File network

分布式存储领域领跑者

File Network白皮书V2.0

2019年10月

File Network 白皮书 V2.0

Filenet.io

前言

自人类社会进入互联网时代以来，为保障网络世界的自由、平等、开放，实现信息的充分流动，科学、技术、工程人员通过不间断的创新或技术变革来突破种种人为的管制与分割。

Filenet 致力于成为分布式存储赛道的领导者，Filenet 自成立以来，已经创造了多个第一，是第一个上线主网的分布式存储公链，是第一个上线交易所的分布式存储公链，第一个采用 DPOS+POC 共识机制挖矿的分布式存储应用公链。同时，Filenet 在创建出低成本且高效率的数据分发网络同时，也将成为未来区块链网络世界的技术基石。

它尊重互联网用户“免费”的行为习惯，无需支付任何代币即可获得存储资源，保证早期开发者能免费开发出各种 DApp。

数据开放共享是推动数据产业产业发展的源动力，数据是未来世界的石油和源动力，然而现在的数据市场，数据提供方将数据存在在单方私有的数据存储中心，其他需求方下载数据以实现分析。这种模型已经被证实存在较大的弊端，数据交易缺乏透明性，数据所有者的数据所有权和控制权依赖于单方存储节点的职业道德，无法保证数据的安全。

Filenet 的理念就是要改变目前数据交易缺乏透明的弊端，让数据能够自由流通，自由的存储、分析和使用，同构不同安全级别不同宽带的存储节点，分级存储可公开验证和可匿名验证的不同类型的不同等级的数据，从而推动人类公共数据的共享和共有，从而做到共享分布式存储带来的巨大利好。

1.

2. Filenet 介绍

1.1Filenet 是什么

Filenet 是全球分布式存储第一应用公链，以奖励矿工共享自己的存储资源和网络资源，是一种基于分布式存储分发网络提供内容共享的超级云系统，致力于存储和分发有价值内容。

Filenet 因为其独有的共识机制、商业模型、经济模型、生态策略和治理结构成为分布式存储领域的领跑者，使得区块链存储可以突破桎梏发展到全新格局，并为其它区块链存储系统的发展提供关键作用。

在共识层面上，Filenet 在 POC 存储挖矿的前提下，采用了 DPOS+POC 机制作为分发的共识机制，完美避开了设备效率与资源配置的直接矛盾，极大改善了区块链 3.0 时代的挖矿模式。DPOS 算法具体运作过程是由利益相关者（stakeholders）也即由 Token 的持有者、矿工进行投票，通过选举程序选出 Filenet 超级节点（Filenet Super Nodes），然后区块的超级节点们会被确定性随机打（pseudorandomly），在规定的时间内 Filenet 超级节点可以选择是否出块。

在经济模型上，Filenet 采用贡献资源挖矿的模式，以及由资产背书的 资源通证与总数固定的流通币构成的双层通证模式。通过巧妙的设计保证商业用 户购买存储空间价格稳定在低价，但流通币价值会长期不断推高；

在治理结构上，Filenet 第一次提出了一个完备的去中心化治理结构， 解决彻底去中心化时“谁定规则”、“规则如何执行”、“出现任何一个人作恶 或不作为时由谁来管理”等问题。

Filenet 独有的激励模式使得存储资源拥有者将其硬盘空间贡献给 Filenet 后，反而可以获得更多的存储空间，并得到额外的数字货币奖励， 而且该模式无需任何补贴，是长期可无限持续的；

在商业模型上，Filenet 具有强大的与企业用户对接的专业能力，包括 技术上与中心化存储的应用无缝对接的专业能力、深刻了解市场需求和用户痛点 的专业能力、与商业用户销售模式打通的专业能力和调动企业存储行业资源切入 市场的专业能力，能够形成商业闭环，可直接无缝迁移现有中心化存储市场，兑 现区块链存储的强大优势；

FN 商业模式成熟，落地场景巨大。在流量分发领域，我们创新性的使用了多节点共享带宽的模型，可以为字节跳动、腾讯微视、SNAPCHAT 等有高频流量分发需求的内容平台提供一站式解决方案。在大规模云存储领域商业落地场景巨大，在冷数据存储领域，而 FN 能将云存储的平均成本降低至阿里云存储成本的 20%。

在生态发展上，Filenet 一方面可直接迁移现有数百万种 IT 应用，另一 方面提供开放平台将自有核心能力开放出来，并且让开放平台上的区块链存储系 统可以共享去重红利，第三方区块链存储系统加入 Filenet 生态即可获得关 键技术能力，还能马上实现收入倍增。

1.2Filenet 技术背景

1.2.1 共识机制

区块链的核心技术是共识机制。

目前比较常用的共识机制有 PoW（Proof-Of-Work，工作量证明）、PoS（Proof-Of-Stake，权益证明）、DPoS（Delegated-Proof-of-Stake，委托权益证明）、PoC（Proof-of-Contribution，贡献证明）。

PoW 机制，需要矿工解决复杂的密码数学难题，依赖计算能力，优点是系统安全可靠，缺点是消耗能源和计算能力、有 51%算力攻击可能、吞吐量小。

PoS 机制，根据权益选举矿工打包数据，优点是不消耗资源，缺点是安全性较低，股权越多的人话语权越高。

DPoS 机制，多数有投票权的人将投票权委托给少数节点来代理，优点是系统效率高，吞吐量和并发数高，缺点是话语权掌握在少数节点手上，不安全。

PoC 机制，根据节点所作的贡献来分配打包权，优点是不浪费资源、按劳分配，缺点是贡献计算方法要根据具体的场景来定。区块链 3.0 时代，共识机制朝着不浪费资源、适当考虑安全性、提高吞吐量和并发数方向发展。

