BKKI Whitepaper

V1.0 CopyRight BKKI 基金会 HK（香港）2020

**BKKI**

**BKKI** V1.0 CopyRight BKKI 基金会 HK（香港）2020



目录

[**1、项目概述** 3](#_Toc50056511)

[**2、主要技术架构** 3](#_Toc50056512)

[2.1 采用 PoW/工作量算法 3](#_Toc50056513)

[2.1.1 PoW 工作量证明 4](#_Toc50056514)

[2.1.2 PoW 工作量证明流程 6](#_Toc50056515)

[2.1.3 PoW 共识记账 8](#_Toc50056516)

[2.2 结合 PoS/权益证明机制 9](#_Toc50056517)

[2.2.1 PoS 权益证明 9](#_Toc50056518)

[2.2.2 PoS 设计下的区块生成 10](#_Toc50056519)

[2.2.3 基于 PoS 的造币（ML） 12](#_Toc50056520)

[2.2.4 校验机制:保护历史数据 13](#_Toc50056521)

[2.2.5 区块签名及双重权益协议 14](#_Toc50056522)

[2.2.6 节能 15](#_Toc50056523)

[2.3 BKKI 挖矿机制 15](#_Toc50056524)

[2.3.1 节点计划 15](#_Toc50056525)

[2.3.2 节点挖矿 15](#_Toc50056526)

[2.3.3 挖矿半衰期 16](#_Toc50056527)

[**3、商业前景** 17](#_Toc50056528)

[**4、发行计划** 17](#_Toc50056529)

[4.1 BKKI 发行 17](#_Toc50056530)

[4.2 BKKI激励机制 19](#_Toc50056531)

[4.3 BKKI 分配方案 19](#_Toc50056532)

[4.4 BKKI 公募计划 19](#_Toc50056533)

[**5、项目团队** 21](#_Toc50056534)

[**6、开发计划与进程** 22](#_Toc50056535)

[**7、免责声明** 22](#_Toc50056536)

[**8、联系我们** 23](#_Toc50056537)

