区块链跨链技术综述

郭朝[1]，郭帅印[1]，张胜利[1]，宋令阳[2]，王晖[1]
（1. 深圳大学区块链研究中心，广东 深圳 518060；
2. 北京大学电子工程与计算机科学学院，北京 100871）

摘　要：随着区块链技术的发展，区块链项目也越来越多。由于区块链的封闭性，导致不同区块链形成一个个价值孤岛，不同区块链之间的信息交互与价值转移问题亟待解决。跨链技术解决了不同链间资产与数据等跨链操作问题，在过去几年里已经有许多尝试和发展，跨链的主要模式包括哈希锁定、公证人机制、侧链与中继技术等。介绍了目前主要跨链技术的基本原理，总结分析了各个跨链技术的优势与劣势。

关键词：区块链；跨链；哈希锁定；公证人；侧链；中继
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.2096−3750.2020.00162

A survey on cross-chain technology of blockchain

GUO Zhao[1], GUO Shuaiyin[1], ZHANG Shengli[1], SONG Lingyang[2], WANG hui[1]
1. Research Center of Blockchain, Shenzhen University, Shenzhen 518060, China
2. College of Electronic Engineering and Computer Science, Peking University, Beijing 100871, China

Abstract: With the development of blockchain technology, more and more blockchain projects have appeared. Due to the closure property of the blockchain, different blockchains have become islands of value. The information interaction and value transfer problems between different blockchains need to be solved urgently. The cross-chain technology is to solve the cross-chain operation problems of assets and data between different chains. There are many attempts and developments on cross-chain technology in the past few years, and the major models of cross-chain include Hash lock, notary mechanism, side chain and relay technology, etc. The concept of each cross-chain technology was introduced, and the advantages and disadvantages of each cross-chain technology were summarized and analyzed.

Key words: blockchain, cross-chain, Hash lock, notary, side chain, relay

1　引言

区块链技术是分布式数据存储、点对点传输、分布式共识算法、加密算法等计算机技术的集成应用。从狭义角度来讲，区块链是一种按照时间顺序将数据区块以顺序相连的方式进行组合的一种链式数据结构，并以密码学方式保证数据不可篡改和不可伪造的分布式账本。从广义角度来讲，区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新账本数据、利用密码学方式保证数据传输和访问安全、利用智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式[1]。基于时间戳的链式区块结构、分布式节点的共识机制、灵活可编程的智能合约是区块链技术最具创新性的技术环节。

2008 年，Satoshi[2]发表了“bitcoin: a peer-to-peer electronic cash system”，通常被认为是区块链技术的起源。在文献[2]中提出了一种去中心化、按时间顺序排序的数据，数据由所有节点维护、可编程和密码学上安全可信的分布式账本技术构成，用于解决比特币（BTC, bitcoin）在去中心化网络中的信任问题。作为比特币的底层实现技术，该技术被认为是构建下一代“信任互联网、价值互联网”的关键技术。

收稿日期：2019−08−27；修回日期：2020−02−18

作为区块链技术的一个成功应用，比特币验证了区块链技术的可行性。目前，区块链技术已经应用到社会的很多领域，如“数字货币”、跨境支付、供应链、制造业以及能源领域等。随着各界人士对区块链技术研究的逐步深入，越来越多的区块链应用出现在各种场景中，但是区块链结构体系、共识算法[3]、对用户隐私的保护[4]、智能合约开发、系统底层性能、交易吞吐量以及不同区块链系统之间的跨链通信等技术挑战越来越制约区块链技术及其行业的发展。不同应用场景所用的区块链系统不同，这些链可能应用于不同的领域，也可能具有不同的运行机制，而不同区块链存储的区块信息之间的隔离不可避免地造成了区块链的价值“孤岛”效应[5]。

随着区块链行业的蓬勃发展，多种公有链、私有链和联盟链的出现产生一个问题，即不同区块链之间如何进行通信甚至价值交换。

本文深入探讨了跨链的本质、意义以及跨链需要解决的关键性问题，回顾了跨链技术的发展历程，利用具体跨链项目分析了主要的跨链模式，并对跨链技术的未来进行了展望。

2　跨链技术研究现状

2.1　跨链技术的发展历程

从区块链的产生到现在，跨链技术主要包括以下 3 种模式：公证人机制（notary scheme）、侧链/中继（side chain/relay）和哈希锁定（Hash-locking），跨链技术发展历史线如图 1 所示。

单链发展（2009—2012 年）：在行业早期相当长一段时间内，区块链技术都是基于单链的发展。当时，行业的普遍认知为区块链的性能优化和技术升级可以在单链上完成，一旦链内成员就项目发展方向无法达成一致时，只能通过硬分叉或重新设计一条区块链来解决。

单链扩展时期（2012—2015 年）：由于出块时间、区块大小的限制以及所用智能合约解决复杂实际问题的能力不足，比特币的具体应用受到了很大制约。为此已有一些工作用于解决上述问题，如瑞波实验室在 2012 年提出 Interledger 协议[6]以解决不同区块链系统之间的协同问题；2013 年 5 月，Tier[7]在 BitcoinTalk 论坛上提出了原子转移（atomic transfers），原子转移又称原子交换（atomic swap），是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 3 种中间状态[8]。该方案经过改进后成为一种主要的跨链模式，即哈希锁定模式。随后出现更多创新如莱特币、比特股以及以太坊，加速了比特币核心开发组的危机感。因而，在 2014 年 10 月，BlockStream 首次明确提出了侧链的概念，锚定式侧链（pegged sidechain）利用双向锚定（two-way peg）机制[9]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（sidechain with strong federation），通过引入由多方控制的多重签名地址有效地减少了侧链与主链之间的时延，并提升了互操作性。2015 年，比特币闪电网络（lightning network）[10]中提出利用哈希时间锁（Hashed

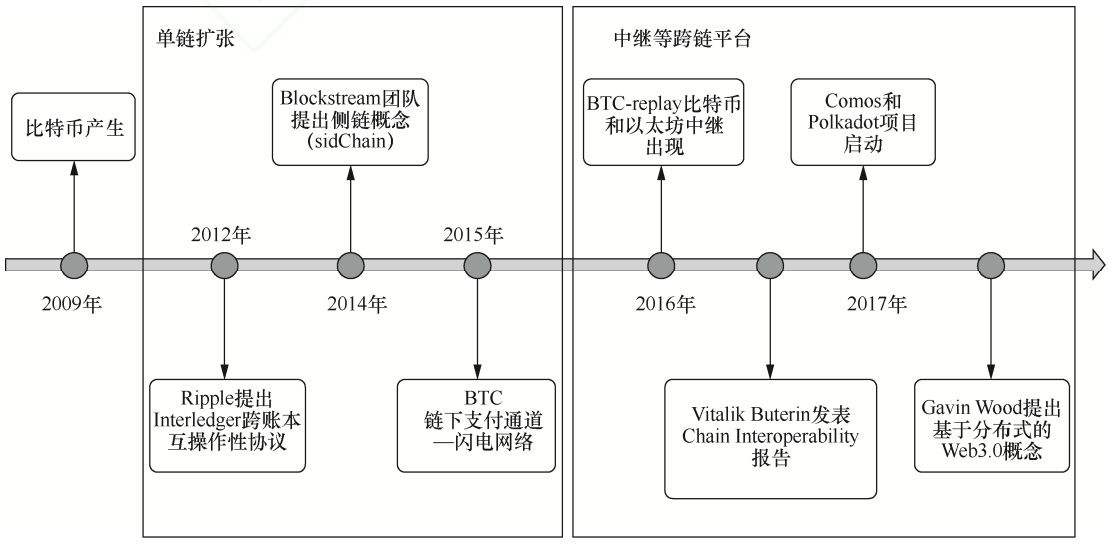

图 1　跨链技术发展历史线

timelock）机制，开通了比特币链下快速交易通道，提高了比特币系统的交易效率。

中继链/跨链平台时期（2016 年—至今）：2016 年，BTC-Relay 提出采用基于中继跨链方案实现比特币到以太坊的单向跨链通信。同年，文献[11]对区块链互操作问题进行了详细、深入地分析。2017 年，跨链项目 Polkadot 和跨链项目 Cosmos 提出了搭建跨链基础平台的方案，通过基础平台可以兼容所有区块链应用，目前这两个项目还在开发中。同年，Polkadot 创始人 Gavin[12]提出一种基于分布式的 Web3.0 概念，其中涉及 Web3.0 催生垄断主义到数据平权运动，而区块链是数据平权运动的急先锋。数据平权运动让 Web3.0 概念自然地产生，Web3.0 不是技术范畴，而是对某个行业应用趋势的抽象化。

