**MATRX 共识算法框架**

**版本: V1.0.6**

**作者：MATRIX 基金会北京研究院**

**日期：2018.07.31**

任何情况下，与本系统及其衍生产品，以及与之相关的全部文件（包括本文件及其任何附件中的全部信息）相关的全部知识产权（包括但不限于版权、商标和技术秘密）皆属于 MATRIX 基金会所有。

本文件中的信息是保密的，且仅供用户指定的接收人内部使用。未经 MATRIX 基金会事先书面同意，本文件的任何用户不得对本产品和本文件中的信息向任何第三方（包括但不限于除用户指定接收人以外的管理人员、员工和关联公司）进行披露、出借、许可、转让、出售、分发、传播或进行与本产品和本文件相关的任何其他处置，也不得使该等第三方以任何形式使用本产品和本文件中的信息。

未经 MATRIX 基金会事先书面允许，不得为任何目的、以任何形式或任何方式对本文件进行复制、修改或分发。本文件的任何用户不得更改、移除或损害本文件所使用的任何商标。

本文件按“原样”提供，就本文件的正确性、准确性、可靠性或其他方面，MATRIX 基金会并不保证本文件的使用或使用后果。本文件中的全部信息皆可能在没有任何通知的情形下被进一步修改，MATRIX 基金会对本文件中可能出现的任何错误或不准确之处不承担任何责任。

在任何情况下，MATRIX 基金会均不对任何因使用本软件产品和本文件中的信息而引起的任何直接损失、间接损失、附带损失、特别损失或惩罚性损害赔偿（包括但不限于获得替代商品或服务、丧失使用权、数据或利润；或商业中断），责任或侵权（包括过失或其他侵权）承担任何责任，即使 MATRIX 基金会事先获知上述损失可能发生。

MATRIX 基金会保留所有权利

# 目 录

[目 录](#_Toc29601)

[变更记录](#_Toc4690)

[1 引言](#_Toc18043)

[1.1 文档用途](#_Toc2878)

[1.2 术语](#_Toc9071)

[1.3 使用对象](#_Toc18654)

[2 整体框架](#_Toc27192)

[2.1 矿工服务](#_Toc32295)

[2.1.1 普通节点 Hash计算服务](#_Toc5013)

[2.2 随机数生成服务](#_Toc29709)

[2.2.1 随机数投票](#_Toc29457)

[2.2.2 随机数生成服务](#_Toc19629)

[2.3 拓扑生成服务](#_Toc21520)

[2.3.1 网络拓扑生成服务](#_Toc30898)

[2.3.2 网络拓扑更新服务](#_Toc13341)

[2.3.3 测试接口](#_Toc14556)

[2.4 广播节点服务](#_Toc11469)

[2.4.1 私钥验证收集服务](#_Toc5339)

[2.4.2 在线时间收集服务](#_Toc29120)

[2.4.3 广播区块生成服务](#_Toc14806)

[2.4.4 测试接口](#_Toc11127)

[2.5 投票服务](#_Toc1623)

[2.6 节点在线服务](#_Toc32289)

[2.7 Leader身份服务](#_Toc30325)

[2.7.1 Leader身份计算服务](#_Toc17294)

[2.7.2 重选leader控制服务](#_Toc31349)

[2.7.3 重选主节点会话服务](#_Toc31198)

[2.7.4 重选从节点会话服务](#_Toc21298)

[2.7.5 测试接口](#_Toc13497)

[2.8 区块验证服务](#_Toc11023)

[2.8.1 投票服务](#_Toc3327)

[2.8.2 结果收集及验证服务](#_Toc5958)

[2.8.3 测试接口](#_Toc11101)

[2.9 区块生成服务](#_Toc19655)

[2.9.1 挖矿结果验证服务](#_Toc11305)

[2.9.2 普通区块生成服务](#_Toc27919)

[2.9.3 区块验证header生成服务](#_Toc20334)

[2.9.4 测试接口](#_Toc12945)

[3 详细设计](#_Toc15892)

# 变更记录

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 修订日期 | 设计内容 | 作者 | 评审者 | 评审日期 |
| 2018-07-24 | 1.0.4 版 | 胡源凯，张文 |  |  |
| 2018-07-28 | 1.0.5 版 | 胡源凯，张文 |  |  |
| 2018-07-31 | 1.0.6 版 | 胡源凯，张文 |  |  |

