目前区块链主要的跨链技术与其特点

在区块链所面临的诸多问题中，区块链之间互通性极大程度的限制了区块链的应用空间。不论对于公有链还是私有链来看，跨链技术就是实现价值互联网的关键，它是把区块链从分散的孤岛中拯救出来的良药，是区块链向外拓展和连接的桥梁。

区块链非常需要跨链的技术，以太坊创始人vitalik为R3撰写的报告中提及了三种方案，分别是公证人机制、侧链/中继器模式、哈希锁定模式。不过随着技术的进步，近年来涌现出了一些新的跨链解决方案，如分布式私钥控制技术、公证人机制+侧链混合技术等。

目前主流的跨链技术包括：

**1、公证人机制（Notary schemes）**

**2、侧链/中继（Sidechains/relays）**

**3、哈希锁定（Hash-locking）**

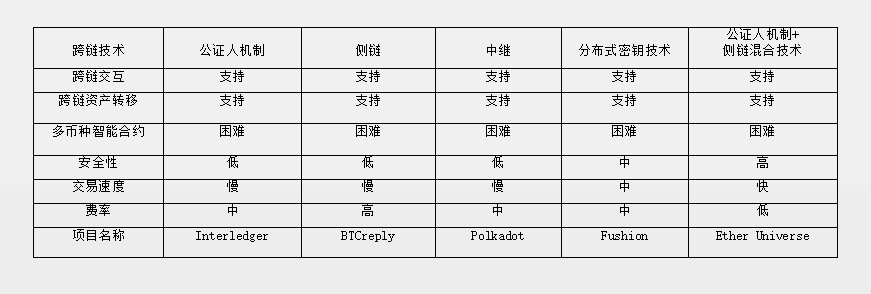
**4、分布式私钥控制（Distributed private key control）**

**5、公证人机制+侧链混合技术（Notary schemes+ Sidechains** **Mixing technology）**

列表比较一下：

<img src="https://pic3.zhimg.com/v2-e75746efecaeb37fa548fe44ff11f5b2\_b.jpg" data-caption="" data-size="normal" data-rawwidth="831" data-rawheight="495" class="origin\_image zh-lightbox-thumb" width="831" data-original="https://pic3.zhimg.com/v2-e75746efecaeb37fa548fe44ff11f5b2\_r.jpg">

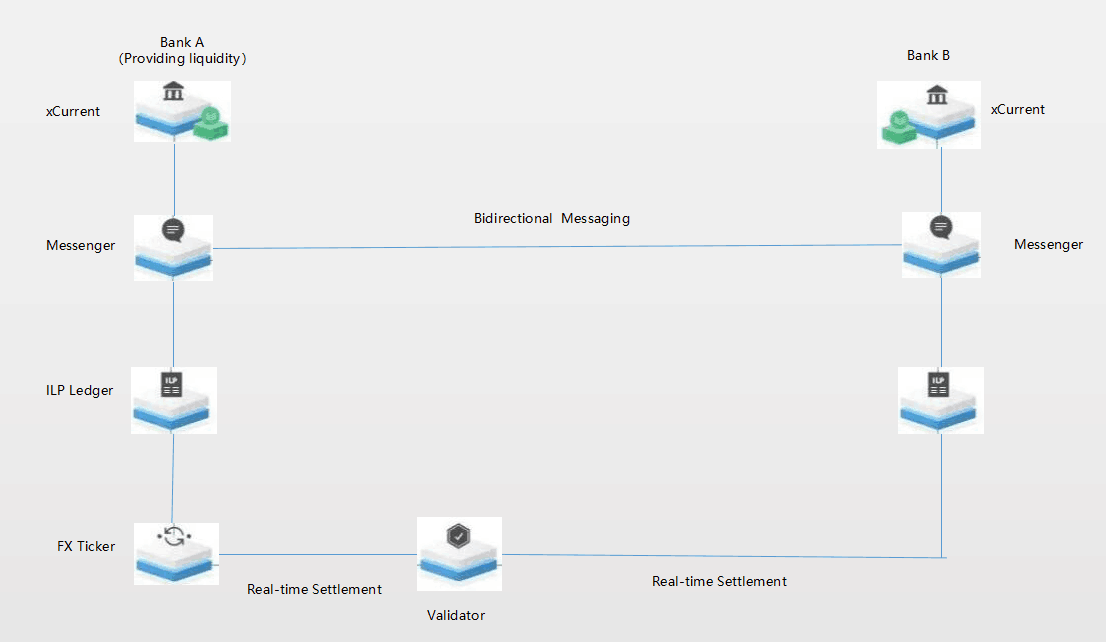
上表列出了各种跨链技术的基本区别，早期跨链技术以Interledger和BTC Relay为代表，它们更多关注的是**资产转移**；现有跨链技术以Polkadot为代表更多关注的是**跨链基础设施**；新出现的FUSION则强调资产**智能合约**的实现，Ether Universe强调的是**高性能、去中心化的跨链基础设施**，并接入各种跨链应用，侧重**商业落地**。



