FileStar Project Litepaper

A Web3.0 Decentralized Storage，Verifiable Computation，Mensurable Bandwidth Physical Infrastructure

文曲星项目 白皮书初稿

搭建 Web3.0 的分布式存储、可验证计算、可度量带宽 物理世界基础设施

By dev@filestar.net

2020.10.20

摘要

我们认为区块链世界遇到了巨大的发展瓶颈，只能依赖巨大的技术创新来推动区块链行业摆脱目前的困境。2009 年中本聪发布了比特币的白皮书，开启了一个基于互联网的免信任的电子现金的时代，受制于比特币网络的处理能力，比特币已经从最初的电子现金的愿景偏离，并被历史的车轮推到了电子黄金的地位。以太坊在比特币的思想上，赋予了转账 交易更多的灵活性和可编程性，引入了智能合约虚拟机的概念，通过提供不同于脚本语言的更强大的处理能力，以太坊取得了蓬勃的发展，但是依然面临巨大的发展制约。

不论是比特币还是以太坊，本质上都是在一个点对点的网络中，取得计算和数据的一致性，因为链上资源的极度稀缺，比特币网络只能处理比特币本身的交易，以太坊网络也只能处理以太坊本身和各种以太坊 token 符号的交易和有限的逻辑。某种意义上，你可以把现有的区块链网络当做一个极度封闭的网络。不论是比特币还是以太坊，其所依赖的全节点物理硬件设备有巨大的局限性，也必然制约了以太坊网络的处理能力。如果你把以太坊当做一个微型的 cloud, 那么这是一个全局一致性但是处理能力非常有局限性的云服务。

Filecoin 是第一次打破了区块链世界和物理世界的隔阂，通过时空证明，链接了大量的高端服务器和硬件资源，也打破了区块链世界的内循环。FileStar 文曲星 将在 Filecoin 的基础上，更进一步，不同于 Filecoin 只激励大家构建分布式存储的基础设施，FileStar 文曲星 将致力于同时构建分布式存储，可验证计算 和可度量带宽的基础设施，致力于未来服务于所有区块链的项目，例如未来大量以太坊的 Rollup 的证明工作可以在 FileStar 网络上进行验证。FileStar 项目将在 Filecoin 的基础上进一步迭代，通过不断的技术创新，构建 Web3.0 的物理基础设施。

我们认为区块链本身只是提供了一套分布式的清结算协议，如果上面只能清结算由社区弱信用所发行的各种 Token，那么区块链的价值会大打折扣。FileStar 项目将致力于链接链下的物理世界，不同于预言机只能链接简单的价格信息，并提供到链上，FileStar 文曲星 将致力于链接互联网上真实的 计算、存储、带宽资源，并形成统一的资源 度量衡和资源表示方法，将这些资源迁移到区块链世界，来构建未来分布式互联网的物理基础设施。

项目背景

2020 年 10 月 15 日，Filecoin 主网在 148888 高度激活，宣告了行业内最受瞩目的去中心化存储网络的正式上线。Filecoin 提出了一套存储证明机制，通过复制证明（PoRep）、时空证明（PoST）等一系列技术创新，首次实现了现实世界链下存储资源的度量和链上表示。在这一技术基础上，Filecoin 通过一套经济激励机制吸引了大批拥有高端服务器的矿工加入网络，在一定程度上整合了大量高性能的计算、存储和带宽资源。Filecoin 协议背后蕴藏的核心理念为未来区块链+互联网基础设施的发展方向提供了重要参考，是行业内具有里程碑意义的创新。

然而，在 Filecoin 协议创新的背后， Filecoin 项目在实现上仍留有一定遗憾，有可能会阻碍这个新型去中心化存储网络的进一步发展：

- 不同于 Filecoin “去中心化”存储的理念，Filecoin 项目的开发和管理模式偏向“中心化”，开发团队在主网上线前仍在对共识机制、关键特性和经济模型进行修改，在一定程度上影响了网络的稳定性；
- FIL 代币的分配和释放规对矿工较不友好，在主网上线之初，矿工只能高价从市场上买入 FIL 代币才能继续维持挖矿的开销，因此才会有目前主网一上线矿工就大规模“停摆”的现象，这显然不利于对基础设施提供者（即矿工）的长期激励；除矿工外，生态中其他的参与者未获得足够激励，参与维护网络发展的意愿不强；