# 引言

## 文档用途

本文档详细介绍了 MATRIX 的共识算法框架

## 术语

| **术语** | **备注** |
| --- | --- |
|  |  |

## 使用对象

阅读对象主要针对熟悉相关业务、技术和应用知识的人员，包括：研究院全体同事

# 整体框架

各服务以微服务的形式存在，及只依赖消息驱动，即可完成服务，提供输出



## 矿工服务



### 普通节点 Hash计算服务

#### 接口设计

* 功能：

提供hash计算算力，根据合法的validator区块header，进行计算工作，将计算结果广播给所有的validator。

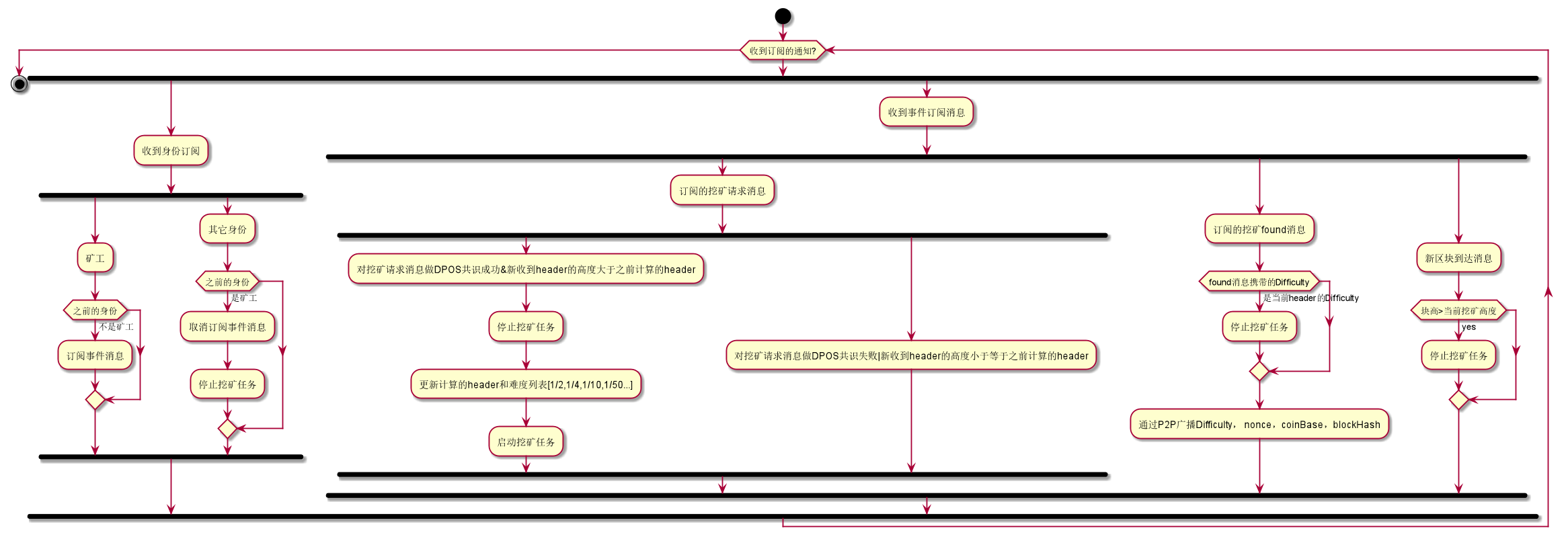
* 输入：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 名称 | 消息码 | 消息体 | 来源 | 实现方式 | 备注 |
| 身份变更消息 | 待定 | 新身份枚举 | CA服务 | 消息订阅 | 矿工、验证者、普通节点等身份发生变化时通知 |
| 挖矿请求消息 | 待定 | header头 | CA服务 | 消息订阅 | 需要CA验证来自合法的validator |
| 新区块到达消息 | 无 | block指针 | 内部blockchain | 消息订阅 |  |
| 区块同步消息 | 无 | 无 | 内部downloader | 消息订阅 |  |
| found消息 | 待定 | header头 | 挖矿成功消息 | 内部消息订阅 |  |

* 输出：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名称 | 消息码 | 消息体 | 实现方式 | 备注 |
| 挖矿结果广播 | 待定 | nounce、coinbase、blockhash | 待定 | 进过CA签名后广播给所有validator |

#### 流程图



## 随机数生成服务



### 随机数投票

#### 接口设计

* 功能：

验证者在广播区块广播区块之前-10个区块时生成公私钥对，暂存私钥，并将上次暂存的私钥和本次生成的公钥发送给广播节点

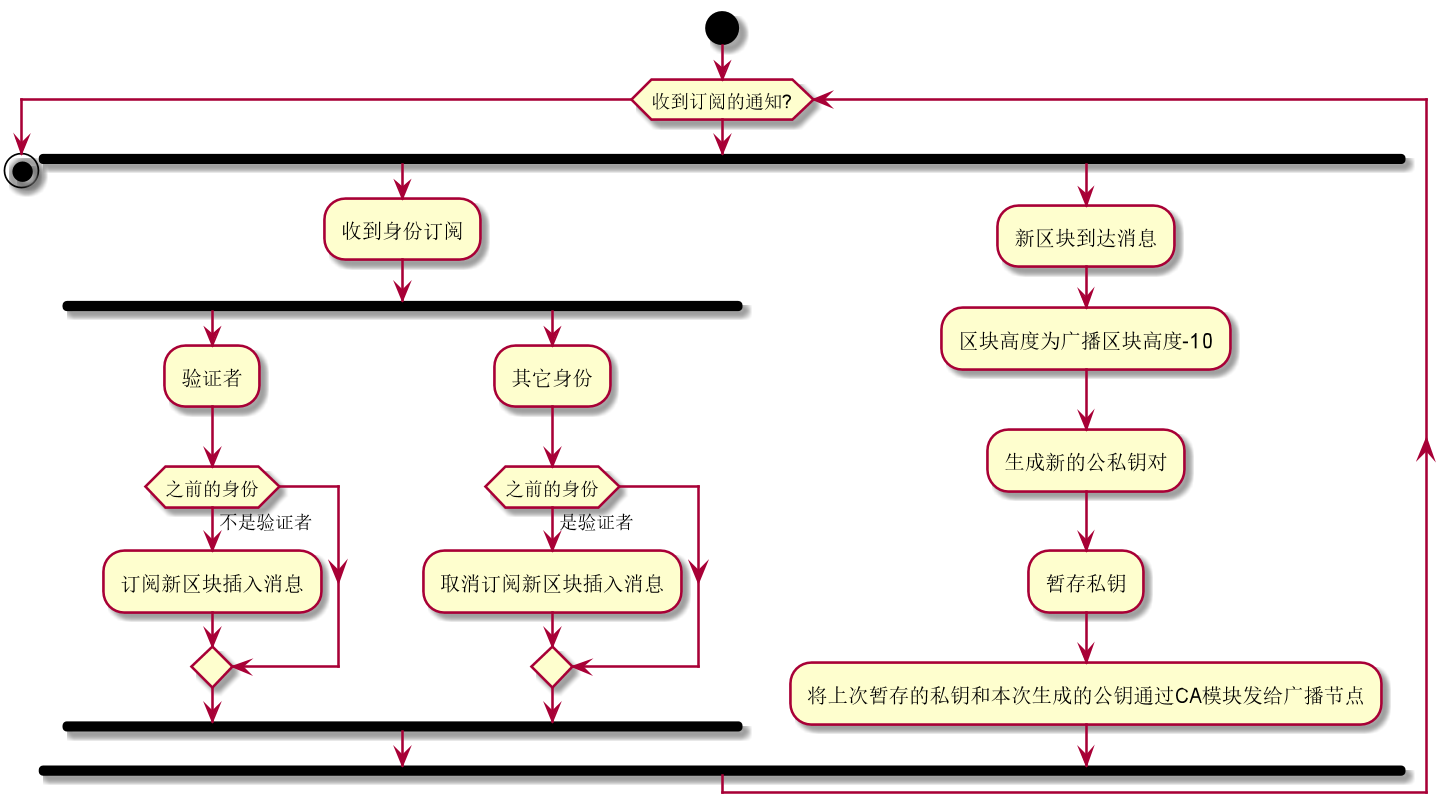
* 输入：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 名称 | 消息码 | 消息体 | 来源 | 实现方式 | 备注 |
| 身份变更消息 | 待定 | 新身份枚举 | CA服务 | 消息订阅 | 矿工、验证者、普通节点等身份发生变化时通知 |
| 新区块到达消息 | 无 | block指针 | 内部blockchain | 消息订阅 |  |

