# 总体框架

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



## Hash计算服务

* 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。

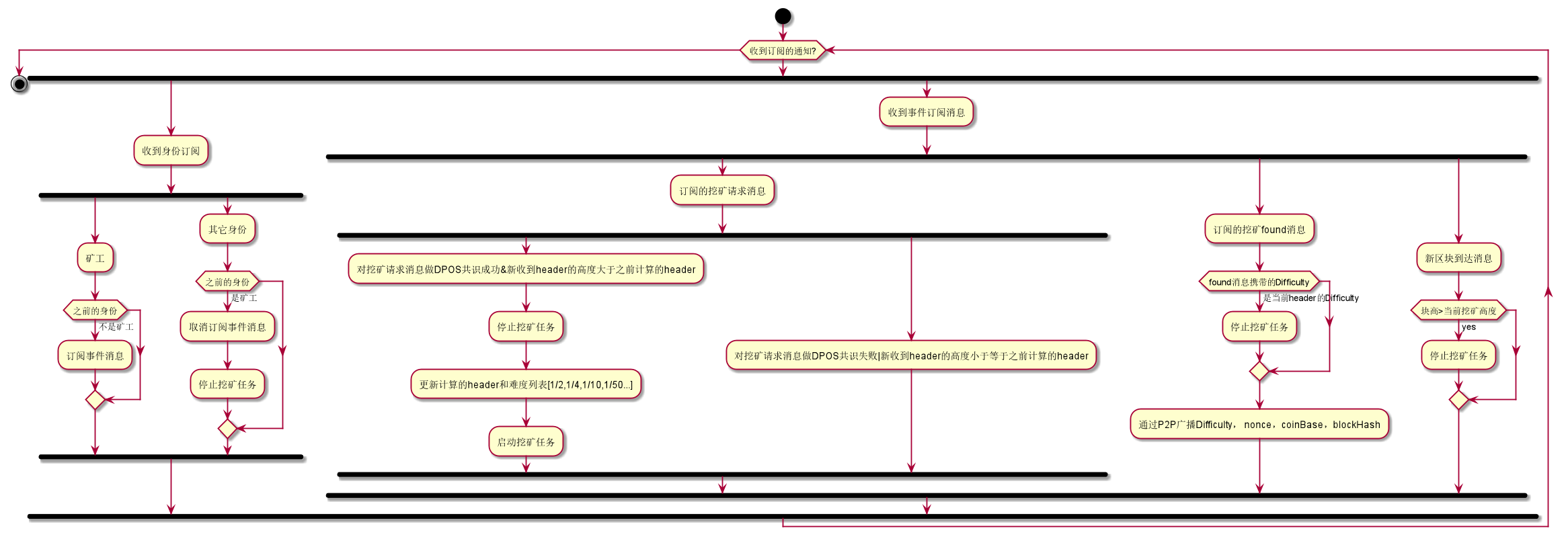
* 输入：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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

