

Arweave 的潜力是复兴亚历山大图书馆，而非 Filecoin 替代品

为什么 Arweave 不是 Filecoin 的替代品，而是更值得关注的重大创新？

撰文：刘毅，Cdot Network 创始人，Random Capital 合伙人

Arweave 是个「非典型」区块链项目，大部分人对其一无所知，稍有所了解的人，也常把它看作是众多陪跑 Filecoin 的去中心化存储项目之一。极少数有耐心找来该项目的白皮书和黄皮书研究的朋友，看完也难免是一头雾水。因为通篇是围绕冷门概念——「信息永久存储」的阐述，看不到扩容、密码学创新、DeFi 支持、价值捕获等等能令币圈和链圈眼前一亮的概念。



谁会需要永久数据存储并为之付费？人生不过百年，凭什么我们要关心永久保存人类的知识和历史？

Arweave 创始人及核心团队自有其特立独行的理由。作为 Arweave 黄皮书的中文译者，我打算从典型的币圈和链圈的视角解读一下 Arweave，以免国内区块链创业者和投资者与这一重大创新失之交臂。首先，请允许我将 Arweave 音译为「阿维」（尽管这个中文名字尚在中文社区讨论中，并未最终确定），以便于在中文加密社区传播。

阿维与 Filecoin/IPFS 之比较

IPFS 是中心化存储领域的开创者，从 2014 年上线开始，如同 BT 一般自由生长，已经存储了大量数据。但是要让 IPFS 成为商业可用的存储系统，而不是随意的数据分享平台，必须提供服务质量保障。这就是 Filecoin 要解决的问题，即 IPFS 的经济激励层。从提出 Filecoin 概念，到今年主网「即将」面世，可谓是迁延日久。作为开发了 IPFS、libp2p 等硬核技术的协议实验室（Protocol Labs），为何会迟迟搞不定 Filecoin？

Filecoin 协议构建了两个市场：数据存储市场和数据提取市场。有存储需求的用户到数据存储市场申明自己的需求：我要存 ** 大小的数据，要求 ** 个副本，存储 ** 天。市场中的存储服务商（存储矿工）对这项存储需求报价，用户接受报价就跟矿工签订合同，支付费用。当用户需要使用数据时，就到数据提取市场提出需求；再由提取矿工给出报价，满足数据访问需求。

上述过程看上去不算复杂，实现起来却有几个困难：

矿工需要提供存储了用户数据的不可伪造的密码学证明；

在合同有效期内，协议要持续检查矿工如约保存了数据。如果违约，矿工要遭受罚款；

为了**鼓励矿工**存储数据，要让已存储数据的容量比空闲的容量赚取的更多**增发奖励**。同时需要防止矿工注水垃圾数据骗取增发奖励。

Filecoin 设计了**复制证明**（PoRe）解决第 1 个问题，采用**时空证明**（PoTS）和质押机制解决问题 2。通过精密地调校**经济模型**[1]，并引入对真实用户的认证，来解决第 3 个问题。

虽然 Filecoin 在一定程度上解决以上难题，但又不可避免地产生了一些不良后果。首先是**系统复杂性高**，矿工除了支付必要的存储成本，还要承担高昂的证明成本和质押 Filecoin 损失的期权成本。要知道，相对而言，计算比存储更昂贵。根据 Filecoin 提供的适合小规模挖矿[2]的推荐配置[3]，8TB SSD 硬盘只需 300 美元，但 AMD 3.5Ghz 16 核高端 CPU 则需要 **700 美元**，还有成本超过 500 美元的至少 128GB 的内存（作为对照，阿维挖矿的推荐最低内存是 8GB）。

挖矿成本高势必导致 Filecoin 系统的**存储服务价格高**。此外，验证真实用户是个微妙的问题，验证太严会影响用户使用体验，太宽则不能阻止矿工伪装成用户，验证就失去了意义，其间的平衡很难掌握。

同时，Filecoin 作为一种加密资产，价格会与加密市场总体行情高度关联，即**波动性很高**。如果 Filecoin 价格暴跌，矿工可能认赔离场，造成用户数据丢失。此外大幅度的价格波动还增加矿工质押 Filecoin 的**隐含期权成本**。隐含期权成本被大多数 PoS 经济模型研究忽视了，我认为至少解锁期损失的期权成本应该被考虑在内（甚至也有人认为应该计算整个锁定期的期权成本）。

解锁期是从提出解锁请求到获得可流通通证的期限，在此期间质押人不能转移通证，相当于放弃了一份**现价欧式期权**（不同于美式期权，欧式期权只能到期行权）[4]。以 Tezos 为例，设现价和行权价都为 2.53 美元，年化波动率为 185%[5]，解锁期为 14 天（更长的解锁期意味着更高的期权成本），无风险利率 4%（不影响计算结果），使用 B-S 期权计算器[6]，得出每份欧式期权价值 0.363 美元（由于行权价等于现价，因此看涨和看跌期权价值相等），相当于本金价值的 14.3%。可见由于加密通证价格波动率很高，质押引发的隐含期权成本不应被忽略。

Filecoin 协议将存储和提取分为两个市场，就需要建立**两套激励机制和定价机制**，而且用户的数据访问权得不到保障。假设你通过 Filecoin 存储了重要数据，支付了一定量的存储费用。后续你或者其他用户（例如你的客户）访问该数据，还要根据提取市场的行情支付费用，如果提取市场价格很高，相当于数据被矿工「挟持」，用户面临要么**支付高价**、要么**迁移数据**的困境。

