IPSE

# 星际搜索引擎

# 黄皮书

(2019)

# The Yellow Book

## 下一代价值互联网的流量入口

ipse.io

# 目录:

# 1. 引言

## 1.1 背景

时间到了2019年，分布式存储逐渐进入了落地阶段，不管是以往在分布式存储领域试水的Sia、Storj等前辈项目，还是目前正在走向测试阶段的Filecoin，还是数个等不及Filecoin上主网而推出的对飙型的分布式存储公链项目，例如Lambda、Yotta和Filestorm等，这些项目不管其共识机制如何，都基本有一个特点，那就是在构建一个开放的存储市场方面做出了优秀的尝试，同时它们会面临一个极具挑战的问题，那就是一个开放的分布式的存储市场，用户是否愿意一开始将让数据付费存储进去。

## 1.2 摘要

IPSE是基于IPFS网络的搜索引擎，实现了将IPFS网络上的数据标签化，同时肩负着一个重大的使命，那就是使IPFS网络从节点少且很难使用的状态，过渡到节点广泛存在、使用起来轻松简单的状态。

IPSE提供一个基于IPFS网络的存储内容的快速检索入口，同时建立了用户分享数据和存储空间的奖励机制，IPSE将采用*PoST(Proof-of-Storage-True)*算法保证数据的高效存储和利用。未来，IPSE主链将采用21个超级节点的*DPoS*共识机制，保证共识网络高效运转和可靠性。

IPSE将是第一个走完数据完整生命流程的分布式存储类项目：从数据的来源，到数据的存储，到数据的检索， 到数据的访问，都将在IPSE的体系中完成。IPSE将不同于Filecoin等分布式存储公链项目，IPSE将不提供一个分布式的存储空间市场，而是通过一个分布式的存储任务分发系统，基于IPFS的底层存储网络，以及基于石墨烯技术的成熟且高效的共识网络，让IPSE成为价值互联网的检索入口。基于此入口，IPSE将构建一个DAPP矩阵，包括通证激励内容，内容打赏，版权保护，版权繁荣，流媒体门户，分布式广告平台等。

## 1.3 技术组件

IPSE主要有以下技术组件构成：

共识网络：IPSE的共识网络由21个超级节点，100个备选节点，基于*DPoS*作为底层共识。IPSE的共识网络将承担所有链上逻辑运算，包括为存储空间提供者(存储矿工)奖励token，质押部分奖励token，罚没质押token，黑名单状态维护，数据提供方的奖励，抵押token，罚没抵押token等，同时整个共识网络的底层虚拟机是支持图灵完备和支持智能合约轻松部署。

存储网络：IPSE的存储网络是以IPFS为底层的存储网络，目前是支持IPFS底层存储网络，当然不排斥后面接入更多的底层存储网络。存储网络在IPSE系统中是逻辑解耦的，存储网络跟共识网络是完全异构的网络，只是IPSE检索出来的数据，访问层要兼容不同存储网络平台。

任务分发系统：IPSE有一个分布式的任务分发系统，此分发平台不仅有数据下载任务的分发，还有数据下载源的分享，IPSE也会将此种分享行为视为挖矿行为，也将会有奖励。总之，此任务分发系统，将

保证数据既有来源，又有去处。

节点客户端：IPSE会在数据访问层推出自己的节点客户端，如果底层存储不仅仅是IPFS网络，还有其它网络的接入，就需要节点客户端来整合所有的这些P2P网络。同时，IPSE的节点客户端将优化Peer的查找，使得IPSE中所有Peers都能加入种子列表。总之，用户下载IPSE的节点客户端就能畅享IPSE上的所有数据。

## 1.4 流程简述

IPSE是一个将数据在分布式网络中存储并构建起索引入口的下一代价值互联网基础设施。POST作为IPSE的原生数字token。IPSE中的超级节点将肩负多重任务，21个超级节点和100个备选超级节点将是IPSE的共识网络的维护者，同时将担负起验证者的角色。包括两方面的验证：一个是数据持有性检验，一个是数据源真实性检验。整个存储网络的安全性，需要依靠超级节点验证者的维护，实现方式是主要通过罚没抵押在合约中的token奖励。同时，整个数据源头需要从任务分发系统进行对接，而接入任务分发系统是开放的，数据源是否可以下载数据并存储，就需要超级节点进行验证，并通过罚没抵押的规则来维护网路。