1.2.2 有向无环图

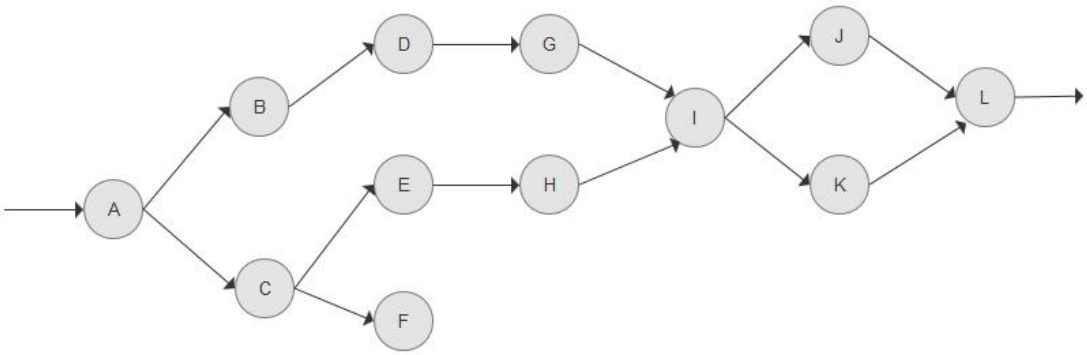


图 1 有向无环图

比特币的区块链结构是一个单向链表，这种结构是区块链早期采用的，存在很多问题，如区块存储容量小、交易速度慢、数据总量大、单节点存储压力大、每秒交易数少。

DAG（Directed Acirclic Graph，有向无环图）是一种新型的区块链数据结构。DAG 和链表结构都能由上一个节点来确定下一个节点，所不同的是，链表结构只能是一对一，而 DAG 支持一对多、多对一，只要不产生回环就行，也就是通过前面节点来验证后面节点二者是否一致，但链表结构同一时间只能有一个分支，而 DAG 结构可以有多个分支，所以 DAG 结构并发数更高，同时存储的数据更多。

同时，DAG 记账是一个异步的过程，数据是弱同步，可以接受一定程度的数据差异，在后续异步确认过程中再来修正。这样可以大大节省确认时间，提高交易速度。

1.2.3 默克尔树

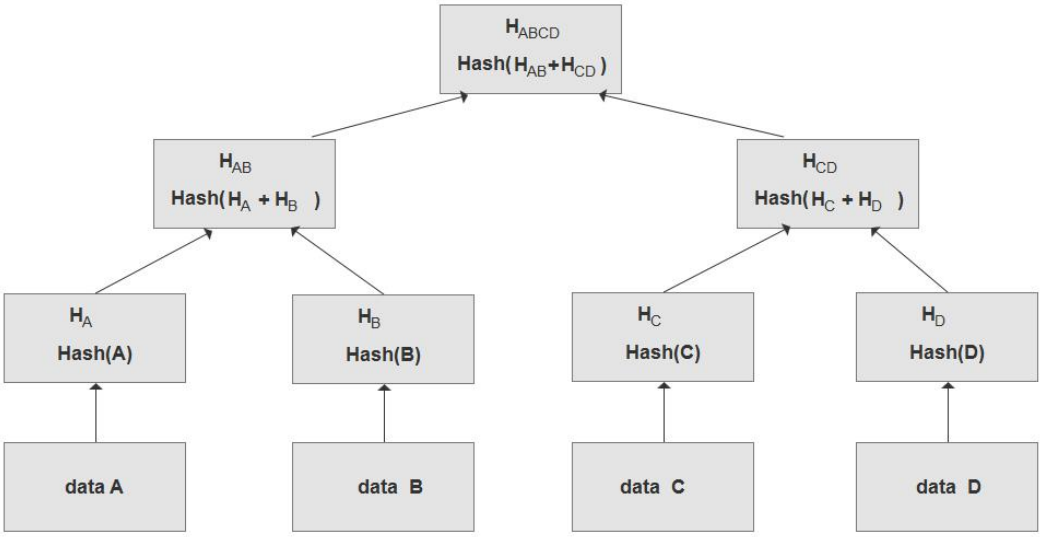


图 2 默克尔树

默克尔树是快速验证数据的一种方式，在比特币中有采用，在点对点数据传输等领域也广泛采用。默克尔树将数据分成很多小块，每一块计算出一个 hash 值，多个数据块合并生成一个 hash 值（一般是两个），并最终生成汇集到一个根节点，生成一棵树（一般是二叉树）。

由于数据分块，并且提供了 hash 值索引，在数据很大，或者是点对点系统中，无需得到所有数据，再验证数据是否正确。哪怕只得到了一小块数据，只需要在这棵树上找到数据所在的位置，确定树上关键位置上的数据和 hash 值，就能验证数据是否正确。

1.2.4 星际文件系统

IPFS（Interplanetary File System，星际文件系统）是一种点对点的分布式文件系统，旨在连接所有相同的文件系统的计算机设备。在某些方面，IPFS 类似于 web，但 web 是中心化的，而 IPFS 是一个单一的 Bittorrent 集群，用 Git 仓库分布式存储。换句话说，IPFS 提供了高吞吐量的内存寻址块存储模型——具有内容寻址的超链接。

这形成了一个广义的 Merkle DAG 结构，可以用这个结构构建版本文件系统、区块链甚至是永久性网站。IPFS 结合了分布式哈希表、带有激励机制的块交换和自我认证命名空间，IPFS 没有单故障点，节点之间不需要相互信任。

