prajna paramita

# 白皮书

PRAJNA FUND

版本：V1.00

更新时间：2018.05.15

官网：www.prmichain.com

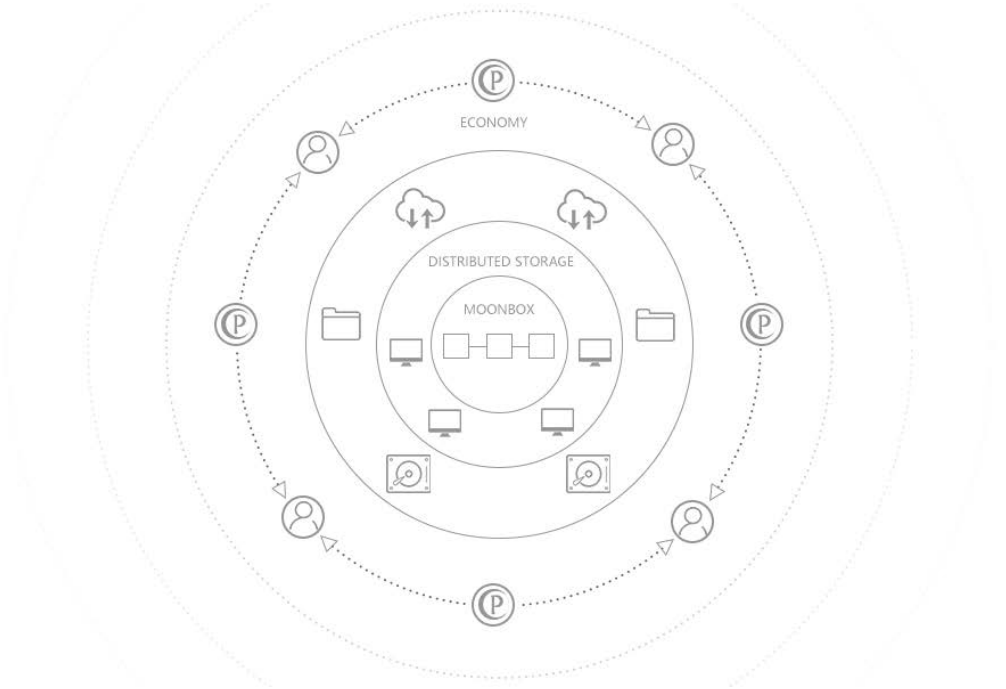
# 摘要

随着互联网+区块链时代的到来，我们网络环境正在悄然发生一场变革：集中式服务器正在被去中心化开放服务器所替代、信任式参与被可验证式计算所替代、脆弱的位置寻址被弹性的内容寻址所替代、低效率的整体式服务被点对点算法市场所替代、区块链技术已经证明去中心化账本的可行性。客户端加密的点对点云存储网络将允许用户传输和共享数据，而无需依赖第三方存储提供商。取消中央控制将缓解大多数传统的数据故障和中断，同时显著提高安全性、隐私性和数据控制。

Prajna Paramita Cloud是一个去中心化的区块链分布式云计算服务平台，它让云存储变成一个算法市场。这个市场运行在有着本地协议令牌的区块链链条上。区块链上的矿工可以通过自己的剩余空间、带宽和文件等数据资源参与到分享和交换来获取PRMI奖励。Prajna Paramita Cloud的云存储网络为整个过程提供安全保障，因为内容在客户端端对端是加密的，而存储提供者和其他用户不能访问到解密密钥。Prajna Paramita Cloud可以为任何数据提供存储基础架构的IPFS最上面的激励层。它对去中心化数据、构建和运行分布式应用程序，以及实现智能合同都非常有用。

# Prajna Paramita Cloud概要

Prajna Paramita Cloud是一个去中心化的区块链分布式云计算服务平台。通过Prajna Paramita Chain、MoonBox（分布式硬件终端）、去中心化存储网络、点对点超媒分发协议技术实现全球分布式云计算平台，它是一个面向全球的、点对点的分布式云存储计算平台。




## 背景

在过去云存储几乎完全依赖于大型存储供应商作为可信的第三方来传输和存储数据。该系统存在基于信任的模型固有的弱点。由于客户端加密是非标准的，传统的云容易受到各种安全威胁的影响，包括中间人攻击、恶意软件和暴露私人消费者和公司数据的应用程序缺陷。此外，在这个全民上网的时代，集中式服务器显然不能满足日益增长的上网需求。

## 区块链技术的发展

自2009年比特币诞生，区块链技术开始登上历史舞台。区块链技术的核心优势是不再需要一个传统的中心化机构，仅通过加密算法、共识机制、时间戳等技术手段，在分布式系统中实现了不依赖于某个信用中心的点对点交易、协调和协作，从而规避中心化机构普遍存在的数据安全，协同效率和风险控制等问题。

近些年，人们主要围绕区块链的去中心化、共识算法、安全匿名进行创新，如：石墨烯、闪电网络对交易性能的提升；权益证明（Proof of Stake，简称 POS）、委托权益证明（DPOS）、实用拜占庭容错（Practical Byzantine Fault Tolerance，简称 PBFT）对共识算法的丰富和改进；零知识证明（Zero-knowledge Proof，简称 ZKP）、混币提升交易安全等。

## Prajna Paramita Cloud的意义

### 资源合理利用

通过去中心化和共享文件的方法，解决了个人电脑硬盘、CPU等资源的闲置问题，将用户的闲置硬盘和CPU资源进行收集分配，可以将分布在各处的资源合理利用，，形成集Prajna Paramita Chain链上生态体系中的应用。

### 存储优势

通过分布式存储技术解决了存储空间的浪费，可以自动重新分配数据，提高了存储空间的利用率，将所有具有相同文件系统的计算设备连接在一起。原理用基于内容的地址替代基于域名的地址，也就是用户寻找的不是某个地址而是储存在某个地方的内容，不需要验证发送者的身份，而只需要验证内容的哈希，通过这样可以让网页的速度更快、更安全。

**提升效率，解决网络拥堵**

通过分布式存储具有高容错、高吞吐、就近原则和可移植性使得数据调取不受地域限制更加便捷，出错概率大大降低。点与点之间都是一个自主代理，能够执行这些操作，而无需进行重大的人工交互。

**去中心化网络**

利用去中心化网络DSN聚集全球用户作为存储提供商，并且能自我协调的提供存储数据和检索数据服务给客户。这种协调是去中心化的、无需信任的：通过协议的协调与个体参与者能实施验证操作，系统可以获得安全性操作。DSN可以使用不同的协调策略，包括拜占庭协议，gossip协议或者CRDT，这取决于系统的需求。

## Prajna Paramita Chain

Prajna Paramita Chain 是一个基于区块链的去中心化分布式共享系统，用于端对端之间形成和执行存储契约，在Prajna Paramita Chain上端对端协商契约、传输数据、验证远程数据的完整性和可用性、检索数据和内容地址可寻。Prajna Paramita Chain 通过对出块间隔、区块容量、共识算法的优化，理论上可达到 1000TPS 的可用性能。Prajna Paramita Chain作为Prajna Paramita Cloud平台核心部分链接着所有的终端，让所有的网络终端节点不仅仅只充当 Browser或Client的角色，都可以作为这个网络的运营者，人人都可以是服务器。

