全球区块链产业全景与趋势

[2021-2022年度报告]

联合发布单位：火币研究院 BLOCKCHAIN ASSOCIATION SINGAPORE 支持单位：火币科技 Huobi Singapore

摘要

2021 是值得区块链行业铭记和回味的一年。Coinbase 上市，比特币 ETF 获批，比特币在萨尔瓦多成为法币，小动物们掀起 Meme 风潮等事件，反映了区块链从技术极客的圈子逐渐走向大众。2021 年新公链也成为市场关注的重点。为此，我们建立了一个公链评估模型，通过每日交易笔数、总交易手续费等指标来评估公链的价值和未来潜力。从结果看，除以太坊外，Solana 目前获得了高分。此外，有发展潜力的公链还有 Cardano，Polkadot，Terra。

在加密金融领域，比特币被越来越多的机构投资者认同，欧美等国的上市公司开始大量买入比特币；在 Defi 领域，DeFi 生态开始向其他公链溢出，solana 等新公链相继崛起；另一方面，为追求更好的流动性解决方案和更高的资金利用率，出现了诸如 OlympusDao、Abracadabra 等 DeFi 2.0 项目；以永续合约、期权、合成资产和利率衍生品为代表的链上衍生品也开始崭露头角。

在加密市场领域，NFT 被主流社会接纳并认可，Meme 币也成为加密货币市场上的热门话题；另一方面，DAO 也开始兴起，ConstitutionDAO、OpenDAO 等引发社会的热议；此外，2021 年最火的词汇当属“元宇宙”，全球各大科技公司纷纷布局元宇宙赛道；最后，本年度区块链游戏的“王者归来”，GameFi 打着“Play to Earn”的口号在市场上迅速崛起。

在加密技术领域，Rollup 扩容方案开始兴起，随着 zkEVM 的上线，ZK Rollup 将逐渐成为市场主流；另一方面，多条高性能公链的崛起，跨链交互的需求迅速涌现；最后，Web 3.0 在年末成为市场讨论的焦点，我们认为 Web3 最重要的特性是个人对平台或组织的治理权，个人数据资产的所有权。

在监管政策方面，根据火币研究院的整理，2021 年以来，全球有超过 40 个主权国家和地区对于加密行业采取了共计 151 项监管措施和指导，同比上升约 75%；其中，以中性政策为主占所统计政策的 59%，其次为积极类政策占比 23%，而消极类政策则占 18%。此外，稳定币、NFT、元宇宙、DAO 也成为政策制定者重点关注的加密领域。

在加密行业未来展望上，我们提出 2022 年度的十大预测。我们认为：（1）全球流动性收紧，比特币将迎来熊市；（2）DAO 逐渐成为链上治理主流形式；（3）跨链将成为多链时代下的基础设施；（4）DeFi 进入 2.0 时代，链上永续合约和期权产品迎来爆发；（5）CBDC 逐步落地推行，跨境支付成探索重点；（6）面向机构的加密借贷市场开始兴起；（7）NFT 借贷/衍生品市场迎来爆发；（8）新公链杀出重围，多足鼎力格局或将形成；（9）加密保险市场或将崛起；（10）中期主流扩容方案迎来发展机遇。

目录

作者

火币研究院
李慧，李炼炫，宁方璞，韩晓鹏，王天琛，蒋梦初，张兆睿，陈雨萱，魏烨艳

第一章 2021 年区块链行业回顾

1.1. 区块链行业发展综述

1.1.1. 加密货币市场迎来繁荣期

从 2021 年初起，包括 MicroStrategy、Tesla、Galaxy Digital Holding 等上市公司和投资机构开始大举购买比特币，推高了 BTC 和加密货币整体的价格。根据 tradingview 数据，全球加密货币总市值从年初的 7660 亿美元增长到了 2.263 万亿美元，年增长率为 195%。根据 companiesmarketcap 数据，如果把比特币看作公司，其市值可以排到全球公司市值的第 8 位，力压英伟达、伯克希尔哈撒韦、TSMC、腾讯等一大批知名企业。以太坊可以排到第 12 位，JPMorgan Chase、Visa、三星被它甩在身后。

图 1-1：2021 年加密货币市场总体市值

来源：Trading view

稳定币是连接传统世界和加密世界的桥梁，稳定币发行量的上升意味着有更多资金涌入加密市场。根据 The Block 数据，2021 年全球稳定币的发行量从 293 亿美元增长到 1498 亿美元，年增长率 411%。

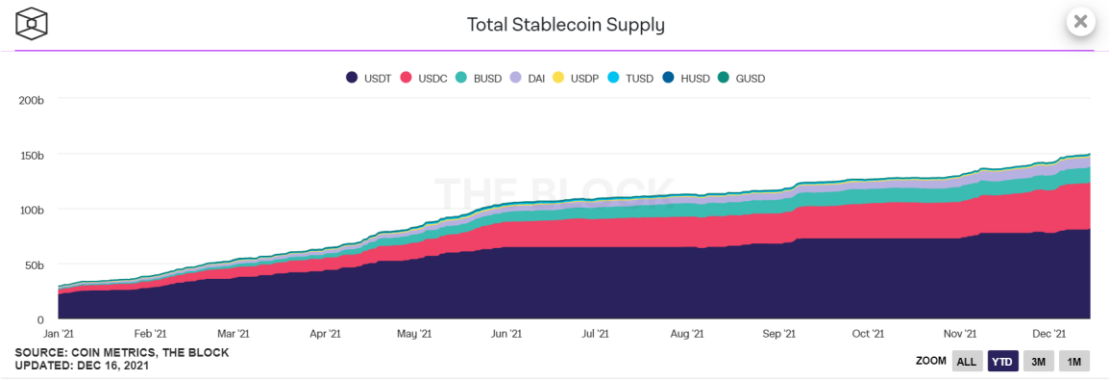


图 1-2：2021 年以来稳定币的总发行量

来源：The Block

近两年来 DeFi 是区块链行业创新的前沿，TVL 能够作为判断 DeFi 领域是繁荣还是冷清的标准。根据 DeFi llama 数据，2021 年各区块链上 DeFi 项目的 TVL 总和从 219 亿美元增长到 2491 亿美元，增长率为 1035%。以太坊仍然是 DeFi 的主要战场，而 BSC、Solana、Terra、Avalanche 等一批公链抓住了以太坊 2.0 短期难以上线、Layer2 暂未获得大规模应用的宝贵时机，依靠手续费低、速度快、生态基金扶持等方式，吸引了包括 Curve、Aave、Sushiswap 等一批项目跨链部署，也培育出了大量原生项目。今年除以太坊外，部署其他公链上的 DeFi 项目的 TVL 从 5.7 亿美元增长到 852 亿美元，一年间翻了近 150 倍。

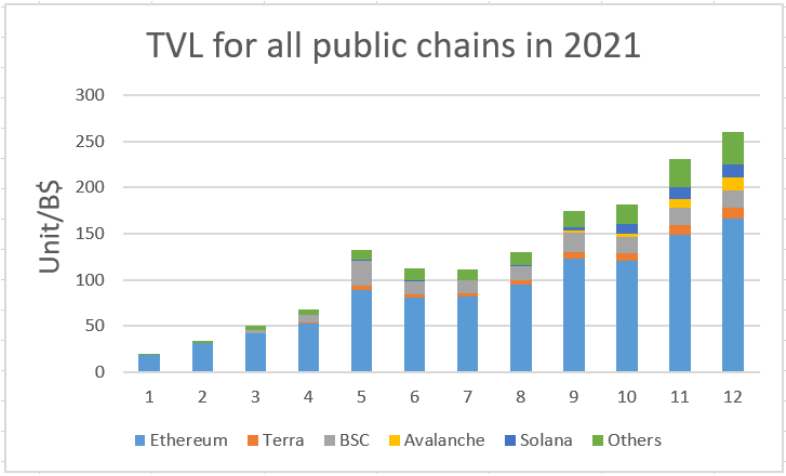


图 1-3：2021 年各公链 DeFi 项目 TVL 总和

来源：DeFi Llama，火币研究院

NFT 是今年非常热门的赛道，频繁创出的天价让其成为了各种媒体头条上的常客。根据 NFTGO 数据，截止 12 月 26 日，其收录的 NFT 总价值为 103 亿美元，比年初翻了 168 倍。NFT 日均交易额从年初的 50 万美元左右暴增到了近期的 5000 万美元左右，也有了百倍的增长。

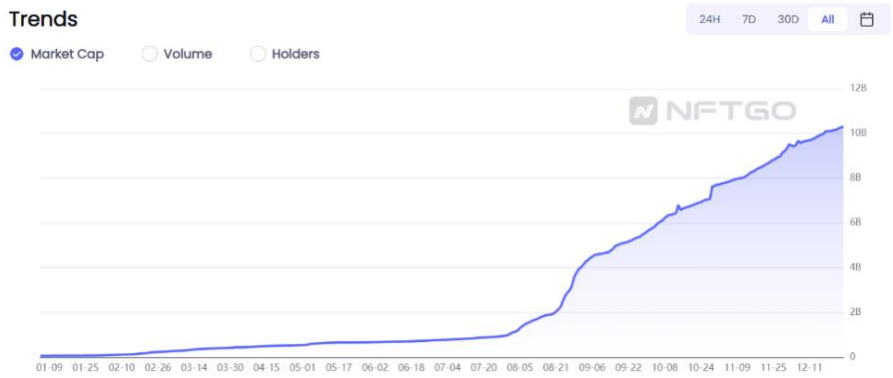


图 1-4：2021 年 NFT 市值变化

来源：NFTGO

1.1.2. 公链生态应用的大爆发

公链应用生态的丰富度是衡量一条公链未来发展的重要指标。根据 Dapp Radar 数据，每日连接到 DApp 的 UAW 数量从年初的不足 40 万增长到了 270 万，一年间增长了 592%。这主要得益于 3 类应用的发展，DeFi 类应用在今年保持了热度并持续迭代升级；游戏类应用快速成长，成为了当今区块链行业用户最多的应用；NFT 类应用是游戏和 Metaverse 的基础设施，而且非常易于理解和传播。

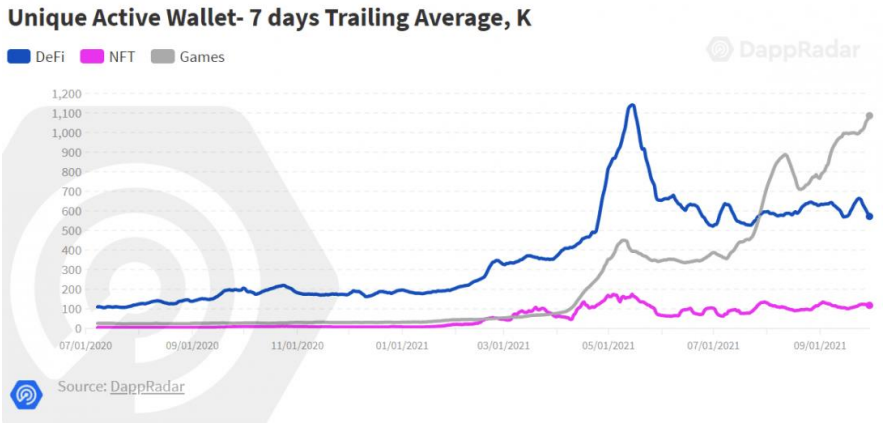


图 1-5： 连接到 DApp 的每日唯一活跃钱包（UAW）数量走势

来源：Dapp Radar

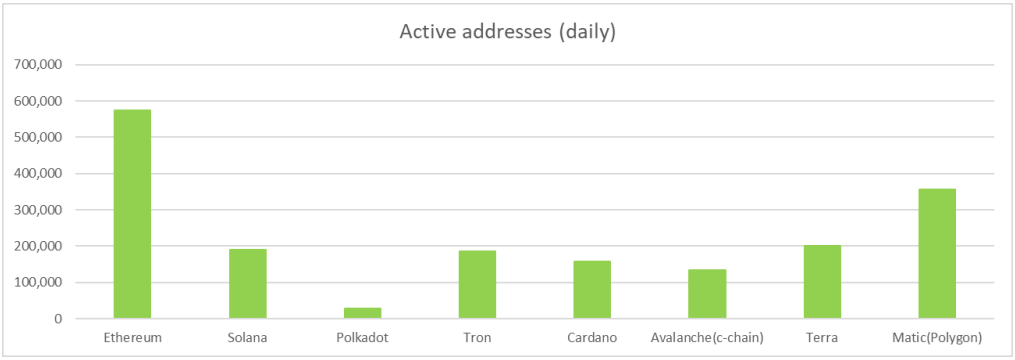


图 1-6 各公链每日活跃地址数量（2021 年 12 月 22 日值）

来源：火币研究院整理

目前，以太坊是应用数量最多、资金承载最大的智能合约平台。根据 Glassnode 数据，2020 年年初，以太坊每日活跃地址数约为 20 万个，其后持续增长，并在 2021 年 5 月到达巅峰，接近 70 万个，后有回落但仍能保持在 50 万以上。2020 年初每日合约调用数约为 35 万次，经过半年的快速增长（俗称 DeFi 之夏），每日合约调用数量到达了 75 万次附近，2021 年全年都保持在这个水平。这表明各类应用已经在持续运行且保持较高使用频率，区块链的用户数量有明显的提升。

图 1-7：近 2 年以太坊每日活跃地址数量和每日合约调用数量（30 日均值）

来源：glassnode

然而，以太坊受制于自身性能的不足，其他公链通过各种不同的方式方法吸引用户，扩展自身生态。公链应用生态随着牛市的繁荣出现了“遍地开花”的局面，包括侧链 BSC、Polygon，新公链 Solana、Avalanche、Polkdot，老牌公链 Cardano、Terra 等，都实现了快速发展。BSC 的每日活跃地址数量一度超过 200 万，Solana、Tron、Cardano、Terra 的活跃

地址数都到达了 15 万以上。此外，公链为了获得优势也越来越注重专注于某些细分领域的赛道，或者直接为某一领域的应用而专门打造一条公链，如销售数量破千万的 NBA Top Shot 基于专为 NFT 而生的 Flow 发行，Axie Infinity 的火爆也离不开专为游戏而生的 Ronin 的帮助。

图 1-8： 公链吸引用户方式

方法	案例
紧跟潮流	BSC在**DeFi潮流中较快速跟上了热点**，才获得了目前的地位。近期正在**gamefi**方向加大投入，BSC上的游戏较简单易上手，短时间带来大量Play to Earn用户与资金。 **IGO，抽奖**
拓宽赛道	区块链的应用不止有DeFi，在如gamefi这样用户数量更多的领域，其他公链凭借高性能优势，可以提升用户体验，占据一席之地。BSC（也包括Polygon）在gamefi上培养生态，实现特色化发展。
持续激励	Avalanche在5月、8月、11月连续出台激励计划，尤其是11月在生态已经有明显增长后继续激励，才能在近期行情下跌时TVL逆势增长。BSC、**Solana**也有巨额生态基金助力生态建设。
打通资金流动渠道	主流通用型公链均能实现与其他链的资产互跨。Avalanche官方桥激励从以太坊跨链超过 75U的用户，吸引资金进入。
培养头部项目	**Terra的主要协议设计以增加以稳定币UST的需求为核心**，并成功并通过支付应用chai，为UST构建了现实世界的支付需求场景。其公链代币LUNA通过捕获UST需求的价值而快速上涨，带来可观的财富效应。

来源：火币研究院整理

除了公链之外，区块链专利申请情况也是反映行业应用状态的一个维度。根据 PatentCould 数据，2021 年全球共申请区块链相关专利 8367 件。今年区块链节点（834 件）、跨链（728 件）、存储（673 件）和智能合约（314 件）的相关技术是最热门的专利申请领域。在应用方向上，数据服务（177 件）、身份授权（166 件）、信息安全（136 件）、支付（85 件）和溯源（66 件）靠前。

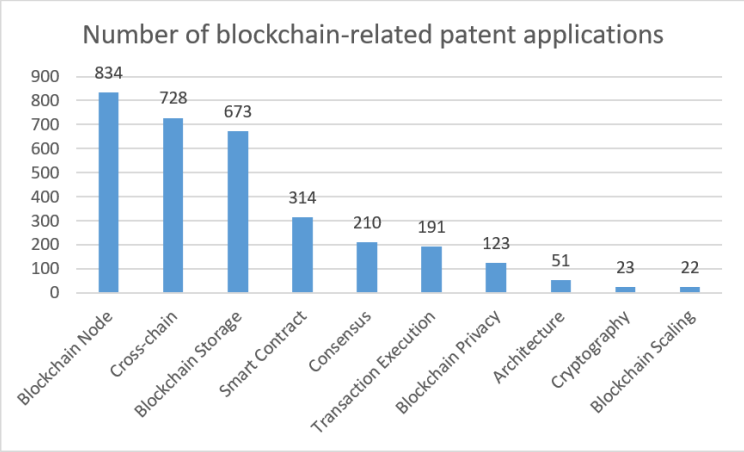


图 1-9： 全球区块链相关专利申请数量

来源：PatentCould，火币研究院整理

1.1.3 公链评估模型

2021 年新公链的崛起让我们不得不重视各公链的性能、生态、交易情况。我们建立了一个公链评估模型，以此来评估公链的价值和未来潜力。公链的市值是整体情况的外在体现，我们不做市值预测，因为一条公链的市值影响因素是多方面的，包括其自身建设情况和宏观影响。

以太坊是当前公链的一个标杆，其数据丰富性可以用来推测各指标对市值的影响。我们考虑了几大指标进行筛选：1. 每日交易笔数；2. 每日活跃地址数；3. 每日总交易手续费；4. 每日总 Gas 消耗量；5. 每月链上总活跃 Dapp 数量；6. 每日链上 DeFi TVL；7. 每月总开发活动。这些指标体现了链上的生态建设情况和代币流通情况。建立公链评估模型的方法是，通过选取以太坊上的代表性指标，与以太坊市值进行数学拟合，判断这些指标对以太坊市值的影响程度，量化各指标权重。整理各公链在这些指标当下的值，计算各指标评分，再通过权重得到各公链的总评分 1。下面对各个指标与市值进行拟合来筛选合适的指标 2。

1. 每日交易笔数与每日活跃地址数

选取了从 2015 年 8 月至 2021 年 12 月的数据。直接看数据面板，市值与每日交易数很难有关系。我们对两组数据进行对数处理，能够发现明显的线性关系。图中，还能发现数据具有周期性聚集现象，这可能是牛市的一个特征：交易量在高位市值过于集中。通过线性回归，得到相关系数 R2=0.9016。

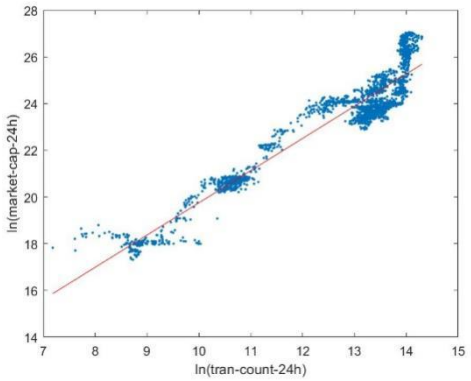


图 1-9：每日交易量对数与市值对数的面板图（2015.08-2021.12）

来源：火币研究院

按照以上的数据处理方法，得到了每日活跃地址数与市值的关系图。同样的，相关系数 R2=0.9159。

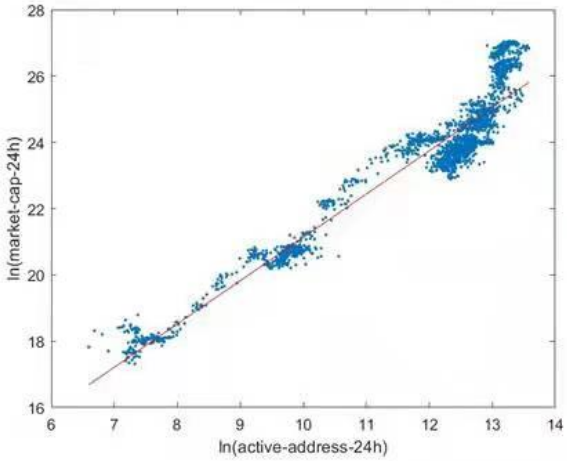


图 1-10：每日活跃地址数对数与市值对数的面板图（2015.08-2021.12）

来源：火币研究院

2. 每日总交易费用与每日总 gas 消耗量

与每日交易笔数类似的方法处理数据，得到图 1-的结果，相关系数 R2=0.8179。在做数据拟合时，我们经常看到相关性很小的数据，拟合结果反而表示有强相关性。强相关的数据，反而拟合结果很差。图 1-中，每日总交易费用对数与市值对数的面板数据并不好去做线性回归结果会出现较大误差，所以这个指标我们暂时不考虑。每日总 gas 消耗量的拟合结果也被排除，因为，在 EIP-1559 出现之后，数据出现断层。

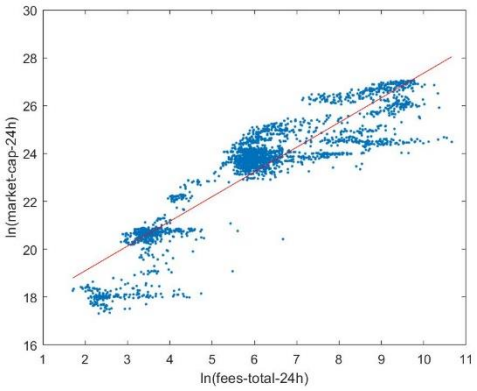


图 1-11：每日交易费用对数-市值对数的面板图

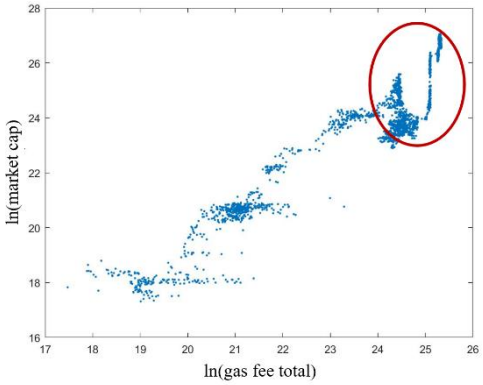


图 1-12：每日总 gas 消耗量对数-市值对数的面板图（2015.08-2021.12）

来源：火币研究院

3. 每月链上总活跃 Dapp 数量

链上活跃的 Dapp 数量能够直接反映该公链生态建设情况。选择每月的数据是因为 Dapp 开发、维护和上线需要时间，每日的数值并没有意义。市值选择每月最大市值，因为突出反映了总活跃 Dapp 数量带来的影响力。

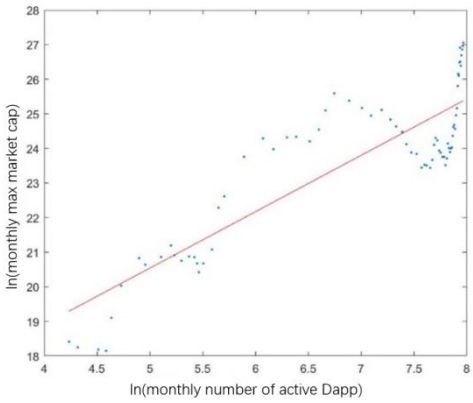
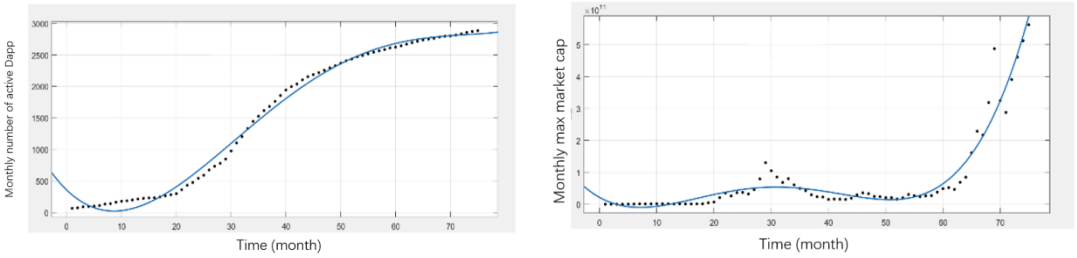


图 1-13：每月链上总活跃 dapp 数量对数-每月最大市值对数的面板图（2015.09-2021.11）

来源：火币研究院

从图 1-中看到采用线性回归的方法不合适，可能原因：1. 采用的数据样本量略少，存在一定偏差；2. 也许 dapp 数量与市值存在非线性关系。从总 dapp 数量和每月最大市值上看，它们对时间利用多项式拟合，都与时间有 4 次方关系。说明 dapp 数量与市值存在紧密联系，但不是绝对的线性关系。对每月总 dapp 数量和每月最大市值求对数，再采用多项式拟合的方法得到结果，如图 1-所示，拟合后相关系数 R2=0.9314。



（1） （2）

图 1-14：（1）时间-每月总活跃 dapp 数量拟合情况；（2）时间-每月最大市值拟合情况

来源：火币研究院

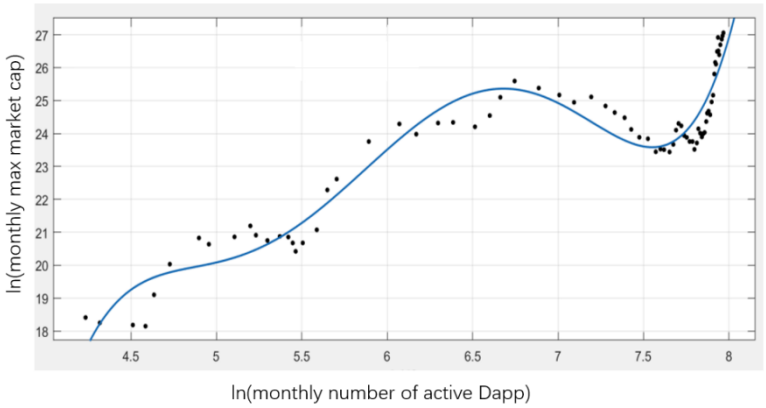


图 1-15：多项式拟合每月总活跃 dapp 数量对数-每月最大市值对数

来源：火币研究院

4. 每日链上 DeFi TVL

DeFi TVL 的数据选取了从 2018 年 11 月开始至 2021 年 12 月止。TVL 的数据和市值关系更加明确，不需要取对数就能看到有明显的线性关系。线性回归后的相关系数 R2=0.9753，是所有指标中，相关性最强的。

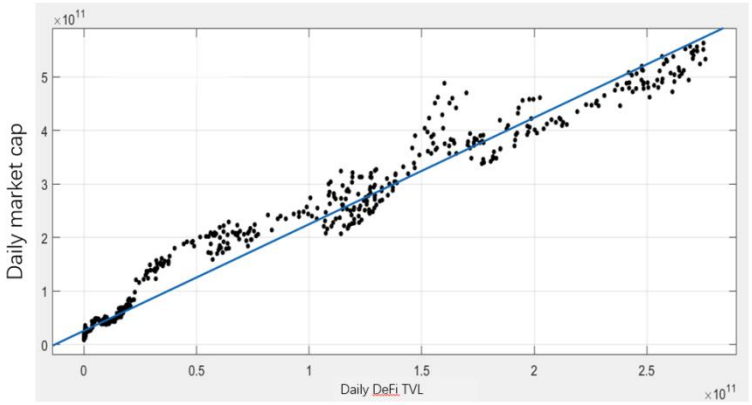


图 1-16：每日链上 DeFi TVL-每日市值关系

来源：火币研究院

5. 每月总开发活动

开发活动也是直接反映了生态建设情况和公链维护情况，考虑这个指标是因为该指标超前于市值，体现了公链的发展潜力。每月市值也取最大值。开发活动的拟合也是采用多线性拟合的方法，可以更为准确的得到相关性。相关系数 R2=0.6405。

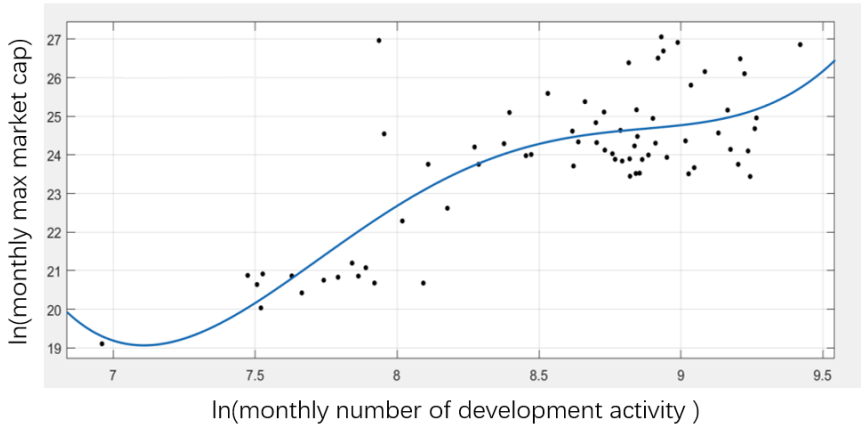


图 1-17：每月开发活动对数-每月最大市值对数多项式拟合结果（2016.01-2021.11）

来源：火币研究院

做这些指标拟合是需要找到各指标对市值的影响力，根据拟合的相关系数去量化各指标的权重，从而避免主观因素去分配权重。从表中可以看到 DAPP 总数和 DeFi TVL 对市值影响是最大的。

指标选择	说明	相关系数 R^2	权重
交易量	代币的流通情况	0.9016	20.6%
活跃地址数	代币流通+生态建设	0.9195	21.0%
Dapp 总数	生态建设	0.9314	21.3%
开发活动	生态建设+性能维护	0.6405	14.8%
DeFi TVL	生态建设	0.9753	22.3%

表 1-1：各指标权重分配

来源：火币研究院

我们选取 Solana，Polkadot，TRON，Cardano ，Terra，Avalanche 6 条公链与以太坊进行比较，查找 12 月 22 日各指标数据计算出表 1-所示的指数。由此得到各公链在 5 个指标上分布的雷达，并通过权重和各指标指数得到总体评分。

