

DSN 去中心存储研究

~yashua

非区块链的分布式存储项目

项目	主要功能	技术特点
Napster	音乐文件分享	首个广泛应用的 P2P
BT 网络	P2P 文件共享	分布式存储+种子服务器，种子服务器记录了碎片位置，半中心化
快播	在 BT 网络基础上，实现了直接播放	BT 网络的方案，加入了自有服务器用来缓存，半中性化
电驴	无中央服务器的 P2P 共享	KAD 网络，任何人都可以运行服务器端担任种子服务器。Jed McCaleb, Mt.Gox 创始人，瑞波创始人，XLM 创始人

Arweave

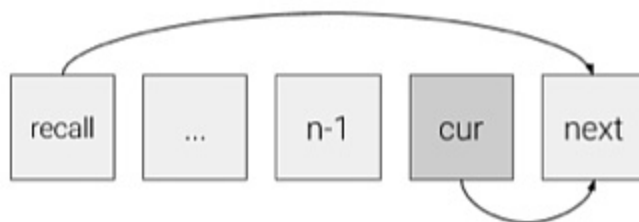
基本情况

1. Arweave 协议的愿景是提供去中心化、可扩展和永久的链上数据存储，vs filecoin 链下存储。
2. 2019 年，Arweave 从包括 Coinbase、a16z 和 Multicoin Capital 在内的知名风险投资公司那里筹集了 500 万美元。2020 年，Arweave 又获得了 830 万美元的资金，他们计划将其用于建立在 Arweave 之上的用户和开发者社区上。这包括 Verto、ArDrive 和 Arweave News 等项目。Arweave 的创造者和创始人是 Sam Williams，“他是一名博士，在去中心化系统设计和实施方面有着丰富的经验”。他在大学期间建立了 Arweave。
3. Arweave 使用一种称为 blockweaves 的新型数据结构，它是对区块链原始设计的迭代更新。每个区块都链接到两个先前的区块：

- 链（类似于比特币等传统区块链）中的前一个区块；
- 来自区块链先前历史的一个区块（「recall 区块」）

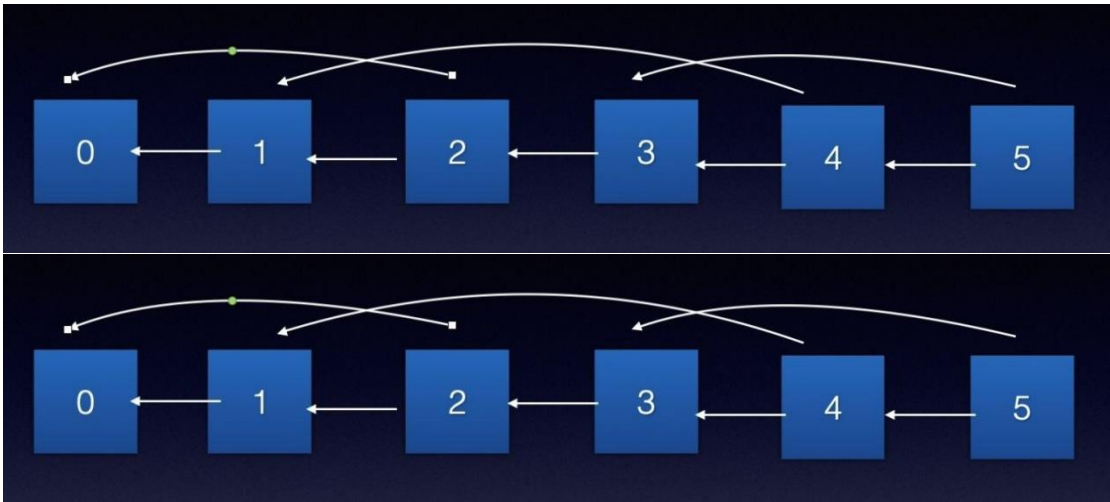
- 4.四大核心技术：Blockweave、访问证明（Proof of Access）、Wildfire、区块影子（Blockshadows）

