

TonBit 重磅

2024

TON生态全景观察及 安全研究报告



媒体合作

 PANews

 金色财经

 CHAIN
CATCHER

 Foresight
News

 TechFlow

 ODAILY

 TECHUB NEWS

 BLOCK TEMPO
— 由社群而生的區塊鏈媒體 —

 MarsBit

目录

CONTENTS

01	前言	01
02	TON生态概述	01
	2.1 TON生态系统简介	01
	...	
	2.2 为什么选择TON	02
	...	
	2.3 2024年TON发展方向与目标概览	04
03	生态发展情况	06
	3.1 生态概况	06
	...	
	3.2 TON 生态系统关键指标	06
	...	
	3.3 TON如何成为一个强大的去中心化游戏平台	09
04	TON生态安全研究	11
	4.1 如何在TON上做安全开发	11
	...	
	4.2 TON生态安全事件回顾	13
	...	
	4.3 TON生态项目方如何做安全审计	17
05	用户如何在 TON 和 Telegram 上保持安全	18
	5.1 常见的诈骗手段	18
	...	
	5.2 警惕Toncoin金字塔骗局	18
	...	
	5.3 如何避免网络诈骗	18
06	TON生态发展总结	19
07	关于TonBit	20

1 前言

本报告由 Web3 区块链安全审计公司 BitsLab 旗下子品牌 TonBit 官方出品。

随着区块链技术的不断发展和应用的日益广泛，TON 生态系统在2024年继续表现出强劲的增长势头，吸引了大量开发者、投资者和用户的关注。

2024年，TON 生态继续在技术创新、应用落地和社区建设等方面取得了显著的进展，进一步巩固了其在区块链领域的地位。然而，随着生态系统的快速发展，安全问题也日益凸显。面对不断演化的安全威胁，如何有效防范和应对成为了 TON 生态的重要课题。

TonBit 始终致力于通过专业的审计服务和安全解决方案，保障 TON 生态的稳定和安全。从2021年开始，TonBit 成员就专注于TON 生态系统，发起了 TONX、TONX API、TonKey、Ton Research 等项目。本报告详细回顾 TON 生态的发展历程，总结了这大半年中发生的主要安全事件，分析了其原因和影响，并提出了相应的防范措施和未来的改进建议。

我们希望通过本报告，能够为 TON 生态的参与者提供有价值的参考，促进生态系统的健康发展，并增强各方对区块链安全的重视。

感谢所有支持和参与 TON 生态建设的伙伴们，让我们共同努力，为打造一个更加安全、透明和繁荣的区块链生态而奋斗。

2 TON 生态概述

2.1 TON 生态系统简介

基本介绍与架构

TON 是 The Open Network 的缩写，是一个由 Telegram 设计的区块链和数字通信协议。它旨在构建一个快速、安全和可扩展的区块链平台，为用户提供去中心化的应用和服务。通过结合区块链技术和 Telegram 的通信功能，TON 实现了高性能、高安全性和高可扩展性的特点。它支持开发者构建各种去中心化应用，并提供分布式存储解决方案。与传统的区块链平台相比，TON 具有更快的处理速度和吞吐量，并采用了 Proof-of-Stake 共识机制。作为一个具有创新性和潜力的区块链平台，TON 推动着加密货币和去中心化应用的发展。

2.2 为什么选择 TON

在与比特币和以太坊强大的流动性和社区竞争时，尽管这些区块链在其初期状态下仍有许多问题，但挑战依然存在。

由 Vitalik Buterin 提出的区块链三难困境描述了 Layer 1 网络在同时平衡安全性、可扩展性和效率方面面临的挑战。必须进行权衡（至少在初始阶段）。以比特币为例，我们可以看到工作量证明（PoW）提供了强大的安全性和更高的去中心化，但其交易速度较慢且费用较高。以太坊尽管最近迁移到了权益证明（PoS）并且支持更多的 Layer 2 解决方案（如 Optimism 和 Arbitrum），但在网络拥堵期间仍会面临高昂的Gas费用。

简而言之，几乎没有任何链（无论是 Layer 1 还是 Layer 2）能够在其现状下与传统银行和金融机构竞争，更不用说在隐私和安全等平衡且务实的激励措施上取得优势。



2.2.1 灵活且可分片的 PoS 架构

与 Solana 和以太坊一样，TON 采用了权益证明共识机制。然而，TON 的关键设计和实现使其在性能和多功能性上领先。其图灵完备的智能合约是一个例子，TON 的异步区块链引入了 Lamport 时间和非常规排序方案等概念。

TON 的闪电般快速且低成本的交易由链的灵活且可分片的架构支持。这种架构允许其在不损失性能的情况下轻松扩展。动态分片涉及初步开发的具有各自目的单独分片，这些分片可以同时运行并防止大规模积压。TON 的区块时间为5秒，最终确定时间少于6秒。

现有基础设施分为两个主要部分：

主链（Masterchain）

负责处理协议的所有重要和关键数据，包括参数及当前值。这包括验证者的地址以及验证的币量。此外，它还包含各种工作链和分片链的数据。在多层区块链中，主链是最重要的；是单一真相源。

工作链（Workchain）

连接到主链的次级链。它包含所有交易信息以及记录的各种智能合约。然而，每个工作链可以有不同规则。这意味着具有不同格式的地址、不同的交易格式以及特定智能合约的不同虚拟机（VM）。正因为如此，TON 区块链可以被称为异构区块链。

2.2.2 扩展用例和优势

TON 基金会是由 TON 核心社区运营的 DAO，为 TON 生态系统中的项目提供各种支持。这些支持包括通过活动和黑客松为开发者提供支持，为 DeFi 项目提供流动性激励计划等。

根据最近的开发者报告，每月活跃开发者增加了8%，而 GitHub 上的开源 TON 相关存储库的贡献者年增长率达50%。这表明社区在不断壮大，促进了合作和创新。

(1) TON Connect 2.0 的推出

TON Connect 2.0 的发布标志着一个重要的里程碑，为用户提供了一种直观的方式连接他们喜欢的钱包和应用程序。受 Tonkeeper 钱包和 OpenMask 支持，已被超过14个服务采用，所有这些都帮助创造了更好的用户体验。

(2) 通过TON Verifier 提高信任和可靠性

由 Orbs 团队创建的智能合约检查器 TON Verifier 现已向社区成员开放，允许开发者在部署前检查其合约的完整性。

(3) Blueprint——开发者的盟友

TON 推出了 Blueprint，这是一种旨在帮助开发者编写、测试和部署智能合约的简单环境。Blueprint 简化了整个过程，使工程师更容易在 TON 上 构建。

(4) Sandbox 开发者工具包

这个最新的工具包扩展了 TON 的功能，适用于从企业到政府的各种用例。Sandbox 工具包赋能主流智能合约开发，为更广泛的采用铺平了道路。

(5) Tact 语言 Beta——拥抱未来

由 Steve Korshakov 和 Tact 社区支持的 Tact 编程语言成功发布了 Beta 版本。简洁的文档鼓励社区学习和反馈，促进了更强大的编程环境。

(6) TON Society 国际化

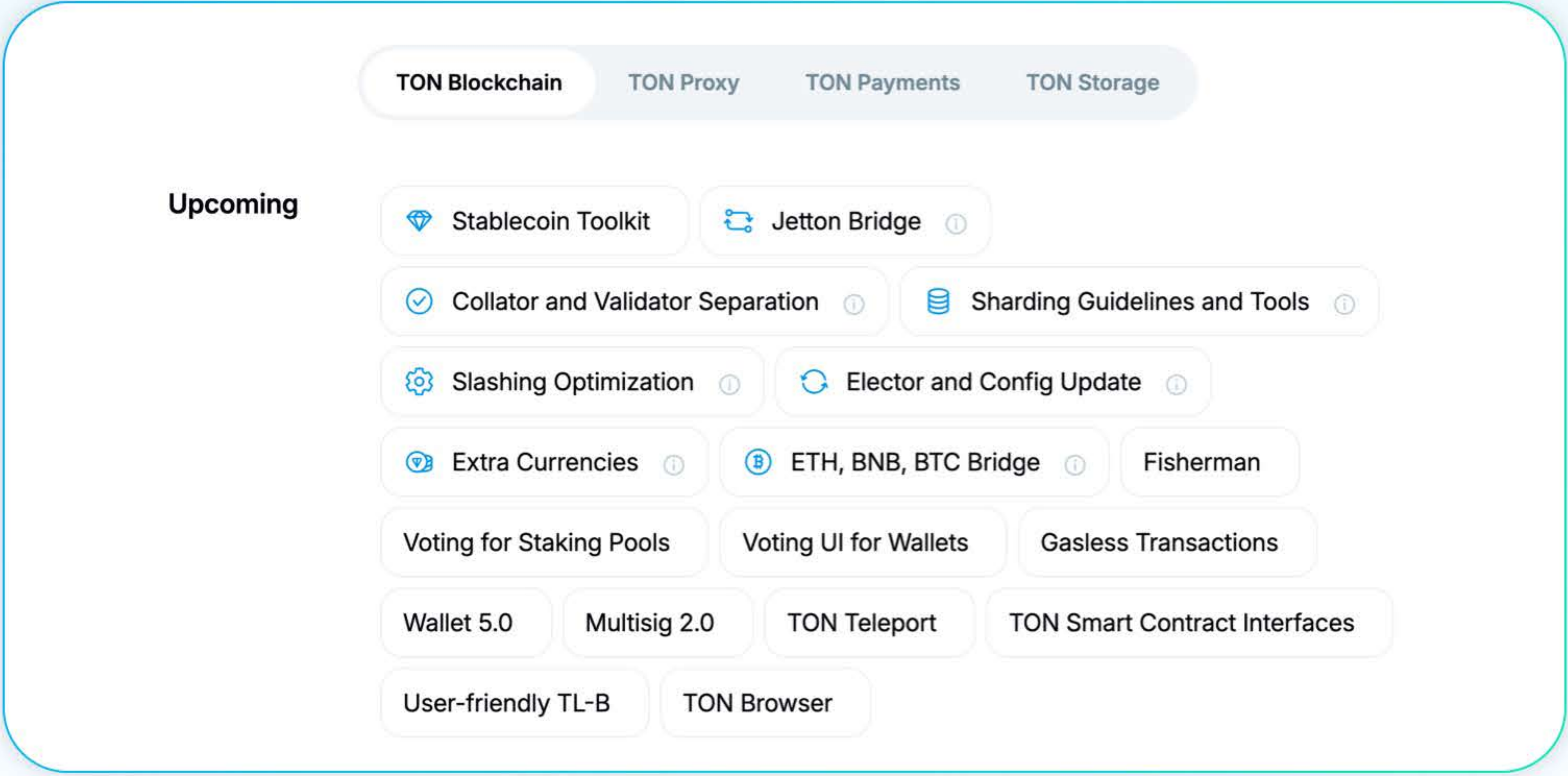
TON 社区还在里斯本、曼谷、海得拉巴（印度）和巴塞罗那启动了国际中心，分享创意并加速项目开发。预计全球将出现更多中心，邀请有兴趣的人参与这一激动人心的事业。

