跨链：打破孤岛，万链互联

——区块链技术引卷之七

通证通研究院
区块链研究报告

专题报告　　行业研究

2019.05.15

通证通 x FENBUSHI DIGITAL

分析师：宋双杰，CFA

Email:master117@bitall.cc

分析师：田志远

Email: tianzhiyuan@bitall.cc

特别顾问

沈波

JX

导读：随着区块链行业的蓬勃发展，多种公有链、私有链和联盟链出现，由此自然而然地出现了一个问题：链与链之间如何互联互通？本篇报告梳理了跨链的含义、意义和跨链需要解决的关键问题，回顾了跨链技术的发展历程，分析了主要的跨链模式。

摘要：

跨链是通过连接相对独立的区块链系统，实现资产、数据等的跨链互操作，跨链的主要实现形式包括跨链资产互换和跨链资产转移。

2013 年之前，区块链的发展主要集中在单一区块链。2013 年以来，跨链技术蓬勃发展，跨链的几种主要模式相继被提出。

实现跨链的两个关键问题分别是跨链交易的原子性和跨链交易验证。哈希锁定模式利用哈希锁和时间锁能够保证跨链交易的原子性，即只有满足一定的时间条件和哈希条件交易才能够完成，从而实现跨链资产互换。对于相互独立的两条区块链而言，为实现跨链资产转移，不得不依赖于外部第三方进行信息交互，根据第三方的工作范围可以分为公证人机制和中继模式。在公证人机制下，第三方负责数据收集和交易验证；在中继模式下，第三方仅负责数据收集，交易验证由目标链完成。

总体而言，跨链技术在过去几年间得到了迅速发展，相关的项目层出不穷。现有的跨链相关项目中，基于侧链/中继模式的项目占比最高；基于哈希锁定的闪电网络自主网上线以来节点数量、通道数量和网络容量不断增长，技术可行性得到了较好的验证；通信协议簇（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）类项目未来能否成为主流跨链方案一定程度上取决于业界对于相关标准规范的接受度。**但是目前跨链技术尚未完全成熟和广泛应用，仍有较大的提升空间。此外除了跨链本身的技术形态演进，跨链技术未来的发展也与跨链技术的应用模式密切相关。**

风险提示：量子计算机技术突飞猛进

目录

图表目录

随着区块链行业的蓬勃发展，多种公有链、私有链和联盟链出现，由此自然而然地出现了一个问题：链与链之间如何互联互通？本篇报告梳理了跨链的含义、意义和关键问题，回顾了跨链技术的发展历程，分析了主要的跨链模式。

1 跨链概述

1.1 什么是跨链

跨链（cross-chain），顾名思义，就是通过连接相对独立的区块链系统，实现资产、数据等的跨链互操作。

跨链的主要实现形式包括跨链资产互换和跨链资产转移。

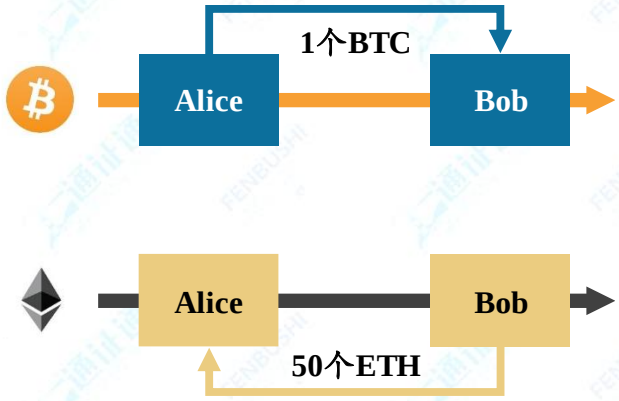
跨链资产互换指将一条链上的资产兑换成等值的另一条链上的资产，每条链上的资产总量不变。跨链资产互换的一个简单例子如下：

Alice 用 1 个 BTC 交换 Bob 的 50 个 ETH，互换成功的结果应该是 Alice 的 ETH 地址收到 Bob 的 50 个 ETH，Bob 的 BTC 地址收到 Alice 的 1 个 BTC。

跨链资产转移指将一条链上资产转移到另一条链上，原链上的资产锁定，另一条链上重新铸造等量等值的资产，每条链上的资产总值发生变化，但两条链的资产总值之和不变。跨链资产转移的一个简单例子如下：

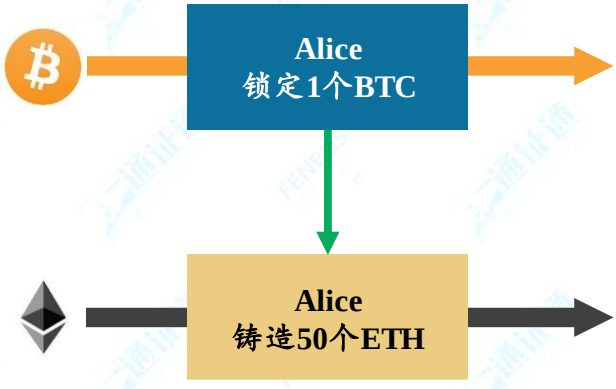
Alice 将 BTC 区块链上的 1 个 BTC 转移到 ETH 区块链，则 BTC 区块链上的 1 个 BTC 被冻结，ETH 区块链上新生成 50 个 ETH。

