HashKey Capital：Web3各领域发展概述

来源：Hashkey Capital

在2024年上半年，我们观察到越来越多的 ZKEVM 项目开始转向 ZKVM 架构，其中以以太坊基金会旗下的 PSE 团队为代表。Taiko 已经在与 Risc0 的 ZKVM 合作，Scroll 也在这一领域做准备。

推动这一转变的催化剂是 Plonky3，其在性能上优于 Halo2（尽管稳定性略逊一筹），并提升了用户体验。



当前该领域可用的虚拟机包括：ZKWASM、Succinct 的 SP1、a16z 的 JOLT 和 Risc0。此外，Polyhedra 的 ZK Prover 表现优异，并计划未来开发虚拟机。Aztec 和 Mina 也在开发各自的虚拟机，但尚未公布其性能基准测试。

推动更广泛采用的关键因素将依赖于多个方面，例如证明成本、证明效率和开发时间。目前普遍认为 zkVM 很适合用来构建和部署可验证应用程序，值得进一步关注。

## ZK Middleware

在中间件方面，我们看到证明验证系统的活跃度依然很高，Brevis、Alignlayer 和 Nebra 都在和 Eigenlayer 合作，以获取安全性。由于 zk 证明相对昂贵，市场也逐渐转向采用 OP 和 ZK 的混合方案来提高证明效率。而在应用方面，诸如可验证 AI、可验证链外数据等催化剂将带来更多应用需求，对这些创新领域可保持关注。

## MEV、链抽象/账户抽象、意图

在 Flashbots，团队一直在实验并开发利用 Intel 软件保护扩展的产品，最近尝试在以太坊虚拟机上使用可信执行环境（TEEs）进行隐私计算。这些用例包括存储和处理敏感数据，确保竞价拍卖免受篡改和数据泄漏的影响。

完全同态加密（FHE）也成为对抗 MEV 的潜在解决方案，因为它始终保持数据加密，消除选择性重新排序的可能性。

## 区块构建者

根据 relayscan 的数据，区块构建市场已高度集中于少数几家构建者，其中包括一些以满足自身交易需求而闻名的高频交易公司。目前，beaverbuild、titan builder 和 rsync builder 是市场上最具主导地位且利润最高的构建者。这种集中化现象引发了关于区块拍卖机制设计的进一步研究，旨在维护以太坊的抗审查能力。

## Relay

Relay 在区块供应中仍然起着至关重要的作用，超过 90% 的区块通过中继传输。Titan builder 今年推出了 Titan Relay，自推出以来增长迅速。

通常在评估Relay时，需要考虑以下几个因素：

性能和可靠性，可以通过在线时间、延迟和出价故障等指标进行分析。

Relay的可扩展性是指其为大量验证者提供服务的能力。

在 MEV 赛道内，我们此前已投资了较多成功项目，包括 preconfirmation 的发明者 Primev、区块构建市场的领导者 Titan、除 Flashbots 外少数成功的 MEV 系统 FastLane 等。下一阶段，MEV 相关项目如何实现价值捕获、如何能成功设计 token 等是较为关键的问题。

## 链抽象和账户抽象

链抽象是实现用户大规模采用的一个持久且关键的概念，旨在提升用户体验，使用户无感知到区块链的存在，甚至无需知道自己正在使用哪条链。NEAR 作为该领域的早期先驱之一，已推出多链签名功能，允许一个账户跨不同链使用。支持的链包括：比特币、以太坊、Cosmos 生态链、狗狗币、XRP Ledger、TON 网络、波卡等。

可参考 Frontier.tech 提出的 CAKE 框架，包括权限层、solver 层、结算层等。其中账户抽象（AA）也可以包含在权限层中。而 AA 领域主要分为两类：智能合约钱包和模块化服务。正如我们在2023年领域回顾中提到的，智能合约钱包在通过以意图为中心的设计提供无缝用户体验方面发挥着至关重要的作用。

每周活跃的智能钱包账户数量也呈上升趋势，其中 Polygon 依然是智能账户数量最多的网络。另一个受欢迎的平台是 Base，这可能得益于 Coinbase 智能钱包的推出，该钱包具有兼容性。

随着EIP-7702纳入以太坊的Pectra升级，这将带来更加无缝且用户/开发者友好的体验，因为它旨在改进之前的账户抽象（AA）设计，如ERC-4337，后者成本较高且不具备将EOA（外部拥有账户）转换为智能账户的原生支持。因此可重点关注基础设施层面的改进是否能带来新的应用。

除 AA 以外，领域内可关注的赛道还包括策略引擎、意图框架、preconfirmation 等。而意图领域内的相关项目目前还在积极开发中，具体表现以及 PMF 还有待观察。

