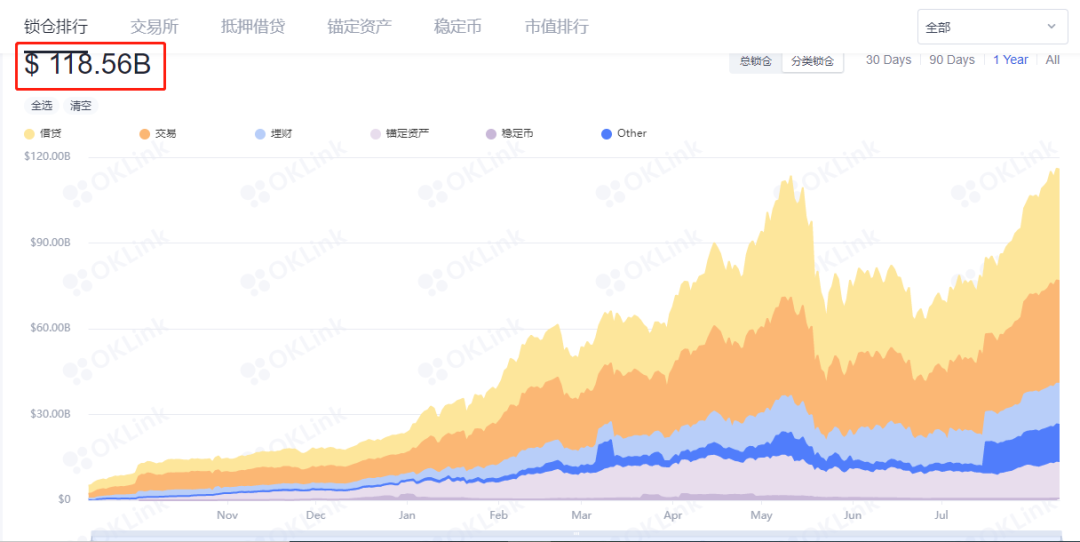
2021-11-12 16:41

**研报 | 深入解析以太坊2.0的最大受益者——Lido**

[[](https://www.defidaonews.com/writer/1056801)加密龙帅](https://www.defidaonews.com/writer/1056801)发布在[海盗号](javascript:;)

 15.6万

**在摩根大通的研究报告里，Staking被描述为400亿美元收入的市场，现在全球的Defi规模才刚刚达到1000亿美元TVL，这意味着以太坊的2.0升级，将在Staking市场再造1个Defi。**



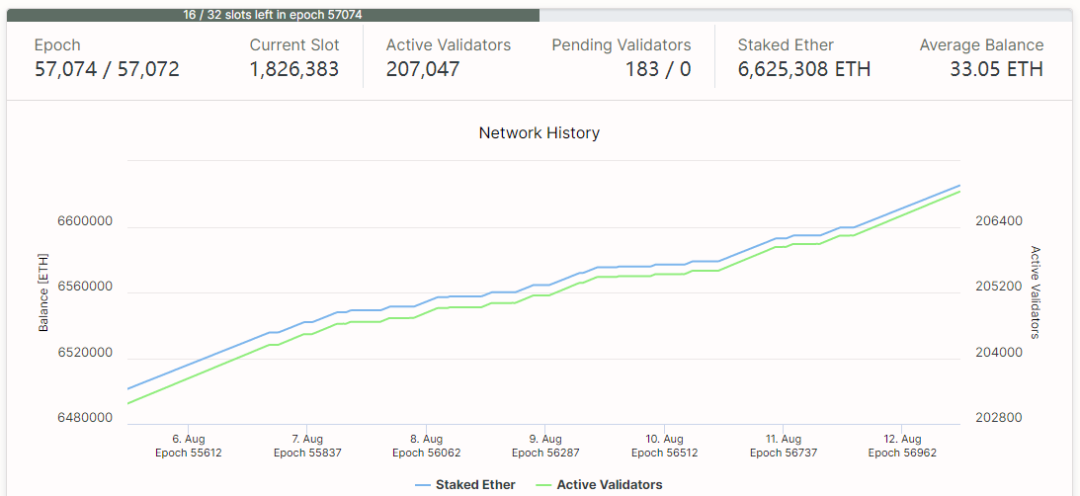
这是1个性感的领域，以太坊从POW转向POS正在加速这个行业。除了以太坊外，其他采用POS机制或者DPOS机制的公链也在成长，包括Polkadot、Tezos、Terra、Cosmos、Solana、Mina等，以太坊的改旗易帜，无疑会加强大众对于POS的信心。



