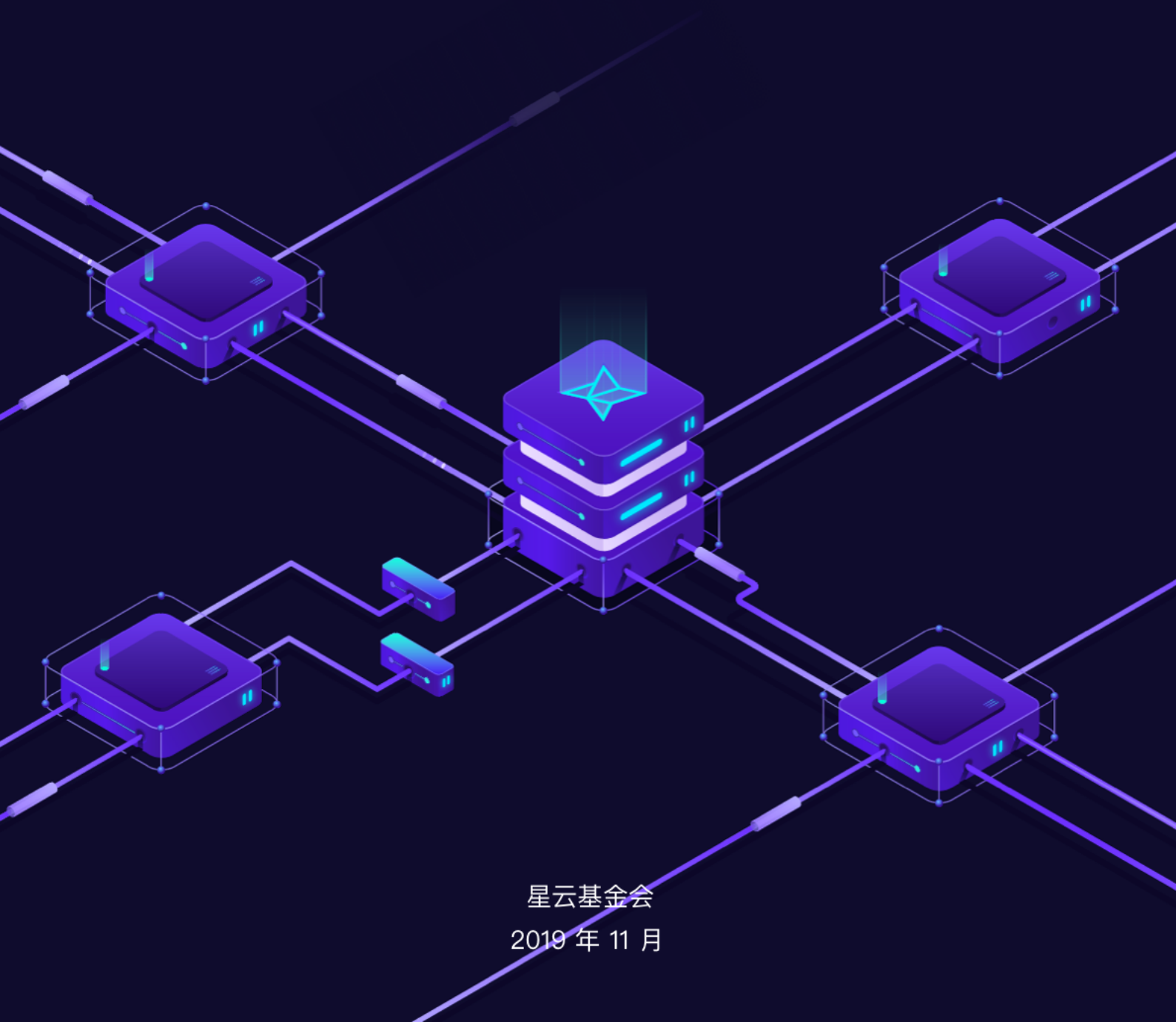


星云节点计划

基于贡献度证明机制 (PoD)

V 1.0



目录

概述	2
1. 贡献度证明机制（PoD）概述	3
1.1 设计目标	3
1.2 构成	3
1.3 激励分配	4
1.4 载体：NAX	5
2. 共识机制	6
2.1 节点入选基础条件	6
2.2 节点选取规则	7
2.2.1 候选节点综合排名算法	8
2.2.1.1 NAX投票数	8
2.2.1.2 出块稳定指数	8
2.2.2 共识节点选取算法	9
2.3 共识算法	10
2.3.1 出块顺序	10
2.3.2 打包出块	10
2.3.3 区块上链确认	10
2.4 退出机制	11
2.4.1 撤销投票	11
2.4.2 节点退出	11
2.5 惩罚和应急响应	12
2.5.1 惩罚	12
2.5.1.1 出块惩罚	12
2.5.1.2 治理惩罚	13
2.5.2 应急响应	13
3. 治理机制	14
3.1 治理委员会	14
3.2 治理范围	14
3.2.1 社区协作	14
3.2.2 社区资产	16
3.2.3 共识机制惩罚	17
3.3 治理手段：投票	17
3.3.1 投票周期	17
3.3.2 投票方法	17
3.3.3 投票结果处理	18
3.4 惩罚机制	18