- 参与 Filecoin 挖矿的门槛较高，需要拥有大量的前置抵押代币，并购买带有 AMD 高端处理器的矿机，这些都阻碍了更多小矿工和大批 Intel 矿机的加入；
- Filecoin 网络本身的架构和技术选型导致实际的链上处理能力（TPS）比较有限，在网络拥堵时甚至无法处理有效存储的证明上链，也无法进行正常转账，这在很大程度上限制了 Filecoin 网络规模的进一步扩大；
- Filecoin 网络中存储的数据的可用性比较有限，只能存储一些使用频率极低的“冷数据”，而对于需要随时存取的“热数据”，Filecoin 网络基本不可用；
- 此外，Filecoin 官方推出的挖矿软件在封装效率上仍有较大优化空间，这从某种意义上说是对现实世界存储、计算以及带宽资源的浪费，无法实现对资源的高效利用。

因此，Filecoin 到真正成为可用的去中心化存储基础设施还有很长的路要走。另一方面，存储始终只是互联网基础设施中的一部分，未来分布式互联网需要一套更加完整的激励协议，激励矿工贡献包括存储，计算和带宽在内的更多资源。

FileStar 项目愿景

FileStar 希望成为 web3（未来互联网）的基础设施，构建基于 IPFS 协议的分布式存储、计算和带宽激励网络，整合全世界互联网基础设施资源，并实现资源的最优化利用。这与只专注于存储的 Filecoin 有本质区别。

与 Filecoin 的主要区别

FileStar 实现了一套更加合理的分布式存储激励机制，并将逐渐从分布式存储进化为分布式互联网的激励层，实现更加精细化的激励，实现计算、带宽和存储资源的最优化利用。FileStar 的优势主要表现在：

- 更低的挖矿门槛，网络启动初期取消前置抵押，取消 SHA256 算法对 AMD 矿机的依赖，激励更多矿工对整个网络贡献网络基础设施资源；

- 更高的可扩展性，通过修改 WindowPoST 的抽查逻辑，引入递归存储证明技术等，全方位提高链上消息处理的能力，提高 TPS；
- 高效的挖矿软件，全面提升现有 Filecoin 挖矿软件的性能，提高网络的整体封装效率；
- 数据的高可用性，可用于存储“热数据”和“温数据”，用户可以快速读取已存储的数据；
- 多方参与的去中心化治理机制，采用社区化的开发和管理模式，开发者、矿工和生态中其他参与者将共同决定网络发展方向；
- 合理的代币分配，无预挖、无募资，绝大部分代币将全部由挖矿产出，同时对生态中所有参与者进行精细化的长期激励，确保生态长期健康发展；
- FileStar 将继承 Filecoin 主网的有效存储，激励 Filecoin 矿工共同维护 FileStar 网络。

FileStar 的技术改进和创新

作为基于 IPFS 协议的分布式互联网激励网络的第一步，FileStar 提出了多项技术改进和创新。

取消前置抵押

根据 Filecoin 的经济模型，前置抵押指的是矿工在封装每一个 sector 并生成有效算力时必须抵押一定数量的代币，直到 sector 生命周期结束后再返还给矿工的一种安全机制。其设计初衷是鼓励矿工长时间存储数据，保证数据的可用性。

然而，目前 Filecoin 网络中前置抵押的设计并不合理：一方面，前置抵押的数量相对较大，在当前网络算力增速下，矿工如果进行抵押极有可能入不敷出，无法持续维护整个网

络；另一方面，目前网络中封装的大部分 sector 都是所谓的“垃圾 sector”，并没有多少包含有效数据的“订单 sector”，而通过前置抵押保证这些垃圾数据的可用性没有任何实际意义。前置抵押是造成目前矿工停摆的最主要原因。

实际上，为了保证数据的安全性，Filecoin 还设计了后置抵押，即所有挖矿奖励只有在矿工持续保存数据的情况下才能逐步解锁，数据的安全性和可用性上已经得到了较大保证。

因此，FileStar 将全面取消 Filecoin 现有的前置抵押，保留奖励的后置抵押，并对 sector 的抵押规则做出如下改进，进一步保障安全性。

- 首先，FileStar 允许垃圾 sector 拥有更短的生命周期。垃圾 sector 的主要意义在于证明网络中存在对应可用的有效存储空间。目前 Filecoin 网络中任何 sector 的生命周期至少为一年，但实际上长期存储垃圾数据是一种资源浪费。FileStar 网络中未存储有效数据的垃圾 sector 将支持较短的生命周期，避免存储资源长期被垃圾数据占用。

- 其次，FIleStar 的订单 sector 需要抵押存储费用。订单 sector 中存储了用户的有效数据，通过抵押用户支付的存储费用，将鼓励矿工优先存储订单 sector，并保证其数据可用性。

取消前置抵押将使矿工可以随时加入网络进行挖矿，并持续贡献算力，共同维护网络的安全性。

新哈希算法

Filecoin 中采用的 SHA256 算法严重依赖于 AMD 处理器的指令集优化，而大量未支持相关指令集优化的 Intel 矿机处于较大劣势，基本无法参与挖矿。这一选择极大地打击了 Intel 矿工的积极性，同时也为 Filecoin 网络未来的发展带来极大的局限性。

