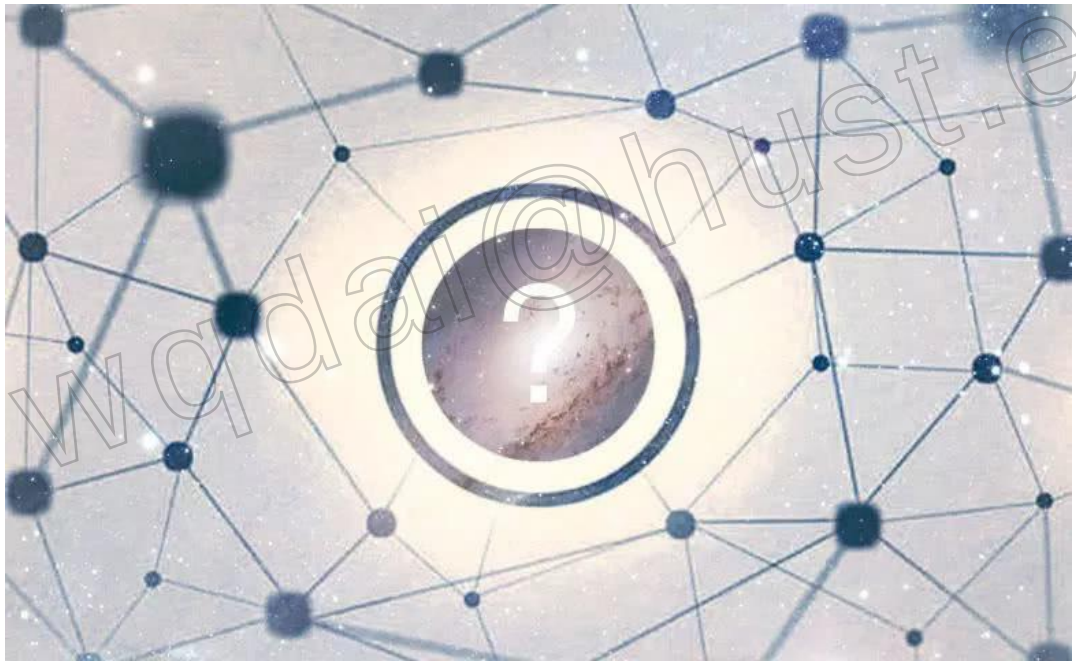
跨链基础需求-资产转移

资产转移：A想把X链的资产（币token）转移到其他区块链上，在x链上锁定，在新的链上重新铸造等量等值的币。



什么是跨链技术

所谓“跨链”就是指原本存储在特定区块链上的资产可以转换成为另一条链上的资产，从而实现价值的流通。



什么是跨链技术

也可以将其理解为不同资产持有人之间的一种兑换行为，这个过程实际并不改变每条区块链上的价值总额。就好比交易平台提供的币币交易一样，不同类型的数字货币之间可以进行兑换，只是交易平台的这一行为没有发生在区块链上而已。