* 输出：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名称 | 消息码 | 消息体 | 实现方式 | 备注 |
| 投票结果广播 | 待定 | 公私钥对 | 待定 | 进过CA签名后发送给广播节点 |

#### 流程图



### 随机数生成服务

#### 接口设计

* 功能：

所有节点在广播区块读取广播节点写入的私钥之和

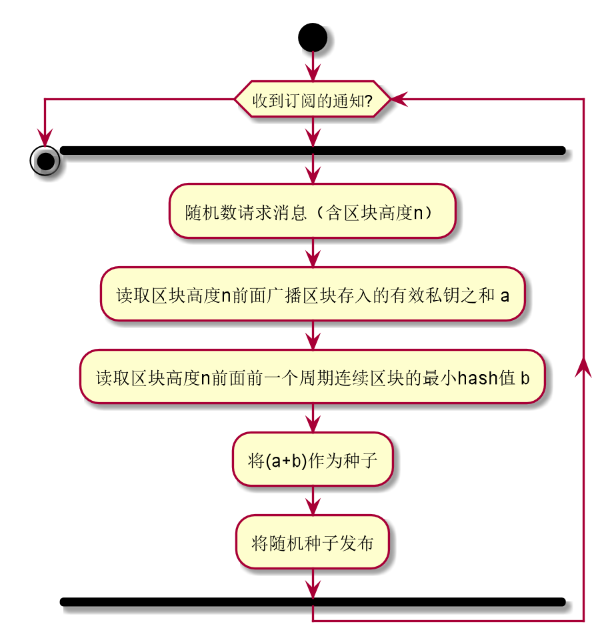
* 输入：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 名称 | 消息码 | 消息体 | 来源 | 实现方式 | 备注 |
| 随机数请求消息 | 无 | 区块高度n | 内部 | 消息订阅 |  |

* 输出：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名称 | 消息码 | 消息体 | 实现方式 | 备注 |
| 随机种子 | 待定 | Byte类型 | 消息订阅 |  |

#### 流程图



## 拓扑生成服务



### 网络拓扑生成服务

#### 接口设计

* 功能：

所有节点根据主节点列表和本地存储的随机种子生成主节点列表

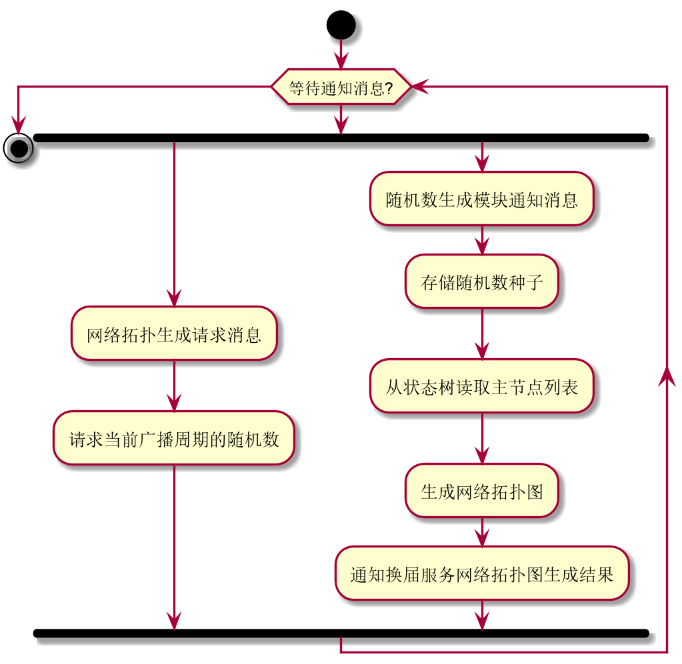
* 输入：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 名称 | 消息码 | 消息体 | 来源 | 实现方式 | 备注 |
| cc主节点列表消息 | 待定 | 无 | CA | 消息订阅 |  |
| 随机种子消息 | 待定 | block指针 | 随机数生成服务 | 消息订阅 |  |

* 输出：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名称 | 消息码 | 消息体 | 实现方式 | 备注 |
| 网络拓扑图 | 待定 | 网络分层结构 | 消息订阅 |  |

#### 流程图



### 网络拓扑更新服务

#### 接口设计

* 功能：

所有节点根据普通区块里顶层节点的在线状态更新主节点列表

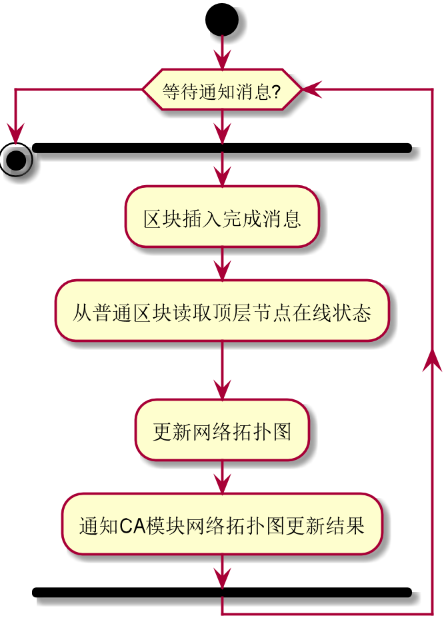
* 输入：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 名称 | 消息码 | 消息体 | 来源 | 实现方式 | 备注 |
| 随机种子消息 | 待定 | block指针 | 内部blockchain | 消息订阅 |  |

* 输出：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名称 | 消息码 | 消息体 | 实现方式 | 备注 |
| 网络拓扑图 | 待定 | 网络分层结构 | 消息订阅 |  |