来自摩根大通报告

一切都要从以太坊的信标链说起，在去年12月份以太坊启动了新的主网，宣告着以太坊正式向权益证明POS过渡。PoS 允许用户质押他们的 ETH ，和运行名为“验证者”的区块生成节点，从而保障整个网络的安全，并获得增发的ETH作为奖励。

POS网络上线8个月以后，已拥有超过20万个活跃验证者，网络中已经质押662万个ETH，几乎占ETH总流通量的6%。截至目前，Staking的年回报率约为6%。



这是以太坊历史中的一次大搬家，那些屯币党们，终于可以质押手中的ETH了。

**如何质押ETH2.0**

要单独质押，用户必须向ETH2存款合约存入32个ETH，**同时指定两个关键参数：**

**验证者公钥：**  
在入金前，用户需为其验证器生成密钥对。私钥用于在区块上签名，而公钥则作为其唯一的标识符。

**存入32个ETH的提现凭证：**  
一旦启用提现，本金（32个ETH）和质押奖励只能提现到该地址。

关键是，公钥和提款凭证不需要由同一实体控制。

之后，用户只需操作一个ETH2验证器节点，并在轮到他们时在区块上签名即可，不遵守协议是要受到惩罚的。



**由于限定条件的出现，质押者会遇到下面这些问题：**

* **早期质押的机会成本：**一旦质押了以太坊，在信标链启用转账功能之前，验证者都无法提出他们的以太坊。这意味着在未来的几个月甚至是几年里，参与质押都是一个单向的过程。
* **缺乏流动性：**在质押的过程中，用户不能转移、交易他们们的 ETH，也不能使用其 ETH 作为抵押品参与 DeFi 协议。无法从信标链中提出质押金，这个代价是尤其大的。
* **高资本要求：**用户质押的 ETH 数量只能是 32 及 32 的倍数，将数量较少或并非为32倍数的用户排除在门槛之外。
* **操作上的负担：**尽管以太坊核心开发者表示质押对硬件和正常运行时间的要求较低，但许多用户仍然偏向于提供资金，然后将运营工作外包给第三方。

**质押池的引入**

为了帮助解决上述问题， 引入了质押池的概念，即将用户的 ETH 集中起来，为他们提供质押服务，一如当年矿池的诞生，但门槛远比POW的矿池低。**这样处理带来了如下好处：**

