计算机

证券研究报告
2019 年 01 月 27 日

跨链技术——区块链大航海时代的基石

跨链概述

区块链技术发展至今，公链野蛮生长的同时，联盟链和私有链也疯狂涌现。然而，链与链之间高度异构化，作为一个孤立的价值体系存在，链与链之间互联操作的重要性日益凸显。跨链就是将同构或异构的区块链系统连接起来，实现资产、数据互操作，是区块链向外拓展和连接的桥梁。

跨链基础需求包括资产兑换和资产转移，但资产的传递不仅仅是一段数字代码信息的传递，在分布式系统中，传递过程中更需要实现精准记账。

跨链的技术实现

根据锁定验证方式不同大致分为四类：公证人机制、侧链/中继、哈希锁定、分布式私钥控制。早期跨链技术主要专注于资产转移，需要通过用户或第三方在链外进行更多的约定和操作，实现底层扩容。后期的项目则更为注重底层跨链基础设施，从区块链底层结构开始构造链结构的跨链技术。

当前跨链技术已然呈现百家争鸣，各辟蹊径态势，未来中继跨链技术比较可能率先出现大规模的落地应用，其可适用于多种场景并兼容异构区块链系统。当然，我们也不能以孤立的方式去评判每个跨链技术，未来可能会出现更优的跨链机制。

未来发展

去中心化交易所会将会是典型的最早跨链技术落地应用的场景之一，也可实现跨链资产抵押、托管、借贷、衍生品等金融应用。同时，跨链应用将逐步走出数字货币领域，实现链内与链外信息的交互，充分实现区块链的商业价值。

目前跨链技术仍处于初步探索阶段，尚未形成稳定体系，仍面临技术性能远远达不到应用的需求、对现有区块链系统的安全性存在一定影响以及落地应用较少等问题。未来跨链技术的发展在于如何实现区块链系统协同交互形成统一的整体，即需要满足生存性、兼容性以及灵活性三个基本条件。

风险提示：跨链技术处于早期发展阶段，存在技术发展的不确定性，面临极大的风险；对区块链行业的相关立法和监管政策尚未正式出台。

投资评级

行业评级	强于大市(维持评级)
上次评级	强于大市

作者

沈海兵 分析师
SAC 执业证书编号：S1110517030001
shenhaibing@tfzq.com

行业走势图

资料来源：贝格数据

相关报告

1 《计算机-行业研究周报:四季度机构持仓略有下降，抓住利空释放带来的投资机会》 2019-01-26

2《计算机行业研究简报》2019-01-23

3 《计算机-行业研究周报:继续重点推荐佳都科技、恒生电子》 2019-01-19

内容目录

图表目录

1. 跨链概述

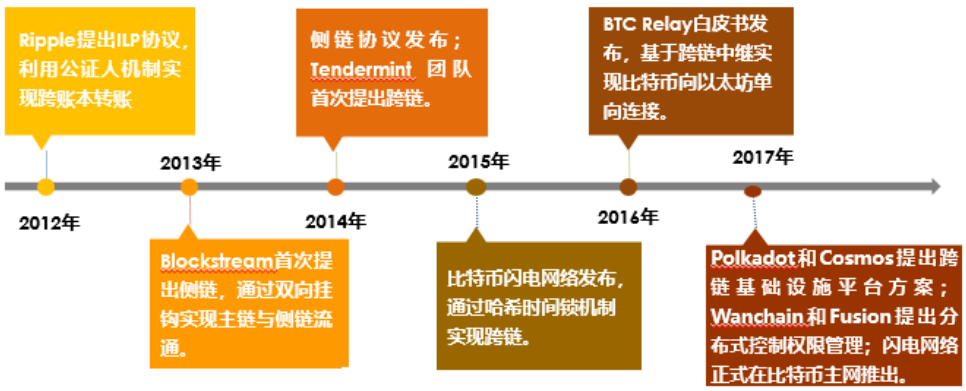
区块链技术发展至今，公链野蛮生长的同时，联盟链和私有链也疯狂涌现。然而，每条链都有一套独立的系统，链与链之间高度异构化，作为一个孤立的价值体系存在。为此链与链互联操作的重要性日益凸显，跨链的需求也由此而来。

跨链就是将同构或异构的区块链系统连接起来，实现资产、数据互操作。若对标互联网，如 20 世纪末通过 TCP/IP 协议连接全世界计算机形成的国际互联网带来的互联网的繁荣一样，跨链技术也将成为区块链实现价值网络的关键，在增加区块链的可拓展性的同时，是拯救分散孤岛的良药，也是区块链向外拓展和连接的桥梁。

1.1. 历史进程

跨链技术最早于 2012 年 ripple 发布的 Interledger Protocol 中出现，通过公证人机制实现跨账本转账，首次提出跨账本互操作方案。2013 年由比特币社区 Blockstream 公司首次提出跨链侧链方案，通过双向挂钩（Two-way peg）机制实现主链与侧链之间进行流通；2014 年 10 月侧链协议在白皮书《Enabling Blockchain Innovations with Pegged Sidechains》中公开。在侧链的理论和技术基础之上，2014 年 Tendermint 团队首次提出跨链（cross-chain）概念。2015 年比特币闪电网络（Lightning Network）发布，通过哈希时间锁（Hashed Timelock）机制，实现比特币链下快速交易通道。2016 年 BTC Relay 白皮书发布，基于跨链中继实现比特币向以太坊单向连接。2017 年，Polkadot 和 Cosmos 提出跨链基础设施中继平台方案。同年，Wanchain 和 Fusion 提出分布式控制权限管理实现跨链技术。2017 年 12 月，闪电网络正式在比特币主网推出，并完成第一笔交易。2018 年受制于技术难度以及整体市场环境的影响，跨链技术上未有明显突破性进展，多数项目仍处于开发阶段。