**BKKI** V1.0 CopyRight BKKI 基金会 HK（香港）2020



# 1、项目概述

BKKI项目开发团队利用区块链思维对社区进行解构和重塑。

互联网时代的社区应该是将具有共同属性的用户聚集在一起并提供共识内容进行互动。社区运营就是

尽可能长时间的维持这样一个聚集在一起有共同属性的用户并产出内容和相互互动的场景。

在区块链社区中都是有相同爱好聚集在一起的用户，在社区中大家可以互相的学习和分享关于区块链

的一些内容进行互动，区块链社区的稳定也是需要一个相互互动的场景，并且是有共同属性的，区块链社

区也是这几年才出现的词汇，但表达的意思其实非常宽泛。

因此，一个优秀的社区应该包括项目方、投资人、开发者、业务伙伴等多种角色，

# 2、主要技术架构

## 2.1 采用 PoW/工作量算法

PoW，全称 Proof of Work，即工作量证明，又称挖矿。大部分公有链或虚拟货币，如比特币、以太

坊，均基于 PoW 算法，来实现其共识机制。即 BKKI区块根据用户挖矿贡献的有效工作，来决定 BKKI 的分配。

## 2.1.1 PoW 工作量证明

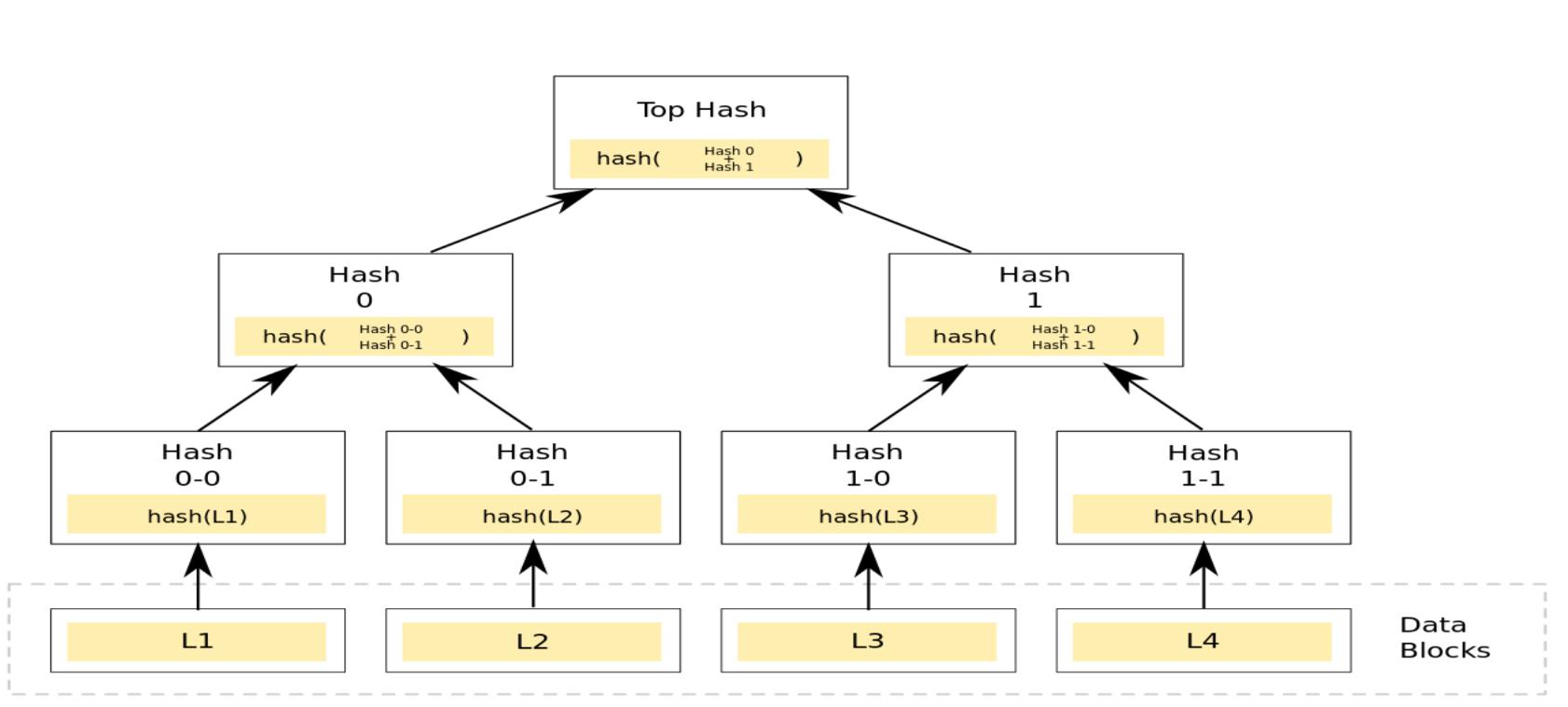
1）工作量证明函数

在 BKKI 中使用的是 SHA256 算法函数，是密码哈希函数家族中输出值为 256 位的哈希算法。

2）区块

区块体的 Merkle 树算法：

**BKKI** V1.0 CopyRight BKKI 基金会 HK（香港）2020



**Merkle 树算法图解**

如上图所示，首先对 4 个交易记录 L1--L4,分别计算 hash(L1)--hash(L4),然后计算 hash0=hash0-0+hash0-1 和 hash1=hash1-0+hash1-1，最后计算出根节点的 hash 值 top hash。

