题目：跨链技术综述

姓名：罗晨刚

学号：22151056

摘　要

本文简要介绍了区块链、跨链技术的概念。本文介绍了跨链技术的研究现状，并详细介绍了哈希时间锁定、公证人机制、侧链。本文还简要介绍了跨链技术的应用。

关键词：跨链技术；区块链；侧链

ABSTRACT

This article briefly introduces the concepts of blockchain and cross-chain technology. This paper introduces the research status of cross-chain technology, and introduces hash time lock, notary schema, and sidechains in detail. This paper also briefly introduces the application of cross-chain technology.

Key words： cross-chain technology； blockchain； sidechains

目 录

第一章　绪论

1.1 区块链技术背景介绍

区块链是一种在不受信任的对等节点之间共享数据的新技术，是一个只支持增加的分布式数据库。区块链允许节点出现拜占庭错误。拜占庭错误包括节点崩溃、节点无法访问、网络延迟或节点的恶意行为。由于使用了加密算法，已记录在区块链中的数据通常无法删除或更改。

为了使区块链不同节点上存储的副本达到一致，需要有共识机制。共识机制是一种用于在区块链的不同节点之间协商区块链当前有效状态的算法。由于分布式系统中的相关特性的固有权衡，共识机制要么达到完全确定性，要么达到概率确定性。在概率确定性中，仅假设数据最终以一定的概率达成共识。

一般来说，区块链分为三种不同的结构：公有链、私有链和联盟链。在公有链中，任何人都可以使用自己的节点加入分布式账本，该节点在读取和写入分布式账本方面具有相同的权限。公有链主要采用仅达到概率确定性的共识机制。而联盟链设计的共识机制达到了完全确定性，因此不会分叉或者仅仅在短时间内分叉。

在区块链中，资产在智能合约的控制下进行转移，智能合约是发布在区块链上的脚本，用于建立和执行将资产从一方转移到另一方所需的条件。

区块链的数据被组织在一个只支持增加的账本中，该账本在多个节点之间复制，这些节点通过共识机制进行数据同步。然而根据著名的 CAP 定理[1]，在任何一个分布式系统中，一致性（Consistency）、可用性（Availability）、分区容错性（Partition tolerance）这三个性质最多只能同时实现两点，不可能三者兼顾。开发人员面临区块链特性的固有权衡。

因此，虽然一种区块链设计可以很好地适用于某个特定使用案例，但它可能不适合于其他使用案例。一刀切的区块链设计是不现实的，这导致了各种不同区块链的出现，每个区块链都单独运行。

1.2 跨链技术的意义

区块链可以在不受信任的节点之间达成基于交易的共识。由于不同区块链之间的独立性，完成不同区块链之间的资产交换是困难的。由此产生了跨链技术的需求。

跨链技术（cross-chain technology）对于克服单个区块链的局限性和防止出现价值孤岛非常重要。跨链技术使得不同的区块链能够互操作。目前异构区块链系统之间的跨链存在很大的障碍。

1.3 研究现状

在文献[2]中，作者构建了一个名为 Practical AgentChain 的跨链交易系统。各种加密货币可以映射到 Practical AgentChain 上对应的代币进行交易。一个或多个交易操作者可以自发地在现有区块链上形成一个服务存款池，并使用代理合约注册一个交易组以获取利润。各交易集团均竞争性地提供跨链交易服务。有兑换币种需求的客户可以自由选择合适的交易组来请求服务，例如将资产映射到代币或提取代币。交易组的选择是根据组的存款和代理合约上记录的组成员的声誉做出的。此外，作者设计了公正的服务仲裁机制和保证金分配方案，以保证系统的可靠性。

大多数现有的解决方案都采用中心化系统来控制物联网设备，这带来了物联网数据管理中的隐私和安全问题。在文献[3]中，作者提出了一个跨链框架来集成多个区块链，以实现高效和安全的物联网数据管理。作者的模型基于公证人机制合并不同渠道中的交易并进行确认。

在文献[4]中，作者提出了一种基于组件的框架，用于在任意区块链系统之间交换信息，称为交互式多区块链架构。作者提出的协议在跨链场景中提供了具有原子性和一致性的交易。

第二章　跨链模型

现有的跨链技术研究主要是建立在实践中的发现之上。所以到目前为止，对跨链技术的研究成果是零散的[5]。目前常见的跨链模型可以分为三种：哈希时间锁定、公证人机制和侧链。其中侧链也就是中继链。根据需要跨链的内容，跨链又可以大体分为资产交换和信息交换。目前资产交换主要依靠中心化交易所来完成，但是去中心化交易所已经处在发展和研究之中。