* 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

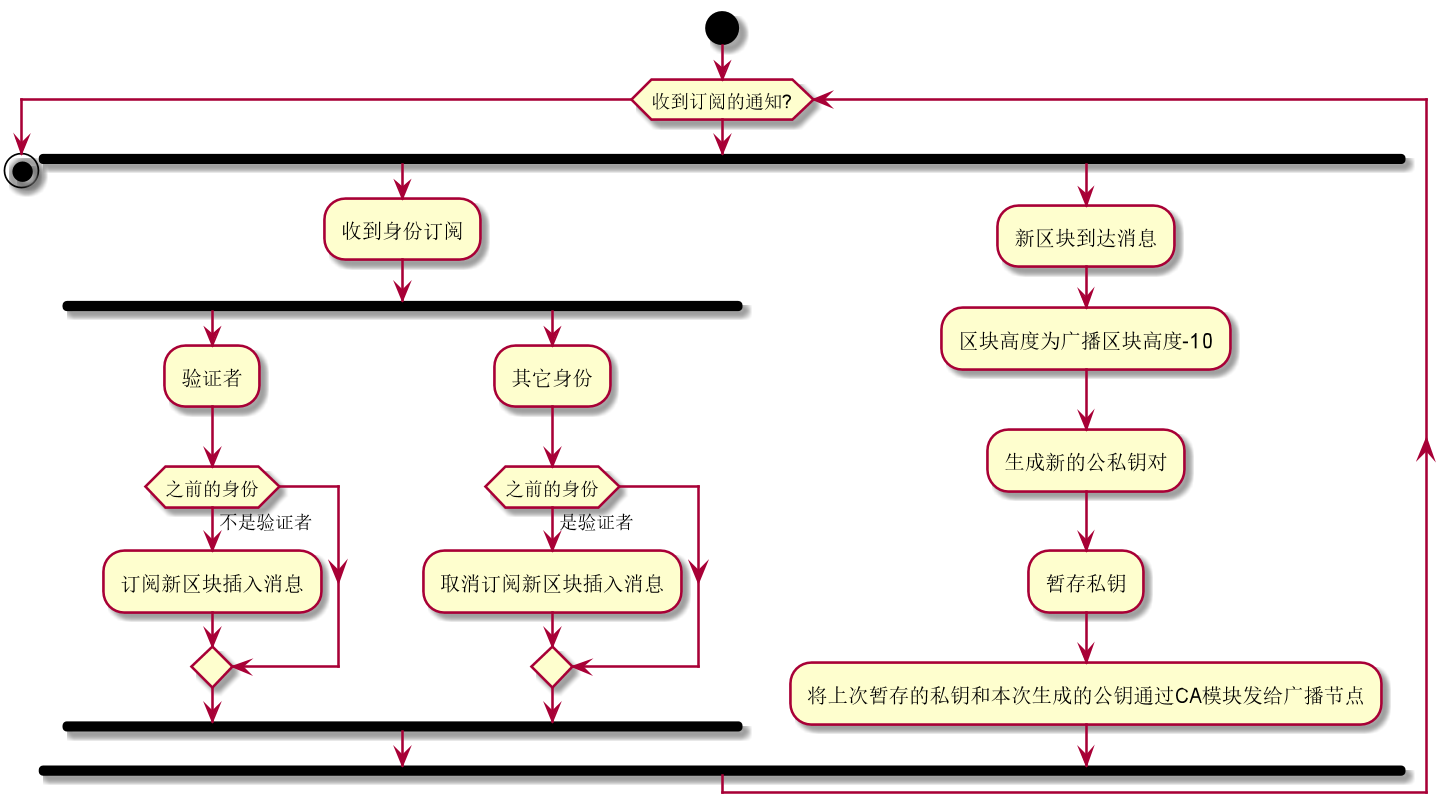
* 输入：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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

* 功能：

所有节点在广播区块读取广播节点写入的私钥之和

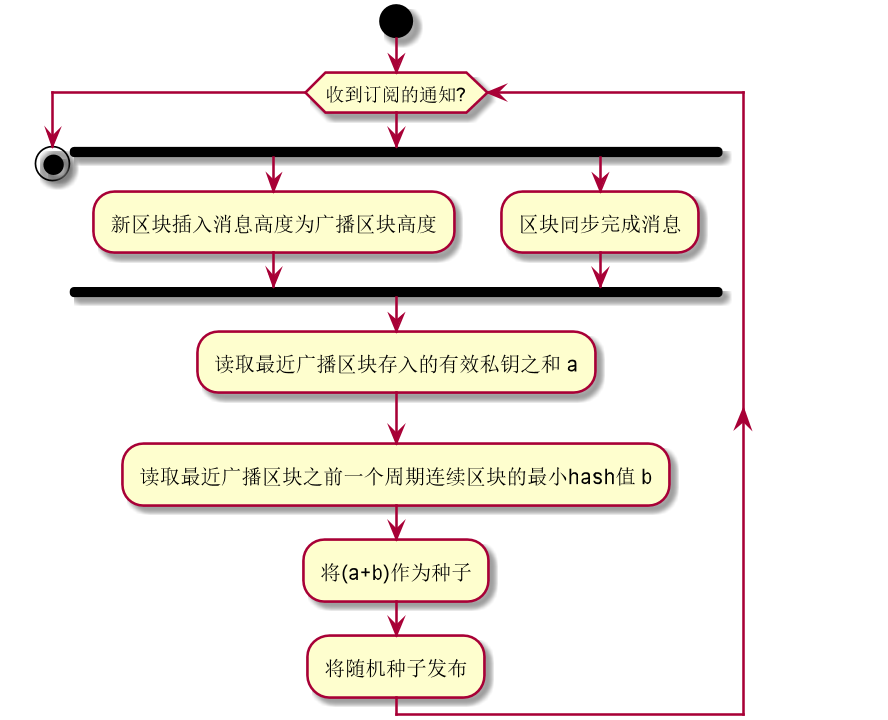
* 输入：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 名称 | 消息码 | 消息体 | 来源 | 实现方式 | 备注 |
| 区块同步完成消息 | 无 | 无 | 内部downloader | 消息订阅 |  |
| 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 |
| 随机种子 | 待定 | Byte类型 | 消息订阅 |  |