Blockchain	Transactions count (daily)		Active addresses (daily)		Total Dapps (monthly)		Development Activity (daily)		DeFi TVL (daily)	
	Value	Index	Value	Index	Value	Index	Value	Index	Value	Index
Ethereum	1,201,550	0.5	574,885	100	2894	100	472	84.4	1.55E+11	100
Solana	247,272,942	100	189,917	33.0	1332	46.0	559	100	1.25E+10	8.0
Polkadot	220,411	0.1	28,706	5.00	260	9.0	373	66.7	1,645,926	0.0
TRON	2,730,035	1.1	184,986	32.2	88	3.0	11	2.0	5.35E+9	3.4
Cardano	119,620	0.1	158,440	27.6	0	0	442	79.1	0	0
Avalanche (C-Chain)	959,720	0.4	134,423	23.4	150	5.2	43	7.7	1.27E+10	8.2
Terra	541,129	0.2	200,000	34.8	152	5.3	110	19.7	1.97E+10	12.7
Weighting	**20.60%**		**21.00%**		**21.30%**		**14.80%**		**22.30%**	

表 1-2：7 条公链在 12 月 22 日的指标情况

来源：火币研究院

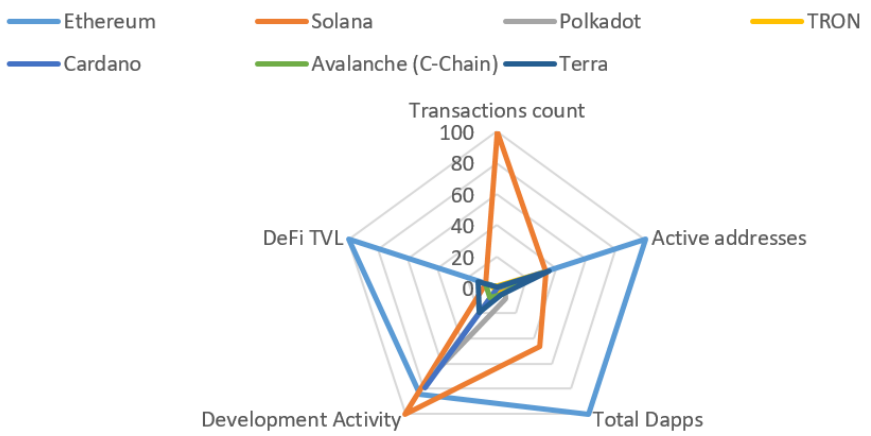


图 1-17：7 条公链各指标情况雷达图

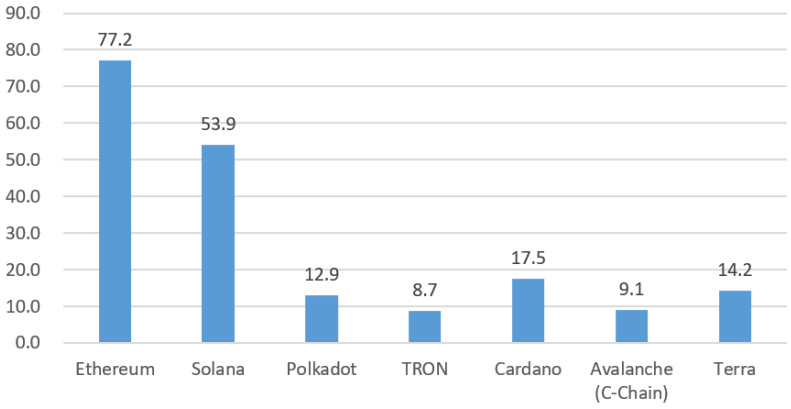


图 1-18：各公链评价总分

来源：火币研究院

从评估结果中可以看出，以太坊各项指标大部分都有很好的评分，但每日交易笔数相对于 Solana 要落后很多，以太坊扩容是亟待解决的问题。每日活跃地址和 DeFi TVL 显示出 Terra 具有很大的用户量和发展趋势。Cardano 在开发活动上获得了高分，虽然它生态还没有起来，但如果开发活跃，后期有一定发展潜力。从总分上看，除以太坊外，Solana 目前获得了高分，其在今年市值也获得了千倍增长。后面有极大发展潜力的是 Cardano，Polkadot，Terra1

1.2 2021 区块链十大事件回顾

1.2.1 美国 BTC 期货 ETF 获批上市，打开主流市场投资通道

千呼万唤始出来，经过漫长等待，美国首支比特币期货 ETF 终于在 2021 年 10 月 19 日上市纽交所。它全称 The ProShares Bitcoin Strategy ，基金代码为 BITO，投资标的是 CME（芝加哥商品交易所）的比特币期货合约。BITO 通过管理比特币期货合约的敞口来寻求资本增值，但该基金不直接投资于比特币，因此所谓的“比特币 ETF”实际上是比特币期货 ETF。

自 2013 年以来，已有近 20 家机构申请推出比特币现货 ETF，但没有一家获得成功，部

[1]评价方法说明：首先感谢 Chad Hahn 在 Medium 发表的文章给予的启发。我们在他的基础上去做了权重的量化，从而排除了主观因素。同时，我们认为市值是总体的表现，并没有放在评价体系之中，而是作为拟合的目标。但目前这种评价方法选取的指标还是有限的，如果数据积累足够，可以添加其它指标，采用同样的方法去量化权重得到评价结果。

[2]各指标数据来源于 glassnode，cyptodiffer，Stateofthedapps，Dappradar，Santiment community API 等，除以太坊外其它公链数据可能会出现偏差。

分原因是比特币本身具有现货特性，并非现金存款，没有银行和第三方可以进行托管，需要另外一套合规托管和私钥安全性管理的方案；其次，市场上没有出现一个以公允价格购买和退出的完整二级平台（指纳斯达克、CME、CBOE 等有着完整盘前、盘后、大宗、做市商席位和清算结算等体系的传统交易平台）。期货 ETF 能提前于现货 ETF 获得批准，是因为期货具有双向性：期货既可做多也可做空，让资金往两个方向流动，这样市场价格就会在多空之间形成一个相对比较均衡的状态；与之相反的，比特币现货做空机制仍不完善，是一个单向市场。

BITO 的推出可视作是加密货币行业和金融市场的里程碑，它标志着 BTC 被正式承认为当前监管视野下的成熟资产或商品，同时，使 BTC 作为投资标的将被更多主流投资者所注意。

"The ETF approval is a watershed moment for the industry," 比特币基金会主席 Brock Pierce 在给 CNN Business 的一份声明中说，"Today begins an era where retail investors can invest directly into Bitcoin through the ETF, and serves as further validation of Bitcoin and cryptocurrencies across the country and on a global basis."

截至 2021 年 11 月 22 日，市场已有 14 支可供投资者选择的比特币 ETF 和其他加密货币基金，其管理的资金规模如表所示。

Name	Assets under management
ProShares Bitcoin Strategy ETF	$1.4 billion
Valkyrie Bitcoin Strategy ETF	$59.2 million
VanEck Bitcoin Strategy ETF	$9.6 million

Name	Assets under management
Global X Blockchain & Bitcoin Strategy ETF	$10.6 million
Amplify Transformational Data Sharing ETF	$1.7 billion
Bitwise 10 Crypto Index Fund	$1.2 billion
Siren Nasdaq NexGen Economy ETF	$309.6 million

First Trust Indxx Innovative Transaction & Process ETF	$142.0 million
Simplify US Equity PLUS GBTC ETF	$121.7 million
Bitwise Crypto Industry Innovators ETF	$141.2 million
Global X Blockchain ETF	$114.4 million
VanEck Digital Transformation ETF	$75.0 million
Bitcoin Strategy ProFund Investor	$29.5 million
First Trust SkyBridge Crypto Industry and Digital Economy ETF	$43.4 million

表 1-3：加密货币基金规模

数据来源：etfdb.com，火币研究院整理

1.2.2 第一家加密货币交易所 Coinbase 登陆美股

2021 年 4 月 14 日，美国最大的加密货币交易所 Coinbase 以直接上市的方式（DPO）在纳斯达克挂牌（代码 COIN），成为了全球第一个上市的大型加密货币交易所。

Coinbase 的上市方式是直接上市，又叫直接公开发行（DPO）。DPO 不像首次公开发行 IPO 那样会发行新股对外筹集资本，而是公司员工和投资者将其权益转换为股票，然后在股票交易平台挂牌。股票上市后，大家可以直接购买股份，之前的投资者也可以随时兑现，也不像 IPO 那样会有一段时间的锁定期。直接上市还可以免除传统 IPO 的中间询价过程、巨额承销费用以及繁琐的准备过程，因此深受科技独角兽公司喜爱。

Coinbase 2021 年一季报显示，其当季营收飙升至 18 亿美元，相较 2020 年同期的 1.906 亿美元增长超 8 倍，净利润在 7.3 亿-8 亿美元之间，较去年同期的 3200 万美元暴增 25 倍。由此可知它有大量的资金和利润，不需要通过募股融资。上市的目的，除了团队权益变现和激励员工之外，主要还是在于借助上市巩固其合规龙头的位置，牢牢把握住合规市场。

Coinbase 在合规运营方面堪称业内典范，获得了非常多的数字资产运营合规牌照。CEO Brain Armstrong 曾透露，Coinbase 从 2013 年左右开始在美国申请汇款执照，并随后相继在欧洲获得了电子货币（Electronic Money）许可证，在纽约获得了用于数字资产活动的营业执照 BitLicense，并在美国金融犯罪执法局（FinCEN）注册了 MSB 牌照，也开始向其他监管机构申请额外的许可证。如今 Coinbase 在纳斯达克上市，直接接受 SEC 的监管，定期

向公众公布财报，合规性和品牌美誉度都达到了顶峰。现在加密货币市场里机构的地位越来越重要，而合规的上市公司 Coinbase 就成了机构资金的首选。

Trading Volume (B$)	2020 Q3	2020 Q4	2021 Q1	2021 Q2	2021 Q3
Retail	18	32	120	145	93
Institutional	27	57	215	317	234
Total	45	89	335	462	327
Institutional share	60%	64%	64%	69%	72%

表 1-4：Coinbase 近期交易额结构

来源：Coinbase Q3 财报，火币研究院

Coinbase 上市是对加密货币的发展具有里程碑意义的大事件：首先，Coinbase 的上市提供了一个让主流资金投资加密货币领域的新通道。其次，Coinbase 的上市为交易所起了示范作用，将带动更多加密货币交易所在合规性上做好保障。对于没有发行平台币的交易所，也可以像 Coinbase 这样通过上市公开募股来融资，这增加了交易所融资的途径。此外，Coinbase 的上市会也让各国监管部门看到新型资产合规发展的潜力，正视数字资产的意义，研究和思考加密资产合规化发展的可能性和实现路径。

1.2.3 萨尔瓦多成为全球首个将比特币列为法定货币的国家

2021 年 6 月，萨尔瓦多总统布克勒宣布把比特币定为法定货币，这项比特币法案得到了萨尔瓦多政府及议会中执政联盟的支持，以 62 票赞成、19 票反对的投票结果获得通过。2021 年 9 月，法案正式实施，比特币和美元一起成为了萨尔瓦多的法币，这是比特币第一次成为了主权国家的法币。

萨尔瓦多位于中美洲北部，工农业和金融基础薄弱，大约 70%的人没有银行账户或信用卡。它的经济严重依赖移民汇款，有超过 200 万萨尔瓦多人生活在国外，定期给家里人汇款，每年侨汇 40 多亿美元。萨尔瓦多总统称使用比特币作为法币将节省侨汇的成本和时间消耗，同时有助于吸引投资，提升非正规就业领域和低收入人群实际收入，推动金融包容性发展和国家经济增长，提供信贷、储蓄、投资和安全转账等渠道。

比特币在萨尔瓦多的应用并非一帆风顺。从 7 月起就有反对比特币的抗议，在该国独立

日当天更是有群众组织抗议游行，并当场烧毁了一台崭新的比特币 ATM 机。反对者认为把比特币定为法币将严重损害国家的经济和民众的腰包，害怕在币价大幅波动中失去储蓄或养老金。国际货币基金组织（IMF）、国际评级机构穆迪、英格兰银行行长、俄罗斯总统等组织和个人也都表示了对此举的质疑。

尽管有人质疑，萨尔瓦多还是在坚定地推进比特币的接受和应用。它建立了 1.5 亿美元的比特币信托基金；推出了电子钱包 Chivo 并将向注册的萨尔瓦多公民免费提供价值 30 美元的比特币；推出了一个由 200 台比特币 ATM 机组成的网络；在全国设立了 51 个培训点，已有超过 7000 名企业家接受了比特币交易的培训；计划在 2022 年发行一支 10 亿美元的债券，债期为十年，年利率为 6.5%，筹集的资金将用于建设一座 “比特币之城”，并将用环保低碳的火山地热资源为比特币矿场供电。政府用比特币信托基金的盈利建设了医院和学校，萨尔瓦多的麦当劳、星巴克和必胜客和一些本地企业逐渐开始接受比特币支付，融合正在发生。

萨尔瓦多政府此举已对拉美地区国家形成“示范效应”，多国陆续开始或加快推进相关立法进程。2020 年至 2021 年，拉美地区国家数字投资增长超过了 100%。

目前，比特币在全球 131 个国家或地区不受限制，其中包括 102 个认为比特币合法和 29 个持中立态度的国家，有 7 个国家认为比特币非法（包括越南、阿富汗等），有 7 个国家限制了比特币的交易（包括中国、埃及等）。目前，有 55 个国家将比特币划分为货币（currency）、23 个国家将货币划分为商品，10 个国家划分为交易物、3 个国家划分为钱（money）。

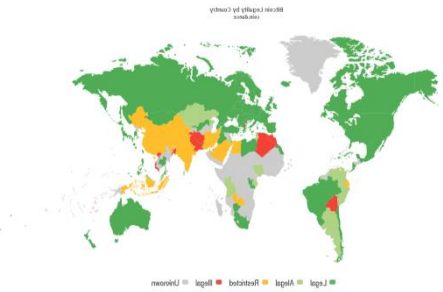


图 1-18：各国对比特币所持态度

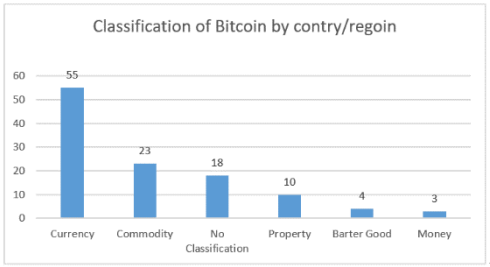


图 1-19：比特币在各国类别统计

来源：coin.dance，火币研究院

1.2.4 佳士得拍卖 NFT 作品以天价成交，NFT 破圈成焦点

2021 年区块链赛道中最耀眼的明星之一就是 NFT。NFT 因其独一无二、不可篡改的特性常被用于稀缺数字资产的确权，这个资产可以是游戏道具、数字艺术品、门票等诸多形式。

2021 年 NFT 艺术品和收藏品拍卖频频爆出天价，NFT 作为基础设施也有力助推了 GameFi 和 Metaverse 的发展。春季，以 Beeple、Whisbe、Pak 为代表的一批艺术家的 NFT 作品受到热捧，Beeple 的作品《Everydays: The First 5000 Days》在拥有 250 多年历史的世界顶级拍卖行佳士得拍出了 6,930 万美元的成交价（含佣金），创造了 NFT 艺术品的拍卖记录。这个作品也排到了在世艺术家的作品价格的第 3 名。数字球星卡 NBA Top Shot 销售额超过 7 亿美元，销售笔数超过 1000 万笔；收藏品的后起之秀 Bored Ape Yacht Club 更是在半年多内就创造了超过 11 亿美元的销售额。8 月，首个 NFT 项目 Crypto Punks 的 CryptoPunk 3100 拍卖出了成交价 42000 枚 ETH，约合 10860 万美元，再次刷新 NFT 作品的单价。爆款游戏 Axie Infinity 上的 NFT 总价值达到了 5400 万美元，交易额为 37 亿美元，促进了 Play to Earn 模式的兴起。

不止是拍卖价格和交易额连创新高，各大品牌也纷纷推出 NFT 联名产品。如国际大牌奢侈品 LV、Burberry、Balmain、Gucci，汽车品牌保时捷、奥迪，还有更大众化的可口可乐和漫威，它们推出了如游戏配件、虚拟服装和可穿戴设备、漫画书、设计稿等多种 NFT 产品。Twitter 的联合创始人& CEO Jack Dorsey 将其有史以来第一条推文作为 NFT 资产出售，英国著名杂志《经济学人》将其 DeFi 主题封面作为 NFT 拍卖。这些国际名企们的知名度和影响力帮助 NFT 实现了出圈，获得了全社会的关注。

2021 年是 NFT 爆发的一年，根据 nonfungible.com 数据，2021 年以太坊上与 NFT 只能合约交互的单日活跃钱包地址数最高到达 140K，第三季度 NFT 的交易额就接近 60 亿美元，前三个季度累积交易额约 87 亿美元，比去年翻了 34 倍。尽管高增长必然伴随着市场不稳定、不切实际的预期和潜在的失望，但可以确定的是，NFT 已近进入了一个新阶段，未来将发挥出更大作用。

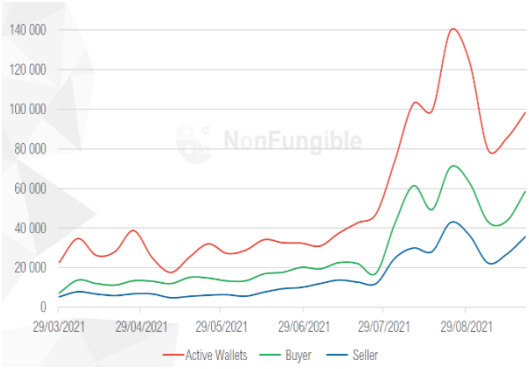


图 1-20：以太坊上与 NFT 智能合约交互的钱包地址数

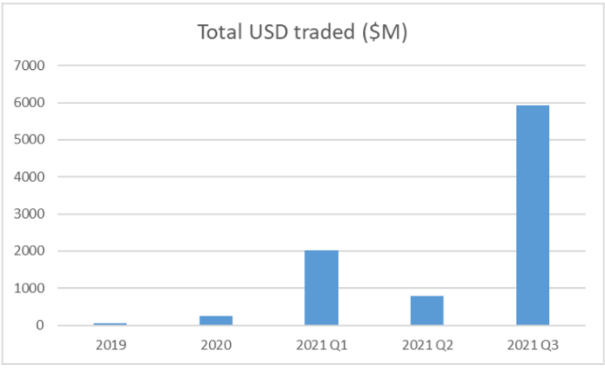


图 1-21：以太坊上 NFT 交易额

来源：nonfungible.com，火币研究院

1.2.5 马斯克“带货”狗狗币，Meme 风潮涌现

2021 年的加密货币市场，有一类币格外引人注目，它们就是 Meme 币。Meme 币是指受到互联网和社交媒体上广泛传播的笑话、流行用语、图片、事件等激发而产生的加密货币。

DOGE 是最早的也是最受欢迎的 Meme 币。2013 年，Adobe 软件工程师 Jackson Palmer 与 IBM 软件工程师 Billy Markus 为了调侃比特币，在比特币代码基础之上创造了这个被他们视为玩笑的加密货币。也许他们也无法想象，这样一个玩笑居然能在 7 年多后一度拥有接近千亿的市值，在所有加密货币中排名第 4。

在 DOGE 价格的大幅上涨中，有一个人功不可没，他就是特斯拉的 CEO，Elon Musk。马斯克是 DOGE 的忠实粉丝，从 2019 年起，他就在 Twitter 上发表过很多支持 DOGE 的言论，还把 Twitter 的简介改成过”Former CEO of Dogecoin”。他的推文引发了众多粉丝关注 DOGE，Dogecoin 的 twitter 粉丝数量达到了 2632k，比以太坊还要多；在 Google Trends 发布的“2021 年度热搜榜-热搜新闻”板块中，Dogecoin 排名第四。大量的关注也带来了价格的暴涨，DOGE 年度最大涨幅高达 156 倍。

图 1-22：以太坊上 NFT 交易额

来源：Twitter @elonmusk

Meme 币中另一个值得关注的是 Shiba Inu（SHIB）。Shiba Inu 在 2020 年就发行了代币，在今年的 Meme 代币风潮中，马斯克发的两条的指向性不是很强的推特，“I’m looking for a shiba pup!”和“I’m getting a Shiba Inu”，为 SHIB 吸引了大量粉丝。人们开始关注到这只怀抱去中心化理想的，代币分配方案中连一个币都没有留给团队的小柴犬。它的价格在 5 月实现了传说级的暴涨，5 月的最高价比年初翻了 43 万倍。

随着 DOGE 和 SHIB 价格的飙升，狗和各种动物成为了一种新的 Meme，市场上出现了很多种像柴犬、秋田犬、萨摩耶、哈士奇、猪、蚂蚁、狐狸这样的动物币。CoinMatketCap 的 Meme 板块共收录 Meme 代币 167 种，其中 70%以上的代币都以某种动物命名。动物伙伴们也都纷纷上涨，那时候加密货币市场变成了动物园。

5 月 13 日，Vitalik 将项目方无偿赠与他的 SHIB、AKITA、ELON 等 Meme 币兑换成 ETH，并将部分 ETH 和 Meme 代币捐赠给多家慈善机构。同时由于市场整体下行压力巨大，Meme 代币都迎来了惨烈的下跌，一场热闹非凡的“疯狂动物城”告一段落。

1.2.6 美国国会举行数字资产听证会

2021 年 12 月 8 日，美国众议院金融服务委员会（House Committee on Financial Services）举行了“数字资产和金融的未来：了解美国金融创新的挑战和利益”主题听证会。众议院成员寻求通过听证会来对加密行业有更深入的了解，并就监管规则展开讨论。来自加密货币交易所 Coinbase 和 FTX、稳定币发行商 Circle 和 Paxos、矿业公司 Bitfury 和 Stellar 发展基金会的共 6 位加密企业高管出席了听证会。他们介绍了加密产品及服务在金融创新中发挥的作用，并表达了对一些现行政策的看法。这次听证会上，议员和加密高管双方态度温和，就加密监管展开了深入的讨论。Compound 总法律顾问 Jake Chervinsky 评价这是“有史以来最积极、最具建设性、两党参与度最高的加密公开活动”。

此次听证会话题范围非常广，核心观点如下：

- 监管问题的核心是稳定币和加密交易所。
- 目前美国还没有全国统一的监管体系，希望能够建立国家层面单一机构的监管体系。
- 加密货币的优势在于门槛低，费用低，速度快，所以比起传统金融能够服务更多人。不宜生搬硬套传统监管规则。
- 加密货币可以提高美国在科技方面的竞争力，增强美元做为全球储备货币的地位。
- 加密的重点是真正的去中心化，不会控制用户，走相反方向的公司最终将失去价值并被遗忘。

1.2.7 多国央行加快研发 CBDC，中国 E-CNY 全面推进试点

2021 年国际组织和多国央行对 CBDC 的态度保持积极，持续推进 CBDC 的研发。

6 月，全球最大的七个经济体（G7）集团在伦敦会晤公报中明确了对 CBDC 的共同兴趣，并表示一直在探索 CBDC 的机遇、挑战以及对货币和金融稳定的影响，承诺作为财政部和央行，在各自的职责范围内，就其更广泛的公共政策影响进行合作。8 月，国际清算银行（BIS）、国际货币基金组织（IMF）和世界银行联合呼吁，全球央行应该就 CBDC 进行合作。BIS 表示将全力推动 CBDC 的发展，以此来实现金融现代化并确保“科技巨头”不会控制货币。

据 Atlantic Council 统计数据，截止 2021 年 10 月，全球已有包括巴哈马、尼日利亚在内的 9 个国家发行了 CBDC，有 79 个国家正在探索创建 CBDC，它们的 GDP 之和占全球的 90%以上。包括中国和韩国在内的 17 个国家目前正处于 CBDC 的试点阶段，并为可能的全面启动做准备。

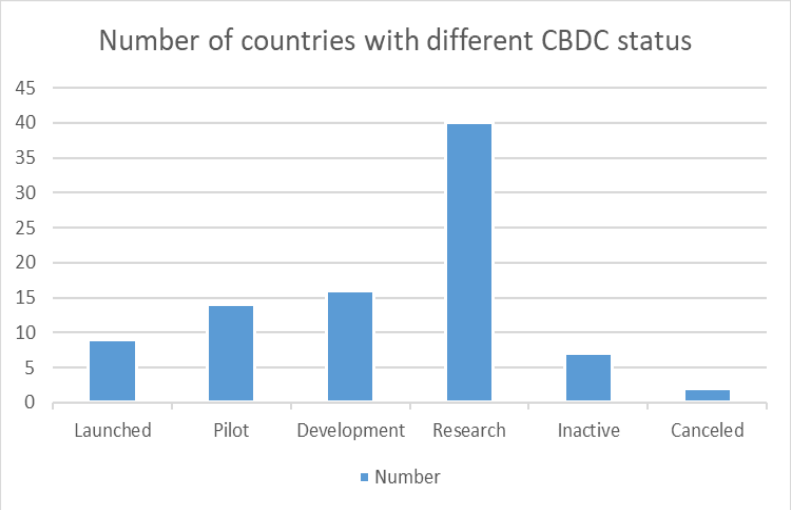


图 1-23：CBDC 不同发展状态的国家数量

来源：atlanticcouncil.org，火币研究院

在 CBDC 的探索进程中，中国走在了世界主要经济体的前列。根据中国人民银行行长易纲 11 月的最新发言，数字人民币依然在稳步试点过程中，在下半年有明显的提速。从试点场景看，已经从今年 6 月末的 132 万个扩展到 10 月 8 日的超过 350 万个，累计开立个人钱包 1.23 亿个，交易金额约 560 亿元。他也表示，下一步中国央行将根据试点情况，有针对性地完善数字人民币的设计和使用。一是参考现金和银行账户管理思路，建立适合数字人民币的管理模式；二是继续提升结算效率、隐私保护、防伪等功能；三是推动数字人民币与现有电子支付工具间的交互，实现安全与便捷的统一；四是完善数字人民币生态体系建设，提升数字人民币普惠性和可得性。

1.2.8 元宇宙兴起，社交巨头 Facebook 更名为“Meta”

2021 年，被称为“元宇宙元年”，元宇宙这一概念于 2021 年 Roblox 上市后迅速在网络中走红，但事实上，这个概念在早在 1992 年就已经提出：美国著名科幻作家尼尔·斯蒂芬森（Neal Stephenson）推出了自己的小说《雪崩（Snow Crash）》，书中描述了一个平行于现实世界的网络世界，并将其命名为“Metaverse”，小说中指出，所有现实世界中的人，在元界中都有一个“网络分身”，这也是关于元宇宙最初的定义。

随着元宇宙概念的火爆，传统巨头凭借敏锐的嗅觉纷纷入场，注册申请元宇宙商标，成为了当下不少企业正在参与元宇宙的凭证。抢占商标注册的背后，是搭建元宇宙基础设施与生态实力的竞争。从今年上半年起，包括 Facebook、微软等不少互联网巨头纷纷加入到了“元宇宙”的竞赛中。2021 年 10 月 29 日，Facebook 更是直接更名“Meta”，再次将元宇宙概念推向风口浪尖，市场情绪持续发酵。根据 Google trend 显示，全球“metaverse”搜索热度在 10 月中旬激增并持续保持在高位。中国大陆、新加坡、土耳其、缅甸和香港是搜索热度排名前五的国家和地区。在搜索热度最高的中国，也出现了抢注商标和专利的高潮。截至 2021 年 12 月 11 日，企查查数据显示，中国有关“元宇宙”的注册商标专利以达到 15000 多件。依靠各界的探索和创造，元宇宙正在走近人类。

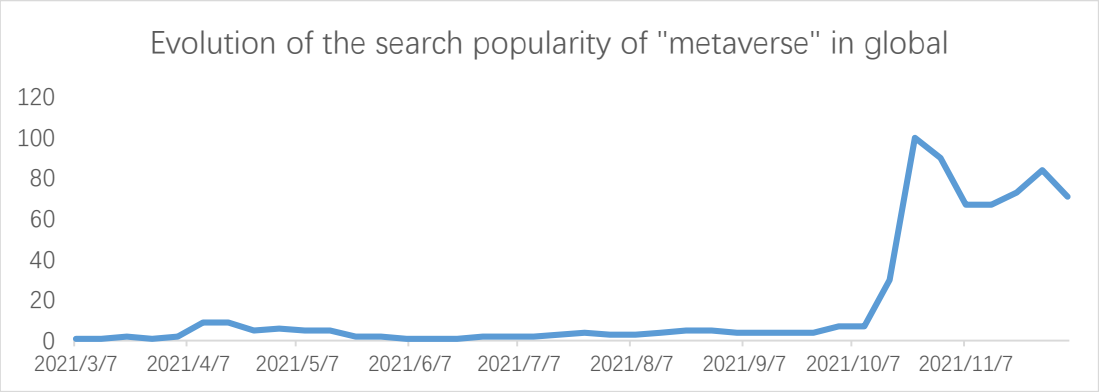


图 1-24：Metaverse 搜索热度

来源：Google trend，火币研究院

1.2.9 EIP-1559 上线，以太坊开启“燃烧销毁”时代

2021 年 8 月 5 日，以太坊正式迎来了伦敦升级硬分叉。在本次升级的内容中，EIP-1559 提案受到行业的广泛关注。

EIP-1559 提案包括两个主要内容：一个是 Gas 拍卖机制的改革，另一个是区块松弛机制。以太坊上的任何操作都需要付出交易手续费 Gas。在此之前，每个区块的 Gas 容量上限是固定的，Gas 由拍卖定价，用户各自出价，价高者赢得拍卖，这部分 Gas 完全奖励给负责打包交易的矿工。

EIP-1559 将每个区块的 Gas 容量上限翻了一倍，但区块的目标使用率是 50%，自动调节 Gas 费用。扩大空间能够缓解突发性的交易拥堵。同时它把 Gas 费用的结构分为“Base Fee”和“Tip”。Base Fee 根据区块空间使用率自动计算，使用率超过 50%就涨价，低于 50%就降价，费用对于每个用户都一样而且必须要交。Tip 用以激励矿工尽快将交易打包在新区块中，用户可以自行决定给多少钱。注意，这里的 Base Fee 不给矿工了，而是直接销毁。

