边界智能
BIANJIE.AI

跨链技术和BSN-IRITA HUB分享

上海边界智能科技有限公司



边界智能
BIANJIE.AI

1. 跨链的需求和价值
2. 跨链的挑战和难点
3. 不同跨链机制及特点
4. BSN IRITA HUB跨链机制
5. 沟通交流

Bianjie Confidential 边界智能机密

边界智能
BIANJIE.AI

1. 跨链的需求和价值

2. 跨链的挑战和难点

3. 不同跨链机制及特点

4. BSN IRITA HUB跨链机制

5. 沟通交流

Bianjie Confidential 边界智能机密

跨链需求的提出

6

万个Github
区块链项目

154

个各国政府推动的
区块链项目

5600

种加密货币区块链系统

“区块链的跨链需求会越来越多，因为区块链一个是联盟链，只是在自己的行业里应用，效益就得不到最优，更多的是行业与行业之间的联盟链的跨越，所以跨链需求会成为区块链的一个拓展方向。”

----银保监会陈伟钢

来源： CoinMarketCap， CAICT

跨链是否有标准定义?

应用维度认知

- 以太坊创始人Vitalik认为跨链是一种具体应用能力，“区块链互操作主要指**两条区块链之间进行资产转移、支付或信息交互的能力**。”
- 法国里昂第一大学（UCBL）研究者认为**跨链应用范围不仅限于区块链间**，“区块链的互操作性有三种类型，一是不同区块链之间的互操作性，二是使用同一区块链的去中心化应用（DApp）之间的互操作性，三是互操作性区块链和其他技术（例如与企业系统的集成）”。

技术维度认知

- 美国国家标准技术研究所(NIST)认为跨链**偏重于数据共享**，“一个互操作区块链架构是由可区分的区块链系统组成，每个区块链系统代表一个唯一的分布式数据帐本，其中执行原子交易可能跨越多个异构区块链系统，并且**记录在一个区块链中的数据可以被另一笔外部交易以语义兼容的方式访问、验证和引用**。”
- 澳大利亚天主教大学（ACU）认为跨链更**强调功能的触发和执行**，“跨链互操作不是将状态直接更改为另一个区块链系统；相反，是在另一个系统上触发一些功能集，而这些功能集有望在其自己的网络内执行操作。”

来源:

什么情况下需要用到跨链?

资产转移/交换

资产的互换与转移包括公链数字资产（通证）互换、联盟链或者私有链链下资产数字化上链后的资产互换或者转移



数据共享

包括各种数据操作的链上凭证等存储在链上的证据数据，原始数据等存储在链下的检索数据等，不同区块链系统的数据格式、存储方式、背书方式等存在差异，导致存证和凭证数据无法在不同系统中互认



服务协同

通过链间的信息交互，可以实现跨链合约的调用完成更复杂功能，实现不同链的功能专业化分工，以及一些以链治链，多链自动化治理和穿透监管



边界智能
BIANJIE.AI

1. 跨链的需求和价值

2. 跨链的挑战和难点

3. 不同跨链机制及特点

4. BSN IRITA HUB跨链机制

5. 沟通交流

Bianjie Confidential 边界智能机密

跨链的实现难点



信息真实性

原链上的交易信息对于另一条链来说是一个外部信息，如何保证这个外部信息进入另一条链时是正确的，且是最终态的（使用中本聪共识机制的区块链没有终局状态，始终存在分叉的情况，只是随着确认块的增加，概率逐渐变小）。



交易原子性

交易作为一个整体来对待，交易包含的处理动作要么全部成功，要么全部失败，而不会存在部分成功，部分失败的情况，无法保证原子性会造成双重支付。跨链双方是两条独立的链，具有不同的共识机制、数据结构、交易处理逻辑。



事务一致性

两条链上事务执行之前和之后的链状态保持一致，如果交易规则得到验证，新的状态有效，如果出现业务逻辑错误（如链A用户转账了100比特币但链B用户只得到相当于60个比特币的以太币），则两条链的状态需要回滚。

主流的跨链技术

公证人机制



不同区块链之间使用共同信任的第三方充当公证人进行跨链消息的验证和转发；

可细分为单签名公证人机制、多签名公证人机制和分布式签名公证人机制等

哈希锁定



哈希时间锁定采用了哈希锁和时间锁，迫使资产接收方在截止时间内确定收款并产生收款证明给付款人，否则资产会归还。收款证明能够被付款人用来获取接收人区块链上的等价值资产或触发其他事件

侧链



采用双向锚定主链资产并使该资产可以在主链和侧链之间进行价值转移，不是货币的转移。暂时将主链上的代币锁定，然后将等价值的代币在侧链上释放

中继



本质上是公证人机制和侧链机制的融合和扩展，可以视为侧链的升级版本。

全球最知名的两个跨链项目 Cosmos 和 Polkadot 采用的都是基于中继链的异构多链系统

ripple

LIGHTNING NETWORK

BTC RELAY

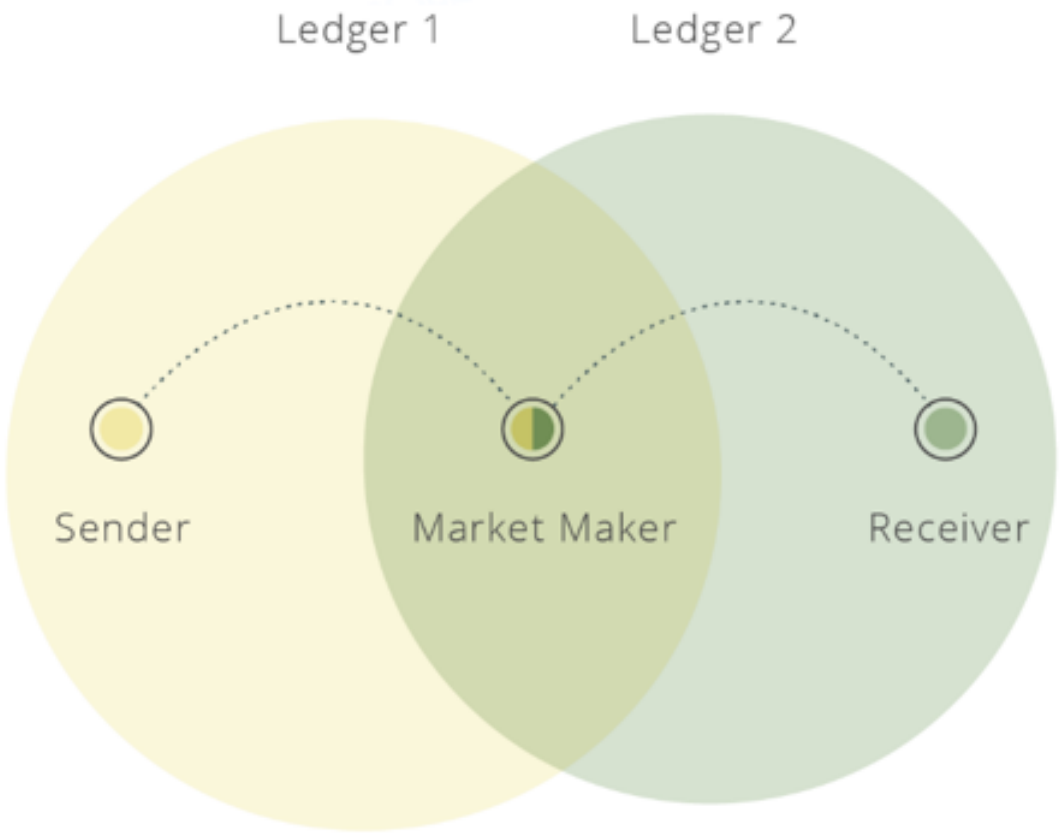
COSMOS Polkadot.

公证人机制（Notary schemes）

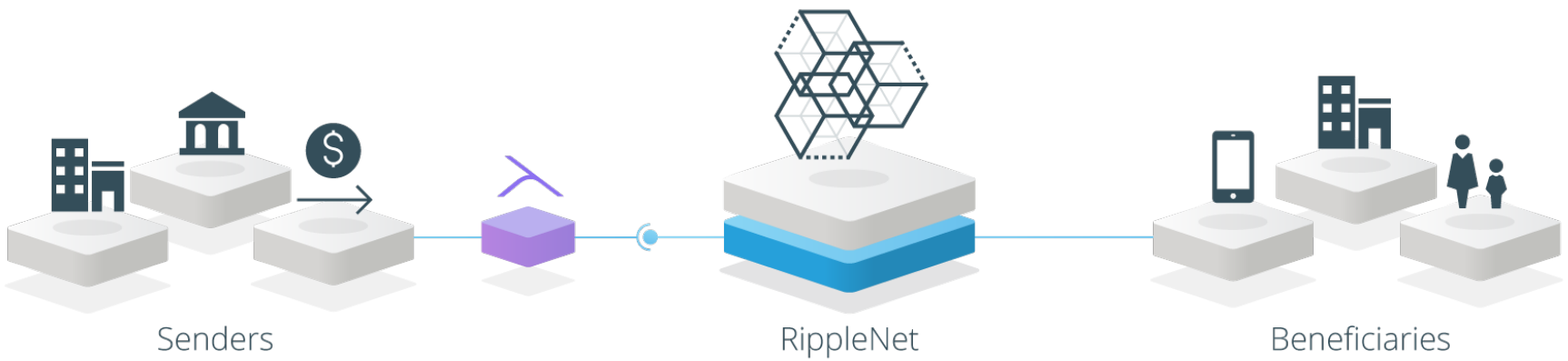
通过引入一个A和B共同信任的第三方作为中介，公证人为交易对手双方创建资金托管，当交易共识达成后自动触发交易