## 比特币

比特币 Rollup 早些时候引起了极大的关注。然而，随着时间的推移，兴趣似乎有所减退，我们在比特币亚洲活动中观察到了这一点。出现的项目减少，当前环境下筹资也显得困难。

尽管如此，我们仍然见证了一些显著的技术突破，如 BitVM。一些 Rollup 项目正在探索与 BitVM 的集成。BitVM 近期迅速创新，例如已创建了 BitVM 跨链桥。该桥可以用于大额跨链交易，而较小额的交易预计将继续依赖多签名或 HTLC 交换以提高经济效率。更多细节，可以参考之前的研究。

总体而言，尽管 Rollup 面临挑战，像 BitVM 这类的技术发展仍可能为 Rollup 提供机会，如互操作性等。

## 收益导向的比特币策略

收益导向的策略也在获得关注，越来越多的项目为持有者提供包装 BTC，给用户收益，同时也容易做出来 TVL。例如，像 Mezo 这样的项目整合了多种产品，其中 Rollup 只是众多组件之一，还有像 tBTC 和 Acre 的 stBTC（流动性质押）等其他产品。

在这个领域，我们继续保持谨慎，投资于具有明确技术优势、清晰市场策略或经过验证的成功经验的团队。

BRC-20 代币的表现仍然疲软，ORDI 相较年初表现不佳，整体 BRC20 目前暂未发现太多亮点和起色。尽管在比特币减半后 Runes 曾引发强烈关注，但这种兴趣也逐渐消退。这与网络活动和费用下降的趋势一致。Taproot 资产与闪电网络的集成可能会重新激发市场兴趣和动能。

总体而言，在比特币资产可持续采用的前提下，为这一不断增长的资产类别提供服务的基础设施提供商可能成为具有吸引力的投资机会。

## Bitcoin Staking

Staking（restake）是属于原本比特币没有，但后来魔改出来的功能。能出现这个赛道，也是因为它可以算做解决了在资金端的 BTC 生息需求、产品端需要和比特币主链有所绑定的需求两方面问题。

Staking 可以按照削减机制 大概分为三类：

会对本金 slash：Babylon 是采用这种方法的一个例子

对利息 slash（失去收益机会）：CoreDAO 主要关注削减潜在收益，而不是削减本金。

不 slash：此类别包括自托管的二层网络（如旨在提高 TVL 并承诺收益的 Rollups）以及像 BounceBit 这样偏理财项目，用户的比特币由资产管理团队管理以获取收益。

Staking（restake）赛道最早的 Babylon 已经自成生态体系，基本上很多做比特币相关的应用都会考虑借助 Babylon 来实现和主链的关联性。Babylon 生态项目中 staking 相关的项目主要会围绕在实现辅助功能上，具体见 Babylon 生态一节。

这个赛道内估计会和 EigenLayer 类似，仿照出一些应用和基础设施，市场表现和生态发展有待主网上线后的进一步观察。例如 Babylon 主网在上线后不久就达到了上限。我们对Babylon的未来发展保持乐观。

## Bitcoin DeFi, MEV

BTCFi: 最近也有不少关于比特币金融应用（BitcoinFi，BTCFi）之类的项目。目前能看到的还是集中在借贷和稳定币的应用上。采用多种方法，如在比特币上锁定资产，同时在 L2 上处理逻辑的发行资产，或选择不同的资产发行方式，都会导致不同的权衡。

Wrapped BTC:WBTC、tBTC、FBTC 和 SolvBTC 最近引起了显著关注。预计这一领域的竞争会愈发激烈。例如，Solv Protocol通过广泛的合作伙伴关系、DeFi集成以及跨链可组合性，见证了巨大的需求，促使协议获得超过13,500的比特币质押。随着越来越多的项目寻求在DeFi应用中利用比特币，我们预计这一领域的竞争将进一步加剧。

比特币 DEX 和相关应用: 链上 DEX 仍主要使用 PSBT，而一些项目如 Satflow 在内存池中使用预确认策略，尽管这种方法有被替代的风险。

MEV: RBF 的激活和新类型资产的引入已经导致比特币上的 MEV 场景更加活跃。像 Rebar 这样的项目旨在建立类似于 Flashbot 在以太坊上所做的 MEV 基础设施，而像 Alkimiya 这样的项目则专注于费用/区块空间市场。目前，MEV 相关活动主要还是来自交易加速服务。我们将继续关注这一领域的持续发展，以及观察新项目不断推出各种服务来缓解MEV对用户的负面影响。更多内容可参考我们此前的报告。

## 比特币技术发展

OP\_CAT

尽管 OP\_CAT 是一个易于实现的操作码，但其激活引入了许多的功能，如比较简单的 Merkle 树验证（两个元素的 hash）到利用叠加 Schnorr 签名进行交易本体验证等更复杂的操作。然而，对其灵活性的担忧可能会引入一些无法预知的风险。