(7) DeFi 流动性激励计划

这是一种渐进的、基于里程碑的方法，为项目提供资金。该计划旨在实现 TON 生态系统内 DeFi 领域的有机可持续性。

2.3 2024年 TON 发展方向与目标概览

TON 的发展路线图包含许多有趣的计划，如稳定币工具包、分片工具以及 BTC、ETH 和 BNB 的原生桥接。



无 Gas 费交易

目前没有其他链提供无 Gas 费交易，因此 TON 可能会彻底改变区块链领域，并吸引更多来自其他生态系统的用户。TON 可能会补贴某些情况下的 Gas 费，例如 Telegram 钱包或 USDT 转账，以吸引更多用户将 TON 用于日常需求。

验证节点与打包节点分离

这是 TON 可扩展性的重大升级。打包意味着收集交易、验证它们并将它们放入一个区块。为此，节点需要存储并不断监控整个网络状态——TON 区块链中所有地址的所有余额。

TON 计划到2028年吸纳5亿 Telegram 用户，并利用分片提供足够的交易执行时间和低交易费。通过分片，区块链被分成几个分片链。2条分片链提供2倍吞吐量，4条分片链提供4倍，依此类推。

每个分片链将有自己的验证节点子集来打包和验证区块。这些验证节点必须频繁旋转子集以确保安全性。问题在于：随机旋转的情况下，验证节点将不得不存储每个分片的状态，而不仅仅是他们自己的分片状态。存储100万个账户的状态需要一个强大的服务器，而在一个地方存储5亿个账户的状态是不可能的。

为了解决这个问题，TON 团队提出将验证和打包分成两个角色：打包节点只存储其分片链的状态并打包区块，而分配到该分片链的验证节点在一定时间内只验证并签署区块。这样负载和风险将得到均衡分配，TON 可以扩展到容纳数十亿用户。

在官方文档中，没有提到质押奖励。虽然只有验证节点会在区块验证中产生风险（验证节点因为在参与共识、验证区块时需要质押一定数量的加密货币。如果他们的行为不符合协议规定，可能会导致部分或全部质押资金被惩罚性削减，即所谓的“惩罚机制”或“Slashing”），这就是所谓的“风险”，但打包节点也应因存储状态和生成区块而获得奖励。

尽管验证过程变得更加复杂，TON 的年增发率是固定的，但是质押的年收益率（APY）会变化。由于 Staking 的人变多了，原本的 APY 高达 25% 现在则是 3.4%

分片指南和工具

TON 成为首批高效利用分片技术的区块链之一，这要归功于杰出的开发者团队。中心化交易所、支付系统，甚至 TON 的服务和应用都需要专门的工具和文档来实现分片支持，因为这是一项他们不熟悉的技术。这就是为什么 TON 开发者希望在今后的将来发布这些工具。

惩罚机制优化

惩罚机制是对执行不力的验证节点的惩罚：错过区块、频繁离线，甚至试图将欺诈交易推入区块。

目前，TON 使用投诉机制来惩罚不当行为的验证节点。任何网络参与者都可以提交带有证据的投诉，并追究不良验证节点的责任。

惩罚机制优化将引入更好的系统来检测和惩罚不当行为的验证节点，从而提高 TON 的鲁棒性。这将分几步实施：首先，流动质押协议不会受到验证节点惩罚的影响，用户的奖励将得到保障。

然后，惩罚将分配到流动质押协议提供的 TON 上，略微降低平均年收益率。

选举人和配置合同更新

TON 质押、流动质押和链上治理都是通过智能合约实现的。Tonstakers 也使用这些合约来汇集 TON，为验证节点提供 TON，并在用户之间分配奖励。

此次选举人和配置合同更新将允许我们的用户投票表决网络提案，使网络对每个人更加开放，并增加每个用户的价值。

TON 稳定币工具包

稳定币工具包将允许任何人发行与本地法定货币挂钩的算法稳定币：英镑、欧元、新西兰元等。

考虑到 TON 与 Telegram 的集成、内置钱包以及最近决定与频道所有者分享广告利润，我们可以推测 Telegram 可能会为内置服务增加本地稳定币支付功能。

Jetton Bridge

TON 已经有了以太坊和BNB链的桥，用于桥接 \$TON 和流行的硬币如 ETH、BNB 和 USDC。Jetton 桥将允许用户将 TON 代币（如tsTON）发送到其他链。

ETH, BNB 和 BTC Bridge

虽然有第三方桥，推出官方桥来引入主要加密货币到 TON 具有合理性。

非原生代币

在 TON 区块链生态系统中，\$TON 充当原生代币的角色，具体用途包括但不限于参与网络的质押机制以及支付交易执行所需的 Gas 费用。\$TON 代币的交互功能，如交易和余额管理，是通过 TON 协议本身内置的智能合约实现的。此外，用户的 \$TON 余额被妥善记录和存储在其链上账户中，确保了交易的安全性和数据的一致性。

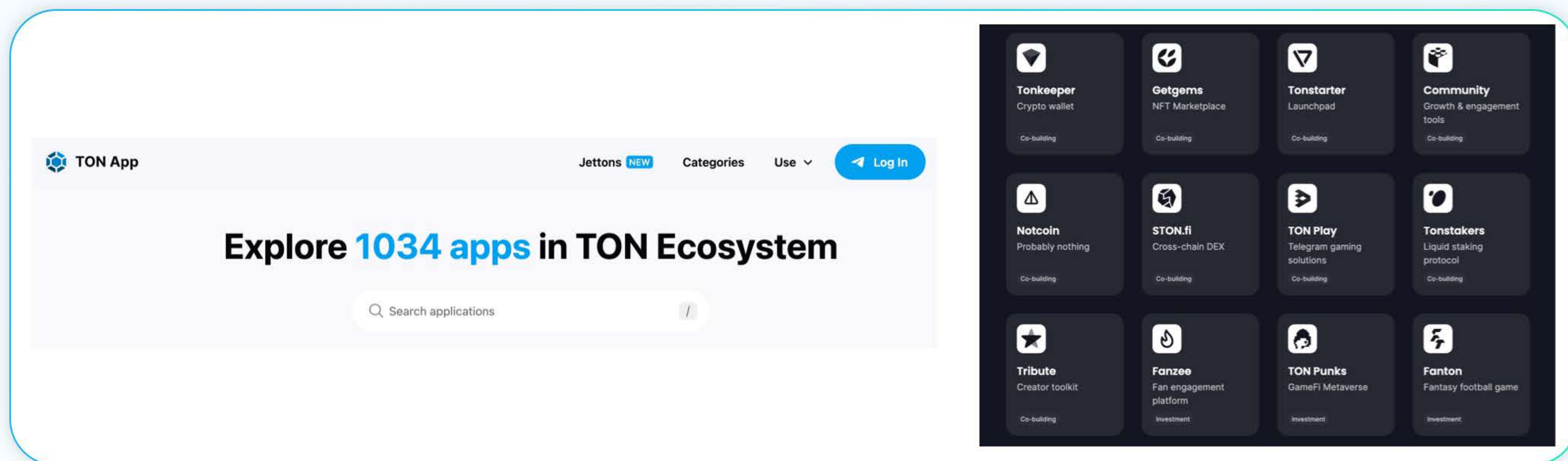
Jettons（如 USDT 和 tsTON 等普通代币）由第三方智能合约操作，不能代替 \$TON 支付费用和质押。用户的余额存储在这些合约中。

非原生代币（Extra Currencies）将允许 TON 用户创建类似原生的代币，这些代币也将存储在账户中。额外货币与 Jettons 的最明显区别是，额外货币的交易应该便宜2-3倍，因为它们将不涉及合约调用。

3 生态发展情况

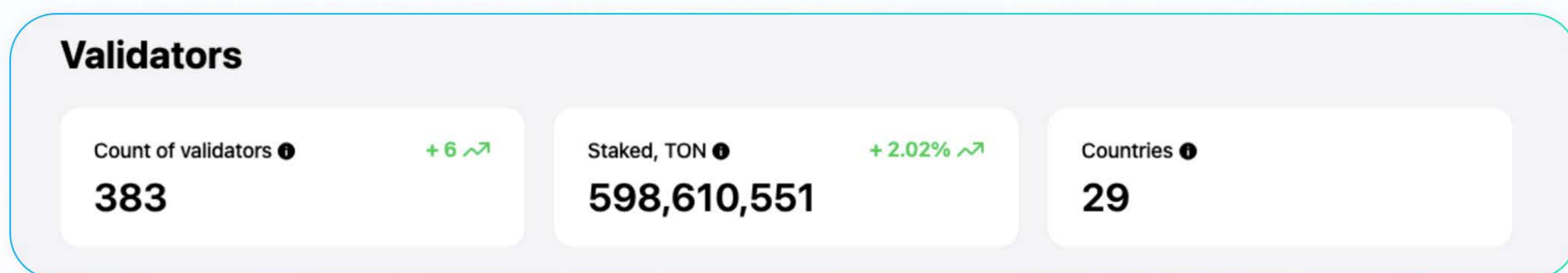
3.1 生态概况

TON 基金会官网目前展示了接近1000个应用程序，这些项目涵盖了广泛的领域，从去中心化金融（DeFi）到游戏、社交媒体和工具类应用，显示出 TON 生态系统的多样性和活力。通过这些项目，TON 基金会不仅展示了其在区块链技术领域的领先地位，还表明了其致力于推动创新和促进生态系统发展的决心。这些项目得到了 TON 基金会的资金支持和技术指导，为开发者提供了宝贵的资源和平台，帮助他们在 TON 区块链上实现创意和商业目标。这种全面的支持和投资策略，使得 TON 生态系统持续增长，吸引了越来越多的开发者和用户加入，为未来的发展奠定了坚实的基础。