优点：技术实现简单，能够比较灵活地支持不同类型的底层区块链体系

缺点：中心化风险，公证人机制的安全性保障完全由公证人系统保障，参与跨链的相关方需要对中间人给予较大的信任，只能实现交换不能实现转移



Ripple网络结构



XVia

帮助各类机构接入 Ripple 支付网络的工具

RippleNet

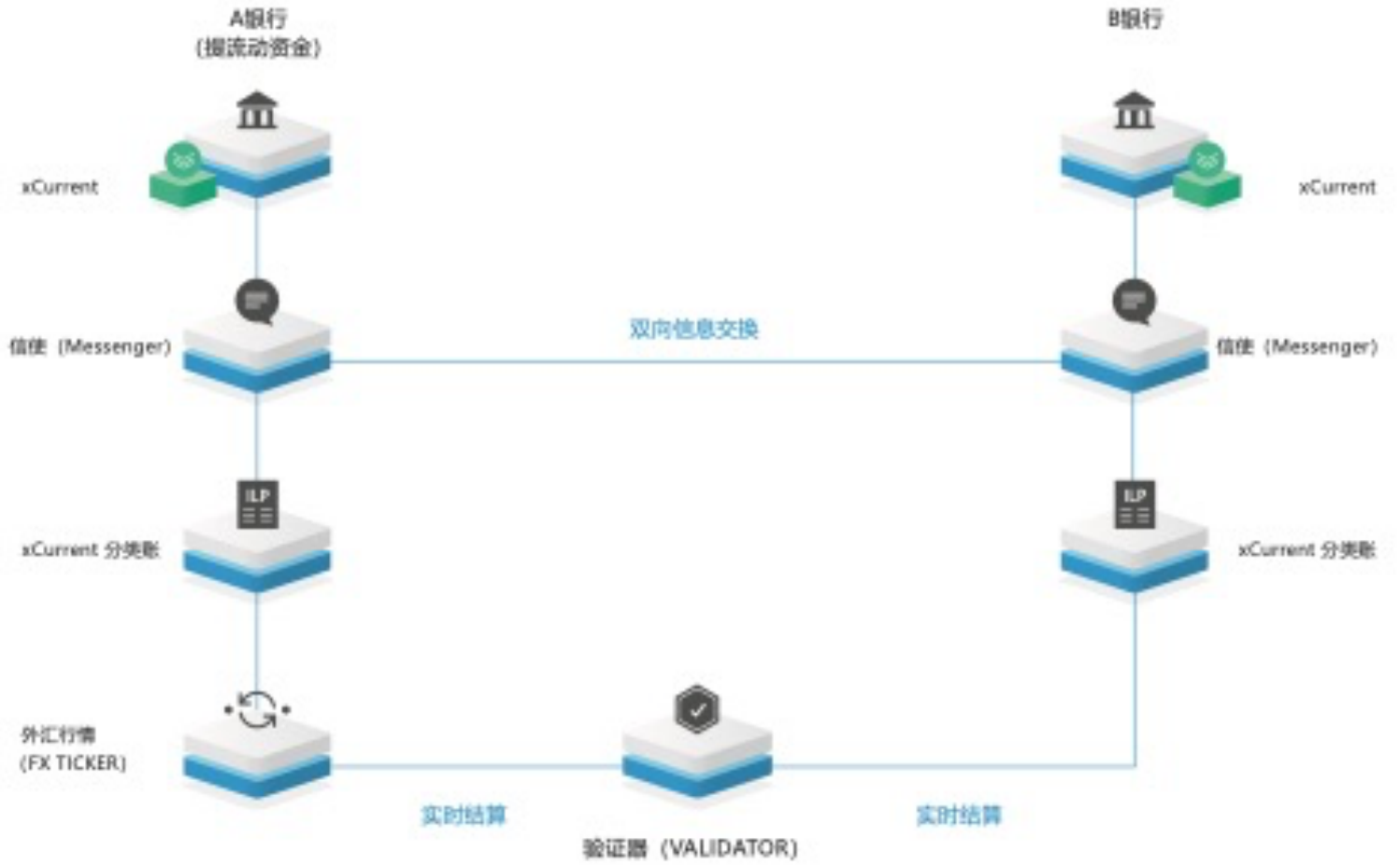
没有中心处理机器，网络中所有的关键信息都是加密的，节点不具备匿名性

xCurrent

在银行系统中处理 Ripple 支付交易的一 个插件模块，安装在银行后端防火墙内

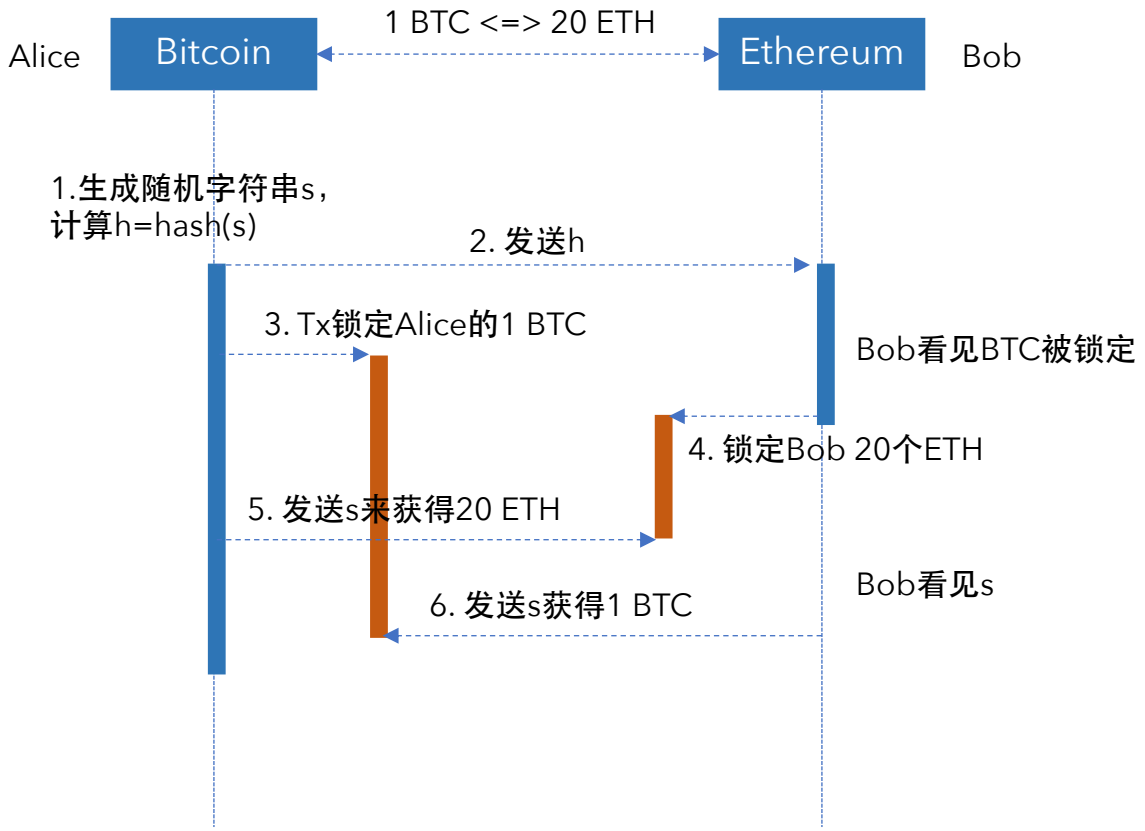
Ripple IPL（跨帐本协议）

1. Alpha公司通过Dollar银行发起给Beta公司支付100欧元的汇款请求
2. Dollar 银行通过 Messenger 连接到 Euro 银行，提交相关汇款信息、 订单信息等
3. Euro 银行根据 Dollar 银行的提交的请求检查:Beta 公司此笔订单 是否满足当地 KYC/AML 监管要求，是否还需向 Dollar 银行申请进一 步的 Alpha 公司信息;检查通过，Euro 银行返回相应的手续费
4. Dollar 银行收到 Euro 银行的应答后，通过 FX Ticker 获得欧元对美 元汇(EUR/USD=1.1429)。Dollar 银行最后呈现出来的是这笔交易的总成本(all-in cost)
5. 一旦 Alpha 公司接受了这个费用，这笔支付即被发起，ILP 账本也同时更新
6. Validator 收到两边银行的资金存入 Hold 账户的证明，共识通过，它就触发双方资金清算，自动记录两边账本



哈希时间锁（Hash Time Lock Contracts）

- Alice 随机构建一个字符串 s，并计算出其哈希 h = hash(s)；
- Alice 将 h 发送给 Bob 的合约；
- Alice 锁定自己的 1 个 BTC 资产，并设置一个较长的锁定时间 t1, 同时设置了获取该 BTC 的一个条件：谁能够提供 h 的原始值 s 就可以得到该 BTC;
- Bob 观察到 Alice 合约中锁定了一个 BTC, 然后 Bob 锁定自己的 20 个 ETH 资产，并设置一个相对较短的锁定时间 t2 , t2 < t1, Bob 也设置了同样获取条件（谁提供 h 的原始值 s 就可以获取 20 个 ETH）；
- Alice 将自己最初生成的字符串 s 发送到 Bob 的合约里取得了 20 个 ETH;
- Bob 观察到步骤 5 中 Alice 的 s 值，将其发送给 Alice 的合约成功获取 1 个 BTC; 至此 Alice 和 Bob 完成了资产的交换。



侧链

相对性
不能单纯的说某条链B是侧链，而必须说这条链B可以是链A的侧链

独立性
链B可以有自己的功能，在它自己运行时不需要链A的支持，出了问题也不会影响主链A

互通性
当要实现跨链的功能时才需要B链和A链进行互通

- 侧链可以虚拟化地横向和纵向提升主链的性能。所谓横向，就是将多个侧链与主链互通，将大部分交易放到侧链上，然后再通过与主链互通实现，可以虚拟地提升主链的TPS
- 侧链可以有主链不具有的功能，通过侧链，主链看上去也像是支持了这些功能