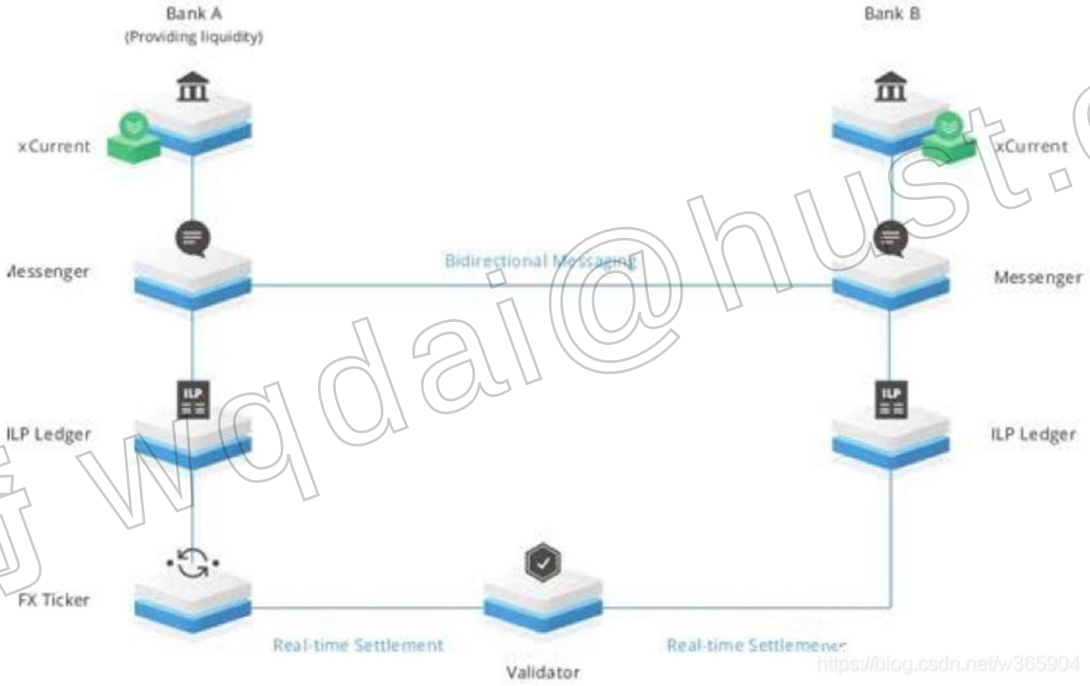
什么是跨链技术

从技术上来看区块链属于分布式账本，而从商业层面来看，它本质上属于一种价值网络，不同区块链之间的孤立性不仅导致了数字资产不能在区块链之间流通，同时也将其价值局限在了一个狭隘的范围内，一定程度上限制了其自身的发展空间。

主流的跨链技术

跨链技术-公证人机制

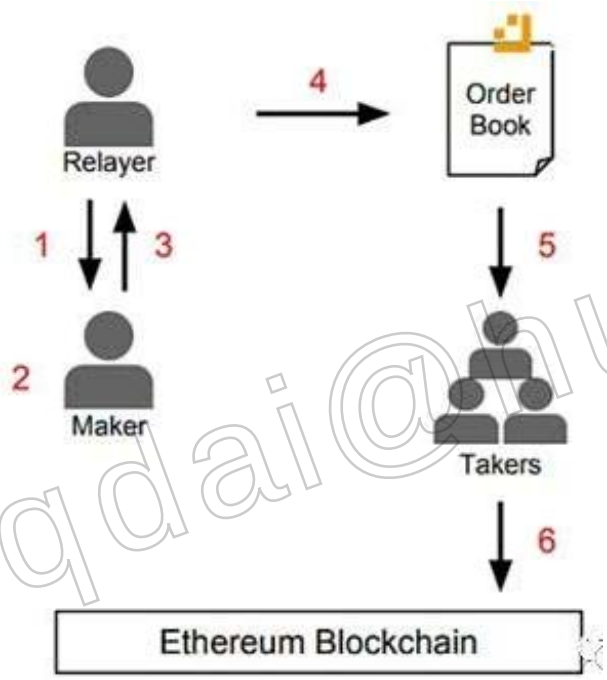
公证技术：瑞波Interledger协议



中心化或多重签名的见证人模式，见证人是链A的合法用户，负责监听链B的事件和状态，进而操作链A。本质特点是完全不用关注所跨链的结构和共识特性等。

跨链技术-公证人机制

去中心化交易所协议-0x协议



0x的技术实现中，引入了Relayer的概念。Relayer可以理解是任何实现了0x协议和提供了链下订单簿服务的做市商、交易所、Dapp等等。Relayer的订单簿技术实现可以是中心化的也可以是非中心化的。