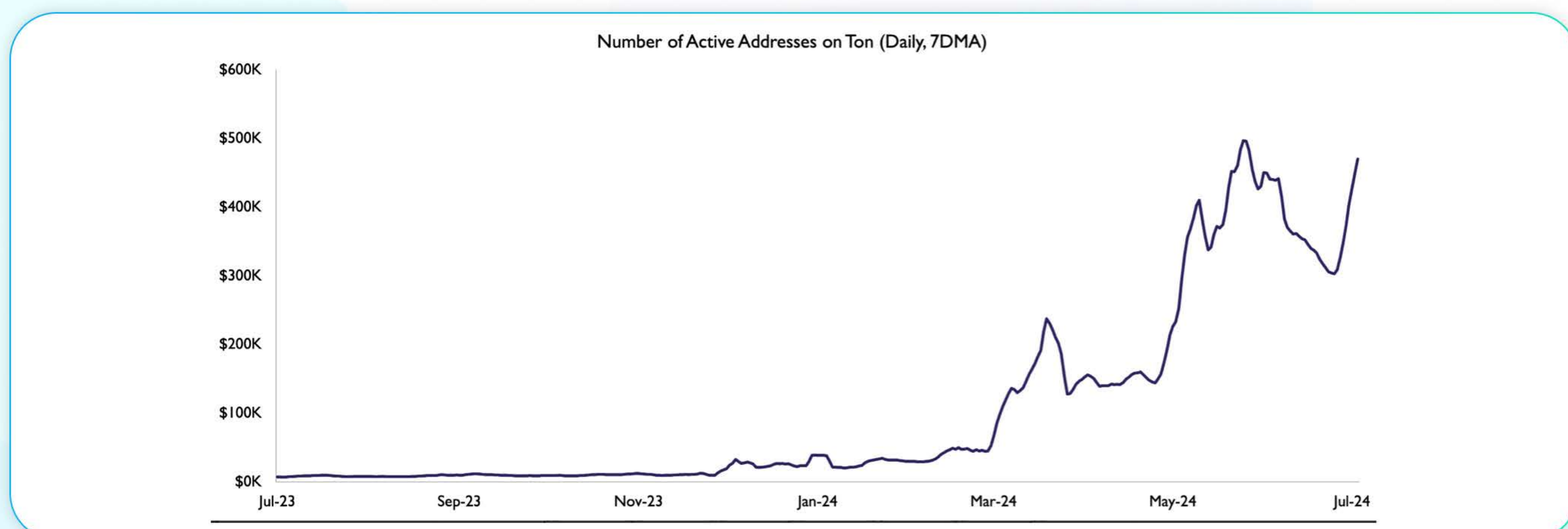


3.2 TON 生态系统关键指标

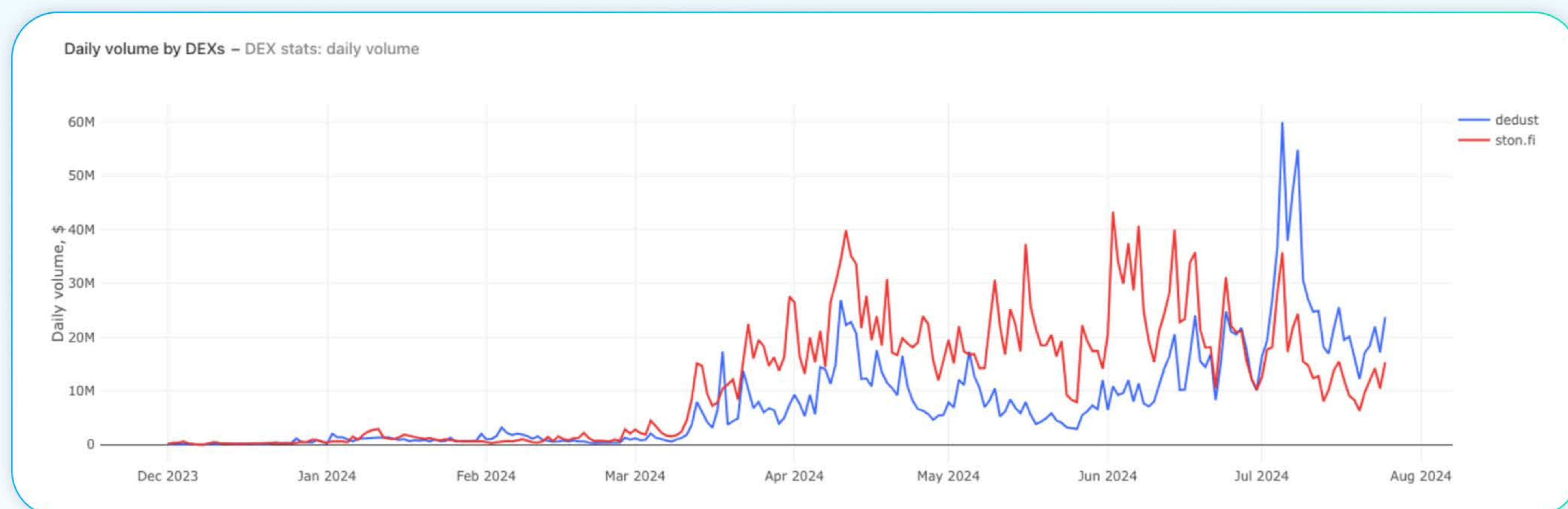
截止7月27日，TON 链上的验证节点数量为383个，PoS 机制下总质押 \$TON 数量为5.9亿多个，分布在29个国家当中。