EIP-1559 将每个区块的 Gas 容量上限翻了一倍，但区块的目标使用率是 50%，自动调节 Gas 费用。扩大空间能够缓解突发性的交易拥堵。同时它把 Gas 费用的结构分为“Base Fee”和“Tip”。Base Fee 根据区块空间使用率自动计算，使用率超过 50%就涨价，低于 50%就降价，费用对于每个用户都一样而且必须要交。Tip 用以激励矿工尽快将交易打包在新区块中，用户可以自行决定给多少钱。注意，这里的 Base Fee 不给矿工了，而是直接销毁。

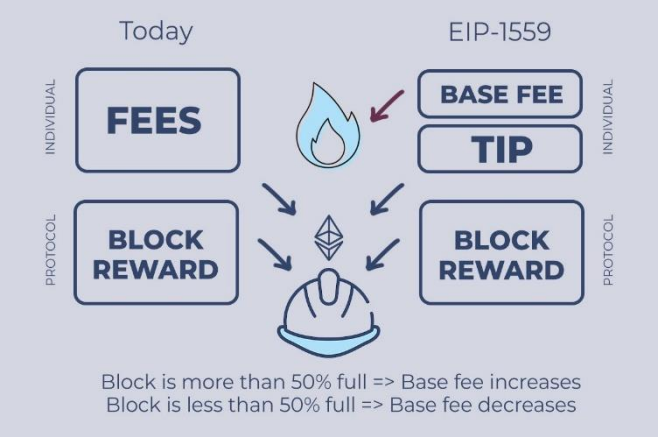


图 1-25：EIP-1559 前后 Gas 费用的结构变化

来源：thecoin.news，火币研究院

伦敦升级之前，社区有很多猜测：一是认为 GAS 费会大幅下降，二是认为矿工收入会大幅下降，三是认为 ETH 将会迎来通缩。提案稳定运行一段时间后我们发现，社区一个都没有猜对。

EIP-1559 的主要目的在于通过改善拍卖中的信息不对称问题，提高 Gas 拍卖效率，而非降低手续费价格。根据 Glassnode 数据，EIP-1559 生效后，以 ETH 计算的交易手续费并

没有大幅下降，尽管不能获得 Base Fee 的收入，矿工以 ETH 计算的收入仅有小幅下降。而考虑到 ETH 价格的上涨，以美元计算的交易手续费和矿工收入都上升了。

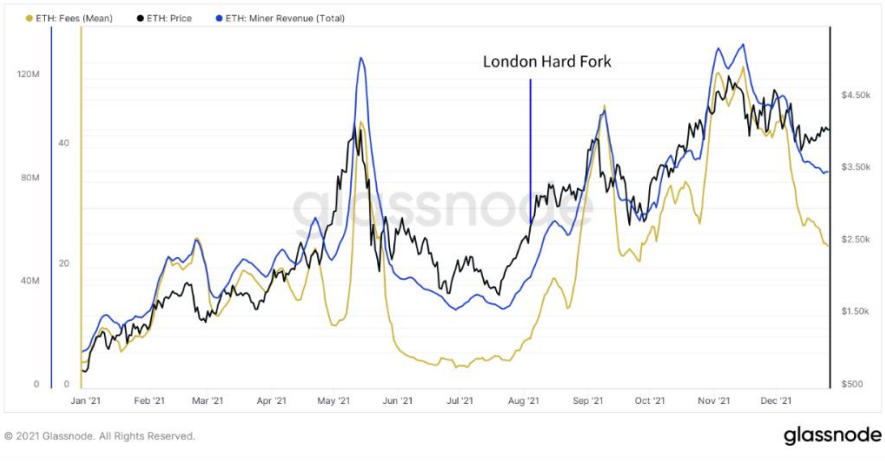


图 1-26：EIP-1559 提案生效后以太坊交易手续费价格和矿工收入，以 USD 计价

来源：Glassnode

EIP-1559 销毁 Base Fee 的主要目的是防止矿工自己生成交易来抬高 Base Fee，并解决“经济抽象”问题，强化 ETH 在以太坊的地位，并不是造成 ETH 的通缩。根据 ultrasound.money 数据，截止 12 月 12 日，EIP-1559 已销毁 ETH 超过 117 万枚，占此期间 ETH 发行量的 68%。它让 ETH 的年通胀率从 4.4%降到了 1.3%（近 1 个月平均值），然而它没有让 ETH 进入通缩。

1.2.10 区块链游戏 Axie Infinity 收入超过《王者荣耀》，进入全球前三

今年区块链领域最受欢迎的动物有 2 种，一种是狗，另一种是小精灵，在游戏 Axie Infinity 里能战斗、能繁殖、能给玩家带来收入的 Axie 小精灵。

Axie Infinity 是今年区块链游戏领域崛起的标杆。玩家操控游戏内的 NFT 小精灵“Axie”进行战斗、繁殖等活动，游戏简单易上手，画风可爱。更重要的是，它建立了“Play to Earn”的新范式。这是一套完整的经济体系：玩家购买 Axie 进入游戏、玩游戏获得游戏币、使用游戏币升级 Axie、出售游戏币或者 Axie 赚取收益。同时它推出了侧链 Ronin 以降低玩家的手续费并提升游戏体验。此外，还有游戏工会为没有钱购买初始 Axie 的玩家提供租赁服务，让更多玩家能够先玩起来。从 2021 年 Q2 开始，Axie Infinity 的活跃玩家快速增长，日活用户数从 100 以内增长到了 10 万人以上，收入同样暴涨，单日最高收入 1848 万美元，甚至一度超过热门手游王者荣耀。近一年来，Axie Infinity 收入高达 12 亿美元，排在所有 DApp

第一名并远远领先其他项目。

图 1-28：近 1 年来所有 DApp 收入

来源：oklinktokenterminal

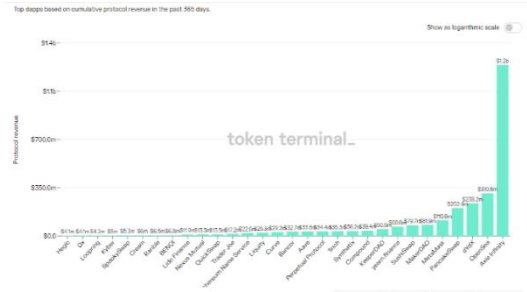


图 1-29：游戏用户数量增长趋势

来源：DappRadar

Axie Infinity 的火爆带动了整个区块链游戏行业的繁荣。根据 BGA 在 10 月发布的区块链游戏报告，10 月平均每天有超过 200 万个唯一活跃钱包（UAW）连接到 DApp，与游戏相关的 UAW 数量占各类应用总数的 55%。游戏也成为了资本关注的焦点，截止 11 月，今年区块链游戏领域共收到投资金额超过 37 亿美元。

第二章 金融篇

2.1 比特币资产正式进入主流

自 2009 年诞生以来，比特币就备受世人的关注，伴随的争议也一直不断。经过近十二年的发展，比特币的价格和市值一路高涨，但仍然没有摆脱“小众”和“极客”的标签。无论是在国内应用还是跨境支付领域，多数央行将比特币等加密数字货币视为一种利基2或不重要的产品。

但从 2021 年起，比特币作为小众另类投资品的资产定位似乎开始发生改变，欧美等国的上市公司开始大量买入比特币。包括马斯克旗下的特斯拉公司、全球最大的资产管理公司黑石（BlackRock）、美国移动支付巨头 Square 在内的众多大型上市公司纷纷斥巨资买入比特币。

在机构投资者纷纷买入比特币现象的背后，正如桥水基金（BridgeWater）创始人瑞·达利欧所言：“比特币正在成为一种能够代替黄金的数字资产。”

本轮比特币牛市中，机构投资者的资金开始流入比特币市场，产生更大规模的交易资金，从而引起比特币价格飙升。通过灰度信托基金能够观察到机构投资者大规模入场的信

[2] 指小众、专业化的产品

号：GBTC 基金有 80%的份额来自机构投资者，而从去年下半年开始，GBTC 的持仓量就开始迅速增长，意味着大量的机构资金开始涌入比特币领域。

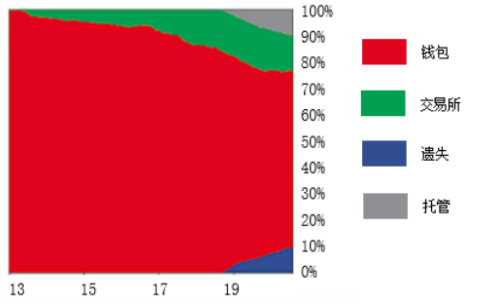


图 2-1：比特币现货分布情况

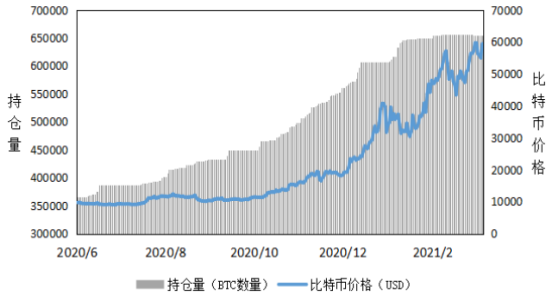


图 2-2：灰度信托基金比特币持仓情况

来源：火币研究院

比特币被越来越多的机构投资者认同的背后，是比特币自身特有的属性和全球宏观经济形势发生深刻变化后的产物。

首先，基于稀缺性（BTC 有总量上限）、易分割、方便携带、全球流通等与黄金相似的特点，比特币被越来越多的人视为一种“数字黄金”。

其次是全球宏观经济形势的深刻变化，这是造成比特币发生结构性转变的根本原因。在 2020 年新冠疫情的冲击下，全球金融市场出现崩盘，即便是黄金、十年期美国债等避险资产也纷纷暴跌。

为了应对疫情带来的经济衰退，各国普遍采取极度宽松的货币政策，推高了市场的通胀预期。为了规避名义本金受损的风险，投资者囤积现金的需求自然演变成对黄金黄金和黄金替代品---比特币的需求，成为市场用来对冲高通胀的资产。正如 MicroStrategy CEO 表示：“未来的年均通胀率将达到 20%，极大地削弱了购买力，持有比特币比持有现金的风险更小。目前，比特币是唯一能让我们获得正收益的资产。”

2.2 DeFi 的变革演进

从 2020 年的 defi summer 到现在，短短一年多的时间，defi 锁仓量迅速增长到了 2543 亿美元，以太坊总用户地址数也快速增长至超过 4M。

今年以来，随着 defi 的爆发，以及以太坊网络的拥堵和高 gas，defi 生态开始向其他公链溢出。从二三月份的 heco 和 bsc，五六月份的 polygon，九十月份的 avalanche 和 solana，

到最近的 terra，各条公链的 defi 生态相继崛起，以太坊的 TVl 占比从年初的 95%将至现在的 63%。Defi 协议不管从规模、用户数、类型和生态丰富度方面，都在迅速增长。

图 2-3：defi TVL

来源：defi llama

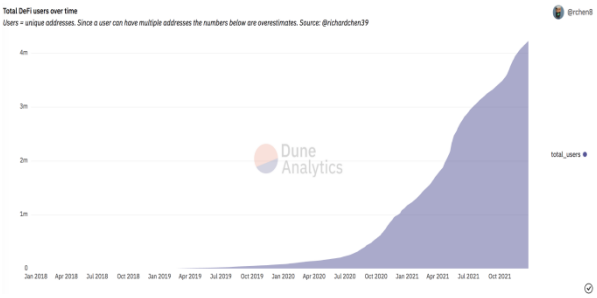
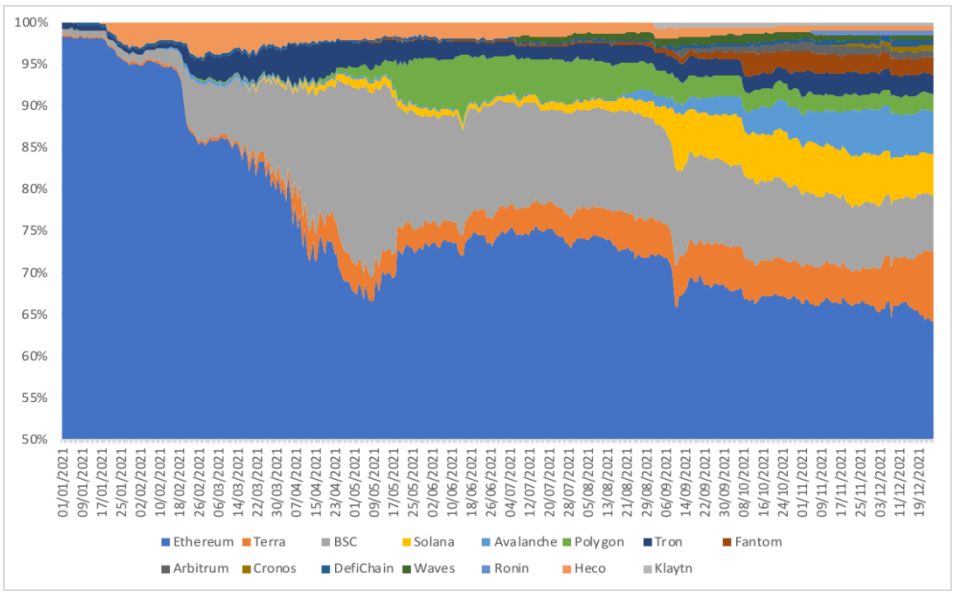


图 2-4：defi 用户地址数

来源：dune analytics

图 2-5：前 15 大公链 TVL 占比变化图



来源：火币研究院，defi llama

2.2.1 市场现状

2021 年以来，defi 的各个赛道 TVL 都在不断增长，占比最大的依然为 dex 和借贷类协议，此两类在总 TVL 中占比约 87%。

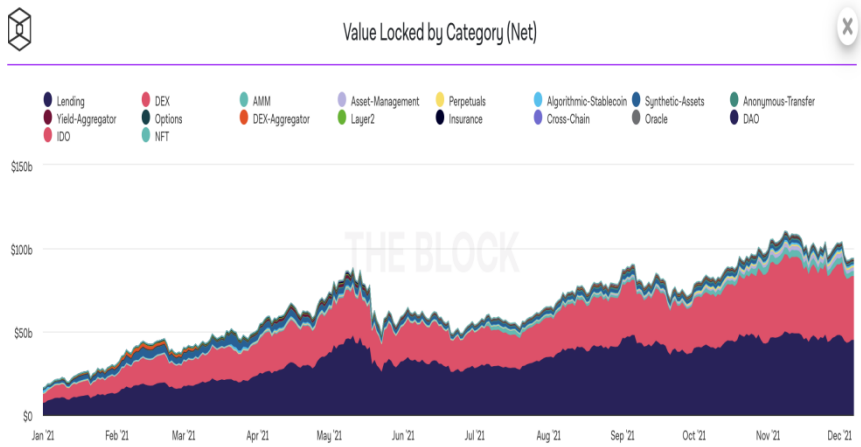


图 2-6：以太坊各类 defi TVL

来源：the block

2.2.1.1 DEX

以太坊上的借贷协议中，TVL 最高的 curve、uniswap、sushiswap 三者累计总 TVL 占比 94%，头部效应明显。过去的一年中，Dex 的优化，主要集中在如何降低滑点、减少无偿损失、提高 LP 资金利用率、以及在 layer2 和新公链上构建的订单薄 dex 等方面。

其中主流 dex 协议中，较大的更新为 uniswap 发布的 v3。v3 的更新主要是围绕资金利用率来进行的，这也与今年四季度的 defi2.0 的主题相契合。

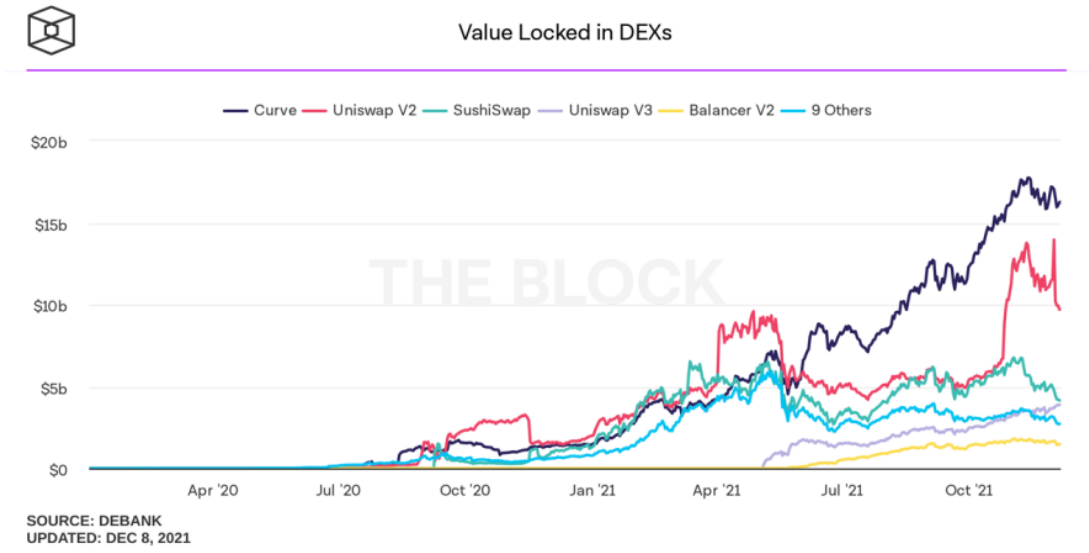


图 2-7：dex TVL

来源：the block

● uniswap v3

2021 年 5 月 5 日，Uniswap V3 正式上线，上线当日交易额便出现激增，v3 交易额在 v3 和 v2 总交易额中占比达到 10%。随后开始稳步增长，份额越来越大，截止至 12 月 6 日，Uni V3 交易量在以太坊主要 dex 中占比达到 66%，增速惊人。

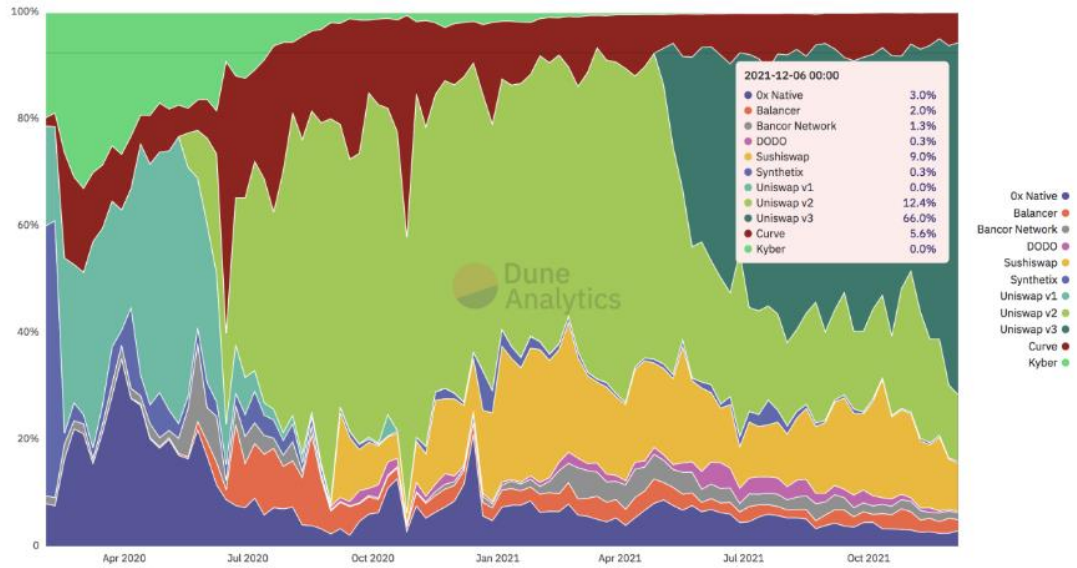


图 2-8：DEX 市场份额

来源：Dune Analytics

Uniswap V3 最核心的理念就是提出了聚合流动性（Concentrated Liquidity）：在指定的价格区间内提供流动性。

在之前的版本中，流动性沿 x*y=k 均匀分布。这种设计，能够在（0，∞）的任意位置提供流动性，但同时也意味着流动性池中的许多资产可能永远不会被利用。

Uniswap V3 允许 LP 选定一个比$(0, \infty)$更小的价格区间来提供流动性，将资金集中在交易较为活跃的区间，以提高资金使用效率。

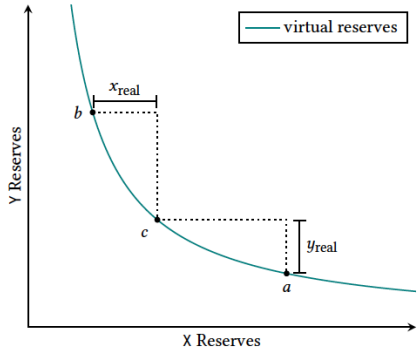


图 2-9：uniswap v3 做市曲线

来源：uniswap v3 whitepaper

除此之外，Uni V3 另一个较大的改动，是推出了更灵活的交易手续费池子。在 Uniswap V1 和 V2 中，每个交易对对应唯一的流动性池，统一收取 0.3%的手续费。虽然这一手续费对于大多数交易，过去一直以来都还算有效。但是对于一些交易对与一些池子显得过高（两个稳定币的池子），对于一些池子又显得过低（波动较大或者成交量稀少的代币）。

Uniswap V3 为每个交易对引入了多个流动性池，对应不同的手续费。同一个交易对，允许使用三种不同的手续费创建池子：0.05%，0.30%，1%。今年 11 月份，又新增了一个 0.01%的手续费选择。

从下图中可以看到，两个稳定币的交易对，交易量最大的都是 0.01%的最低费率池；交易对中涉及一个价格波动较大的币种，交易量最大的都是 0.05%或 0.3%费率的池子；交易对中有波动特别巨大的高风险山寨币时，LP 需要取得较高的手续费来弥补可能遭受的无偿损失，则需要在 1%最高费率的池子交易。

#	Pool	TVL	Volume 24H	Volume 7D ↓
1	USDC/ETH 0.05%	$244.18m	$1.26b	$8.45b
2	ETH/USDT 0.05%	$59.00m	$337.08m	$2.16b
3	DAI/ETH 0.05%	$45.30m	$314.16m	$1.65b
4	USDC/ETH 0.3%	$433.44m	$281.01m	$1.53b
5	ETH/USDT 0.3%	$195.38m	$146.62m	$915.98m
6	USDC/USDT 0.01%	$181.37m	$108.49m	$849.17m
7	DAI/ETH 0.3%	$126.26m	$139.91m	$814.09m
8	FEI/USDC 0.05%	$35.45m	$119.38m	$655.77m
9	DAI/USDC 0.01%	$62.58m	$80.47m	$483.46m
10	WBTC/ETH 0.05%	$71.52m	$46.09m	$356.75m

图 2-10：uniswap v3 中交易量前十的流动性池

来源：uniswap

uni V3 的一个宣传点就是，聚合流动性提高了资金使用效率。但是聚合流动性，只是改变了池子内部流动性供给的结构，并没有改变池子总流动性供给和需求，池子总的资金使用效率是不变的。

这也使得无形中引入了流动性竞争机制，更专业的 LP（比如上面案例中的 B）可以设置更为精准的流动性区间，从而获得更大的收益；而普通的 LP（比如上面案例中的 A）由于流动性区间设置的不合理，资金使用效率与 V2 相比更低。

根据 Topaz Blue 和 Bancor Protocol 在 11 月 17 日发布的一份报告，Uniswap v3 上 49.5%的流动性提供者因无常损失而产生负收益。

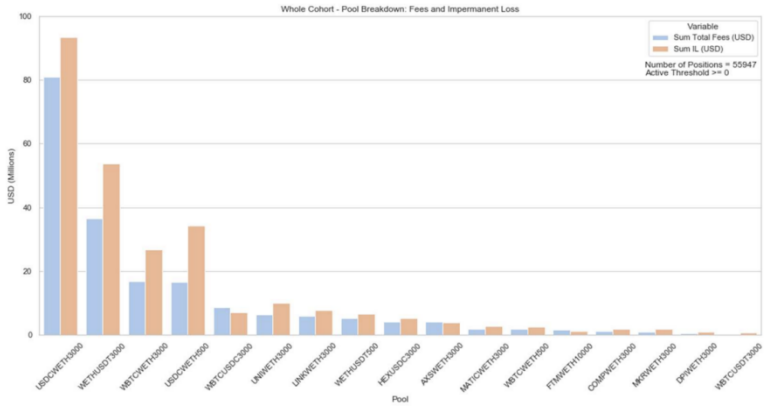


图 2-11：uniswap v3 LP 收益

来源：Topaz Blue、Bancor

2.2.1.2 借贷

以太坊上的借贷协议中，maker、compound、aave 三个协议累计 TVL 占比超过了 88%。借贷协议，在过去的一年中，优化主要集中在推出跨链功能、进行不同资产池之间的风险隔离、更高的 LTV 等方面。其中迭代较大的协议为 aave 发布的 v3。

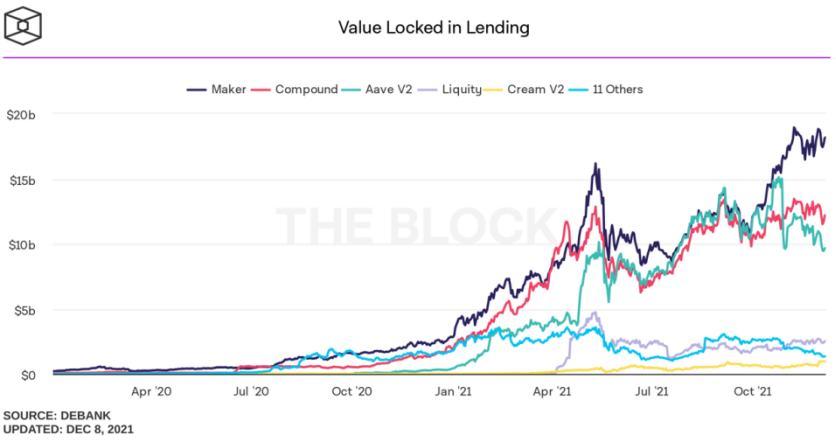


图 2-12：收益借贷协议 TVL

来源：the block

- Aave V3

2021 年 11 月 5 日，Aave 发布了 V3 版本，对资金利用率方面提出了一些改进方案。V3 版本的主要改进有三点：

一是 portal，允许资产在协议内跨链。Portal 通过桥接 Connext、Hop Protocol、Anyswap、xPollinate 和其他利用 Aave 协议流动性以促进跨链交互的解决方案，在原始网络上燃烧 aToken，同时在目标网络上上铸造他们。使得用户可以更简单的实现资产跨链。

图 2-13：Aave V3 桥接协议

图 2-14：Aave V3 eMode

来源：Aave

二是 eMode 模式，大幅提升了资金利用效率。V3 中会对资产划分类别，让临时有其他同类型代币需求的用户（比如抵押 USDT 借 DAI，抵押 ETH 借 stETH），可以使用更大的借贷率。

三是资产风险隔离。当社区成员提交在 V3 上创建新资产市场的治理提案时，可以选择将资产列为「隔离抵押品」，从而这些「隔离」资产的用户只能借入 Aave Governance 已许可的稳定币和指定的债务上限进行借贷，实现对借贷风险的有效隔离。这也使得未来一些高风险的长尾借贷成为可能。此前，rari capital 也在长尾借贷方面做了较多的尝试。

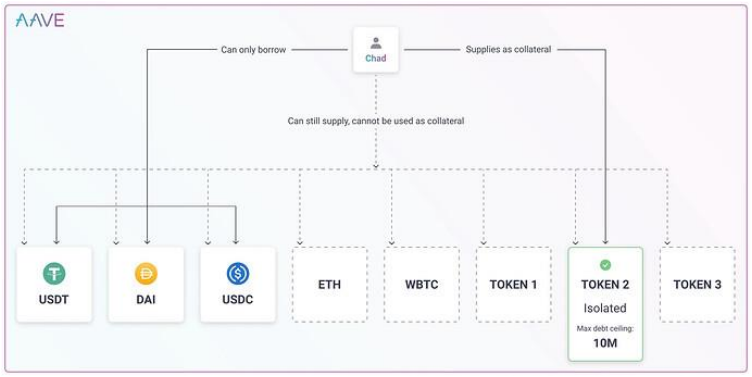


图 2-15：Aave V3 资产隔离

来源：Aave

总的来说，aave v3 没有特别大的创新，但是 portal 这个跨链功能值得关注。包括之前 maker 的 dai 桥，当流动性深度很好的协议开始推出跨链功能之后，未来会不会对现有的跨链应用产生威胁。以及已经在进行多链部署的 curve，拥深厚的稳定币流动性，也不失为跨链桥的较好人选。

2.2.2 Defi2.0

去年夏天开始，由 compound 提出“借贷即挖矿”之后，引爆了 defi summer，使得流动性挖矿成为 defi 协议最常使用的机制。但流动性挖矿是把双刃剑，同时也带来了一些问题。

最近在有一些协议，在此基础上做了一些新的改进和创新，提出了 defi2.0 的概念。相较于 defi1.0，defi2.0 主要流动性和资金利用率上有所改进：

A. 更好的流动性解决方案

Defi1.0 开启的流动性挖矿，虽然创新性的解决了链上早期的流动性问题。但是流动性提供者就是无情的挖提卖机器，没有任何忠诚度，一旦收益下降，流动性立马就会枯竭。而且高额的流动性补贴，造成了矿币的通胀，使得后期矿币的价格萎靡不振。

Defi2.0 创新性的提出了 POL 和 Laas 这两种更好的流动性解决方案，弥补了 defi1.0 的流动性解决方案的弊端：

- protocol-owned-liquidity（POL）

POL（protocol-owned-liquidity）的模式，使得协议能够以较低的成本，拥有自己的永久流动性，并将这部分流动性永久锁定。这种模式改善了流动性挖矿模式依赖高额补贴来维持流动性且流动性在长期不足的弊端。

