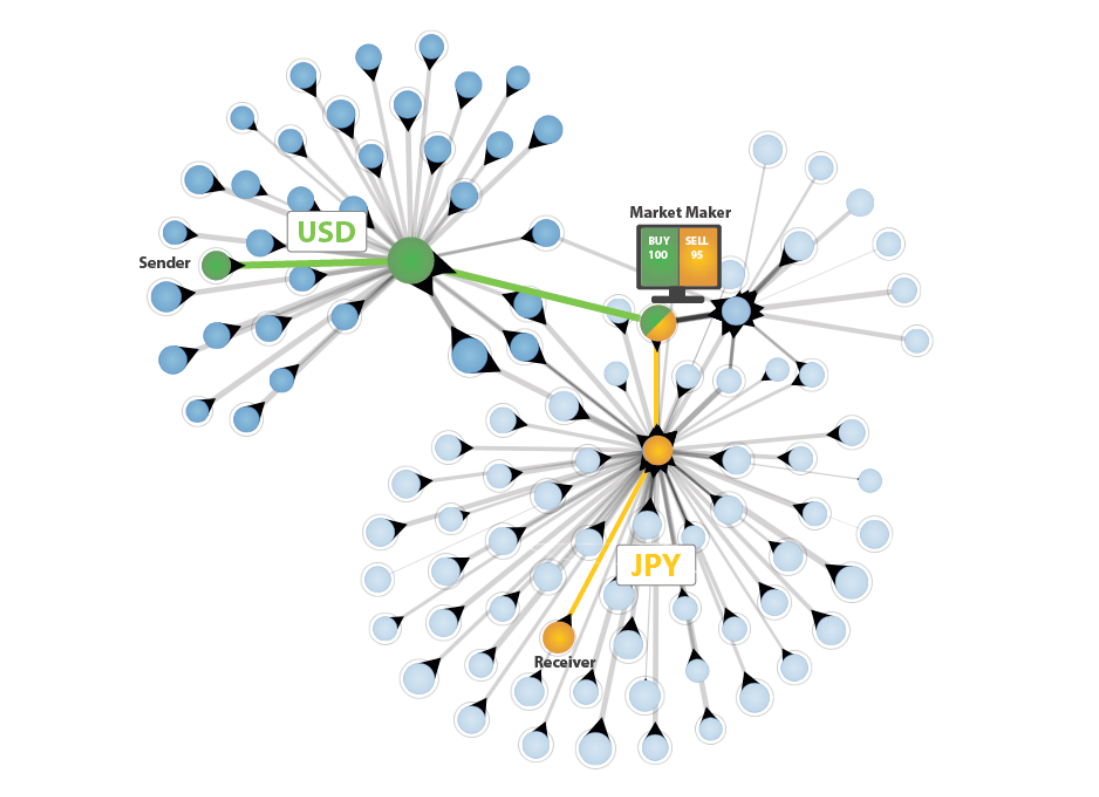
分布式系统主要面临三个方面的挑战:正确性, 一致性和可用性. 共识就是分布式系统对某个提议的结果达成一致的过程. 显而易见, 共识过程处理结果必须是正确的, 并且是可用的, 也就是在可接受时间内完成, 否则系统失去意义. 而分布式网络中共识困难在于有些网络节点是不可信的. 共识过程要满足正确性, 一致性和可靠性, 就必须能抵御坏节点(节点故障或者有意欺骗)对网络的损害. 比特币基于 \*POW\* 的共识完美解决了以上问题. 但是随着分布式加密货币技术的不断演化, 也出现了其他共识方案. 包括本文描述的 \*Ripple\* 和 \*DPOS\*, 它们和 \*POW\* 不同之处在于共识过程的时间非常短, 一般在几秒内完成, 而比特币要完全确认一笔交易需要1个小时.

# Ripple共识

Ripple是一个分布式全球结算系统, 主要用于跨货币结算. 比如你可以使用人民币支付给接收美元的接收者, 或者使用比特币支付给只接收日元的接收者等等. 你可以通过[这里](https://ripple.com/)了解Ripple系统. 本文主要对Ripple共识的\*原理\*和\*实现\*进行描述.