2024 年 5 月，OP\_CAT 作为软分叉在比特币审判客户端（一个在 signet 网络上的客户端）中被启用。软分叉的方式在上次 Taproot 升级中，其实也存在了各种争论和变数。不光是升级内容本身，而是如何软分叉升级的过程也有比较的讨论，因此 OP\_CAT 未必能短时间内启用；如果启用，也一定会伴随各种争论。其他的软分叉升级同理，包括 OP\_CTV（2022年已经大规模争论过一次）、APO 等等。

BitVM

BitVM 在提高比特币表达能力方面取得了重大突破，BitVM2 在之前的设计基础上又进行了改进，增强了复杂计算的验证能力，并减少了信任假设。近期的关键进展集中在 BitVM 桥的开发方面，已经达到了一定的成熟度和安全性，有可能在 2024 年底之前实现测试网/主网上线的成熟度。BitVM 桥可能会主要处理大额资产，留给了其他跨链桥的继续存在的空间。通过多重签名桥或原子交换的替代BitVM桥跨链解决方案仍然对终端用户具有实用性，提供了更快速和成本更低的替代方案。此外，我们还可能会看到未来在 BitVM2 上建立新的验证者网络。

通道、Joinpool 类的方案

通道和 Joinpool 相关的解决方案取得了显著进展。这些解决方案允许两个或更多用户在主链上共享一个 UTXO，而链外可以根据业务逻辑来执行分配（vTXO）。当用户想要退出时，他们可以通过单边退出返回主链进行结算。

除了 Hedgehog，最近的关注点主要集中在 Ark 上。Burak 推出了 Ark v2，提供了更高的资金效率，并提出了一个相关概念，称为 Brollups。

Statechain 是另一种有趣的方案，类似于基于 Joinpool 的 UTXO Mercury Layer。Mercury Layer 在这一领域取得了显著进展，而像 Mach 这样的新项目正在开发底层基础设施。



比特币作为最大的资产，历史上一直被视为数字黄金。然而，随着像BitVM2、OP\_CAT和比特币质押等创新的出现，我们正在见证比特币的更多应用。尽管与以太坊的DeFi生态系统相比，比特币DeFi生态系统仍相对新兴，但我们认为这些催化剂将使比特币DeFi生态系统在未来取得类似的成功。

## Solana

在Consensus期间，Paypal宣布在Solana上线PYUSD。自那以后，由于与Solana上一些大型DeFi协议（如Kamino Finance、Jupiter和Orca等）的集成，PYUSD的市值迅速增长。另一个表明机构对该领域兴趣的信号是，Stripe宣布重新进入Solana，允许用户接受和进行USDC支付。

Solana背后的公司Solana Labs宣布推出Bond，这是一个基于区块链的平台，旨在提升品牌与客户的互动，可能加速机构的采用。

除了机构对Solana日益增长的兴趣外，我们还注意到对Blinks和memecoins等主题的高度关注，这些主要面向零售消费者。

## Blinks

今年六月底，Solana推出了Solana Actions和Blockchain Links（Blinks），为零售用户加入Web3创造了更加无缝的体验。通过Solana Action API，用户可以将任何交易转换为区块链链接，并可以在任何界面上分享。

Blinks的影响在于，应用开发者（尤其是Web2开发者）能够更轻松地在设备和平台之间嵌入链上操作。相应地，专用浏览器（或组件）可以直观地展示这些元素，包括链接、二维码、推送通知、按钮等。

这种方式与Solana推动大规模采用的目标一致。目前，Blink生态系统中约有155个项目，这些项目在采用前都需要经过官方审核。其中，25个项目专门注册了Blink域名，其他项目则注册了Blink兼容性。社区对blnk.fun和BlinkEditor表现出浓厚兴趣（尽管BlinkEditor的官方推特账号目前被暂停）。

这一过程类似于Pump.fun，用户只需设置数量、价格和描述等参数即可发行代币。一但在Twitter等平台上分享，用户无需离开平台即可直接购买该代币。此外，像Jupiter Exchange和Pump.fun等知名项目也在集成Blinks。

## Solana 的 Meme 文化

在Solana上，memecoin仍然是生态系统中的重要组成部分，而pump.fun的推出进一步验证了这一观察。Pump.fun使任何人都可以零成本发行memecoin，这导致了大量memecoin涌入生态系统。自今年一月上线以来，该协议已产生了近5000万美元的收入。然而，尽管发行代币的门槛降低，项目数量和交易量增加，但我们注意到成功项目的概率较低。

在Solana上，值得注意的发展包括推出了token extension 功能，使代币能够具有更多根据不同项目需求定制的功能。随着Firedancer客户端预计即将上线，这不仅带来了多样化的验证客户端，还大幅提高了网络吞吐量并降低了成本，从而巩固了其对开发者和用户的吸引力。