**取消了以太坊的质押门槛**:任何数量的以太坊都被允许，不再有32最小额和32倍数的限制。

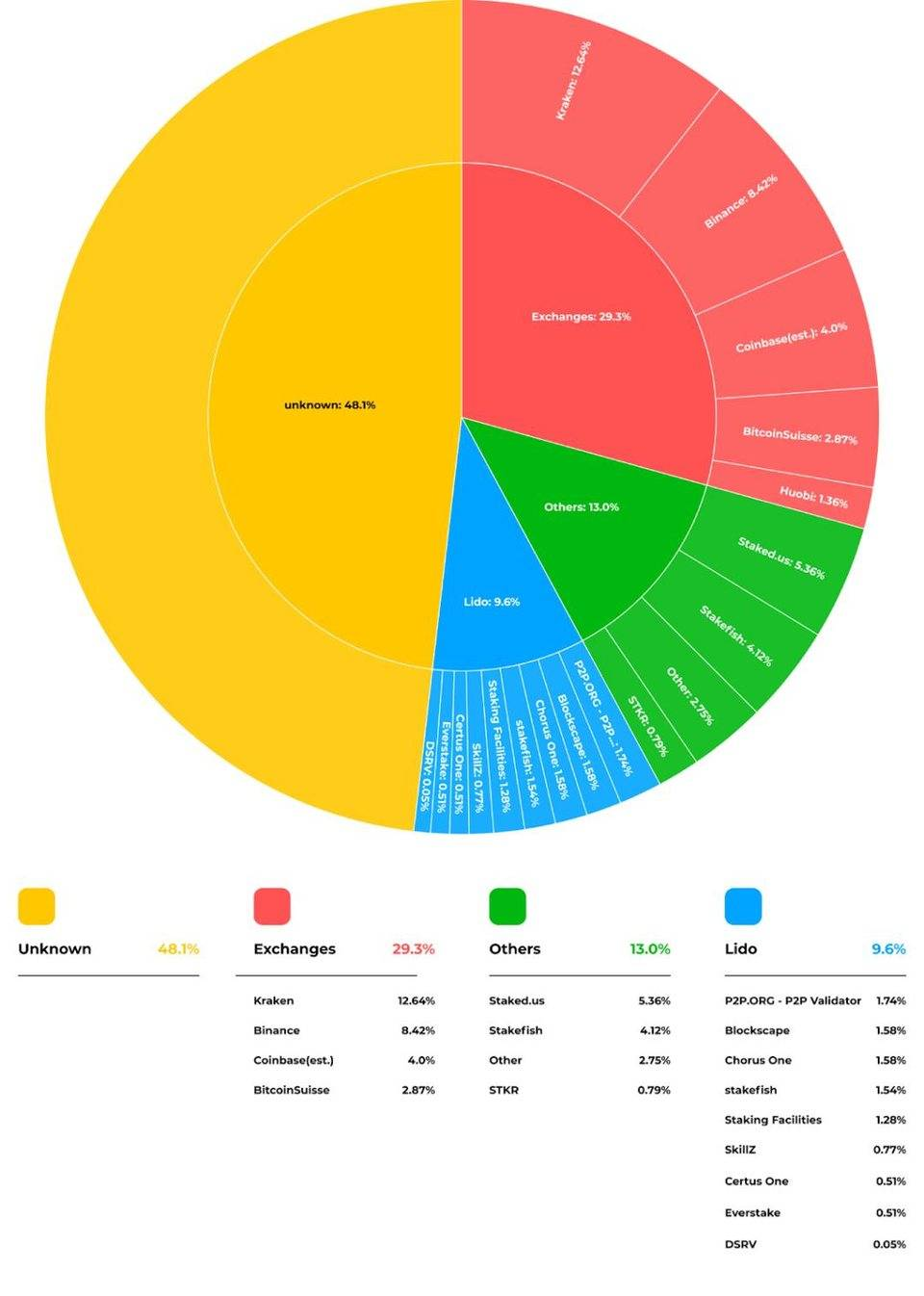
**质押池统一负责验证者节点的操作:**小白用户只需要简单地将以太坊质押过去即可，部分质押池提供保险，防止未遵守协议被罚没的风险。

类似于余额宝，预设不是所有的用户都想要在同一时间提款，这样就可以保持一个流动 ETH 的储备池，以满足立即提款的需求。**这就取消了提款期，让以太坊质押变成了活期储蓄。**

部分质押池会提供质押凭证代币，这些代币被允许在部分Defi协议中使用，从而**获得了想要的流动性**。

**现有的以太坊质押格局**

最早开启以太坊质押服务的是中心化的交易所，为了获取顾客和流动性，一些交易所免费为用户提供这项服务，中心化交易所成为了以太坊质押的早期赢家。由 Kraken 或 Binance 等交易所运营的验证者节点成为占比最大的群体。