## 原理

Ripple共识基于生活中这样一条常识: 互不相干的一组人相互勾结串通欺诈我可能性非常低. 在Ripple网络中, 这组人叫做UNL(Unique Node List), 是节点node信任的验证者(节点接收和处理交易, 分为跟踪节点和验证节点). UNL是Ripple网络中所有节点的一个子集. 每个节点node都有自己的UNL. 这些UNL中的节点可能重合, 所有的UNL节点构成了Ripple网络.

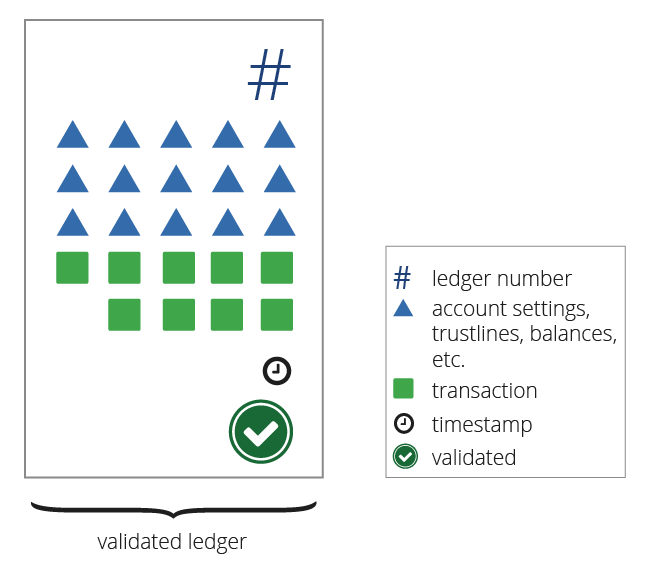
经过证明, 只要UNL中80%的节点是可信的, 并且20%的节点是联通的, 那么一致性和正确性就能够保证, 可用性也能够接受. 具体请参考[Ripple共识白皮书](https://ripple.com/consensus-whitepaper/)

## 实现

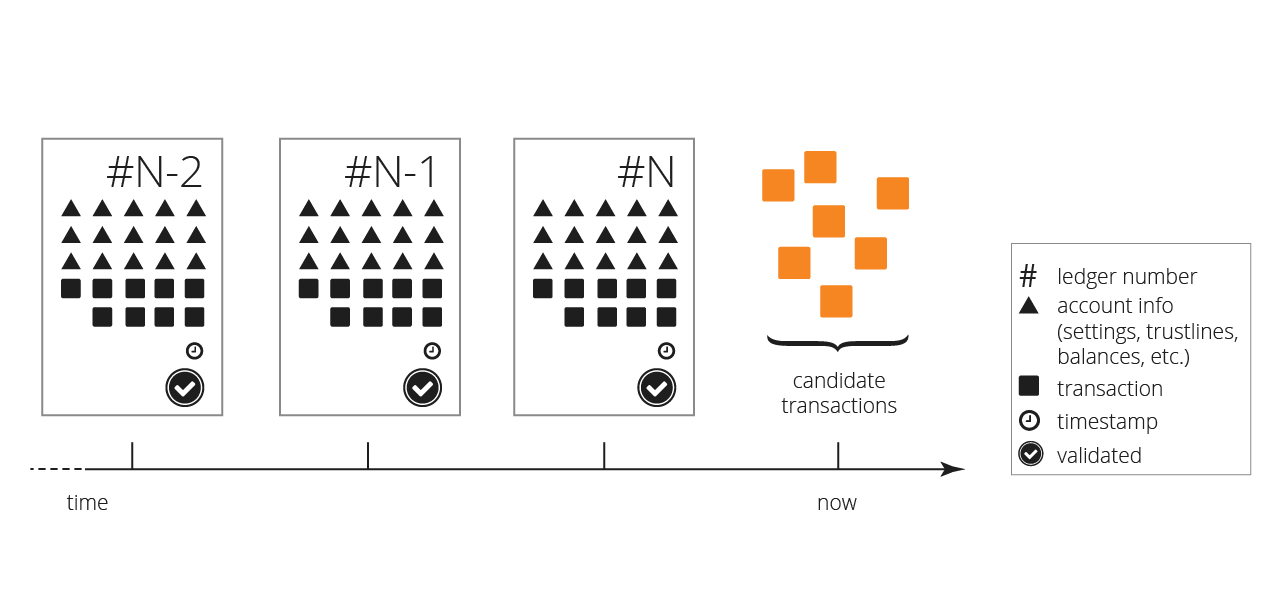
### 总账ledger

Ripple提供类似区块的结构, 名字称为账单-ledger, 总账包含如下数据:

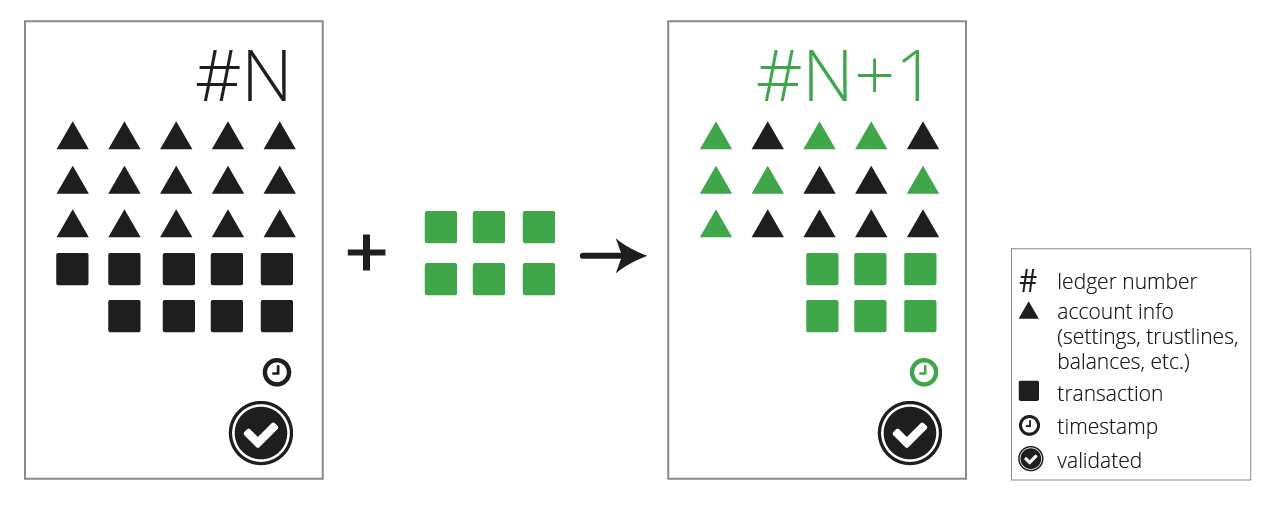
* 用户的设置
* 用户的余额
* 交易
* 时间戳



Ripple每隔几秒达成一次共识, 产生一个新的ledger. 新的交易将被放入到下一个ledger中打包. 如图:

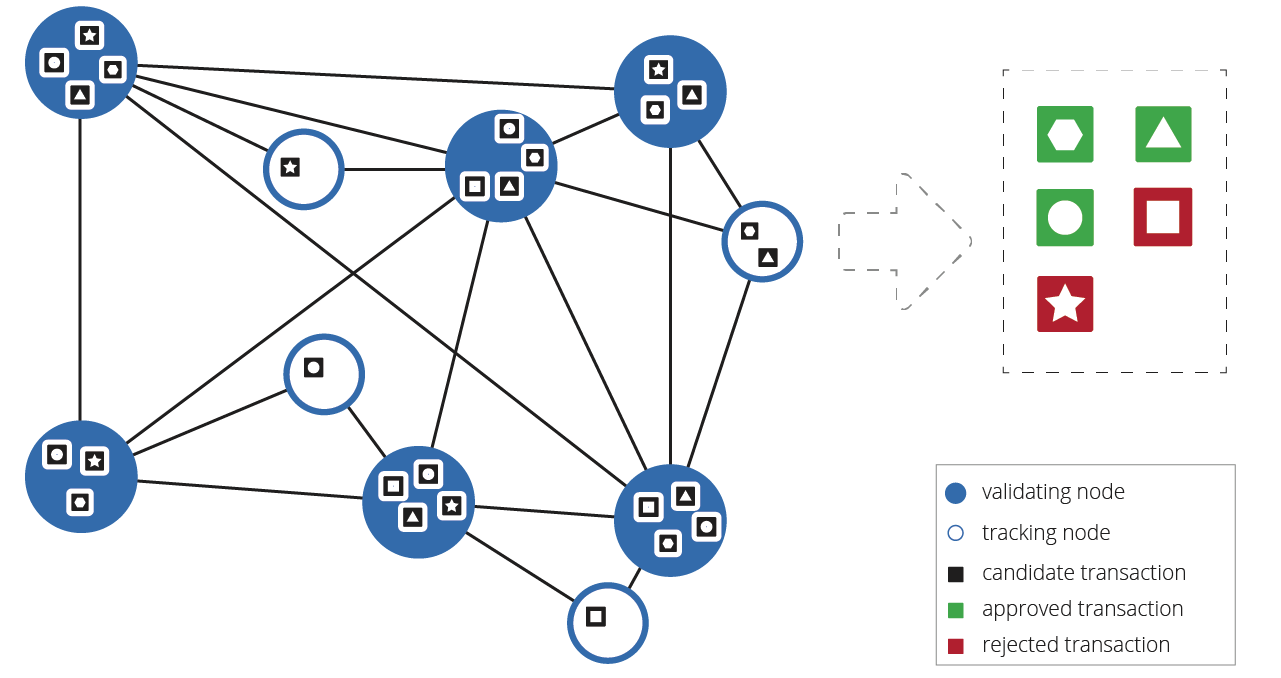


一次达成共识, 形成一个新的ledger叫做一轮. 有些交易在本轮中没有达成被确认, 需要放入下一轮, 或者丢弃(不合法), 如图:

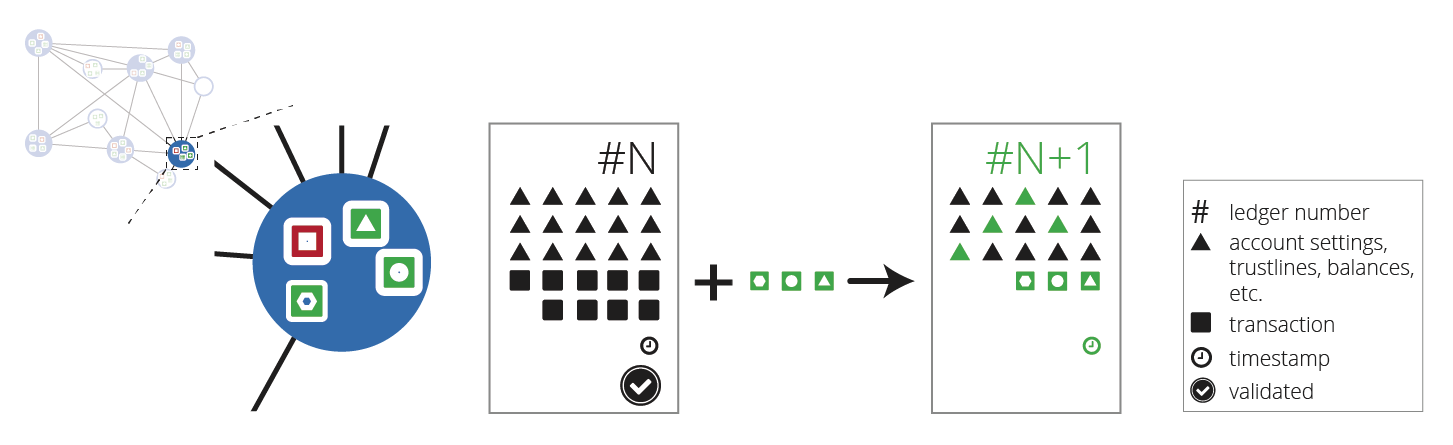


### 共识和验证

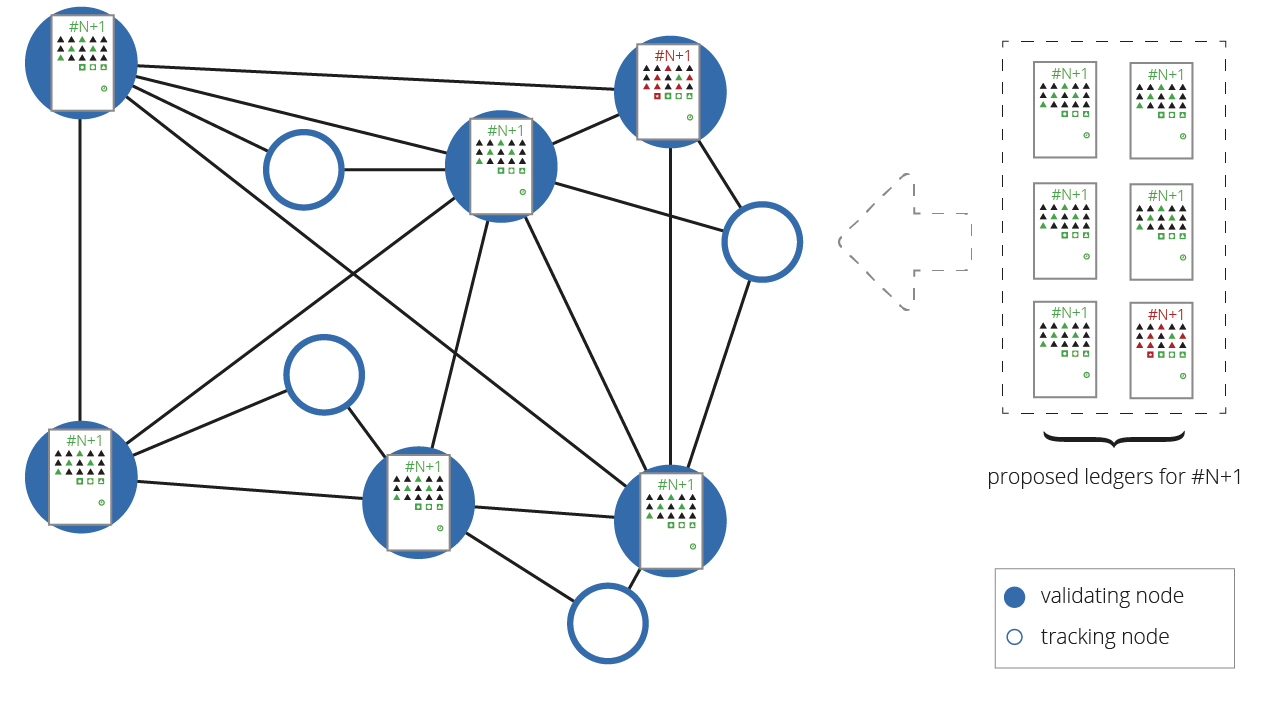
* 每个节点接收到交易, 向UNL广播, 尽力让UNL中的交易一致. 这些交易称为候选集
* 当本轮共识开始时(共识的时间间隔一般为5秒, 可设置), 每个节点向自己的UNL发出提案, 提案中包含候选集中自己认为正确的交易, 这些交易是候选集的一个子集. 节点遍历所有提案, 找出大部分(80%)UNL成员相同的交易作为入选的交易集合, 这些交易将进入下一个ledger, 没有入选的交易将进入下一轮共识.如图:



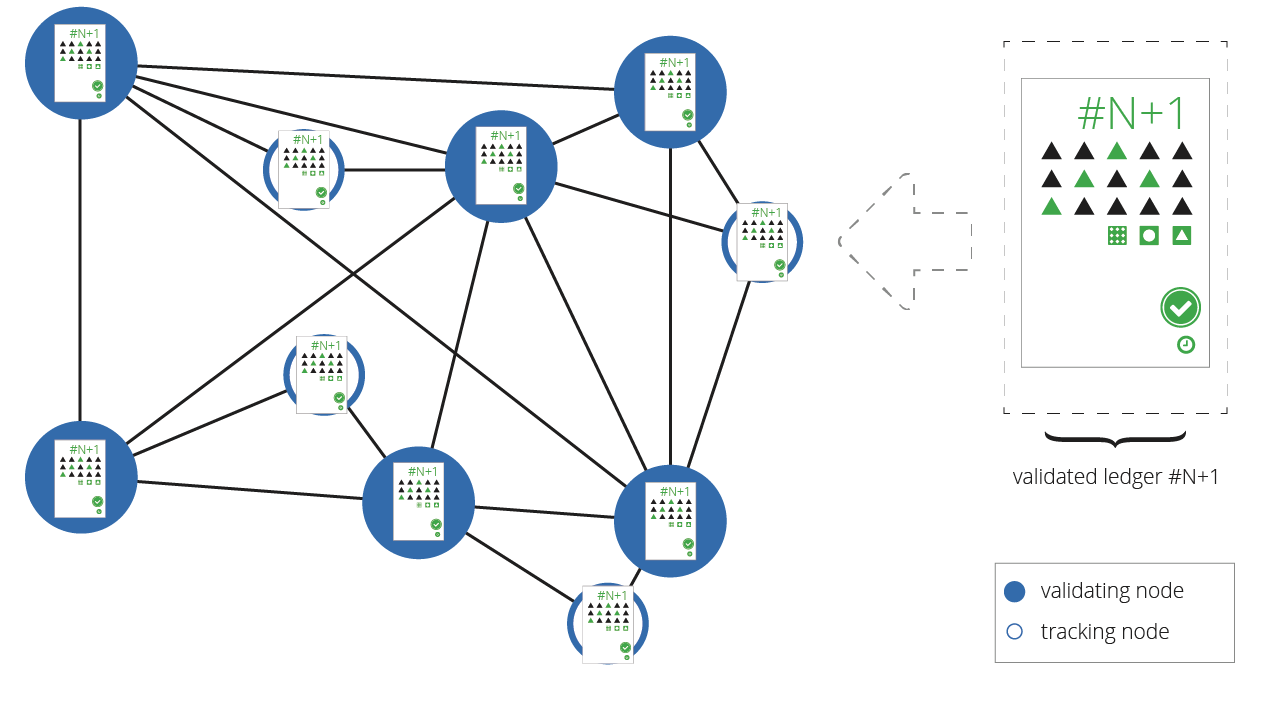
* UNL中每个节点根据入选的交易计算新的ledger:



* 每个验证节点会对新的ledger进行hash和签名, 并把签名hash广播到全网:



* 每个节点找出80% UNL中相同的hash, 这个hash对应的ledger就是新的验证的ledger.



* 如果节点自己的hash和新的ledger hash不一致, 那么它要请求新的ledger, 和全网一致.

# DPOS共识

DPOS(委托股权证明共识 Delegated Proof-of-Stake Consensus)是Bitshares采用的共识方案. Bitshares利用它建立一个智能合约平台, 有关Bitshares的详细介绍, 请参考[这里]( <https://bitshares.org/>). 本文余下的部分介绍DPOS的原理和实现.

## 原理

顾名思义, DPOS借鉴了POS(Proof-of-Stake)的思想, 更深一步, 利用股东的投票权力解决共识的问题. 可以把加密货币系统看作一家公司, 股东就是货币的持有者. 打包区块由股东票选的\*证人\*来完成. 对于网络参数的修改则由票选的股东委员会的\*委员\*来完成.

票选过程采用[同意投票]( <https://en.wikipedia.org/wiki/Approval_voting>) 的方式选出证人. 每人一票, 在证人计票时对投票股东的股权求和, 排序. 选择股东认为合理的证人数量.

## 实现

### 票选证人打包区块

票选证人过程分两步:

第一步决定证人的数量. 每个股东都提出他们认为合理的证人数量, 值越大, 系统越安全. 系统采用51% 的股东建议的数量 N.

第二步选出证人. 每个股东为他们信任的证人投票, 一个证人一票. 投票的票数和第一步中提出的证人数量应相同. 系统根据计算证人的票数权重排序, 选取前N个证人. 票数权重是投票的股东持有的核心资产余额. 比如股东a, b, c都给证人w投了票. 股东a持有2000核心资产, 股东b有3000, 股东c有5000, 那么证人w的票数权重就有2000+3000+5000=10000.

证人选出之后, 由这些当选的证人轮流打包区块. 每个证人都在固定的时间间隙内生产区块. 所有证人都打包完成是一轮. 每轮结束后,证人的顺序重新洗牌.

证人可能打包区块失败(网络原因, 或者是欺诈行为等), 那么由下一个证人代替他完成.

证人每打包一个区块, 都会获取一定数量的费用. 如果打包失败, 不会获取.

每个股东都可以选择修改证人数量, 以及投票新的证人或者撤销之前证人的投票.

证人列表周期性更新(每天一次), 来体现股东的选择.

### 票选委员修改网络参数

委员的选取过程和证人相同. 不同的是委员职责是修改网络参数, 这些参数包括交易费用, 区块大小, 证人打包费用等等.

大多数委员同意修改建议后, 股东被授予两周时间的审查周期. 在这个期间内, 委员可能被踢出委员会, 或者废除修改建议.

委员不被支付, 因为网络参数不会频繁修改.