

## Arweave

# 为永存网络（**Permaweb**）提供动力的区块链

### Arweave 概览

Arweave 是一种去中心化的数据存储协议，可提供永久、可拓展的链上储存。如果说以太坊是世界计算机，那么 Arweave 就是永久不会忘记的硬盘。Arweave 结合了多种新颖的区块链技术，巧妙地通过设计一个博弈论场，来创建健康、可持续的网络。

### 激励矿工永久存储数据的机制

Arweave 使用一种名为区块纺（blockweave）的新型数据结构，改变了区块链存储的工作方式。矿工无需存储整条区块链 - 在该数据结构中，每个新区块都只需要连接到两个先前的区块：

- 链中的前一个区块（和比特币等传统区块链一样）
- 来自区块链先前历史的区块（“回忆区块”）

该协议采用“随机访问的简洁证明”（Succinct Proofs of Random Access，简称 [SPoRA](#)）机制。所有的矿工在添加新区块之前，必须访问一个“回忆区块”，才能够获得奖励。由于回忆区块是随机选择的，无法预测，因此矿工存储的数据越多，访问到正确的回忆区块、获得奖励的机率就越大。这种机制还鼓励矿工存储稀有区块，避免了只有一部分数据被广泛复制的情况，因为存储了稀有区块的矿工，更有希望在未来该区块被选择为回忆区块时，获得奖励。

王坚

[jian.wang@ambergroup.io](mailto:jian.wang@ambergroup.io)

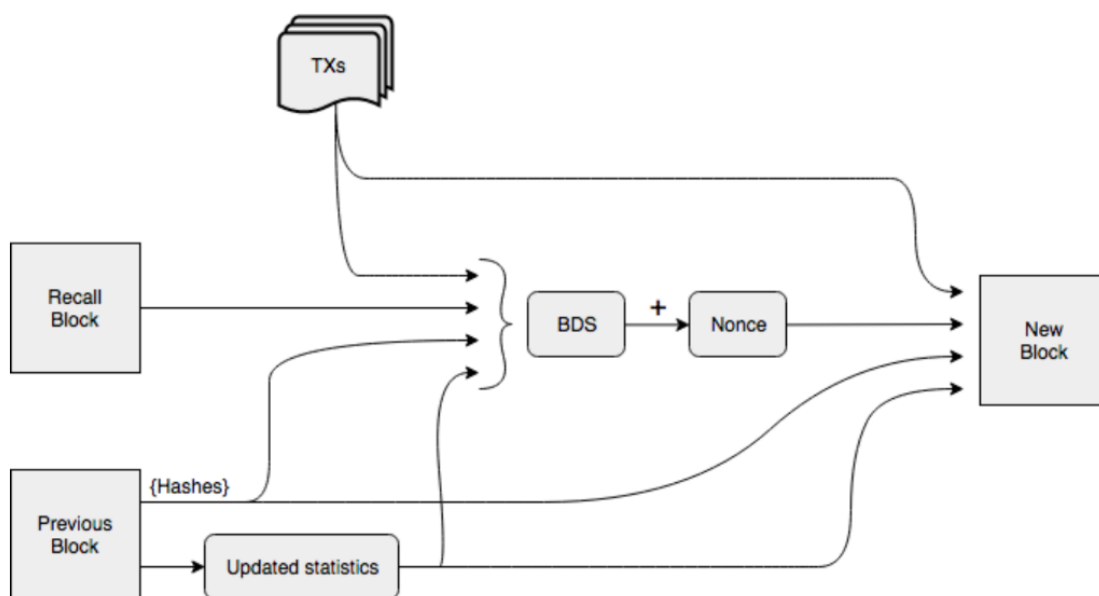
史德洋

[steven.shi@ambergroup.io](mailto:steven.shi@ambergroup.io)

张弛斌

[chibin.zhang@ambergroup.io](mailto:chibin.zhang@ambergroup.io)

## Arweave 区块建设

来源: [Arweave Yellow Paper](#)

矿工获得奖励的概率 = 拥有回忆区块 (历史数据) 的概率 x 第一个找到 hash 的概率

Arweave 通过博弈论的原理, 激励矿工优先存储稀有区块, 使得丢失区块的可能性几乎为零, 从而确保了数据的可复制性, 实现永久储存。同时, 与 PoA 不同的是, Arweave 的 SPOA 机制提高了数据检索速度的权重, 以给用本地硬件的矿工更多奖励的方式, 实现去中心化。