存储挖矿：存储矿工从任务分发中心接收到任务，完成下载，存储到IPFS网络，将完成任务提交到链上，等待超级节点发起数据持有性挑战，存储矿工在接收到超级节点随机发起的挑战后，需要完成数据持有性证明，然后超级节点能验证证明给予存储矿工奖励。

分享挖矿：任务分发节点需要大量存储任务分发，任何人只要有这种存储任务，能够分享给任务分发节点，就能获得奖励。当然这其中有几个主要注意的点，存储任务的数据不能侵犯版权，不能是违法违规数据，数据要能正常下载。

检索和访问数据：IPSE上检索数据是免费的，访问数据是自由的，如果需要付token的版权内容，是需要支付后才能观看的。

## 1.5 术语约定

SuperNode(超级节点)

超级节点是整个IPSE的共识网络的出块节点，并且承担起另外两个核心验证的工作，一个是数据存储证明PDP 的验证者角色，一个是数据源真实性验证者角色。超级节点保证了整个IPSE的共识网络高效稳定运行，同时超级节点并不能出现舞弊行为，因为还有100个备选节点参与候选，超级节点需要得到社区足够多的投票支持才能当选。

StorageMiner(存储矿工)

存储矿工提供存储空间并接收任务分发系统的存储任务，完成数据下载并存储，且需要提供正常的数据访问服务的节点。存储矿工主要是通过存储数据的多少和种类来获得奖励。接收到的任务分发系统分发的任务也是随机的，其挖矿奖励段时间具有随机性，但长时间是稳定的。存储矿工在IPSE生态体系中是

最基础的部分，他们是接下来去中心化价值互联网的基础设施建设者。

DataSourceMiner(数据源矿工)

数据源矿工能够提供数据源的接入节点，所有数据源矿工都要为自己的数据源担负责任，比如数据源不能涉及到数据隐私泄露、数据版权盗用等。数据源矿工参与挖矿也是需要抵押POST，为自己的数据源承担一定的责任，一旦出现举报并被核实，就会罚没挖矿奖励和抵押品。数据源矿工是整个IPSE生态体系中重要的组成部分，在去中心化网络发展的下一个十年，他们承担着将中心化互联网的数据搬迁到去中心化网络的重任，他们是价值互联网中数据和价值的搬运工。

PDPPD(部分授权的可证明数据持有验证)

*PDPPD*是指部分授权的可证明数据持有验证，即*Provable-Data-Possession-Based-on-Partial Delegation*。任务分发节点授权代理对存储矿工存储的数据进行持有验证。此方案基于双线性对及部分授权技术，支持数据拥有者直接通过密钥形方式委任代理方进行数据持有验证，并且数据拥有者可以随时撤销或更换代理方，证明了方案的安全性。此方案主要优点是减少了计算量和通信量，应用场景更加广泛。

SuperNode-PDP（可信超级节点的数据持有证明）

基于可信超级节点的*PDP*证明，在借鉴*PDPPD*方案的优点后，IPSE采用独特数据完整性证明设计。IPSE 将区别于分布式存储型公链，并不会在数据完整性方便做到极致。这是充分考虑到效率而设计，因为存储节点本质应该是去进行数据存储和分发，而不是将大部分CPU用来做数据完整性证明。当然为了数据的基本安全，还是需要持有性证明的，IPSE的数据完整性证明基于*PDP*、*POR*证明，IPSE将采用链上的参数作为随机数，让超级节点承担存储证明的挑战者角色，存储矿工需要执行预定义的证明函数生成多次证明的证据集合，然后提交到链上，然后由超级节点随机挑选验证。

Sector（扇区）

存储矿工使用扇区为单位对存储空间进行划分，然后以扇区为单位对数据完整性进行证明，当超级节点发起对某个扇区进行挑战的时候，存储矿工需要对这个扇区保存的数据进行完整性证明，超级节点也会对这个扇区的数据完整性进行验证，然后这些证明和验证都会记录到区块链上。

DistributionNode（任务分发节点）

任务分发节点是IPSE独有的概念，所有数据源都会通过任务分发节点来进行随机分发。所有存储矿工都需要注册到任务分发节点中来，这样他们会有相应的概率被分发到任务。只要遵循IPSE的任务分发标准，任何节点都可以注册成为任务分发节点。当然，任务分发是需要抵押和有奖励的。