未来，IPFS 将会在 WEB、文件系统、区块链三个领域发挥巨大的作用。

首先，在互联网中用 IPFS 取代传统的 HTTP 协议，IPFS 的优势在于节省存储与带宽资源，大幅度节省成本，同时还提高传输效率。分布式 web 站点的设计让 IPFS 更安全，更稳定，更开放。

其次，IPFS 将构建一个面向全球的分布式文件系统，它将全人类公开的文件全部组织起来，并且通过版本管理，使文件各个历史版本得以保留，形成一个非常全面的文件宝库。

IPFS 将与区块链技术紧密结合，将区块链带入一个全新的时代。IPFS 的底层数据结构完美兼容区块链数据结构，目前常见的区块链数据都能表示成统一的 IPFS 底层数据结构，各种异构的区块链都可以选择 IPFS 作为存储媒介，从而解决目前区块链技术面临的最大难题：数据存储问题。在此基础上，各种性能更好，更方便的区块链产品应运而生。

1.3 “应用共识”

Filenet 提出了一种全新概念——“应用共识”。“应用共识”定义了 Filenet 通证在现实世界的公允价值及其价值体现。

这种概念的提出源于一个关于 IPFS 实际使用场景的问题：如何在用户免费浏览网页的同时，给予矿工有价值的激励？

区块链发展到今天，不止有一种通证流转的逻辑被提出。一种主流的情况是，一些基于某种特定业务的去中心化项目，其内生的业务场景将支撑通证的流转，其中部分项目还将业务的盈利与通证价值锚定。

在 IPFS 的系统中，主要的业务场景将是如何存储和下载数据。如果在这些行为中加入代币的流转生态，或许将意味着，用户即便浏览网页，也需向矿工支付代币——事实上，已经有激励层进行了这样的尝试。

数年的互联网历史可以验证，这种商业模式几乎是不可持续的。经过数年的激烈竞争，中心化的大型互联网企业为人类提供了海量的免费服务，并通过流量、数据等其他衍生业务进行盈利。这些企业在众多互联网企业中脱颖而出，代表了市场需求。

一个新的技术变革理应以人类的需求为出发点，所以从现实角度出发，可以想象如果使用 IPFS 的系统需要高频且高额的付费，那么受众将会显著减少。我们期待去中心化的变革不止在于“反垄断”、“自由”、“安全性”的考量，也理应从商业角度出发来契合大众使用习惯。

由此，Filenet 从 BTC 的价值中得到启发，并提出了“应用共识”的概念。

BTC 的核心价值在于其“共识价值”，这是在其市值上区别于其他 POW 区块链加密系统的核心原因。

“应用共识”的内核是，基于应用的影响力对其释放的加密通证进行价值背书。拥有以下四点特质的项目将具备建设“应用共识”的潜质：

具备颠覆性创新；

潜在的影响力覆盖面广泛；

对一个独立个体的潜在影响深远；

加密通证的释放对其系统维护有着不可磨灭的作用。

IPFS 在性能、安全性及“去中心化”内核的特质上，较之 HTTP 有显著的优势。然而如前述，用户如果承担高频高额的费用将会对其生态造成毁灭性的打击——免费地使用系统反而会更高效地扩大其影响面积，进而形成应用共识。

Filenet 认为，Filenet 通证的价值主要体现在对 Filenet 的应用以及维护 Filenet 系统运转矿工对人类潜在贡献的认同性，并通过对通证价值的认同以形成保障 Filenet 系统持续运转的主观支持。

诚然，在缺乏通证交易场景的 IPFS 体系里，存储数据和下载数据的有效性需要更有力保证，以避免恶意挖矿。Filenet 将通过矿工分配的随机性规避对某特定矿工的恶意挖矿行为，并通过数据晋升制度规避无价值数据的恶意上传，浪费网络资源，此部分将在后续的共识机制中详述。

