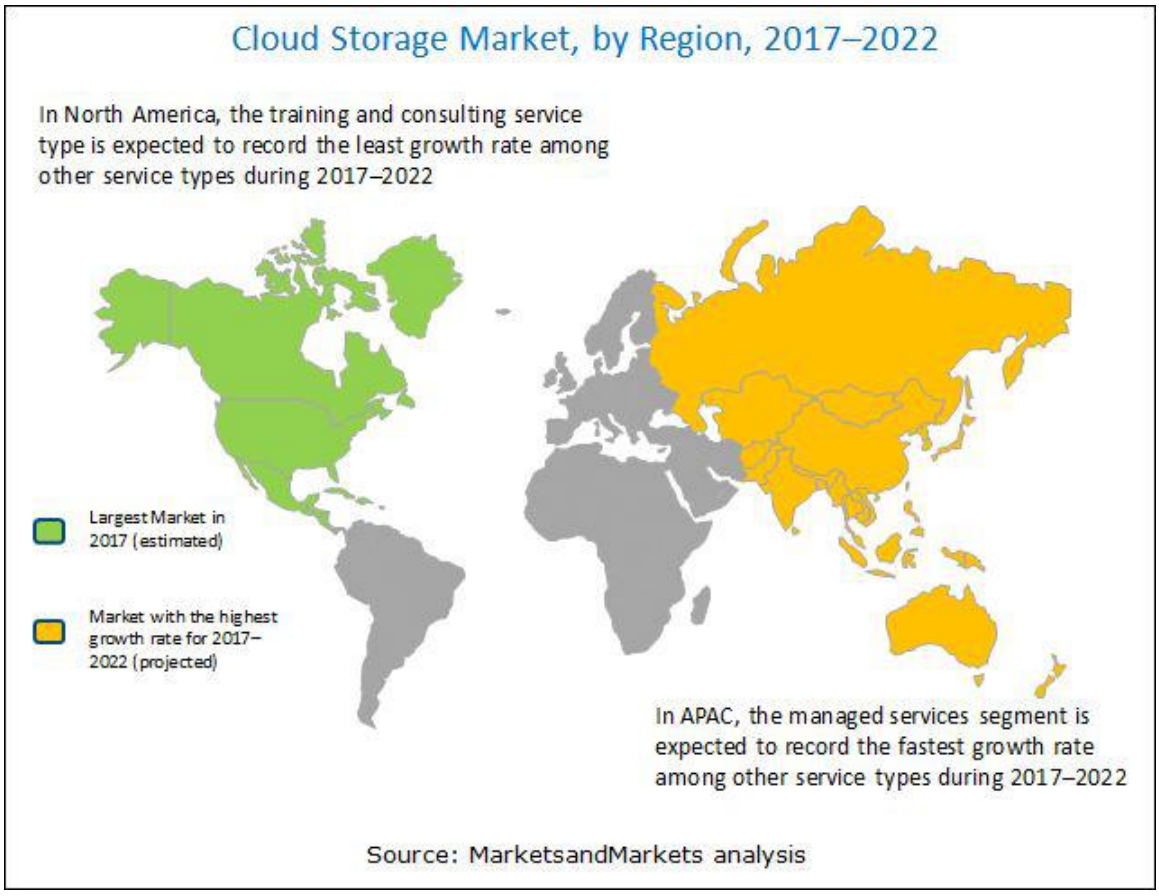
# Spock Chain——下一代去中心化存储应用平台

## 目录

## 1. 前言

据 MarketsandMarkets 的最新报告，预计全球云存储的市场将从 2016 年的 234 亿美元上升至 889 亿美元，年复合增长率为 23.7%。对云存储的需求受到许多因素的驱动，例如人工智能、IoT、VR/AR 的越来越普及，云端数据存储变成许多新技术服务的基础设施，尤其是伴随着 5G 的来临，更是将加速云端存储需求的爆发。随着云存储解决方案和服务的可用性，已经消除了维护本地存储基础架构（例如磁盘存储和磁带设备）的需求。

预计 2017-2022 年北美市场规模将保持最大，而亚太地区（APAC）预计将在云存储市场的预测期内以最高的复合年增长率增长。据称，对高效计算框架和将工作负载转移到云环境的需求日益增长，正在全球推动对云存储的需求。转向云解决方案和服务的组织以及数字业务战略的日益普及是预计将推动北美云存储产品采用的主要因素。