上图可以看到以太坊Staking池的头部，被中心化交易所把持着，这和以太坊去中心的理念是背道而驰的。

**因此，以太坊质押池完全去中心化显得尤为重要：**

**以以太坊的安全为中心：**如前所述，许多用户希望委托其质押服务。但由于以太坊不支持协议内委托，这为第三方质押服务商提供了一个机会。考虑到安全性对于以太坊来说是多么重要，去中心化的质押池比需要信任的和中心化的质押池更为可取。

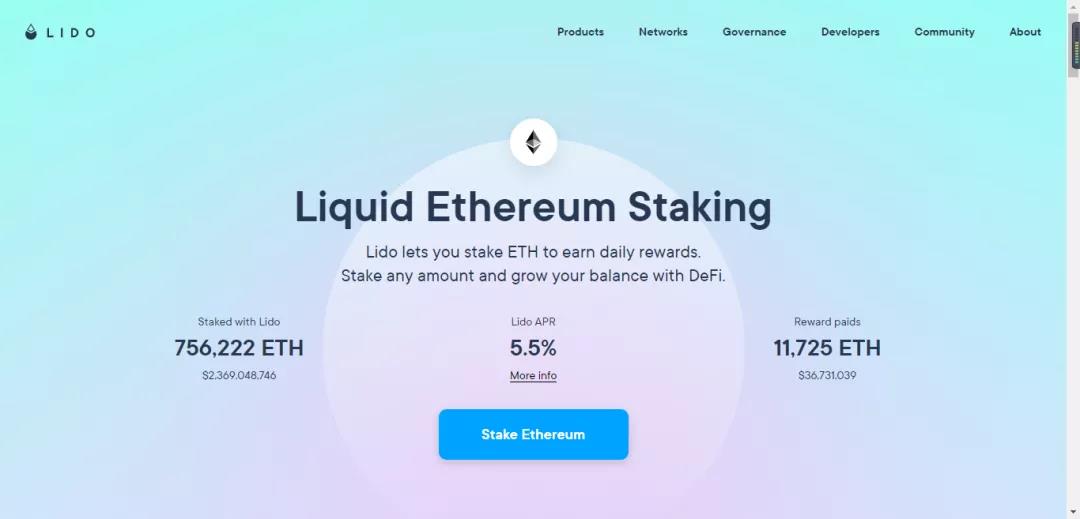
**质押具有中心化力量：**PoS 的 Staking (质押) 可能要比 PoW 的 Mining (挖矿) 更加中心化，支持更加少数、更加集中的赢家。这是因为质押池能够发行一个流动的质押衍生品 (如 stETH) 并以此创造一个强大的网络效应，而这是 PoW 所没有的。

在以太坊社区的扶持下，去中心以太坊质押协议Lido诞生了!!

**Lido是什么**

Lido DAO是一个为Ethereum建立流动性质押服务的社区。Lido允许用户在不锁定资产或维护质押基础设施的情况下获得质押奖励。

当使用 Lido 在以太坊信标链上质押 ETH 时，用户将收到一个代币 (stETH)，该代币以 1:1 的比例代表他们在以太坊信标链上的 ETH。它有效地充当了将 ETH 2.0 的质押奖励带到 ETH 1.0 的桥梁。



随着用户质押的 ETH 产生来自 ETH 2.0 的质押奖励，用户在信标链上的 ETH 余额将会增加。stETH 余额每天会相应更新一次，允许您在 ETH 1.0 上访问您在 ETH 2.0 上获得的质押奖励的价值。  
用户可以以与使用 ETH 相同的所有方式使用 stETH：出售、使用它，并且由于它与 DeFi 兼容，因此可以将其用作链上借贷的抵押品。当在 ETH 2.0 上启用交易时，用户还可以将 stETH 兑换为 ETH。

**Lido的结构组成**

以下是对Lido质押协议的组成部分的大致描述

* **质押池：**管理存款、质押奖励和提款的协议
* 节点运营商注册表
* 提款凭证
* 预言机
* 奖励

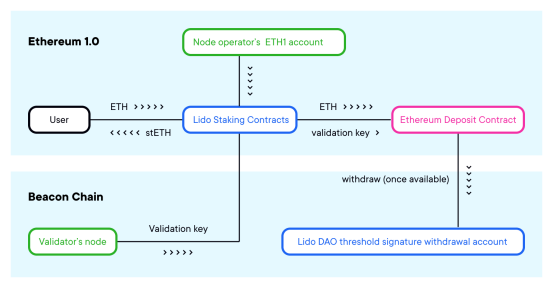
**stETH：**流动质押代币，保持与你的信标链ETH份额1比1的平衡。

**DAO：**管理协议参数的自治组织

**质押池**

**质押池是Lido的核心智能合约。**该合约负责以太坊的存款和提款；铸造和燃烧stETH代币；将资金委托给节点操作员；将费用应用于质押奖励；并接受来自oracle合约的更新。节点操作员的管理逻辑被提取到一个单独的合同。

用户将发送以太坊给质押池合约，以获得铸造的stETH代币作为回报。该以太坊将在节点运营商之间分配，以保持统一的分配，并存入其验证器进行验证。该以太坊的提款凭证将被设置为分布式保管的阈值签名，或者，如果提款到eth1地址将被社区接受，则设置为可升级的智能合约，当它们被启用时将处理提款。



