StarkNet 技术风险、经济模型与评论

作者：
郑金城 新跃社科大学研究员，全球金融科技学院、Biteye 建设者，Ocean Views 专栏作家
李国权 新跃社科大学教授，新加坡经济协会副会长，全球金融科技学院主席

Arbitrum 空投的财富效应点燃了市场对L2的信心，纷纷布局还未发币的L2。而80亿美元高估值的StarkWare自然是备受瞩目。那么StarkWare是有什么独特的技术值得各大机构热捧？旗下的StarkNet想要解决问题？我们将在本文中一一道来。

1.STARKs, StarkEx, StarkNet

1.1 STARKs

STARKs（Scalable, Transparent ARgument of Knowledge）是一种可以证明和验证计算的证明系统，旨在提高以太坊的扩展性。它允许将大型计算从链上转移到链下以降低成本，为计算的正确性生成证明，然后在链上进行少量的计算来验证证明。即验证者通过在链上执行非常少的操作来判断链下完成的计算的完整性。

L2 通过STARKs技术将多笔交易打包在一起进行数以千计的计算，然后使用单个STARK证明在链上验证它们的有效性。该批次内的所有交易共同分担链上处理的成本，从而在继承以太坊安全性的前提下降低了Gas成本，改善用户体验。这模式与共享的士的用户平摊路费相似。

SNARKs （Succinct，Non-Interactive，Argument，Knowledge）是一个简洁的非交互式的证明。STARKs 和 SNARKs 都是ZK Rollups 的解决方案。

SNARKs 和 STARKs 对比

	SNARKs	**STARKs**
可信设置要求	需要可信设置	利用公开可验证随机来建立可信任、可验证的计算系统
扩展性	较少的扩展性	更多的扩展性
抗量子	使用公私钥对，不抗量子攻击	抗量子攻击
证明大小	相对更小	相对更大，但具有对数扩展性
验证时间	迅速	相对更长，但具有对数扩展性
验证成本	大多数情况下成本更低（证明大	大多数情况下成本更大

	数据集的情况下除外）	
开发工具	相对成熟	相对原始
核心算法代码	相对成熟	代码质量有待提高
应用	Zcash、Loopering、zkSync、Scroll、Aztec	StarkEx, StarkNet

来源：SUSS NiFT, ChatGPT

相比 SNARKs, STARKs具有以下三个优势：

去信任

STARKs 公开可验证随机来取代SNARKs的可信设置，减少对参与人的依赖，提高协议安全性。

更强的扩展能力

STARK 具有验证的对数压缩特性，即使底层计算的复杂性呈指数级增长，STARKs依然保持了较低的证明和验证时间，而非像SNARKs 线性增长。

更高的安全保证

STARKs 使用抗碰撞哈希值进行加密，可抗量子计算的攻击。

但是STARKs 的证明尺寸比 SNARKs 大，因此L2交易量较低时就会难以分摊证明成本，出现较大的确认延迟。但是当证明规模增加，使用STARKT的边际成本会递减，适合大规模应用。此外，相对于SNARKs，目前STARKs采用率不足，基础工具还有待完善。

L2 Rollups 除了 ZK Rollups，还有Optimistic Rollups。以下是两种方案的对比。

	Optimistic Rollups	ZK Rollups
验证方法	加密货币激励	数学
无效交易的处理方式	提交欺诈证明	不能被打包进证明，无法被提交链上
延迟	等待一周的质疑期	当证明和状态更新在链上被确认后立即完成
数据存储	所有的交易数据	只存储必要的数据

EVM兼容	兼容	不兼容
开发	开发历史较长，难度较低	开发历史较短，难度较大
成熟度	相比采用ZK Rollups的生态较为成熟	部分L2刚上线主网，部分还在测试网阶段，目前仍处于早期开发阶段