FileStar 的目标是成为未来互联网基础设施的激励层，必然需要激励更加多样化的硬件加入到网络中。因此，需要在保证安全性的前提下，使得基于 x86 体系的矿机挖矿性能处于同一水平，鼓励多样性。目前 FileStar 正在验证哈希算法包括 SHA512，Poseidon，Pederson 和 Blake2s 等，FileStar 将在不同平台上评估这些哈希算法的安全性和实际性能，并从中选择最合适的算法，以支持 Intel 矿机或其他高性能矿机。

递归零知识证明技术

复制证明（PoRep）是 Filecoin 存储证明的重要组成部分，结合零知识证明，PoRep 可以把存储资源量化并在链上生成对应的证明。在 Filecoin 的 PoRep 证明机制中，矿工每封装一个 sector，都需要向网络中提交两个证明，对应的消息分别为 PreCommitSector 以及 ProveCommitSector。实际上，在现有的 Filecoin 网络中，绝大多数的链上消息都是在提交这两种证明。但 Filecoin 网络的链上消息处理能力（TPS）非常有限，当网络发生拥堵时，大量的证明消息将占用绝大多数链上资源，而普通的消息将无法被打包。这同时也导致了大矿工”自私挖矿“行为，小矿工的证明消息基本无法上链。

FileStar 提出了一种递归零知识证明（Recursive ZK-SNARK）技术以解决上述 TPS 瓶颈问题和消息上链的问题。

Recursive ZK-SNARK 的基本原理是把矿工在一定时间内产生的若干 sector 的证明，进行链下证明，组成 Merkle 树，并生成一个聚合证明，最终只需要向网络中提交一次证明即可同时完成多个 sector 的证明上链过程。这样一来，每个矿工需要提交的证明消息将会明显减少，从而提高 TPS，实现网络扩容。不仅如此，通过调节证明聚合的程度，还可以对网络的消息处理能力实现调节，适应未来 FileStar 网络不同发展阶段的需求。

WindowPoST + VRF 机制

在完成 PoRep 后，矿工需要提供时空证明（PoST），证明对数据进行了持续存储。Filecoin 中矿工封装的每个 sector 每天都会被抽查，矿工需要正确提交 WindowPoST 证

明，否则其抵押的 FIL 将被罚没。对于存力较大的的矿工来说，每天提交的证明数量非常大，而且随着网络的进一步发展，网络中需要提交的 WindowPoST 也会越来越多，最终可能也会造成网络的拥堵，降低网络对普通消息的处理能力。

FileStar 在 WindowPoST 的抽查机制中引入了随机抽查机制，使得每个矿工需要提交 WindowPoST 证明的频率大大降低，而不需要每天对算力都提交多次证明。普通的随机抽查函数有可能被预测，从而影响网络的安全性，因为矿工如果能确定自己被抽查的时间，就存在作弊的可能。FileStar 采用了可验证随机函数（Verifiable Random Function，VRF）来进一步提升随机抽查的安全性。

高效的挖矿软件

FileStar 还将对现有开源的挖矿软件进行优化，全面提升矿机的挖矿效率，最大化利用矿机计算资源和存储资源。优化主要集中在任务调度模块和零知识证明模块。

- 任务调度优化。在其他软硬件条件相同的情况下，不同的任务调度策略将直接影响矿机的封装效率。Filecoin 目前的挖矿软件在任务调度上有诸多缺陷，在很大程度上影响了网络有效存储的增长。FileStar 将发布带有任务调度优化的挖矿软件，提升矿机的挖矿效率。
- 零知识证明优化。Filecoin 中无论是 PoRep 还是 PoST 都大量采用了零知识证明算法，但零知识证明的生成过程仍有较大的优化空间。FileStar 的挖矿软件将在零知识证明生成效率上进行大幅优化，并发布给所有矿工使用。

结合以上两点优化，FileStar 的全网挖矿效率会比现有 Filecoin 网络有明显的提升，这意味着在投入的相同硬件的情况下，FileStar 将逐渐成为最大的分布式存储网络。

Filecoin 算力映射

Filecoin 主网有近 600 PB 有效算力，并且仍在快速增长。参与 Filecoin 挖矿的矿工是第一批去中心化存储的基础设施贡献者，也将是未来 web3 基础设施的中流砥柱。FileStar 在上线初期将会对所有 Filecoin 上的有效算力的权益进行一定映射，矿工如果参与 FileStar 挖矿，将有可能获得与 Filecoin 主网算力匹配的奖励，具体映射规则将在 FileStar 主网上线时公布。