2.2　跨链的意义

简单来看，跨链就是让一条链上的代币转移到另一条链上，而区块链上的代币不仅是一种价值，也是一种信息。跨链交易是一种价值的交换，既要保证信息流的精确性，更要保证双向价值流通的可靠性，跨链的意义主要总结为如下两点。

1) 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，区块链系统性能尤其是单链的性能逐渐成为制约区块链发展的瓶颈，通过将部分任务转移到侧链或者链下进行处理，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[13]。

2) 实现跨链互操作

单一的区块链系统相对封闭，不能随意获取外部信息或把链上的信息传输到外部，随着区块链技术的迅速发展，链与链之间的“互操作性”问题逐渐突出，跨链操作的具体应用场景包括但不限于跨链支付结算、去中心化交易所、跨链信息交互等。

2.3　跨链的关键技术问题

自 Blockstream 提出侧链概念以来，跨链一直是区块链技术的一个重点研究内容。目前，跨链机制并没有普遍的适用性，原因在于除了在此之前需求的强烈程度不高之外，技术上的众多难点也是一大障碍。目前，跨链技术面临的主要难点如下。

1) 解决交易的原子性

跨链交易的原子性[14]是指跨链交易只有成功或失败，不存在第 3 种中间状态。一个完整的跨链交易可能由多个子交易构成，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，后续的子交易也能成功；或者后续的子交易失败，前面的子交易能够撤回。

2) 用分布式方式验证另一条链上的交易状态

验证包括两个方面[15]，一方面是交易已经被写入账本并且满足最终确定性；另一方面是进行跨链数据传递，跨链的双方可以验证彼此交易的合法性和有效性[16]。区块链系统需要绝对的信息可靠性，所以大部分系统较封闭，一般不能主动获取外部信息，因此，要确认另一条链中交易的合法性和有效性十分困难，这也是跨链交易的核心难点之一。

3) 两条链上的资产（价值）总量不变且独立安全运行

在资产的跨链互换中，两条链并没有发生实质性的交换，这种交换不会改变各个链的资产总量。在资产的转移过程中，需要减少一个链上的资产，进而在另一条链上增加对应的资产。这种转移使每条链的资产都发生了变化，而要保证这种变化的完全同步性，就要求链的记账必须是原子性的，即都同时记账或都不记。

当两个系统发生交互时，难免会对彼此系统产生影响，如何在完成跨链交易的过程中做到信息可靠，也就是如何保证跨链双方系统的安全性是一个值得思考的问题。若安全性问题无法解决，那么一条链的跨链信息出现问题，将影响整个跨链网络。

4) 跨链平台的实现

若要创造一个独立的区块链网络，需要一个类似计算机互联网的互联平台，而区块链系统中的跨链平台就是要实现各个场景应用以及各种异构链的互操作性。目前，已有许多跨链平台项目正在研究中，如 Cosmos、Polkadot 等项目。但是，目前的跨链研究仍处于初期阶段，要达到真正的商业应用级别，还有许多难点需要解决。

跨链架构如图 2 所示，跨链方式主要分为 3 种：不直接交互、第三方协作交互和区块监听。

3　跨链的 3 种主要机制

跨链交互一般按照参与双方的底层平台技术是否为同构链进行讨论，对于同构链来说，双方的共识算法、区块生成与验证规则、交易广播、安全机制等逻辑都一致，所以跨链交互也相对简单。而异构链的跨链交互相对复杂，如比特币采用 UTXO

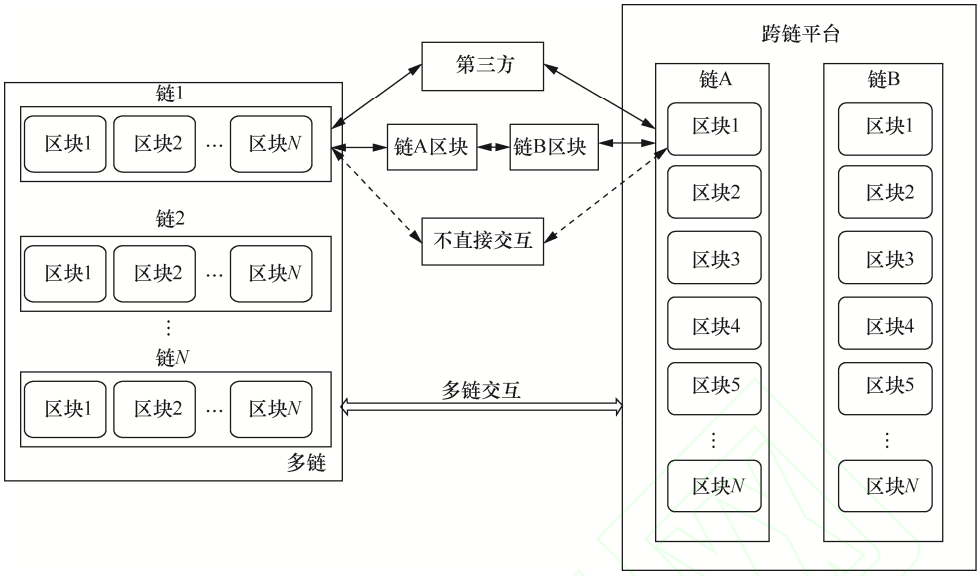

图 2　跨链架构

机制处理交易，而以太坊采用账户机制处理交易，由于区块链的“孤岛”效应，使得一笔交易很难同时被比特币和以太坊处理。异构链的跨链一般需要第三方辅助实现，涉及的具体使用场景不同，也存在去中心化的跨链机制，一般讨论的跨链都是异构链的跨链，跨链的 3 种常见实现技术为哈希锁定、公证人机制和侧链/中继技术。本节对每种跨链技术的实现方式与技术进行了详细介绍与总结。

3.1　哈希锁定

哈希锁定是一种依托于哈希函数的单向性与低碰撞性，同时利用区块链中交易可以延时执行的特点而产生的机制。交易方将设置谜题的交易发布到链上，在指定时间内能够解出谜题的一方便能获得交易的质押金。其中，谜题利用哈希锁定实现。

最早使用哈希锁定技术的项目是比特币的闪电网络项目。闪电网络的愿景是实现一个不需要可信第三方参与的实时海量交易网络，在接触闪电网络之前，需要了解比特币的微支付通道概念。

3.1.1　微支付通道

微支付通道是为了解决金融服务高频小额交易中存在手续费过高的问题而产生的。举例来说，如果每天去咖啡店喝咖啡都用比特币支付，那么每一笔交易产生的手续费可能比咖啡本身还贵，微支付通道对这个问题的解决方案如下。

假设 A 和 B 之间存在一个比特币的微支付通道，A 是消费者，B 是店家。那么，微支付通道的运行机制如下。

1) A 生成一笔 UTXO 交易 Tx_1，解锁条件是提供 A、B 两人的签名（一般采用多重签名方式实现），称 Tx_1 为锁定交易。

2) A 再生成一笔时延的 UTXO 交易 Tx_2，时延时间设为 T_0，交易的输入为之前的 Tx_1，交易的输出是 A 的比特币地址，称 Tx_2 为赎回交易。