### 数据安全性

数据文件在客户端中会默认进行加密后再存储到存储节点。意味着数据存储者实际上无法查看该文件的内容。对于敏感数据，数据所有者可以自行选择使用硬件加密的方式生成加密文件数据后再发布存储到Prajna Paramita Chai节点中。

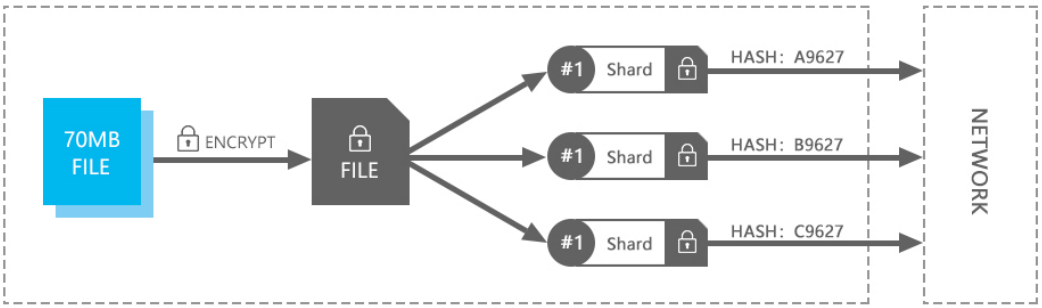
Prajna Paramita Chain要求文件在分片之前应该在客户端进行加密。参考实现使用AES256-CTR，但是可以实现收敛加密或任何其他可调系统。这将保护数据的内容不受存储提供者存储数据的影响。数据所有者保留对加密密钥的完全控制，从而控制对数据的访问。

数据所有者可以分别对文件的分片和在网络中的位置信息进行保密。随着网络中的碎片集合的增长，在不了解它们的位置的情况下找到任何给定的shard集合将变得更加困难。这意味着文件的安全性与网络大小的平方成正比。

碎片大小是一个可协商的合同参数。为了保护隐私，建议将碎片大小标准化为一个字节的倍数，例如8或32 MB。标准化的大小阻止了侧通道试图确定给定碎片的内容，并且可以掩盖通过网络的碎片流。

分片大型文件(如视频内容)和跨节点分发分片减少了内容交付对任何给定节点的影响。带宽需求在整个网络中分布得更均匀，终端用户可以利用并行传输。

由于对等节点通常依赖于单独的硬件和基础设施，所以数据失败是不相关的。这意味着创建碎片的冗余镜像，或者跨碎片集应用奇偶方案是确保可用性的一种极其有效的方法。可用性与存储数据的节点数量成正比。



◇ 文件是加密的。

◇ 加密文件被分割成碎片，或者多个文件被合并成碎片。

◇ 对每个碎片执行审计预处理。

◇ 碎片可以传输到网络。

## 内容寻址

内容寻址存储是通过文件内容生成唯一哈希值来标识文件，而不是通过文件保存位置来标识。相同内容的文件在系统中只会存在一份，节约存储空间。它按照所存储数据内容生成的唯一哈希值来寻址，具有良好的可搜索性、安全性、可靠性和扩展性。

与需要不断改变和更新的结构化数据不同，固定内容的价值源自真实性、长久性、大容量以及可在线获取性等几种特性的结合。内容寻址可以有效应对海量的固定内容信息进行高效地存储、归档、管理、检索和保护。

无重复数据：由于Prajna Paramita Chain链上的每个内容或数据分段都被赋予一个惟一的哈希值，当有重复内容被存储时，因产生同样的哈希值将被系统识别，就避免了相同内容的重复存储。这不仅节省大量空间，提高存储效率，而且极大简化了数据管理。

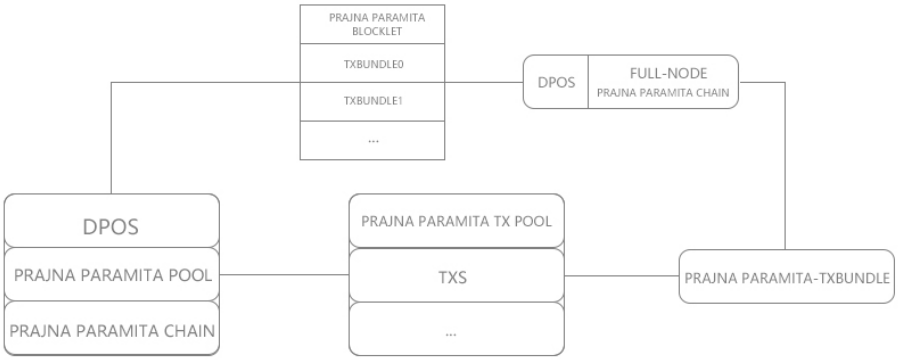
数据完整性：通过赋予数据保留时间等属性轻松实现WORM(只写一次，多次读取)，使数据的真实性与完整性得到完全保护。

提升效率：采用独立节点冗余架构，使用多个标准化的服务器作为节点组成网格，用户访问某个文件，会广播哈希请求，找到存储该文件的节点，传输给用户。

有效降低成本：Prajna Paramita Chain采用近线归档存储，对存储数据通过云计算进行合理归档存储，能够支持大量用户访问和集中管理有效降低成本。

Prajna Paramita Chain通过内容寻址存储有效降低了整个存储系统理解、管理、操纵存储介质上的信息的物理或逻辑位置的难度；同时利用模块化的硬件架构有效地管理存储资源，对用户和应用保持透明，使Prajna Paramita Chain系统全面满足固定内容的可获取性、真实性、长期性和可管理性的苛刻要求。

## 共识和出块



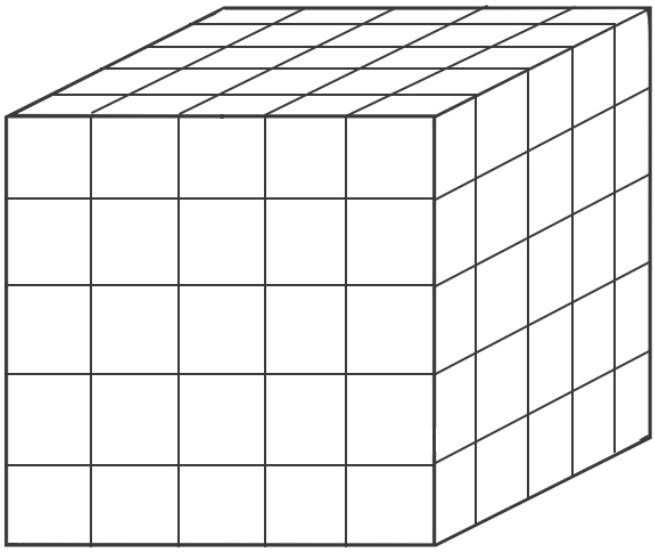

共识出块的是由交易包（Tx-Bundle）、Prajna Paramit Blocklet组成。这种算法是基于DPOS共识机制，一个交易包中包含了Prajna Paramita Chain的交易记录。由全节点生成包含了不同交易包的区块并公布到区块网络上。

信息上链

不是所有的数据和信息都需要发布存储到链上，链上保存的对象是内容可寻地址作为资源地址的标记。除开基本的区块信息外，存储在链上的有：账务交易、对象数据、存储交易、证明交易。