DistributionSystem(任务分发系统)

任务分发系统，是由任务分发节点组成，每个节点都按照IPSE的任务分发规则进行任务分发，同时整个系统将采用新的合约来设计。IPSE基金会将建设一个任务分发奖励池，鼓励社区建设强大的任务分发节

点，让整个IPSE的生态更加丰富和多元化。任务分发系统将是一个奖罚分明的体系，任务上传是需要抵押POST。当下载任务被存储节点完成后，任务上传者将获得部分奖励，如果在数据源澄清期没有出现纠纷，任务上传者将获得所有奖励和抵押。如果上传任务不能下载，或者在澄清期出现纠纷，被数据源合法性仲裁者判定为败诉则将罚没所有奖励和抵押。

DataSourceClearPeriod(数据源澄清期)

任务分发节点接收上传来的数据源，需要有一段时间来澄清其数据源的合法性，此合法性包括数据所有权，会不会侵犯他人版权，是否涉及到儿童色情、恐怖暴力等内容。IPSE合理地设置一个数据源澄清期为1年。

DataSourceValidArbitrator(数据源合法性仲裁者)

在数据源澄清期，如果出现纷争(比如出现了版权的诉说或者投诉)，数据源合法性仲裁者都会担当做出终裁的角色。如果要选出这样权力巨大的仲裁者，就需要IPSE的利益相关方深度参与，在IPSE体系中，超级节点是最大的利益相关方，每个超级节点推选出一个仲裁者是不错的选择。

ProofSet(证明集合)

证明集合是一系列证明的集合。存储矿工以扇区为单位进行存储证明，然后所有扇区的证明集合将上链，然后广播到所有共识节点，由超级节点进行随机挑选挑战验证。打包到区块并完成存储矿工工作量证明，给予相应的奖励。

PledgeRatio（抵押率）

存储矿工在存储挖矿时，并不会在第一时间得到所有token，而是有一个抵押比例的token被质押在合约里，然后在接下来的5年内释放给存储矿工。这个抵押比例就是抵押率，抵押率是会动态变化的，跟IPSE的矿工信用度相关。

CreditDegree（信用度）

信用度是节点信用度指标。IPSE中存储矿工接入后，信用度是非常低的，随着时间的积累，矿工都能够稳定存储数据来挖矿，这样矿工能够不断积累自身的信用度。

ChallengeJump（挑战跳跃）

超级节点在存储矿工完成存储后，会进行第一次的挑战。但为了整个系统的负载平衡，并不会长期进行挑战，会根据存储矿工信用度在时间上跳跃来挑战。存储矿工信用度越高，跳跃时间越长，挑战频率就会降低，反之则挑战频率升高。

SystemContracts（系统合约）

系统合约是IPSE的系统合约是内置合约，基本跟随EOS体系会一直升级更新。因此，随着EOS这一优秀的公链发展，IPSE也将会有优秀的共识层，并且吸取EOS最强的社区治理模式和经验。

Wallet（钱包）

IPSE钱包，跟随EOS钱包生态一起发展。EOS生态会逐渐成为最主流的区块链生态之一，IPSE钱包也将受益于此生态的多元化。IPSE钱包将在众多平台适配，包含移动端、桌面端和服务器端等。IPSE是下一代价值互联网的入口，而真正承载价值闸门的将是IPSE钱包，IPSE钱包将易用性和兼容性做到极致。

# 2. IPSE的出发点

## 2.1 从0到1

一个有价值的项目一定包含两部分，第一部分是Production，也就是产品从0到1点阶段，打磨好具有市场口碑且极具产品力的产品；第二部分是Distribution，这个打磨好的产品能够进行快速复制且拥有比较低的成本优势。深入分析所有这些分布式存储项目，其经济模型和技术特点决定了其1到N的分发复制将是巨大的优势，只要能从0到1做到真正落地实现，没有理由怀疑其不能成长为未来的主流存储选择。但这些项目都有一个致命的缺陷， 那就是一个先有鸡还是先有蛋的问题。