然而如今，中心化的私有服务正在被去中心化开放服务所替代，可信任中心被可验证式计算所替代， 正是由于传统的中心化数据服务面临着以下一些挑战：(a) 托管和分发 PB 级别的数据成本高昂。(b) 隐私数据泄露以及滥用。(c) 跨组织的大数据计算。

本文介绍 Spock Network, 一个去中心化数据存储网络，旨在解决上述这些问题。Spock Network 综合了过去许多系统的经验和教训，精心设计了一条可以最终达成大规模去中心化存储网络的实现路径。

## 2. 项目介绍

Spock Network 是一个去中心化存储的平台，在早期阶段，Spock Network 主要存储以 Proof of Capacity (POC) 的共识数据为主，以有效的利用目前最合适的去中心化技术激励提供硬盘空间的矿工，同时，在这个基础之上，也增加了智能合约的支持，以支持去中心化应用以及 POC 类代币发行。在未来，Spock Network 存储的数据会支持文档、视频、图片等任意格式的文件，真正完成让区块链技术能够人人受益的理想。

Spock 是美国经典科幻剧集星际迷航中的男主角，这个人物代表了理性、正义、以及探索未知的勇气，我们选择了将 Spock 作为项目名称也代表了团队持续不断探索区块链新的可能性的精神。

### 2.1 Proof of Capacity (POC)

比特币是一个成功的去中心化资产网络，然而伴随着 Asics 芯片矿机的发展，已经逐渐远离中本聪在比特币白皮书中希望 one-cpu-one-vote 的初衷，同时，对电力资源的巨大消耗也是被诟病许久的问题。

Burst 在 2014 年针对这个问题推出了自己的主网，它提出采用 Proof of Capacity(也被称为 Proof of Space)共识算法用来取代比特币的 Proof of Work 共识，使得挖矿的过程中极大的节省了对电力资源的依赖。

Spock Network 除了改进了挖矿的 POC 共识算法，还将引入更好的经济模型以激励矿工加入到挖矿的队列中来，同时也将构建以 Solidity 为基础的图灵完备的脚本语言以支持智能合约，去中心化应用等生态建设，同时也支持开发者利用现有的共识”算力”构建自己的 POC 类项目。

众所周知， Proof of Works(POW)是被中本聪在比特币系统中引入进来作为一个解决”双重支付”问题的方案，它的核心算法是对于一个值α, 一个随机预言函数 H, 如果我们希望哈希值 H(a)满足前 t 位都是 0，则需要耗费 2^t 次哈希计算才能找到这个α值，POW 的核心价值就是在所有人都遵循这个验证规则的条件下，除了执行这么多次哈希计算，没有人可以加速计算的过程，所有矿工只能老老实实的执行这么多次运算来找到合适的 nonce 值，最先找到的矿工就能负责下一个区块的写入，同时获得奖励。于是为了更快的完成这些 Hash 计算，矿工们经历了从 CPU、GPU 到 Asics 芯片矿机挖矿的转变，由于大量的计算需要耗费大量的电力，对于像比特币这样的大规模 POW 网络来说，甚至被诟病为是破坏生态环境，

同时，对于淘汰了的 Asics 芯片 矿机，它们只能被当成垃圾处理，因为它们除了挖矿什么也干不了。

Proof of Capacity(POC) 也被称为 Proof of Space，它的基本思路是把计算放在初始化阶段，也就是将哈希计算的结果事先写到硬盘中，在执行阶段，通过检索硬盘中的数据来降低 POW 算法中需要大量用到哈希计算，只有少量的哈希计算会在执行阶段被用到。通过这样的方式，整个网络在以下几个方面获得了提升：

- 环保：当一台矿机被初始化之后，挖矿代价是比较小的，每次出块只需要少量的磁盘访问和少量的计算。
- 经济：很多个人电脑都有未被使用的磁盘空间，将这些空间用于挖矿的边际成本很小，即时奖励很小，也可以用于挖矿。不至于像比特币矿机那样必须考虑电费成本。
- 平等：今天比特币已经变成 Asics 矿机和大型矿场的天下，小规模投资人已经很难参与到比特币挖矿生态中，而基于 POC 的矿机几乎不会面临像比特币专有矿机那样不断更新迭代以至于被彻底淘汰出局的情况。
- “算力”共享：BCH 是 BTC 硬分叉的链，所以 BTC 的专有矿机也能挖 BCH，但是它却不能同时挖 BTC 和 BCH，而 POC 机制可以使得对于不同的链，只要硬盘空间上”算力”数据结构一致，那这些”算力”可以同时被用于挖这些链上的资产。