## 丢块概率敏感度表

		复制率(%)								
		20%	30%	40%	50%	60%	70%	80%	90%	100%
节点	50	1.4 E-05	1.8 E-08	8.1 E-12	8.9 E-16	1.3 E-20	7.2 E-27	1.1 E-35	1.0 E-50	0.0 E+00
	100	2.0 E-10	3.2 E-16	6.5 E-23	7.9 E-31	1.6 E-40	5.2 E-53	1.3 E-70	1.0 E-100	0.0 E+00
	150	2.9 E-15	5.8 E-24	5.3 E-34	7.0 E-46	2.0 E-60	3.7 E-79	1.4 E-105	1.0 E-150	0.0 E+00
	200	4.1 E-20	1.0 E-31	4.3 E-45	6.2 E-61	2.6 E-80	2.7 E-105	1.6 E-140	1.0 E-200	0.0 E+00
	250	5.9 E-25	1.9 E-39	3.4 E-56	5.5 E-76	3.3 E-100	1.9 E-131	1.8 E-175	1.0 E-250	0.0 E+00
	300	8.5 E-30	3.4 E-47	2.8 E-67	4.9 E-91	4.1 E-120	1.4 E-157	2.0 E-210	1.0 E-300	0.0 E+00
	350	1.2 E-34	6.1 E-55	2.3 E-78	4.4 E-106	5.3 E-140	9.8 E-184	2.3 E-245	0.0 E+00	0.0 E+00
	400	1.7 E-39	1.1 E-62	1.8 E-89	3.9 E-121	6.7 E-160	7.1 E-210	2.6 E-280	0.0 E+00	0.0 E+00

来源: Amber Group

蓝色高亮接近当前的网络状态。请注意, 以上的数字为假设的矿工随机储存区块, 因为矿工会被激励去存储更稀有的区块, 所以掉落区块的实际概率将低于所反映的。

## 一次付款，永久保存

用户仅支付一次费用，就能将数据永久存储在 Arweave 上（至少 200 年）。这与 Web2 或 Web3 上的一些存储平台（例如 Amazon Web Services、Google Cloud 或 Filecoin）形成鲜明对比。在这些平台中，用户常常会被重复计费。并且，使用即用即付订阅的客户可能会受价格上涨和条款变化的影响，而 Arweave 的用户支付完存储费，后续访问数据都是免费的。我们相信 Arweave 的模型，可以为客户提供一种完全不同的、更适合 Web3 的体验。

所有的用户都必须支付交易费，但是最多只有 14% 的交易费用才会立即转给矿工。其中，约 86% 会进入捐赠池。捐赠池的资金会随着时间的推移，逐渐发送给矿工，用来覆盖挖矿成本，以确保可持续的矿工经济（以及永久存储）。目前，捐赠池仍在积累资金。预计在 Arweave 的永存网络扩张几倍之前，都不会发放补贴给矿工。

Arweave 的价格机制和经济学中的禀赋模型类似。用户在购买永久存储服务的时候，必须支付一笔 AR 币。随着时间的推移，这笔 AR 币会不断地积累利息，并用来支付给那些提供硬盘空间的矿工。由于存储价格一直在不断下降（在过去的 50 年里，存储成本的年下降率高达 30.6%），AR 币的购买力相较而言就会上升，并确保用户的数据能够保存 200 年以上。此外，Arweave 的定价模型对于存储价格的估计相当保守（[预估存储成本每年仅下降 0.5%](#)），更使得捐赠池模型的长期可持续性得到了保障。

数据密度和存储价格成反比 - 数据密度越高，存储成本越低。事实上，数据密度从 50 年前开始就一直在以 15% 至 50%（年均 30%）的速度增长，而这意味着 Arweave 仅追加的硬盘容量就将增长 15% 至 50%。因此，即使是以当前的速度，理论上，Arweave 至少也需要 400 多年才会达到理论极限。也就是说，Arweave 有几个世纪的时间，用科技进步来解决这一问题。