**1公证技术：瑞波Interledger协议**

在2012年，瑞波实验室提出 Interledger协议，旨在连接不同账本并实现它们之间的协同。

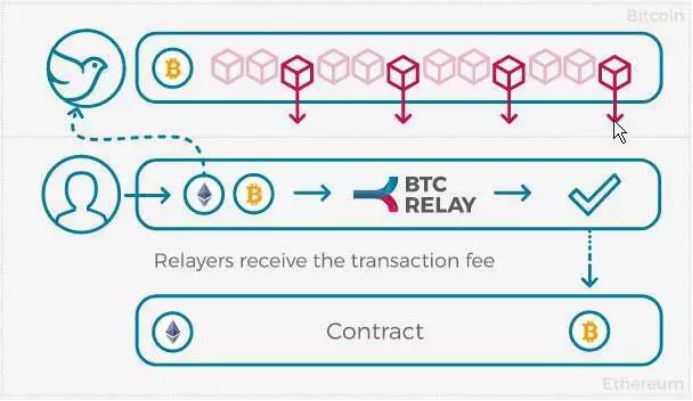
<img src="https://pic4.zhimg.com/v2-1fdc73d2f73bd13ee7a3002e5f209667\_b.jpg" data-caption="" data-size="normal" data-rawwidth="693" data-rawheight="436" class="origin\_image zh-lightbox-thumb" width="693" data-original="https://pic4.zhimg.com/v2-1fdc73d2f73bd13ee7a3002e5f209667\_r.jpg">



Interledger协议使两个不同的记账系统可以通过第三方“连接器”或“验证器”互相传输货币。

**2侧链技术：BTC Relay**

侧链是连接各种链，其它区块链则可以独立存在。

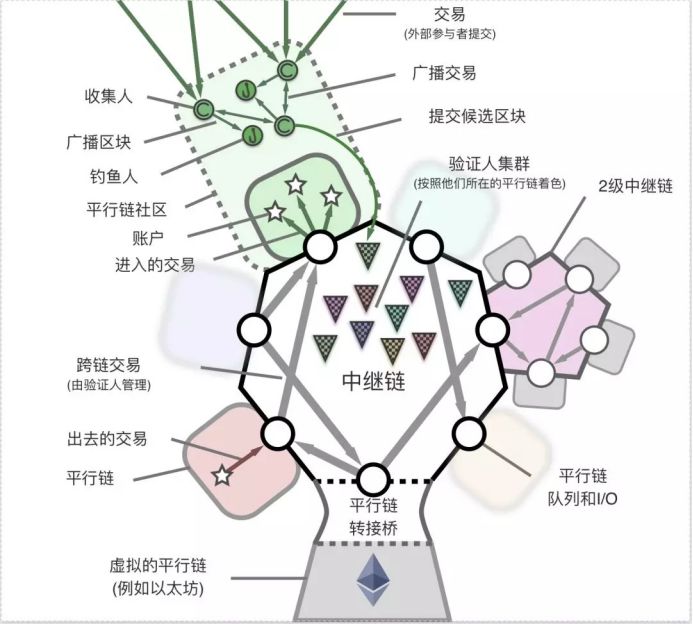
<img src="https://pic3.zhimg.com/v2-3122a815cbd4cee9a31c002d466760da\_b.jpg" data-caption="" data-size="normal" data-rawwidth="693" data-rawheight="401" class="origin\_image zh-lightbox-thumb" width="693" data-original="https://pic3.zhimg.com/v2-3122a815cbd4cee9a31c002d466760da\_r.jpg">

BTC Relay是在以太坊基金会支持之下诞生并成长起来的，属于早期的侧链技术。BTC Relay把以太坊网络与比特币网络通过使用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。