最早提出这个概念的，是 OlympusDao 中的债券机制，用户可以以一定的折扣价格，使用 OHM/DAI、OHM/ETH、OHM/LUSD 等 LP 对来换取 OHM，而债券没有赎回机制，使得这些 LP 对流动性可以永久归协议所有，进行永久锁仓。从 OHM 的运行结果来看，sushi 和 uni 上的 OHM 池子流动性有超过 95%的为协议所持有。

Olympus Pro 还提供了一个债券销售的平台，出售锁定流动性方案给其他项目方。使得其他的协议，也可以在此平台出售债券，来获得 POL。

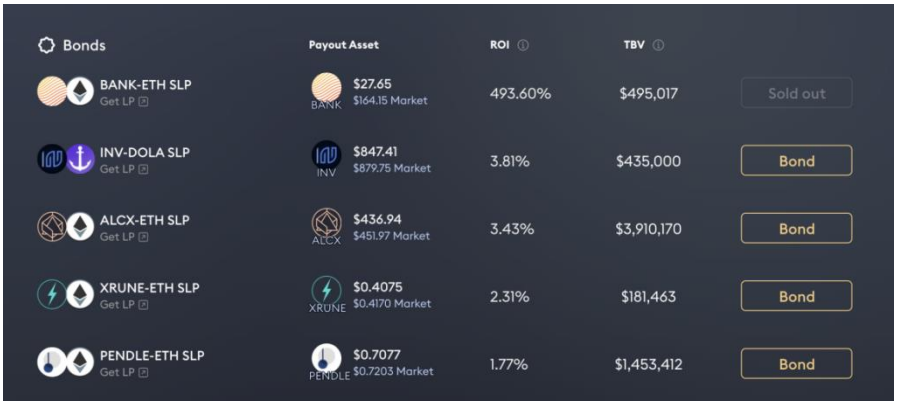


图 2-16：Olympus Pro 债券销售市场

来源：Olympus Pro

- **Liquidity-as-a-service（Lass）**

Liquidity-as-a-service（Laas）的模式，指为其他协议提供增加流动性的服务。这种模式可以帮助一些初创的去中心化项目提供流动性。初创项目早期往往需要花费大量的资源和精力来解决流动性不足问题，不管是引入中心化的做市商，还是通过 yield farming 的形式，成本都是非常高昂的。Laas 就解决了这个问题。

这种模式的代表，为流动性引导协议 Tokemak。Tokemak 通过引入流动性引导者 LD 的角色，让 LD 可以通过质押 TOKE 代币来引导用户存入资产的流动性去向。项目方可以通过质押 toke 代币，使用较为低廉的成本获取持续的流动性。

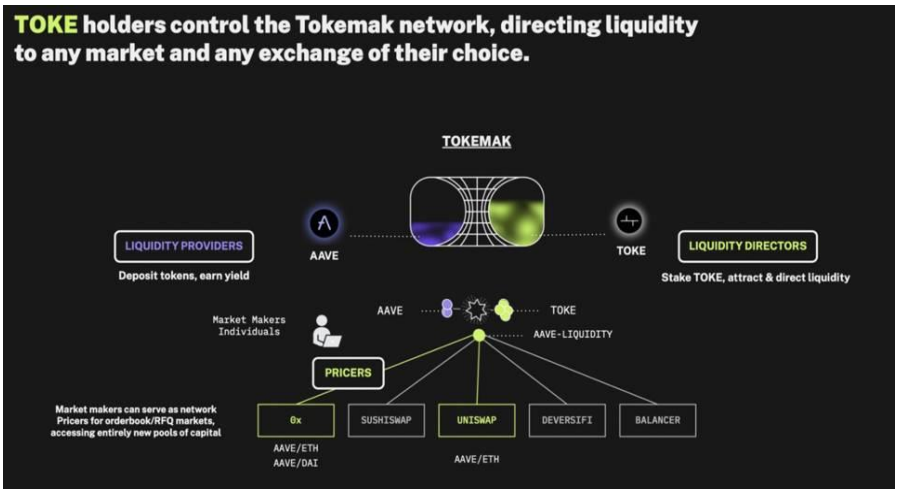


图 2-17：Tokemak 运行图

来源：Tokemak

B. 更高的资金利用效率

- **释放生息资产流动性**

在 defi 1.0 中，像 xSUSHI, veCRV, yvVault 等这类生息资产持有用户，只能定期获得相应锁仓协议的收入分红或投票治理权益。但由于不支持市面流通或交易，用户的很多生息资产只能躺在钱包里，无法被高效利用。Defi 2.0 通过释放这些闲置资产的流动性，使用户可以获得更高的资本利用率。

较为代表性的协议为 Abracadabra，用户可以把 yvUSDT 、 xSUSHI 等生息资产存入，然后用生息资产作抵押，铸造稳定币 MIM(Magic Internet Money)。MIM 与 USDT、DAI 、USDC 这类稳定币一样，允许在市场上流通和交易。用户拿到 MIM，可以比如在 curve 的 mim-2crv 进行挖矿，也可以比如换成 USDT，存入 YFI 中，拿到 yvUSDT 再去 Abracadabra 中借出 MIM，进行循环借贷。通过这种方式，把原本闲置无用的生息资产利用了起来，从而提高了资金产的利用率。

Collateral	LTV	Initial Max	Interest
yvWETH	75%	300M	1.5%
yvUSDC	90%	300M	0.8%
yvYFI	75%	80M	1.5%
yvUSDT	90%	300M	0.8%
xSUSHI	75%	80M	1.5%

图 2-18：Abracadabra LTV

来源：Abracadabra

上表是 Abracadabra 的质押借款率 LTV（loan-to-value），以 USDC 为例，90%的质押率，如果利用这种循环借贷的模式，假如有 100USDC，存在 YFI 中，拿到的 yvUSDC 去质押，可以贷出来 100*90%=90MIM，MIM 换成 USDC 再去 yfi 中质押，拿到的 yvUSDC 可以贷到 90*90%=81 MIM，然后这 81MIM 可以再继续进行循环贷。把杠杆拉满的话，由等比数列求和公式可知，一共可借出 90/(1-90%)=900MIM，也就是说，可以放大 9 倍的资金量，而且都是稳定币之间的借贷，理论上是没有什么清算风险的。

- **未来现金流前置**

defi 2.0 中，还通过提前使用未来的挖矿收益，前置未来现金流的方式，提高资金利用率。

比较有代表性的是 Alchemix 的「自我偿还贷款（self-repaying loan）」，允许用户将 DAI 存入 Alchemix，铸造出存入金额 50%的 alUSD，存入的 Dai 将部署到 Yearn Finance v2Dai vault 中赚取收益，用于偿还 alUSD 债务。只要时间够久，借出来的钱就自动被还清了。不存在清算风险，借贷设置也非常灵活，没有最短的锁定时间和到期日期，可以随时偿还债务来退出头寸。通过这种未来现金流前置的模式，允许用户提前使用未来的利息收入，提高了资金周转效率。

总的来说，defi 2.0 主要是在流动性和资金利用效率上，对原有 defi 协议进行了一些小改进和微创新。除此之外，defi 2.0 中，社区的作用也变得越来越重要，以及社区之间的联动也变得更为紧密。

2.3 链上衍生品的崭露头角

链上衍生品可分为六大类：永续合约、期权、合成资产、利率衍生品、二元期权和波动率指数。其中永续合约最成熟，应用也最广泛。

链上衍生品具备 5 大优势：没有中心化交易所运营商，长期来看费用更低；访问无需许可；用户自持资金，没有交易对手风险；交易品种无许可，任何有公开喂价的资产都可以被交易；无提款限制或交易规模限制。但是当前部分链上衍生品由于体量较小，存在交易体验较差、流动性不足、事故责任主体不明确等问题。

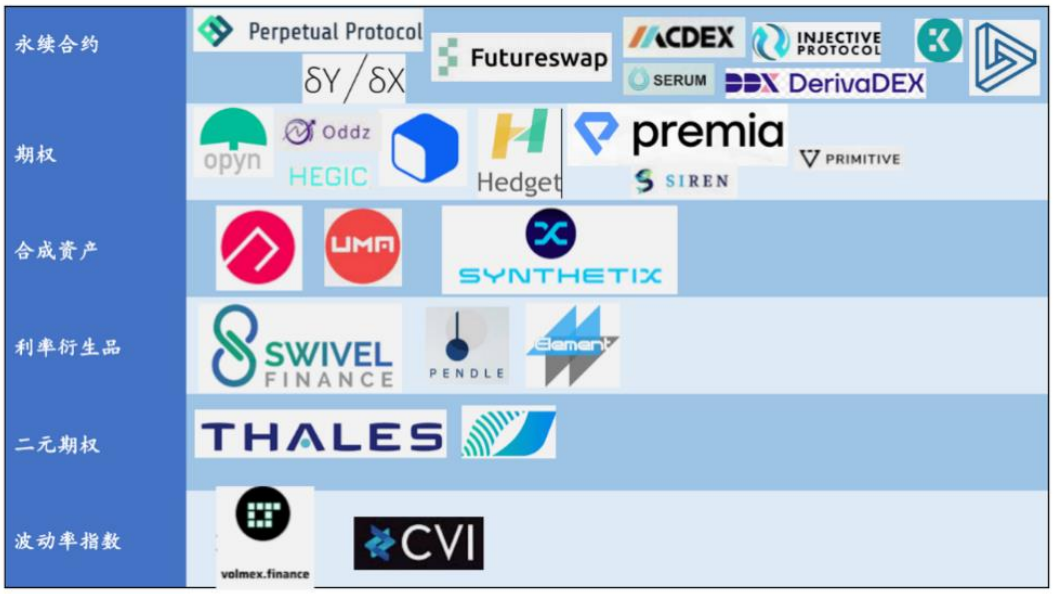


图 2-19：链上衍生品全景图

来源：火币研究院

2.3.1 永续合约：

最早是由 BitMEX 在 2016 年提出的，永续合约具有无需展期，且单一产品 流动性聚集的特点。代表产品包括 dydx，Perpetual Protocol，Futureswap 等。

稳定机制的工作原理可以概括如下。永续合约的多头需要每天支付空头资金费用(Funding Fees)。资金费用的计算公式为(mark price-Index price):mark price 为合约的交易价格;Index price 为标的资产的实际价格。如果合约价格远高于标的资产价格，多头将会支付高额的 Funding Fees，导致多头卖出合约，从而拉低合约价格，促使合约价格与现货指数价格保持一致。

- **项目：dYdX**

dYdX 是最早成立并推出可用产品的去中心化衍生品交易所，采用订单簿模式。底层架设在以太坊二层网络 Starkware 上，运营模式相对其他 DEX 更接近于中心化交易所。目前由于交易挖矿的推动，以及 9 月末的境内监管，导致大量用户涌入衍生品 DEX，以及 epoch1 的结束导致交易量激增，令 dYdX 在衍生品 DEX 中排第一。

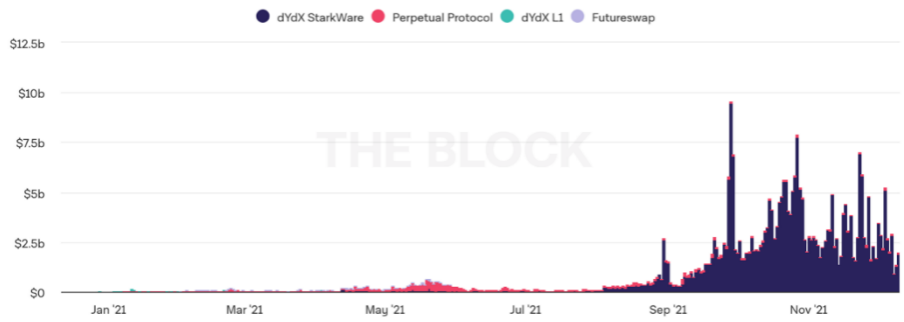


图 2-20：永续合约交易量

来源：The Block

dYdX 包含永续合约交易、保证金交易和现货交易。交易业务中最核心的撮合环节是在链下完成的，再由 Stark Contract 将数据打包上链。这个环节在本质上与 CEX 没有根本性区别，在交易上都由专门的做市商、Maker 和 Taker 三方共同参与，这也是 dYdX 的交易体检良好，与 CEX 交易界面相差无几的关键原因。

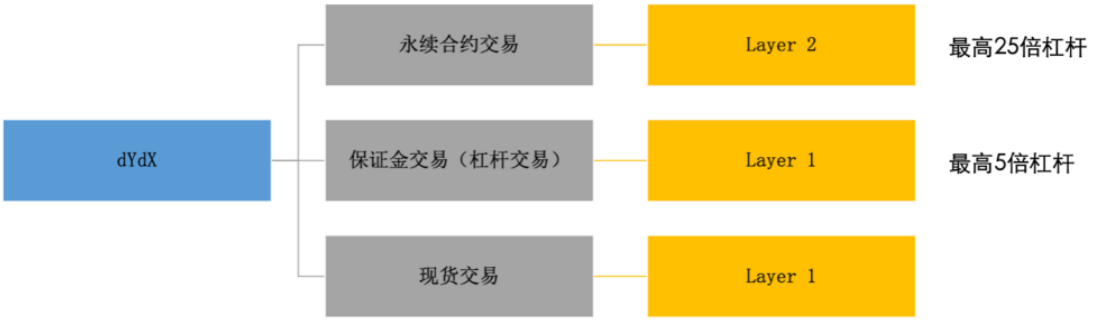


图 2-21：dYdX 产品业务线

来源：火币研究院

2.3.2 期权：

Opyn 是老牌期权项目，占据绝大部份链上期权的交易量份额。Opyn 构建的集成协议 Ribbon 促进了期权交易量的提升。Ribbon 将期权打包成一种收益率产品，解决了期权在 DeFi 中面临的两个挑战，即集中流动性和迎合散户投资者。Opyn 提供的 Perpetual Vault 模板允许任何人构建自己需要的期权。

- **永续期权：**

由 FTX 创始人 Sam Bankman-Fried 和加密机构 Paradigm 研究员 Dave White 在今年 5 月份提出。基本原理与永续合约相似。唯一的区别就是资金费用(Funding fee)是通过(mark price-payoff)，即合约的交易价格和期权回报的差值来计算的。举个例子来说，当 ETH 现货价格为$2900(Index price)，期权的行权价为$3000(strike price)，期权的交易价格为$150(mark price)，那么期权的回报则为$100(payoff)。依据上述公式，资金费用为$150-$100=$50/天。

Deri Protocol 是第一个实现永续期权产品的协议。利用与 Uniswap 相似的机制，利用一池子衍生品做交易者的对手方。流动性池作为流动性媒介，令交易员和 LP 之间进行基础代币的交易。头寸代币和流动性代币分别代表交易员的头寸和 LP 的流动性股票。该协议自九月上线以来，三个月总交易量已达到$130 亿。

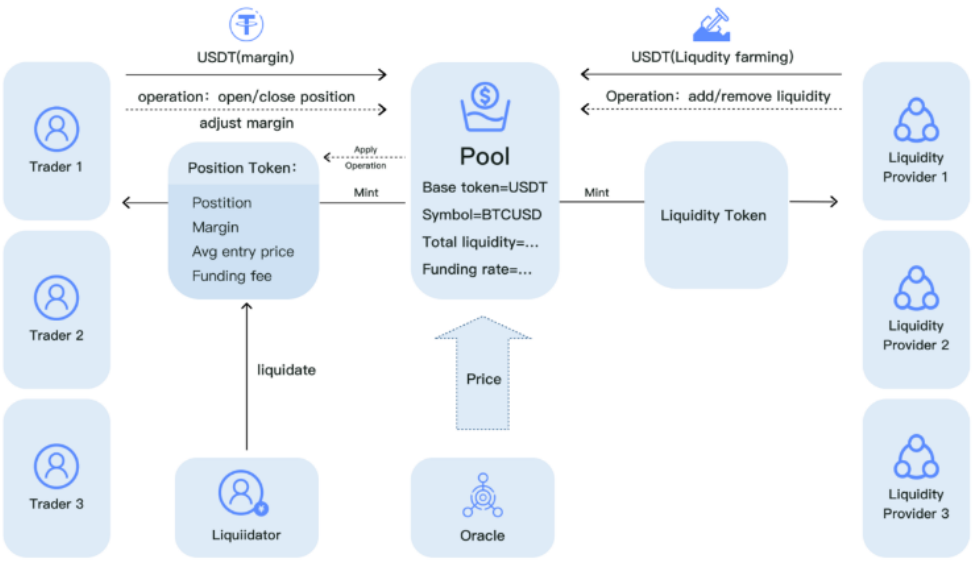


图 2-22：Deri protocol 运行机制

来源：Deri protocol whitepaper

2.3.3 合成资产：

合成资产是由一种或多种资产/衍生品组合并进行代币化的加密资产，DeFi 生态早期的合成资产以稳定币 DAI、跨链包装资产 WBTC 为代表，此后基于现实世界中股票、货币、贵金属、以及基于各种有交易价值的数据等的合成资产也越来越丰富。其理念是为投资者提供多种资产类别的风险敞口，但并不要求他们持有标的资产或信任托管人。

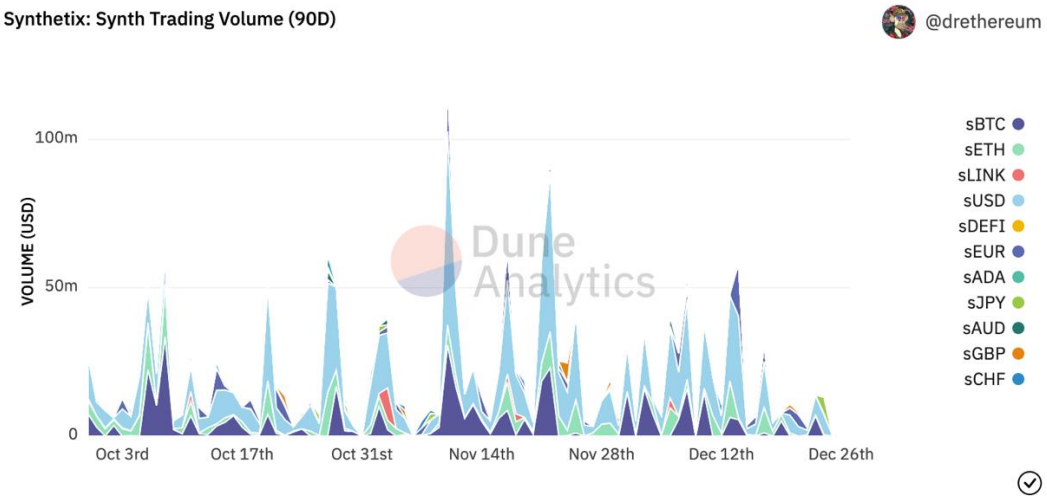


图 2-23：Synthetix 交易量

来源：Dune Analytics

合成资产在衍生品领域是继永续合约和期权外的另一细分赛道。根据 defillama 的数据，代表项目 Synthetix， UMA 和 Mirror 总 TVL 达 26.4 亿美元。Synthetix 上合成资产日均交易额通常在 5000 万美元以内，sBTC 和 sETH 是应用最广泛的资产。Mirror 中 mAssets 总市值达 3 亿 UST，日均交易笔数超过 3 万次，其中 mDOT 是最受欢迎的资产。UMA 已与 72 个项目部署了合成资产，通过代币投票决定上线合成资产，UMA 持币地址数为 1.7 万，流通市值 6.8 亿美元。

2.3.4 利率衍生品：

利率衍生品是指以利率为基础的衍生品，通常被用做对冲工具，以保护投资者免受市场利率变化的影响。在传统金融市场中，由于借贷利率的波动率较高，且绝大部分投资者风险偏好较低，因此利率衍生品已成为规模最大的衍生品市场。但在 DeFi 中，借贷协议和收益聚合器的收益机制几乎都是浮动的，对作为对冲的工具来说并不友好，因此利率衍生品的市场份额不高。随着越来越多固定利率的协议出现，利率衍生品市场的未来会更加广阔。

2.4 合规加密业务的如日方升

从 2020 年开始，全球的机构持续涌入加密市场，为市场带来了空前的繁荣，也将虚拟资产投资带向主流。目前，加密市场总市值超过 2.22 万亿美元，最近一年增长了超 300%。

图 2-24：虚拟资产市值

来源：tradingview

机构们也正以加密资产持有者、结构产品投资者、加密服务提供商等多种身份参与到市场中。直接或间接投资于加密资产的机构数量越来越多。根据 Coinbase（NASDAQ: COIN）Q2

2021 报告，其机构用户交易量达 3170 亿美元，占其总交易额的 68.6%；加密资管巨头 Grayscale Q3 2021 AUM 达 38.7B，其机构用户占比约 90%。随着越来越多的用户，尤其是机构客户的涌入，合规性也变得越来越重要。

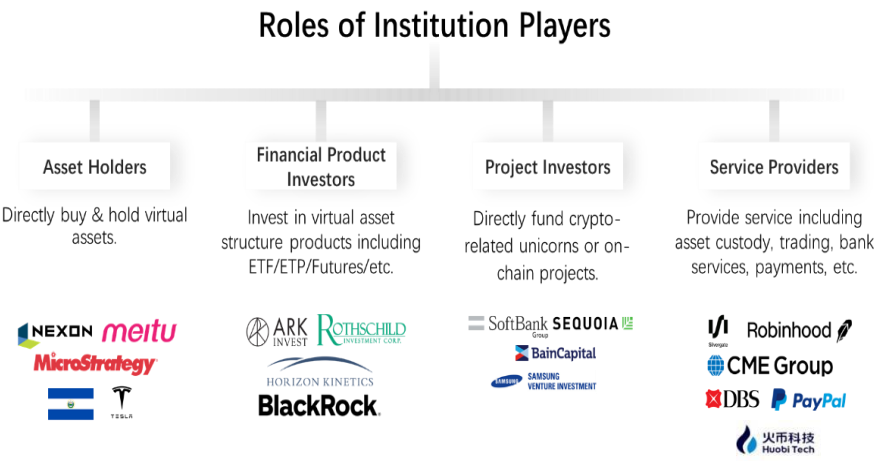


图 2-25：不同类型的机构参与者代表

来源：火币研究院

从行业成熟度看，受美国监管趋于稳定、传统金融机构纷纷进场投资或提供服务影响，美国的产品及服务更为多元，已形成了资管、借贷、OTC 等主经纪商配套服务，各服务均经历快速增长且有行业龙头出现。

今年，火币科技在合规业务方面也取得了很大进展，区块链业务收入同比增长超 5 倍。火币资管获得了香港证监会批准可管理 100%虚拟资产投资组合，并推出了五只基金产品。火币信托也注册成为香港信托公司，并且提供虚拟资产托管业务。截止 2021 年 9 月底，其资产托管规模突破 20 亿美元。Huobi Brokerage 旗下的 Huobi Lending 也开始为机构客户提供场外质押借贷服务。

2.4.1 借贷

- **用户画像及需求**

CeFi 借贷的主要用户包括个人（小散）、高净值客户、矿工、以及包括基金、做市商等专业机构，从资金规模上看以机构、高净值客户及矿工团体等为主。

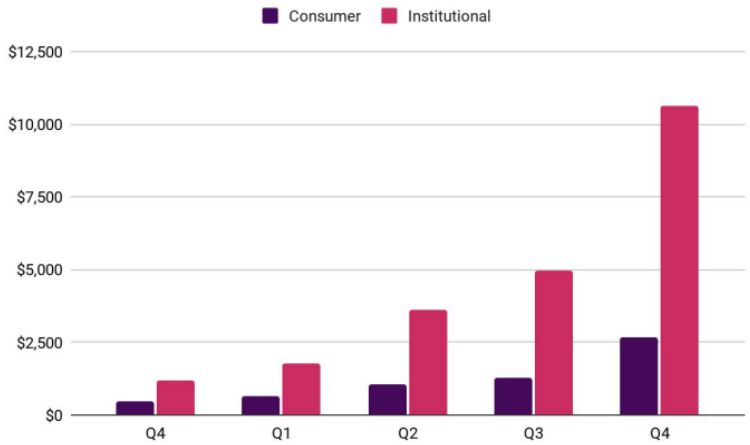


图 2-26：2019Q4-2020Q4 CeFi 借贷市场活跃在贷余额

来源：CredMark 2020 年终报告，火币研究院

根据 CredMark 加密资产信用报告显示，截止 2020 年末，CeFi 借贷市场3活跃在贷余额 $133 亿，其中零售贷款同比增速近 450%，机构贷款同比增速超 800%，显著高于零售端增长；年内机构贷款余额占比自 70%左右上升至 80%。

上述几类客户进行借贷的诉求各不相同，而平台一般会就其主要目标客户（尤其是非零售类客户）进行定制化产品开发及提供附加服务。贷出方的诉求基本一致，一般都是希望在持币的同时获得利息收入；借款方在倾向持有资产的基础上，借款动机差异较大。

	质押借贷（借款）	杠杆借贷（借款）
个人	其他币种短期需求，如参与流动性挖矿、获得 IDO 资质等	交易性需求，类似合约和 ETP
高净值客户	法币流动性；其他币种需求等	交易性需求
矿工团体	法币流动性；币种保值对冲等	套保对冲
基金/做市商等	平衡币种间头寸等	平衡币种间头寸，对冲等

表 2-1：不同 CeFi 借款人需求对比

来源：火币研究院

足额质押借贷场景下，CeFi 的非零售用户需求更有针对性。CeFi 提供的法币流动性对如高净值客户或矿工团体等拥有很大吸引力，可保证其在持有资产的前提下覆盖短期现实生活成本。同时，CeFi 借贷通过 KYC 及个人尽调等其他手段可为高净值客户提供最高可至 100%

[3] 《TheCryptoCreditReport Q4-2020》：Private Lending，统计来源基本为 CeFi 借贷，故本文中归入 CeFi 借贷。

质押率的增信服务，一定程度上缓解了借贷过程中资金利用效率较低的弊端。另一方面，据调查，矿工群体倾向于以最高的质押率借出最多的资金，这种行为增加了市场剧烈波动带来的清算风险，CeFi 更长的补仓时间及专人联系可降低矿工的风险，本质上是 CeFi 平台通过自由资产或风控承担了一部分客户风险。此外，投资基金、对冲基金及做市商等有平衡头寸需求的群体，为避免策略暴露一般希望更隐匿地进行大额借贷，CeFi 体系下可较好地保护其隐私，并为其一些特殊币种需求提供 OTC 服务。

综上，CeFi 质押借贷依靠其更“人性化”的服务满足不同用户群体的特定需求，从而形成粘性。其中如增信、风险分担、法币流动性、隐私性等是目前 DeFi 借贷产品较难提供的。

与质押借贷相比，Cefi 杠杆借贷场景下，由于可以提供更高的资金杠杆，客户需求主要以交易性需求为主，类似合约和 ETP，其中机构和有丰富经验的交易用户占比较多。同时由于杠杆借贷可以提供更高的资金抵押利用率，因此也会有矿工和做市商用来套保和对冲。

- **合规性**

合规视角下，目前整体 CeFi 借贷市场监管框架尚不明晰，各地区基本划归现行放贷牌照下展业且主要针对涉法币的服务，加密资产-加密资产的借贷规管由于针对加密资产本身的法律法规缺失而缺失。

	MTL	MSB	美国各州借贷	香港	海外
Genesis	/	BitLicense	/	/	PSA 豁免
BlockFi	20	2	14	/	/
Nexo	5	1	14	CR	加拿大 MSB；澳洲 ASIC、AUSTRAC 注册
OSL	/	/	/	1 号/7 号	PSA 豁免
Matrix	/	/	/	TCSP	PSA 申请
Copper	/	1	/	/	英国 CiSP 成员

表 2-2：部分 CeFi 借贷项目牌照矩阵

来源：火币研究院

观察主流的一些 CeFi 借贷平台的牌照发现，美国企业如 BlockFi、Nexo 均在不同州取得了放贷人牌照，但龙头 Genesis 并未公布其是否拥有借贷类牌照。结合美国各部门目前对加密资产本身的监管缺乏一致性可推测，该地区对非法币类加密借贷仍处于主动合规阶段，尚无定论借贷牌照是否是必须的。

整体看，CeFi 借贷市场的盈利模式清晰简单、目标客群定位明确。拥有流量或品牌信誉、加密货法币资金、合规渠道的企业可相对快速地推出产品。但这也意味着产品同质化程度较高，在赛道逐渐有热度的情况下市场竞争将加剧。此外，行业监管尚处于早期，合规上存在较大不确定性。

2.4.2 托管

● 用户画像和需求

在加密资产的保管方面，由于在线保管有黑客攻击风险，而离线保管又有硬盘丢失风险。因此对于机构投资者来说，自行进行保管风险更大，需要专业托管服务，使得保证资产安全同时，方便管理和交易。美国证券交易委员会 SEC 也规定， 机构投资者持有的客户资产超过 150,000 美元，必须将其持有的资产存放在“合格的托管人”处。在此背景下，诞生了大量的托管服务需求。

托管服务的使用方主要为加密货币交易所、OTC 柜台、做市商、基金、借贷公司、支付处理公司等机构。

托管服务的提供方主要为硬件钱包服务商、交易所、传统金融机构如信托服务商、银行等。服务内容包括：资产保管、资产报告、投资监督、财务报告、保存纪录等。

● 合规性

托管是较为基础的一样服务，各家合规机构之间的主要在技术安全性以及是否为托管资产上保险上有一些差异，但总体差异不大。

各家机构的主要竞争点，在于在托管基础上，衍生出的其他服务，比如对交易、资管、defi 等方面的支持。

公司	对象客户	牌照相关	技术安全性	财务安全性
Genesis	机构客户	Bitlicense	冷存储与 MPC 的混合技术。	未提及
Gemini	机构客户+个人客户	NYDFS 的 Trust 信托牌照	1，完全离线的冷存储。 2，多重签名技术、基于角色的治理协议，多层生物识别访问控制，物理安全	定期接受审计，遵守传统金融机构的资本公积要求、合规标准。
BitGo	机构客户	南达科他州银行部的 Trust 信托牌照	多重签名、多用户策略控制、密钥管理、高级安全配置	定期接受管理机构的审计， 在资本化、反洗钱程序、保密、审计、报告、存储方面，符合合规标准。
Coinbase	机构客户	纽约州特许信托、BitLicense	1，完全离线的冷存储。 2，安全设置：M of N 签名共识、地址白名单、胁迫协议设置	定期接受外部财务审计

