

区块链

以太坊 Layer2: 区块链应用的钥匙, 元宇宙创新之基石

经过几年的发展, Layer2 (二层网络) 从理论雏形进入到应用落地阶段, 其成熟将为更大规模的区块链应用, 乃至元宇宙落地奠定基础。本文从几种主流方案出发, 以发展潜力最大的 **OptimisticRollups** 和 **Zero-KnowledgeRollups** 等几个典型的二层网络解决方案为案例, 对 Layer2 发展进行深入剖析。

Layer2 旨在解决区块链主网可拓展性问题, 主流的 **ETH Layer2** 方案按技术原理可分为 **Plasma**、**Rollups** 和 **Sidechains**, 它们在实现逻辑、安全性、可拓展性和去中心化程度等方面各有优劣。

基于 OptimisticRollups 的代表: 采用的交互式欺诈证明的 Arbitrum。

以太坊主网 (L1) 好比是管理者全校学生的作业情况的系统, 而为减轻以太坊的直接工作量, Arbitrum 将每个班的作业打包 (即 rollup 块) 后统一录入以太坊主网。而作业具体情况是否有欺诈则采用多轮欺诈证明来解决争议。这就好比设置了几位检查委员, 按照算法去检查包内作业的真实情况, 检查委员要以押上个人学分 (即以以太坊上的 ETH 代币抵押) 来确保公正处理争议。经过一周的争议窗口期后, 最终以太坊才最终确认作业的批改情况。因此, Arbitrum 用户将资产从 L1 转到 L2 则相当于以太坊主网转账一样是实时的, 但是从 L2 撤回资产到 L1 则要经过一周的窗口期时间。Arbitrum 的 DeFi 生态发展进入了良性循环。随着总锁仓价值和用户数量的双增, 越来越多的 DeFi 项目也乐于部署在 ArbitrumOne 主网上; 而项目的增长也有利于进一步吸引资金和用户进入 ArbitrumOne。未来, ArbitrumOne 仍是最值得关注的 Layer2 方向之一。

基于 ZK-Rollups 的代表项目: 可与传统 CEX 交易所匹敌的 dYdX。 基于 Zero-Knowledge Rollups 原理的 Layer2 项目衍生出了两种技术路线, 分别是 ZK-SNARKs 和 ZK-STARKs。它们的代表项目有 zkSync、StarkEX 和 StarkNet。dYdX V3 是架构在 StarkEx 系统之上的去中心化永续合约。自从 2021 年 8 月 3 日公布了其平台治理计划以来, 其交易量增长迅猛, 高峰时单日交易量一度达到了 93 亿美元, 成为全网交易量最大的 DEX (去中心化交易所)。借助于 StarkEx 服务, 使得 dYdX 可以采取订单簿模式交易撮合——这是资本市场最为熟悉的交易撮合模式, 同时确保撮合效率。dYdX 解决了 ETH 网络上合约交易者面临的痛点。在 ETH Layer2 网络上进行合约交易, 既可以媲美在 ETH 主网的安全保障, 又可享受接近中心化交易所的结算速度和低廉的手续费。dYdX 的交易撮合效率与传统中心化交易所 (CEX) 几乎无异。

就目前的技术而言, 无论何种 **Layer2** 路线都无法真正实现与 **ETH 主网** 相同的安全性:

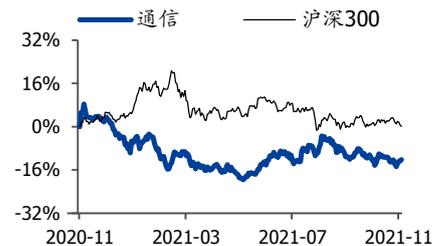
其中, **Sidechains** 的安全性最弱。首先, 在共识实现机制上, Sidechains 的安全性远逊于 ETH 主网。其次, 侧链上的 DeFi 项目可能存在更多智能合约漏洞;

Rollups 的安全隐患包括智能合约漏洞、博弈机制失灵、人为交易排序和密码学漏洞等。在 **ArbitrumOne** 的服务器中存在中心化的交易排序器, 如果运营商利用它抢先打包交易, 即使其他节点率先提交“欺诈证明”, 验证节点的保证金也会落入运营商的手里。

风险提示: 区块链商业模式落地不及预期; 监管政策的不确定性。

增持 (维持)

行业走势



作者

分析师 宋嘉吉

执业证书编号: S0680519010002

邮箱: songjiaji@gszq.com

分析师 任鹤义

执业证书编号: S0680519040002

邮箱: renheyi@gszq.com

相关研究

- 1、《通信: 工信部再发文! 从3点边际变化, 看工业互联网发展提速》2020-02-25
- 2、《区块链: 布隆伯格建言加密货币监管框架, 央行发布《金融分布式账本规范》》2020-02-24
- 3、《区块链: 央行发布《金融分布式账本规范》, 区块链金融有望提速》2020-02-24

内容目录

1 核心观点	3
1.1 本文核心观点和内容	3
2 以太坊 Layer2 是什么?	3
2.1 以太坊 Layer2 是拓展区块链性能的重要方案	3
2.2 以太坊为什么需要 Layer2?	3
2.3 以太坊 Layer2 的技术原理有哪些?	4
3 以太坊 Layer2 各方案的发展状况如何?	6
3.1 Plasma、闪电网络的发展情况	6
3.2 Sidechains (侧链) 遇到了增长瓶颈	7
3.3 Rollups 发展潜力大、爆发迅速	9
4 以太坊 Layer2 的代表项目有哪些?	9
4.1 基于 OptimisticRollups 的代表项目	9
4.2 基于 Zero-KnowledgeRollups 的代表项目	11
4.2.1 基于 Zero-KnowledgeRollups 的 zkSync	11
4.2.2 StarkEX、StarkNet 和 dYdX 的发展情况	12
5 以太坊 Layer2 的潜在风险与发展方向?	14
风险提示	15

图表目录

图表 1: 2020 年底以来 ETH GasPrice 走势	4
图表 2: 各 Layer2 方案的特点	6
图表 3: 闪电网络的节点和支付通道数据	6
图表 4: ChivoWallet 在萨尔瓦多的用户量和交易数据	7
图表 5: ETH、BSC 和 Polygon 上智能合约中锁定的所有资产的总价值 (美元)	8
图表 6: ETH 和 BSC 上智能合约中锁定的所有资产的总价值 (美元)	8
图表 7: BSC 和 Polygon 上智能合约中锁定的所有资产的总价值 (美元)	8
图表 8: Solana 和 Terra 上智能合约中锁定的所有资产的总价值 (美元)	9
图表 9: Arbitrum One 主网的总锁仓价值 (美元) 和用户量增长情况	9
图表 10: Arbitrum One 主网上 DeFi 项目总锁仓价值 (美元) 排行榜	10
图表 11: Arbitrum One 主网上 Sushiswap 的 AMM 资金池	10
图表 12: ZKSync 在 gitcoin 的支付页面	11
图表 13: ZKSync2.0 中 Uniswap 的兑换页面	12
图表 14: StarkEX 的业务实现逻辑	12
图表 15: dYdX 订单簿撮合效率与传统 CEX 几乎无异	13
图表 16: 2021 年下半年以来 dYdX 永续合约的交易量	14
图表 17: StarkNet 的业务实现逻辑	14