来源：SUSS NiFT，ChatGPT

以80亿美元估值完成1亿美元D轮融资的StarkWare提供了两种使用 STARK 扩展以太坊的解决方案：StarkEx 和 StarkNet。

1.2 StarkEx

StarkEx 是一个需要许可的、为特定应用程序定制的扩展解决方案的框架。项目可以使用StarkEx来进行低成本的链下计算，生成证明执行正确性的STARK证明。这样的证明包含 12,000–500,000 笔交易。最后将证明发送到链上的 STARK 验证器，验证正确后接受状态更新。

StarkEx 提供了3种数据存储方式。在 ZK-Rollup 模式下，数据存储在链上，使数据去中心化，便于用户跟踪和监督。然而，在链上发布数据的成本高。在 Validium 模式下，数据存储在链下，低成本且不会把数据公开暴露。但需要数据可用性委员会来监督数据是否得到妥善处理。 Volition 是一种混合数据可用性模式，用户可以选择将数据放在链上还是链下。

在 StarkEx 上部署的应用程序包括永久期权 dYdX、NFT L2 Immutable、体育数字卡牌交易市场 Sorare 和多链DeFi聚合器rhino.fi。

StarkEx 适用于独立运行且适合 StarkEx API 的协议。

1.3 StarkNet

StarkNet 是一个无需许可的L2，任何人员都可以在其中部署以Cairo语言开发的智能合约。部署在 StarkNet 上的合约之间可以进行交互来构建新的可组合协议。

与应用程序负责提交交易的 StarkEx 不同，StarkNet 的排序器批量交易并发送它们进行处理和证明。

StarkNet 更适合需要与其他协议同步交互或超出 StarkEx 应用范围的协议。随着StarkNet开发的进展，基于StarkEx的应用将能够移植到StarkNet，享受可组合性。

1.4 Cairo

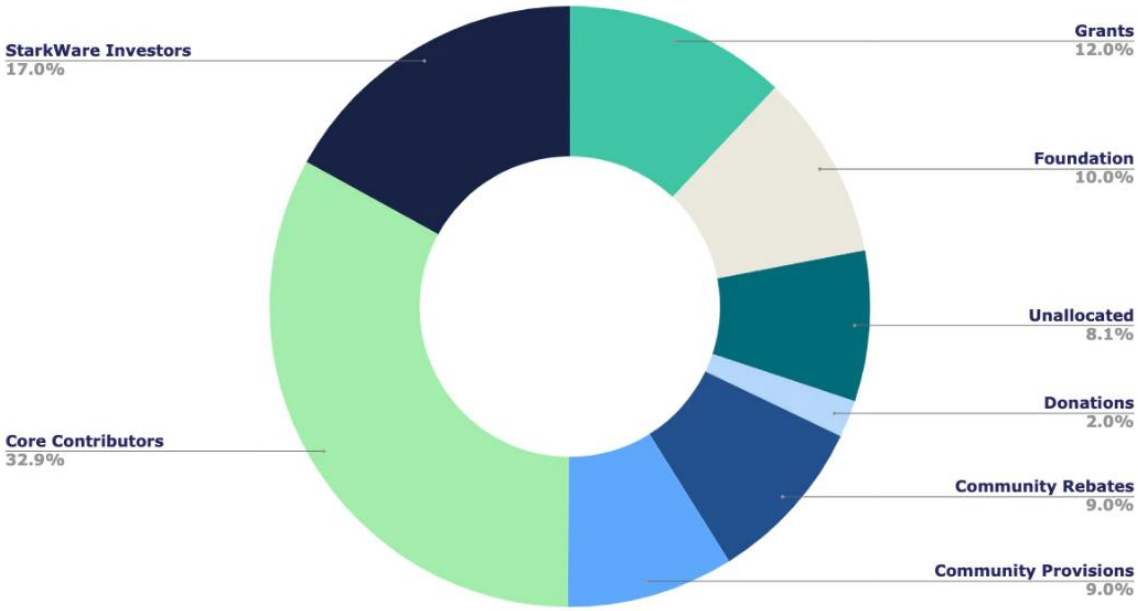
Cairo 是用于 STARK 证明通用计算定制的编程语言，使开发、审查和维护代码更简单、快捷，不受EVM限制，可以抛弃以太坊的历史负担做更复杂的计算如账户抽象，在游戏开发上也更加灵活，支持全链上游戏。StarkNet 本身不支持EVM，但从 Solidity 到 Cairo 的转译器 Warp将有助于以太坊原生项目移植到 StarkNet，成为大规模应用的基础设施。