Filenet 作为一种基于去中心化项目发行的、自由流通的通证，基于“应用共识”，其可能衍生的交易场景涵盖人类社会绝大多数支付行为。

比如，在文件传输领域，Filenet 也将提供支持，如用于支付指定文件的版权费用等场景。

2.1 架构

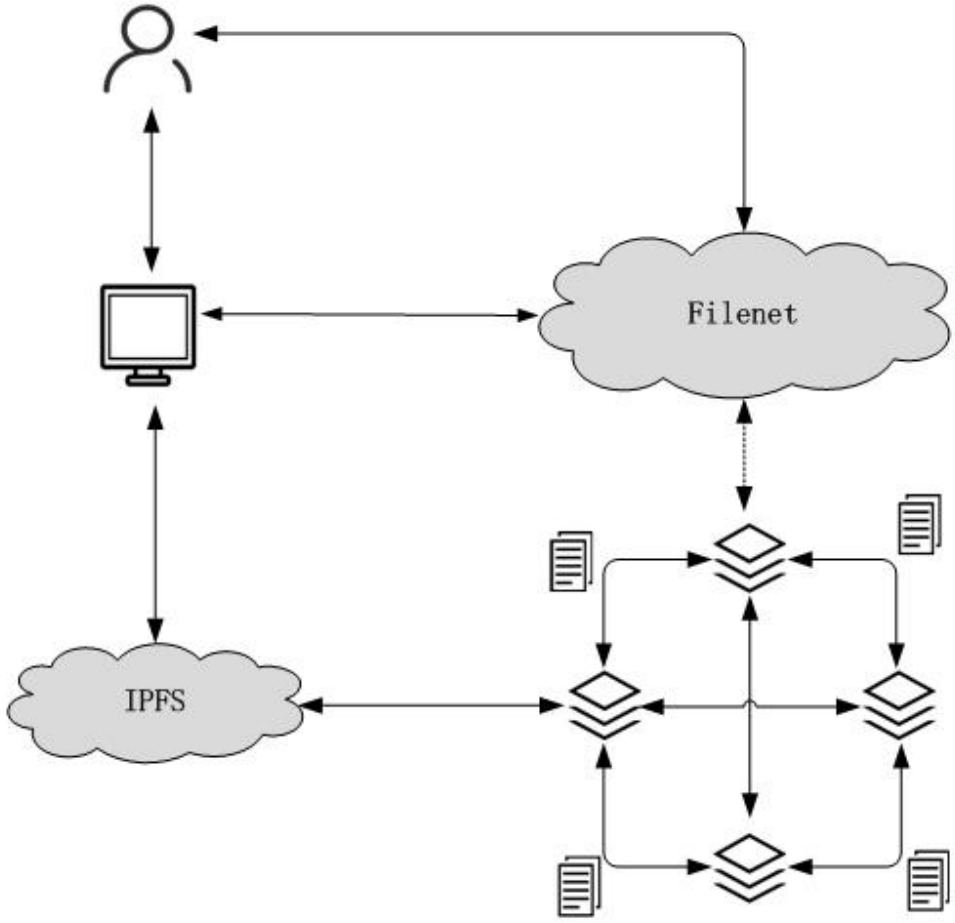


图 3 Filenet 架构图

分布式数据存储、P2P 网络传输、分布式计算等底层功能由 IPFS 协议和 Mine 物理设备一起完成。

在 IPFS 中，包含两种类型的节点：普通节点和专属节点，各节点通过 P2P 网络互联互通。专属节点一般是用户的私有节点，上传数据时，数据首先被存储于专属节

点，待数据被多次检索至一定阈值，专属节点上的数据才能进入 IPFS 网络中的任意节点，即数据晋级制度。

在 Filenet 的设计中，数据流入节点没有代币奖励，数据流出节点才有代币奖励。数据流出节点的目标既可以是 DApp，也可以是 IPFS 中其它节点。

Filenet 作为激励层，需要完成区块管理、共识机制、智能合约。DApp 运行在 Filenet 之上，用户可以直接通过 Filenet 和 DApp 上传数据。

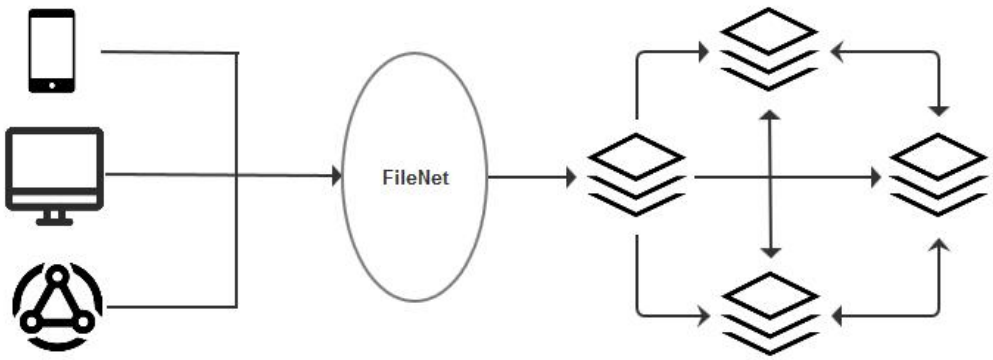


图 4 Filenet 存储管理示意

Filenet 去中心化存储网络(Decentralized File Network)(DFN)，提供数据晋级制度。当用户通过一个设备上传数据，此数据存储在本地，当数据被检索次数越来越多，就会逐步进入公开网络，成为热门数据，此时该数据才可以参与挖矿。

2.2 数据结构

Filenet 区块保存所有数据痕迹参数，上传至 Filenet 数据种类多、数量大。传统的链表结构会使区块冗余，表达繁琐复杂，而 Filenet 采用的是 Merkle 树和 DAG（有向无环图）结构的区块链数据结构。DAG 结构比传统区块链链式结构更灵活，性能更高，速度更快，极大地提高了区块打包的效率，从而提高了 Filenet 网络的性能。Merkle 树不需要完整的区块信息，只需要关键的 Merkle 节点信息，就能对区块链数

据进行验证，从而让节点变得更轻巧，将更多精力与资源用于业务处理和为 Filenet 网络提供服务。同时 Merkle 树也能简化验证流程，进一步提高网络性能。

具体的区块结构我们会在技术黄皮书中详细说明。

2.2.1 账本

用户的数据、矿工状态表和信任表，我们称之为账本，用户在任何时间内都可以访问，账本是一个按照时间推进不断增加的数据链。

2.2.2 表格

a 数据的检索量表格

检索量表格是比较复杂的数据关系，涉及的数据类型、数据被访问的时间、数据访问量是不断的变化的。然而，通过 DAG 结构来保存这张表格，变化的参数不会前后相互受影响。

b 矿工运行状态表格

对于数据存储与检索，矿工运行状态、空间闲置量、网络环境会存储在当前的区块中，这种表格是公开可查的。

2.3 角色

2.3.1 使用者

使用者即使用客户端上传文件的用户。用户可以通过 Filenet 客户端（DApp）直接参与数据存储和检索。用户的存储和检索操作均为免费。

2.3.2 服务者

服务者即矿工。矿工提供存储资源、存储数据、为用户提供数据检索分发，通过被检索使用获取收益。

矿工存储了用户的数据，根据特定的时间生成分发证明并提交到区块链网络来证明在这段时间内数据分发量及活跃度。根据分发量在全网占比获得 Filenet 奖励，如果不能提供证明或者证明无效，则不能获得奖励。

矿工存储了用户数据间断性向区块链网络上报自己的运行状态，当用户检索数据时，Filenet 会依照网络状态和设备状态去检索数据，如果矿工不能在规定的时间内上报当前状态或者状态有虚假，将可能会影响矿工的收益。

