

# IPWeb

## — P2P分布式存储高性能公链

IPWeb - High performance public chain based on P2P storage

——引领去中心化互联网的未来

## 摘要

随着区块链技术的迅猛发展，智能合约技术的不断完善，区块链应用的落地将拉开大幕。P2P 分布式存储是区块链应用落地的关键所在，智能合约技术 + 分布式存储技术的实现将推动区块链 3.0 时代快速到来。相比于中心化存储，P2P 分布式存储提高了存储和网络效率，通过分布式技术解决了存储空间和网络资源的浪费，可以自动分配数据，从而实现了弹性扩展，降低运营成本，避免资源浪费。P2P 分布式存储替代传统中心化存储将是大势所趋。

### IPWeb: 一个基于 P2P 分布式存储的高性能公链。

P2P 分布式存储不仅提供了安全可靠、低成本的存储平台，任何人都可以自己定义智能合约的同时，自由地使用 IPWeb 提供的 P2P 分布式存储。IPWeb 旨在以多链多共识为基础，并结合可验证的存储证明和通证经济，实现高效的链上节点治理。IPWeb 的目标是建立新型的分布式加密存储网络，为用户提供高效的存储服务，并在此基础上打造功能丰富的链上分布式应用 (DApp)。

#### ——IPWeb 让数据的存储更安全

容错机制会保证用户的数据被复制了一定数量并存放在不同的节点上，即使某一个节点的数据因异常情况消失，通过其他节点的备份也可以完整恢复用户的数据，这就极大的保证了存储在 IPWeb 上的数据安全性。分布式的数据存储，降低了因为战争、自然灾害、人为等原因造成的数据遗失损坏，利于让有价值的数据被永久保存。数据文件被拆分成块，分布到不同的存储节点，数据的安全性更高，很难被窥探或被复制。IPWEB 网络几乎不会受到 DDOS 攻击的影响，这是由于 IPWEB 网络是去中心化的，不存在中心化服务器，所以大量集中访问进入网络时就会被分散到不同的节点，不可能造成网络拥堵甚至崩溃的问题。

#### ——IPWeb 让数据存储更高效

一个文件可以被分散成很多份，存储在全球不同的存储节点中，用户要下载文件时，只需查询相应的地址 (Hash 值)，就可以从各个存储节点中同时获取数据，比起中心化存储，速度会快上许多。在数据传输速度方面，IPWeb 也是更有优势的，当用户需要读取数据时，所有的存储者会同时为用户发送自己保存的那一份数据，服务器接收后自动进行拼接处理，用户的下载速度将不再受制于服务器的带宽，而主要取决网络下载带宽。

#### ——IPWeb 让存储成本更低廉

在 IPWeb 网络中，所有的文件都是独一无二的，不会重复，更不可能被恶意篡改，在很大程度上减少了存储资源的浪费，降低了存储资源的成本。IPWeb 分布式的存储，充分利用了公众闲散的存储资源和带宽资源，提高了资源的使用率，降低了使用成本。

#### ——IPWeb 能更好的支撑区块链应用

区块链发展瓶颈之一就是分布式的存储能力，目前，大部分公链的最大问题是没法存储大量的超媒体数据在自己的链上。IPWeb 的分布式存储将成为所有区块链项目的基础设施，为区块链应用的大规模发展打下良好的集成。

# Contents

## 目录

01 背景	4
02 什么是IPWeb?	5
03 IPWeb的使命	6
04 IPWeb的基础设施	7
05 IPWeb的技术体系	8
06 IPWeb的通证经济模型	16
07 IPWeb的官方通证-IPW	18
08 IPWeb的应用场景	21
09 IPWeb的生态建设	22
10 IPWeb的发展规划	23
11 团队架构	24
12 社区治理	26
13 风险申明	28
14 免责申明	30

## 01 背景

当前,全球处在一个由工业时代逐步过渡到信息时代的阶段,数据正在成为世界上最有价值的资源。伴随人类的各种行为,产生了庞大的数据,如何存储这些数据并进一步利用好数据,这个问题变得越来越重要。从内部部署存储迁移到云存储是过去十年的主题,而且这一趋势正在加速。另一方面,大量的存储空间在世界各地的人们的硬盘上未被使用,很多资源在无形中被浪费了。

区块链技术的诞生,为软件定义存储的发展开辟了新的道路。它创造了一种可能:在技术层面和经济体系层面重新思考云存储并解决行业困境。首先,存储的池化可以在更广阔的空间,以更丰富的形态来实现。其次,区块链的Token激励机制,可以驱动大家将企业级存储、服务器、PC、移动存储等的剩余存储空间贡献出来。最后,每个节点实际存放的数据只是数据的一些切片,而且这些切片还以加密的方式保存起来。数据能够更安全地保护起来,即使提供存储节点的用户有机会查看这些切片,看到的也是没有实际意义的数据段。区块链的DAO这种分布式商业模式,有机会借助全球的资源 and 人才,类似众人拾柴火焰高一样,加速分布式存储产业的发展。与现有云存储解决方案相比,基于区块链的分布式存储更安全、更快、成本更低、更具审查性,并且分布更广。它创造了一个允许人们把他们备用存储空间货币化的市场,全球存储市场的涌入的供应将降低存储价格。区块链能够保证以安全、去信任、点对点的方式做到这一点。从中心化存储到去中心化存储。从中心化互联网到去中心化互联网。我们正站在历史的转折点。

### 基于区块链的分布式存储优势:

- 1) 分布式存储真正发挥了共享经济的优势。用户可以将硬盘的空余空间充分的利用起来,并且获得收益。
- 2) 数据被切割成小块后,需要经过加密后才会分散到众多节点上。即避免了中心化存储“窃取”文件的事件,同时即便解锁某一块数据,也只是部分数据,并非全部。另外,也不用担心中心化服务器因为故障造成的数据泄露等风险。
- 3) 文件在下载的过程中,碎片会进行重组,并行的速度会远大于中心化存储。
- 4) 通过智能合约,网络可以自动判定使用情况以及使用奖励等。

## 02 什么是IPWeb?

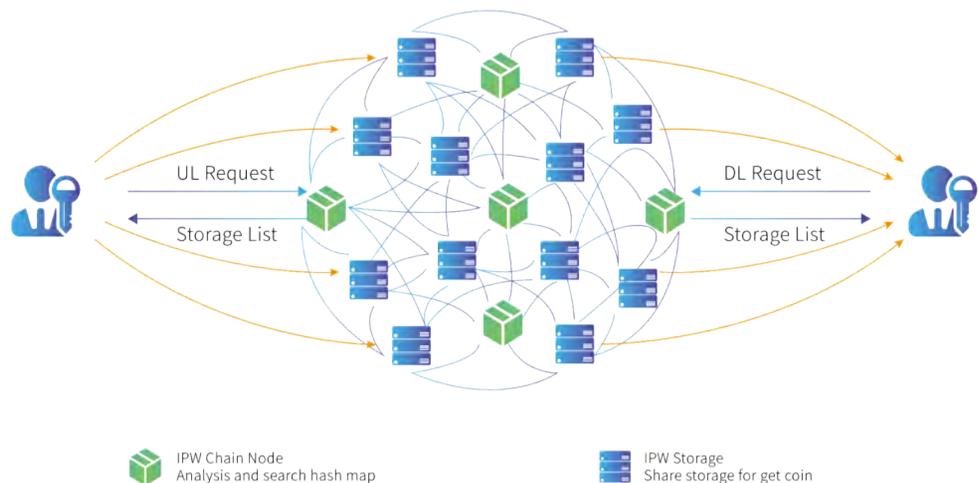
### IPWeb: 一个基于 P2P 分布式存储的高性能公链。

在此基础上构建的分布式存储服务平台,比中心化存储更快捷、更安全、成本更低。将文件分割成多个小的部分(保证一定的冗余性),分散存储在网络众多节点上,只要一定数量节点的正常运转,就能保证文件的安全和完整。