3.4.1 单个治理节点惩罚	19
3.4.2 治理失效	19
4 路线图	20
附录	21
附录A 推荐硬件配置和环境	21
附录B 节点共建	21
附录C 收益模拟	22
附录D 注释	22
附录E 参数表	24
E.1 基本参数	24
E.2 共识机制相关参数	24
E.3 治理机制参数	25
E.4 激励分配参数	25

概述

星云节点计划是星云愿景的实践：让每个人从去中心化协作中公平获益^[1]。推动自治元网络（Autonomous Metanet）^[2]落地。

该计划核心为贡献度证明机制（Proof of Devotion，以下简称PoD）^[3]，可以简单地概述为以社区贡献者贡献大小为基础构建的机制，包括共识机制和治理机制两部分。通过节点选取组建共识委员会，实现主网节点去中心化；并由优质节点组成的治理委员会以代议制的形式组织社区治理。星云将构建全新的面向复杂数据网络的去中心化自治组织（Decentralized Autonomous Organization, DAO）^[4]。

1. 贡献度证明机制（PoD）概述

1.1 设计目标

要建设可持续发展的良性公链生态，需要同时兼顾共识机制的快速和不可逆性，以及治理的公平性。

当前我们面对新的应用场景，信息交互从单一、简单的功能向复杂、多样发展，用户角色也越来越多。协作场景已经从人与人面对面合作，升级到全球化的跨越多地区、并有多组织参与的协作。协作的目标结果也更为多变，成果从实物到虚拟，协作的时间跨度也变得更长、更灵活^[5]。

要保证新应用场景的治理公平性，需要采用新的协作方式。传统的中心化治理无法应对复杂的新场景。面对复杂的数据交互形态和丰富的用户角色，中心化的单一评判标准很难做到广而全面，有相当的局限性。

而传统的去中心化协作方式因为没有考虑到更多角色的存在引起的新的利益分配情况，或多或少存在利益分配不均、无法长期良性发展或者发展缓慢的情况。

如何保障社区成员的利益，让生态沉淀出价值深度，是星云在思考和实践的方向。在优先保证效率和不可逆的前提下，我们设计PoD就是为了从贡献度角度出发，尽可能追求公平性，维护社区用户的利益。

1.2 构成

PoD可以简单地概述为以社区贡献者贡献大小为基础构建的机制，该机制包括共识机制和治理机制两部分。参见图1.1。

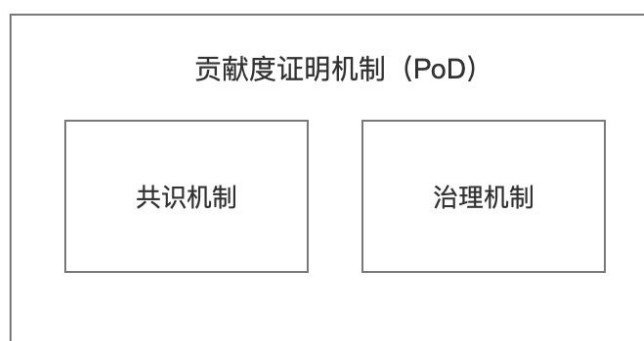


图1.1 PoD构成

PoD的人员组成涉及两个执行委员会：共识委员会和治理委员会。

- 共识委员会：共识机制由共识委员会执行。共识委员会通过综合排名算法从所有节点中选出。
- 治理委员会：治理机制由治理委员会落实而治理委员会由共识委员会中贡献最大的共识节点组成。

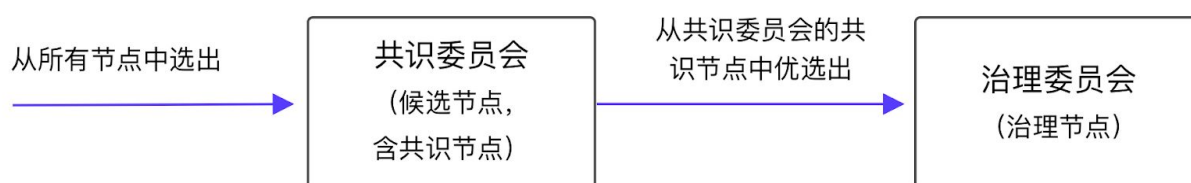


图1.2 PoD执行委员会

1.3 激励分配

自2018年3月31日星云主网上线以来，临时共识机制DPoS^[6]每日全网产生8,219.1744 NAS记账收入，每年全网产生2,999,941 NAS。这部分记账收入将全部用于星云节点计划。其中，共识机制和治理机制两部分的激励比例约为5:1。即：