- **Blockweave**



- **访问证明 POA**，典型的 PoW 系统只依赖上一个区块来生成每个连续的区块，而 PoA 算法则从之前的区块中随机选择一个区块（即“重调”区块），然后借助该区块的数据来生成新区块。一旦某个区块有较少节点存储那么拥有这个区块的节点获得记账权的概率就会变大，从而其他节点也来存储该区块。而如果按照均匀分布计算，某个区块丢失的概率为 $(1 - \text{平均每个节点存储的区块数} / \text{网络中所有区块})^{\text{网络中节点数}}$ ，由于网络中节点数不断增加，区块丢失概率非常之低。
- **Wildfire**，就是一种可以在去中心化网络中解决数据分享问题的系统，它使在网络中快速满足数据访问的请求成为参与挖矿的一个必要条件。Wildfire 的工作原理是在每一个节点本地创建一个排名系统，基于节点对网络请求的响应速度和从其它节点那里接收数据的速度来对节点进行排名，并根据这个排名来决定新区块和交易分发到节点的速度。节点之间按照它们的排名顺序来提供服务，表现不佳的节点将会列入全网的黑名单。节点们受到经济上的激励，在彼此的排名中保持良好的排名，于是它们就可以花最多的时间进行有效的挖矿。总而言之，Wildfire 系统确保了新区块的快速分发，并以低延迟保持了数据的可用性。
- **Blockshadows**，在传统的区块链系统中，当挖掘一个新块时，无论一个节点已经拥有多少块数据，每个完整的块都会分配到网络中的每个节点。这不仅浪费大量数据，而且极大地降低了网络就块达成共识的速度。为了促进安全的去中心化、快速的区块共识和高吞吐量，Arweave 引入了一个新概念——Blockshadows。区块影子不是在交易期间广播一个完整的区块，而是传输一个由接收节点重建的“影子”。区块影子不包含块内的交易列表，而是仅包含交易哈希列表。使用这种本质化的变体，任何拥有完整交易列表、钱包和哈希列表的节点都可以复制完整的区块。

生成新块



1. 当前末尾区块是区块 5，节点 A 存储了区块 2 和 3
2. 生成区块 6 的需要携带区块 2 的数据，节点 A 进行 POW
3. 通过比拼节点 A POW 竞争中胜出，获得记账权
4. 节点 A 打包事务并按照规定存入区块 2 的部分数据，整体打包生成新的区块
5. 节点 A 将新的区块和 recall block 广播给其他节点
6. 其他节点验证新的区块是否有效，有效包含区块的随机数符合 POW 以及区块中是否包含 recall block 的部分数据。

Arweave vs Filecoin

	Arweave	Filecoin
目标	实现永久存储	充分利用存储提供商的存储空间以降低存储价格

冗余性	由 blockweave 结构和 POA 激励保证数据的冗余性以达到数据冗余	未支持冗余性，需要存储者主动向不同存储提供商存储多次以达到冗余。
有效期	一次付费永久存储	需要和存储提供商商议存储时长
存储位置	链上存储	链下存储，通过复制证明和时空证明不断验证
容量	较大	没有冗余，理论上存储容量要大于 Arweave
分发	arweave 的分发是基于 http 并增加了 wildfire 系统能够有较为稳定的体验。	filecoin 本身的查询检索非常缓慢，通常都需要和 ipfs 搭配使用。而 ipfs 和网络中各个节点有关，理论上是可以达到比 http 更好的体验，但就目前看还有不小差距。

SmartWeave

SmartWeave 是 Arweave 的智能合约平台，其机制是在链下执行合约调用，然后将状态存储在 Arweave 中，有点像 layer2。SmartWeave 并不需要发布者证明其发布的状态正确性，而是采用惰性评估，即每次合约调用者在调用合约的时候，需要将合约相关的交易全部执行一次进行状态转移。相当于将状态的正确性交由下一次合约的调用者来验证。这种方式极大地释放了链上计算量，使得 SmartWeave TPS (吞吐量)大幅优于其他 L1 链。