#### 流程图



### 测试接口

## 广播节点服务



### 私钥验证收集服务

#### 接口设计

* 功能：

将验证者发送过来的私钥进行验证收集，并计算出结果

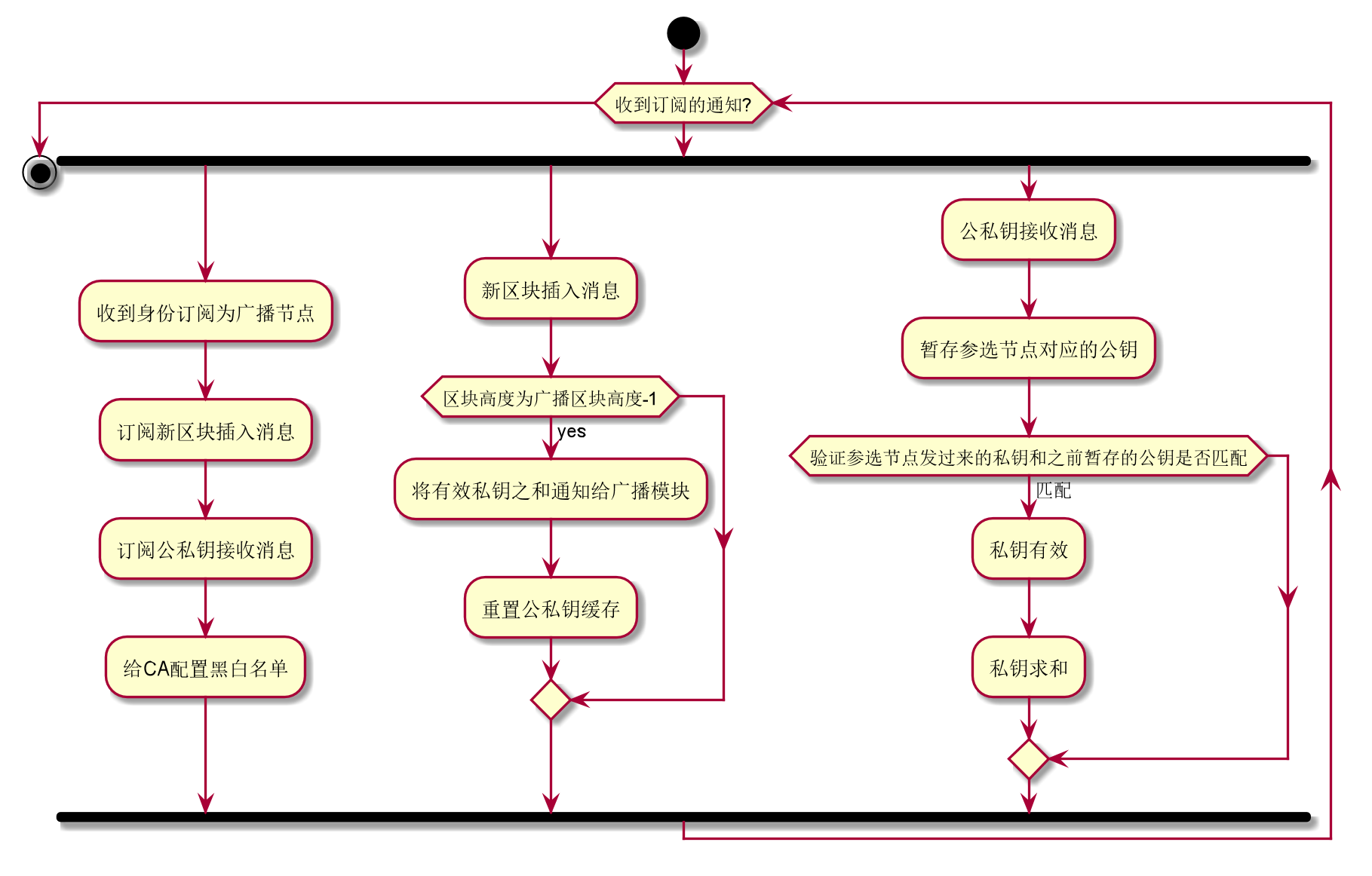
* 输入：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 名称 | 消息码 | 消息体 | 来源 | 实现方式 | 备注 |
| 公私钥消息 | 待定 | 公私钥对 | CA服务 | 消息订阅 |  |
| 区块插入消息 | 无 | block指针 | 内部blockchain | 消息订阅 |  |

* 输出：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名称 | 消息码 | 消息体 | 实现方式 | 备注 |
| 收集结果 | 待定 | 私钥之和 | 消息订阅 | 通过CA签名后发送给所有节点 |

#### 流程图



### 在线时间收集服务

### 广播区块生成服务

### 测试接口

## 投票服务

## 节点在线服务

## Leader身份服务



### Leader身份计算服务

#### 接口设计

* 功能：

根据块高计算某轮次的leader，缓存当前leader的nodeid，可由更换leader结果消息修改。Leader变更时提供更变消息，并提供接口查询当前leader 。

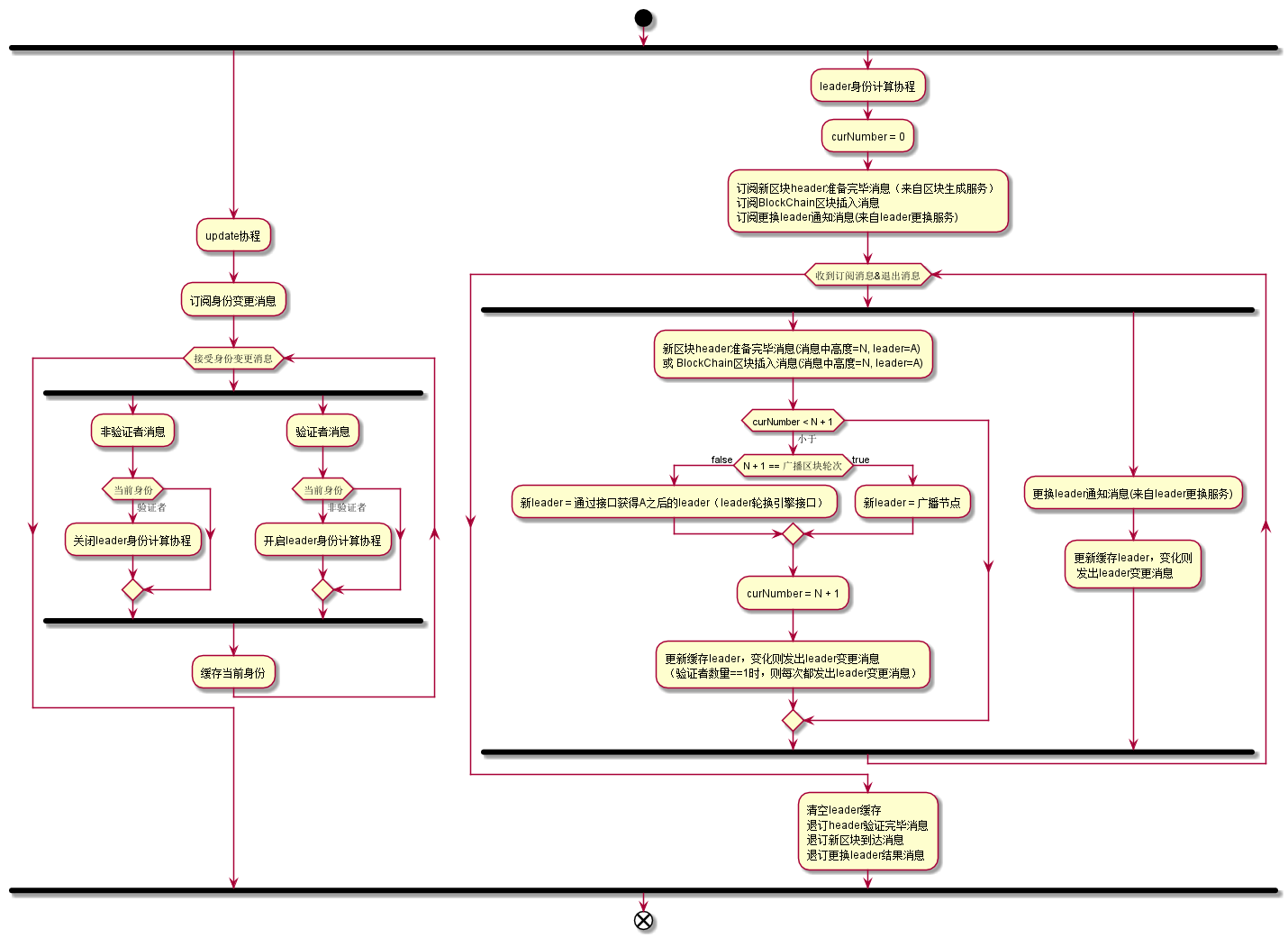
* 输入：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 名称 | 消息码 | 消息体 | 来源 | 实现方式 | 备注 |
| 新区块Header准备完毕消息 | 待定 | Header指针 | 区块生成服务 | 消息订阅 | 矿工挖矿结果验证完毕后的消息 |
| Blockchain区块插入消息 | 待定 | header指针 | Blockchain | 消息订阅 |  |
| 更换leader成功消息 | 待定 | 节点信息 | 重选leader控制服务 | 消息订阅 | 节点信息为空表示当前无leader |

