银行间市场区块链系统架构设计

数据科学与计算机学院 邹哲鹏

联系方式：13802401913

邮箱：503951764@qq.com

一.系统需求分析

经调研，银行间市场主要包括同业拆借市场、票据市场、债券市场和外汇市场等，主要特征是：

1. 以商业银行作为参与主体。
2. 由商业银行总行负责处理银行间市场业务。
3. 反映商业银行彼此的结算关系。

结合课题要求，可知在完成基本业务的前提下，系统还应当保证以下属性需求：

1. **数据一致性**：区块链系统中每个节点所拥有账本的内容与记录顺序都相同。
2. **数据安全性**：商业银行的事务记录难以被窃取或篡改。
3. **数据隔离性**：商业银行的事务记录不会被竞争对手知晓，只有参与过某事务的商业银行才有查阅账本上该事务记录的权限。
4. **可监管性**：监管机构验证事务的正确性，并拥有查阅账本上所有事务记录的权限。

二.系统架构设计

2.1 整体架构

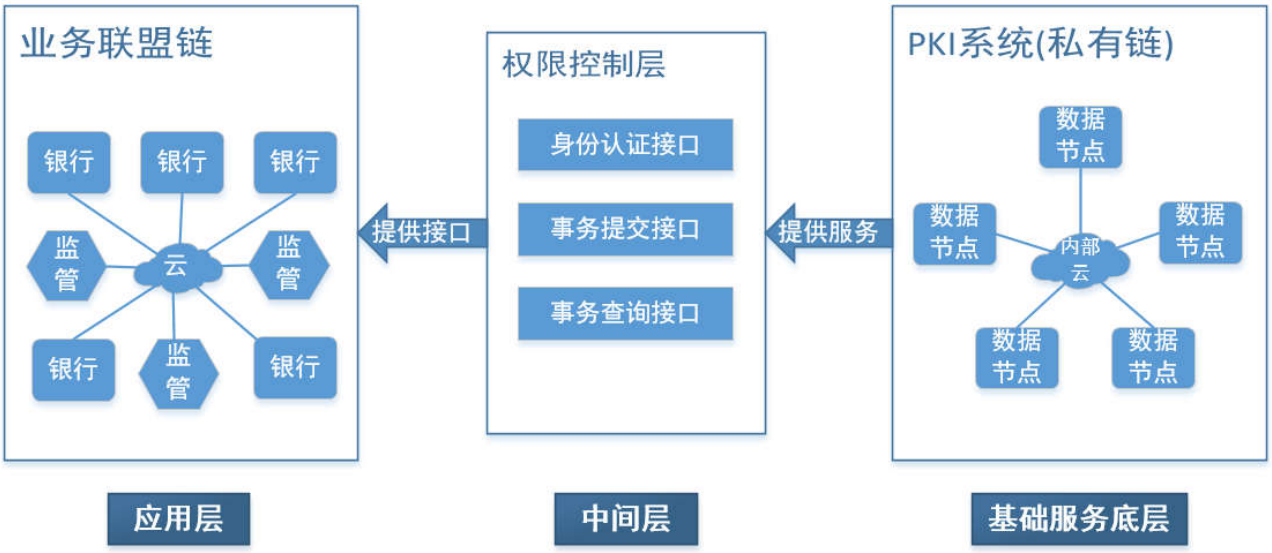

图 2-1 整体架构图

在整体架构上，银行间市场区块链系统是一个半中心化的分层系统，它由三部分组成：

1. **业务联盟链**：执行业务的主要实体，位于架构中的应用层。联盟链中各节点由商业银行或监管机构组成。

2. **基于智能合约的权限控制层**：通过智能合约建立的权限管理机制。位于架构中的中间层，是一个软件实体。

3. **基于私有链的 PKI 系统**：位于架构底层的服务支持平台，提供身份认证、事务权限管理、密钥管理等基础功能。

2.2 业务联盟链

出于数据隐私和可监管性的考虑，相比于公开链和私有链，使用联盟链记录银行间事务更加符合实际应用场景。

业务联盟链是最主要的业务实体，负责记录所有商业银行在银行间市场业务中产生的所有事务。联盟链中的节点分为两种类型：一种是由商业银行组成的**非验证节点**，每个非验证节点都有根据系统决议记录事务以及申请发布事务的功能；另一种是由监管机构组成的**验证节点**，每个验证节点都有验证事务正确性以及共同形成系统决议的功能。