图表1：跨链资产互换示意图



资料来源：通证通研究院

图表2：跨链资产转移示意图



资料来源：通证通研究院

1.2 为什么跨链

突破底层公链性能和功能瓶颈。随着区块链网络的快速发展，性能逐渐成为制约区块链发展的重大瓶颈，通过将部分事务处理转移到侧链或链下能够提升区块链网络的性能。部分功能创新也可以通过侧链实现，从而保证主链的安全性。

实现跨链互操作。单一的区块链系统相对封闭，随着区块链技术的迅速发展，链与链之间的“互操作性”问题逐渐凸显。跨链互

操作的具体应用场景包括但不限于跨链支付结算、非中心化交易所、跨链信息交互等。

1.3 跨链发展历程

2013 年之前，区块链的发展主要集中在单一区块链。2013 年以来，跨链技术蓬勃发展，跨链的几种主要模式（公证人机制（Notary schemes）、侧链/中继（Sidechains/relays）、哈希锁定（Hash-locking））**相继被提出。**

2013 年 5 月，Tier Nolan 在 BitcoinTalk 论坛提出了“原子转移（atomic transfers）”，原子转移又称原子交换（atomic swap），指构成一笔完整跨链交易的子交易同时发生或不发生，不存在第三种中间状态。该方案经过改进后成为跨链的一种主要模式，即哈希锁定模式。

2014 年 10 月，BlockStream 首次明确提出侧链的概念，锚定式侧链（Pegged Sidechains）利用双向锚定（two-way peg）机制，能够实现加密资产按照某种汇率在侧链和主链之间转移。2016 年 12 月，BlockStream 进一步提出了强联邦侧链（Sidechains with Strong Federations），通过引入由多方控制的多重签名地址减少延迟并提升互操作性。

2015 年 2 月，Poon 发布了闪电网络（Lightning Network）白皮书，基于哈希锁定实现资产 BTC 链下交易。

2015 年 10 月，Interledger Protocol 白皮书发布，基于公证人机制实现不同账本间资产的转换。

2016 年 5 月，BTC Relay 基于中继实现 BTC 到 ETH 的单向跨链连接。

2017 年，Polkadot 和 Cosmos 提出跨链基础设施中继平台方案。

图表3：跨链技术发展历程

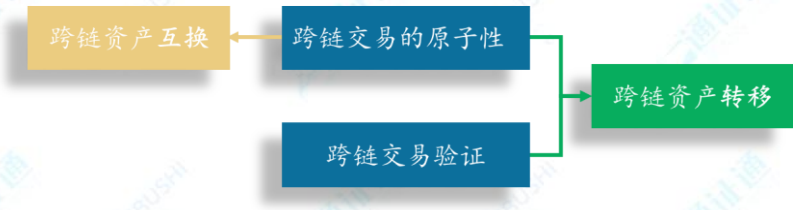
时间	事件
2009 年-2013 年	单一区块链发展
2013 年 5 月	Tier Nolan 提出原子转移
2014 年 10 月	BlockStream 首次明确提出侧链概念
2015 年 2 月	闪电网络白皮书发布，基于哈希时间锁实现资产 BTC 链下交易
2015 年 10 月	Interledger Protocol 白皮书发布，基于公证人机制实现不同账本间资产的转换
2016 年 5 月	BTC Relay 基于跨链中继实现 BTC 到 ETH 的单向跨链连接
2017 年	Polkadot 和 Cosmos 提出跨链基础设施中继平台方案

资料来源：通证通研究院

1.4 跨链关键问题

实现跨链的两个关键问题分别是跨链交易的原子性和跨链交易验证。通过保证跨链交易的原子性能够实现跨链资产互换，具体实践中主要依靠哈希锁定实现。跨链资产转移还需要进行跨链交易验证。

图表4：跨链资产互换和转移的实现条件



资料来源：通证通研究院

跨链交易的原子性是指跨链交易要么成功，要么失败，不存在第三种中间状态。一个完整的跨链交易由多个子交易构成，子交易分别发生在不同的区块链系统中，彼此相互独立，跨链交易的原子性要求保证一笔子交易成功后，后续的子交易也能够成功，或者后续的子交易失败，前面的子交易能够撤回。

