沙师弟区块链概要设计方案

[1. 背景及必要性 3](#_Toc514531341)

[2. 建设目标 3](#_Toc514531342)

[3. 业务流程分析 4](#_Toc514531343)

[3.1. 角色定义 4](#_Toc514531344)

[3.2. 业务流程说明 4](#_Toc514531345)

[3.2.1. 主流程 4](#_Toc514531346)

[3.2.2. 发票流程 5](#_Toc514531347)

[3.2.3. 保险流程 5](#_Toc514531348)

[3.2.4. 账户流程 6](#_Toc514531349)

[3.3. 业务模块说明 7](#_Toc514531350)

[3.4. 数据类型说明 7](#_Toc514531351)

[3.4.1. 货源信息数据 7](#_Toc514531352)

[4. 模块设计 8](#_Toc514531353)

[4.1. 货主与司机信息管理模块 8](#_Toc514531354)

[4.2. 货源信息管理模块 11](#_Toc514531355)

[4.3. 货运订单管理模块 13](#_Toc514531356)

[4.4. 物流信息管理模块 16](#_Toc514531357)

[4.5. 发票业务模块 17](#_Toc514531358)

[4.6. 账户业务模块 18](#_Toc514531359)

[4.7. 保险业务模块 21](#_Toc514531360)

[5. 部署方案 23](#_Toc514531361)

[6. 环境需求 24](#_Toc514531362)

[7. 计划进度 24](#_Toc514531363)

[8. 问题沟通 25](#_Toc514531364)

# 背景及必要性

随着区块链技术的日益成熟，其去中心化及不可篡改等特性使得其公信力度更加可靠，在为企业节约成本的同时，更能使工作效率得到跨越式的提升。

沙师弟（重庆）网络科技有限公司作为国内知名的货运企业，如在其货运系统中引入区块链技术，可使其在同行业竞争中更具竞争力及可信度，为企业的良好发展奠定坚实的基础。长期以来，“小、散、乱”一直是货运物流行业的标签，也成为被社会所诟病的焦点，并将其视为导致行业经营不规范、服务质量不高、总成本居高不下的重要原因。对于“小、散”的道路货运市场而言，诚信体系是确保市场机制发挥作用的重要基础，而诚信体系缺失也成为我国物流行业乱象众多的重要原因。互联网的发展将使得行业的各类信息更加易获取、更加透明化、更加具有商业价值，从而为我们客观利用这些大数据对物流企业进行诚信评判提供了现实条件。

货运物流市场交易中，区块链技术可以贯穿于物流市场交易的全链条环节，由于没有中介机构的存在，所有东西都通过预先设定的程序自动运行，这样不仅能够大大降低成本，还能提高效率。而由于每个交易主体都有相同的账本，能确保账本记录过程公开透明。采用区块链技术互联并分布式记账，每个司机的行车记录都记录到统一账本，根据真实可靠不可篡改的详细运单记录信息，用户支付的资金可以直接付给承运人或司机账户，替代中心化的结算中心，降低现有清算中心负担，提升运营效率，降低运营成本。区块链技术的使用为物流市场尤其是零担货运市场提供了以更低成本和更高效率，实现分散经营主体集约整合的手段。

# 建设目标

本项目建设目标是将沙师弟货运物流信息平台与航天信息区块链基础平台进行融合，打造一个“区块链货运物流平台”。

“区块链货运物流平台”降低用户间信任风险，提高交易结算效率，降低业务运营成本，加强账本数据安全性，营造一个可信的数据环境。又为后续业务扩展提供方便的接入方法。

增加物流交易各环节的诚信度，还原物流场景真实性，做到部分环节的溯源,实现基于区块链技术的物流链路查询。为保险和物流交易纠纷提供真实依据。建立真实可信交易流水，为物流金融产品提供可靠数据。形成联盟链的基础构架，让更多物流方参与进来。

