目前的跨链技术

1. 状态通道

以太坊是一个全球化的基于交易的状态机，在链上的每一个交易都会产生新的状态，不同的是，状态通道在链外进行状态维护，在完成后参与多方签名确认后，才将最终结果上链。链上只进行结算处理，状态通道将部分流程移出到链外来提高区块链的效率，同时不会增加参与者的风险，目前状态通道的应用仍然是纯粹的支付通道，如闪电网络，旨在解决小额交易昂贵的手续费和极低的效率问题。

状态通道有许多优点，如提高并发、降低交易成本、原子事务操作。

但状态通道也存在较多的问题，如状态通道的维护成本高、链下状态维护，数据的不可靠和不安全性使得状态数据结算变得异常复杂。

1. Interledger协议

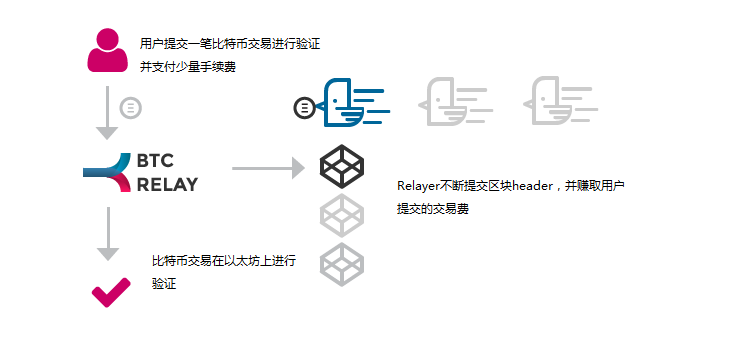
2012年，ripple实验室提出Interledger协议，旨在连接不同账本并实现他们之间的协同。Interledger协议适用于所有记账系统、能包容各记账系统的差异性。

Interledger协议使用第三方连接器或者验证器在不同记账系统之间自由的传输货币，但记账系统无需信任第三方，因为该协议采用密码算法在连接器为这两个记账系统创建资金托管，当所有参与方对交易达成共识时，便可交易。

1. 侧链技术

侧链是以锚定某种源链上的货币为基础的区块链，侧链连接各种源链，源链是完全独立存在的。侧链机制允许用户发送交易到其他区块链。

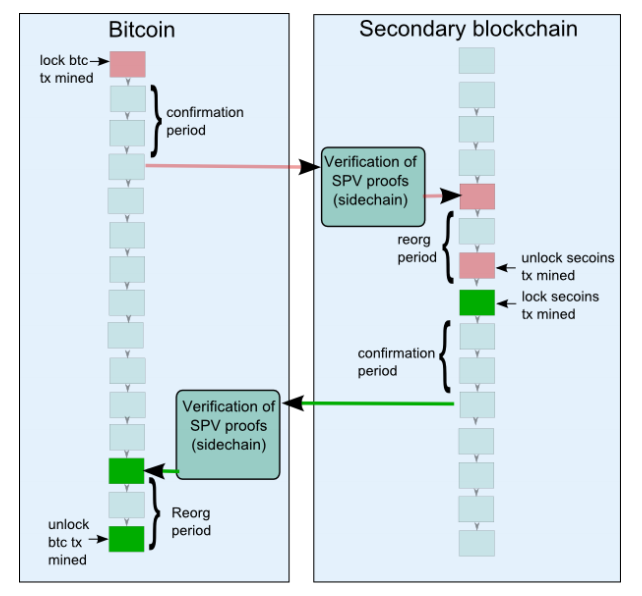
BTC Relay侧链主要原理是BTC Relay把以太坊网络和比特币网络以一种安全去中心化的方式连接起来，通过使用以太坊智能合约功能可以允许用户在以太坊区块链上验证比特币交易。这种侧链很难做到跨链智能合约，所以很难实现各种金融功能，这正是现有区块链在股票、债券、衍生品等领域尚未取得进展的原因，同时也只能进行支付验证，并不能向主链发送交易，依附主链进行，并不能解决当前区块链主要的性能问题，相反还增加了区块链交易拥堵问题。