跨链技术-公证人机制

去中心化交易所协议-0x协议

Relayer从成交交易中收取手续费获利。交易过程大致如下：

1. Relayer设置自身的交易服务费用规则，并对外提供订单簿服务；

2. Maker选定一个Relayer进行挂单创建和填充必要的订单，手续费信息，并用私钥签名；

3. Maker将签名后的订单提交给Relayer；

4. Relayer对订单做必要的检查，并将其更新到自身的订单簿；

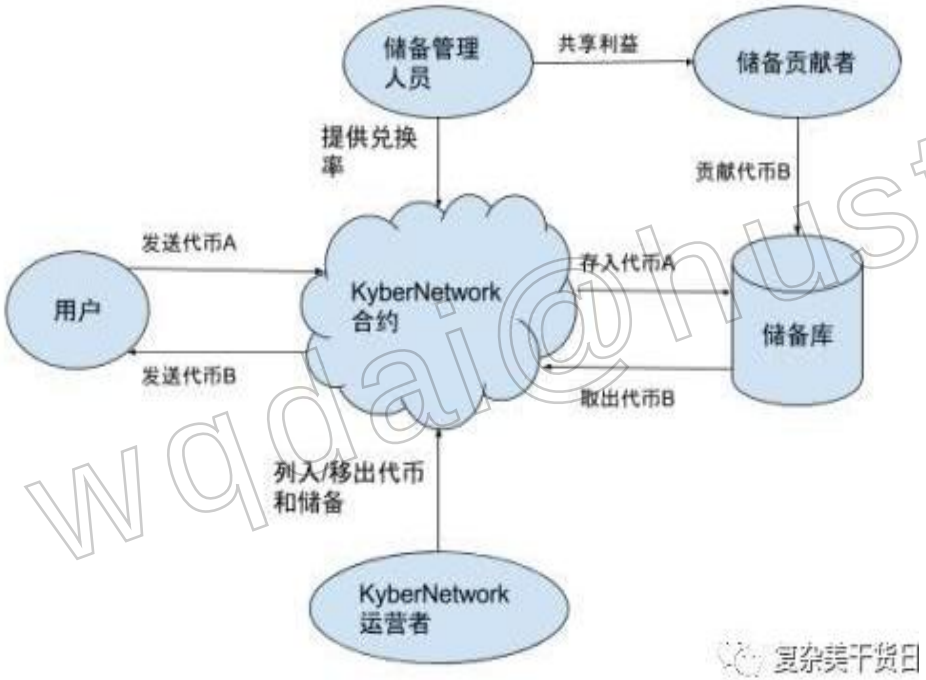
5. Takers监看到订单簿的更新，并选中成交订单；

6. Takers对选中的订单进行填充，并广播至区块链完成最后的成交。

注：Looping是0x的加强版，可以自动完成多环路撮合交易。

跨链技术-公证人机制

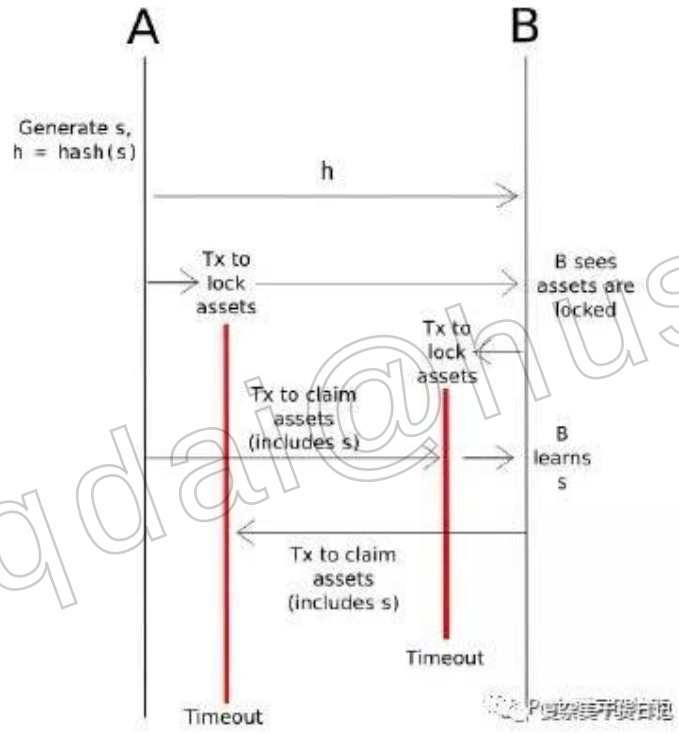
去中心化交易所协议-Kyber网络



Kyber引入了储备贡献者的角色为代币储备库提供代币，引入了储备库管理者来管理运营储备库。储备管理者负责周期性设置储备库兑换率，并利用储备库对普通用户提供的兑换折价来获取利益，储备库与储备库之间是互相竞争关系，以保障给用户提供最优的兑换价格。