我在 2017 年阅读了 Filecoin 白皮书，随即放弃了对该项目的研究。程序员的直觉告诉我，复杂的外推式方案通常不会成功。什么是外推式方案？就是对问题无需深入思考就自然得出的办法，也可以称之为「**想当然的办法**」。Filecoin 的外推法就是：既然矿工需要（持续地）证明已经妥善保存了用户的数据，协议就应该包含一套**密码学算法**实现这些证明。至于高度复杂的证明不可避免地带来系统复杂度高和成本高的问题，只能留待以后慢慢解决。但是 Filecoin 的竞争对手——中心化云存储不需要证明和验证，云服务厂商和客户之间签订的是**法律合同**，法律保证了客户的访问权和追索权。可见只要证明成本居高不下，去中心化存储就难以提供有竞争力的价格。

Sia、Storj等协议虽然在技术上与 Filecoin/IPFS 不同，但是它们都属于**基于合同**的去中心化存储协议。即用户和矿工通过协议签订合同，用户支付合同规定的费用，矿工承担合同规定的义务，协议（或者用户）对矿工履约情况进行检查（挑战），并对违约行为进行惩罚。基于合同的去中心化存储协议都面临前面分析过的基本难题。

科技发展的常态是，当大部分人试图用「想当然的办法」解决复杂问题时，总有人能**另辟蹊径**，用其他人未曾预料到的、通常是简单得多的办法解决难题。果不其然，在对去中心化存储领域旁观三年之后，偶然的机缘让我了解到「**阿维 Arweave**」——去中心化存储破局者。

只有明白 Filecoin 的艰难，才能理解阿维的**巧妙**。阿维是一套完整的去中心化存储协议，不基于 IPFS，或者说它相当于 Filecoin + IPFS。阿维如何解决矿工证明的问题呢？答案是无需证明。阿维协议通过机制设计鼓励矿

工尽量多存数据，而且优先存储副本少的**稀缺数据**。至于每个矿工存了多少，存了哪些，那是矿工自己的事情，既不需要证明，也不需要检查。就好比学校希望同学们认真学习，可以采用两种方法。一种是老师天天盯着每个人，是否专心听讲、认真完成作业，发现不认真的就批评罚站。另一种方法是**通过考试**，不管平时怎么学习，最后凭考试成绩说话，考得好有奖。两种办法都能提升学习效果，但是显然后一种要简单得多。

基于合同的去中心化存储类似于「盯人」，阿维协议则像「考试」，这种方式被称为基于激励的去中心化存储。可以这样来直观地理解其优势：Filecoin 要管理成千上万个不同的存储合同，检查每个合同的执行情况，分别提供奖励或执行惩罚。阿维协议只处理一个合同——**所有数据永久保存**。因此协议非常简洁，运行成本低，服务的价格和可靠性都优于基于合同的系统。

阿维的「访问证明」（PoA）是 PoW 的简单扩展。每一轮 PoW 谜题都跟某个过去的区块（回忆块）有关，只有存储了**回忆块**的矿工才有资格参与 PoW 竞猜。由于回忆块是随机确定的，事先无法预测，因此矿工存储的区块越多，参与 PoW 竞猜的机会越大，获得出块奖励的可能性越高。如果矿工的存储空间有限，不能保存全部区块历史，他会优先保存在网络中副本数量较少的区块。因为每个块被选为回忆块的概率相等，当一个稀缺区块被选为回忆块，就只有少数矿工有资格参与 PoW 竞赛，因此**存储稀缺区块**对矿工更有利。

有朋友可能会问，如果恰好所有节点都没有存储某个区块，那这个区块不就**永久丢失**了吗？是这样的，这个可能性存在。不过，我们可以量化计算单一区块永久丢失的风险[7]。

首先需要引入**复制率**的概念，复制率是矿工平均存储的区块历史的比例。例如网络一共出了 100 个块，平均每个矿工存储了 60 个块，那么复制率就是 60%。复制率也是任选一个矿工，他拥有**随机挑选**的某个区块的概率。反过来，随机挑选某个区块和某个矿工，矿工没有这个区块的概率是 1-复制率。当网络中有 N 个矿工节点时，所有矿工都没有某个区块的概率是 $(1-\text{复制率})^N$ 。存在一个丢失区块的概率是 $(1-\text{复制率})^N \times \text{区块总数}$ 。

假设阿维网络有 200 个矿工节点，复制率为 50%，区块总量为 200000，那么存在一个丢失区块的概率是 6.223×10^{-61} ，是一个可以忽略不计的极小概率事件。当前阿维网络的矿工节点约为 330 个，复制率是 97%，已出区块 51 万多个[8]，存在**区块丢失的概率**比前面的计算结果还要低得多，在数量级上与**发生私钥碰撞**的概率相当。而且上述计算的假设是矿工随机存储区块历史，考虑到矿工优先存储稀缺区块，丢失区块的可能性更低。

阿维协议只有一个市场，用户也**只需要支付存储费**，后续访问数据是免费的。能够做到这一点是因为阿维协议采用类似于 BT 的机制设计[9]，网络中所有节点都是平等的（不区分矿工节点和用户节点），所有节点都尽量快速地响应其他节点的请求。跟 BT 一样，上行贡献越多，下行速度越快。自私节点会被其他节点降权，逐渐被网络排斥在外。

要全面理解阿维协议的设计，最好的方法是**阅读黄皮书**

（https://github.com/toliuyi/arweave_notes/blob/master/arweave-yellow-paper-cn.pdf）。虽然黄皮书篇幅较长，也有不少公式，但是不必担心，有中学数学基础就能看懂。