## 流程图



# 拓扑生成服务



* 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

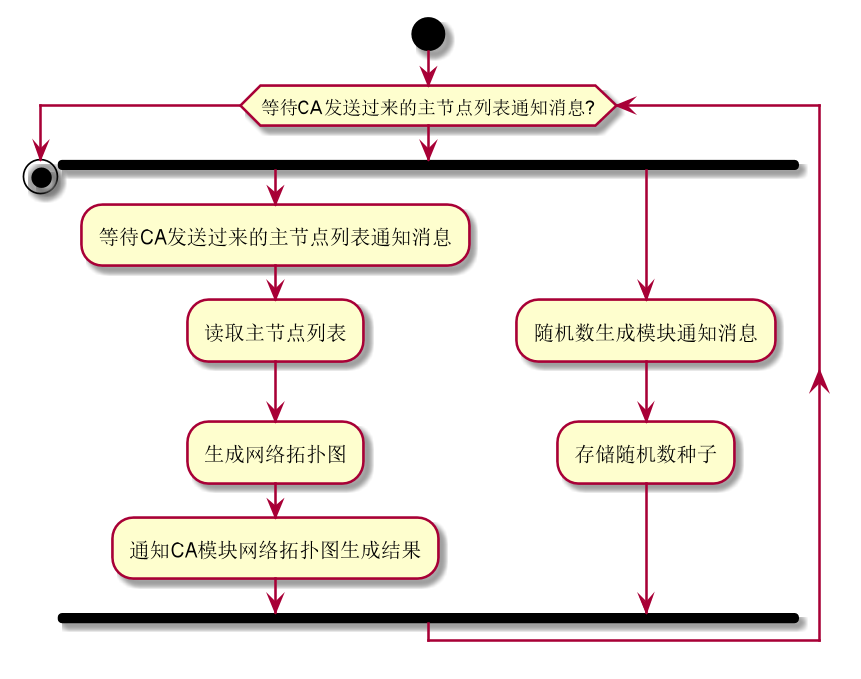
* 输入：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 名称 | 消息码 | 消息体 | 来源 | 实现方式 | 备注 |
| 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



# 广播生成服务

# 投票服务



* 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

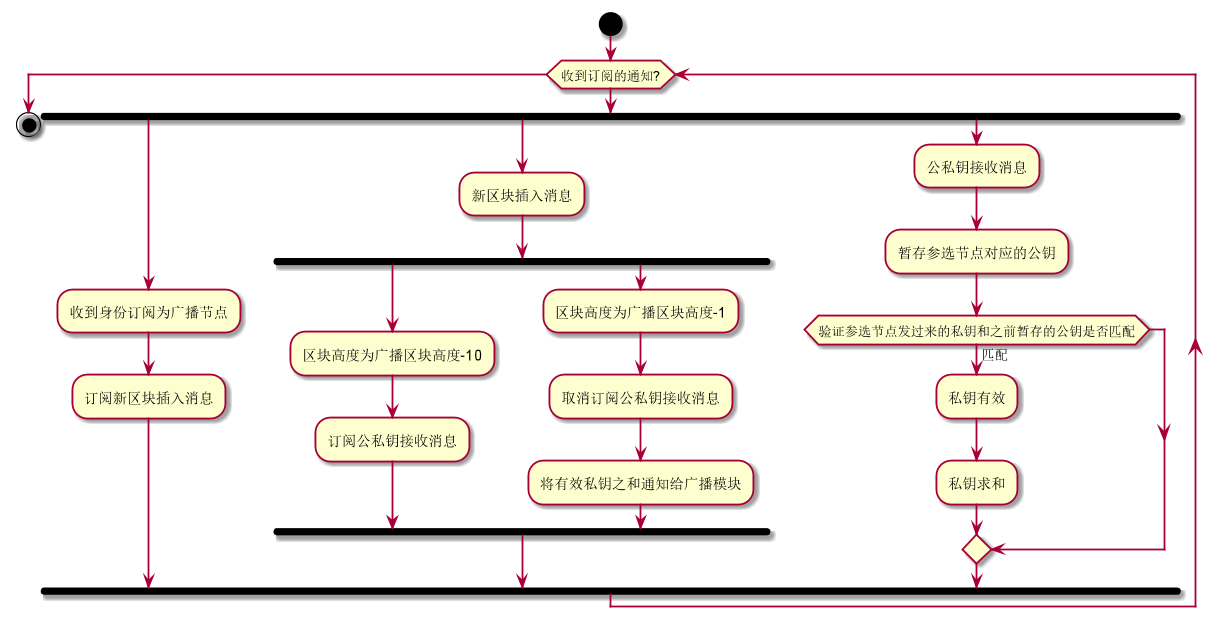
* 输入：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 名称 | 消息码 | 消息体 | 来源 | 实现方式 | 备注 |
| 投票消息 | 待定 | 公司钥对 | 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