跨链技术-哈希锁定

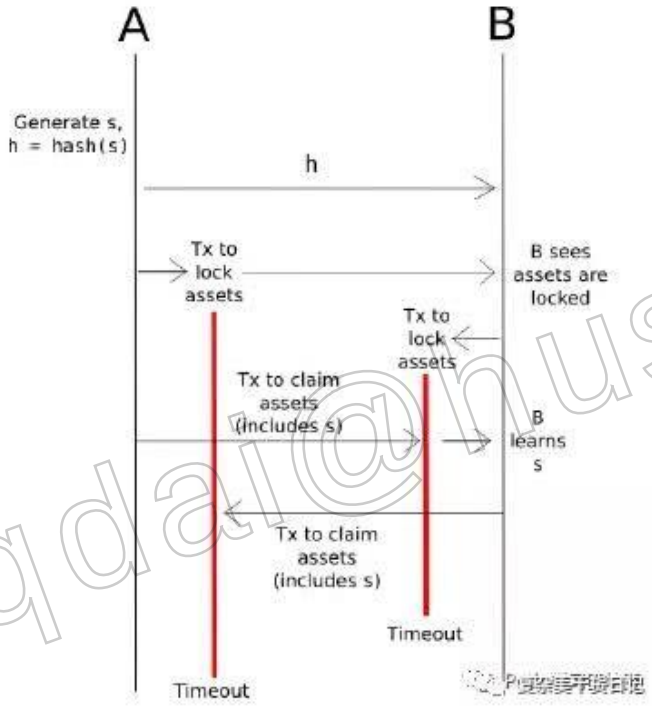
使用Hash-locking来实现20ETH和1BTC的原子交换



哈希锁定起源于闪电网络的HTLC（Hashed TimeLock Contract），如今也使用较为广泛。它实现的过程如下：

跨链技术-哈希锁定

使用Hash-locking来实现20ETH和1BTC的原子交换



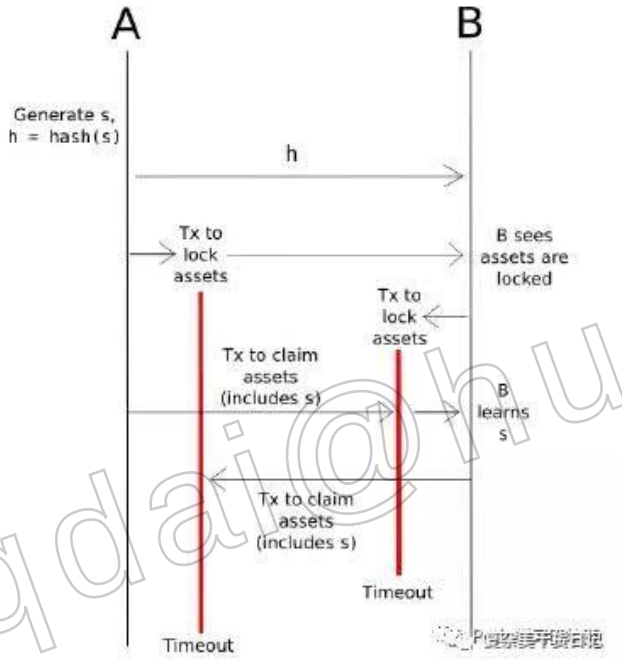
例如使用Hash-locking来实现20ETH和1BTC的原子交换过程:

1.A生成随机数s，并计算h = hash(s)，将h发送给B;

2.A生成HTLC，超过时间设置为：2小时，如果2小时内B猜出随机数s，则取走1BTC，否则A取回1BTC；这里A用h锁住BTC合约，同时B也有相同的h。这样A和B都有相同的锁h，但A有钥匙s