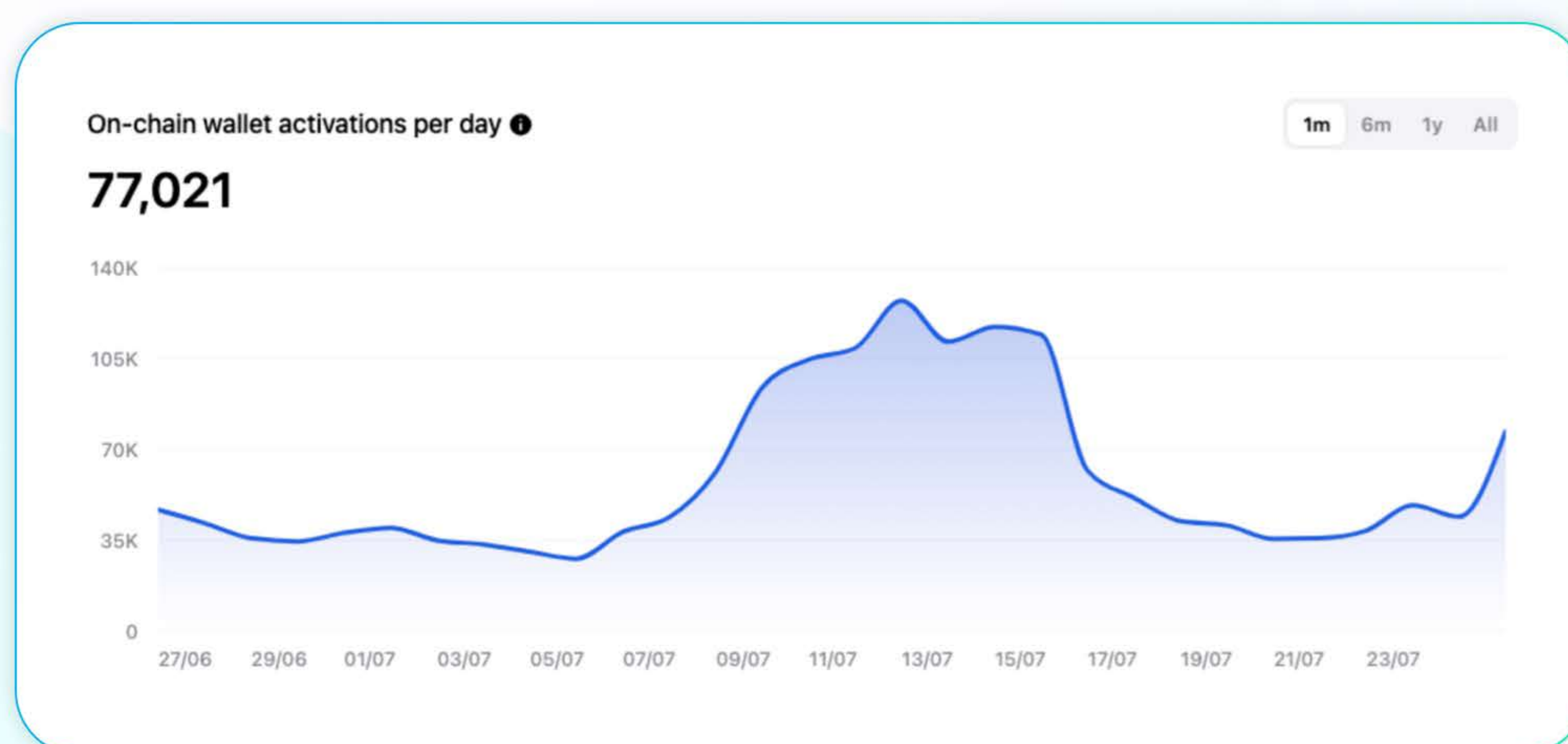
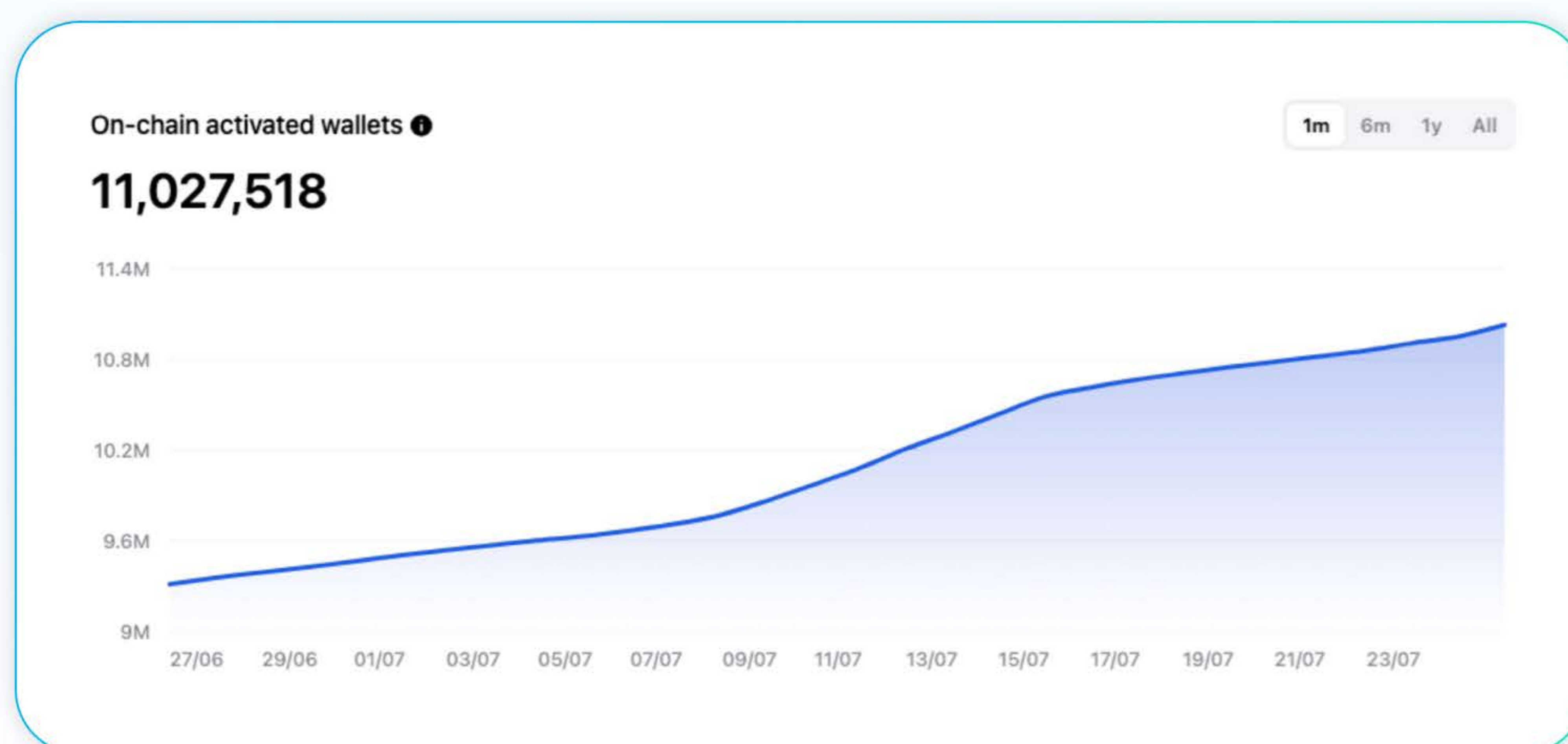
截止7月中旬，目前 TON 网络的每日活跃地址数达到37.3万个，较去年同比增长了5360%。这一显著增长反映了 TON 区块链在用户中的受欢迎程度和日益增加的采用率。

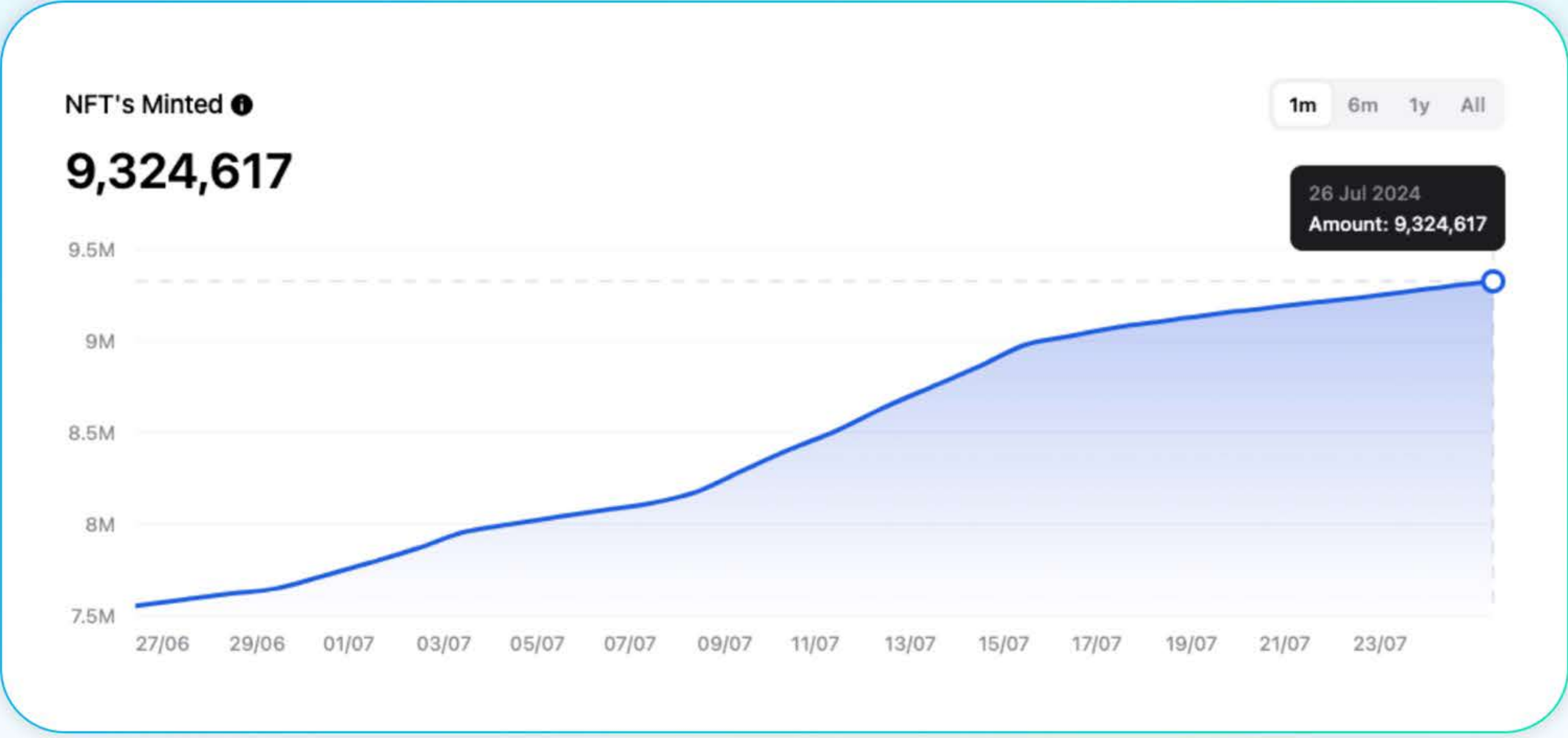


TON 网络的 DeFi 生态系统展现出强劲的发展势头和广泛的用户基础。关键指标显示，独立用户数量已经达到1,784,089，表明大量用户正在积极参与和使用 TON 网络上的 DeFi 服务。此外，总锁仓量（TVL）达到了706,307,873美元，这一数额不仅反映了用户对 TON DeFi 生态系统的信任和认可，也显示了其在区块链金融领域的显著地位。流动性提供者的数量也达到了26,297，进一步证明了 TON 网络在吸引投资者和促进流动性方面的成功。