## 借鉴经过市场验证的的博弈论策略

于 2001 年问世的 BitTorrent，是世界上最大的 P2P 文件共享协议，一度占全球互联网流量的 60% 以上。它的成功很大程度上归功于一种称为“以牙还牙”（Tit-for-Tat）的博弈论策略：在多轮囚徒困境的情况下，BitTorrent 节点在初始时，会乐观地与其他节点合作，但是也会报复连续多轮不合作的节点。同时，为了避免陷入彼此永无止境互相报复的怪圈，随机地选择一个之前不合作的节点，释放友好信号。

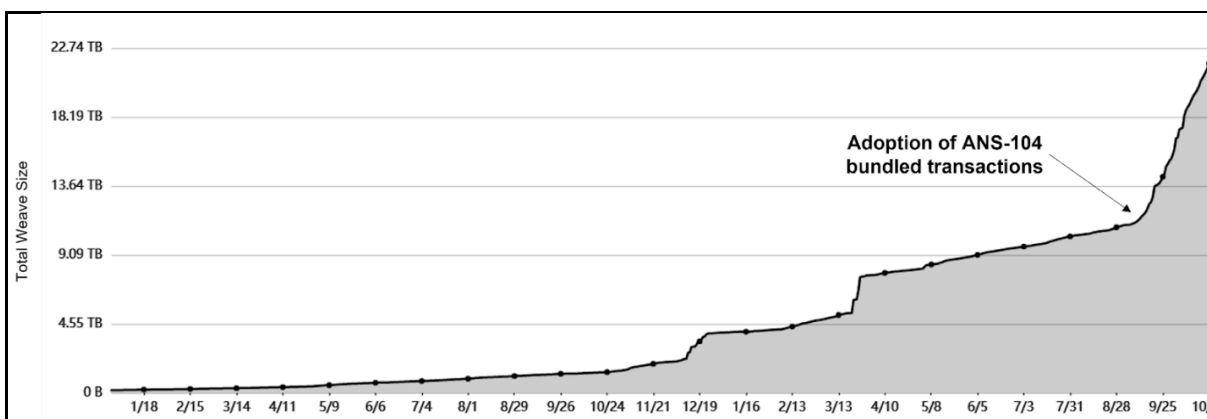
Arweave 借鉴了这个经过验证的框架，其网络中的每个矿工都会根据一个专有算法对其他节点进行排名，并根据这个排名来决定稀缺资源的分配方式。为了获得更好的资源，节点们就会有动力以友好的方式来对待其他节点，使得自己的排名靠前。因此，Arweave 具有很强的弹性和适应新环境的能力。

例如，今年 3 月，Arweave 侦测到有一部分矿工使用不利于数据复制最大化的池化软件（pooling software）。[其他矿工对此修改了他们的排名算法，降低这部分矿工的优先级](#)，阻止了只收钱不办事的行为，从而改善整体网络的健康状况。

## 捆绑 (Bundles)：释放可扩展性

今年 9 月，Arweave 发布了第二层有效扩展解决方案：[Bundles](#)。每笔 Arweave 交易都会被移出链，与其他交易捆绑后，作为一个交易组放回主链。也因如此，超大的数据文件可以很容易地被上传到 Arweave 的网络。9 月，[有一个单块上传了 47GB 的数据](#)。同时，捆绑还提高了交易的确定性，改善了开发人员的体验。捆绑的发布推动区块的大小实现阶梯式增长，这表明用户和开发人员之间产生了强烈的共鸣。

### 捆绑销售带来的快速增长



来源: Viewblock

## 市场格局

Arweave 常常被拿来与著名的去中心化存储平台 Filecoin 比较。



Filecoin 由 [Protocol Labs](#) 于 2014 年创立。而 Protocol Labs 也是星际文件系统 (IPFS) 的幕后团队。IPFS 是基于内容寻址的去中心化存储技术协议。与中心化网络根据服务器位置来定位不

同, IPFS 通过数据内容寻址。通过一些内容标识符, 用户可以彼此之间共享文件。Filecoin 则充当 IPFS 的经济层, 用来激励节点托管 IPFS 数据。

Arweave 和 Filecoin 之间的经济模型在很多方面都不同。Filecoin 采用即用即付模式, 与 AWS 和 Google Cloud 非常相似。并且与 Arweave 不同的是, Filecoin 主要提供临时存储解决方案而不是永久解决方案。

此外, 在 Filecoin 的协议中, 用户和节点之间有数千种不同的合约, 每一种都有不同的存储条款 (例如价格、持续时间、复制次数等)。相比之下, Arweave 就只有一种合约: 数据永久保存。