# 业务流程分析

## 角色定义

货主：货运物流服务的需求方。

司机：货运物流服务的提供方。

沙师弟：互联网物流信息整合平台。

保险公司：为司机和货主的货物提供保险服务。

合作单位：与“沙师弟”作用类似的参与方。

开票方：具有开具电子发票权利的参与方。

## 业务流程说明

区块链应用业务流程包括以下几个流程：主流程、发票流程、保险流程、账户流程。

### 主流程

主要涵盖了货源发布、订单记录及维护等主要业务流程，保证交易全流程连贯执行。



### 发票流程

将电子发票信息记录在链，用来保证发票与订单信息一致性，杜绝虚开、假开等操作，提高行业规范，为税务部门提供监管手段与依据。



### 保险流程

将保险信息记录在链，用来保证保险与订单信息一致性，与保险公司打通信息孤岛，提高用户购买保险的可信度，为保险公司提供真实可信的数据源。



### 账户流程

账户流程主要处理货主、司机资金来往，如货主支付运费到平台，平台划拨运费给司机等。营造可信的资金交易环境，提高货主、司机对账户信息的可信度，同时规避平台内部使用传统数据库带来的管理及技术风险。

如货主支付运费X元到平台后，货主账户增加冻结资金X元，交易完成后，货主账户冻结资金支付给司机账户Y元，司机体现申请通过后，司机账户提取Z元。如交易失败，货主账户冻结资金解冻，可申请体现。所有账户操作只能通过智能合约执行，变化情况记录在链可追溯，从而建立可信的账户操作环境。



## 业务模块说明

上述业务流程中将会设计到一个或多个业务模块，每个业务模块由多个相关功能组成，具体说明在下节详细说明。

业务模块包括货主与司机信息管理模块、货源信息管理模块、货运订单管理模块、物流位置信息管理模块、账户业务模块、保险业务模块、发票业务模块等。

## 数据类型说明

链上有多种数据类型，需要与应用系统交互，主要包括：货主信息数据、司机信息数据、货源信息数据、订单信息数据、物流位置信息数据、账户信息数据、保险信息数据、发票信息数据等。

其中每项信息需要与应用系统数据结构对应，目前先描述货源信息数据，其他数据待下期版本根据业务系统数据结构进行设计。

### 货源信息数据

{

发货位置信息；

收货位置信息；

发货时间；

发货人信息；

收货人信息；

货物名称；

货物类型；

货物属性（体积、重量）；

货物信息（图片、文字描述）；

货物价格信息（价格、支付方式、运费信息等）

车辆需求；

其他需求（发票、保险）；

时间限制；

}

# 模块设计

## 货主与司机信息管理模块

a. 司机信息写入接口

|  |  |
| --- | --- |
| 名称 | 司机信息写入接口 |
| 输入 | 司机信息（接口设计时考虑什么字段是K值，与司机证书关联） |
| 输出 | 成功响应 |
| 业务逻辑 | 判断是否已有该记录，如果有，返回错误；判断信息是否符合链码规定格式，如果不符合，返回错误；记录司机信息在链 |
| 调用方 | 沙师弟平台、合作单位  司机通过实名认证后，将司机信息记录在区块链 |
| 隐私保护 | 关键实名信息保护？只能经过授权后获取？ |

b. 货主信息写入接口

|  |  |
| --- | --- |
| 名称 | 货主信息写入接口 |
| 输入 | 货主信息 |
| 输出 | 成功响应 |
| 业务逻辑 | 判断是否已有该记录，如果有，返回错误；判断信息是否符合链码规定格式，如果不符合，返回错误；记录司机信息在链 |
| 调用方 | 沙师弟、合作单位  货主通过实名认证后，将货主注册信息记录在区块链 |
| 隐私保护 | 关键实名信息保护？只能经过授权后获取？ |

c. 司机信息查询接口

|  |  |
| --- | --- |
| 名称 | 司机信息查询接口 |
| 输入 | 司机id |
| 输出 | 司机信息详情 |
| 业务逻辑 | 智能合约进行权限判断， 是否能进行该操作；通过司机id，在区块链上查询司机信息详情；存在该司机信息，返回信息，否则返回失败。 |
| 调用方 | 沙师弟平台、司机、货主、保险、合作单位  在需要验证司机信息时调用，如保险公司取证 |
| 隐私保护 | 关键实名信息保护？只能经过授权后获取？ |

d. 货主信息查询接口

|  |  |
| --- | --- |
| 名称 | 货主信息查询接口 |
| 输入 | 货主id |
| 输出 | 货主信息详情 |
| 业务逻辑 | 智能合约进行权限判断， 是否能进行该操作；通过货主id，在区块链上查询货主信息详情；存在该货主信息，返回信息，否则返回失败。 |
| 调用方 | 沙师弟平台、货主、司机、保险、合作单位  在需要验证司机信息时调用，如保险公司取证 |
| 隐私保护 | 关键实名信息保护？只能经过授权后获取？ |