* 输出：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名称 | 消息码 | 消息体 | 实现方式 | 备注 |
| Leader变更消息 | 待定 | 节点信息 | 消息通知 | 节点信息为空表示当前无leader |
| 当前Leader查询接口 | 无 | 节点信息 | 接口 | 同上 |

#### 流程图



### 重选leader控制服务

#### 状态图



#### 接口设计

* 功能：

控制重选leader的流程，包括何时启动重选会话及最后更换结果的通知。包含状态机。

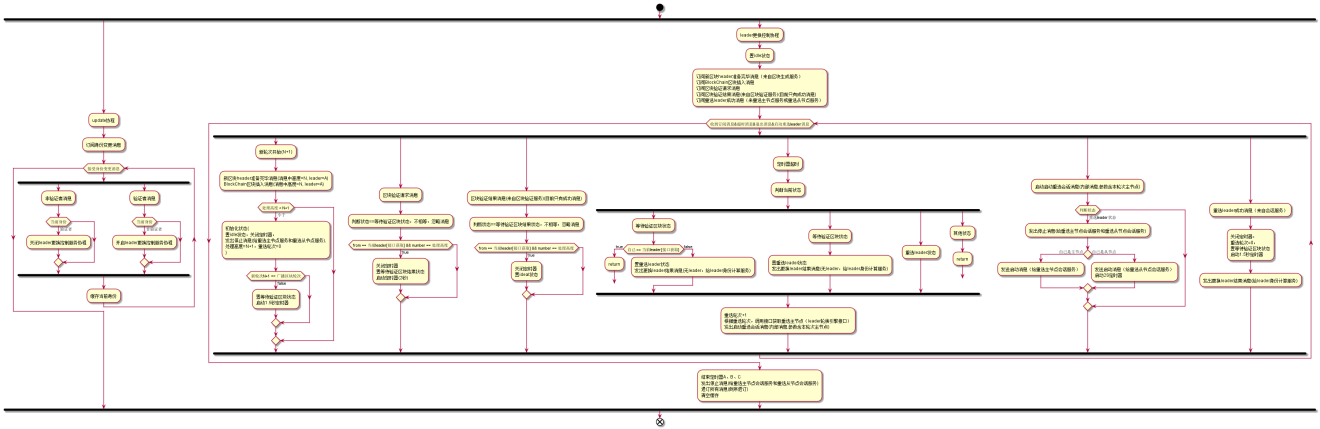
* 输入：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 名称 | 消息码 | 消息体 | 来源 | 实现方式 | 备注 |
| 身份变更消息 | 待定 | 新身份枚举 | CA服务 | 消息订阅 | 身份变更通知 |
| 新区块Header准备完毕消息 | 待定 | header头 | 区块生成服务 | 消息订阅 | 矿工挖矿结果验证完毕后的消息 |
| 区块验证请求消息 | 待定 | header头 | CA服务 | 消息订阅 | 经过CA验证来自合法的validator |
| 区块验证结果消息 | 待定 | 消息体(leader、高度，结果) | 区块验证服务 | 消息订阅 | 目前只有成功消息 |
| 重选leader成功消息 | 待定 | 包含Leader差距值和投票列表 | 重选会话服务 | 消息订阅 | 主从节点会话都会发出该消息 |

* 输出：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名称 | 消息码 | 消息体 | 实现方式 | 备注 |
| 更换Leader成功消息 | 待定 | 节点信息 | 消息通知 | 节点信息为空表示当前无leader |
| 会话启动消息 | 待定 | 重选主节点信息 | 消息通知 |  |
| 会话停止接口 | 待定 | 无 | 消息通知 |  |