1 核心观点

1.1 本文核心观点和内容

市场普遍担心区块链的并发性、可拓展性会成为限制其上应用落地的瓶颈，尤其对于公链生态而言，尚不能支持大规模、高复杂性应用。以以太坊为例，作为全球最大规模的公链生态，一直在讨论如何升级、扩容，而对主网的改动难度较大，Layer2（二层网络）成为可行方案，也是下一阶段其上的元宇宙生态能否繁荣的基础。

经过几年的发展，Layer2（二层网络）从理论雏形进入到应用落地阶段。本报告对几种主流方案出发，以发展潜力最大的 OptimisticRollupsRollups 和 Zero-KnowledgeRollups 等几个典型的以太坊二层网络解决方案为案例，对 Layer2 行业发展进行深入剖析。

Layer2 对 Dapp（去中心化应用）的发展推动效果是明显的。就 DEX（去中心化交易）来说，由于效能较低的主链限制，促进了 AMM（自动化做市）的崛起，但对于交易用户来说（尤其是量化、期货合约用户），订单簿撮合模式显然是最为方便的。Layer2 显然是实现链上订单簿型交易所的最佳方案，这方面典型的案例是 dYdX，其订单簿撮合效率与 CEX（中心化交易所）几乎无异，且用户在链上完成注册，整个交易过程透明可信。

最后，我们对 Layer2 潜在的风险与发展方向做了简单探讨。Layer2 难以达不到主网的安全程度，同时也存在不同于主网的安全风险。同时，其上衍生的各类大规模应用也逐步进入监管的视野。

2 以太坊 Layer2 是什么？

以以太坊网络为例，数以千计的 Dapp（去中心化应用）运行其上，而底层的一致共识区块链网络则出现了较为严重的拥堵现象，为分担底层网络的负担，Layer2（二层网络）想在二层网络上解决各类应用的运行速度和扩展性等问题。本节以以太坊的二层网络为例进行梳理。

2.1 以太坊 Layer2 是拓展区块链性能的重要方案

以太坊（ETH）Layer2 是一类拓展以太坊区块链性能的方案，其基本思路是通过在“主链外”的二层网络上进行计算、交易等业务处理，以获得较快速的响应、高扩展性和低费用，并将最终的状态变更结果反馈到“主链上”，从而减少“主链上”的负担，实现区块链网络的可拓展性。

对于任意一条区块链网络，都存在着安全性、可拓展性和去中心化的“不可能三角”问题。ETH Layer2 则可视为针对这一问题的“中间解”，即在牺牲部分安全性的条件下，保留去中心化性质，极大地增强区块链网络可拓展性的方案。而二层网络上面的数据结果会反馈到主链上获得共识。

2.2 以太坊为什么需要 Layer2？

随着以太坊用户的激增和无数 Dapp 的兴起，以太坊的性能不足问题愈发明显。由于以太坊区块容量和每个区块 Gas 上限的限制，使得其 TPS 仅能达到 15 左右，这就导致了交易确认时间过长、高峰时网络拥堵严重和网络手续费（gas fee）居高不下等问题，进而阻碍了低净值用户的进入、小额高频交易和许多长尾项目的发展。而在 ETH 2.0 遥遥无期的情况下，ETH Layer2 是当下以太坊扩容的最佳方案。

例如，根据 gasnow 网站的统计，在 2021 年上半年，ETH GasPrice 几乎一直保持在 100 以上、个别时段达到了 200 以上、最高峰时甚至接近 400。这些数据意味着在 ETH 网络上进行一笔基础的兑换操作时，需要花费价值约 140 美元的 gasfee，这一数字对于一些小额高频交易者和低净值用户来说是难以负担的。而 ETH Layer2 通过将交易的具体运算放在“链下”完成后再将最终结果传回“链上”，可以大大降低所消耗的 gasfee，从而降低了用户的使用成本。

图表 1: 2020 年底以来 ETH GasPrice 走势



资料来源: gasnow.org, 国盛证券研究所

2.3 以太坊 Layer2 的技术原理有哪些?

主流的 ETH Layer2 方案按技术原理可分为 Plasma、Rollups 和 Sidechains，它们在实现逻辑、安全性、可拓展性和去中心化程度等方面各有优劣。

1. Plasma

Plasma 实际上是以太坊对比特币闪电网络的模仿，它最早由以太坊核心开发者 Vitalik 和比特币闪电网络开发者 Joseph Poon 在他们的论文《Plasma: Scalable Autonomous Smart Contracts》中提出。Plasma 的实现逻辑是，将交易的具体计算和储存转移到子链上，仅将最终的状态变更结果记录在主链上。如果用户对提交上链的结果存在异议，可以在规定的“挑战期”内提供“欺诈证明”，一旦“欺诈证明”被主链节点验证有效，正确的结果将会覆盖错误的，挑战者也可获得原验证节点的部分押金。

理论上来说，Plasma 可以达到无限的拓展空间，但在实践中，其安全性存在较大风险。由于交易的具体内容保存在链下，除个别验证节点外，其他节点无法获得原始的交易数据，倘若所有的验证节点同时怠机，用户在子链上的资金将无法取回。受限于此，Plasma 方案在 ETH Layer2 中的应用不如其他方案。

2. Rollups

Rollups 即汇总交易的意思，是 ETH Layer2 的主要发展方向之一。相较于 Plasma，Rollups 在可拓展性方面略逊一筹，但在安全性方面有了极大地提升。Rollups 的改进之处在于将原始的交易数据也记录在主链上，使得任何节点都可根据交易数据成为新的验证节点。如此一来，用户不再依赖于特定的验证节点，哪怕原始的验证节点怠机，用户也可正常提取资金。

Rollups 可进一步被细分为 OptimisticRollups 和 ZK-Rollups。

OptimisticRollups 即乐观汇总交易，依靠验证节点和挑战者间的博弈保障资金安全。验证节点将交易数据和最终状态变更结果打包上链后，会进入一个“挑战期”，期间资金将被锁定，无法转移。如果其他节点发现验证节点提交的结果和交易记录有出入，即可提交“欺诈证明”，使得正确的状态变更结果将错误的覆盖，并获得原验证节点的押金。在“欺诈证明”被证实前，其他节点默认原验证节点提交的状态变更结果是正确的，所以这类 Rollups 被称为乐观汇总交易。

OptimisticRollups 的优点在于开发门槛较低，可以兼容较复杂的智能合约。例如由 OffChainLabs 团队开发的 ArbitrumOne，已经兼容了许多 ETH 主网上的热门 DeFi 项目，包括 Balancer、Curve、Uniswap 和 Sushiswap 等。

OptimisticRollups 的缺点在于可能发生的安全风险和漫长的“挑战期”。**OptimisticRollups** 的安全性依赖于挑战者和验证节点间的博弈，实际上是由验证节点的押金而非代码担保的。在博弈过程中，有可能会受到“审查攻击”，即验证节点串通矿工不打包挑战者的“欺诈证明”，一旦“挑战期”结束，错误的结果将无法回滚，用户的资金就有被盗的风险。为保障潜在的挑战者有充足的时间监督验证节点，“挑战期”一般被设置为 7-14 天，这一漫长的过程对于追求资本效率的用户来说是无法容忍的。