e. 司机信息更新接口

|  |  |
| --- | --- |
| 名称 | 司机信息更新接口 |
| 输入 | 司机id、更新项内容 |
| 输出 | 成功响应 |
| 业务逻辑 | 智能合约进行权限判断， 是否能进行该操作；判断是否已有该记录，如果没有，返回错误；判断信息是否符合链码规定格式，如果不符合，返回错误；更新司机信息在链 |
| 调用方 | 沙师弟平台、合作单位  司机实名信息发生变化 |
| 隐私保护 | 无 |

f. 货主信息更新接口

|  |  |
| --- | --- |
| 名称 | 货主信息更新接口 |
| 输入 | 货主id、更新项内容 |
| 输出 | 成功响应 |
| 业务逻辑 | 智能合约进行权限判断， 是否能进行该操作；判断是否已有该记录，如果没有，返回错误；判断信息是否符合链码规定格式，如果不符合，返回错误；更新货主信息在链 |
| 调用方 | 沙师弟平台、合作单位  货主实名信息发生变化 |
| 隐私保护 | 无 |

g. 司机信息追溯接口

|  |  |
| --- | --- |
| 名称 | 司机信息追溯接口 |
| 输入 | 司机id |
| 输出 | 司机信息历史变化记录 |
| 业务逻辑 | 智能合约进行权限判断， 是否能进行该操作；判断是否已有该记录，如果没有，返回错误；返回司机信息历史变化记录及提交人 |
| 调用方 | 监管方  核实司机信息变化痕迹时调用 |
| 隐私保护 | 无 |

h. 货主信息追溯接口

|  |  |
| --- | --- |
| 名称 | 货主信息追溯接口 |
| 输入 | 货主id |
| 输出 | 货主信息历史变化记录 |
| 业务逻辑 | 智能合约进行权限判断， 是否能进行该操作；判断是否已有该记录，如果没有，返回错误；返回货主信息历史变化记录及提交人 |
| 调用方 | 监管方  核实货主信息变化痕迹时调用 |
| 隐私保护 | 无 |

## 货源信息管理模块

a. 货物信息写入接口

|  |  |
| --- | --- |
| 名称 | 货源信息写入接口 |
| 输入 | 货源信息 |
| 输出 | 成功响应 |
| 业务逻辑 | 判断是否已有该货源记录，如果已有，返回错误；智能合约判断货源与写入者是否匹配；判断货源信息格式是否匹配，进行限制判断；将货源信息记录在链 |
| 调用方 | 沙师弟平台、货主、合作单位  Case A：货物信息先登记到沙师弟平台，再由沙师弟平台写入区块链；  Case B：货物由货主直接写入区块链，沙师弟平台可从区块链同步货物数据； |
| 隐私保护 | 货源信息是所有联盟链成员都能看到？目前应该大货司机通过沙师弟平台可获得所有货源信息，是否不需要隐私保护 |

b. 货源信息查询接口

|  |  |
| --- | --- |
| 名称 | 货源信息查询接口 |
| 输入 | 货源id |
| 输出 | 货源信息 |
| 业务逻辑 | 任何人都可以访问货源信息？  判断链上是否存在该货源，不存在返回失败，存在返回货源信息。 |
| 调用方 | 沙师弟平台、司机、货主、保险、合作单位  查看或验证货源信息时调用，如司机查看货源详细信息、货主查看已发布货源 |
| 隐私保护 | 货源信息是所有联盟链成员都能看到？目前应该大货司机通过沙师弟平台可获得所有货源信息，是否不需要隐私保护 |

c. 货源信息更新接口

|  |  |
| --- | --- |
| 名称 | 货源信息更新接口 |
| 输入 | 货物id、货源信息 |
| 输出 | 响应成功 |
| 业务逻辑 | 判断是否已有该货源记录，如果没有，返回错误；智能合约判断货源与更新者是否匹配；判断货源信息格式是否匹配，进行限制判断；将货源信息记录在链 |
| 调用方 | 沙师弟平台、货主、合作单位  Case A：货物信息先登记到沙师弟平台，再由沙师弟平台写入区块链；  Case B：货物由货主直接写入区块链，沙师弟平台可从区块链同步货物数据； |
| 隐私保护 | 货源信息是所有联盟链成员都能看到？目前应该大货司机通过沙师弟平台可获得所有货源信息，是否不需要隐私保护 |

d. 货源信息更新历史查询接口

|  |  |
| --- | --- |
| 名称 | 货物信息更新历史查询接口 |
| 输入 | 货物id |
| 输出 | 对应的货物历史更新记录 |
| 业务逻辑 | 智能合约进行权限判断， 是否能进行该操作；判断是否已有该记录，如果没有，返回错误；返回货源信息历史变化记录及提交人。 |
| 调用方 | 司机、货主、保险  在需要验证货源信息时调用，如对货源信息真实性质疑 |
| 隐私保护 | 无 |