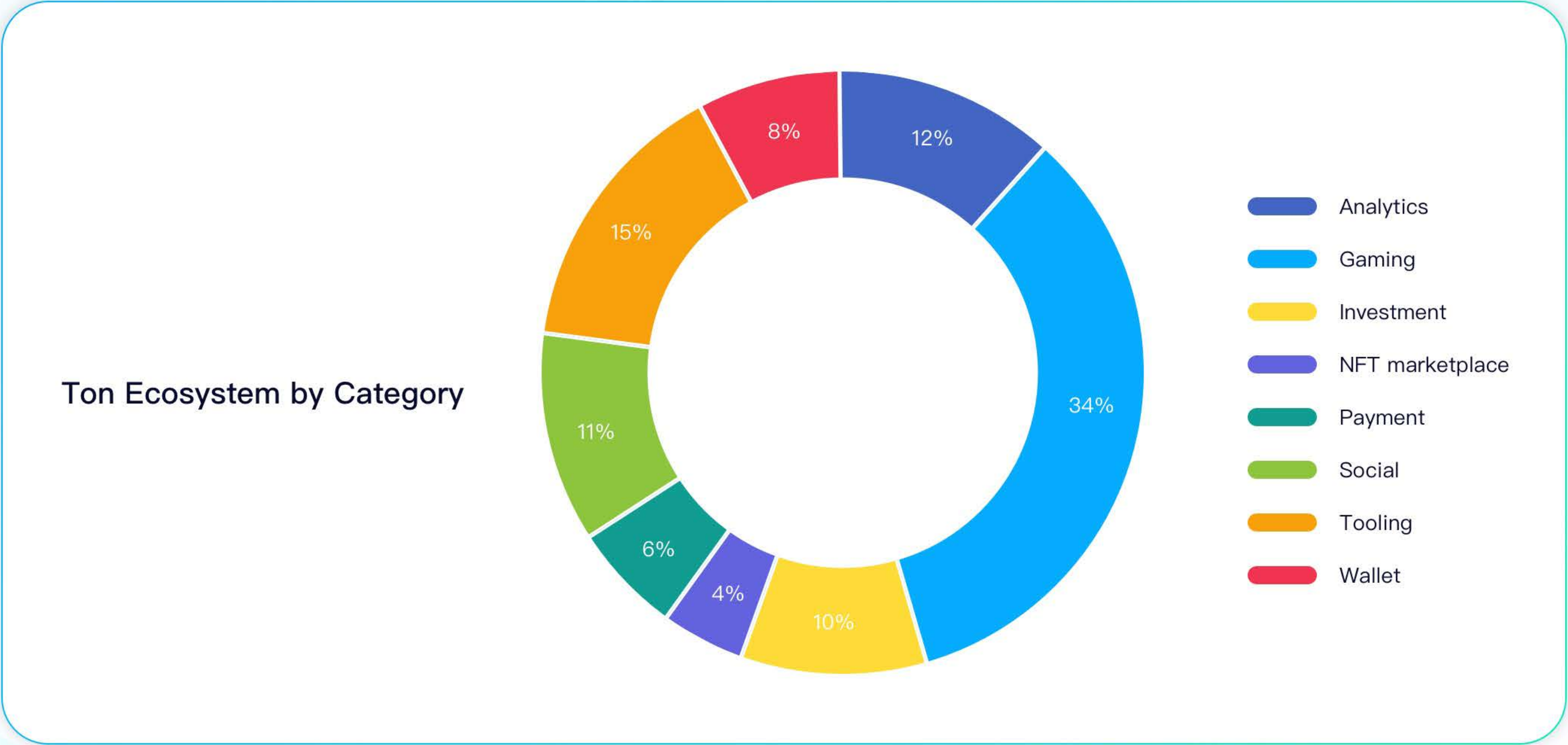
截至7月27日，TON 网络的链上活跃钱包数量达到了11,027,518个，显示了该网络在用户基础上的广泛吸引力和持续增长。此外，每日链上钱包激活量达到77,021个，表明新用户和现有用户的持续活跃和参与。同时，NFT 铸造数量达到了9,324,617个，反映出 TON 生态系统在数字资产创建和交易方面的繁荣发展。这些数据共同展示了 TON 网络在区块链行业中的强大生命力和不断扩展的生态系统。





根据 The Block 7月中旬的统计，TON 上超过一半的项目都是作为 Telegram 上的机器人构建的，这突显了 TON 与社交平台 Telegram 之间的紧密联系。

TON 与 Telegram 的整合为开发者提供了便捷的开发环境和广泛的用户基础，使其成为项目构建和推广的理想平台。



TON 生态系统中的主要项目类别包括游戏和投资（特指一些泛金融类应用），显示出多样化的社区兴趣。游戏类项目利用 TON 的高速交易处理和低费用，为玩家提供了流畅的游戏体验和丰富的游戏内经济。而投资类项目则利用 TON 的去中心化特性和安全性，吸引了众多投资者和金融应用的开发者。

TON 生态系统的不断扩展不仅表明了其技术优势和平台潜力，还展示了其在各类应用场景中的广泛适用性。随着更多开发者和用户的加入，TON 有望继续推动区块链技术的发展，并在未来的数字经济中扮演更加重要的角色。

3.3 TON 如何成为一个强大的去中心化游戏平台

3.3.1 构建基于 TON 的去中心化游戏的主要原因

基于 TON 区块链开发去中心化游戏为企业和开发者提供了一系列优势，旨在重新定义游戏产业的格局。让我们来看一下 TON 为何成为去中心化游戏首选平台的关键原因。

与 Telegram 的集成

TON 与 Telegram 的集成为开发者提供了超过9亿月活跃用户的访问权限，使得游戏可以直接在 Telegram 上快速、轻松地发布，这与传统应用商店形成了鲜明对比。

在 iOS 和 Android 等操作系统上，用户通常需要经过多个步骤，如下载和授权。而基于 TON 的 Telegram 游戏允许用户通过直接打开机器人或通过 Telegram 应用中心立即开始游戏。

强大的用户获取和留存工具

利用 TON 和 Telegram，开发者可以获得一套综合工具，旨在提升用户留存率并改善游戏内的用户体验。这些工具包括：

- Telegram 应用中心，这是一个一站式工具、实用程序和游戏的目的地，全部集成在 Telegram 生态系统中。
- Telegram 广告可以在几乎任何 Telegram 频道上执行广告活动，将游戏广告投放给数百万用户。
- 可以在信使内直接发送通知，确保相比于游戏中的原生推送通知有更高的打开率。
这些工具专为保持玩家在游戏环境中的积极参与而设计，从而帮助开发者维持一个充满活力的用户群体。

快速且高效的区块链

TON 区块链以其高速度而闻名。它能够处理每秒超过100,000笔交易，同时保持低费用。这些特点对于维持去中心化游戏的性能和可扩展性至关重要，尤其是在处理高吞吐量的玩家互动时。

多样化的货币化机会

TON 为开发者提供了多种货币化策略，从应用内广告和可交易和出售的非同质化代币的集成，到反映现实世界经济原则的游戏内经济体的创建。这为开发者打开了多样化的收入来源，并增强了游戏项目的财务可行性。

简单且易于访问

TON 是一个用户友好且易于访问的区块链，这对于游戏行业的广泛采用至关重要。

对于 GameFi Web3 开发者和玩家来说，TON 提供了一整套工具，使其成为那些希望过渡到去中心化游戏世界的理想选择。

3.3.2 TON 在去中心化游戏中的应用案例

TON 区块链迅速成为一个充满活力的去中心化游戏生态系统，以下是一些正在定义 TON 游戏体验的最受欢迎的示例。

- Notcoin: 一款点击赚取游戏，玩家通过点击赚取代币
- Catizen: 一款空投赚取游戏，玩家通过养猫赚取\$CATS代币
- Fanton Fantasy Football: 一款玩赚游戏，玩家组建足球队并获得奖励

(1) Notcoin

Notcoin 是一款简单而有趣的点击赚取游戏，由于其简单的玩法和有趣的机制，迅速在 Telegram 上流行起来。玩家通过点击赚取代币，他们的成就被记录在联赛排名中。玩家还可以通过加入 Telegram 频道和聊天组队，完成各种任务，攀登排行榜。

(2) Catizen

Catizen 是一款融合了元宇宙、GameFi 和 AI 元素的有趣的空投赚取游戏。游戏玩法涉及通过将猫拖放在一起进行繁殖，以提高其等级并赚取 \$CATS 代币。玩家还可以通过钓鱼赚取鱼币，这些鱼币用于游戏内的提升和升级。

在 Catizen 中，玩家可以购买提升道具以加速猫的繁殖，获取新猫，并提升整体游戏体验。游戏商店允许购买 \$CATS 和鱼币代币用于 TON。

随着玩家挖矿更多代币，他们在青铜、白银、黄金、铂金和钻石联赛中不断进步，反映出他们的成就。

(3) Fanton Fantasy Football

Fanton Fantasy Football 是首款与 Telegram 集成的玩赚游戏。在这款游戏中，玩家组建一支由五名足球运动员组成的队伍：守门员、后卫、中场、前锋和替补。玩家在实际足球比赛中的表现决定了他们在游戏中获得的积分。

玩家通过各种场上行动获得积分，例如进球、助攻、扑救和其他重要贡献。球队获得最多积分的用户有机会赢得有价值的奖品，包括加密货币和NFT。这使得每场比赛都充满了潜在的回报。

由于与 Telegram 的无缝集成，TON 极大地简化了游戏发布，使得游戏发布变得比以往任何时候都容易。再加上其先进的用户获取和留存工具，为开发者提供了创建引人入胜且盈利的去中心化游戏体验的能力。但是在开发这类项目时，安全风险同样不可忽视。

4 TON 生态安全研究

4.1 如何在 TON 上做安全开发

为了确保智能合约的安全性，我们需要采取一系列安全措施，以下是一些 TON 生态关键的安全实践：

(1) 访问控制

描述：当合约中有一些重要的逻辑或者敏感操作需要特定授权用户来执行时，我们应该做好访问控制，避免攻击者执行敏感操作，从而造成严重的损害。

实践：

- 确定哪些操作需要权限控制。
- 对需要权限执行的操作通过校验消息的发送方来限制访问。
- 定期审查和更新访问控制策略，以适应合约需求的变化。

具体提案可参考：

<https://github.com/ton-blockchain/TEPs/pull/180>

<https://github.com/ton-blockchain/TEPs/pull/181>

(2) 验证消息输入

描述：智能合约中如果缺乏对外部输入的适当验证或过滤，会导致恶意用户或攻击者输入恶意数据，从而可能导致不安全行为或漏洞。

实践：

- 对所有外部输入进行严格的验证和过滤，这包括验证数据类型、检查边界条件以及清理用户输入。
- 考虑所有可能的输入场景，包括边缘情况和意外输入。
- 定期审计和测试输入验证逻辑。

(3) 检查 Gas 使用量

描述：在处理内部消息时，发送者通常需要支付 Gas 使用费。当处理外部消息时，合约会支付 Gas 使用量。这意味着需要小心外部消息中的 Gas 使用。应该始终测试合约的 Gas 使用情况，以验证一切是否按预期运行，并避免可能耗尽合约余额的漏洞。