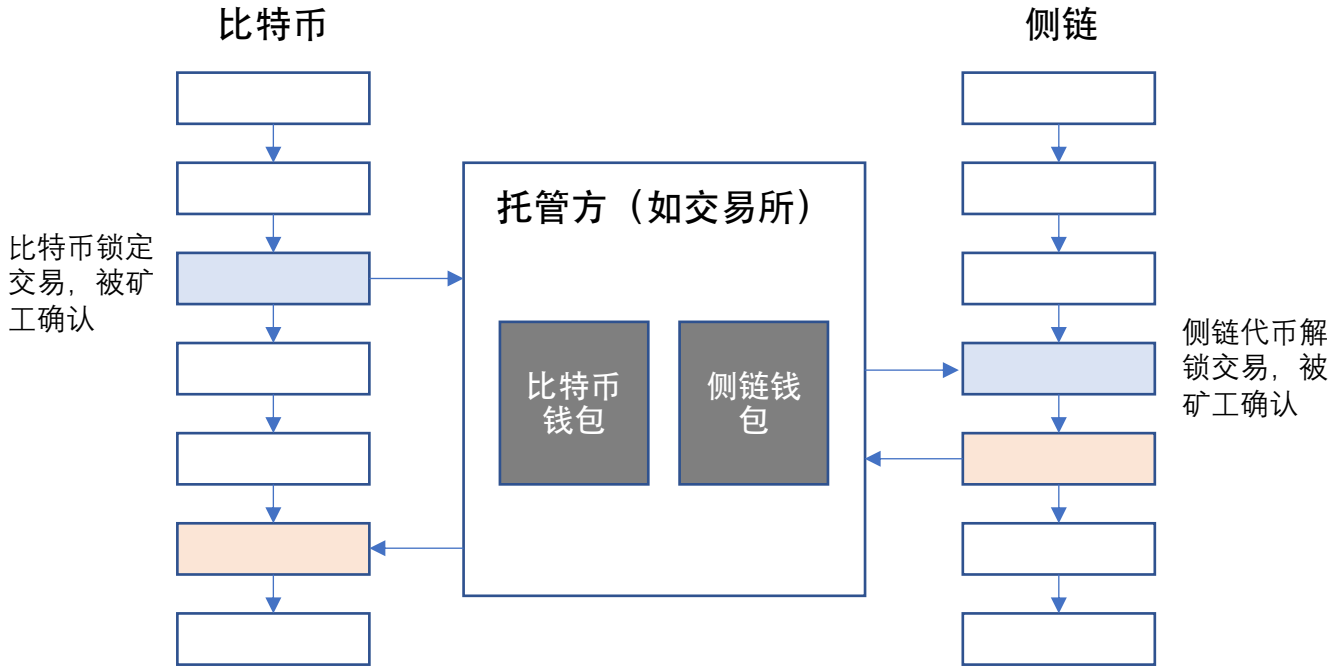
单一托管模式 Single Custodian

单一托管模式其实就是中介模式

将主链上的数字资产发送到一个托管方，类似于交易所的形式，当托管方收到相关信息后，就往侧链转移等价值的侧链币，反之亦然

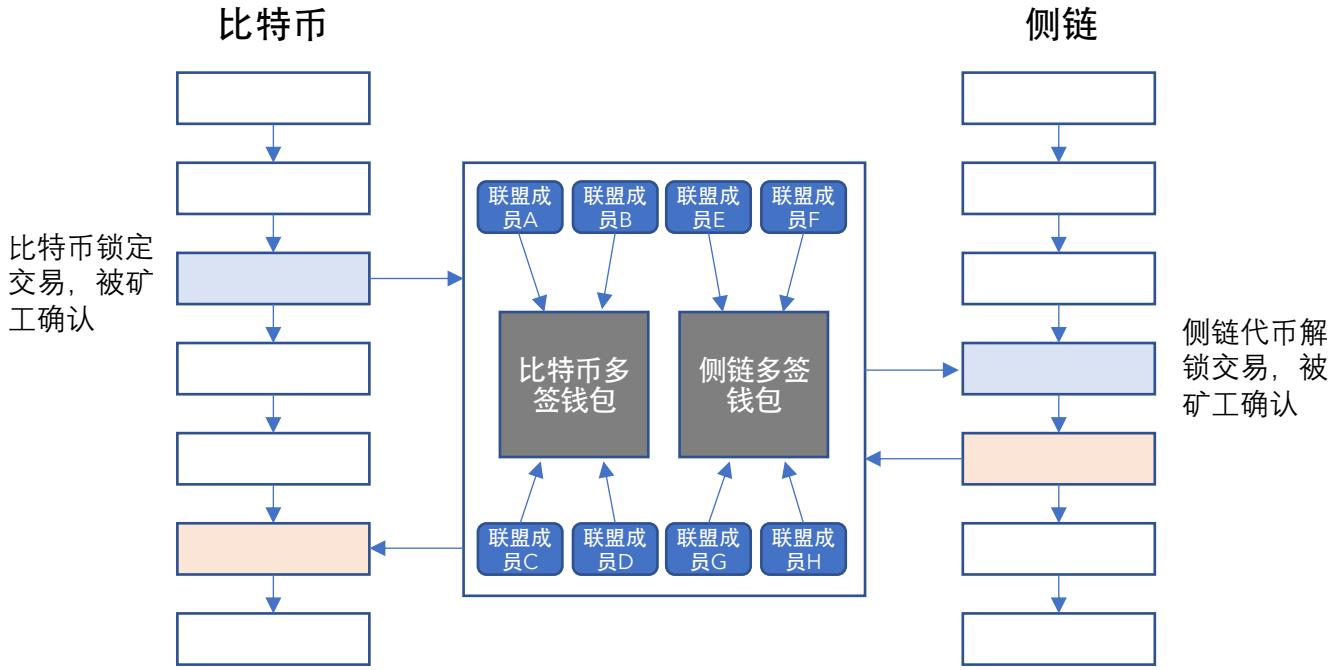
优点：简单

缺点：中心化



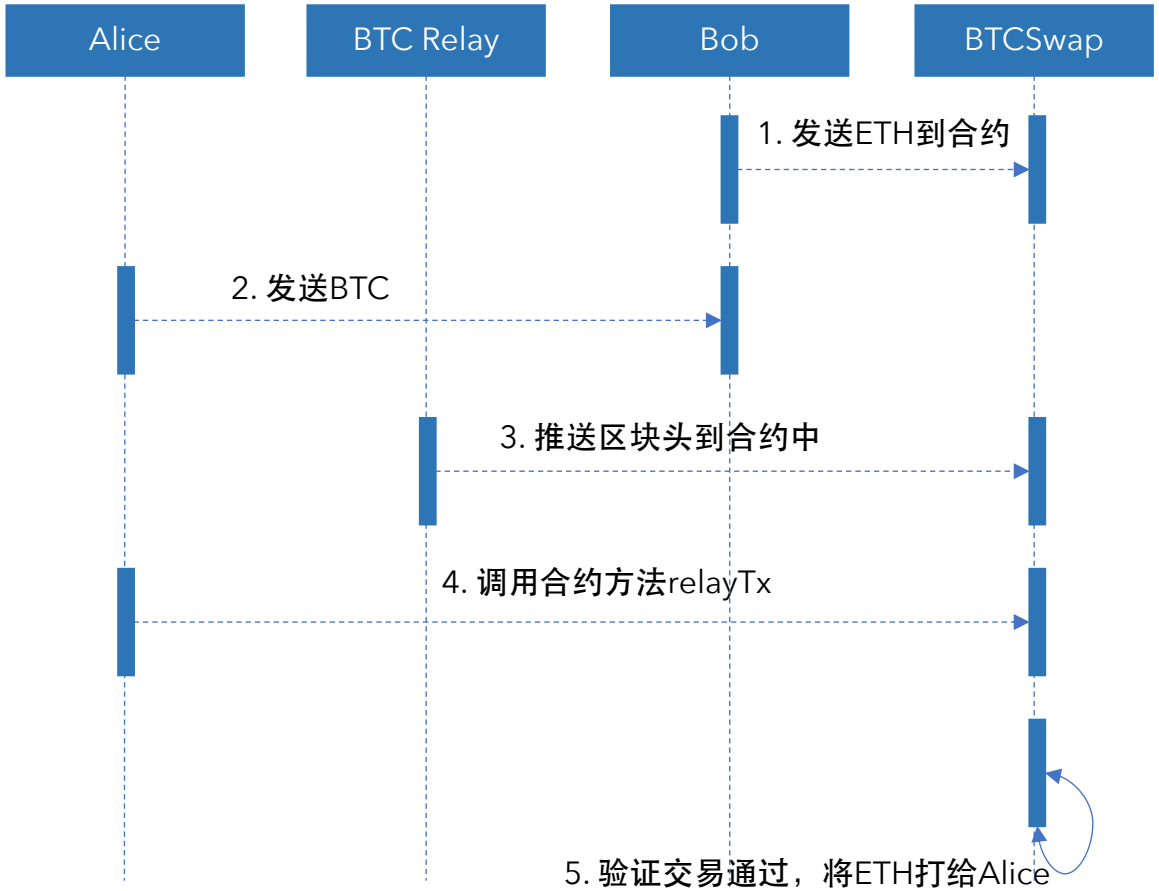
多签联盟模式 Federated peg

多签联盟模式和单一托管模式的区别就是，中间的托管方不是一个，而是多个，每一笔交易需要 M-of-N 多重签名确认



SPV(Single Payment Verification)证明模式

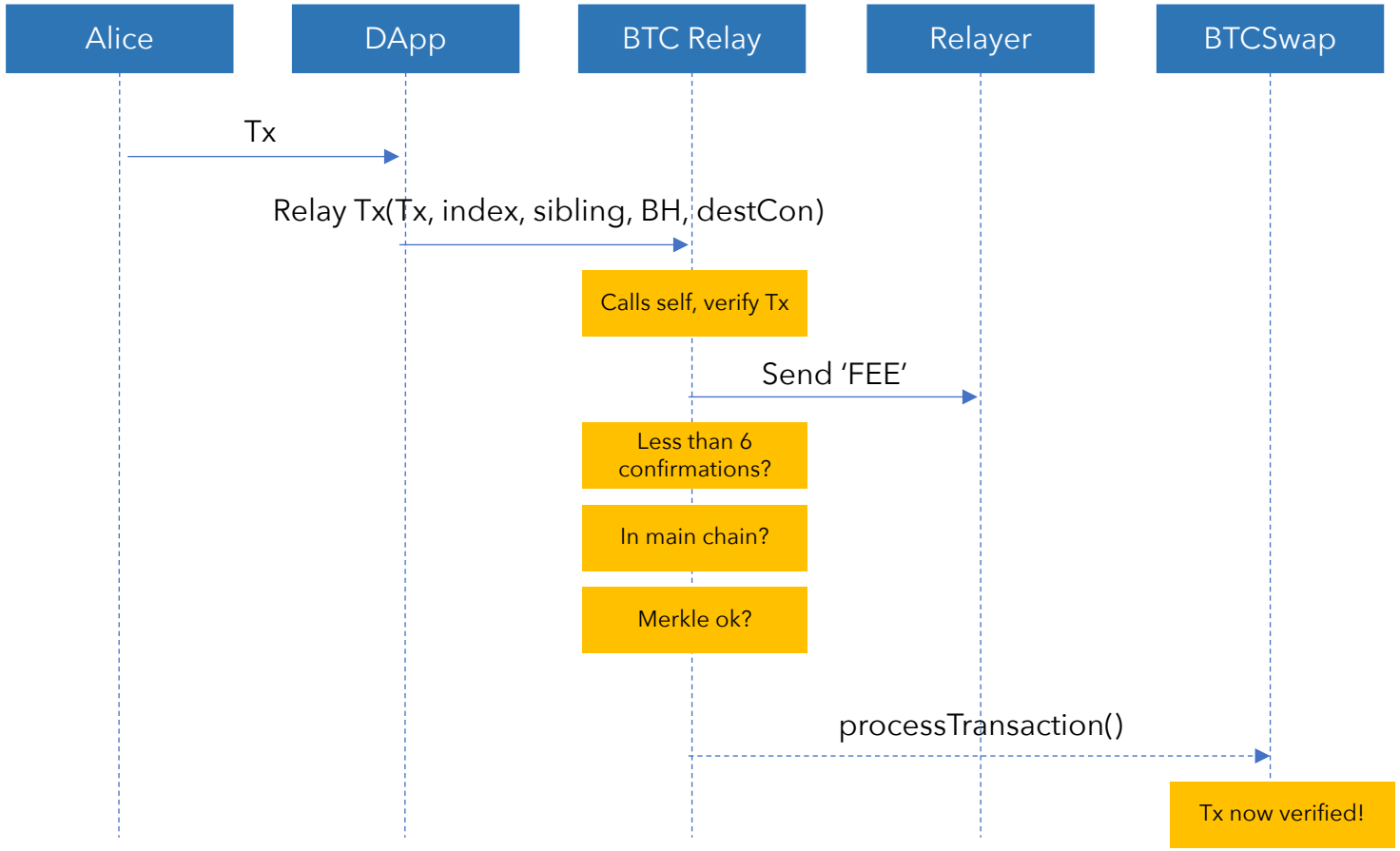
1. Bob将50ETH发送到BTCSwap的合约进行冻结(该合约若确认Bob接收到来自Alice的1BTC就自动将50ETH转给Alice)；
2. Alice确认Bob冻结信息后，将1BTC转到Bob比特币账户；
3. BTC-Relay将比特币区块头推送到BTCSwap合约；Alice将自己转BTC给Bob的交易tx发给合约BTCSwap合约，请求50ETH；
4. BTCSwap合约结合tx和比特币区块链进行SPV验证，验证通过则将50ETH转到Alice的以太坊地址；