#### 流程图



### 重选主节点会话服务

#### 接口设计

* 功能：

重选leader流程中，自己为主节点情况下的会话流程。主要负责发出重选leader请求、收集投票结果、并广播成功消息。

* 输入：

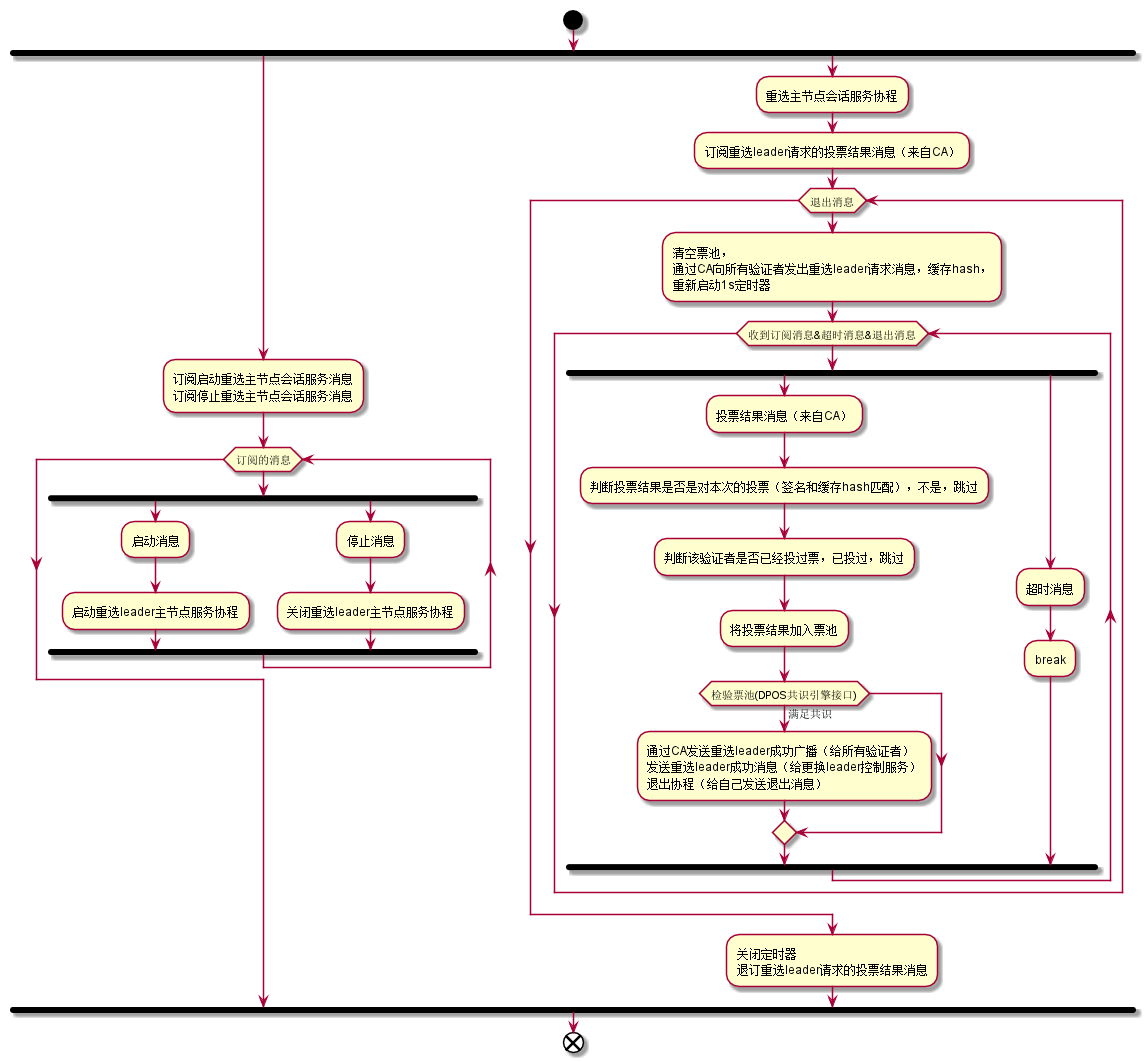
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 名称 | 消息码 | 消息体 | 来源 | 实现方式 | 备注 |
| 会话启动消息 | 待定 | 重选主节点信息 | 更换leader控制服务 | 消息订阅 |  |
| 会话停止消息 | 待定 | 无 | 更换leader控制服务 | 消息订阅 |  |
| 投票结果消息 | 待定 | 投票结构体待定 包含签名 | CA服务 | 消息订阅 | 经过CA验证来自合法的validator |

注：需要CA提供接口获取验证者列表（包含节点ID和权益值），用于判断投票是否满足条件

* 输出：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名称 | 消息码 | 消息体 | 实现方式 | 备注 |
| 重选leader请求消息广播 | 待定 | 请求结构体待定  包含leader差值和发起者id | 消息通知 | 投票结果进过CA签名后广播给所有validator |
| 重选leader成功广播 | 待定 | 结构体待定  包含Leader差距值和投票列表 | 消息通知 | 投票结果进过CA签名后广播给所有validator |
| 重选leader成功消息 | 待定 | 新leader节点信息 | 消息通知 | 给重选leader控制服务的消息 |

