区块链跨链体系及其安全分析

北京交通大学
计算机与信息技术学院
信息安全系

李超 (li.chao@bjtu.edu.cn)
段莉 (duanli@bjtu.edu.cn)

目录

- 区块链基本概述
- 区块链跨链技术及其应用
- 区块链跨链安全分析

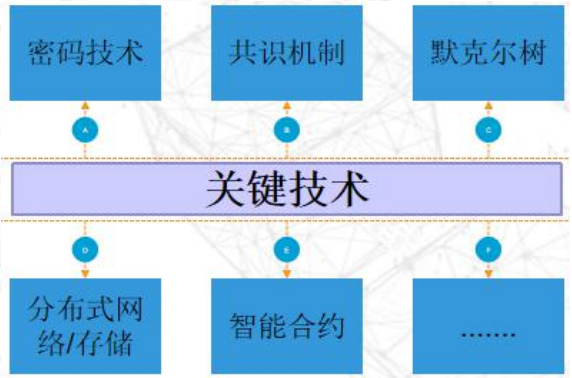
区块链概念

区块链是一种按照时间顺序将数据区块以链条方式组合成特定数据结构，并以密码学方式保证的不可篡改和不可伪造的去中心化共享总账

狭义来讲

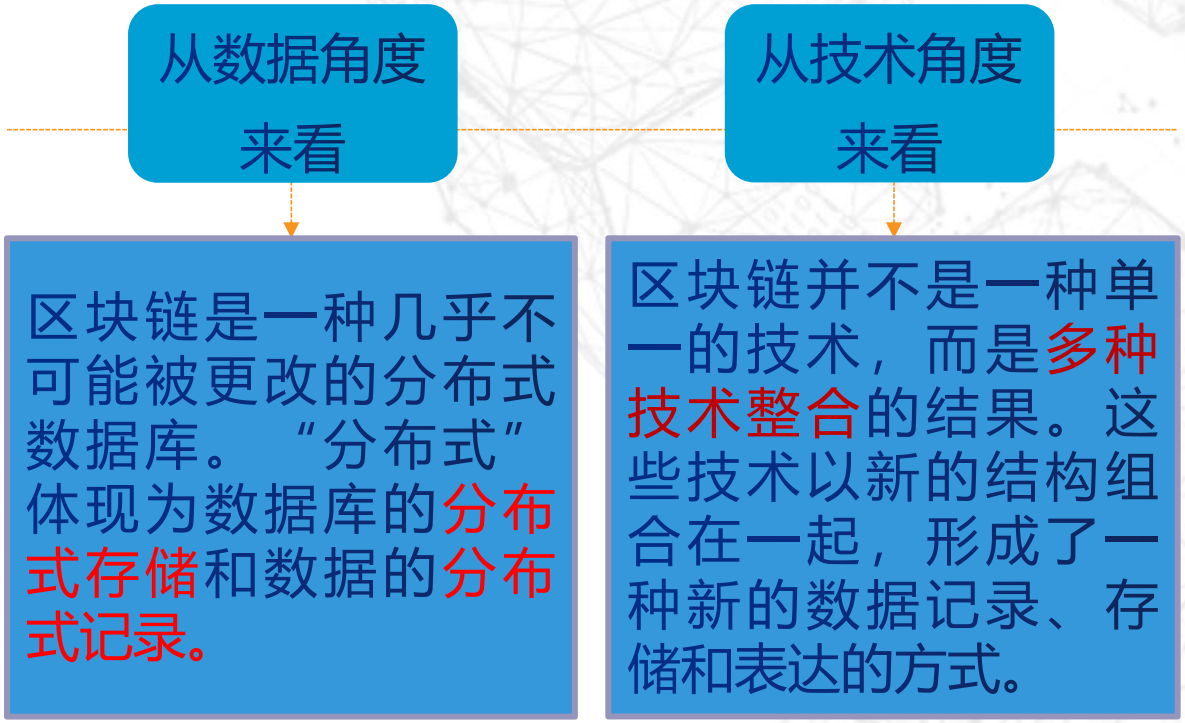
广义来讲

区块链是一种利用加密链区块结构来验证与存储数据，利用分布式共识节点算法来生成和更新数据，利用自动化脚本代码来编程和操作数据的一种全新的去中心化基础架构与分布式计算范式

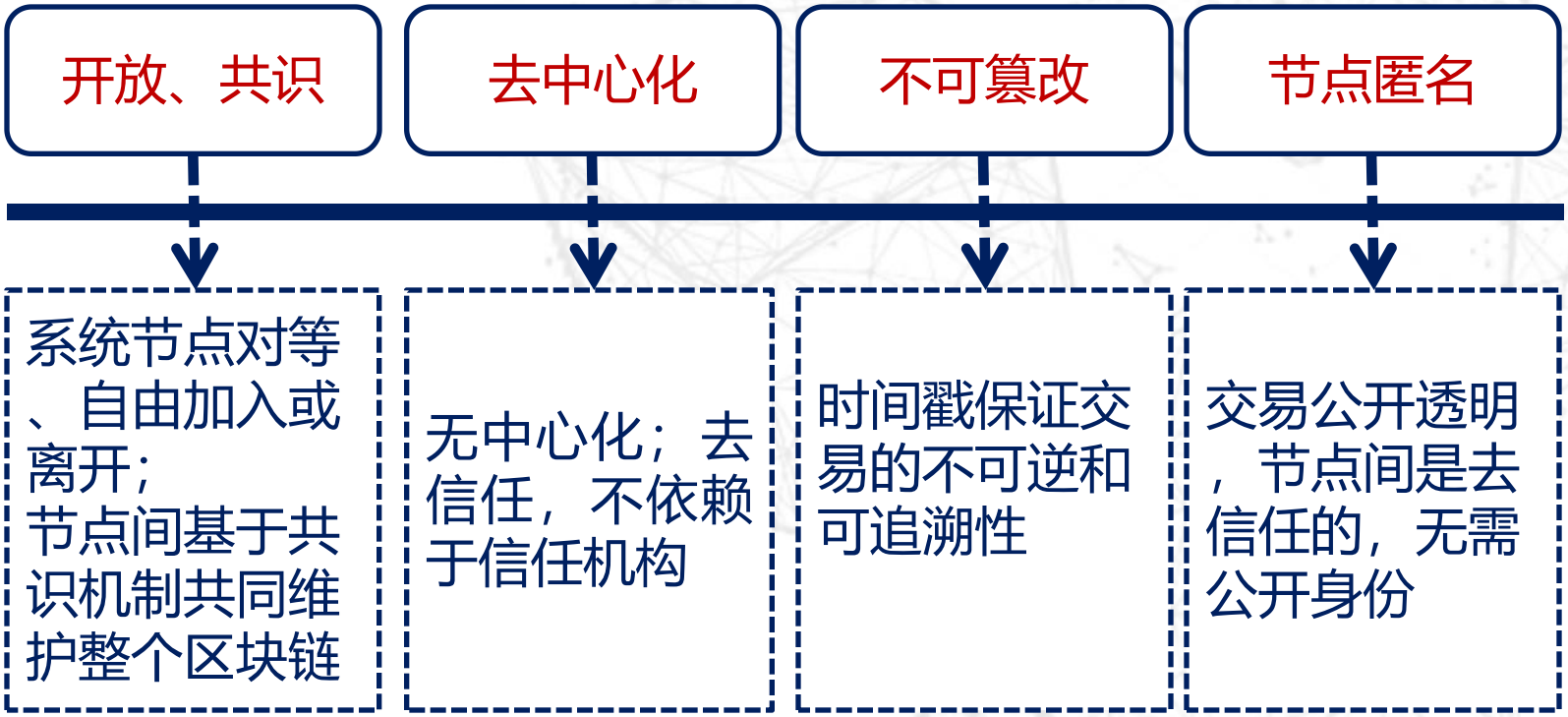


区块链概念

- 区块链是一个分布式账本，一种通过去中心化、去信任的方式集体维护一个可靠数据库的技术方案。



区块链特征


开放、共识
去中心化
不可篡改
节点匿名
系统节点对等、自由加入或离开；
节点间基于共识机制共同维护整个区块链
无中心化；去信任，不依赖于信任机构
时间戳保证交易的不可逆和可追溯性
交易公开透明，节点间是去信任的，无需公开身份

区块链发展

区块链1.0

2008（数字货币）

- 典型代表：**比特币**
- 点对点交易：以**扩机算力**为依托的去中心化的数字货币交易
- 代表了虚拟货币的应用,包括其支付,流通等虚拟货币的职能

区块链2.0

2013（智能合约）

- 典型代表：**以太坊**
- 可编程区块链：为**智能合约**提供可信任的执行环境
- 主要应用于金融基础设施领域，如支付清算设施、跨境支付设施

区块链3.0

2015(Token经济)

- 典型代表：Hyperledger
- 通证经济的提出：去中心化的互信网络、去中心化的信任特征
- 主要应用领域扩展到的金融行业之外，涵盖社会生活的方方面面

区块链类型

01 公共区块链

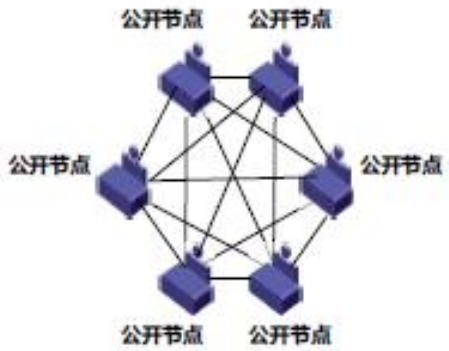
网络中的节点可任意接入，网络中数据读写权限不受限制，任何人都能参与共识过程，**比特币、以太坊**属于典型的公有链。