表 2-3：部分合规托管机构信息

来源：火币研究院

2.4.3 资管

资管方面，整体市场规模还小，但增长速度很快，且不同形态的产品正在陆续出现。截止 Q3 21 市场整体规模近一年增长近 600%至 51.4 B，其中 Trust 类产品长期占据 80%以上份额。Trust 类产品持续占据市场背后的逻辑，是为已持有虚拟资产的机构提供一种金融产品敞口获得纳税及审计便利；而对未持有资产的机构则省去了存储问题和托管成本。

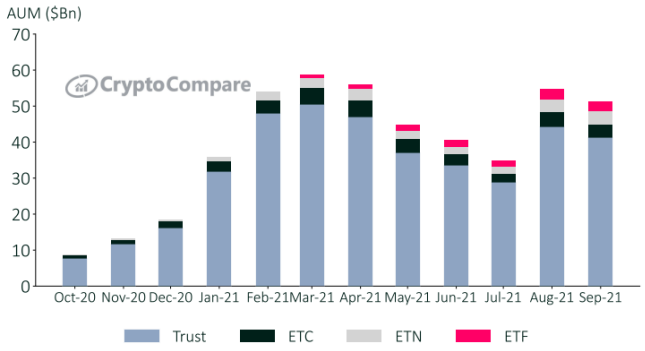


图 2-27：加密货币市场资管总额（$Bn）

来源：Cryptocompare

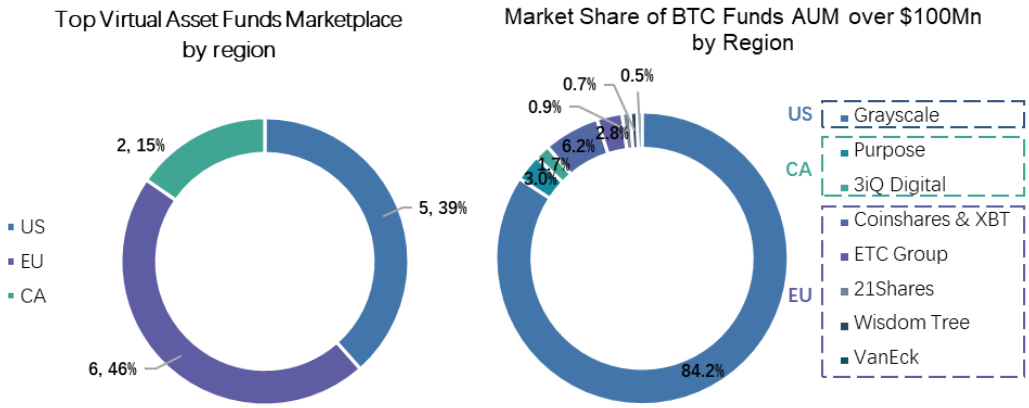


图 2-28：产品的地域分布

来源：火币研究院

从产品的地域分布上看，目前净值过亿的资管产品主要位于美国、欧洲和加拿大境内，但美国私募产品更多。从 BTC 产品 AUM 的地域分布看，美国、加拿大、欧洲过$100M 产品分别占 84.2%、6.8%和 4.7%，灰度以近乎垄断的地位占据欧美市场。

此外，机构的需求也持续刺激着传统金融和加密行业的创新。如近期德国 BaFin 首次通过的游戏发行商证券化代币 EXO、新加坡 Cyberdyne Tech Exchange （CTX）已推出的碳中和代币（CNTs）等；加密世界则有支持实物资产抵押进行链上稳定币借贷的项目 Centrifudge、NAOS 等。

整体看，美国、加拿大、欧洲等区域虚拟资产行业发展迅速，这主要是由于当地合规进度较快、行业上下游服务商众多，保证了客户在整个产品使用周期都有完善且稳定的配套服务可用，且整体合规风险较小。但亚洲市场用户基数大，且整体配套服务不完善，除交易外市场规模较小，也意味着极大的发展空间。

第三章 市场篇

3.1 流行文化的新宠儿---NFT

3.1.1 NFT 市场现状

NFT 全称为 Non-fungible Token，即非同质化通证，是一种记录在区块链上，不能被复制、篡改、切分的通证。NFT 因其独一无二、不可篡改的特性常被用于稀缺数字资产的确权。

2021 是 NFT 成为主流的一年。在 8、9 月，主流 NFT 交易平台 Opensea 的月交易额、月活均发生了 10 倍以上的爆发性增长。

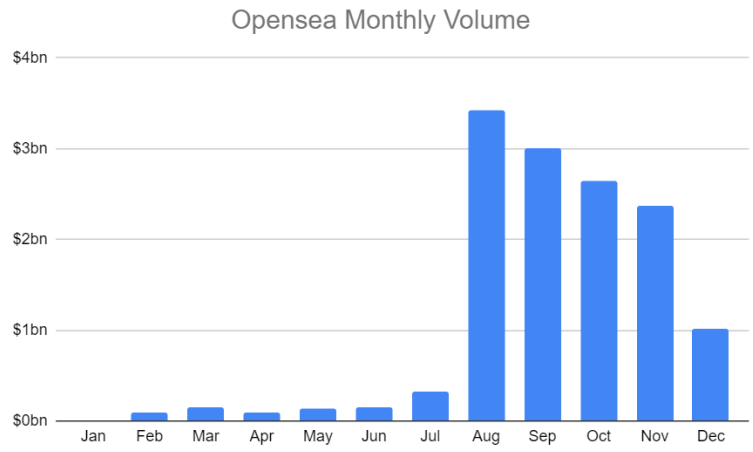


图 3-1：Opensea 月交易额

来源：Dune Analytics，火币研究院

NFT 市场的主要构成有艺术类，头像类，游戏道具三种。艺术类的代表作有 Beeple 和 Artblocks 的数字画作，大多为艺术家利用素材和 AI 算法生成；其内容较为抽象，受众以现代艺术收藏者为主，主要采用拍卖形式出售，价格较为高昂。头像类的代表作有 Bored Ape Yacht Club，是一组固定数量的、随机生成稀缺特征的、固定价格铸造的盲盒 NFT，其具有较强的社区属性与财富效应，受到大量加密原生用户的追捧，是项目数量最多、情绪最热的 NFT 市场。游戏道具类的代表是 Axie Infinity 里的小精灵 Axie，其作为游戏道具可以进行战斗获得奖励代币，或是进行新的 Axie 的孵化并售卖；游戏道具类 NFT 可以作为游戏的生产资料赚取收入，因而具有更为稳定的需求与更充足的流动性。

图 3-2：各类 NFT 代表作品

来源：Opensea，火币研究院

此外以 loot 和 rarity 为代表的实验性质的、自下而上可组合 NFT，以及元宇宙项目如 Decentraland 和 Sandbox 的土地 NFT，均是一定时间内的市场热点。

3.1.2 NFT 大放异彩的原因

我们认为以下四个因素是 2021 年的 NFT 市场繁荣的推手：

1. NFT 满足产权的四大特性，即其是明确的（内容和所有人可验证）、专有的（NFT 具有稀缺性）、可转让的、可操作的（NFT 可编程，可在区块链内互操作）。这样的产权是一个资源配置高效的市场的必要组件。

2. NFT 具有出圈属性，即 NFT 能赋能外部 IP，是加密领域少有的适合与传统领域结合的赛道。可以观察到非加密原生 IP 如可口可乐快速进场发行 NFT，同时非加密原生玩家正在购买 NFT，如 NBA 球星库里屡次购买 BAYC。

图 3-3：NFT 与传统领域的结合

来源：Opensea，火币研究院

3. NFT 满足社交需求。我们发现 Beeple 作品的高价买家都是加密领域的资深人士，比如以近 7000 万美元价格拍下 Beeple 作品的买家印度裔买家 Metakovan，是 NFT 基金 Metapurse 的创始人。在马斯洛需求层次理论中，人的需求分成五个层次，并且需求是由低到高逐级形成并得到满足的。对于加密数字货币行业众多的新贵而言，低层次需求已经得到

满足，然而却未真正获得社会的认可和尊重。所以当看到 NFT 开始出圈，受到世界的瞩目时，“币圈人士”也愿意去花钱围观实现自己的顶层的尊重需求和自我实现的需求。

4. NFT 基于以上三点，是理想的炒作对象。所以大量投机资本涌入，创造头部 NFT 的财富光环；尔后散户入场，进一步扩大市场规模，尤其是盲盒模式进一步创造了散户的财富奇迹。

3.1.3 NFT 的问题与潜在解决方案

从 10 月起，NFT 市场的热度有所下滑，虽相比年初仍维持在较高水平，但大量 NFT 的地板价（24 小时最低成交价）的波动较大。

图 3-4：Bored Ape Yacht Club 地板价变动情况

来源：Opensea，火币研究院

NFT 市场的较大波动，和当前 NFT 存在的三个问题相关：

1. NFT 的价格发现较弱。因 NFT 头部项目数量稀缺，单价高，又不可拆分，导致 NFT 当前流动性稀缺，价格波动较大。目前有 Fractional，Unicly 等 NFT 碎片化方案，通过锁定 NFT 到合约然后铸造对应 ERC20 代币；但是 NFT 碎片化后具备了金融中“证券”的一些特征，存在金融监管的风险。除了碎片化，还有 Pawn.fi 一类的 NFT 点对点抵押借贷的方案，以及 Paradigm 提出的地板价永续合约方案（一种合成 NFT，可跟踪给定 NFT 项目的地板价，且可以通过锁定该项目 NFT 的途径来进行铸造，地板价永续合约让 NFT 持币者可以获得流动性并防御地板价波动，同时无需放弃对 NFT 的所有权）。

2. 支撑 NFT 的基础设施还有待建设。目前绝大多数 NFT 存在于以太坊一层网络，带来超高使用门槛；我们预计随着如 Immutable X、Solana 等 layer 2 和新公链的发展，NFT 的应用成本会快速降低。

3. 目前绝大多数 NFT 的使用价值匮乏。除游戏类 NFT 外，大多数 NFT 只有二级市场溢价，在市场情绪褪去后的流动性极差。我们认为 NFT 不是一个应用层的赛道，而是一个协议层的基础元件。创作者经济、游戏与元宇宙作为开放、低准入、互通的内容载体能为 NFT 带来巨大的使用价值；而 NFT 对数字内容的确权能够激励用户生成内容，这也是三类场景重要的特性。

3.2 MEME 文化的蓬勃发展

今年 Meme 币在加密货币市场是一个热门话题。它创造了今年的年度最大涨幅（SHIB，54 万倍），引发了一批企业家、投资家和加密货币从业者的热议，吸引大量新人进入市场，并频繁出现在圈内外媒体的报道中。它的背后 Meme 文化在这场风潮中起到了至关重要的作用，下面我们一起探究这场运动的原因和启示。

3.2.1 Meme 文化的含义

Meme 是通过模仿而传播的文化基本单位，也可以理解成文化的符号或者基因。它是 1976 年由英国进化生物学家 Richard Dawkins 在他的著作《自私的基因》中提出的，是指“在诸如语言、观念、信仰、行为方式等的传递过程中与基因在生物进化过程中所起的作用相类似的那个东西。”

3.2.2 Meme 币的特点

Meme 代币有如下 5 个特点：

代币发行量非常大，单价非常低。发行量为千亿、万亿的 Meme 币比比皆是，DOGE 和 SHIB 的发行量都是 1000 亿枚，而且 DOGE 每年还增发 50 亿枚。而它们的单价往往非常低，通常是小数点后跟着一长串 0，花 1 美元就能买到 3 万枚 SHIB。

代币分配方案强调公平，社区占比高，投资人、项目团队占比极少或者根本没有。一个比较极端例子是 SHIB，它把一半代币发送给了 Vitalik，另一半代币与 ETH 配对，在 Uniswap 上提供流动性，有很多项目效仿这种分配方案。

重视宣传和社区推广，参与人数多。DOGE 和 SHIB 依靠马斯克这个超级名人的流量加持，都用超过 200 万以上的 Twitter Followers，其他市值靠前的 Meme 项目则通过社区推广吸

引用户的注意。尤其是在 Meme 币涨势好的时候，“错过了 DOGE，不要错过 XXX”这样的广告语遍地可见。造富的神话和大力的宣传吸引了很多新人入场，他们都不知道那个后来抛售 Meme 币的 Vitalik 是谁。

价格波动非常大。由于 Meme 币社区中散户和新人用户占比高，很多人都是带着碰运气的心态投资，币价受群体情绪影响极大。一条推特就能推高币价，而马斯克说这（DOGE）是个骗局，价格也能应声暴跌 30%。大多数 Meme 币往往在一次暴跌之后就彻底消失在人们的视野之外。

实用性差。很多 Meme 代币诞生时并没有具体的目标和可行的发展规划，一个社会热点、一个流行词语就足以催生一种 Meme 币。很多项目在运行机制上、经济模型上完全没有创新，甚至在崩盘之前连产品都没有。

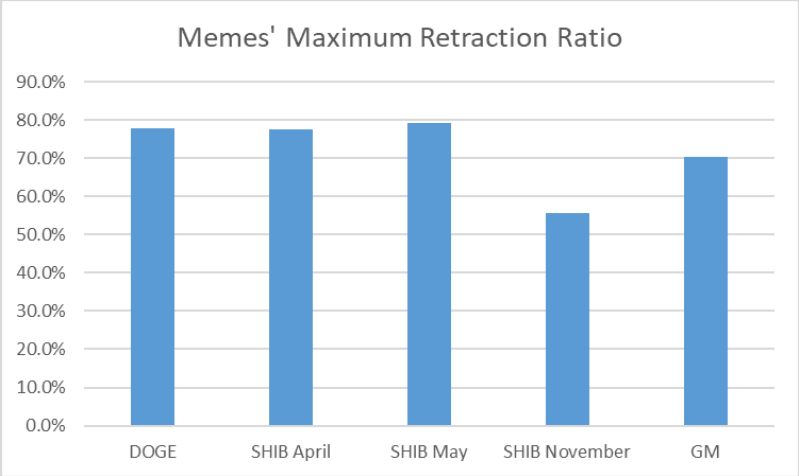


图 3-5：热门 Meme 币年度最大回撤比例

来源：CoinMarketCap，火币研究院

3.2.3 Meme 风潮形成的原因

首先，Meme 易于接受。DOGE 的柴犬 Logo 很有趣，它的诞生也是一种调侃行为，这也为后辈们建立了一种“行业标准”。大多数 Meme 币无关于货币的未来、金融的创新、互联网的变革等宏大的主题，它们就是一个符号+一个币，非常简单，一般人一听就懂。理解起来容易，获得大众的认同和传播也就容易。

第二，Meme 币完美符合了很多人的暴富幻想。在 Meme 币涨幅大，当有人展示出他在短时间内获得了成百上千倍的收益时，旁观者难免会产生 FOMO（Fear of Missing Out）情绪。又因为 Meme 币单价低，花很少的钱就能买到大量币，容易带给新手满足感，甚至产生亏钱

了也亏不多的错觉。人人都希望迅速致富，这是很多生意能够存在的原因。在 2021 年的加密货币市场，暴富幻想的存在方式是 Meme 币。

第三，Meme 币代表了一种反精英文化，或者叫草根文化的抬头。

无论是在政府还是公司，世界一直被精英阶层控制着，普通人的作用微不足道。不管在什么领域，总有少部分人会在很大程度上影响历史的发展，这太正常了。

区块链带着去中心化的理想而生，这是一个属于平民的世界吗？当然不是，区块链的世界也是由精英搭建而成。中本聪是加密极客，他们邮件组里的都是密码学专家；Vitalik 从小就会编程，他的老爸就是计算机科学家。除了这样的杰出人物以外，精英阶层在区块链的发展中占据着越来越重的地位。从去年起，大量传统金融机构开始配置比特币，比特币成为了华尔街和巨鲸们的筹码。不管是在运行机制还是经济模型，以太坊上的项目也在变得越来越复杂，以太坊成为了技术专家的竞技场。

那如果仅依靠普通人的力量就能够创造历史呢？在股票市场，有 WSB 组织起散户大战华尔街的故事，在加密货币市场，同样的事也可以发生。

普通人团结起来，你买 20 美元，我买 50 美元，谁都不卖，大家一起让一个代币涨到天上去。这个听起来有点不切实际的想法，就实实在在的发生了。

马斯克在 Meme 币的暴涨中确实起到了推波助澜的作用，不过他在加密世界可不是什么大企业家，他只是一个影响力大一点的普通人。由他带头，群众的集体情绪找到了一个出口，于是有了这一场群众运动。

普通人要的不多，他们只是想看到自己的力量，Meme 币帮他们做到了。

3.2.4 Meme 币的启示

首先，不管是高调还是低调，一定要干实事。大多数 Meme 币难以逃出这样的周期律：

高调宣传+社区追随+FOMO=一飞冲天。

光说不练+注意转移+获利离场+恐惧抛售=一败涂地。

而 DOGE 和 SHIB 跳出了上面两条公式，实现了可持续发展。根据 CoinMarketCap 数据，它们的市值之和占所有 Meme 代币总和的 97%，交易量占之和占比为 92%。这两只小狗能生存下来很不容易，尤其是 DOGE，自 2013 年底诞生以来，经历过 2 轮牛熊，期间无数代币归零，它却一直生命力顽强。除了实干，它们没有其他秘诀。

DOGE 的使用场景只有支付和打赏，但它用这样的基础功能做了很多对社会有益的事。DOGE 社区层筹集 DOGE 向牙买加雪橇队、为有特殊需要的儿童提供服务犬的慈善机构、植树节基金会和清除海洋垃圾的组织捐助。当然，也必须捐款多建一些狗窝。支付的应用场景不断扩大，包括 Coinbase Commerce、Binance Pay 等支付平台和美国 AMC 院线、旅行平台 GetYourGuide、巴西汉堡王等一大批商家支持 DOGE 支付。

SHiba Inu 在今年 7 月推出了去中心化交易所 ShibaSwap，交易额在所有 DEX 中排名前 30。发行了柴犬主题 NFT 并支持 NFT 艺术孵化器。此外，Shibarium 区块链和 Shiboshi 游戏的开发正在进行中。

它们用真实的行动续写了 Meme 币的公式：

社区持续活跃+真实应用=继续存活。

整体行情上涨+重新吸引注意=东山再起。

第二，重视社区建设，重视普通人的价值。

在 Meme 币的风潮中我们已经看到了群众的力量，而在 Constitution DAO 的运动中，人民的力量更是发挥到了极致。区块链作为一种前沿的技术，总免不了要从小众走向大众。这个过程中，谁能更容易让普通人理解他的想法，谁就有可能获得市场的先机，实现快速的发展。

中本聪有一句名言，如果你不相信我，或者不明白，我没有时间说服你，对不起。这句话在区块链早期发展的时代很正确，但在今天也许有点过时了。在代币分配、投票治理让普通人获得更多利益，公关宣传让普通用户更容易理解，在很多方面都有探索的空间。动员起群众的力量，这种力量会大到难以想象。

3.3 DAO 的初露锋芒

当我们觉得这一年该火热的概念都已经炒完了的时候，ConstitutionDAO 给我们带来了惊喜，2022 年的开端无疑是 Web3。我们对 DAO 一直以来都不陌生，但今年似乎在 DeFi、NFT、GameFi、Metaverse 的大背景中很难找到它的踪迹，直到其他声音消逝，我们才能去探听到属于它的故事。

3.3.1 DAO 的发展

关于 DAO 的定义，Vitalik Buterin 在 2014 年做了一个很好的描述，DAO 是“一个生活在互联网上的实体，自主地存在，但也严重依赖雇佣个人来完成某些自治机制本身无法完成的任务”。 从时间维度看，DAO 的演化大致可以分为四个时期。

- 2011-2014 间的萌芽期：概念形成。
- 2015-2016 之间的混沌期：DashDAO 出现至 The DAO 陨落。
- 2017-2019 间的重构期：Aragon、Maker DAO、Moloch DAO 治理框架陆续出现。
- 2019 下半年-至今的探索期： 各场景、多应用的 DAO 出现。

2016 年发生的 The DAO 事件，仅仅一个多月筹集了超过 1200 万以太坊。可以看出人们对 DAO 这种崭新的组织形式有着极大的热情和探索欲。但也暴露两个严重的问题：（1）与智能合约的深度结合放大了技术风险的传导；（2）美国证监会（SEC）2017 年判 The DAO 项目违规出售证券，意味着此类项目面临较大的合规风险。这两个问题同样出现在 2021 年。

2021 年 11 月，Mochi 项目方利用自身协议的 USDM 稳定币购买了大量的 Convex 的治理代币，控制了 Curve 池子中 mochi 的收益率，造成 Curve 损失 3000 万美元。同样也是 11 月，美国证券交易委员会（SEC）对位于美国俄亥俄州的去中心化自治组织 CryptoFed DAO 提起诉讼，要求其停止“Ducat”和“Locke”这两款数字代币的证券注册。

图 3-6：DAO 的发展历程

来源

图 3-6：DAO 的发展历程

来源：火币研究院

3.3.2 DAO 的现状

2021 年，DAO 进入目前的探索期—在不同的目的、应用场景、生态内探索 DAO 的效用和边界。按应用场景分类，DAO 包括了投资类、协议类、社交类等。占比最大的是协议类 DAO，这些 DAO 包括 MakerDAO、Compound、Uniswap、AaveDAO 等，主要为通证持有者参与协议治理服务，覆盖参数调整、合约升级、业务决策等方向。

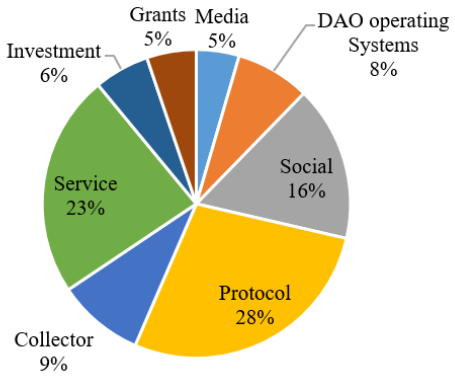


图 3-7：不同类型的 DAO 占比情况，总数 154 DAOs

来源：COIN 98 ANALYTICS

2021 年，从资产规模看，DAO 整体 AUM 快速增长，自年初约 40 亿美元规模最高增长至超 150 亿美元。除了 DeFi 巨头 Uniswap 外，今年比较瞩目的 DAO 是 Bybit 成立的 BitDAO，也是 6 月 DAO 资产总值大幅上涨的原因。从治理活跃度看，尤其 12 月 ContitutionDAO 在 11 月的出圈，治理决议活动达到历史新高。目前为止，提案数量最多的是 BerezkafLexDAO、Dxdao、Decentraland 等，但选民最多的则是 Sushi、Badger、Balancer。

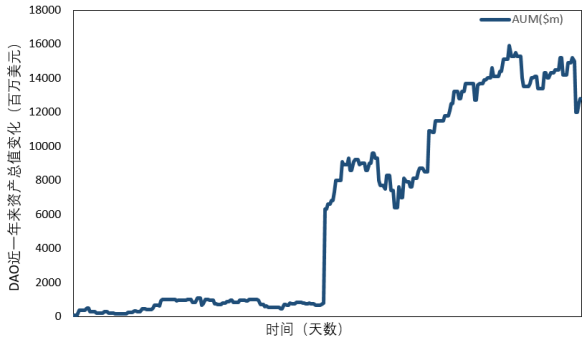


图 3-8：DAO 近一年来资产总值变化情况

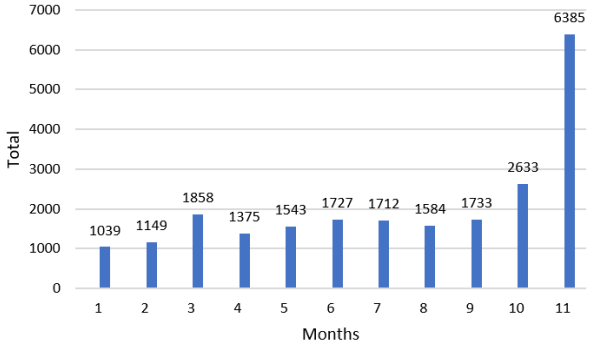
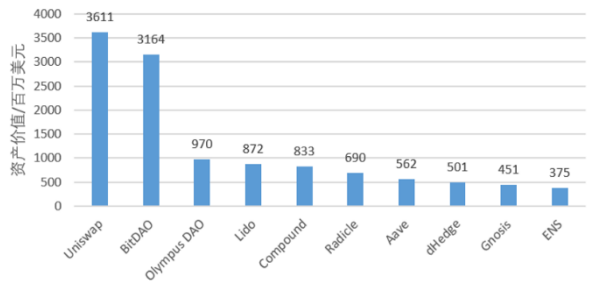


图 3-9： 2021 年 DAO 的治理决议活动统计

来源：deepDAO



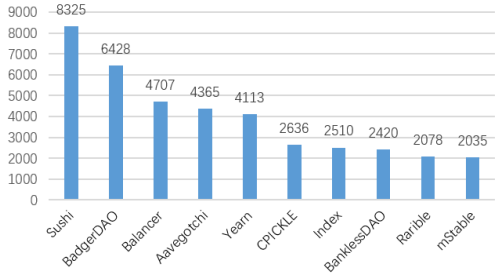


图 3-10：资产规模排名前十的 DAO 项目　　图 3-11：DAO 选民数量排名

来源：deepDAO

在基础设施建设上，目前已经发展出一批服务于 DAO 的治理、管理、平台类工具。我们在这里做一个简单的分类。这些基础设施将在 Web3 中发挥重要作用。

- 治理工具：包括了治理框架类工具及投票系统。
- 社交管理：提供提议或者讨论的平台，以及一些聊天门槛的设置
- 资产管理：提供了组织资产管理工具，包括一些多签方案。
- 铸造平台：主要是提供 DAO 组织内，成员的数字身份 NFT
- 社群价值管理：是评估成员的活跃度、以及组织带来的价值，并根据评估结果发放奖励。
- 创作平台：目前还是比较少的，多以文字输出为主。

DAO 基础设施类别	代表项目
治理工具	Gnosis, Aragon, WithTally, Snapshot, Boardroom, Sybill
社交管理	Discourse, CollabLand
资产管理	Coordinape, Parcel, Gnosis Safe
铸造平台	POAP, MinGate
社群价值管理	SourceCred, RabbitHole
创作平台	Mirror

表 3-1：DAO 基础设施分类及其代表项目

来源：火币研究院

3.3.3 代表性 DAO

今年，有 BitDAO 和 ConstitutionDAO 这两个代表性的 DAO 组织给我们提供了在治理框架和影响力可能性上的不同思路。

1. BitDAO

BitDAO 是由 Bybit 组织成立的平台资金库，5 月开始公开募资，目标是在研发、资金、流动性上推动 DeFi 的增长。BitDAO 采用 Snapshot 和多签验证的方案管理资金库。但 Bybit 始终是治理代币 BIT 的最大持币方，占比 60%。自 BitDAO 方案启动后，可以明显看到对 Bybit 的积极作用：（1）利用 DAO 的方式得到了广泛宣传，并在短时间内筹集到了巨额资金；（2）代币场景具有很大的想象空间，比如 10 月与 FTX 进行代币互换。BitDAO 是一个新的方向，或可带动外部社区、合作方共建交易所生态。

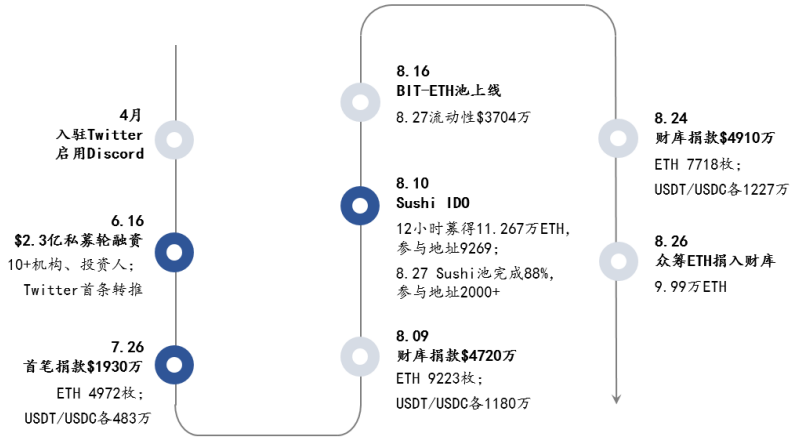


图 3-12：BitDAO 发展时间线

来源：火币研究院

2. Constitution DAO

ConstitutionDAO 的出现点燃了 11 月对 Web3 的热议。这种自发成立的 DAO 在短短一周的时间内，完成了组织、募集、决议执行、投票、发币等环节。这让我们看到 DAO 的基础设施目前可以完全支持一个 DAO 的自组织和自运转。而这种迅速出圈的影响力，也为 DAO 这种形式的行为模式展开了更多的想象力。ConstitutionDAO 也成就了一个新的 meme coin：$PEOPLE。

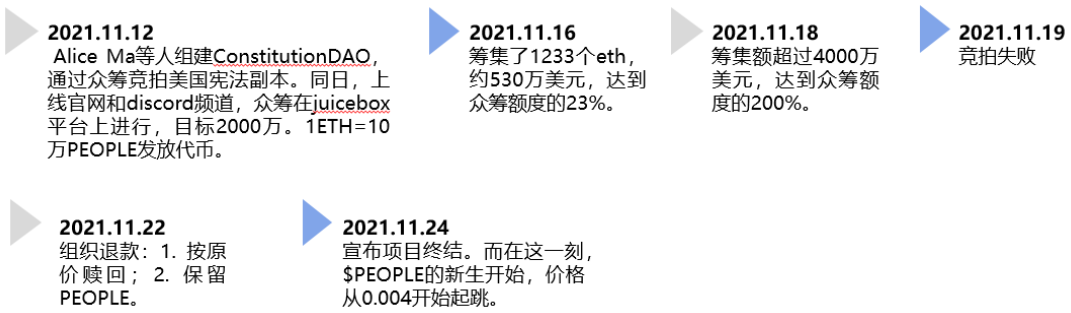


图 3-13：ConstitutionDAO 发展时间线

来源：火币研究院

展望未来，我们认为 DAO 将在短期内向着更多元的场景、更明确的身份、更高的参与度发展；而长期看，DAO 若可以不断破圈，吸引外部人才加入，优化各类问题，在 Web3 的体系下，其或将优先成为实体经济的一环提供生产要素，同时也或将衍生出自己的新经济体系。我们期待 DAO 在 2022 年带来更多的可能性。