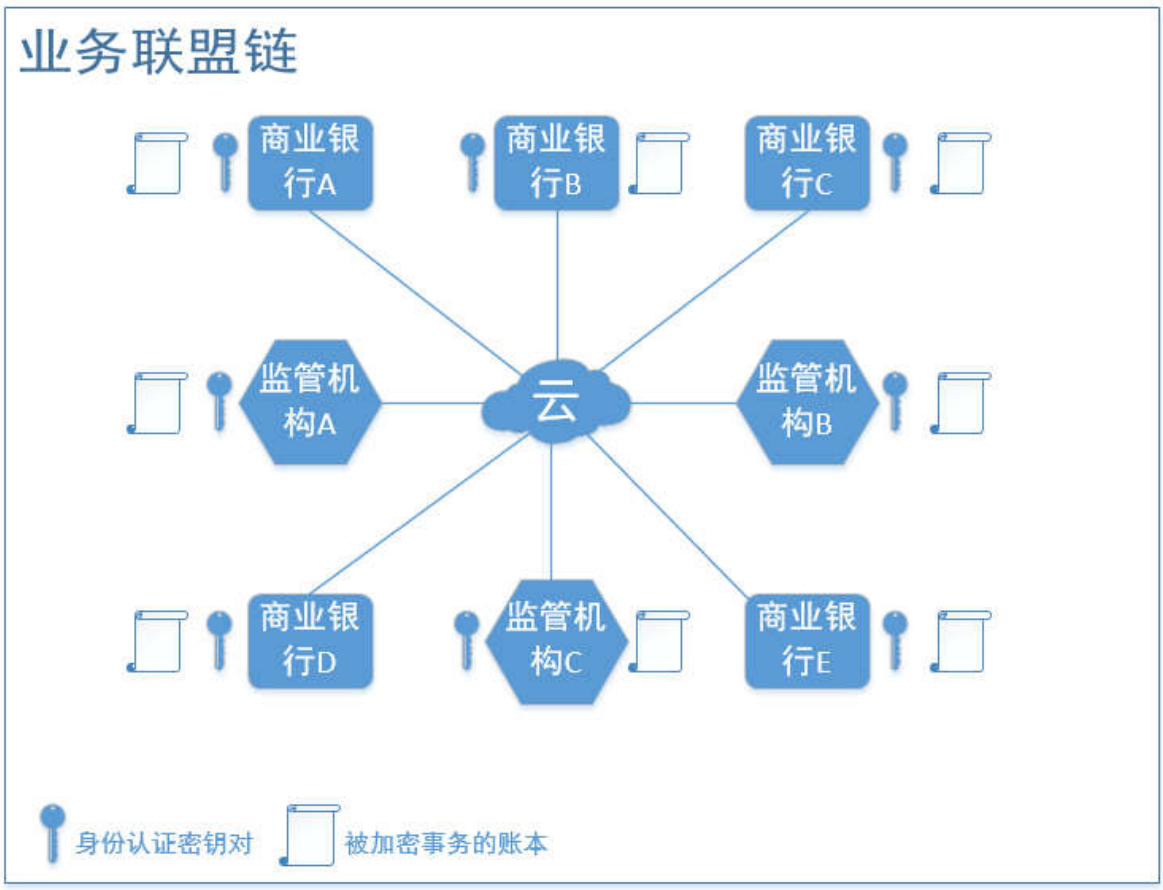

图 2-2 业务联盟链架构图

如上图所示，商业银行节点与监管机构节点均通过云（互联网或者专门架设的内部网络通道）彼此互连，任意两个节点都可以直接通信。联盟链中每个节点都拥有一个**记录系统中发生的所有事务、但每条事务都被加密的账本**，且每个账本的内容都相同。此外，每个节点都有一个用于标识身份的非对称密钥对，其中公钥对系统公开，私钥由节点单独保存。密钥对用于节点的数字签名和事务传输时的加解密。

当一个节点申请发布一个事务时，通过调用权限控制层的接口设置事务权限后，在联盟链中广播。当形成“通过该事务”的系统决议时，该事务即可被所有节点成功添加到各自的账本中。