Zk-Rollups (ZeroKnowledgeRollups)，即零知识汇总交易，依靠密码学原理保障资金安全。**Zk-Rollups** 选取的是“有效证明”的思路，其实现逻辑是，验证节点会将一个“零知识证明”一同打包上链，其他节点只需要运算该证明即可认定验证节点提交的状态变更结果是正确无误的。这样做的好处是，运算“零知识证明”要比直接运算每笔交易简单、快捷得多，而且其正确性是由密码学原理保证的，而非验证节点的押金所担保的。

Zk-Rollups 的优点在于摒弃了 **OptimisticRollups** 中“挑战期”的设定，使得主链与子链间资金转移的速度极快。**Zk-Rollups** 的缺点在于技术不成熟导致的安全隐患和较差的兼容性。在一些零知识证明算法中，如简洁非交互零知识证明，算法中一些与安全相关的随机数是由初始节点选取的，倘若有恶意节点保存了这些随机数，就可以生成虚假的零知识证明，从而盗取子链上的资金。此外，由于生成“零知识证明”要比具体运算每笔交易复杂得多，对于一些复杂的智能合约，尚没有通用的、简单的生成方法，使得 **Zk-Rollups** 暂时还无法兼容大部分 DeFi 项目。目前，**Zk-Rollups** 的 Layer2 网络仅能够实现“转账”、“期货交易”和“铸造 NFT”的操作。

3. Sidechains (侧链)

Sidechains (侧链) 指兼容以太坊虚拟机、与以太坊网络并行运行的独立区块链。侧链不是以太坊网络的子链或直接的二层网络，为了提升交易吞吐量并加快交易确认速度，它们所采用的共识模型一般也与以太坊不同。例如 **BSC (Binance Smart Chain)** 和 **Polygon (Matic)** 网络，它们采用的都是权益证明 (**ProofofStake**) 共识机制，而非工作量证明 (**ProofofWork**)。尽管侧链在可拓展性和效率上有了显著提升，但其安全性和去中心化程度都要弱于以太坊网络。

图表 2: 各 Layer2 方案的特点

	Plasma	OptimisticRollups	Zk-Rollups	Sidechains
实现逻辑	不在主链保存原始交易数据、专门的验证节点和“欺诈证明”	在主链保存原始交易数据、专门的验证节点和“欺诈证明”	在主链保存原始交易数据、专门的验证节点和“有效证明”	与主链相互独立、自行负责安全性和共识实现过程
安全性	低	中	中	低
可拓展性	高	中	中	高
去中心化程度	低	中	中	低

资料来源: 国盛证券研究所整理

3 以太坊 Layer2 各方案的发展状况如何?

3.1 Plasma、闪电网络的发展情况

闪电网络是比特币的二层网络，其原理是在比特币钱包地址间构建点对点的支付通道，再由支付通道共享节点来搭建支付网络。与 Plasma 类似，二层网络中的交易不会被记录在主链上，只有提取资金时才将余额变更结果上传至主链。同样地，提取闪电网络中的资金需要等待一段时间的挑战期，如果期间支付通道的另一方提出异议并提供“欺诈证明”，则可获得另一方的保证金并覆盖错误的余额变更结果。

图表 3: 闪电网络的节点和支付通道数据



资料来源: explorer.acinq.co, 国盛证券研究所

闪电网络的发展状况要比 ETH Plasma 好得多，无论是在用户数量还是应用场景方面。截止至 2021 年 10 月，闪电网络拥有 15566 个节点和 73076 条支付通道。萨尔瓦多在正式支持比特币作为该国的法定货币后，也推荐其国民使用闪电网络进行日常支付或转账。根据闪电网络钱包服务商 ChivoWallet 显示的数据，累计有超过 220 万的萨尔瓦多公民使用过闪电网络钱包，而这一数字已经超过了萨尔瓦多任何一家银行的用户量。除此之外，著名社交平台推特也在 2021 年 9 月 23 日宣布支持用户通过闪电网络向博主支付比特币小费。这一举动无疑也可为闪电网络带来更多的用户和交易。

图表 4: ChivoWallet 在萨尔瓦多的用户量和交易数据



资料来源: explorer.acinq.co, 国盛证券研究所

Plasma 可以视作以太坊开发者对比特币闪电网络的借鉴,但这一模式并不适合以太坊网络,所以其发展几乎停滞。以太坊网络与比特币网络并不完全相同,以太坊是一个虚拟机,其地址的账户状态可被任意节点调用,Plasma 中的每笔交易都会影响整个二层网络的账户状态。在闪电网络中,用户仅需要盯住与自己共同构建支付通道的节点没有提交虚假的余额变更结果即可保证安全;在 Plasma 中,用户需要关注整个二层网络的交易和状态变更,而监控如此庞大的数据量对于普通用户来说是难以实现的。

3.2 Sidechains (侧链) 遇到了增长瓶颈

Sidechains 由于开发的便利性优势,最先承接了 ETH 的溢出价值。ETH 网络的拥挤和 Rollups 方案缓慢的研发进度为侧链的爆发创造了条件。2020 年 6 月,随着 Compound 开启“流动性挖矿”和“借贷挖矿”,所谓的“DeFi 之夏”掀起了序幕,越来越多的项目、用户和资金涌向了 ETH;与此同时,ETH 主网交易确认速度慢、gas fee 过高和交易吞吐量不足的缺点愈发暴露明显。侧链的开发者们果断地抓住了这次机会,推出了兼容以太坊虚拟机的区块链网络,移植了以太坊上热门 Dapp 的智能合约,配合各种营销策略,迅速吸引到了许多 ETH 溢出的用户、资金和项目。

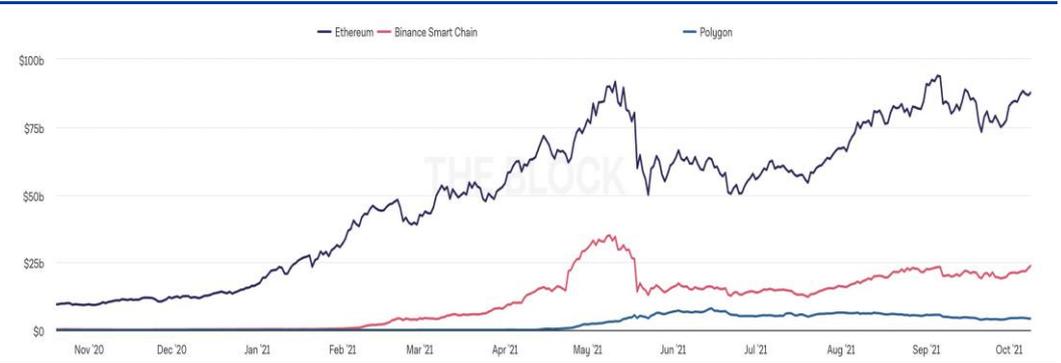
最具代表性的侧链包括 BSC (BinanceSmartChain) 和 Polygon (Matic) 网络。

BSC 是由币安交易所资助开发,采用了权益证明共识机制的智能区块链,也是最早上线的 ETH 侧链之一。相较于 ETH, BSC 以牺牲去中心化程度为代价,换取了更快的交易确认速度、更大的交易吞吐量和更低的 gas fee;同时,有着全世界现货交易量最大的中心化交易所币安的隐性背书, BSC 在获得用户流量的同时也打消了用户的安全顾虑。于是乎,自 2021 年 2 月以来, BSC 上的用户量、总锁仓价值和项目量都实现了快速增长,一跃成为总锁仓价值仅次于 ETH 的智能区块链,并远远甩开了其他 ETH 侧链竞争者。