**3中继技术：Polkadot**

Polkadot为通过中继链（relay-chain）技术将原有链上的token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。

<img src="https://pic1.zhimg.com/v2-82a57e53e49dc2b6cef370d054cd42cc\_b.jpg" data-caption="" data-size="normal" data-rawwidth="693" data-rawheight="624" class="origin\_image zh-lightbox-thumb" width="693" data-original="https://pic1.zhimg.com/v2-82a57e53e49dc2b6cef370d054cd42cc\_r.jpg">

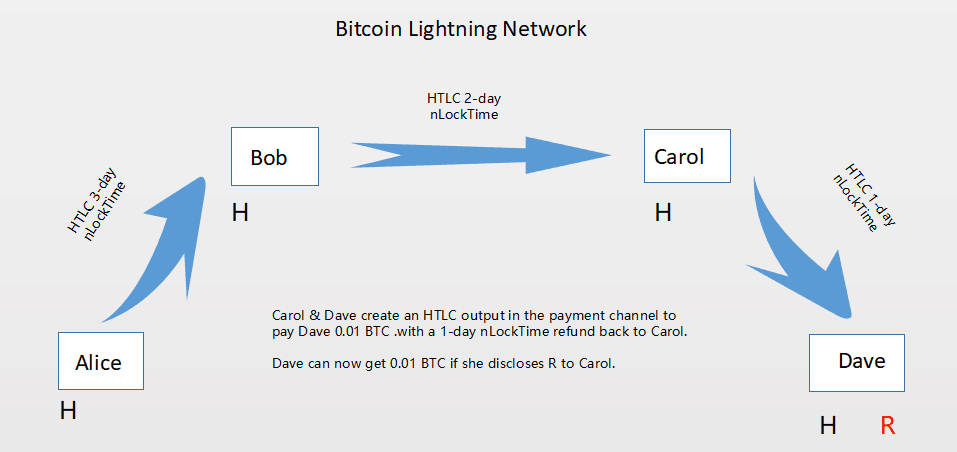


Polkadot目前还是以第二代区块链平台以太坊为主，实现其与私链的互连。

**4哈希锁定技术：Lighting network**

**闪电网络的关键技术是HTLC哈希锁定，**基本原理如下：Alice和Bob可以达成这样一个协议：协议将锁定Alice的0.1 BTC，在时刻T到来之前，如果Bob能够向Alice出示一个适当的R（称为秘密），使得R的哈希值等于事先约定的值H(R)，Bob就能获得这0.1 BTC；如果直到时刻T过去Bob仍然未能提供一个正确的R，这0.1 BTC将自动解冻并归还Alice。

<img src="https://pic3.zhimg.com/v2-e884db47c265164102ff3389ade447fa\_b.jpg" data-caption="" data-size="normal" data-rawwidth="682" data-rawheight="390" class="origin\_image zh-lightbox-thumb" width="682" data-original="https://pic3.zhimg.com/v2-e884db47c265164102ff3389ade4

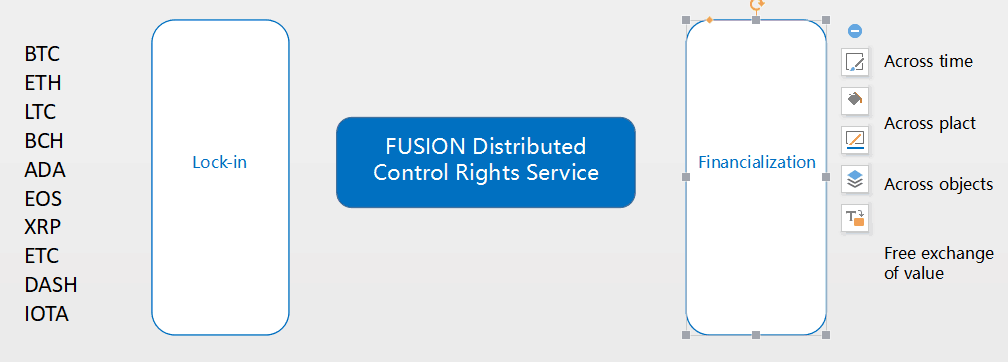
47fa\_r.jpg">

虽然哈希锁定能实现跨链资产的交换，但是不能实现跨链资产的转移，更不能实现跨链合约，所以它的应用场景比较受限。

**5分布式私钥控制技术：FUSION**

私密资产通过分布式私钥生成与控制技术被映射到FUSION公有链上。实现和解除分布式控制权管理的操作称为：锁入和解锁。锁入是对数字资产实现控制权和资产映射的过程。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。