跨链交易验证指对另一条链的交易进行验证。验证包括两个方面，一是交易已经被写入账本并且满足最终确定性，二是进行跨链数据传递，一条链能够验证另一条链的交易状态。

2 跨链的主要模式

通过哈希锁定能够保证跨链交易的原子性，对于相互独立的两条区块链而言，为实现跨链交易验证不得不依赖于外部第三方进行信息交互，根据第三方的工作范围可以分为公证人机制和中继模式。

在公证人机制下，第三方负责数据收集和交易验证。

在中继模式下，第三方仅负责数据收集，交易验证由目标链完成。

2.1 哈希锁定：跨链资产互换

2.1.1 提出背景

哈希锁定源于原子交换，最早的应用是 BTC 的闪电网络，闪电网络提供了可扩展的微支付通道，通过将部分交易转移到链下进行解决区块链网络的交易拥堵问题。

2.1.2 基本思路

简单而言，哈希锁定模式利用哈希锁和时间锁保障跨链交易的原子性，即只有满足一定的时间条件和哈希条件交易才能够完成。HTLC（Hashed Time-Lock Contract，哈希时间锁协议）是原子互换协议的具体实现。

哈希锁：Alice 对密钥 a 进行哈希运算得到 H（a），并将函数 H 和 H（a）告诉 Bob，Bob 利用 H 和 H（a）验证 Alice 提供的密钥的正确性。

时间锁：以 BTC 系统为例，BTC 时间锁的实现方式有两种，一种是绝对锁定，即回撤交易在某个时间范围内不生效，另一种是相对锁定，即相对某个时间或事件锁定交易。

HTLA（Hashed Time-Lock Agreements，哈希时间锁定合约）是 HTLC 的泛化协定，由 Interledger 提出。在该协定下，任何中心化

或非中心化账本无论能否支持 HTLC，均可利用 HTLA 实现跨链资产互换。

2.1.3 案例：闪电网络

闪电网络针对 BTC 网络提出，其主网已于 2018 年 3 月 15 日上线。2018 年 3 月 20 日，闪电网络受到 DDOS 攻击，200 多个节点被攻击下线。闪电网络主网上线以来节点数量、通道数量和网络容量不断增长，根据 BitcoinVisuals 数据，截至 2019 年 4 月 24 日，闪电网络节点数量超过 4200 个，通道数量超过 38000 个，网络容量约为 575 万美元。

闪电网络的两种主要协议分别是 RSMC（Revocable Sequence Maturity Contract，序列到期可撤销合约）和 HTLC（Hashed Time-Lock Contract，哈希时间锁协议）。RSMC 的作用是鼓励交易双方尽可能久的利用通道进行交易，对于主动终止通道的交易方进行惩罚，即主动终止通道的一方资金到账时间更晚。HTLC 的存在使得交易双方之间即便没有支付通道，但是只要能够找到一条支付路径即可实现交易。

（1） 创建交易

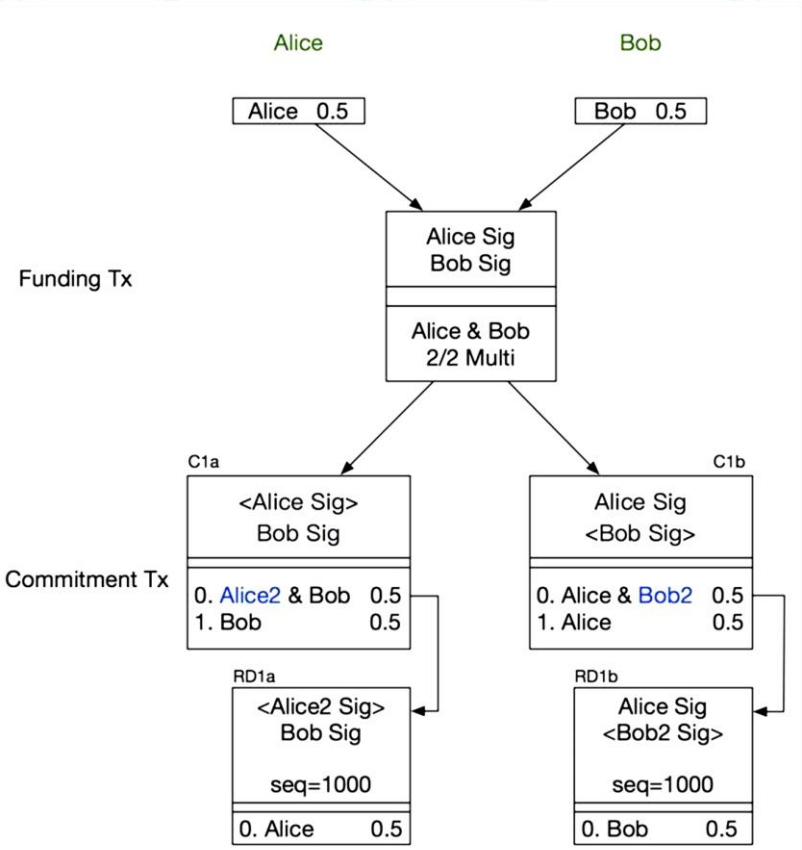
Alice 和 Bob 通过闪电网络转账，双方各拿出 0.5BTC，构建一笔保证金交易 Funding Tx，输出需要 Alice 和 Bob 多重签名。此时，双方未对 Funding Tx 签名，交易不广播到区块链上。