## TON

Ton在2024年上半年表现出色，录得超过200%的涨幅，这归因于在TON上开发的小程序争相吸引Telegram的庞大用户群。我们选择聚焦TON的原因可以分为以下几点：

Telegram上的活跃生态系统：Telegram拥有约9亿月活跃用户，这使其对寻求分一杯羹的开发者具有吸引力。再加上应用内钱包以及内置的法币入金通道，我们对Telegram将大量Web2用户带入Web3持乐观态度。

与其他流行的消息应用（如微信）相比，我们认为TON有潜力复制微信在大规模变现上的成功。微信目前有13亿月活跃用户，其中约4亿活跃在游戏领域。游戏是小程序中最受欢迎的类别，其次是电商和日常服务。前100名小游戏每季度产生130万美元的收入，而热门游戏的月收入可达1500万美元。

Notcoin是TON上的一款tap-to-earn游戏，在2024年上半年获得了广泛关注。拥有超过4000万用户的Notcoin树立了一个积极的范例，并为开发者、投资者和零售用户提供了加入TON生态的动力。然而，这也导致了流量膨胀和一定程度的过度炒作。

在生态发展方面，TON在今年二月推出了广告分成机制，允许频道所有者获得50%的广告收入，并以TON进行结算。目前，TON设立了一个规模为9000万美元的生态基金和2.2亿美元的社区激励计划，专门用于投资和发放资助（grants）。在合规性方面，TON推出了TON Star Coin模式，直接与苹果商店（Apple Store）绑定，用户可以通过Apple Pay购买游戏内的虚拟道具，而Telegram仍将使用TON来结算给项目方。对于链上充值需求，大部分应用程序内设有支持第三方充值的机器人，而不是采取一刀切的方式。

然而，Telegram首席执行官, Parel Durov,最近因网络和金融犯罪指控而被捕，以及因TON原生meme币，DOGS，造成的网络中断，成为了对生态不利的因素。尽管这值得警惕，但TON背后的团队重申该项目将继续保持运营。鉴于我们对TON生态系统的关注，团队将等待TON在基础设施方面的进一步发展，以提升生态系统的成熟度。

## 重质押 （Restaking）

Eigenlayer

在2024年上半年，重质押成为了最热门的话题之一，而Eigenlayer是这一趋势的主要推动力。

Eigenlayer的成功体现在多个方面：

锁仓总价值（TVL）最高达到了200亿美元。

Eigenlayer的重质押功能催生了至少5个流动性重质押代币（LRTs）和超过20个活跃验证者服务（AVS）。

这使得以Pendle和AAVE为代表的以太坊DeFi领域焕发新生。

Eigenlayer成功地将其叙事从仅仅提供共享安全（为以太坊节点提供额外奖励）转变为补充以太坊治理系统的重要角色。

Eigenlayer的核心在于其AVS。目前有16个活跃的AVS（活跃验证者服务），其中只有EigenDA支持Eigen代币重质押，涉及370万枚ETH。其他AVS如Omni和Eoracle分别有80万至200万枚ETH，共计至少20亿美元的资产用于保障安全。ZK（零知识）项目与AVS的契合度较高，通过将部分ZK验证任务转移到链下，由质押者处理，从而降低成本并提高效率。如果未来基于 AVS 的基础设施对现有以太坊生态的基础设施产生较强的替代效应，会发挥出 Eigen 代币的效应并对其价格产生支撑。

而在 LRT 方面，各项目方采用了不同设计、策略，也导致各项目表现各异。但整体来看，LRT 的表现也很大程度上依赖于整体市场表现和 EigenLayer 未来是否表现强劲。尽管取得了初步成功，我们仍需关注LRTs未来可能面临的挑战。LRTs的过度金融化可能会影响以太坊链上生态的稳定性。预计这一领域的竞争会日趋激烈，留给新进场玩家的机会不多。

Babylon

Babylon是一个平台，允许比特币持有者在无需信任的情况下质押比特币以保障权益证明（PoS）链的安全性。

根据Babylon官网，目前列出的生态项目有91个，涵盖7个类别：Layer 2、DeFi、流动性质押、钱包和托管人、Cosmos、终局性提供商和Rollup基础设施。其中：