2.1 基于哈希时间锁定的跨链

哈希时间锁定和普通的区块链交易的不同之处在于采用了哈希锁和时间锁的技术。收款人需要主动在时间锁指定的限定时间内进行收款操作，否则加密货币自动退回原账户。

哈希时间锁合约在 t 期间使用哈希值 sh 锁定资产。当在时间段 t 内提供哈希值等于 sh 的原始数据 s 时，资产被解锁。

哈希时间锁定合约通常用于跨链资产交换，该解决方案可以容忍交易失败[6]。

2.1.1 原子跨链交换

原子跨链交换是一种分布式协调任务，多方在多个区块链之间交换资产，例如用比特币换以太币[7]。

原子交换协议保证：

（1）如果所有各方都遵守协议，那么所有交换都会发生。

（2）如果某个联盟偏离协议，那么没有遵守协议的一方最终会变得更糟，并且

（3）没有联盟有偏离协议的动机。

然而交换协议仍然容易受到拒绝服务攻击。对手反复提出有吸引力的交换，然后未能完成协议，触发退款，但暂时无法访问资产。

2.1.2 手动资产交换

手动资产交换(Manual Asset Exchange)是最简单的跨链技术模式。手动资产交换遵循金融交易的典型生命周期：结算、订单匹配和清算。在第一阶段，A 结算一个新的资产交换订单，A 使用某个秘密（比如哈希值的原像）将资产锁定在

相应的分布式账本上。在第二阶段，A 必须找到相应的交易所合作伙伴 B 对订单的资产汇率达成一致，比如 1BTC 兑换 10ETH。在手动资产交换中，此类订单匹配是在链下进行的，例如通过个人互动进行。双方约定交换后，B 将资产锁定在对应的分布式账本上。在第三阶段，订单清算，实际资产交换发生。因此，A 和 B 交换秘密，分别解锁锁定的资产。通常，手动资产交换不采用自动订单匹配。手动资产交换可能受到欺诈。如果 A 先收到 B 的秘密，并且没有机制作为回报来解锁 A 的秘密，则 A 可以使用 B 的秘密来解锁 B 的资产，而无需将自己的资产转移 B。这将导致 B 的财产损失。为了防止交易双方进行欺诈活动，原子性对于资产交换至关重要。手动资产交换实现原子性最突出的协议是原子跨链交换协议，它基于哈希时间锁定合约。

下面简单介绍一个使用哈希时间锁定完成跨链资产交换的例子。假设比特币网络上的 Alice 需要用 BTC 换取 ETH，而以太坊上的 Bob 需要用 ETH 换取 BTC。假设双方约定用 1BTC 来交换 10ETH，并且双方都在这两个网络上有账户。

1) 首先 Alice 生成一个只有自己知道的秘密数 s，通过哈希操作得到一个哈希值 Hash(s)，并把这个哈希值告诉 Bob。

2) Alice 在比特币网络上发起一笔交易，转账 1BTC 给 Bob 在比特币网络上的账户，条件是在超时时间 T1 内，Bob 可以提供 Bob 的签名和一个秘密数 s'使得 Hash(s') = Hash(s)。

3) Bob 在以太坊网络上发起一笔交易，转账 10ETH 给 Alice 在以太坊网络上的账户，条件是在超时时间 T2 内，Alice 可以提供 Alice 的签名和一个秘密数 s'使得 Hash(s') = Hash(s)。其中 T1 > T2，Bob 出于对自己利益的考虑会这么设置，否则 Bob 的 10ETH 将被 Alice 无偿转走。

4) Alice 在以太坊网络上提供自己的签名和秘密数 s，从而得到 Bob 转的 10ETH，此时公开了秘密数。

5) Bob 在以太坊网络上看到公开的秘密数 s 后，用自己的签名和秘密数 s 获得 Alice 在比特币网络上转给他的 1BTC。Alice 无法阻止 Bob 获得这 1BTC，因为超时时间 T1>T2。Bob 无法阻止 Alice 获得 10ETH，因为 Alice 知道秘密数 s。

这样双方在没有第三方参与的情况下，完成了一次跨链转账，并且实现了交易的原子性。不管在什么情况下，跨链转账要么都成功，要么都失败，从而实现

了跨链资产交换的原子性。

2.2 基于公证人机制的跨链

在公证人机制中，受信任的第三方在分布式账本之间建立连接。公证人机制提供诸如矿工的基础设施和诸如订单匹配的服务，以促进资产转移。在对分布式账本执行操作之前，公证人必须首先同意另一个分布式账本上发生了某个事件，比如一笔交易。考虑加密货币交易所的情况，在这里，公证人必须首先验证分布式账本 A 上的交易是否成功完成，然后才能向分布式账本 B 发出相应的交易。因此，分布式账本之间的数据交换完全由公证人管理。公证人机制使用中心化架构以实现跨链互操作性。