02 私有区块链

写入权限仅在一个组织手里的区块链，对读取权限或者对外开放权限进行限制。如摩根大通的**Quorum**

03 联盟区块链

介于公有链和私有链之间。公开节点：网络中的节点部分可以任意接入，授权节点：则必须通过授权才可以接入的区块链。比如**Hyperledger**。

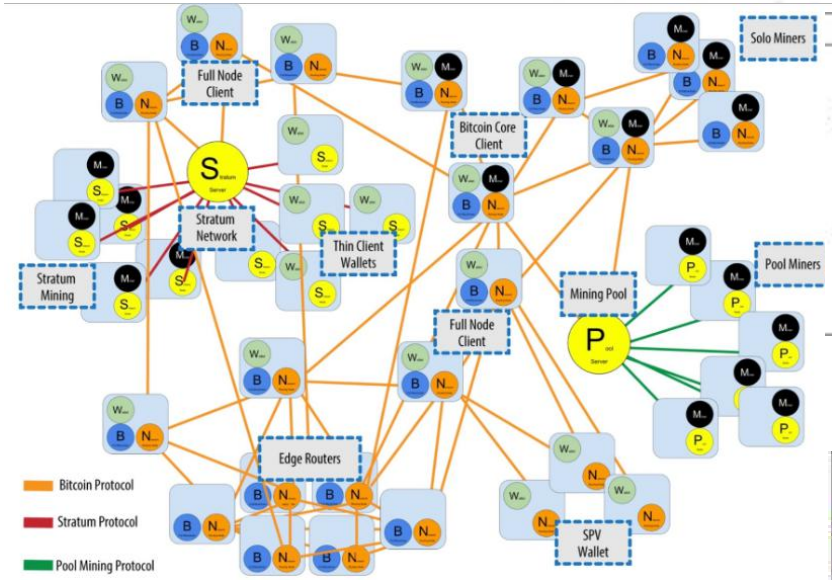


(a) 公有链

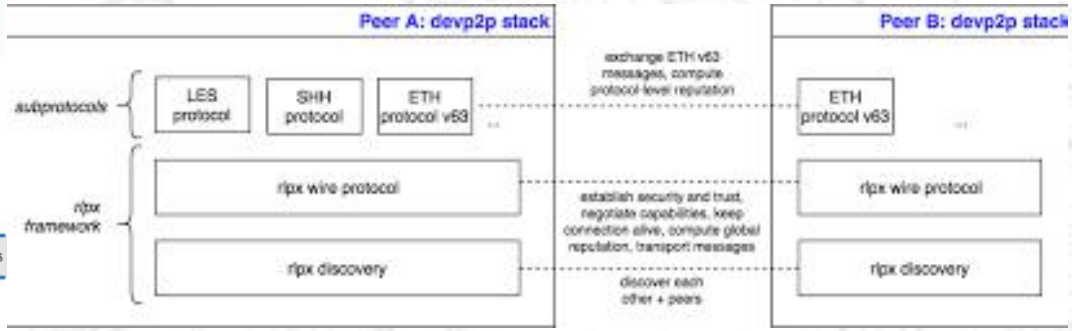
(b) 私有链

(c) 联盟链

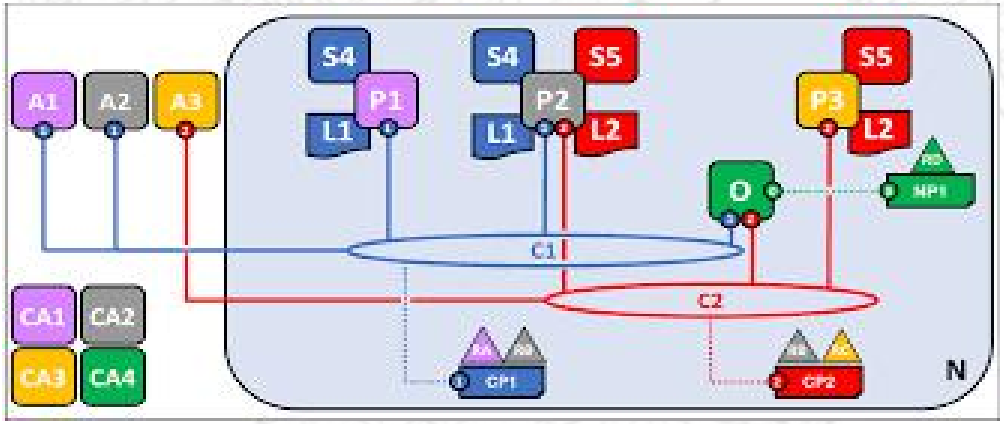
区块链传输机制



比特币泛洪机制

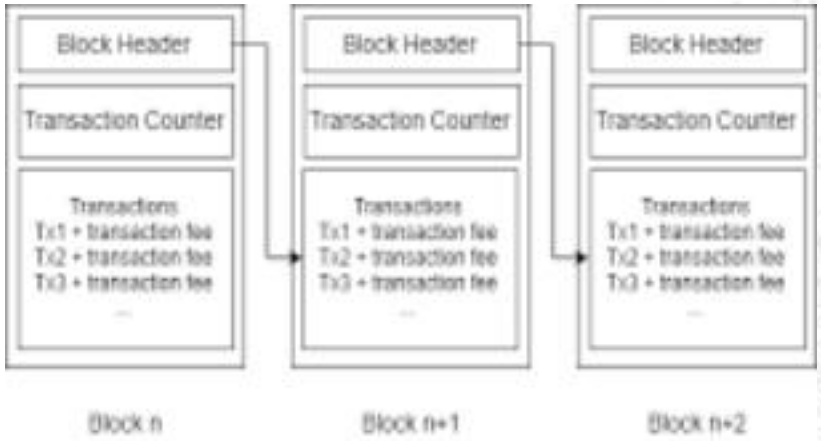


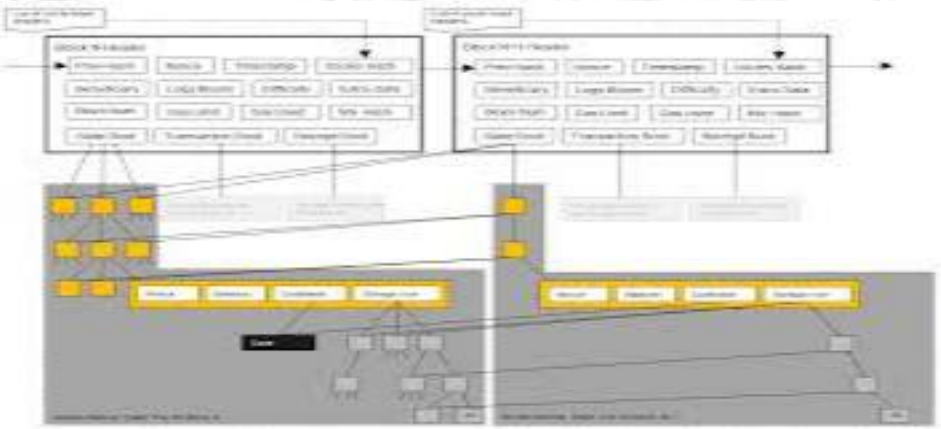
以太坊gossip机制



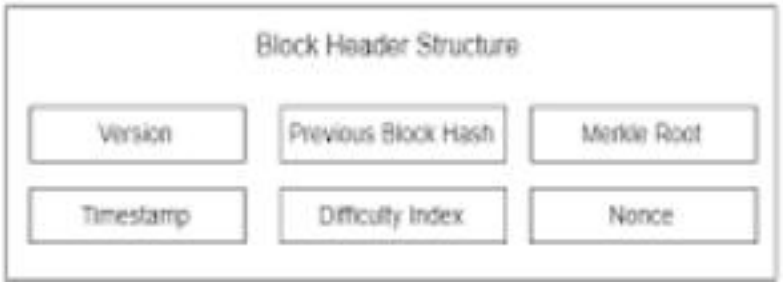
Fabric 通道机制

异构的区块结构

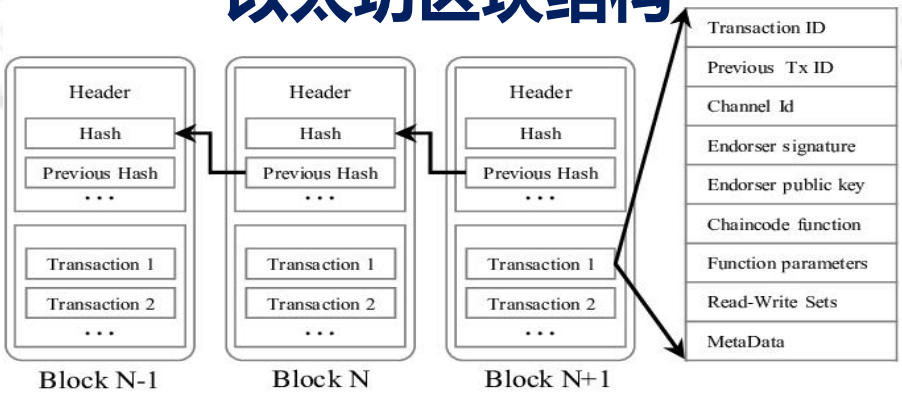




以太坊区块结构

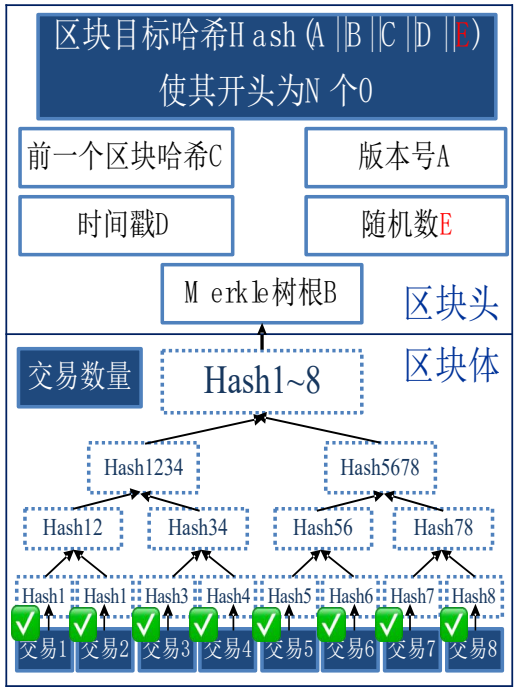


比特币区块结构

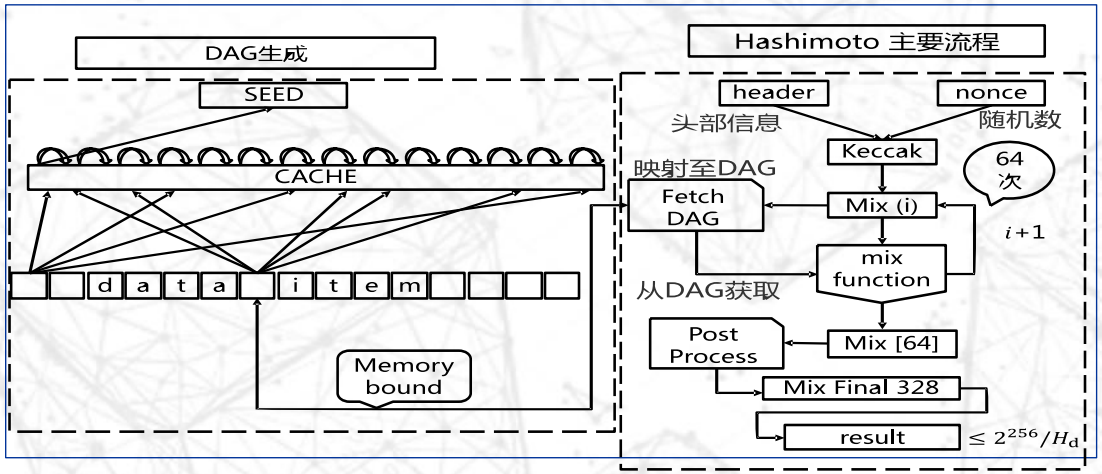


Fabric区块结构

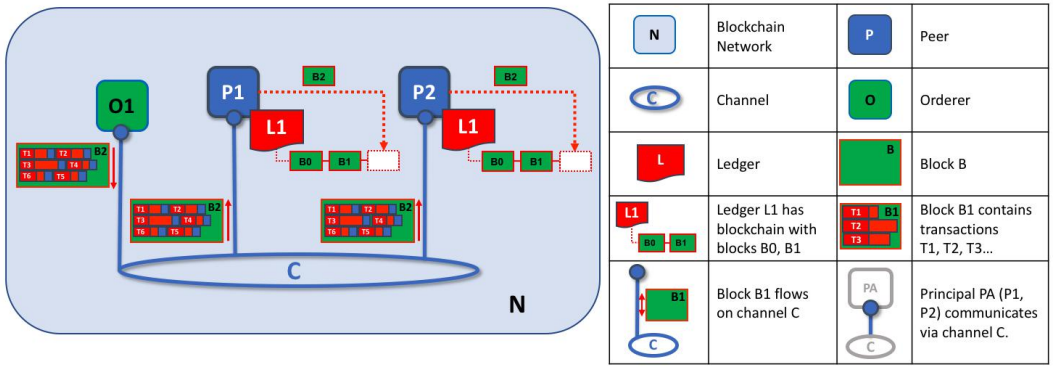
区块链共识机制



PoW共识



PoA共识



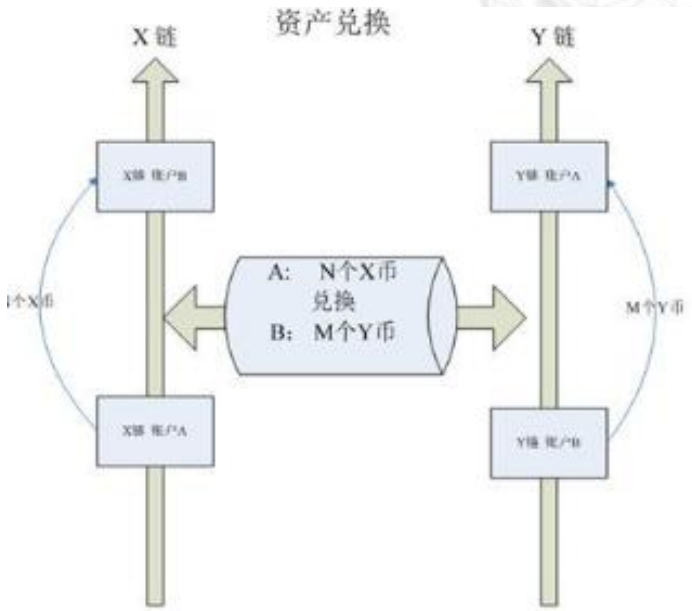
Fabric排序和生成区块

跨链必要性

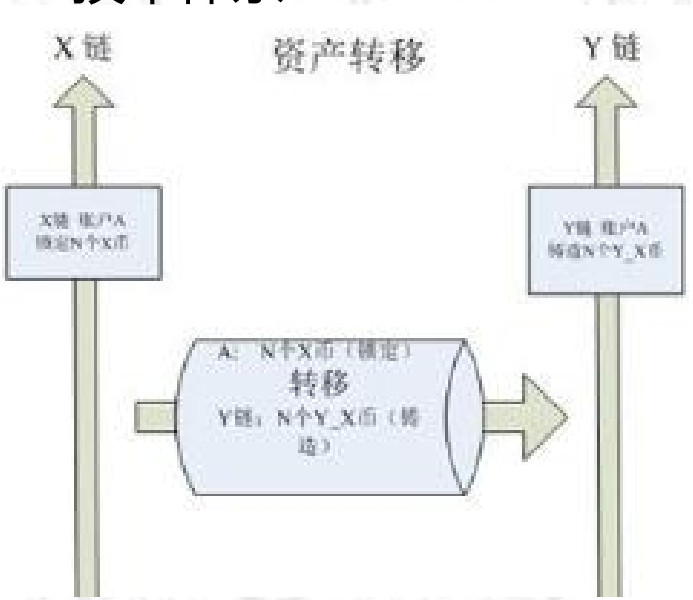