当用户输入一个 URL 在网页浏览器来获取网上信息时, URL 会解析到一个 IP 地址。这个 IP 地址会找到存储着用户所需要寻找的信息的那台服务器。网上的几乎每个发布者,供应商和服务都会把信息存在他们控制的特定的数据中心的服务器里,这就让我们今天的网络变得中心化。

IPWeb 网络协议本身能确保用户的文件得到存储。作为 IPWeb 挖矿过程中产生的副产品,创新的加密证明给客户创造了一套有用且有价值的服务。矿工被激励去用他们的硬盘空间在 IPWeb 的可验证的存储市场上赚钱,他们将会得到等量的奖励:矿工存储的量越大,他们将会赚取更多的权益证明-Token。

我们相信,这些新增的去中心化的储存空间供应会让客户减低网络存储花费且享受到更优质的存储服务。作为一个去中心化的协议,网络上储存的数据和与这些数据的链接不会被一个中央点所控制,这种设置能提高牢靠性。比起现在单一集中的服务器和大型内容分发网络,在 IPWeb 矿工间被大规模传送的信息会被储存在更靠近用户的地方,使信息搜索更加快捷。在 IPWeb 上通过加密算法被编入检索的数据能够使客户更加高效地管理和更新庞大的数据。最后,作为一个开源项目,不同于今天大多数的云存储与分发平台,IPWeb 软件本身公开接受检查,验证和提升。随着 IPWeb 的不断升级与新功能不断地被加入,我们希望 IPWeb 的网络可以成为一个面向大众(即使不是所有人)的网络信息存储和分发的平台。

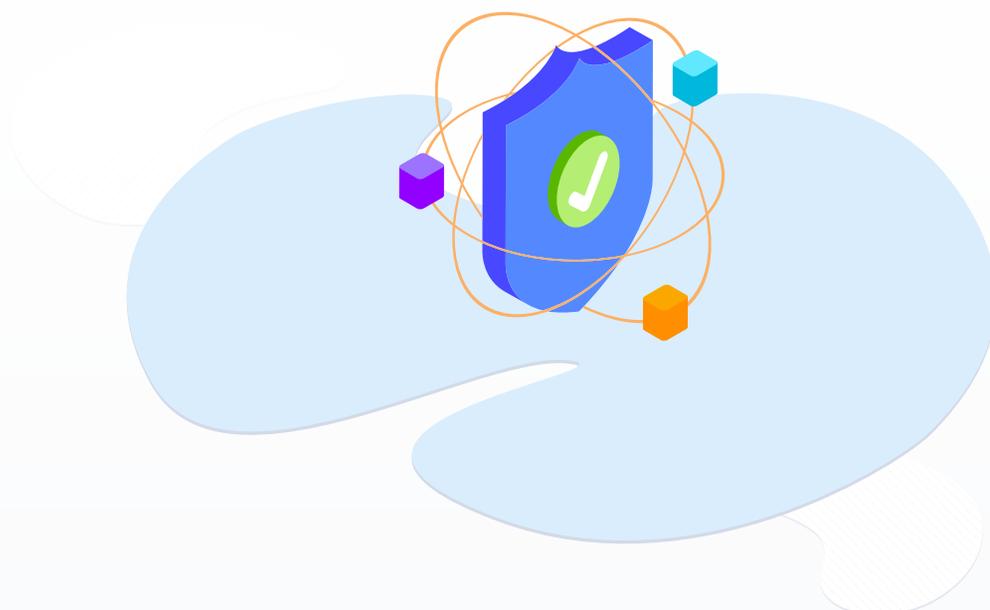


## 03 IPWeb的使命

引领去中心化存储和去中心化互联网的光明未来。

IPWeb在发展过程中将始终坚持以下原则：

- **价值共享原则：** IPWeb将实现共享生态的价值传递。通过有效的激励机制，鼓励用户共享闲置存储空间，不断的扩大存储网络的规模，形成良性的生态圈。
- **数据安全原则：** 存储的数据会通过设备进行分块、编码等过程，再分发到分布式存储网络中，从而将安全性提升到很高的级别，用户数据在这个网络中没有其他任何人或公司能够窥探。
- **平台化发展原则：** IPWeb通过规范化的底层技术平台并提供配套的标准工具，使得分布式资源可以提供给有需要的公司或组织使用，包括存储资源、算力等。公司或组织可以在这个平台上开发自己的DAPP（分布式应用）。
- **可扩展性原则：** IPWeb可以同时多路传输许多点对点的连接，通过这样一个动态的灵活性和可延性，IPWeb的可扩展性将和HTTP一样，可实现无上限扩张。



## 04 IPWeb的基础设施

**IPWeb 将为所有生态参与者提供多种基础设施，包括：**

- 基于共享经济模式的 P2P 云存储服务；
- 连接全球数据的 P2P 数据交易平台；
- P2P 去中心化互联网：IPWeb 协议下的域名系统、浏览器；
- 去中心化服务和内容平台；
- 区块链：高性能公有链、自定义侧链；
- 基于去中心化互联网生态的数字货币。

文件浏览器 (IPWeb.io)

IPW存储矿机

区块浏览器

自治节点网络

文件存储系统

文件共享系统

IPW数字钱包

检索矿机

搜索引擎

## 05 IPWeb的技术体系

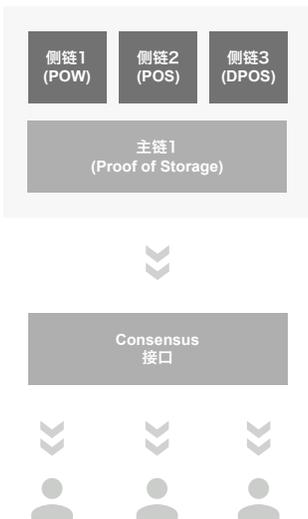
### 5.1 总体架构设计



IPWeb计算文件的哈希值作为系统中对象的唯一标识，文件进行加密、编码后产生的碎片为对象数据。存储节点将对象数据存储在自己的存储单元中，超级节点负责维护对象数据到存储节点的映射关系。其中存储节点是完全对等的，通过一套 P2P 传输协议，存储节点间可相互传输数据。超级节点作为调度者，接受存储节点的信息，并根据广播更新存储对象的实时信息，以使用户访问存储对象时可快速的返回对象位置。

#### 5.1.1 双层网络设计

IPWeb将存储和检索两层网络分离，提高了网络效率，也降低了挖矿门槛。存储和检索对于矿机的要求是不一样的。检索需要昂贵的算力和能源消耗，而存储需要存闲置的存储资源和带宽资源。存储和检索分离更有助于以低成本的矿机为IPWeb贡献。



#### 5.1.2 多链结构（主侧链设计：多链多共识）

IPW Chain主链采用PoRep（复制证明）、PoE（提取证明）。IPW Chain提供 Consensus接口，提供POW、POS、DPOS等实装。开发者可以通过主链提供的 Consensus接口创建并完成自己节点的部署。对性能要求高的侧链可以采用 DPOS，对去中心化要求高的可以采用POW。

## 05 IPWeb的技术体系

### 5.2 存储网络

#### 5.2.1 DHT

P2P 的本质即是一种新的网络传播技术。这种新的传播技术打破了传统的架构，逐步地去中心化，扁平化，从而达到节点平等的未来趋势。P2P 文件分享的应用 (BTs/eMules 等) 是 P2P 技术最集中的体现。IPWeb 是以 P2P 文件分享网络作为入口，围绕一个文件网络系统，将其可操作性结合区块链的公式算法设计出新型扁平化，去中心化的云存储网络。同时保留了区块链公开，透明的特性。