Polygon 是一种生态系统,可用于创建与以太坊兼容的区块链网络和拓展解决方案,其主网正式上线于 2021 年 5 月。相较于 BSC, Polygon 主网的交易确认速度和手续费低廉

程度有过之而无不及，也吸引到了不少的用户和项目，其总锁仓价值在所有 ETH 侧链中仅次于 BSC。

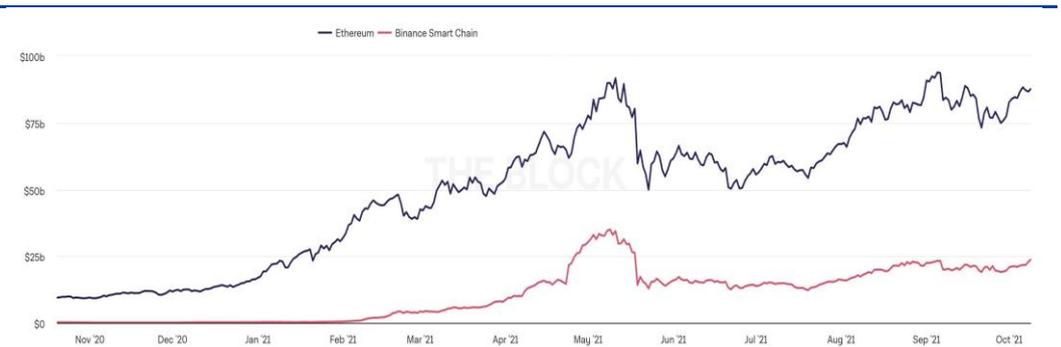
图表 5: ETH、BSC 和 Polygon 上智能合约中锁定的所有资产的总价值 (美元)



资料来源: theblockcrypto.com, 国盛证券研究所

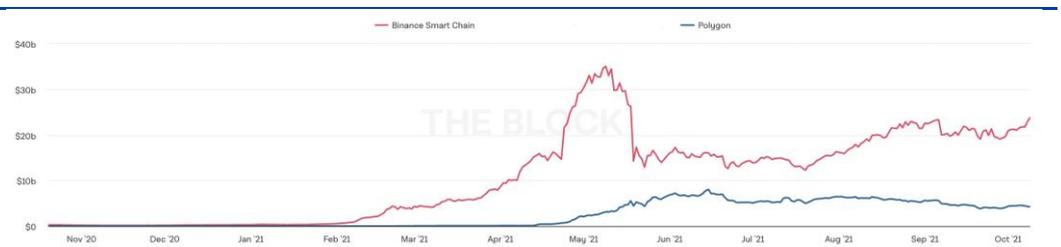
Sidechains 的价值捕获能力目前已遇到了增长瓶颈。以 BSC 为例，将其总锁仓价值走势与 ETH 对比可以发现，在“5.19”去杠杆之前，BSC 跟随 ETH 一路上涨，甚至在一些时段增速更快；而在“5.19”之后，当 ETH 总锁仓价值突破前高时，BSC 却几乎停滞，并没有表现出曾经的强势。而 Polygon 尽管其总锁仓价值在“5.19”之后不但没有回落还实现了增长，但由于其绝对体量较小，即使将它与 BSC 相加，所有以太坊侧链的总锁仓价值距离历史高点仍有不小距离。

图表 6: ETH 和 BSC 上智能合约中锁定的所有资产的总价值 (美元)



资料来源: theblockcrypto.com, 国盛证券研究所

图表 7: BSC 和 Polygon 上智能合约中锁定的所有资产的总价值 (美元)

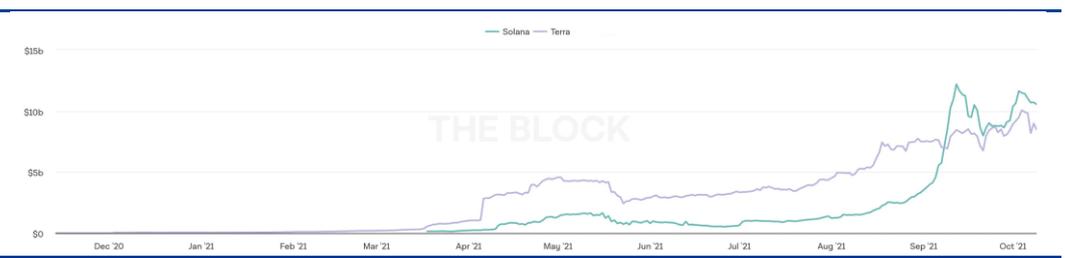


资料来源: theblockcrypto.com, 国盛证券研究所

侧链遇上增长瓶颈的原因包括：短时间涌现出其他性能更强、费用更低的非以太坊侧链区块链网络分流；更为值得关注的是，在去中心化、安全和技术方面更先进的 RollupsLayer2 网络分流。首先，不同于工作量证明共识机制，权益证明共识机制不具备算力这一客观参考指标来衡量其网络的抗冲击能力，哪怕一些侧链有着中心化机构的背书，它们能够凝聚的共识和承载的价值都是有限的。其次，非以太坊侧链区块链网络的异军突起也分流了不少侧链的用户。例如，Solana 和 Terra 的总锁仓价值在 9 月份和 10 月份都曾突破 100 亿美元。最后，被部分用户誉为“Real Layer2”的 RollupsLayer2 网

络陆续上线，使得侧链的发展空间进一步被压缩。

图表 8: Solana 和 Terra 上智能合约中锁定的所有资产的总价值 (美元)



资料来源: theblockcrypto.com, 国盛证券研究所

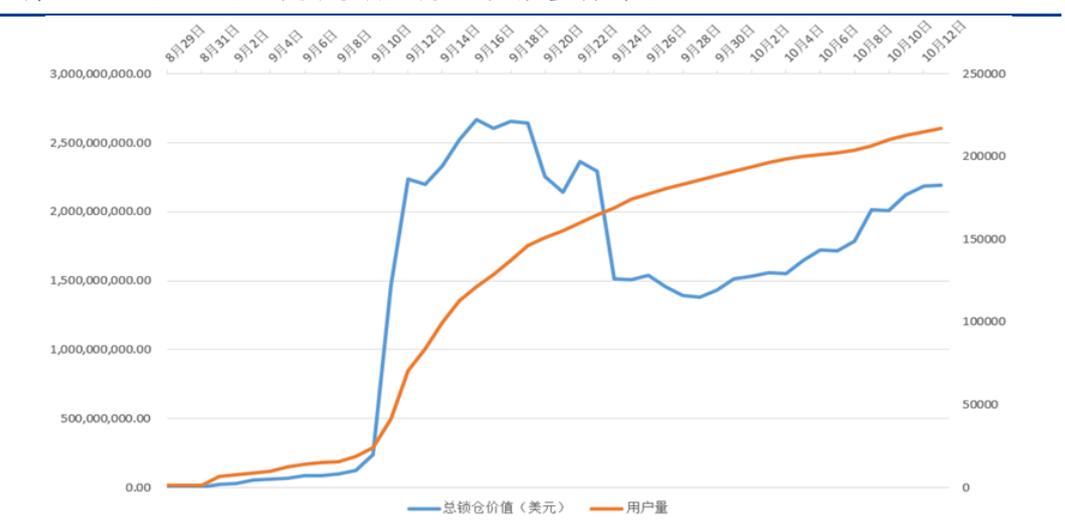
3.3 Rollups 发展潜力大、爆发迅速

Rollups 或将超越 Sidechains, 成为被普遍接受的 Layer2 方案。相对于 Sidechains, Rollups 是更安全、更去中心化的解决方案。过去一段时间, 受限 Rollups 方案在技术上尚未成熟, ETH 生态的溢出价值被 Sidechains 所捕获; 最近, 随着基于 Rollups 原理的 Layer2 主网正式上线, 用户、资金和项目已展现回流趋势。