跨链技术-哈希锁定

使用Hash-locking来实现20ETH和1BTC的原子交换



3.B在以太坊里部署智能合约，如果有谁能在1小时内提供一个随机数s，让其hash值等于h则可以取走智能合约中20ETH；

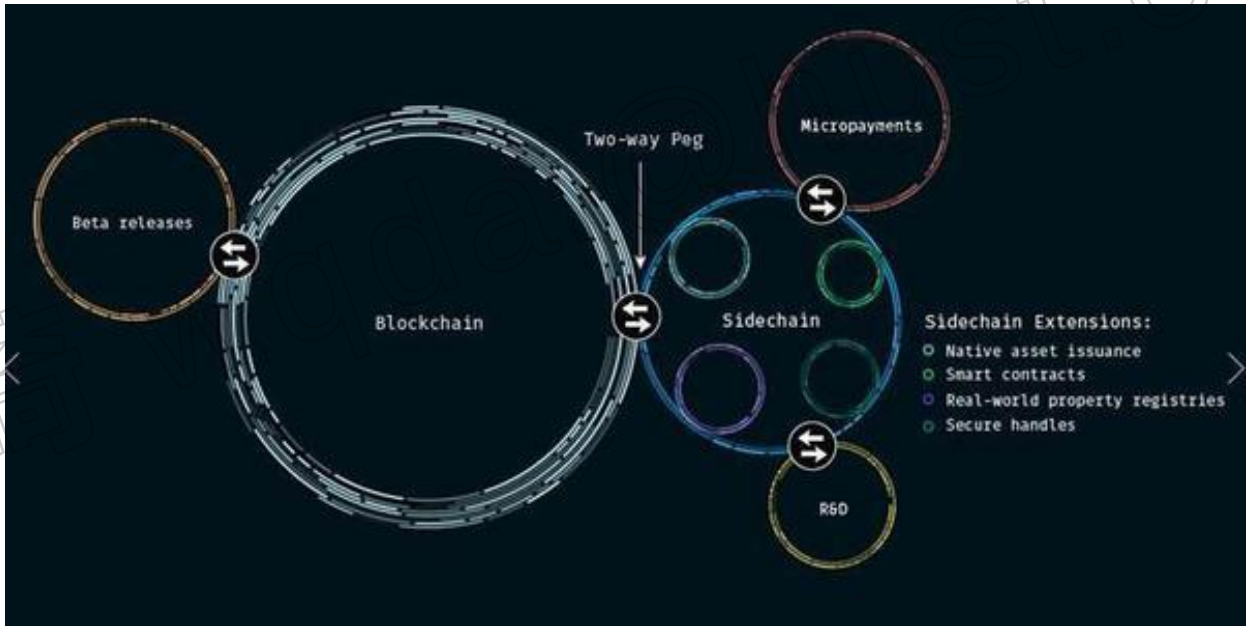
4.A调用B部署的智能合约提供正确的s，取走20ETH；

5.B得知s，还有1小时时间，B可以从容兑现A的HTLC的1BTC。
一旦超时，交易失败，符合原子性。

注意：这里引入时间的参数主要是为了，一旦时间超时，当前用户可以收回自己的币。不然自己的币可能被恶意无限制锁定。

跨链技术-侧链/中继

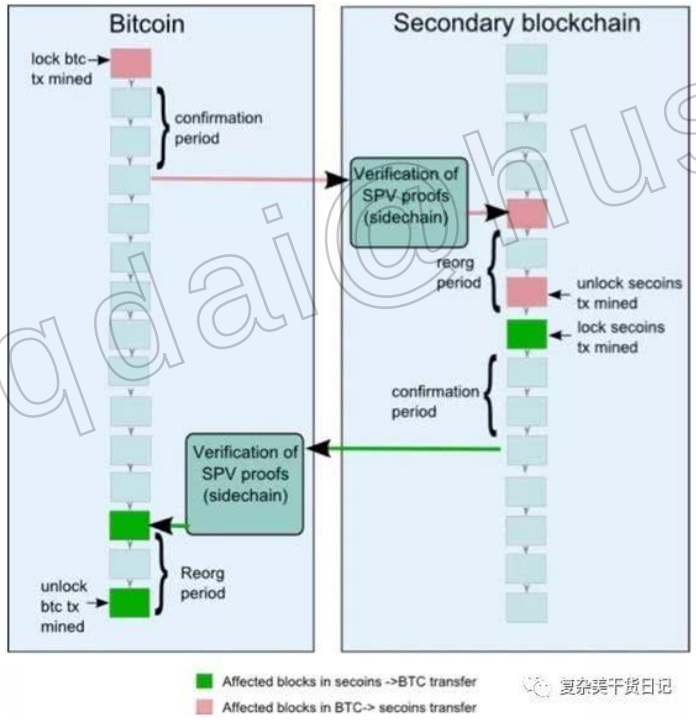
侧链系统可以读取主链的事件和状态，即支持SPV（Simple Payment Verificaiton），能够验证块上Header、merkle tree的信息。本质特点是必须关注所跨链的结构和共识特性等。一般来说，主链不知道侧链的存在，而侧链必须要知道主链的存在；双链也不知道中继的存在，而中继必须要知道两条链。