应用层实现的主要难点在于如何保证系统决议的形成、数据一致性以及克服拜占庭错误。已知的成熟解决方案包括 Paxos、Raft 和 PBFT 等共识算法。

2.3 基于智能合约的权限控制层

系统通过智能合约构建一个用于管理事务隐私和控制节点权限的抽象中间层，这个权限控制层向业务联盟链提供以下接口：

1. **身份认证接口** ：当一个节点需要获取其他节点公钥时调用此接口。接口返回所需节点的公钥。

2. **事务发布接口**：当一个节点准备发布事务时调用此接口。接口对事务进行权限设置后广播到联盟链中，直至验证节点形成系统决议来确认事务能否成功提交。

3. **事务查询接口**：当一个节点查阅账本上的被加密事务时调用此接口。接口检查节点是否拥有查阅该事务的权限，若有则允许该节点进行查询。

这些接口的实现依赖于联盟链中各节点按照智能合约履行职责，以及 PKI 系统提供底层服务。

权限控制层实现的主要难点在于使用何种方式实现智能合约。一个可行的解决方案是智能合约作为链上代码存在于联盟链的区块中。开源社区以太坊也已经通过该方式向开发者提供了自定义智能合约的接口。

2.4 基于私有链的 PKI 系统

PKI(Public Key Infrastructure)系统是一个提供密钥管理和身份认证管理的成熟商业系统，在架构中作为底层支持平台向权限控制层提供基础服务。

由于架构中的 PKI 系统管理联盟链账本上所有加密事务的解密公钥以及节点权限名单，出于安全性的考虑，在实现方式上可使用私有链维护这些敏感数据。在组织架构上，PKI 系统还可以作为监管机构的一部分交予监管方进行运营。

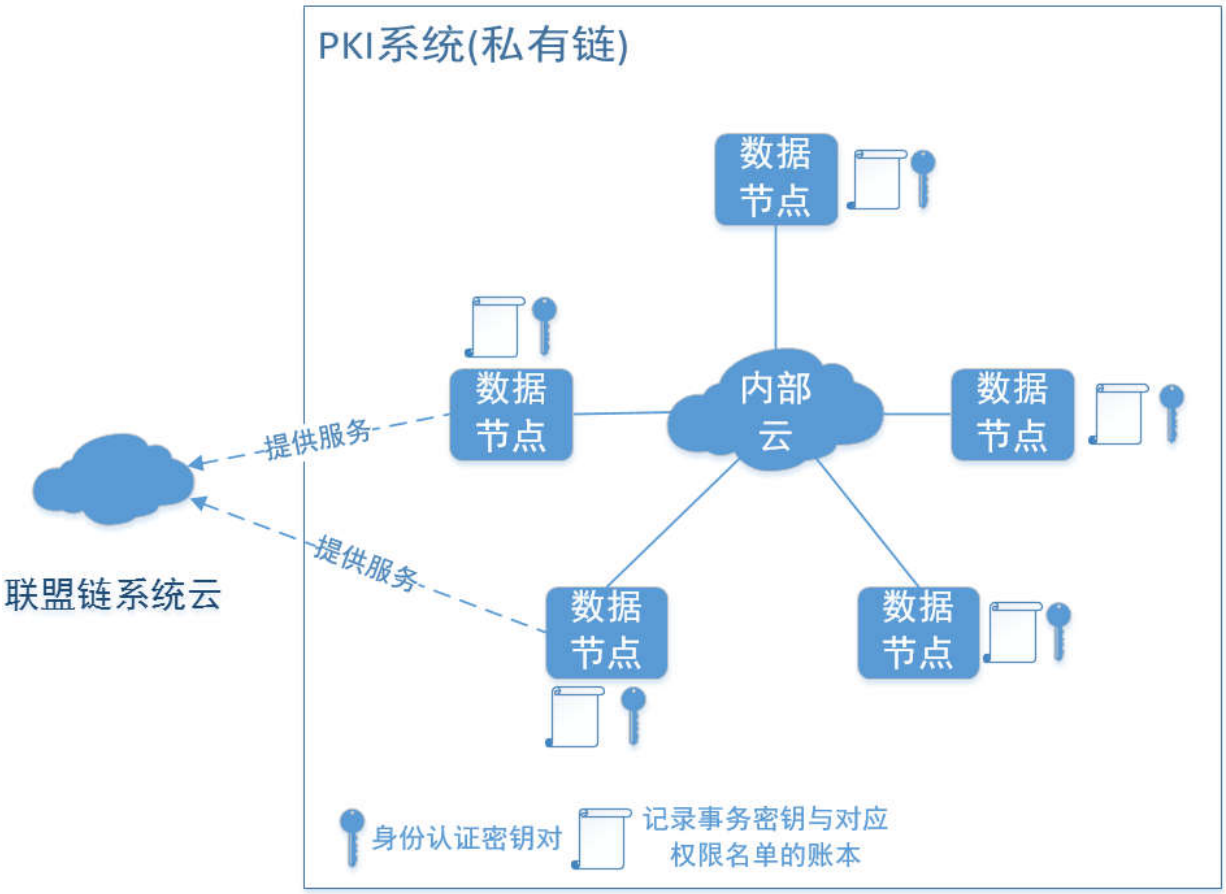

图 2-3 基于私有链的 PKI 系统架构图

如上图所示，PKI 系统中的私有链节点都分别拥有一个账本，用于记录事务密钥和事务对应的权限名单（所有账本内容相同）。其中部分节点作为 PKI 系统的服务代理，向联盟链系统提供服务。