1. 每年全网共识机制激励总量：2,499,951 NAS
2. 每年全网治理机制激励总量：499,999 NAS

共识机制激励由共识委员会轮询周期内出过块的共识节点均分。没有入选共识节点的候选节点在该周期内没有激励。

治理机制激励由治理委员会治理周期内参与过**所有**投票的治理节点均分。没有参与或只参与过部分投票的治理节点在该周期内没有激励。

1.4 载体：NAX

贡献度证明的载体是NAX^[7]。NAX仅可以通过去中心化质押（dStaking）^[8]的方式，质押NAS而得。根据《星云链NAX白皮书》^[9]所述，NAX采用动态分发策略，实际总发行量与全局质押率相关，某地址获得NAX的数量与NAS质押量以及币龄相关，可以看作是衡量了该地址对社区作出的持币贡献。因此，NAX可以被看作为星云生态的贡献有效凭证。

在星云社区协作平台Go Nebulas（go.nebulas.io）上，也将以NAX作为生态贡献激励，鼓励社区成员建设社区。

2. 共识机制

共识机制使用智能合约自动管理，主要由节点选取规则和共识算法两部分组成，联合完成出块，保障主网正常运行。

星云链平均出块时间为15秒。设定每个轮询周期内，21个共识节点轮番出块，每个节点出块10个。故一个轮询周期默认为**210个区块高度**，约为52.5分钟。每个轮询周期内的共识机制执行流程如下图所示：

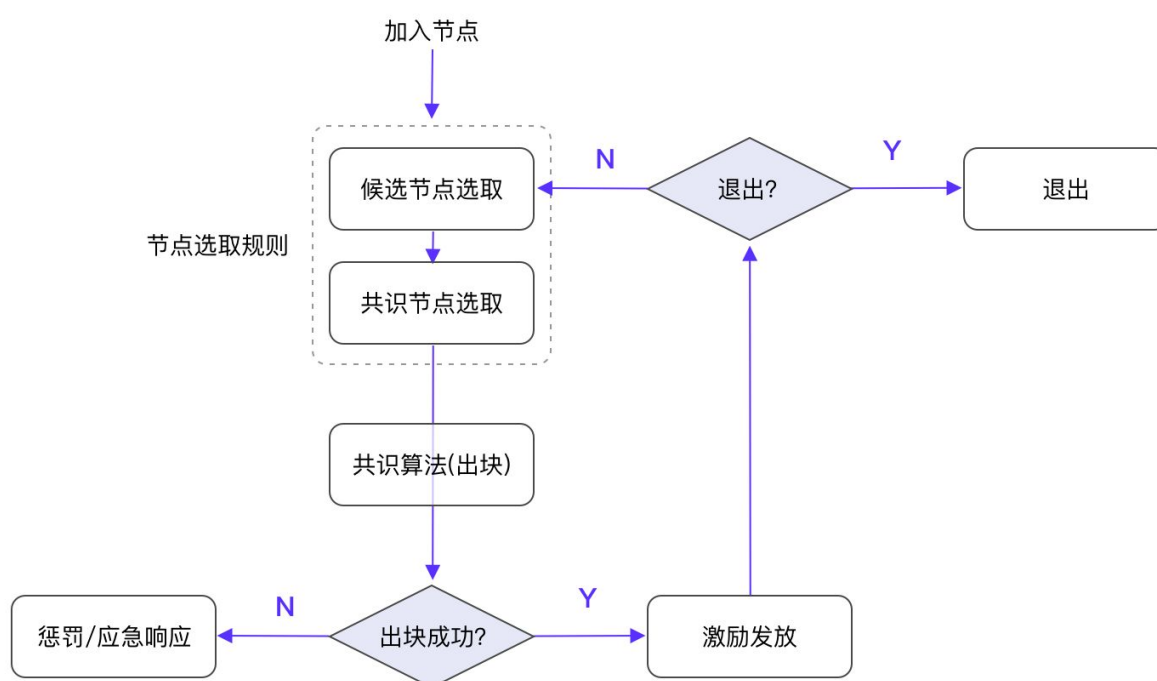


图2.1 每个轮询周期的共识机制执行流程

2.1 节点入选基础条件

任何个人或组织均可申请成为节点，必须满足以下所有要求才有资格参与候选节点选取：

- 服务器满足基本要求（参见[附录A 推荐硬件配置](#)）；
- 服务器保证运行中；

- 质押（即投票）不小于10万NAX；
- 保证金质押2万NAS；
- 没有高安全等级作恶记录（参见[2.5.1 惩罚](#)）

2.2 节点选取规则

节点选取规则包括两个步骤：

1. **候选节点选取**：在每个轮询周期内，在满足基本入选要求的所有节点中，按候选节点综合排名算法，选出51个候选节点；
2. **共识节点选取**：在每个轮询周期内，按共识节点选取算法，在稳定且最能代表用户权益的一组候选节点中选出21个共识节点。共识节点负责出块，可以获得共识机制激励。