图 1：跨链技术历史进程



资料来源：时戳资本跨链研究报告，天风证券研究所

1.2. 整体市场情况

从整体情况看，跨链项目可以分为三大类：最早出现的跨链项目在设计上专注于交易和金融服务，借助跨链技术来提高区块链的拓展性或者实现跨链支付的功能；第二类跨链项目主要作为其他区块链的跨链基础设施，比如 Polkadot、Cosmos 等项目；最后一类是针对 DApp 提供模式化的跨链接口，为 DApp 实现多条链的兼容，这类跨链项目主要以 Ark、Arcblock 为代表。

从市场表现看，受数字货币市场整体环境的影响，在 2018 年跨链项目的跌幅都比较大，但其中仍不乏优质的项目，比如 Ripple。Ripple 旨在建立一个基于区块链的全球支付网络，

其提出了 Interledger 协议，用于和各大支付、银行、清算等传统金融机构之间，以建立相互链接，使得 Ripple 的底层分布式账本能和各大传统金融机构的中心化账本互联互通，目前 Ripple 的市值高达 129.87 亿美元，在数字货币市场中排名第二位，在跨链项目中排名第一位。当然，目前市场上还有大量的跨链项目目前面临经营困难，币值归零的风险。

表 1：2019 年 1 月跨链项目市场情况

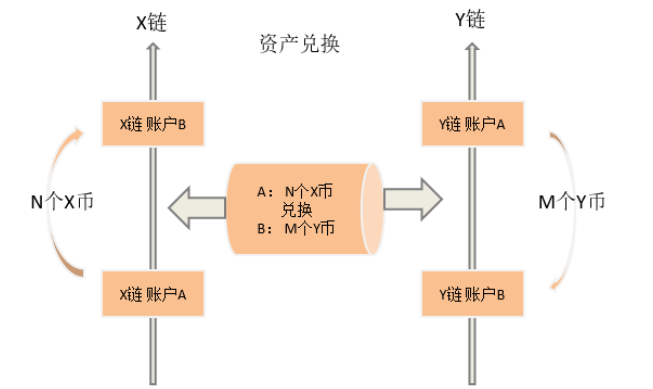
排名	名称	价格（美元）	流通市值（万美元）	近一年涨跌幅（%）
1	Ripple	0.3164	1298700	-81.66%
2	Stellar	0.1026	196400	-80.78%
3	Lisk	1.2240	14000	-95.20%
4	Bytom	0.0749	7506.52	-83.18%
5	Mixin	99.6200	4981.11	17.02%
6	Zipper	0.0003	4689.31	-30.38%
7	AION	0.1450	3975	-98.05%
8	Wanchain	0.3043	3260.24	-13.02%
9	Elastos	2.1391	3102	-87.53%
10	Aelf	0.1028	3084.7	-94.18%
11	LOOM	0.0450	2801	-78.37%
12	IGNIS	0.1624	1236	-98.72%
13	VTC	0.0237	1131	-96.08%
14	Fusion	0.3351	997.04	-83.80%
15	BLOCK	1.6200	896.8	-95.94%
16	ARK	0.0090	96.84	-94.59%
17	ICON	0.0095	0.5631	-95.83%

资料来源：非小号，天风证券研究所

1.3. 跨链的基础需求

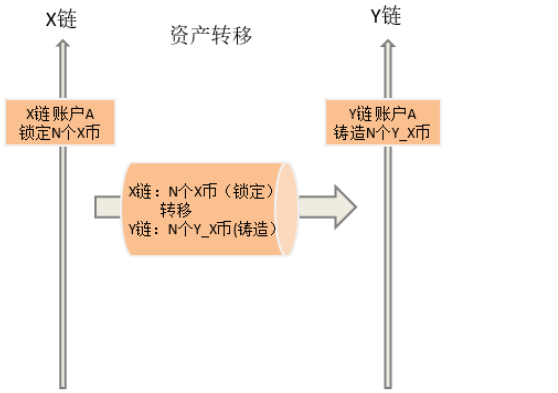
跨链基础需求包括资产兑换和资产转移。资产兑换即需要将一条链上资产（token）兑换成等值的另一条链上资产（token）。资产转移则是将链上的资产（token）转移至另一条区块链上，即需要将原有链上的资产进行锁定，并在另一条链上重新铸造等量等值的资产（token），以此来实现资产转移。资产兑换中每条链的资产总量是不变的，只是资产所有权发生改变，且所有权的变更需要同时发生；但资产转移是资产价值的转移，各链中的资产总量随着发生相应的增减。无论对于资产转移还是资产兑换，最重要的在于如何保障跨链交易的原子性，即交易要么成功，要么失败，不存在第三种中间状态。

图 2：资产兑换



资料来源：天风证券研究所

图 3：资产转移



资料来源：天风证券研究所

简单来看，跨链是解决如何让一条链上的资产转移至另一条链上，但资产的传递不仅仅是一段数字代码信息的传递，在分布式系统中，传递过程中更需要实现精准记账。在单一区块链中只需要解决在分布式系统下如何精准对账，但在两个或多个账本发生价值传递的时候，则需要在多个账本中同时更新数据，保持账本一致性，以此来避免双重支付等。