- 如何避免独立区块链“信息”孤岛问题？
- 如何实现区块链之间的互联互通和价值转移？

跨链必要性

- 跨链应用需求
  - 资产兑换和资产转移
  - 跨链数据共享和业务协同



- 技术现实
  - 区块链是去信任环境下的节点网络，对外部数据不信任
  - 缺少面向联盟链的通用跨链技术体系



- 业务的开放性发展趋势对封闭的区块链网络技术体系提出挑战：需要跨链交互

跨链本质

跨链是指原本存储在特定区块链上的资产可以转换成为另一条链上的资产，从而实现价值的流通。

跨链交互需解决的问题

- 消息真实性证明
- 消息路由
- 消息执行结果证明
- 消息状态有效性保证

跨链技术实现

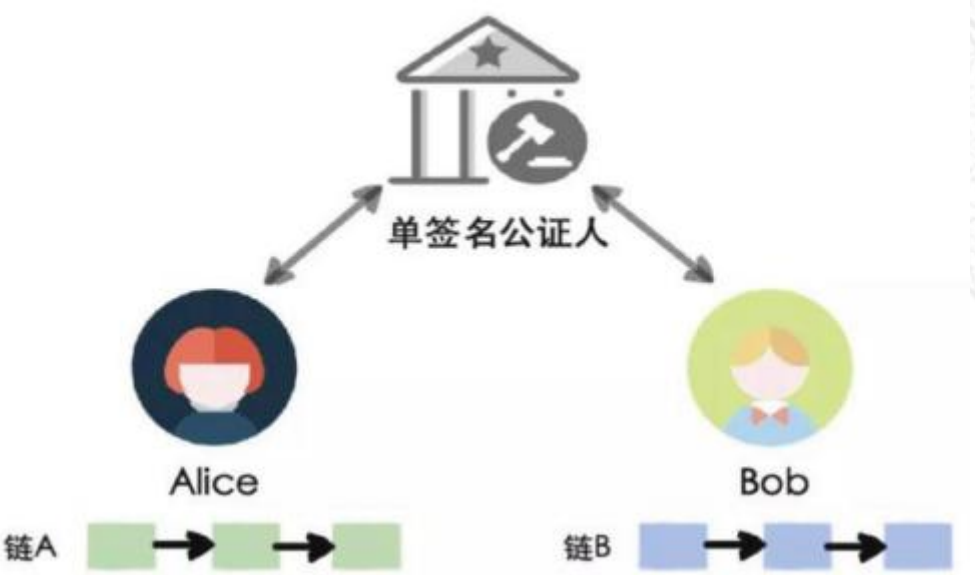
- A 公证人机制 → Ripple Interledger
- B 侧链/中继 → BTC Relay, Polkadot, Cosmos
- C 哈希锁定 → 闪电网络Lighting Network
- D 分布式私钥控制 → 万维链Wanchain

公证人机制

- 公证人机制：引入共同第三方中介进行跨链消息的转发和验证

- 过程：

位于两条链上的节点Alice和Bob想跨链转移价值100美元的资产，此时需要引入第三方交易所进行，Alice先将钱托管到第三方交易所，由第三方交易所进行资产的置换和消息的转移。



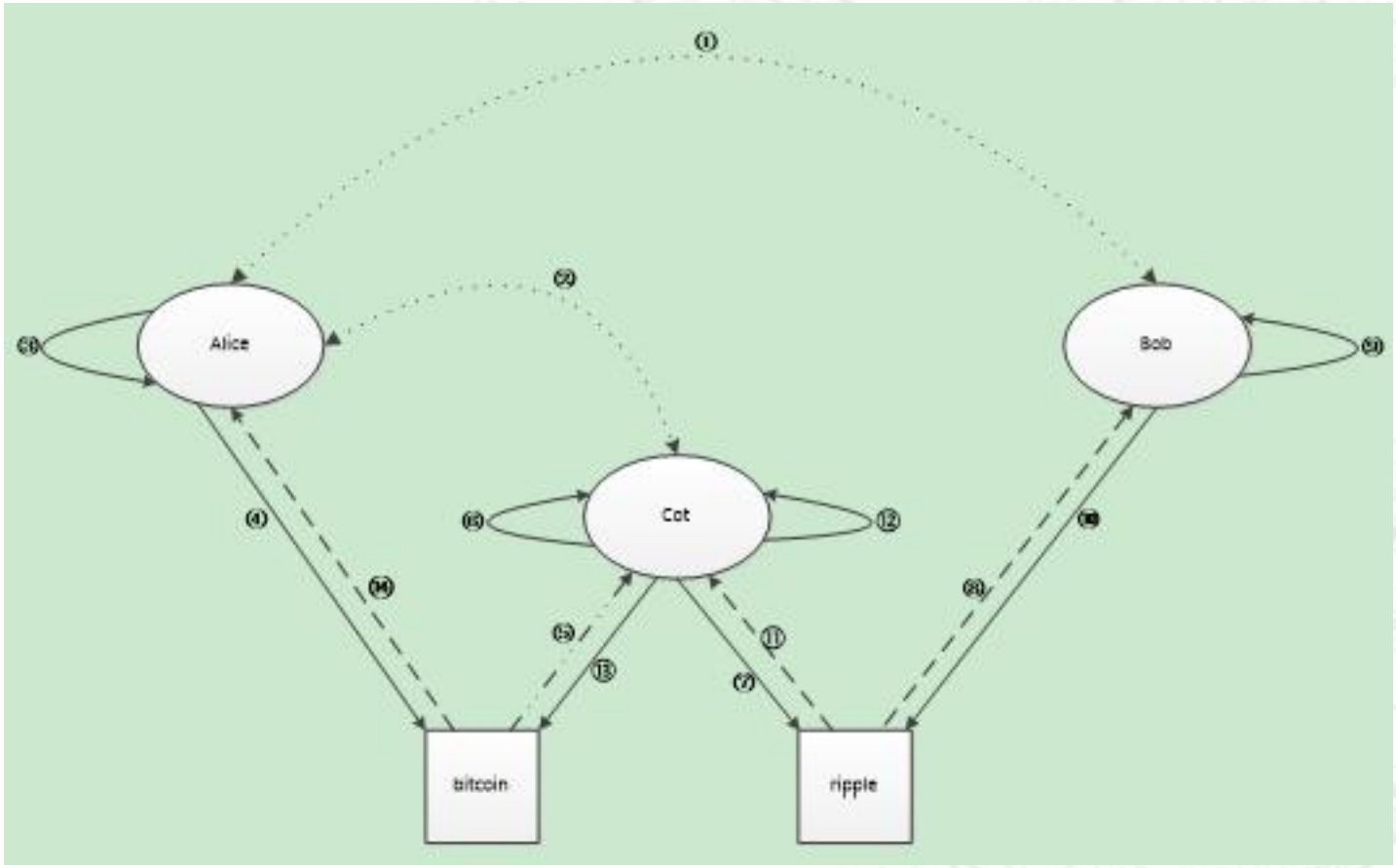
公证人机制

- 使用受信任的一个获一组团体向一条链声明另一条链发生了某事件，或者确定该声明是否正确。

- 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。
- Corda是由R3CEV推出的一款分布式账本平台，其借鉴了区块链的部分特性，其面向的是银行间或银行与其商业用户之间的互操作场景。

