



# 星云链 NAX 白皮书

NextDAO Lab

2019 年 8 月  
版本号:1.0.0

# 目录

1	星云理念与愿景	1
2	NextDAO	1
2.1	区块链协作	1
2.2	公链通证经济	2
3	NAX 通证经济设计	2
3.1	设计目标	2
3.2	核心机制	3
3.2.1	资产公平性	3
3.2.2	去中心化质押 - dStaking	3
3.2.3	NAX 发行模型 - NDM	4
3.2.4	动态分发策略	4
3.2.5	周期内分配策略	5
3.2.6	NAX 生态基金池	6
3.3	合约框架	6
4	应用场景展望	7
4.1	生态贡献激励	8
4.1.1	Go Nebulas 激励	8
4.1.2	基金会核心成员激励	8
4.2	PoD 共识探索	9
4.3	链上治理场景	9
4.4	星云生态推广	10
5	总结	10
	附录 A NAX 分析	12

A.1	发行量分析 . . . . .	12
A.2	权重与币龄的关系 . . . . .	12
A.3	追加质押对币龄的影响 . . . . .	12
附录 B	Change Log	12

# 1 星云理念与愿景

区块链技术是由一系列学科和技术（包括密码学，分布式系统，博弈论等）的组合而产生的创新。比特币 [1] 创造了“一个去中心化电子现金系统”的完美设计，打开了区块链世界的大门。以太坊 [2] 进一步提出了支持图灵完备语言的智能合约框架，并发明了 ERC20 的区块链融资范式，区块链技术因此取得了空前的繁荣和发展。

星云链致力于践行“让每个人从去中心化的协作中公平受益”的技术愿景。在白皮书 [3] 中也提出了自己的区块链理念和路径，其中包括：星云指数 (NR)，开发者激励协议 (DIP)，星云原力 (NF) 以及星云贡献证明 (PoD) 等。星云团队根据自身优势以及在行业中积累的经验，将继续专注于区块链在协作方向应用的探索，方向不局限于白皮书中的内容，将包含一些新的尝试，如 NextDAO 等。

## 2 NextDAO

### 2.1 区块链协作

以太坊 ERC20 的出现，以区块链智能合约技术为基础，成为了一种新型、快捷、低成本的融资方式，但融资过后的协作和管理问题并没有得到很好的解决。这一直都是区块链重要的发展方向之一，并同时带来了很多问题。

The DAO (Decentralized Autonomous Organization) [4]，又叫“去中心化自治组织”一个以公开透明的计算机代码来体现的组织，其受控于股东，并不受中心化组织影响。The DAO 发布之后，很快被黑客攻击并盗走价值千万美金价值的以太坊，最终导致以太坊硬分叉。虽然 The DAO 存在着缺陷，但给后续的工作带来了很多借鉴的作用。

星云链致力于区块链协作的发展，并在此基础上提出了基于区块链协作的框架范式集合：NextDAO。具体包含：公链协作、治理、去中心化金融 (DeFi) 等，详细如图1所示。NextDAO 尝试着解决目前区块链的协作当中存在的几个问题：

- (a) 激励方式仍以出块奖励为主
- (b) 公平与正向博弈缺失
- (c) 协作方式单一

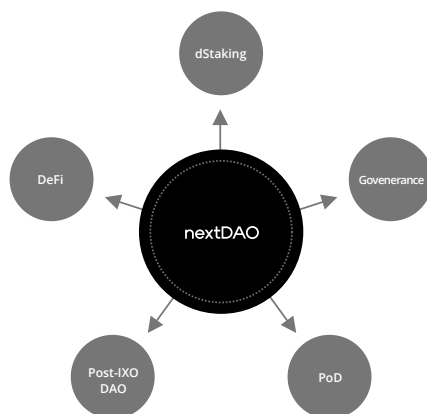


图 1: 区块链协作范式集合: NextDAO

## 2.2 公链通证经济

通证经济 (Token Economy)，具体表现为包含通证产生、流通、回购、激励等经济模型。通证经济存在于区块链世界各个角落，例如公链生态、DApp 应用内部等。公链生态通证经济的典型的案例是以太坊的 ERC20，它便利了融资的同时，刺激和繁荣了以太坊生态，也同时带动了整个区块链行业的大发展。因此，公链的价值和创新不仅仅源于在“不可能的三角”上的技术本身的创新，也来源于技术所带来的模式和商业创新。