2. 跨链的技术实现

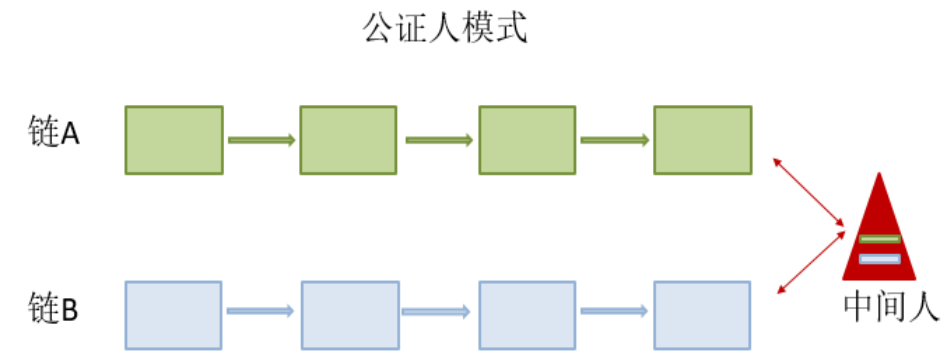
对于两条相互独立且较为封闭的系统，想要实现跨链，我们必须关注几个问题：如何验证原链上的交易状态？如何进行信息传递并确保传递过程准确及时？如何完成对另一条链的交易确认？如何防止双重支付？目前主要根据锁定验证方式不同大致分为以下四类：公证人机制（Notary Schemes）、侧链/中继（Sidechains / Relays）、哈希锁定（Hash-Locking）、分布式私钥控制（Distributed Private Key Control）。

2.1. 公证人机制

2.1.1. 公证人机制概述

公证人机制是在交易双方不能互相信任的情况下，选取双方共同信任的且相对独立的一个或一组节点来充当公证人作为中介来验证并确保交易的合法性。公证人作为双方的连接者，在链与链之间进行资产兑换或转移时，需要同时追踪两条链的数据状态并告知交易双方，而交易双方完全依赖于公证人传递的信息进行判断并实现交易。

图 4：公证人机制示意图



资料来源：火币区块链产业专题报告跨链篇，天风证券研究所

根据公证人的选取情况，可分为中心化/单签名公证人机制、多重签名公证人机制以及分布式签名公证人机制：

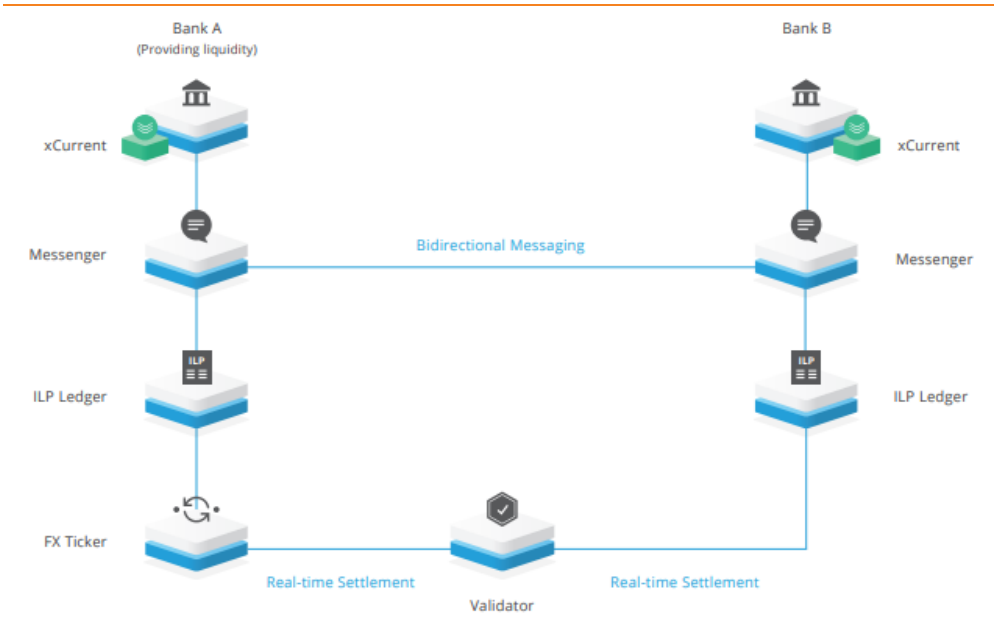
- 中心化公证人机制，即选取单一制定的独立节点或机构做为公证人，此为最简单的模式。
- 多重签名公证人机制，即需要由多个公证人在各自的账本上共同签名达成共识后方可以实现跨链交易。该机制改善了单签名公证人机制中心化的问题，提高公证人的可信度，但该机制要求交易链需同时具备支持多重签名的功能。
- 分布式签名公证人机制，即基于密码学生成秘钥，并拆分成多个部分分发给随机抽取的公证人，允许一定比例的公证人共同签名后即可拼凑出完整的秘钥。该机制的实现较为复杂，但也相对较为安全，降低了单点故障风险。

公证人机制是实现区块链之间互操作性中较易实现的一种，无需进行复杂的工作量证明或权益证明，易于对接现有的区块链系统。此外，该机制是较为中心化的跨链处理方案，其运行处理效率相对较高。但是，公证人机制存在中心化风险，即一旦公证人遭受攻击不可信，整体公证系统将停滞或处于较大的安全风险中，存在严重的单点故障风险。虽然业界提出了多重签名和分布式签名公证人机制弱化中心化风险，但仍有潜在的作恶风险，仅作为目前的一种权衡方案。

2.1.2. 案例：Interledger Protocol

公证人机制的最早应用在 2012 年 Ripple 提出的 Interledger Protocol 的早期版本，其旨在链接不同账本并实现协同。Interledger 协议是通过第三方“连接器”或“验证器”实现相互自由的转换资产，交易过程中的每一步都需要公证人的参与和确认。Interledger 协议通过拜占庭容错共识算法在一组公证人之间就交易事件达到共识，以此为基础进行多重签名发送交易信号。