公证人机制

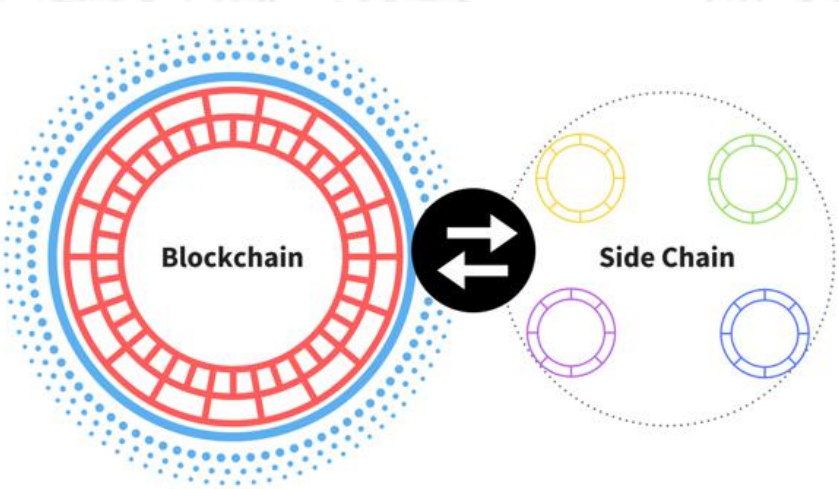
Ripple 跨链技术



侧链/中继

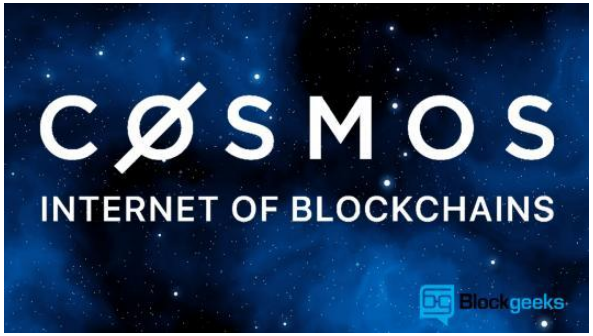
- 以A区块链作为主链，其他区块链作为侧链，二者通过双向锚定技术（two-way peg），实现从A主链上的代币转移到侧链进行流通。

- 过程
  - 将数字资产在主链中锁定，同时将等价的数字资产在侧链中释放
  - 当等价的数字资产在侧链中被锁定的时候，主链的数字资产也可以被释放。



侧链/中继

- 假设区块链拥有区块头和区块体，区块头中有Merkle等证明信息，可以将链A的区块头写入链B的区块中，链B使用和链A一样的共识验证方法。链B可以通过Merkle分支的证明信息证明链A的数据和操作。



Polkadot是由原以太坊主要核心开发者推出的公有链。计划将私有链/联盟链融入到公有链的共识网络中，同时又能保有私有链/联盟链的原有的数据隐私和许可使用的特性。

Cosmos是tendermint团队推出的一个支持跨链交互的异构网络。Cosmos Hub是一种多资产权益证明加密货币网络。通过简单的管理机制来实现网络的更新，还可以通过连接其他空间实现扩展。

侧链/中继

- Polkadot

2020年5月，Polkadot发表了《Polkadot 概述及其设计注意事项》。其在2016年Gavin Wood 首次发表 Polkadot 白皮书 的基础上，对 Polkadot 及其设计考虑进行了扩展，对 Polkadot 的设计组件和子程序进行了全面的更新。

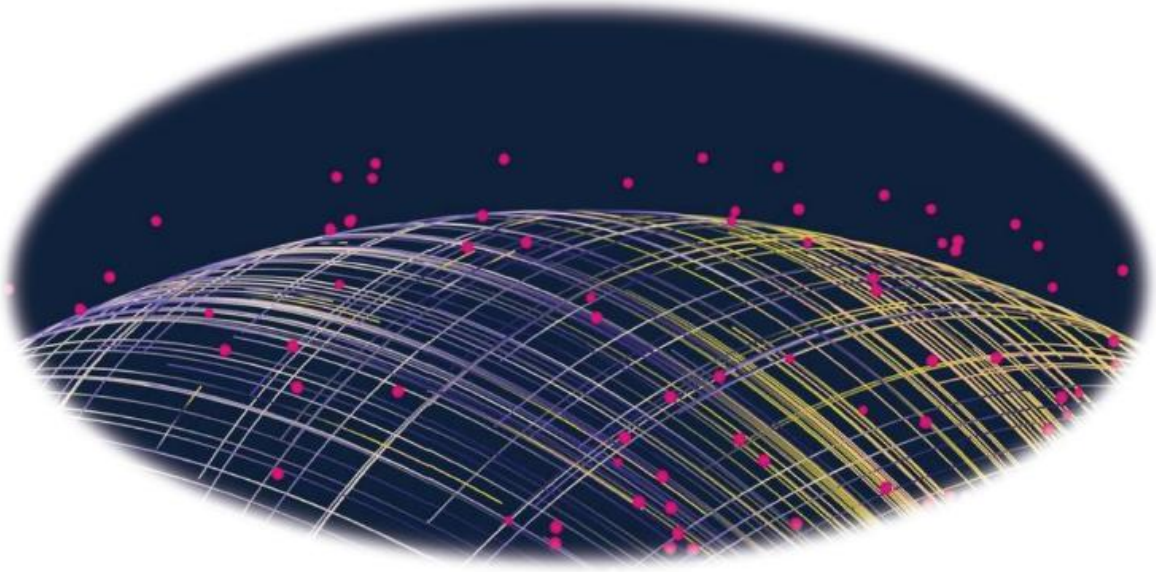
①治理

②NPoS 机制

③区块生产和共识

④有效性和可用性

⑤跨链消息传递



侧链/中继

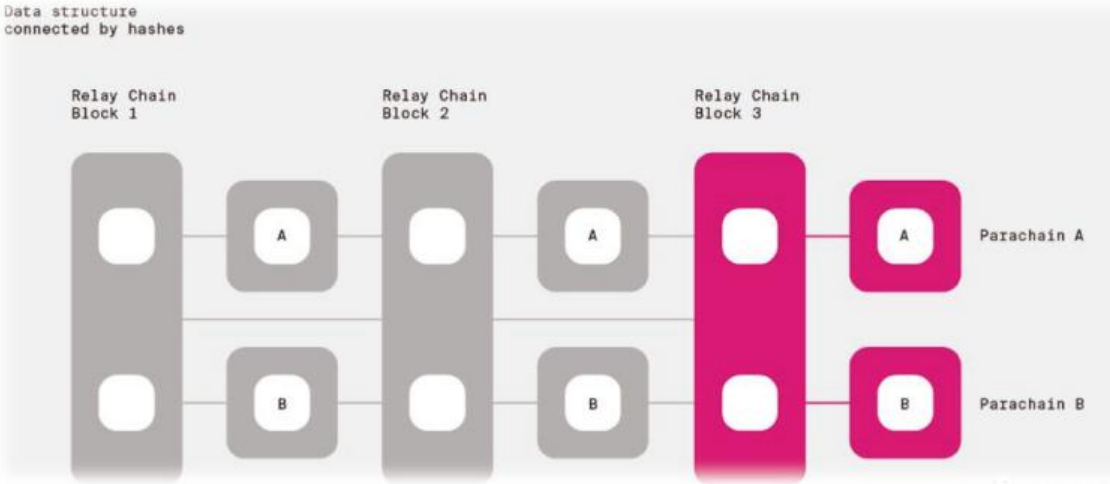
- Polkadot

跨链消息传递(XCMP)

跨链消息传递（XCMP）可以让消息以安全、无信任的方式、快速、有序地在不同的平行链之间传递。XCMP 的主要目标之一是为在平行链之间传递的消息提供一致的历史记录。

- 一致的历史记录：平行链块输出队列上的元数据包含在中继链上，稍后由另一个接收的平行链进行消息验证。
- 可靠传递：与此元数据对应的消息正文需要从发件人分发到收件人。