侧链Sidechains--RSK

侧链是以锚定某种原链上的代币为基础的区块链，如法币对黄金的锚定一样。

一个区块链系统性能能够理解其它区块链的共识系统，能够实现在获得其它区块链系统提供的锁定交易证明之后，自动释放比特币。可以用下图来描述：

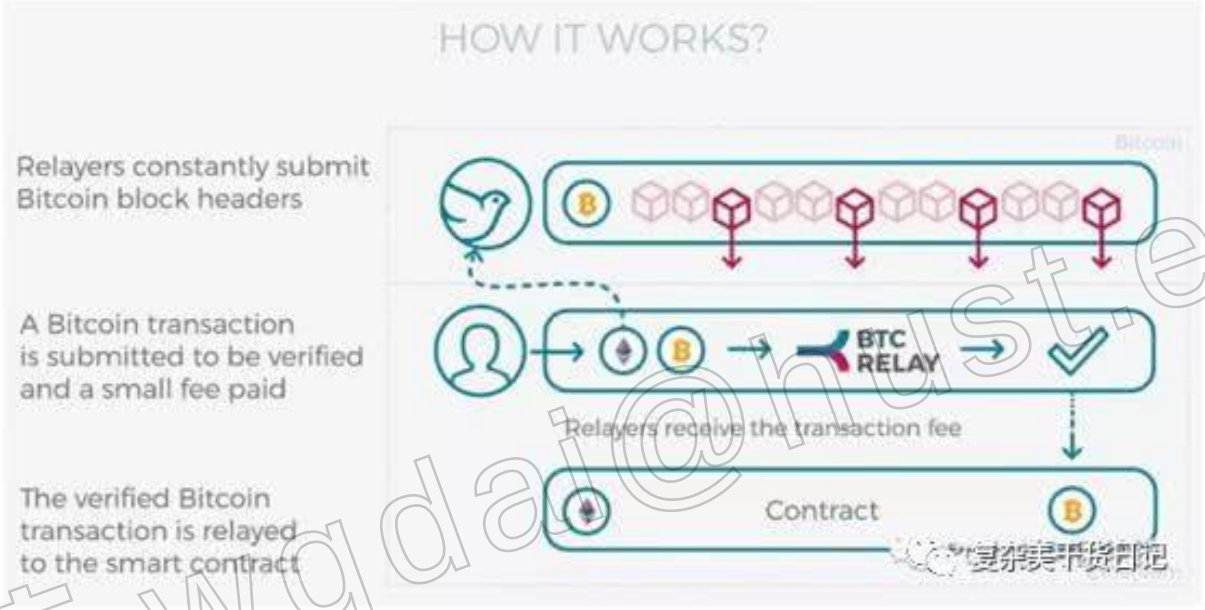


侧链是以锚定某种原链上的代币为基础的区块链，如法币对黄金的锚定一样。该技术最初是为了解决主链扩展性问题而想出来的扩容技术，每个区块链可以通过协议来实现强制执行的共识。

中继(Relays)—BTC Relay

BTC Relay是把以太坊当作比特币的侧链，与比特币通过以太坊的智能合约连接起来，可以使用户在以太坊上验证比特币交易。

中继(Relays)—BTC Relay



主要原理是BTC Relay利用BTC区块头在etherum上储存比特币区块头构建精简BTC区块链，类似SPV钱包，以太坊DApp开发者可以从智能合约向BTC Relay进行API调用来验证比特币网络活动。

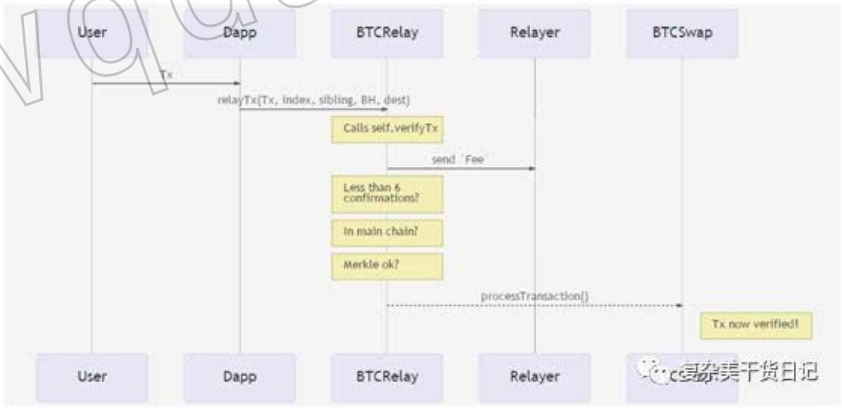
中继(Relays)—BTC Relay的使用场景

1.Alice和Bob同意使用BTCSwap合约来进行交易，Alice要买Bob的eth，Bob把他的 eth发送到BTCSwap合约

2.Alice向Bob发送bitcoin，她希望BTCSwap这个合约能知道这件事以便BTCSwap合约可以释放Bob之前的eth

3.Alice通过bitcoin的交易信息以及BTCSwap合约地址来调用btcrelay.relayTx()，btcrelay验证这笔交易通过后就触发BTCSwap合约里面的processTransaction方法

4.BTCSwap合约在被触发后确认这个btcrelay地址是一个合法地址，然后释放之前Bob的eth，交易完成。



中继(Relays)—cosmos

Cosmos是tendermint团队推出的一个支持跨链交互的异构网络。cosmos hub作为relay。Zone分区承担relayer角色，cosmos hub 承担verifier和relay的角色, 只传递消息，本身不作为一个链维护。

中继(Relays)—cosmos

什么是IBC?

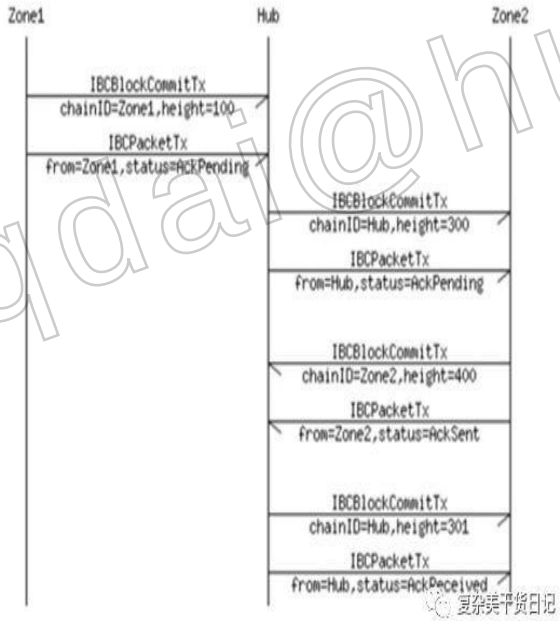
IBC是链间通信协议的缩写（Inter-Blockchain Communication Protocol）。通过数据包交换在多个不同的区块链网络之间转移数据和状态信息。最初的用途更多是通过IBC协议实现跨链通证转移。