候选节点和共识节点共同构成共识委员会。选取流程如下图所示：

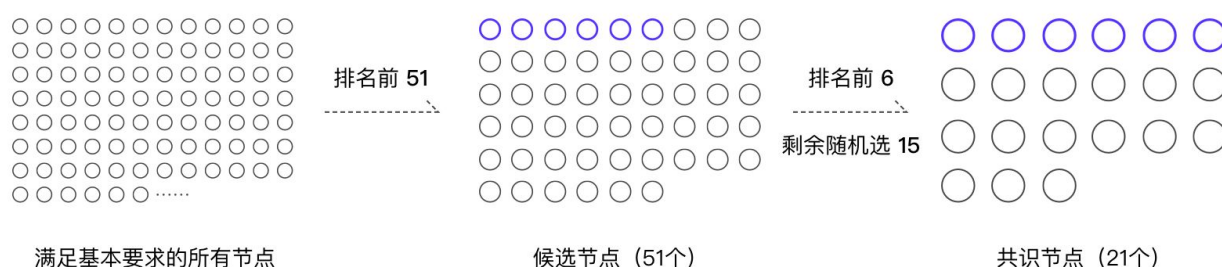


图2.2 节点选取流程

2.2.1 候选节点综合排名算法

在满足申请节点基本要求（[2.1 节点入选基础条件](#)）的前提下，将所有节点按候选节点综合排名算法进行排名，靠前的51个节点为候选节点。候选节点综合排名算法参考两个因素：NAX投票数 $V_{(i)}$ 和出块稳定指数 $S_{(i)}$ 。候选节点综合排名指数 $R_{(i)}$ 为：

$$R_{(i)} = V_{(i)} \times S_{(i)}$$

假设 $S_{(i)}$ 相同，NAX投票数 $V_{(i)}$ 也相同，则最先达到NAX投票数 $V_{(i)}$ 的节点入选。

2.2.1.1 NAX投票数

NAX投票数 $V_{(i)}$ ：所有社区成员和节点负责人都可以向支持的节点投出NAX，助力该节点提升排名。

2.2.1.2 出块稳定指数

出块稳定指数 $S_{(i)}$ ：由共识节点成功出块的比率决定。未出过块的节点初始值 S 为0.8。在每个轮询周期内，一个候选节点有未参与出块、成功出块、漏出块三种情况。

A 未参与出块

未参与出块的候选节点下一周期的 $S_{(i+1)}$ 为：

$$S_{(i+1)} = S_{(i)} + 0.01$$

如果该节点持续未参与出块， $S_{(i)}$ 最高恢复到初始值 $S=0.8$ 。

B 成功出块

共识节点在一个轮询周期内需要出块10个。如果10个块全部出了则下一周期的 $S_{(i+1)}$ 为：

$$S_{(i+1)} = S_{(i)} + 0.1 \quad (S \leq 1)$$

$S_{(i)}$ 逐步提升到1。一般情况下，稳定出块的节点 $S_{(i)} = 1$ 。

C 漏出块

如果该共识节点发生漏出块的情况，则下一周期的 $S_{(i+1)}$ 为：

$$S_{(i+1)} = S_{(i)} \times (10 - C) / 10$$

其中， C 为漏出块个数。 C 越大， $S_{(i)}$ 值约低。如果 $S_{(i)}$ 降至阈值 K （ K 初始值为0.5），则该共识节点在未来20个轮询周期中都不能入选候选节点，详见[2.5.1 惩罚](#)。

2.2.2 共识节点选取算法

共识节点从51个候选节点中选出。从候选节点中选取共识节点的具体方式如下：

1. 排名前6的候选节点直接入选。
2. 剩余15个共识节点的名额按如下公式从排名第7到第51名的候选节点中选取：

$$R_{\text{Consensus}} = (R_{(i)} / \text{Sum}(R)) \times \text{Random}()$$

各参数说明如下：

$R_{\text{Consensus}}$ ：共识节点排名指数。

$R_{(i)}$ ：候选节点综合排名指数。 $R_{(i)}$ 已经综合了两个因素：NAX投票数 $V_{(i)}$ 和出块稳定指数 $S_{(i)}$ ，故可以认为 $R_{(i)}$ 同时考虑了节点的社区支持度和历史出块贡献。

$\text{Sum}(R)$ ：51个候选节点的综合排名指数总和。 $R_{(i)}/\text{Sum}(R)$ 可以看作是该节点的贡献度在所有51个候选节点中的占比。

$\text{Random}()$ ：随机概率。

2.3 共识算法

共识算法基于DPoS共识机制，通过共识委员会共识节点调度生产下一个轮询周期的区块。21个共识节点轮流出块。在一个轮询周期结束后，切换到下一个轮询周期的共识节点，轮流出块。