SPV证明模式： BTC Relay

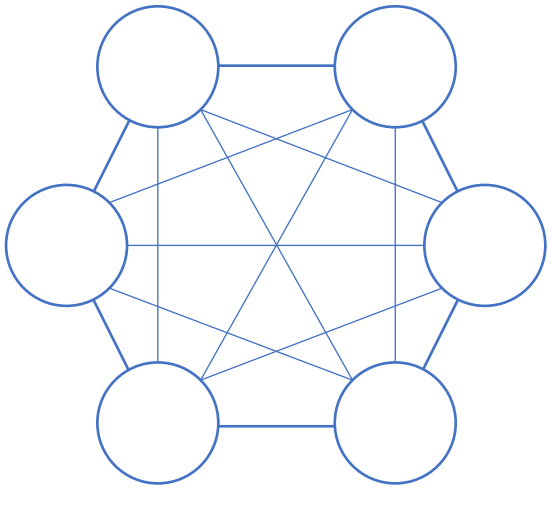
BTC-Relay功能

- 验证比特币的交易
- 传递比特币交易到以太坊智能合约
- 存储比特币区块头部信息
- 检查智能合约内部最新的比特币块信息



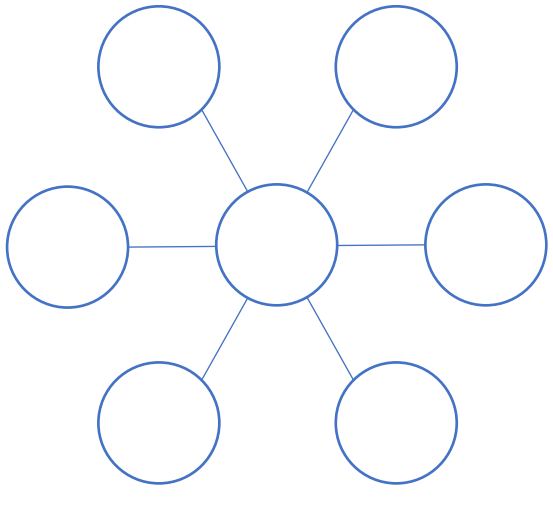
中继链： 侧链+公证人

侧链方式

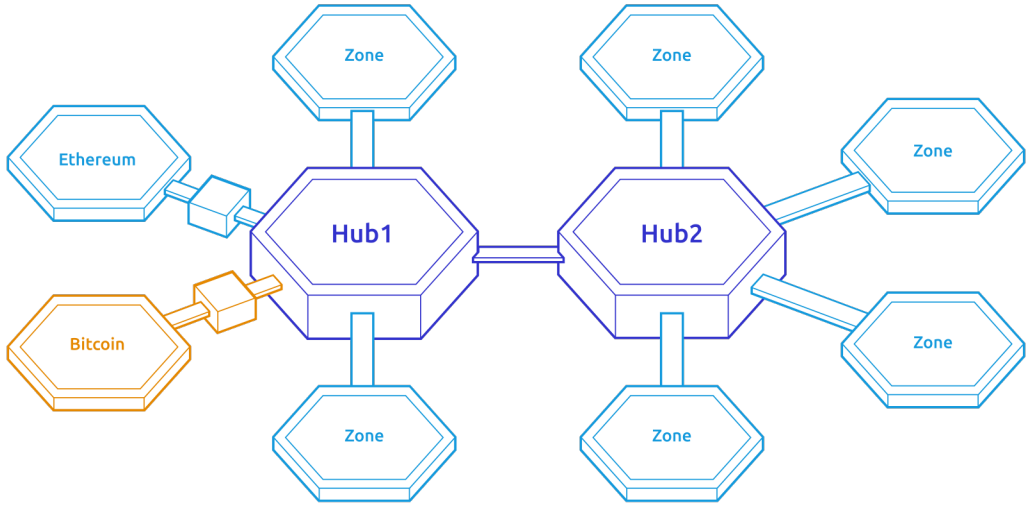


复杂度 N*(N-1)/2

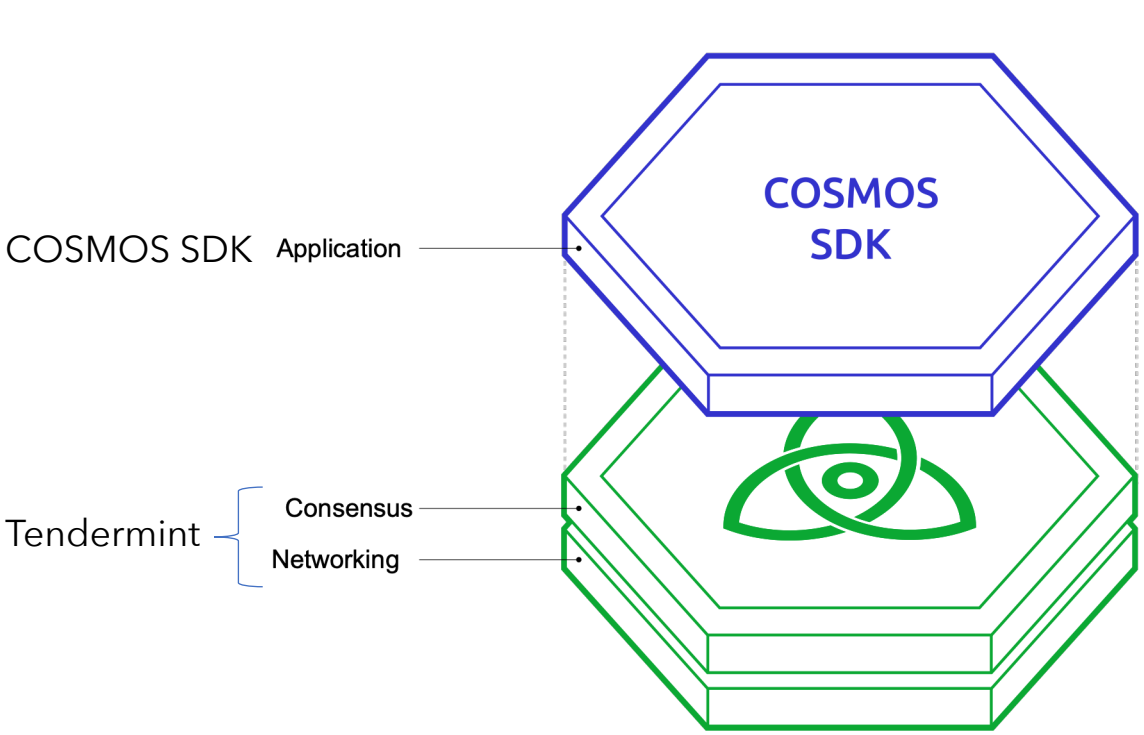
中继链方式

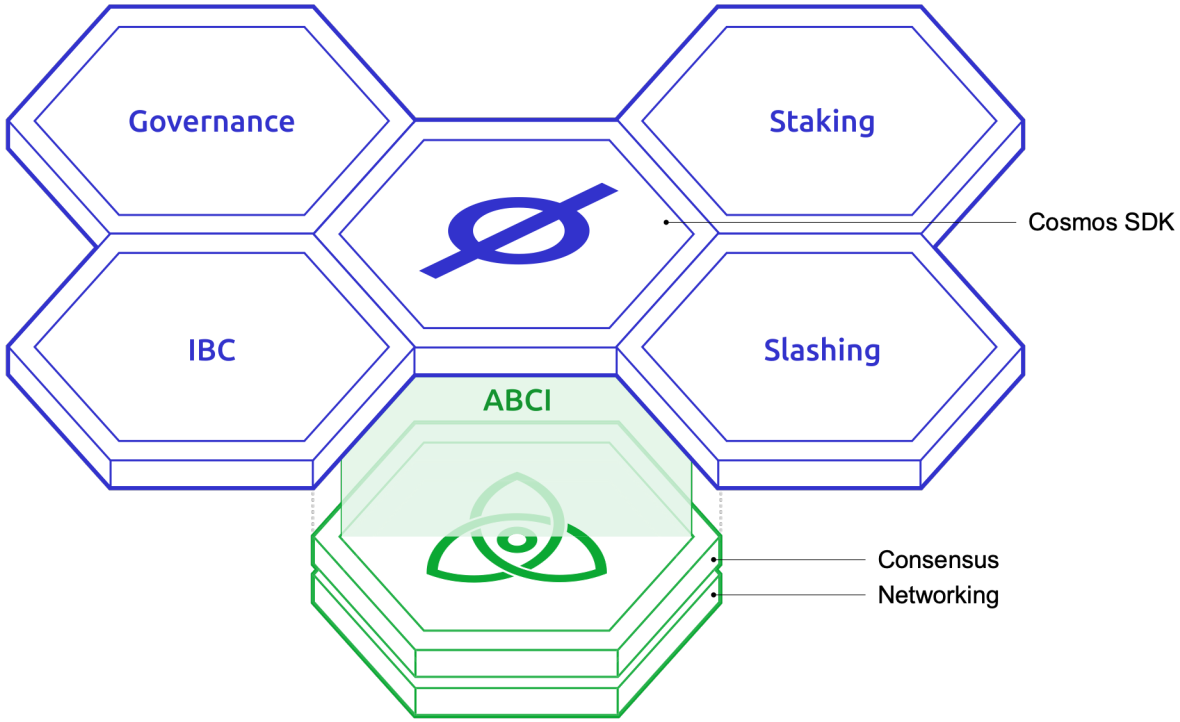


复杂度 N



代表项目：COSMOS

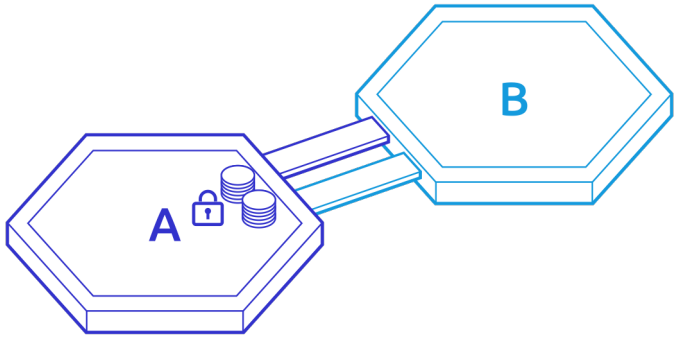

COSMOS SDK
Application
COSMOS
SDK
Tendermint
Consensus
Networking


Governance
Staking
Cosmos SDK
IBC
Slashing
ABCI
Consensus
Networking

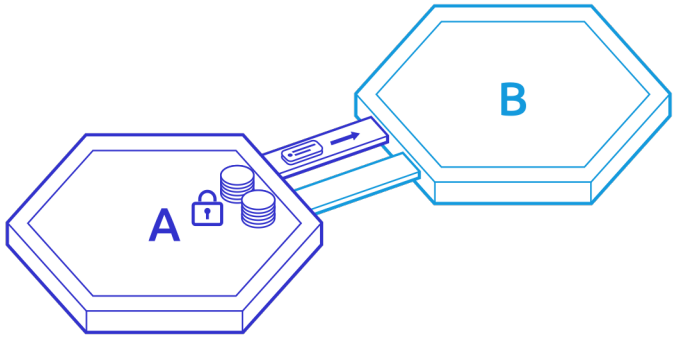
IBC跨链运作解析

链A上的一个帐户要发送10个通证链B。