分布式哈希表 DHT (Distributed Hash Table) 是一种分布式存储方法。在 DHT 中，一类可由键值来唯一标示的信息按照某种约定 / 协议被分散地存储在多个节点上，可以有效地避免“中央集权式”的服务器 (比如: Tracker) 的单一故障而带来的整个网络瘫痪。和中心节点服务器不同，DHT 网络中的各节点并不需要维护整个网络的信息，而是只在节点中存储其临近的后继节点信息，大幅减少了带宽的占用和资源的消耗。DHT 网络还在与关键字最接近的节点上备份冗余信息，避免了单一节点失效问题。

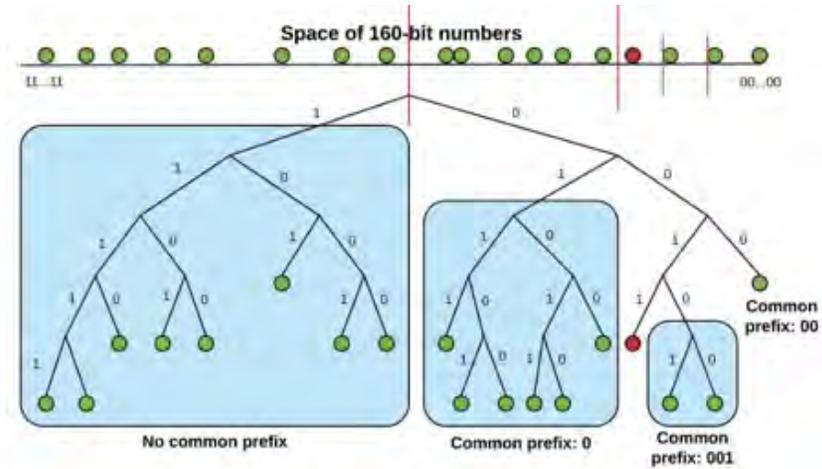
实现 DHT 的技术 / 算法有很多种，如 Chord、CAN、Pastry、Kademlia 等。考虑技术成熟度以及市场运用情况，IPWeb 使用 Kademlia 算法。Kademlia 通常又被称为第三代 P2P 技术，是一种 P2P 通用协议，适用于所有的分布式点对点计算机网络。Kademlia 定义了网络的结构，规划了节点之间的通讯以及具体的信息交互过程。在 Kademlia 中，网络节点之间使用 UDP 进行通信，通过一种分布式哈希表来存储数据，每个节点都会有一个自己的 ID，在用来标识节点本身的同时，也用以协助实现 Kademlia 算法和流程。

#### 5.2.2 KAD 网络

KAD DHT 存储网络中的节点(Node)包括如下特性:

- NodeID 在 KAD 中需要是 160bits 或者 20bytes;
- Contact 包含 NodeID(NodeID), Address(string),UDP Port Number;
- Bucket[VaugeKConst]\*Contact 用在 Node 的 Routing 中，一个 Bucket 能包含的 k 个 Node, 所有的 Node 在 60 分钟后消失;
- VaugeKConst 统计上设为 20;
- Router 包含 Contact 和 KBucket, KBucket 是在 ID 的每一个 bit 中, 都有一个 Bucket.

## 05 IPWeb的技术体系

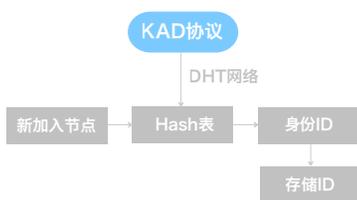


Kademlia使用键值来确认在KAD网络上的节点和数据。KAD的键值是不透明的，长度160个比特。参加进来的电脑每一个都会拥有一个键值，称为NodeID，填充在160比特的键值空间中。由于KAD存储内容的时候是由KV (key-value) 对来存储的，每一个在KAD DHT中的Data也都是独立于160位键值中的key对应的空间的。在开始时，一个Node不了解任何其他的Nodes。当新的Nodes注册后，找到这个节点的链接，然后将新的NodeID存起来。当存储满溢，Contact会被选择性去掉，然后在bucket内部被组织。从一个Node找一个NodeID的方式，是从一个已知的路由表中，从一个Node找到另一个最近的Node，直到找到RequestNode。

每个KAD节点都有160比特的NodeID，每个数据的键值也是一个160位的标识符。想要确定KV对存在哪个节点中，KAD用了两个标识符间距离的概念。在给定两个160位标识符，x和y下，KAD通过他们两个的“异或”来确定他们之间的距离，并表达为一个整数 $d(x,y)=x\oplus y$ 。XOR(异或)获得到的是系统二叉树框架中对距离的定义。在一个完全的160位ID二叉树ID中，两个ID距离的大小是最小的包含两个节点的子树。当树不是一个完全二叉树的时候，距离IDx最近的叶是与x共享最长公共前缀的叶。举例来说，在0011和1001之间的距离则是 $0011\oplus 1001=1010$ ，1010通过整数表达则是10，所以在这两个节点的距离则是10。

### 5.2.3 节点身份ID

对等节点身份信息的生成以及路由规则是通过Kademlia协议生成制定，KAD协议实质是构建了一个分布式松散Hash表，简称DHT，每个加入这个DHT网络的人都要生成自己的身份信息，然后才能通过这个身份信息去负责存储这个网络里的资源信息和其他成员的联系信息。如果新节点A需要寻找另外一个节点B的联系信息，而A节点没有节点B的联系方式，那么节点A可以通过联系任意和节点B有联系的节点来获取节点B的联系信息。



## 05 IPWeb的技术体系

### 5.2.4 查找算法

在KAD里面的节点查找过程是通过KAD根据给定的键值去定位k个最近节点的。KAD在节点查找中选择采用的是递归算法。发起查找的一方首先从非空k-bucket中找到一个节点（或者，如果那个bucket有比  $\alpha$  少的键值对数组，那他就只能通过键值得到  $\alpha$  个最近节点）。发起方通过并行异步方式发送FIND\_NODERPC给选到的  $\alpha$  个节点。  $\alpha$  是一个系统的并发参数。在递归的阶段，发起方重新发送FindNode给之前发过RPC的节点。无法迅速回应的节点就会被移除，除非直到这些节点回复。

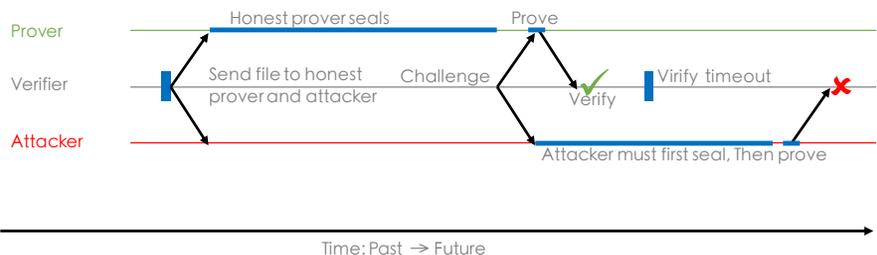
如果一轮下来寻找节点没有找到任何比最近观察节点更近的节点，发起方会重新发送FindNode给那些没有被请求过的节点中寻找k个最近的。当发起者请求后得到k个最近观察节点的回复后，查找过程就会结束。每一个节点至少知道它每个子树中的一个节点，每一个节点都可以通过NodeID定位到其他节点。要存一个KV对，节点需要通过键值定位对应k个最近节点然后发送STORERPC。要找一个KV对，节点需要查找到对应键值最近的k个节点。但是，值（value）的查找会使用FIND\_VALUE而不是FIND\_NODE，而且这个过程当任何节点返回值的时候立刻停止。

### 5.2.5 存储争议解决

在分布式存储网络中，数据节点分散在不可信任的边缘网络中，需要确保数据存储在数据节点上，并可抵挡女巫攻击、外包攻击、代攻击等作弊手段。在考虑存在恶意节点情况下，分布式存储系统需要防范各种攻击，IPWEB通过零知识证明（zkSNARK）和封装（Seal）来实现复制证明（PoRep）和提取证明（PoE），实现占用资源少并且效率极高的存储证明。