图 5：Interledger Protocol 跨链运行机制示意图



资料来源：Ripple 白皮书，天风证券研究所

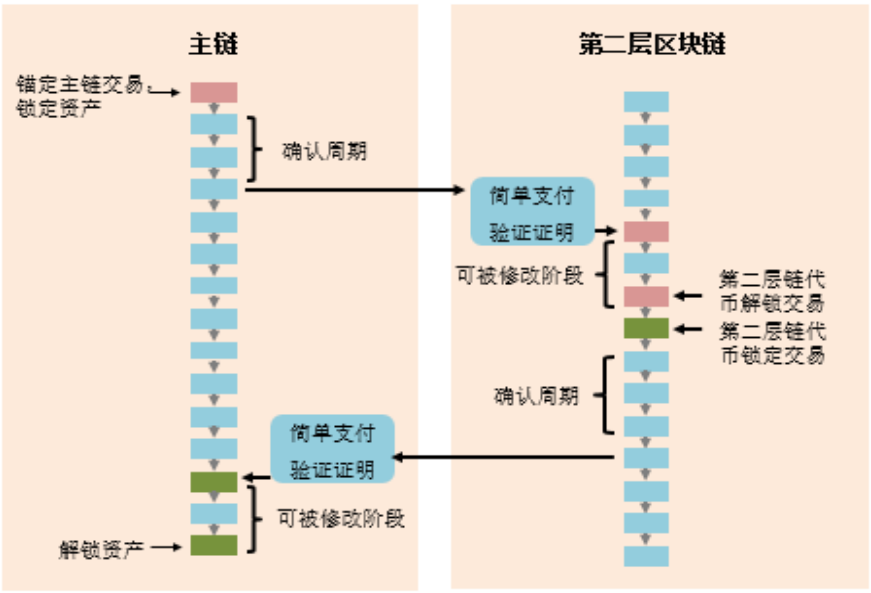
后期 Interledger 跨链技术由公证人机制转化为 HTLA（哈希时间锁定协议）与公证人融合机制。即两个不同的账本系统可以通过第三方“连接器”来互相自由地转换货币。同时，“账本”提供的第三方会向发送者保证，发送者的资金只有在“账本”收到证明，且接收方已经收到支付时，才将资金转给连接者；第三方同时也保证连接者，一旦对方完成了协议的最后部分，他们就会收到发送方的资金。

2.2. 侧链/中继

2.2.1. 侧链和中继机制概述

侧链主要针对的是两条同构链，即一个区块链系统能够理解另一条区块链的系统构架，实现在获得其他区块链系统提供的锁定交易证明之后，自动释放代币，一般是通过双向锚定机制实现资产转移。但其实资产也并未真正实现转移，只是当资产在原链上锁定时，等量等价资产在另一条链上被释放，而资产在另一条链上被锁定后，原链上的资产将被释放。侧链相对容易实现，是最早出现的跨链技术，早期跨链项目 BTCRelay、Blockstream 使用的是均为侧链机制。

图 6：双向锚定图

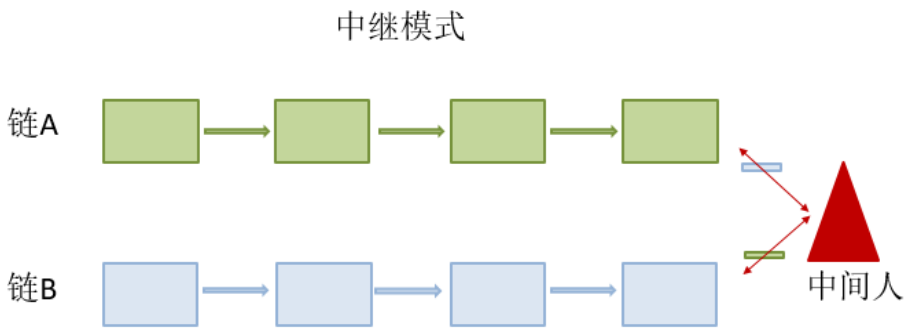


资料来源：《Enabling Blockchain Innovations with Pegged Sidechains》，天风证券研究所

侧链协议的设计难点在于如何让资产在主链和侧链之间安全流转，即接受资产的链必须确保发送资产的链上的币被可靠锁定。为此根据验证方式不同，可分为托管模式、驱动链模式、SPV 模式，三种模式也并不一定单独使用，可以在主链、侧链使用不同锚定技术的混合模式。

- 托管模式，类似于跨链技术的公证人机制，即通过可信第三方确保公平交易。依据可信第三方的数量具体可分为单一托管模式、联盟模式。单一托管模式是指将数字资产发送到一个主链单一托管方（类似于交易所），当单一托管方收到相关信息后，就在侧链上激活相应数字资产；而联盟模式为缓解单一托管模式的过度中心化问题，选取一个可信团体作为公证人，对来往交易信息进行确认，并将验证结果发送给接受方，但是这并没有从根本上解决中心化问题，侧链安全仍然取决于公证人的诚实度。
- 驱动链模式，类似于托管模式，但是其公证人限定于链上的矿工，由矿工监管被锁定的数字资产。矿工全体投票表决交易信息的正确与否，系统的安全性完全依赖于矿工在公证时的参与度和可信度。而且一般侧链初建时，主链上的矿工加入侧链的比例很小，很容易导致权益攻击，严重危害区块链安全。
- SPV 模式，即简单支付验证技术，主要原理就是验证交易已被放在了链上，并且在包含该交易区块的后面有足够数量的区块。具体来讲，SPV 是 A 链上的交易发送者将币发到一个特殊的地址，从而将币锁定。这笔交易的 SPV 证明随后会被发送到 B 链，B 链上的矿工验证 SPV 通过之后，就会在 B 链上解锁对应数量的 B 链币。
- 中继模式（Relays）则一般适用于链接两个异构或同构区块链，是更为直接的实现互操作性的方式，即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链内读取并进行自我验证，其验证方式依据自身结构不同存在显著差异。而这里的中间人仅仅充当中继桥梁的作用，负责数据收集工作。