公链通证经济要考虑的问题是人与人的博弈，需要避免公地悲剧 [5]，通过正向激励促进公链生态的繁荣和发展。大多数公链远达不到以太坊的社区力量，因此以探索区块链应用落地为导向，发展区块链技术，扩大社区共识，才能建立一个适合自身的优秀的公链通证经济，这与发展公链技术创新同等重要。接下来的章节，将详细介绍星云链根据自身的愿景和特点，提出来的基于 NextDAO 框架的公链通证范式: NAX。

## 3 NAX 通证经济设计

### 3.1 设计目标

公链通证经济设计的目标除了形成正向博弈、激活生态之外还应当符合一定的原则，例如：公平受益、正向激励、逻辑简洁，场景多样等。总而言之，公链的通证经

济需要公正的获取场景和多样的消耗场景，拥有较高的持有价值，从而促进公链的发展和壮大，使得整个生态变得更加有活力和动力。总结起来 NAX 的设计目标是：

- (i) 公平受益
- (ii) 正向激励
- (iii) 简洁有效
- (iv) 场景丰富

## 3.2 核心机制

### 3.2.1 资产公平性

公链通证经济的有效性的根本来自于资产获得的公平性和正当性。资产的获取规则应当简单透明，对绝大多数人应当是信息对称的。在星云生态中，用户所持有的 NAS 资产具有相对的公平性和正当性，因此通过质押（Staking）NAS 的方式作为获取通证权益的主要途径是符合要求的。不会因为规则不清晰、信息不对称，或者系统漏洞导致资产分配不公平的现象，并使得博弈的结果是有利于公链生态发展的方法。

### 3.2.2 去中心化质押 - dStaking

传统的中心化的质押方式是用户将资产转入到智能合约当中暂为保管，资产安全问题维系在一个智能合约中，合约资产安全性问题历史上屡见不鲜，攻击者利用了合约漏洞使得投资者产生巨大的经济损失，也使得投资者对合约安全性产生担忧。另一方面，质押同时也给公链项目方带来非常大的压力，大量资产保存在一个合约当中，使得合约的管理及安全性成为一个发展瓶颈。区块链核心是去中心化及资产的确权性，质押的目的是减少流动性，并不是获得资产的本身。

我们提出了一个新式的质押方式：去中心化质押（dStaking - decentralized Staking），如图2所示，在确保用户资产仍然属于用户的前提下，用户与质押合约签定的质押契约记录在合约上。质押合约的作用只是通过链上随机检查用户是否仍在履行契约。当地址的余额大于等于契约的数额的时候，被认为是有效质押，否则将视为退出质押。当用户在原地址追加质押数量的时候，系统会根据新质押的数量重新计算一个平均币龄，这部分将在附录中讨论。dStaking 的优势在于：

- (a) 保障用户对资产确权

(b) 提高质押积极性

(c) 提高资产安全性

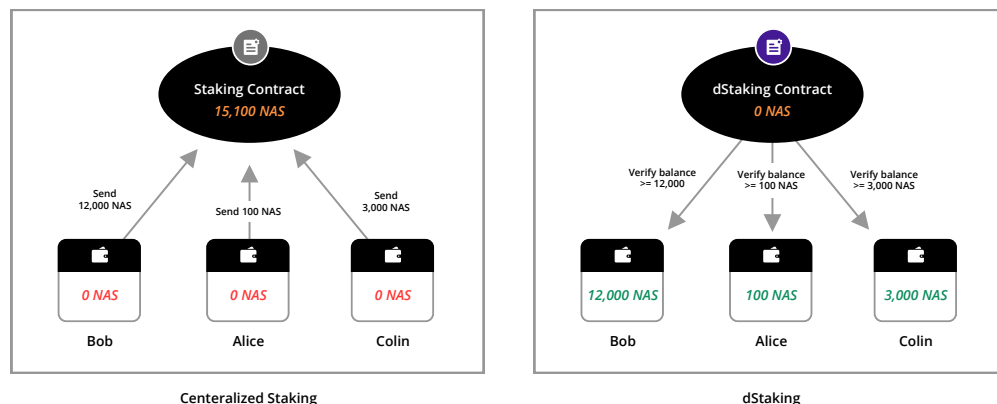


图 2: 中心化质押 vs 去中心化质押

### 3.2.3 NAX 发行模型 - NDM

在保障资产发行的公平性与正当性基础上，确保用户质押资产所有权神圣不可侵犯的前提下，用户贡献出资产的流动性以获取相应的生态权益，我们称这种新式发行模式为 NDM (Nebulas Devotion Mining)。NAX 的预计发行总量上限是 100 亿 ( $10^{10}$ )。发行周期为每 6,000 高度（一天左右），每个周期预发行数量呈递减规律，衰减系数  $\mu = 0.999$ ，预计 12 年左右接近发放总量。预发行 NAX 数量随周期数增长的变化图3所示，累积预发行 NAX 数量如图4所示。