3）难度值

关于难度值，我们直接看公式：

新难度值=旧难度值\*（过去 2016 个区块花费时长/20160 分钟）

目标值=最大目标值/难度值

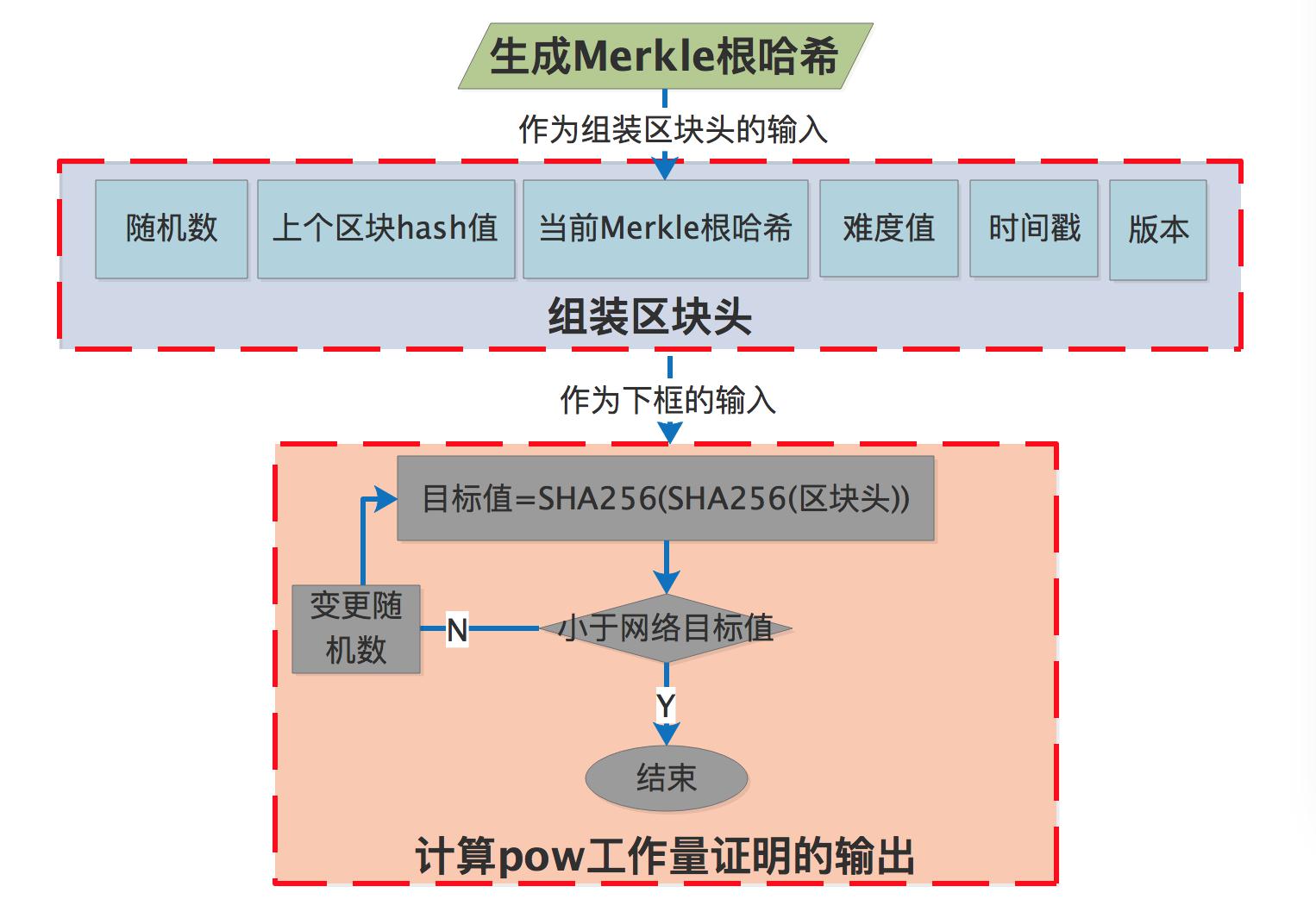
新难度值解析：撇开旧难度值，按比特币理想情况每 10 分钟出块的速度，过去 2016 个块的总花费接近 20160 分钟，这样，这个值永远趋近于 1。

目标值解析：最大目标值为一个固定数（具体可查阅资料了解，这里不做详述），若过去 2016 个区块花费时长少于 20160 分，那么这个系数会小，目标值将会被调大些，反之，目标值会被调小，因此，比特币的难度和出块速度将成反比例适当调整出块速度。