使用基于 Merkle 树的简单排队机制来解析消息的顺序，以确保准确度。



侧链/中继

Polkadot

2020年5 月 26 日，Web3 基金会官宣，Polkadot 在在经过三年的开发工作后终于发布了备受期待的版本Polkadot CC1。

- Polkadot 的第一个候选链（CC1）已经发布，它很可能成为 Polkadot 主网。

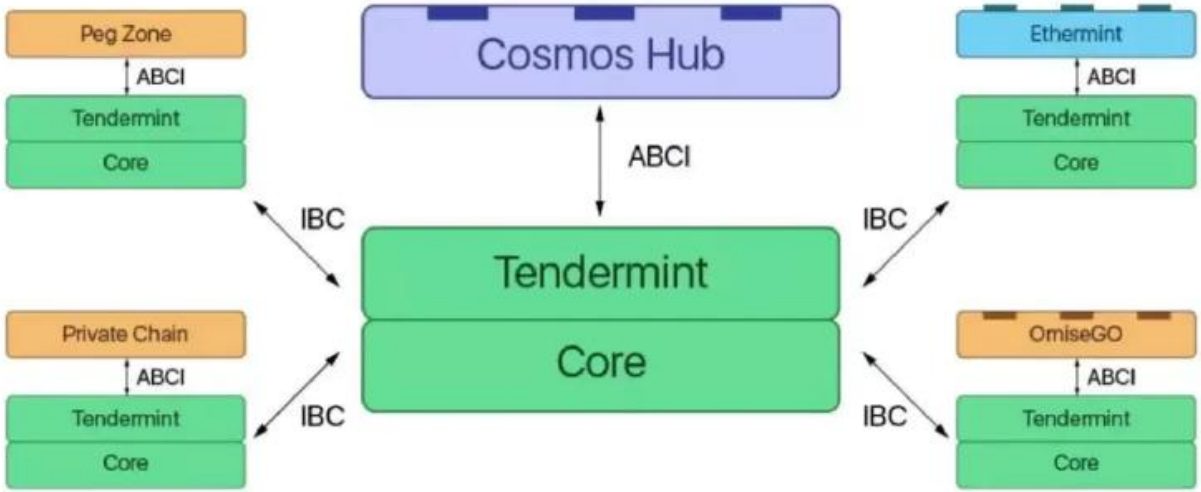
- Polkadot CC1 的第一个阶段提供了两个关键功能：映射 & 声明和 staking。

侧链/中继

- Cosmos

跨链通信-IBC

IBC协议提供了一种通用的跨链协议标准。IBC的设计使得跨链交易可以在多个Hub之间进行安全路由和转发，类似目前互联网的TCP/IP 协议。但是目前的Cosmos设计也只能够支持资产的跨链，而且由于不同区块链的业务不同其共识速率的不一致也会影响跨链交易有效性的证明。



侧链/中继

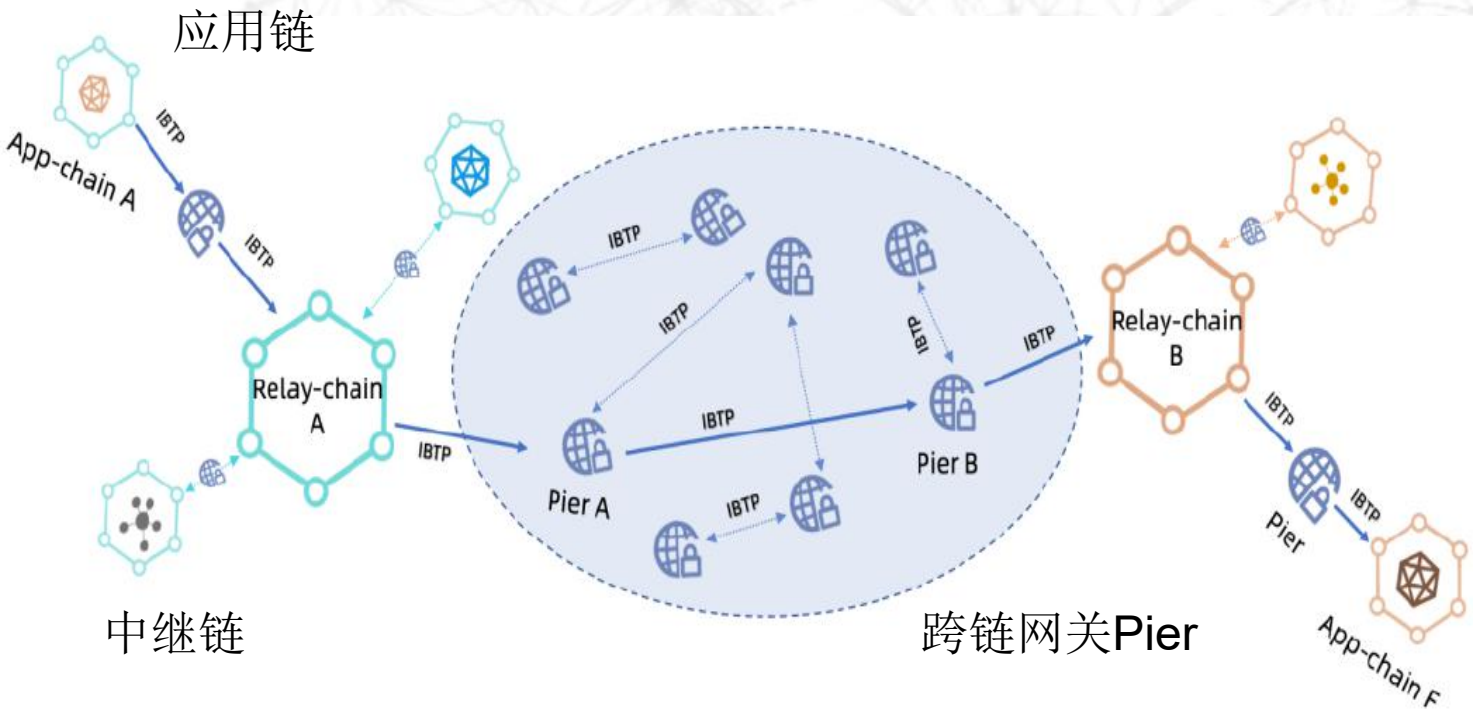
- BitXhub

异构区块链跨链交互架构模式

网关
解决跨链交易的获取和提交问题。

+

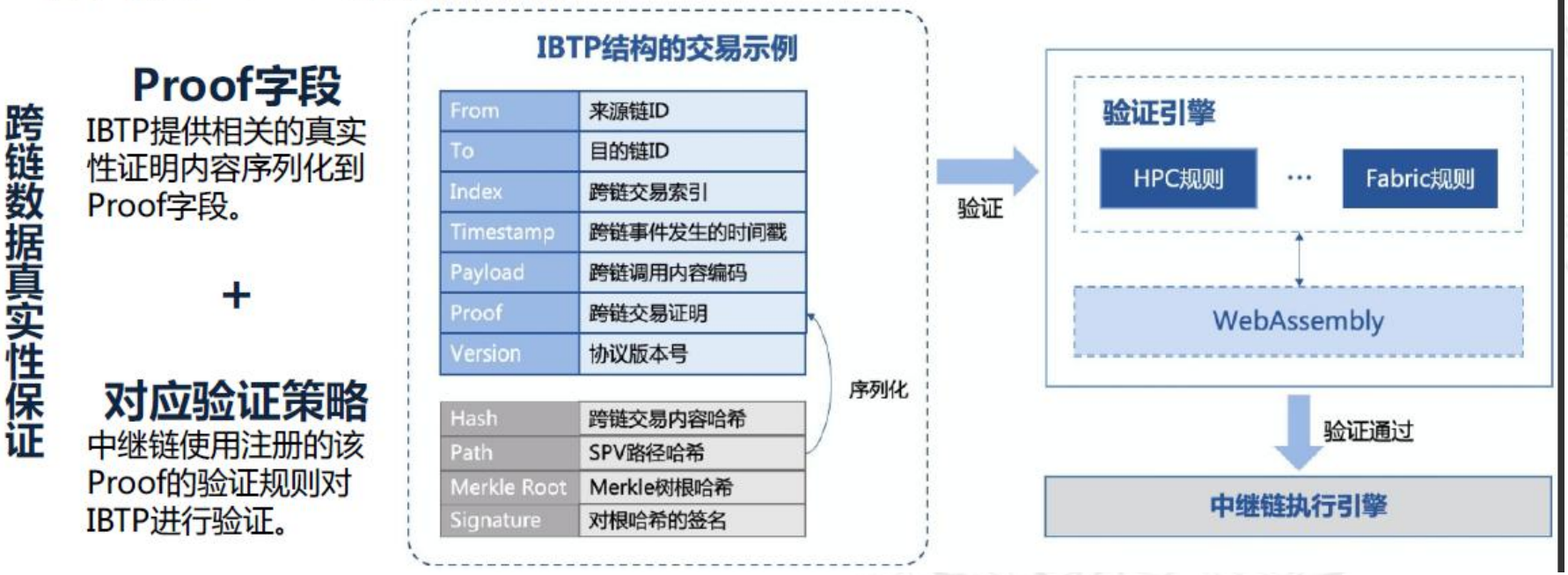
中继链
结合IBTP(链间通用传输协议)解决跨链交易的验证和路由问题。



侧链/中继

- BitXhub

2020年4月20日，趣联科技发布了其针对跨链平台BitXHub架构设计的十个问答，传递BitXHub的设计思路。



侧链/中继

ODATS

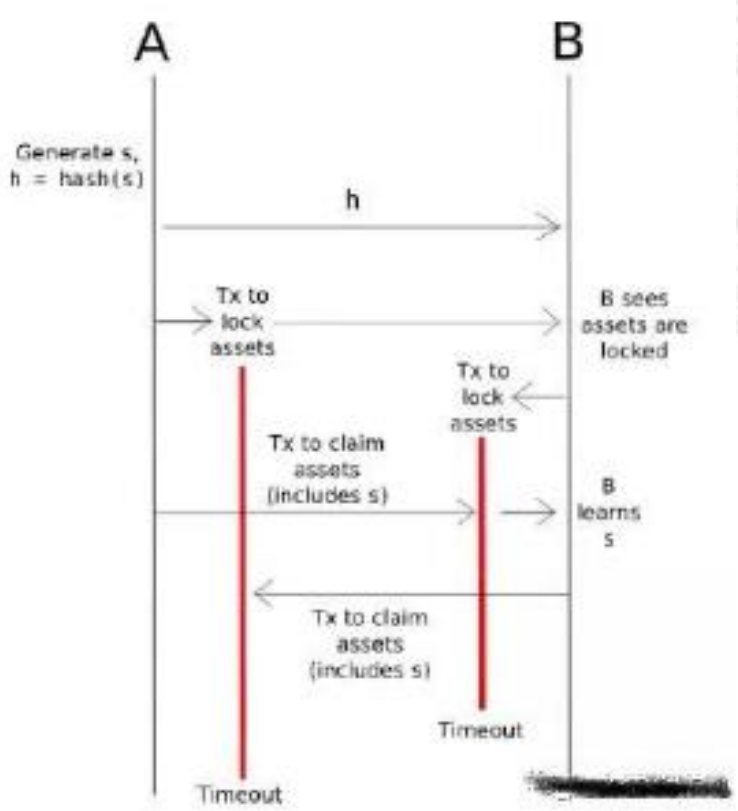
2019年9月26日，蚂蚁金服发布了ODATS（Open Data Access Trusted Service）跨链产品。