3.4 元宇宙的扬帆起航

3.4.1 元宇宙发展历程

1992 年，科幻小说《SnowCrash》首次描述了一个平行于现实世界的虚拟世界，人类通过 VR 设备进入其中并能够虚拟人共同生活，而这个平行世界便被命名为元宇宙。事实上，元宇宙概念早在 20 世纪 70 年代末便开始出现雏形，1979 年世界上首个拥有文字交互界面的开放世界游戏 MUDs 诞生，掀开了多人实时联系的社交序幕，1994 年 Web World 问世，其开启了游戏中的 UGC 时代，而到了 1995 年首个基于《Snow Crash》打造的元宇宙项目 Active Worlds 正式问世，其为用户提供了用以改造虚拟环境的内容创造工具，允许用户登录，给自己命名，探索他人创建的 3D 虚拟世界，以及创建自己的世界。到了 21 世纪，在 2003 年第一款现象级虚拟游戏《Second Life》问世，在其中玩家能够实现社交、购物、商贸等，在其最火爆的时候 BBC 等媒体曾在其上进行新闻播报，瑞典甚至在其中建立了自己的大使馆。2006 年多人在线创作沙盒游戏平台 Roblox 问世，2017 年沙盒游戏 Fortnite 正式上线。当时间来到 21 世纪第三个 10 年的起点，2021 年被业界普遍喻为元宇宙元年，因为这一年不仅有元宇宙第一股的上市，更有知名科技巨头 Facebook 宣布更名为 Meta，向元宇宙生态建设方向大步迈进 。

图 3-14：元宇宙发展时间线

来源：火币研究院

3.4.2 元宇宙发展现状

随着全球科技巨头的相继布局，“元宇宙”关注度持续提升。全球对“元宇宙”概念的关注度提升进程基本一致。2021 年 9 月，字节跳动收购 VR 硬件厂商 Pico，中国市场对元宇宙的关注度出现明显升温；10 月底，科技巨头相继高调布局 Metaverse，Facebook 更是更名为 Meta，“元宇宙”概念正式破圈，在全球范围内的关注度达到新的高峰。从国家的角度看，韩国对元宇宙搜索意愿较高，首尔已发布元宇宙计划，由政府主导进场，其次是中国、新加坡、新西兰和美国等地。

根据谷歌搜索量数据显示，随着科技巨头 Meta 明牌入场元宇宙，这一概念迅速破圈并受到全球关注，元宇宙谷歌搜索量迅速上升。

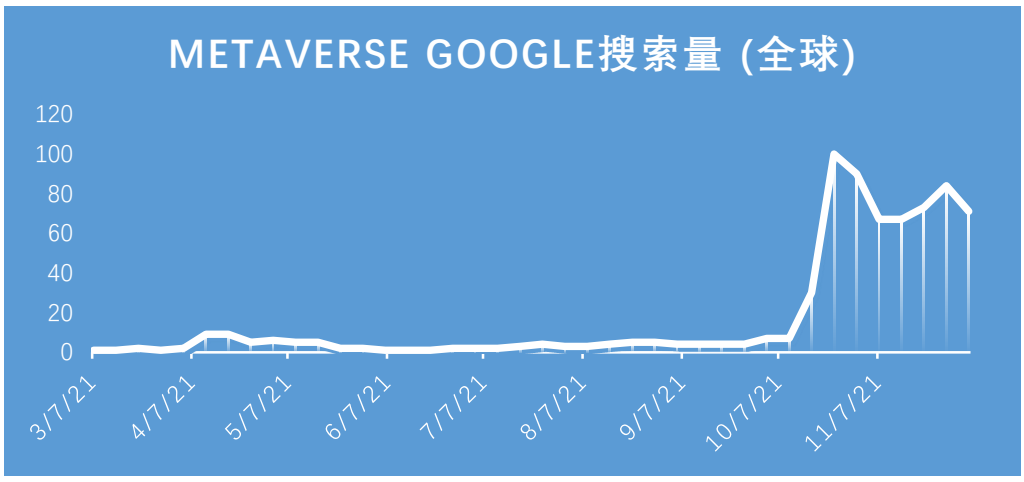


图 3-15：元宇宙全球搜索量

来源：Google，火币研究院

根据 JonRadoff 对于元宇宙产业链的划分，其产业链包括：体验层、发现层、创作者经济层、空间计算层、去中心化层、人机交互层以及基础设施层，共计 7 个层次。依据这一划分目前参与元宇宙生态建设的包括：传统科技巨头、软硬件基础设施提供服务商以及基于区块链技术的去中心化加密社群三类主要参与者。其中传统科技巨头凭借其巨大流量的初始禀赋通过抢占体验层、发现层等进入元宇宙生态；而软硬件基础设施服务商如 VR 设备制造商、3D 技术提供商等；加密社群则主要通过利用去中心化基础设施平台提供元宇宙建设关键的创作者经济层以及去中心化层入局元宇宙生态。

图 3-16：元宇宙主要参与者

来源：Jon Radoff，火币研究院

3.4.3 元宇宙代表模式

2021 年 10 月 28 日，知名社交公司 Facebook 正式宣布转型成为面向未来的元宇宙社交公司 Meta，该消息一经宣布瞬间引起全球舆论关注。同一时间段，知名加密投资公司 A16Z 负责人在一次访谈中在探讨 Meta 建设元宇宙社区时，表达出由中心化公司建立的元宇宙未来终将以失败告终。暂且不论这一言论是否客观，毫无疑问，无论是以公司为主导的中心化元宇宙模式还是以去区块链作为底层技术的支撑的去中心化元宇宙模式，未来将在很长一段时间共存甚至是相互融合共同推进元宇宙建设。

由于当前元宇宙生态建设尚处于早期阶段，因此无论是中心化元宇宙建设模式还是去中心化元宇宙建设模式，其竞争的本质是为了抢占元宇宙流量入口。两种模式之间既有共同点也有差异，从总体上来看二者的发展应该是求同存异而非相互排斥，相互攻击，因为在元宇

宙并未成为主流社交模式之前，对于致力于打造全生态元宇宙的企业、社区而言应该共同推动元宇宙建设，使之所倡导的愿景与生活方式成为全社会所能接受的共识。尽管如此，我仍将在这里对二者所可能展现出的差异进行初步的分析与描述，在尽可能展现出二者之间的区别之外，进一步分析未来两种模式间存在的潜在合作点。

- **建设主体的集中化程度**

两种元宇宙建设模式之间最大的差异在于项目集中化程度，以公司为建设主体的元宇宙模式将采用自上而下的建设模式，其表现出的特征是将对于元宇宙生态的建设往往具有完整的规划；而以去中心化组织为建设主体的元宇宙模式将大概率采用扁平化的元宇宙建设模式，其表现出的特征是以社区协作为主，缺乏对于元宇宙生态建设的完整规划，但是建设内容更加符合参与用户的偏好。

- **数据所有权的归属**

正如当前移动互联网中互联网巨头对于用户数据的掌控力一样，中心化元宇宙用户的数据仍将拥有参与用户的大量数据，从而赋予其对于其生态中用户行为的全面掌握与追踪；而去中心化的元宇宙模式则通过去中心化的数据存储模式，参与者拥有高度的个人数据主权，从而在一定程度上保障用户个人数据的隐私性。

- **效率及用户体验**

这里所指的效率与用户体验的差异并非是绝对的，但是相较于去中心化社区构建的元宇宙应用，中心化应用在一定程度上将能够以更快的应用迭代速度改进产品用户体验，其中最主要的原因是中心化元宇宙往往不需要进行社区集体决策过程，同时由于拥有更多的用户使用数据，因此能够更快的作出相应的决策。

- **安全性**

相较于开源的去中心化元宇宙，企业为主导的元宇宙在应用安全性管理上通过设置更多层级的管理权限以及更高水平的应用进入审核机制，从而在一定程度上提升其上应用的安全性；去中心化元宇宙开源机制在鼓励更多打造更多应用的同时，也为潜在的钓鱼应用提供了窗口，因此具有一定的不安全性。

尽管在两种元宇宙模式中，由组织架构所决定的原生差异，但是二者所追求的共同目标都是利用元宇宙这样一种模式，打造面向未来的商业模式、社交网络，因此在推动元宇宙建造所需要的基础设施模式、元宇宙商业模式普及方面拥有广泛的宣传共同点，在当前元宇宙

生态发展初期，合作所带来的收益将会比互相排斥带来的损失大，因此二者之间的合作将具有广阔前景。

3.5 区块链游戏的枯木逢春

3.5.1 区块链游戏的“王者归来”

尽管 2017 年底一款名为 CryptoKitties （加密猫）的基于以太坊智能合约的养成类游戏火爆全球，之后策略类、PRG、模拟经营类等区块链游戏也纷纷上线，带来了一股”区块链游戏热”。但早期的区块链游戏普遍存在形式单一、娱乐和体验性不强的问题，当游戏对大众的新颖感下降，热度减弱后，区块链游戏热也逐渐偃旗息鼓。

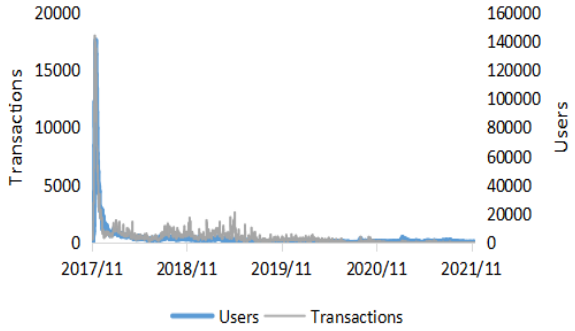


图 3-17：CryptoKitties 日活跃用户和交易量变化

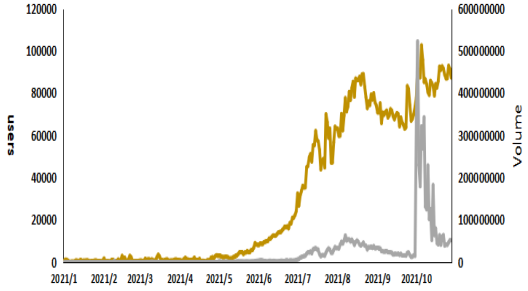


图 3-18：Axie Infinity 运营

来源：DappRadar，火币研究院

正当人们以为区块链游戏已成为过去时，自今年 6 月以来，一众带有 NFT，DeFi 等元素特征的区块链游戏，打着“Play to Earn”的口号，凭借其特殊的机制设计，在市场上迅速崛起。这其中的代表则是近期市场热议的 Axie Infinity。Axie Infinity 是一款宠物类小游戏。然而，这类看似普通的小游戏，曾以单日收入 972 万美元的吸金能力超过著名手游《王者荣耀》，治理资产 AXS 和游戏道具类资产 SLP 也一路水涨船高，两个月内涨幅均超过 3 倍。

这类新型的区块链游戏，也被称为 GameFi，即创造金融和商业的游戏化。从链上数据看，GameFi 自今年夏季开始迅速崛起。在 DApp 排行榜中，前 9 名中有 5 个都是 GameFi 类应用；从链上活跃的独立钱包地址数（独立用户）看，自今年夏季开始，GameFi 的独立用户数开始超越 DeFi，成为 Dapp 主要的用户来源，并且还在不断增长，截止至 12 月初，GameFi 的周活跃用户数已经达到了 921 万，创下历史新高。

排名	项目名	类别	TVL	用户	成交量
1	PancakeSwap	Exchange	$2.57 B	5.09 M	$ 172.69 B
2	Alien Worlds	GanmeFi	$12.43 M	1.55 M	$ 24 M
3	Axie Infinity	GanmeFi	$4.4 B	852.85 K	$1.79 B
4	Splinterlands	GanmeFi	$267.76 K	672.12 K	$ 444.63 K
5	Uniswap	Exchange	$10.56 B	467.35 K	$ 18.91 B

表 3-2：2021 年 12 月 Dapp 排行榜

来源：DappRadar，火币研究院

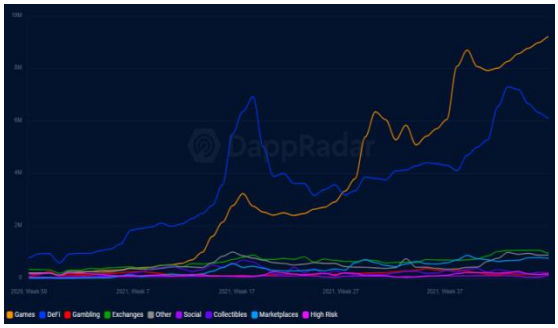


图 3-19：Dapp 活跃的独立钱包地址数变化

3.5.2. GameFi 崛起背后的原因是什么？

很多人将 GameFi 的成功归因于其“Play To Earn”的模式，即玩家可以通过玩游戏获取收益。然而，在传统游戏行业“Play To Earn”早已成为一种传统---从魔兽世界的打怪获取装备，到英雄联盟的玩游戏获取皮肤碎片或蓝色精粹，无一不是这一模式的真实写照。那么 GameFi 成功的真正原因是什么呢？

目前市场上对 GameFi 的主流解释，一般将其其概括为一个等式：GameFi = Game + DeFi，这一概括点出了 GameFi 成功的关键所在：GameFi 凭借其特殊的 DeFi 机制，极大地降低了交易费用，提升了用户游戏体验，主要体现在以下两点：

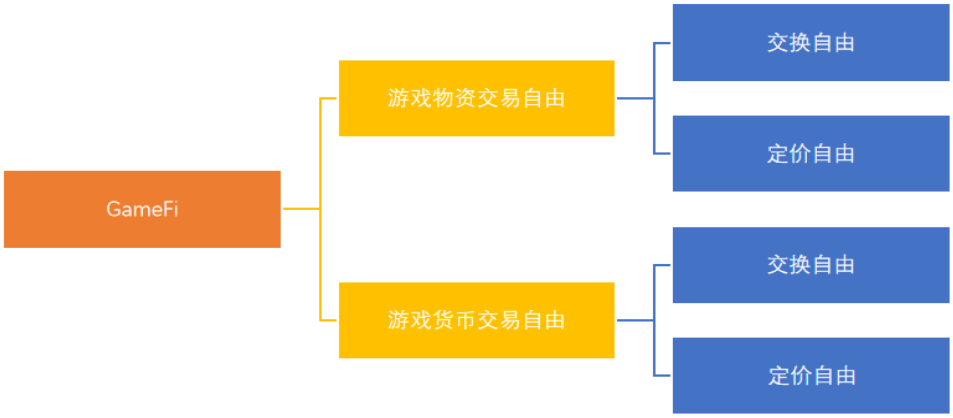


图 3-20：GameFi 交易费用降低途径

来源：火币研究院

首先是游戏物资的自由交易，这不仅仅体现在买卖对象的交换自由上，也体现在交易价格的自由上。不同于传统游戏规定只允许与官方交易、官方统一定价的交易模式，GameFi 通过赋予交易更广泛的自由，使得交易成本进一步下降，提高了用户体验。

其次是游戏货币的自由交易和定价。传统游戏通过游戏货币---装备道具---现金（官方交易/地下黑市）的方式变现获取收益，交易代价较大。GameFi 游戏货币的自由交易与定价极大降低了交易成本。

因此，GameFi 的火爆并非是因为“Play To Earn”，尤其是在传统游戏的打金活动早已形成产业链的当下。从深层次看，是因为 GameFi 可显著降低“打金活动”的交易费用，用户能以极低的代价迅速获得极大的收益，相较于其他游戏更具吸引力。

最后，GameFi 的成功离不开对产权的保障。

一般认为只有符合以下三个条件，资源才属于私有财产：

1）使用权，只有所有者才有权决定如何使用这些资源，并且有拒绝他人使用的权利；

2）收益权，有运用资产赚取私有收入的权利

3）转让权，有转让或售卖资源给任何人的权利

上述三者构成私有产权的三要素，缺一不可。对于多数传统游戏而言，收益权和转让权并不能得到保障。而在 GameFi 上，私有产权的拥有者可以选择出售或不出售某种资源的权利，扩大了选择的范围，同时也激发了市场竞争，从而节省了交易费用。

那为什么传统游戏产商不在先前建立此类私有产权制度安排呢？原因在于，改变原有的经济制度也是需要付出交易成本的。在此之前，游戏开发商建立该套产权制度的成本过于高昂，而所带来的收益远小于其成本，此时产权制度的变革没有必要性；然而，随着区块链技术的兴起，NFT 技术的推广应用，GameFi 可以在公链上以极低的成本建立一套完善的私人产权制度，这是传统游戏开发商所不具备的优势，也是相关公链在游戏领域应用的真正价值所在。

第四章 技术篇

4.1 Rollup 方兴未艾，以太坊何去何从？

以太坊自从 V 神创立以来，运行到现在已经有些疲惫不堪，远远不能支持人们对性能的需求。随着以太坊价格的攀升，使用以太坊网所需要的 gas fee 越来越高，甚至离谱地超过了总交易费用的 80%。

为此，Layer2 技术应运而生，Layer2 通常被称为“链下解决方案”（把针对以太坊主网的改造方案“ETH2.0”称之为“链上解决方案”）。

而众多 Layer2 方案中最有前途的非“Rollup”莫属。Rollup 是将原本分布再区块中的大量交易数据，打包成一笔集合的交易（简单理解起来就是做成“压缩饼干”）然后再放到以太坊主网上。Rollup 技术主要有 2 条技术路线。一条是 Optimistic Rollup，我们简称它为 op 系，代表项目 Arbitrum、Boba Network、Optimism，它们在今年迎来了黄金发展期，生态项目数量和 TVL 都快速增长。目前仅这 3 个项目，已近占据所有 Layer2 项目 TVL 的近 70%。另一条

技术路线是采用零知识证明技术(一种不给对方看钥匙但又能证明你拥有该房间钥匙的技术）的 ZK Rollup，我们简称它为 zk 系，代表项目 dYdX、Loopring、zkSync，它们的市场份额就小得多了。

No.	Name	TVL	Breakdown	7d Change	Market share	Purpose	Technology
1.	Arbitrum	$2.65B		-5.94%	40.04%	Universal	Optimistic Rollup
2.	Boba Network	$1.31B		-8.77%	19.81%	Universal	Optimistic Rollup
3.	dYdX	$896M		-6.70%	13.54%	Exchange	ZK Rollup
4.	Loopring	$642M		-14.59%	9.71%	Payments, Exchange	ZK Rollup
5.	Optimism	$466M		-4.13%	7.05%	Universal	Optimistic Rollup
6.	ZKSwap V2	$202M		-13.36%	3.06%	Payments, Exchange	ZK Rollup
7.	ImmutableX	$188M		-28.50%	2.84%	NFT, Exchange	Validium
8.	DeversiFi	$103M		+22.40%	1.56%	Exchange	Validium
9.	Metis Andromeda	$60.42M		+46.06%	0.91%	Universal	Optimistic Rollup
10.	zkSync	$54.89M		+27.36%	0.83%	Payments	ZK Rollup

图 4-1：以太坊代表项目

来源：L2Beats

从技术的角度来说，Optimistic Rollup 简单易行，更容易实现，但也有自己难以逾越的缺点。由于使用了乐观主义精神“欺诈证明”（人如其名），提取资金的时间通常需要一周左右。相比于“欺诈证明”，更有技术挑战性的 zkRollup 要求二层运营者提供“有效性证明”，即，二层运营者直接证明其提交的状态转换是有效的(正确的)，自证清白。在该种

方式下，提交即正确，用户不必担心欺诈，提取资金也不会有冻结期。但，zkRollup 技术难度系数也更高，实现起来较为困难，目前面向大众提供服务的 zkRollup 方案只能打包简单的转账交易，而不能运行智能合约，换而言之就是 zkRollup 目前并不支持 zkEVM（对零知识证明友好，同时兼容现在的以太坊虚拟机的虚拟机）。

	ZK Rollup					Optimistic Rollup		Validium	Arbitrum
	ZKSync	Loopring	Aztec	ZKSwap	Hermez	Optimism	Fuel	StarkEx	OffChainLabs
取款时间	5 小时	2 小时	4 小时	20-40 分钟	20 分钟	7 天	7-14 天	10 分钟	7-14 天

表 4-1：各项目取款时间

来源：火币研究院

但随着技术的发展，拥有 zkEVM 的 zkRollup 方案即将到来。未来根据实现方案的不同，也会分为两种侧重点不同的 zkEVM 技术路线，在这里我们把他们简称为“EVM 友好型技术路线”和“零知识证明友好型技术路线”。“EVM 友好型技术路线”，把兼容用 Solidity 指令集写成的 EVM 放在首要位置，支持原生的 EVM opcode（以太坊虚拟机操作码），在此基础上再需求对零知识证明的友好。“零知识证明友好型技术路线”则是把对零知识证明的友好性放在了首先考虑的位置，会抛开原有的 EVM opcode，直接设计一套对零知识证明更友好的指令集，再寻求与原本的 EVM 适配。

技术路线	EVM 友好型	ZKP 友好型
优点	兼容性好，安全性好	灵活性好
缺点	部分 opcode 不易生成 ZKP，工作量大	需额外适配工作，可能产生安全隐患
Projects	Hermez; the Ethereum Foundation EVM	zkSync

表 4-2：两种 zkEVM 技术路线优缺点及代表项目

来源：火币研究院

总而言之，zkEVM 的到来会使 zkRollup 方案真正完整，这首先会使 zkRollup 方案在 Layer2 中占有更多的市场份额。而最有可能成熟的拥有 zkEVM 完整的 zkRollup 方案就是走第二种“零知识证明友好型技术路线”的 zkSync2.0。目前其测试网已经上线了 uniswap，其团队 Matter Labs 也完成了 a16z 领投的融资，使用 zkSync 的小伙伴未来有可能获得 airdrop（空投奖励）。

由于 ETH2.0 的分片的实现难度很大，针对 ETH2.0 的开发可能旷日持久。从短期来看，Rollup 解决方案会是以太坊当下最火热的二层技术，帮助以太坊的用户获得更好的服务体验，抵御那些挑战以太坊的新公链。

从长期来看，Rollup 技术的未来依然远大，而不只是一种暂时性的过渡方案。正如 Vitalik 所说，对于以太坊而言，Rollups 是短中期，也可能是长期的唯一无须信任的可扩展性解决方案。未来，即使在新公链中也可能会有 Rollup 的一席之地。老城区(以太坊)在道路大规模改造之后（ETH 2.0），交通压力也会大大缓解。新城区（新公链），可能由于设计理念更先进，人少车也少，不容易出现堵车问题。但总有一天车会越来越多，到那时候如果出现拥堵，还是可以将现有的 Rollup 技术应用到新公链之上。

4.2 跨链桥的风起云涌

随着多种 layer 2 网络的锁仓量快速增长，多条高性能公链的崛起，跨链交互的需求迅速涌现，跨链桥因而成为链上重要的基础设施之一。由于各个 layer 2、公链网络的底层架构差异大，跨链互操作的实现难度较高，当前跨链桥主要扮演流动性桥梁的角色，提供代币在不同网络间流转的服务。

代币跨链的形式主要有资产铸造与资产互换两种。资产铸造指需求方将代币存入发起链的智能合约并被锁定，经过一定的机制得到确认后，目标链的智能合约铸造对应代币；资产互换指需求方将代币发送至发起链的服务节点的地址，经过一定的机制得到确认后，服务节点在目标链将相应代币发送至需求方的地址。

资产铸造的跨链桥根据确认机制可分为原生跨链桥与共识跨链桥两种。原生跨链桥是指一个部署在目标链的轻节点，通过验证发起链轻节点产生的状态证明来确认代币在发起链的存入，进而在目标链进行代币铸造；共识跨链桥是指一组额外的验证者对发起链的代币存入达成共识并在目标链进行代币铸造。原生跨链桥因需在目标链进行轻节点智能合约部署，通

常只提供单一跨链服务，如 Ethereum 与 Near 之间的 Rainbowbridge，而因其轻节点需要进行状态证明的生成与验证，总体花费的 gas 也较高，但其优点是不涉及到额外的共识机制而相对安全；相反，共识跨链桥不涉及复杂的轻节点而有更强的部署能力，更快速的响应能力，更低的成本，通常提供较多跨链服务，但因其额外的共识机制而安全性较低，曾经发生过多起安全事件。

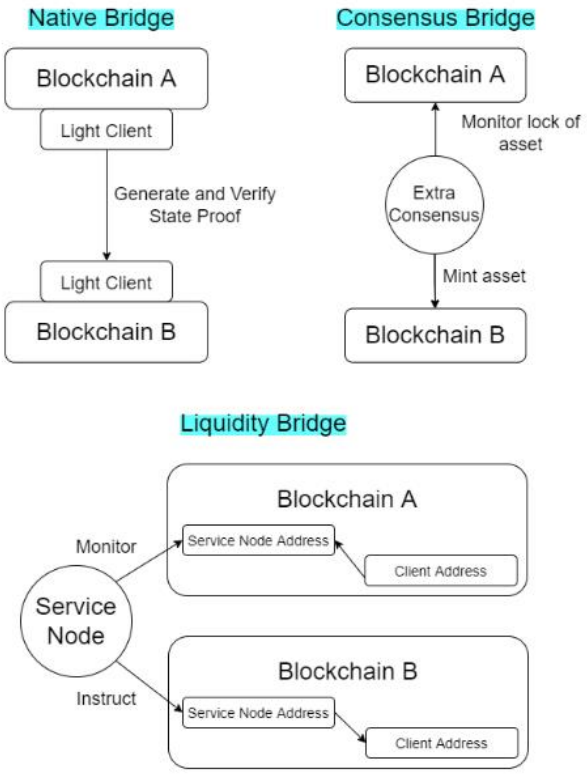


图 4-2：各类跨链桥机制梳理

来源：火币研究院

资产互换的跨链桥又称流动性跨链桥，主要利用原子交换技术来保证其安全性。其因为涉及到目标链和发起链的流动性，部署能力弱于共识跨链桥，且需要成本来补贴流动性的量和种类。其响应能力与使用成本与共识跨链桥基本持平

以下是我们对主流跨链桥的数据汇总：

	协议代币市值	总锁仓量	支持链数	技术形式	服务类型	服务特色
WBTC	未发币	$14269M	2	共识跨链桥	单向跨链	仅支持BTC跨链
Ren Protocol	$760M	$970M	7	共识跨链桥	单向跨链	支持BTC，ZEC等跨链
Anyswap	$167M	$4620M	23	共识跨链桥	多链互跨	支持的公链最多，币种最全
Synapse Protocol	$394M	$623M	7	共识跨链桥	多链互跨	支持Boba Network与Harmony
Wormhole	未发币	$619M	5	原生+共识跨链桥	多链互跨	支持rust公链：Solana与Terra
Chainswap	$2M	未知	23	共识跨链桥	多链互跨	部署在Anyswap上
cBridge	$610M	$21M	9	互换跨链桥	多链互跨	正在开发支持智能合约调用的通用链间互操作协议
Hop Protocol	未发币	$104M	5	互换跨链桥	Layer2互跨	支持的layer 2最多
Connext	未发币	$10M	8	互换跨链桥	多链互跨+Layer2互跨	正在开发支持智能合约调用的通用链间互操作协议

表 4-3：主流跨链桥数据汇总

来源：火币研究院

可以从上图当前该领域的主要特征：

已经出现了锁仓量占据优势地位、支持链数量较多的头部跨链桥，如 Anyswap：此类跨链桥一般服务于 EVM 系公链间跨链，因为技术角度上由于使用的是同一虚拟机，跨链合约可以较快部署；流动性角度上 EVM 系公链流通的资产较为同质化，如 ETH、USDC。

同时，该领域日趋成熟，已经出现了三个细分市场：BTC 跨链（如 WBTC），layer2 跨链（如 Hop，现已支持除 zkrollup 系以外的所有 layer2 网络），非 EVM 系公链跨链（如 Wormhole，主要服务于 Solana 跨链到其他公链）。

最后，我们对跨链桥领域的未来发展做出以下三点构想：

1. 跨链成本、资金效率进一步优化。当前共识跨链桥大量使用 AMM 机制来保证封装资产与目标资产的等比兑换，因此需要使用代币来补贴流动性提供者。同样对于一些还未发币的资产互换的跨链桥，也需要付出流动性成本来提供比当前更高额度的跨链服务。我们认为多链部署的 DEX 可能在这个角度具有一定优势，即他们在各条链已经具有充足的、多样的主流代币的流动性，尤其是高额度的跨链需求通常是以稳定币为载体，而诸如 Curve 的专注稳定币 DEX 可提供更低价格的服务。

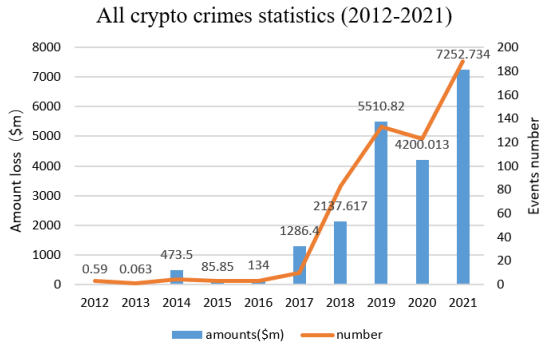
2. 跨链机制进一步去中心化。当前共识跨链桥的安全性相比其他两种跨链桥较低，其因存在过于中心化的共识发生过较多安全事件，而一些共识跨链桥推出的验证者质押且在违