#### 复制证明（PoRep - Proof of Replication）

存储证明区别于工作量证明、权益证明等，存储证明是一种用于分布式存储领域的共识算法。是根据用户对分布式云存储平台贡献的存储空间，并结合流量、带宽、在线时长等因素进行激励。证明允许存储提供用户通过提供副本证明（ $\pi$ ）来说服验证者，在验证者发出随机挑战时，提供证明：证明数据X相对于证明者的特定副本Y已经存储在唯一的专用物理存储区了。PoRep算法可以保证每份数据的存储都是独立的，可以防止女巫攻击，外源攻击和生成攻击。



## 05 IPWeb的技术体系

PoRep的三个构建阶段：

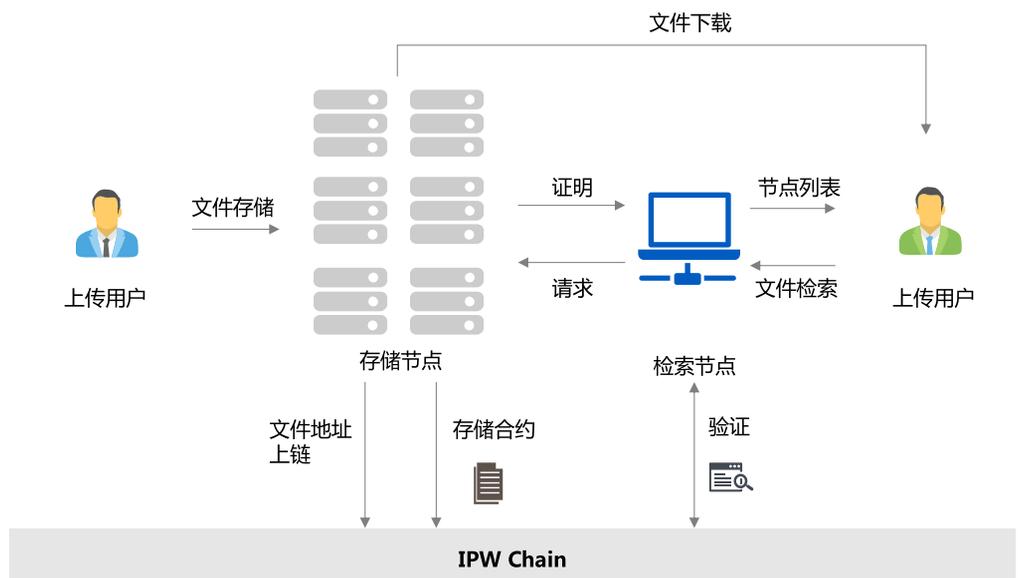
- PoRep.setup() --> 副本 Y, 副本 Hash 树根 Merkle root of Y, 封装证明  $\pi$ SEAL。
- PoRep.prove() --> 存储证明  $\pi$ PoRep。
- PoRep.Verify() --> bit b ( 存储有效性证明 b1 ( $\pi$ PoRep) ^ 封装有效性证明 b2 ( $\pi$ SEAL) ) 。

### 提取证明 (PoE - Proof of Extract)

为了避免一遍遍的检索存储节点是否按照要求正确的存储了数据，造成算力资源的浪费，IPWeb设计了新的证明算法提取证明 (Proof of Extract)，通过通证经济的利益驱动，当存储节点响应用户的检索及下载需求时，存储节点主动提供一个证明信息返给检索矿工。IPWeb不需要再频繁地检索某个存储节点是否正确存储文件，只有当文件能被成功检索到时，网络会执行一个奖励智能合约，该存储节点才能获得奖励。

整个流程如下：

- IPWeb和存储节点先签订一个存储合约，比如存储节点拿出100G的空间用于存储挖矿；
- 存储节点开始储存文件；
- 用户检索文件时，检索节点根据存储合约发送请求给到存储节点；
- 存储节点收到检索请求后，返回一个存储证明给到检索节点；
- 检索节点验证存储节点反馈的证明信息；
- 用户成功从验证的存储节点列表调用该节点的文件；
- 存储节点获取存储到本次检索的存储奖励。



## 05 IPWeb的技术体系

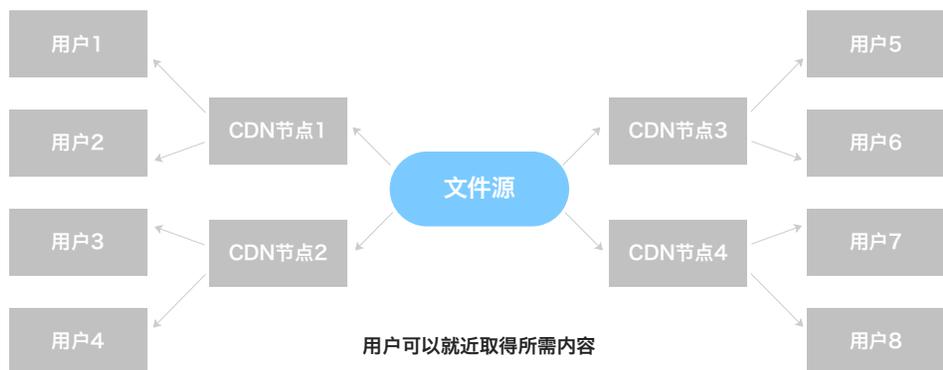
### 5.2.6 冗余处理

如果一个节点巡查失败或者不可到达，系统就发起一个网络复制过程，通过把网络上一个现有的副本转移到一个新的节点上。因此，网络就能在每次巡查之后恢复正常。每个碎片都是唯一加密的。这意味着，当恶意用户只有一个文件副本时，不能假装拥有多个冗余副本。我们可以通过在集中加密碎片时，加入确定性的混淆值来完成。即使解密密钥是一个已知的特定文件，恶意用户也不能完成他们没有被分配到的碎片的审核。这样，我们可以证明一个特定的碎片的冗余，因为每一个冗余副本是独一无二的。

另外，用户和应用都被K-M纠删码技术的参数和分布式的冗余控制。对于简单的数据存储，用户可以选择推荐的文件存储级别设置。如果数据特别重要，用户可以选择高级别的文件存储设置，把数据分散到多个存储节点（含多个超级节点）中，这能保护数据免受特殊情况的侵扰（如自然灾害等）。

### 5.2.7 文件分发网络

其核心思路是避开互联网上有可能影响数据传输速度和稳定性的瓶颈和环节，使文件传输的更快、更稳定。通过在网络各处放置节点服务器所构成的在现有的互联网基础之上的一层智能虚拟网络，CDN系统能够实时地根据网络流量和各节点的连接、负载状况以及到用户的距离和响应时间等综合信息将用户的请求重新导向离用户最近的服务节点上。其目的是使用户可就近取得所需内容，解决Internet网络拥挤的状况，提高用户访问网站的响应速度。



## 05 IPWeb的技术体系

### 5.3 加密安全（可搜索加密/IP隐蔽）

在数据保护中，个人信息的隐私性是需要得到优先考虑的，其次要支持的就是动态数据的改动，也就是Dapp对于去中心化数据存储的修改。IPWeb基于业务场景，使用可搜索对称加密（SSE: SearchableSymmetricEncryption）方法，SSE由五个算法组成：

$K=KeyGen(k)$ ：输入安全参数 $k$ ，输出随机产生的密钥 $K$ 。该操作通常在数据拥有者端本地执行。

$(I,C)=Enc(K,D)$ ：输入密钥 $K$ 和明文文件集 $D=(D1,D2,...,Dn)$ ，输出索引和密文文件集。该操作在数据拥有者端本地执行。

$Tw=Trapdoor (K,W)$ ：输入密钥 $K$ 和关键词 $W$ ，输出关键词对应的陷门。该操作在数据拥有者端本地执行。

$D(W)=Search (I,Tw)$ ：输入索引 $I$ 和待搜索关键字的陷门 $Tw$ ，输出包含关键字 $W$ 的文件的标识符集合。Search操作在Genaro中由密钥分发控件执行。

