

TON Ecosystem Panorama and Security Report 2024



Media Partners



CONTENTS

01	Introduction	01
02	TON Ecosystem Overview	01
	2.1 TON Introduction	01
	...	
	2.2 Why TON	02
	...	
	2.3 Trends and Targets of TON in 2024	04
03	Ecosystem Development	06
	3.1 Overview	06
	...	
	3.2 Key Metrics of the TON Ecosystem	06
	...	
	3.3 How TON Becomes a Powerful Decentralized Gaming Platform	09
04	TON Ecosystem Security Research	11
	4.1 How to Develop Securely on TON	11
	...	
	4.2 Review of Security Incidents in the TON Ecosystem	13
	...	
	4.3 How TON Ecosystem Projects Conduct Security	17
05	How Users Can Stay Safe on TON and Telegram	18
	5.1 Common Scams	18
	...	
	5.2 Beware of Toncoin Pyramid Schemes	18
	...	
	5.3 How to Avoid Online Scams	18
06	Summary of TON Ecosystem Development	19
07	About TonBit	20

This report is produced by TonBit, a sub-brand of BitsLab, the blockchain security auditing company.

With the continuous development of blockchain technology and its increasingly widespread applications, the TON ecosystem has shown strong growth momentum in 2024, attracting significant attention from developers, investors, and users alike.

In 2024, the TON ecosystem has made remarkable strides in areas such as technological innovation, application deployment, and community building, further solidifying its position within the blockchain field. However, as the ecosystem evolves rapidly, security issues have become increasingly prominent. Effectively preventing and addressing these evolving security threats has become a critical challenge for the TON ecosystem.

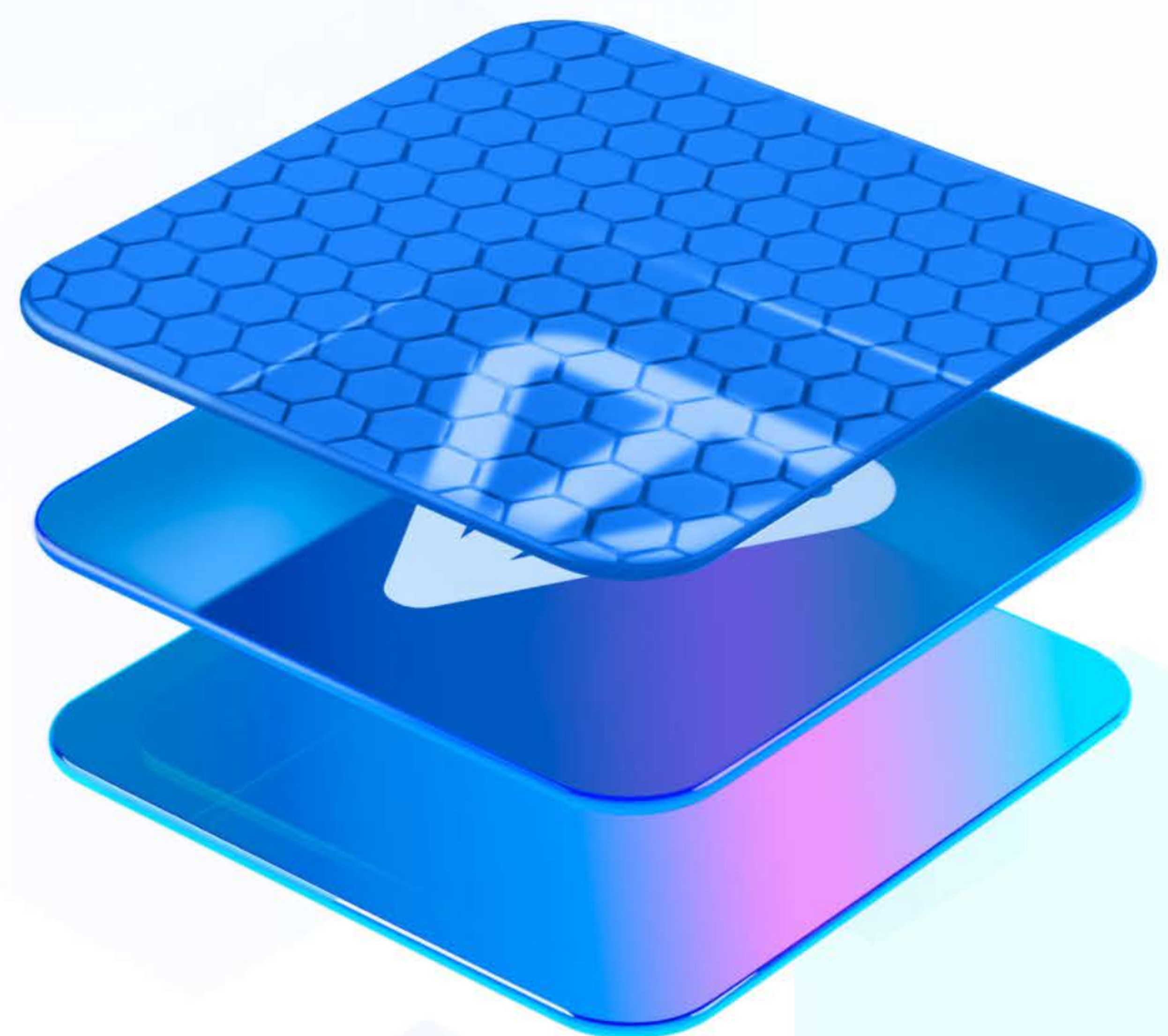
Since 2021, TonBit team members have been deeply engaged with the TON ecosystem, initiating projects such as TONX, TONX API, TonKey, and Ton Research. This report provides a comprehensive review of the TON ecosystem's development, summarizing the major security incidents over the past six months, analyzing their causes and impacts, and proposing corresponding preventive measures and recommendations for future improvements.