## 去中心化存储网络

在去中心化计算的应用中，有一个划时代的概念那就是受激励的去中心化在线文件存储系统。目前，如果你想你的文件或者数据安全地在云端备份，你有三种选择：1、上传它们到自己的服务器；2、使用一个中心化的应用，如 Google drive 或者 Dropbox，或者是；3、使用已经存在的去中心化的应用，如 Freenet。这些方法都有它们自己的缺点：第一种方法有着昂贵的建立和维护费用；第二种方法依赖于一个单可信任实体，并且常常涉及重大价格上涨；第三种方法速度慢，对每一位用户在空间容量方面有着很高的限制，因为它依赖于用户自愿奉献存储空间。受激励的文件存储协议有潜力成为第四种方法，通过去中心化激励执行者 (存储用户数据的客户) 参与其中成为节点，提供高容量存储与高质量服务。



简单来说你拥有一个 10 GB 大小的文件，你想将其分散到网络中。首先，你加密该文件，然后你分割该文件为 125 块。你安排这些块组成一个 3 维的 5X5X5 的立方体，指出每一个轴的多项式，并且扩展每一个轴，到最后你可以得到一个 7X7X7 的立方体。你可以寻找乐意存储这些块的 343 个节点，并且只告诉每一个节点它属于那一轴

的节点们的实体信息。为了下载整个文件，你会针对所有块发出一个请求，然后查看进来的哪一块拥有最高的带宽，只要满足最小数量的块到达，你可以使用数学运算来解密该文件，并且在本地复原该文件。

去中心化存储，技术上不同于分布式存储。去中心化存储是在一个更加分散、更加不可信的网络环境中，满足一个更加安全、更加可信、更加可控的存储的需求。去中心化存储的目标主要有三：

首先是安全性，传统中心存储很容易被黑客攻击，例如日本的比特币交易所就被黑客攻击，各个国家的银行系统都被黑客攻击过，甚至出现监守自盗的情况，而去中心化存储，将数据切割，分散存储在整个网络上，黑客无法都全网匿名节点展开攻击。

其次是速度快，效率高，中心化服务器并不是离所有用户都近，而Genaro的去中心化存储优先选取离每个用户最近的节点。

最后是性价比高。去中心化存储网络形成交易市场，利用的是闲置资源，成本比中心化固定成本要低很多，并且分享者自由竞价从而达到一个最低价格，用户对每个文件的存储可以自定义设置不同的安全等级，花费也不同。

## Kademlia协议

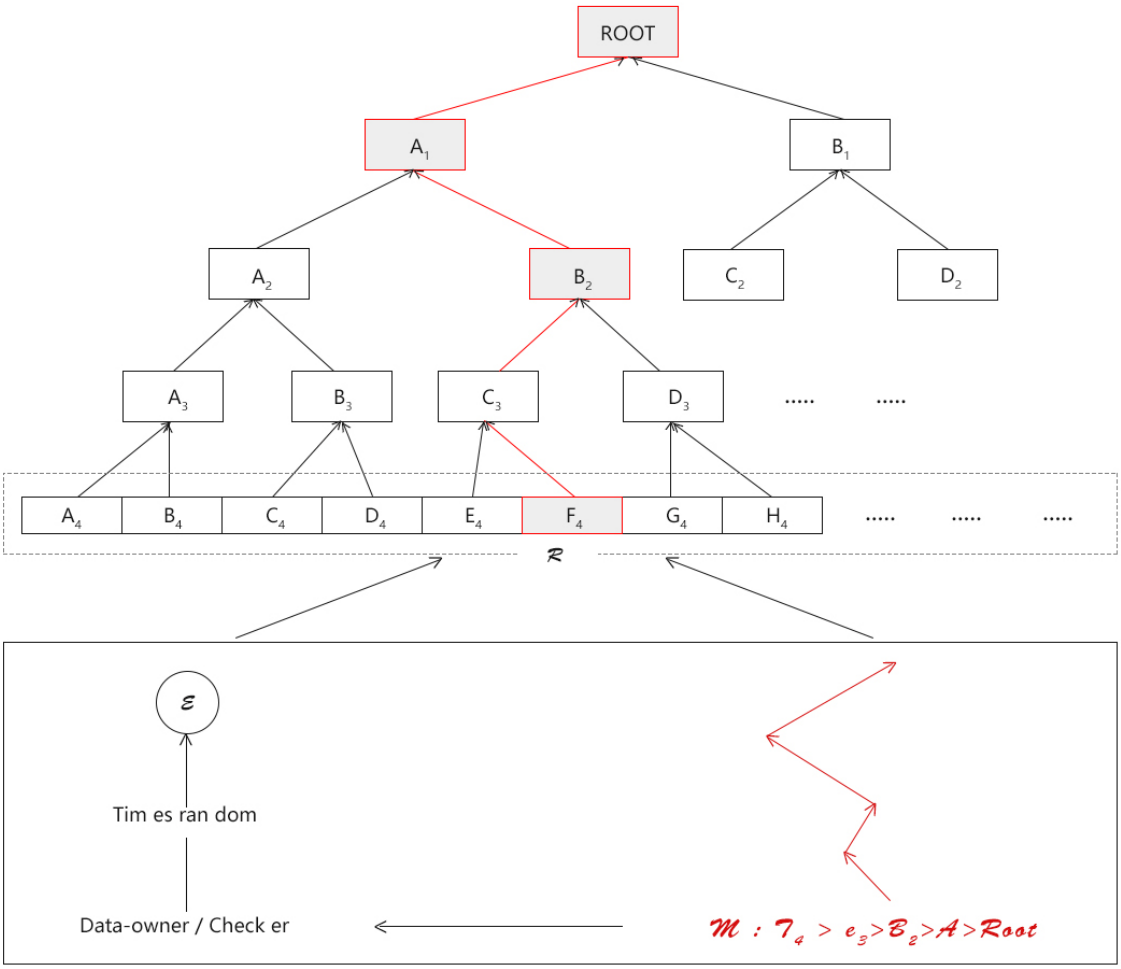
Prajna Paramita Chain的设计需要构建一个拥有众多用户和随时有节点加入和退出的对等网络。因此一个好的路由表维护和查找算法是非常重要的。Kademlia协议作为基础来构建P2P对等网络。Kademlia以异或算法（XOR）为距离度量基础构建的分布式哈希表（Distributed Hash Table），大大提高了路由查询速度。这对于存在大量存储节点的Prajna Paramita Chain网络是非常重要的。Kademlia网络的实现会分成两步，首先我们会构建基于简单路由表的P2P网络，在开放存储节点客户端的同时完成Kademlia网络的开发。

Kademlia协议中K桶的节点列表维护正好符合我们对节点的在线要求，不过未来可能会根据POC中对接点的信用评级作为排序和换出的一个权重值，以帮助观察者挑选核实的最近节点进行数据分布的调整。

## 存储证明

引入Merker Tree和Zh-Snark构成POR（备份证明Proof-of-Replica）和POST（存储市场证明Proof-of-Storage&Time）作为存储者（Storer）存储出具的量化凭证。信用等级高的存储节点允许采用POR用较短时间就可以提供证明，信用评级较低的会要求使用POST提供存储市场证明。

### 备份证明Proof-of-Replica



数据所有人可间隔一段时间就向Prajna Paramita Chain网络请求相应的备份证明：

◇ 数据所有人基于时间生成一个校验数C发送到Prajna Paramita Chain网络；

◇ 存储者需要根据C找到对应的数据碎片并生成→（Merkle校验树）；

◇ 如果校验通过Prajna Paramita Chain网络会更新存储账本（Store-Book）和奖励账本（Reward-Book），并解锁存储账本（Store-Book）中该笔交易的部分奖励作为存储报酬。