# Leader身份服务



## Leader身份计算服务

* 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 |
| Header验证完毕消息 | 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 |
| 更换leader结果消息 | 待定 | NodeID字符串 | Leader更换控制服务 | 消息订阅 | 字符串为空表示当前无leader |

* 输出：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名称 | 消息码 | 消息体 | 实现方式 | 备注 |
| Leader变更消息 | 待定 | NodeID字符串 | 消息通知 | 字符串为空表示当前无leader |
| 当前Leader查询接口 | 无 | NodeID字符串 | 接口 | 同上 |
| 某轮次Leader查询接口 | 无 | NodeID字符串 | 接口 | 某轮次正常状态下的leader，不能为空 |

## 更换leader控制服务

* 功能：

控制更换leader的流程，包括何时启动leader模式、follower模式下的更换服务及最后更换结果的通知。

* 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 |
| Header验证完毕消息 | 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 |
| 更换leader成功消息 | 待定 | 包含Leader差距值和投票列表 | CA服务 | 消息订阅 | 经过CA验证来自合法validator |
| 某轮次Leader查询接口 | 无 | NodeID字符串 | Leader身份计算服务 | 接口调用 |  |

* 输出：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名称 | 消息码 | 消息体 | 实现方式 | 备注 |
| 更换Leader结果消息 | 待定 | NodeID字符串 | 消息通知 | 字符串为空表示当前无leader |
| 启动消息 | 待定 | 主持更换流程leader的NodeID | 消息通知 |  |
| 停止接口 | 待定 | 无 | 消息通知 |  |

## Follower模式下的更换服务

* 功能：

更换leader流程中，自己扮演follower角色情况下的处理流程。主要响应主持更换的leader的请求。

* 输入：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 名称 | 消息码 | 消息体 | 来源 | 实现方式 | 备注 |
| 启动消息 | 待定 | 主持更换流程leader的NodeID | 更换leader控制服务 | 消息订阅 |  |
| 停止消息 | 待定 | 无 | 更换leader控制服务 | 消息订阅 |  |
| 更换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 |

* 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 |

## Leader模式下的更换服务

* 功能：

更换leader流程中，自己扮演leader角色情况下的处理流程。主要发出更换leader请求并收集投票结果。

* 输入：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 名称 | 消息码 | 消息体 | 来源 | 实现方式 | 备注 |
| 启动消息 | 待定 | 主持更换流程leader的NodeID | 更换leader控制服务 | 消息订阅 |  |
| 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 |
| 更换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 |
| 更换leader成功消息广播 | 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  需要同时发送给自己 |