钱包和托管人：主要是成熟的钱包和托管解决方案。

终局性提供商：主要是质押服务。

Cosmos：主要是Cosmos生态系统中的较老项目。

这三类项目中较少有新项目。新的项目主要集中在Layer 2、流动性质押和DeFi领域：

Layer 2：Bison Labs、BSquared Network（我们的投资组合公司）、Lorenzo、Map Protocol等。

DeFi：Kinza Finance、LayerBank、Levana、Mars Protocol、Stroom和Yala Finance（投资组合公司）。

流动性质押：Bedrock、Chakra、Lombard、pSTAKE、Solv、Nomic、PumpBTC。

此外，我们还看到其他协议如Satlayer正在Babylon上构建重质押平台，Nubit则利用Babylon增强其比特币原生数据可用性层。

随着许多 DeFi 收益项目围绕比特币展开，利用闲置比特币生成收益的需求显而易见。我们预计会有更多项目提供比特币流动质押服务，并且随着比特币收益/比特币DeFi叙事的持续发展，我们可能会看到其他生态系统的资金流入比特币。

## Modularity

数据可用性（DA）

数据可用性（DA）领域的参与者较少，包括以太坊、Celestia、EigenDA、Avail 和 NearDA，这些项目的进展各不相同。DA 项目主要关注安全性（包括数据完整性、网络共识）、可定制性、互操作性以及成本。2024年上半年的 DA 领域呈现出复杂的局面，例如 Celestia 的 DA 代币已经从历史高点回落，而竞争对手 Avail 则在最新的 A 轮融资中筹集了 7500 万美元，由 Founders Fund、Dragonfly 和 Cyber Fund 领投。

在 DA 领域，主要竞争者包括以太坊和 Celestia。在对比 Celestia 和以太坊时，我们看到以太坊仍然是 rollups 的首选。



以太坊 DA 的主要用户包括 Taiko、Base、Scroll、Arbitrum 和 OP Mainnet。相比之下，Celestia 的主要用户包括 Orderly、LightLink、Manta Network、Lyra 和 Hokum。尽管以太坊 DA 成本较高，但其需求和使用量已超过 Celestia，从而为以太坊带来了显著的收入增长。

随着 DA 领域的成熟和竞争加剧，市场已趋近饱和，项目成功的关键在于客户获取和生态系统的活跃度。项目还应关注其他领域，如去中心化交易所（DEXs）、游戏、桥梁和支付，以实现规模扩展。除了作为纯数据可用性服务外，提供不同的服务也将有助于更容易地吸引和留住客户。

总体而言，我们看到数据可用性领域的竞争日益激烈，各参与者在定价方面的竞争越来越激烈，这可能对他们的长期盈利能力构成挑战。

## Rollup Frameworks & RaaS

在 rollup 领域，Arbitrum、Base 和 OP Mainnet 领先优势明显，其中 Arbitrum 处于领先地位。Base 在 Coinbase 的强力支持下不断缩小差距，并将自己品牌化为一个消费用户应用中心，推出了如 Farcaster 和 Friend.tech 等应用。

OP Rollups 和 ZK Rollups 取得了不同程度的成功，其中基于 OP Stack 的 OP Rollups 占据了领先地位。总体而言，RaaS（Rollup-as-a-Service）由 4 个主要解决方案提供：Arbitrum Orbit、OP Stack、ZK Stack 和 Polygon CDK，每个解决方案都有其自身的优缺点。然而，这些不同 RaaS 提供者的共同结果是 rollup 数量的不断增加。

利用 OP Stack 的优势，通过OP Superchain等概念存在将 OP Stack 链统一的机会，例如通过共享排序 。除了通过高吞吐量性能扩展以太坊，这些 rollup 也可以通过实施 AA 功能和引入持久且受欢迎的消费应用来实现差异化。随着它们继续面临来自如 Solana 和 Sui 等 L1 的挑战，这将保持它们的竞争力。

与 rollup 相关的 sequencer 赛道，近期没有太多新项目，老项目主要集中在 3 个方向上的优化改进：UX、MEV、去中心化。



随着部署rollup的难度降低，Rollup-as-a-Service 服务提供商将在生态系统规模、跨链互操作性以及配备全面集成的模块化工具包等多个方面展开竞争。

## DePIN

作为区块链技术中最持久的用例之一，DePIN 在 2024 年上半年获得了显著的关注，这可以归因于 Solana 作为 DePIN 应用中心的吸引力以及对人工智能领域的极大兴趣。AI 与加密技术的交叉点突显了这两个领域之间日益增长的协同效应。节点销售是在 2024 年非常流行的货币化策略，已被证明在启动社区和为项目筹集额外收入方面取得了成功。然而，尽管引起了广泛关注，DePIN 在过去三个月的回报率仍然不尽如人意。

## 物联网传感器 / 可穿戴设备

这一领域涵盖了各种物联网传感器和消费类可穿戴设备，如手表、手环、戒指等。该领域的核心基础提议在于数据的收集，利用 Web3 技术使数据更易于访问和货币化。该细分市场的一个关键问题是激励用户参与数据挖掘并通过数据分发赚取奖励，而这一点与 Web2 解决方案相比尚未取得广泛成功。对于可穿戴设备而言，消费者购买的前三大动机是（1）健康与保健，（2）健身追踪，（3）增强对智能手机和其他智能设备的访问性。在社区启动过程中，提供令人满意的用户体验并加上可持续的代币经济学和价值累积机制至关重要。