例如, 自从基于 Optimistic Rollups 技术的 ETH Layer2 主网 ArbitrumOne 在 2021 年 9 月 1 日正式上线以来, 其用户数量和总锁仓价值都实现了飞速增长。不仅如此, ETH 主网上的许多头部项目也已在 ArbitrumOne 上线, 例如 1INCH、Uniswap、Sushiswap、Curve 和 Balancer 等, 使得其生态日趋完整。

总体而言, ArbitrumOne 的总锁仓价值和用户量保持了增长的趋势。在 9 月 12 日, 两项数据都实现了暴涨, 随后几天尽管总锁仓价值突破在 25 亿美元后又回落到 15 亿美元, 但后续仍保持了稳步增长的势头, 逐步稳定在 20 亿美元以上; 用户量的增速虽然有所下降, 但整体趋势仍是向上的, 并且突破了 20 万大关。

图表 9: Arbitrum One 主网的总锁仓价值 (美元) 和用户量增长情况



资料来源: arbiscan.io, 国盛证券研究所

4 以太坊 Layer2 的代表项目有哪些?

4.1 基于 OptimisticRollups 的代表项目

Arbitrum 是一款由 OffChainLabs 团队开发的、基于 OptimisticRollup 技术的 ETHLayer2 项目，也是所有 RollupsLayer2 项目中发展最好的，其用户量、项目数量和总锁仓价值均是第一。根据 DeFiLlama 的统计数据，Arbitrum 上总锁仓价值排名前十的项目中，Sushiswap、Anyswap、Curve 和 Abracadabra 的锁仓量均达到了 3 亿美元。

图表 10: Arbitrum One 主网上 DeFi 项目总锁仓价值 (美元) 排行榜

Name	Chain	1d Change	7d Change	TVL ↓	Mcap/TVL
1 SushiSwap	Arbitrum	+0.24%	-	\$387.89m	-
2 AnySwap (AN...	Arbitrum	+0.68%	-7.65%	\$342.43m	-
3 Curve (CRV)	Arbitrum	+0.88%	+8.69%	\$329.26m	-
4 Abracadabra (SP...	Arbitrum	+1.51%	+19.21%	\$300.17m	-
5 Synapse (SYN)	Arbitrum	-8.28%	-	\$260.04m	-
6 Balancer (BAL)	Arbitrum	-2.45%	+3.93%	\$107.04m	-
7 dForce (DF)	Arbitrum	-2.53%	-1.43%	\$72,038,270	-
8 DODO (DODO)	Arbitrum	+0.16%	+12.06%	\$55,697,311	-
9 Beefy Finance (...)	Arbitrum	+2.39%	+17.97%	\$52,558,773	-
10 Uniswap v3 (UNI)	Arbitrum	+2.34%	+8.86%	\$52,415,377	-

资料来源: defillama.com, 国盛证券研究所

以总锁仓价值最高的 Sushiswap 为例，WETH/MIM（以太坊与稳定币）交易对资金池的深度已达 2.2 亿美元，基本可以将单笔百万美元级别的交易滑点控制在 1% 内。

图表 11: Arbitrum One 主网上 Sushiswap 的 AMM 资金池

Pool	TVL	Rewards	APR
SPELL/WETH SushiSwap Farm	\$64,234,619	15.00 SUSHI / DAY 17,374,321 SPELL / DAY	195% annualized
WETH/MIM SushiSwap Farm	\$224,484,329	15.00 SUSHI / DAY 24,157,440 SPELL / DAY	77.10% annualized
USDC/WETH Kashi Farm	\$116,717	12.00 SUSHI / DAY	41.42% annualized
USDT/WBTC Kashi Farm	\$120,679	12.00 SUSHI / DAY	40.06% annualized
USDC/LINK Kashi Farm	\$147,327	12.00 SUSHI / DAY	32.82% annualized

资料来源: defillama.com, 国盛证券研究所

Arbitrum 在技术上更具优势，它采用的交互式欺诈证明是更高效、灵活的，可以最小化链上仲裁节点的工作量。交互式欺诈证明的方法基于对争议的剖析，假如验证节点一共担保了 N 个步骤的交易，挑战者将与验证节点在链下进行多轮交互，直至将双方存在争议的部分缩至最小范围，再提交给链上仲裁节点解决。

可以这样理解 Arbitrum 运行机制：以学校作业管理系统为比喻（每份作业就好比链上的交易任务），以太坊主网（L1）管理者全校学生的作业情况，而为减轻以太坊的直接工作量，学校每个班设置一个课代表负责收取并批改每份作业，打包（即 rollup 块）后统一录入以太坊主网。而作业具体情况是否有欺诈则采用多轮欺诈证明来解决争议。这就好比设置了几位检查委员，按照算法去检查每个包内作业的真实情况，检查委员要以押上

个人学分（即以太坊上的 ETH 代币抵押）来确保公正。经过一周的争议窗口期后，最终以太坊才最终确认作业的批改情况。

因此，Arbitrum 用户将资产从 L1 转到 L2 则相当于以太坊主网转账一样是实时的，但是从 L2 撤回资产到 L1 则要经过一周的窗口期时间。

Arbitrum 的生态发展进入了良性循环。随着总锁仓价值和用户数量的双增，越来越多的项目也乐于部署在 ArbitrumOne 主网上；而项目的增长也有利于进一步吸引资金和用户进入 ArbitrumOne。未来，ArbitrumOne 仍是值得关注的 Layer2 项目之一。

4.2 基于 Zero-KnowledgeRollups 的代表项目

基于 Zero-Knowledge Rollups 原理的 Layer2 项目衍生出了两种技术路线，分别是 ZK-SNARKs (Zero-Knowledge SuccinctNon-interactive Arguments of Knowledge; 简洁非交互零知识证明)和 ZK-STARKs (Zero-Knowledge Scalable Transparent Arguments of Knowledge; 简洁全透明零知识证明)。它们的代表项目有 zkSync、StarkEX 和 StarkNet。

ZK-STARKs 被认为是 ZK-SNARKs 的改进版本，旨在解决 ZK-SNARKs 的许多缺点。首先，在 ZK-SNARKs 中，一些与安全相关的随机数是需要初始节点选取的，如果有恶意节点保存了这些初始数据，它就可以利用初始数据生成虚假的证明，从而偷走用户在 Layer2 的资金；但在 ZK-STARKs 中，并不需要设置初始化可信值，而通过哈希函数碰撞进行更精密的对称加密方式。此外，在 ZK-SNARKs 中，所需的计算越多，验证者和证明者之间的通信量也就越大；但在 ZK-STARKs 中，验证者和证明者之间的通信量相对于计算的任何增量都是保持不变的，所以 ZK-STARKs 的整体数据量远小于 ZK-SNARKs。

