Matrix共识算法设计(2018-06-27)

参与者以及职能：

矿工(Miner)：收集子节点的交易数据，并发送给验证者(Validator)。打包区块。有否决打包区块的权力

验证者(Validator)：收集其它节点发来的交易数据，验证交易是否有效，验证区块是否有效，广播区块。

验证者Leader：Leader收集验证通过的交易数据，打包交易，生成新的区块，发送给矿工(Miner)打包

区块验证方法：

Leader提供的验证block信息：

1. Block Header： ParentHash、 UncleHash、 Root、 ReceiptHash、 Bloom、 Difficulty、 Number、 Time、 GasLimit、 GasUsed
2. Block Tx Hash

验证者验证消息：

1. ParentHash是否为最后一个签名确认块的Hash
2. Block Tx 是否正确
3. Block Header是否有效

验证者签名信息：

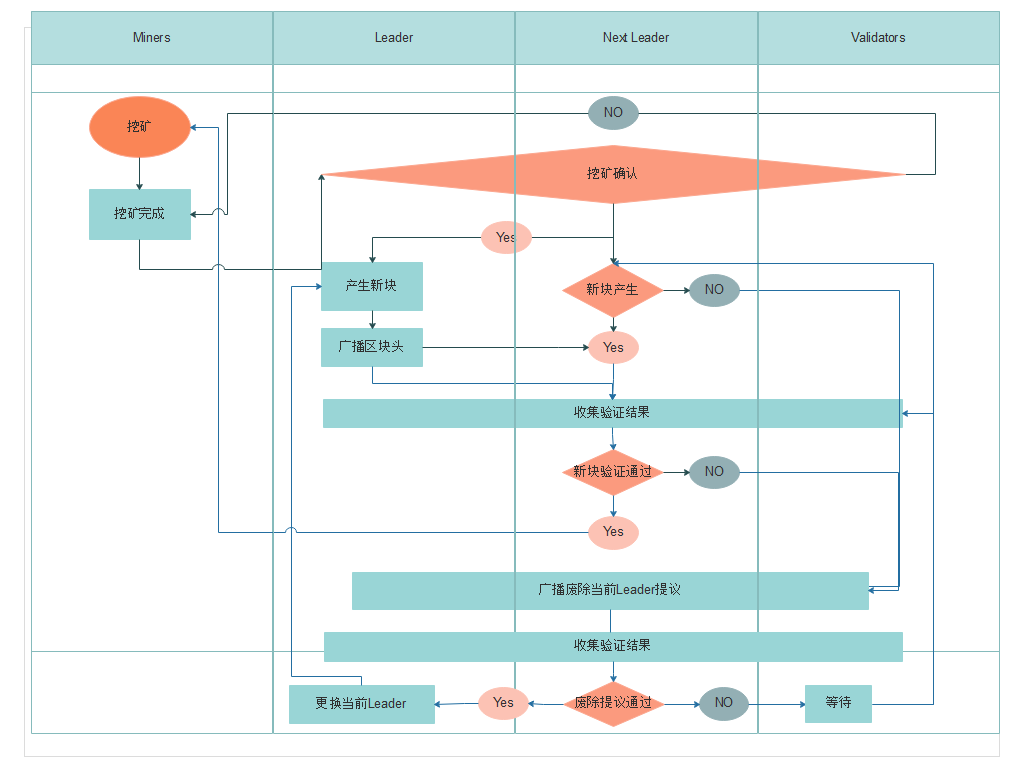
BlockHeader的hash

验证者签名判决：

1. 验证者签名广播给所有的验证者，不给矿工
2. 区块验证结果所有的验证者都知道
3. 如果验证失败，所有Validator都可以及时发起废除当前Leader的提议，而且如果Leader强行出块，下一个区块验证不通过
4. 如果验证成功，每一个Validator都向矿工广播带有75%签名结果的区块头，不会因为Leader做恶而不出块
5. 矿工根据BlockHeader可以确定签名正确与否。Leader不能伪造签名。只能拿旧的区块回放，矿工知道当前区块高度，拒绝挖旧的区块
6. 当前区块验证由下一个Leader验证，必须得到有效区块才能开始新一轮的区块验证

区块结构

挖矿流程（交易验证流程与挖矿流程并行）



共识算法设计：

线程1：交易广播与验证

1. Miner向Validator广播交易
2. Validator之间交易验证

线程2：区块验证与挖矿

1. Miner挖出上一个块，通知Validator
2. Validator验证通过，得到最少一个成功区块
3. Leader选择Parent Block Hash， Uncle Hash， Block Tx集合，创建新的区块
4. Leader广播Block Header，Block tx Hash集合
5. Validator验证Block Header，签名并广播给Validator
6. 所有的Validator都收到了签名验证
   1. 如果区块验证成功，各自打包区块头，包括验证信息，发给Miner
   2. 如果验证失败，或者超时，任何一个Validator都可提议废止当前Leader
   3. 全体Validator签名，共识通过则leader更换为下一个Leader，回到第3步
   4. 如果公式不通过则等待一段时间再进行一次共识
7. Miner挖新矿，回到第一步

共识算法流程图：