同时，为了更好的构建 Spock Network 的生态，我们将参考 Proof of Stake(POS)共识的某些特性，在共识算法中引入 Staking 机制，矿工需要持有一定数量的代币才能挖矿，详细内容见第 4 章。

## 2.2 去中心化存储网络(DSN)

在 DSN 网络中，文件会被分片、复制并上产至若干个节点，并通过分布式哈希表维护相应的数据。客户通过支付网络费用进行存储和检索，矿工提供磁盘空间和带宽来获得奖励。

### 2.2.1 分布式哈希表(DHT)

分布式哈希表（distributed hash table，缩写 DHT）是分布式计算系统中的一类，用来将一个键（key）的集合分散到所有在分布式系统中的节点。这里的节点类似哈希表中的存储位置。分布式哈希表通常是为了拥有大量节点的系统，而且系统的节点常常会加入或离开。

### 2.2.2 Kademlia 算法

Kademlia 是一种通过 DHT 的协议算法，它是由 Petar 和 David 在 2002 年为 P2P 网络而设计的。Kademlia 规定了网络的结构，也规定了通过节点查询进行信息交换的方式。

# 3. 核心技术

## 3.1 POC 共识算法

POC 共识算法最早被 Stefan Dziembowski 在 2013 年被提出，Burst-coin 则是第一个以 POC 共识算法为基础的区块链项目，同时，Burst-coin 在 2018 年完成了 POC2 的共识升级，使得 POC 网络更加安全。

### 3.1.1 术语

在基于 POC 的区块链系统中，有些术语和基于 POW 挖矿的系统类似，但是不太一样，为了方便理解，我们将一些主要的需要强调的术语列在下面。

- Shabal/Sha256/Curve25519

  Shabal,Sha256, Curve25519 是 Spock Network 中使用的加密哈希函数，Shabal 是主要使用的函数，Shabal 是一个并不是一个高效的加密哈希函数，但是由于我们的哈希计算主要发生在 plot 阶段，对于我们运行时所需要的验证工作来说它已经足够了。我们主要使用它的 256 字节的版本，也就是 Shabal256。

- 哈希值

  哈希值表示一次加密哈希函数的计算结果，如果没有特别说明，本文中提到的哈希值一般为 32 个字节。

- Plot 文件

  当挖矿时，挖矿程序会从磁盘中读取事先计算好的 Hash 值，这些值被存储在磁盘的文件中，这些文件就是 Plot 文件。

- Nonce

  一个 plot 文件中，存了若干组 nonce，一个 nonce 包含 8192 个哈希值，因此一个 nonce 的大小为 256K 字节，每个 nonce 都有一个独立的长度为 8 字节的的编号，编号范围为 0-18446744073709551615 (2^64)。

- Scoop

  每个 nonce 所包含的 8192 个哈希值被放入 4096 个不同的地方，每个 scoop 中放入 2 个哈希值。

- Account ID

  当创建 plot 文件时，这个文件是和矿工的数字账号 Account ID 关联起来的，这个 ID 会被用于创建 nonce，不同的矿工创建的 nonce 不一样，尽管可能他们使用的 nonce 编号是一样的。

- Deadline

Deadline 是挖矿过程中不同矿工之间用于互相竞争的值，这个值是基于 plot 文件上的 nonce 计算出来的，当这个值被提交到钱包时，并且钱包没有在 deadline 时间(秒)内收到网络中来自其他节点的区块广播，则会进行打包。