实践：

- 在开发过程中监控和优化 Gas 使用情况。
- 使用 Gas 限制来防止高消耗操作。
- 定期测试合约在不同情景下的 Gas 消耗情况。

(4) 时间戳依赖

描述：一些智能合约的行为依赖区块时间戳，而区块时间戳可能会被验证者操纵。例如，验证节点可以有选择地包含或排除某些交易，或者调整时间戳以服务于某些目的。这种行为可能会导致合约逻辑被操纵，带来安全风险。

实践：

- 避免直接依赖区块时间戳进行关键逻辑判断。
- 如果必须使用时间戳，请确保使用更可靠且不可控的方法。
- 采用时间缓冲机制，允许时间在一定范围内变化，减少对单个时间点的依赖。
- 定期审查合约逻辑，确保不会受到时间戳操纵影响。

(5) 整数溢出

描述：整数上溢和下溢是超出变量表示范围的指数值运算，导致计算结果不正确。整数溢出通常发生在加、减、乘等运算中。如果不加以控制，可能会导致严重的安全问题，例如余额计算不正确或意外的资金转移。

实践：

- 使用安全的数学库来处理整数运算。
- 在所有数学运算前后添加溢出检查。
- 定期审计合约代码，确保所有整数运算均受到保护。

(6) 舍入误差

描述：舍入误差风险是指由于数值运算中精度限制或舍入方法不当而导致计算结果出现误差。特别是在处理货币或高精度数值时，舍入误差可能会导致资金损失或分配不公平。

实践：

- 使用高精度数值库或定点数库来处理货币运算。
- 定期测试和验证数值运算逻辑，确保精度符合预期。
- 在代码中明确标注舍入方法，确保一致性。

(7) 拒绝服务

描述：拒绝服务风险是指消耗智能合约的计算资源或触发错误条件，导致合约无法正常执行或陷入无休止的操作。这可能会阻止合法用户与合约交互，甚至阻止合约状态更新。

实践：

- 限制循环次数或递归深度以避免长时间运行的操作。
- 关键操作前检查剩余 Gas，避免因 Gas 不足导致交易失败。
- 定期审查和优化合约逻辑，确保效率和可靠性。
- 使用事件日志记录重要操作，便于故障排查和恢复。

(8) 业务逻辑

描述：业务逻辑漏洞是指智能合约在实现其业务流程时的设计缺陷或实现错误，导致合约在某些情况下表现异常。这些漏洞可能被恶意用户利用，导致资金损失、数据篡改或合约功能失效等严重后果。业务逻辑漏洞通常不是编码错误，而是业务需求和流程的误解或不完善的实现。

实践：

- 深入理解和分析业务需求，确保逻辑设计正确。
- 定期进行代码审计和逻辑验证，及时发现并修复漏洞。
- 编写全面的测试用例，覆盖所有可能的业务场景。

通过上述安全实践，我们可以大大提升智能合约的安全性，降低风险，确保合约的稳定运行和用户的资金安全。

4.2 TON 生态安全事件回顾

在2024年，TON 生态系统中发生了多起安全事件，揭示了其安全性方面的挑战。以下是一些重要事件的详细描述、分析事件的原因、影响及其解决方案，并对一些典型的安全漏洞进行了盘点。

4.2.1 常见的攻击类型

在2024年，TON 生态系统中发生了多起重大安全事件，对于项目方和用户而言都造成一定的影响，这些事件揭示了区块链技术在安全性上的一些脆弱性。以下是常见的攻击类型及其简要描述：

(1) 输入验证不正确

描述：输入验证是指验证输入数据的完整性、准确性和安全性。当智能合约无法充分验证和清理用户输入时，就会发生不正确的输入验证，从而使他们容易受到各种类型的攻击。此类漏洞可被利用来操纵合约逻辑、注入恶意数据或导致意外行为。正确的输入验证可确保合约仅处理有效且预期的数据，从而降低被利用的风险。

(2) 计算错误

描述：计算错误是指系统在执行某些计算时出现错误，导致意外行为或漏洞。这类错误可能源于智能合约代码中的逻辑错误或编程错误，攻击者可以利用这些漏洞来操纵计算或在合约中获得优势。

(3) 预言机/价格操纵

描述：价格操纵是指攻击者通过操纵市场价格来获取不正当收益。在 TON 生态系统中，攻击者可能会通过操纵 DEX（去中心化交易所）上的交易量或订单簿，影响特定代币的价格，从中获利或引发市场恐慌。攻击者还可能通过干预预言机所报告的数字资产价格等外部信息，导致智能合约做出错误决策。

(4) 弱访问控制

描述：弱访问控制指系统未能有效限制用户对资源或操作的访问权限，导致未经授权的用户能够执行敏感操作。在 TON 生态系统中，这可能包括未经授权的用户能够访问管理接口、更改智能合约设置或窃取用户资产。

(5) 拒绝服务攻击

描述：拒绝服务（DoS）攻击是指消耗智能合约的计算资源或触发错误条件，导致合约无法正常执行或陷入无休止的操作。这可能会阻止合法用户与合约交互，甚至阻止合约状态更新。在 TON 生态系统中，攻击者可能利用 DoS 漏洞恶意锁定所有资产，这将直接导致项目方和用户的资金损失。这不仅会影响项目的正常运营，还会损害用户的信任。

(6) 钓鱼攻击

描述：钓鱼攻击是一种社会工程学攻击，攻击者通过伪装成可信赖的实体，诱骗用户提供敏感信息如用户名、密码或私钥。在 TON 生态系统中，钓鱼攻击者可能会伪装成官方渠道或合作伙伴，发送欺诈性邮件或消息，诱骗用户点击恶意链接或提供个人信息。

这些攻击类型不仅揭示了 TON 生态系统在安全性方面的挑战，也强调了加强安全措施和提高用户警惕性的重要性。

其中受影响的项目类型包括 Lanuchpad、Staking、Dex、Lending、Gaming，这些事件不仅暴露了各个项目的脆弱性，也为整个生态系统的安全性提出了严峻的挑战。以下是具体的安全事件、漏洞盘点。

4.2.2 安全漏洞盘点

1. 某协议的质押合约遭受攻击，导致大量代币损失

时间： 2024年5月22日

损失金额： /

根本原因： 参数配置错误

描述：

在庆祝 TON 生态系统繁荣的质押活动后，由于协议参数配置错误，某协议的质押合约遭受了黑客攻击，导致合约中大量代币被盗。事件发生后，项目方立即暂停了质押奖励领取功能，并分配了大量 \$USDT 用于回购丢失的307,264个代币。

攻击发生后，这个项目方迅速联系了 TonBit 进行审计。TonBit 展示了其专业性，迅速反应并调集安全专家团队，对项目的核心代码进行了全面而细致的安全审计。TonBit 的安全专家们发现了6个低危问题，并立即与项目方团队进行了详细的沟通。凭借丰富的经验和专业的技术能力，TonBit 不仅提供了问题的具体解决方案，还协助该团队迅速完成了所有问题的修复工作，确保了合约的安全性和稳定性。

```
/// Set the configuration for the launcher
/// Config parameters can be changed prior to launch
receive(msg: SetLauncherConfig) {
    self.requireOwner();
    require(!self.config_validated || now() < self.config.start_time, "Already started");

    self.config = msg.config;
    let i: Int = 0;
    let total_weight: Int = 0;
    repeat (msg.config.claim_config.total_phases) {
        let phase_config: ClaimPhaseConfig = msg.config.claim_config.phase_config.get(i)!!
        total_weight = total_weight + phase_config.weight;
        i = i + 1;
    }
    self.total_claim_weight = total_weight;

    emit(LauncherConfigSetEvent{config: msg.config}.toCell());
    refund_gas();
}
```

TonBit 审计发现的和配置相关的 issue：

TLF-3 Missing Time Check

Severity: Minor

Status: Fixed

Code Location:

contracts/tonup_launcher_fixed_price.tact#331

Descriptions:

start_time and end_time are not checked in the SetLauncherConfig function.

Suggestion:

It is recommended to add a check as:

```
require(phase_config.start_time >= config.end_time, "Invalid claim start time");
```

Resolution:

This issue has been fixed. The client has adopted our suggestions.

解决方案：修改参数配置

2. 黑客利用钱包展示可控的 comment 信息误导用户

时间： 2024年5月10日

损失金额： 22,000 TON

根本原因： 钱包进行交易时展示的 comment 信息可能误导用户

描述：

在 TON 中处理 transfers 消息时，虽然可以添加注释（comment），但部分钱包在展示这些注释时的界面UI设计存在潜在误导风险。这种设计缺陷被黑客利用，通过操控 transfers 消息的注释内容，黑客能够在交易过程中向用户展示虚假信息，从而实施欺诈行为，导致用户误操作，造成资金损失。

解决方案：

为了解决这一问题，钱包应用在展示这些信息时需要添加醒目的注释，提醒用户这些内容并不可信。此外，钱包开发团队应改进UI设计，确保交易信息展示的透明度和可靠性。同时，用户也需要提高辨别能力，警惕可疑交易信息。

进一步措施：

TonBit 建议钱包开发团队在展示交易注释信息时引入多层验证机制，例如对注释信息进行源验证，确保信息的可靠性。此外，定期进行用户教育，发布安全提示，帮助用户识别和防范潜在的欺诈行为。通过技术手段和用户教育相结合，可以有效减少此类安全事件的发生。