IBC的目标是在两个独立的七层网络之间传递应用信息，所以需要链外的relay把数据包在链A和链B的网络之间做中继。链B收到链A的数据后必须能独立验证它所包含的证明信息，该证明代表了链A上的某个状态（及其对应操作）的真实性。为了让IBC协议能够工作，必须依赖基础的信任机制，要相信链A和链B里各自的共识算法，也要相信轻客户端验证，通过对区块头信息的验证，证明在区块链上曾经发生过的事情。

中继(Relays)—cosmos

什么是IBC?

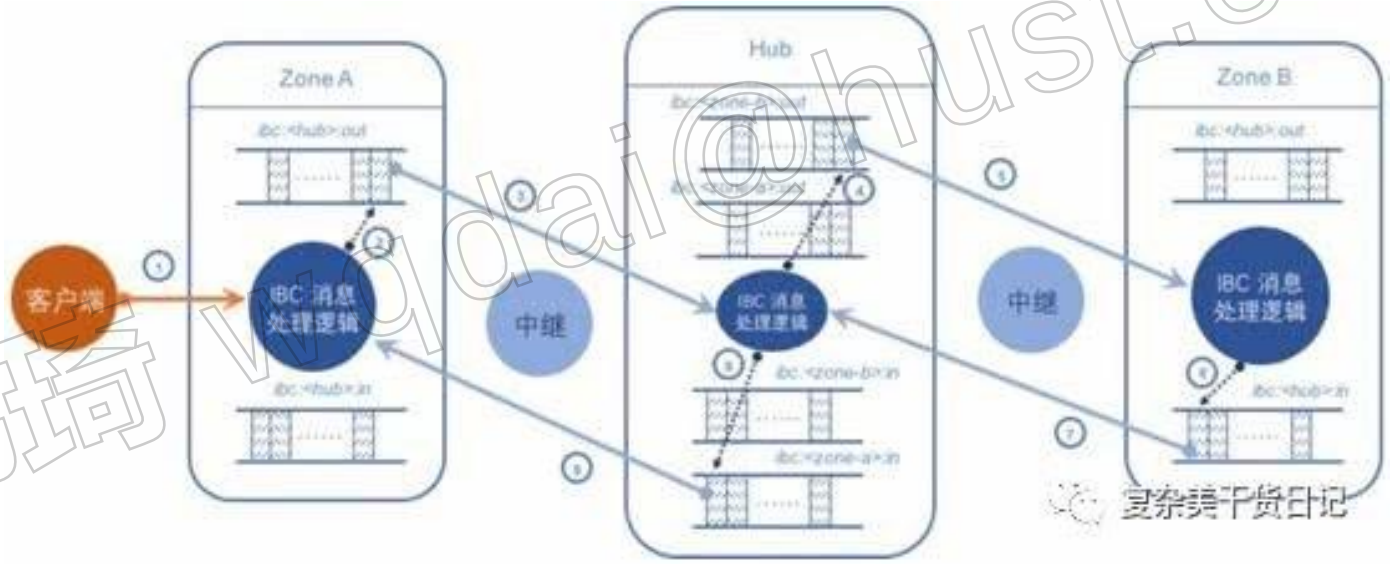
IBC协议定义了最主要的两个交易类型的数据包。一个就是IBCBlockCommitTx。它做的事情实际上就是把发起的这条链的当前最新的区块的头部信息传到目标区块链。这样的目标区块链就获得了当前最新的这个链里面Merkle Root。



中继(Relays)—cosmos

什么是IBC?