3) A 将 Tx_2 发给 B，B 对其进行签名后发回给 A，A 再对 Tx_2 签名后将 Tx_1 和 Tx_2 发布到比特币网络上。

4) 此后每次进行实时支付时，A 只需要生成一笔支付交易 Tx_n（其中，$n>2$），Tx_n 的输入是最初的锁定交易 Tx_1，交易的输出是 A 和 B 各自应得的余额分配，同时设置时延为 T_1，$T_1<T_0$。

A 对支付交易 Tx_n 签名后发给 B，B 不需要发布到链上。以后每次进行支付时，只需要更新这些链下的交易即可。当交易终止时，B 把最近的一笔交易发布到链上即可获得自身应收的比特币。

3.1.2　闪电网络

微支付通道虽然解决了交易双方之间的高频小额支付的高手续费问题，但是支付通道的建立成本较高，需构建两笔交易，若要实现大规模的交易支付网络不够现实。闪电网络的出现是为了复用已存在的支付通道，如 A、B 之间存在支付通道，B、C 之间存在支付通道，那么，A、C 之间就不必再次建立支付通道，而可以通过复用 A、B 与 B、C 之间的支付通道进行支付，这就是闪电网络的作用。

闪电网络基于微支付通道演化而来，在其基础上设计了两种类型的交易合约：序列到期可撤销合

约（RSMC, revocable sequence maturity contract）和哈希锁定合约（HTLC, Hashed timelock contract）。

RSMC 的创建类似于微支付通道的创建流程，在支付通道时间未过期之前，双方都可以通过把最近一笔交易发布到链上而终止这个合约，所以称为序列可撤销合约。而为了让支付通道的声明周期尽量长，RSMC 规定先发起退出的一方会缴纳一部分违约金给另一方。

HTLC 是实现闪电网络的另一个核心，对于没有支付通道的 A、C，如果想进行交易，就可以借用 A、B 和 B、C 之间的支付通道进行交易。如 A 需要转账给 C，那么 A 可以生成一个随机数作为哈希原像，然后利用 A、B 之间的支付通道设置时延 T_1，只有正确给出哈希原像才能解锁交易。作为通道的服务提供者，可以收取一定的手续费。B 利用 B、C 之间的支付通道把交易发送给 C，并设置时延为 T_2，C 因为知道哈希原像，所以可以解锁交易，获得 A 的转账。A 解锁之后，哈希原像就暴露在链上，所以 B 可以利用哈希原像解锁 A、B 之间的锁定交易获得手续费，从而完成闪电网络的构建。

3.1.3 基于哈希锁定的原子互换

原子交换如图 3 所示，基于哈希锁定的原子互换可以保证不同链间资产交易的安全性与原子性，而不需要第三方参与，此方式于 2013 年由 TierNolan 在 Bitcoin 论坛上提出。A 与 B 的原子交换哈希锁机制可以简单描述如下（设 A 使用链 A 上的代币 a 与 B 交换链 B 上的代币 b）。

1) A 产生随机数 s，计算哈希值 $H(s)$，其中，H 表示哈希函数。

2) A 使用 $H(s)$和一个时间 t_1 在链 A 上产生一个合约交易 $Tx_1 = T(H(s), t_1)$，Tx_1 会锁定 A 链上需要交易的代币 a，锁定时间为 t_1。

3) A 把计算的 $H(s)$发送给 B，并发送交易 Tx1 至 A 链上，证明已经锁定了自身的待交易代币 a。

4) B 使用 $H(s)$与时间 t_2 生成合约交易 Tx_2，锁定需要交易的代币 b 并将交易上链，其中，锁定时间为 $t_2(t_2 < t_1)$。

5) A 使用 s 解锁链 B 的锁定交易 Tx_2，获取 Tx_2 锁定的代币 b，此时随机数 s 暴露。

6) B 使用公开的 s 解锁链 A 上的 Tx_1，获取 Tx_1 锁定的代币 a。

交易支持哈希锁定[17]的条件有两个：1) 哈希锁，只有提供目标哈希的原像才能解锁交易；2) 时间锁，只有在指定时间之前完成交易才有效。

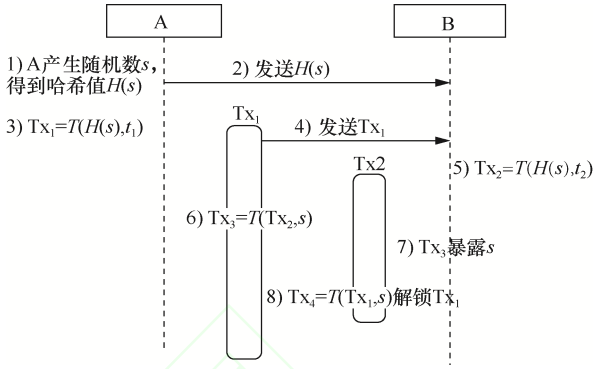

图 3　原子交换

对于比特币系统，资产的哈希锁定可以通过构建 HTLC 完成。假设交易双方为 A 和 B，A 构建 HTLC 需要两笔 UTXO。A 首先产生一个随机数 s，计算 $H(s)$，只有提供原像 s 才能计算出 $H(s)$，实现哈希锁定。然后，A 生成一笔 UTXO 发送一定数量的比特币到一个比特币脚本，脚本中设置 UTXO 的花费条件有两个：1) 提供 B 的签名和原像 s；2) 提供 A 和 B 的签名。通常称这笔交易为存款交易（fund transaction），表示资产的锁定。A 产生另外一笔交易，把存款交易作为第二笔 UTXO 的输入，输出为 A 的地址，同时设置 nTimeLock 字段为 Tlock，表示到达 T 后才允许被打包生效，实现时间锁定，称这笔交易为退款交易（redeem transcation）。这两笔交易共同构成了一个比特币系统上的哈希锁定合约。A 把这两笔交易发给 B，如果 B 同意则在第二笔交易上签名并发回给 A。

对于以太坊这种图灵完备的链而言[18]，可以产生一个合约。合约逻辑设为：在 t 时间内（实现时间锁）如果 A 的地址能提供哈希原像 s（实现哈希锁定），则可取走合约中锁定的资产，然后发送需要锁定的资产到合约上。

比特币闪电网络采用了 HTLC，HTLC 使得没有支付通道的双方也可以通过其他支付通道最终实现资产转移[19]。比特币的支付通道是指利用比特币交易的时间锁定特性，可以在交易双方生成未来生效的交易，在交易生效之前的交易变动都是在链下完成，不必发到链上，最后一笔交易上链清算即可，可以减少手续费开销，提高了交易执行效率。发送方选取随机数 s 生成哈希值 $H(s)$并私下把 s 告知接收人，然后利用自身的支付通道和中间人构建 HTLC，设置时间为 t_1，中间人再通过 H 利用可用

支付通道构建 HTLC，设置时间 $t_2(t_2 < t_1)$，最终实现在连通接收者的支付通道上构建同样的 HTLC。当接收者利用 s 取走支付通道里的比特币时，s 暴露并被依次传到上层 HTLC，最终所有人都可以取走个人应得的比特币。

瑞波的 InterLedger 协议中通用模式的实现也是基于原子交换，其基本原理与闪电网络类似，与闪电网络的区别在于交易双方不在同一条链上，可实现跨多个链的资产交换，前提是这些链都要支持哈希锁和时间锁[20]。原子交换存在如下 3 个缺点。

1) 对于比特币这种非图灵完备的链来说，构建一个 HTLC 需要生成两笔交易，如果交易最终达成，那么这两笔交易都要上链，操作复杂且手续费高。

2) 原子互换要求双方在线完成，这限制了原子交换的交易量。

3) 现实中存在汇率波动，对手方可以根据汇率的波动来选择是否完成这笔交易。

3.2　公证人机制

引入一方或多方可信实体做信用背书的跨链机制都称为公证人机制，公证人机制是技术上可实现的、最简单的跨链机制。在公证人机制中，一个或一组公证人负责监听链上的事件，并对另一条链采取对应的操作。公证人在跨链的双方链上需要有账号进行交易的协调。公证人机制的实现方式包括如下 3 种：1) 单签名公证人机制，即一个节点做公证人；2) 多签名公证人机制，指多个节点利用多签名机制做公证人组；3) 分布式签名公证人机制，指多个公证人持有一份密钥的碎片，密钥碎片随机发给公证人。