3. BookPad 使用带有后门的合约骗取资金后携款跑路

时间： 2024年4月15日

损失金额： 74,424 TON

根本原因： BookPad 使用后门合约吸取用户资金后跑路

描述：

BookPad 发布了一份存在后门的且不开源的智能合约，开始进行预售活动。在收到了足够的资金后，他们利用合约中的后门取出资金，然后迅速携款跑路。

解决方案：

为防止类似事件再次发生，用户在参与任何项目的投资活动前，应尽可能多地搜集项目方的信息，选择那些开源且经过严格安全审计的项目。

TonBit 建议用户特别关注以下几点：

- 1.项目开源性： 确认智能合约代码是开源的，这样可以让独立的安全专家对其进行审查，确保没有隐藏的漏洞或恶意代码。
- 2.安全审计： 选择经过知名安全审计机构审核的项目。安全审计能发现并修复合约中的潜在漏洞，提供额外的保障。
- 3.项目背景调查： 调查项目方的背景、团队成员的信誉和历史记录。透明度高、信誉好的项目方更值得信赖。
- 4.社区反馈： 关注社区对项目的反馈，参与讨论，了解项目的声誉和潜在风险。

进一步措施：

TonBit 建议在 TON 生态系统中引入更加严格的监管和审核机制，对新项目进行资质审核，确保其符合安全标准。此外，可以设立一个公共的合约代码库，只有通过审核的合约才能被使用。这将大大降低用户资金被盗的风险，提升整个 TON 生态系统的安全性和可信度。

4. 黑客伪造钓鱼链接骗取资金

时间： 2024年4月26日

损失金额： /

根本原因： 黑客钓鱼攻击

描述：

黑客伪造了一个NFT项目，并利用该项目伪造了一个泰达币（USDT）的官方网站。当用户进入这个伪造的泰达币官网后，会被诱导填写敏感信息，并将所有 USDT 转移到黑客的账户。通过这种方式，黑客成功欺骗了许多用户，使他们的资金受到威胁。

解决方案：

为避免类似钓鱼攻击，用户在访问陌生网站时应采取以下措施来验证域名的真实性：

- 1.检查域名：** 确认域名的拼写和字符的准确性，注意相似但不同的字符，特别是那些恶意使用的假冒域名。
- 2.官方渠道获取链接：** 始终从官方渠道（如官方社交媒体、应用程序、公告等）获取正确的域名链接，避免通过不可靠的消息来源访问网站。
- 3.检查安全证书：** 确认网站的 SSL/TLS 证书是有效的，浏览器地址栏应显示安全锁标志。点击安全锁标志查看详细信息，确保证书由可信的认证机构颁发并与该域名匹配。
- 4.工具辅助：** 使用浏览器的反钓鱼和安全插件来识别和阻止虚假网站。利用在线工具和服务检测网站的安全性和信誉，例如通过 VirusTotal 或 PhishTank 等服务来验证网站的合法性。
- 5.教育和意识：** 提高用户的安全意识，定期进行网络安全教育，了解最新的钓鱼手段和防范措施。特别是对于新兴的NFT项目和加密货币交易平台，用户应保持警惕，避免轻信未经证实的信息。

进一步措施：

TonBit 建议在 TON 生态系统中引入更多的安全教育和防范措施，例如通过官方渠道发布安全提示和指南，帮助用户识别和避免钓鱼攻击。同时，加强对新项目和网站的审查力度，确保其合法性和安全性，为用户提供更加安全的使用环境。

5. 黑客冒充项目方在 Telegram 上大肆行骗

时间： 2024年2月4日

损失金额： /

根本原因： 黑客冒充 Ton_fish 项目方，在 Telegram 发布虚假空投信息骗取资金。

描述：

黑客冒充 Ton_fish 项目团队，在 Telegram 群组内发布虚假的空投信息，以诱骗用户参与。他们利用社会工程学手段和高度仿真的账号，设法博得用户的信任。黑客会模仿官方账号的名称、头像和发布风格，使用户误以为这些信息是真实的。受害者一旦与之互动，便有可能被引导至钓鱼网站或被要求直接转账至黑客控制的账户，最终导致资金损失。

解决方案：

为防止类似欺诈行为，用户在使用 Telegram 等社交平台时应采取以下措施来提升鉴别能力和保护资金安全：

- 1.多方渠道验证信息：** 在参与任何空投或其他活动前，用户应通过多个官方渠道（如官方网站、官方社交媒体账号、公告等）验证信息的真实性，避免仅依赖单一信息来源。
- 2.检查账号真实性：** 用户应仔细检查发布信息账号的真实性，关注账号的创建时间、发布内容和互动情况。官方账号通常有较长的创建历史和大量的粉丝关注，而假冒账号可能存在创建时间短、互动少等特征。
- 3.避免点击陌生链接：** 对于陌生或可疑的链接，用户应保持警惕，避免点击。可以使用安全浏览器插件或在线工具来检测链接的安全性。
- 4.直接与官方确认：** 在遇到任何可疑信息时，用户应直接通过官方提供的联系方式与项目方确认，避免通过不可靠的第三方渠道进行验证。
- 5.提高安全意识：** 用户应定期进行网络安全教育，了解最新的诈骗手段和防范措施。特别是在参与加密货币和区块链相关活动时，保持高度警惕，避免轻信未经证实的信息。
- 6.使用双重认证：** 为进一步保障账号安全，用户应启用 Telegram 等社交平台提供的双重认证功能，以增加账号的安全防护层。

4.3 TON 生态项目方如何做安全审计

随着 TON 生态系统中的项目数量日益增加。然而，伴随而来的安全问题也越来越多。为了确保项目的安全性，进行全面的安全审计至关重要。

安全审计的一般步骤包括：

1. 项目初期评估

了解项目背景和需求，确认审计范围和版本，熟悉协议架构，并制定详细的审计策略。

2. 自动化检测

使用静态和动态分析工具对项目代码进行全面检测，发现可能破坏合约功能或安全性的问题。

3. 人工审计

安全专家团队将对每一行代码进行细致检查，识别潜在的错误和漏洞，并和项目方保持紧密沟通，并定期反馈问题。

4. 初审报告

审计人员起草一份初审报告，总结代码缺陷和其他问题，反馈给项目方。项目方确认审计问题，对有效问题进行修改，并通知审计人员进行复审。

5. 终审报告

提交详细的审计报告，包含发现的问题和修复建议。与项目团队沟通，确保所有问题都能得到有效解决。

6. 持续监控与支持

提供链上的持续安全监控，及时发现并应对新出现的安全问题。定期进行安全审查，保持项目的长期安全性。

TonBit 拥有一支由区块链安全专家和资深开发者组成的团队，具备深厚的技术背景和丰富的实战经验。团队成员在区块链安全领域有多年的从业经历，能够精准识别并解决潜在的安全隐患。以下是 TonBit 在 TON 生态的审计流程。

Audit Activities

	Planning		Audit				Reporting
Portfolio Selection	Audit Scoping	Analysis Protocol Analysis	Code Review > Verification Initial Report Iteration				Close-out
			Static code analysis, Manual review, Construct, & Test Reviews				
Role	Scoping	Analysis	Code Review	Verification	Initial Report	Iteration	
Lead Auditors	Protocol Requirement Review; Test Case Review;	Protocol Analysis; Contract Structure Analysis; Hold meetings to discuss business architecture	Identify vulnerabilities and bugs; Code walkthrough	Vulnerability verification	Hold meetings to discuss business and resolve issues; Classification of Contract Errors:	Identify vulnerabilities and bugs; Vulnerability verification: Audit feedback	
Auditors	Auditability Evaluation; Audit effort Evaluation;	Audit Strategy Creation; Protocol Requirement Analysis; Contract Structure Analysis;	Identify vulnerabilities and bugs; Code walkthrough	Vulnerability verification	Discuss business logic Draft an initial report	Identify vulnerabilities and bugs; Vulnerability verification;	

5 用户如何在 TON 和 Telegram 上保持安全

随着 TON 和 Telegram 生态系统的迅速发展，如今已有超过3800万个活跃账户，随之而来的关注度也带来了更大的风险。骗子和恶意行为者瞄准了涌入的新手用户，即使在最安全的生态系统中，保持警惕了解潜在风险仍然至关重要。这些最常见的诈骗手段你需要多加注意。

5.1 常见的诈骗手段

1. 急需帮助的朋友：骗子冒充朋友或家人，紧急请求资金。请务必核实其身份。
2. 钓鱼网站：假冒网站模仿真实网站，窃取登录信息。核对网址，避免点击来历不明的链接。
3. 投资骗局：这些骗局在加密货币领域非常常见，承诺高回报但没有证明。深入研究；如果听起来好得不真实，可能就是骗局。
4. 假调查：提供参与调查的奖励以窃取个人信息。避免向未知调查者提供详细信息。
5. 假工作机会：吸引人的招聘广告要求提供个人信息或支付费用。通过官方渠道核实。
6. 分类广告骗局：假冒的广告引导您到虚假的 Telegram 机器人以窃取信息。
7. 拉高出货：团体操纵加密货币价格以牟利，导致其他人亏损。始终研究并核实投资建议。
8. 浪漫骗局：网络关系中，骗子要求钱财或个人信息。对在线认识的人要求钱财保持警惕。

5.2 警惕 Toncoin 金字塔骗局

Telegram 对 TON 区块链的支持不幸吸引了一些骗子，他们试图利用毫无戒心的用户。以下是该骗局的详细分析：

1. 设局：骗子发送链接到“独家赚钱计划”，看似来自朋友或联系人。他们引导用户加入一个非官方的 Telegram 机器人，谎称是用于存储加密货币。
2. 投资：用户被指示通过合法渠道（如钱包、P2P 市场或加密货币交易所）购买 Toncoin。这增加了虚假的可信度。一旦购买，用户必须将其 Toncoin 转移到诈骗机器人。
3. 加速器：受害者被迫通过一个单独的机器人购买“加速器”，费用在5到500 Toncoin之间。在此阶段，用户失去了他们的加密货币。
4. 招募：骗子推广推荐计划，要求用户创建私人 Telegram 群组并邀请朋友。他们承诺每推荐一个人可获得25 TON 的固定支付及基于推荐人购买的加速器的佣金。