We hope this report serves as a valuable reference for participants in the TON ecosystem, promoting the ecosystem's healthy development and heightening awareness of blockchain security. [We extend our gratitude to all partners who support and contribute to the TON ecosystem's growth. Together, let us strive to build a more secure, transparent, and prosperous blockchain ecosystem.](#)

2.1 TON Introduction

Brief Introduction and Framework

TON (The Open Network) is a blockchain and digital communication protocol created by Telegram. It aims to build a fast, secure, and scalable blockchain platform that provides users with decentralized applications and services. By integrating blockchain technology with Telegram's communication features, TON achieves high performance, robust security, and strong scalability. It supports developers in building various decentralized applications and offers distributed storage solutions. Compared to traditional blockchain platforms, TON delivers faster processing speeds and higher throughput, employing a Proof-of-Stake consensus mechanism. As an innovative and promising blockchain platform, TON is driving the advancement of cryptocurrencies and decentralized applications.



2.2 Why TON

Despite the significant liquidity and strong community support of Bitcoin and Ethereum, they still have their own issues. This is why there is a need for newer blockchains and ecosystems to address these problems.

The blockchain trilemma, introduced by Vitalik Buterin, describes the challenges Layer 1 networks face in simultaneously balancing security, scalability, and efficiency. For example, Bitcoin provides robust security and greater decentralization through Proof-of-Work (PoW), but its transaction speed is slow, and gas fees are high. Although Ethereum has transitioned to Proof-of-Stake (PoS) and supports more Layer 2 solutions like Optimism and Arbitrum, it still faces high gas fees during periods of network congestion.

In short, almost no chain (whether Layer 1s or Layer 2s) is currently capable of competing with traditional banks and financial institutions in its present state, let alone gaining an edge in balancing practical incentives such as privacy and security.



2.2.1 Flexible and Sharded PoS Architecture

Like Solana and Ethereum, TON employs a Proof-of-Stake consensus mechanism. However, TON's key designs and implementations set it apart, enhancing its performance and versatility. An example of this is its Turing-complete smart contracts and its asynchronous blockchain, which introduces concepts like Lamport timestamps and unconventional ordering schemes.