<img src="https://pic2.zhimg.com/v2-a2e7831f46237ba3f8b907937a8f9275\_b.jpg" data-caption="" data-size="normal" data-rawwidth="675" data-rawheight="301" class="origin\_image zh-lightbox-thumb" width="675" data-original="https://pic2.zhimg.com/v2-a2e7831f46237ba3f8b907937a8f9275\_r.jpg">



**6公证人机制+侧链混合技术：Ether Universe**

Ether Universe是世界首个基于第三代区块链平台[http://EOS.IO](https://link.zhihu.com/?target=http://EOS.IO" \t "_blank)构建的跨链服务平台，采用公证人机制+侧链混合技术，侧链技术首先实现高效通信，而公证人机制实现快速价值交换，是一套创新的解决方案。

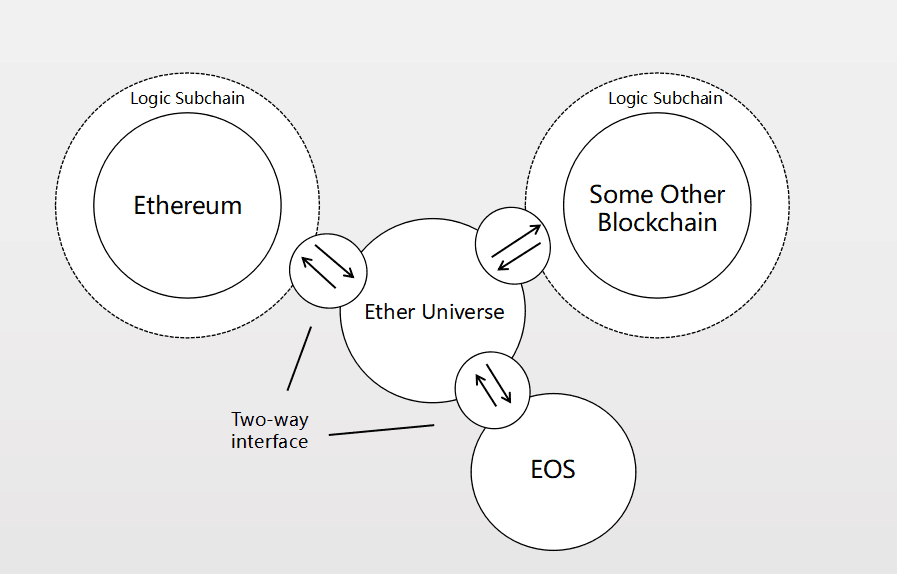
Ether Universe侧链技术实现以太坊网络与EOS网络通信原理如下：首先在Ethereum区块链上实现一个逻辑子链，逻辑子链是主链通过逻辑的方式形成，ETU通过逻辑子链与其他区块链主链进行双向锚定，实现锁定在内的关联操作，ETU通过EOS的区块链通信功能与EOS主链进行通信交互。（注：ETU为Ether Universe平台的token）

Ether Universe通过第三方“连接器”和“验证器”连接以太坊网络、EOS网络、其他网络，而分布式节点充当了连接器的作用。记账系统无需信任“连接器”，因为协议采用密码算法为这两个记账系统托管资产，当所有参与方交易达成共识时，便可相互交易。同时，只有参与其中的记账系统才可以跟踪交易，交易的详情可隐藏起来，“验证器”通过加密算法运行，因此不会直接看到交易的详情。