去中心化治理机制

FileStar 开发团队负责维护 FileStar 项目，但整个项目的开发和管理将采用社区化模式。在 FileStar 社区中，任何人都可以提交代码，同时需要提交完整的测试代码。所有新提交的代码在经过充分测试后才会合并到测试网络，并在稳定运行一段时间后再上线主网，从而保证主网的安全性和稳定性。

FileStar 项目充分尊重生态中所有社区参与者的意见，每一个新特性的开发和上线，都需要通过社区成员的投票决定。FileStar 生态中的开发者、矿工以及普通用户都可以参与投票，共同决定网络的发展方向。

代币经济模型

FileStar 协议中原生的代币为 STAR，主要用于支付消息手续费和存储费用，矿工参与挖矿可以获得 STAR 挖矿奖励和手续费奖励。为了吸引矿工贡献存储、计算和带宽等资源，同时激励更多生态参与者的加入，FileStar 设计了更加精细化的代币激励模型。

STAR 代币总量为 2,000,000,000 STAR，不对外募资，团队无预挖，代币的分配规则如下（具体分配细节可能会在主网上线时进行微调，以主网上线时为准）：

- 70 % 由挖矿产生，产量逐天减少，每 6 年产量减半
    - 30 % 用于激励提供存储资源的矿工
    - 15 % 用于激励提供计算资源的矿工
    - 15 % 用于激励提供带宽资源的矿工
    - 10 % 用于激励提供其他有价值计算的矿工，包括零知识证明服务，AI，大数据等各类有价值的计算，由社区共同投票决定
- 30 % 用于对生态中其他参与者的长期激励
    - 15 % 分配给 FileStar 基金会，主网上线一年后分 5 年线性解锁，用于项目的长期维护和迭代升级；
    - 7 % 分配给社区开发者
    - 5 % 分配给 FileStar 生态中企业和应用
    - 1 % 分配给媒体和社区
    - 1 % 分配给支持 FileStar 的交易所和钱包
    - 1 % 用于处理法律关系，确保项目遵守当地法律法规

项目发布计划

- 2020 年 10 月 20 日　发布白皮书初稿
- 2020 年 10 月 30 日　发布 Filestar 第一版代码，实现基于 filecoin 的改进，免抵押，并修复 filecoin 多个 bug
- 2021 年 02 月 28 日　实现白皮书中的大部分内容，包括新的封装 Hash 算法，递归零知识证明实现链下消息聚合提高全网 TPS 和 引入随机抽查 Window PoST+VRF 等
- 2021 年 08 月 30 日　推出可验证计算网络，激励 Filestar 的部分矿工，转向可验证计算网络
- 2021 年 12 月 30 日　推出可度量带宽网络，激励 Filestar 的部分矿工， 转向可度量带宽网络

未来工作

实现分布式存储的激励网络是 FileStar 第一阶段的目标，其目的在于吸引一批高质量的服务器，提供丰富的存储，带宽和计算资源。在第一阶段网络稳定后，FileStar 将提供更加丰富的激励机制，激励 web3 基础设施的搭建。方向包括：

- 提出计算资源、带宽资源证明机制，进一步吸引不同的基础资源提供者，实现分布式计算网络和分布式带宽网络；
- 激励网络中的计算资源为其他节点提供零知识证明计算服务；
- 为网络中其他节点提供可验证计算服务。

总结

FileStar 在 Filecoin 核心创新的基础上，实现了一套更好的分布式存储网络激励层：通过取消前置抵押、采用新哈希函数等改进，全面降低了矿工参与挖矿的门槛；结合递归零知识证明，PoST+VRF 等技术创新，解决了 TPS 和消息上链问题，极大的提搞了 FileStar 网络的可扩展性；对挖矿软件的优化使挖矿效率显著提升，提高了网络中硬件资源的利用效率。

FileStar 采用了更加公平的代币分发规则以及去中心化社区治理，极大地提升了协议的公平性，有助于项目的长远发展，并最终实现基于 IPFS 协议的分布式存储、计算和带宽激励网络，成为未来 web3 基础设施的重要组成部分。

不同于 Filecoin 只激励大家提供分布式存储，FileStar 将在分布式存储的基础上，激励大家提供可验证的计算和可度量的带宽资源，并最终和 Filecoin 形成巨大的差异化。我们相信随着区块链行业的整体发展和 Filestar 团队的全力开发，一个分布式互联网的世界正在我们眼前慢慢展开。

联系我们

官网：https://filestar.net
开发者：dev@filestar.net
媒体：media@filestar.net

社区

github：https://github.com/filestar-project

slack: https://join.slack.com/t/filestarworkspace/shared_invite/zt-infr76dh-S3m3SwbjMTMAXIUUU54efw

Twitter：https://twitter.com/FileStarProject

Telegram：https://t.me/filestarofficial

微信：filestarofficial