Alice 和 Bob 分别构造 Commitment Tx：Alice 构造 C1a 和 RD1a，Bob 签名后交给 Alice；Bob 构造 C1b 和 RD1b，Alice 签名后交给 Bob。双方均完成对 commitment Tx 的签名并交换后，再对 Funding Tx 进行签名。

C1a 的第一个输出需要 Alice 的另一把私钥 Alice2 和 Bob 的多重签名，第二个输出为给 Bob 0.5BTC。RD1a 为 C1a 第一个输出的花费交易，输出给 Alice 0.5BTC，此类型交易带有 sequence，作用是阻止当前交易进块，只有前向交易 C1a 经过 sequence 个确认才能被打包进区块。

由于 C1a 和 C1b 花费的是同一个输出，故这两个交易中只有一个能被打包进区块。若 Alice 广播 C1a，则 Bob 立即拿到 0.5BTC（C1a 的第二个输出），而 Alice 需要等 C1a 得到 sequence=1000 个确认，才能通过 RD1a 的输出拿到 0.5BTC。同理，若 Bob 广播 C1b，则 Alice 立即拿到 0.5BTC，Bob 需要等待 C1b 得到 sequence=1000 个确认，才能通过 RD1b 的输出拿到 0.5BTC。

图表5：RSMC 创建交易

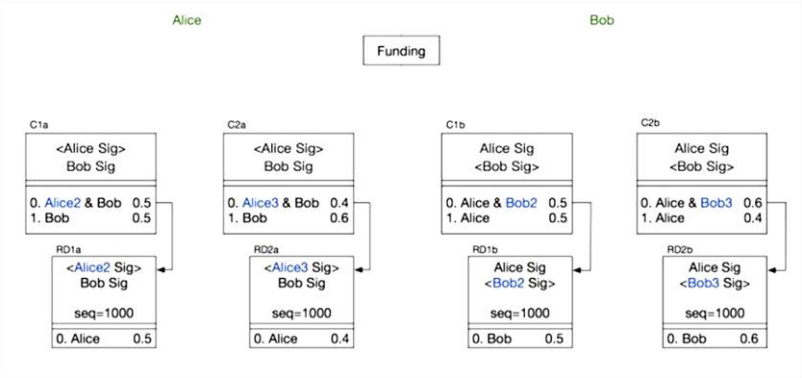


资料来源：《区块链之闪电网络》，通证通研究院

（2）交易更新

RSMC 更新过程如下：Alice 向 Bob 支付 0.1BTC，双方创建新的 Commitment Tx，即 Alice 创建 C2a 和 RD2a，Bob 创建 C2b 和 RD2b，此时需要废弃掉无效的状态 C1a 和 C1b。

图表6：RSMC 交易更新：创建新状态

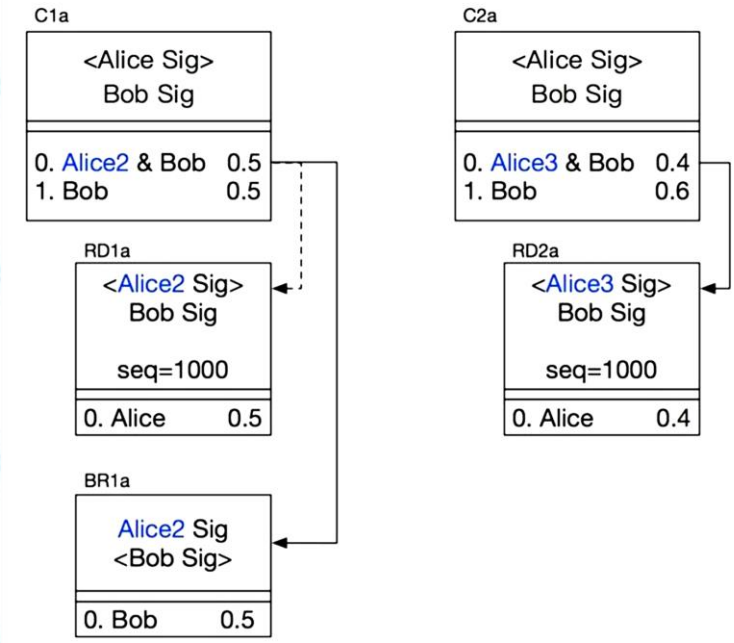


资料来源：《区块链之闪电网络》，通证通研究院

Alice 将 Alice2 的私钥交给 Bob，表示 Alice 放弃 C1a，承认 C2a。RD1a 中 sequence 的存在使得 Bob 可以在 Alice 违约后有一定的时间实施惩罚交易，即如果 Alice 违约，Bob 能够修改 RD1a 的输