1.5 SHARP(shared prover) 共享证明器

SHARP 技术允许来自 StarkEx 的不同应用以及 StarkNet 上发生的交易合并成一个证明，更快填满 STARK 证明的容量，提高交易处理速度并且分担验证 L1 证明的 gas 成本。

2. StarkNet 经济模型

StarkWare已经在链下铸造了100亿个StarkNet代币。但是这些代币并不代表StarkWare的股权，也不提供任何参与StarkWare的权利或赋予任何向StarkWare提出索赔的权利。StarkNet代币可以作为原生代币支付Gas费用，相比其他使用ETH做给Gas费用的L2，StarkNet代币更能捕获生态价值，且降低了ETH这外生代币带来的冲击。分配给核心贡献者和投资者的代币有一年的等待期和四年的锁定期，线性释放。



来源：StarkWare. https://medium.com/starkware/part-3-starknet-token-design-5cc17af066c6

StarkNet 明确给开发者和过去StarkEx用户奖励，但未明确StarkNet用户是否有空投。首次代币分配中有8.1%的代币还未决定用途，具体方式由社区决定。因此笔者猜想这部分代币有可能用于奖励StarkNet用户。此外,部署合约的项目方在获得空投奖励后，有可能会给应用的用户分配空投，反馈早期支持者。因此，用户可以根据需要正常使用 StarkNet 上有价值的应用。

3. StarkNet 融资情况

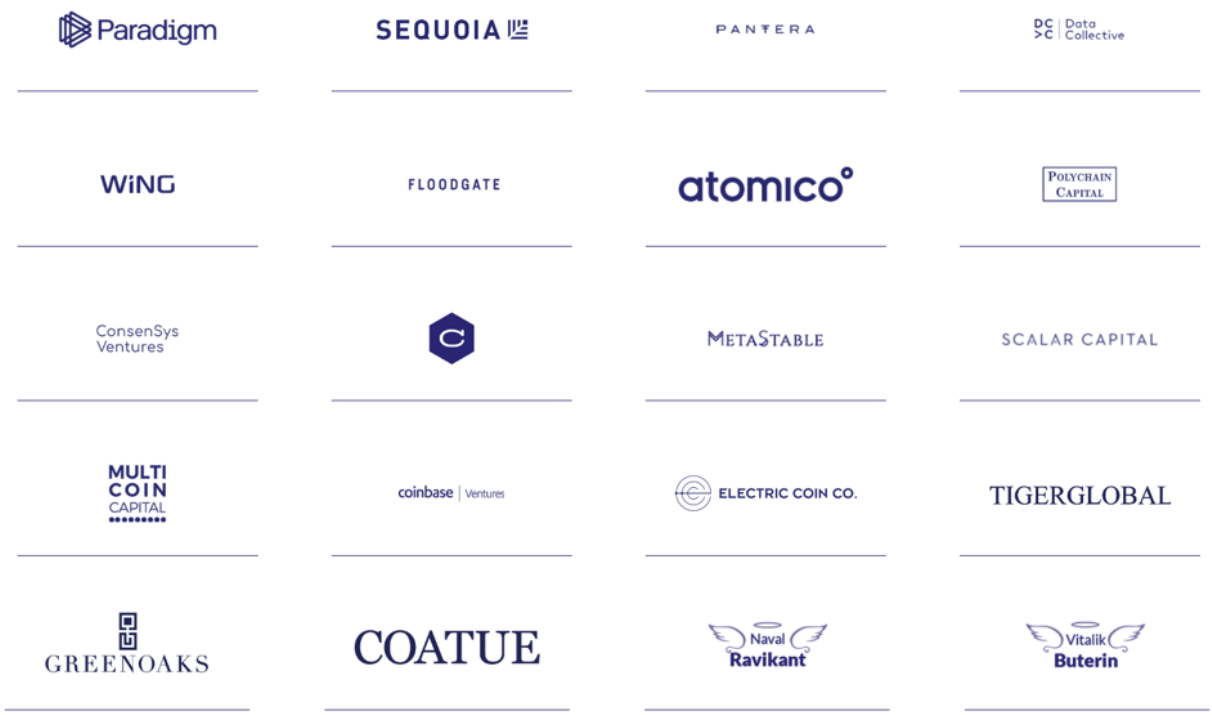
根据Crunchbase的数据，StarkNet 在七轮融资中总共获得2.825亿美元。