**存储市场证明Proof-of-ST（Storage and time）**

POR虽然能够保证数据存储者至少会保存数据一次，但是无法避免作恶者进行欺骗，考虑以下场景：

1、存储者在第一次按要求对数据进行备份后，对所有的数据切割和拆分序列计算其Merkle校验数，并删除数据碎片文件仅保存Merkle校验树。

2、存储者收到证明指令后，请求其他保存了数据备份的节点获取数据，并计算出C相应的→（Merkle校验树）。

3、以上场景中，作恶者使用极低的计算和存储成本就可以获得存储报酬。因此引入POST，以确保只要数据存储者没有存储数据碎片文件就无法正确计算出Merkle校验树，也就无法获得报酬：

- 数据切割成碎片后生成一个熵值序列S，然后使用S和数据碎片再生成哈希值R
- 每隔一段时间数据所有者向Prajna Paramita Chain网络发送Sx （基于时间的熵值，全局唯一），存储者需要根据Sx 和对应的数据碎片计算出Rx，并根据Rx 生成相应的Merkle校验树。

有了前置熵值序列，还可以实现由观察者代理进行数据检查。数据所有者可以提供一部分熵值序列交由观察者，由观察者来完成POST的证明校验。为了更加安全地执行，未来会依靠智能合约来实现代理检查逻辑。

### 信用证明Proof-of-Credit

在Prajna Paramita Chain协议中信用证明是和账户绑定的，具体评分体系根据不同客户端有所不同：

- 存储节点：存储总量、存储时长、在线时长、被惩罚量；
- 全节点：最大交易处理量、出块速度、分叉收敛速度、在线时长；
- 观察节点：索引服务性能、在线时长；
- 数据所有者：存储数据量、交易量；
- 证明人：证明量；

## 共识机制

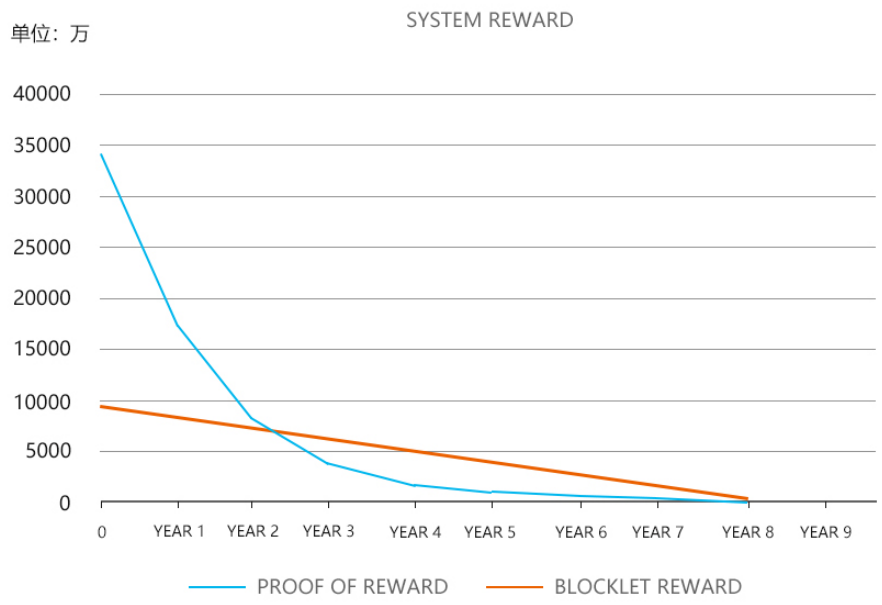
由于分布式的特点，区块链需要共识机制才能正常运转。Prajna Paramita Chain选取DPOS 共识机制，DPOS不需要消耗额外算力即可实现产块后的权益分配，它还能会根据网络的交易状态动态决定由代理或全体节点验证智能合约的执行结果。

持有 Prajna Paramita Chain 的 Token 不仅可获得合约发布、网络分叉等区块链基础服务，还能参与投票，有机会成为代理节点提供服务获得 Token 奖励。 Prajna Paramita Chain 把这种 Token 命名为 PRMI，每一个 AAC 持有者称之为权益人，根据所持的PRMI 数量分配相应的投票权重。代理节点由权益人投票选出。得票最多的前 31 个成为代理节点，依次轮流验证交易，工作顺序由得票多少决定。代理节点正常工作可以获得收益，若工作异常或不工作，则会受到惩罚。

## 奖惩制度

### 系统奖励

Prajna Paramita Chain网络为了鼓励更多节点加入，形成更加健全的生态体系。对各个做出贡献的节点发放系统奖励。




出块奖励 出块的时间设置为5分钟（最快能10秒产出一个区块）。每天能产出288块区块，一年能产出105,120块区块。矿池节点第一年每产出一个Prajna Paramita Chain区块约获得1623个PRMI奖励，每台矿机根据所提供算力值和所处矿池整体算力来获得相应奖励；每产出105,120个区块奖励减半，预估8年完成3.4亿个PRMI奖励发放。

证明奖励 Prajna Paramita Chain网络预留了80,000,000个PRMI作为证明人奖励，激励和邀请具有公信力的组织或者机构担任证明人，为链上数据提供证明服务。

**系统惩罚**

Prajna Paramita Chain会对一下危害生态的情况进行系统惩罚，包括扣除奖励币PRMI并降低其信用等级。

丢失数据　不再支付后续存储数据的报酬，降低其信用评级，低到阈值后该用户会被加入黑名单并无法再连入Prajna Paramita Chain网络。

恶意攻击　不管是蓄意攻击而不出块，还是大量通过非正常手段获取PRMI，对Prajna Paramita Chain网络和程序仅供都将会触发最高级别的惩罚：该节点和关联用户被加入黑名单并无法再连入Prajna Paramita Chain网络，还会魔兽该账户上所有的PRMI币。

欺诈　欺诈通常会被发现于时候，目前无有效办法追回已支付的报酬和系统奖励。只能降低其信用评级，降低到阈值后该用户会被加入黑名单并无法再连入Prajna Paramita Chain网络。

### 智能合约机制

智能合约使得Prajna Paramita Chain的用户可以花费令牌向市场请求存储/检索数据和验证存储证明。用户可以通过将交易发送到账本触发合约中的功能函数来与智能合约交互。我们扩展了智能合约系统来支持Prajna Paramita Chain的特定操作（如市场操作，证明验证）。