与 Filecoin 相比，阿维网络有两大优势。一是**成本低**。虽然 Filecoin 主网还没有上线，我提前做个预测：在 Filecoin 主网上线一年后（经济模型进入稳定状态），1MB 文件在阿维网络做几百个副本永久存储的价格，会低于在 Filecoin/IPFS 网络上 5 个副本存储 5 年的价格，而且阿维网络的数据访问是永久免费的。第二，阿维协议的激励机制使数据存储和访问都**更加可靠**。通过简洁巧妙地解决了去中心存储的最大难题，不需要 2 亿美元的募资和长达三年的开发，阿维主网已经上线两年多。

阿维不是 Filecoin/IPFS 的陪跑者，而是最有希望**让大规模去中心化数据存储成为现实**的加密协议。

阿维与以太坊之比较

阿维很少被拿来跟**以太坊**比较，毕竟在**Web3.0**协议栈中，它们处在不同的层级，看上去是互补关系。但是深入研究阿维协议，就会发现更多的可能性。

以太坊（以及其他智能合约公链）为支撑**去中心化应用 DApp**而生。DApp 是公平透明地执行，不能被个别或者少数人控制的互联网应用。从软件架构角度，网络应用（包括互联网应用和 DApp）可以分为表现、业务逻辑和持久化（数据）三层。我们不妨分别从这三层分析 DApp 的发展瓶颈，以及阿维协议的应用潜力。

迄今为止，DApp 的表现层仍然停留在和中心化 Web 应用相同的状态，即由开发者部署在**云服务器**，再下载到用户客户端执行。因此开发者和云服务提供商仍然具有停止和审查 DApp 的权利，网络中断、服务器宕机、DNS 劫持等故障和攻击也仍然威胁着 DApp 的**可用性和安全**。此外，DApp 的 IT 基础设施成本会随用户数量的增长而提高，令开发者必须采用某种货币化手段，以维持 DApp 的运行。货币化手段要么是 Web2.0 式的，即**贩卖流量**；要么带有加密协议的特色，即**发行通证**。一旦货币化失败，开发者可能放弃运行 DApp，用户只能转而寻找替代品。而即便侥幸存在替代品，还是面临同样的问题。可以维持运行的 DApp 也常会遇到「**强制升级**」的问题，即新版本不一定不比老版本更受用户欢迎，但用户不能阻止其升级，也不能继续使用老版本。

综上所述，去中心化应用的**表现层**仍然是中心化的，仍然能够被个别或者少数人控制。

阿维协议的应用层被称为**永在网**（permaweb），其主要（不是唯一）的应用程序架构是**无服务器**

（Serverless）式的。无服务器 DApp 的开发类似于传统 Web 的前端开发，开发者使用 HTML、Javascript 和 CSS 开发 DApp 的表现层。不同之处是，表现层的部署不是上传到云服务器，而是打包**存储在阿维网络**，保存的费用很低，而且是一次付费永久服务。用户仍然使用原有方式访问 DApp，阿维 DNS 和 TLS 与普通浏览器兼容，不需要用户安装和学习使用新客户端。无论 DApp 用户如何增长，都不会再给开发者带来开销。

由于阿维是**去中心化网络**，无论是开发者还是阿维矿工，都不能阻止或者审查用户使用 DApp。开发者可以开发 DApp 的新版本，但是新版本不能覆盖旧版本，使用哪个版本的选择权在用户手中。可见阿维实现了 DApp 表现层的去中心化，因此有越来越多的 DApp 把**表现层**移植到阿维，包括：**Synthetix Exchange、Tokenlon、KyberSwap、UniSwap、Oasis App、Curve.fi**等等[10]。

需要说明的是，使用去中心化存储实现 DApp 表现层的去中心化，这个概念并不是阿维协议的创造。早在 2014 年，**Gavin Wood**博士在描述 Web3.0 网络形态的论文[11]中就把「**静态内容出版**」列为 Web3.0 的四个基础组件之一。这一思考的实践结果是**Swarm**项目[12]。Swarm 和 IPFS 都曾被寄予厚望，以解决 DApp 表现层的去中心化问题。但是由于多种原因，这一愿望至今尚未实现。直到阿维协议出现，DApp 表现层的去中心化才有了切实可行的方案。

以太坊等智能合约公链实现了**DApp 业务逻辑层和数据层**的去中心化，但是众所周知存在**扩展性瓶颈**。扩展性和价格是一体两面的问题，扩展性限制源自计算和存储资源稀缺，在去中心化网络中，竞争使用稀缺资源的结果就是价格高企。由于价格更加容易量化，本文选择从**价格**角度进行分析。

先看**数据层**。以太坊存储 256 位整型数据要消耗 20,000 gas[13]，存储 1MB 数据需要 6.25 亿 gas。按 gas 价格 20gwei（本文写作时恰逢 DeFi 热潮，gas 价格常高达 100gwei 以上），ETH 单价 400 美元计算，在以太坊链上存储 1MB 数据的花费**高达 5000 美元**，显然是难以负担的高价。有数据存储需求的 DApp 大都采用混合存储方案，即加密资产等高值数据和附件的哈希存储在链上，详细数据、多媒体数据等存储在链下。如果采用中心化的链下数据存储，例如**关系型数据库或者 NoSQL 数据库**，则 DApp 仍然是部分中心化的，仍然会被个别或少数人（云服务厂商和开发者）控制。因此，很多 DApp 更倾向于选择去中心化存储，如 IPFS 等。