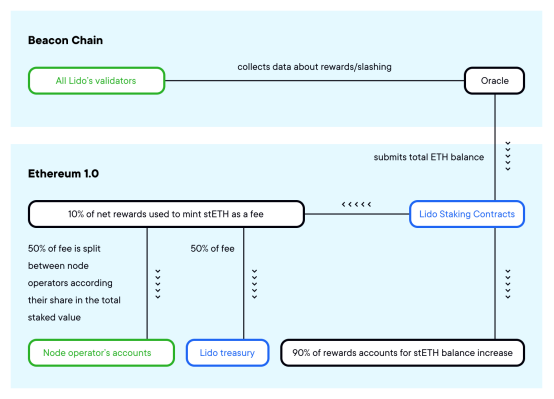
**节点运营商**

用户质押ETH到Lido协议后，所有质押都按32 ETH划分，并分配给节点运营商，由他们负责验证这些质押存款的使用。节点运维商永远不能直接访问用户的以太网络。节点运维商由Lido DAO负责核实审批，目前通过Snapshot治理投票。节点运维商先进入Lido测试网络进行测试，然后才进入主网正式节点运行。Lido不要求节点运营商存放等量的质押头寸。相反，Lido DAO选择的节点运营商必须有资产押注的经验，风险由于Lido DAO里面的保险提供兜底。目前看，这种方法将使该体系的资本效率更高。

Lido智能合约资金存入Lido协议智能合约，然后锁定在以太坊权益证明存款合约中。由Lido DAO控制的阈值签名帐户被指定为驻留提取地址，目前是由Lido DAO控制的多签负责。只有当传输和智能合约在以太坊2.0（最快2021年底）实现时，质押的以太坊才可以退出。那时Lido协议将进行升级，每个用户将自己控制自己的私钥，无中间控制层。

**预言机**

**预言机是一个跟踪DAO的验证者在信标链上的余额的合约。**余额可以因为奖励的积累而上升，也可以因为退出和质押的惩罚而下降。预言机是由DAO分配的。数据每天发送，用于为用户提供stETH代币的准确余额。在有奖励的日子里，有少量的stETH代币被铸造给节点运营商和DAO的保险和发展基金，代表奖励费。

