免责声明：本文旨在传递更多市场信息，不构成任何投资建议。文章仅代表作者观点，不代表MarsBit官方立场。

小编：记得关注哦

来源：veDAO研究院

近期Arbitrum因为发行空投，再一次将Layer 2叙事带火，当OP Rollup上，两大赛道optimism和Arbitrum纷纷落地，且带来了巨大的财富效应。另一大L2叙事主力ZK赛道便成为了当前行业目光最为关注的对象之一。事实上，从落地前景上来看，ZK Rollup尽管难度比OP Rollup大很多，但其发展前景也会比OP Rollup更广阔。

毕竟OP Rollup的发展，只针对ERC范畴，未免有种螺丝壳里做道场的局限。但ZK Rollup则能为ERC范畴以外的领域提供助力，甚至零知识证明的实现能够对整个现实社会的信任证明带来帮助，更具有现实意义。

3月24日，Matter Labs CEO Gluchowski在接受The Block采访时表示，zkSync在约一年时间内将实现序列器去中心化（发布Token）。

由于OP和ARB两大基础设施空投的经验，许多人都认为zkSync给行业预留出了一年的“撸空投”窗口期。因此，veDAO研究院汇总了当前行业ZK赛道还未发行Token的12个项目，或许能对2024减半周期以及zk生态爆发下的财富预期提供一些先见。

ZK是终局？

首先，我们需要对zk有一个简单的认知：

零知识证明（英语：zero-knowledge proof）或零知识协议（zero-knowledge protocol）是一方（证明者）向另一方（检验者）证明某命题的方法，特点是过程中除“该命题为真”之事外，不泄露任何资讯。因此，可理解成“零泄密证明”。例如，欲向人证明自己拥有某情报，则直接公开该情报即可，但如此则会将该细节亦一并泄露；零知识证明的精粹在于，如何证明自己拥有该情报而不必透露情报内容。这也是零知识证明的难点。

举个例子：

- 一间屋子，大门和窗户均被加上了密码锁。在大门口，Alice想进入房间但不知道密码；
- Bob看到后告知Alice，他知道大门和窗户的密码，如果Alice需要，可以100美元卖给她；
- Alice对Bob的密码真实性表示怀疑，除非Bob提前告知Alice密码，并经由Alice验证，验证成功后，Alice将向Bob支付100美元；
- Bob担心密码被分享之后，自己的信息不再具有唯一性，将失去价值，因此提了一个建议；
- Alice站在大门以外20米处，由Bob先打开大门，进入房间并把窗户打开；
- Alice只要看到窗户打开，则证明Bob所掌握密码是真实有效的；
- 而Bob也不用担心密码因为提前分享丧失价值。

在整个过程中，Bob的验证行为和Alice的确认行为，均没有造成密码泄露。

这一逻辑，就是零知识证明的根本。零知识证明之所以能够在区块链和加密货币领域得到追捧，是因为人们在数字交易中对隐私和安全性的需求日益增长。随着区块链技术和加密货币的兴起，人们越来越需要一种既能验证交易又不泄露敏感信息的方法，而ZKP可以满足这一需求。

该技术对于提升区块链、加密货币和去中心化金融(DeFi)隐私和安全性的重要性日益提升。许多DeFi项目已经将ZKP应用至借贷和交易等服务中，为用户提供更好的隐私和安全性。许多Layer 1区块链正在添加基于ZKP的汇总或零知识以太坊虚拟机(zkEVM)。随着零知识证明应用的采用率日益提升，其有望在区块链和Web3领域发挥越来越重要的作用。在2022年开发者大会(DevCon)上，超20%的讨论均围绕零知识证明技术展开，表明该技术广受欢迎。

ZK前景：

事实上，随着零知识证明概念的普及，当前已经有越来越多的DeFi类产品开始接受并使用这一新的技术。尤其是zk Rollup，目前也与OP Rollup一起成为了以太坊扩容的首选二层网络解决方案。通过使用Rollup，与一层网络相比，用户可以将燃料费减少多达100倍。