生态



















everPay, 支付+DEX, everPay 协议目前支持 Ethereum 和 Arweave, 也支持 Arweave 利润分享代币 (PSTs)。

ArDrive, AR 上的 Dropbox

KYVE, 区块链存储中间件

- 解决 Arweave 扩容问题
- 通过标准化框架上传和验证数据
- 实现数据跨链存储

Web3 index

#	Network	Blockchain	30d Fees ⓘ		90d Fees ⓘ		30d Trend ⓘ
			Explicit ∨	Implicit	Explicit	Implicit	
1	 Arweave (AR)	Arweave	\$54,842	\$0	\$206,963	\$0	 ▼ -21.06%
2	 Storj (STORJ)	Ethereum	\$34,695	\$0	\$64,599	\$0	 ▲ 206.54%
3	 Livepeer (LPT)	Ethereum	\$30,994	\$0	\$73,934	\$0	 ▲ 51.09%
4	 The Graph (GRT)	Ethereum	\$19,050	\$0	\$84,682	\$0	 ▼ -29.05%
5	 Sia (SC)	Sia	\$12,799	\$0	\$29,341	\$0	 ▲ 42.31%
6	 Akash (AKT)	Akash	\$2,869	\$0	\$9,268	\$0	 ▼ -31.82%
7	 Helium (HNT)	Helium	\$1,580	\$0	\$11,309	\$0	 ▼ -26.18%
8	 Pocket (POKT)	Pocket	\$0 ⓘ	\$415,105 ⓘ	\$0 ⓘ	\$2,733,977 ⓘ	 ▼ -57.02%

SCP (Storage-based Consensus Paradigm)

基于存储共识的设计范式是由 everFinance 的 Founder outprog 所提出的，灵感来源于 Arweave 的 SmartWeave 以及以太坊的二层 Rollup。在 everPay 的白皮书中这样描述它：以太坊中，计算会被区块链网络中的所有节点执行，所有节点都会生成和存储全局状态以供查询。不同于以太坊模型，SCP 分离了计算和存储，区块链不进行任何计算仅进行数据存储，所有计算由链下的用户客户端或服务器执行，生成的状态也由链下客户端或服务进行保存。SCP 使用了链下智能合约，智能合约可以使用任何的语言进行编写，这些程序的所有输入参数都来自存储型区块链。在范式中，区块链更像是计算机的硬盘，链下智能合约可以在任何具备计算能力的机器上进行。

简而言之，SCP 就是用比特币或者 Arweave 来存储状态的结果，或者再存储链外智能合约的内容，来保证存储的可信，实现一个与底层区块链分层的高性能 Layer2 网络。这里所说的 Layer2 实际上可以算是 Layer1，因为比特币或 Arweave 链上是没有智能合约运算能力的，它们可以说是更底层的 Layer0。

Outprog:

<https://mirror.xyz/0xDc19464589c1cfdD10AEdcC1d09336622b282652/5pujoWWTtETICrInwhsceEhMOkpJmjYNfFXhkLGI BJA>

与 Solana 达成深度合作

Arweave 和 Solana 合作推出了 SOLAR Bridge，使 Solana 能够在 Arweave 的永久网络上存储数据。据估计，Solana 每年产生多达 4 PB 的数据。此外，Arweave 正在为可与业内其他区块链互操作的分散存储选项铺平道路。而成为了 Solana 官方御用的存储方案，Arweave 拥有着跟 Solana 代币价格非常相似的增长趋势。



代币分配

总量 6600 万，流通 3400 万左右，矿工们在 Arweave 中有两个收入来源:1) 网络手续费；2) 区块奖励。区块奖励遵循算法设计呈下降趋势，不受外部因素的影响。手续费主要来源于用户的一次性付费，每一笔用户付费中至多有 14% 会直接分给矿工，并加入流通量。另一部分 (~86%) 将进入捐赠池。