### 3.2.4 动态分发策略

动态分发策略是指，系统会根据一些变量决定实际分发 NAX 的数量，以促进生态的正向博弈。在 NAX 起初，我们引入质押率影响因子，根据质押率的增加或减少，动态调整实际分发比例。将来根据需要，我们还将引入更博弈的因素。如图5所示，周期  $i$  内系统预分发  $C_i$  个 NAX 给当前周期内正在质押的用户。在实际分发的过程中，根据当前的质押率水平  $\lambda$ （参与质押 NAS 的总量/总体 NAS 流通总量,  $0 < \lambda < 1$ ），实际分发 NAX 为： $C_0 \mu^i \lambda$ 。

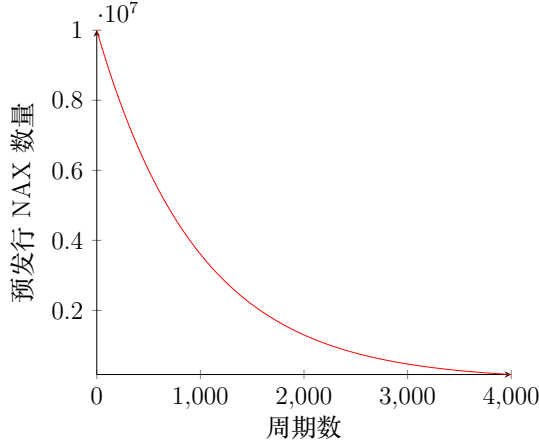


图 3: 预发行数量与周期关系

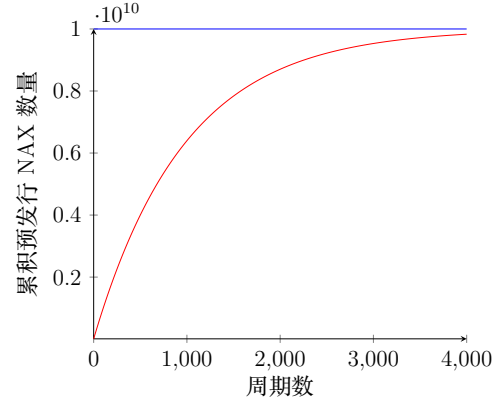


图 4: 累积预发行数量与周期关系

### 3.2.5 周期内分配策略

在一个分发周期内，不同的质押周期数将获得不同的分发权重。系统根据每个质押用户的质押数量  $V_{i,j}$  以及质押权重  $f(T_{i,j})$  决定最终所获得的 NAX 分发量。假如第  $i$  周期内，有  $N$  个地址正在有效质押，其中第  $j$  地址质押数量为  $V_{i,j}$ ，有效质押周期数为  $T_{i,j}$ 。因此，该地址所能分发到的 NAX 数量  $K_{i,j}$  如以下公式所示。

$$K_{i,j} = \frac{V_{i,j} f(T_{i,j})}{\sum_j V_{i,j} f(T_{i,j})} \lambda_i C_i \quad (1)$$

其中， $f(T_{i,j})$  是第  $i$  期用户  $j$  的质押的有效权重函数。质押权重与质押周期数的关系，如下公式所示，其中函数关系如图6所示。

$$f(T) = 1 - \frac{\sqrt{(aT + b)^2 + c^2} - (aT + b)}{2} \quad (2)$$

公式中的参数  $a$ ， $b$ ， $c$  等将会在附录中讨论。总的来说，同一个周期内，系统会根据质押数量以及相应的质押时间长短来分配发行的总量，以达到公平的效果，即质押数量越多，质押时间越长，所分配到的发行数量也会更多。但同时使得让新进来的质押用户有更高的积极性，新用户的权重也会维系在一个可观的水平上。该设计会达到以下博弈场景：