要获取数据资源，矿工需要不间断提供自己的空间、带宽、运行状态，这些参数共同保存在一个表格里，我们称之矿工的信任表。Filenet 会依照信任情况来分配数据，如果数据容量小但是使用频次很高，我们会将它保存在网络环境稳定的矿工设备中；如果数据容量大但是使用频次低，我们会将它保存在空间很大的设备中；如果矿工设备出现故障或者环境不稳定，Filenet 将会减少数据派发量。

2.4 协议

我们把用户和矿工抽象成两种实例，实例均有属性和状态。用户和矿工遵守共同的 Filenet 协议规则。

2.5 挖矿(mining)

Filenet 为高频数据提供更好的存储和分发，同时也不会让低频数据占用系统的存储资源。所有的用户都是通过 DApp 将自己原文件发布，这些文件随着逐渐被用户检索，流传到 Filenet 网络中而分配到矿机中。这些 DApp 可能是一个云盘、社交软件、新闻客户端等。文件被上传的同时，其 hash 值将被记录到 Filenet 网络。

2.5.1 概述

用户存储的数据可以分为低频数据和高频数据。Filenet 挖矿的一种方式是共享高频数据来获得，通过 Filenet 的激励机制，让这些高频数据在其生命周期内得到极大限度的传播，进而获得增益的财富，同时也因其共享，让数据成为人们共有的财富资源。

2.5.2 资格获取与保证金

服务者钱包里必须持有一个以上 Filenet 代币，才能作为实际账户，获得挖矿资格。

Filenet 采用一种“保证金”模式，鼓励服务者认真维护自己的节点，保障节点稳定可靠地工作。这可以被视为一种保证金模式，但是，节点将不会因为故障或环境不稳定被扣罚保证金。

2.5.3 收益

IPFS 出矿的概率与数据活跃度成正比。上传的数据必须要有其他用户下载使用才能确定其为有共有数据，下载的用户越多、活跃度越高，即可获得相对应更多挖矿奖励。

2.5.4 硬件

Filenet 志在连接一切闲置存储空间，理论上凡是可以连接上网的存储空间都可以参与到挖矿之中，包括但不限于云服务、数据服务中心、电脑、笔记本、手机，甚至车载电脑、智能手环等各类终端。

3. 共识机制

3.1 基于 DPOS 机制的检索分发证明

Filenet 在 POC 存储挖矿的前提下，采用了 DPOS 机制作为分发的共识机制，完美避开了设备效率与资源配置的直接矛盾，极大改善了区块链 3.0 时代的挖矿模式。

DPOS 算法具体运作过程是由利益相关者（stakeholders）也即由 Token 的持有者、矿工进行投票，通过选举程序选出 Filenet 超级节点（Filenet Super Nood），然后区块的超级节点们会被确定性随机打散（pseudo-randomly），在规定的时间内 Filenet 超级节点可以选择是否出块。

Filenet 依据 DPOS 最长链原则（longest-chain rule），也就是说在相同时间内，拥有最多矿工拥护的那条链会比其他链生长得更快，也就是说如果存在两条链，则生长速度快的这条链，最后一定会成长为最长链。

传统的 DPOS 算法和 POW 一样都是依循最长链原则，在这种原则下，只要在一个时刻任何人生产出了一个合理的最长链，那么剩余的所有节点都会切换到这条链上。

就 DPOS 相对于 POC 的优点，好处就是其达成共识的效率被大大提升了，同时所能提供的不可逆保证也是相似的。因为不再是由全网达成共识，而是由被选举出来的生产者之间达成共识，所以效率得到了极大地提升，这对于应用而言是比较重要的，因为对于类似高频的场景和小额的情况，用户难以忍受长时间的等待。

Filenet 去中心化的同时，速度、效率和节点数量是没法同时得到的。Filenet 选择了 DPOS，倾向于选择了速度和效率。

分发证明 Podt(Proof-of-distribution)是一种新型的证明方式。这是一种适当减少了实现难度的方案，无须构建复杂机制防止攻击难题，只需证明数据分发的频次和使用度，即可与挖矿系统结合，形成完整方案。

在 Filenet 中有两种证明，状态证明(Proof-of-state)及检索量证明(Proof-of-retrieval)，用以反映矿工的即时状态及其已创造的价值。

Proof-of-retrieval，简称 Pore，是一个汇总矿工数据分发频率的协议，它将间接反映 CDN 的消耗并在每个周期内定时更新。这种方法是单向的，无法相互检查矿工的真实情况。这些协议依赖零知识证明机制（Zero-Knowledge Proof），证明者（被验证者）能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的。

3.1.1 Pore 协议

用户将数据发到 Filenet 网络，Filenet 将跟踪、考核并将数据发送给矿工。以下是 Filenet 对检索进行验证的过程：

1.Send：
输入：
Prover Key pair（M，D）
证明者的钥匙对数据参数产生的公钥
Prover send key Pksend
Parameter P，矿工的数据参数
Date D，矿工提供的数据
Relation P&D→N

输出
Replice R 数据的参数 P 的一个副本。

DAG Root rt of R 对副本产生有向无环的 hash 根
Proof πseed 副本分发证明
过程：
1.计算数据的 hash 值 HN:=CH(N);
2.封装 R：=seal（N,skM）；
3.计算 R 的 hash 根 rt：=DAG CH(N);
4.》X：=（pk HN，rt）；
5.》W：=（skP，N）；
6.计算 R 的分发证明πsend：=SCIP.prove（pkseed，X，W）；
7.输出结果 R rt πseed