相较于OP Rollup，其优势在于：安全性更高，交易确认的时效性更强，TPS和交易成本显著优于OP Rollup；但是其劣势在于不易兼容EVM。

目前，零知识证明广泛存在于以下的赛道中：

- 身份认证：零知识证明可用于验证用户身份，而不会泄露任何敏感的个人信息。
- 信用记录：用户可以有选择性的向另一方出示自己的信用记录，一方面可以有选择的出示满足对方要求的记录分数，同时证明信用记录的真实性。
- 去中心化存储：服务器可以向用户证明他们的数据被妥善保存，并且不泄露数据的任何具体内容。
- 匿名治理：允许选民投票，可以验证，但投票人的身份不会暴露。
- 交易保密：通过使用ZK技术的加密货币，发送者和接收者地址以及交易金额可对公共区块链屏蔽，提升了用户交易的隐私性。
- 合规性：一些国家在收集和分享金融信息方面设有严格的法规，而去中心化平台可能很难遵守这些法规。零知识证明可用于与监管机构共享所需信息，同时对其他各方保密。

一直以来，ZK赛道就被市场赋予了极高的预期财富回报率。这不仅是因为以太坊二层网络的实现会对行业产生会产生极大助力，更是因为在全球监管日益严厉、且因为金融危机、银行暴雷等种种黑天鹅导致用户对中心化金融世界日益加深的不信任感。基于去中心化网络的一个健全、可靠的身份、信息验证概念便越来越被重视。以至于ZK赛道的重要产品，比如zkSnyc、StarkNet和LayerZero、Arbitrum、Sui Network一起被称之为2023/24年最热门的空投标的。

以下为veDAO研究院特地筛选出来的，具有潜在财富效应，且尚处于“上车”早期的zk Alpha产品。

项目

zkSync

官网：https://zksync.io/

推特：https://twitter.com/zksync

更多信息：https://app.vedao.com/projects/

zkSync是一条2链，使用ZK
rollup技术来解决以太坊当前的可扩展性问题。该链自2019年以来由Matter Labs开发，目前处于Baby alpha阶段，正在进行内部主网测试。

zkSync通过使用ZK SNARK技术的低交易成本（每笔交易几美分）、受益于以太坊安全性的安全性以及去中心化等多种功能脱颖而出。zkSync还提供了互操作性，这要归功于其于2022年2月推出的V2，这使其成为第一个与EVM兼容的ZK-Rollup，这一成就本应花费数年时间。

zkSync专注于5个主要的以太坊相关属性：

- 作为一种通用协议；
- EVM兼容性；
- 以ETH支付的gas费；
- 开源和去中心化。

Aleo

官网：https://www.aleo.org/

推特：https://twitter.com/AleoHQ

更多信息：https://app.vedao.com/projects/

Aleo是第一个支持私有和可编程应用程序的去中心化开源平台。通过默认选择退出隐私，Aleo实现了一个可持续、公平的Web3世界，可以满足开发人员、消费者和企业的需求。

Aleo使用零知识密码学来实现隐私和可编程性。零知识密码学和零知识证明允许第三方验证一条信息的真实性，而无需我们直接透露。Aleo以此作为称为ZEXE（零知识执行）系统的基础。在ZEXE中，用户离线执行状态转换。这个过程产生了一个证明，它被捆绑到一个链上交易中。该交易通过消费/创建链上记录来更新系统的状态。与Zcash一样，该系统为我们提供了强大的隐私保证，因为交易仅包含证明，而不包含生成它的输入。与以太坊一样，ZEXE可以支持智能合约，使用户能够以预定义的方式进行交互或转移价值。

StarkWare

官网：https://starkware.co/

推特：https://twitter.com/StarkWareLtd

更多信息：https://app.vedao.com/projects/

StarkWare通过利用简洁的零知识证明技术，来保护区块链隐私数据，可用于从可验证计算到隐私保护加密货币等各种用途的应用。StarkWare的目的是为区块链带来透明隐私和可扩展性。StarkWare正致力于利用STARK技术改进区块链世界中至关重要的两个因素：可伸缩性和隐私。其作用不仅是促进STARK技术的使用，而且还提供“零知识、简洁、透明、明显、安全”的密码证明。

StarkWare将开发一个完整的验证堆栈：软件和硬件，以支持用于一般计算的计算完整性证明的快速和可靠的生成和验证。其报告中首次实现了一个透明的ZK系统（ZK-STARK），其中验证的规模比数据库规模快得多。