区块确认使用BFT^[10]共识保证区块上链的一致性，以实现PoD的稳定性、公平性和安全性。

2.3.1 出块顺序

一个轮询周期内的出块顺序由21个共识节点经过VRF^[11]随机排序。在每个轮询周期内，负责出块的共识节点和顺序始终保持不变。

2.3.2 打包出块

共识节点在出块时会打包交易缓存池中的交易。具体方式如下：

1. 共识节点严格按照该轮询周期内的出块顺序和时间打包出块；
2. 在打包时间内尽可能多的打包未上链交易；
3. 优先打包GasPrice高的交易；
4. 不可上链的交易在执行失败后会被丢掉。

2.3.3 区块上链确认

共识节点的区块上链确认保证了链的一致性和安全性，并对作恶节点进行惩罚。区块上链遵循如下规则：

1. 优先选取最长子链作为最优链；
2. 在长度一致的子链中按哈希排序选择最优链；
3. 最后不可逆区块使用BFT共识需要 $\frac{2}{3}+1$ 的共识节点确认；
4. 对非出块时间出块，双花等攻击采取惩罚机制（参见[2.5.1 惩罚](#)）。

2.4 退出机制

PoD的投票是公平的自由博弈场景。所有社区成员都可以随时申请撤销NAX投票或退出节点选取。

2.4.1 撤销投票

所有社区成员或组织，可以随时发起撤销投票的申请。当撤销投票申请成功提出后，该节点的NAX投票数（[2.2.1.1 NAX投票数](#)， $V_{(i)}$ ）即刻下调，即时影响下一轮询周期该节点排名。按照[2.1 节点入选基础条件](#)，如果NAX投票数低于10万NAX，该节点无法入选候选节点。

所撤销投票的额度：可以任意设置。但所有社区成员或组织只能申请撤销自己投出的NAX。

NAX返还时间：撤销投票申请成功提交后120个轮询周期（约为5天）后返还NAX至原地址。

2.4.2 节点退出

所有节点都可以随时退出。一旦选择退出，该节点将即刻失去成为下一周期候选节点的资格。

保证金返还额度：一次性全额返还，不可选择额度。

保证金返还时间：节点退出申请成功提交后820个轮询周期（约为1个月）后返还NAS至原地址。

NAX返还时间：节点退出申请成功提交后120个轮询周期（约为5天）后返还所有参与者的NAX至原地址。

2.5 惩罚和应急响应

2.5.1 惩罚

2.5.1.1 出块惩罚

为了维护PoD系统的安全性，根据情节严重情况进行相应的惩罚，增加节点作恶成本。三种针对共识节点的出块惩罚如下：

安全等级	危害	举例	惩罚	
			选取限制	惩罚金
低	造成系统不流畅	发生漏出块等间断性不参与共识的情况	出块稳定指数 $S_{(i)}$ (2.2.1.2) 下降，当降至0.5以下则20个轮询周期内（约为1天）不得入选候选节点	不冻结
中	造成系统不稳定	一个周期内一个块也没出	20个轮询周期内（约为1天）不得入选候选节点	冻结5%保证金
高	威胁系统安全	同一高度出多个块或在不应出块的时候出块、女巫攻击等	永久冻结	冻结全额保证金和该节点所有NAX（含用户所投）

表2.1：共识机制安全等级表

中、高安全等级惩罚处理流程：

1. 当发生安全问题时，选取限制自动执行，并冻结相应惩罚金。
2. 在最近一个治理周期投票阶段，由治理委员会投票判定该节点惩罚是否成立。
 - a. 如果投票通过该共识节点危害PoD系统安全性的行为属实，则对该节点的惩罚有效，选取限制继续执行，冻结中的惩罚金捐赠给Go.nebulas社区协作基金（参见[3.2.2 社区资产](#)）。
 - b. 如果投票不通过，该节点未对系统安全性造成危害，则选取限制终止，出块稳定指数 $S_{(i)}$ 恢复为惩罚前的数值，已被冻结的惩罚金解冻。

具体参见3.2 治理范围的[3.2.3 共识机制惩罚](#)和[3.3.3 投票结果处理](#)。

2.5.1.2 治理惩罚

除了出块惩罚，当出块节点当选治理节点后，如果在连续2个治理周期内没有完成治理任务，则820个轮询周期内（约一个月）不能入选候选节点。详情参见[3.4.1 单个治理节点惩罚](#)。

2.5.2 应急响应

如果发生黑客攻击主网等突发事件，为了保证主网可以快速相应，降低危害，星云基金会预留应急合约管理方法，星云基金会可以即刻将有问题的地址加入黑名单，禁止该地址转账。

整个流程公开透明。紧急处理后星云基金会应回溯事件过程和处理方式，接受社区监督。

3. 治理机制

星云链关注不同角色在去中心化协作中对生态作出的贡献，治理机制是PoD的重要组成部分。治理机制是由治理委员会负责，以链上投票为主要手段，对社区协作和社区资产进行管理，从而实现社区自治的一系列机制。