双向锚定侧链

双向锚定技术经常被认为是一种将BTC转移到SBTC（智能比特币，这里我们可以理解为就是现在的侧链）的方法，反之亦然。实际上，当BTC被交换成SBTC，区块链之间并没有货币被“转移”。没有任何一笔交易实施了这个动作。 这是因为比特币不能验证另一条区块链上的余额属性。当用户打算把BTC转换成SBTC， 将锁定部分比特币在比特币区块链上，同时在RSK上释放等量的SBTC。当SBTC需要换回比特币时，再次在RSK上锁定SBTC，同时在比特币区块链上释放等量的比特币。通过安全协议保证相同的比特币不会在两条区块链上同时释放。

当比特币用户想要使用双向锚定时，他发送一笔交易到由联盟保护资金的多重签名钱包上。RSK区块链使用这笔交易中比特币相关的公钥来存储智能比特币（SBTC）。这意味着比特币区块链上控制比特币的私钥可以用来控制RSK链上的账户。



1. 中继技术

Polkadot将私有链和联盟链融入到公有链的共识网络中，同时保护私有链和联盟链原有数据的隐私和许可使用特性。

Cosmos是一个支持跨链交互的异构网络，cosmos上第一个空间叫hub，hub是一种多资产权益证明加密货币网络。Hub和各个zone可以通过区块链间通信（IBC）协议进行沟通，代币可完全快速地从一个空间传递到另一个空间，两者之间无需提现汇兑流动性，相反，空间内部所有代币的转移都会通过cosmos中心，它会记录每个空间所持有的代币总量。

1. 分布式私钥控制技术

WanChain万维链也支持主流公有链间的跨链交易，但首先需要完成在万维链上的注册，确保万维链能够对该链进行唯一识别。对于跨链交易，万维链利用多方计算和门限密钥共享方案。当一种未注册资产由原有链转移到万维链上时,万维链节点会使用一个基于协议的内置资产模板,根据跨链交易信息部署新的智能合约创建新的资产。当一种已注册资产由原有链转移到万维链上时,万维链节点会为用户在已有合约中发放相应等值代币,确保了原有链资产在万维链上仍然可以相互交易流通。

万维链通过分布式的方式完成不同区块链账本的连接及价值交换。它采用通用的跨链协议以及记录跨链交易、链内交易的分布式账本，公有链、私有链还是联盟链，均能接入万维链，实现不同区块链账本的连接及资产的跨账本转移。

但是，实现各种链映射到一条链上只是完成了第一步，如果上面的智能合约还是像现在的仅为交易触发，智能合约没办法实现分布式运算和多触发机制，那多币种智能合约能实现仍然是相当有限的功能。

三种跨链方式：

|  |  |  |  |
| --- | --- | --- | --- |
|  | notaries | relays | Hash-locking |
| Interoperability types | All | All(if relays exist on both chains;otherwise one-way causality only) | Crosss-dependency only |
| Trust model | Majority of notaries honest | Chains do not fail or get 51% attached | Chains do not fail or get 51% attached |
| Usable for cross-chain exchange | Yes | Yes | Yes |
| Usable for cross-chain asset protability | Yes(but requires universal long-term notary trust) | Yes | No |
| Usable for cross-chain oracles | Yes | Yes | Not directly |
| Usable for cross-chain asset encumbrance | Yes(but requires long-term notary trust) | Yes | In many cases, but with difficulty |

几种跨链项目特性对比

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | 事务类别 | 跨异构链 | 通信手段 | 并行 | 共识 | 特色 |
| Polkadot | 状态转移 | 是 | 区块链 | 否 | Pos+bft | 角色分工 |
| Aeternity | 状态转移 | 否 | 状态通道 | 是 | Pos+pow | 状态通道 |
| Anlink | 状态转移 | 是 | 区块链 | 否 | Ds+pbft | 链网络 |
| Interledger | 资产转移 | 是 | 中间人 | 否 | 哈希锁/中间人 | 信任的传递 |

1. 请求代理通信

其中唯一的问题是付款人和收款人能实际使用之间存在轻微的时间差。

多链上双方(或多方)智能合约和数字资产并没有明显的区别，存在同类的权限限制。

诸如金融领域的身份验证这类应用程序可能会涉及数字资产转账系统和身份管理系统之间的互操作过程，在这里进行异步处理并没有太大的问题。

原子化交易实施方案将需要处理一些特殊的案例，即双方尝试同时参与一笔交易，锁定机制和由合约生成的退款交易机制是处理这个问题最显然的策略了。

但基于区块链技术并实时处理交易的系统看上去是