**BKKI** V1.0 CopyRight BKKI 基金会 HK（香港）2020



## 2.1.2 PoW 工作量证明流程



**PoW 工作量证明流程图**

从流程图中看出，PoW 工作量证明的流程主要经历三步：

1）生成 Merkle 根哈希

生成 Merkle 根哈希在第二章节中的第 2 要素中已经有讲解，即节点自己生成一笔筹币交易，并且与其他所有即将打包的交易通过 Merkle 树算法生成 Merkle 根哈希，所以为什么说区块是工作量证明的三要素之一。

2）组装区块头

区块头将被作为计算出工作量证明输出的一个输入参数，因此第一步计算出来的 Merkle 根哈希和区块头的其他组成部分组装成区块头，这也就是为什么我们在前言中大费周章的去提前讲解比特币的区块头。3）计算出工作量证明的输出

下面我们直接通过公式和一些伪代码去理解工作量证明的输出：

1. 工作量证明的输出=SHA256(SHA256(区块头))
   1. if（工作量证明的输出<目标值），证明工作量完成

**BKKI** V1.0 CopyRight BKKI 基金会 HK（香港）2020



iii.if（工作量证明的输出>=目标值）,变更随机数，递归 i 的逻辑，继续与目标值比对。

## 2.1.3 PoW 共识记账

首先，客户端产生新的交易，向全网广播

第二，每个节点收到请求，将交易纳入区块中

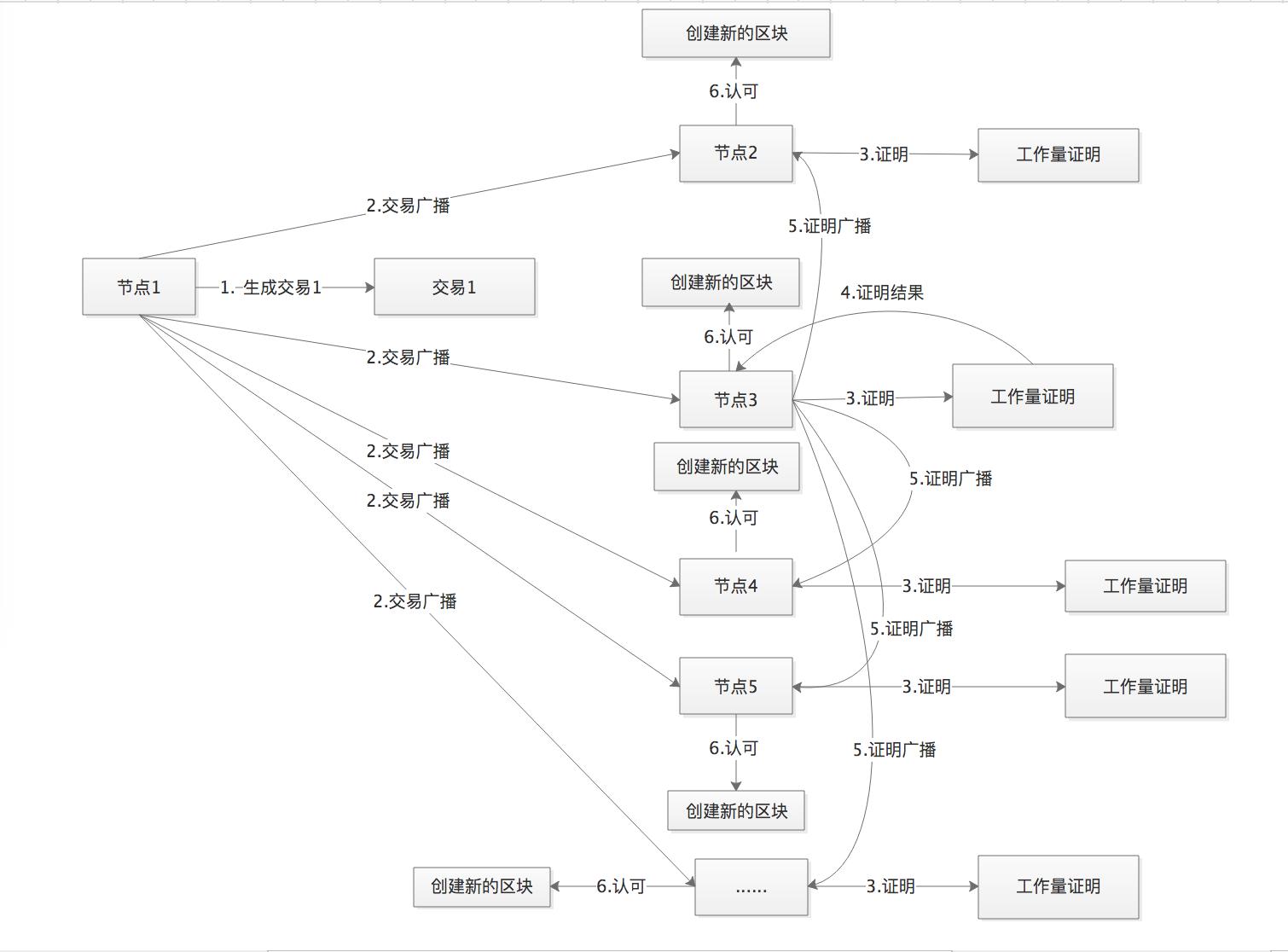
第三，每个节点 PoW 工作量证明

第四，当某个节点找到了证明，向全网广播

第五，当且仅当该区块的交易是有效的且在之前中未存在的，其他节点才认同该区块的有效性

第六，接受该区块且在该区块的末尾制造新的区块

大概时序图如下：