- 它为链与链之间提供的是关于区块链基于信任中立的数据牟定以及网络路由。
- 基于安全技术，会提供链与链之间的信息互联，和各类多样化的外部数据源到链上的可信传递。
- 在底层提供UDAG全栈跨链协议组件，面向智能合约的链下可信计算框架MYTF，以及新的自研可信硬件智能合约计算引擎。
- 在链上定义端与端之间类TCP协议的底层TCP接口，同时，面向应用的开发会提供跨链资产以及跨链事物管理的中继件服务。
- 开发了面向蚂蚁区块链的各类异构链的适配组件，并已经在大规模溯源场景、数字资产流转场景当中得到验证。

哈希锁定

- 主要支持跨链资产的原子交换，最早用于比特币闪电网络中，其原理是通过时间差和隐藏哈希值实现资产的原子交换。

- 同时打开**哈希锁**和**时间锁**的条件是，在规定的时间内输入哈希值原本的值



哈希锁定

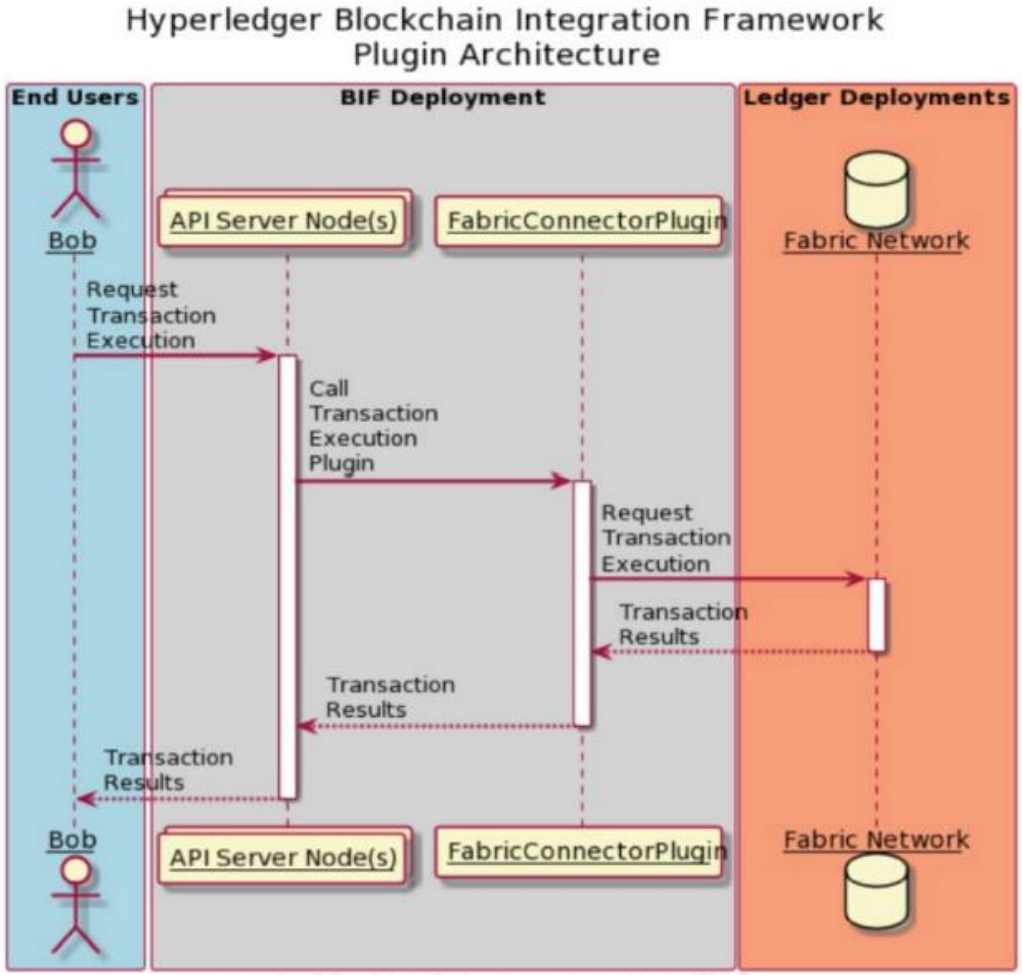
Fabric

hyperledger-labs基于哈希锁定解决跨链问题。

1.用户对单链或多个链之间的操作进行API调用，该API调用通过区块链集成框架路由接口发送到业务逻辑插件。

2.业务逻辑插件通过区块链集成框架路由接口，向链插件请求对链操作，链插件向其连接的链请求操作，该操作在链上结算。

3.链插件监视其连接的链上的交易数据。如果链插件收到与步骤2的操作相关的交易数据，它将验证交易并将已验证的交易信息通过区块链集成框架路由接口发送给业务逻辑插件，然后进行业务逻辑插件接收并记录此信息。



哈希锁定

- WeCross

2020年2月，微众银行区块链团队发布了WeCross跨链技术白皮书。

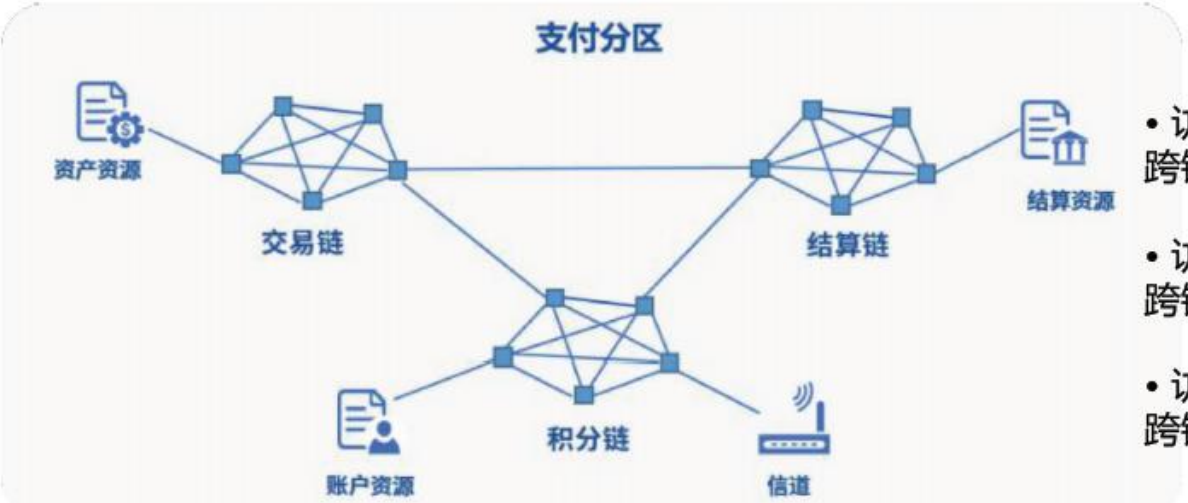
WeCross 对区块链的多层次抽象可以类比 Java ORM（Object Relational Mapping）对数据库的多层次抽象。

哈希锁定

- WeCross

数据层

- 统一资源范式：对主流区块链的关键数据结构进行提炼，设计普适跨链场景的抽象区块数据结构，实现“一次适配，随处可用”。
- 统一资源寻址协议：跨链路径定义为 **[跨链分区].[业务链].[区块链资源]** 。



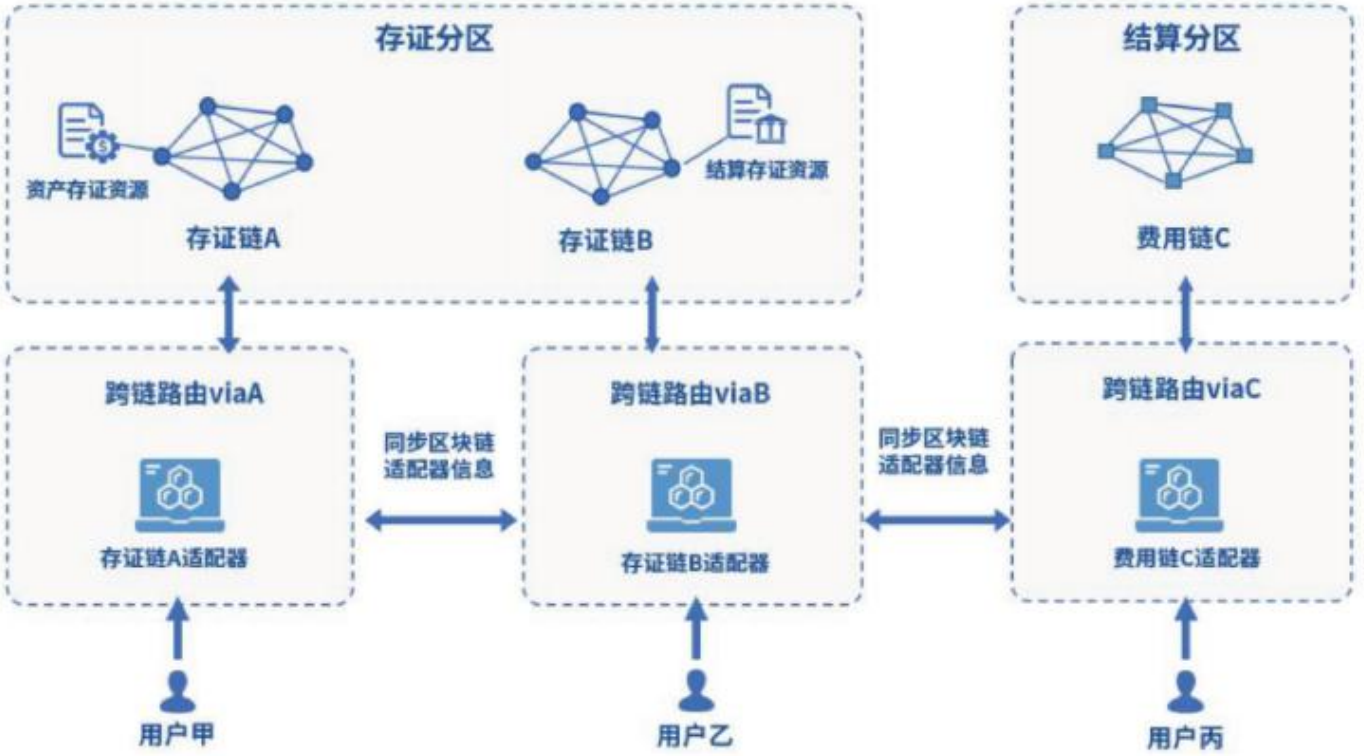
- 访问交易链的资产资源，
跨链路径为：支付分区 . 交易链 . 资产资源
- 访问结算链的结算资源，
跨链路径为：支付分区 . 结算链 . 结算资源
- 访问积分链的账户资源，
跨链路径为：支付分区 . 积分链 . 账户资源