3.1 治理委员会

治理机制的执行由治理委员会负责管理。治理委员会由治理节点组成。

治理周期：每820个轮询周期（约1个月）为一个治理周期。

治理节点选取：治理节点从共识委员会中选出，在一个治理周期内（820个轮询周期），出块数最多的51个共识节点有资格成为下一治理周期治理节点。如果出块数一样多，则先达到该出块数的节点排名靠前。

3.2 治理范围

3.2.1 社区协作

星云社区的提案机制是星云自治元网络的重要组成部分。当前星云社区的提案和项目都通过星云协作平台Go.nebulas（go.nebulas.io）展示和管理，所有社区成员都可以在Go.nebulas上提出自己对星云未来发展的意见和建议，提案包括但不限于^[12]：

1. 星云主网研发
2. 社区协作流程优化、治理建议等
3. 现有星云社区产品的升级迭代、Bug提报
4. 社区生态产品的开发和维护
5. 社区运营和市场拓展

一个建议从提出到落地执行，会经过四个阶段：

1. 提案期
2. 立项期
3. 项目执行期
4. 验收期

每一步都需要通过治理委员会投票决议。治理委员会在每个治理周期内有3类投票任务：

1. 提案投票：对该周期内星云社区的提案进行投票，决定是否通过。
2. 项目立项投票：对该周期内参与立项的项目进行投票，决定是否可以执行并批准预算。
3. 项目验收投票：对该周期内提交测试的项目进行投票，决定项目是否可以验收结算。

治理委员会治理流程如下图：

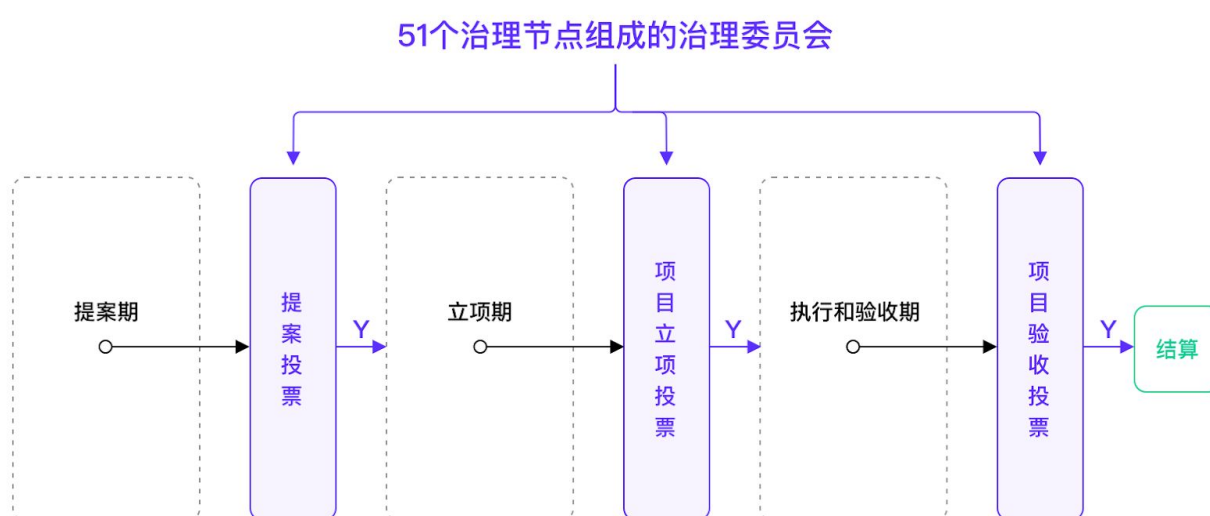


图3.1 治理委员会投票治理流程

提案期：社区成员在星云协作平台Go.nebulas（go.nebulas.io）上自由发起和分享提案。

立项期：对通过提案投票的项目进行处理。按照执行情况，提案分为两类：

1. **无需申请预算的提案。**比如提案内容为星云发展方向探讨、治理组织结构调整建议、主网参数调整等。通过提案投票后，可以由相关负责人快速推进执行。

2. **需要申请预算的提案。**此过程由Go.nebulas运营团队协助沟通，并对预算进行把关。提案人可以按照Go.nebulas的标准模版提出预算、项目目标、执行步骤和工期，申请自己执行或在社区悬赏执行人。

执行和验收期：执行和验收期为Go.nebulas内部运作流程，治理委员会无需亲自参与。主要分为三个阶段：

1. 悬赏期：由提案人或Go.nebulas运营团队担任项目发起人，发起项目悬赏，社区成员可自由申领；
2. 执行期：项目发起人确认项目负责人，项目负责人开始执行并提交项目结果；
3. 测试期：项目发起人Go.nebulas运营团队组织验收，并出具是否通过该项目的建议报告，供治理委员会参考。

3.2.2 社区资产

治理委员会负责管理社区公共资产的使用。社区公共资产包括：

1. Go.nebulas社区协作基金的使用和分发

此部分资金的初始来源是自星云2018年3月30日主网上线至节点去中心化之前，已经产生的DPoS记账收益。其中，除去已使用的部分（如星云激励计划奖励），剩余部分将在节点去中心化之后归入Go.nebulas社区协作基金。