存储空间是有成本的，而数据又是无处不在的，两者看似能够轻松结合起来，但到了实际操作层面，结合却很难。分布式存储公链项目能够轻松构建出一个具有透明价格的存储空间市场，价格是浮动且合理的。但数据是否愿意存储进网络？按照目前市场的反馈来看，可能并没有多少人愿意为之买单。为何会出现这种看似不合理的局面呢？其中的逻辑其实比较清晰，站在项目方的角度，构建一个低成本优势的分布式存储空间，自然就会有用户付费让数据存储进来；站在数据存储方的角度，一个没经过绝对考验的分布式的存储空间，数据是不能轻易存储进去的。对于数据存储方而言，数据存储成本低于数据分发时的网络成本。存储在中心化服务器更加高效，而按照目前的Filecoin的分布式存储解决方案，检索数据还需要付费，对于大规模分发数据，不仅不能降低成本，反而增加了成本。

如果挖掘其本质去看待这一问题，数据存储具有强烈的服务属性。对于客户（数据存储需求方）而言，其并不关心底层存储硬件使用寿命，如何灾备，数据迁移，硬件故障等一系列问题。客户付费存储数据只关心一 点:我的数据要安全保存且成本可控。数据存储就是一个服务行业，效率是第一位。如果放到去中心化存储方案里，数据存储方可能既要担忧数据安全存储问题，还要考虑成本不可控问题。

## 2.2 致命的低效

到目前，在多个分布式存储公链中，技术最为严谨且发展路线最为清晰的当属Filecoin项目。但从根本性的设计角度去观察，Filecoin目前遇到了几个挑战点：

1.消耗大量的CPU做复制证明计算，相对于中心化存储还具有成本优势吗？

2.海量的撮合交易在*DSN（Distributed Storage Network）*市场是否能够最终高效地完成？

3.检索数据能否做到高效且免费？

4.无公网ip存储节点能否贡献有效存储空间?

以上四个问题考虑到了效率问题。观察目前的分布式存储型公链，它们或多或少都需要解决一些技术难点。如果每个存储节点使用非常高性能的CPU都不能满足网络中数据复制证明的需求，那就意味着还需要更加昂贵的GPU来解决这个问题。这样虽然可以实现，但成本远远超过可控程度。中心化存储节点相对简单容易得多。

如果在去中心化的撮合交易市场中，无法完成大量的订单交易，那这个存储空间市场就会因为成本问题难以发展，同时，很难通过基于该分布式存储网络来进行DAPP，因为高效的优势不再存在。如果检索数据不能够像中心化存储服务节点那样高效且接近免费，那么分布式存储市场的很难具备优势。如果分布式存储节点还需要一个公网ip，那其相比中心化存储，既不会那么分布式，也不会那么低成本。

## 2.3 PoST(Proof of Storage True)

IPSE的通证简称$POST$，并不是时空证明$(Proof\ of\ Space\ Time)$的缩写，而是IPSE存储算力证明使用到的共识机制的缩写。IPSE的共识机制为$Proof\text{-}of\text{-}Storage\text{-}True(PoST)$，中文翻译为*存真证明*，刚好对应中文“*去伪存真*”的含义。存真证明指的是真正存储数据，证明存储真实有效，并且存储真实有价值数据。

当绝大多数项目都还在为先有鸡（具有成本优势的分布式存储空间）还是先有蛋（能够在分布式存储空间上存储的数据）探索的时候，它们从0到1的探索中难以找到出路。IPSE进行了另外的探索，先把海量数据真实存储到分布式的存储空间，而不是让海量的分布式存储空间空在那里，傻傻的等待数据过来存储。如果没有数据过来存储，还要傻傻的花费几乎所有的CPU去做复制证明，只为证明存储空间还是空的，然后所有人去参与炒币，没有人关心那些分布式存储空间是否真的被高效利用起来。IPSE绝不是这样一个无聊游戏的参与者，其存真证明共识就自然而然让所有节点真正存储数据，并且需要证明存储真实有效。