# 区块POS验证服务



## POS投票服务

* 功能：

对区块头进行验证并进行投票

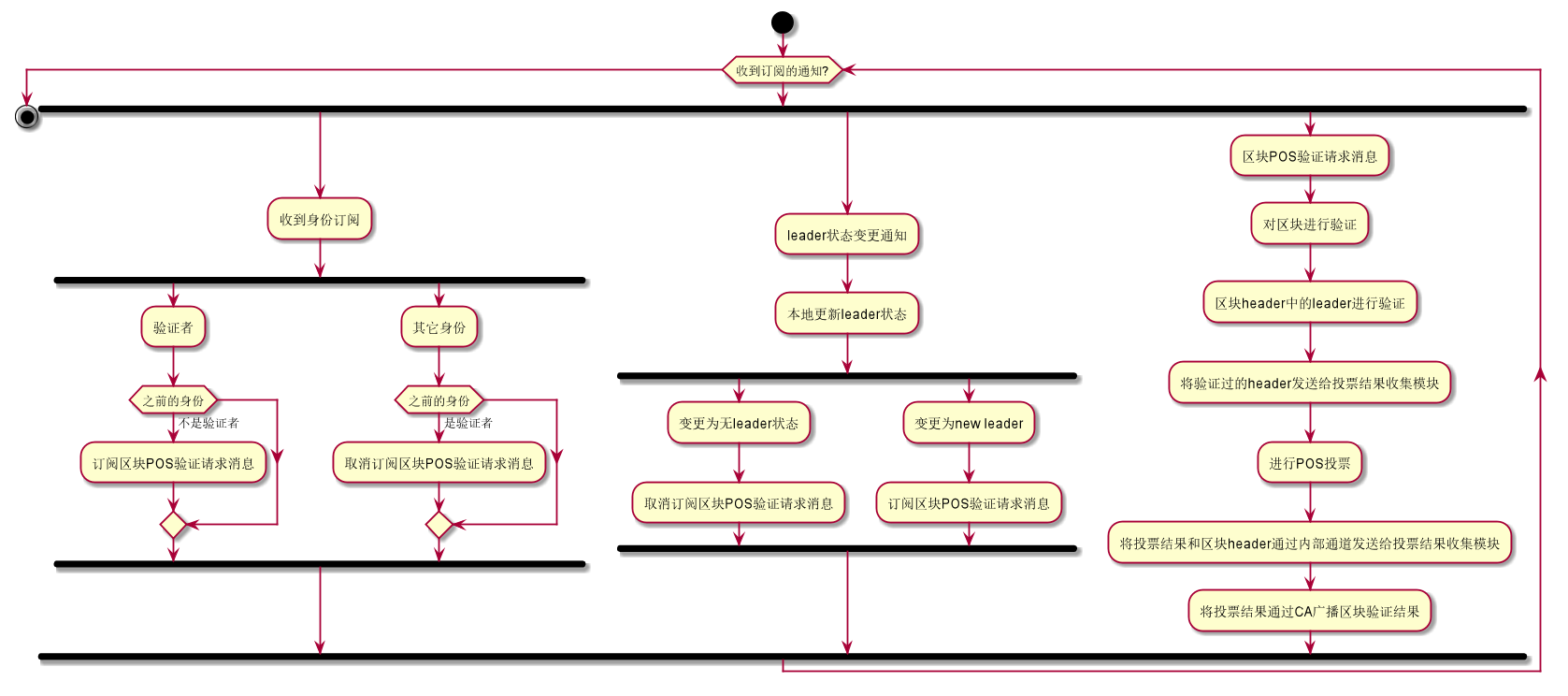
* 输入：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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 |
| 更换leader结果消息 | 待定 | NodeID字符串 | Leader更换控制服务 | 消息订阅 | 字符串为空表示当前无leader |
| 区块POS验证消息 | 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 |

