**区块链技术在网络货运中**

**应用框架研究**

**负责人：** 陈志立

**研究人员：**庞雄韬、韦健、符捷、杨豪

**完成单位：**华东师范大学&中交智运

**提交日期：** 2022.03.01

**目 录**

[**1 总体框架 1**](#_Toc116311103)

[**2 网络货运应用框架 3**](#_Toc116311104)

[2.1 数据存证 3](#_Toc116311105)

[2.2 存证结构 5](#_Toc116311108)

[2.3 数据共享 6](#_Toc116311109)

[2.4 交易溯源 9](#_Toc116311113)

[2.5 结算清账 10](#_Toc116311114)

[2.6 货运方案总体应用框架设计 11](#_Toc116311115)

[**3 供应链金融应用框架 14**](#_Toc116311119)

[3.1 框架介绍 14](#_Toc116311120)

[3.2 系统框架 15](#_Toc116311121)

[3.3 监管及融资 16](#_Toc116311122)

[3.4 智信流转 17](#_Toc116311126)

[**4 Fabric系统架构设计 23**](#_Toc116311130)

[4.1 组织划分和管理 23](#_Toc116311131)

[4.2 Channel设计 25](#_Toc116311134)

[4.3 我司遗留系统的兼容 26](#_Toc116311135)

[**5 总结 29**](#_Toc116311136)

# 1 总体框架

“区块链+网络货运”平台总体框架主体包含两部分，分为四层结构，其中SCF(ServiceChain of Finance，供应链金融)与网络货运平台共同组成了整个应用框架的数据来源，二者基于多技术融合资源层构建，数据都存证于区块链层的联盟链上，同时接受基础业务层和扩展层提供的多项服务，保障了整个物流体系的交易双方身份认证，司机级别及企业级别的权限管理，网络货运平台内的关键三单(订单、运单、账单)的存证，SCF平台内基于应收账款所发行并流通的智信存证和流转，全物流体系内所需的智能合约逻辑正常执行等。

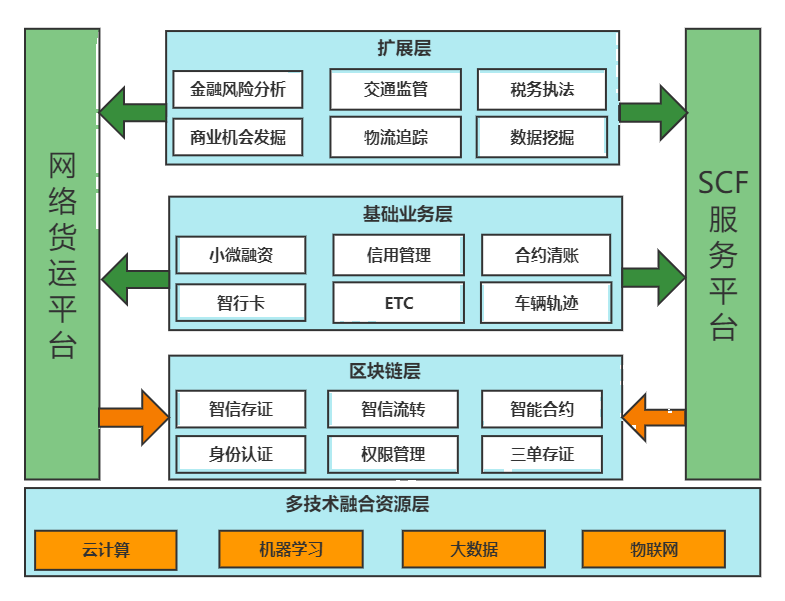


图1. 系统框架

平台总体分为四层：资源层，区块链层，基础业务层，扩展层。

资源层：多技术融合的资源层，包括计划应用云计算、机器学习、大数据、物联网等技术。其中，通过云计算将深度与区块链相融合，实现对区块链节点、框架、网络等虚拟化的表达，实现节点资源动态扩容、远程运维，最终实现了区块链系统的快速部署、快速运维和敏捷开发等；通过机器学习与区块链相融合，实现对区块链上存储物流数据、供应链金融数据价值的充分挖掘，为小微企业提供及时有效的融资服务和风险评估，为金融机构精准定位优质客户及企业，同时提供建设信用管理体系；基于大数据与区块链相融合，实现区块链的高性能可扩展性，实现业务所需的千万级吞吐量目标；通过物联网与区块链相融合，实现物流运输过程中的物品状况的全流程检测，为车辆轨迹获取，损坏运输物品定责提供证据数据支撑。

区块链层：区块链层包括身份认证，权限管理，三单存证，智信存证，智信流转和智能合约等功能。通过将区块链与网络货运相结合，由于区块链所具有的的去中心化、不可篡改的特性，有望解决在目前物流市场中所存在的多方不信任问题，同时，构建于区块链2.0的智能合约可以进一步实现交易的自动化，去除掉人工干扰等不信任因素，并大幅降低物流交易、对账清算的费用。

基础业务层：通过区块链层提供的智信流转数据和链上权限管理、身份认证等功能，可在基础业务层集成智行卡，ETC，车辆轨迹，小微融资，信用管理，合约清账等功能。

扩展层：扩展层将实现金融风险分析，交通监管，税务执法，商业机会发掘，物流追踪，数据挖掘等功能。其中，金融风险分析帮助银行系统在进行供应链融资过程中提供数据和分析支持，最大化降低融资风险，提高融资效率；商业机会发掘通过对链上数据的再利用，帮助银行系统发现更多优质的潜在客户；交通及税务监管部门，作为联盟链的共治节点之一，可有效利用链上数据实现交通监管和税务清算核对；物流信息实时同步更新到链上，货主和收货人可随时了解到货品的物流信息。

区块链将能够克服传统物流信任流程中的多方互信痛点问题并提高供应链流程的效率。通过区块链技术，将实现链上多方的数据共享，从而创建“统一账本”，此外，还将通过实现精简、自动化和图灵完备的智能合约来帮助节约物流成本。

# 2 网络货运应用框架

2.1 数据存证

### 2.1.1 存证内容

数据存证模块定义标准规范的数据格式、接口，实现供应链中各节点企业之间的物流信息上链存证，统一规范。通过对登记的交易方身份、运单、提货信息、货运线路、路检信息、验收等全流程关键信息上链存证，发挥区块链数据确权、数据保真、数据安全防护功能，提供信息完整性、时效性的保护和验证机制，增加防篡改、隐私保护和多种约束条件下的数据访问控制功能，并开发对应接口和服务追踪、溯源目标交易，防止数据泄露。链上数据主要包括如下类型：

1. 用户信息，供应链中各节点企业之间的关于物流管理运行的各种信息，例如：客户信息、销售数据、库存信息等等；
2. 货运物流过程各个环节的流转信息，如发车、配送、到货等信息，即整个供应链上的组织分享信息资源和进行反馈的过程；
3. 货运订单数据，包括：询价、报价、配送、妥投等环节，并生成基于区块链的电子运输结算凭证；
4. 传感器、定位数据，如承运过程中通过RFID、区块链传感器等物联网技术，确保物流配送过程数据收集的真实性，配合车载定位系统收集位置数据，及信息流和实物流一致性核验数据；
5. 交易清结算数据：包括计费规则、交易数量、订单、结算单、保险等数据；
6. 异常记录数据：包括系统异常预警、信用预警、订单异常、车辆异常等数据；
7. 日志记录数据：包括用户操作日志、系统日志等；
8. 其它数据：随着系统的升级，未来涉及更多的业务数据上链需求，比如仓单信息、水上运输、陆运、跨境运输及支付等需要上链的重要数据。

其中将货运业务中关键的表数据进行上链存储，货运信息表清单如下：

|  |  |  |
| --- | --- | --- |
| 序号 | 数据表 | 名称 |
| 1 | TMS\_ORDER | 订单表 |
| 2 | TMS\_ORDER\_GOODS | 订单货物信息表 |
| 3 | TMS\_WAYBILLS | 运单表 |
| 4 | TMS\_WAYBILLS\_GOODS | 运单货物信息表 |
| 5 | TMS\_CHARGES | 账单表 |

表1:货运订单信息表

### 2.1.2 存证方式

数据存储的设计目标是构建基于区块链的货运物流信息存证平台。如图2，数据从当前平台旁路导入，对当前平台的业务逻辑不造成冲击，同时保证数据的原子性和原始性。数据存储在区块链的存证保护之下，借助平行数据库保存，同时可与现有大数据平台结合，以节省资源。设计的存储数据的形式有服务器数据库，区块链以两类存储方式。以服务器数据库为主，在成功存储到数据库之后，从数据库利用主从复制技术将数据同步到区块链系统中。