哈希锁定

WeCross

交互层

- 建设通用区块链适配与路由中继网络。

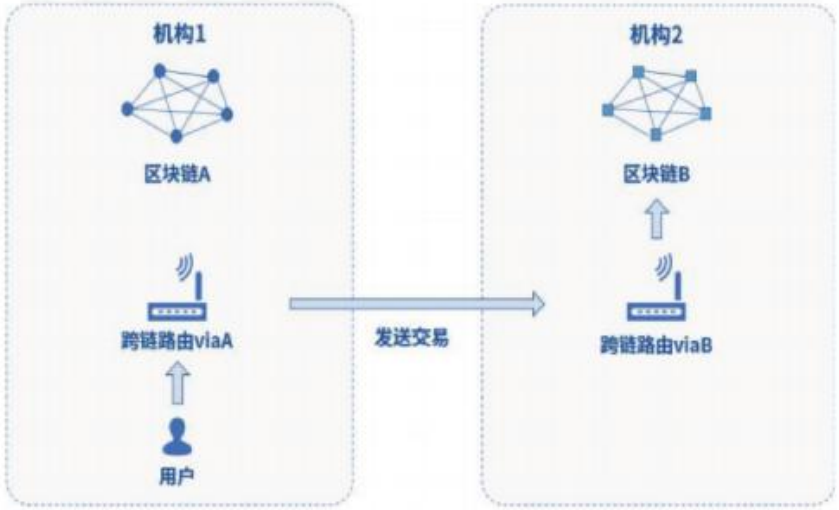


哈希锁定

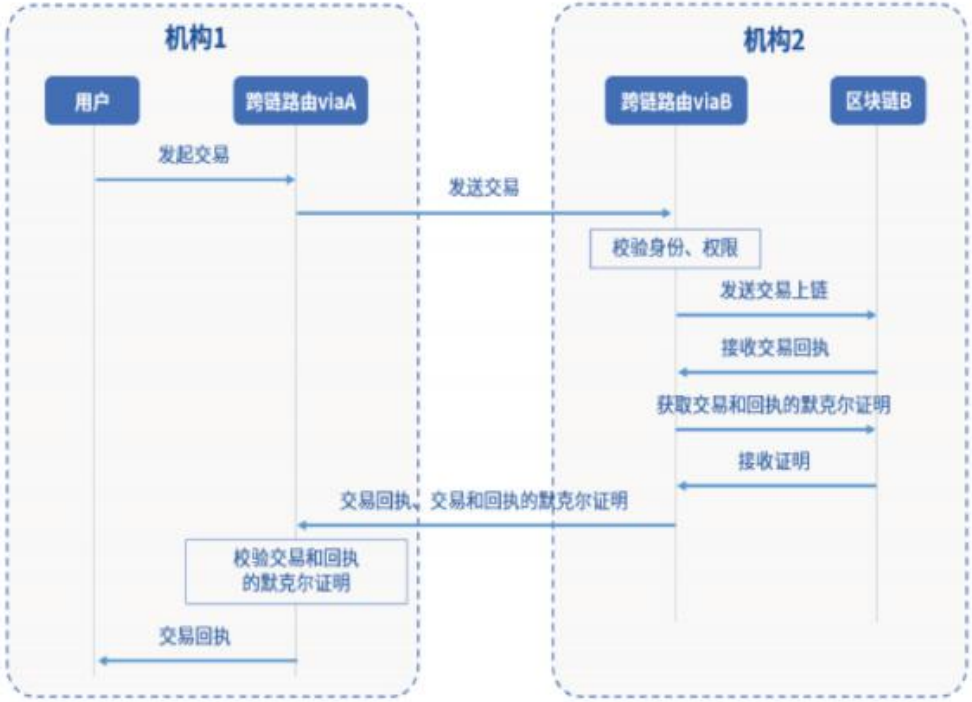
WeCross

交互层

- 结合标准默克尔证明机制，实现可信交互流程。



机构 1 的用户要访问机构 2 的区块链 B，并要求访问结果真实可信。



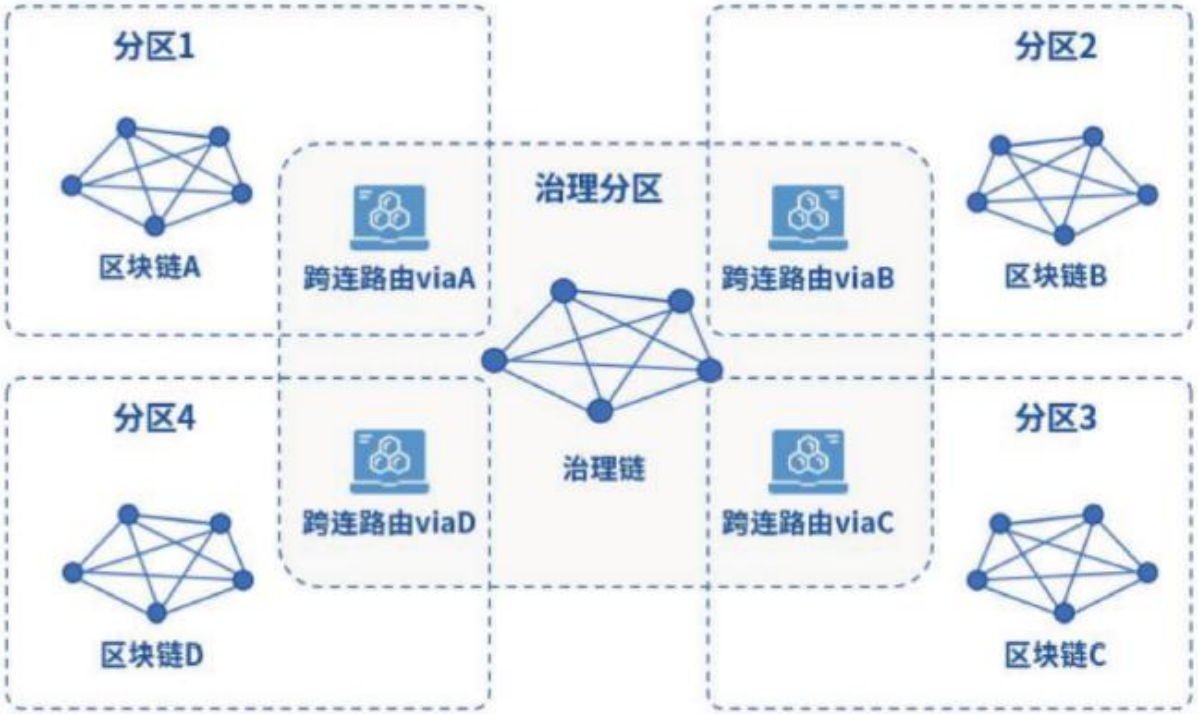
可信跨链交互时序

哈希锁定

WeCross

事务层

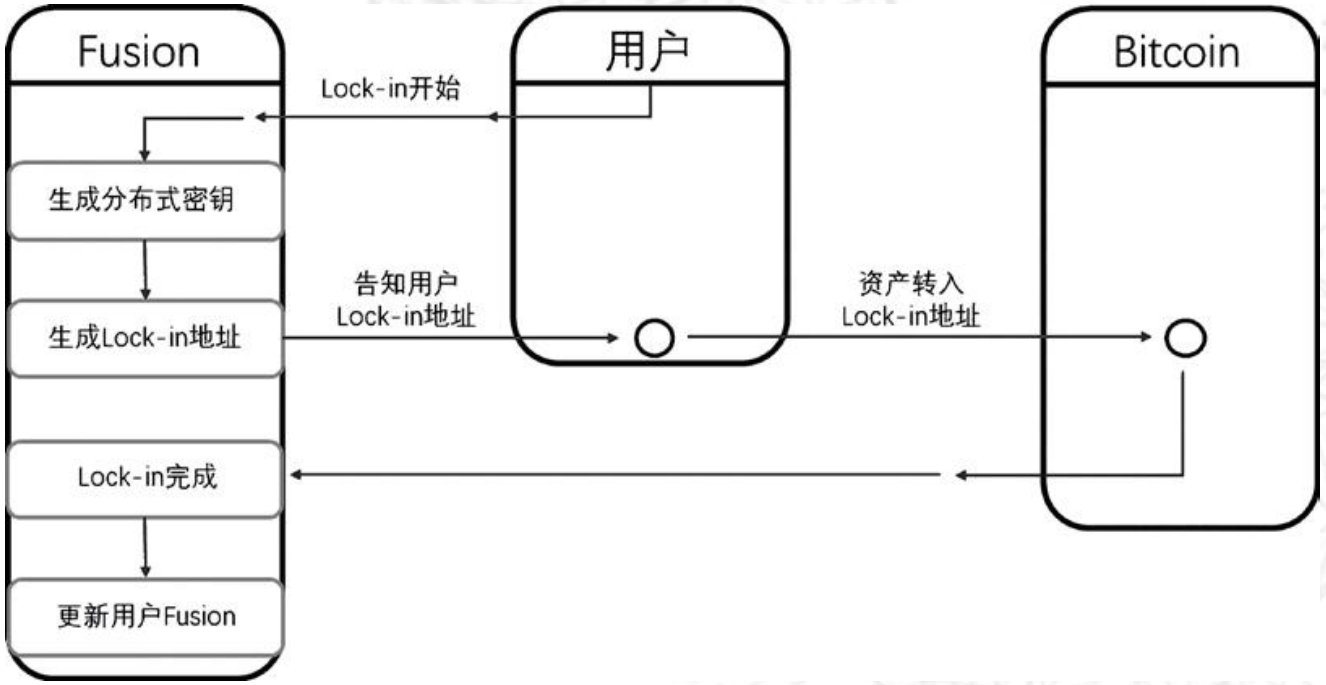
- 建立治理链，构建多边跨域治理(MIG)，实现多个区块链安全可信地执行事务。



分布式私钥控制

- 通过私钥生成与控制技术，把加密货币资产映射到基于区块链协议的内置资产模板的链上，根据跨链交易信息部署新的智能合约，创建出新的加密货币资产。

区块链项目 **Fusion**



主流跨链技术方案对比

跨链技术	公证人机制	侧链/中继链	哈希锁定	分布式私钥控制
互操作性	所有	所有（需要所有链上都有中继，否则只支持单向）	只有交叉依赖	所有
信任模型	多数公证人诚实	链不会失败或者收到“51%攻击”	链不会失败或者收到“51%攻击”	链不会失败或者收到“51%攻击”
适用于跨链数据交换	支持	支持	支持	支持
适用于跨链资产转移	支持（需要长期公证人信任）	支持	支持	支持
适用于跨链Oracles	支持	支持	不直接支持	支持
适用于跨链资产抵押	支持（需要长期公证人信任）	支持	大多数支持但是有难度	支持
实现难度	中等	难	容易	中等
多币种智能合约	困难	困难	不支持	支持
实现案例	Ripple	Polkadot/Cosmos	Lighting Network	Wanchain/Fusion