公证人机制可以对应于单个公证人（中心化公证人机制或中心化交易所）或公证人联盟（去中心化公证人机制或去中心化交易所）。在中心化公证人机制中，单个公证人可以为每个连接的分布式账本创建一个节点。例如，当公证人决定启用从比特币到以太坊的资产转移时，公证人会创建一个比特币和以太坊节点来管理两个分布式账本上交易的接收和发布。公证人单独确认事件是否发生（例如交易接收）并触发相应的事件（例如交易发布）。为了使公证人联盟之间的事件确认民主化，增加透明度，已经引入了去中心化公证人机制。

为了在去中心化公证人机制中为事件发出相应的交易，受信任的第三方通常共享例如分布式私钥或使用多重签名钱包。只有当一定数量的公证人确认事件（例如锁定分布式账本 A 上的资产）时，才会执行相应的事件（例如解锁分布式账本 B 上的资产）。

2.3 基于侧链的跨链

通常，侧链(sidechain)是连接到中央分布式账本（主链）的从属分布式账本，例如比特币或以太坊。侧链在技术上独立于主链，因此可以拥有自己的共识机制、代币(token)和矿工。最初，开发侧链是为了通过资产转移来增强现有分布式账本的可扩展性。侧链可以读取和验证来自主链的数据，例如，将资产从主链转移到侧链，也就是单向锚定。单项锚定机制是指如果在比特币主链上销毁了一定数量的比特币，那么在一条侧链上就能够获得相应数量的代币。这个过程是不可逆的，

销毁的比特币无法再拿回来。在这种资产转移中，一些资产（例如比特币）被锁定在主链上。资产的锁定由目标侧链的验证机制确认，最终生成相应数量的原生代币。例如，BTC Relay 扩展了比特币区块链，支持智能合约。原始的侧链只允许资产转移在一个方向：从主链到侧链。

目前侧链还支持双向锚定机制，该机制允许在主链上收回已经销毁的比特币。在双向锚定机制中，需要将比特币发送到一个不由任何人控制的地址，这个地址仅由一段脚本进行控制。如果用户能提供在侧链销毁了一定数量的代币的证明，那么这段脚本会把比特币转回用户的账户。为了能够将资产转移回主链，主链还必须能够验证侧链上的数据。

2.4 综合比较

在哈希时间锁定中，订单匹配具有挑战性，因为没有自动寻找交易伙伴的机制。相比之下，公证人机制由于受信任的第三方的参与而加速了跨链交易，该第三方管理订单匹配、交易验证并负责跨链平台的维护。

在去中心化方面，哈希时间锁定和侧链是目前最去中心化的模式，因为在这两种模式中，分布式账本可以直接相互通信。与公证人机制相比，哈希时间锁定和侧链的去中心化程度更高。公证人机制更利于审查和监管。

第三章　跨链技术的应用

下面主要介绍三个使用案例：资产转移、跨链预言机(cross-chain oracle)和跨链智能合约(cross-chain smart contracts)。

3.1 资产转移

在资产转移中，资产从一个分布式账本转移到另一个。资产交换是一种特殊的资产转移。资产交换对交易的原子性提出了要求，以防止财务损失。

3.2 跨链预言机

跨链预言机不是移动资产，而是将信息从一个分布式账本移动到另一个。因此，可以使用跨链预言机来验证某些事件（例如交易）是否发生在另一个分布式账本上。例如，可以将数据从一个分布式账本迁移到另一个分布式账本。在供应链管理中，一个用于支付的分布式账本可以请求另一个分布式账本上的货物的当前状态以进行跟踪以执行有条件的支付。

3.3 跨链智能合约

跨链智能合约描述了在另一个分布式账本上触发智能合约执行的能力。与跨链预言机相比，跨链智能合约的执行需要在目标链上发布交易，这会导致分布式账本的状态发生变化。

参考文献

[1] Gilbert, Seth, and Nancy Lynch. "Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services." *Acm Sigact News* 33.2 (2002): 51-59.

[2] Hei, Yiming, et al. "Practical AgentChain: A compatible cross-chain exchange system." Future Generation Computer Systems (2021).

[3] Jiang, Yiming, et al. "A cross-chain solution to integrating multiple blockchains for IoT data management." Sensors 19.9 (2019): 2042.

[4] Kan, Luo, et al. "A multiple blockchains architecture on inter-blockchain communication." 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C). IEEE, 2018.

[5] Kannengießer, Niclas, et al. "Bridges between islands: Cross-chain technology for distributed ledger technology." (2020).

[6] Xu, Jiahua, Damien Ackerer, and Alevtina Dubovitskaya. "A game-theoretic analysis of cross-chain atomic swaps with HTLCs." 2021 IEEE 41st International Conference on Distributed Computing Systems (ICDCS). IEEE, 2021.

[7] Herlihy, Maurice. "Atomic cross-chain swaps." Proceedings of the 2018 ACM symposium on principles of distributed computing. 2018.