出给自己，即形成交易 BR1a，Alice 将面临失去全部保证金的处罚。这种机制使得双方都会选择删除旧的状态，广播更新后的状态。

图表7：RSMC 交易更新：废弃旧状态



资料来源：《区块链之闪电网络》，通证通研究院

（3）交易关闭

按照最终余额构造 Commitment TX，无需设置多重签名和构造惩罚交易等。哈希锁定模式实现了跨链的资产互换，每条链上的资产总量不变，只是资产持有者发生了改变，跨链资产转移需要保证跨链交易的真实性，因此涉及到实现跨链交易验证的两种模式：公证人机制和侧链/中继模式。

2.2 公证人机制：依赖第三方验证交易

2.2.1 提出背景

2015 年 10 月 Interledger Protocol（ILP，跨账本协议）白皮书发布，这一协议由 Stefan Thomas 和 Evan Schwartz 创建，其目的就是让跨账本交易变得更加方便，瑞波随后引入了这一协议。之所以称为跨账本而不是跨链，是因为该协议不仅支持非中心化的区块链账本，还支持银行等机构的中心化账本，是更广义的“跨链”。

2.2.2 基本思路

由一个或一组节点作为公证人进行数据收集和交易验证。公证人同时跟踪两条链的状态并告知对方，交易双方完全依赖于公证人验证和实现交易。

依据公证人的构成和签名方式，公证人机制具体分为三类。公证人可以由一个或一组节点充当，由一个节点作为公证人即为**中心化公证人机制**，在由一组节点作为公证人的情况下，根据各个节点的签名方式不同分为**多重签名公证人机制**和**分布式签名公证人机制**。

中心化公证人机制：单一节点或机构充当中心化公证人。中心化公证人机制是相对比较简单的模式，与传统的两个主体通过第三方间接交易类似，公证人同时兼容两个或多个系统，其优点在于处理速度较快，技术结构相对简单，但是这种方式的问题也很明显，即中心化的公证人的安全风险。

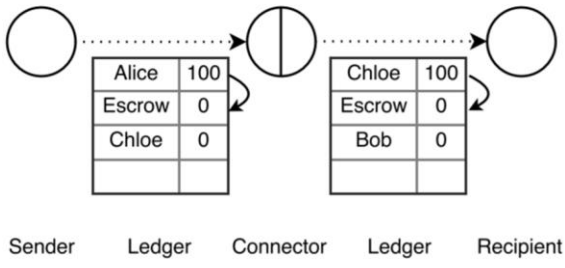
多重签名公证人机制：多个公证人在各自账本共同签名达成共识。这种机制弱化了中心化公证人机制的中心化问题，安全性相对更高，前提是交易链需要支持多重签名功能。

分布式签名公证人机制：与多重签名公证人机制的主要区别是采用了多方计算的分布式签名。对于跨链交易，系统仅产生一个密钥，密钥以碎片形式发送给每个公证人节点。

2.2.3 案例：Interledger Protocol

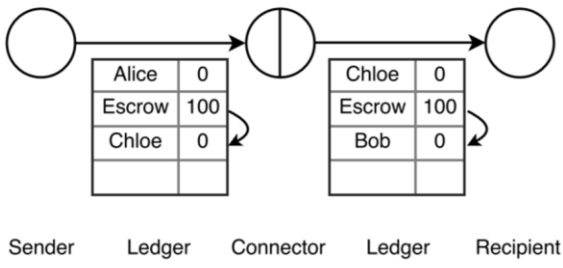
Interledger Protocol 最初是公证人机制的代表，在发展过程中融入了哈希锁定的理念。在该协议下，处于不同账本系统的发送者与接收者可以通过一个或多个连接者进行跨账本交易，连接者提供转发数据或资金的服务并收取相应的费用。通过为跨账本交易的参与方提供资金托管，只有在分类账收到接收方已经收到资金的证明时，才会将相应的资金发给连接者，同时保证当连接者完全执行协议后将会收到来自发送者的资金。交易托管与执行分为两种方式，其中，“原子模式”是由参与者选出一组公证人来协调交易；“通用模式”无需公证人，通过参与者给予激励以及反向执行指令来确保安全支付。

图表8：发送者和连接者的资金托管



资料来源：A Protocol for Interledger Payments，通证通研究院

图表9：资金转移给连接者和接收者



资料来源：A Protocol for Interledger Payments，通证通研究院

2.3 侧链/中继：目标链自行验证交易

2.3.1 提出背景

2014 年 BlockStream 首次明确提出侧链概念。2014 年 10 月，BlockStream 发布白皮书《Enabling Blockchain Innovations with Pegged Sidechains》，首次明确提出侧链的概念，按照白皮书中的定义，侧链是验证来自另一条区块链的数据的区块链，通过双向锚定（two-way peg）机制，加密资产能够按照某种汇率在侧链和主链之间转移。