$Di=Dec(K,Ci)$ ：输入密钥 $K$ 和密文文件 $Ci$ ，输出解密后对应的明文文件 $Di$ 。该操作在数据拥有者端本地执行。

另外，IPWeb将存储和检索两层网络分离，提高了网络效率，提升了用户体验。但检索节点是整个P2P网络最容易被寻找和攻击的部分，需要对检索节点有额外保护，通过对检索节点的IP地址加密保护，用户无法通过IP直接查询，实现对节点的保护。

## 05 IPWeb的技术体系

### 5.4 其他技术创新

#### 5.4.1 分散存储

把文件分散成碎片能更好的保证数据的安全性，以致于只要存储的文件是标准碎片大小，就没有用户拥有一个完整的副本。我们把出租他或者她的硬盘空间给网络的用户定义为用户。定义标准碎片大小为字节的倍数（8KB/16KB/32KB/256KB/1024KB，根据文件大小，智能筛选分散标准）。这些都是保持在预先设定的大小，以阻止试图恶意存储小文件（对于大文件，大数量的碎片切割更有优势。对于小文件，特别是对小于一定大小（如64M）的文件，小文件的P2P传输效率很低，对网络容易造成额外负担）。

#### 5.4.2 Peer评级/节点分级

在Filecoin里所有节点都是同级的，这带来了更多的去中心化，但牺牲了效率。IPWeb会把存储节点按可靠性分级。初步决定把存储节点分为手机、个人计算机、专业矿机、企业级节点、超级节点。超级节点和企业级节点会有非常高的可靠性，所有文件的碎片会首先在超级节点和企业级节点备份，以提高IPWeb网络的效率和可靠性。

#### 5.4.3 存储级别设置

用户可以根据自己的需要对文件存储级别进行设置。比如将文件丢失恢复比设置为1/3、1/2、2/3。级别越高，安全性越高（丢失的风险越小）。

#### 5.4.4 防作弊机制

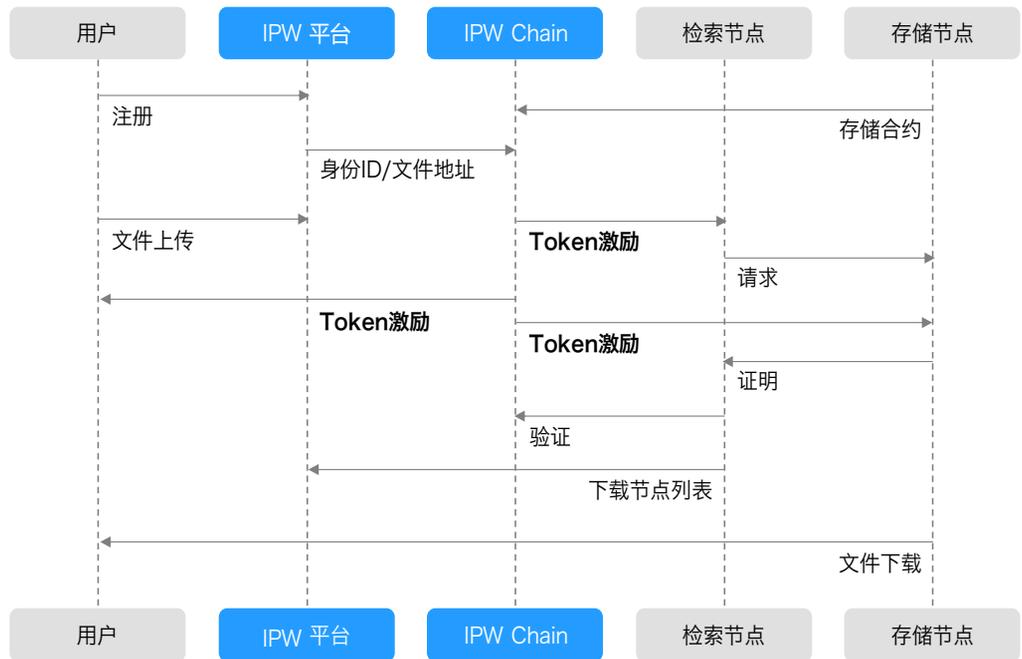
存储节点A和用户B可能会串通作弊骗取存储奖励。比如存储节点A谎称自己存储了1T的文件F，而用户B谎称自己成功检索到了存储在A的文件F。对于这种作弊行为，我们有多重防范。首先，我们会采取动态IP机制（防刷机作弊、检索作弊、存储作弊）（每次换Peer）。其次，大文件更容易用于作弊，但是大文件也会被分成更多数量的文件存在很多节点。用户B可能会付出检索费用却只能A节点获得了很少的奖励，而其他节点获得了绝大多数存储奖励。这同样能有效抑制刷机套利作弊的行为。

#### 5.4.5 IPWeb浏览器

IPWeb浏览器是可以访问IPWeb协议网络的浏览器，同时也兼容HTTP协议。不仅如此，用户还可以通过浏览器设置个人设备的存储空间用于挖矿。浏览器将能极大地增长IPWeb用户数和社区。更多的人能为IPWeb网络做贡献，也能成为IPWeb生态的消费者。IPWeb还将自带钱包功能。所有浏览器装机用户也会有自己的钱包。在必要的时候，IPWeb浏览器也可以兼容IPWEB协议，成为IPWEB生态的流量入口。

## 06 IPWeb的通证经济模型

IPWeb 的经济模型是一套激励生产者（服务提供者）和消费者参与到 IPWeb 体系的经济激励机制，是一套激励数据存储和检索的经济激励机制。IPWeb 有简洁明确的底层激励模型，和丰富、可拓展的多层激励模型。



从基础设施到 C 端内容消费 / 服务提供, 互联网生态中有丰富的生产 - 消费关系。多层次的、丰富的生产消费关系才能刺激了生态的蓬勃发展。在互联网最初诞生的时候, 互联网的生态是很简单、单薄的, 只有大型科学项目和大企业在使用互联网。甚至很多时候生产者和消费者是同一批人, 互联网是他们工作的工具。后来, 有了一些人在互联网上创造了一些内容, 另一部分人需要一个入又浏览这些内容。这个时候, 浏览器应运而生。生产者和消费者开始分化。除了内容的生产者以外, 第一层工具(浏览器)的生产者也开始出现。再往后, 网站日益变多, Yahoo一类的门户网站成为了互联网生态的新入又。互联网的生产者和消费者进一步增加, 第二层工具(门户网站)的生长者也出现, 生产 - 消费关系进一步丰富。我们可以看到只有多层次的、丰富的生产 - 消费关系才能支持一个伟大的生态体系。

在底层经济模型里, IPWeb 的生产者主要是存储节点和检索节点, 消费者主要是发起数据存储和检索请求的用户。消费者在 IPWeb 发起数据存储请求和数据检索请求, 并支付代币 IPW 作为存储 Gas 和检索 Gas。存储节点贡献闲置的存储空间和带宽, 为消费者提供 P2P 分布式数据存储服务, 并获得存储 Gas 作为奖励。检索节点则贡献闲置的算力和带宽, 为消费者提供 P2P 分布式数据检索服务, 并获得检索 Gas 代币。除了存储奖励和检索奖励以外, 部分超级节点还可以参与 IPW Chain 的记账, 获得区