- Block Reward

  当某个矿工负责打包区块时，他就能获得区块奖励。区块奖励详细信息见第 3 章。

- Base Target

  Base target 是根据过去 24 个块的出块情况计算出来的。这个值用于调整挖矿的难度，这个值越小，则对于矿工想找一个小的 timeline 越难。

- Network Difficulty

  这个值相当于用于体现当前网络中用于挖矿的总的硬盘空间，以 T 为单位。

- Block Generator

  当新的区块被打包时，打包时需要用到的账号就是 block generator。也就是找到 deadline 所需要用到的 nonce 所对应的账号。

- Generation Signature

  Generation signature 是基于上一个区块的 generation signature 和 block generator，这个值被用于打包一个区块，长度为 32 字节。

- Block Signature

  Block signature 是被 block generator 在打包区块时创建的，是将 block 内大部分数据以及 block generator 的私钥进行 Sha256 和 Curve25519 哈希计算后的签名，长度为 64 字节。

- Solo/Pool 挖矿

  独立挖矿和矿池挖矿，独立挖矿也就是矿工提交的结果是跟整个网络内其他独立矿工和矿池提交的结果进行直接竞争，获胜时则可获得全部区块奖励。矿池挖矿则是将结果提交给矿池，由矿池在收获了矿池内其他矿工的以确定拿到的最小的 deadline 值之后，和网络内其他独立矿工和矿池提交的结果进行比较，若胜出，则矿池会根据自己的分配机制，公平的分给相关参与挖矿的矿工。

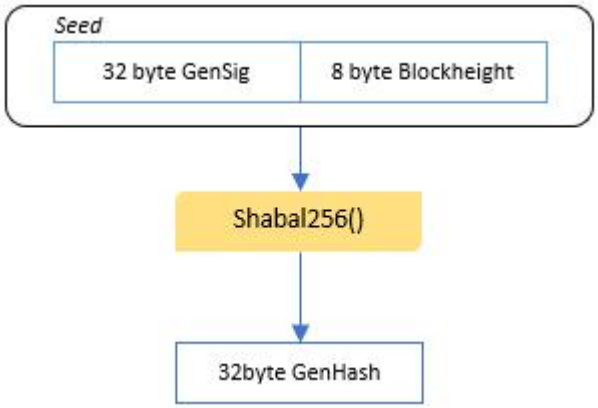
- 奖励分配

  奖励分配主要针对矿池挖矿说的，当矿工设置了奖励分配归属为矿池之后，矿工相当于通知了网络矿池接管了矿工的区块奖励，也就是说当本来区块

奖励时分配给矿工的，现在分配给矿池的账号，同时，若从矿工处接收到的 deadline 值，则由矿池负责打包出块。

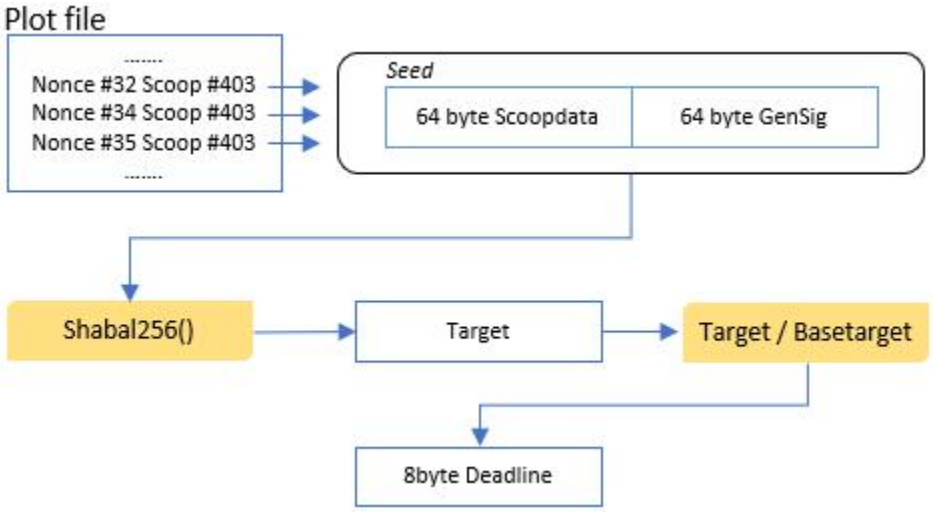
### 3.1.2 挖矿过程

当开始挖矿时，挖矿程序会从钱包这里获取挖矿信息，如 generation signature, base target 和下一个区块高度，其中，generation signature 是由钱包程序在上一个 generation signature 和上一个出块的矿工 Id 组合在一起后通过 Shabal256 计算后生成。挖矿程序将 generation signature 和区块高度组合在一起作为 Shabal256 的 seed，以得到一个 generation hash。