4.2.1 基于 Zero-KnowledgeRollups 的 zkSync

zkSync 是由 MatterLabs 团队开发的一个基于 Zero-KnowledgeRollups 原理的 ETH Layer2 网络，它采用的有效证明方式是 ZK-SNARKs。

zkSync 网络中最主要的产品是 zkWallet，它是用户在 Layer2 网络中的钱包，目前只兼容“转账”这一特定的交易行为。zkWallet 的优点是在同时进行多笔转账时，仅需要支付一次 gasfee，帮助用户节省转账成本。例如，用户在 Gitcoin Grants 为众筹项目批量捐款时，可以至多一次性完成 50 笔转账操作。根据官方公布的数据，zkWallet 累计完成了近 400 万笔交易，包括第 8-11 轮 Gitcoin Grants 中 98% 的交易。

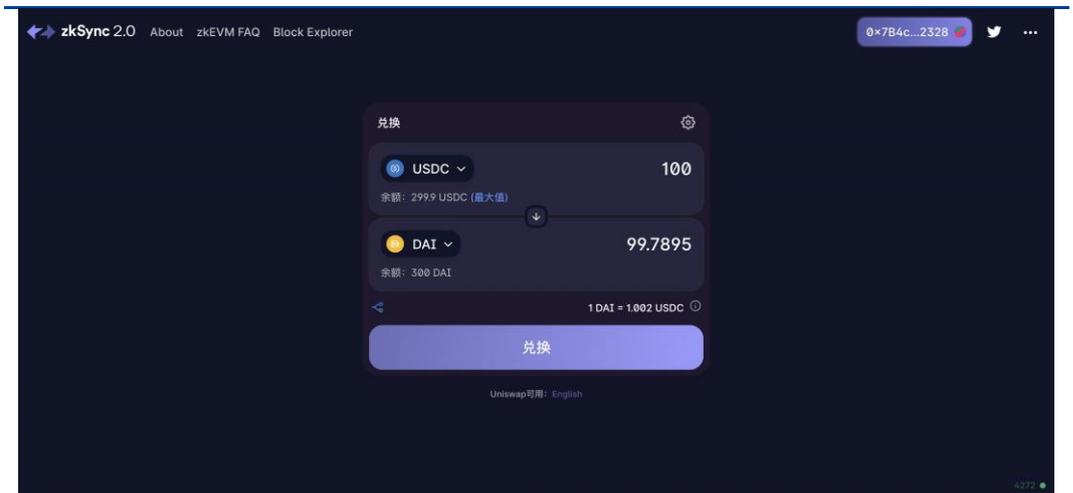
图表 12: zkSync 在 gitcoin 的支付页面



资料来源: gitcoin.co, 国盛证券研究所

除了 zkWallet 之外，MatterLabs 也在积极开发 zkEVM，它是一种以兼容零知识证明计算的方式执行智能合约的虚拟机。目前已在测试网上线了支持 Uniswap 的 zkSync2.0，这也是 ZK-Rollups Layer2 网络首次兼容主网上的项目。

图表 13: ZkSync2.0 中 Uniswap 的兑换页面



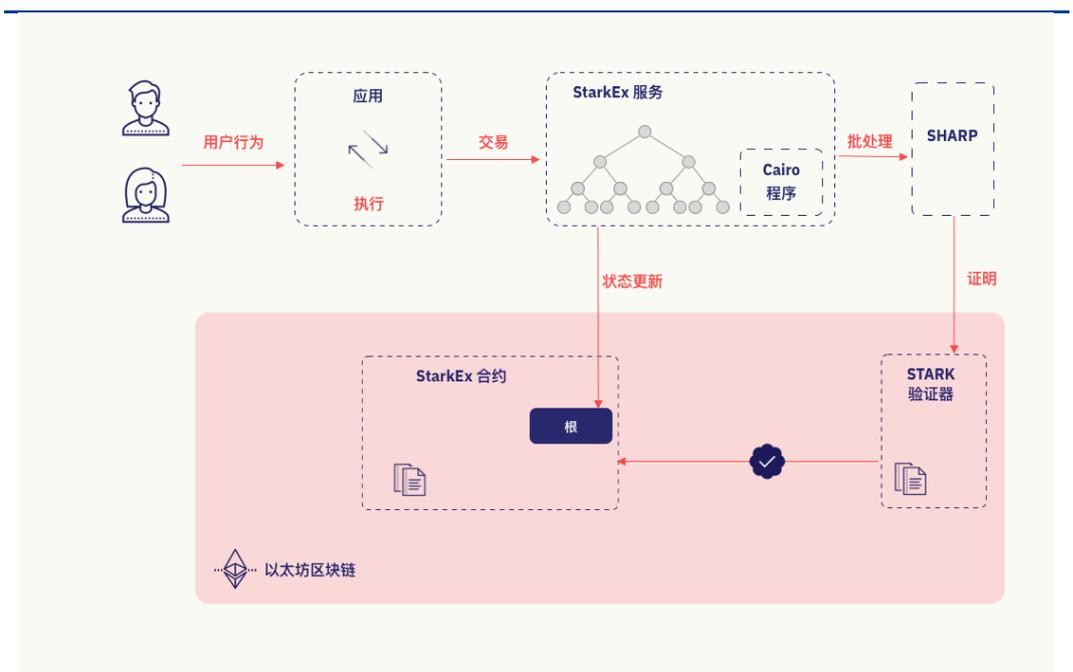
资料来源: gitcoin.co, 国盛证券研究所

4.2.2 StarkEX、StarkNet 和 dYdX 的发展情况

StarkEX 和 StarkNet 都是由 StarkWare 公司开发的产品，前者是 ETH Layer2 可拓展引擎，后者是 ETH Layer2 网络，它们采用的有效证明方式都是 ZK-STARKs。

StarkEx 是一个较为成熟的平台，自 2020 年 6 月起已部署在 ETH 主网上，截止到 2021 年 10 月 5 日，累计完成了 2700 万笔交易和 800 亿美元的交易额。作为 ETH Layer2 可拓展引擎，它允许 DeFi 项目将它们的应用程序部署、运行在 StarkEx 服务上，并为它们的交易结果生成零知识证明，最终将原始交易数据、状态变更结果和相应的证明记录在 ETH 主网上。

图表 14: StarkEX 的业务实现逻辑



资料来源: starkware.co, 国盛证券研究所

StarkEx 系统具有链上组件和链下组件。链下组件负责记录各账户的实时状态，执行系统中的交易并生成相应的零知识证明，再将交易后的状态变更结果和相应的证明发送到链上组件。链上组件负责保管系统内的资产，验证链下组件上传的证明的有效性，并将状态变更结果记录在 ETH 主网上。

在使用 StarkEx 服务的项目中，dYdXV3 是交易量最大、用户数量最多的，也是运行在 ETH Layer2 上的项目的典型代表。

dYdXV3 是架构在 StarkEx 系统之上的去中心化永续合约交易所。自从 2021 年 8 月 3 日公布了其平台治理代币的分发计划以来，其交易量增长迅猛，高峰时单日交易量一度达到了 93 亿美元，成为全网交易量最大的 DEX（去中心化交易所）。