Prove
输入：
Prove proof-of-distribute key pkPodt 数据的分发公钥。
Replica R
Random challenge C 检查随机数，代表 hash 子节点。
输出：
πPodt 分发证明

3.2 信用度度量

Filenet 网络选举矿工执行数据检索、数据分发、区块打包的任务时，依据的是各矿工的信用度值。

为保证各信用度等级的矿工都有机会被选中，同时发挥信用度的作用，我们采取了如下策略：信用度分等级，首先按照信用度等级进行初次选举，信用度等级越高，被选中的概率越高；初次选举后，即对同一级信用度的矿机实行等概率选举。矿工的信用度值计算公式：

$$T=(1 - e^{-cm}) * 100\%$$

T：信用度值

m：持币量

c：调节因子

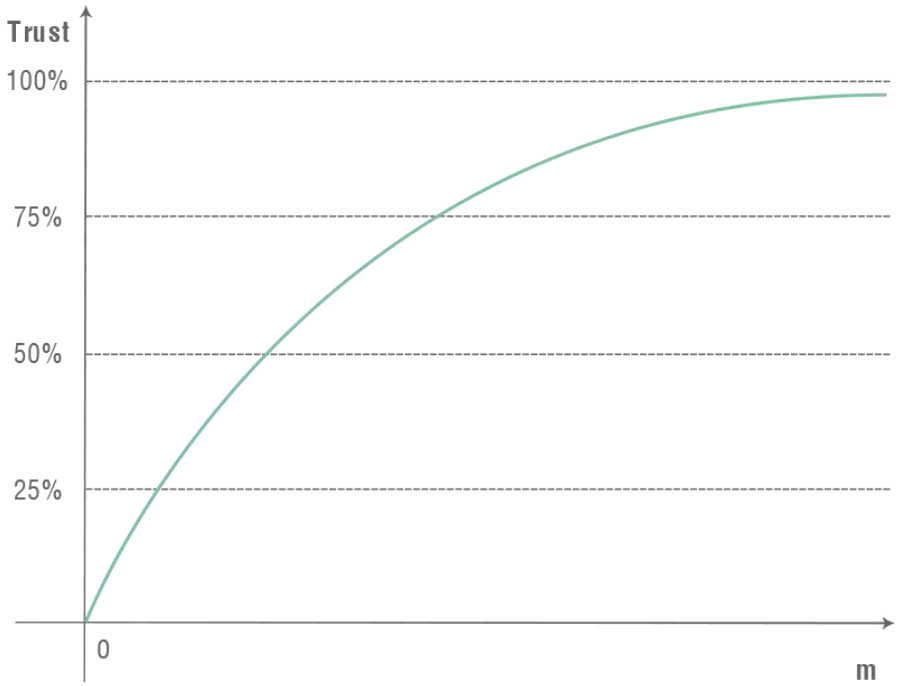


图 5 信用度曲线

Filenet 的去中心化存储网络可以建立在诸多共识协议上，只要符合分发证明的验证即可。

3.3 通过 Podt 方式计算矿工的算力

因为在每个周期都会产生一个区块，矿工 Yn 都会被要求生产一个分发证明到网络，只有网络中的大多数验证通过，分发证明才会被添加到区块链中，随之 Filenet 全节点将更新矿工的空间信息，并将失效的记录删除，因此矿工的 Yn 的算力可以通过累加并检验矿工的分配情况确定。

对于大型节点，Yn 的算力可通过累计从创世区块到当前区块的关于 Yn 的所有分发记录得出。

同时，小型节点可以从可信的大节点处获取信息。矿工 Yn 的分发记录，将从最新的区块头部到创始块，在哈希树中进行排序——Merkle 路径将保证其真实性和完整性。通过这个方式，小节点可以把验证 Podt 证据的工作委托给网络。

如果矿工要恶意伪造自己的算力，就需要伪造自己的分发证明，这将执行 send 操作，并在操作中伪造虚假证明到区块链上。由于 send 有校验过程，如果能成功 send 操作，那么 Filenet 就认为是真实的证明。因此 Filenet 完全是依靠 Podt 协议维护真实性，而在分发证明章节已经证明了 Podt 是安全的。

Filenet 通过算力达成共识。算力将采用 PoC+PoS 的模式，并把信任度、保证金额度和时长视作一种权益（Stake）。Filenet 将在每一个周期内通过概率选举出多名矿机共同出块，同时被选举的矿工会增值信任分。

POC+POS 是一种随机选举，无法预测，选举出矿工作用就是在一个区块周期创建区块并广播到全网，数据块以 DAG 的数据结构管理，因此区块越多主链越安全。

3.4 共识机制算法

T：某一出块周期的结算时刻。

Random（t）：随机数

P_J^t：在出块周期内矿工的算力。

L：H（Yn）是一个 hash 函数 L 是其中长度。

<Yn>msn:矿机 Yn 对消息 msn 的签名。

<Yn>msn=（（Yn）SIGmsn（H（Yn））） ————————————--1

Mine：Yn
Compute
H（<t||random（t）>Yn）*$2^L \leqq Pt/\sum_j P_J^t$ ————————————--2

π=<t.r>i

verifier Node： Verfy(π，t，Yn) ————————————--3

1.π is valid signature。
2 P_j^t： is Power of Yn at time t
3. check H（π）/2^L= $Pt/\sum_j P_J^t$

矿工通过上面的不等式来确认自己当前自己是否被选为出块者，其中公式 1 表达当前出块的时间生成一个随机数。根据时间生成一个随机数 hash，Yn 对 hash 值签名，然后再做一次 hash2 将 hash2 除以 2 的 L 次方，得到一个 0~1 之间的数字。