### Arweave 与 Filecoin 经济模型的差异

		
经济模式	一次付款, 永久保存	按次计费 <ul style="list-style-type: none"> <li>- 存储一次性支付</li> <li>- 未来按每次检索请求支付</li> </ul>
数据复制	SPoRA: 矿工需要证明之前区块的访问权限(随机生成的)来开采新的区块	复制证明: 节点证明数据在存储处理后已被复制到专用存储空间上 时空证明: 验证者持续检查节点在一段时间内存储数据
合约方式	一种在用户和协议之间永久存储数据的合约	数千个不同的存储合同, 在价格、持续时间、复制等方面有不同的条款
数据存储	矿工将选择存储哪个数据; 被激励去存储更多和更稀有的数据	合同规定的存储数据的内容
竞争品/替代品	IPFS	Web2: 亚马逊网站服务, 谷歌云, 阿里巴巴云等 Web3: Sia, Storj, Swarm, SAFE

因此, 我们不认为 Arweave 会直接与 Filecoin (以及其它类似的协议) 竞争。甚至, 我们还认为他们的解决方案可能还可以互补。在某些情况下, 一次性付费来永久存储会更划算; 而在其他情况下, 为短期存储付费更有意义。

事实上, 很难找到另一个与 Arweave 价值主张类似的平台。IPFS 最接近, 但如果没有经济激励, 文件就会从 IPFS 的网络中删除。例如, Infura 的 IPFS 固定服务 [会删除六个月内未访问的用户的数据](#)。

**Arweave, Filecoin 与 Sia 三者的对比**

	Arweave	Filecoin	Sia
代币符号	AR	FIL	SC
主网发行	18 年 6 月	20 年 10 月	15 年 6 月
付款	One-Time	Contract-based	Contract-based
已募集 (US\$)	22mn	257mn	9.6mn
网络规模(TB)	21	34,680	1,920
节点数量	362	700	664
价格 (US\$)	51.23	63.81	0.01813
流通供应(mn)	50	114	49,133
市值 (US\$mn)	2,567	7,295	891
30 天 收益 (US\$)	220,457	29,563	277
根据 30 天收益推算的年收入	957	20,283	264,753

来源: Web3 Index, Viewblock, Siastats, Filecoin, Chronobot, CoinGecko 网站的新闻稿

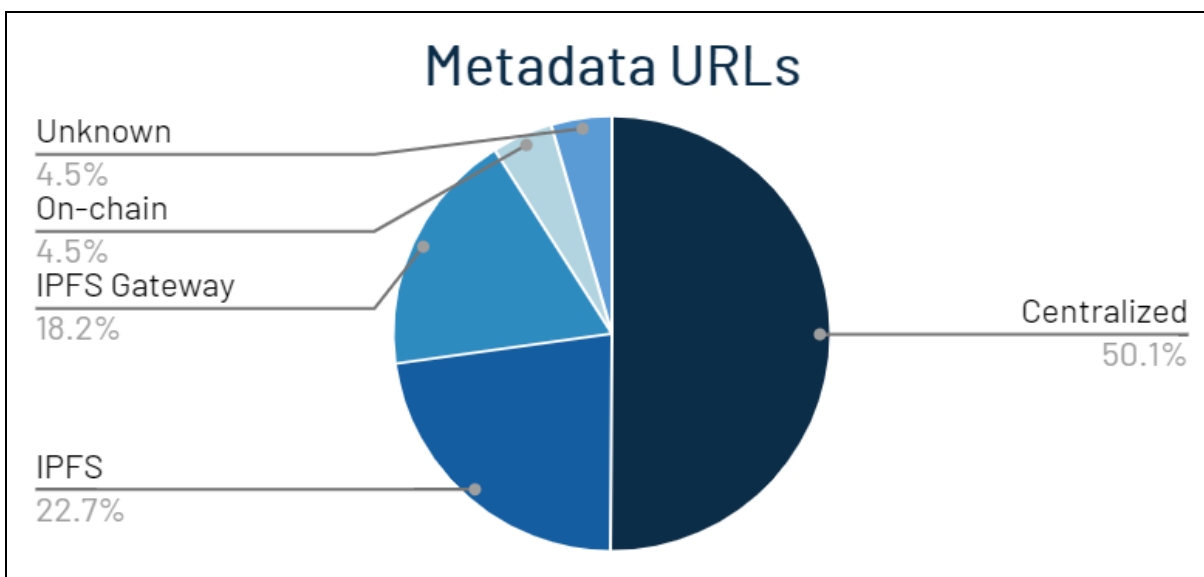
## Web3 堆栈中的用例

Arweave 在主网启动时增长缓慢，但今年却凭借着 web3 应用程序，获得了显著的市场吸引力。下面，我们会概述一些例子，来展示 Arweave 是如何找到市场契合点，并介绍 PermaWeb 带来的独特机遇。