- (a) 早期参与质押的用户，有更大的概率获得更多的系统发行
- (b) 随着质押率增加，系统发行数量也会相应提高，以鼓励更多人加入质押



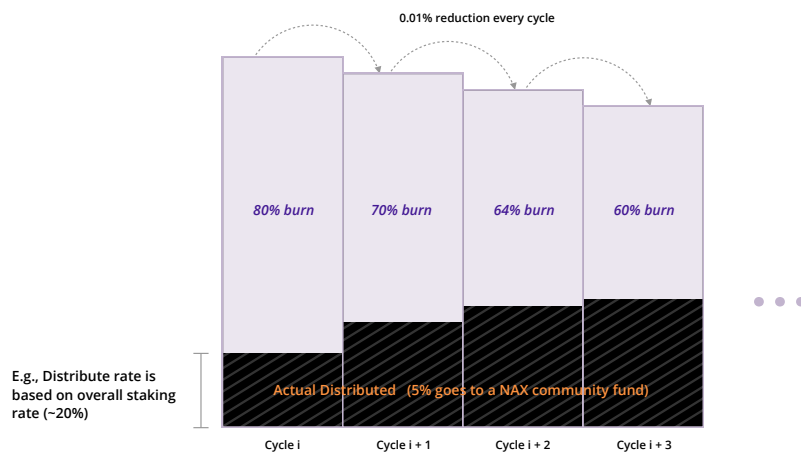


图 5: 动态分发策略示意图

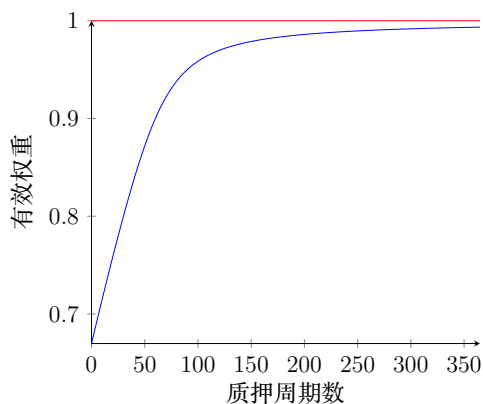


图 6: 质押的有效权重与周期数的关系

### 3.2.6 NAX 生态基金池

为了便于在生态上更好地在投资、孵化，扶持等活动中有更多的空间和主动权，将设立一个 NAX 生态基金池。系统在实际分发过程中，将分发给质押用户的 NAX 中，扣除 5% 转到这个基金池中，该基金池接受社区监督。具体的活动内容将在白皮书发布之后披露。

## 3.3 合约框架

NAX 是扩展性的 NRC20 合约，由一组合约组成，并配合多签合约管理整个合约里的数据和参数，详细如图7所示。

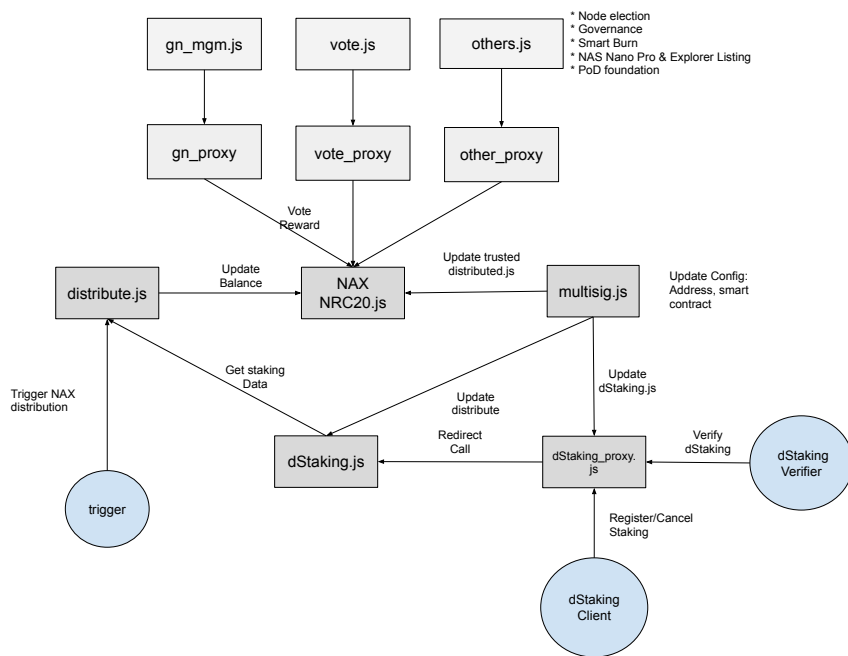


图 7: NAX 合约组件示意图

## 4 应用场景展望

为了尊重资产的公平性，正当性，确权性，我们把分发模型的设计简洁、明了、有效。结合星云的生态特点，将更多的激励和博弈场景交给了应用场景本身，应用场景中的激励和消耗场景可以更加变化、多样。在本章节中，我们针对星云中已经存在的或是未来的应用场景进行一些展望，如图8所示，我们可以比较清晰的勾勒出 NAX 在星云生态的正向激励作用。