接下来挖矿程序会将 generation hash 值对数值 4096 取模来计算该使用哪个 scoop 中的数据。

然后挖矿程序会读取所有 nonce 所对应的该 scoop 的数据，将 scoop data 和 generation signature 作为 seed 得到一个新的 target 值，再将 target 值除以 base target 并取前 8 个字节作为 deadline 值。



挖矿程序会所有计算得出的 deadline 值中选取一个最小的值，如果该值还有值得提交的意义(如果数值过大，则没有必要提交结果，因为提交了也不会被采纳)，提交的信息中包含和该 plot 文件关联的矿工 ID，以及通过当前的 scoop data 所找到的最优 deadline 所对应的 nonce 值。

### 3.1.3 打包过程

钱包程序(或者矿池程序)在接收并验证了挖矿程序提交的信息之后，会观测在 deadline 数量的时间(秒)内，是否收到网络上别的矿工广播的有效区块，如果收到，则钱包放弃打包区块，否则钱包将使用目前的 deadline 信息打包区块。

每个区块可以最多包含 255 个交易信息以及最多 44880 字节的 payload 数据。钱包程序会尽可能的将未确认的交易信息放入正在打包的区块中，针对每一笔需要打包的交易，钱包程序会对签名、timestamp 等信息进行校验，校验通过才会放进区块中。 区块信息只包含打包的交易的 Transaction ID，每个交易的详细信息如交易数量，手续费等信息是独立存储的。

### 3.1.4 Nonce 生成

前面我们已经提到，和 POW 的 nonce 是通过执行随机预言函数计算得出不同，POC 则是将 nonce 值进行处理后存储在硬盘中，每个 nonce 的大小是 256K 字节，并且 8192 个哈希值组成。

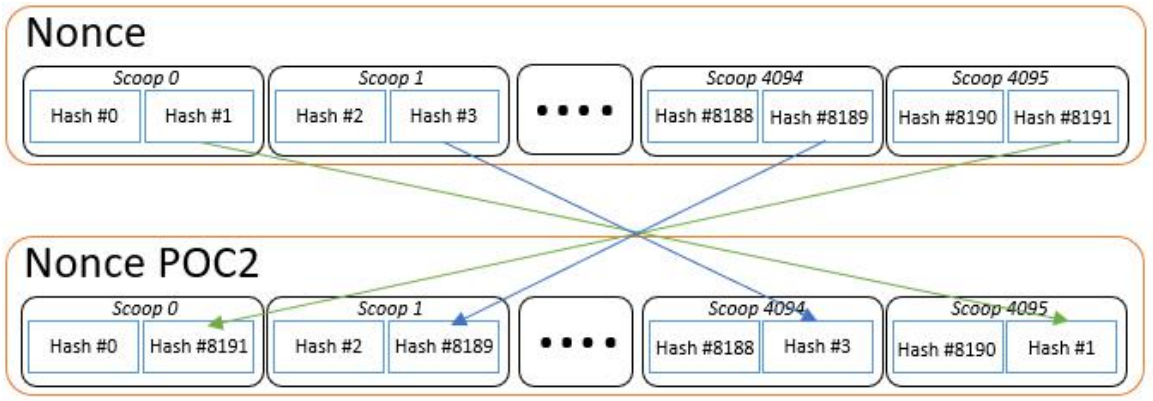
创建 nonce 的第一步是创建 seed，第一个 seed 是一个 16 字节长的值，有矿工 ID 和 nonce 编号组成，我们通过 Shabal256 获得第一个哈希值，我们将这个值放在第一个 seed 前，形成第二个 seed，同时再通过 Shabal256 函数获得第二个哈希值，再将这个值放到上一个 seed 前，形成第三个 seed，以此类推来产生 8192 个哈希值（当拼接的 seed 超过 4096 个字节时，会选择前 4096 个字节作为 seed），最后我们将所有 8192 个哈希值并且初始的 16 个字节拼接，作为最终的 seed，通过 Shabal256 得到一个最终的哈希值。以上过程的伪代码如下:

```
1.  seed= account_id+ nonce_id //8 bytes + 8 bytes
2.  for(i = 0; i < 4096; ++i){
3.      hash = Shabal256(first 4096 bytes of seed)
4.      seed = hash + seed;
5.  }
6.
7.  final_hash = Shabal256(seed);
```