## 数据市场

在这一领域，关键挑战是数据市场的可扩展性和采用率。创建一个孤立的数据市场尤其在数据丰富的环境中可能会面临挑战。

## 无线网络

在无线网络领域，许多项目试图使用 Web3 概念来提高穿透率，但除了少数成功的项目（如 Helium Network）外，普遍存在的问题包括用户体验差、兼容性问题、服务可靠性不足等。在2024年，由于成本、地理位置和经济发展等各种因素，全球某些地区的互联网普及率仍然较低。由社区提供支持的无线网络可以填补这一空白，可以借鉴Helium网络的成功经验。

## AI x Crypto

由 OpenAI 的 ChatGPT 引发的对人工智能的巨大需求，导致了对存储、计算和网络资源需求的激增。中心化的 AI 基础设施提供商面临投入门槛高、资源不匹配和数据不可控等各种问题。在此背景下，区块链技术成为了一个可行的解决方案，通过代币激励等机制，鼓励了用户和社区的积极参与。

AI 也会是我们后续在 DePIN depin领域看的最积极的细分领域，主要是因为AI和机器学习模型的训练的确需要大量的算力，而DePIN项目通过分布式网络，和激励机制鼓励用户共享其闲置的计算资源是能够产生实际收入且体量还不小的。模式在成本效益上，也的确相对于中心化服务是有较大的优势。市场上已有项目已经在实际应用中证明了其价值，场景涵盖AI模型的训练和推理服务，为游戏提供渲染能力等，都能说明这个领域的需求还是真实存在的。

在计算基础设施领域，可以在计算网络中添加隐私保护，例如数据隐私和模型隐私。区块链技术的核心原则是安全的、隐私保护的验证。在这方面，虽然各种方法（如ZKML、OPML、TEEML）存在不同的权衡，但都在不断发展。

以往较为活跃的数据赛道也越来越多的和 AI 进行结合，为 AI 服务。因为区分大模型之间效果的主要因素就来自于数据集。数据赛道的方向包括：提供数据源（数据 DAO）、数据相关基础设施（向量数据库、知识图谱、去中心化数据库等）、数据隐私（FHE、TEE 等）。

这些发展凸显了数据驱动的AI生态系统日益受到关注，并强调了数据隐私和去中心化基础设施在未来AI应用中的重要性。以下是一些关键参与者，推动了AI与加密领域的蓬勃发展：

数据源、标注、市场：Grass、Vana、Dria、DIMO、Hivemapper、Sahara Labs、Ocean Protocol、Singularity Net

计算网络：Aethir、io.net、Akash Network、Bittensor、Filecoin、Render、Nosana、Ritual AI、Gensyn AI、Together.ai

验证网络：Modulus Labs、Giza、Ora、Vana Labs、Aztec

代理网络：ChainML、MyShell AI、Spectral Labs、Autonolas、Fetch.ai、Delysium

AI驱动的应用：Kaito.ai、0xScope、Ringfence AI、Kai-Ching

## AI 与加密领域的显著趋势

随着对 AI 和机器学习训练需求的指数增长，计算能力成为一种极其宝贵的资源。许多项目涌现出来，旨在全球范围内集聚计算资源以满足这一需求。

随着基础模型的普及，越来越多的关注也转向了模型的微调和优化，以满足企业的具体需求。

无代码/低代码平台在个性化 AI 代理部署方面出现了更多创新。在 Web3 AI 中，一些值得关注的项目包括 MyShell AI、Hyperbolic Labs、Prime Colony 和 Wayfinder。

展望未来，DePIN领域中的人工智能、物联网、去中心化无线（DeWi）和去中心化能源等领域值得进一步关注。

## RWA

现实世界资产（RWA）领域仍然是加密货币的基石，使得 Web3 技术与传统资产类别紧密相连。现实世界资产为加密货币带来了许多好处，例如多样化的实际收益和更容易访问流动性差或私有资产类别。该领域在这一方面继续取得重大进展，从代币化联盟章程的形成、Mantra 的 5 亿美元房地产代币化、Blackrock 的 BUIDL 基金，到对 Securitize 和 Ironlight 的重要投资，以促进代币化资产的采纳。

现实世界资产中有许多资产类别，但最受关注的领域是私人信贷和美国国债。美国国债的前三大发行者是 Blackrock BUIDL 基金、Franklin Templeton 的美国政府货币市场基金以及 Ondo Finance 的 USDY。在私人信贷领域，竞争由 Maple Finance、Centrifuge 和 Goldfinch Finance 等几个关键玩家主导。在传统金融中，私人信贷的估计规模为 1.5 万亿美元，预计到 2028 年将增长到 2.8 万亿美元。相比之下，Web3 私人信贷仍然较小，但未来增长前景看好。