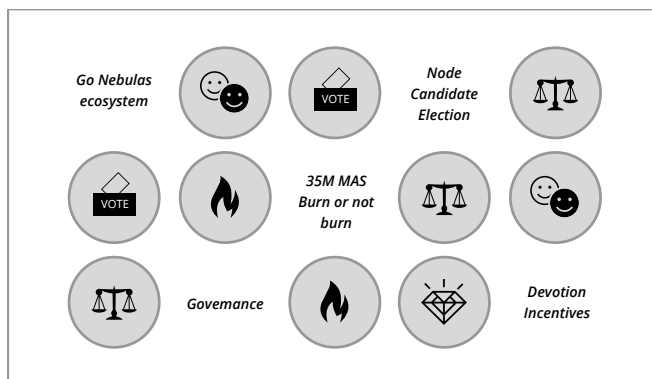


图 8: NAX 在星云生态中的使用场景

## 4.1 生态贡献激励

在白皮书中，从贡献证明的共识算法（PoD, Proof of Devotion），到星云的愿景的提出：在去中心化的协作中公平受益，再到 2019 年初，Go Nebulas 平台的上线，都始终贯穿着星云对生态贡献度衡量的探索。这些都是星云进一步朝着 Autonomous Metanet 目标前进的重要环节。为此提出一种以质押投资基金为权益证明的激励方式，使之运用到不同场景的激励当中。具体的操作是，将项目投资基金（通常以 NAS 形式存在）进行质押，这部分资金质押所得的 NAX 权益，将作为该生态场景的 NAX 激励权益基金。

### 4.1.1 Go Nebulas 激励

星云基金会将会投入不少于 3,000,000NAS 资金，用于资助 Go Nebulas 平台上的项目，而且根据需求，基金会还将随时追加资金的投入。这部分资金可以投入到质押当中，产生的权益将用来激励在 Go Nebulas 平台上做出不同贡献的权益证明，即在获得 NAS 资金作为报酬之外，还将获得由 Go Nebulas 平台制定的规则下的 NAX 激励，作为对星云生态做出贡献的权益，可以在星云生态上行使相应的权益和治理。详细的激励方案将由 Go Nebulas 的运营团队管理者或社区的参与者共同制定。激励可以分为以下几类：

- (a) 核心基础建设
- (b) 市场拓展
- (c) 推广与邀新
- (d) 提案与参与

Go Nebulas 平台除了是一个投入社区建设，获得 NAX 激励的重要方式之外，同样是一个 NAX 的重要使用场景，消耗场景包含（不局限）于以下几类：

- (a) 创建和发起提案
- (b) 提案通过与否决
- (c) 项目进行中的质押

### 4.1.2 基金会核心成员激励

成为基金会核心团队的成员，包括兼职的人员，在获得相应的工资作为报酬之外，也将获得由基金会质押所产生的 NAX 权益作为额外的贡献证明。

## 4.2 PoD 共识探索

随着星云对 PoD 研发的推进，去中心化是星云链的必由之路，NAX 将可能在 PoD 中扮演重要角色，有效地结合主网正在研发的 PoD 技术创新成为新型共识算法的基础和方向。上一节讨论了 NAX 在生态中的激励场景，加上 NAX 的单一的质押的发行方式，获得 NAX 的方式只能通过以下方式获得：

- (i) 贡献资产的流动性
- (ii) 投入星云链建设
- (iii) 参与社区治理场景

从另一外角度不难得出，NAX 可以被看作为星云生态的贡献凭证。PoD 顾名思义是贡献度证明，区别于 PoW、PoS 的本质在于，星云链更看中区块链协作当中，以不同角色对生态的贡献作为出块奖励的依据，而不仅依赖算力的大小或是筹码多寡。

在选择共识委员会的时候，可以引入 NAX 的权益多少来影响出块的概率大小。共识节点委员会的产生，无论是链下还是链上产生，NAX 也将可以成为投票的重要依据。现在先链下节点竞选为例，阐述说明节点可能的方式，最终的形式将以官方发布的 PoD 技术文档为准：

- (a) 节点委员会成员由 NAX 投票选出来
- (b) 需要销毁相应量的 NAX，并质押 NAS
- (c) 节点将分多个赛道，丰富生态多样性
- (d) 主网 PoD 共识算法将引入 NAX 作为参数影响出块权益的分配