表达式 2 是本矿机在全网的算力比例，由此体现此共识机制的公平性。

每个参与者在一个出块周期内只有一次选举机会，所有选举都为随机选举。Random（t）是无法预测的。计算无法并行且不能被恶意操控。

由于需要私钥验证，恶意矿工将无法伪造其他矿工签名。

同时，挖矿过程是可公开验证的。如果矿机计算出自己为胜出者，那么他需要向全网提交验证证据，而任何时候矿机的算力和他产生的随机数 hash 值都可以被验证。

4. 智能合约

Filenet 是面向开发者的一条公链，它为 DApp 提供了特殊的编程原语与存储的数据交互。这些原语包含在 EVM（以太坊智能合约虚拟机）内。由此，在智能合约中也可以访问有关数据位置，存储节点和矿工的信息。

全球首款基于 Filenet 网络开发的分布式存储 DApp“纸条”目前已经面市，该应用内所有聊天数据将以碎片化形式存储于全球任意节点、凭私钥调取，且应用内生态均以 **Fn** 为支付代币进行流通、结算。

在该 DApp 内，所有用户数据（包括实时传输与存储）都将以高度隐私的安全级别得以留存。由于 IPFS 网络的特殊性，即使单个/小面积服务器遭遇不测，损失数据将完全能够通过私钥重新恢复并再次得以存储，不存在任何风险。

纸条 DApp 将颠覆当前互联网中心化社交 App 中的隐私及数据存储安全等问题。

Filenet 的智能合约主要应用于矿工的持币。我们所开发的智能合约可能会通过 EVM（以太坊智能合约虚拟机）及 Solidity 来快速实现。

Filenet 本身具有实现智能合约机制的潜力，我们相信未来版本的 EVM 和 WASM 将会与 Filenet 的功能天然整合，并允许其他的主链在 Filenet 上受益。

4.1 生态应用开发

目前大部分区块链项目都是基于 Ethereum 开发，在面对大数据并发和大存储的应用时束手无策，比如当需要开发去中心化的视频、游戏、直播平台，以及更广阔的物联网应用时。而基于 Filenet 的技术特点，能提供有效的解决方案。