在这个环节上，阿维提供完全去中心化的、低成本、高可靠性的永久数据存储，从而成为以太坊的得力助手。不必牺牲去中心化，目前阿维存储 1MB 数据**仅需 0.1 美分**。你没有看错，是以太坊的五百万分之一。按当前价格计算，在阿里云存储 1MB 数据 100 年的开支是 2.6 美分。而且仅支持同城冗余复制，数据同步和数据访问的网络开销另行计费。而阿维网络是全球五大洲**数百个节点冗余复制**，数据同步和访问全免费。你还是没有看错，去中心化的阿维网络已经比中心化云存储的**价格更低**。无怪乎有 Solana[14]、SKALE[15]、Prometheus[16] 等 Layer 1、Layer 2、DApp 协议选择阿维作为**数据存储层**。还有 InfNFT、Mintbase.io 和 Machi X 等 NFT 项目使用阿维存储 NFT 媒体资源、元数据和代码[17]。

智能合约是 DApp 的**业务逻辑层**。与数据层类似，智能合约的瓶颈是扩展性 / 计算成本问题。根据Vitalik Buterin的估计，以太坊的计算和存储成本是亚马逊云服务的大约 100 万倍[18]，前文对 DApp 数据层成本的估算也能印证此估计。公链计算和存储成本高昂的根本原因是其**全冗余架构**，即所有的链上数据都被每一个全节点存储，所有的计算都在每一个全节点执行。实现公链扩容的思路有**代议制、分层和分片**三种，更深入的讨论请参见拙作《**Polkadot 架构解析**》（<https://www.chainnews.com/articles/346896273320.htm>）。

阿维的**Smartweave**智能合约[19]则完全另辟蹊径。Smartweave 智能合约是 Javascript 开发的程序，存储在阿维网络上，因此具有不变性。与合约代码同时提交给网络保存的，还有合约的创世状态。与以太坊（以及其他公链）的智能合约不同，Smartweave 不是由矿工节点执行，而是下载到**合约调用者**的计算机执行。执行的过程是从合约的创世状态开始，按确定的顺序执行合约历史上的全部交易，最后执行合约调用者的交易。完成后，合约调用者将自己交易的输入和执行后的合约状态提交到阿维网络，进入永久存储。后续的合约调用重复以上过程。

也就是说，对于一笔智能合约交易，阿维网络**只需一个节点**——调用者自己的节点来执行（注意阿维网络不区分全节点和轻客户端）。由于调用者节点执行（同时验证了）了合约历史上的全部交易，因此他无需信任或依赖任何节点，就能得到**可信的计算结果**（即智能合约的新状态）。因此，可以把每个 Smartweave 合约都看成阿维的**二层链**，执行智能合约就是对二层链的全量同步和验证。这一设计使得 DApp 业务逻辑层的**可扩展性**/ 计算成本难题迎刃而解。智能合约几乎可以不受限制地包含任何复杂计算，只需付出很低的边际成本，因为通常情况下调用者的计算设备已经被购买或者长期租用了。

有朋友可能会问：随着交易数量增长，智能合约执行岂不是越来越慢？确实如此，但是有办法可想。例如，由调用者对合约的结果状态进行命名，从而形成**合约状态快照**。如果该调用者值得信任（例如调用者是智能合约开发者的情况），后续的调用者可以指定状态快照作为初始状态，就只需执行快照之后的交易。状态快照不一定导致信任集合扩大，毕竟智能合约可靠的前提已经包含了对初始状态的信任。

当然，Smartweave 仍然处于开发之中，当前版本是**V0.3**。以上内容应该视为对 Smartweave 潜力的探讨。要达到商业使用，Smartweave 还需要解决很多问题，例如**可组合性**。

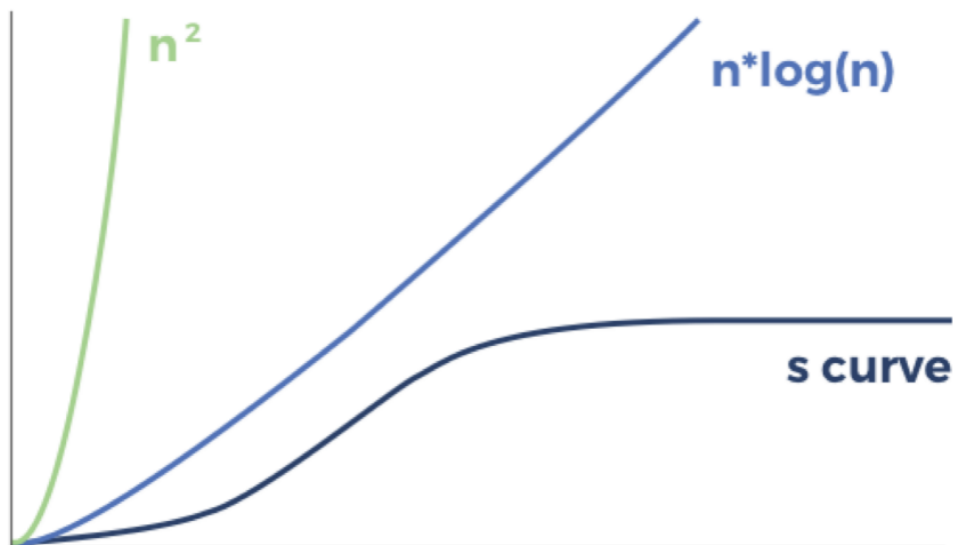
从我对 Smartweave 运行机制的理解，实现可组合性没有特别的技术障碍。但是，我一直认为以太坊智能合约的可组合性**「太过强大」**，以至于很难限制合约系统复杂度的指数式增长。期待 Smartweave 团队有更令人惊喜的创新，用好可组合性这柄双刃剑。