# 3. IPSE Consensus

## 3.1 奖励规则

IPSE是让数据真实存储，这种普遍发生的存储行为，不能只是仅仅考虑存储数据的大小，还要考虑数据的其它维度。IPSE的奖励规则设计是非常清晰的，考虑的维度有三个方面：第一个方面是存储数据大小，第二个维度是数据的类别，第三个维度是数据的保存份数。如果数据大小为s，数据类别为$c \in C$，保存份数为$n$，那么其算力$w$的计算公式为：

$$w = s * c * 1/n$$

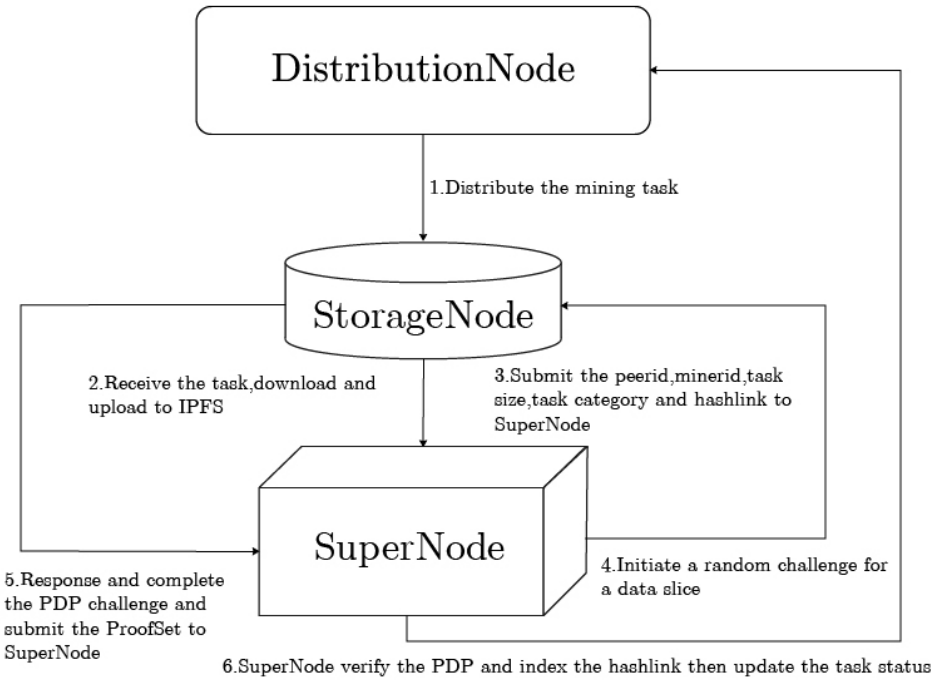
矿工产出通证量$t$，还要考虑全网总算力，这个全网总算力是上一天的全网总算力$TW$，还有当日通证总产量$TT$，矿工每次挖矿产出通证的计算公式如下：

$$t = w / TW * TT$$

摇摆攻击

假设，矿工们联合起来，第一天消极挖矿，导致全网总算力下降非常多，第二天又联合起来异常积极挖矿，这样会导致第二天产出非常高。这种现象称为摇摆攻击。IPSE使用两个机制来防治摇摆攻击：第一个是设置了全网算力下降阈值（矿工联合起来虽然可以使得全网算力下降非常多，但算力并不是无限下降的，而是会有一个限制，下降到一定程度时无法再下降）；第二个是设置当日总产量稳定机制（当日总算力超过昨天总算力的时候，就会导致当日通证总产量$TT$快速下降）。这两个机制将非常好地防止矿工摇摆攻击，基本保证每天的通证总产量保持稳定不变。

## 3.2 共识流程




IPSE Consensus的算法基本步骤如下：

1）任务分发节点随机从任务数据库中抽取任务，随机发放给注册的存储矿机，*taskid* 是任务的ID。

2）存储矿工接收到任务后，进行下载并通过本地IPFS节点上传到IPFS网络的数据传送至*hashlink*。

3）完成下载和上传任务后，需要上报挖矿成果给超级节点。其中包括：*hashlink, minerid, taskid, size, category* 等参数。

4）超级节点接收到挖矿成功后，将这些信息上链，让另外的超级节点随机挑选一个数据切片发起挑战。另外的超级节点也开始随机验证。当有其中一个超级节点发起了挑战，其他超级节点将不再发起相同的挑战，这样可以有效防止超级节点和大矿工进行合谋。