链A和链B都需要运行一个对方链的轻客户端，连续地接收对方链的区块头信息

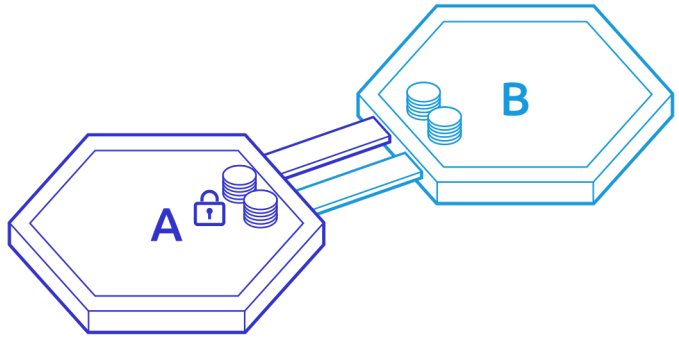
触发IBC传输后，ATOM被锁定在链A上



将10个ATOM绑定的证明从链A中继到链B

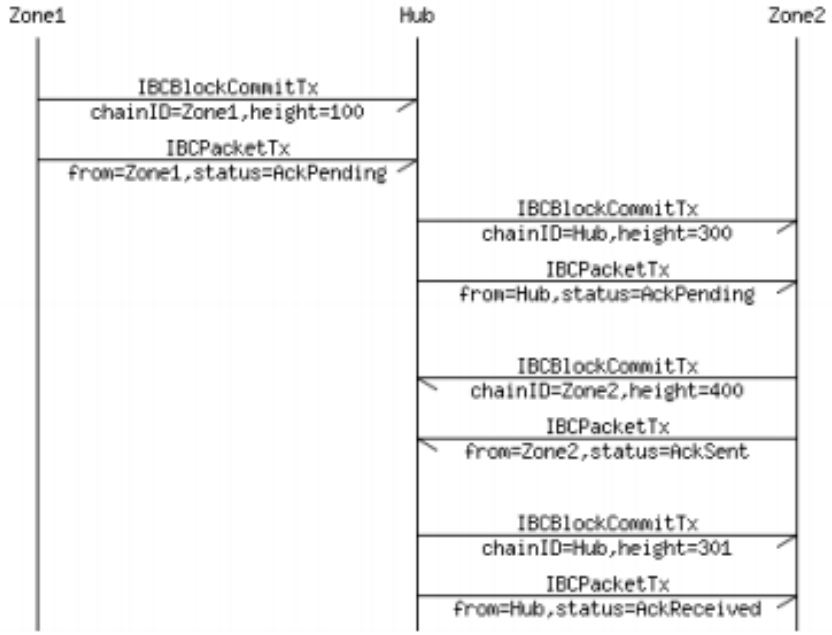


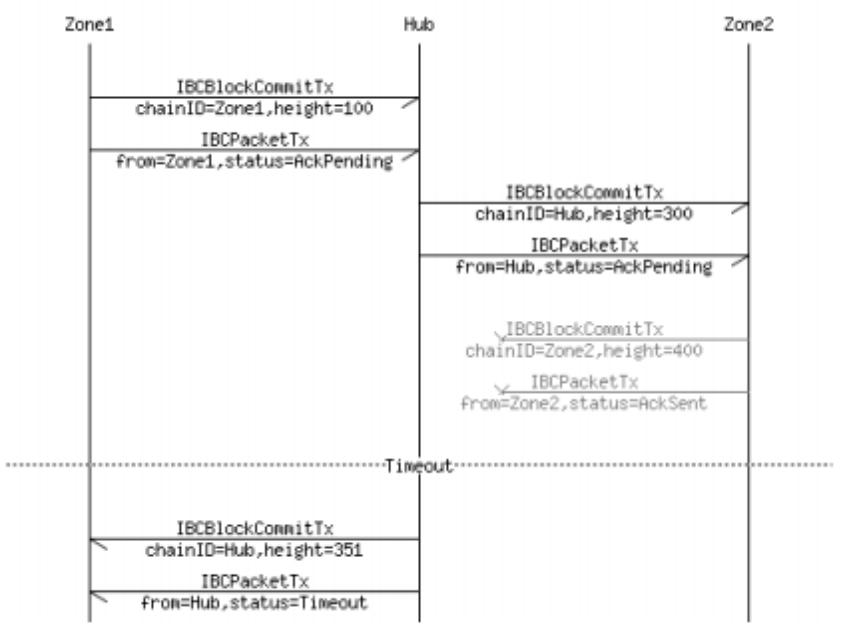
在链B上对照链A的区块头验证，如果有效，则在链B上创建10个ATOM凭证



IBC跨链互操作安全协议

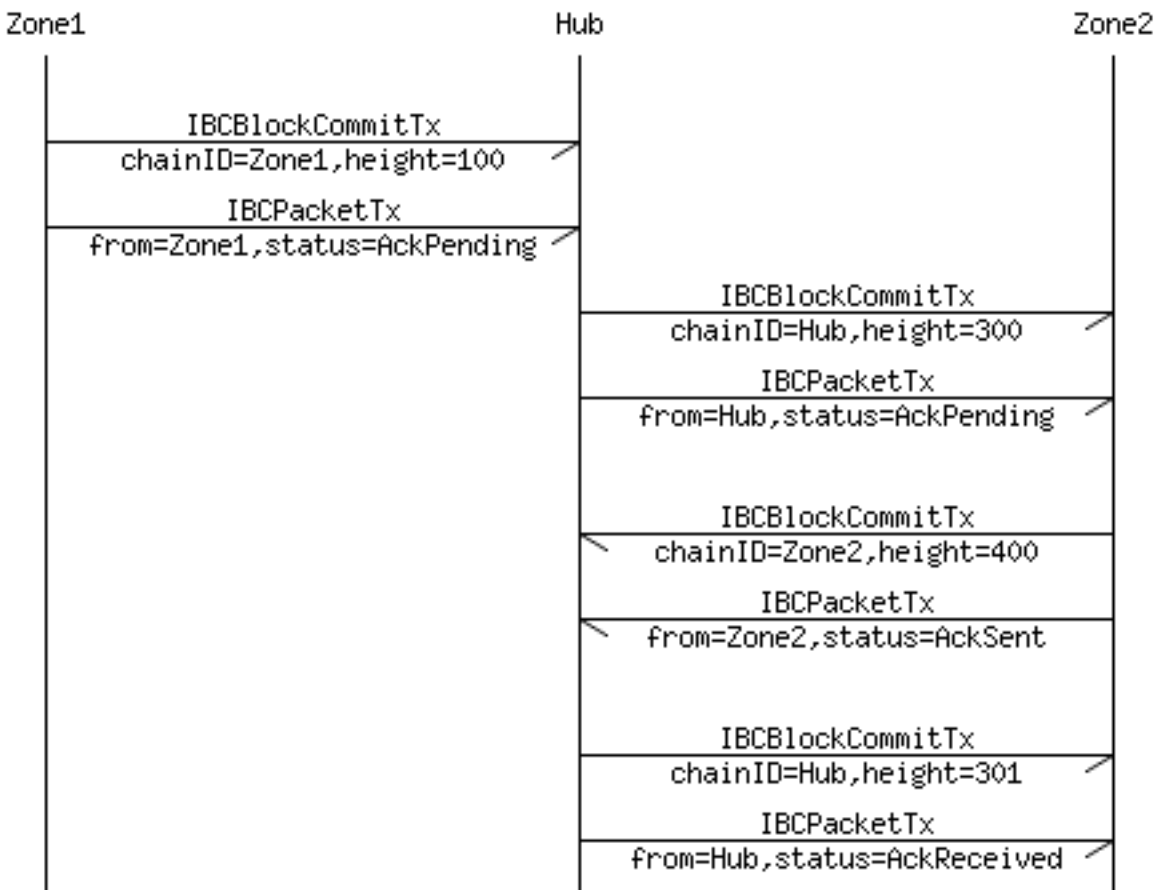
- IBC 协议，区块链的 TCP/IP 协议，包括 IBC/TAO、IBC/APP 等
  - IBCBlockCommitTx：从一个链向另一个链发送其最近的区块高度信息
  - IBCPacketTx：一个链向另一个链证明其所发的区块高度信息的真实性





IBC原理

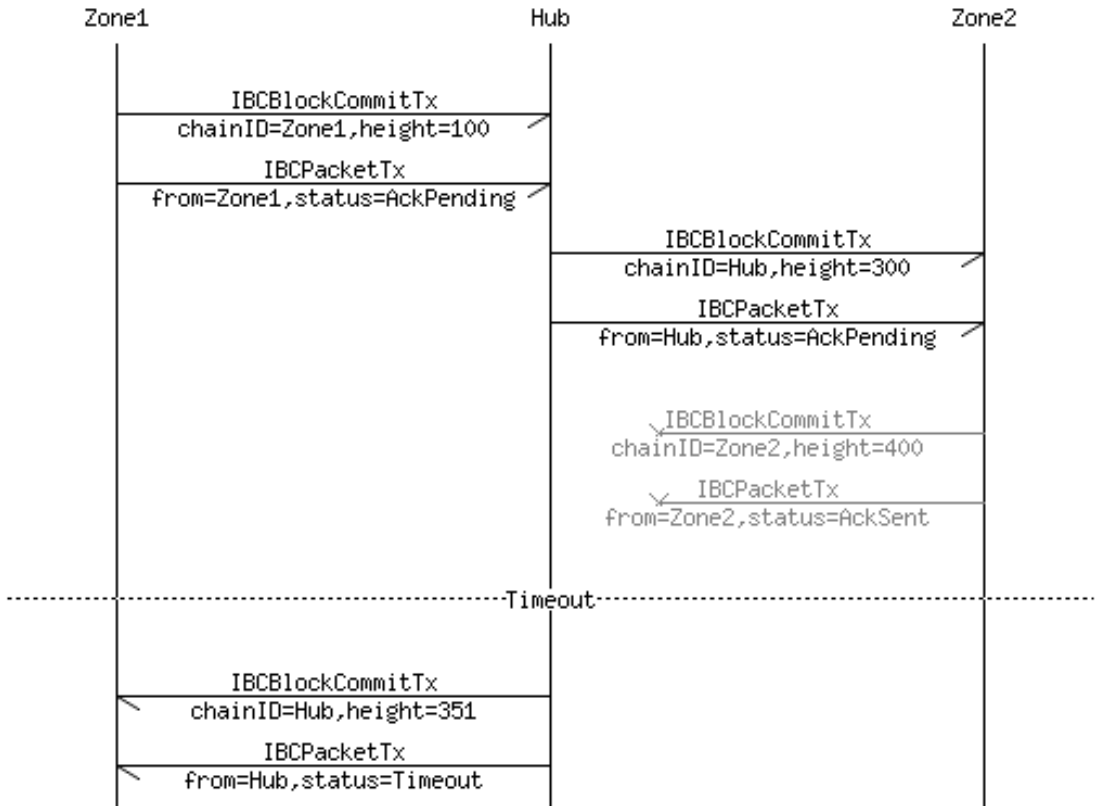
1. Zone 1发起IBCBlockCommitTx交易，将新区块头部信息（包括所有验证人的公钥）传递到HUB;
2. Zone 1发起代币转移交易;
3. Zone 1对该交易进行逻辑验证，是否合法有效;
4. 将该合法交易放到面向HUB的消息队列中;