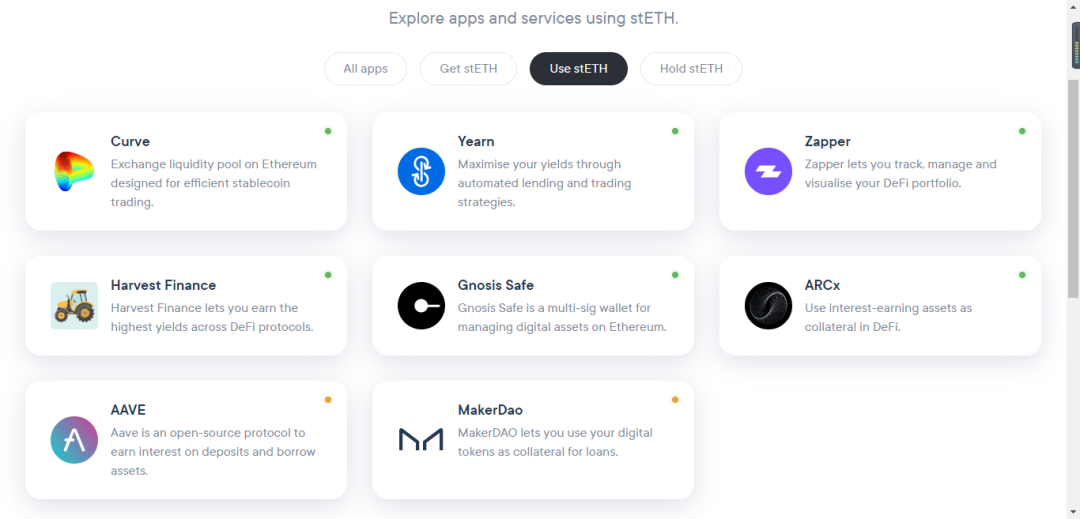


**stETH代币**

**stETH 是 Lido 的流动代币，相当于抵押的以太坊凭证。**

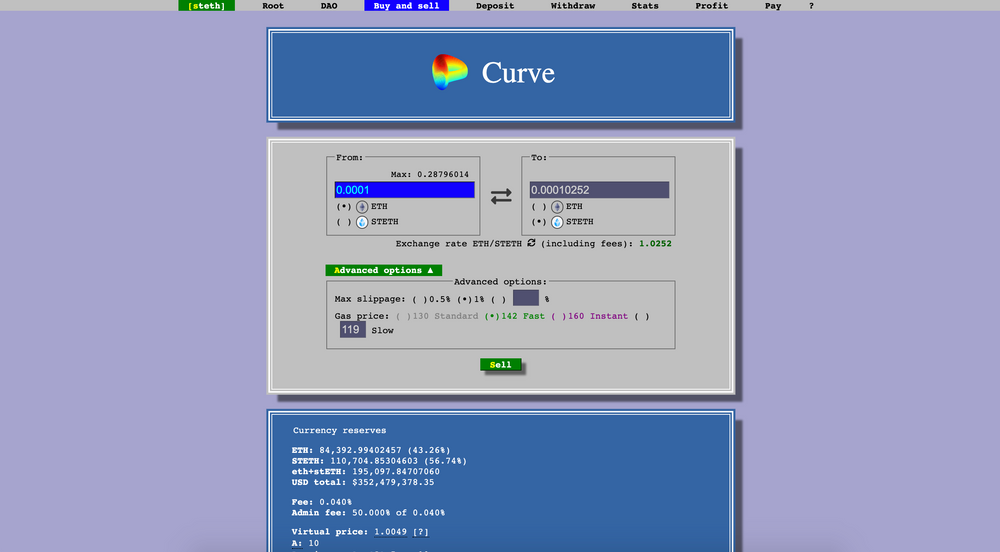
用户可以通过 Lido 质押他们的以太币，绕过直接质押 Eth2 存款合约的限制（流动性不足、不可移动性和不可访问性）。

Lido 的 stETH 完全旨在适用于各种不同的 DeFi 协议。这些用例可以包括借贷协议、DEX 或流动性池、收益聚合器、收益优化器、衍生品等。



除了为用户提供以太坊 2.0 质押服务外，stETH 所能参与的 DeFi 生态也是项目重要的一环。目前，Lido 已与 Curve，Yearn、ARCx 等达成合作。

**stETH 可以与普通 ETH 一起汇集到流动性池中。**这反过来又允许用户间接取消抵押他们的 ETH 并通过池交换收回他们的初始 ETH 存款，如果用户决定他们想要取消抵押，则绕过了等待 Eth2 上的交易启用所需的时间。



Curve Finance 上的 stETH/ETH 矿池

**Lido DAO**

要在Lido DAO中拥有投票权，必须持有其治理令牌LDO。LDO投票权重与投票人在投票合同中的LDO份额成比例。LDO锁定在用户的投票合同中越多，投票者获得的决策权就越大。

**目前拥有的投票治理权限是：**

**初始阶段:**

1.部署协议智能合约,设置费用等协议参数,在愿意提供服务的有信誉的个人或组织中选择门槛签名方案参与者,方便多方计算仪式，创建计分奖励的门槛签名账户,分配初始的dao审查节点操作符。

2.建议和更新Lido的参数

3.批准对实现DAO目标的各方的激励(例如，stETH流动性提供者)