**PoW 工作量证明共识机制时序图**

**BKKI** V1.0 CopyRight BKKI 基金会 HK（香港）2020



# 2.2 结合 PoS/权益证明机制

## 2.2.1 PoS 权益证明

PoS 权益证明（Proof-of-Stake）是一种公共区块链的共识算法类别，它依赖于验证者在网络中的经济利益 。 在基于工作证明（PoW）的公共区块链（比如比特币和当前实施的以太坊）中，算法奖励解决密码难题的参与者，以验证交易并创建新的区块（即采矿）。 在基于 PoS 的公共区块链（例如以太坊即将推出的 Casper 实现）中，一组验证者轮流在下一个区块提出投票并投票，每个验证人投票的权重取决于其存款的大小（即股权）。 PoS 的显着优势包括安全性，集中化风险降低和能源效率 。

一般来说，赌注算法的证明如下所示。 区块链跟踪一组验证器，任何持有区块链基础加密货币（在以太坊的情况下为 ether）的人都可以通过发送一种特殊类型的事务来锁定他们的以太币进入存款 ，从而成为验证器。 然后通过所有当前验证者都可以参与的共识算法完成创建和同意新块的过程。

PoW 是中本聪在技术上的主要突破，但 PoW 的本质意味着 BTC 需要消耗能源来维护运行，维护这样

一个网络的运转需要消耗大量的成本。这是用户通过通货膨胀及交易费的组合来支撑的。随着 BTC 网络采

矿产出下降，最终其可能提高交易费用来维持整个网络的安全性。很自然地我们就会问：是否一个去中心

化的电子货币，都必须消耗大量能源（来维持运行）呢？因此 ML 在理论上和技术上都是一个非常重要的

突破，即 P2P 的电子货币系统并非一定要依赖能源消耗才能维持其安全。

早在 2011 年 BTC 圈子中就有了对 PoS 权益证明这个概念的讨论。大概说来，PoS 指的是一种对货币

所有权的证明。一笔交易所消耗的币龄可被视为 PoS 的一种形式。我们在 2011 年 10 月独立发现了 PoS

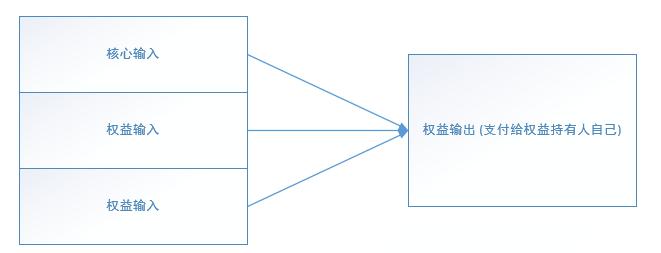
及币龄的概念，当时我们意识到通过对 BTC 造币及安全模式精心地进行重新设计，PoS 实际上可以取代