图 7：中继机制示意图



资料来源：火币区块链产业专题报告跨链篇，天风证券研究所

无论是侧链还是中继，最基本的需求就是需要采集原链的信息。侧链与中继的区别在于：

从属关系上侧链锚定从属于主链，是主链与附属链之间去信任交互的方案，且被限定在主链与侧链之间，更多着眼于可拓展性而非可伸缩性，而中继采用了中心辐射设计，不从属于某条主链，更像是“调度中心”，只负责数据传递，不负责链维护；执行过程看，侧链需要同步所有的区块头，验证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；此外，安全性方面，侧链的安全性是建立在侧链能有效激励矿工进行一致性验证交易，主链的安全性无法在侧链上起作用，而中继是由主链自行验证，安全性有一定保证。

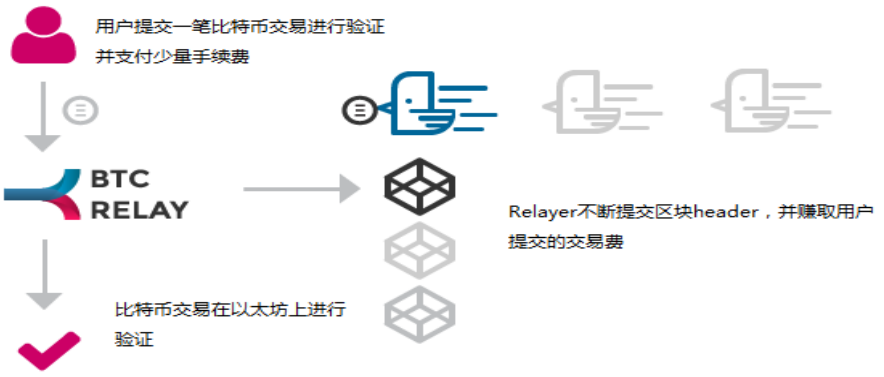
总体而言，侧链/中继模式的成本较高，效率较低，这是由于该模式下需要等待信息上链，确定不会发生回滚后方可确认。

2.2.2. 案例：BTC Relay

2016 年 5 月，ConsenSys 团队正式推出 BTC Relay，被认为是首个侧链项目。BTC Relay 锚定的是比特币系统，通过使用以太坊的智能合约功能允许用户在以太坊上验证比特币交易，以实现以太坊和比特币网络相连互通。

BTC Relay 首次引入了区块链侧链概念，尝试跨区块链通信，打开了链与链之间的通道。但其并未完成完整的中继跨链技术，只是通过智能合约主动请求比特币原链系统进行信息验证，而不是通过侧链中继而来。

图 8：BTC Relay 原理图



资料来源：BTC Relay，天风证券研究所

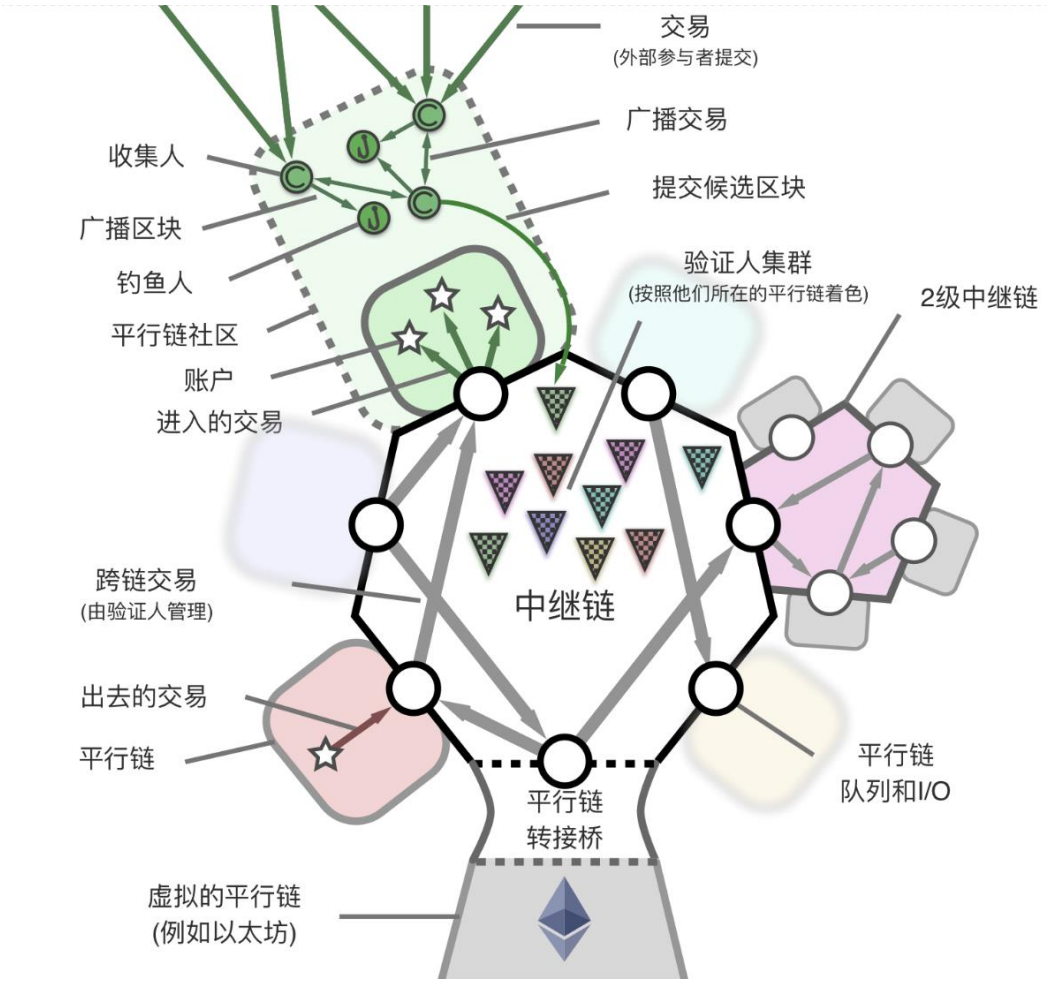
2.2.3. 案例：Polkadot

2017 年，Ethereum 社区发起的 Polkadot 为典型的采用跨链中继结构的项目，其目标就在于建立一种异构的多链架构，通过中继链（relay-chain）链接现存所有的区块链，包括各种公有网络、私有网络或联盟网络。