这个哈希值会和以上 8192 个哈希值进行一一异或计算以得到一组总共 8192 个新的哈希值，这组哈希值就是我们写入磁盘的 plot 文件的内容。


### 3.1.5 POC2

2.1.4 中提到的 nonce 生成是基于 POC1.0 的，但是它存在一个公平性问题：由于一个产生的哈希值是顺序的方式依次存入 scoop 中，对于某些”作弊”的矿工，它可以不预先生成 8192 个哈希值，而是只生成 1 个哈希值，剩下的 8191 个哈希值可以在需要进行 deadline 计算时再算出来，如此，原本矿工需要 256K 字节空间的数据，只需要 32 个字节就可以了。 这个问题并不是一个严重的安全漏洞，因为这些”作弊”的矿工只是利用数据结构的特点节省了空间，并没能改变打包区块、验证区块的规则。基于此，POC2.0 被提出来解决这样一个问题，主要就是将原本依次顺序存储在 scoop 中的哈希值进行了调整，调整规则如下：




在 Spock Network 中，我们将采用 POC2 来作为共识算法，POC1 的数据格式不会被兼容。

## 3.2 基于状态转移的区块链系统

和以太坊一样，Spock Network 是一个状态转换系统，通过建立终极抽象的基础层和内置的图灵完备编程语言的系统使得任何人都可以创建智能合约和去中心化应用。

### 3.2.1 账户

在 Spock Network 中，状态是由账户的对象和两个账户之间转移价值和信息状态转换构成。账户包含以下几个部分的：

- 随机数，用于确定每笔交易只能被处理一次的计数器
- 账户目前的代币
- 账户的合约代码，如果有的话

- 账户的存储
- 账户的标识标号

### 3.3 虚拟机

虚拟机环境(SVM)是任何一个支持脚本语言的区块链项目都需要的功能，同时为了更好更快速的发展开发者生态，SVM 将支持 Solidity 语言，使得现有的 Solidity 开发者几乎不需要二次开发就可以引入到 Spock Network 中。

### 3.4 智能合约安全检查

以太坊上的智能合约经常会爆出层出不穷的安全漏洞等方面的问题，通过 Spock Network 在智能合约的部署的时候会通过智能检测平台检测智能合约漏洞，让对应的智能合约能够将一些潜在的安全隐患扼杀在摇篮之中。

## 4. 发行

SPOK 是 Spock 生态系统内基本流通单位的名称，也是唯一的商业与金融传递截至。除了用于记录账户余额和支付以外，SPOK 还可以应用于系统内的智能合约。

### 4.1 基本信息

| | |
|---|---|
| 总量 | 4,200,000,000 |
| 证明方式 | POC |
| 验证算法 | Shabal256 |
| 区块大小 | 8MB |
| 区块间隔 | 180 seconds |
| 初始单区块产量 | 1800 |
| 减产周期 | 13440 |
| 减产比例 | 1% |

### 4.2 发行

SPOK 共计有 42 亿，由公开预挖的 8%和 POC+POS 挖矿机制的 92%组成。

### 4.3 POC+POS

该发行机制通过 POC+POS 的共识挖矿实现。分为三个阶段，这三个阶段分别被命名为起源阶段、生态发展阶段、生态成熟阶段。

#### 4.3.1 POS 机制(第 2001-无限区块)

当矿工打包一个区块时，若它的地址余额满足抵押的区块量，则可以获得全部收益，否则，矿工的收益= 区块奖励 / 矿工需 Staking * 矿工实际 Staking。