侧链提出的背景：BTC 创新与安全的权衡。一方面随着区块链技术的发展，越来越多的创新开始出现，Ethereum、Bitshares 等带来的智能合约和非中心化应用广受人们追捧，反观 BTC 则需要在性能和功能等众多方面做出提升，但是出于安全考虑，BTC 的创新一

直相对保守；另一方面竞争通证和山寨通证的大量出现也引发了BTC 核心开发团队对于开发和市场碎片化的忧虑。侧链（sidechain）能够在保证主链安全性的条件下，实现性能和功能方面的扩展，成为 BTC 的理想选择。在这种情况下，Adam Back、Matt Corallo 等 BTC 核心开发者共同发起成立了 BlockSream 公司。

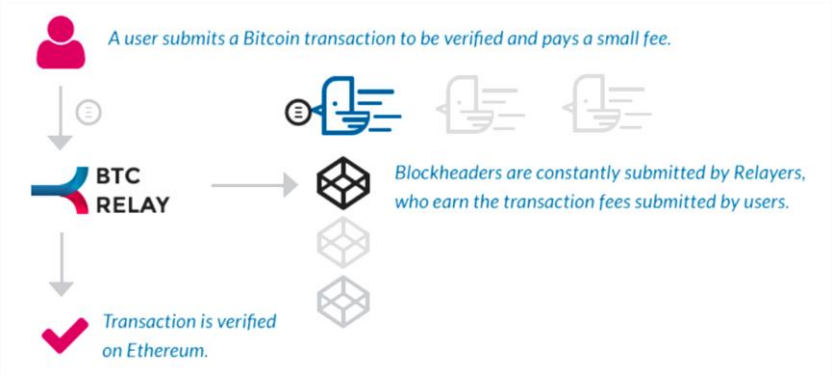
2.3.2 基本思路

侧链/中继模式下，目标链不依赖于第三方进行交易验证，而是自行验证来自发送链的数据，具体的验证方式有所不同，如 BTC-Relay 是通过 SPV（Simple Payment Verification，简单支付验证）进行交易验证，Cosmos 是通过节点签名数量。

2.3.3 案例：BTC Relay

BTC Relay 是 ETH 上的一个智能合约，通过存储 BTC 区块头验证 BTC 交易。由于 BTC 区块链的交易信息以 Merkle tree 的形式存储在区块头中，BTC Relay 可以利用 SPV 机制验证 BTC 交易。BTC Relay 的功能实现依赖于 Relayer 提交正确的区块头数据，及时提交正确的区块头数据的 Relayer 将会得到奖励。BTC Relay 通过相对简单的设计实现了 ETH 用户能够创建依赖于 BTC 区块链事件的智能合约，但是 BTC Relay 只实现了 BTC 到 ETH 的单向跨链。

图表10：BTC Relay 方案示意图

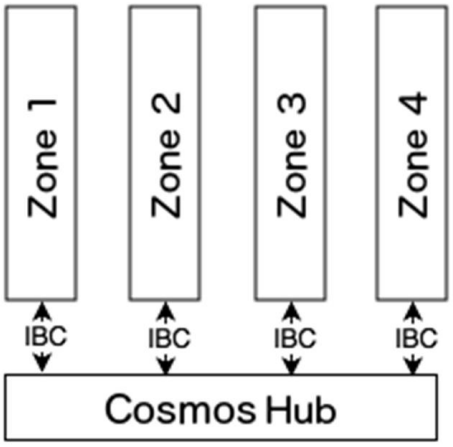


资料来源：btcrelay.org，通证通研究院

2.3.4 案例：Cosmos

2016 年 6 月，Jae Kwon 提出了 Cosmos，支持各种区块链接入与互操作。Cosmos 由由 Hub（枢纽）和 Zone（分区）两部分组成，分区采用 Tendermint 共识，可以支持多种区块链，同时分区数量可以扩展。分区之间通过枢纽遵照 IBC 协议（InterBlockchain Communication Protocol，链间通信技术规范）进行交易，IBC 协议定义了区块链注册、数据包格式、交易类型和数据包交付确认流程等内容。