我们开发这条公链是希望开发者能轻松开发自己的超级应用，践行自己改变世界的梦想，公链将持续优化开发语言，并提供 DApp 运行必要的存储空间和网络。

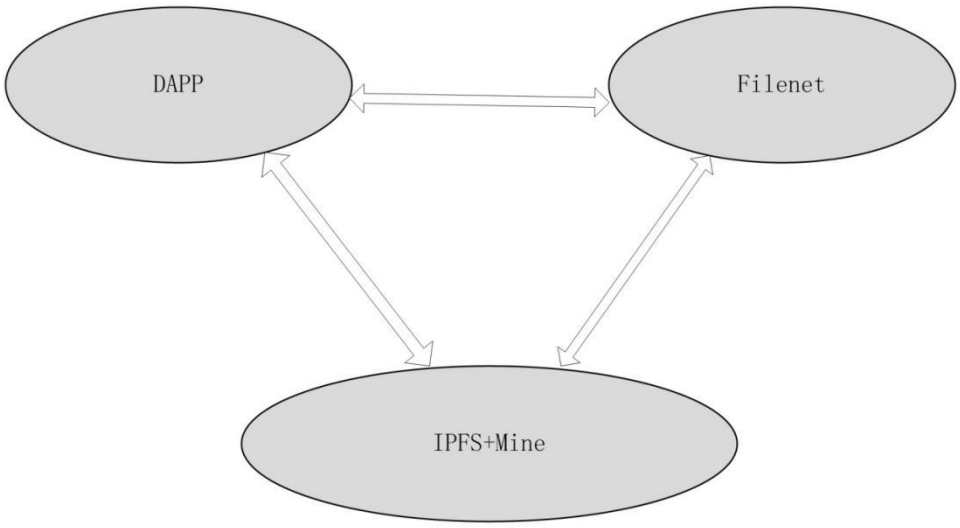


图 6 生态应用开发

4.2 通证分配

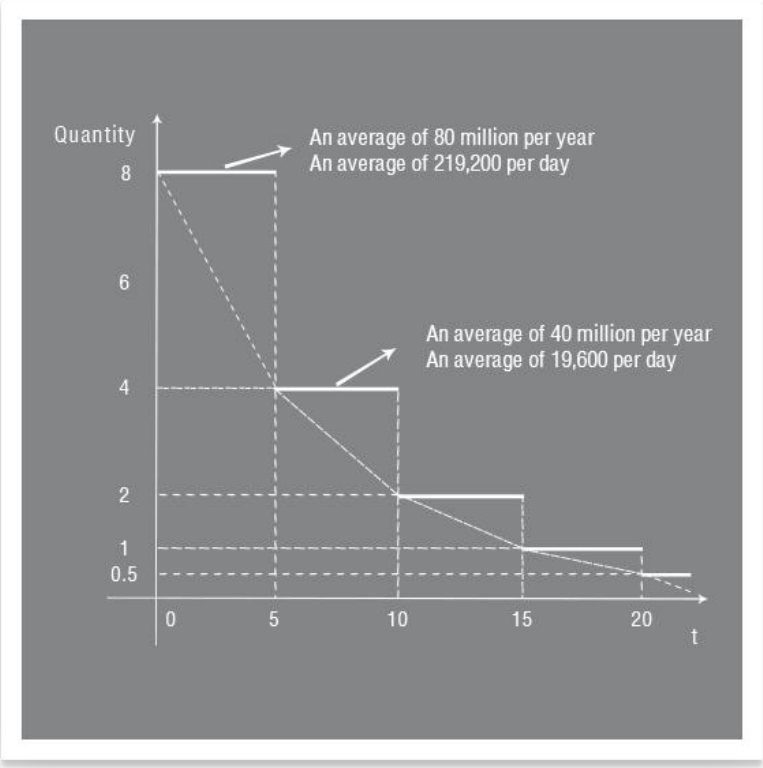
，其中：

回报

技术社区代码贡献者　　内

7　用于投资 Filenet 生态 DApp。

3%用于奖励早期社区成员



4.3 技术伙伴

4.4 战略伙伴

5. 后续关注

本文档为 Filenet 白皮书（第二版），主要阐述当下的思考及技术规划，技术 Filenet 黄皮书会在后续工作中公布。

开发小组的技术实现方案，会采用社区化的开发方式，后续的技术问题我们将在 Filenet.io 或者社区公开征集。Filenet.io 项目采用社区自治方式，任何开发者都可以参与，只要愿意加入并付出自己的时间。

感谢 IPFS 社区开发者朋友提供的众多技术指导意见。目前，Filenet 所有的信息和公告只有一个通知窗口 Filenet.io，请广大社区支持者关注 Filenet.io 网站。

6. 法律结构和风险提示

6.1 法律结构

技术开发团队法律主体为 FILENET FOUNDATION LIMITED.

Filenet 将**不会**通过销售通证进行任何公开或私下募集等行为。Filenet 作为一种具有实际用途的虚拟商品使用，不是证券，也不是投机性的投资工具。

Filenet 基金会持有的代币，将由基金会主要用于技术开发、社区建设、市场推广、运营、财务审计等用途。

Filenet 依然有可能受到来自不同国家主管机构的质询或监管。为了满足和遵守当地法律法规，Filenet 可能只在某些区域或某些时段提供正常服务。

6.2 风险提示

6.2.1 监管风险

区块链技术以及相关运营活动，尚处于早期阶段，国际和中国国内尚没有明确的法律规章对设置、信息披露、交易等进行明确的合规规定。并且，国家相关部门仍处于观望阶段，没有最终的明确结论。国际环境的变化，以及国家政策的调整，都可能对 Filenet 的价值和流动性产生影响。

6.2.2 竞争风险

区块链领域已经成为热门的创业方向，被部分媒体及个人报道或认为系第二次互联网革命。众多优秀人才和雄厚资金的涌入，不仅给这个领域带来巨大的发展机会，也将带来巨大的竞争。Filenet 所汇集的精英人才，对此虽有充分认知和应对决心，但我们难以确保团队、生态社区、项目一定会取得理想的效果。这种难以预测的风险，需要投资者审慎考量。

6.2.3 人才流失风险

Filenet 项目已经准备吸引更多人力资源资深、技术资深以及市场资深人才加入。他们也都有信心和承诺，为此付出心血和劳动。但在未来发展中，难以避免有核心管理或技术人员选择离开，我们尊重团队成员的个人选择，也需要强调这或许会对项目发展带来不良影响。

6.2.4 黑客攻击风险

Filenet 在发展和运营过程中，将可能遭受到来自于黑客、竞争对手等恶意攻击。他们攻击的手段、方式和时间点都难以预测，有可能给投资者带来损失。

6.2.5 未保险损失风险

链上的账户，不同于以往投资者所熟知的银行或者金融机构账户，存在于 Filenet 上的账户没有保险保障。在可能出现的任何风险情况下，没有任何机构或个人会对投资者的损失进行保险或担保。

6.2.6 未知的风险

除了白皮书提及的风险，还会存在一些创始团队尚未预料或者提及的其他风险。这些风险可能突发爆发，以及已提及的风险组合式爆发。望广大参与者，能够充分了解项目情况，以便做出理智的投资决策。

6.3 免责声明

本文档仅作为信息传递用途。文档内容仅作为参考，不构成对 Filenet 项目相关公司交易股票、证券的任何建议、教唆或邀约。本文档不组成也不理解为提供任何买卖行为，也不是任何形式的合约或承诺。

鉴于不可预知的情况，本白皮书所列的目标可能发生变化，尽管项目团队会尽力实现项目目标，但投资者在二级市场购买 Filenet 须自行承担风险。本白皮书部分文档可能随着市场环境和技术发展进行调整，若发生上述情形，管理团队将通过新版白皮书予以公示。

Filenet 明确表示不承担参与者造成的直接或间接损失包括：

1.依赖文档的内容；

2.本文信息错误、疏忽或是不准确信息；

3.由本文导致的任何行为。

项目团队将努力实现白皮书所列的项目目标，但基于不可抗力的存在，团队无法也不能做出完全实现的承诺。

通证 Filenet（Fn）是实现项目效能的激励工具，并非法定物品或投资品。Filenet 不是一种所有权或控制权。控制 Filenet 不代表对生态、系统或数据的控制。Filenet 并不授予任何个人或团队拥有对生态、社区、系统等控制和影响决策的权力。

参考文献

[1]Filecoin: A Decentralized Storage Network, Protocol Labs

[2]IPFS - Content Addressed, Versioned, P2P File System, Juan Benet

[3]Disrete Mathematics and Applications Seveth Edition,Chinese Abridgement

[4]Computer Networking A Top-Down Approach Sixth Edition, James F.Kurose Keith W.Ross

[5] Peter J. Braam. The Coda Distributed File System, School of Computer Science，Carnegie Mellon University, HTTP://www.coda.cs.cmu.edu

[6] Lustre File System White Paper HTTP://www.sun.com/software/products/lustre/index.xml

[7] The Google File System, SOSP'03, Sanjay Ghemawat,Howard Gobioff, Shun-Tak Leung

[8] Network File System, HTTP://www.faqs.org/rfcs/rfcl094.html