## Prajna Paramita Chain设计原理

节点不可靠假设：基于区块链的中心化网络组织结构，允许单点故障和短时间内节点处于不可用状态；

所有权和隐私：数据所有者具有数据的所有权和完全访问权，数据是加密并具有隐私性的。经过所有者授权后其他角色才能访问和使用数据；

可量化的贡献度：参与协议各方的贡献度都应该有相应的量化标准和可被观测的贡献度。比如POST和POR作为存储空间和存储时间的量化证明；

最终状态一致性：允许数据对象在不同节点处于不同状态，但其状态能快速收敛获得全网节点一致；

可检测和可恢复：能检测整个网络的可用性和数据对象的全网状态，并根据策略一定程度自主修复；

可审计和监管：可在某些特定领域或场景进行一定程度的监管和审计，前提是数据所有者知悉并同意；

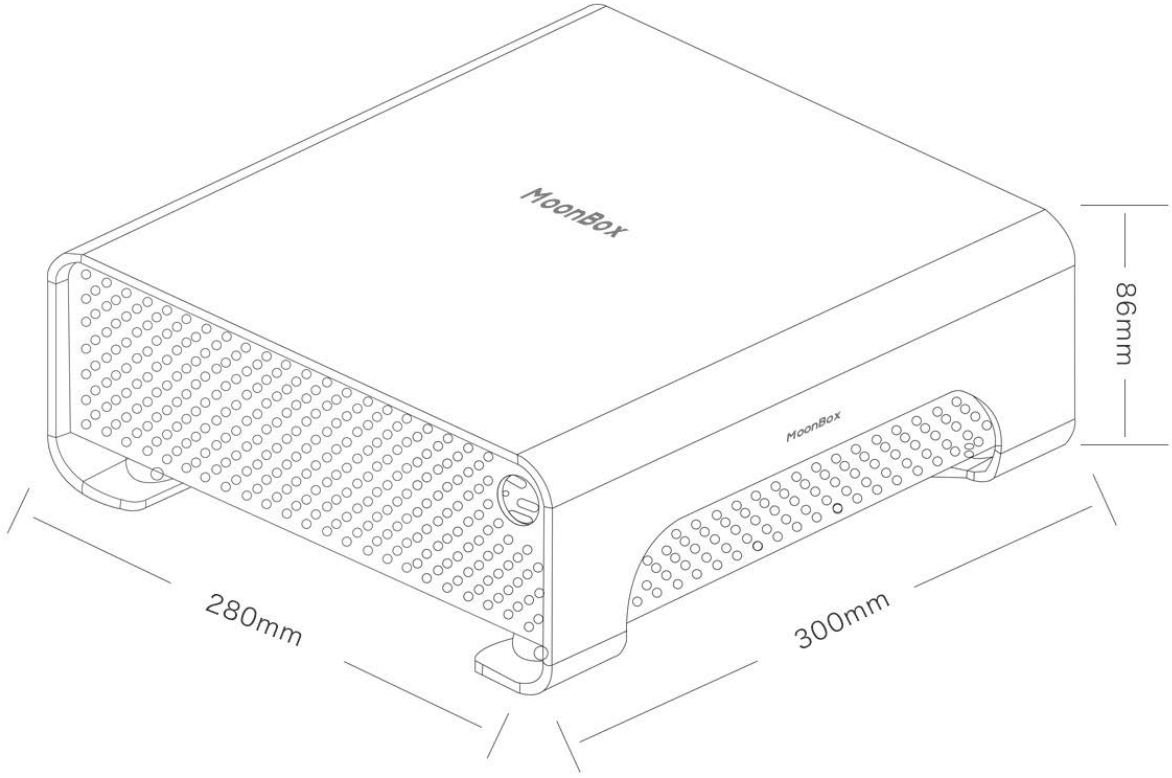
可拓展API：具有很高拓展性和易用性的API。

共识机制：基于DPOS共识机制

## MoonBox介绍

MoonBox 是一款基于区块链技术的硬件产品。通过智能合约对用户制定奖励制度的通用硬件主机。内部设有128GSSD 硬盘存储，并且可外接硬盘存储设备，凭借用户提供的闲置资源为互联网业务提供全面稳定的 CDN 服务，为下载平台、UGC 加速平台、流媒体平台、动态加速平台等一系列创新而有价值海量业务加速服务，未来Prajna Paramita Cloud将开放更多的海量服务能力，为用户提供更满足互联网业务需求的CDN 加速服务。用户可以通过 MoonBox共享闲置的存储空间与带宽参与到Prajna Paramita Chain节点中来赚取PRMI币。

作为 Prajna Paramita Cloud 的核心部分之一的 MoonBox将成为 Prajna Paramita Cloud 的节点，随着节点的数量发展，Prajna Paramita Cloud 的分布式云空间加大，算力增强，从而实现分布式云计算系统。




MoonBox设计尺寸仅为300mm*280mm*86mm更加mini小巧便携，整体时尚美观，性能卓越的基础上，兼具静音环保，办公、家用、挖矿轻松搞定。

# 应用场景


**办公、上网、游戏娱乐**

MoonBox 是一台基于 Win10 系统，集办公、上网、游戏等多种功能为一体的硬件设备。无论是日常办公软件、作图工具或是高性能游戏等，MoonBox都能轻松驾驭，小巧的机身，高速的运算能力，极快的数据读取速度和强大的软件兼容性的特性让企业办公变得便捷又环保。

**共享存储**

MoonBox 可提供海量、安全、可靠、低成本的 CDN 云存储服务，提供数据的可靠性。用户开启MoonBox链接网络可以在互联网上进行存储和访问，可外接硬盘设备，使容量和处理能力弹性扩展，多种存储类型供选择全面优化存储成本。