5. Zone 1的中继程序（relayer）监听到队列中有新的消息，即生成Merkle Proof，并作为IBCPacketTx的Payload发送给HUB。（每个Zone都有一个独立的第三方中继程序，负责从原链生成Merkle Proof并组装成Packet，并发起交易，传递到目标链上）;
6. HUB验证Merkle Proof是否有效，若有效则发送消息给Zone 2（HUB给Zone2发送消息的过程同步骤1~5）;
7. Zone2在接收到HUB的消息后验证Zone1为真实有效的交易，发送消息给HUB确认可接收来自Zone1的资产;
8. HUB给Zone2发送消息，将资产发送给Zone 2，完成了资产在不同区块链之间的一次转移;



IBC原理

1. 异常情况下Zone 2 发送给 Hub 的消息丢失：
   - Hub 在等待一段时间后，发送消息给 Zone 1，告知当前交易超时，交易失败

2. 数据信息的跨链传递流程相同，以链上交易形成呈现与传递

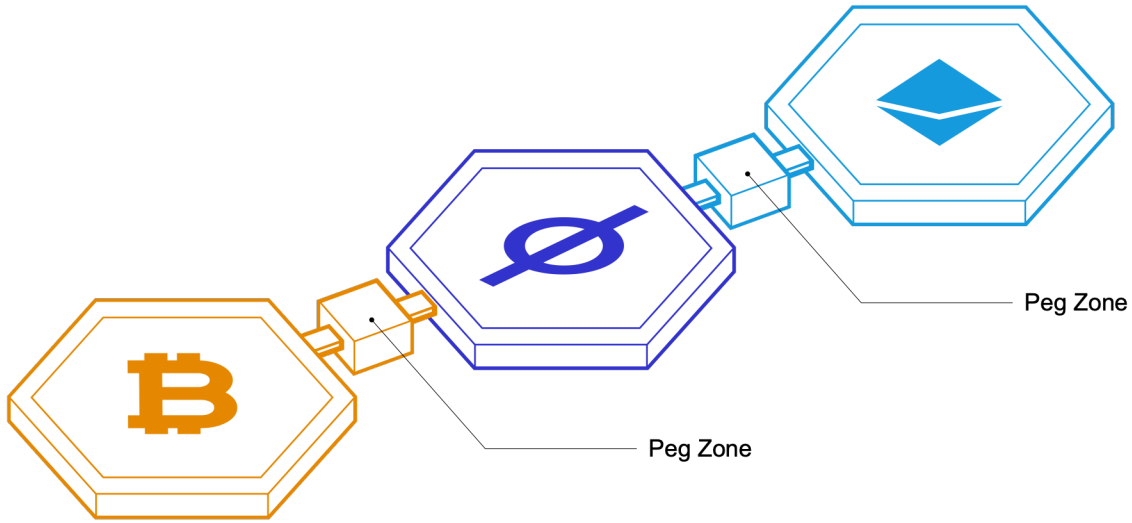


对非Tendermint共识链的支撑

即时最终链
Tendermint/PBFT

快速最终链
使用任何快速确定共识算法的区块链都可以通过调整IBC与Cosmos连接。例如，如果以太坊要切换到Casper FFG，则可以通过使IBC与Casper配合使用，在以太坊和Cosmos生态系统之间建立直接连接