#### 流程图



### 重选从节点会话服务

#### 接口设计

* 功能：

重选leader流程中，自己扮演从节点情况下的会话流程。主要响应主节点的请求。

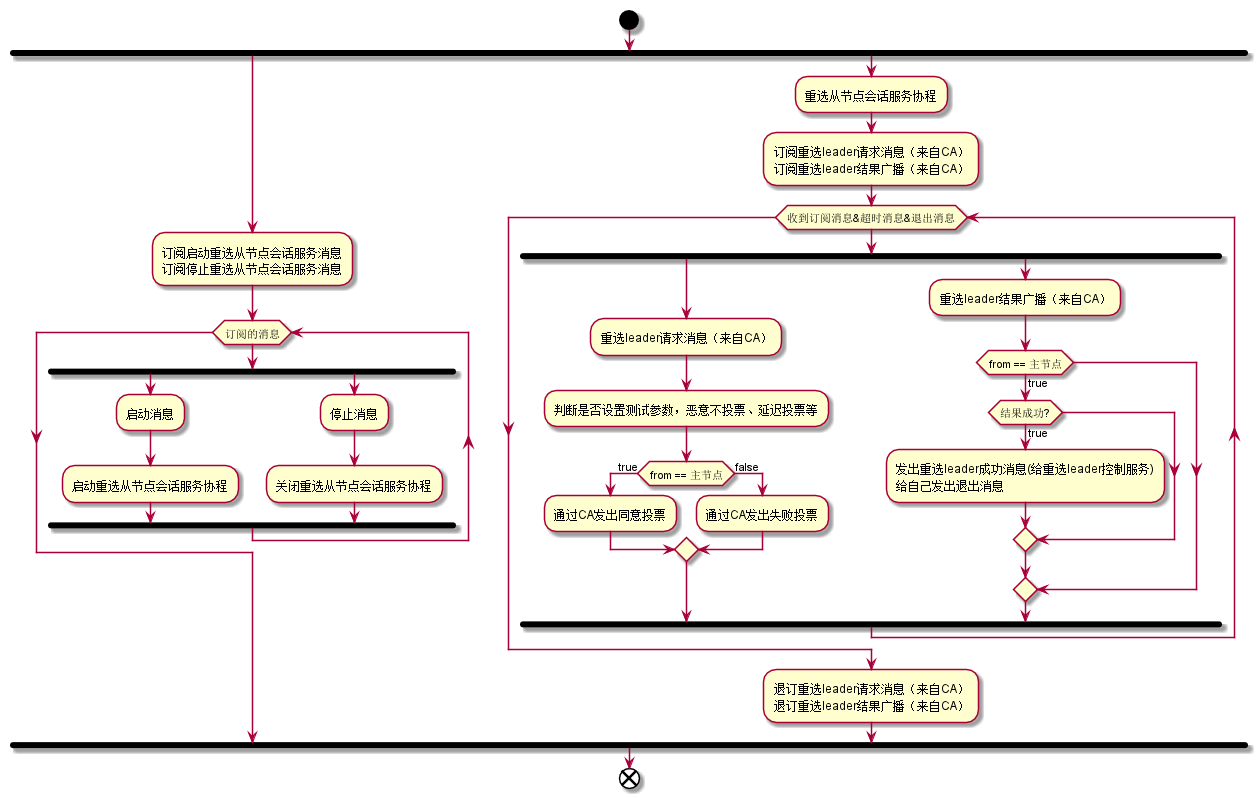
* 输入：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 名称 | 消息码 | 消息体 | 来源 | 实现方式 | 备注 |
| 会话启动消息 | 待定 | 重选主节点信息 | 重选leader控制服务 | 消息订阅 |  |
| 会话停止消息 | 待定 | 无 | 重选leader控制服务 | 消息订阅 |  |
| 重选leader请求消息 | 待定 | 请求结构体待定  包含leader差值和发起者id | CA服务 | 消息订阅 | 经过CA验证来自合法的validator |
| 重选leader成功广播 | 待定 | 结构体待定  包含Leader差距值和投票列表 | CA服务 | 消息通知 | 经过CA验证来自合法的validator |

* 输出：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名称 | 消息码 | 消息体 | 实现方式 | 备注 |
| 投票结果消息 | 待定 | 投票结构体待定 包含签名 | 消息通知 | 投票结果进过CA后通过P2P发送给请求者 |
| 重选leader成功消息 | 待定 | 新leader节点信息 | 消息通知 | 给重选leader控制服务的消息 |

#### 流程图



### 测试接口

## 区块验证服务



### 投票服务

#### 接口设计

* 功能：

对待验证的区块header进行验证并进行投票

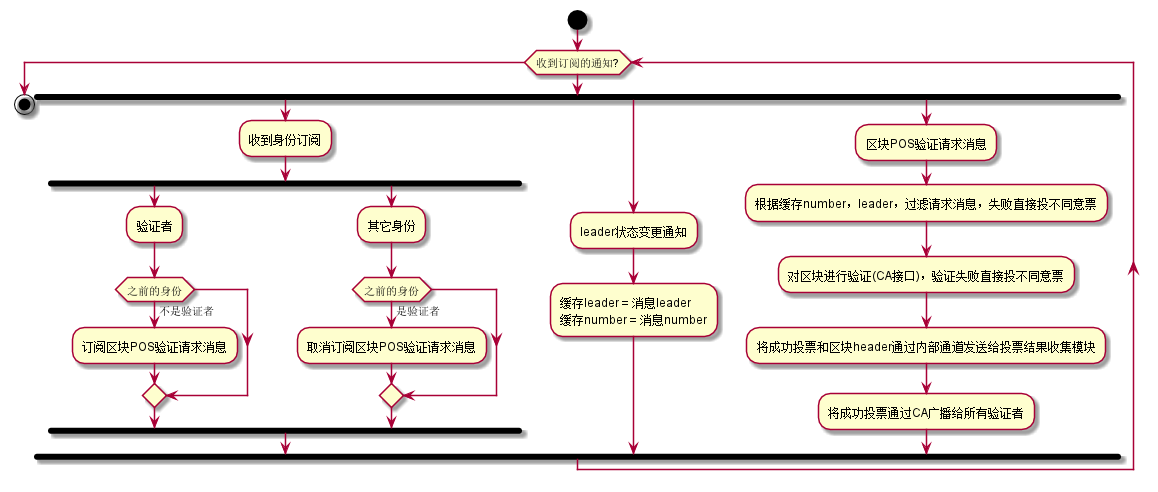
* 输入：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 名称 | 消息码 | 消息体 | 来源 | 实现方式 | 备注 |
| 身份变更消息 | 待定 | 新身份枚举 | CA服务 | 消息订阅 | 矿工、验证者、普通节点等身份发生变化时通知 |
| Leader状态消息 | 待定 | 节点信息 | Leader身份服务 | 消息订阅 | 信息为空表示当前无leader |
| 区块验证请求消息 | 待定 | Header和交易列表 | CA服务 | 消息订阅 |  |

* 输出：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名称 | 消息码 | 消息体 | 实现方式 | 备注 |
| 投票结果 | 待定 | Hash、投票结果 | 待定 | CA将投票结果和hash进行签名 |
| Header和投票结果消息 | 待定 | Header指针、投票结果 | 通道 | 内部消息，通道通知 |