PoW 的大部分功能。这主要是因为，和工作量证明 PoW 一样，PoS 权益证明也不可能被轻易伪造。当然，

这也是货币系统中的一个关键特性-防止伪造。从哲学角度而言，货币在过去就是一种“工作量证明”，因

此其本身可以代替工作量的证明。

**BKKI** V1.0 CopyRight BKKI 基金会 HK（香港）2020



## 2.2.2 PoS 设计下的区块生成

**PoS 交易的结构**

在这种新型区块里 PoS 是一种特殊的交易称利息币(coinstake)（依据 BTC 当中的特殊交易：币基(coinbase)而命名）。在交易中，区块持有人可以消耗他的币龄获得利息， 同时获得为网络产生一个区块和用 PoS 造币的优先权。利息币的第一个输入被称为 核心（Kernel），并需要符合某一 Hash 目标协议。由此 PoS 区块的产生具有随机性，这一过程与 PoW 相似。但有一个重要的区别在于，（PoS）随机散列运算是在一个有限制的空间里完成的（具体来说为 1 hash/未消费钱包的输出\*秒），而不是象 PoW 那样在无限制的空间里寻找，因此无需大量的能源消耗。

权益核心(kernel)所要符合的随机散列目标是以在核心中消耗的币龄的目标值（币\*天 coin-day）（这与 BTC 的 PoW 是不同的，BTC 的每个节点都是相同的目标值）。因此核心消耗的币龄越多，就越容易符合目标协议。例如，如果李明的钱包里放了 100 个 ML，而且 1 年都没有动，那么他可望在 2 天内产生一个权益核心（个人理解为 PoS 的区块）；同理，如果韩梅有 200 个 ML，也放了 1 年没有使用，那么她可能在 1 天内就能产生一个权益核心。

在我们的 PoS 及 PoW 设计中，随机散列的目标值都是持续调整的。这与 BTC 约每两周一次调整不同。

主要目的是为避免采矿产出的突然波动。

### 2.2.3 基于 PoS 的造币（ML）

除了 BTC 的 PoW 区块之外，在 ML 中还有一种新型的 PoS 造币过程。PoS 区块将根据在交易中所消

**BKKI** V1.0 CopyRight BKKI 基金会 HK（香港）2020



耗的币龄产生利息币。设计时设定了每币一年将产生 1 分（利息），以避免将来的通胀。

虽然我们在造币时保留了 PoW，使最初的造币更加方便，但是可以预料到的是在一个纯粹的 PoS 系统里，最初的造币可以种植在创世区块里，形式类似于现实证券市场中的 IPO。

## 2.2.4 校验机制:保护历史数据

使用消耗币龄总数来决定主链的不足之处在于其降低了攻击整个区块链历史的成本。即使 BTC 在保护历史数据方面有较强的机制，但中本聪仍在 2010 年提出了校验机制来保护区块链历史，防止任何可能在校验点之前对区块链的修改。

另外一个忧虑是双重支付的成本也可能降低了，由于攻击者可以累积一定量的币龄来迫使区块链重组。为使此系统在商业上具操作性，我们引入了一个中心校验机制，每一天大概会向全网广播若干次，以冻结区块链及结算交易。这种新型的校验机制与 BTC 的警报系统类似。

Laurie(2011) 提出 BTC 并没有完全解决大家的担忧，即校验机制没有发布给大家。我们尝试设计一种可行的去中心化的校验机制，但发现在对抗网络分叉(fork)时很困难。虽然向全网广播的校验机制是一种中心化的形式，但在没有去中心化的解决方案之前，我们认为这是可以接受的。