Polkadot 于 2018 年 5 月份正式发布关于项目的核心部分——中继实现理论证明。即在 Polkadot 结构中，原链可保持原有的协议运行而不受影响。原链上发出需要中继的交易时，中继链技术将原有链上的资产转入多重签名控制的原链账户中，并对其暂时锁定。实际运作中，中继结构中的收集人（collator）负责收集需要中继的交易信息，并打包成一个区块广播至验证人（validator）；验证人拥有最高权限，进行签名投票决定交易是否有效，确认交易有效后立即将原链中包含确认信息的区块头放进中继链中，以此来避免发生链重构或双花。同时，中继链将交易信息转移至目标链，成为目标链可执行的交易，以此实现跨链通信。此外，中继结构中还引入钓鱼人（fisherman）对交易进行监督举报。

目前 Polkadot 仍处于开发阶段，前期着重以以太坊为主，实现以太坊与私链的互连，后续将升级至其他公有链网络，实现全网跨链互联互通。

图 9：Polkdadot 中继机制示意图



资料来源：Polkdadot 白皮书，天风证券研究所

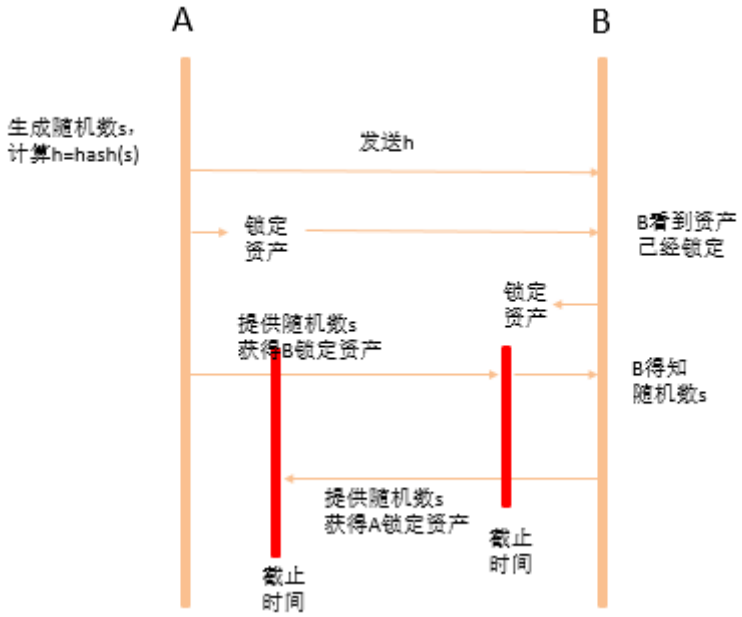
2.3. 哈希锁定

2.3.1. 哈希锁定技术概况

哈希锁定最早出现在 Bitcoin 的闪电网络中，其通过资产锁定，并设置相应的时间、解锁条件实现公平交易。哈希锁定具体来讲分为以下阶段：1)A 生成随机数 s，并计算出 h=hash(s) 发送给 B。2 ）A 通过智能合约锁定资产，并在智能合约中设定：若 B 在 2x 时间内提供随机数 s，使得 hash (s) =h，则 A 锁定的资产将转移给 B。3) 同样，B 看到 A 锁定资产后，B 也进行锁定资产，并在智能合约中设定：若 A 在 x 时间内提供随机数 s，则 B 锁定的资产将转给 A。基于该设定，整个交易最长在 2x 时间段内完成。

这里的原子性是可以被验证的。即 A 为了获得 B 的资产，将在 x 时间内提供随机数 s 至智能合约，并获得 B 锁定的资产；B 从公告中获悉随机数 s 之后将在 x-2x 时间段内提供给智能合约并领取 A 锁定的资产，至此，双方实现公平交易。若 A 并未在 x 时间内提供随机数，则资产将退回给双方。若 A 在 x-2x 时间内提供了密码 s，则 B 将获得 A 锁定的资产，而 A 分文不得。若 B 未在 x-2x 时间内提供随机数 s，则 B 分文不得。但后两种情况是由于交易双方自身的过错，且可以轻松避免的。

图 10：哈希锁定示意图



资料来源：Chain Interoperability，天风证券研究所

哈希锁定是系统之间进行原子交易的基本框架，保障跨链交易的原子性，即要么成功，要么失败，不存在任何第三种状态，可拓展应用于中心化账本或去中心化账本的系统之间。然而，哈希锁定只能实现跨链的资产互换，即各链资产总量保持不变的情况下，资产的持有人变化，而无法真正将资产转移至另一条链上，为此对于资产转移，还需要配合其他跨链技术方可实现。另一方面，要形成有规模的网络还需要更为完善的协议。

2.3.2. 案例：闪电网络

在实际的应用中，哈希锁定通常与状态通道（state channel）搭配起来，以此来提高交易速率。2015 年 2 月，比特币闪电网络（Lightning Network）发布，其是在比特币上运行的一个项目，通过构建微支付通道，在比特币区块之外进行撮合交易，以此来实现大量的小额交易，大幅提高比特币交易网络的性能。2017 年 12 月闪电网络正式在比特币主网推出，并完成第一笔交易。