## 货运订单管理模块

a. 订单数据写入接口

|  |  |
| --- | --- |
| 名称 | 订单数据写入接口 |
| 输入 | 订单数据、货主公钥 |
| 输出 | 成功响应 |
| 业务逻辑 | 智能合约进行权限判断， 是否能进行该操作；判断该订单是否在链上已存在，已存在返回错误；调用账务业务模块，设置货主账户该订单支付金额X元，冻结状态；若用户已购买保险，调用保险业务模块，写入该订单保险信息；生成回执码，并使用货主公钥加密；将订单信息、支付记录、提取码、回执码HASH值记录在链，设置订单状态为待发货。回执 |
| 调用方 | 沙师弟平台、合作单位  平台撮合交易完成，货主支付运费给平台后，由平台将订单信息写入进链 |
| 隐私保护 | 订单信息关键数据只能沙师弟、货主、大货司机查看？开具发票或保险公司查看经授权后方可查看？  交易双方信息是否需要保护？ |

b. 订单数据查询接口

|  |  |
| --- | --- |
| 名称 | 订单数据查询接口 |
| 输入 | 订单id |
| 输出 | 加密后的订单数据 |
| 业务逻辑 | 智能合约进行权限判断， 是否能进行该操作；判断该订单是否在链上已存在，不存在返回错误；返回加密后的订单数据。 |
| 调用方 | 沙师弟平台、司机、货主、保险公司、开票企业、合作单位  货主、司机APP查看订单功能，可以从沙师弟平台中获取，也可以从区块链上获取，是否APP加入两种方式订单查看方式？  保险公司、开票企业等需要查看订单信息时，需从沙师弟平台得到授权密钥。 |
| 隐私保护 | 司机、货主、保险公司只能查询与自己相关的订单数据  订单信息关键数据只能沙师弟、货主、大货司机查看？开具发票或保险公司查看经授权后方可查看？  交易双方信息是否需要保护？如保护，密文验证需要考虑 |

c. 回执码获取接口

|  |  |
| --- | --- |
| 名称 | 回执码获取接口 |
| 输入 | 订单ID |
| 输出 | 回执码密文 |
| 业务逻辑 | 判断该订单是否在链上已存在，不存在返回错误；智能合约判断是否货主发起请求；判断该订单状态是否未完成；设置订单状态为已获取回执码，返回回执码密文。 |
| 调用方 | 货主  订单生成后，货主通过APP获取指定订单的回执码，该回执码只能由货主获取。 |
| 隐私保护 | 无 |

d. 司机完成送货确认接口

|  |  |
| --- | --- |
| 名称 | 司机完成送货确认接口 |
| 输入 | 订单id、收货回执码 |
| 输出 | 成功响应 |
| 业务逻辑 | 判断该订单是否在链上已存在，不存在返回错误；智能合约判断是否为该订单货运司机发起请求；判断该订单状态是否未完成；计算回执码HASH值与链上数据比对，比对成功设置该订单状态为送货确认，并将回执码验证过程上链。 |
| 调用方 | 司机  司机送货完成获取回执码，由司机APP直接访问区块链确认该订单已送达。  沙师弟平台何时从链上获取订单状态？ |
| 隐私保护 | 无 |

e. 货主确认收货接口

|  |  |
| --- | --- |
| 名称 | 货主确认收货接口 |
| 输入 | 订单id |
| 输出 | 成功响应 |
| 业务逻辑 | 判断该订单是否在链上已存在，不存在返回错误；智能合约判断是否为该订单货主发起请求；判断该订单状态是否未完成；调用账务业务模块，设置货主账户转入司机账户X元；支付记录上链，更新订单信息；设置该订单状态为已完成。 |
| 调用方 | 货主  货主确认线下收货完成后，由货主APP直接访问区块链确认该订单已完成。  沙师弟平台何时从链上获取订单状态？ |
| 隐私保护 | 无 |