另外一个包的类型就是IBCPacketTx。这个就是传递了跨链转代币的交易信息，这个交易信息实际上是在消息体里面实际包含的payload信息。这个消息在原链上的一个Merkle Proof。

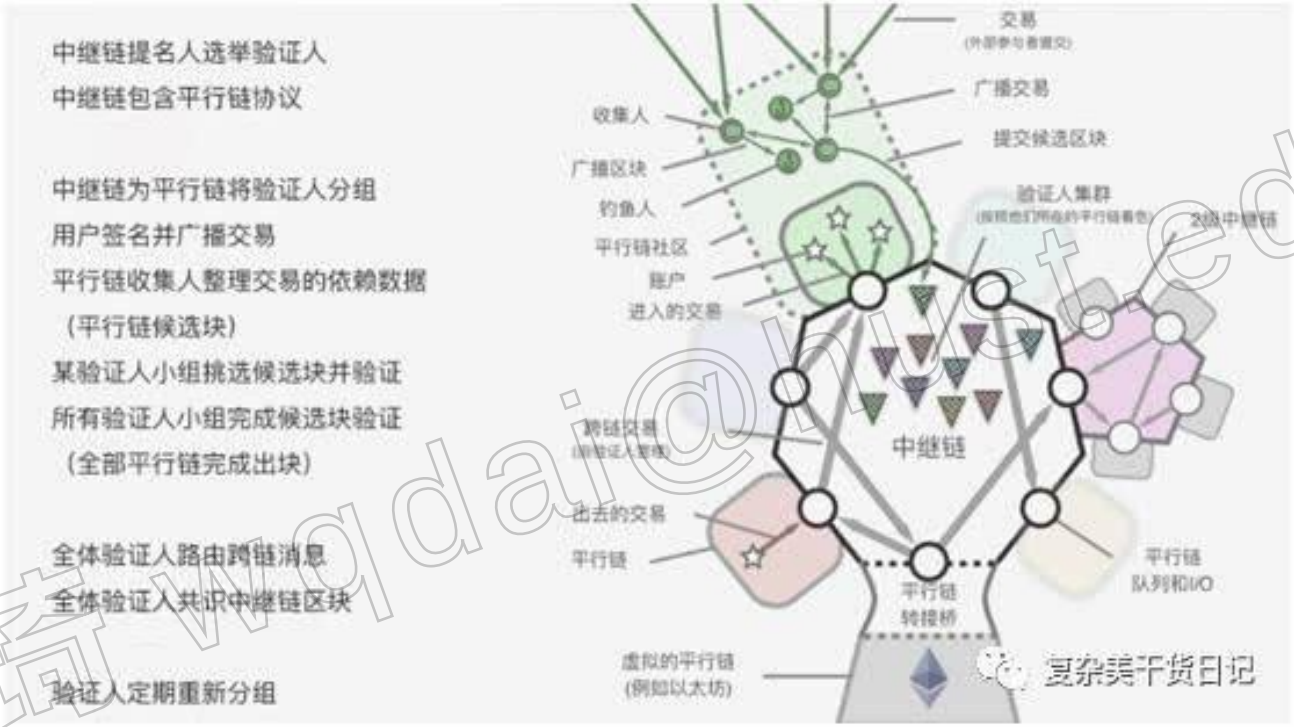


中继(Relays)-Polkadot

Polkadot技术是Gavin Wood 由以太坊核心开发Ethcore（Parity公司）开发的公有链，Polkadot计划将私有链/联盟链融入到公有链的共识网络中，同时又能保有私有链/联盟链的原有的数据隐私和许可使用的特性。

Polkadot基于Notary、**侧链**和**中继技术**，采用**多链融合**的设计模式parachains+relay-chain，兼具**拜占庭**和POS**的共识协议**来建立自己的技术路线。它将所有其它区块链都视为平行链，Polkadot为通过中继链（relay-chain）技术能够将原有链上的代币转入类似多重签名控制的原链地址中，对其进行暂时锁定，在中继链上的交易结果将由这些签名人投票决定其是否生效。
平行链（可并行化的链）是更简单的区块链形式，它附着在由“中继链”提供的安全性上，而不是由自己提供安全。之所以称之为中继链，是因为它不仅可以为平行链提供安全性，而且可以保证它们之间可以安全地传递消息。

中继(Relays)-Polkadot



Polkadot畅想了一种新的区块链形态，由单独的中继链去统一管理共识安全和数据交互，用百花齐放的平行链技术去满足各种应用需求，进一步分离共识和状态转换。

分布式私钥控制

各种加密资产可以通过分布式私钥生成与控制技术被映射到FUSION公有链上。

分布式私钥控制

多种被映射的加密资产可以在其公有链上进行自由交互。实现和解除分布式控制权管理的操作称为：锁入（Lock-in）和解锁（Lock-out）。锁入是对所有通过密钥控制的数字资产实现分布式控制权管理和资产映射的过程。解锁是锁入的逆向操作，将数字资产的控制权交还给所有者。

总结

早期跨链技术包括以瑞波和BTC Relay为代表，它们更多关注的是资产转移；现有跨链技术以Polkadot和Cosmos为代表更多关注的是跨链基础设施；新出现的FUSION实现了多币种智能合约，在其上可以产生丰富的的跨链金融应用。