出块奖励目前 2/block，挖矿通胀率不到 1%，出块奖励略低。

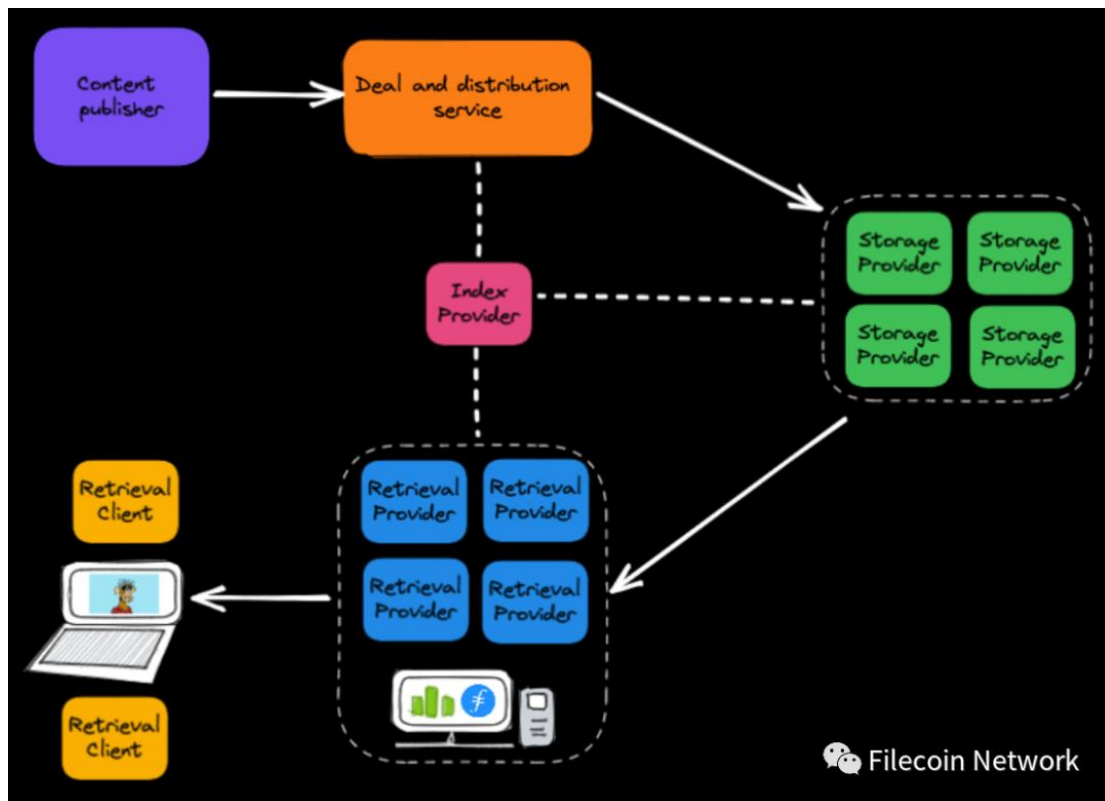
总结

- 1.Arweave 致力于链上永久存储，与 filecoin 是差异化的，目前在 sol 生态已经有较多应用，是相对有落地场景的应用；
- 2.Blockweave, Smartweave 等诸多创新，能否有效落地还需观察，但值得跟进；
- 3.目前节点较少，挖矿奖励很低，猜测中心化程度较高；
- 4.生态应用已经比较丰富，项目方比较佛系，关注 Smartweave 落地，兼容 EVM 等；