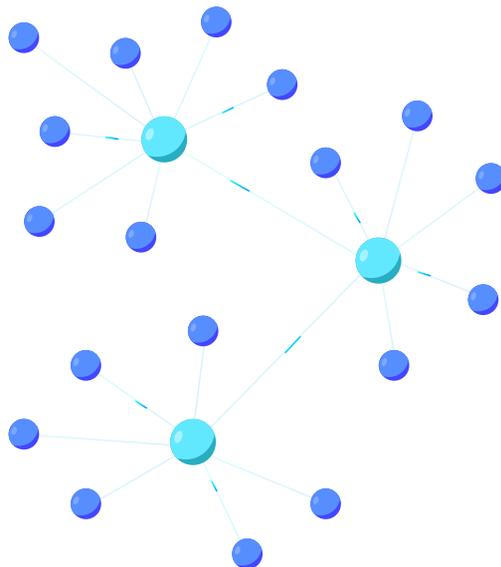
## 06 IPWeb的通证经济模型

块产生奖励。

单纯的存储和检索服务只是一个去中心化数据存储和检索平台。这是一种可以对标中心化云存储服务的平台。但是这样的基础设施也类似于互联网的第一个阶段，只有大企业和大项目（比如视频影像公司）会考虑到 P2P 存储成本成为企业付费用户。只有底层设施，没有丰富的应用层生产者和消费者，IPWeb无法支撑去中心化互联网的伟大构想。所以 IPWeb 还设计了建立于底层经济模型之上的高层次经济模型。

第二层经济模型里，IPWeb 浏览器作为 IPWeb网络的流量入口的承载了。IPWeb 浏览器会内置存储挖矿和 IPW 钱包两大功能。用户可以在浏览器里设置把闲置的存储空间贡献出来进行存储挖矿。得到了存储奖励会直接到用户的 IPW 钱包里。浏览器挖矿能让几乎所有用户都能成为生产者获得 IPW 激励。用户也可以便捷地在浏览器中进行支付和转账等操作。钱包里拥有 IPW 的用户会更容易参与到高层的经济活动中。

第三层经济模型里，我们有一套经济机制来鼓励开发者开发基于 IP-Web 的网站和应用。在这一层的生态中，去中心化互联网生态与中心化互联网生态已经趋于接近。IPWeb 的目标就是塑造一个去中心化版的互联网应用生态，并让 IPW 成为这个应用生态的通货。让开发者可以用 IPW 支付技术成本，可以从消费者手里获得 IPW 的盈利。IPWeb 通过多层次的、不断完善的经济模型激励更多节点和用户加入到去中心化存储和去中心化互联网的技术浪潮中来。这是共享经济和区块链技术带来的崭新时代。



## 07 IPWeb的官方通证-IPW

IPW是IPWeb共享生态下的一种数字资产,是系统内建的、工具属性的价值度量、存储和激励工具,IPW发放总量为1亿IPW,永不增发。可在主链与侧链之间、侧链与侧链之间转移价值,比如:支付交易费、购买存储服务、激励贡献等。IPW是基于区块链的权益凭证,是分布式存储系统的关键要素。驱动用户贡献存储空间和带宽的经济动力。IPW的价值就是以这些存储和带宽以及利用这些资源获得的收益作为背书的。通过实现平台的商业化运营从而来逐步提升IPW在生态下的实际价值。另发行IPWT(IPW Token)作为流通代币,发行数量初期为100亿,发行后一年内分期销毁至1亿。主网币(IPW)和流通币(IPWT)为等值,即:1 IPW = 1 IPWT 官方提供兑换渠道。

IPW	
来源	IPW Chain
应用	支付交易费、购买存储服务、激励贡献等
用户	IPWeb生态参与者

### IPW 使用

IPW 是 IPW Chain 发行的原生 Token, 将有如下用途:

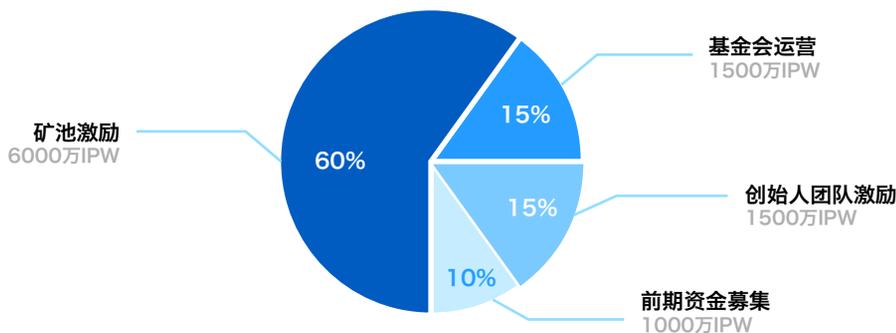
- 生态激励 (包含公共账本维护、内容上传共享、存储空间贡献、检索算力贡献);
- 支付文件存储、智能合约部署等手续费用;
- 检索及文件下载支付的费用;
- 用于支付交易的燃料 (Gas)。

用户可通过以下几种方式获取 IPW:

- 竞选超级节点, 参与公共账本维护, 获取平台的记账奖励;
- 参与检索节点, 共享算力, 获取平台的检索奖励。
- 通过共享存储空间, 获得平台的存储激励;
- 参与平台的流量贡献, 上传内容, 分享内容, 让更多的用户共享优质内容。
- 市场交易 (包含赠与、购买等)。

## 07 IPWeb的官方通证-IPW

### 7.1 IPW 分配

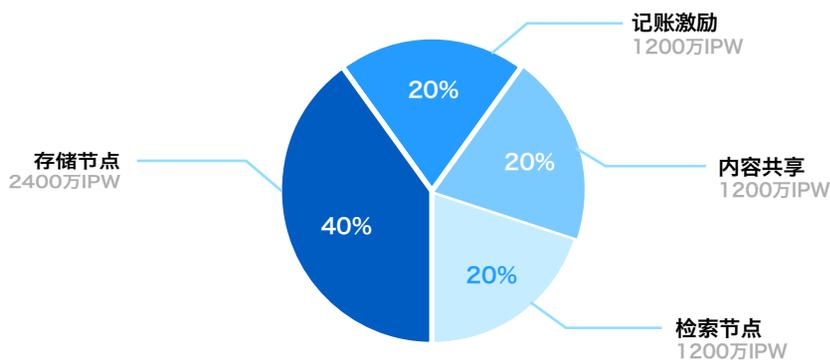


备注：创始团队持有的 15% IPW，团队承诺锁定 2 年，之后分2年线性释放。

### 7.2 IPW 激励

用户可以通过贡献自身的资源（存储空间、算力、内容等），来获得 IPW。IPWeb 提供整个 IPW 总量的 60%（6000 万）激励用户建设 IPWeb 生态。这其中 20% 用于公共账本维护，用于保证整个 IPWeb 基础的公共账本的稳定性和有效性。40% 用于存储节点的挖矿激励。20% 用于用户的内容上传分享激励，用以丰富 IPWeb 的生态。20% 用于检索节点的检索奖励。

#### 矿池激励（6000万IPW）



## 07 IPWeb的官方通证-IPW

### 7.3 IPW释放

从启动挖矿之日，块产出会逐渐递减，总量10年内出完。出块时间为1s。10年后区块不再产生新的IPW。IPWeb平台上线需求对接系统，之后的矿工激励由需求方付费提供。在IPW生态中，用户贡献的资源越多，获得的IPW就会越多。IPW每24小时分配一次，系统将24小时内的用户及节点在每个有效期获得的IPW分配，并写入IPWChain。



## 08 IPWeb的应用场景

### 8.1 分布式文件存储

IPWEB 分布式存储云能够提供基础的云存储服务。通过 OpenAPI, 客户可以很容易的接入和使用 IPWEB 云存储服务。分布式存储云能够提供更安全、更可靠和具有极高性价比的云存储服务。