服务器数据库存储数据的原始值，服务器数据库作为主要的数据存储渠道。服务器端通过HTTPPOST请求进行调用。区块链保存重要关键信息，如用户信息，订单信息，物流信息和其他核心数据。区块链中存储关键数据的Hash值，上链时使用设备指纹、时间戳与数据内容等进行封装，用SHA512生成对应的摘要，并利用密码学技术自动用上传设备的公钥对每条数据进行签名，第三方可用上传设备的公钥对签名进行验证。然后通过超级账本中的共识算法，使得大部分节点进行备份。

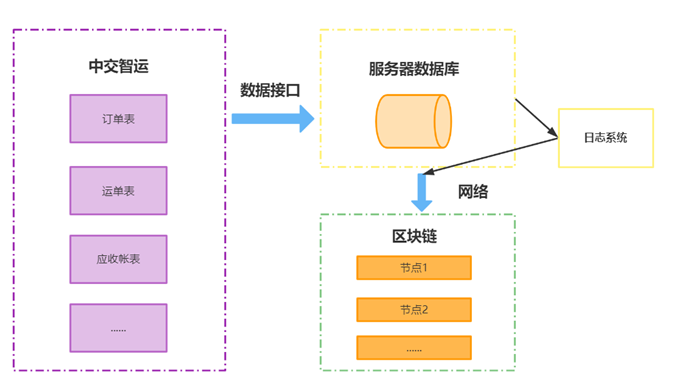


图2.数据上链存证

在区块链存证中，哈希(Hash)上链时，如果安全级别要求高可再进行加密。区块链技术可以在本地生成源文件证据的哈希值，并将其写入区块链某一区块中，而后一区块在新生成时，又会将前一区块的哈希值包含进去，以此类推。于是，作为源文件证据的哈希值就被永久保存在区块链链式数据库中。如果有人想要篡改数据，就必须要将这个区块的的数据以及后来所有区块的数据都进行修改，这是很难实现的，而且成本十分高昂。

2.2 存证结构

为了之后更好的进行各个订单数据字段的核验，我们设计Merkle树的存储结构来对”三单“的信息进行存储。Merkle树的叶子是数据块(例如，文件或者文件的集合)或者数据块的哈希值。如图3，非叶节点是其对应子节点哈希值串联字符串的哈希，最上层的根节点也由其叶子节点哈希值串联字符串的哈希构成。Merkle树的特点是底层任意数据的变化，都会传递到其父节点，最终传递到树的根节点。Merkle树主要用来进行完整性验证。基于此，我们把”三单“中的字段信息当成叶子结点，生成哈希形成Merkle树，具体如下图所示：

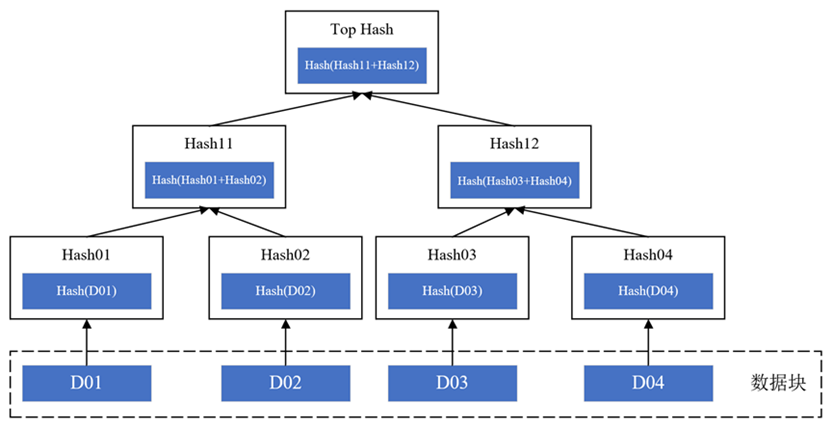


图3.数据存储结构

对于每个订单，我们使其成为一个区块，区块中包含该订单的Merkle根哈希，而Merkle根哈希由这个订单的字段对应的哈希组成，具体如图4：

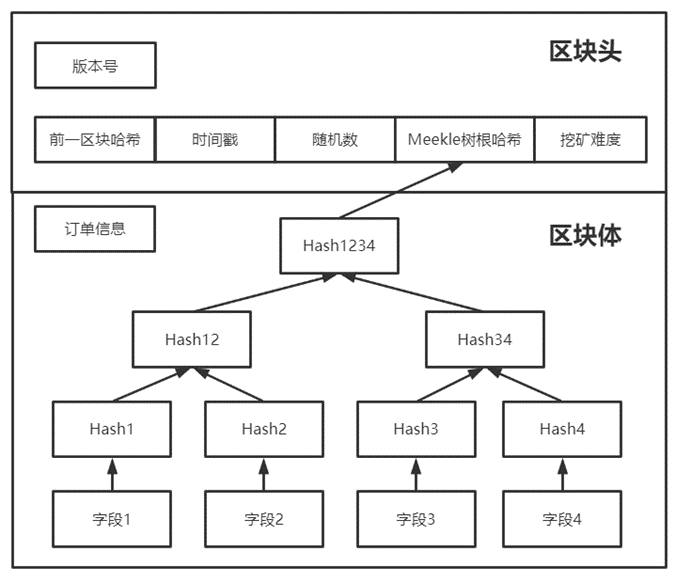


图4.区块结构

2.3 数据共享

### 2.3.1 P2P协议

本平台中区块链节点组成了一个P2P(peertopeer)的网络。网络中的每一个节点既能充当网络服务的请求者，又能响应其它节点的请求，提供网络资源和服务，以达到资源共享的目的。P2P网络自身有多方面优点，在区块链的应用如下:

1. 去中心化：区块链的资源和服务分布在所有参与节点上，通过共识机制维护区块链网络一致性，无须中心系统的存在;
2. 可扩展性：区块链节点可以自由加入、退出，网络系统根据节点自由扩展;
3. 健壮性：区块链网络没有中心节点，也就没有了攻击对象。参与节点分布在网络中，部分节点遭到破坏对区块链系统无影响;
4. 隐私保护：区块信息采用广播机制，无法定位广播初始节点，防止用户通信被监听，保护用户隐私;
5. 负载均衡：区块链通过限制节点连接数等配置，避免资源负载、网络阻塞。

通过区块链的P2P协议、自动同步机制、数据共识方法等实现各方数据实时同步。新进参与方能够方便的获得授权加入区块链平台。总的来说，区块链可以在保证物流交易和过程数据记入区块链后，对于整个参与区块链的实体都能透明的看到其中每个环节信息，且信息不会被人为的篡改。信息容易回溯到记入的每个交易点，且避免了单点数据损坏没有备份的威胁。区块链还能够实现对数据的确权，明确数据提供方管理方和使用方责任和权益，锁定数据源，为数据真实性提供保障。区块链技术给我们在交易管理上带来一个全新的思路，让我们扫除信息盲点，带来更多的交易信息细节价值。P2P网络中数据共享架构如图5：

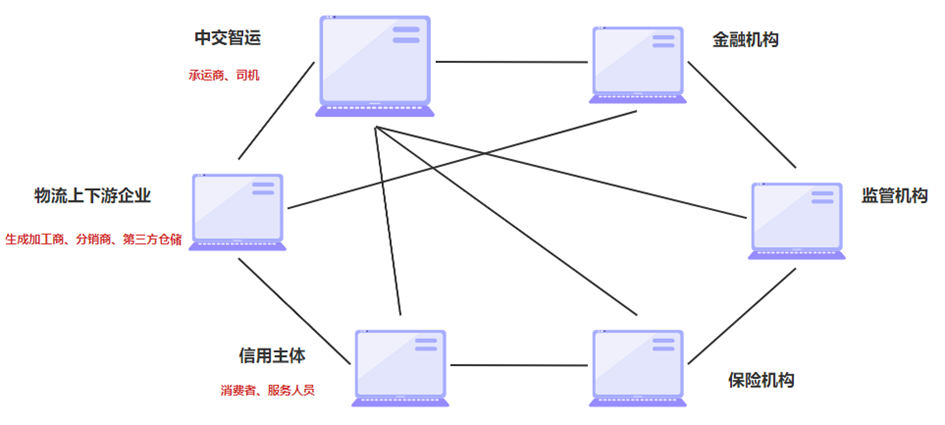


图5.货运物流区块链数据共享联盟节点

参与数据共享的单位如图所示，各方能够实时共享数据。获得授权的部门加入区块链平台简单便捷，通过服务界面注册认证后，申请一个节点服务器资源即可。系统将自动为加入的部门分配CA证书和密钥。

### 2.3.2 节点同步机制

采用节点同步机制可以使得参与数据的单位能够实时记录数据，可以在保证物流交易和过程数据记入区块链后，对于整个参与区块链的实体都能透明的看到其中每个环节信息，且信息不会被人为的篡改。信息容易回溯到记入的每个交易点，且避免了单点数据损坏没有备份的威胁。