闪电网络底层技术中主要运用了序列到期可撤销协议（Recoverable Sequence Maturity Contract）和哈希时间锁协议（Hashed Time-Lock Contact）实现跨链原子级交换。前者解决了交易的确认问题，即类似于提供一个准备金机制，交易双方共同放入一定量的资金，并记录双方资金所占份额，交易后双方进行多重签字确认，资金池的比例份额将同步持续更新，直至一方提现，最终资金占比方在区块链上确认。而后者解决了支付通道的问题，通过哈希时间锁定协议来提供限时转账功能，实现交易双方安全转账，避免了因交易取消或推迟无法拿回资金的情况。

2.4. 分布式私钥控制

2.4.1. 分布式私钥控制技术概况

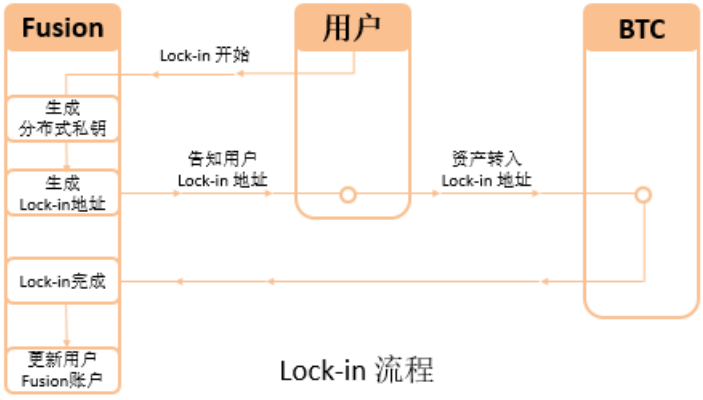
分布式私钥控制模式是通过分布式节点控制各种资产的私钥，并将原有链资产映射至跨链中，确保各种资产在同一条链上实现互联互通。

其实现模式类似于公证人机制，但用户始终拥有对资产的控制权，只是在存储数字资产的秘钥上采用了分布式存储的方式，这在一定程度上避免了公证人模式下中心化风险。此外，账户锁定机制不需要采用双向锚定方式，所有的交易是在验证节点重构后传入原链网络，不改变原链特性，为此各链均可自由低门槛接入链中，降低跨链接入成本。但由于不改变原链，跨链则需要根据原链的特性适配开发，且跨链速度也将受制于原链交易确认时间等因素的影响。

2.4.2. 案例：Fusion

2017 年，Fusion 提出通过利用分布式私钥控制模式进行跨链交易处理，以支持多平台跨链资产转移，从而构建加密金融应用运行的基础平台。即通过将各数字资产的私钥置于分布式节点的控制之下，实现所有权和使用权分离，通过 Lock-in 和 Lock-out 让 fusion 成为所有现有区块链的侧链，将现有区块链的代币映射到 fusion 这一公链之上，使得所有的代币在同一条链上具有互通性。截至目前，fusion 已经完成概念验证，公链还在开发中。

图 11：Fusion Lock-in 示意图



资料来源：Fusion 白皮书，天风证券研究所

该跨链机制的核心在于分布式控制权管理，即将资产的所有权和使用权分离，将原链上数字资产的控制权安全地转移至非中心化系统中，实现方式是通过数字资产 Lock-in 和 Lock-out 的两个基本步骤：在 Lock-in 的过程中，分布式生成秘钥即实现秘钥分片以及分片秘钥分布式保管，随后将资产转入原链上指定账户并由 fusion 节点进行验证，实现控制权的分布式管理；对于 Lock-out 也是如此，先检查 fusion 映射账户中数据情况，满足条

件后发起交易，fusion 各节点通过各自保存的分片秘钥进行验证，解除分布式控制权管理以及资产映射。分布式控制权完成交接后，智能合约将在 Fusion 映射账户中同步更新账户状态数据，以体现 Lock-in 和 Lock-out 完成情况，其记账过程实际上是通过 Fusion 向映射账户发放或收回等量等额数字资产的记账过程。

2.5. 小结

总的来说，跨链就是为两条链建立联动，早期跨链技术主要专注于资产转移，如公证人机制、侧链/中继技术，都需要通过用户或第三方在链外进行更多的约定和操作，且能提高原链交易效率，实现底层扩容。后期的项目则更为注重底层跨链基础设施，从区块链底层结构开始构造链结构的跨链技术。下表简要就四种不同跨链技术的优劣势进行对比分析。

表 2：跨链技术的优劣势对比

跨链技术	公证人机制	侧链/中继	哈希锁定	分布式私钥控制
优势	无需进行复杂的工作量或权益证明，易于实现； 使用范围广，可对接中心化和去中心化账本； 运行效率较高；	对原链没有特定要求，适用范围广； 中继支持同构或异构链互联互通，实现多条链连通；	容易实现； 对原链没有严格的要求，适用范围广； 实现交易的原子性；	容易实现； 分布式私钥存储，消除中心化风险； 不改变原链性质，适用范围广；
劣势	公证人的信任风险； 中心化风险；	实现难度较大； 等待原链确认时间较长，运行效率较低； 侧链只能实现与主链互联；	仅适用于资产兑换，无法单独实现资产转移；	需要适配原链搭建，开发难度大； 等待原链确认时间较长，运行效率较低；

资料来源：天风证券研究所

从当前跨链技术的发展情况来看，已呈现百家争鸣，各辟蹊径态势。针对上述四种跨链技术，未来中继跨链技术比较可能率先出现大规模的落地应用，可适用于多个场景，包括跨链交换、资产转移、资产抵押等，并能兼容多个区块链系统。