借助于 StarkEx 服务，使得 dYdX 可以采取订单簿模式进行交易撮合——这是资本市场最为熟悉的交易磋商模式，同时确保撮合效率。dYdXV3 解决了 ETH 网络上合约交易者面临的痛点。在 ETH Layer2 网络上进行合约交易，既可以得到媲美在 ETH 主网上交易的安全保障，又可以享受到接近中心化交易所的结算速度和低廉的手续费。用户存入 dYdX 的资金实际上都被锁定在 dYdX 部署在 ETH 主网的智能合约中，并且随时都可以提取；而交易的结算则发生在 Layer2 网络上，用户只需要在存入和取出资金时支付 gasfee，并不需要为每笔交易都支付，也就大大节省了交易成本。从体验上来看，dYdX 的交易撮合效率与传统中心化交易所（CEX）几乎无异。

图表 15: dYdX 订单簿撮合效率与传统 CEX 几乎无异



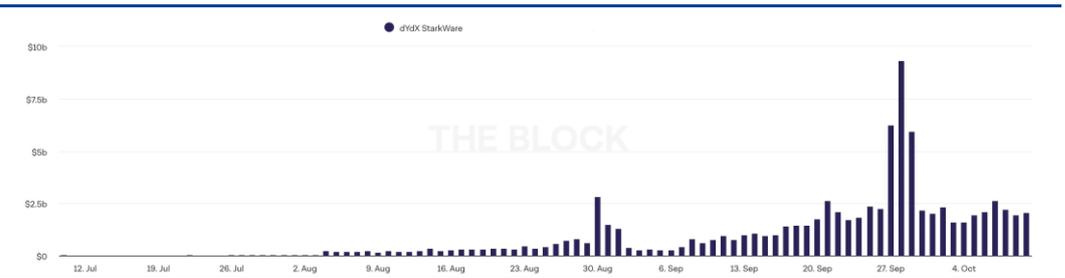
资料来源: dYdX 官网, 国盛证券研究所

对于 ETH 网络的用户，使用 dYdXV3 的学习成本并不高，可以快速上手，使用者利用钱包签名即可注册。与在 ETH 主网上进行交易时需要私钥持有者签名确认类似，用户在 Layer2 网络上的交易也需要由“starkKey”签名确认。所以，初次使用时，用户首先通过以太坊地址连接到 dYdX 的智能合约，智能合约会将用户的以太坊地址与特定的“starkKey”绑定，在此之后用户才可将资金转入 dYdX 部署在 ETH 主网的智能合约中。等到 Layer2 网络中的应用程序接受存款后，用户即可使用其资金进行交易。

不同于 CEX 的交易逻辑，dYdX 引入“交易即挖矿”的逻辑，用户只需要在 dYdX 上进行合约交易即可获得奖励。其具体模式是，以 28 天为一个周期，按照用户的交易积分占比，将 3835616 个 DYDX 代币作为奖励分配。交易积分的计算公式实际上是一个柯布一道格拉斯生产函数，交易手续费的权重为 70%，平均持仓量的权重为 30%。例如，某用户在某期分发中贡献了 1000 美元的交易手续费，其平均持仓量为 100000 美元，那么他的交易积分 = $1000^{0.7} * 100000^{0.3} = 125.89 * 31.62 = 3980.64$ 。假如，本期所有产生的交易积分为 1000000，那么他可以分配到 DYDX 的数量 = $3835616 * (3980.64 / 1000000) = 15268.21$ 个。在这样的分配模式下，只要用户能够分配到的 DYDX 的市值高于所花费的手续费，他就有动力继续刷高自己的交易积分，进而推动了 dYdX 平台交易额和未平

持仓量的上涨。

图表 16: 2021 年下半年以来 dYdX 永续合约的交易量

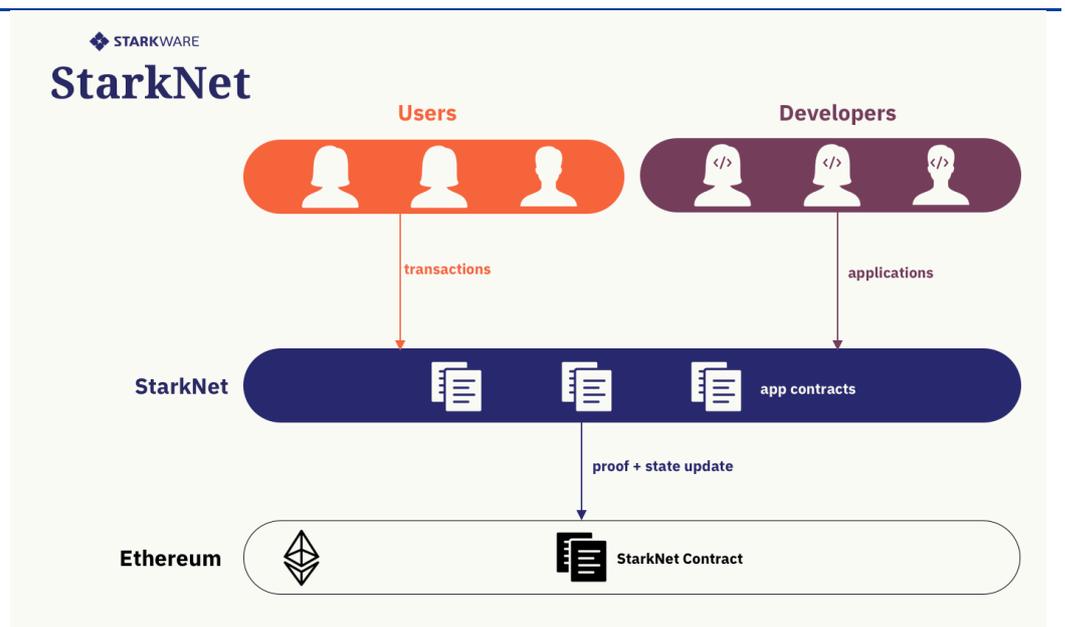


资料来源: theblockcrypto.com, 国盛证券研究所

StarkNet 是一个较新的项目，但代表了 StarkWare 公司未来的开发方向。StarkNet 已在测试网上发布了 3 个版本，并计划在 2021 年 11 月正式上线部署于 ETH 主网的 StarkNetAlpha。根据官方的公开文档，StarkNetAlpha 将支持 EVM 架构的智能合约，从而实现 Layer2 与主网的可交互性，拓展 Zk-RollupsLayer2 网络的兼容性。

StarkNetAlpha 的业务实现逻辑与 StarEx 类似，但可以实现更好的兼容性。开发者可以将部署在 ETH 主网的智能合约移植到 StarkNetAlpha 上，用户则可按相同的操作逻辑进行合约交互；最终，所有的交易数据、状态变更结果和相应的零知识证明都会被 StarkNetAlpha 的节点上传至主网。

图表 17: StarkNet 的业务实现逻辑



资料来源: starkware.co, 国盛证券研究所

5 以太坊 Layer2 的潜在风险与发展方向?