### 为 NFT 提供安全性

NFT 的购买者常以为 NFT 是永久且不可变的。然而，由于基本上没有 NFT 是完全储存在区块链上的 - 大多数 NFT 都只是将实际内容存储在一个简单的令牌 URI 中，再指向数字对象实际所在的互联网地址。对于大多数 NFT 项目来说，链上存储的成本高得令人望而却步。

这其中有一个重要的问题：大多数 URI 不能保证永久性或不变性。例如，World of Women NFT 项目 [将图像文件存储在 Amazon Web Services 上](#)，以便将来更改和删除这些文件。然而，[@pencilflip](#) 在对前 22 个 NFT 项目调查时发现，50% 的项目将他们的文件存储在中央服务器上。

**50% 的顶级 NFT 项目托管在中央服务器上**

来源: Pencilflip

即使是 IPFS 也不能保证永久性。比如, CheckMyNFT 就发现过一些托管在 IPFS 上的[蓝筹艺术家的资产](#)发生过短暂离线的情况 (涉及包括 Grimes、Deadmau5 和 Steve Aoki)。再比如, nft.storage 曾宣称可以将数据“无限期地存在于 IPFS 网络中”。但是, 其[服务条款](#)又规定, “数据将无限期地继续存留, 直到 Protocol Labs 决定结束 [NFT.storage 项目](#)为止。”

由于这个问题越来越突出, 包括 Beeple 和 Jay-Z 在内的艺术家们开始更多地使用 Arweave 的 NFT 存储平台。

“这个 NFT 的持久性被评为优秀。与此 NFT 相关联的元数据高于当前的行业标准。它的元数据存储智能合约中, 并且符合被各个 NFT 平台采用的以太坊改进提案 (EIP) 中的所有标准。与此 NFT 相关的媒体数据存储在最强大的分布式文件存储系统 Arweave 上。”

- 来自苏富比关于 Jay-Z 的第一个 NFT [《王位继承人》](#) 的状况报告

除图像之外, Mirror (文本型 NFT) 和 Pianity (音频 NFT) 等媒体平台也将文件托管在 Arweave 上。由于 Arweave 可以提供去中心化的永久性和不变性, 我们预计它将在 NFT 和创作者经济中继续增长。



## 用户界面 - 中心化的隐藏点

DeFi 的爆炸式增长说明，可以通过为用户提供自由自主访问、且透明的平台，来解锁创新的数量密码。然而，这些平台面临着一个隐藏的中心化风险：前端用户界面。云服务提供商具有停止和审查 DApp 的权利，即使大多数用户更喜欢旧版本，开发人员也可以强制前端“更新”。

这已经是发生过的事了。今年 7 月，Uniswap 出于对美国监管的担忧，从其前端删除了代币化股票。尽管用户的智能合约存还在，开发人员仍然想把它隐藏起来。作为回应，[用户在 Arweave 上上传了 Uniswap 审查之前、允许用户访问的 UI](#)。而其他平台，诸如 [Sushiswap](#)、[Compound](#) 和 [linch](#) 也可以在永久网上使用，从而最大限度地减少了审查的威胁。

## 区块链存储

区块链是不断增长的电子记录列表。这些电子记录列表应该被永远保存，但很少有人愿意存储旧链数据。而随着区块链的发展，这个问题只会越来越严峻 - 尤其对于像 Solana 这样的高性能区块链来说。

目前，Solana 的区块数量是以太坊、比特币、Polkadot、Algorand 和 Cosmos 的区块数量总和的两倍多。

有趣的是，Solana 的开发人员并没有通过设计内部方案来解决这个问题，却转而寻求 Arweave 的技术支持。

*“构建高性能智能合约平台的挑战之一是，确保账本数据具有高度容错、分散的存储解决方案.....在多链未来，区块链应该变得越来越专业化，且可以互相操作。当一个完美的解决方案已经存在，并且比我们可以构建的任何东西在经济上更合理时，构建一个专用的存储网络、强加给验证者的负担，是没有意义的。”*