瑞波的 InterLedger 协议[21]中原子模式的实现方式是典型的公证人机制，在 InterLedger 协议中，包括发送者、连接者、接收者和公证人等角色。发送者把资产转给公证人组多签地址进行资产托管，接收者确认收到转账后在收据上签名。当前账本公证人根据收据将资产转给连接者，支付链如图 4 所示。

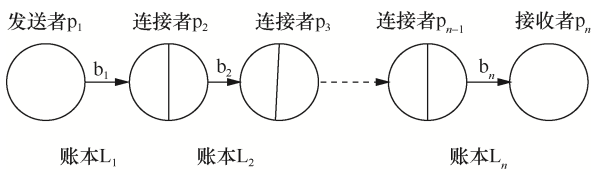

图 4　支付链

每个账本上都有各自选出的公证人 N_i。在准备阶段，发送者 p_1 和公证人 N_1 在账本 L_1 上利用多重签名锁定发送者的资产 b_1。以比特币为例，p_1 可以构建数额为 b_1 的 Tx_1，设定 Tx_1 的输出条件需要 p_1 和 N_1 的签名，然后交易上链实现资产锁定。之后 p_1 构建一笔 Tx_2 花费、Tx_1 锁定的资产，输出给连接者 p_2，对交易签名后把交易交给公证人 N_1 托管，N_1 通知连接者 p_2。连接者 p_2 验证交易正常托管并且数额合理后，在账本 L_2 执行相同的操作然后通知 P_3。以此类推，直到最后一个账本 L_n 上的托管交易构建完成，并通知接收者 p_n，交易的支付链完成准备阶段。

接收者 p_n 确认公证人 N_n 托管了连接者 p_{n-1} 发给个人的 b_n 个代币的交易后，会在一份收据上签名并发给公证人 N_n，N_n 得到收据后就会签名交易使其生效，完成转账。然后把收据发送给上一轮的公证人，每一轮的公证人得到收据后会依次签名托管交易使其生效，最终整个支付链完成交易。

对于跨多个账本的转账，为了保证交易的原子性，公证人会发出 D_Excute 和 D_Reject 两种类型的消息来指导下一组公证人做出决定。公证人验证托管交易（所有托管条件必须取决于公证人的 D_Excute 消息或者 D_Abort 消息，从而保证交易的原子性），然后签发出 D_Execute 消息通知连接者，连接者把资产转给下一组公证人托管，最终转给接收者。接收者决定签发收据或者拒绝接受，各个参与方会把最终结果原路传回所有参与公证人组。如果最终交易成功，则每个参与的连接者会收到各自应得的资产；如果交易最终或者某一步骤失败，则公证人会把资产退回到发起人账户。

公证人机制实现比较简单，已在多数项目中得到应用。但是公证人机制有个明显的缺陷即需要对公证人有足够的信任，对于单节点公证人机制有很大的中心化风险；对于多签名公证人机制，需要目标链上支持多重签名机制。

3.3　侧链/中继技术

2010 年，相关研究者在比特币论坛上提出 bitDNS 想法，以比特币为锚定，在比特币链上扩展出任意资产，这种想法促成了后来的域名币（namecoin）、彩色币（coloredcoin）等附生链。以域名币为例，域名币的实现是通过比特币的第一笔交易（称为 coinbase 交易）写入域名币链的区块头信息，从而使域名币可以借助比特币区块链存在。

域名币等技术的局限是比特币一个区块只有 coinbase 交易才可以写入少量信息。BTC0.9 版本之后，在交易中引入 OP_RETURN 字段，在比特币锁

定脚本中，以 OP_RETURN 字段开头的信息属于“备注信息”，输出到 OP_RETURN 的 UTXO 都是不可花费的 UTXO，相当于销毁了对应数量的比特币。利用这个字段销毁比特币并在备注中写明侧链信息，这个过程又称为 proof-of-burn，侧链可以依据交易证明产生侧链代币。这些想法形成了后来的 omni 协议，USDT 则是遵循此协议在比特币上发行的一种代币。

BlockStream 在 2014 年发表了侧链白皮书，定义了侧链是一条能够验证其他区块链数据的链。在目前的讨论中，侧链大多数还是指 BlockStream 所说的锚定式侧链（pegged sidechain）[22]。而这里所说的锚定式侧链主要是指支持资产的双向锚定，即资产在主链与侧链之间的流通。当前，双向锚定侧链的实现方式包括如下 4 种。

1) 单一托管模式

单一托管模式是实现双向锚定最简单的方式，其基本原理与单一公证人机制相同。交易参与方把数字资产发送给托管方，托管方在侧链上将相应资产发送给交易方侧链账户。

2) 联合锚定模式

联合锚定使用公证人联盟的形式作为资产托管方，利用多重签名的方式来减少单中心的风险。

3) 驱动链模式

驱动链概念是由 Bitcoin Hivemind 创始人 Paul 提出的。在驱动链中，交易处理节点代表公证人组的角色，负责资金托管和解锁。交易处理节点把其他链上的资产锁定信息提交到区块中，发起提案，经过投票与确认之后，在当前链上解锁指定资产。

4) SPV 锚定模式

SPV（simple payment verification）是 Satoshi 在比特币白皮书中提到的概念，指的是轻客户端不需要下载所有区块数据就能对某一笔交易的存在性进行验证[23]。一个 SPV 证明包含两个部分：1) 区块头列表；2) 表示某一输出发生在列表中某一区块的密码学证明，如默克尔证明。

如果要证明某笔交易存在于某个区块内，只需要使用此交易的哈希值与其他相关交易哈希值计算最终的默克尔树根与区块头的树根作比较。如果计算结果与区块头的交易树根一致，则证明交易存在于本区块中。SPV 模式下的双向锚定如图 5 所示。

1) 锁定主链资产，可以使用多签名账户实现。

2) 在主链上等待一个确认期，可以是一天或者两天，确保生成足够的工作量，从而抵抗拒绝服务攻击。

3) 主链确认期结束后，用户可以在侧链上产生一笔铸币交易，并且提供主链锁币交易的 SPV 证明，生成的侧链资产处于锁定状态，需要等待一个竞争期。

4) 用户在侧链上等待一个竞争期，设置竞争期的目的是防止双重花费。如果在竞争期内，用户把主链上锁定的币转走，其他用户可以用最新的 SPV 证明此事，则侧链铸币交易失效，称此证明为重组证明。

5) 竞争期结束后（约 1~2 天），侧链代币生成，可以在侧链流通。

6) 侧链代币返回主链流程重复上述 5 个步骤。

Liquid 是 Blockstream 的开源侧链项目，使用比特币双向锚定技术，Liquid 的目的是实现比特币可以在主链和侧链中互转，旨在提高隐私性、降低成本、加速价值转移及结算流程。

此外，BTCRelay 是一个典型的中继项目，所谓中继是指可以在本链上自行验证另一条链上数据而不需要依赖第三方。BTCRelay 是以太坊上的

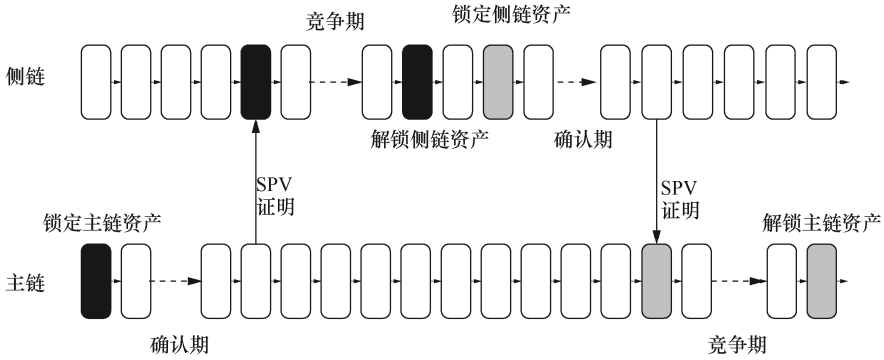

图 5　SPV 模式下的双向锚定

一个智能合约，通过存储比特币区块头使得 BTCRelay 充当一个比特币轻节点。由于比特币的交易是以默克尔树的形式存储并在区块头存储了树根，所以可以利用 SPV 验证交易是否存在。BTCRelay 的正确性取决于是否上传了正确的区块头，BTCRelay 通过设置奖励机制与审查机制来避免存储错误的区块头，BTCRelay 只能实现单向跨链。