f. 订单历史痕迹追溯接口

|  |  |
| --- | --- |
| 名称 | 订单历史痕迹追溯接口 |
| 输入 | 订单id |
| 输出 | 订单历史痕迹 |
| 业务逻辑 | 判断该订单是否在链上已存在，不存在返回错误；智能合约判断是否有操作权限；判断该订单状态是否未完成；返回订单痕迹记录。 |
| 调用方 | 货主、司机、沙师弟平台、保险公司、监管方  查看区块链上记录的订单操作痕迹，何时、何人、何操作  货主或司机通过APP查看、保险公司出险查看、出现纠纷监管方审计等。 |
| 隐私保护 | 无 |

## 物流信息管理模块

a. 物流位置信息写入接口

|  |  |
| --- | --- |
| 名称 | 物流信息写入接口 |
| 输入 | 物流GPS信息、订单ID |
| 输出 | 成功响应 |
| 业务逻辑 | 判断该订单是否在链上已存在，不存在返回错误；智能合约判断是否有操作权限；判断该订单状态是否未完成；将物流位置信息及时间上传进链，并与该订单绑定。 |
| 调用方 | 沙师弟平台  沙师弟收集司机运输中的物流信息，判断写入时机，将信息写入区块链中 |
| 隐私保护 | 无 |

b. 物流位置信息查询接口

|  |  |
| --- | --- |
| 名称 | 物流位置信息查询接口 |
| 输入 | 订单id |
| 输出 | 物流位置信息 |
| 业务逻辑 | 判断该订单是否在链上已存在，不存在返回错误；智能合约判断是否有查看权限；返回该订单物流位置信息记录集（何时、何地）。 |
| 调用方 | 保险公司、监管方、合作方  物流信息可信存证，供事后查验。 |
| 隐私保护 | 无 |

## 发票业务模块

a. 发票数据写入接口

|  |  |
| --- | --- |
| 名称 | 发票数据写入接口 |
| 输入 | 订单ID、发票数据 |
| 输出 | 成功响应 |
| 业务逻辑 | 判断该订单是否在链上已存在，不存在返回错误；智能合约判断是否有记录电子发票操作权限；判断该订单状态是否已完成；将发票号码、代码、HASH值经电子发票校验码加密后上传进链，并与该订单绑定。 |
| 调用方 | 开票方  订单完成后，开票方根据订单数据给受票方开具电子发票，开票方将电子发票信息写入区块链。 |
| 隐私保护 | 只有持有电子发票信息的方可查看 |

b. 发票查验接口

|  |  |
| --- | --- |
| 名称 | 发票查验接口 |
| 输入 | 发票信息、订单ID、订单授权密钥 |
| 输出 | 验证结果 |
| 业务逻辑 | 判断该订单是否在链上已存在，不存在返回错误；智能合约判断是否有查验操作权限；判断该订单是否已开具发票；解密订单信息及发票信息，进行数据比对，返回数据结果。 |
| 调用方 | 开票系统  税局对电子发票开具审计与监管时查验。 |
| 隐私保护 | 无 |

## 账户业务模块

a. 支付运费接口

|  |  |
| --- | --- |
| 名称 | 支付运费接口 |
| 输入 | 支付方账户、收款方账户、金额 |
| 输出 | 成功响应 |
| 业务逻辑 | 智能合约判断请求方是否为支付方；判断是否存在支付方账户；判断支付方金额是否大于转账金额；判断是否存在收款方账户；支付方账户减少金额，收款方增加冻结金额。 |
| 调用方 | 沙师弟  货主支付运费给沙师弟后，由沙师弟作为支付方调用该接口 |
| 隐私保护 | 基于通道的隐私保护还是零知识证明？保护交易记录与账户余额。 |

b. 账户提现申请接口

|  |  |
| --- | --- |
| 名称 | 账户提现申请接口 |
| 输入 | 提现账户、提现金额N |
| 输出 | 提现交易ID |
| 业务逻辑 | 智能合约判断请求方是否为提现方；判断是否存在提现方账户；判断提现方未冻结金额是否大于提现金额N；生成提现交易申请记录在链，提现方可用金额减去提现金额N，提现方冻结金额加上提现金额N，提交交易状态为已申请。 |
| 调用方 | 司机、货主  从账户中申请提现，先发起提现申请交易  沙师弟何时获得提现交易ID？ |
| 隐私保护 | 基于通道的隐私保护还是零知识证明？保护交易记录与账户余额。 |