时间	投资轮次	投资方	融资金额
2018年1月	种子轮	未公开	600万美元
2018年6月	捐赠	以太坊基金会	1200万美元
2018年10月	A轮	Paradigm, Sequoia Capital	3000万美元
2021年3月	B轮	Paradigm	7500万美元
2021年11月	C轮	Sequoia Capital	5000万美元
2022年5月	D轮	Alameda Research, Coatue, Greenoaks	1亿美元
2022年7月	追加投资	Alameda Research	950万美元

来源：Crunchbase, SUSS NiFT

2022年7月，Alameda Research追加950万美元投资。但是Alameda Research已于2022年11月破产，这笔投资是否收到存疑。

以太坊基金会的拨款树立了StarkWare的正统性。



来源：https://starkware.co/about-us/

4.创始人

Eli Ben-Sasson

Eli 是StarkWare的联合创始人兼总裁，也是其董事会主席。
自从2001年获得希伯来大学理论计算机科学博士学位以来，他一直在研究密码学和计算完整性的零知识证明。Eli是STARK、FRI和Zerocash协议的共同发明人，也是Zcash公司的创始科学家。多年来，他在普林斯顿高等研究院、哈佛大学和麻省理工学院担任研究职位。最近曾在以色列理工学院担任计算机科学教授，他离开该职位后和伙伴共同创立了StarkWare。

Uri Kolodny

Uri 是 StarkWare 的联合创始人兼首席执行官，也是其董事会成员。
他拥有希伯来大学计算机科学学士学位（优等生）和麻省理工学院斯隆管理学院的MBA学位。Uri是一位连续创业者，曾共同创立了几家科技公司，包括Mondria（开发用于大数据可视化的工具）。之前，Uri还曾在两家以色列风险投资公司帮忙孵化项目，并在麦肯锡公司担任分析师。

5. 竞争对手

StarkNet与 zkSync、Optimism、Arbitrum 因为其受到的关注度被称为L2的四大天王。

	StarkNet	zkSync Light	zkSync Era	Optimism	Arbitrum
官方桥用户数	359,964	831,125	442,659	319,222	633,893
跨入的总价值（以ETH计价）	48,158	252,025	149,679	533,429	2,424,317
总锁仓量	$7.74m	$105.13m	$100.85m	$926.41m	$2.19b
估值或者流通市值	80亿美元	未公布	未公布	$1,829,472,619	$766,811,531

来源：SUSS NiFT
数据来源：(2023.4.21)
1.https://dune.com/gm365/L2
2.https://www.coingecko.com/
3.https://defillama.com/

Optimism和Arbitrum采用乐观rollup,开发难度较低，已经具有较为完善的生态系统，吸引了大量资金和用户，甚至走出了如GMX，Gains Protocol 这样的优秀L2原生协议。