采用Raft的节点同步机制，其是一种基于状态机负责的共识机制，为故障容错协议。Raft的核心由日志复制与领导者选举两部分构成，节点的状态将会根据不同的条件在领导者(Leader)、跟随者(Follower)、候选者(Candidate)之间变迁。系统在任意时刻只拥有一个领导者，并与所有跟随者之间维持周期性的心跳消息。当跟随者超时仍未收到领导者的心跳消息时，将会转变为候选者状态。候选者将会向其他节点发送投票请求消息，申请成为新的领导者，如果此候选者在超时前收到超过半数节点的确认消息，则转换为领导者。

在raft中，节点状态的详细变迁过程如图6，Leader选出后，就开始接收客户端的请求。Leader把请求作为日志条目(Logentries)加入到它的日志中，然后并行的向其他服务器发起AppendEntriesRPC复制日志条目。当这条日志被复制到大多数服务器上，Leader将这条日志应用到它的状态机并向客户端返回执行结果。

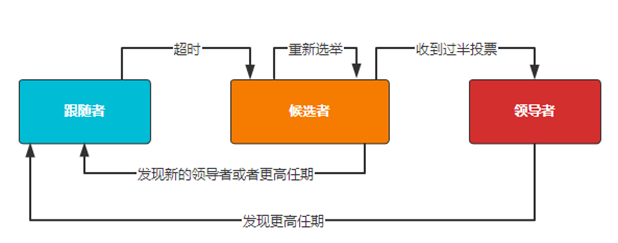


图6.raft节点状态变更

在物流货运场景中，图7所有的交易均由领导者打包生成区块并向所有的跟随者广播，在收到超过一半的跟随者回复后，领导者将会向所有节点发送确认信息，此时该区块将会被提交上链。Raft算法的通信复杂度为O(N)，共识效率较高，具有良好的扩展性。Raft算法在系统内不超过一半的节点宕机时仍能正常工作。

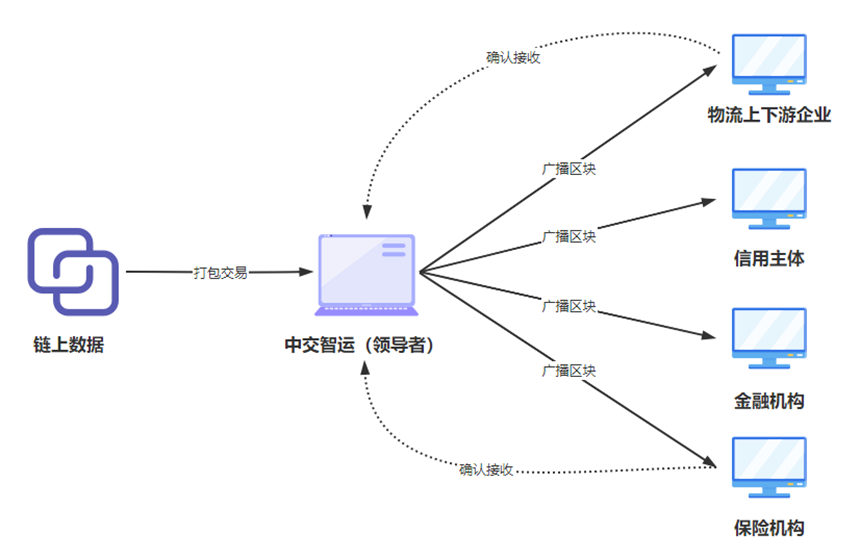


图7.raft交易广播

### 2.3.3 数据正确性验证方法

基于区块链的数据核验，设计两种数据核验的方式，基于区块链的数据核验，主要提供两种数据校验服务：

被动核验，即用户通过服务接口，调用数据核验功能，查询并验证自己所需的数据是否被篡改，区块链平台提供服务智能合约，从区块链账本数据库中调取所查验数据的哈希值，并计算所查验数据的哈希值作对比分析，数据一致则认为通过验证。

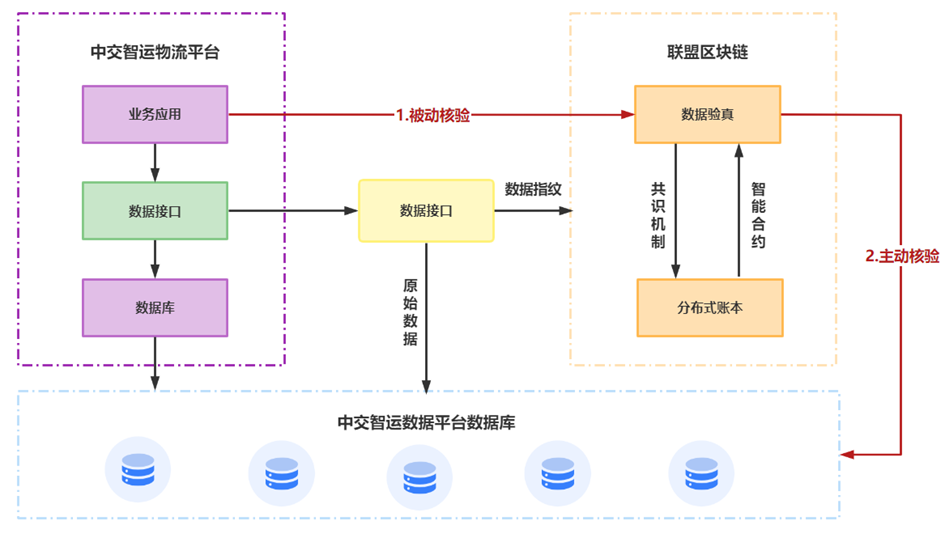


图8.数据验证流程

数据主动核验，即区块链平台在一定的时段(比如夜间业务数据处理压力较小的时段)，主动对当前物流平台的数据进行核验服务，数据核验通过计算待核验数据的Hash值，与从链上取得的待核验数据Hash进行对比，如果一致则通过核验。如果不同，则认为数据遭到篡改。

用户提交数据核验的请求，并向系统提交结构化或非结构化的待核验数据的Hash值，区块链调用数据验真服务模块，调用相应的智能合约，根据提交的指纹在分布式账本中定位查询，根据链上存储的可信Hash值进行对比验证，如果两者不相等，继续核验默克尔树的子节点，逐层往下，直到最后的叶子节点，即具体的篡改字段。将验证核实的结果返回给用户，并把验证结果通过共识机制上链记录。

2.4 交易溯源

交易在区块链中是通过Merkle树进行组织的，多个交易聚合成为一个Merkle根，随着交易数量的增多，区块链数据也在快速增加，在实际使用中，需要对存储数据的节点进行区分。区块链中的区块包含区块头和存放全部交易数据的区块体，对于需要存储全部数据以备查询的节点，称之为全节点。对于只存储区块头的节点，称之为轻节点，轻节点所需存储很小，只需要使用Merkle根完成hash验证即可。在交易验证时，以交易3为例，由轻节点持有交易3的hash向全节点发起查询请求，全节点提供由hash4、hash12组成的hash链，轻节点按照Merkle树构造规则计算得出Merkle根并于本地验证是否正确，验证路径如图9：

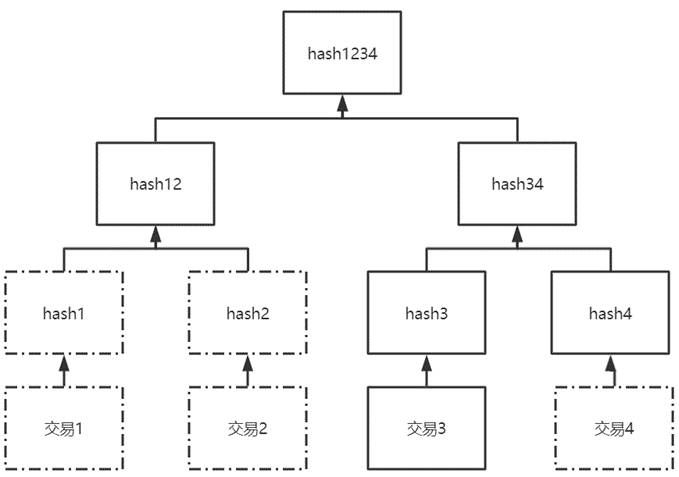


图9.交易验证路径

在网络货运中，一次交易涉及多单，每种单据类型根据交易复杂程度可扩展至多个，需要对交易数据建立数据库以满足更为复杂的查询需求。当有新交易发生时，全节点根据交易所属和交易类型建立键值数据库，并附加验证所需hash链。轻节点可使用单据hash向全节点发起查询请求，验证通过后便可向请求者提供对应密级的信息，数据库存储格式设计如图10：

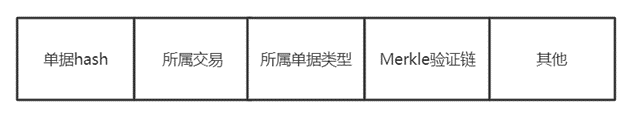


图10.数据库存储格式设计

2.5 结算清账

在交易过程中，某个单据在上传至区块链并确认后，还需要进行结算并完成状态变更。由于区块链的不可更改性，状态变更无法通过修改区块达到，通过额外数据库管理则破坏了区块链的安全性。对于需要进一步操作完成状态变更的单据，本节设计了一种方法用于管理单据的状态更新。