综上所述，阿维协议支持 DApp 真正实现全面的去中心化，并且解决困扰公链领域多年的计算和存储的**可扩展性 / 成本**问题。从这个意义上说，阿维更应该归为 Blockstack[20]所倡导的**「Web3.0 全栈协议」**，而不仅仅是去中心化存储。

阿维与比特币之比较

比特币是加密协议的开创者，也是加密货币之王。一直以来，业内都有一个争论不休的话题：比特币的王者地位是否可能被取代？即便是**比特币保皇派**，也承认经过 10 年发展，比特币早已不是技术最先进的加密货币。但是他们认为：**超主权价值存储型货币**是加密货币最大的用例。比特币协议运行时间最长、知名度最高、安全性最好。而且加密货币的竞争壁垒不是技术，是**流动性**。流动性有网络效应，即产品或服务的效用随着用户增长而增加的机制。比特币协议已经建立起**流动性优势**，这一优势只会随着加密货币普及持续加大。因此，比特币的王者地位无可撼动。

流动性网络效应优势是否可能被打破？回答这个问题需要对网络效应进行定量研究。相信很多人会马上想到**梅特卡夫定律**，即网络的价值与用户数量的平方成正比。梅特卡夫定律是第一个网络效应的定量模型，但是近些年的研究表明，没有一种网络的价值按梅特卡夫定律增长，至少到用户数量较大时，网络价值增长曲线**必然变得平坦**[21]。



有研究表明[22]，部分互联网业务的网络效应是 $n \cdot \log(n)$ ，部分是**S 曲线**。S 曲线是网络价值随用户增长，是先慢后快的指数型增长，达到饱和之后增长速度趋缓。S 型曲线的重要推论是，强者愈强是成立的，但不是赢家通吃。如果所有的互联网平台的网络效应都符合梅特卡夫定律，那么在互联网行业的每个细分领域，都会形成**单一寡头**的局面。但是现实是不论在全球还是中国的互联网行业，大多数的**细分领域**都有不止一个平台长期存在。

那么**流动性网络效应**是以什么曲线（公式）增长？假设某一项加密资产，平均每个参与者每天的交易量占资产总市值的万分之一。1 万个投资者则日均换手率为 100%，2 万个投资者换手率就是 200%。也就是新增 1 万投资者，换手率增加了 1 倍。如果投资者从 10 万增加到 11 万，换手率从 1000% 增长到 1100%，只增加了十分之一。所以**投资者越多**，新增投资者对流动性的**贡献比例就越小**，其网络效应与参与者的数量呈 $\log(n)$ 的关系。

$\log(n)$



以上关于流动性网络效应的量化模型和图片全部来自**Multicoin Capital**的研究[23]。此项研究的结论非常重要，例如交易所竞争的是流动性，头部交易所达到一定规模之后，流动性网络效应带来的价值增长会趋缓，使后来者有赶超的机会。如果是流动性是 $n \cdot \log(n)$ 甚至 n 平方的网络效应，就不会出现币安、Kucoin、MXC 杀出重围后来居上，也不会存在上万家交易所。 $\log(n)$ 的数量关系说明流动性是越大越强，但不保证强者恒强。

还有一个因素使比特币的流动性优势更容易被打破，我称之为「**流动性传导**」。就是新生的加密货币能够使用已经建立起来的全球化交易网络，从而跟已有的加密货币**共享流动性**。例如在以太坊诞生时，包括交易所和支付平台等在内行业基础设施已经发展了 6 年，它们很容易就**集成 ETH**。ETH 只要跟比特币形成高流动性的交易对，就跟主要的法币间接具有了流动性，因此以太坊不再需要经历漫长的市场导入、基础设施建设阶段，一跃成为具有高流动性的加密货币。

在自由竞争状态下，货币之间比较的是**货币性**。货币性包括稀缺性、可互换性、可验证性（难于伪造、易于辨识）、可及性、可分性，还有保存、携带和转移的成本等。所有的加密货币都是比特币的直系后代，也都继承了比特币强大的货币性。在以太坊之前，加密货币创新主题是「**更好的比特币**」，也就是创造货币性更强的加密货币。例如莱特币、达世币、恒星币**转账速度更快**、交易费更低。ZCash、门罗币**私密性更好**，可互换性更有保障，但是他们都没有威胁到比特币的地位。因为量的改进不足以挑战网络效应优势，必须有质的创新，才能实现「**范式转移**」。例如，微软不是发明了更好的大型机打败 IBM，苹果也不是用更好的 PC 机打败微软。革命性的创新者都是对老霸主实施**降维打击**，才成为新王者。

业内普遍认同以太坊是区块链 2.0 的代表，因为以太坊是全新层面的创新，通过**引入 EVM**，令加密货币具有了强大的**可编程性**。换代式创新不是你做的事我能做得更好，而是我能做你不能做的事。

以太坊智能合约能够实现去中心化资产发行、资金募集和资产交易，在上一轮 ICO 浪潮中，ETH 被当作主要的**货币和价值存储**使用，对 ETH 的需求暴涨，也推动其市值最高达到 BTC 的 60%。当然，ICO 存在**严重的信息不对称**，不可避免地产生普遍的反向选择和道德风险问题，泡沫破裂是必然结果。高度可编程的加密货币则具有无穷的创新空间，**DeFi**的兴起将是以太坊对比特币的新一轮挑战。可惜 ETH 的价值捕获机制不健全，如果早几年实施 EIP1559，ETH 应该已经进入通缩阶段，DeFi 热潮很可能推动其市值超越 BTC。