实际上，这就是典型的金字塔骗局。骗子赚钱，而其他人失去投资。

5.3 如何避免网络诈骗

为了保护自己免受网络诈骗并确保 Telegram 账户的安全，请遵循以下基本步骤：

1. 启用 Telegram 的两步验证：进入“设置 > 隐私和安全 > 两步验证”，为您的账户增加额外的安全保障。
2. 验证联系人：对未经请求的消息保持警惕，尤其是要求提供个人信息或资金的消息。通过其他方式确认发件人的身份。
3. 定期检查Telegram账户活动：进入“设置 > 设备 > 活跃会话”，检查账户是否有未知设备或会话。
4. 报告可疑活动：如果遇到诈骗行为，请向 Telegram 举报。
5. 避免快速致富计划：对这些计划保持警惕，即使是朋友或家人推荐的，他们可能也是受害者。
6. 不要将加密货币转移到未知钱包：在转移加密货币之前，始终验证接收者的身份，以避免被骗。

在 TON 和 Telegram 中保持安全需要警惕和意识。通过识别常见的诈骗手段并遵循这些安全提示，您可以保护您的资产和个人信息。始终核实来源，对好得不真实的优惠保持怀疑，并仅通过官方渠道进行交易。保持信息灵通和谨慎，您便能安心享受 TON 和 Telegram 带来的好处，而不会成为欺诈的受害者！

6 TON 生态发展总结

选择 TON 的理由在于认识到Telegram本身的生态系统。在 TON 上部署你的Web3项目可以利用 Telegram 庞大的用户群，月活跃用户超过7亿。这种集成为去中心化应用的繁荣提供了肥沃的环境，类似于Apple的应用商店和 Steam 支持开发者的方式。

为了更好地理解其重要性，可以考虑以下类比：共生关系在自然界中是基础，无论是小丑鱼和海葵之间的互利关系，还是病毒的寄生关系。这些关系在塑造地球生物多样性方面至关重要，是进化的关键驱动因素。通过网络和合作，共生关系中的物种能够增强其生存能力，超越单独行动所能达到的程度。这同样适用于科技和 Web3，特别是为了繁荣，Web3生态系统必须在不同参与者之间实现共生关系。

这些技术中的共生关系促进了合作，带来了协同效应，最终使所有参与者受益，推动了 Web3 领域的进步和改进。

总体而言，开发者可以在不妥协激励或价值的情况下，受益于主要社交网络（如Telegram）的用户群，为其去中心化应用构建一个强大的未来。这种集成提供了一个理想的环境，使去中心化世界得以繁荣，强调了为什么 TON 是开发者寻求在开放网络上部署项目的战略选择。

7 关于 TonBit

TonBit 是 Web3 区块链安全审计公司 BitsLab 旗下的子品牌，专注于 TON 生态系统的安全审计与分析。作为一支专业且经验丰富的团队，TonBit 致力于确保 TON 生态系统的安全性和可靠性，为开发者和用户提供高水平的保障。

1. **TON 生态早期参与者：**从2021年开始，TonBit 成员就专注于 TON 生态系统，发起了 TONX、TONX API、Tonkey、TonResearch 等项目。



2. **全面审计：**TonBit 提供全方位的安全审计服务，包括智能合约审计、协议安全评估和代码漏洞检测等。通过全面的审计，确保项目在各个环节的安全性，防范可能的攻击和风险。

TonBit 优势包括

1. 高效审计流程：

TonBit 采用先进的审计工具和自动化技术，能够快速、高效地完成安全审计任务。在保证审计质量的同时，大幅缩短审计时间，为项目节省宝贵的开发周期。

2. 定制化解决方案：

TonBit 根据每个项目的具体需求，提供定制化的安全解决方案。从初期的设计评估到上线后的安全监控，TonBit 为项目的整个生命周期保驾护航。

3. 业界最高的安全审计标准：

为提高智能合约安全审计标准，并全方位保障审计项目代码的安全性和可靠性，BitsLab 旗下 3 个子品牌（MoveBit、ScaleBit、TonBit）将推出专门为智能合约安全审计启动的活动「Secure+」。凡参与此活动的审计项目，在完成审计（出具最终审计报告）后一个月内，若在代码未改动的前提下，由其他审计机构或自行审计发现重大问题（Major 级别及以上），TonBit 承诺将退还 30-50% 的审计费用。

TonBit 通过以下几方面护航 TON 全生态的安全

1. 预防性审计：

在项目上线前，TonBit 通过全面的安全审计，提前发现并修复潜在的安全漏洞，确保项目上线后的安全性。

2. 实时监控：

TonBit 提供7x24小时的安全监控服务，实时监控项目的运行状态，及时发现并应对安全威胁，保障项目的平稳运行。

3. 安全响应：

在发现安全问题后，TonBit 迅速响应，提供应急处理方案，帮助项目方迅速解决问题，降低安全事件带来的影响。

4. 社区协作：

TonBit 积极参与 TON 社区的安全建设，与社区成员共享安全知识和最佳实践，共同提升整个生态系统的安全水平。

TonBit 致力于为 TON 生态系统提供全面的安全保障，助力项目实现更高的安全标准和用户信任度。作为 TON 生态的安全守护者，TonBit 将继续努力，为区块链技术的发展贡献自己的力量。

Contact US



www.tonbit.xyz



[@tonbit_](https://twitter.com/tonbit_)



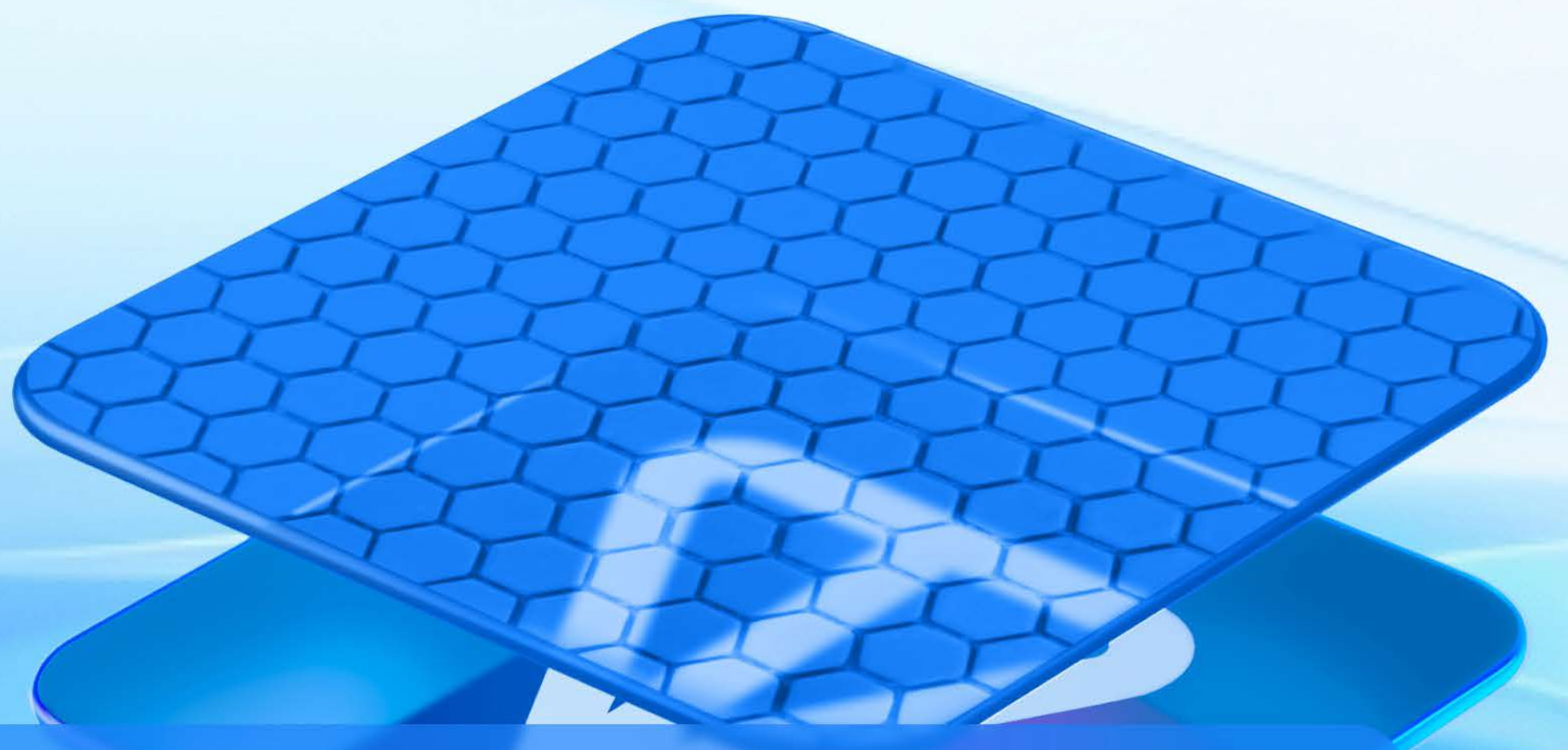
[@paul_li2024](https://t.me/paul_li2024)



[@starchou](https://t.me/starchou)



contact@bitslab.xyz



免责声明： 本报告仅为信息提供之用，不构成任何形式的投资建议、推荐或担保。读者在做出投资决策前应自行进行独立调查和分析。

数据准确性： 本报告中的数据已尽可能准确和最新，但由于市场的快速变化，某些数据可能在报告发布后发生变化。

报告局限性： 由于信息获取的限制，本报告可能无法涵盖所有安全事件和市场变化。读者应结合其他来源进行综合判断。

版权声明： 本报告的内容受版权保护，未经许可不得复制、转载或用于商业目的。

安全提示： 用户应提高自身安全意识，定期更新安全软件和防范措施，避免成为网络攻击和诈骗的受害者。

参考文献： 除了 TON 官方基金会的数据外，本报告还参考了多个来源，以确保内容的全面性和可靠性。

<https://blog.ton.org/>

<https://x.com/DegenonTON/status/1783738318850789494>

<https://x.com/DegenonTON/status/1779729268953813381>

<https://x.com/realScamSniffer/status/1788749945459318868>