基于私有链的 PKI 系统的具体功能与实现原理如下：

1. **节点认证功能**：当联盟链中节点需要获取其他节点的公钥时，PKI 系统则回溯私有链账本查找对应节点的数字证书，取出其公钥返回给请求节点。

2. **事务加密功能**：当联盟链中节点准备发布事务时，PKI 系统随机生成一对非对称密钥，使用密钥对中的私钥对事务进行加密，并临时记录密钥对的公钥和

该事务的权限名单（名单成员包括事务参与者和联盟链中的验证节点）。PKI 系统根据智能合约把加密后事务向联盟链广播，并在系统决议通过后，再把公钥和事务权限名单以及事务 ID 等信息正式写入 PKI 的私有链中。

3. **事务解密功能：**当联盟链中节点查询事务时，PKI 系统回溯私有链确认该节点是否在该事务的权限名单上，若在则向节点返回该事务的解密公钥。

基于私有链的 PKI 系统实现的难点在于如何把成熟的传统 PKI 系统与私有链结合。不过目前也有 CertCoin 等解决方案实现了 PKI 区块链。

三.业务场景详解

3.1 发布事务

发布事务的执行过程如下：

1. 联盟链节点 A 生成一个事务，用私钥对其签名，用节点 B 公钥加密消息后发往 B。

2. 节点 B 用私钥解密来自 A 的消息，用 A 的公钥验证了 A 的签名后，用 B 私钥对事务签名。准备发布事务。

3. 节点 B 调用权限控制层接口，把事务发送给 PKI 系统中某个被合约指定的代理服务节点。

4. PKI 私有链中代理服务节点收到来自联盟链中节点发送的事务后，随机生成一个密钥对，用私钥加密事务后返回给联盟链中某个随机验证节点 S，并在私有链中使用一个临时支链来临时记录该事务的 ID、公钥和权限名单（包括事务参与者和所有验证节点）等信息。

5. 验证节点收到 PKI 返回的加密事务后，把事务向其他验证节点广播。

6. 每当一个验证节点收到加密事务时，按照合约向 PKI 系统请求该事务的公钥，PKI 系统从私有链的分叉支链中读取权限名单验证后，取出公钥返回给验证节点。

7. 验证节点用公钥解密被加密事务，验证事务内容与参与者签名无误后确认通过。

8. 多个验证节点通过共识算法达成系统决议，通知联盟链所有节点写入该被加密事务。

9. 验证节点 S 根据合约通知 PKI 系统：该事务已被系统决议通过。

10. PKI 系统剪除私有链上该事务的临时支链，并把事务的 ID、公钥以及权限名单等信息正式写入 PKI 私有链的主链中。事务发布完成。

3.2 查询事务

查询事务的执行过程如下：

1. 节点 A 准备查询多个事务，调用权限控制层的查询事务接口。

2. PKI 系统中服务节点根据收到的来自 A 发送的批量事务 ID，回溯私有链进行查询。

3. 若这些事务的权限名单上均有节点 A，则取出这些事务的解密公钥返回给 A。

4. 节点 A 使用公钥对联盟链账本上对应的事务进行解密。事务查询完成。

四.架构优缺点分析

4.1 优点

1. 构建了权限控制中间层，使应用层与底层服务解耦，有利于提升安全性与开发效率。

2. 权限控制机制有效保证银行数据的安全性、隔离性以及可监管性。

3. PKI 系统通过私有链维护所有事务的密钥与权限名单，使数据难以被攻击或篡改。

4. PKI 系统与智能合约都已有较为成熟的架构实现，可行性高。

4.2 缺点

1. 当联盟链中验证节点数量过少时，系统的鲁棒性较差。

2. PKI 系统使用区块链维护数据，降低了查询性能。

3. 在提交事务过程中，需要至少两次区块链同步，因此联盟链或 PKI 的节点过多的情况下可能形成性能瓶颈。