当然，我们也不能以孤立的方式去评判每个跨链技术，没有人知道这一切将通向何方，就像互联网早期的构架师也难以想象现在基于其发明的流媒体音乐、网络语音电话或在线电子市场等等。人类的发展史本就是在不断打破生存状态中存在的种种局限，对于跨链技术目前遇到的安全性、性能等问题，我们正在不断探索他们的解决渠道，未来可能也会出现更优的跨链机制。

3. 跨链技术未来发展

3.1. 应用场景

目前区块链头部交易所均为中心化交易所，其逐渐显露出的信息不透明、资产不安全、平台不合规以及隐私泄露等问题正一点点腐蚀用户的信任。为此，伴随着跨链技术等底层技术的成熟，去中心化交易所的性能、用户体验不断加强，去中心化交易所会是典型的最早跨链技术落地应用的场景之一。

此外，跨链技术也可进行跨链资产抵押、托管、借贷、衍生品等金融应用，如通过在 A 链抵押资产获得 B 链的资产，到期若顺利归还 B 链资产，则用户可取回 A 链抵押资产；反之，B 链有权自由处置 A 链抵押资产。

当然随着区块链技术性能不断提高，跨链应用不会只局限或止步于数字货币领域的应用，将价值圈在一个小范围中，将由单一向多元化发展。跨链技术也将逐步应用于跨链智能合约、多平台 DApp 部署、跨链通信预言机等等，通过跨链技术实现链内与链外信息的交互，即完成跨链信息的传递、共享等，充分实现区块链的商业价值。

3.2. 风险和挑战

虽然跨链技术能够为现有区块链生态带来显著的发展，比如实现价值互联，促进价值流通，解决信息孤岛问题，侧链技术还能大大提高区块链交易吞吐量等优势。但目前跨链技术仍处于初步探索阶段，尚未形成稳定体系，存在很多问题有待改善。

- 对现有区块链系统的安全性或存在一定影响。跨链中两条链存在交互，这过程中难免会对原有链上的系统产生影响，那么一条链上或侧链上发生安全问题，可能会影响另一条链的安全。如侧链安全问题，尤其是基于 POW 共识的区块链，由于初期并没有多少矿工加入侧链挖矿，而主链的矿工算力远远大于侧链，很容易造成权益攻击。为此跨链不仅要充当连接者的角色，同时还需要隔离主链，避免对跨链的攻击直接影响主链。
- 性能问题。目前区块链自身的性能远远达不到应用的需求，现有项目提出的目的之一就在于解决性能问题，但通过双向锚定或哈希锁定方式，虽然能实现原子性转账，但资产为保证资产转移的安全，需要等待很长一段确认期，才能在另一条链上解锁对应的数字货币；此外，随着网络拓扑结构的发展，跨链交易确认时间将会呈指数型增长，延迟将进一步放大。
- 商业落地应用还较少。一方面，跨链项目主要集中于近两三年发起，跨链项目从数量上来说不多，尤其后期从区块链底层基础设施设计跨链的项目目前多数还处于概念验证阶段，实际应用仍未落地。另一方面，跨链技术尚不成熟，安全性以及性能问题也进一步抑制跨链落地应用。

为此实现跨链技术的关键是如何在保证安全性的情况下，实现资产互通的原子性和高效性。

3.3. 未来发展

区块链从技术上是去中心化数据库和分布式账本技术，从商业层面则是价值网络，在这个价值网络中，连接的有效节点越多、越分布，可能产生的价值叠加会越大。跨链技术作为其中的链接器，其体系结构也必须满足互联网构架相同的基本条件：

- 生存性，即跨链连接必须无条件存在。
- 兼容性，跨链技术必须能够协调多种不同类型的区块链系统，包括公有链、联盟链、私有链等，以及共识机制、可拓展性、存储等内在核心要素皆不同的区块链系统。
- 灵活性，可使得在面临新的变化时系统能较容易增加或修改原有的组件，做出快速的调整改进，以链接未来可能出现的新的区块链系统。无状态的架构是系统高扩展性的基石。

总体而言，未来跨链技术将不断打破现存状态中的种种局限，探索新的解决方法，构建价值网络的高速公路，实现各个区块链系统协同交互形成统一的整体，行业也将迎来曙光。

分析师声明

本报告署名分析师在此声明：我们具有中国证券业协会授予的证券投资咨询执业资格或相当的专业胜任能力，本报告所表述的所有观点均准确地反映了我们对标的证券和发行人的个人看法。我们所得报酬的任何部分不曾与，不与，也将不会与本报告中的具体投资建议或观点有直接或间接联系。

一般声明

特别声明

投资评级声明

类别	说明	评级	体系
股票投资评级	自报告日后的 6 个月内，相对同期沪深 300 指数的涨跌幅	买入	预期股价相对收益 20%以上
		增持	预期股价相对收益 10%-20%
		持有	预期股价相对收益-10%-10%
		卖出	预期股价相对收益-10%以下
行业投资评级	自报告日后的 6 个月内，相对同期沪深 300 指数的涨跌幅	强于大市	预期行业指数涨幅 5%以上
		中性	预期行业指数涨幅-5%-5%
		弱于大市	预期行业指数涨幅-5%以下

天风证券研究

北京	武汉	上海	深圳
北京市西城区佟麟阁路 36 号	湖北武汉市武昌区中南路 99	上海市浦东新区兰花路 333	深圳市福田区益田路 5033 号
邮编：100031	号保利广场 A 座 37 楼	号 333 世纪大厦 20 楼	平安金融中心 71 楼
邮箱：research@tfzq.com	邮编：430071	邮编：201204	邮编：518000
	电话：(8627)-87618889	电话：(8621)-68815388	电话：(86755)-23915663
	传真：(8627)-87618863	传真：(8621)-68812910	传真：(86755)-82571995
	邮箱：research@tfzq.com	邮箱：research@tfzq.com	邮箱：research@tfzq.com