规时被罚没的方案降低了资本效率。采用更去中心化的方案，进而降低安全成本，是共识跨链桥未来的重要迭代方向。

3. 跨链桥领域未来的重头戏是研发跨链互操作协议。当前跨链桥主要满足代币跨链的需求，基本无法实现跨链互操作，即实现跨链合约调用，因此不同公链间的生态几乎无可组合性，公链生态成为新的孤岛。当前正在开发的有原生兼容跨链的公链方案如 Cosmos 与 Polkadot，以及 L;ayerzero 的跨链通讯协议。

4.3 区块链安全的攻与防

2021 年是区块链行业收获的一年，也是区块链安全面临考验的重要转折点。据公开的安全事件统计显示，本年度区块链行业经济损失总计约 72 亿美元，较 2020 年增长 98%，安全事件数量 188 起，历年最高。按攻击对象，安全事件的主要类型有交易所、公链、数字钱包、各公链生态等。其中，交易所与 ETH 生态为黑客攻击的主要目标，损失金额约占 56%。



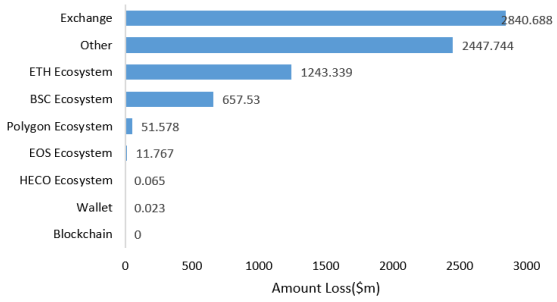


图 4-3：2012-2021 年区块链安全事件数量及损失金额统计 图 4-4：根据不同攻击目标对损失金额统计

来源：SlowMist Hacked，火币研究院

由于 DeFi 智能合约在今年的蓬勃发展，其开放性和创新性带来了前所未有的新风险。2021 年 DeFi 漏洞和欺诈造成的损失总额约为 22 亿，较 2020 年的 15 亿美元增长了 46.7%。今年最值得关注的漏洞攻击事件包括 Poly Network 的 6.1 亿美元损失、PAID Network 的 1.8 亿美元损失、Cream Finance 的 1.3 亿美元损失、Badger DAO 前端遭黑客攻击损失约 1.96 亿美元。尽管如此，也阻止不了资金对区块链行业的偏爱，仅整个 DeFi 的总价值就已达到 2580 亿美元。DeFi 的安全事件类型主要有 3 种情况，一是欺诈，二是智能合约漏洞，三是利用闪电贷操纵代币价格。

除 DeFi 之外，其他类别的典型安全事件或新闻也值得我们关注。

● 6 月，加密货币投资平台 Africrypt 创始人失联，6.9 万比特币被转移。

● 日本加密交易所 Liquid 在 8 月遭遇了黑客攻击，黑客入侵了 Liquid 的热钱包并盗走价值约 9000 万美元的加密货币。

● 除了黑客攻击，诈骗案件也是区块链安全事件中不容忽视的类型。最大加密骗局之一，Bitconnect 在 9 月被美国证券交易委员会指控为金融欺诈，其在 2017 年曾非法集资超过 20 亿美元。

4.3.1 风险类别

根据近十年来的安全事件统计，上述不同的攻击对象面临如下安全风险：

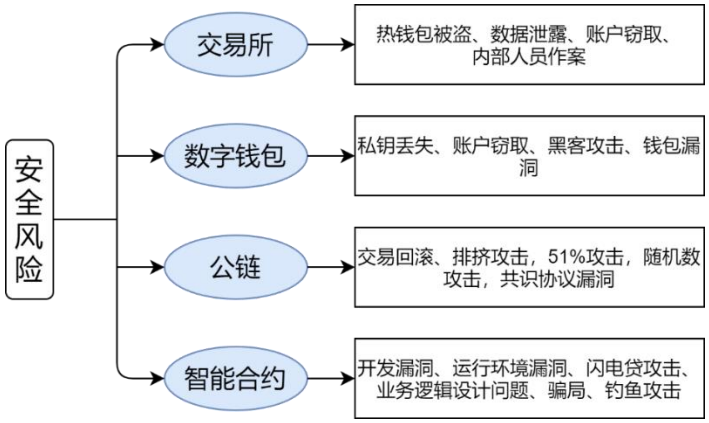


图 4-5：针对攻击目标的不同攻击类型

来源：火币研究院

交易所和智能合约为近两年来损失金额最大的两个主体。对交易所来说，应该建立完善的安全风控紧急预案，能够及时响应并处理风险，提高员工的责任心。在智能合约项目方面，其上线前，对合约进行安全审计，购置保险合约类产品。上线后，仍然需要跟踪链上活动，同时不容忽视前端系统被黑的情况。作为用户和投资者，切不能贪图高额收益，盲从跟风。

4.3.2 区块链安全产业链初成

区块链安全解决方案和安全技术也在不断更新迭代，产生了诸如安全审计、安全咨询、应急响应等多种服务，造就出 SlowMist、Quantstamp 等专注区块链安全领域的明星公司，从事前审查的角度保证智能合约的安全，这些公司的业务规模在近两年均有很大的增长。

2021 年是加密安全投资的标志性年份，对该行业的风险投资已超过 14 亿美元，而去年在该行业的投资不到 1 亿美元。这其中还包括了安全硬件钱包 Ledger 在 6 月份完成的 3.8 亿美元 C 轮融资，Certik 在今年的融资完成了 1.4 亿美元。以及 Fireblocks 完成了 3.1 亿美元的 D 轮融资和 4 亿美元的 E 轮融资。Fireblocks 虽然是一个数字资产平台，但它帮助解决了从安全到合规再到治理的各种围绕数字资产的业务问题。

智能合约安全审计类公司，即使经过事前审查，但并不能保证合约没有漏洞，比如 11 月发生的 Monox Finance 漏洞攻击事件。在出现漏洞后，审计公司也不会为此负责。从开发者角度出发，对可事后赔偿的定制化保险产品的需求更大。同时，定制化保险产品的推出，则从事后索赔的角度解决了投资者的后顾之忧。因此，未来智能合约安全保险类产品的业务规模将远高于现有的几家明星安全审计公司。

整体上，区块链安全产业链已初具规模。我们从上下游公司类型和服务出发，总结了目前产业链的情况：

类型	服务项目	面向客户	代表企业
区块链安全	智能合约审计；漏洞审核和处理	交易所、公链、项目方	Certik, Slowmist, PeckShield, Consensys Dilligence
解决方案提供商	提供加密、签名和身份验证服务；网络安全解决方案	公链、钱包	Thales, HB Security, Stark Ware
安全开发模块	构建安全的智能合约开发工具	合约开发人员	Forta Protocol
安全监控	市场和风险监控和预警	投资机构	Solidus Lab, Fire Blocks, Elliptic
保险	智能合约保险	合约用户和项目方	Yearn. Finance, InsurAce

表 4-4：区块链安全产业链整体情况

来源：火币研究院

虽然区块链领域的造福神话吸引了很多人，但在这个去中心化的世界里，财富与风险并存。这个行业需要更多人加入，那些徘徊在区块链之外的低风险偏好者，作为行业从业人员，我们有必要提供一个更安全的环境，我们才有资格去说服他们，说服监管者，让这些人也能感受到区块链给整个世界带来的好的变化。

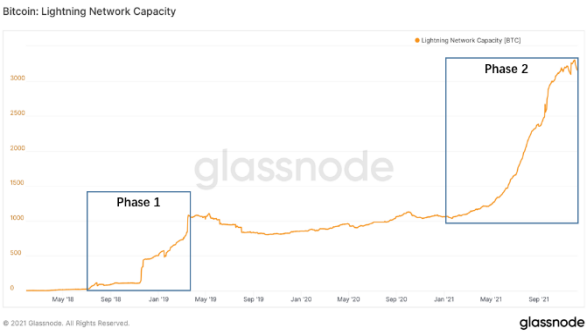
4.4 比特币的升级之路

我们如期看到在比特币第三次减半后，整个加密市场繁荣了一整年。在这一年里，比特币除了价格外，还有两个值得关注的地方。

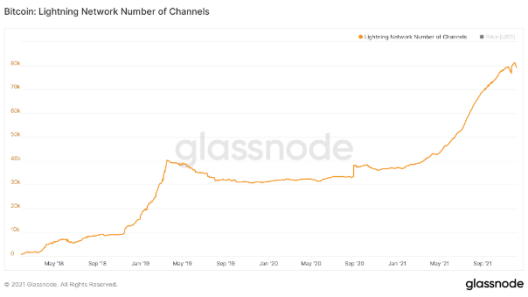
4.4.1 闪电网络

闪电网络作为比特币的二层解决方案已经发展了 6 年的时间，目的是加快比特币的交易处理时间，可扩展性，降低交易费用。

2021 年，闪电网络发展势头强劲，根据 Glassnode 上的数据， 2021 年初以来，闪电网络容量呈指数级增长，目前已超过 3100BTC，较 1 月初增加了 190%。活跃节点数为 18343，增长了 120%，活跃通道数为 79150，增长了 110%。根据闪电网络容量变化情况，可以看出闪电网络经历了两个飞跃式的阶段。



（1）容量



（2）通道数

图 4-6：比特币闪电网络容量及活跃通道数变化情况（2018.01-2021.12）

来源：glassnode，火币研究院

（1）阶段一：2018 年 6 月至 2019 年 5 月，闪电网络推出主网后的试验期，主要是大节点的贡献，占比特币容量的 50%以上。

（2）阶段二：2021 年 1 月至今，闪电网络在 2020 年开始用户采用后，开发人员努力提升闪电网络的性能。由于今年比特币减半牛市的影响及萨尔瓦多等国家对比特币的开放态

度，同时 Paxful 交易所集成了闪电网络、Strike 钱包在 twitter 小费应用、以及 Chivo 钱包在萨尔瓦多的推出，闪电网络的容量和钱包的支付量在 9 月之后得到了大幅增长。

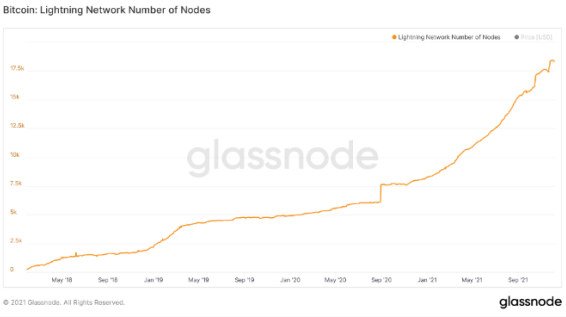


图 4-7：比特币闪电网络活跃节点数变化情况（2018.01-2021.12）

来源：glassnode，火币研究院

除了性能指标上的提升之外，闪电网络无论在基础设施还是应用场景上都有显著增加。闪电网络不仅仅局限于线上服务的付费，还能够用于日常生活。根据 Arcane Research 报告数据显示，9 月闪电网络的用户数量增加了 11,164%，达到 970 万，并且商家支付和礼品卡在内的个人转账的使用量增长了 122%。很多金融产品也开始搭建在闪电网络上，比如衍生品交易市场 LN Markets 和 Kollider。

虽然闪电网络在安全性和通用性上还有所欠缺，但萨尔瓦多的比特币合法化和 Twitter 小费应用给了我们很大的想象空间。我们也看到近期 Tether 创立的 Synonym 希望通过闪电网络扩大比特币的采用率。也许在未来，有更多国家会承认比特币的合法地位，同时比特币的小额支付将出现在各种音乐、购物、视频付费上。如此，闪电网络将在提高比特币应用场景方面发挥关键作用。

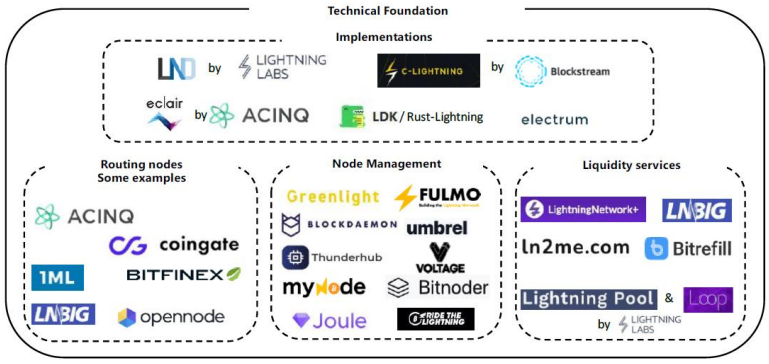


图 4-8： 2021 年闪电网络生态

来源：Arcane Research Report

4.4.2 Taproot 升级

2021 年 11 月 14 日，比特币迎来了 Taproot 软分叉升级，从 18 年由 Gregory Maxwell 提出到激活也经历了漫长的探讨，这被认为是“比特币在下一阶段的重要技术”。比特币区块链在创建的时候并没有考虑到智能合约，只有存储和转移比特币的功能。Taproot 升级能够有助于改善比特币区块链的这一缺陷。

图 4-9： Taproot 升级时间线

来源：火币研究院

Taproot 包含了 3 个 BIP：

● Schnorr 签名（BIP340）提供了一种更隐私、更安全、更易验证的密码学签名，取代原有的 ECDSA 签名，具有“密钥聚合”功能，节省了区块空间。

● Taproot（BIP341）提出了 Pay-to-Taproot（P2TR）输出类型规则，实现了 Merklized Abstract Syntax Tree（MAST）仅将交易执行条件提交给区块链，使 Schnorr 签名产生的交易与链上单签名交易相同。这改变了区块的数据结构，加强了匿名性、隐私性和可扩展性。

● Tapscript（BIP342）为以上两个 BIP 更新了脚本编码语言，还使比特币未来的操作码更新变得更容易实施。

这三个 BIP 的实施能够加强比特币交易的隐私性和安全性、优化区块容量、降低交易费用。Taproot 激活之后还没有获得广泛的应用，目前区块仍同时具有 Schnorr 签名和 ECDSA 签，这可能还需要几个月的时间才能完成升级。主要原因是所有节点需要完成升级，同时如钱包类第三方应用还需要一段时间完成改造测试。

比特币的每一次升级都显得那么谨慎。虽然我们认为成为第二个以太坊并不是比特币的目标，并且比特币可能很难实现与以太坊一样的智能合约功能，但此次 Taproot 升级可以看出比特币正在往需求端靠拢，在比特币作为价值储存、支付货币之外的带来更多的可能性：

（1）Schnorr 签名使得比特币的侧链网络以低成本创建多重签名库，给侧链更大的发展空间；

（2）多重签名也让 DeFi 协议在比特币部署的成本降低，未来可能出现更多的 DeFi 产品。甚至能否搭载更多功能的智能合约成为热议话题。目前在比特币上的 DeFi 协议共有 25 个，与以太坊 DeFi 生态相比还差很远；

（3）隐私性增强之后，兼容 Taproot 的闪电网络将获得更广泛的应用。

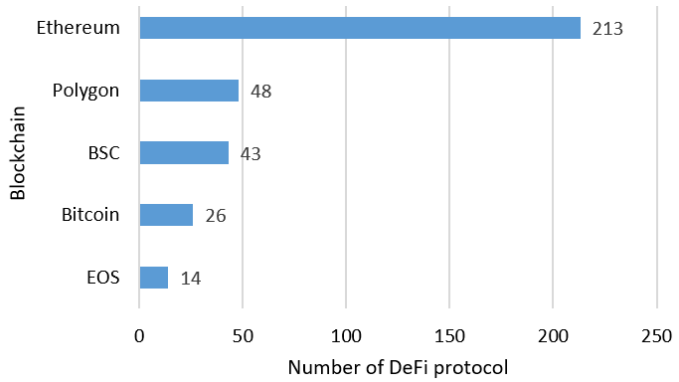


图 4-10：各区块链 DeFi 协议数量对比

来源：defiprime.com，火币研究院

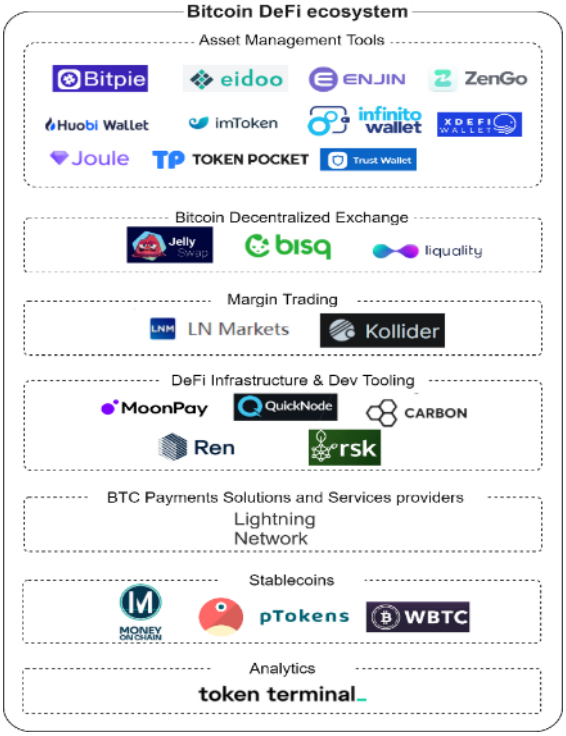


图 4-11：比特币 DeFi 生态图

来源：火币研究院

4.5 探索前行的 Web 3.0

Web3 是互联网发展变迁的新一章节。Web1 时代从 1990 年起，是以 Linux、Netscape 为代表的一系列开源协议，以及如个人博客等以静态网页形式存在的信息流产品，是 Web 的基石。Web2 时代从 2005 年起，是以 Facebook、Amazon 为代表的一系列平台，服务于聚合商品、内容的生产者与消费者，主要利用公司对平台的中心化所有权，以收取平台佣金、控制推荐算法进行广告推送的方式产生利润。

Web2 平台的生产者与消费者长期以来存在着对 Web2 经济模型的不满：Web2 平台背后的公司用收取高额佣金（如苹果 App Store 收取 30%的手续费）、侵犯个人隐私数据（Facebook）、算法杀熟（淘宝）等方式从平台利益最大化，导致平台用户产生的价值被剥削。

4.5.1 什么是 Web3？

以上问题是 Web3 概念兴起的重要推手，我们认为 Web3 最重要的特性是个人对平台或组织的治理权，个人数据资产的所有权：

- Web3 是在基于区块链的社区控制、社区治理的互联网产品上形成的经济体，社区成员对社区、产品拥有治理权。
- Web3 经济体旨在实现个人数字资产、身份、隐私的的所有权，并在此之上实现更为公平的价值分配。

	Web 1.0	Web 2.0	Web 3.0
交互方式	阅读信息	读写信息	读写信息，拥有平台
载体	静态内容	可交互内容	虚拟经济体
组织形态	公司	平台	社区
基础设施	个人电脑	云服务	区块链
控制权	中心化	中心化	去中心化

表 4-5：历代互联网的特征

来源：火币研究院

4.5.2 Web3 的现状与展望

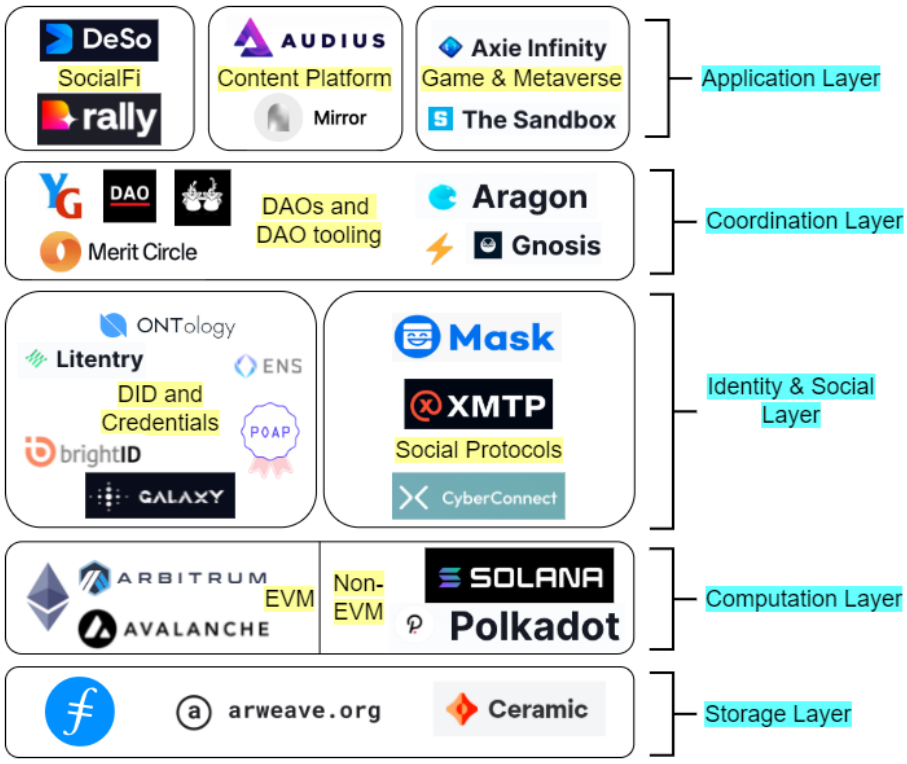


图 4-12：web3 生态结构

来源：火币研究院

我们认为 Web3 的生态结构可分为存储层、计算层、身份与社交层、协作层及应用层。其中应用层又分为 SocialFi、内容平台、游戏与元宇宙三个子版块。

● 存储层，指的是 Web3 为保证个人数字资产绝对所有权，需要将数据进行去中心化存储。当前除 Filecoin，Arweave 等成熟方案以外，也出现了细分领域的解决方案，如针对智能合约状态存储的 Ceramic Network。

● 计算层，指的是 Web3 通过去中心化计算处理业务逻辑的一层。目前的主流解决方案为使用 EVM 虚拟机的 Ethereum、Layer2、以及通过改进共识实现更高性能的 EVM 公链如 BSC，Avalanche；同时也出现了非 EVM 的解决方案如 Solana，使用 WASM 虚拟机的 Polkadot 等。

● 身份与社交层，指的是 Web3 为保证个人身份、个人社交关系的绝对所有权，需要去中心化的身份、社交图谱、通讯工具的解决方案。当前此层有不少各具特色的方案，如域名服务 ENS，提供去中心化身份的 Ontology，验证区块链地址唯一性的 BrightID，专注成就系统的 POAP，制作社交图谱的 Cyberconnect，以及 Web3 地址间通讯工具 XMTP。

● 协作层，指的是 Web3 为保证社区对平台的控制权，需要去中心化的社区解决方案。DAO 十分契合 Web3 的社区控制与治理的范式；同时，此板块也有不少 DAO 工具协议，如投票协议 snapshot，一站式 DAO 解决方案 Aragon 等。

● 在 Web3 应用方面，内容平台是最契合的场景之一：Web3 让创作者、消费者形成的内容社区在价值分配上得到话语权，从而抹除平台寻租成本，更直接地激励创作者；代表有 Audius。Web3 的另一大应用场景是 SocialFi：个人身份的绝对所有权使得平台间的“围墙”不复存在，个人身份得到跨平台聚合，释放出大量真实、可验证的身份信息，因此社交应用可以进行更为高效地匹配与金融化。游戏也是 Web3 的重要应用：相比传统游戏，Web3 游戏拥有完整的经济系统，更繁荣的用户生成内容，在开放互通性上也有较大进步。

第五章 国际政策篇

2021 年，随着加密市场的火热发展，全球监管当局对于这一新兴领域的认知和理解也逐渐加深丰富。这一年最大的两件行业相关的热点事件分别来自中国和萨尔瓦多，其中中国政府出于维护市场稳定的考量，于 2021 年 5 月起通过系列政策措施完全禁止加密行业相关活动，这也是全球主要经济体中首个完全禁止加密行业的国家，对于加密市场造成了不小的负面冲击；与此同时，萨尔瓦多政府成为全球首个将比特币作为法币的独立主权国家，随即

受到全球广泛关注。可以说，对于加密行业而言，2021 年将成为其发展历程的一个关键分水岭。

本章通过对全球 2021 年 1-11 月加密政策汇总统计，对全球加密政策发展现状及趋势进行相应分析，考虑到由于中国加密政策木已成舟且在短期内不易出现明显变化，因此本章所涉及政策分析主要为除中国全境外的其他国家和地区。

5.1 全球加密政策总体情况

根据火币研究院对于全球除中国外其他国家和地区 2021 年加密政策统计显示，2021 年以来，全球有超过 40 个主权国家和地区对于加密行业采取了共计 151 项监管措施和指导，同比上升约 75%。

从地区来看，美国、韩国和印度采取的监管措施更为集中与密集。其中美国联邦与各州政策共计 45 项，韩国紧随其后共计产生监管 24 项，印度则产生了 8 项相关监管指导。毫无疑问，加密政策的密集程度与该国或地区加密行业的发展水平具有一定的相关度，美国作为全球最大经济体，加密行业的发展同样受到全球市场的关注，随着加密业态的不断丰富与发展，美国政策所涵盖的领域也在不断扩充与丰富。例如，今年以来，美国加密政策所涉及领域包含了 DAO、DeFi、稳定币等多个新领域，同时美国首次通过了比特币期货 ETF 的发行，这也进一步激发了全球加密行业的发展热情。

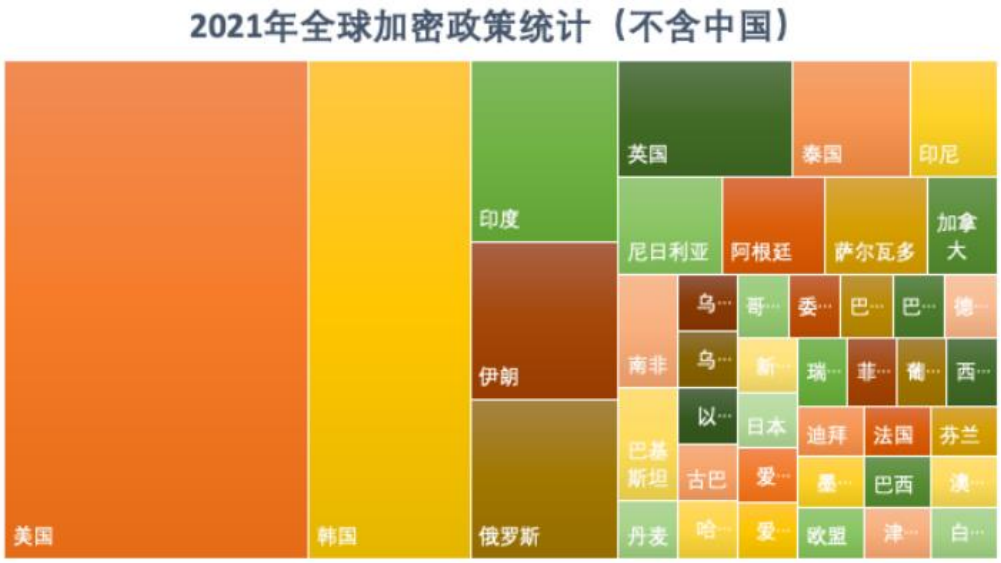


图 5-1：全球加密政策热力图

来源：火币研究院

为进一步分析全球监管当局对于加密行业政策制定的政策取向，我们根据政策类型分别划分为积极类政策、中性类政策、消极类政策，其中积极类政策是指对于加密行业有积极促进作用的政策，日萨尔瓦多将比特币列为法币，中性类政策是指对于加密行业进行常规化管理而不存在利好或利空作用的政策，如美国纽约警察局发布加密货币交易分析规范工具等；而消极类则为禁止性政策或相关的行政处罚等，如英国 FCA 禁止加密货币衍生品散户禁售令生效等。

根据这一划分规则，可以发现 2021 年全球加密行业政策以中性政策为主占所统计政策的 59%，其次为积极类政策占比 23%，而消极类政策则占 18%。这一数据显示出在 2021 年，全球除中国外所统计的其他 40 余个国家或地区对于加密行业的监管取向以中性偏积极为主，这表明对于关注加密领域的国家而言，其偏向于在适度监管的基础上对于加密行业进行相应的规范和引导，以防由于政策限制导致对于这一新兴领域的创新性的打击。

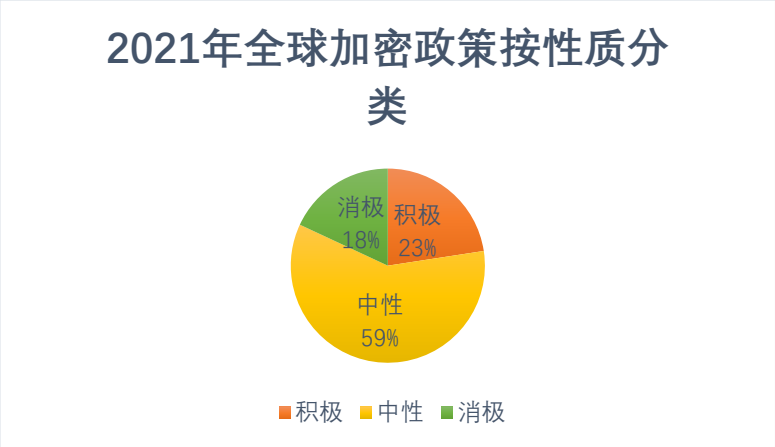


图 5-2：全球加密政策性质饼状图

来源：火币研究院

在此基础上，我们进一步按照政策所涉及的加密领域进行划分，发现所涉及的加密领域包括：监管指导、交易、税收、稳定币、挖矿等 11 个方向，其中政策指导、加密交易以及加密征税分列所有政策的前三，其中加密政策指导 54 项、针对加密交易的政策 41 项、加密征税 23 项共计 118 项，占所统计政策数量近 80%。这表明针对加密行业的发展，全球多数国家或地区均在积极推动相应的加密监管框架制定以及相应业务的监管指导，除此以外，针对加密交易存在的监管缺失进行相应的主管机构职能的确定以及对加密交易准则进行规范。同时，随着加密市场的不断壮大，各国监管机构也开始重视这一领域所存在的潜的税收问题，原因在于加密行业所使用的挖矿机制耗费了大量社会资源同时在减碳环保成为全球共识的