4　跨链项目

关于区块链的跨链技术，目前讨论最多的技术是侧链和中继，现阶段的主流项目主要使用的也是侧链/中继技术。大部分区块链跨链项目都是为了解决公链交易吞吐量和交易速度的问题，也就是“可拓展性”问题。侧链主要用于解决这一问题，本节主要介绍目前主流的 4 种跨链项目，并详细讨论了跨链项目的实现。

4.1　Polkadot

2016 年 11 月，Polkadot 在白皮书中提出了一种支持多种链结构的异构多链跨链平台，实现了去中心化、去信任地进行跨链交互。Polkadot 的链不涉及任何功能应用，其通过提供一个中继链（relay-chain），链上以区块链的数据形式存储所有连接到中继链上的其他链的信息，这些信息是可验证、全局依赖的动态数据结构，这些数据来自连接在中继链上的各个独立运行的链，所以称这些平行的、结构化的区块链为平行链（parachain），尽管不要求它们必须是一条链[24]。Polkadot 跨链平台会实现两个非常重要的方面：1) 不同链合并的安全性；2) 去信任的跨链交易性。

网络中的 4 类参与方包括：验证人（负责验证平行链的数据）、收集人（负责采集平行链的数据并提交给验证者）、提名人（为验证者提供押金和信用背书）和钓鱼人（负责举报和证明恶意行为），跨链架构如图 6 所示。

验证人：在 Polkadot 中继链上有最高权限，主要负责验证收集人所收集的各平行链的区块，对其打包并记录在链上。

提名人：是一个拥有权益的群体，可以选择验证人，将自身拥有的权益质押给验证人，即验证人是由提名人选举的。通过这种质押让信任的验证人代表其维护整个网络，同时也会受到和验证人相同比例的奖励和惩罚。

收集人：主要任务是在各个平行链中收集全部必要的交易信息，打包并执行相应的交易，然后将执行交易的结果附上一个零知识证明，提交给该平行链的验证人。

钓鱼人：相当于 Polkadot 网络中的检察官，不直接参与区块打包的过程，减少了网络中恶意行为的发生。钓鱼人可以通过举报一个有质押的参与方存在的非法行为，并提供带有签名的有效证明，就能获得奖励。非法行为包括验证人对两个有相同父块的不同区块进行签名，或者在平行链上验证通过一个无效的区块等。

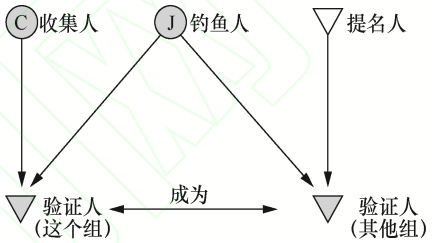

图 6　跨链架构

Polkadot 通过与平行链之间的信息通道以及通信规则进行跨链通信，统一的通信规则使得 Polkadot 成为一个可伸缩的跨链平台，即一条平行链中执行交易时，可以给第二条平行链或中继链转发一个交易。

在 Polkadot 网络中，跨链交易使用了一个队列机制，这个队列用默克尔树的数据结构来保证数据真实性。交易从出口队列通过中继链的转发进入目标链的入口队列，被转发的交易会被中继链记录。这些队列由中继链管理，由于跨链交易的原子性，如果一条跨链交易在任何一个环节出现问题，那么这笔交易经过的整个过程都作废，由中继链负责传递交易的验证和执行结果。Polkadot 整体框架如图 7 所示。

在系统架构上，Polkadot 由一个中继链、若干平行链以及异构链的转接桥 Bridges 组成，如图 7 所示。

中继链的主要功能是转发各平行链产生的跨链交易，记录各平行链的交易状态，并传递交易的验证和执行结果，它是一个具有安全共识的网关。Polkadot 在中继链上的共识算法是拜占庭容错（BFT, byzantine fault tolerance）算法，通过 BFT 使有效区块达成共识[25]。中继链本身不包含任何交易，只负责最顶层跨链交易的路由，应用均在平行

链上进行开发和部署。

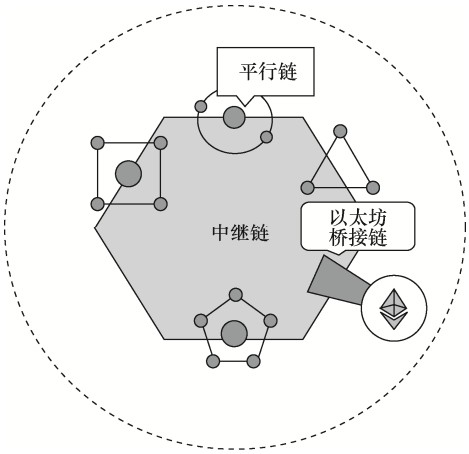

图 7　Polkadot 整体框架

平行链用于 Polkadot 网络中应用的开发与部署，其各自并行存在，但是都依赖于中继链提供的安全性保证。在平行链中可以使用不同的区块链底层技术，应用的开发者可以根据特定领域的问题，选择平行链的底层区块链系统，如不同的共识算法、区块结构等。

转接桥是针对异构链开发设计的一个跨链结构，如当以太坊需要与 Polkadot 中继链进行交互时，以太坊的数据需要通过针对以太坊底层系统专门开发的转接桥结构，对跨链的信息进行规范化处理，才能转换成在 Polkadot 网络中交互所需的模式。

4.2　Cosmos

Cosmos 对跨链[26]部分的设计与 Polkadot 的某些理念相似，通过一个中间链对跨链信息进行中转，从而创造一个异构的跨链平台。在 Cosmos 中提出了两个新的概念 Hub 和 Zone：Hub 是用于处理跨链交互的中继链，Zone 是 Cosmos 中的平行链。

为了支持平行链之间的跨链互操作，Cosmos 提出了一种跨链交互协议 IBC（inter-blockchain communication protocol）[27]，并利用 tendermint 共识算法的即时确定性实现多个异构链之间的价值和数据传输。因此，Cosmos 中平行链需要具备如下两个前提条件。

1) 快速确定性（fast finality）：该特性由共识算法保证，即 Cosmos 的跨链不直接支持概率确定模型的区块链。

2) 强监管性（sovereignty）：每个平行链都具备一组验证者能够决定其出块。

也就是说，如果要连接概率链（如以太坊），需要额外的结构支持，为此，Cosmos 提出了 Cosmos-Bridge 链，负责与概率链完成异构跨链。

Cosmos 网络之外的其他异构链如果需要接入 Hub，则需要通过一个 Bridge-Zone 转接层，该转接层的作用是对异构链的跨链交易进行中转，并对跨链信息的数据结构进行规范化处理。Bridge-Zone 负责对接 Hub 与其他异构链，包括对原链的交易确认、在 Cosmos 网络中生产或销毁相应代币等工作。Cosmos-Bridge 跨链通信如图 8 所示，如果以太坊网络中的用户要把资产转移到 Cosmos 网络中，首先需要在以太坊上部署一个 Bridge-Contract 智能合约，在智能合约中可以编写跨链交互的规则与逻辑，并负责跨链交易的处理。当用户需要转账到 Cosmos 时，可以先将以太坊区块链的代币（ETH）转移到 Bridge-Contract 合约中，ETH 转移到合约后将被锁定，如果跨链交易失败，那么系统将被回退到交易执行前的状态。或者当 Bridge-Contract 检测到 Cosmos 有跨链交易时将资产转移到以太坊，那么合约中将解锁相应的资产，Bridge-Contract 会追踪 Bridge-Zone 验证节点的状态，Cosmos-Bridge 可以和 Cosmos Hub 共享同一组验证节点。当跨链交易被 Bridge-Zone 的验证节点接收时，将对以太坊发送给 Bridge-Contract 智能合约的交易进行验证。验证通过将在 Bridge-Zone 生成对应的 Cosmos-ETH（SPV 验证）[28]。将 Cosmos-ETH 转移到以太坊的过程也类似，不过 Bridge-Zone 转到以太坊的 Cosmos-ETH 将被销毁，而冻结在 Bridge-Contract 的 ETH 会被解锁，并转移到某账户地址中。