*- Anatoly Yakovenko, Solana Labs 的联合创始人*

除了 Solana 外，Arweave 还已经与 [Cosmos](#)、[Polkadot](#)、[Avalanche](#)、[NEAR](#) 和 [Skale](#) 合作。并且，区块链索引协议 Graph，[也将支持 Arweave](#)，从而允许用户更有效地访问存档的区块链数据。



## 其他用例

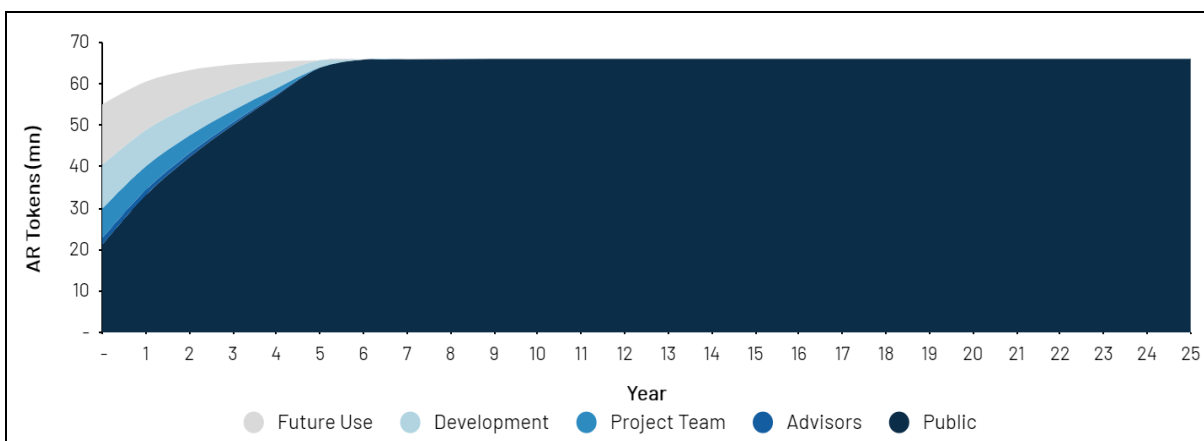
我们在上面只展示了几个例子，但 Arweave 的技术解决了几个 Web3 和现实世界的问题，例如[财务审计](#)、[媒体发布](#)和[信息存档](#)。此外，我们相信通过创造新的特性和功能，Arweave 的技术将创造新的市场和用例，扩大可用市场的总量。

## 代币经济学

Arweave 以 5500 万个 AR 币的创世供应量发布，其最大供应总量为 6,600 万 AR。新 AR 币的发行模型与比特币类似：发行的代币将定期减半。区别只是 Arweave 在持续不断地将发行率减半，而比特币是在某一特定时间点减半。

目前，Arweave 总共发行了约 6,400 万个 AR 币，其中，约 22% 由其顾问和项目团队持有，用于将来的使用 and 开发。这表明，目前代币持有者将会面临最多 24% 的稀释（22% 已释放的代币 + 2% 剩余生命周期的通货膨胀）。