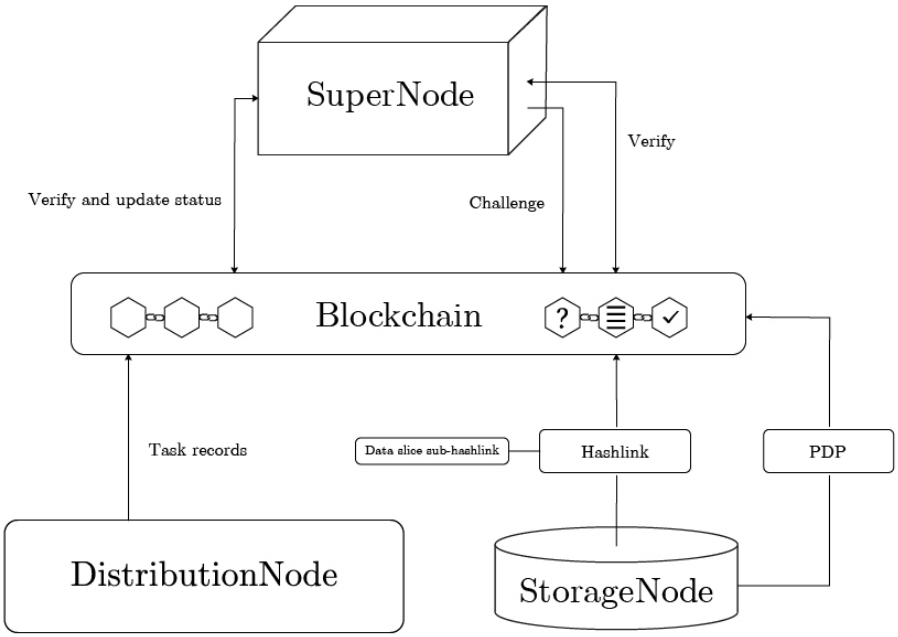
5）存储矿工需要对这些数据切片涉及到的扇区进行数据持有性PDP证明，并且将这些证明集合提交

给超级节点。

6）超级节点验证这些PDP证明，如果通过了验证，将给予存储矿工奖励，最终奖励结果将同步到共识网络。然后索引起 *hashlink*，然后将下发任务的状态进行更新。

> *注：①如果存储矿工无法下载下发任务，也将结果提交给超级节点，超级节点将验证下发任务有效性，这部分将在下章详述；②如果存储矿工无法完成PDP证明，或者超级节点验证其PDP证明无法通过时，存储矿工将面临怎样的惩罚，将在下章详述。*

## 3.3 数据持有性证明 PDP(Provable Data Possession)




取决于检查在协议中的作用的不同，数据持有性证明分为两种基本类型：一种是私人检查（私人可验证性），只有数据所有者可以检查服务器上的数据；另外一种是多个（公共）验证（公共可验证性），任何主管当局可以执行检查程序。IPSE的数据所有权归属在任务分发系统中做出了详细描述，任务分发节点是拥有对数据的所有权的，按理来说任务分发节点会去检查数据的持有性，但IPSE系统中任务分发节点会委托超级节点来进行数据持有性的检查。

1）任务分发节点将为每个任务注入一个*tag*，每个任务都会有自己的一个 *taskid*，这是任务的唯一标识符。并且任务分发节点也会将自己的签名加入其中，这样保证不会有其他任务分发节点充当女巫节点来分发任务。

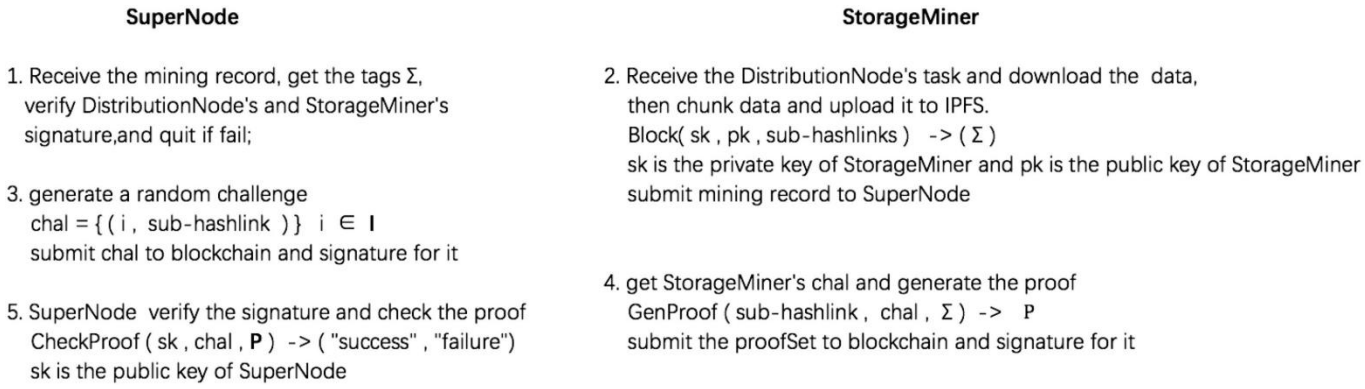
2）超级节点将对存储矿工 *hashlink* 中的一个数据切片 *sub-hashlink* 发起挑战，这个 *sub-hashlink* 可能涉及到一个扇区，也可能涉及到多个扇区，这个*challenge*中包含超级节点从上一个区块中获取的随机数。