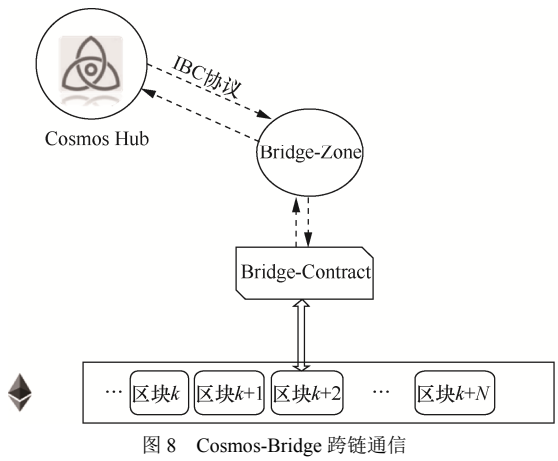

图 8　Cosmos-Bridge 跨链通信

Cosmos 的 IBC 协议是实现跨链的关键部分，IBC 协议用于该网络的枢纽及各个分区的沟通。代币可以安全、快速地从一个 Zone 传递到另一个

Zone，两者之间无需体现汇兑流动性。枢纽会将每个 Zone 与其他故障 Zone 隔离开，当新的分区产生时，在线治理社区的投票会决定新的分区是否可以连接到 Cosmos 枢纽，所以 Cosmos 也可以支持未来新的安全高价值区块链接入。具体来看，当 Zone1 向 Zone2 发出跨链消息时，Zone1 先产生消息分组，并将其证明发布在 Hub 上。接下来，Hub 会生成 Zone1 的跨链消息分组已在 Hub 上的存在证明发布于 Zone2。然后，Zone2 收好消息分组，并给出证明发布于 Hub 上。最后，Hub 再给出 Zone2 的收妥证明发布于 Zone2，完成整个跨链消息传递。以 Zone1 平行链向 Zone2 平行链转移代币的过程为例，说明 IBC 跨链通信协议的详细过程，IBC 通信协议时序如图 9 所示。

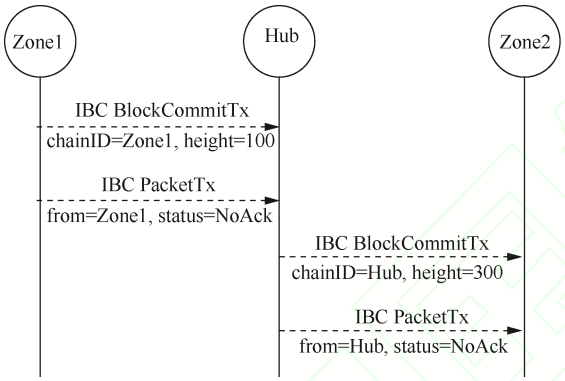

图 9 IBC 通信协议时序

1) Zone1 发起一笔 IBC BlockCommitTx 交易 γ，将其区块的头部信息 h 以及所有验证人的公钥信息 $\{P_i\}$ 传递到 Hub 上，该交易为

$$\gamma := \langle h, \{P_i\} \rangle \tag{1}$$

2) 当 Zone1 发起一笔代币转移交易 φ 时，Zone1 先对该交易进行合法性验证，如果有效则将该交易发送到自身的出口队列中，等待被发送给 Hub，该笔交易可以表示为如式(2)形式，f 是交易的发起 Zone，h_t 是在发起 Zone 中确认的区块高度，t 是目的 Zone。

$$\varphi := \langle f, h_t, t \rangle \tag{2}$$

3) Zone1 的中继程序将消息队列中的交易生成默克尔证明用于 Hub 对交易的验证，并作为 IBCPacketTx 的有效载荷发送到 Hub。

4) Hub 中的验证者验证默克尔证明是否有效，若有效则发送消息给 Zone2（Hub 给 Zone2 发送消息的过程重复上述步骤）。

5) Zone2 在接收到 Hub 发送的跨链交易后，验证其为 Zone1 发起的真实有效交易，并发送消息给 Hub 确认可接收来自 Zone1 的资产。

6) Hub 给 Zone2 发送消息，将资产发送给 Zone2，到此完成了资产在不同区块链之间的一次转移。

目前，Cosmos 已经有一些应用案例，如作为以太坊的二级扩容方案。以太坊在此之前已经有以太坊共识协议 Casper 作为一级的扩容方案，目标是让以太坊能转向 POS（proof of stake）共识机制。而 Cosmos 在设计时也为以太坊做了一个以太坊虚拟机（EVM）的兼容，并且其底层采用一种 POS 协议 tendermint 的区块链称为 Ethermint。2017 年，以太坊创始人 Vitalik 代表以太坊生态基金会 ECF（Ethereum Community Foundation)与 Cosmos 合作，Cosmos 将为以太坊的二级扩容开发做出贡献。

如果以太坊自身的网络因为扩容不够而导致以太坊上的应用无法正常运行，那么可以通过 Cosmos 给以太坊提供 Hub，将以太币转到 Cosmos 的 Ethermint Zone 上，当然该 Zone 可以开发出多个。如在 2017 年以太坊的网络因为“加密猫”游戏的流行拥堵不堪，如果这个应用在 Cosmos 为以太坊开辟的 Zone 中运行，这些“猫”之间的交易可以在 Zone 中自由进行，如果要回到以太坊，可以通过 Zone 的跨链机制随时转移到以太坊上。Cosmos 的扩容功能更像是侧链，但却比侧链更具有灵活性的跨链应用。

如果从 Cosmos 反观跨链的意义，就可以真正看到跨链不仅可以扩容，更可以提高可操作性。如果想对比特币进行智能合约的编程，可以直接借助 Cosmos 的 Hub 把比特币转到以太坊进行编程。同时，如果想让比特币的私密性更强，可以直接借助 Cosmos 的 Hub 使比特币转到门罗币的网络。

4.3 Plasma

Plasma 是以太坊的一种二层协议扩容方案[29]，因为扩展以太坊的交易 TPS（指 1 s 内能处理的交易数）而被提出。与闪电网络相似，Plasma 是一系列运行在区块链上的智能合约，通过智能合约与侧链间接交互实现跨链[30]。这样可以实现将主链上的交易转移到侧链（线下）执行，主链只记录一段时间侧链上执行的结果，大幅度提升了交易的执行效率。Plasma 的实现有多个版本，本节主要介绍了 Plasma MVP 的实现。

Plasma MVP 基于 UTXO 模型，只支持转账，

不支持智能合约的部署与脚本执行。Plasma 侧链中的共识机制采用授权证明（POA），依赖一个管理者节点生成侧链区块，然后把侧链状态提交到主链上，Deposit 实现流程如图 10 所示。