c.提现确认接口

|  |  |
| --- | --- |
| 名称 | 提现确认接口 |
| 输入 | 提现交易ID，提现方转账记录 |
| 输出 | 响应成功 |
| 业务逻辑 | 智能合约判断请求方是否为平台方；判断是否存在提现方账户；判断提现方账户冻结金额是否大于提现交易中金额；提现方账户冻结金额减少交易金额，提现平台方账户增加金额。提现交易状态设置已完成，并绑定转账记录。 |
| 调用方 | 沙师弟  沙师弟获取提现交易ID后，线下支付完成后，调用该接口。 |
| 隐私保护 | 基于通道的隐私保护还是零知识证明？保护交易记录与账户余额。 |

d.交易接口

|  |  |
| --- | --- |
| 名称 | 交易接口 |
| 输入 | 支付方账户、收款方账户、金额 |
| 输出 | 响应成功 |
| 业务逻辑 | 智能合约判断请求方是否为支付方；判断是否存在支付方账户；判断支付方冻结金额是否大于转账金额；判断是否存在收款方账户；支付方冻结账户减少金额，收款方增加可用金额。 |
| 调用方 | 货主  货主确认收货后，订单完成，智能合约自动触发调用该接口。 |
| 隐私保护 | 基于通道的隐私保护还是零知识证明？保护交易记录与账户余额。 |

1. 账户信息查询

|  |  |
| --- | --- |
| 名称 | 账户信息查询接口 |
| 输入 | 用户ID |
| 输出 | 返回账户信息 |
| 业务逻辑 | 判断是否存在该用户账户；智能合约判断请求方是否为该账户持有人或平台方；返回账户可用余额与冻结余额。 |
| 调用方 | 沙师弟、司机、货主  货主、司机通过APP可获取链上账户信息，该账户不可被非法篡改，真实可信 |
| 隐私保护 | 基于通道的隐私保护还是零知识证明？保护交易记录与账户余额。 |

1. 账户交易信息查询

|  |  |
| --- | --- |
| 名称 | 账户信息查询接口 |
| 输入 | 用户ID |
| 输出 | 返回账户交易信息 |
| 业务逻辑 | 判断是否存在该用户账户；智能合约判断请求方是否为该账户持有人或平台方；返回账户可用余额与冻结余额的历史交易信息。 |
| 调用方 | 沙师弟、司机、货主  货主、司机通过APP可获取链上账户历史交易信息，该账户不可被非法篡改，真实可信 |
| 隐私保护 | 基于通道的隐私保护还是零知识证明？保护交易记录与账户余额。 |

1. 提现信息历史查询

|  |  |
| --- | --- |
| 名称 | 提现信息历史查询接口 |
| 输入 | 用户ID |
| 输出 | 返回账户所有提现历史信息 |
| 业务逻辑 | 判断是否存在该用户账户；智能合约判断请求方是否为该账户持有人或平台方；返回账户历史提现基本信息及提现交易ID。 |
| 调用方 | 沙师弟、司机、货主  货主、司机通过APP可获取链上账户历史提现信息，该账户不可被非法篡改，真实可信 |
| 隐私保护 | 基于通道的隐私保护还是零知识证明？保护交易记录与账户余额。 |

1. 提现信息查询

|  |  |
| --- | --- |
| 名称 | 提现信息查询接口 |
| 输入 | 提现交易ID |
| 输出 | 返回账户所有提现信息 |
| 业务逻辑 | 判断是否存在该用户账户；智能合约判断请求方是否为该账户持有人或平台方；判断提现交易ID是否该用户账户中交易；返回该提现交易详情，如申请、确认、时间、证据、操作者等。 |
| 调用方 | 沙师弟、司机、货主  货主、司机通过APP可获取某指定提现交易详细情况，不可被非法篡改，真实可信 |
| 隐私保护 | 基于通道的隐私保护还是零知识证明？保护交易记录与账户余额。 |