3）存储矿工根据被挑战的数据块内容，*tag*信息，*challenge*信息以及自己生成的一个随机数计算得

到一个*proof*。

4）超级节点以*challenge*、*proof* 以及用户公钥为参数，通过预先定义的验证函数去检验存储矿工是否真实存储了数据。

PDP形式化定义如下图：




# 4. 共识安全

## 4.1 安全和效率的权衡

IPSE的存储贡献共识机制为*PoST(Proof of Storage True)*,其最显著的特点也是IPSE最鲜明的特点，那就是效率优先。大部分数据存储在磁盘介质上是为了数据被访问到，特别是热门数据更是被频繁访问到。IPSE将数据建立索引，能够快速被用户检索并访问，注定了IPSE能够保存IPFS上最多的热门数据，并且依靠强大的检索引擎，IPSE也将能够掌握IPFS上数据的热点区域。

效率对IPSE而言是数据能够被快速访问到，安全对IPSE而言是数据在特定机制下被访问到。因为IPSE并不是分布式存储型公链，并不保证数据将安全按照合约期限保存在分布式的存储节点上。那么IPSE将如何实现其所追求的安全呢?

●数据多份保存和多节点分散保存。IPSE的任务分发机制决定了数据并不会单份保存，IPSE的存储成本足够支持数据多份保存，并且将在不同节点分布式保存。

●数据保存期限将和机器硬件使用寿命同步，IPSE假设硬件机器使用寿命在5年左右，数据的生命周期也将在5年左右。5年后，数据随着机器淘汰而逐渐丢失的时候，IPSE将力所能及再次分发这些陈旧的任务。

●IPSE要求存储矿工对挑战到的数据切片做出PDP持有性证明，虽然也是效率优先的原则，只需要对被随机挑选中的数据切片做持有性证明。但为了避免惩罚，矿工的最佳策略还是完整保存数据并且在矿机使用寿命范围内不删除数据。

## 4.2 奖励和惩罚

## 真实存储奖励

IPSE的挖矿奖励分为两部分，其中核心部分就是真实存储数据得到的奖励，这部分奖励不同于分布式存储公链，是不需要矿工进行提前抵押的，只是会将产出的token进行部分质押到合约里，然后在未来5年逐渐释放给用户。这就涉及到质押比例的问题。由于IPSE是一个去中心化的系统，没有一个权威机构能保证矿工的可信度。IPSE定义了一个信任度$cd\ (CreditDegree)$ 的概念，其计算公式如下：

$$cd = \text{接入稳定天数} \ / \ 1825$$

接入稳定天数：存储矿工自接入IPSE第一天开始算起，如果当天没有出现数据丢失，PDP持有性证明全部通过验证，稳定天数加1.

质押率$pr$（$PledgeRatio$）的计算公式如下：

$$pr = \begin{cases} P_0 - cd \\ 0\ (pr < 0) \end{cases}$$

质押在合约的token，会在未来5年线形释放给存储矿工，每年释放质押总token的20%。随着存储矿工稳定挖矿，保证机器稳定运行不掉线不轻易宕机，其信用度就会积累升高，其奖励token被质押的比例就会逐渐降 低，得到的收益也会越来越高。

## 分发任务奖励

IPSE奖励的另外一部分是给任务分发节点的奖励，节点也会给上传数据源奖励。IPSE会对不同的数据源给予不同的权重，其计算方式和算力计算方式是一致的，只是任何任务分发节点在分发一个任务下去之前，都会对这个任务进行声明，包括数据源的类别和大小，当存储矿工完成任务后，只要类别和真实大小跟申明大小没有太大差距，然后数据源通过了澄清期后没有出现纠纷，那么其数据源就是合法的。任务分发节点申明一个任务的时候，是需要质押token的，这是为了防止出现大量垃圾任务的情况。