概率最终链
Peg Zone本身具有快速确定性，因此与IBC兼容。它的作用是为所桥接的区块链确定最终性



各种跨链方案的比较

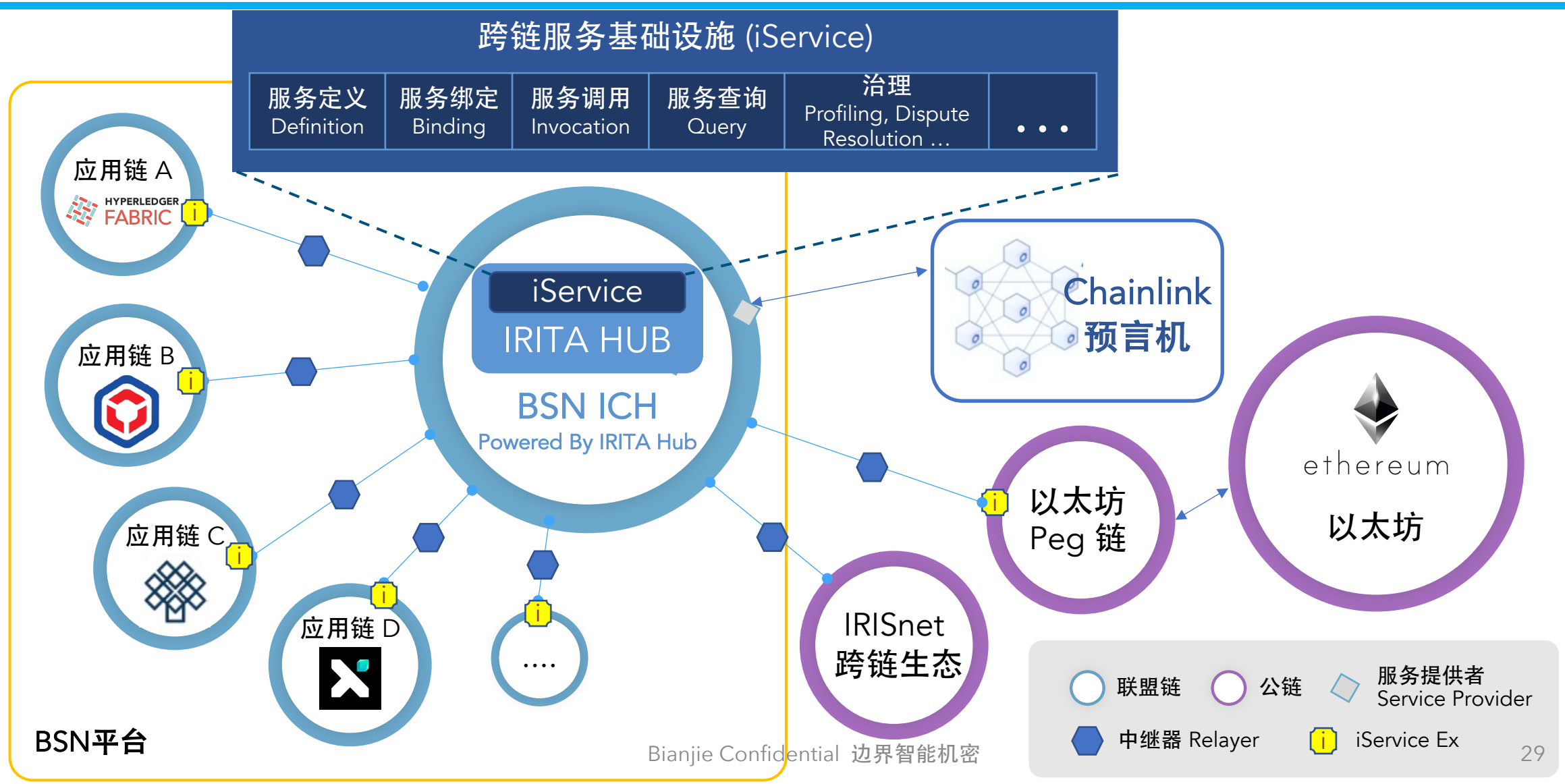
跨链技术	哈希锁定	公证人	侧链/中继
互操作性	只有交叉依赖	所有	所有(需要所有链上都有中继，否则值支持单向)
信任模型	链不会失败或者51%攻击	多数公证人诚实	链不会失败或者51%攻击
适用跨链资产转移	不支持	支持(需要共同的长期公证人信任)	支持
适用跨链预言机(Oralces)	不直接支持	支持	支持
适用跨链资产抵押	大多数支持但有难度	支持(需要长期公证人信任)	支持
实现难度	容易	中等	难

边界智能
BIANJIE.AI

1. 跨链的需求和价值
2. 跨链的挑战和难点
3. 不同跨链机制及特点
4. **BSN IRITA HUB跨链机制**
5. 沟通交流

Bianjie Confidential 边界智能机密

BSN IRITA HUB跨链服务



Bianjie Confidential 边界智能机密

IRITA HUB 跨链机制类似互联网

边界智能 BIANJIE.AI

TCP/IP 模型

应用层：HTTP
支撑 WWW的请求-响应协议

传输层：TCP

网络层：IP

链路层：网络接口及硬件

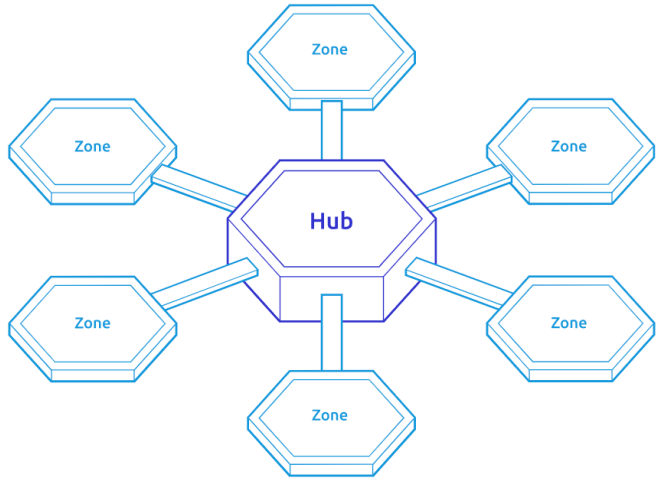
IRITA 区块链跨链通讯模型

应用层：iService 为分布式应用提供面向服务的交互协议

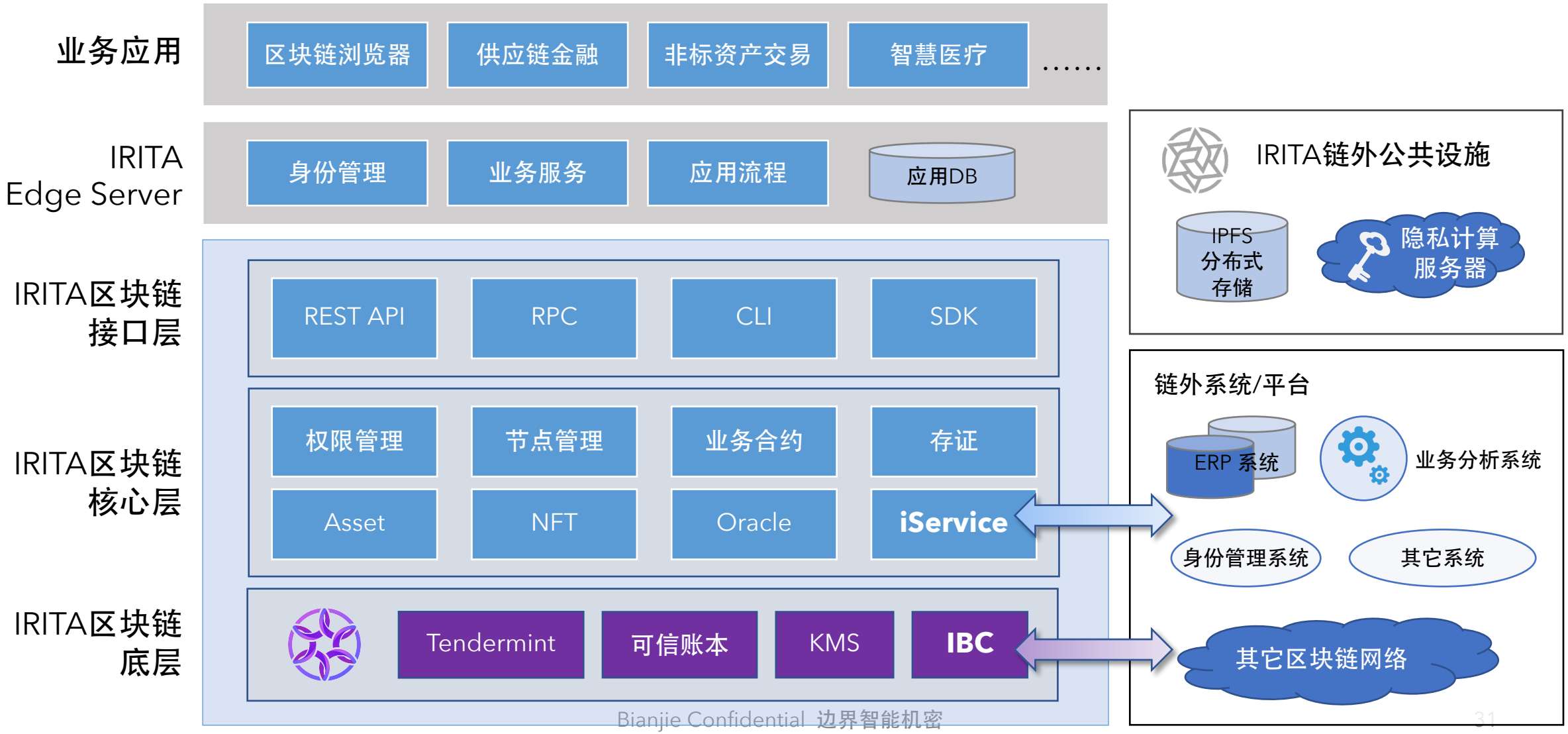
传输层：IBC 支持数据包在多个不同的区块链网络之间可信交换以转移数据和状态信息