矿工需要 Staking 的量 = 矿工被评估算力 * F(x)，x 等于当前全网算力。

F(x) = 1200 – (算力(P) / 10 – 1) * 8。

当矿工在链上没有满足满 Staking 要求时，少收获到的币将销毁。

#### 4.3.2 起源阶段(第 0-2000 个区块):

所有区块的奖励发行全部都由矿工获得。起源号之后，POS 机制将会启动。

#### 4.3.3 生态发展阶段(第 2001-174720 个区块)

这一时期全网将进行给予 PoS 的 PoC 生态挖矿及基于智能合约的生态建设。

#### 4.3.4 生态成熟阶段(第 174720-无限区块)

这一时期，全网的 Dapp 和开发者生态已经发展较好，由社区进行链上投票决定社区治理奖金池的分配以及后续的生态发展。

### 4.4 治理

Spock 是第一个支持 Solidity 智能合约的 POC 共识公链项目，通过智能合约的支持，社区治理将更加符合区块链精神。

作为一个高度社区自治化的区块链项目，社区的治理会通过持币者投票的方式进行，社区的成员将通过智能合约进行投票决定项目功能拓展及社区治理奖金池的使用。

每当有一个议题需要被讨论时，社区成员可以发起一个智能合约投票，并通过社区广播出去，持有币的用户可以通过钱包程序对该投票进行签名并提交投票结果，当超过 60%持币量的用户时则社区开发人员会遵守社区决定进行系统升级。

议题的发起和投票都会通过智能合约进行，任何人都可以在区块链浏览器上查看议题的投票结果。

## 5. 技术路线图

在技术路线图中，我们以星际迷航的知名剧集作为阶段名称，以此激励我们勇敢无畏的探索未知。

| 阶段 | 时间 | 内容 |
|---|---|---|
| **起源** | Q4, 2018 | 技术研究、方案探讨、筹备 |
| **下一代** | 7 月,2019 | 项目官网、测试网上线 |
| **海航家号** | 8 月,2019 | 主网、创世矿池上线 |
| **企业号** | Q4,2019 | 智能合约平台上线 |
| **发现者号** | Q1,2020 | 扩大开发者生态 |
| **深空九号** | Q2-Q4,2020 | 存储层协议共识升级, 支持多文件 |
| **未来之城** | 2021 | 构建去中心化存储数据应用网络 |

## 6. 引用


1. Dziembowski S., Faust S., Kolmogorov V., Pietrzak K. (2015) Proofs of Space. In: Gennaro R., Robshaw M. (eds) Advances in Cryptology -- CRYPTO 2015. CRYPTO 2015. Lecture Notes in Computer Science, vol 9216. Springer, Berlin, Heidelberg. https://eprint.iacr.org/2013/796.pdf
2. Park, S., Pietrzak, K., Kwon, A., Alwen, J., Fuchsbauer, G., Gaži, P.: Spacemint: A cryptocurrency based on proofs of space. Cryptology ePrint Archive, Report 2015/528 (2015). http://eprint.iacr.org/2015/528
3. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf
4. Buterin, V.: A next-generation smart contract and decentralized application platform. White Paper (2014b)
5. Burst wiki https://burstwiki.org
6. Burst blog https://www.burstcoin.ist


## 7. 附录

本白皮书本文件是 SpockChain 项目阐述的概念性文件【白皮书】，并非出售或者征集招标相关公司的股份、证券或其他受管制产品。这份文件可能随时会被修改或者置换，然而我们没有任何义务更新此版本白皮书，或者提供读者额外资讯的渠道。

**法律申明**

SPOCK Token (“SPOCK Tokens”)的销售内容仅作为针对特定面向的人群或参与者的交换 媒介，也不是任何形式的招股说明书或要约文件，也不打算构成任何形式的证券要约、商业信 托中的单位、集体投资计划中的单位或任何其他形式的投资，或任何司法管辖区中任何形式的 投资的要约。 没有监管机构审查或批准本白皮书中列出的任何信息。 本白皮书尚未在任何管 辖区的任何监管机构注册。 通过访问和/或接受拥有本白皮书或其部分(视情况而定)中的任何 信息，默认您符合以下条件：

(a) 您不在中华人民共和国境内，也不是中华人民共和国的公民或居民(税收或其他方面)， 或居住在中华人民共和国境内；

(b) 您不在美利坚合众国，也不是美利坚合众国的公民、居民(税收或其他方面)或绿卡持有 者，或居住在美国；

(c) 根据您所在地区的法律、法规要求或规则，您不在禁止、限制或未经授权以任何形式 或方式出售令牌的司法管辖区内，无论是全部还是部分；

(d) 您同意符合以上描述的条件限制和约束。

**风险提示**

本信息并不代表投资建议、或同意销售的许可，以及引导和吸引任何的购买行为。