背景下，针对其所产生的负的社会外部性进行征税也具有现实意义，因此多个国家也开始聚焦这一领域进行政策制定。

除了前三大政策密集区以外，2021 年的监管政策还呈现出的一个新的特征是监管细化，从所统计的数据看，稳定币、NFT、元宇宙、DAO 也成为政策制定者关注的加密领域，这表明政策制定者对于加密行业的产业结构有了进一步认知，政策制定也更加具有针对性。

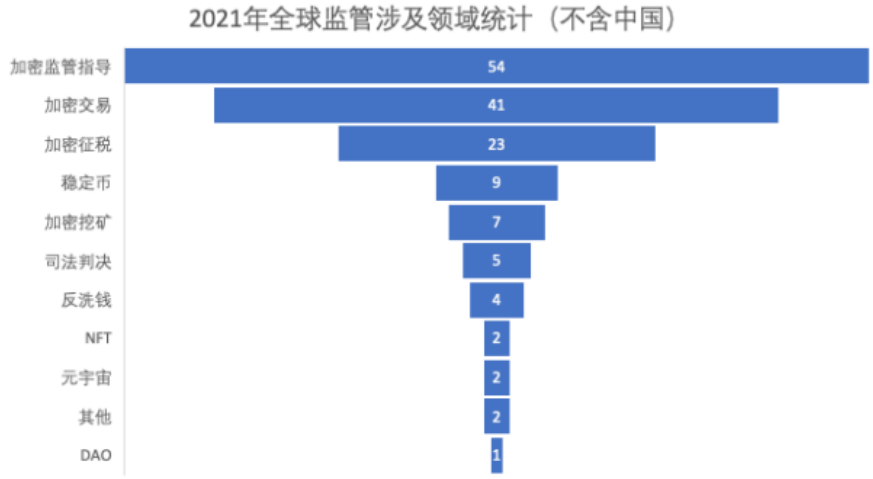


图 5-3：全球加密政策涉及领域

来源：火币研究院

5.2 全球监管新特征

在对全球加密政策梳理过程中，我们发现 2021 年全球监管呈现出一些新的特征，首先是联合监管趋势开始上升，其次是在一定程度上对于目前的国际竞争格局产生了影响，最后是不同国家针对加密监管的态度出现了不同程度的反复。

● **特征一：联合监管趋势加强**

联合监管包括两个维度，一个是主权国家内部的跨部门联合监管趋势，另一个则是国际间跨国联合监管趋势的出现。由于加密行业所具有的全球开源、业务范围广等特点，使得传统监管部门使用的分业管理模式受到了一定程度的挑战。具体表现为业务边界不明导致无法明确行业监管主体、跨国交易导致的反洗钱难度增加等对于主权国家间的监管提出了更高的挑战。目前随着社会各界对于加密行业的认知度不断提升，监管部门也提出了新的监管思路，例如美联储、美国联邦存款保险公司以及货币监理署未来将联合成立针对加密货币监管的

“跨部门冲刺小组”、韩国则考虑成立专门的中央加密货币监管机构等；除此以外，在跨国联合监管上国际货币基金组织号召各国应联合实施针对加密行业监管的全球标准、欧盟雨美国金融监管机构也正就稳定币以及数字资产合作进行讨论。预计未来这一趋势将进一步增强，从而适应加密行业 7*24 小时全天候、全球性业态新模式。

● **特征二：一定程度改变国际竞争格局**

由于当前各国对于加密资产的属性、定义以及观点不同，因此不同的国家在面对这一新兴业态表现出了不同的监管态度。然而，随着加密行业规模的不断扩大，所产生的财富效应不断凸显，其具有的应用价值逐渐得到关注，围绕加密行业的政策变动通常会成为国际关注的重点。此前名不见经传的萨尔瓦多因为其公开承认比特币的法币地位，成为国际讨论的热点话题，一定程度上提升了萨尔瓦多的国际影响力；于此同时，加密资产也成为了国际竞争中的一个新的工具，俄罗斯外长曾表示未来不排除通过“数字资产”以及其他货币取代美元在该国的国际结算业务中的使用率。毫无疑问，随着新兴加密资产的出现，未来国际间的竞争模式将会进一步出现变革，这对于推动全球治理朝着扁平化模式或将产生一定的积极意义。

● **特征三：针对加密监管出现不同程度反复**

随着加密行业的发展，不同国家对于这一新兴行业的认知也在不断进行变化，而这一反复过程对于理解新鲜事物也是一种正常现象。在目前全球见过环境中，变化最为反复的莫过于印度，印度各监管机构对于加密行业的观点不尽相同，在经历了印度央行宣布加密交易违法到印度高院认定加密交易不违法，尽显其高层对于加密行业观点的不同观点，而最近印度宣布将通过立法禁止加密业务。事实上，除了印度，还有韩国与美国也同样出现了政策上一定程度的反复，例如韩国 10 月已对外宣布 2022 年一季度将开始对加密资产进行征税而到了 11 月再次宣布这一决定将被延迟，对此韩国财政部长公开表示“损害了政策的一致性”，而美国货币监理署随着代理署长的调整，此前由 Brooks 制定的开放银行业从事数字货币业务政策也被新任代理署长叫停，尽管程度不算完全相反，但至少也表示即使是监管最为积极的国家也依然对于这一行业的发展认知上存在着波动。

总体而言，纵观 2021 年全球加密行业政策，可以认为整个加密行业随着不断发展正在受到监管部门和传统社会的高度关注，这种关注将推动着加密行业监管体系的建设，从而规范加密行业发展路径，从长期来看，将对整个加密行业步入社会主流提供相应的制度基础。

第六章 未来篇 2022 年区块链行业展望

6.1 全球流动性收紧，比特币或迎来熊市

今年 11 月 4 日，美联储 FOMC 会议宣布正式启动 Taper，从 11 月起每月减少国债购买 100 亿美元，MBS 50 亿美元。Taper 意味着美元流动性的边际递减，虽然这一变化并不改变流动性本身的扩张或收缩方向，但却可能会改变资金的流动或资产错配的程度。尤其对于比特币这种另类高风险资产，其对美元流动性变化的敏感程度在理论上会更高。

在上一轮 Taper 中，美联储在 12 月正式宣布启动 Taper，这一时间点正是比特币 2013 年牛市的顶点，随后比特币深陷熊市之中。

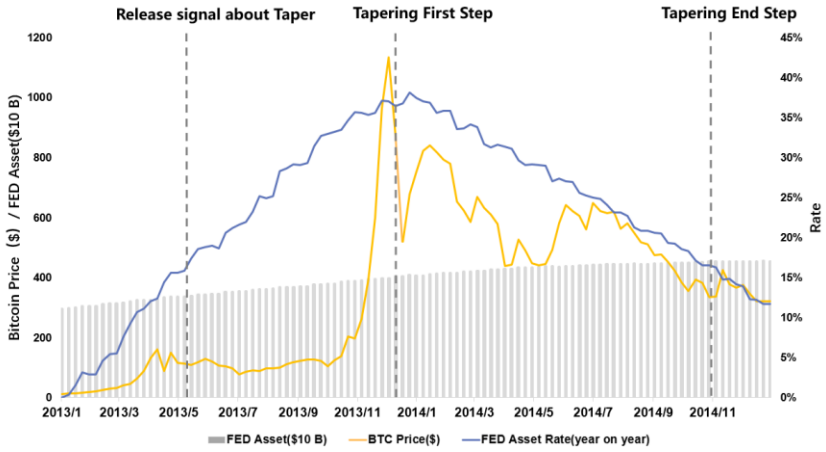


图 6-1：美联储上一轮 Taper 期间比特币价格走势（2013-2014）

来源：Wind，火币研究院

另一方面，根据美联储货币政策的正常操作，在 Taper 结束后，随后而来的便是加息，加息即意味着流动性的收缩，将对包括比特币在内的各类风险资产造成巨大冲击。目前，多位美联储高官先后暗示可能会加快 Taper 进行。加快 Taper，则意味着加快 QE 的退出，这意味着流动性的拐点将提前。因此，在市场预期作用下，以比特币为代表的各类高风险资产，未来很难继续上涨，甚至不排除进一步下跌的可能。

6.2 DAO 逐渐成为链上治理主流形式

DAO 作为区块链技术上的一种组织形式，其目的是协同组织成员的利益，最终完成组织管理和组织决策。自 2021 年下半年以来，Constitution DAO 众筹竞拍美国宪法副本、OpenDAO 空投 SOS 等事件表明，DAO 仍在不断地强化和深化、甚至逐步溢出影响到主流世界的社会生活中。

DAO 的发展已经颇具规模。根据 DeepDao 的数据，目前已经有 188 个 DAO 管理着 115 亿美元以上的资产，整体 AUM 快速增长，由年初的 40 亿美元达到目前的 170 亿美元。然而，DAO 也存在缺乏有效的协调机制、完善的基础设施等缺陷。因此在未来，DAO 领域的核心需求主要是 DAO 组织的管理需求和 DAO 资金的管理需求。特别是 DAO 资金的管理未来可能会和各类 defi 应用进行打通，进行财库管理。

Rank	PROTOCOL	AUM	TOKEN PRICE
1	Gnosis	3.42B	$445.63
2	Uniswap	3.26B	$18.50
3	Ethereum Name Service	3.07B	$42.80
4	Aave	1.54B	$294.93
5	Gitcoin	803.53M	$14.46
6	Dydx	699.25M	$9.43
7	Compound	662.23M	$222.84
8	Lido DAO	649.54M	$2.66
9	Radicle	570.83M	$11.28
10	Synthetix	275.63M	$6.19

图 6-6：AUM 排名前十的 DAO

来源：Boardroom

6.3 跨链将成为多链时代下的基础设施

2021 年公链进入百家争鸣的时代，大多数优质项目会同时登陆多个公链，由于对跨链桥产生了强烈的市场需求，诞生了诸如 Anyswap，Synapse Protocol 等多个跨链龙头项目，各项目锁仓量均达数亿美元。可预见的是，随着高性能公链，layer 2 网络的快速增加，安全、快速的跨链桥成为重要的基础设施之一。

项目	总锁仓量	支持链数	服务类型	服务特色
WBTC	$14269M	2	单向跨链	仅支持BTC跨链
Ren Protocol	$970M	7	单向跨链	支持BTC，ZEC等跨链
Anyswap	$4620M	23	多链互跨	支持的公链最多，币种最全
Synapse Protocol	$623M	7	多链互跨	支持Boba Network与Harmony
Wormhole	$619M	5	多链互跨	支持rust公链：Solana与Terra
Chainswap	未知	23	多链互跨	部署在Anyswap上
cBridge	$21M	9	多链互跨	正开发支持智能合约调用的通用链间互操作协议
Hop Protocol	$104M	5	Layer2互跨	支持的layer 2最多
Connext	$10M	8	多链互跨+Layer2互跨	正开发支持智能合约调用的通用链间互操作协议

图 6-7：市场头部跨链项目

来源：Huobi Research

然而，未来用户不仅仅满足于跨链这项基本功能，其核心诉求是通过跨链来追逐利润（套利，提高资本效率等）。因此，未来开发简单的跨链桥已没有明显的市场竞争力，跨链项目会进一步向专业化、精细化方向发展，在跨链交易聚合、跨链收益聚合仍有一定的市场前景。

此外，受制于公链性能影响，未来项目不会满足于开发 Dapp，更会追求开发自己的公链，因此通用跨链协议如 Cosmos、Polkadot 会迎来一段时间的增长期，这些协议生态上的优质项目有投资潜力。

6.4 DeFi 进入 2.0 时代，链上永续合约和期权产品迎来爆发

在过去一年，DeFi 迎来飞速发展，TVL 达到了 2467.7 亿美元，以 AMM，借贷，聚合器为代表的 DeFi 项目成为市场热点。然而，DeFi 1.0 仍然存在资本效率低下、流动性不足、损耗高等问题，严重制约了 DeFi 在未来的发展。市场上于是出现了对 DeFi 2.0 的思考。

从未来发展看，DeFi 2.0 至少将满足市场对以下几个方面的需求：

- 更高的流动性需求：这要求 DeFi 在不依赖“流动性挖矿”的前提下解决流动性问题，一般有 POL（Protocol Owned Liquidity）和 Laas（Liquidity-as-a-service）两种方案；

- 更高的收益率需求：为提高用户收益率，一般有两种方案，一是提高资本利用效率；二是降低损耗（典型的是 AMM 的无偿损失）；
- 更多的交易产品需求：目前 DeFi 在衍生品领域的发展缓慢，但市场对固定利率、永续合约、期权、CDS 等衍生品均有强烈的需求，预计 DeFi 2.0 时代将出现链上衍生品交易的井喷。

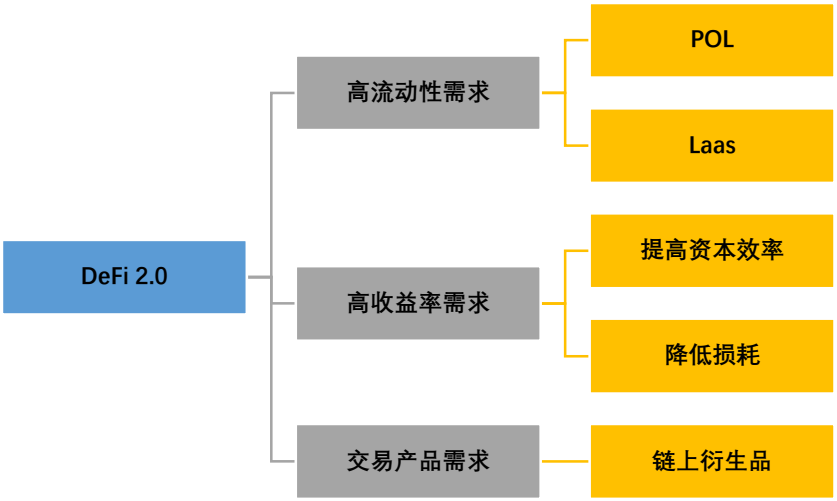


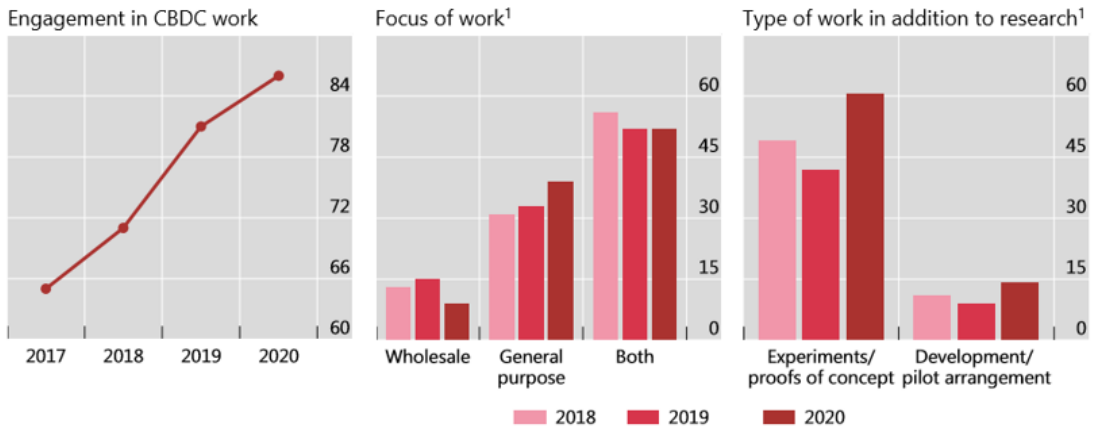
图 6-8：DeFi 2.0 发展路径

来源：Huobi Research

目前以 OlympusDAO、Alchemix 为代表的 DeFi 2.0 项目均取得了巨大的成功，而在加密货币市场逐步转熊的 2022 年，生存将成为各 DeFi 项目的第一需求，而 DeFi 2.0 凭借其在流动性、高收益和创新性等方面的优势，更能适应快速变化的市场环境，届时我们也将看到越来越多的 DeFi 2.0 项目出现。

6.5 CBDC 逐步落地推行，跨境支付成探索重点

根据国际清算银行近些年对全球 60 多家央行的调查显示，在过去的四年里，越来越多的中央银行开始进行对 CBDC 的研发工作，目前这一比例已经达到了 86%。从使用场景和对象看，央行数字货币又被分为通用型（又称零售型）和批发型；前者主要面向公众，后者主要在央行与金融机构之间使用，调查显示零售型 CBDC 受到央行的普遍欢迎，但目前大多数央行要么同时关注批发型和零售型 CBDC，要么将工作范围缩小到仅零售型 CBDC。



[1] Share of respondents conducting work on CBDC.

图 6-9：BIS 对全球多家央行关于 CBDC 的调查

来源：BIS，Huobi Research

此外，目前大多数国家都已经认识到了央行数字货币的重要性，然而对发行央行数字货币多持谨慎态度。调查显示，大部分央行对 CBDC 的工作仍处于概念验证阶段，只有少部分国家进入了实际研发阶段。根据最新的消息，中国将在 2022 年北京冬奥会前后正式推出自本国的央行数字货币---E-CNY，而 2022 年也将成为全球 CBDC 落地推广的元年。

值得注意的是，目前 CBDC 在跨境支付方面的用途（Mulit-CBDC Bridge）受到各国的关注。CBDC 有助于减轻跨境支付的风险和摩擦。2021 年 9 月 2 日，国际清算银行宣发与澳大利亚、马来西亚、新加坡和南非的中央银行联手测试 CBDC 在跨境支付中的使用。随着 CBDC 的不断落地成熟，这种跨境支付的安排很有可能取代当前以 SWIFT 为核心的全球跨境清算体系。

6.6 面向机构的加密借贷市场开始兴起

目前加密借贷市场主要为质押借贷市场，而信用借贷市场迟迟不能发展的原因在于，加密货币社区的用户大多为匿名的个人用户，容易产生违约风险。然而，自 2021 年以来，加密货币市场涌入了大量的机构投资者。机构用户在声誉、信用方面优于个人用户，这为信用借贷市场提供了生长的土壤。

目前在 DeFi 领域已经出现了诸如 TrueFi、GoldFinance 等去中心化信贷项目。其中，TrueFi 上线至今不足一年，已经发放了约 10 亿美元的信用贷款，且没有一笔贷款发生违约，反映出加密信贷市场的巨大潜力。随着行业中机构用户的不断增多，面向机构的信贷业务将成为下一个重要市场，未来市场规模预计可比肩 OTC 市场。

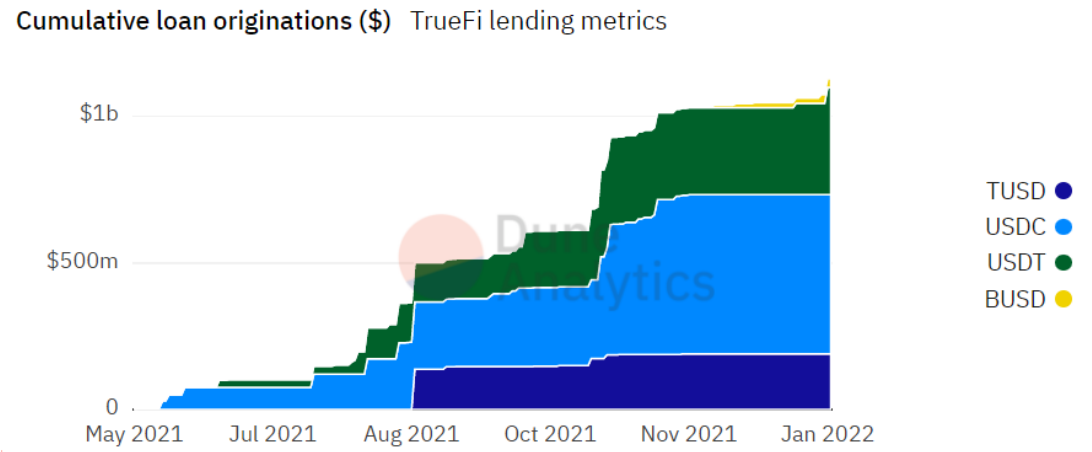


图 6-10：TrueFi 贷款存量

来源：Dune Anatytics，Huobi Research

6.7 NFT 借贷/衍生品市场迎来爆发

NFT 作为投资者的新宠，在过去一年的时间里呈现了爆发式的增长，目前整个 NFT 市场市值达到 87 亿美元，持有者达到 107 万人，已经逐步被主流社会所认可。

从市场发展的历史经验看，NFT 下一步便会向借贷/衍生品市场发展。然而，NFT 的特殊之处在于其定价较为困难，缺乏市场流动性。因此想要发展 NFT 借贷/衍生品市场，必须要先解决 NFT 定价问题，即开发 NFT 预言机。可以预测的是，2022 年 NFT 预言机/定价方案将是加密市场上的明星项目。

此外，从 NFT 的特点看，未来 NFT 借贷/衍生品市场将分化出两条发展路径，区别在于接受的抵押品类型不同：

一是基于 NFT 本身所展开的借贷/衍生品业务，这类业务的特点是资本效率高（以 NFT 本身的价格为参考进行借贷和衍生品交易），但流动性低；

二是基于 NFT 地板价所展开的借贷衍生品业务，这类业务的特点是资本效率低（NFT 地板价低于 NFT 价格），但流动性高。特别地，同一类但不完全相同的 NFT 地板价可组成连续的报价和充足的流动性，容易成为相关衍生品的标记价格，可保证 NFT 衍生品交易的安全。

6.8 新公链杀出重围，多足鼎力格局或将形成

Total Value Locked All Chains

Chain	TVL	Protocols	1d Change	7d Change	30d Change	7d Protocols Growth	30d Protocols Growth
Ethereum	163,946,561,442.26	322	-5.67%	-5.19%	-9.4%	0	33
Binance	18,660,041,983.72	200	-3.30%	-6.81%	-15%	3	47
Terra	12,930,525,288.91	10	-8.12%	0.03%	20%	0	0
Avalanche	12,584,406,358.88	86	-5.78%	-8.31%	22%	10	25
Solana	11,474,113,437.62	38	-8.43%	-19.45%	-19%	0	7
Tron	7,218,544,197.94	5	-3.10%	-4.87%	-28%	0	-1
Fantom	6,765,304,053.09	83	-2.43%	-9.69%	-17%	3	15
Polygon	4,934,139,522.48	122	-5.83%	-1.00%	-2.7%	2	15
Arbitrum	2,198,877,698.63	44	-5.63%	-0.73%	-27%	3	6

图 6-11：涌现出的新公链

来源：footprint analytics

Solana、Avalanche、Fantom 等新兴公链在今年下半年异军突起，资产表现亮眼。根据 DefiLlama 的数据，截至 12 月 11 日，各条公链的 DeFi 协议中的总锁仓量（TVL）总共 2468 亿美元，其中 Ethereum 1630 亿美元、BSC 160.8 亿美元、Terra 128.6 亿美元、Solana 112.8 亿美元、Avalanche 112.5 亿美元、Polygon 48.2 亿美元、Fantom 45.6 亿美元。

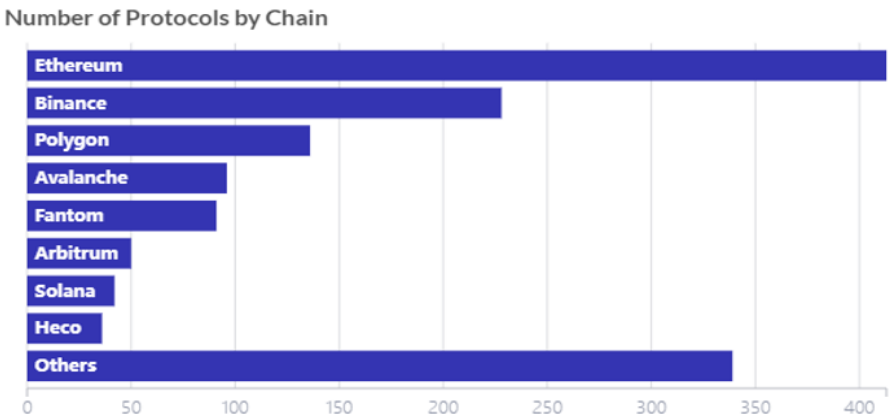


图 6-12：主流公链上的协议数量

来源：footprint analytics

因为以太坊拥堵，手续费昂贵等限制，其价值外溢到其它公链。随着 Solana、Avalanche 等为生态建设推出激励基金，公链进入快速发展时期。新公链的活跃是对现有结构的优化，尽管当前的链上生态乏善可陈，但打造基础需要时间，只有在链上生态积累一定程度后才能量变带来质变。

6.9 加密保险市场或将崛起

随着 DeFi 的持续繁荣以及公链生态的逐步壮大，加密资产安全问题越来越突出。当前区块链行业解决智能合约安全问题的方案是对合约进行审计，由此造就出诸如 SlowMist、Quantstamp 等专注区块链安全领域的明星公司，从事前审查的角度保证智能合约的安全；而定制化保险产品的推出，则从事后索赔的角度解决了投资者的后顾之忧。

目前在 DeFi 领域有众多保险创业项目，部分项目的锁仓价值已经超过 1 亿美元。然而，根据 Bitcoinist 的数据，目前仅有 2%的 DeFi 价值被投保，因此保险市场在未来还有进一步的增长潜力。

排名	名称	部署公链	锁仓价值（M$）
1	Armor	Ethereum	620.76
2	Nexus Mutual	Ethereum	578.7
3	Unslashed	Ethereum	91.3
4	InsurAce	Ethereum、BSC、Polygon	38.5
5	Sherlock	Ethereum	30.6
6	Guard	BSC、Polygon	20.4
7	Bridge Mutual	Ethereum	14.3
8	Itrust Finance	Ethereum	9.5
9	Bumper Finance	Ethereum	8.6
10	Tidal Finance	Polygon	7.1

图 6-13：DeFi 市场前十大保险产品

来源：DeFi Llama

在业务收入预测方面，自 2020 年 DeFi 迅速崛起以来，各大智能合约审计公司的业务规模均带来不小的增长，但事前审查并不能保证合约没有漏洞，并且在出现漏洞后，审计公司也不会为此负责；从开发者角度出发，对可事后赔偿的定制化保险产品的需求更大。因此，未来智能合约安全保险类产品的业务规模将远高于现有的几家明星安全审计公司。

6.10 中期主流扩容方案迎来发展机遇

自以太坊诞生以来，其低下的交易处理能力，导致以太坊网络时常发生堵塞，且 Gas 费用高涨，严重地限制了以太坊生态的发展。为此，以太坊扩容问题一直被市场所关注。然而，几年前的状态通道、Plasma 等 Layer 2 方案无法满足 DeFi 的要求，分片技术又是一个遥远

的目标。正是“往者不可谏，来者也不可追”，Rollup 自然而然成为了在短中期应对以太坊扩容方案的最佳方案，成为迈向以太坊 2.0 的中场接力手。

从总体上看，Rollup 中的 zk-Rollup 最具市场竞争力，其低成本、速度快和高安全的特征使得其他 Layer 2 方案相形见绌。自今年下半年各 Rollup 主网上线以来，Rollup 发展取得了快速发展截止 12 月末，其总锁仓量达到了 55 亿美元；其中 Arbitrum 占据了大部分市场份额，TVL 达到了 24 亿美元。

No.	Name	TVL	Market share	Technology
1	Arbitrum	$2.43B	44.06%	Optimistic Rollup
2	dYdX	$975M	17.68%	ZK Rollup
3	Loopring	$546M	9.90%	ZK Rollup
4	Boba Network	$508M	9.22%	Optimistic Rollup
5	Optimism	$437M	7.93%	Optimistic Rollup

图 6-15：市场前五大 Rollup

资料来源：L2BETA

然而，目前的 zk-Rollup 实现都是针对特定的应用，无法实现具有可组合性的通用型应用，因此 zk-Rollup 的普及必须要开发通用的 zkEVM。在过去，受制于技术上的困难，zkEVM 一直未被成功研发出来；但目前随着查找表参数和自定义小工具的出现，以及递归证明技术的成熟，zkEVM 的研发取得了极大的进展，预计将在 2022 年 zkEVM 会获得突破，届时 ZK-Rollup 将成为以太坊扩容方案的主流。

关于火币研究院

火币区块链应用研究院（简称“火币研究院”）成立于 2016 年 4 月，于 2018 年 3 月起致力于全面拓展区块链各领域的研究与探索，以泛区块链领域为研究对象，以加速区块链技术研究开发、推动区块链行业应用落地、促进区块链行业生态优化为研究目标，主要研究内容包括区块链领域的行业趋势、技术路径、应用创新、模式探索等。本着公益、严谨、创新的原则，火币研究院将通过多种形式与政府、企业、高校等机构开展广泛而深入的合作，搭建涵盖区块链完整产业链的研究平台，为区块链产业人士提供坚实的理论基础与趋势判断，推动整个区块链行业的健康、可持续发展。

联系我们:

官方网站: https://research.huobi.cn

Twitter: @Huobi_Research https://twitter.com/Huobi_Research

Medium: @Huobi Research https://medium.com/huobi-research

免责声明

1. 火币区块链研究院与本报告中所涉及的项目或其他第三方不存在任何影响 报告客观性、独立性、公正性的关联关系。
2. 本报告所引用的资料及数据均来自合规渠道，资料及数据的出处皆被火币区块链研究院认为可靠，且已对其真实性、准确性及完整性进行了必要的核查，但火币区块链研究院不对其真实性、准确性或完整性做出任何保证。
3. 报告的内容仅供参考，报告中的结论和观点不构成相关数字资产的任何投资建议。火币区块链研究院不对因使用本报告内容而导致的损失承担任何责任，除非法律法规有明确规定。读者不应仅依据本报告作出投资决策，也不应依据本报告丧失独立判断的能力。
4. 本报告所载资料、意见及推测仅反映研究人员于定稿本报告当日的判断，未来基于行业变化和数据信息的更新，存在观点与判断更新的可能性。
5. 本报告版权仅为火币区块链研究院所有，如需引用本报告内容，请注明出处。 如需大幅引用请事先告知，并在允许的范围内使用。在任何情况下不得对本 报告进行任何有悖原意的引用、删节和修改。