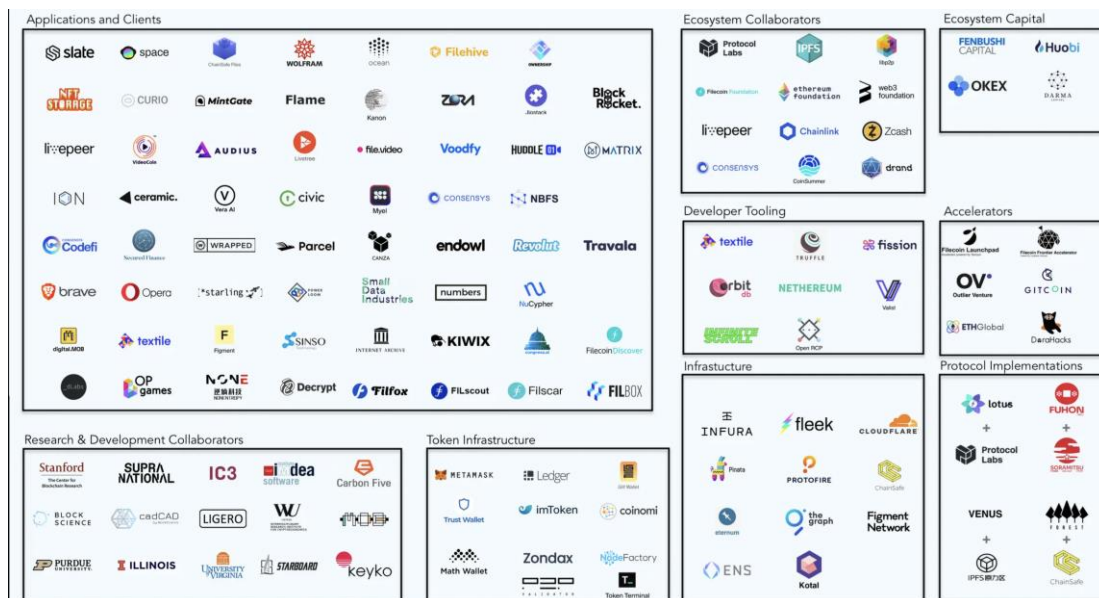
Filecoin

基本情况

1. 基于 IPFS 成立协议实验室，诞生于 2015 年，2017 年以 filecoin 做了公募。
2. 团队。IPFS 的团队是 Protocol Lab 团队，JUAN BENET，IPFS 创始人，斯坦福大学博士，Protocol Lab 协议实验室负责人。NICOLA GRECO，Protocol Labs 核心成员。MATT ZUMWALT，Protocol Labs 核心成员。
3. Http vs IPFS。位置寻址 vs 内容寻址，Http 会 404，高度中心化，重复下载浪费带宽。IPFS 分布式，但是缺乏激励。
4. IPFS 和 Filecoin 的关系。IPFS 只是一个协议，Filecoin 是一个区块链存储方案，使用了 IPFS 协议来运行系统。Filecoin 和 IPFS 协议都是由 Protocol Labs(协议实验室)开发维护。
5. 在 Filecoin 中有 3 组用户：客户、存储矿工以及检索矿工。



生态展示



代币分配

Token 持有详情

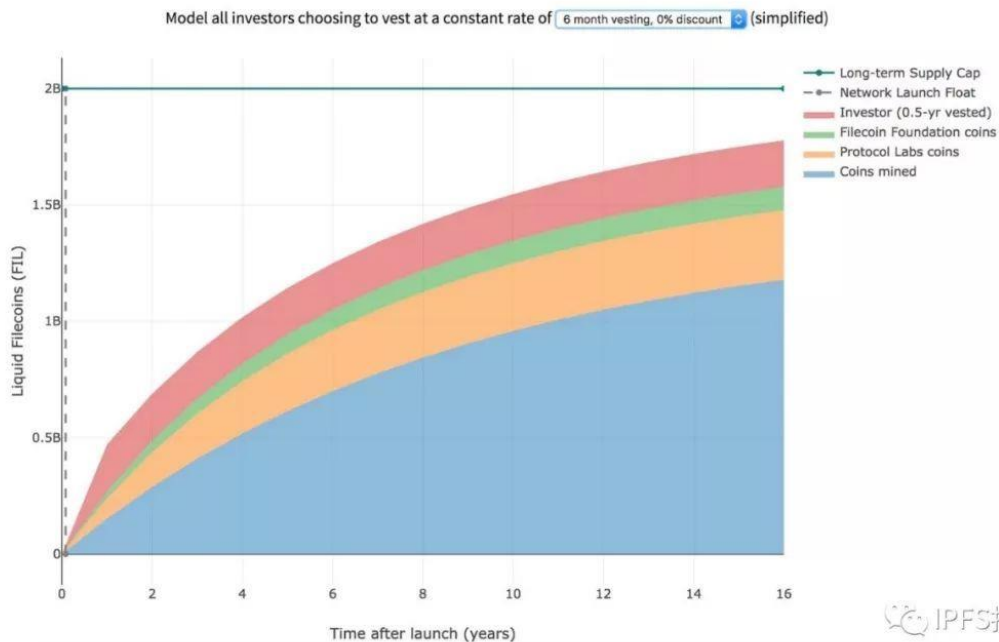
- 矿工：70%
- 协议实验室：15%

- 投资者：10%（公募+私募）
- Filecoin 基金会：5%

Token 分发详情

- 开始时间：Filecoin 网络上线开始算时间，例如：6 个月分发期(vesting period)，网络上线后 6 个月内发放完毕
- 投资者（爱西欧）：1 年最低分发期（私募），6 个月最低分发期（公募）
- 协议实验室：6 年，线性释放
- Filecoin 基金会：6 年，线性释放
- 矿工：6 年分发一半

Coin Supply



IPFS指南

现状

Filecoin 目前主要还是垃圾数据挖矿阶段，并没有实现有效数据的链上撮合，检索和可读功能。主要有几个难点：1) filecoin 链本身性能低下（tps 20）无法做链上撮合只能链下撮合；2) 为了防止生成攻击和外包攻击，必须对存储数据做多重加密，导致数据不可直接读取。

链上计算空间被大量的矿工交易占据，百分之 80 左右的消息，都是扇区的密封，证明等消息，留给 fvm 空间很小。目前 Filecoin 存储只能达到传统冷存储的性能标准。为了获得与其他热存储解决方案相同的性能，目前大多数用户将 Filecoin 和 IPFS 缓存结合在一起。一起使用。这些混合的多层存储解决方案使用 IPFS 进行热存储，并使用 Filecoin 进行可负担的，频繁的和版本化的备份，这可以实现与传统热存储相当的检索性能，同时更安全，更便宜。当前有混合存储产品，包括 Powergate 和 Textile Buckets。