4.建议并更新Lido实现，使用DAO资金引入以太坊2.0特性;分配oracle来提供奖励/削减率饲料,以帮助建立st ETH代币平衡

5.对新的节点运营商进行甄别，对以太坊2.0规则触碰的现有节点运营商进行惩罚

6.管理LidoDAO的保险和发展资金

7.一旦在以太坊2.0可用，管理解除绑定和提现

**融资情况**

Lido Finance经历过两轮豪华机构团的融资：

2020 年 12 月，Lido Finance 完成了200 万美元的融资，投资人包括：Semantic Ventures、ParaFi Capital、Terra、KR1、Stakefish 和 Staking Facilities 等公司，以及包括 MakerDAO 的 Rune Christensen、Aave 的 Stani Kulechov 和 Synthetix 的 Kain Warwick 等个人。

2021 年 4 月份，Lido DAO 通过了将财政部预留的 LDO 代币进行融资的提案。本轮总计出售了 1 亿个 LDO,总计募集了 21600 个 ETH，相当于 0.000216ETH/LDO。投资机构包括：Coinbase、三箭、Paradigm 以及个人投资者 AAVE，Maker，DCG、SNX 等项目创始人参与投资，累计募资 7,500 万美元。

值得要说的机构是Paradigm。2018年6月，Fred和黄共宇共同创立了Paradigm，致力于说服顶级机构投资者参与到加密领域。创立Paradigm时，Fred Ehrsam、Matt Huang（黄共宇）均为29岁，而后加入的合伙人Charles Noyes至今才21岁，仅仅3年时间，Paradigm成为了加密机构里的佼佼者。

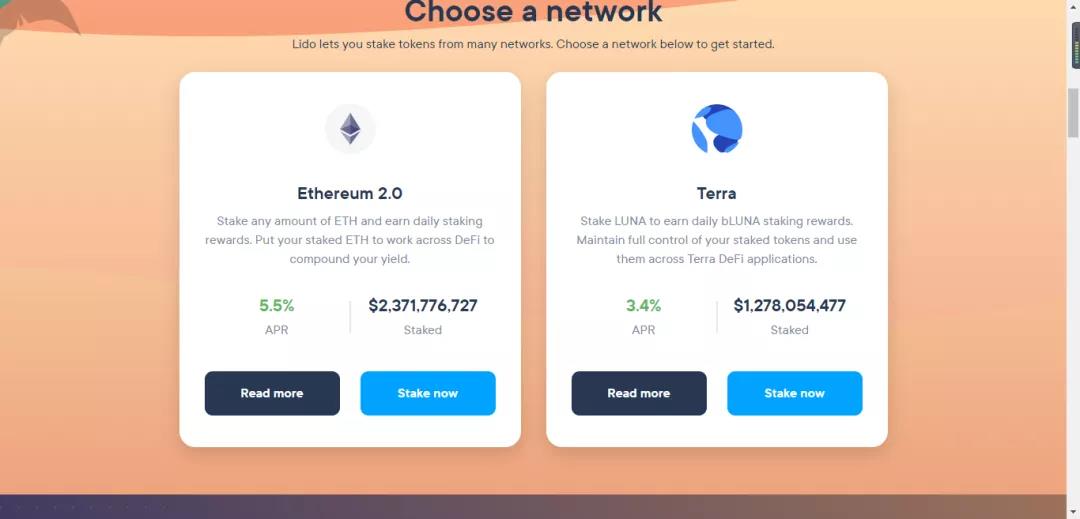
其投资版图几乎都是明星项目:

**从StarkWare、Mina、Uniswap、Compound、MakerDAO、Yield到Optimistic、Amber、Fireblocks、Synthetix、Opyn、TaxBit、BlockFi、Chainalysis、Gitcoin、Lido、dYdX、FTX……**

更有意思的是，在创立Paradigm的5年前，黄共宇从硅谷到北京游玩，结识了刚刚创办今日头条的张一鸣，黄共宇果断出手，成为了今日头条的天使投资人，这笔投资为他来了2500倍的收益。

Lido拥有如此豪华机构的投资，以及各大Defi项目的加持，其业务线的拓展尤为可期。

**总  结**



Lido在去中心化Staking中具有龙头优势，目前已经获得了以太坊Staking市场10%的份额，并在所有Defi协议中TVL排名第十一，接近超过Sushiswap。

相信随着以太坊2.0的进一步进展，越来越多的人会参与到ETH的去中心Staking中，stETH庞大的网络效应，将使Lido成为这个赛道最受益的明星项目。