加密资产市场有两大投资主题：**健全货币**和 Web3.0。健全货币是去中心化的、超主权的加密货币，以**比特币**为代表。Web3.0 是应用区块链技术，重构社会生产关系，代表项目是**以太坊**。我认为健全货币和 Web3.0 两大投资主题**可以兼得**，即去中心化的、高度可编程的区块链平台，既能支持 Web3.0，其原生加密资产同时具备健全货币的性质，就可以鱼与熊掌兼得，成为未来的加密货币之王。新王者应该具备以下性质：高度去中心化（隐含了超主权）、用途广泛、共识协议外部性低、稀缺性好，高度可编程、合规。

鉴于以太坊 1.0 的扩展性问题，即便登上王位也难以持久。哪个项目才是区块链 3.0 的代表？以太坊 2.0、Polkadot、Cosmos 和阿维协议都是有力竞争者。阿维协议也具备成为**加密货币之王**的潜质：

去中心化程度高，网络不会被个人、机构或政府控制；

用途广泛，作为 Web3.0 全栈协议，是各类去中心化应用创新的理想平台；

PoA 共识不会大量额外消耗**电力**，详细讨论见下一章；

阿维协议原生通证 AR 的增发率低，**稀缺性好**，详细讨论见下一章；

高度可编程，智能合约图灵完备。DApp 和智能合约均采用 Javascript 等成熟 Web 技术，有利于形成广泛多样的开发者社区；

阿维非常类似于以太坊，在主网上线前进行 ICO。主网上线后分发了功能性通证。ETH 的功能是支付以太坊的计算和存储费用；AR 的功能是支付阿维网络的**存储费用**。随着时间推移，AR 被越来越多人使用，持币也越来越分散，符合大宗（虚拟）商品的法律定义。

阿维经济模型详解

加密协议的**经济模型**就是如何协调服务提供者（矿工）、服务使用者（用户）和持币者之间的利益关系。矿工为加密协议网络提供计算、带宽和存储资源，保障协议安全可用，用户使用协议要向矿工付费。矿工的收益分为两个部分：一是用户直接支付的**交易费**；二是协议向矿工分发新铸造的通证，即**增发奖励**。增发奖励是全体持币者按照持币数量分摊的铸币税。在几乎所有加密协议经济模型中，矿工的主要收益都是增发奖励（铸币税）。例如，虽然比特币已经经过三次增发奖励减半，增发奖励仍然**占矿工总收益的 95%**，交易费仅占 5%。这实际上是持币者对用户使用协议进行补贴的机制。

在我研究过的所有加密协议经济模型中，阿维协议的经济模型是**对持币者最友好的**。在创世区块中，协议生成了 5500 万个 AR，然后每个区块都会增发 AR。增发量计算公式如下：

其中：

将常量带入，公式简化为：

阿维协议平均 2 分钟一个区块，创世块之后每个区块增发大约 29 个 AR，增发量每年减半，一共最多增发 1100 万个 AR。也就是说，阿维主网上线 2018 年 6 月后的每一年，都会**挖出剩余 AR 的一半**，即第一年挖出 550 万个 AR，第二年挖 275 个，第三年挖 137.5 万个 ...（阿维主网于 2018 年 6 月上线，出块奖励发放有两多月的滞后）。

在本文写作之时，阿维网络正面临**第二次减半**（预计为 2020 年 9 月 10 号左右）。二次减半后一年（即第三年）的增发率是 $137.5 / (5500 + 550 + 275) = 2.17\%$ 。到第四年，AR 的增发率将低于同期的比特币。

另外一个稀缺性指标可能更具说法力，待开采率 = 未开采量 / 总量。目前未开采的 AR 只剩大约 198 万个，**待开采率为 3%**。作为对照，目前还有大约 255 万个 BTC 未被采出，待开采率为 12%。可见 AR 增发量少，增发速度衰减快，具有健全货币高度稀缺的典型特征。

但是请读者注意，根据阿维团队提供的数字，目前 AR 的流通量约为 3800 万个，这意味着有**大约 2600 万个 AR 处于非流通状态**。我不清楚这部分通证的所有权构成和解锁计划，只能推测其属于早期投资者、团队和基金会。如果有人了解这方面的情况，请告知作者，不胜感激。

阿维经济模型的原则可以大致概括为：用户为**存储服务**支付足够的费用；矿工的**收益超过成本**，维持基本的大致固定的利润率；持币者获得 AR 通证增值的几乎全部收益。按照 AR 此前长期盘整的币价 4 美元计算，今年阿维矿工从增发获得收益为**550 万美元**，这些收益将由全球数百个矿工节点分享。与此相比，比特币矿工每天获得的增发收益高达 1000 万美元以上，每年超过 36 亿美元。

阿维 PoW（作为 PoA 访问证明的一部分）采用**RandomX 算法**[24]。RandomX 是一种 CPU 友好的算法，需要大量内存执行，专用硬件的优势很小。继阿维协议之后，门罗币于 2019 年 11 月将 PoW 算法升级为 **RandomX**[25]，作为对**ASIC 挖矿**的最新（也许是最后）的抵抗。鉴于阿维挖矿不是单纯的算力竞争，而且挖矿的总体收益有限，阿维很可能不会形成专门的挖矿产业链，而是保持全球几百个挖矿节点（有些节点会成为矿池）和**较高的复制率水平**，网络电力消耗不高。主流挖矿硬件很可能不是 ASIC 矿机，而是普通商用计算机。

当然，不排除在 AR 热度提高后，有人会推销阿维矿机。那时候你应该了解，购买阿维矿机几乎不可能带来像样的回报。长远看来，阿维可能成为 Web3.0**去中心化 CDN 网络**，届时面向企业的 CDN 服务才是阿维矿工的核心商业模式。

