Arweave第17版白皮书解读（一）：空间与时间的穿越

作者：Arweave Oasis中文；来源：作者推特

## 写在前面

经过此前多篇关于Arweave共识机制迭代文章的「前情铺垫」。相信关注 Arweave 的朋友肯定对这个协议的共识机制有了比较直观的了解。但笔者自己却总有一个小小的疑惑：既然 2.6 版本那么具有里程碑意义，为什么它的共识机制却没有一个具体的命名呢？（我之前用的是限速版 SPoRA 机制来命名）。带着这个问题，我与Arweave官方的核心共识机制工程师作了深度的讨论，得知 SPoRes 简洁复制证明其实就算是 Arweave 2.6 的共识机制名称。

好吧，那也就意味着官方在 2023 年 12 与 26 日发布的题为《Arweave: The Permanent Information Storage Protocol》的第 17 版白皮书基本就是 Arweave 2.6 的官方解释文件，只不过那时的版本号已经到了 2.7.0。好消息是此前 《一文读懂 Arweave 的共识机制迭代历程》《Arweave 2.6 也许更符合中本聪的愿景》这两篇文章，基本上涵盖了 Arweave 机制的重要内容。对于想浅尝的朋友来说这些就够了。

但我还是决定对第 17 版白皮书做一些更加深入的逐章解读，这对于高阶 Arweave 参与者来说很有必要。因为如果你读过它，那满坑满谷的数学公式与建模论证会让人望而却步，不过也许这才是协议之美的最好表达。

白皮书地址：https://www.arweave.org/files/arweave-lightpaper.pdf

## 跨越空间与时间

印刷术之于人类文明有着深远的影响。它的出现让人类信息的传播与膨胀速度急剧增加，直至 20 世纪末互联网的出现让其达到了顶峰。信息的高效传播让社会透明度增加并促成了个体意识的觉醒。尽管如此，互联网仍受中心化机构的控制与审查，由于中心化分发意图操纵信息流传播的原因而导致的信息茧房是目前人类个体面临的最大问题。每年都会有一定比例的有用信息因此而丢失。

Arweave 的诞生就承载了解决该问题的使命。在其白皮书开篇，明确定义了 Arweave 协议为：

在空间和时间两个维度中以去中介化（Disintermediated）的形式传输信息的协议。

这里提到了两个维度：空间与时间。区别于地球上 99% 的数据存储服务，它就像是一颗「时间胶囊」，不仅承载着信息数据，还将时间这个重要维度加入其中。



将这两者相结合之后，Arweave 协议的形态就成为了一个永久性的信息存储系统。「永久性」这个词有多种定义：《牛津英语词典》将其定义为「持续存在或无限期保持不变」，而《韦氏词典》则将该词定义为「继续或持久存在，无基本或显著变化」。



基于这两个对永久性的定义，Arweave 应该是在以最大可能的期限范围内存储数据，且数据不能发生任何变化。为了实现这个目标，Arweave 的协议由需要有三个核心原则：

加密存储证明：一个简洁的加密证明系统，用于验证数据的复制和可访问性。

存储保险基金：一个可预测的、自执行的保险基金，利用随时间发展而发生的技术进步带来的通货紧缩效应来支付永久存储的费用。

激励演化：通过生成和奖励非强制性的网络升级，允许协议长期具有健康的迭代机制。

而实现它们的主要方式是通过「简洁复制证明 SPoRes」这一全新的区块链共识机制来达成目标，这是一个能够以最大化去中心化程度的同时，还保持最小化计算成本与带宽需求的协议。它和与之配合的存储保险基金一同构建了一个激励数据复制存储的模式，让网络得以完全以自主、透明和可预测的方式持续运行几百年。

## 对中本聪共识的调整

去中心化共识是分布式计算的一个子领域，它涵盖了对网络中的参与者，即使是有竞争关系的参与者，也能就某一个状态达成一致协议的重要研究。这个子领域随着比特币「中本聪共识」的出现而获得广泛的关注，该机制首次允许在竞争和无需许可的环境中达成一致共识。由于这一创新，比特币创造了第一个不依赖于中心化人类行为者来管理货币政策的数字货币，并一直良好地运行了 10 多年。

Arweave 从比特币工作量证明机制中获得达成共识的灵感，并对其进行了一些调整，让其符合网络内信息的永久性存储的目标。

Arweave 是一个由「节点」组成的全球去中心化共识系统，这些节点共同存储上传到系统的所有数据的多个副本。希望在 Arweave 上存储信息的用户向网络的存储基金支付一次性的存储费用，并通过将数据传输给网络内的节点来上传相应的数据。每当某个节点成功挖掘（确认）出一个区块时，节点们就会定期对新进入全球分布式数据库网络中的数据达成共识。一个区块中包含着一个交易列表，每个交易又包含了要存储到网络中的新数据，或者是其数字货币AR的转账交易，或者两者都有。挖矿是指每个节点在接受新数据进入网络的同时，也验证先前上传数据的存储情况的一个过程。节点在确认包含交易的区块后，便从网络中的其他节点「拉取」他们想要复制以进行挖矿的数据。

## 协议设计的原则

该协议设计的两个主要原则是：

极简主义：协议设计旨在保持直接和最小程度的主观判断，以促进尽可能广泛的网络共识。Arweave 仅在构建其数据结构和算法时使用了经过良好测试的加密原语。

通过激励进行优化：协议不是以规定其所期望的行为为主要目标，而是以激励参与者达成其理想结果为主要目标。所以实现这些结果的具体机制将是自然产生，并随时间而演化的。

Arweave 协议只专注于永久且可扩展的数据存储这个愿景，在这种极简且专注的设计原则之下，使得建立在协议之上的应用层有高度的可扩展性和可组合性，网络的应用范围也变得更加广泛且多样化。这在近几年中催生出了大量去中心化智能合约平台、数据库和应用程序。此外，Arweave 的高效证明系统对硬件和带宽的要求极低，最大化了网络的参与度和去中心化程度。





比特币中高效挖矿的激励措施已促成了计算哈希速度的显著提升以及成本的降低

而以激励为促进优化的方式也非常有效。我们以比特币网络为例，比特币奖励矿工发现一个随机数（nonce），该随机数与一个候选区块一起，产生一个低于某个特定值（难度系数）的哈希值。这激励了矿工不断寻找以最低成本计算最大数量哈希值的方法，所以就有了专用 ASIC 矿机的发展，自 2011 年以来，每秒可计算的哈希数暴增了 10^13 倍。比同周期内的摩尔定律（10^10）增长速度还要快。此外，这也导致了同期比特币网络中每个哈希的成本下降了 100 万倍，具体曲线可见图示。因此，基于这种原则的启发，我们在 Arweave 协议中，将比特币的激励机制调整为以激励参与者优化解决存储证明和数据传输问题的解决方案。

这就是 Arweave 协议背后基于空间与时间考量的机制设计原则。下一篇文章将系统性地解读白皮书中非常核心的的部分——存储的加密证明是如何实现的。