### 8.2 分布式文件共享

分布式共享云是利用分布式存储云一共的存储服务作为基础, 用户可以把他们拥有的一些文件 (数字媒体或其他有价值的内容) 进行共享。共享时可以根据具体的内容设定一定额度的 IPW 打赏要求。如果其他用户希望能够完整的下载或观看该文件, 就需要支付相应额度的 IPW 作为打赏给上传者。作为一种文件共享服务, IPWEB 将严格按照运营所在地的法律要求对用户的上传内容进行审核和管理。

### 8.3 多媒体应用

目前传统在线视频网站采用的是中心化存储服务, 这需要高额的储存费用和带宽费用, 相关的费用会转化为: 观看长时间的广告及限制非会员观看等。而使用了 IPWeb 作存储服务, 将大大降低了相同资源的冗余, 同时节约了大量用户播放视频时产生的带宽成本, 使得观看视频更加高效和低廉。

### 8.4 数字内容交易

由于采用了区块链和分布式存储技术, IPWEB 存储云非常适合为长尾内容的版权交易提供存储能力。分布式账本能够为交易提供公开、透明和不可篡改的交易记录。也能为数字内容作品在区块链上留下不可篡改的、唯一的数字签名作为版权所有的标识。在 IPWEB 平台的支持下, 大量的长尾视频、音频和摄影创作能够有了一个低成本、可持续运作的交易平台。

### 8.5 社交应用

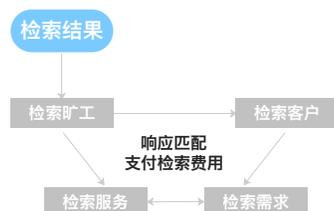
使用 IPWeb 技术创建一个去中心化的社交网络。作为一个去中心化的应用程序, IPWeb 网络可以让社交应用可以在没有任何中心点的情况下工作, 完全点对点。

## 09 IPWeb的生态建设

### 9.1 存储生态

存储矿工为网络提供数据存储，存储矿工通过提供磁盘空间和响应客户请求来参与 IPWeb 运作。要想成为存储矿工，用户需要提供存储空间及带宽资源。矿工将用户的数据片段存储到扇区，并以此赚取 IPW。存储矿工通过在特定时间内存储数据，来响应用户的存储请求。存储矿工生成证明并提交到区块链网络，来证明他们在特定时间内存储了数据。如果数据失效或丢失，存储矿工将被罚没部分抵押的 IPW。存储矿工工作流程：

- 存储矿工在区块链中存放抵押的 IPW，来保证向网络提供稳定的存储。抵押品为了保证服务而存在，如果矿工为所存储的数据生成了存储量证明，抵押品就会被退回。如果没有成功生成存储量证明，矿工将失去抵押品。
- 一旦抵押交易在区块链中出现，矿工就可以在存储市场中提供存储服务。
- 一旦订单匹配，客户就将数据发给存储矿工。存储矿工数据接收完成后，矿工和客户签署交易订单并提交到区块链。
- 当存储矿工被分配了数据时，必须重复生成存储量证明来确保他们正在存储数据证明被发布在区块链中，并由网络来验证。
- 验证成功后，存储矿工将会获得相应的存储奖励。



### 9.2 检索生态

检索矿工为网络提供数据检索服务，检索矿工通过提供用户检索请求所需要的数据来参与 IPWeb 运作。和存储矿工不同，他们不需要抵押品，不需要提交存储数据，也不需要提供存储证明。

### 9.3 应用开发者生态

IPWeb 需要更多的商业来繁荣整个生态，需要有相应的应用开发商来经营业务，让更多的存储需求进来。

### 9.4 应用服务生态

IPWeb 为用户提供文件存储及检索服务，用过通过 IPWeb 浏览器使用 IPWeb 提供的各项服务。

## 10 IPWeb的发展规划

**2018**  
Q2

- IPWeb立项
- IPWeb团队建立

**2018**  
Q4

- IPWeb主链（测试版）
- 区块浏览器（测试版）
- 文件浏览器（兼容HTTP协议）
- 图片分享网站（www.ipweb.io）
- IPW矿机原型产品

**2019**  
Q1

- IPW矿机预售
- IPWebChain主网公测
- IPWeb浏览器公测
- IPW钱包公测
- 应用层产品公测

**2019**  
Q2

- IPW矿机销售及生态建设
- 应用层开发者生态建设等
- 浏览器上线（浏览器挖矿）
- IPWeb域名推广
- IPW钱包上线推广
- IPWebChain主网上线

**2019**  
Q3

- 生态建设
- 应用层生态产品上线

## 11 团队架构

### Richard

CEO创始人

日本工学硕士。

模糊数学，人工智能专业。

曾经引领开发过语音识别、图像识别、分布式存储、P2P 通信、区块链技术等众多项目。创建千人以上规模软件公司。

### Edward Nakamoto

联合创始人

15 年以上金融系统软件研发经验。

参加过数个大型金融软件系统构架、基盘研发。

2015 年开始参与数个区块链 POC 项目、精通联盟链、私有链设计、智能合约设计。

现专注于区块链技术推广、商业提案以及区块链项目落地。

### Zhu

大数据及应用平台架构师

清华大学计算机系。

曾就职于 IBM、摩托罗拉公司。

20 年软件行业经验，在物联网及大数据平台的架构与应用方面有丰富的项目经验。

### Tom Li

区块链架构师/IT架构师

IT 咨询师，系统架构师，精通商业提案。

2013 年起研发区块链产品，设计 ICO 发行。

曾任职于 IBM、KPMG。

历任企业区块链首席研究员、讲师等。

### Phenix Cho

系统架构师

15 年+ 大规模系统的平台架构的设计和实际构筑经验。

痴迷开源软件技术。

曾任某电子音乐分享社区技术合伙人。

丰富的应用开发实战经验。

## 11 团队架构

### Taiyong King

人工智能架构专家

日本九州大学工学博士(计算机系)。  
近20年软件行业经验，熟知多种开源技术。  
在工业互联网，人工智能，大数据领域有丰富的项目实践和管理经验。

### Ian

开源软件及网络通信专家

20年以上系统软件研发经验，熟知多种开源软件技术。  
专注互联网应用系统开发。  
对WEB前端，移动端，后端均有丰富的研发实战经验。

### Peter Pan

互联网全栈工程师

互联网全栈工程师。  
擅长网站开发，手机APP应用开发。后台应用，服务器设置。

### Tommy

区块链工程师

IT 工程师，丰富的 Web 设计开发及以太坊智能合约设计及开发经营。  
擅长手机 APP 应用开发设计。Ethereum の smart-Contract 经验丰富。

### Logan Yokoyama

媒体推广专家

SNS的新媒体推广专家。  
美国硅谷5年经验。  
熟悉日本和美国的各种媒体推广。

### Charity Liu

社区推广负责人

精通市场策划、宣传推广统筹。  
日文英文渠道营销经验丰富。

### Cony Hirano

数据分析及市场策划

擅长区块链行业数据分析和市场信息搜集。  
精通市场活动策划。

## 12 社区治理

为保证 IPWeb 项目健康有序的发展，IPWeb 团队提出了一个去中心化的治理结构，解决区块链项目的治理结构问题。设立去中心化的治理结构，通过全体持币者的投票机制来解决公平决策的问题。全体 IPW 持有者都可以通过投票参与 IPWeb 社区的治理及，1 个 IPW 为 1 票。

### 12.1 治理机制

IPWeb 拟采用社区大会（网络形式）、自治委员会和运营委员会三层结构进行运营治理：社区大会是全体 IPW 持有者大会（网络形式进行），社区大会为 IPWeb 项目最高决策机构，IPW 持有者在社区大会上具有投票权、选举权和被选举权。IPWeb 基金会是 IPWeb 治理的主体，对社区大会负责，全面负责执行社区大会决议，选任运营委员会成员，监督运营委员会的工作，维护 IPW 持有人的权益，宣传推广 IPWeb 品牌等。运营委员会负责 IPWeb 项目日常运营管理工作，下设区块链研发中心、商业中心、财务部、法务与风控部、综合事务部等多个职能部门，分别完成相应的工作任务。