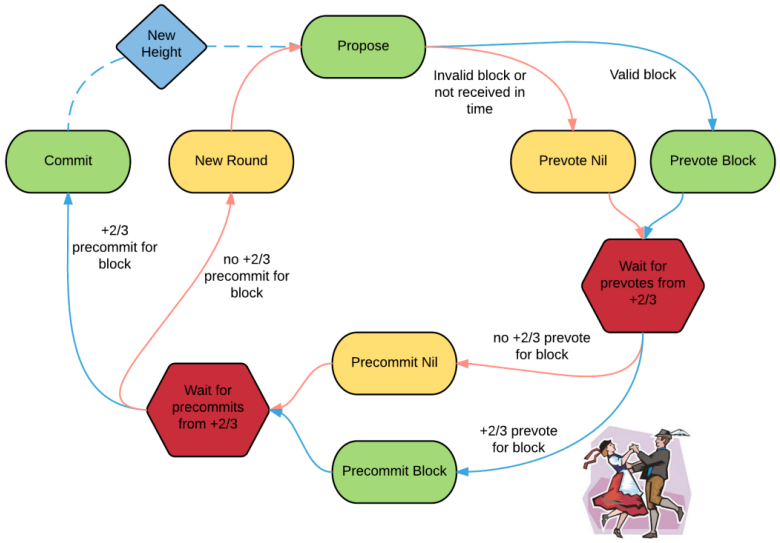
图表11：Cosmos 枢纽和分区



资料来源：Cosmos 白皮书，通证通研究院

Tendermint 共识过程与 BFT 类共识类似，开始时节点对新一轮的区块进行提议，合格的提议区块在预投票（Prevote）环节获得 2/3 以上投票则进入预认可（Precommit）环节，再次获得 2/3 以上的预认可后即获得正式认可（Commit）。

图表12：Tendermint 共识机制

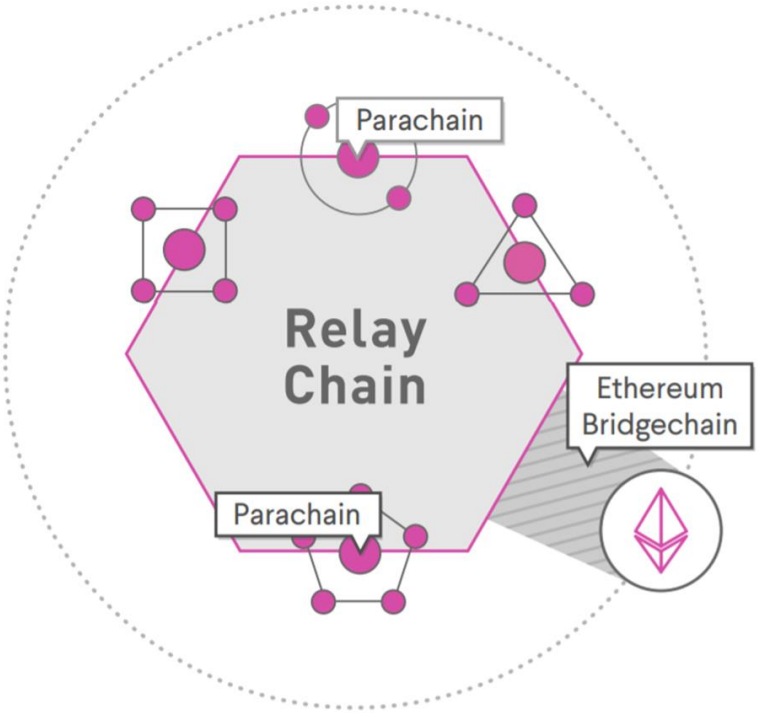


资料来源：Develop PBFT Consensus based application on tendermint，通证通研究院

2.3.5 案例：Polkadot

2016 年 11 月，Polkadot 白皮书发布，提出了一种异构的多链架构，支持多个高度差异化的共识系统去中心化、去信任地进行互操作和访问。Polkadot 网络由中继链（Relay chain，负责协调链间的共识和交易）、平行链（Parachains，负责收集和处理交易）和转接桥（Bridges，负责连接其他异构的区块链）组成。

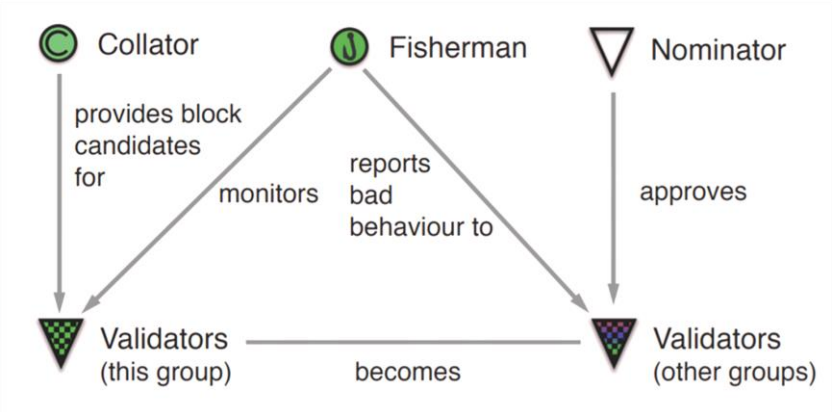
图表13：Polkadot 网络构成



资料来源：polkadot.network，通证通研究院

网络中的四类参与方包括验证者（Validators，负责验证平行链的数据）、收集者（Collator，负责采集平行链的数据并提交给验证者）、提名者（Nominator，为验证者提供押金和信用背书）和渔夫（Fisherman，负责举报和证明恶意行为）。