## 4.3 链上治理场景

在星云生态的发展进程中，会出现各种各样的评选、选举等活动。为了提高社区生态中的参与度，每个活动将根据需要，使用 NAX 作为权益证明介质将会在投票和激励策略中发挥重要作用。

例如接下来关于如何处理社区预留的 35,000,000NAS 的方案，将成为比较早期的由社区来贡献方案，并由社区来投票决定处理方案的活动案例。星云基金会曾提议销毁，其中一种可能的方案是，每个月发起一次使用 NAX 的投票销毁社区预留剩余 NAS 总量的  $\lambda\%$ ， $\lambda\%$  是当前 NAS 质押率占流通总量的份额，我们也鼓励社区提供更加有效、积极的方案，共同决定这部分资产的使用。

## 4.4 星云生态推广

星云基金会扶持开发的，基础生态产品是星云链生态使用的重要入口，这里包含现在的，还有将来基金会孵化的星云生态产品，例如：NAS nano Pro [6]、Explorer [7] 和 Nebulas DEX 等。随着 NextDAO 的推进以及社区治理的前进，社区里将会出现越来越多的 NRC20 Token 和治理尝试。这些币种有对生态工具的强烈需求，例如：NAS nano Pro 和 Explorer 等。资源空间有限的情况下，为了使得星云生态相关的产品推出更多优秀好的项目，将可能会使用 NAX 作为平台征选优秀项目的工具以及保证金，这些保证金也同样可以作为生态项目的活动和激励经费，用于投入到平台的建设当中。

## 5 总结

为了更好地实现星云的理念与愿景，结合自身生态的特点，提出了适应自身理念和发展的通证经济。在整个文章当中，我们分析了 NAX 的公平性，正当性，确权性，激励性等，贯穿整个星云的理念、生态建设、发展、协作与治理。这只是我们开展 NextDAO 方向的一个示范和开端。在这个过程当中，更多有趣，有价值的想法将会涌现出来，同时期待社区的加入一起丰富 NextDAO 的内容。

## 参考文献

- [1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” Wwww.Bitcoin.Org, p. 9, 2008.
- [2] V. Buterin et al., “Ethereum white paper,” 2013.
- [3] “Nabulas Technical Whitepaper.” <https://nebulas.io/docs/NebulasTechnicalWhitepaperZh.pdf>. 2018-04-01.
- [4] “DAO.” [https://en.wikipedia.org/wiki/Decentralized\\_autonomous\\_organization](https://en.wikipedia.org/wiki/Decentralized_autonomous_organization).
- [5] “Tragedy of the Commons.” [https://en.wikipedia.org/wiki/Tragedy\\_of\\_the\\_commons](https://en.wikipedia.org/wiki/Tragedy_of_the_commons).
- [6] “NAS nano Pro.” <https://nano.nebulas.io>.
- [7] “Nebulas Explorer.” <https://explorer.nebulas.io>.

## 附录 A NAX 分析

### A.1 发行量分析

我们给 NAX 设置了一个总的发行量上限为 100 亿 ( $10^{10}$ )，那么可以推导出第 0 期预发行的规模如下：

$$\sum_{i,j} K_{i,j} = \sum_i C_0 \mu^i = \frac{C_0}{1 - \mu} \quad (3)$$

令此上界为 100 亿 ( $10^{10}$ )，可解出  $C_0 = 10^{10}(1 - \mu) = 1.0 \times 10^7$ 。

### A.2 权重与币龄的关系

为了鼓励早期参与质押的用户，同时激励新用户加入质押，因此系统币龄产生的权重做了进一步处理。随着周期数的增加，当质押周期超过 90 后，权重将趋于平稳达到最峰值 1，而新用户的起始权重从 0.67 开始。根据上述的讨论以及白皮书中的权重公式，可以计算出相应的系数，其中  $a = 0.005$ ， $b = -0.3$ ， $c = 0.2$ ，该函数效果如图6所示。

### A.3 追加质押对币龄的影响

为了便于在原地址上追加质押，用户只需要对质押合约再进行一次契约交易。系统会根据过去质押和新质押的数量，重新计算出平均币龄。例如，用户当前质押 100NAS，质押了 10 个周期，用户再追加质押 100 NAS 并通知合约后。那么新的质押数量为 200 NAS，而币龄则是两次质押的平均值为 5 个周期。

## 附录 B Change Log

- 0.0.1 Release.