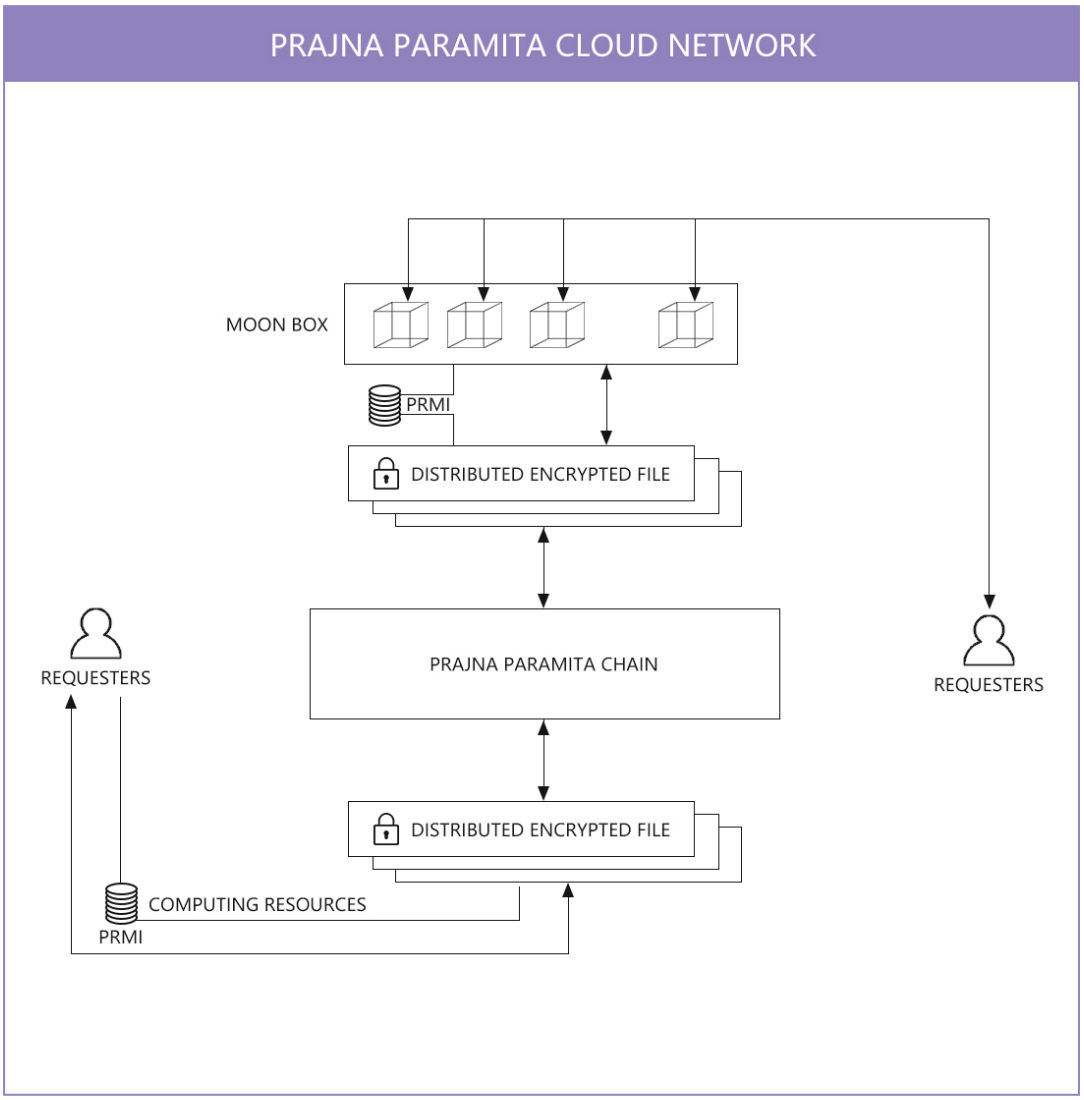
**获取PRMI奖励**

MoonBox基于 Prajna Paramita Chain 生态激励机制的终端节点，用户可贡献自己的闲置空间、带宽、算力获取 PRMI奖励。

# Prajna Paramita Cloud生态

Prajna Paramita Cloud是一个去中心化的区块链分布式云计算服务平台。通过Prajna Paramita Cloud个人可以分享自己的剩余空间、带宽和流量参与到数据资源分享和交换中来，每个普通用户可以成为中心化共享云计算系统里的资源节点并获得区块奖励—PRMI币。

## Prajna Paramita Cloud概述



Prajna Paramita Cloud平台采用雾计算作为核心，雾计算是半虚拟化的服务计算架构模型，与云计算相比，雾计算所采用的架构更呈分布式，更接近网络边缘。雾计算将数据、数据处理和应用程序集中在网络边缘的设备中，而不像云计算那样将它们几乎全部保存在云中。数据的存储及处理更依赖本地设备，而非服务器。所以，云计算是新一代的集中式计算，而雾计算是新一代的分布式计算，符合区块链的“去中心化”特征。

雾计算是以个人云，私有云，企业云等小型云为主，雾计算以量制胜，强调数量，不管单个计算节点能力多么弱都要发挥作用，并且雾计算不要求使用者连上远端的大型数据中心就能进行存取服务。雾计算有几个明显特征： 低延时和位置感知，更为广泛的地理分布，适应移动性的应用，支持更多的边缘节点。这些特征使得移动业务部署更加方便，满足更广泛的节点接入。

雾的主要目标是提高效率，并化解传送到云端计算、储存时可能产生的网络塞车现象。数据产生甚至收集的设备不具备计算能力和存储资源，无法执行各种高级分析计算和机器学习任务。因此，雾能够发挥作用，因为它在网络边际运作，在某种意义上更接近云端。云端服务器拥有完成这些项目所需的所有功能，但它们通常太远而无法及时帮助。因为雾让各端点更接近，能够更好的进行数据存储共享。

雾计算是在终端和数据中心之间再加一层，叫网络边缘层。如再加一个带有存储器的小服务器或理由器，把一些并不需要放到”云”的数据在这一层直接处理和存储，以减少”云”的压力，提高了效率，也提升了传输速率，减低了时延。

搭配分布式的雾计算，通过智能路由器等设备和技术手段，在不同设备之间组成数据传输带，可以有效减少网络流量，数据中心的计算负荷也相应减轻。雾计算可以作为介于M2M（机器与机器对话）网络与云计算之间的计算处理，以应对M2M网络产生的大量数据——运用处理程序对这些数据进行预处理，以提升其使用价值。

Prajna Paramita Cloud 是基于 P2SP 技术的支持下，实现可向企业输出的共享计算服务。并且 Prajna Paramita Cloud 将应用区块链技术，建立公平、透明的奖励机制，激励普通个人参与到数据资源的分享和交换中来，使 Prajna Paramita Cloud 的共享计算服务彻底向个人用户开放，每个普通用户都可成为去中介化云计算系统里的共享资源节点，并从这一系统中获得收益。

## Prajna Paramita Cloud特性

### 可靠性

Prajna Paramita Cloud拥有广泛的地域分布，为了服务不同区域用户，相同的服务会被部署在各个区域的区块点上，使得高可靠性成为Prajna Paramita Cloud的内在属性，一旦某一区域的服务异常，用户请求可以快速转向其他临近区域，获取相关的服务。此外，由于Prajna Paramita Cloud减少了发送到云端和从云端发送的数据量，安全可靠性进一步增加。

### 便捷性

Prajna Paramita Cloud支持很高的移动性，手机和其他移动设备可以互相之间直接通信，信号不必到云端甚至基站去绕一圈！此外，Prajna Paramita Cloud也支持实时互动、多样化的软硬件设备以及云端在线分析计算等

### 低延迟

Prajna Paramita Cloud在网络拓扑中位置更低，拥有更小的网络延迟（总延迟=网络延迟 计算延迟），反应性更强。

### 分布式

Prajna Paramita Cloud架构采用分布式，更接近网络边缘，数据的存储及处理不依赖云端服务器。

## Prajna Paramita Cloud工作原理

Prajna Paramita Cloud提供给用户的服务是对所有设施的利用，包括处理、存储、网络和其它基本的计算资源，用户能够部署和运行任意软件，包括操作系统和应用程序。Prajna Paramita Cloud通过分布式云存储以低廉的存储价格为个人或中小企业提供服务器服务、CDN加速服务、文件存储服务、数据交换服务。

### 计算（Computing）

一套控制器，用于为单个用户或使用群组管理虚拟机实例的整个生命周期，根据用户需求来提供虚拟服务。负责虚拟机创建、开机、关机、挂起、暂停、调整、迁移、重启、销毁等操作，配置 CPU、内存等信息规格。

### 持久性对象存储

Prajna Paramita Cloud基于内容寻址，点对点的超媒体协议，高容错、可扩展，更安全、更开放的实现对象存储。可为 Glance 提供持久镜像存储，为 Cinder 提供卷备份服务。

### 身份服务（Identity Service）

Keystone。为 OpenStack 其他服务提供身份验证、服务规则和服务令牌的功能，管理Domains、Projects、Users、Groups、Roles。

### 网络&地址管理（Network）

提供云计算的网络虚拟化技术，为 OpenStack 其他服务提供网络连接服务。为用户提供接口，可以定义 Network、Subnet、Router，配置 DHCP、DNS、负载均衡、L3 服务，网络支持 GRE、VLAN。插件架构支持许多主流的网络厂家和技术，如 OpenvSwitch。