图表14：Polkadot 网络中的四类参与方



资料来源：polkadot.network，通证通研究院

Polkadot 跨链交易信息传输的简单过程如下：

（1）平行链 A 上的收集者收集交易并验证交易的有效性，将交易打包进区块；

（2）验证者验证其收到的只包含有效交易的区块，并支付一定押金；

（3）在提名者为验证者支付了足够的押金后，广播该区块到中继链；

（4）验证人对中继链区块达成共识并将平行链 A 的交易信息传输到平行链 B。

3 总结

总体而言，跨链技术在过去几年间得到了迅速发展，相关的项目层出不穷。现有的跨链相关项目中，基于侧链/中继模式的项目占比最高；基于哈希锁定的闪电网络自主网上线以来节点数量、通道数量和网络容量不断增长，技术可行性得到了较好的验证；除了上述的三种跨链主要模式，还有一类项目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，这类项目称为通信协议簇类项目，这类项目未来能否成为主流跨链方案一定程度上取决于业界对于相关标准规范的接受度。

目前跨链技术尚未完全成熟和广泛应用，仍有较大的提升空间。一方面跨链所面临的技术问题具有一定的复杂性，另一方面区块链技术也在飞速发展，区块链的类别和技术复杂度等不断提升，导致对于跨链技术更迭的要求也在不断提升。

跨链技术发展与跨链技术的应用模式密切相关。除了跨链本身的技术形态演进，跨链未来的进一步发展也依赖于跨链应用模式的构建和发展，随着区块链行业应用的逐步落地和不断丰富，对跨链的需求将不再局限于交易。

图表15：跨链相关项目

技术/项目	提出时间	跨链模式
原子转移	2013 年	哈希锁定
BlockStream 锚定式侧链	2014 年	侧链
闪电网络	2015 年	哈希锁定
Interledger（Ripple）	2015 年	公证人机制、哈希锁定
RootStock	2015 年	侧链
BTC Relay	2016 年	侧链
Corda	2016 年	公证人机制
Cosmos	2016 年	中继（通信协议簇）
Elements	2016 年	侧链
Polkadot	2016 年	中继
Aelf	2017 年	侧链
Aion	2017 年	（通信协议簇）
Block Collider	2017 年	（通信协议簇）
Bytom	2017 年	中继
Elastos	2017 年	侧链
Hcash	2017 年	中继
Loom	2017 年	侧链
MIXIN	2017 年	侧链
Fusion	2017 年	公证人机制
ICON	2017 年	公证人机制
Lisk	2017 年	侧链
Plasma	2017 年	侧链
Wanchain	2017 年	公证人机制
Zcash XCAT	2017 年	哈希锁定
Minimal Viable Plasma	2018 年	侧链
OneLedger	2018 年	（通信协议簇）
Plasma Cash	2018 年	侧链

资料来源：通证通研究院

附注：

因一些原因，本文中的一些名词标注并不是十分精准，主要如：通证、数字通证、数字 currency、货币、token、Crowdsale 等，读者如有疑问，可来电来函共同探讨。

免责声明

本报告由通证通研究院和FENBUSHI DIGITAL提供，仅供通证通研究院和FENBUSHI DIGITAL客户使用。本报告仅在相关法律许可的情况下发放，所提供信息均来自公开渠道。通证通研究院和FENBUSHI DIGITAL尽可能保证信息的准确、完整，但不对其准确性或完整性做出保证。

本报告的完整观点应以通证通研究院和FENBUSHI DIGITAL发布的完整报告为准，任何微信订阅号、媒体、社交网站等发布的观点和信息仅供参考，通证通研究院和FENBUSHI DIGITAL不会因为关注、收到或阅读到报告相关内容而视相关人员为客户。

本报告所载的资料、意见及推测仅反映通证通研究院和FENBUSHI DIGITAL于发布本报告当日的判断，相关的分析意见及推测可能会根据后续发布的研究报告在不发出通知的情形下做出更改，投资者应当自行关注相应的更新或修改。

市场有风险，投资需谨慎。本报告中的信息或所表述的意见仅供参考，不构成对任何人的投资建议。投资者不应将本报告为作出投资决策的唯一参考因素，亦不应认为本报告可以取代自己的判断，通证通研究院或FENBUSHI DIGITAL、通证通研究院或FENBUSHI DIGITAL员工或者关联机构不承诺投资者一定获利，不与投资者分享投资收益，也不对任何人因使用本报告中的任何内容所引致的损失负责。

通证通研究院和FENBUSHI DIGITAL对本免责声明条款具有修改和最终解释权。