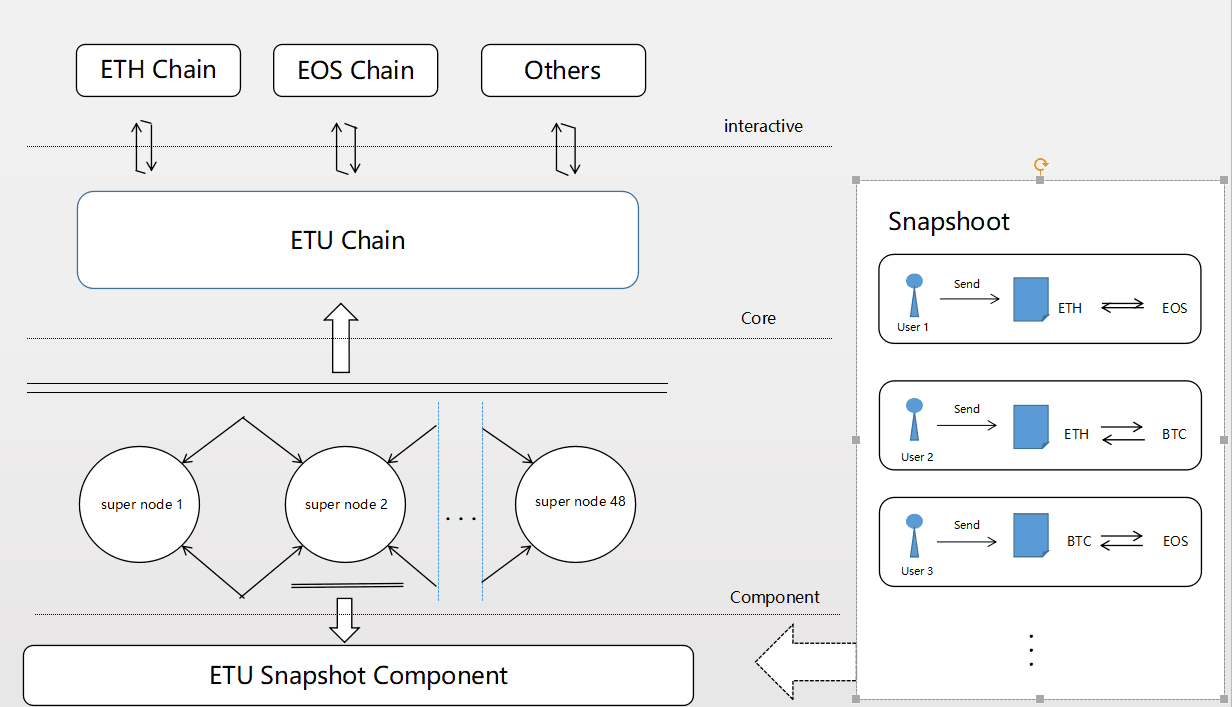
Ether Universe在全球布置48个超级节点，并联接受实时用户交易所产生的快照，并进行相应的数据同步以及数据认证。以太宇宙网络将验证每一个节点对其交易快照的判断，最终确认其交易的有效性，由于交易快照并联传输加上网络实时认证，以太宇宙交易可以在2秒至30秒（主要受网路延迟影响）内完成交易确认，使全球每一个服务设备成为相应的交易快照认证节点。

<img src="https://pic4.zhimg.com/v2-3bd6ab2e104e7ae90269e61d72900743\_b.jpg" data-caption="" data-size="normal" data-rawwidth="692" data-rawheight="414" class="origin\_image zh-lightbox-thumb" width="692" data-original="https://pic4.zhimg.com/v2-3bd6ab2e104e7ae90269e61d7290

0743\_r.jpg">



Ether Universe继承了EOS的优点，一秒可以承受百万笔实时交易并产生相应的交易快照，在交易确认后，执行相应的交易指令集。任何单一或者多个节点被黑客攻破，只要多数节点正常工作，仍能完成交易认证，保障交易顺畅进行。

<img src="https://pic4.zhimg.com/v2-edfb6b37ae7a6037c0dd6941e9368ee3\_b.jpg" data-caption="" data-size="normal" data-rawwidth="687" data-rawheight="387" class="origin\_image zh-lightbox-thumb" width="687" data-original="https://pic4.zhimg.com/v2-edfb6b37ae7a6037c0dd6941e9368ee3\_r.jpg">

Ether Universe构建的跨链基础设施，将会开放API和状态通道，供第三方开发者和商业应用接入跨链平台。

Ether Universe是跨链领域的后起之秀，相比Interledger等前辈，它是基于[http://EOS.IO](https://link.zhihu.com/?target=http://EOS.IO" \t "_blank)构建，“公证人+侧链”混合技术在性能上有天然优势，交易速度更快，每秒能承受10000笔交易量，每笔交易的手续费不足0.5元人民币，比同行低10倍左右，这让它在商业应用中具有碾压优势。