## 保险业务模块

a. 保险取证接口

|  |  |
| --- | --- |
| 名称 | 保险取证接口 |
| 输入 | 保单id |
| 输出 | 订单号 |
| 业务逻辑 | 智能合约进行权限判断， 是否能进行该操作；判断该保单是否在链上已存在，不存在返回错误；查找该保单对应的订单，返回订单号。 |
| 调用方 | 保险公司  当发生事故，需要进入理赔，保险公司通过该接口获取订单号 |
| 隐私保护 | 无 |

b. 保险数据写入接口

|  |  |
| --- | --- |
| 名称 | 司机信息查询接口 |
| 输入 | 订单ID、保单ID、保险信息 |
| 输出 | 成功响应 |
| 业务逻辑 | 智能合约进行权限判断， 是否能进行该操作；判断链上是否存在该订单；判断链上是否存在该保险信息，存在返回失败；在链上记录该保单信息，并关联到该订单 |
| 调用方 | 沙师弟平台  如货主、司机购买保险，购买成功后沙师弟调用该接口 |
| 隐私保护 | 无 |

c. 保险数据更新接口

|  |  |
| --- | --- |
| 名称 | 司机信息查询接口 |
| 输入 | 订单ID、保单ID、保险信息 |
| 输出 | 成功响应 |
| 业务逻辑 | 智能合约进行权限判断， 是否能进行该操作；判断链上是否存在该订单；判断链上是否存在该保险信息，不存在返回失败；判断保险基础信息是否一致，不一致返回失败；在链上更新该保单信息，并关联到该订单 |
| 调用方 | 沙师弟平台  如前期只产生保单号，后续生成保单等具体信息后沙师弟调用该接口 |
| 隐私保护 | 无 |

# 部署方案

区块链货运系统部署在沙师弟、公网、保险公司、合作单位、开票方等地点，可以采用部署在服务器或公有云的不同方式。

在物流联盟链网络中，应该包含沙师弟节点、用户节点（为司机和货主提供与区块链交互的功能）、合作单位节点、开票节点、保险节点、监管节点。

一期首先部署沙师弟节点、用户节点、监管节点、合作单位节点。

建议节点数沙师弟节点2个、用户节点2个、监管节点1个、合作单位节点1个，共需6台服务器，另外，需要3台服务器部署kafka与zookeeper集群，共9台服务器。



# 环境需求

其中，部署区块链网络有以下需求，请提前准备：

|  |  |
| --- | --- |
| 环境需求 | 说明 |
| 服务器配置 | 双路4核CPU，32G内存，500G硬盘，百兆网卡 |
| 网络需求 | 具备外网IP、端口，内网机器可互通，带宽》20M |
| 操作系统 | UBANTO |
| 人员需求 | 熟悉LINUX操作，熟悉网络配置的运维人员1名 |

# 计划进度

|  |  |
| --- | --- |
|  | 时间 |
| 设计方案 | 5月25日之前完成一期设计方案 |
| 集成方案 | 5月25日之前完成一期集成方案 |
| 开发 | 5月27日~6月1日 一期开发工作 |
| 部署 | 5月27日~6月1日 一期部署工作 |
| 集成 | 6月4日~6月9日 一期集成工作 |
| 测试 | 6月11日~6月15日完成测试工作 |
| 试运行 | 6月16日开始试运行 |

# 问题沟通

在设计过程中，考虑有以下问题，需要与沙师弟进行沟通了解：

1. 物流联盟链中用户角色及权限需具体明确？
2. 未来如何向外扩展，构建物流链，信息如何打通？

（2）订单信息具体包含什么内容？不同用户对订单信息的读写权限需确定？

（3）物流信息（GPS）是否上链？记录的频率（记录节点）是多少？用户需要查看物流信息时更新不及时怎么办？（如何保证GPS信息源数据真实性？）

（4）货主与司机信息上链需求是否合理？是因为方便后续与其他大型物流公司、仓库物流园接入扩展?（数据由沙师弟写入）

（5）货源信息由谁写入？写入方是由沙师弟还是货主直接写入？A.沙师弟写入存在中心化问题；B.货主直接写入，沙师弟获取数据的方式？）

（6）开发与区块链直接交互应用，如何进行身份认证（私钥保存、证书、用户名+密码）？

（7）如何创建证书？如何发放证书？

（8）货主发布货物信息连接的节点是哪个？前端让用户感受到与区块链交互的体验？

（9）回执码由货主调用接口产生，记录在链，回执码应该以密文形式存在链上。

（11）订单取消业务流程如何处理，是否都记录在链？