#### 1、IPWeb 社区大会

IPWeb 社区大会由全体 IPW 持有者组成，是 IPWeb 项目的最高权力机构，行使以下职权：

- 修改 IPWeb 管理章程；
- 监督 IPWeb 管理章程的实施；
- 选举和变更 IPWeb 基金会委员（考虑 IPWeb 初始阶段的特殊性，第一届 IPWeb 基金会委员，由 IPWeb 项目法人单位和创始团队决定）；
- 撤销 IPWeb 基金会的适当的决定；
- 批准 IPWeb 重大变更事项。

以上决议表决权，按照 IPW 持有者所持 IPW 的币数和币龄权重的形式，进行投票表决。

IPWeb 管理章程是 IPWeb 自治体系的宪法，公示窗口为 IPWeb 官网，计划在 IPWeb 上线试运营半年内公布 IPWeb 管理章程，第一版管理章程由自治基金委员会制定公布。

IPWeb 社区大会每年举行一次，若 IPWeb 基金会认为有必要，或者五分之一以上 IPW 持有者提议，可临时召开 IPWeb 社区大会。

#### 2、IPWeb 基金会

IPWeb 社区大会由全体 IPW 持有者组成，是 IPWeb 项目的最高权力机构，行使以下职权：

## 12 社区治理

- 负责召集 IPWeb 社区大会，并向大会报告工作；
- 执行 IPWeb 社区大会的决议；
- 聘任或者解聘 IPWeb 运营委员会首席执行官，根据 IPWeb 运营委员会首席执行官的提名聘任或者解聘执行委员会其他成员；
- 决议 IPWeb 基本管理制度；
- 决议 IPWeb 开源代码重大问题和资金使用重大问题的解决方案；
- 应对 IPWeb 出现的紧急事件。

IPWeb 基金会成员 6 名，设主席委员 1 名。IPWeb 基金会成员任期 1 年，可以连任，IPWeb 基金会主席由委员会投票选举产生。IPWeb 基金会至少每半年召开一次全体会议，会议由半数以上委员或主席提议后召开，每次会议召开前十五日通知全体委员。IPWeb 基金会所做的会议决议，必须经过 IPWeb 基金会的投票通过，并在 IPWeb 官网上公告。

IPWeb 基金会主席行使以下职权：

- 主持 IPWeb 社区大会和召集、主持 IPWeb 基金会会议；
- 检查 IPWeb 基金会决议的实施情况；
- 拥有对 IPWeb 基金会会议决议的一票否决权；
- 签署 IPWeb 对外合作协议。

### 3、IPWeb 运营委员会

IPWeb 运营委员会负责 IPWeb 项目日常运营管理，运营委员会设首席执行官一名，首席执行官对 IPWeb 基金会负责，运营委员会委员主要由各职能部门负责人担任。

运营委员会首席执行官行使以下职责：

- 主持 IPWeb 日常运营管理工作，组织实施 IPWeb 基金会决议。拟定 IPWeb 管理制度；
- 决定聘任或者解聘运营委员会委员或者其他高级管理人员；
- 拟定 IPWeb 开源代码问题和资金使用问题的解决方案。

### 12.2 信息披露

为保护投资人的利益，加强 ICO 众筹到的数字资产监督管理和使用效率，促进 IPWeb 项目的健康发展，IPWeb 项目设置信息披露制度：每个会计年度之日起三个月内编制并披露年度报告、每个季度结束后的两个月内披露季度报告。报告内容包括但不限于 IPWeb 项目技术开发进度，市场运营状况，数字资产管理情况，核心团队成员履职、变更情况，财务收支状况，重要商务合作事项，涉及到 IPWeb 的法律诉讼等。

## 13 风险申明

IPWeb项目的参与者，请仔细阅读本项目白皮书，全面认识IPWeb的技术特性，IPWeb的风险收益特征，并综合考虑自己的风险承受能力，理性参与，谨慎决策。无论作为购买者、使用者还是投资者，都可能面临包含：政策风险、经济周期风险、开发进度风险、网络安全风险、人才流失风险、交易风险、市场竞争风等以下风险：

### 政策风险

区块链技术已经成为世界上各个主要国家的监管主要对象，但目前区块链、数字货币等领域的政策监管不明朗，如果未来相关政策变动有可能给项目带来或积极或消极影响。

### 开发进度及技术风险

由于外部因素或产品开发方案执行不到位，可能出现开发进度被拖慢的问题；IPWeb落地应用后，可能由于更新不及时、严重功能缺陷等技术不完善问题，导致用户体验差甚至引起损失。

### 网络安全风险

黑客或其它组织或国家均有以任何方法试图打断IPWeb应用或IPWeb代币功能的可能性，包括服务攻击，Sybil攻击，游袭，恶意软件攻击或一致性攻击等。此外，密码学的飞速发展或者科技的发展诸如量子计算机的发展，或将破解的风险带给加密代币和IPWeb平台，这可能导致IPWeb代币的丢失。

### 购买者凭证相关的风险

任何第三方获得购买者的登录凭证或私钥，即有可能直接控制购买者的IPWeb代币，为了最小化该项风险，购买者必须保护其电子设备以防未认证的访问请求通过并访问设备内容。

### 人才流失风险

区块链领域人才资源短缺，团队核心技术人才和运营人才的流失，泄露核心技术机密，不利于项目发展。

### 市场竞争风险

IPWeb应用存在没有被大量个人或组织使用的可能性，这意味着公众没有足够的

## 13 风险申明

兴趣去开发和发展这些相关分布式应用。这样一种缺少兴趣的现象可能对IPWeb应用造成负面影响。IPWeb平台对传统商业保理和银行质押业务发起冲击，未来竞争对手可能进行市场调整，引起项目部分用户及资源流失。

### 交易风险

财产损失——IPWeb应用当前正处于开发阶段，在发布正式版之前可能会进行比较大的改动，任何IPWeb自身或购买者对IPWeb应用功能或形式(包括参与者的行为)的期望或想象均有可能达不到预期，任何错误地分析，导致价格上下波动等均有可能导致用户财产损失。

未参与保险的风险——不像银行账户或其它金融机构的账户，存储在IPWeb账户或以太坊网络上通常没有保险保障，任何情况下的损失，将不会有任何公开的个体组织为你的损失承保，但诸如FDIC或私人保险公司将会为购买者提供保障。

IPWeb存在的解散风险——存在这样的可能，出于各种原因，包括ETH自身价格的波动，IPWeb应用发展遭遇问题，生意关系的破裂或知识产权索赔等可能性原因，IPWeb项目随时都有可能遭遇重大打击或直接解散。

## 14 免责声明

---

IPWeb是公益性、非营利系统，系统未来的内部奖励机制、运营维护机制均采用虚拟数字资产(即虚拟商品)，而非采用货币奖励机制。系统自身产生的数字Token，可以作为系统维护的奖励，但为了满足系统与其他系统或其他社会主体的资源交换，需要一定量比特币等其他虚拟数字资产的介入。据此，IPWeb所获取的资产也仅为类似的虚拟数字资产，如比特币。本白皮书只用于传达信息之用途，不构成任何投资建议，投资意向或教唆投资。本白皮书不组成也不理解为任何买卖行为，或任何邀请买卖、任何形式证券行为，也不是任何形式上的合约或者承诺。IPWeb项目参与者，请务必仔细阅读此白皮书，全面认识区块链的技术风险收益特征，并充分考虑自身的风险承受能力，理性判断，审慎决策，一旦参与项目即表示了解并接受该项目风险，并愿意为此承担一切相应结果或后果。

IPWeb - High performance public chain based on P2P storage

官网: <http://www.ipweb.io/>

邮箱: [contact@ipweb.io](mailto:contact@ipweb.io)