TON's lightning-fast and low-cost transactions are supported by its flexible and sharded architecture, enabling easy scalability without sacrificing performance. Dynamic sharding involves the development of separate shards with specific functions that can operate concurrently to prevent large-scale backlogs. TON's block time is set at 5 seconds, achieving finality in less than 6 seconds.

The existing infrastructure is divided into two main components:

Masterchain

The Masterchain is responsible for processing all important and critical data of the protocol, including parameters and their current values. This encompasses the addresses of validators and the amount of tokens they have staked. Moreover, it holds data from various workchains and shard chains. In a multi-layered blockchain architecture, the Masterchain is paramount and acts as the single source of truth.

Workchain

The Workchain is a secondary chain connected to the Masterchain. It houses all transaction data and records of various smart contracts. Each Workchain can operate under distinct rules, which means it may support addresses in different formats, diverse transaction structures, and unique virtual machines (VMs) for specific smart contracts. Due to these characteristics, the TON blockchain is described as a heterogeneous blockchain.

2.2.2 Scalability Examples and Advantages

The TON Foundation is a DAO managed by the core TON community, providing various forms of support to projects within the TON ecosystem. This support includes facilitating developer engagement through events and hackathons, as well as offering liquidity incentive programs for DeFi projects.

According to recent developer reports, the number of active developers has increased by 8% monthly, and the annual growth rate of contributors to open-source TON-related repositories on GitHub has reached 50%. This growth signifies a strengthening community that promotes collaboration and innovation.

(1) Launch of TON Connect 2.0

The release of TON Connect 2.0 marks a significant milestone by offering users an intuitive method to link their preferred wallets and applications. Supported by the Tonkeeper wallet and OpenMask, it has been adopted by more than 14 services, collectively enhancing the user experience.

(2) Enhancing Trust and Reliability with TON Verifier

Created by the Orbs team, TON Verifier is a smart contract checker now available to community members. It enables developers to verify the integrity of their contracts before deployment.

(3) Blueprint—An Ally for Developers

TON has launched Blueprint, a tool specifically designed to assist developers in writing, testing, and deploying smart contracts within a simplified environment. Blueprint streamlines the entire process, facilitating easier development on the TON platform.

(4) Sandbox Developer Toolkit

This latest toolkit enhances TON's capabilities, accommodating a broad spectrum of use cases from enterprises to governments. The Sandbox toolkit enables mainstream smart contract development, paving the way for wider adoption.

(5) Tact Language Beta—Embracing the Future

Supported by Steve Korshakov and the Tact community, the Tact programming language has successfully launched its Beta version. Its concise documentation encourages community learning and feedback, thereby fostering a more robust programming environment.

(6) Developer Engagement and Support

In partnership with DoraHacks, the TON Foundation has launched a three-month online hackathon featuring a prize pool of up to \$300,000. Additionally, TON has organized a DoraHacks Onboarding Week to encourage participants to engage in learning through live sessions.