#### 流程图



### 结果收集及验证服务

#### 接口设计

* 功能：

收集投票结果并进行验证，并对满足dpos共识的header进行广播

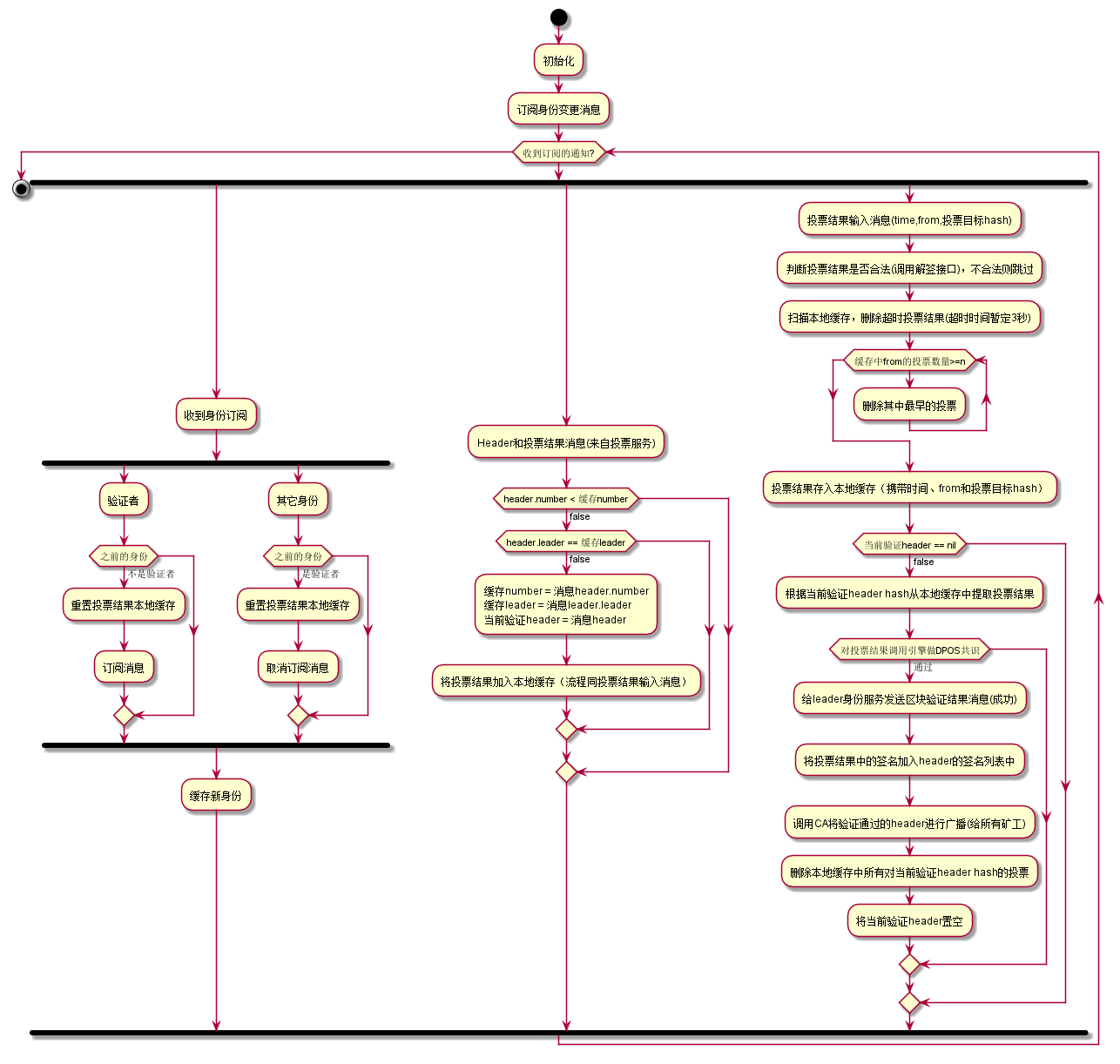
* 输入：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 名称 | 消息码 | 消息体 | 来源 | 实现方式 | 备注 |
| 身份变更消息 | 待定 | 新身份枚举 | CA服务 | 消息订阅 | 矿工、验证者、普通节点等身份发生变化时通知 |
| 投票结果输入消息 | 待定 | 签名 | CA服务 | 消息订阅 |  |
| Header和投票结果消息 | 待定 | Heard、投票结果 | 投票服务 | 消息通道 | 内部消息 |

* 输出：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名称 | 消息码 | 消息体 | 实现方式 | 备注 |
| 满足dpos共识条件的投票结果 | 待定 | Header | CA |  |

#### 流程图



### 测试接口

## 区块生成服务



### 挖矿结果验证服务

#### 接口设计

* 功能：

缓存DOPS验证完成的header和tx编号集合。等待矿工的挖矿结果。收到挖矿结果后，验证nounce、coinbase填入后计算的blockhash是否满足要求。

* 输入：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 名称 | 消息码 | 消息体 | 来源 | 实现方式 | 备注 |
| 身份变更消息 | 待定 | 新身份枚举 | CA服务 | 消息订阅 | 身份变更通知 |
| 矿工挖矿结果消息 | 待定 | Nounce、coinbase、blockhash | CA服务 | 消息订阅 | 经过CA验证，来自合法的miner |
| DPOS验证结果消息 | 待定 | header头 | 区块POS验证服务 | 消息订阅 | 验证通过的header |
| 交易获取接口 | 无 | 交易数据 | 验证者交易池 | 接口 | 输入为交易编码 |

* 输出：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名称 | 消息码 | 消息体 | 实现方式 | 备注 |
| Header验证完毕消息 | 待定 | Header头 | 消息通知 |  |
| 区块获取接口 | 无 | Header及交易列表 | 接口 |  |

### 普通区块生成服务

#### 接口设计

* 功能：

打包普通区块，并进行广播。

* 输入：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 名称 | 消息码 | 消息体 | 来源 | 实现方式 | 备注 |
| 身份变更消息 | 待定 | 新身份枚举 | CA服务 | 消息订阅 | 身份变更通知 |
| Leader状态变更消息 | 待定 | Nodeid字符串 | Leader身份服务 | 消息订阅 |  |
| 区块获取接口 | 无 | Header和交易列表 | 挖矿结果验证服务 | 接口调用 |  |

* 输出：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名称 | 消息码 | 消息体 | 实现方式 | 备注 |
| 区块广播 | 待定 | Block结构 | 消息通知 | 插入blockchain并广播区块 |
| 启动header生成消息 | 待定 | 块高number | 消息通知 |  |

### 区块验证header生成服务

#### 接口设计

* 功能：

生成待验证header和tx编号集合，并广播给所有的验证者进行DPOS验证。

* 输入：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 名称 | 消息码 | 消息体 | 来源 | 实现方式 | 备注 |
| 身份变更消息 | 待定 | 新身份枚举 | CA服务 | 消息订阅 | 身份变更通知 |
| 启动header生成消息 | 待定 | 块高number | 普通或广播区块生成服务 | 消息订阅 |  |
| 区块交易获取接口 | 接口 | 2秒前的所有交易编号 | 验证者交易池 | 消息订阅 | 获取交易编号 |
| 区块获取接口 | 无 | Header和交易列表 | 挖矿结果验证服务 | 接口调用 |  |

* 输出：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名称 | 消息码 | 消息体 | 实现方式 | 备注 |
| 区块验证header广播 | 待定 | Header和交易列表 | 消息通知 | 经过CA加上自己的签名并广播给所有validator |

### 测试接口

# 详细设计