Filecoin Plus

认证客户端，经过“公证人”认证的 datacap，区块奖励提高到 10 倍，以此激励客户和存储提供商在 Filecoin 上存储真实数据。Filecoin Plus 产生了立竿见影的影响。实际数据日增量从 2021 年 9 月的 457 TiB (1 PiB = 1024 TiB)增长到 2022 年 6 月的 100 PiB 以上。总算力 100EiB。

web3.storage

项目方搞了个网站，用户可以把数据上传到这里，数据会被存储到 IPFS 的节点中，再备份到 filecoin 网络中，备份这些数据的矿工可以获得 10 倍算力。有效数据的分发机制不明确。

NFT.storage

原理差不多，专为 NFT 设计

2022 路线图

第一个是核心协议增强部分，第一季度是快速交易升级与 CC 扇区的可验证用户数据无需重新密封，现在存在 FIL 上面的东西，叫做存储空间承诺。存放的 CC 数据属于垃圾数据，没有太大作用，而现在我们要存真实有效的数据进来，得把这些 CC 的数据全倒掉，然后再把有效数据全装进来，通过快速交易到底可以用一些算法把有效的数据往这些 CC 数据上面覆盖，变成有效数据了，用这种方式的话节约大量的时间及成本。

第二个是 Filecoin 的虚拟机，WASM 同时兼容 EVM，以后 Filecoin 上面的虚拟机是可以直接兼容运行以太坊的虚拟机。以太坊上面写的智能合约搬到 FIL 上面来可以直接运行，也就是说以太坊以后能做的事情 FIL 都能做。FIL 不仅能在以太坊能做的基础上，还能给它提供安全有效的存储。

第二季度第一个是引入递归证明。所谓递归证明就是把验证结果进行多次的压缩，让每次上链的这个消息缩小再缩小，这样一个区块就能承载更多的信息，可以提升 TPS。第二个工作是检索市场，实现部分数据的下载功能。第三个虚拟机的自定义智能合约，之前官方就已经上传了一个虚拟机的初阶版本，但是初阶版本里面还没开放可以自定义的权限，像计算证明、存储证明、时空证明这一类，在没有上传虚拟机之前，大家要去调用这些功能，都是从 Filecoin 这个项目库里面去直接调用这些功能，这就相当于要计算时找一个计算器来进行使用。而现在上传了一个初期的虚拟机的自定义智能合约，相当于拥有了一个电脑，不仅可以在电脑上面去运行计算器了，还可以在上面创造更多各种各样的程序来使用。

总结

- 1.Filecoin 目前还比较早期，处于基本不可用状态，基本当做矿币；
- 2.每天产出 28w，全年通胀 38%；
- 3.FVM 有一定意义，但是主链性能低可做的事情不多，需要尽快解决数据可读性、检索市场和主链性能问题；
- 4.时空证明+零知识证明对链下存储的验证，是独创发明，价值比较大，看未来是否有项目借鉴。
- 5.协议实验室对 gas 的设计、

Storj

老项目，半中心化的，通过一个桥来传输文件，分发给分布式节点，只能算作分布式存储而不是去中心存储。

Ceramic

链上动态文件存储系统，Ceramic 的核心功能是从存储协议上的静态和不可变数据中获取可变的动态数据。这一点至关重要，因为用户数据（尤其是社交数据）是高度动态的。

web3 社交，DID

Crust

Crust 属于 Polkadot 平行链，背后用的 ipfs 做的存储，抄袭了时空证明，没有实现零知识证明，只用了隐私计算。质押的越多奖励越多。

Chia

BitTorrent 的发明者 Bram Cohen 创建，写入垃圾数据挖矿，消耗 SSD，纯矿币。

ZeroNet

zeronet 是一个利用 bt 加密技术和比特币技术开发的去中心化网络，分布式网站，非区块链，无激励，但可用，体验良好。

总结

去中心存储有三个主要价值的方向：1) 链下存储；2) 链上永久存储；3) 链上动态存储，数据库。

目前看起来 Arweave 运行良好，但是缺点是节点少去中心化程度低，不兼容 EVM。Filecoin 独创了时空证明+零知识证明验证链下存储，但是链性能还需提高，数据无法读取只能作为冷备份。

假如有一个链，一方面是 Arweave 的链上存储，利用 smartweave 和时空证明扩展链下存储，再兼容 EVM 就比较完美。

投资角度，file 暂时通胀太严重，矿工大量质押等着卖，不建议。Arweave 和 Ceramic 值得跟踪。