对于状态变更的交易，在交易数据后方增设状态变更来源，用于存放上次交易的hash值，重新上传至区块链，并增设当前状态字段，对于初次上传的单据，可以设置状态为待清账，对于结算完成后再次上传的单据，设置状态为已清账。修改后的交易存储格式为：



图11.修改后的交易存储格式

在交易验证过程中，轻节点持有交易hash向全节点发起查询请求，全节点从区块链最新区块向前遍历，得到的最新交易视为有效交易，并验证其状态,验证流程如下：

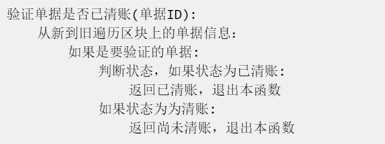


图12.交易有效性验证

在管理过程中，全节点构建单据数据库，在原先的基础上增加状态变更来源和当前状态选项，在未完成状态变更的单据上，状态选项改为待清账等字段。单据数据库的构建可以使全节点能够快速响应查询信息，避免网络堵塞。单据数据库的存储格式如下:

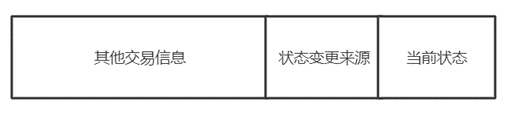


图13.单据存储格式

构建单据数据库的流程如下：

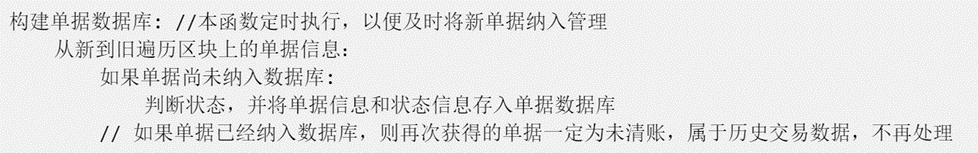


图14.构建单据流程

2.6 货运方案总体应用框架设计

### 2.6.1 主子链框架概述

基于本项目的实际需求，我们设计了一个专门用于本项目的主子链应用框架。实现了基于区块链主子链架构的跨链方法，包括在Fabric场景下，构建主子链架构。并构建专门用于跨链交易转发的跨链交易核验channel；若整个跨链流程中有任何一步出现异常或者是超时，则进行交易回滚；各个channel间通过编写的特定链码进行跨链交互以及验证。

主子链体系结构由单个主链和一组子链组成，用价值交换层连接子链和主链，以及子链之间的交互。与旨在创建具有全球交易账本的单一区块链的现有区块链架构相比，该架构允许一组区块链与另一组区块链并行运行，同时保持互操作性。主链采用成熟的共识算法机制，而子链可根据业务需求设置适合自己场景的共识算法，通过原子交换或跨链节点与主链形成双向锚定的方式，与其他子链进行跨链交易。这种主子链机制可帮助子链在满足每秒数千级别性能的前提下同时获得主链所提供的最终一致性保障。子链既可以是公链，也可以是联盟链，其链结构与主链类似，但因业务需求不同，可以采用不同的共识算法，达到数千的TPS性能，或者其他的定制开发功能。

图15展示了多链体系结构的层次结构。该体系结构的核心是主链，它管理着许多半独立的子链。主链的设计原则是用最小的数据量、计算资源和网络带宽来提供一个可信的主网络。主链保存来自子链的事务元数据，但为了提高性能，不会包含细节。

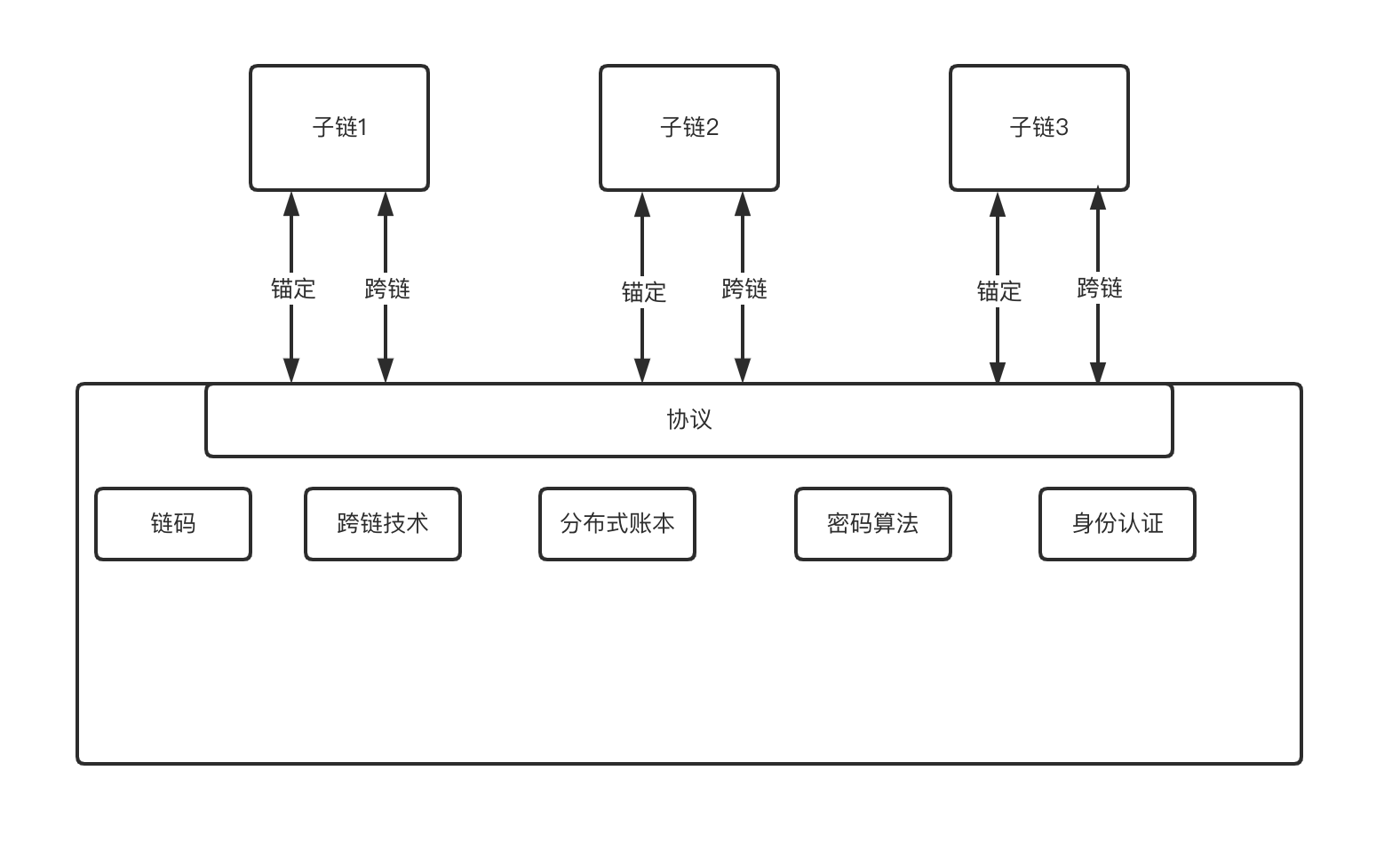


图15.多链体系结构

子链设置在某种程度上类似于数据库分片技术。一般来说，子链独立于主链运行，除了它的创建，然后它们被合并回主链。在合并子链信息后，将这些子链的最终结果提交给主链，以使主链保持最新。类似地，当创建子链时，相关信息会从主链镜像到相应的子链，以便子链跟上主链的状态。

### 2.6.2 交易核验流程

首先，我们需要根据场景的需求来构建一条专门用于跨链消息转发的中继Channel，称为Xchannel。中继Channel的背书方应该包括所有参与方。所有的背书方都有权对中继Channel中的消息进行验证，并根据交易概要，对消息进行转发，从而实现跨链的功能。在跨链交易的流程中，我们将跨链来源方的channel，称为Achannel，将跨链交易接受方的Channel，称为Bchannel。流程如下：

1. 当Achannel中发出跨链交易时，外部监测脚本将其交易转发，发送到Xchannel中。同时，Achannel上的链码将会生成跨链准备事件；Xchannel中的背书节点负责对跨链准备事件进行验证，当验证通过，Xchanne的节点负责向Bl的跨链核验组件发送跨链交易准备消息；
2. 当Bchannel上收到来自Xchannel背书节点的跨链准备消息时，则进行对应的跨链操作，并在Bchannel上生成跨链通证铸造事件；
3. 当Bchannel上生成跨链通证铸造事件后，Xchannel的背书节点负责对跨链通证铸造事件进行验证，验证成功后，由Xchannel的背书节点向Achannel发送铸造成功消息；
4. 若步骤3中出现异常或超时，Bchannel将会生成交易回滚事件，并回滚到步骤1；
5. Achannel接收来自Xchannel的背书节点发送的铸造成功消息后，会生成锁定成功事件，Xchannel的背书节点负责对跨链交易完成事件进行验证，验证成功后，由Xchannel的背书节点向Bchannel发送锁定成功消息；
6. 当Bchannel上的收到锁定成功消息后，将会解锁通证，并生成解锁事件；Xchannel的背书节点负责对解锁事件进行验证，验证成功后，跨链流程完成；