阿维与加密资产投资

从 2013 年初开始投资比特币，从此后的 7 年多时间里，我听许多人谈起过，如何得知比特币、对比特币的第一印象、如何与巨额财富擦肩而过等等。有个一直困扰我的问题是：**是什么决定了我们当时对比特币的看法？**大多数人浑不在意，部分人认定比特币是披着高科技外衣的资金盘，少数人出于各种不同的心理投资比特币或者开始挖矿，其中又有极少数人坚持下来，被比特币改变了命运。

这**极少数的人**常被当作预见未来的天才。但是要知道任何一项新奇的事务，都有一群早期参与者，但在无数的新奇事务中，对社会产生广泛影响的寥寥无几。与其把早期参与比特币而一跃成为大佬的人视为天才，倒不如说他们是幸运儿。但问题是，这样的鸿运是否以大致相等的概率随机地降临到每个人头上？以我这些年对这个问题的思考，可能也不尽然。

对大多数人来说，加密资产市场**最多算是赌场**。在牛市中赚取的几倍或更高的收益，很容易就在熊市里悉数交还给市场，甚至还要赔上本金。根本原因在于，加密协议的失败率非常高。直接的证据是，五年前还位列市值榜前十的加密货币[26]，到今天**大部分已经归零或者接近归零**。

加密协议不是解决一切问题的**万能良方**。现在市场上数以千计的加密协议，试图建立各种无信任的互联网平台。但是在五到十年之后，会有相当大一部分加密协议的出发点被证明是错的，也就是加密协议不适用于这些领域。而在那些适用的领域，由于加密协议具有网络效应、没有地域限制能够服务全球用户，在同一领域内获得成功的加密协议数量应该是屈指可数。因此在五到十年的时间里，现有市场上的数千种加密资产，绝大多数都会归零或者接近归零。

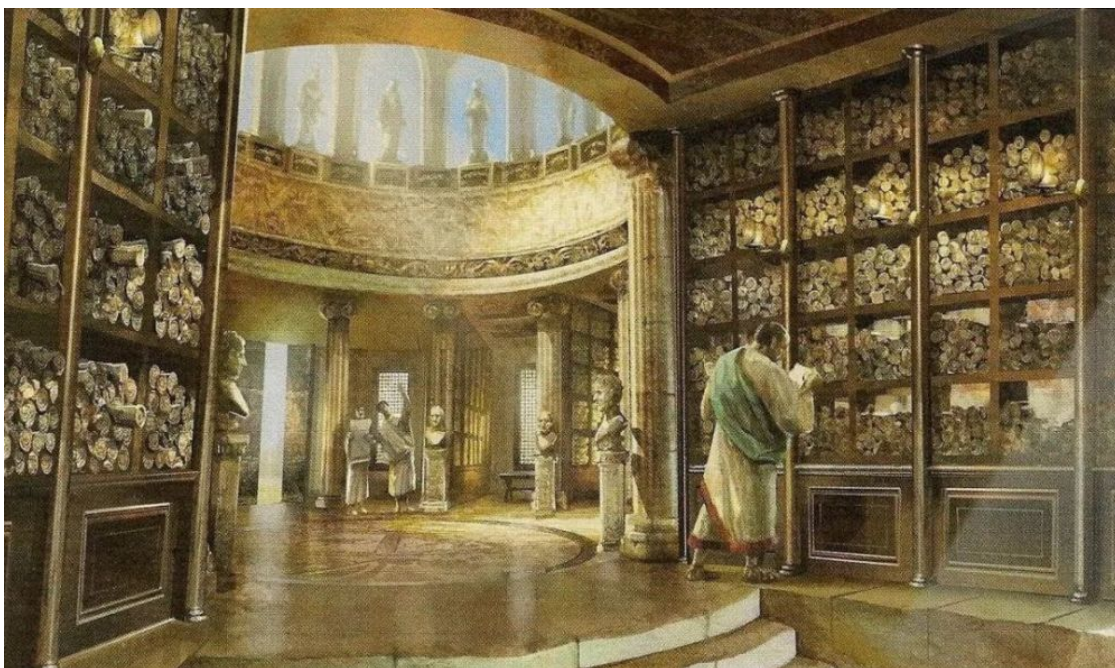
理性的投资者为什么甘愿冒着归零风险投资加密资产？在 2014 年中，比特币正处于上一轮熊市的低谷，美国司法官办公室分四次公开拍卖 10 万枚比特币。硅谷著名的风险投资家、德丰杰投资的掌门人**Tim Draper**拍下其中的大部分。拍卖结束后，Tim Draper 接受媒体采访解释了他买入比特币的逻辑。他说比特币很有可能会归零，但也有一定概率涨上百倍，所以是一项很好的投资。假定在他买入开始的五年以后，比特币 80% 概率归零，20% 的概率涨了 100 倍。那么这项投资的期望收益率是**每年 82%**，显然高于长期国债的无风险收益率。

我看到了拍卖的新闻，也听到了 Tim Draper 对他投资逻辑的解读。我认同他的逻辑，所以又用一笔能亏得起的资金，加仓了比特币。事实证明，这个投资逻辑是成立的。