在代币化商品方面，黄金仍然是主导资产，其中排名前两位的商品是Paxos Gold和Tether Gold。

在代币化收藏品方面，这个领域仍然相当小众和孤立，因此，产生持久的需求并为代币化收藏品提供资产可组合性对项目来说至关重要。

## 机构对代币化的需求

机构投资者对利用区块链技术代币化金融产品的兴趣不断增加。然而，大多数高管仍将监管风险置于首位，因此对公共区块链的暴露仍然有限。要在这一领域中前行，需要关注市场结构发展、违约风险管理和流动性管理。只有通过关注合规性和基础设施安全，现实世界资产领域的参与者才能捕获零售和机构的采纳。一个在区块链领域取得显著进展的是Avalanche。通过Avalanche Evergreens，该网络与Citi、JP Morgan和ANZ等多家机构建立了合作关系，展示了其对机构的吸引力，能够成功地为机构提供了一个安全、可定制且高效的链上RWA平台。目前，我们对RWA相关的叙事感到兴奋的包括RWA指数代币、RWA支持的稳定币、RWA支持的DeFi用例等。

RWA 采纳可能更多地由机构推动，而非零售用户。然而，随着监管政策逐步明晰，我们预计将会出现更多项目，提供超越国债的各种代币化证券，以满足不同投资者的风险偏好，促使投资者越来越倾向于接受 RWA 的概念。

## 游戏与娱乐

在 2024 年上半年，除了 TON 迷你游戏外，市场对游戏的情绪依然低迷。表现较好的游戏包括 TON mini games 如 Notcoin，Catizen、Hamster Kombat 等等。

## 生态系统

除了我们在 TON 一节讨论的 Telegram 游戏生态之外，目前，IMX、Polygon 和 Ronin 仍然是按日均 UAW（活跃钱包用户）计算的热门游戏链。Ronin 在一级游戏生态系统中继续占据领先地位，得益于像 Pixels 这样拥有强大游戏社区的游戏，其 7 天 UAW 达到 60 万。其网络上拥有约 380 万月活跃用户（MAU）。Ronin 对中小型游戏仍具吸引力，该生态系统能够为游戏开发者提供用户流量。截至目前，Ronin 已吸引了超过 12 家游戏工作室入驻。此外，Ronin 还与 Polygon 的 CDK 合作以启用 zkEVM，允许开发者在 Ronin 上推出自己的 L2 链。这可能成为 RON 的一个积极催化剂。

另一方面，IMX 主要涵盖中大型游戏，并持续吸引大型的 Web2 游戏工作室，为其提供全面的部署解决方案。Immutable 与 Netmarble 的子公司 Marblex 联合推出了 2000 万美元的生态系统支持计划，以进一步推动 Immutable zkEVM 上的游戏生态发展。

我们持续欢迎进入 Web3 领域的工作室，以及那些善于学习、敏感于加密文化并以用户为中心的游戏制作人和 KOL 创始人。

## 游戏与人工智能（AI）

游戏与AI的结合仍未见明显进展。游戏玩法仍然高度集中，Web3 中的消费者驱动、AI 生成的内容尚处于早期阶段。对在 NPC、伙伴和脚本编写中应用 AI 的兴趣主要集中在 B2B 游戏开发者中。



总体而言，游戏生态系统竞争激烈，关键在于平衡激励措施和社区建设。专注于培养忠实用户的策略，如提供优质的游戏体验、积极的用户反馈和战略合作伙伴关系，可能在实现长期成功方面发挥有效作用。

## SocialFi

SocialFi 已成为热门话题，总结为Friend.tech的延续，Farcaster的突围和Ton/TG社交应用的爆发，主要的三大因素。

Friend.tech

自 2023 年推出以来，Friend.tech 引发了关于其模型的长期性和可持续性的持续讨论。尽管初期发布非常成功，但用户活动在今年有所下降。2024 年 5 月发布的 V2 版本引发了新的兴趣，引入了付费群组俱乐部、创新的费用结构和高 APY 等功能，导致用户数量暂时激增。然而，社区对代币流动性和空投分配的批评，以及来自其他社交平台的激烈竞争，导致用户参与度再次稳定下来。尽管对其长期可行性存在疑虑，但 friend.tech 的推出为社交金融领域带来了一个新的模型，关键有三点启发：（1）社交影响力的代币化可能性，（2）Web3 中的付费群组俱乐部，（3）具有跨平台互操作性的社交资产。