### 2.6.3 中继channel运行流程

在一般的跨链流程中，往往需要链下计算的组件帮助跨链消息进行转发。在本次设计中，我们采用了中继链方案进行转发。下面我们将描述中继链在本方案中的运行运行流程。Xchannel的运行过程如下：

1. Xchannel对主子链架构中的其他channel进行交易事件监听；
2. 当监听到跨链交易事件时，Xchannel的背书节点将会根据该跨链交易事件生成对应验证交易，将该验证交易根据其出现时间进行交易排序，放入自身交易池；
3. 根据Xchannel的共识算法流程，进行共识确认后，将验证交易进行确认上链。

# 3 供应链金融应用框架

3.1 框架介绍

本章针对物流交易在供应链全流程流转的业务特点，结合网络货运平台万亿规模的物流运单业务带来的供应链上下游紧密协同的业务关系建立Fabric联盟链。研究将供应链参与者在参与过程中所产生的全流程的业务数据记入不可篡改的区块链中，并与物联网、大数据、云计算等多种技术融合，利用先进的加密技术确保链上物流信息安全、准确、可靠。实现开发的信息验证、信息追溯、信息筛选等应用服务实用性、复用性。最后设计了供应链金融服务模块，并指导相应功能开发，解决物流供应链中的小微型企业融资难、融资慢的融资问题，有效降低金融风险，服务物流领域的小微企业。

中交智运供应链金融管理平台，是一个面向货主，运输企业，保险机构，税务部门，交通部门等多方的数据服务提供平台。通过将区块链与供应链金融管理平台相结合，打造可信，安全，高效的数据存储平台，解决中小型企业融资难，融资效率低的问题。具体来说，我司目前的业务流如下：货主下单；平台派单给承运商；承运商找司机送货；司机送货；货主确认订单完成；平台结算。整体流程持续时间相对较长，且由于资金流是由货主付款给平台，这中间会产生2-4个月的账期，但平台需要在每单确认1周内结算给承运企业，这就导致了平台将承担较大的垫资压力和金融风险。如果货主拖延货款，应收账款长期无法回收，将给平台资金周转带来巨大不利影响。此外，在应收账款账期中，大多数的承运商企业都会承担非常大的资金周转压力；当承运商企业遇到资金周转难题或者希望扩大规模时，承运商企业会向银行或第三方金融机构进行贷款，但由于大多的承运商企业是中小微企业，内部审查难度较大，风险系数较高，银行或第三方金融机构往往在对承运商企业贷款中加大难度，设置门槛，不予放贷。

本方案提出应用区块链技术保障链上的运输、订单、交易以及企业等信息真实有效，不被篡改，通过供应链金融平台的监管模块，可为交通税务部门提供信用凭证，查税核对等功能，减少供应链金融平台上信息的不透明性；通过建设供应链金融平台将企业用户和金融机构精准对接，实现快速借贷放贷，减少企业用户资金压力，帮助金融机构、平台方、用户方实现三赢。SCF服务平台将提供以下服务：

1. 提出了基于应收账款的“智信”链上流转全流程，降低企业融资门槛；
2. 实现了基于“智信”的可信存储，操作全流程由智能合约监管并上链存证，供实时调阅和溯源；
3. 提供交通部门和税务部门的可信监管服务，优化税务流程；
4. 智能合约固化资金清算路径，减少故意拖欠资金等违约行为的发生。

3.2 系统框架

如图15所示，基于区块链的SCF服务平台必须要和网络货运平台，银行系统进行交互。其中，SCF服务平台和网络货运平台的交互是单向的数据交互，即网络货运平台通过物流过程中产生的三单信息为SCF平台提供数据支持；SCF服务平台和银行系统的交易是双向的，包括银行系统通过对中交智运企业的信用评估进行SCF服务平台上的流通智信额度的授权，SCF服务平台通过大量的物流数据和链上金融服务数据向银行系统提供的信用管理功能和风险评估功能。

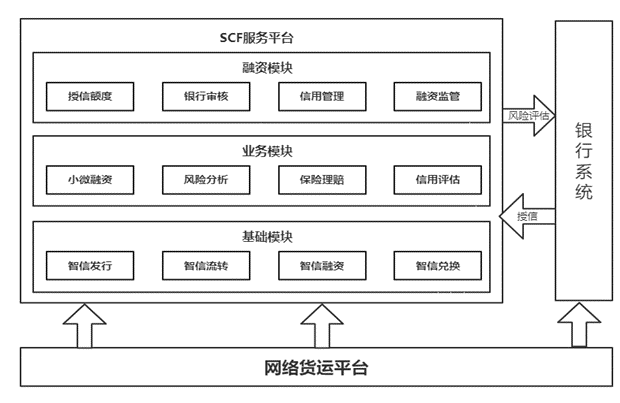


图16. 供应链金融系统框架

首先网络货运平台通过物流过程中产生的三单为SCF服务平台提供数据支持，包括货主端下单产生的订单，司机运输过程中的运单及最终收货人签收后所生成的账单。然后SCF服务平台基于网络货运平台中得到的数据进行有效信息提取，其中收货人签收后所生成的账单是关键信息，运单和订单为校验账单正确性的辅助信息，校验过程可以集成到SCF服务系统内由系统完成，也可通过中交智运中心服务平台系统外审核。最后，SCF服务平台基于上述有效信息——基于应收账款的合法账单生成SCF平台流通性电子票据——智信。智信是中交智运SCF服务平台中特有的一种继承了传统电子票据债权功能的Token，其可以基于ERC721合约标准设计成非同质化通用性Token。需要指出的是，上述Token只是SCF服务平台中应收账款的债权承载工具，其本身没有任何价值量体现。

3.3 监管及融资

### 3.3.1 组织结构

如图16所示，SCF服务平台监管及融资框架是SCF服务平台内可实现的应用框架之一，在该框架中，由中交智运作为联盟核心，与监管部门，银行系统共建SCF服务平台。可拓展地，也可加入其他与中交智运同水平的合作企业作为联盟链共建方之一。SCF平台建设好后，将由多方共同管理，包括平台准入管理，数据权限管理，联盟成员管理等。其中，平台在与银行对接时，需要在银行开通结算账户并提供运营资质证明等基础材料，与银行签订《银企合作协议》；平台在与监管部门对接时，需与监管部门确认数据所有及查询权限，并提供相应联盟链技术支持。

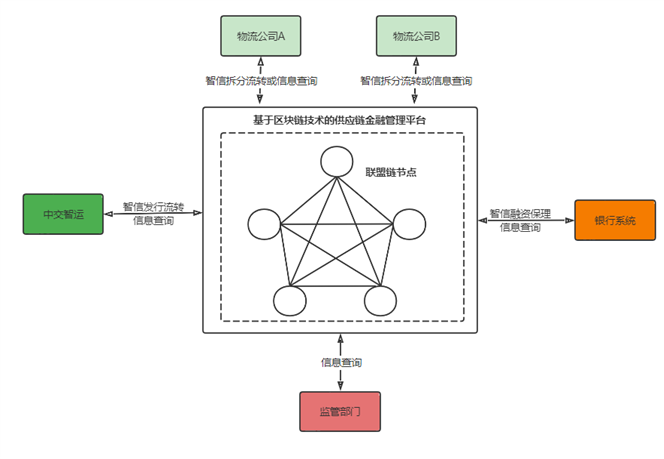


图17. 监管融资框架

### 3.3.2 交通监管

SCF服务平台将提供交通监管功能，主要包括为道路运输电子证照及交通运输行业信用评价应用服务提供有效保障，例如：

1. 开展基于区块链技术的网络货运平台研发，提供追踪运单信息服务，保证交易真实、可信、透明，有效保护物流交易各方的利益，同时能吸引更多货主、货运司机、物流企业、后市场服务商使用中交智运的服务，促进用户量、交易量提升，进而提升公司经济效益。
2. 开展基于区块链技术的信用系统研发，可获取更多外部机构的共识数据，构建基于多源数据更可信、严谨、全面的信用数据模型，提升信用评价服务群体画像准确度，对内支撑业务开展，对外为行业提供更具可信度的信用报告等数据服务产品，为行业创造更多价值。
3. 开展基于区块链技术的物流供应链应用服务，通过供应链上下游真实数据的监测与分析，可降低金融风险，把握物流交易参与的资金需求，精准助力金融授信、保理、担保等增值服务开展。
4. 开展基于区块链技术的道路运输电子证照服务，是发挥网络货运平台、信用系统、物流供应链价值的根基。完备的电子证照鉴权服务，保证了交易的真实、有效，降低服务风险，保证交易安全可靠。