## 流程图



## POS结果收集及验证服务

* 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

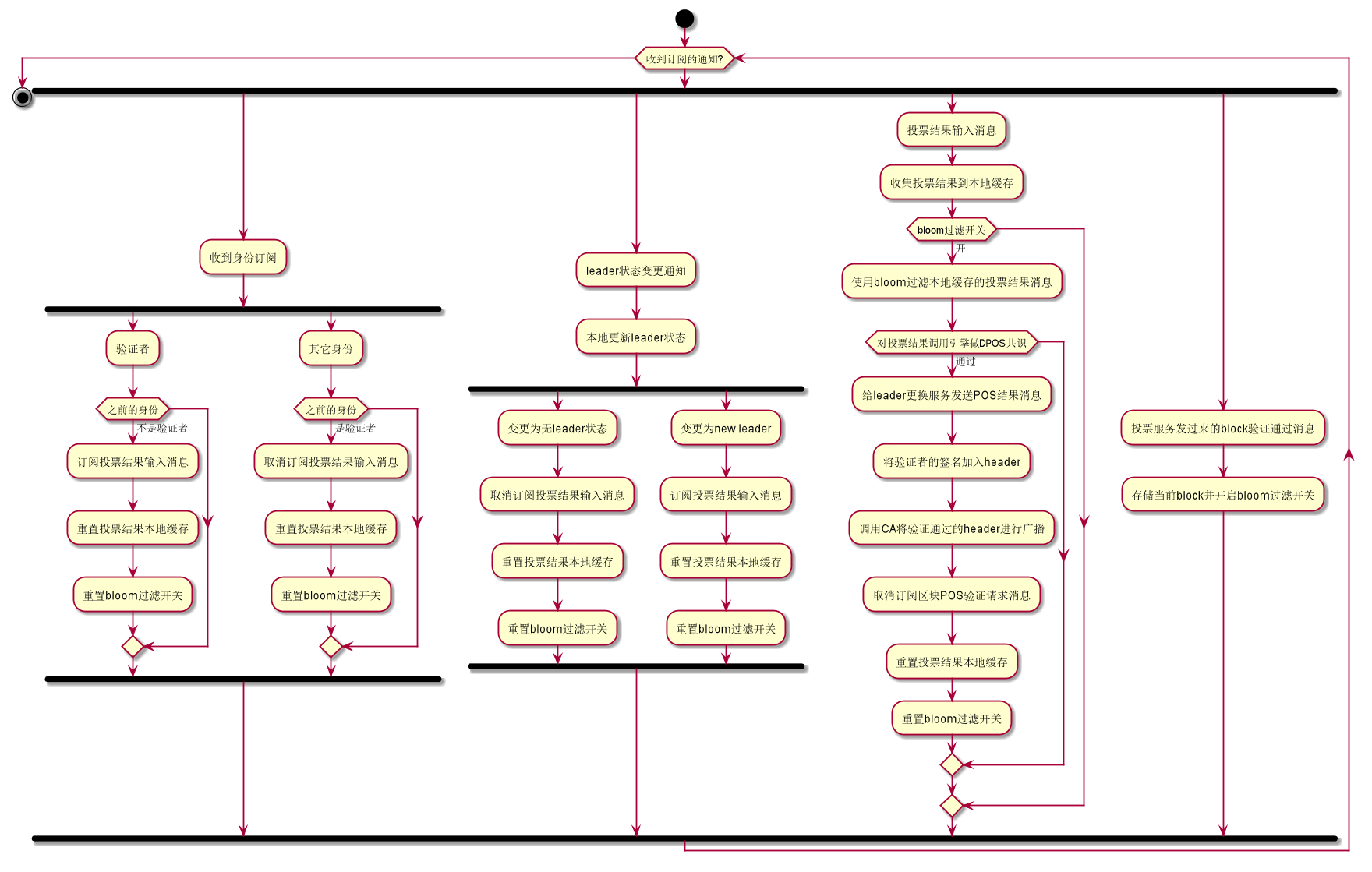
* 输入：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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 |
| 更换leader结果消息 | 待定 | NodeID字符串 | Leader更换控制服务 | 消息订阅 | 字符串为空表示当前无leader |
| 投票结果输入消息 | 待定 | 签名 | CA服务 | 消息订阅 |  |
| 投票服务验证成功通知 | 待定 | Heard | 投票服务 | 消息订阅 |  |

* 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



# 区块生成服务



其中leader的轮换启动是由矿工输入驱动的，而不是由新区块到达驱动。这个部分有待进一步讨论，看是否能调整为由新区块到达驱动，从而和其他部分保证一致性

## 挖矿结果验证服务

* 功能：

缓存POS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 |
| POS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

* 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 |  |

## 广播区块生成服务

* 功能：

打包广播区块，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 |  |
| 广播区块信息消息 | 待定 | 信息待定 | CA服务 | 消息订阅 | 广播节点发来的广播区块信息，需要经过CA验证 |
| 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POS验证header生成服务

* 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POS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 |