StarkWare正在大力推广以色列理工学院研发的“zk-starks”区块链隐私解决方案。该解决方案通过零知识证明协议来保护区块链隐私数据，在无需耗费大量算力和专门部署安装软件的前提下验证隐私信息，而且还能把数据压缩的更小，提高了效率、透明度和安全性。运用StarkWare技术，可以提高区块链的可扩展性和隐私性。

Aztec Network

官网：https://aztec.network/

推特：https://twitter.com/aztecnetwork

更多信息：https://app.vedao.com/projects/

Aztec Network的定位为基于以太坊上的隐私型ZK Rollup，旨在帮助用户私密、高效地访问以太坊生态的Dapps。该项目当前已推出了两款主要产品，一是基于Aztec Rollup的隐私转账协议zk.money，二是链接以太坊Dapps及Aztec Rollup的隐私桥Aztec Connect。

依靠zk.money和Aztec Connect，用户可以在不暴露自身信息（地址、资金等等）的情况下自由转账，并安全地访问Lido、Element、Aave、Compound、Uniswap等多个主流DeFi协议。

值得注意的是：今年3月13日，Aztec Network宣布将逐步关停其DeFi隐私桥项目Aztec Connect，并将在一周后禁用从zk.money和其他前端（如zkpay.finance）将资金存入Aztec Connect合约。

团队未来将把注意力集中到两款新的主要产品之上：

- 支持零知识证明的通用开发语言 Noir；
- 全新的隐私型区块链。

Scroll

官网：https://scroll.io/

推特：https://twitter.com/Scroll_ZKP

更多信息：https://app.vedao.com/projects/

Scroll致力于创建更通用的零知识证明扩容方案，并大胆宣布把权力下放到社区，让节点、证明人、开发者和用户一起构建Scroll社区。通过与社区一起公开建设并为链上证明和排序创建可靠路径，Scroll致力于确保所有层面均能实现去中心化。

zkLend

官网：https://zklend.com/

推特：https://twitter.com/zkLend

更多信息：https://app.vedao.com/projects/

zkLend是一个货币市场协议将zk-rollup可扩展性、卓越的交易速度和成本节约与以太坊的安全性相结合。 zkLend是一个建立在StarkNet上的L2货币市场协议，它结合了zk-rollup具有以太坊安全性的可扩展性，使参与者能够有效地赚取利息存款和无缝借入资产。Zklend发行的zend token将会由三个大的作用1.优惠借款利率；2.提高借款能力，以及3.治理参与。

目前zkLend已经完成了500万美元种子轮融资，由Delphi Digital领投，其他主要投资者包括StarkWare、Three Arrows Capital、Genesis Block Ventures、Alameda Research、CMS、MetaCartel DAO、DCVC、Amber Group、TPS Capital、Ascensive、D3 Web Capital、 4RC和SkyVision Capital，以及其他天使投资者等。

Mint Square

官网：https://mintsquare.io/starknet

推特：https://twitter.com/MintSquareNFT

更多信息：https://app.vedao.com/projects/

Mint Square是ETH Layer 2 ZK Rollup上的NFT平台。Mint Square 是ETH Layer 2 ZK Rollup 上的 NFT 平台，目的在于建立最好的多链ZK Rollup NFt市场，集成StarkNet和zkSync Era两大平台。

ZKEX

官网：https://zkex.com/

推特：https://twitter.com/ZKEX_Offical

更多信息：https://app.vedao.com/projects/

ZKEX是一个去中心化的L2多链订单簿交换（DEX），建立在三个ZK-rollup之上：zkLink、Starkware和zkSync。 用户将能够以Binance或Coinbase类似的体验去交易来自多个不同链的资产，但ZKEX将是去中心化的、信任最小化和非托管的，交易由零知识证明保护。

Iron Fish

官网：https://ironfish.network/

推特：https://twitter.com/ironfishcrypto

更多信息：https://app.vedao.com/projects/

Iron Fish是一种全新的加密货币，使用zk-SNARKs和Sapling协议，保护每一笔交易。任何人都可以运行一个节点并为其代码库作出贡献。

Iron Fish通过使用零知识证明，可以构建完全隐藏发送者、接收者和金额的私人交易，同时提供交易有效的证明。Iron Fish上的每笔交易都是私密的——除非所有者通过查看密钥授予只读权限，否则任何人都无法看到帐户的详细信息。