### 3.3.3 小微融资

SCF服务平台将区块链的共识机制、存在性证明、不可篡改、可追溯等特性引入供应链金融，不需要第三方增信机构鉴定供应链上各种相关凭证的真实性，从而降低融资门槛、减少融资成本、缩短融资周期，为物流供应链中的小微企业提供快速方便的融资服务。具体的融资流程如下：

1. SCF服务平台获取到基于应收账款产生的有效账单数据后，为相应的应收账款企业发行智信；
2. 持信企业(智信的接收方)面临较大资金压力需要融资时，通过SCF服务平台向银行系统提出融资申请；
3. 银行系统对上述申请进行审核，审核通过后将申请发送到区块链网络上进行共识，当交易被打包后，交易确认，银行向申请企业放款；
4. 智信账单到期后，中交智运通过SCF服务平台上已部署的智能合约进行清账结算智信，核对智信账单无误后，将无误确认作为一笔交易发送到区块链网络上进行共识，当交易被打包后，交易确认，中交智运兑付当前所有智信，包括上述融资过程中银行所回收持有的智信。

3.4 智信流转

### 3.4.1 智信介绍

基于物流运费结算具有小额高频的特点，本节以核心企业在物流过程中产生的应付账款为依托，以数据库内的账单为元数据，由核心企业发行带有核心企业信用体现的智信，智信的字段如表2所示：

|  |  |  |
| --- | --- | --- |
| **字段** | **名称** | **数据类型** |
| PK | 主键 | varchar |
| ZX\_CODE | 编号 | varchar |
| ZX\_STATE | 状态 | varchar |
| ZX\_CURRENT\_OWNER | 当前所有者 | varchar |
| ZX\_ISSUER | 发行人 | varchar |
| ZX\_MNY | 金额 | numeric |
| ZX\_FROM\_PATH | 来源路径 | varchar |
| ZX\_ISSUE\_TIME | 发行日期 | timestamp |
| ZX\_MATURITY\_TIME | 到期日期 | timestamp |
| ZX\_RANDOM | 随机数 | varcahr |

表2. 智信字段

智信是一种链上基于ERC721合约标准的由链上核心企业发行的Token，ERC721又称为非同质化代币标准，基于该标准实现的Token具有独一无二的编号，可用来标的现实中的艺术品，投票权及本方案内物流场景中的电子票据，其目的是通过上述Token记录物流过程中产生的账单，用以替代传统的收据票据及电子票据。但与传统票据不同的是，智信只在链上流通，无实体，具有数字化特性，同时具有不可替代性，可看做承载债权功能的一种供应链金融工具。采用区块链技术，完整真实地记录智信的发行、流通、拆分和兑付过程。由于区块链上的数据经多方确认、不可篡改、不可抵赖、可以追溯，从而实现智信的可信存储，并且能够追溯至登记上链的初始智信，使核心企业的信用得以在平台上快速可信传递，使更多供应链上下游的供应商获得平等、高效、可信、低成本的普惠金融服务。智信基于实际发生的真实合同(本方案中体现为数据库内已产生的运费账单)，真实合同是由业务人员在我司网络货运平台中开具的还有应付运费金额的电子账单。智信的法律实质是应收账款债权，智信自开立后，具有以下功能：

1. 可流转，智信在多级流转的过程中，可作为支付工具,在线上实现对下游运输公司及多级运输公司的付款；
2. 可融资，运输公司可将智信转让给担保方,实现资金融通；
3. 可拆分，在实现流转、融资的过程中,可依据金额需要进行拆分，灵活使用；
4. 可兑付，核心企业到期兑付智信，实现运费到账。

### 3.4.2 流转过程

在处理智信时有两个重要的概念：状态和交易。状态是智信的存储对象，交易是推动智信状态转变的动作逻辑。在本项目中智信共3种状态，包括签发、流转、承兑；促进智信状态改变的交易共有5种，包括开立、出让、融资、拆分及到期兑换，下面介绍交易的具体流程及约束条件。

**1.开立** 如下图所示，核心企业开立智信时，首先需要由核心企业的经办向平台发起开立申请，经核心企业复核、下游运输企业经办审核、下游运输企业复核、平台接收开立叫阿姨，完成系统确权。交易及智信正式上链后，签发智信正式生效，下游运输公司获得上述所签发智信的债权。



图18.开立流程

**2.**出让 如下图所示，当持信企业希望流转智信时，需要由其经办提出流转请求，经其复核、下游接收企业经办审核、下游接受企业复核，平台审核并接收交易完成系统确权，方可生效。交易及智信正式上链后，出让智信正式生效，下游接收企业获得上述所出让智信的债权。

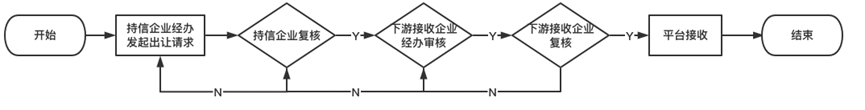


图19. 出让流程

**3.**融资 当小规模持信企业有供应链外采购或服务需求时，可能会面临较大资金压力。若此时直接向银行申贷融资，由于企业规模较小，可能会面临银行风险审批困难，融资流程复杂等各种问题。我们平台上的小规模持信企业可直接使用智信向授信担保人申请融资，智信是由担保人授信的，且其交易和状态的全程都在平台上，所以担保人可以避免复杂的手续，同时降低风控风险向请求企业融资。如下图所示，融资流程需要由持信企业经办提出融资请求，经其复核、担保方经办审核、担保方复核，平台接收交易完成智信确权。交易及智信正式上链后，融资智信正式生效，担保方获得上述所出让智信的债权。



图20. 融资流程

**4.**拆分 某些场景下，企业需使用持有智信同时对多个下游企业进行支付流转，因此需要对单个进行拆分交易，满足同时进行多企业支付的需求。但需要注意的是，基于ERC720产生的Token不支持可拆分，因此必须改造ERC721的拆分方案，具体方案在下一节进行讨论，此处我们先假设智信可拆分，如下图所示，拆分流程需要由持信企业经办提出拆分请求，经其复核、平台方审核、平台方方复核，平台接收交易完成智信确权。交易及拆分后的智信正式上链后，拆分智信正式生效，拆分交易接收方获得上述所出让智信的债权。

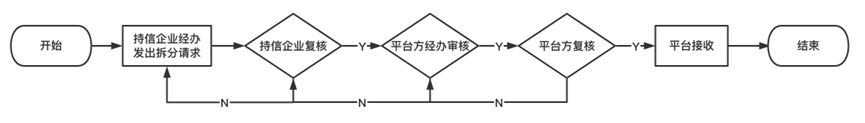


图21. 拆分流程

**5.**到期兑换 智信到期后，智能合约可自动根据当前链上存证的智信持有状态进行到期兑换，智能合约是由核心企业在开立智信前预输入参数部署完成的。如下图所示，到期兑换需要到期时间作为触发条件，由智能合约自动提出兑换请求，经持信企业复核、平台方经办审核、平台方方复核，平台接收交易完成智信的到期兑换操作，到期兑换后的智信会被注销。



图22. 到期兑换流程

### 3.4.3 拆分过程

现实世界中的物理凭证由于空间限制，一个很大的缺点就是其不可拆分性，但基于区块链的供应链金融平台所发行的智信可实现灵活拆分，例如面值为N的凭证，在总价值不变的前提下，可以根据持有者的意愿拆分成任意面值的智信碎片。考虑到供应链系统中的多级供应商，智信碎片将在多级供应商之间进行流转，因此智信的可拆分性是必要的，并且拆分需要具有良好的可扩展性。为了实现智信的灵活可拆分，我们在专利《一种基于区块链技术的电子票据拆分方法和装置》中设计了一种新的数据结构——树列，用于存储智信的流转过程，来解决智信的拆分存储问题。通过树列的引入，为智信提供了灵活可拆分的性质。例如面值为N的凭证，在总价值不变的前提下，可以根据持有者的意愿拆分成任意面值的智信碎片。。

首先，树列(TreeLink)是本方案创新提出的一种由列表和树复合成的数据结构，具体而言，树列是一组树的集合，特别地，树列将集合中所有树的根节点有序列地组织成一个有序列表。