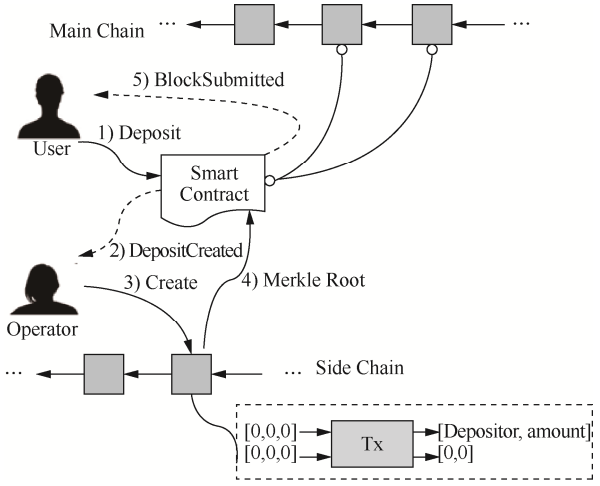

图 10　Deposit 实现流程

1) 用户（User）向主链智能合约发起一个 Deposit 调用的交易 Tx，交易执行后会产生一个 DepositCreated 的事件。

$$\mathrm{Tx} := \langle \mathrm{Deposit}, \mathrm{amount} \rangle \tag{3}$$

2) 管理者（Operator）监测到该事件后，创建一个只包含一笔交易的区块，为用户创建侧链资产 Creat (DepositCreated, amount)。

3) 侧链上的交易 Tx_1 由两个输入 UTXO 和两个输出 UTXO 组成，在充值情况下，只有第一个输出有值，其他输出都为 0。

$$\mathrm{Tx}_1 := \langle \text{输入}(U_{i1}, U_{i2}),\ \text{输出}(U_{o1}, U_{o2}) \rangle \tag{4}$$

4) 管理者把该区块的默克尔树根提交到主链智能合约，合约会发送 BlockSubmitted 事件。用户可以监听到这个事件，并验证其有效性。

如果用户要把侧链资产重新转回主链，则需要启动退出（Exit）流程，Exit 实现流程如图 11 所示。

1) 用户向主链智能合约发起一个 startExit 调用，同时提供一笔保证金（EXIT_BOND）。

$$\mathrm{Tx}_{\mathrm{Exit}} = \mathrm{startExit}(\mathrm{Exit\_bond}, \mathrm{account}) \tag{5}$$

2) 合约把该请求放入一个优先队列中，优先级排名等于区块高度 h_t × 1 000 000 000 + 区块中交易 index × 10 000 + 交易中 UTXO 的 index。从而保证在出现非法交易时，之前的所有合法 UTXO 都可以安全退出。

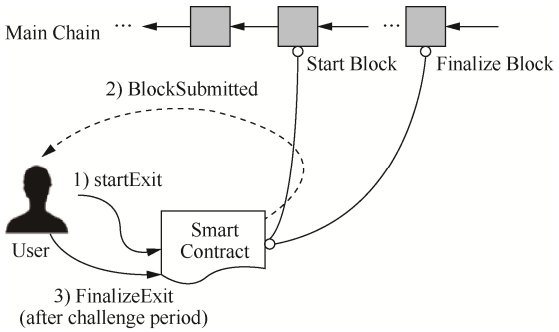

图 11　Exit 实现流程

$$\mathrm{rank} = h_t \times 1\,000\,000\,000 + \mathrm{Tx}_{\mathrm{index}} \times 10\,000 + U_{\mathrm{index}} \tag{6}$$

3) 退出请求需要等待一段时间才能生效，可以理解为“公示”。等待时间长度等于 Max((UTXO 创建时间+2) 周，(当前区块时间+1) 周)，即最快 7 天、最慢 14 天即可完成提现操作。

在用户申请退出期间，其他用户可以发起挑战退出（challengeExit），提供一个有效的默克尔证明，如果挑战成功，那么被挑战的交易将从 Exit 的退出申请队列中删除，同时把 EXIT_BOND 作为奖励转给发起挑战的用户。ChallengeExit 实现流程如图 12 所示。

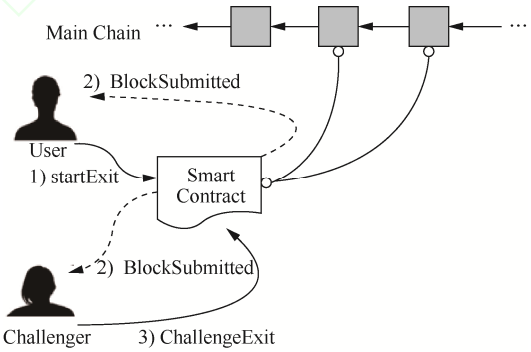

图 12　ChallengeExit 实现流程

5　总结与分析

在现有的区块链跨链项目中，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从主网上线以来，节点数量、通道数量和网络容量一直在增长，技术可行性得到了较好的验证[31]。然而，现有的跨链技术方案在不同方面存在一定的缺陷。

1) 公证人机制：公证人机制通常也被称为见证人机制，本质上是一种采用第三方中介跨链的方案。跨链的双方首先需要选择一个共同信任的第三方作为中介，由双方共同信任的中介负责将跨链的消息或交易打包转发到双方的链上。其优点在于能

够通过简单的方式实现跨链，并支持不同结构的区块链跨链，仅要求公证人能访问双方链上的信息。这种方案的缺点较明显，首先该跨链方式在一定程度上违反了区块链去中心化的特性，公证人存在修改跨链信息的可能，即存在中心化的风险。

2) 哈希锁定：最早起源于比特币闪电网络的哈希锁定技术主要利用原子交换实现跨链。其优点是通过对交换信息进行哈希运算并锁定，可以保证交换信息的真实性；缺点在于哈希锁定只能做到交换，而不能做到信息或资产的跨链转移，使用场景受到极大地限制。基于哈希锁定的资产转移实现有一个窗口期，窗口期内的汇率波动需要考虑；此外，使用哈希锁定需要构建多笔交易，操作复杂。

3) 侧链：侧链是一个和主链相对独立运行的区块链，其运行依赖于主链。侧链实现的技术基础是双向锚定（two-way peg），通过在侧链和主链中锁定资产，并提供有效验证方式，从而在其主链或侧链上生成或释放等价值的资产。优点是这种跨链实现方式简单，侧链相对于哈希锁定技术能提供更多的实现场景；缺点是侧链的实现通常需要利用智能合约，随着交易量的增多，智能合约内部的数据存储存在膨胀问题，可能会造成交易处理速度慢，甚至出现交易堵塞的情况。

4) 中继链：中继链本质上是公证人和侧链机制的融合和扩展。其优点是提供了一个跨链交互的平台或中继区块链，各种不同的链都可以接上中继链，实现跨链交互，极大地提高了实用性；缺点是该跨链实现方式复杂，开发难度大，并且在一定程度上依赖于自身的一套跨链协议，对异构链的接入存在一定困难[32]。另外，中继链与各平行链的安全性在一定程度上也受到链双方的影响，如 Polkadot 的平行链之间的安全性保证主要来自共享安全。

区块链因其在许多领域的适用性及其影响而备受关注[33]。但是，为了让区块链满足各种应用场景的需求，必须解决可伸缩性问题。本节将比较并分析上述 4 类区块链扩容方案的性能，根据各方案对区块链系统的吞吐量、成本以及容量带来的影响，进而比较其解决方案的优缺点，扩容方案的比较分析如表 1 所示。

综合上述主流的跨链场景和方案分析，一个成功的跨链交互需要解决以下 4 个问题。

1) 跨链信息的真实性证明，即该信息是否确实存在于 A 链上，是否确实是 A 链发送给 B 链的。

表 1　　扩容方案的比较分析

类别	方案	吞吐量	成本	容量
链上扩容	Big block	↑	↓	↑
	Segwit	↑	↓	—
	Bitcoin-NG	↑	↓	↓
	Sharding	↑	—	↓
链下扩容	Lighting Network	↑	↓	↓
	Raiden Network	↑	↓	↓
侧链/子链	Plasma	↑	—	↓
	ZK Rollup	↑	↑	↓
	Polkadot	↑	↑	↑
	Cosmos	↑	↑	↑

2) 跨链信息的路由，如何做到让跨链消息安全、可靠地跨系统路由。

3) 跨链信息的有效性证明，此有效性是指来自 A 链的消息如何让 B 链认可其到达 B 链时的状态仍然是有效的，如转移的资产是否是冻结的，有没有发送双花（即在区块链里指同一笔资产使用了多次，造成系统总资金不对称的后果）的可能，该状态是否在路由期间未发生改变等。