**块存储 （Block Storage）**

为运行实例提供稳定的数据块存储服务，它的插件驱动架构有利于块设备的创建和管理，如创建卷、删除卷，在实例上挂载和卸载卷。

**数据传送（Data Transfer）**

数据通过Prajna Paramita Chain传输。用户公开客户端应用程序可能上载或下载碎片的端点。客户的请求通过先前交付和检索消息提供的令牌进行身份验证。

**网络存取（Network Access）**

数据所有者必须承担网络存取的负担，以维护Prajna Paramita Chain网络上的数据的可用性和完整性。因为节点不能被信任,和隐藏信息安全挑战集不能外包给一个不可信的对等，数据所有者负责预处理碎片、发行和验证审核，提供支付、管理文件状态通过碎片的收集管理文件加密密钥,等等。

**审计付费**

矿工只有在网络可以审计他们的服务是否正确提供的时候才会收到付款。

# 发展路线

**2017年Q3**

Prajna Paramita项目立项；

**2017年Q4**

完成MoonBox硬件外观设计和内部结构搭建；

**2018年Q1**

Prajna Paramita Chain网络搭建和测试；

**2018年Q2**

MoonBox客户端正式上线；

**2018年Q3**

Prajna Paramita Cloud平台搭建；

**2018年Q4**

Prajna Paramita Cloud测试版上线开启公测；

**2019年Q1**

Prajna Paramita Cloud正式版上线。

# Prajna Paramita Token / PRMI介绍

在Prajna Paramita Cloud平台上用户可以通过MoonBox主机提供存储空间、带宽等数据资源成为Prajna Paramita Chain链上的节点来获取PRMI奖励。和比特币一样，Prajna Paramita Cloud上的旷工们为了巨大的奖励而竞争式挖区块，但Prajna Paramita Cloud的挖矿效率是与存储活跃度成比例的，这直接为客户提供了有用的服务。这种方式给旷工们创造了强大的激励，激励他们尽可能多的聚集存储器并且把它们出租给客户们。

## RPMI

Prajna Paramita Token / PRMI是基于ERC20发行的标准代币，发行总量6亿。PRMI基于去中心化云计算和区块链技术，通过智能合约来保证用户共享计算资源及内容的付出和收益对等；通过去中介化的账本记录，保证所有交易真实、公开、透明。

PRMI作为Prajna Paramita Cloud平台的支付代币，用户可使用 PRMI支付存储空间、内容查阅、共享带宽等一系列交易行为。

Prajna Paramita Cloud上参与奖励的人越来越多，获取难度越来越大，前期参与更有优势。平台鼓励更多个人用户加入，为共享计算生态输送出更多数据节点和带宽、存储、计算等资源，从而使得整个生态在得以保持良好的循环。

## PRMI分配方案

PRMI作为Prajna Paramita Cloud平台流通的媒介，包含交易支付存储空间、文件共享、带宽共享等结算和充值。

PRMI恒量发行总量6亿，为维护整个生态良性运转70%币子将用作MoonBox奖励发放剩余部分将留于技术团队、运营宣传、基石投资和基金会，具体分配方式如下：

**奖励产生： 70%**

总发行量的70%将会通过MoonBox奖励机制发放给用户；

**技术团队：10%**

总发行量的10%发放给技术开发团队，用于平台生态后续技术开发升级和维护。自代币上线交易所后一个月开始逐月解锁，每月解锁1%，共分10个月解锁完成；

**品牌宣传：5%**

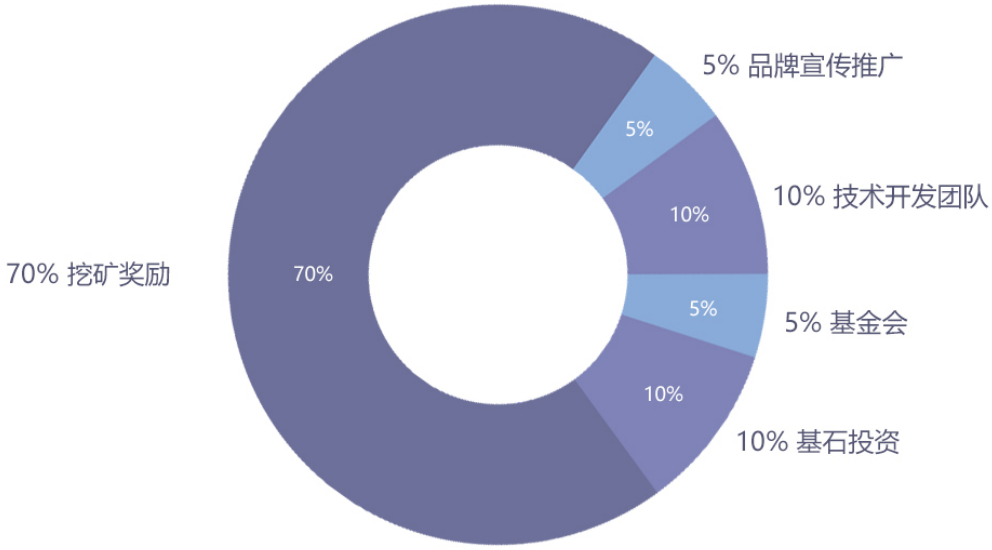
总发行量5%作为项目运营宣传费用，用于生态品牌线上线下宣传推广；

**基石投资：10%**

总发行量的10%发放给合作伙伴和投资机构。自代币生成后解锁5%，自代币上线交易所后一个月开始逐月解锁，每月解锁1%，分5个月解锁完成；

**基金会：5%**

总发行量的5%作为基金会储备金，用于项目正常运转和国内外社区运营维护。此部分自代币生成解锁2.5%，自代币上线交易所后一个月开始逐月解锁，每月解锁0.5%，分5个月解锁完成。




## PRMI获取方式

PRMI通过共享 MoonBox主机硬盘资源、上行带宽、CPU 计算能力等与生态奖励机制生成。

◇ 用户可购买 MoonBox主机，并激活 PRMI 奖励计划，执行活动任务获得 PRMI；

◇ 用户可贡献上行带宽、共享闲置硬盘存储空间、CPU 计算能力和硬盘读写能力等资源通过区块链智能合约算法获得 PRMI；

◇官方公布的其他活动，根据活动规则，获得相应的 PRMI。

## PRMI奖励算法

在Prajna Paramita Cloud平台每一个用户都是传输节点，通过点对点数据传输用户可通过共享闲置资源获得的PRMI作为奖励。每一台 MoonBox 都将成为一个数据存储、传输的节点、终端服务器。

**发币算法**

PRMI是基于MoonBox主机硬件能力、上行带宽、可共享存储大小、有效在线时长等贡献进行多维度打分进行奖励等。Prajna Paramita Cloud平台通过其当天的贡献，按照相关权重向MoonBox用户进行分配当日产生的币。

◇ MoonBox 分数 A=（硬件能力×（CPU 因子+内存因子）+带宽×带宽因子 + 存储值×存储值因子）×（有效在线时长÷24 小时×有效在线时长因子）×当天发币总量=Ct；

◇ 产量公式：$\frac{A1}{A1+A2+A3+\cdots+An} * Ct$

**公式分析**

◇ 硬件能力：

MoonBox的 CPU 效率和内存大小。CPU 因子权重 20，内存因子权重权重 10；

◇ 带宽：

可信节点测得的上行带宽。为鼓励分布式节点的参与，带宽因子在 1-8M 时为 10，在 9-20M 时衰减为 5，在 21-100M 时衰减为 1；100M 以上按照 100M 进行计算；采用阶梯累进算法（详见下文举例）；