由于当前每个治理周期的项目总金额上限为不大于30,000 USDT，故启动治理机制后半年的实际使用为180,000 USDT等额NAS。

2. 星云节点计划激励分配

星云节点计划激励包括共识机制激励和治理机制激励两部分。来源为DPoS每日产生的8,219.1744 NAS记账收入。具体分配方法参见[1.3 激励分配](#)。

公共资产的使用、分配方案改动等，都需要经过提案流程，由治理委员会投票决议通过后方可执行。

3.2.3 共识机制惩罚

治理委员会同时需要对该治理周期内发生的中、高安全等级惩罚（参见[2.5.1 惩罚](#)）情况进行投票决议。

1. 如果投票通过该共识节点危害PoD系统安全性的行为属实，则对该节点的惩罚有效，选取限制继续执行，已冻结的惩罚金捐赠给Go.nebulas社区协作基金。
2. 如果投票不通过，该节点未对系统安全性造成危害，则选取限制终止，出块稳定指数 $S_{(i)}$ 恢复为惩罚前的数值，已被冻结的惩罚金解冻。

3.3 治理手段：投票

3.3.1 投票周期

治理节点可以在前一个治理周期结束后120个轮询周期内（约为5天）进行投票。逾期视为自动放弃。

3.3.2 投票方法

治理节点投票为公开非匿名链上投票。治理节点应参与该治理周期内的**所有**投票。每个投票有三种选项（必选一个）：

- 支持
- 反对
- 弃权

每个提案只能投一次，每次投出1 NAX。投票使用的NAX直接销毁，不返还。

3.3.3 投票结果处理

一个提案或项目的通过在不同投票阶段需要满足以下不同条件：

投票阶段	治理节点参与度	通过率	预算限制
提案投票	不少于26个	50%以上	无
项目立项投票	不少于26个	67%以上	单个项目预算不大于15,000 USDT [*] ； 该治理周期内通过的项目总金额不大于30,000 USDT ^{**}
项目验收投票	不少于26个	67%以上	/
共识机制惩罚	不少于26个	67%以上	/

表3.1：投票结果处理表

* 单个项目预算如果超出，建议拆分为多期项目进行。

** 如果该治理周期内通过的项目总金额超预算，则按支持率排名，排名靠后的提案顺延到下一治理周期立项。

3.4 惩罚机制

3.4.1 单个治理节点惩罚

如果一个节点连续2个治理周期成为治理节点却没有完成全部治理投票，则820个轮询周期内（约一个月）不能入选候选节点。

3.4.2 治理失效

1. 如果某治理周期内参与投票的治理节点少于26个，本次治理宣告失效，则治理机制激励捐赠给Go.nebulas社区协作基金（参见[3.2.2 社区资产](#)）。
2. 如果某治理周期内一个提案和项目都没有，即没有可进行的投票，则本次治理宣告失效。治理机制激励捐赠给Go.nebulas社区协作基金。

4 路线图

为了更好地完成主网节点去中心化的过渡，星云节点计划将逐步开放节点申请。诚邀当前星云生态中活跃的项目方、合作伙伴和社区成员，提前搭建节点并体验治理流程，为测试和改进提供宝贵建议。路线图如下：

- 2019.11.20 - 《基于贡献度证明机制（PoD）的星云节点计划》发布
- 2020.1月初 - 上线测试网，启动测试悬赏
- 2020.1月 - 节点申请开启邀请制，共识机制启动
- 2020.2月底 - 节点开放公开申请
- 2020.3月底 - 第一次治理投票，治理机制启动

附录

附录A 推荐硬件配置和环境

每月推荐配置服务器支出约为：150 USDT/月

- CPU：>=4核（推荐8核）
- RAM：>=16G
- Disk: >= 600G SSD
- NTP: 安装NTP服务确保服务器时间同步

节点安装教程参见[星云技术文档：Nebulas 101 - 01 编译安装](#)。

推荐使用docker安装节点：

- 安装[docker](#)和[docker-compose](#)
- 在[节点根目录](#)下执行docker命令

```
sudo docker-compose build
```

```
sudo docker-compose up -d
```

附录B 节点共建

节点可以由个人、公司、组织等运营。**节点利益分配由节点运营方决定。**

支持一个节点是社区用户的自主行为，用户应在充分考察节点运行情况后作出决定。PoD仅能保证质押NAX的正常质押和提取，不对节点运营者的承诺负责。

为了方便社区用户参加，初始阶段星云基金会将组建示范性共建节点。该节点服务器由星云基金会代为运维。所有社区用户都可以通过投出NAX来支持该节点，所获利益扣除服务器运维基本费用后，由参与共建的所有社区用户按投出的NAX额度均分。