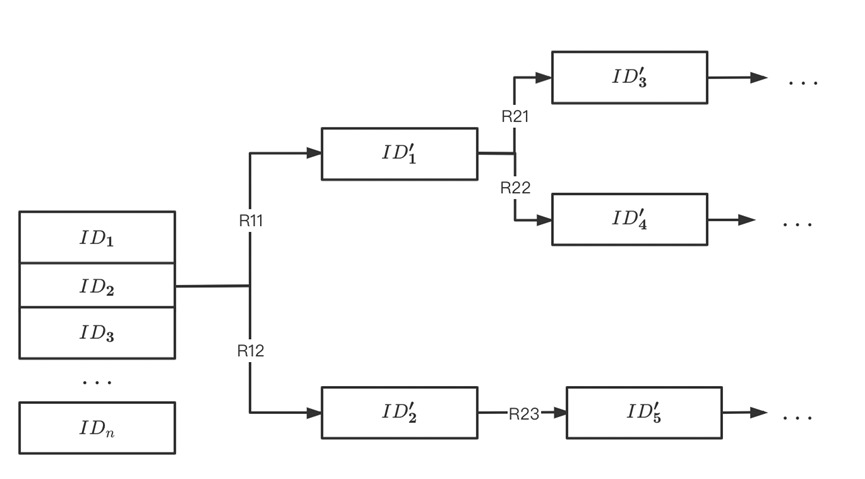


图23. TreeLink

如上图所示，每个智信的所有权使用一棵逻辑树来存储，逻辑树的根节点表示核心企业直接开立的智信，后面所有的子节点都表示来源于该智信所拆分产生的债权。同时，可使用非对称加密对子节点上的具体内容进行加密，实现隐私安全；在债权中引入128bit随机参数提高债权安全空间，防止债权的恶意篡改；利用数字签名对债权进行交易双方的交易确认。通过本方案中的拆分方式，可实现智信所有权的快速拆分、安全查验、高效溯源以及隐私保护。

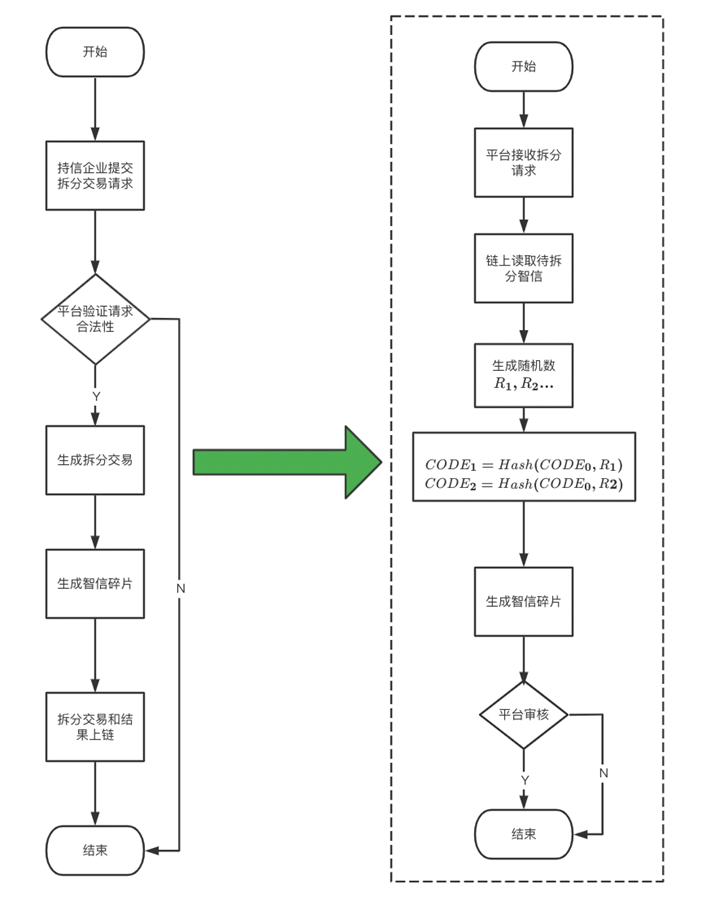


图24. 拆分流程

如上图所示，智信的拆分分为提交、验证、执行拆分、确认上链四个步骤。首先，持信企业产生拆分需求时，通过平台构造拆分交易，并向平台递交拆分交易请求。平台验证拆分请求合法性，包括拆分来源智信的存在性，拆分金额与来源智信金额是否相等，发起人签名是否与智信所有人一致，发起时间是否合法等。若平台验证请求合法，将根据拆分请求生成拆分交易；若不合法，则直接驳回拆分请求，同时可对多次提交恶意拆分请求的节点加入黑名单。拆分交易在拆分请求的基础上增加了与拆分数量相等的128bit随机数，加入随机数的目的一方面是为了唯一生成拆分后子智信碎片的编号，为后续智信碎片的溯源查证提供证据；另一方面，通过随机数增大了智信碎片编号的安全空间，为智信拆分提供了安全保障。

拆分交易提交到链上，由智能合约根据拆分交易中的需求自动进行智信拆分，并返回拆分结果。智能合约所执行的功能包括证发起人签名和拆分目标合法、根据原智信ID和随机数生成子智信的ID、作废原智信、生成子智信。拆分后的结果即时返回到平台，平台通知原智信的持有企业和拆分智信的新接受企业拆分结果，确认无误后进行交易打包，共识上链存证。

# 4 Fabric系统架构设计

4.1 组织划分和管理

组织是Fabric中非常重要的概念，所有Peer节点、用户账号都必须属于同一个组织。Fabric的组织可以对应现实中的一个公司、一个部门或者一个协会。在Fabric中，组织通常是具有承担数据信用责任的区块链系统参与方。在考虑应用Fabric作为业务框架时，第一步必须要理清当前业务系统中的组织关系，找出能够承担数据信用责任并且能够承担联盟链节点运营业务的参与者，并从中划分出Fabric的组织结构关系。组织成立以后，不仅物理层面上需要进行数据的验证和存储，而且还需要承担相应的数据安全责任，当然也同时享有部分的数据使用权和拥有权。第二步需要确定组织间的管理关系，Fabric是联盟链，这意味着链上的治理权限是具有范围性的，所以根据业务场景的需要，可选取中心集权式的管理方式或者联盟分散式的管理方式。下面以我司网络货运场景业务为例，进一步给出Fabric应用的具体意见。

### 4.1.1 确认组织

首先，在确认组织之前，我们必须明确参与者的责任，权利以及对等地位是否足以成为一个组织。这是非常重要的，因为联盟链的设计中，无论组织过多或过少都可能影响联盟链的性能和安全。目前，如何设置一个组织，Fabric中并未给出明确的指导意见，结合调研情况，我们认为如果某个参与者要想成为联盟链中的一个组织，应当具备以下条件：

* 是否对区块链中的数据具有有效性检查的权利；
* 是否具有独立发展下线成员的资格;
* 是否对系统的核心业务不可或缺；
* 是否必须参与联盟链的治理；

我们认为，具备上述条件的参与者有资格成为联盟链中的组织。参与者成为组织后，将会有自己的组织编号、域名、证书等信息。成为Fabric系统组织的参与者将有机会在联盟链策略允许的情况下参与到channel的治理中，同时可以维护自己的fabric-ca作为组织的身份认证系统，从而发展下线成员。

综上我们对网络货运场景下的组织划分参考意见如下：

|  |  |
| --- | --- |
| **组织名称** | **链上职能** |
| 中交智运 | 负责联盟链成员组织的加入审核，运力协调，系统维护 |
| 一级承运商A | 负责链上数据有效性验证，下级承运商的运力协调，系统维护 |
| 二级承运商B | 负责货运数据的全流程上链，物流状态更新 |
| 银行系统 | 负责链上数据有效性验证，提供金融支持 |
| 监管执法部门 | 负责链上数据审查及公证 |

表3. 组织划分

### 4.1.2 组织管理方式

组织确认后，需要进一步明确系统对组织的管理方式，组织管理中的核心问题是组织的加入方式。Fabric中的组织管理方式可从宏观上划分为联盟分布式和中心集权式，二者最本质的区别即在于组织的加入方式。对于联盟分布式，各组织共同对联盟链进行治理，任何组织的加入和退出都需要经过全体组织的审批，对应到链上即为全体组织的数字签名，换言之，当需要从链上删除某个组织时，需要经过全体组织的同意，包括被删除组织。这在实际应用中是一个很大的局限性，所以联盟分布式更适合应用于组织数量较少，各组织之间较为熟悉，且数量相对稳定的情况下。对于中心集权式，我司(中交智运)掌握联盟链的准入权限，任何组织的加入和退出都只经过我司的审批，但联盟链的治理是通过各组织共同完成的。这种管理方式的好处很明显，链上维护效率跟高，同时更有利于我司进行业务部署以及数据管理，缺点是削弱了联盟链的去中心化性。接下来分析我司在网络货运场景下所需应用的组织管理方式。

首先，网络货运中的组织数量和关系不是一成不变的，甚至由于物流场景的复杂性，往往牵扯到多级运输商，这将造成一方面组织数量将会比较庞大，另一方面组织可能会经常变动，稳定性较差。其次，物流过程中将会产生非常大的数据量，这在一定程度上无法设置过多组织，因为有些小型企业不具备运营一个组织的能力。最后，网络货运中产生的大量数据的使用权可归链上所有组织共有，但所有权需要进一步明确，我们认为，链上的数据所有权很大程度上取决于组织的管理方式。