在加密资产市场大获成功的人都是乐观的、关注大问题的**长期主义者**。所谓大问题就是影响互联网乃至人类社会发展的基本问题。在 2011 年、2013 年甚至 2015 年，你都可以列出比特币将会失败的上百条理由，这些理由也都站得住脚。但是如果你关注以下几个大问题（或者其中之一）——互联网需要原生的、**不依赖特定机构**的价值传输；**互联网平台和金融中介**已经攫取了全社会经济活动的大部分利润；**央行**不断增发货币推动经济发展已经无以为继等等——就会认识到比特币出现的跨时代意义。而且，一个乐观主义者，要相信比特币虽然有上百个理由失败，但也可能有获得成功。至于说到长期主义，与**关注大问题**本就是一体两面。如果有人获得几倍利润就清仓了比特币，很难相信他真的关注大问题。

永久保存人类的知识和历史当然是大问题，而且很可能它的重要性对人类无出其右。毕竟现代人就智力和体能而言，跟几万年前的智人祖先没什么不同。我们过着与先人截然不同的生活，唯一的原因就是我们继承并利用了人类在数万年的历史中**沉淀的知识和经验**。

对于托勒密王朝的统治者来说，**亚历山大图书馆**也许只是国家富饶的点缀。但是对于后人，亚历山大图书馆远比托勒密王朝要重要得多。虽然凯撒被历史学家蒙森称为：罗马帝国唯一的创造性天才。但是凯撒的千秋功业，也弥补不了**烧毁亚历山大图书馆的过失**。今天的科技是否已经发展到了临界点，世界可以不再依赖个人、机构或者国家，无论他们如何强大，来永久地保存全人类的知识和历史？如果在这一代人实现这个旷古未有的伟大成就，能参与其中的我们将是何其幸运！



所以阿维并不是 Filecoin/IPFS 的替代品或者竞争对手。Filecoin/IPFS 的目标是颠覆中心化云服务厂商对存储市场的垄断，这当然是互联网行业的重要问题，但是与阿维的目标相比，还远远算不上是「大问题」。当我读完阿维黄皮书，一瞬间仿佛时空穿梭回到初识比特币的时候。这一次，奇迹还会上演吗？

引用文献

1. <https://filecoin.io/zh-cn/2020-engineering-filecoins-economy-zh-cn.pdf>
2. Labs, P. A Guide to Filecoin Storage Mining. Filecoin Available at: <https://filecoin.io/blog/filecoin-guide-to-storage-mining/>.
3. <https://pcpartpicker.com/user/tperson/saved/H2BskL>
4. Venturo, B. The economics of Ethereum's Casper. Medium (2018). Available at: <https://medium.com/@brianventuro/the-economics-of-ethereums-casper-6c145f7247a2>.
5. https://www.reddit.com/r/CryptoCurrency/comments/982x9l/top_100_cryptocurrencies_ranked_by_annualized/
6. <http://app.czce.com.cn/cms/cmsface/option/Calculator/utCal.jsp>
7. Project, T. A. Decentralised storage: Incentives vs Contracts. Medium (2019). Available at: <https://blog.goodaudience.com/decentralised-storage-incentives-vs-contracts-b74ee0b7eff1>.
8. <https://viewblock.io/arweave/stats>
9. Bram Cohen. Incentives build robustness in bittorrent. In Workshop on Economics of Peer-to-Peer systems, volume 6, pages 68{72, 2003. [19] Matt Corallo. Compact block relay. bip 152, 2017.
10. Project, T. A. Arweave News: July. Medium (2020). Available at: <https://medium.com/@arweave/arweave-news-july-7905d5e0c84f>.
11. DApps: What Web 3.0 Looks Like Available at: <http://gavwood.com/dappsweb3.html>.
12. Swarm Available at: <https://swarm.ethereum.org/>.

13. G. Wood, Ethereum: A secure decentralised generalised transaction ledger, In: Ethereum Project Yellow Paper 151 (2014).
14. Solana - Arweave Bridge: ArweaveTeam Funded Issue Detail. Gitcoin Available at: <https://gitcoin.co/issue/ArweaveTeam/Bounties/30/100023463>.
15. SKALE Network - Arweave Bridge: ArweaveTeam Funded Issue Detail. Gitcoin Available at: <https://gitcoin.co/issue/ArweaveTeam/Bounties/27/4468>.
16. Labs, P. New primary storage for Ignite. Medium (2020). Available at: <https://medium.com/prometeus-network/new-primary-storage-for-ignite-94096e2e8506>.
17. Project, T. A. NFT Permanence with Arweave. Medium (2020). Available at: <https://medium.com/@arweave/nft-permanence-with-arweave-35b5d64eff23>.
18. Wang, B. Ethereum is about 1 million times less efficient for storage, network and computation. Next Big Coins (2018). Available at: <https://www.nextbigcoins.io/ethereum-is-about-1-million-times-less-efficient-for-storage-network-and-computation/>.
19. Project, T. A. Introducing SmartWeave: building smart contracts with Arweave. Medium (2020). Available at: <https://medium.com/@arweave/introducing-smartweave-building-smart-contracts-with-arweave-1fc85cb3b632>.
20. <https://www.blockstack.org/>
21. Odlyzko, Andrew & Tilly, Benjamin. (2020). A refutation of Metcalfe's Law and a better estimate for the value of networks and network interconnections.
22. The Network Effects Bible. NFX (2020). Available at: <https://www.nfx.com/post/network-effects-bible/>.
23. Kyle Samani, On the Network Effects of Stores of Value. phoenix Available at: <https://multicoin.capital/2018/05/09/on-the-network-effects-of-stores-of-value/>.
24. tevador. Randomx. <https://github.com/tevador/RandomX>, 2019.
25. Shevchenko, A. & Shevchenko, A. Monero Penalizes GPU and ASIC Mining with RandomX Upgrade. Crypto Briefing (2019). Available at: <https://cryptobriefing.com/monero-penalizes-gpu-mining-randomx/>.