另外一个使用中心化的广播校验机制的原因是：为了抵御一类 DOS 攻击，在每个节点都接纳一个 PoS 区块到本地数据库（区块树）之前，权益核心必须得到验证。由于 BTC 的节点数据模式（交易索引），需要为数据校验设定一个最后期限，以确保在采纳 PoS 区块进入区块权之前，所有节点都有能力校验与每个权益核心的联接。从实用角度考虑，我们决定不修改节点的数据模式而是使用中央校验机制。我们的解决方案是修改币龄的计算，设置一个最低币龄，比如说一个月，低于这个数字将计算为零。然后中央检验机制被用于确保所有节点都认可过去所有大于 1 个月的交易，由于核心要求不低于零的币龄，这样就让允许权益核心得以验证，这样就必须使用大于一个月的输出。

## 2.2.5 区块签名及双重权益协议

每个区块都必须由其拥有者签名，以避免同一 PoS 受到复制并被攻击者使用。

**BKKI** V1.0 CopyRight BKKI 基金会 HK（香港）2020



为了抵御攻击者使用单个 PoS 来产生多个区块进行 DOS 攻击，我们在设计上采用了双重权益协议。

每个节点都会收集其接触到的（核心，时间戳）配对的所有利息币交易信息。假如一个已接收到的区块包

含与其它之前收到的区块中的配对信息（核心，时间戳）是重复的，我们会忽略此区块直到后者被孤立

(orphaned)出去。

## 2.2.6 节能

当 PoW 采矿产出趋近于零时，其对矿工的激励作用就会越来越弱。长远来看，由于矿工失去使用 PoW 方式采矿的兴趣，网络消耗的能量就会降到非常低的水平。除非交易量/交易费用升到相当高的水平，否则 BTC 网络将难以维持这样能源消耗。在我们的设计中，即使 PPC 网络中消耗的能源接近于零，其仍被 PoS 保护着。假如一种电子密码货币允许 PoW 趋于零的话，我们将这种币称为长期节能货币。

# 2.3 BKKI 挖矿机制

## 2.3.1 节点计划

多层次的节点计划

## 2.3.2 节点挖矿

每个节点对应相应的挖矿系数，每 24 小时为一个计时周期。

## 2.3.3 挖矿半衰期

每达到 BKKI 币可挖矿总量的一半即产量减半一次，创世挖矿总量为发行量的 55%，5500万个，挖出 1430 万个第一次减半后续减半以此类推。

**BKKI** V1.0 CopyRight BKKI 基金会 HK（香港）2020



# 3、商业前景

一是在社区层面建立强有力的共识机制，对社区群组进行引导，可以有效提升社区的凝聚力和战斗力，

改变纯炒币社区一团散沙的局面。

二是在社区统一共识的基础上，根据需要，建立不同方向和领域的群组，形成群组独有的特点，给群

组更多的自主权和激励手段，可以有效提高群组的活跃度，形成百花齐放的局面，让社区更具活力和吸引

力。

三是通过群组各自优势的有效互补，形成大规模的协作网络，促进群组的协同发展和社区的整体繁荣。

四是创新业务，BKKI 社区将持续深入研究数字资产市场，提供更多的金融创新产品和服务。

利用区块链的思维理念构建社区生态，稳步推进的BKKI 生态节点计划。BKKI公链生态节点计划，将社区的中心化管理，转变为有效去中心化的管理，由BKKI 基金会提供技术支持和激励机制，由各个节点团队选择发展方向、进行业务拓展。节点充分发挥自身优势，并进行有效协作，节点也可以带来外部资源，各个

节点为整个公链生态的繁荣做出贡献，也分享着生态发展的成果。

# 4、发行计划

## 4.1 BKKI 发行

BKKI，是BKKI 官方发行的原生加密数字货币令牌，是基于以太坊 ERC20 发行的 token。BKKI 是一个去中心化，社区自治理的区块链平台，BKKI 采用持币即挖矿的机制，持有 BKKI 将享有投票，分红等权益。BKKI 应用链的唯一基础 TOKEN，将用来作为社区奖励、结算、交易、以及BKKI应用链的智能合约履约使用。