YellowSubmarine

官网：https://ys.finance/

推特：https://twitter.com/Yellow_Subm

Yellow Submarine是首个也是唯一一个为所有与EVM兼容的链提供隐私交易的dApp。它创建了一个能够跨越任意以太坊生态系统的隐私层。

通过YS的直观界面，用户可以用MetaMask钱包在任何EVM兼容链存入一枚稳定币，如USDC，并从另一条EVM兼容链上以BUSD或USDT的形式取出，而无需任何公开的可追踪链接。YS的未来版本将允许用户保留他们持有的隐私通证——用户无需透露他们持有的通证类型，并且可随意支配。

Yellow Submarine还为加入其流动性金库的加密资产持有者们提供了一站式解决方案，使其可以从各种EVM兼容链中选定DeFi应用程序来获利。这类似于向DeFi应用程序（如借贷池）提供流动性，并从跨链费用收入中获得额外收益。与使用常规DeFi应用程序相比，通过增加流动性激励以及一对实用型通证（CUN）和治理通证（veCUN），YS的流动性提供者可以从多个来源获得更高的收益。

Nulink

官网：https://www.nulink.org/

推特：https://twitter.com/NuLink_

更多信息：https://app.vedao.com/projects/

Nulink是一个用于分布式应用程序的隐私保护技术平台，允许用户保持匿名（Daaps）。该项目将为开发者、初创企业、小企业和企业带来企业级的安全解决方案，以实现这一目标。作为其技术基础，Nulink技术平台包括区块链、访问控制（代理重加密、基于属性的加密）和安全计算（零知识证明、安全多方计算、全同态加密）技术。它在企业范围内提供数据交换和处理能力。

Nulink正在通过结合一流的技术建立一个坚实的技术基础。应用层、密码器层、存储层、区块链层和观察者网络(Watcher Network)的整合是通过这个矩阵实现的。对于Nulink用户来说，集成到单个API中并访问各种存储和区块链解决方案是非常轻松的。该网络集成了NuCypher进行密钥管理。比特币矿工可以通过提供分散的存储设施来赚取$NLK，并且他们可以通过将信息从ETH传递到观察者层来赚取$NLK。

Starkswap

官网：https://www.starkswap.co/

推特：https://twitter.com/starkswap

更多信息：https://app.vedao.com/projects/

Starkswap是第一个基于公共ZK-Rollup的StarkNet构建的AMM DeFi产品；Starkswap建立在底层基础设施之上，用户将以更便宜的成本（最初是无气体）享受闪电般的快速交易，同时仍然受益于第1层以太坊的安全性。

Starkswap是Starknet上主要AMM的有力竞争者。该团队在3月推出了测试网，并宣布从头开始重建V1，支持自定义曲线。

他们最近还与Yearn 一起推出了Iron Fleet，这是Starknet上的一个新协议，用户在与第一层DeFi协议互动时可以将他们的资产集中起来。这使得Gas可以在用户之间分摊，降低了每个人的操作成本。

总结

单纯从撸空投的角度来看，以前的OP也好、当前的ARB也好，或者即将到来的Aptos、Sui以及明年的zkSync，基础设施一直是“大毛”，是财富效应的重要体现。

而财富效应的传达，往往先从公链、中间件等基础设施开始，然后到达生态的基础应用，比如稳定币、借贷、交易所等，最后传达到非基础应用（社交、游戏）。

目前，在zk赛道爆发前夜，我们有必要对zk赛道的基础设施和基础应用持有充分的注意力。

参考资料：

一文盘点2023年Layer2潜力未发币项目 | ODAILY

链接：https://www.odaily.news/post/5184314

关于veDAO

veDAO是致力于发掘早期潜力项目的投融资社区。通过集结大众智慧和专业意见，为社区参与者、投资人、项目方提供公平、透明、民主的项目评价及投融资流程，让所有参与者共享项目发展红利。

Website: https://app.vedao.com/

Twitter: https://twitter.com/vedao_official

Telegram：t.me/veDAO_zh

Discord：https://discord.gg/NEmEyrWfjV