比HTLC，公证人机制：

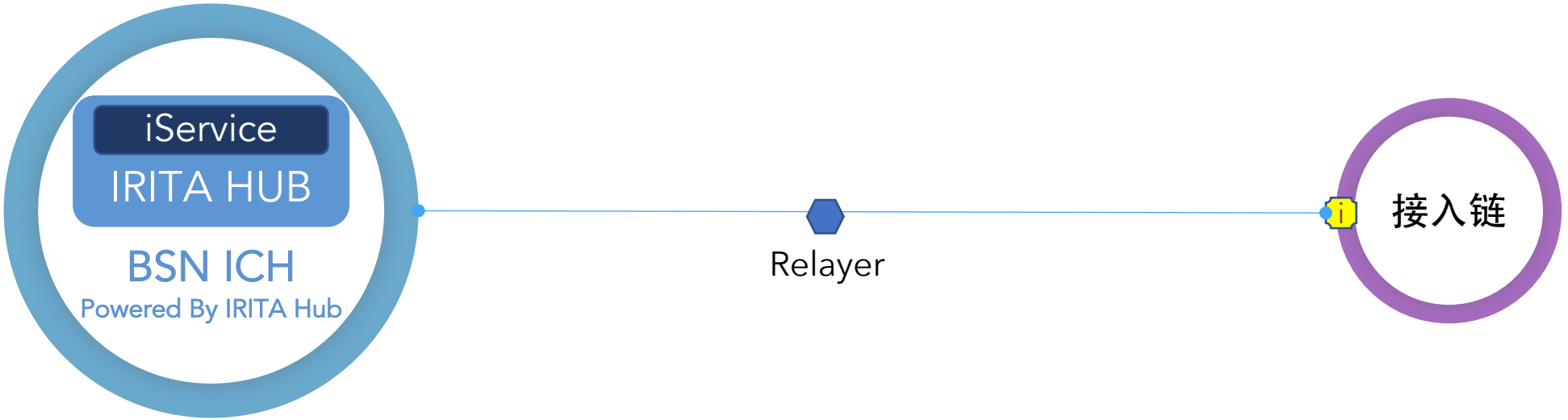
- 更安全
- 更通用
- 更具有扩展性



IRITA HUB


业务应用
区块链浏览器
供应链金融
非标资产交易
智慧医疗
.....
IRITA
Edge Server
身份管理
业务服务
应用流程
应用DB
IRITA区块链
接口层
REST API
RPC
CLI
SDK
IRITA区块链
核心层
权限管理
节点管理
业务合约
存证
Asset
NFT
Oracle
iService
IRITA区块链
底层
Tendermint
可信账本
KMS
IBC
IRITA链外公共设施
IPFS
分布式
存储
隐私计算
服务器
链外系统/平台
ERP 系统
业务分析系统
身份管理系统
其它系统
其它区块链网络

IRITA HUB跨链组件



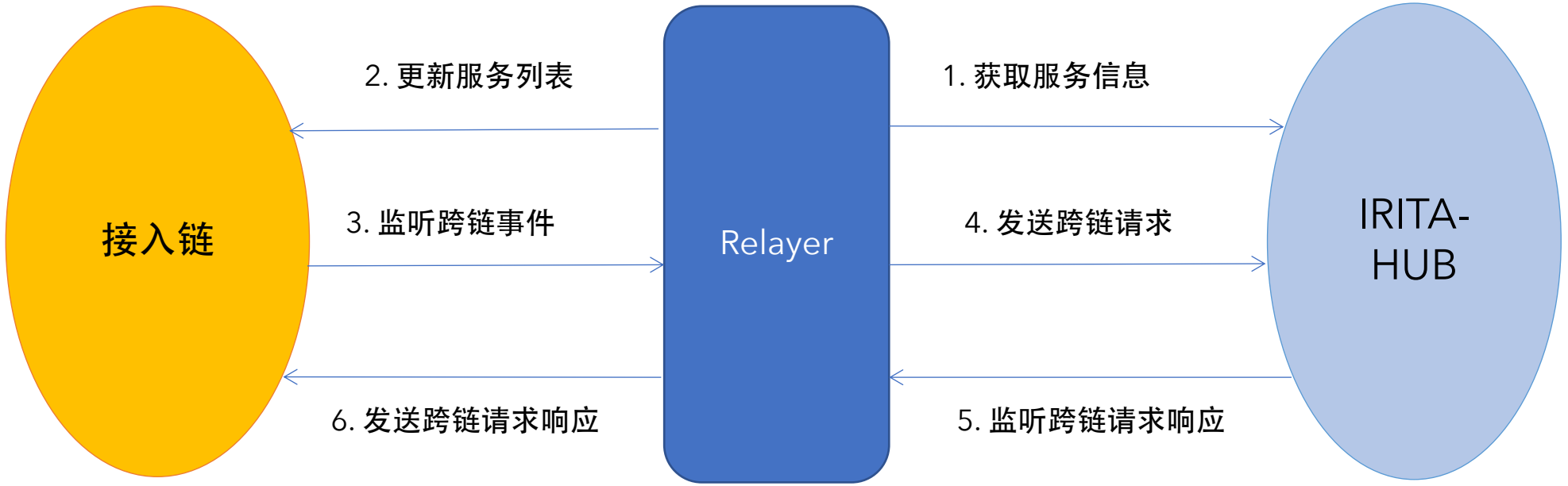
iService服务框架是在底层区块链网络上构建一个服务集成和治理层，实现对服务的定义、绑定、调用、查询、服务结算和治理等功能，完成对服务全生命周期管理

Relayer维护了HUB及接入链的轻客户端，负责跨链信息的传递

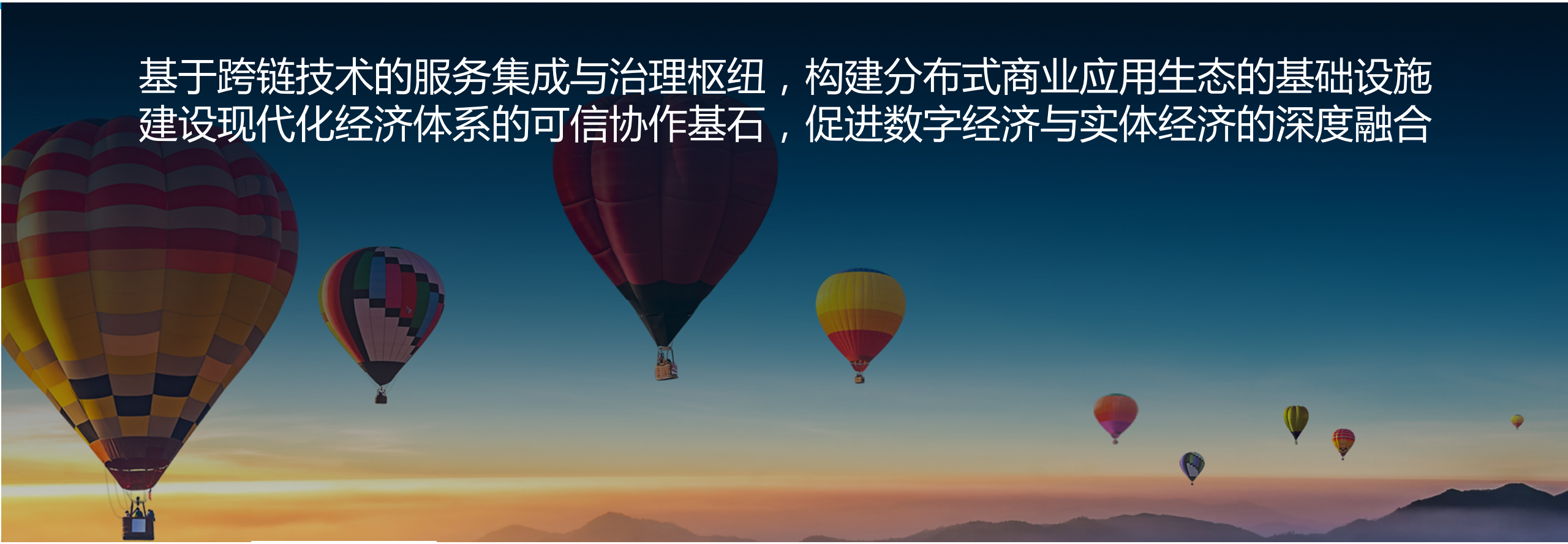
支持iService/IBC

1) iService Core Ex：负责服务的调用与响应
2) iService Market Ex：帮助接入链获取要使用的服务及服务提供商相关信息

Relayer 工作模型



上海边界智能科技有限公司



谢谢关注