◇ 存储：

可信节点测得的可用于获得奖励的存储空间，为鼓励用户多分享自己的闲置存储资源，设定存储值在小于 200G 时为 0，200G-1000G 时为 1，大于 1000G 为 2；存储因子为 5；

◇ 读写：

读写速度 1MB/S-99MB/S 读写为 1，读写速度 100MB/S-200MB/s 读写为 2，读写速度 200MB/s 以上读写为 3。读写因子为 10；

◇ 有效时长因子：

有效时常因子为 1，连续 7 天有效在线时长为 24 小时，有效时常因子为 1.1，期间有效 时常发生中断，那么有效时常因子从 1 开始重新计算。

◇ 在线时长： 可信节点每日会对前一天有效在线时长进行总计，并进行全网分数的计算以及PRMI的分发。

MoonBox分数算法举例：

◇ 当上行带宽为 1M，存储为 100G，硬盘读写速度 20MB/s，在线时长为 12 小时；MoonBox分数=[1*(20+10)+1*10+0*5+1*10]*(12/24*1)=25

◇ 当上行带宽为 10M，存储为 500G，硬盘读写速度 50MB/s，在线时长为 24 小时；MoonBox分数=[1*(20+10)+[8*10+(10-8)*5]+1*5+1*10]*(24/24*1)=135

◇ 当上行带宽为 100M，存储为 1500G，硬盘读写速度 100MB/s，在线时长为 24 小时；MoonBox分数

=[1*(20+10)+[8*10+(20-8)*5+(100-20)*1]+2*5+2*10]*(24/24*1)=280

◇ 当上行带宽为 100M，存储为 1500G，硬盘读写速度 100MB/s，在线时长为 24 小时；持续 7*24 小时；MoonBox分数

=[1*(20+10)+[8*10+(20-8)*5+(100-20)*1]+2*5+2*10]*(24/24*1.1)=308

出币衰减算法

◇ 衰减周期 y：

每次产量减少的周期设置 y=1 年（365 天）

◇ 衰减因子 d：

每次产量减少的比例采用减半法，设置 d=50%

◇ 初始发币量 C：

开始获取奖励币时每单位时间奖励的币个数根据总量等综合计算，设计 C=62w/天

则获取奖励产生的总币量=每个区块产生的PRMI产量每 365 天减半一次，则获取奖励产生的总币量无限趋近于约4.2亿。

## 应用场景

**云存储服务：**

根据自己实际存储大小、时间、备份数量的需求， 兑换所需要的云存储空间；

**共享云计算服务：**

兑换安全、稳定的云计算服务。提供超大规模分布式底层架构、去中介化及专属云加密技术为用户的云服务。

**共享 CDN 服务：**

基于优质网络基础设施和云计算技术，兑换低成本、高性能、可扩展的互联网内容分发服务。

# 团队介绍

Blaise Rego 毕业于新加坡南洋理工学院，拥有理工学院计算机工程科学与商科双学士，在2006年为移动java开发者，后来他转到服务器端java软件，和工作了两年半的系统上进行电子发票。2011、他回到移动开发，此后他写的大多是独立于平台的C++和java的Android。在他的日常工作，他一直在处理其他各种技术包括JavaScript、Python、java SE。

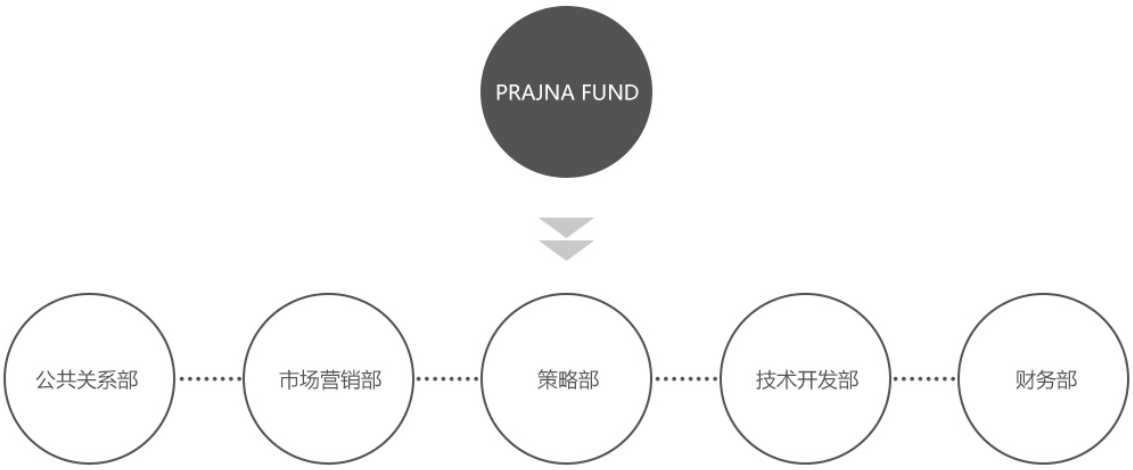
Carlos Plouviez毕业于新加坡南洋理工学院，计算机工程学士学位，在P2P通信网络安全方面和文件共享有深入的研究，精通 PHP、C#、Javascript、Lua 等多种开发语言，2017年开始研究区块链技术。

Francois Petkov是一名专攻C++经验的程序员，主要专注于Ethereum及其虚拟机。Francois Petkov是evmjit的联合创始人，大型企业的软件应用设计、开发和部署方面有10年的经验。在创立evmjit之前，Francois Petkov领导了软件AG领先的主机集成产品的开发和产品管理。

Clarence Lam是一个拥有超过十五年的专业经验的软件工程师，服务器端java开发者。在区块链开发、计算机语言等有较深研究和应用

# 组织架构

Prajna基金会（以下简称“基金会”）致力于 Prajna Paramita Cloud 的开发建设和治理透明度倡导及推进工作，促进开源生态社会的安全、和谐发展。基金会将通过制定良好的治理结构，帮助管理开源社区项目的一般事宜和特权事项。基金会治理结构的设计目标主要考虑开源社区项目的可持续性、管理有效性及运营资金的安全性。基金会由策略部、技术开发部、市场营销部、财务部门、公共关系部五组成。



# 声明

本白皮书只做交流之用，其中包含的信息或分析不构成购买提议或劝导。本白皮书不构成也不应理解成为提供任何买卖的行为，或邀请购买任何相关产品和虚拟商品的行为，也不是任何形式上的合约或承诺。

任何人参与PRMI的购买行为均基于其自己本身对Prajna Paramita Cloud和PRMI的认知和理解。本白皮书不构成任何Prajna团队出售 PRMI的意图，不提供任何形式的投资决策。这篇白皮书中所包含的任何内容都不能作为一个承诺或陈述来作为未来的Prajna Paramita Cloud的表现，无论其技术规格、参数、性能或功能等。

Prajna基金会和Prajna团队将不会对任何实体或个人做任何声明、保证或承诺。RPMI用户应仔细考虑和评估与PRMI销售相关的所有风险和不确定性（包括财务风险和法律风险及其他不确定性）。

本白皮书可以翻译成其他语言，翻译版本之间发生冲突或歧义时，以英文版本为准。白皮书会根据Prajna Paramita Cloud生态发展需要，定期更新调整，详情请查看官网更新记录。


Prajna Paramita Chain全球节点规划布局