**Arweave 代币供应计划**



来源: Arweave 黄皮书, Amber Group 预测

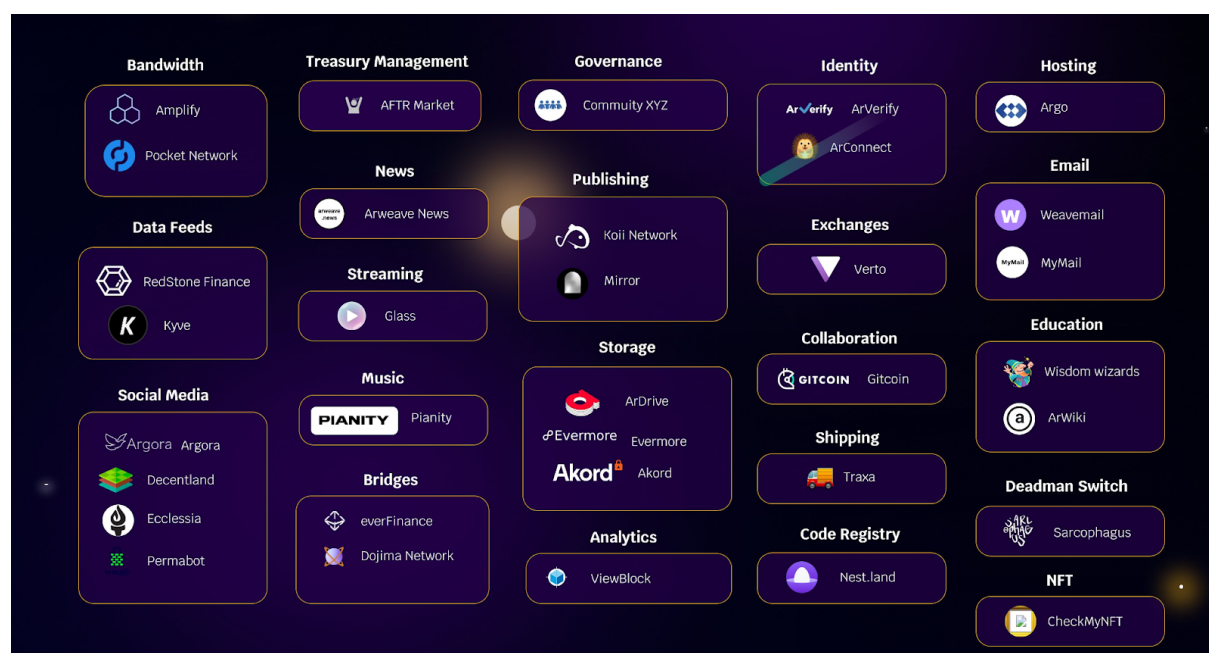
随着永存需求的增加，AR 币的价格预计会上涨。另外，由于大部分的交易费用被发送到捐赠池，AR 币也在不断退出公共流通。举个简单的例子，如果 Arweave 的总网络增长到 10PB，每 TB 的费用约为 200AR（当前成本约为 480AR/TB），那么将约有 170 万个代币退出公共流通。而这些代币最终还是会被重新引入流通（毕竟矿工需要将它们卖掉来支付存储成本），但这个重新流通的过程是随着时间的推移渐进发生的。

因此，AR 币的价格升值潜力来源于固定 AR 币产量下的永存需求增加，以及进入到捐赠池部分的交易费用。

## 结语

Arweave 团队通过全方位的思考，平地打造起一个永存网络。它引入了利润分享机制，使得应用程序开发者们可以在应用构建完成并启动时，通过出售代币来获取他们未来的部分利润。同时，Arweave 还定期举办 Open Web Foundry。这一项为期六周的计划，旨在帮助创业者将他们的想法在 Arweave 的平台上推向市场。所有这些都有助于 Arweave 生态系统的蓬勃发展。

### Arweave 生态 (2021 年 10 月)



来源: Verto 协议

当前，Arweave 还在早期阶段，还会面临各种风险和挑战。尽管如此，Arweave 是有无限潜力的。如果它成功的话，将会充当 Web3 应用程序的去中心化数据平台。它的愿景，是建立起一座真正永久的人类知识图书馆。

## 更多参考

- [Arweave.org](https://arweave.org): Arweave 官网
- Arweave [Medium](#)、[Twitter](#) 和 [Discord](#)
- [Arweave.news](#): 关于 Arweave 生态探索的社区新闻组织
- [Viewblock](#): Arweave 区块浏览器

## 免责声明

本报告中提及的知识产权归 Amber Global Limited（“Amber Group”）所有。未经 Amber Group 事先同意，任何数据都不允许未经授权的使用，包括但不限于复制，转发，传输或以其他方式呈现数据。Amber Group 对此处包含的内容或信息（“数据”），数据中的任何错误，不准确，遗漏或延误，或基于此的任何行为不承担任何责任及义务。在任何情况下，Amber Group 均不对因使用数据而产生任何特殊的、偶然的或间接的损害承担责任。

本报告不构成、也不应被视为 Amber Group 对购买或出售任何特定证券，金融工具或金融服务的要约。本报告中提供的分析具有一般性质，仅供参考。本报告不能构成作为提供任何适用或非适用的特定投资策略或投资组合的投资建议。本报告不会也不应被解释为就任何个人或实体“购买”、“出售”、“持有”特定投资是否适当提供任何建议。