BKKI共发行总量 1.1亿枚。由BKKI 基金会一次性创设出来，其总量上限已设定，不可更改，不可增发。BKKI 将按照一定的规则和比例分配给不同的持有人。

**BKKI** V1.0 CopyRight BKKI 基金会 HK（香港）2020



## 4.2 BKKI激励机制

BKKI 社区将根据社群发展情况推出持币激励，激励方案后续定制。

## 4.3 BKKI 分配方案

BKKI 计划发行总量为1.1亿枚，团队保留百分之15锁定分批解锁用于BKKI生态建设。

基金将会对团队持有的代币实行两年逐步释放的方案，为保证BKKI发行成功过后，团队能持续完成项目开发计划。

|  |  |  |  |
| --- | --- | --- | --- |
| 百分比 | 用途 | 冻结时间 |  |
|  |  |
|  |  |  |  |
| 5% | Sale | 锁仓两年，每半年按等比例释放代币 |  |
|  |  |
|  |  |  |  |
| 20% | Foundation | 锁定/销毁两年用于构建BKKI生态 |  |
|  |  |
|  |  |  |  |
| 15% | Team | 锁定两年，每半年按等比例释放代币 |  |
|  |  |
|  |  |  |  |
| 5% | Marketing | 两年内使用，用于推广和商务合作 |  |
|  |  |
|  |  |  |  |
| 55% | Mining | 用户挖矿贡献奖励，挖完即止 |  |
|  |  |
|  |  |  |  |

## 4.4 BKKI 市场以及募集计划

BKKI项目无公募私募计划

|  |  |  |  |
| --- | --- | --- | --- |
| 轮次 | 占比 | ETH | 比例 |
|  |  |  |  |
| 机构私募 | 0% | 0 | NULL |
|  |  |  |  |
| 公开白名单 | 0% | 0 | NULL |
|  |  |  |  |

**BKKI** V1.0 CopyRight BKKI 基金会 HK（香港）2020



# 5、项目团队

Ye Zhao， BKKI 联合创始发起人。

多年的技术研发及大型研发项目管理经验。对底层文件数据存储、分布式应用架构有丰富的实战经验和独特见解。对区块链底层技术原理有深入研究，目前带领团队专注于区块链技术创新研发，坚信技术力量将给人类带来更多的生活改变。

Andy Wang，首席战略官。

2016 年开始进入区块链行业发展，区块链信仰者。区块链专家/密码货币顾问/财务顾问。区块链开发和技术加密货币实现绩效管理、谈判项目管理。

Min Xiao，财务系统技术总监。

2017 年开始进入区块链行业发展。对区块链⾦融创新、区块链与传统应用场景结合有独到见解。目前带领团队专注于支付体系建设、社区共识管理、区块链技术创新研发，并认定区块链发展将会开启互联网第二纪元。

Neo，大连理工大学软件博士，BKKI 联合创始发起人。

2018 年进入区块链行业，拥有区块链、媒体等领域经验。拥有丰富的管理实战经验，并建立了完善的方法论和管理体系，擅长于区块链项目营销运作，对互联网新型媒体与区块链传播结合有深入的研究和见解。

**BKKI** V1.0 CopyRight BKKI 基金会 HK（香港）2020



# 6、开发计划与进程

2020年 Q2完成支持积分化的BKKI平台构思

2020 年 Q3 BKKI通过积分化安全审计

2020 年 Q3 完成BKKI与钱包融合，完成PC，IOS，Android全平台开发

# 7、免责声明

BKKI 未授予参与本基金会或其资产的权利。BKKI 基金会未向BKKI 持有人提供本基金会的

任何所有权或其他利益。获得BKKI 不等于可以用 TOKEN 换取本基金会任何形式的股份或本基金会

资产（包括知识产权）。

# 8、联系我们





**网站：https://bkki.com**