跨链安全性

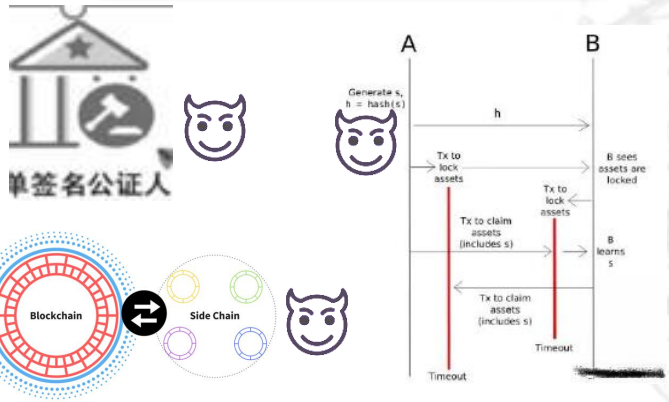
安全性的要求主要来源于两方面，一方面来源于区块链自身安全，包括网络通信安全、数据安全、应急处理等等。另一方面来源于跨链机制安全，包括消息有效性及互操作的合法性控制。

如何实现跨链机制的安全性是多链架构中的重要考量。在协议设计上需要达到以下几点：

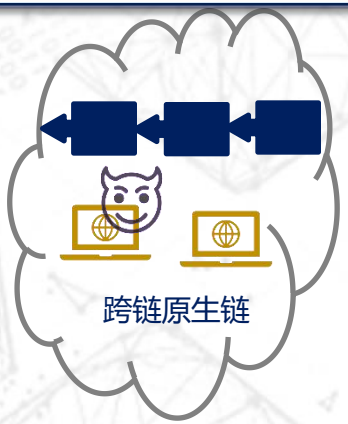
- 消息的高效路由机制
- 消息发送方的身份证明
- 消息接收方的存在证明
- 消息有效性的自我证明
- 消息的生命期管理

跨链安全问题

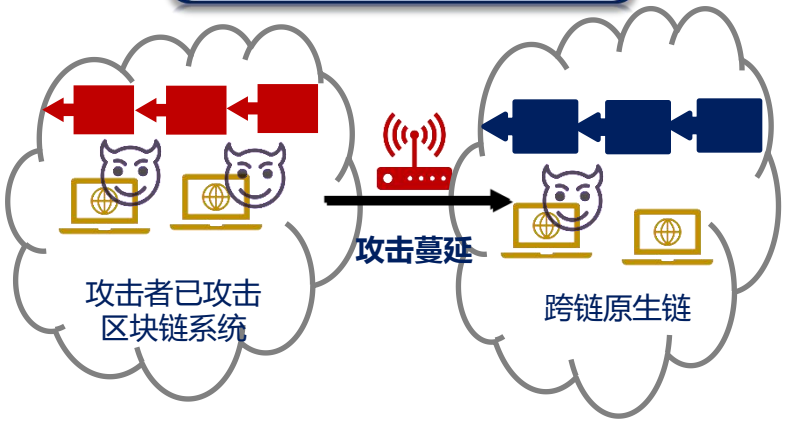
跨链实现机制攻击



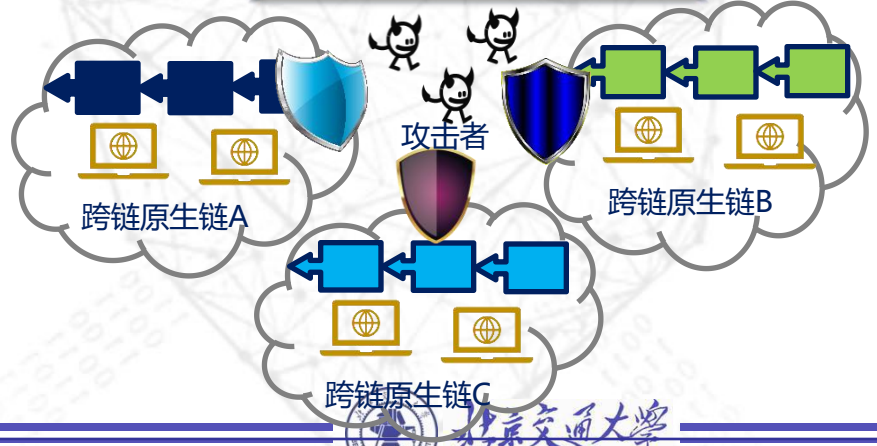
原生链（模块）攻击



链间攻击扩散



组合安全攻击

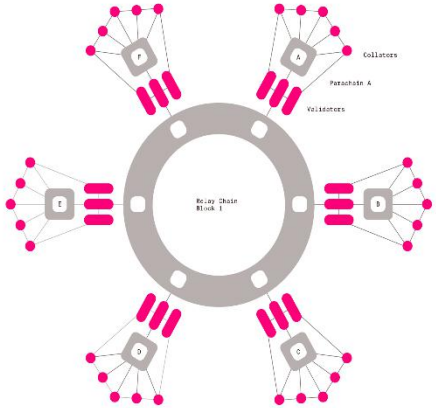


国内外研究现状

Web3基金会
Polkadot

Relaychain
Shared security
Inter Chain Message Passing

Parachain
Blockchain that has own logic



多链互通依赖于**中继可信**

InterChain基金会
Cosmos

跨链安全依赖于**验证者诚实**

国内外研究现状

蚂蚁金服
蚂蚁区块链

跨链安全依赖于**可信执行环境**

跨链攻击及安全防护

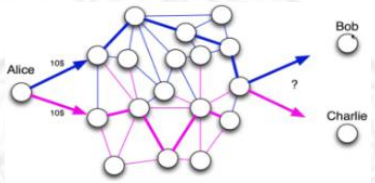
跨链安全需求

跨链交互安全需求

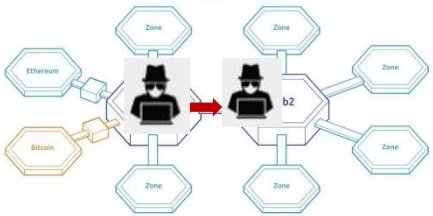
- 异构多链组合安全
- 原生链攻击防护
- 链间攻击防扩散
- 一致性安全验证
- ……

跨链安全需求多样性

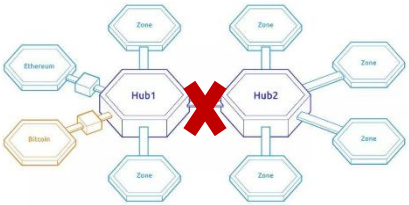
跨链攻击类型



跨链模块安全攻击



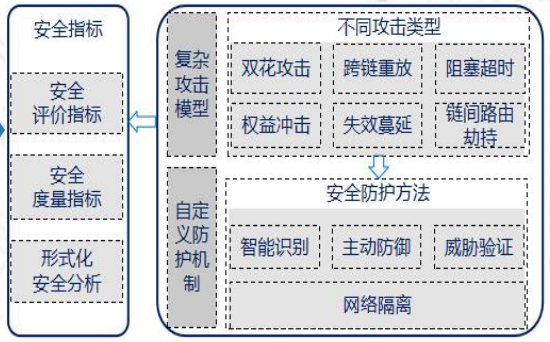
原生链安全攻击



链间交互安全攻击

跨链安全模型

不同攻击的安全机理
与攻击路径



安全分析模型

多维度的跨链攻击
及安全分析模型

保障两条链的独立安全性

两条链之间应该保持各自的独立性，尽量通过第三方节点或者独立的模块处理跨链事务

第三方节点或者独立模块要具备检测安全事件的能力，并且具备响应能力

主要由跨链交易的原子性以及保障交易最终确认性来完成

多层次链间风险控制方法

跨链模块安全防护模型

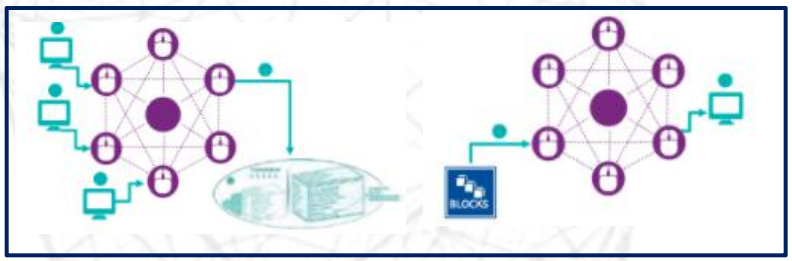
多模态安全防护模型

链间安全事件检测机制

链闸机制

链间交互安全防护模型

链间攻击放扩散



分布式容错机制

多层次链间风险控制

跨链系统多层次安全防护方法

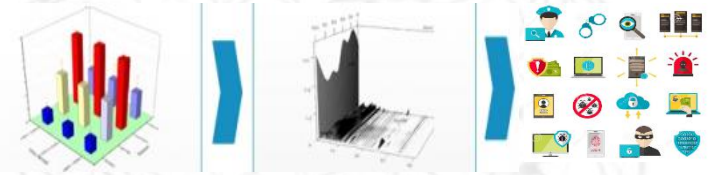
链间交互合约安全

合约漏洞检测

跨链合约调用安全

链间数据安全

数据一致性安全验证



跨链数据传输潜在攻击发现

异构多链交互的智能防护机制

跨链—致性

在跨链场景中，跨链交易的一致性问题可以退化为跨链交易原子性问题，其可以
分为两类：

· 一次共识过程解决跨链原子性问题，解决问题的着力点在共识算法创新上。

公证人模式

· 通过双向锁定、资产托管的方式来实施过程控制。可以归结为多次共识过程。

中继模式、哈希锁定模式

跨链可用性

可用性代表的是区块链网络的数据可访问性。在跨链场景中，某个单链的不可用
会影响本链的请求和其他链发出的跨链交易请求，导致其他链自身交易处理失败，
进一步降低整体可用性。
因此在跨链交易场景中，具体而言，有几点需要考量：

- 交易时延的要求
- 交易对原子性的要求
- 交易状态的背书对一致性的影响
- 治理模型失败的影响

总结

- 区块链基本概述
- 区块链跨链技术
- 区块链跨链安全分析