就目前的技术而言，无论何种 Layer2 方案都无法真正实现与 ETH 主网相同的安全性。

其中，**Sidechains 的安全性最弱**。首先，在共识实现机制上，Sidechains 的安全性远逊于 ETH 主网。区块链网络的核心要义是去中心化和不可篡改，而侧链恰恰是在这方面做出了牺牲，导致攻击者篡改侧链账本的成本显著低于篡改以太坊账本。其次，侧链上的

DeFi 项目可能存在更多智能合约漏洞。由于 ETH 主网上的智能合约多是开源的,于是乎,有许多代码开发能力不强的仿盘团队将其简单改动后移植至侧链上。哪怕这些仿盘项目最初可以获得第三方审计公司出具的审计报告,但在后续的迭代版本中,出现新的智能合约漏洞的情况也十分常见。

Rollups 的安全隐患包括智能合约漏洞、博弈机制失灵、人为交易排序和密码学漏洞等。首先,无论是 OptimismRollups 还是 ZK-Rollups,都是利用智能合约将用户存入 Layer2 网络的资金锁定在主网上,如果智能合约本身存在漏洞或被恶意篡改,用户的资金就有可能被盗。此外,OptimismRollups 的博弈机制未必有效,潜在的挑战者未必能够审查验证节点发布的所有状态变更结果,一旦挑战期结束,即使状态变更结果与交易记录不符,错误的结果也无法回滚,Layer2 中的资金就有可能被盗。再者,OptimismRollups 的交易排序是可被人为控制的。例如 ArbitrumOne 的服务器中有一个中心化的交易排序器,如果运营商利用它抢先打包交易,即使其他节点率先提交“欺诈证明”,验证节点的保证金也会落入运营商的手里。最后,**ZK-Rollups 依靠的密码学原理也有可能存在漏洞。ZK-STARKs 发展时间较短,属于较新的和实验性的密码学原理,需要更长时间来证明其安全性;ZK-SNARKs 中的“有毒废料”更是一直被诟病的漏洞。**

在“区块链网络不可能三角”的框架下,首先应当保证的是安全性,其次是去中心化程度,最后才是可拓展性,对于 ETH Layer2 也不例外。综合比较各 Layer2 方案,从长远角度来说,采用 ZK-STARKs 的 Zk-Rollups 是最为均衡的。首先,从安全性角度考量,Rollups 优于 Sidechains, Zk-Rollups 优于 Optimism Rollups, ZK-STARKs 优于 ZK-SNARKs。其次,从去中心化程度角度考量,ZK-Rollups 依靠的密码学原理是客观事实,经得起反复验证,不需要通过博弈机制保障其有效性,也消除了中心化的交易排序问题。最后,从可拓展性角度考量,虽然目前 Zk-Rollups 的兼容性不如 Optimism Rollups,但随着技术的成熟,Zk-Rollups 的 Layer2 网络陆续上线,实现对 ETH 主网上 DeFi 项目的兼容,届时 Layer2 网络的高交易吞吐量将使可拓展性得到极大提升。

风险提示

区块链商业模式落地不及预期: 基于区块链的稳定币是创新金融产品,相关项目处于发展初期,存在商业模式落地不及预期的风险。

监管政策的不确定性: 加密货币和稳定币在实际运行过程中涉及到多项金融监管政策,目前各国监管政策还处于研究和探索阶段,并没有一个成熟的监管模式,所以行业面临监管政策不确定性的风险。前期中国已颁布限制虚拟币交易相关政策,中心化交易所已尽数退出中国市场,未来仍有监管进一步收紧的可能性;同时,虽然美国已通过比特币期货 ETF、Coinbase 也登陆了纳斯达克,但原有监管体系也是基于银行账户系统,当前 DeFi (去中心化金融)的发展突飞猛进,或将突破原有监管框架,9 月份《经济学人》杂志封面文章也表达了对 DeFi 优劣势的描述——虽然高效但监管治理不完善。

免责声明

国盛证券有限责任公司（以下简称“本公司”）具有中国证监会许可的证券投资咨询业务资格。本报告仅供本公司的客户使用。本公司不会因接收人收到本报告而视其为客户。在任何情况下，本公司不对任何人因使用本报告中的任何内容所引致的任何损失负任何责任。

本报告的信息均来源于本公司认为可信的公开资料，但本公司及其研究人员对该等信息的准确性及完整性不作任何保证。本报告中的资料、意见及预测仅反映本公司于发布本报告当日的判断，可能会随时调整。在不同时期，本公司可发出与本报告所载资料、意见及推测不一致的报告。本公司不保证本报告所含信息及资料保持在最新状态，对本报告所含信息可在不发出通知的情形下做出修改，投资者应当自行关注相应的更新或修改。

本公司力求报告内容客观、公正，但本报告所载的资料、工具、意见、信息及推测只提供给客户作参考之用，不构成任何投资、法律、会计或税务的最终操作建议，本公司不就报告中的内容对最终操作建议做出任何担保。本报告中所指的投资及服务可能不适合个别客户，不构成客户私人咨询建议。投资者应当充分考虑自身特定状况，并完整理解和使用本报告内容，不应视本报告为做出投资决策的唯一因素。

投资者应注意，在法律许可的情况下，本公司及其本公司的关联机构可能会持有本报告中涉及的公司所发行的证券并进行交易，也可能为这些公司正在提供或争取提供投资银行、财务顾问和金融产品等各种金融服务。

本报告版权归“国盛证券有限责任公司”所有。未经事先本公司书面授权，任何机构或个人不得对本报告进行任何形式的发布、复制。任何机构或个人如引用、刊发本报告，需注明出处为“国盛证券研究所”，且不得对本报告进行有悖原意的删节或修改。

分析师声明

本报告署名分析师在此声明：我们具有中国证券业协会授予的证券投资咨询执业资格或相当的专业胜任能力，本报告所表述的任何观点均精准地反映了我们对标的证券和发行人的个人看法，结论不受任何第三方的授意或影响。我们所得报酬的任何部分无论是在过去、现在及将来均不会与本报告中的具体投资建议或观点有直接或间接联系。

投资评级说明

投资建议的评级标准		评级	说明
评级标准为报告发布日后的6个月内公司股价（或行业指数）相对同期基准指数的相对市场表现。其中A股市场以沪深300指数为基准；新三板市场以三板成指（针对协议转让标的）或三板做市指数（针对做市转让标的）为基准；香港市场以摩根士丹利中国指数为基准，美股市场以标普500指数或纳斯达克综合指数为基准。	股票评级	买入	相对同期基准指数涨幅在15%以上
		增持	相对同期基准指数涨幅在5%~15%之间
		持有	相对同期基准指数涨幅在-5%~+5%之间
		减持	相对同期基准指数跌幅在5%以上
	行业评级	增持	相对同期基准指数涨幅在10%以上
		中性	相对同期基准指数涨幅在-10%~+10%之间
		减持	相对同期基准指数跌幅在10%以上

国盛证券研究所

北京

地址：北京市西城区平安里西大街26号楼3层
 邮编：100032
 传真：010-57671718
 邮箱：gsresearch@gszq.com

南昌

地址：南昌市红谷滩新区凤凰中大道1115号北京银行大厦
 邮编：330038
 传真：0791-86281485
 邮箱：gsresearch@gszq.com

上海

地址：上海市浦明路868号保利One56 1号楼10层
 邮编：200120
 电话：021-38124100
 邮箱：gsresearch@gszq.com

深圳

地址：深圳市福田区福华三路100号鼎和大厦24楼
 邮编：518033
 邮箱：gsresearch@gszq.com