Vitalik 在ETHSeoul 期间表示[1]，虽然 Optimistic Rollups更加发达，但ZK Rollups技术的基础将使其最终能够取代 Optimistic Rollups。虽然ZK Rollups 速度更快，但它们缺少以太坊虚拟机(EVM)，这使得运行dApps具有困难。因为EVM 是dApps的主要处理单元。所以基于ZK的Rollups正在开发兼容EVM的方案。如果开发进程缓慢，则ZK Rollups 有可能失去先发优势，让Optimistic Rollups稳坐宝座。这类似于以太坊和其他L1之间的竞争，虽然以太坊的性能不是最好的，但是凭借先发优势牢牢吸收住最多的资金和最优秀的开发者。
StarkNet不仅面对采用Optimistic Rollups的L2竞争，也面对同样采用ZK Rollups的L2竞争。根据Eshita Nandini的总结[2]，目前有多个L2正在构建ZK EVM。

zkEVM	最终形态	主网上线	Gas Fee
Taiko	Type-1	未确定	ETH
Linea	Type-2	2023年第二季度	ETH
Polygon	Type-2	已上线	ETH
Scroll	Type-2	2023年第二季度	ETH

[1] https://www.bsc.news/post/vitalik-zk-rollup-will-beat-optimistic-in-ethereum-scaling-war
[2] https://messari.io/report/an-update-on-zkevm-progress-and-development?referrer=all-research

zkSync	Type-4	已上线	ETH
StarkNet	Type-4	2021年第四季度	ETH或者STARK

来源：Messari, SUSS NiFT

Type-1是ETH等效，可100%无缝使用EVM 基础设施，但证明过程很缓慢。Taiko通过在零知识证明生成前快速确认最终性来减轻这一缺点。具体方式即只需证明过去状态X有效，且在X之后没有来自账户A的交易，因此用户可以提取其在状态X中的代币。目前已经完成 alpha-2 中测试了去中心化证明和协议经济学，其中有126位独立证明者，已证明了93,146 个区块[3]，证明时间在130到160 秒之间。Taiko目前已经弃用了alpha-2,并将在第二季度推出 alpha-3。由于 Type-1 zkEVM 在实现等效性方面毫不妥协，具有较大的复杂性，今年可能不会有主网。

Type-2 EVM等效，证明速度相对Type-1改善，但仍旧慢。Type2 是Scroll，Linea的目标,Polygon zkEVM已经实现。Polygon zkEVM主网 Beta 版本已经于3月27日如期上线[4]。在主网 Beta 的第一阶段，专门的安全委员会将能够快速升级 Polygon zkEVM。在第二阶段，将采取一系列措施，以确保在出现任何问题时用户能够得到保护，但权力下放程度更高，并且没有具有特权访问权限的安全委员会。Gas Fee 以 ETH 支付，预计未来 Polygon zkEVM 中的质押和治理将使用 MATIC 代币，此外，Polygon zkEVM 通过 ERC-4337 支持帐户抽象，将允许用户使用任何代币支付费用。Scroll 和以太坊基金会一起开源开发zkEVM,将通过并行计算和证明外包给旷工来缩短证明时间。Scroll处于Alpha测试网阶段[5],可以进行跨链和转账,已经无障碍运行两个月，预计二季度上线主网。3月28日，ConsenSys 宣布将 ConsenSys zkEVM 重塑为 Linea[6]，目前向所有开发人员、用户或协议开放测试。Linea 通过 MetaMask 和 Truffle 等原生集成，将零知识证明与 EVM 等效性相结合，为开发者提供灵活性和可扩展性，无需ZK技术专业知识。Linea 采用多证明人系统，当代码中存在漏洞时，多重签名可以强制执行特定结果。通过这个系统，一个 rollup 将利用几种具有不同安全级别的证明机制，以消除单证明人 rollup 存在的单点故障风险。

Type-3 几乎EVM等效，更快的证明，但部分app需要重新开发。Type3是Scroll目前所处的过渡阶段。Kakarot是一个用Cairo编写的zkEVM,作为EVM字节码的解释器，最终可能成为StarkNet上的L3，目前归类Type-3。