Farcaster的突围：

今年，Farcaster 取得了显著的进展，成为该领域的主导玩家。相比之下，其他社交协议大多已经从聚光灯下消失，有些甚至似乎处于衰退边缘。Farcaster 推出的 Frames 受到了积极的反馈，它引入了一种新的社交、链上交互方式，使用了熟悉的 Web2 界面，显著提升了Farcaster的用户体验，使其DAU激增，并吸引了加密开发者和用户的关注。此外，Farcaster与meme代币的结合，特别是像Degen这样的代币的成功，显著推动了平台的用户增长和活跃度。空投活动有效地提升了用户参与度，并促进了一个充满活力的社区的形成。

Farcaster 生态系统可以大致分为以下几类：

客户端：Warpcast、Recaster、Supercast、ampcast、Farcord、Firefly、far.quest 等。

去中心化应用（dApps）：Jam.so、DeBox、Paragraph、CasterBites、Unlonely、Bountycaster、Wildcard、AlfaFrens 等。

工具：sharecaster、Alertcaster、Searchcaster、Farcaster storage、farcaster.vote 等。

API 服务：Neynae、Pinata、Airstack 等。

总体而言，SocialFi领域的成功情况参差不齐，网络效应仍然是决定项目成功的关键因素。在这一领域，我们关注能够克服冷启动问题并吸引多样化用户群体的项目，要求其提供类似于Web2的用户体验，并在奖励创作者和平台增长之间找到微妙的平衡。

## DeFi

2024年上半年的 DeFi 增长主要归因于 Eigenlayer 的巨大关注，该项目向以太坊引入了再质押（restaking）的概念，以及 Ethena，这是一种现已积累超过30亿美元 TVL 的对冲中性稳定币。

稳定币受到了开发者的新一轮关注，更多的 RWA 支持的完全抵押稳定币项目试图复制 Maker 和 Tether 所取得的成功。尽管兴趣增加，但稳定币在链上找到持久的使用场景仍然具有挑战性，当前主要用于中心化交易所。这可能对那些希望通过本地治理代币提供价值的去中心化稳定币项目构成挑战。

Eigenlayer 在 2024 年上半年占据了大部分关注，生态项目如 Ether.Fi、Pendle 和 Renzo 利用对重质押的激增兴趣来争取显著的市场份额。尽管受到很多关注，但 Eigenlayer 未能完全满足用户的期望，部分原因是宏观环境的疲软。

从区块链的角度来看，以太坊继续在 TVL（总锁仓价值）方面处于领先地位。Blast 和 Base 在 2024 年上半年表现显著。随着各种激励活动的推出，Scroll 的 TVL 已超过 10 亿美元。

在非 EVM 链中，Solana 的最大 TVL 贡献者是 Jito 的 JitoSOL，其他催化剂包括蓬勃发展的 meme 文化和借贷生态系统。与 BTC 相关的链也引起了兴趣，但由于激励计划结束后 TVL 下降，维持兴趣仍然具有挑战性。

最近流行的CeDeFi 模式反映了对链上资产可持续、安全回报的需求。无论是通过 ENA 收费挖矿还是 RCH 的期权结构化，最终的支付者都是中心化交易所用户。

DeFi 已经展现了其通过丰厚收益吸引资本的能力。目前，AAVE依然是许多Layer 2和公链上的主要资金去处，而Uniswap仍然是主要的资金池。然而，长期成功的关键在于协议是否能够为持有者积累价值并满足长期预期。随着链数量的增加，流动性逐渐分散，这为我们看到了机会。多样化的 DeFi 解决方案满足了不同需求，从而推动了对意图导向平台的潜在需求。

## 机构服务

自去年底到今年初，市场普遍预计随着ETF的获批，2024年将是机构采用加密货币的创纪录年份，交易基础设施/机构级质押/CeFi借贷/收益型稳定币/衍生品平台等会是值得下注的方向。从一级角度，的确投资者们还在下注这几个方向，今年完成融资代表性的项目包括sercuritize(rasied $47M)，Bitstamp(acquired with $200M), Flowdesk(raised $50M), Sygnum(raised $40M), Kiln(raised $17M), Agora(raised $12M)。但公开市场上受益于 ETF 的标的目前主要是 Coinbase，其他较为容易上市的企业均为挖矿企业。

从我们的角度会愈发把这个赛道视作 fintech 领域。而从全球的fintech相关公司的融资趋势来看，融资额在持续下降的过程中，2024年第一季度金融科技领域的融资是自2017年以来的最低季度水平，而且投资者更青睐中后期公司，更倾向于自己已经能够造血且接近于盈利的公司。不过积极的方面是crypto相关的fintech公司在这个大领域里面算是表现的比较活跃，但主要集中在早期+A轮。

总结来看，赛道上我们还是定的以交易基础设施/机构级质押/CeFi借贷/收益型稳定币/衍生品平台为主要观察方向。在投资方面比较关注那些已经展现出成长潜力和稳定性的公司。