附录C 收益模拟

假设一个节点在一个月內每日都在候选节点之列，则当月最多获得共识机制激励约为9,920 NAS。

因一个月內轮询周期超过700次，该节点当月一定可以入选共识节点。但考虑到共识节点综合排名算法有随机数因素的存在，平均收益预计在3,307 NAS左右。

假设一年內每月入选的51个治理节点都参与了治理，则每个治理节点每月可获得治理机制激励预计为816 NAS。

附录D 注释

[1] <https://nebulas.io/cn/vision.html>

[2] **Autonomous Metanet 自治元网络**：一种基于区块链技术构建的，面向复杂数据和交互的开放协作体系。

[3] **Proof of Devotion (PoD) 贡献度证明机制**：可以简单地概述为以社区贡献者贡献大小为基础构建的机制，包括共识机制和治理机制两部分。通过社区贡献者组建共识委员会，实现主网节点去中心化；并通过治理委员会代议制的形式参与社区治理。

[4] **Decentralized Autonomous Organization (DAO) 去中心化自治组织**：也叫分布式自治组织。是一个以公开透明的计算机代码来体现的组织。一个分布式自治组织的金融交易记录和程序规则是保存在区块链中的。

[5] **Orange Paper: Nebulas Governance 星云治理橙皮书**：

<https://nebulas.io/docs/NebulasOrangepaperZh.pdf>

[6] **Delegated Proof of Stake Consensus (DPoS)**：由持币的利益相关方投票来选择代表，代表们再以民主投票的方式决定共识问题。包括但不限于：所有网络参数、费用估算、块间隔、交易规模等。

[7] NAX：通过去中心化质押产生。nextDAO上的首个Token。用户通过质押NAS获得NAX。NAX采用动态分发策略，实际总发行量与全局质押率相关，用户个人获得NAX的数量与NAS质押量以及币龄相关。

[8] dStaking 去中心化质押：区别于需要向合约转账的传统质押，去中心化质押的合约记录着用户的质押契约，用户资产仍然存放在用户个人地址之上。

[9] Nebulas NAX White Paper 星云NAX白皮书：

- Github：https://github.com/nebulasio/nax_whitepaper,
- PDF：https://nextdao.io/static/docs/nax_whitepaper_zh.pdf

[10] BFT (Byzantine Fault Tolerance) 即拜占庭容错：是分布式计算领域的容错技术，拜占庭容错来源于拜占庭将军问题。拜占庭将军问题是对现实世界的模型化，由于硬件错误、网络拥塞或中断以及遭到恶意等原因，计算机和网络可能出现不可预料的行为。拜占庭容错技术被设计用来处理现实存在的异常行为，并满足所要解决的问题的规范要求。

[11] VRF (Verifiable Random Function) 可验证随机函数：是一种将输入映射为可验证的伪随机输出的加密方案。该方案是由Micali (Algorand的创建者)、Rabin以及Vadhan于1999年提出的。至今VRF已广泛应用于各种加密场景、协议和系统中。

[12] Go Nebulas帮助文档：

<https://www.notion.so/Go-nebulas-io-09e7158463b443f3822fbc624bb394fd>

附录E 参数表

E.1 基本参数

平均出块时间：15秒

轮询周期：210个区块高度，约52.5分钟

治理周期：820个轮询周期（约1个月）

共识节点：21个

候选节点：51个（含21个共识节点）

治理节点：51个（每个治理周期内出块最多的共识节点）

保证金：2万NAS

候选节点最小质押量（投票量）：10万NAX

保证金返还时间：节点退出申请成功提交后820个轮询周期（约为1个月）

NAX返还时间：撤销投票或节点退出申请成功提交后120个轮询周期（约为5天）

E.2 共识机制相关参数

节点应出块数：10个（每个轮询周期内）

出块稳定指数 $S_{(i)}$ 初始值：0.8

出块稳定指数 $S_{(i)}$ 最大值：1

出块稳定指数触发惩罚机制的临界值：0.5

惩罚金（中级）：5%保证金

惩罚金（高级）：全额保证金 + 该节点上质押的所有NAX

共识机制惩罚时长（安全级别低级和中级）：20个轮询周期（约1天）内不得入选候选节点

共识机制惩罚时长（高级）：永久

E.3 治理机制参数

治理节点投票时长：120个轮询周期内（约为5天）

治理节点最小参与度：26个

提案投票通过率：50%以上

项目立项投票、项目验收投票和共识机制惩罚投票通过率：67%以上

触发治理惩罚机制的次数：连续2次治理周期未参与全部治理投票

治理机制惩罚时长：820个轮询周期（约1个月）

E.4 激励分配参数

每日全网记账收入：8,219.1744 NAS

每年全网记账收入：2,999,941 NAS

每年全网共识机制激励总量：2,499,951 NAS

每年全网治理机制激励总量：499,999 NAS

单项目预算：不大于15,000 USDT

项目总金额上限：不大于30,000 USDT（一个治理周期内）