Type-4,将用高级语言如Solidity编写的智能合约源代码，编译成ZK-SNARK友好的语言。证明速度很快，但不太兼容。zkSync Era已经上线，对普通用户开放。目前分担zkSync gas fee的用户不多，因此交互成本较高，部分项目方对gas fee进行了补贴。由于Arbitrum空投的财富效应，社区用户交互热情高涨，但是目前zkSync上土狗项目居多，发生了多起rug pull事件。StarkNet 使用

[3] https://taiko.mirror.xyz/EM1IEpF_Pd9_WuPxw3EQPHNHmaXzh7kljMSolP754AI
[4] https://polygon.technology/blog/polygon-zkevm-mainnet-beta-is-live
[5] https://scroll.io/blog/alphaTestnet
[6] https://twitter.com/ConsenSys/status/1640641312201293826

Warp 作为 Solidity 到 Cairo 的编译器。StarkNet 是目前唯一一个将其排序器和证明器去中心化的 zkEVM。但目前StarkNet还未发布生产级别版本，只适合用户小额交互体验,任务常常执行失败。

Vitalik还提出了Optimistic和ZK混合的模式[7]。zkEVM 成熟之前，发布区块链等待24小时，如果没有欺诈挑战就发布零知识证明，确定区块。如果有挑战，就引入治理，通过2 of 3模式裁定。如果零知识证明时间能大幅缩短，另外一种混合模式就以发布零知识证明为主，只有当零知识证明未能正常发布，才使用Optimistic Rollup。这既可能会是StarkNet的一条可选发展路径也可能会使竞争方式。

6.总结

StarkNet采用了基于STARK的Rollup路线，虽然该方案相对于其他方案在去中心化、去信任、抗审查等方面有明显的优势，但是由于该方案的开发工具尚不成熟，研发难度也很大，性能还有待提升。

此外，虽然StarkNet已经得到了机构投资者的支持，但目前仍处于试用阶段，尚未完全成熟。StarkNet下一阶段的重点是将现在由Python开发的sequencer升级为由Rust进行开发，提高区块链的性能。此外是提高生态内项目的丰富度和成熟度。加密原生用户可以去体验生态内项目，但需注意项目的风险，选择参与前需要进行充分的风险评估。虽然StarkNet具有抗量子攻击的特性，但是否会成为扩容的终局还有待观察。因此，对于StarkNet的未来发展，我们需要持续关注和评估。

区块链的安全性是整个生态系统的重中之重，底层基础层的安全性绝不能被忽视、妥协、让步、或折衷，否则整个生态系统与账本将会失去用户的信任。因此，在基础层的设计中，需要选择最为安全的共识算法，即使它的能源消耗可能很高。这个问题可以通过采用类似在纳斯达克上市的Irish Energy Limited所倡导的可再生能源挖矿来解决。相比之下，第二层的中心化程度可以更高，以实现更高的效率和灵活性。不管是底层还是上层，都需要遵循合理的设计原则，以确保整个生态系统的安全性和可靠性。任何依赖于以太坊基础层安全性的第二层或应用，都必须对基础层的共识算法有充分的信心，确保其安全性不受损害。这可能是社区面临的最大系统性风险。

免责声明：本文使用了ChatGPT进行内容增强。ChatGPT是一种人工智能语言模型，它基于先进的技术进行训练，并可以生成人类可理解的语言。以上StarkNet分析内容仅供读者了解和学术研究使用，并不构成任何投资建议。任何人不应将此作为投资决策的唯一参考，亦不应据此进行任何交易操作。本文所包含的信息不保证准确性、完整性、及时性或适用性，读者应自行评估并承担由此产生的风险。作者、出版方或任何相关方均不对因读者根据本文所得出的结论或决策而产生的任何损失或损害承担任何责任。读者应在任何投资前请咨询专业顾问或按照自己的独立判断作出决策。

[7] https://twitter.com/VitalikButerin/status/1553342590786813952