## 存储矿工惩罚

存储矿工如果没有完成PDP数据持有性证明，就会面临惩罚。存储矿工不能完成PDP数据持有性证明的情况是多种多样的，例如删除数据、宕机、断网、数据盘损坏等。惩罚的力度跟罚没抵押token直接相关。扣罚抵押token比例的计算公式如下：

$$slashratio = \rho * n * (1\text{-}cd)$$

- ρ 为系统初始参数
- n 为未通过PDP持有性证明的次数
- cd 为存储矿工的信用度

当然惩罚还不仅只是限于扣罚存储矿工的抵押token，还会降低存储矿工的信用度。存储矿工的信用度和未通过PDP持有性证明的次数存在如下关系：

$$cd' = cd - \alpha * n$$

◆ α 为系统初始参数

### 任务分发节点惩罚

任务分发节点下发的任务影响整个IPSE系统的运转，其任务是否合法是没有中间地带的。如果出现数据源不能下载的情况，或者在澄清期出现纠纷并被判败诉的情况，将直接罚没所有的奖励和抵押，任务上传时抵押的token还是任务分发节点的，如果任务分发节点下发垃圾任务，不仅得不到奖励，还会面临损失。

## 4.3 他山之石

IPSE跟Filecoin等分布式存储型公链完美兼容。分布式存储公链是构建一个去中心化存储市场，然后让去中心化的存储节点保证数据安全存储，IPSE是尽可能把分布式存储的数据都能检索到。这两者完全可以合作互通。如果一个分布式存储公链上的数据经过数据所有者授权，愿意将数据索引到IPSE生态中，并且其本身是在类似Filecoin完成了复制证明，那IPSE可以借鉴起数据完整性证明，在其贡献了数据的索引后，给予部分token奖励。

IPSE数据来源可以多样化，既可以是任务分发节点做搬运工，将传统中心化互联网的数据搬运到分布式价值互联网，同时，那些一开始就会存在分布式价值互联网的数据也能索引进IPSE而获得token奖励。

# 5. 路线图

## 5.1 第一阶段：中心节点高效挖矿

在EOS主网部署合约进行挖矿，将整个存储贡献奖励机制、抵押机制和惩罚机制通过合约部署到EOS主网。中心节点验证存储真实性，验证接入到存储矿工的合法性。为了防止攻击，中心节点授权存储矿工来挖矿。

这个阶段已经实现，研发时间是从2018-07 到 2019-05。

## 5.2 第二阶段：分发任务挖矿

在EOS主网部署新的合约，让中心节点任务分发也能实现奖励。将整个奖励机制、抵押机制和惩罚机制都通过合约部署到EOS主网，可信中心节点验证任务合法性。

这个阶段已经开始研发，研发时间从 2019-06 到 2019-09。

## 5.3 第三阶段：侧链启动

基于EOS结合社区发行侧链，需要改写底层的代码，实现超级节点来随机发起PDP持有性证明挑战，还要验证存储矿工PDP持有性证明的存储真实性。这个阶段，存储矿工需要做真实的存储数据持有性证明，然后数据持有性证明要上链，超级节点充当TPA(Third Party Auditor)的功能，超级节点一旦通过

存储矿工存储数据的PDP验证，就可以调用合约给予奖励。这个阶段挖矿节点接入将开放，存储矿工信用度机制将开始工作。

这个阶段将在2019-10 到 2020-03 进行研发和测试。当然在这个阶段并不会影响IPSE在EOS主网上的运营， 一旦侧链启动成功，原先EOS主网的token和抵押token都将一一映射到侧链上。

## 5.4 第四阶段：分布式任务分发

中心化任务分发转向分布式任务分发，IPSE将构建一个完整的任务下发标准，标准首要考虑就是任务分发节点和存储矿工合谋，将任务定向下发给某个存储矿工而进行舞弊。任务下发奖励、抵押和惩罚机制合约需要迁移部署到侧链上。分布式任务分发构造完成，数据的来源问题将彻底解决。依靠社区的治理，数据来源有激励，数据存储和分发有激励，数据访问时免费，数据版权有保护，数据版权繁荣有激励。

这个阶段将在2020-04 到 2020-08 完成。