综上所述，我们选定中心集权式的组织管理方式，在这种方式下，我司将成为Fabric中的一个中心组织，该中心组织统一管理区块链中的所有组织。管理的具体方式是：当组织申请加入联盟链时，我司向其颁发数字证书或给予中间CA，同时将其加入需要的通道中，获得对应通道中的数据使用权；当组织申请进行链上业务变动时，如创建新的Channel，加入其他Channel，必须通过我司的数字签名才可以发起相应链上业务；当组织需要退出联盟链时，我司收回其数字证书和销毁中间CA，然后在联盟链上删除该组织并整理遗留数据。

4.2 Channel设计

Fabric的数据存储结构被设计成多账本体系，每一个账本在Fabric中被称为Channel，加入Channel中的每个Peer节点都是对等的，也就是说同一个Channel中的所有Peer节点都保存一份相同的数据。但是Fabric目前并没有提供分布式存储的解决方案，这导致了加入了同一Channel的Peer节点服务器中都会存在存储相同的数据。这种存储数量在数据量非常大的时候会影响Peer节点读取数据的性能。基于Fabric的存储特性，在设计Fabric系统的时候需要对Channel存储方式进行相关的设计。Fabric对Channel存储方式进行设计的内容主要是：首先对Channel的大小进行评估，如果单个Channel的数据量或者数据的存储空间都非常大，那么可以将一个非常大的Channel拆分成若干个相对较小的Channel。

我们举一个例子来说明如何拆分Channel。假设在网络货运场景下，我们有这样一个Channel，该Channel中包含的数据可能超过10亿条，数据文件的大小可能超过500G。如果按照Fabric现有的设计方式，Channel和节点的分布如图24所示：

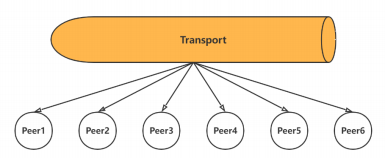


图25. 大Channel下的数据存储

根据图24所示，以后的Peer都需要存大约500G的数据，这显然对单个Peer节点造成了较大的压力。这时候我们可以采取对Channel进行分割，我们将每个Channel的数据限制在2000万条，经过分割之后的Channel结构如图25所示：

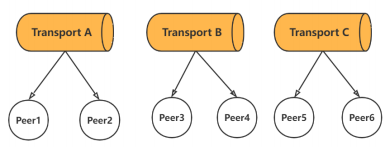


图26. Channel分割

如上图，经过分割之后的Channel体积缩小到原来的三分之一。对Channel进行分割的另一个好处就是，如果数据继续增长，我们只需要再增加一个新的Channel以及组织新开一个peer节点即可。但是，很明显上述方案并没办法应对数据无限增长的情况，更好的方案应该是对Channel中的数据进行归档处理，遗憾的是，Fabric目前并不支持数据的归档处理操作，所以，我们在技术调研方案中提出了我们的“大数据集下的联盟链高效数据归档”方案，希望能够进一步解决上述问题。

综上所述，下图是我们对于网络货运场景下的Fabric中的Channel设计：首先，我们在初期Channel的时期并未考虑Channel将存储的不同业务的业务量，所以此处仅根据业务的不同对Channel进行划分，但如上所述，对大数据量的Channel进行改造是很容易实现的，只需要对原Channel进行分割或新增新的Channel即可。其次，在该设计中未考虑银行和监管部门的数据需求范围，我们默认银行系统和监管部门将加入所有Channel实行监管审查。

|  |  |  |
| --- | --- | --- |
|  | **通道名称** | **存放数据** |
| 1 | Order | 订单表 |
| 2 | Bill | 账单表 |
| 3 | WayBill | 运单表 |
| 4 | Member | 组织信息 |

表4. 通道划分

4.3 我司遗留系统的兼容

我司在采用Fabric架构的系统时，可能会遇到系统兼容的问题，例如需要将现有的网络货运系统和Fabric系统对接。在Fabric系统之前我司已经有了一个基于传统技术加购的系统，且该系统已经运行了一段时间并且已经积累了大量的数据，现在提高物流供应链的效率准备将所有的历史货运数据存放到区块链中，并且在系统改造完成之后，新产生的货运数据也需要存放到区块链中。在这种需求下，最核心的问题就是历史遗留系统和Fabric的结合。针对这样的业务需求，我们建议首先从账号同步和数据融合这两个方面来进行考虑。

首先是业务系统的历史账号和Fabric账号的同步，这个问题可以从账号是否会继续增加和现有账号数量两个纬度来进行考虑：

**1.**历史遗留系统中账号体系中的账号是固定不变的在这种情况下如果账号的数量比较少，可以通过Fabric的cryptogen模块生成相应数量的账号信息，然后将生成的账号文件和历史遗留系统的账号进行绑定。如果账号的数量比较多，那么可以借助Fabric-ca-server来对这些账号进行管理，通过Fabric-ca-server提供的RESTAPI接口可以将历史遗留系统的账号导入到Fabric-ca-server中。在

调用Fabric-ca-server提供的RESTAPI导入历史数据时，每次调用成功都会返回当前创建账号的证书等信息，通过这些信息可以完成与历史遗留系统账号体系的绑定。

**2.**历史遗留系统的账号会持续增加如果是这种情况，那么只能采取Fabric-ca-server来管理账号，通过Fabric-ca-server提供的RESTAPI接口将历史遗留系统的现有账号导入到Fabric-ca-server中完成绑定。对于新增的账号，每次创建账号之后，调用Fabric-ca-server的接口生成新的账号并完成绑定。

其次是业务系统历史遗留数据和Fabric的融合，关于历史遗留系统的已有数据如何保存到区块链中是一个比较麻烦的问题。在处理这个问题的时候会有一个矛盾。由于历史遗留数据是发生在过去的，但是区块链中每条交易会在系统级别记录一条数据的时间戳。这个时间是客户端无法修改的并将永久保存。这个实践如果进行数据初始化就会发生数据存储时间不一致的问题，即历史数据的系统时间戳和业务时间戳不一致。这可能会导致数据的有效性受到质疑。这个时候区块链技术已经无法解决这个问题了，只有联盟链的所有参与方达成共识，统一接受这样的事实才可以。针对这种问题我们推荐两种解决方案供大家参考，这两种方案分别是：时间截取法和Channel截取法。

•时间截取法时间截取法是通过设定某个特定的时间点，在该时间点之前的数据为历史数据,时间点之后的数据为新数据。当系统中需要用数据的时间戳的时候，对于时间节点之前的数据为新数据。当系统种需要用数据的时间戳的时候，对于时间节点之前的数据以存在交易记录中的历史时间为准，对于时间点之后的数据以系统时间戳为准。

•Channel截取法在使用Channel截取法的时候，将历史数据存储在特定的通道中。当需要使用历史数据的时候从特定的通道中获取相关的数据，如果需要使用新产生的数据则从新创建的Channel中获取数据。

上述两种方法都需要在历史数据保存到区块链中的时候将历史数据中的时间戳一并保存到区块链中。

# 5 总结

区块链技术应用于网络货运的关键在于如何结合区块链的优势，同时克服区块链吞吐量不高和可扩展性弱的缺陷，深度落地于网络货运场景。本方案针对网络货运需求，提出基于HyperledgerFabric的联盟链构建中交智运网络货运平台和SCF服务平台，研究网络货运物流中和供应链金融中区块链的应用场景，具体而言，主要研究了以下方面内容，并提出了应用框架：

以Fabric联盟链为基础，研究网络货运中实际可落地场景，包括但不限于：

* 货运信息的存证。包括交易方身份、电子运单、提货信息、货运路线、路检信息、验收等全流程关键信息。
* 多方数据共享。通过P2P网络、节点同步机制及共识算法等实现数据实时同步，且各参与方都存在完整账本。
* 交易溯源。货运全程交易信息上链，并开发对应接口和服务追踪、溯源目标交易，使网络货运平台生态真实、可信、透明。

结合网络货运区块链平台提供的海量可信数据，构建供应链金融服务平台，包括但不限于：

* + 微融资。针对物流供应链中的小微企业由于账期问题造成资金困难，提出了链上Token“智信”取代传统账单，降低了小微企业的融资门槛，简化了融资流程。
  + 交通及税务监管。针对物流供应链中的流程复杂性以及存在的不透明性，引入了监管部门作为联盟组织实现穿透式监管，保证联盟链治理的合规性与可信性。

基于以上应用框架，区块链物流将利用运单各阶段信息实时加密签名登记上链，辅以第三方签名佐证，不可抵赖，无法篡改；保证各交易主体的信息安全和隐私的同时完成了物流资金流数据流三流合一的数据交叉验证；SCF服务平台在银行系统的授权下，发行智信在链上流转，给予供应链内的小微企业提供普惠金融服务。