4) 跨链信息的执行结果证明，即 *A* 链需要确认跨链操作是否成功以及成功操作的相应回执。

6　结束语

针对目前跨链技术遇到的关键性问题，一种有效的方式是设计一个在底层平台就遵循统一的跨链协议标准的区块链系统，就像现在的操作系统对 TCP/IP 协议的支持一样。而通用的区块链跨链系统需要支持以下 5 方面内容。

1) 提供跨链消息的输入和输出口径，如 Cosmos 和 Polkadot 的跨链队列。

2) 提供跨链消息的真实性证明，区块链需要提供类似 SPV 的证明方法。

3) 消息的有效路由需要构建跨链消息的统一格式，定义消息的来源和去处以及消息的内容，如 Cosmos 的 IBC 协议。

4) 消息状态的有效性证明，区块链可能需要设计新的、类似 UTXO 的可验证存储结构，方便做类似 SPV 的证明方案，否则目前的基于 KV（key value）的数据存储方式很难做有效性证明。

5) 跨链执行结果证明，与有效性证明类似，需要全新的数据结构和运行算法支持该功能。

除此之外，跨链系统的设计还需要考虑系统的稳定性、可扩展性以及如何升级系统、容错等方面。总之，跨链技术在过去几年间发展迅速，但目前的跨链技术尚未完全成熟，没有得到广泛应用，仍有较大的提升空间。一方面，跨链所面临的技术问题有一定的复杂性；另一方面，区块链技术在飞速发展，区块链的类别和技术复杂度也在不断提升，导致对于跨链技术更迭的要求不断提高。其次，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与发展，随着区块链行业应用的逐步落地和不断丰富，对跨链的需求也必定不再局限于交易。

参考文献：

[1] KOENS T, POLL E. Assessing interoperability solutions for distributed ledgers[J]. Pervasive and Mobile Computing, 2019, 59: 101079.

[2] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[R]. Manubot, 2019.

[3] AMOUSSOU-GUENOU Y, DEL P A, POTOP-BUTUCARU M, et al. Correctness and fairness of tendermint-core blockchains[J]. arXiv: 1805.08429, 2018.

[4] 祝烈煌, 董慧, 沈蒙. 区块链交易数据隐私保护机制[J]. 大数据, 2018, 4(1): 46-56.
ZHU L H, DONG H, SHEN M. Privacy protection mechanism for blockchain transaction data[J]. Big Data Research, 2018, 4(1): 46-56.

[5] VITALIK B. Ethereum 2.0 mauve paper[S]. 2016.

[6] HOPE-BAILIE A, THOMAS S. Interledger: creating creating a standard for payments[C]//Proceedings of the 25th International Conference Companion on World Wide Web. 2016: 281-282.

[7] HERLIHY M. Atomiccross-chain swaps[C]//Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing. ACM, 2018: 245-254.

[8] YIE A, CASALLAS R, DERIDDER D, et al. Realizing model transformation chain interoperability[J]. Software & Systems Modeling, 2012, 11(1): 55-75.

[9] ASGAONKAR A, KRISHNAMACHARI B. Solving the buyer and seller's dilemma: a dual-deposit escrow smart contract for provably cheat-proof delivery and payment for a digital good without a trusted mediator[C]//2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE, 2019: 262-267.

[10] POON J, DRYJA T. The bitcoin lightning network: scalable off-chain instant payments[J]. DRAFT Version 0.5, 2015.

[11] BUTERIN V. A next-generation smart contract and decentralized application platform[J]. White Paper, 2014, 3: 37.

[12] WOOD G. Polkadot: vision for a heterogeneous multi-chain framework[J]. White Paper, 2016.

[13] BUTERIN V. Ethereum sharding faq[S]. 2017.

[14] BUTERIN V. A next-generation smart contract and decentralized application platform[J]. White Paper, 2014, 3(37): 1-36.

[15] 钱卫宁, 金澈清, 邵奇峰, 等. 区块链与分享型数据库[J]. 大数据, 2018, 4(1): 36-45.
QIAN W N, JIN C Q, SHAO Q F, et al. Blockchain and sharing database[J]. Big Data Research, 2018, 4(1): 36-45.

[16] TEUTSCH J, REITWIEßNER C. A scalable verification solution for blockchains[J]. arXiv: 1908.04756, 2019.

[17] NAOR M, WIEDER U. A simple fault tolerant distributed hash table[C]//International Workshop on Peer-to-Peer Systems. Springer, Berlin, Heidelberg, 2003: 88-97.

[18] WARREN W, BANDEALI A. 0x: an open protocol for decentralized exchange on the ethereum blockchain[S]. 2019.

[19] SASSON E B, CHIESA A, GARMAN C, et al. Zerocash: decentralized anonymous payments from bitcoin[C]//2014 IEEE Symposium on Security and Privacy. IEEE, 2014: 459-474.

[20] BUCHMAN E. Tendermint: byzantine fault tolerance in the age of blockchains[D]. , 2016.

[21] HOPE-BAILIE A, THOMAS S. Interledger: creating a standard for payments[C]//Proceedings of the 25th International Conference Companion on World Wide Web. 2016: 281-282.

[22] BACK A, CORALLO M, DASHJR L, et al. Enabling blockchain innovations with pegged sidechains[J]. 2014, 72.

[23] BAIRD L. The swirlds hashgraph consensus algorithm: fair, fast, byzantine fault tolerance[J]. Swirlds Tech Reports SWIRLDS-TR-2016-01,2016.

[24] POON J, BUTERIN V. Plasma: scalable autonomous smart contracts[J]. White Paper, 2017: 1-47.

[25] EYAL I, GENCER A E, SIRER E G, et al. Bitcoin-NG: a scalable blockchain protocol[C]//13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16). 2016: 45-59.

[26] KWON J, BUCHMAN E. A network of distributed ledgers[J]. Cosmos, 2018: 1-41.

[27] KWON J. Tendermint: consensus without mining[J]. Draft v. 0.6, fall, 2014, 1: 11.

[28] BUTERIN V. Ethereum 2.0 mauve paper[C]//Ethereum Developer Conference. 2016.

[29] WOOD G. Ethereum: a secure decentralised generalised transaction ledger[J]. Ethereum Project Yellow Paper, 2014, 151(2014): 1-32.

[30] POON J, BUTERIN V. Plasma: scalable autonomous smart contracts[J]. White Paper, 2017: 1-47.

[31] CORBET S, LUCEY B, YAROVAYA L. Datestamping the bitcoin and ethereum bubbles[J]. Finance Research Letters, 2018, 26: 81-88.

[32] MAYMOUNKOV P, MAZIERES D. Kademlia: a peer-to-peer information system based on the XOR metric[C]//International Workshop on Peer-to-Peer Systems. Springer, 2002: 53-65.

[33] 查选, 王旭, 倪巍, 等. 区块链技术的一致性和容量的研究与发展及在物联网中的应用[J]. 物联网学报, 2017, 1(1): 21-33.
ZHA X, WANG X, NI W, et al. Blockchain for IoT: the tradeoff between consistency and capacity[J]. Chinese Journal on Internet of Things, 2017, 1(1): 21-33.

[作者简介]

郭朝（1994– ），男，湖南邵阳人，深圳大学硕士生，主要研究方向为区块链原理与技术。

郭帅印（1995– ），男，安徽阜阳人，深圳大学硕士生，主要研究方向为区块链原理与技术。

张胜利（1978– ），男，河北沧州人，博士，深圳大学教授、博士生导师，物理层网络编码创始人，主要研究方向为无线网络、区块链、物理层网络编码等。

宋令阳（1979– ），男，辽宁人，吉林大学学士、英国约克大学博士、挪威奥斯陆大学博士后、英国飞利浦研究院高级研究员，现为北京大学博雅特聘教授、学科建设办公室副主任、电子学系副主任、信息与通信研究所所长。主要研究方向为无线通信网络、信号处理和机器学习。

王晖（1969– ），男，陕西西安人，博士，深圳大学教授、博士生导师，主要研究方向为物联网、无线网络等。