(7) TON Hubs in Global

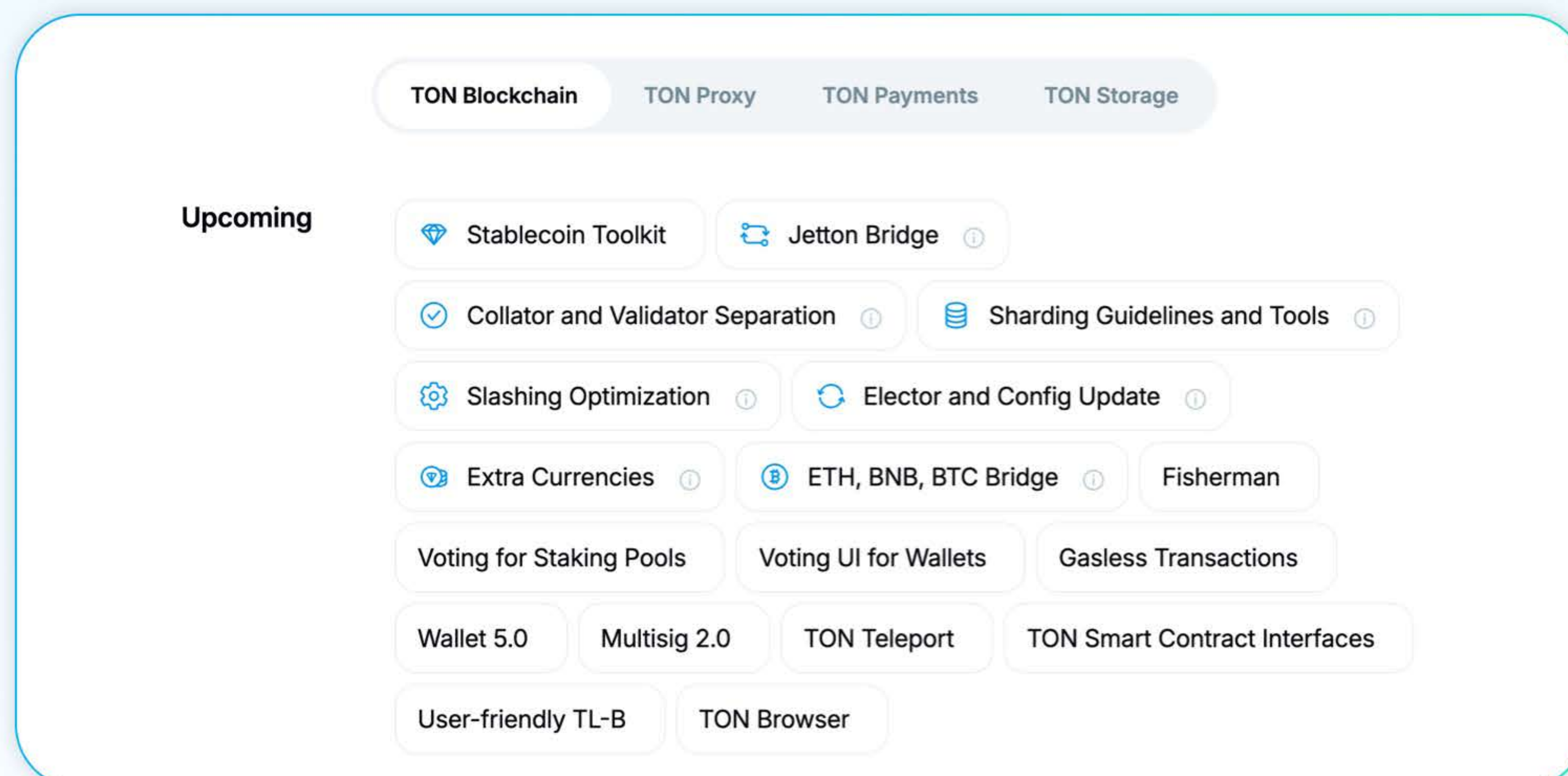
The TON community has established international hubs in Lisbon, Bangkok, Hyderabad (India), and Barcelona. These centers facilitate the sharing of ideas and accelerate project development. Additional hubs are anticipated worldwide, inviting individuals to participate in this exciting initiative.

(8) DeFi Liquidity Incentive Program

This progressive, milestone-based program funds projects and aims to foster organic sustainability within the DeFi sector of the TON ecosystem.

2.3 Trends and Targets of TON in 2024

The development roadmap for TON includes many exciting initiatives, such as a stablecoin toolkit, sharding tools, and native bridges for BTC, ETH, and BNB.



Gas-Free Transactions

As no other major blockchain offers gas-free transactions, TON has the potential to revolutionize the blockchain industry and draw users from other ecosystems. TON may subsidize gas fees in specific scenarios, such as transactions through Telegram wallets or USDT transfers, to encourage more widespread use of TON for everyday needs.

Separation of Validation Nodes and Block Production Nodes

This represents a significant upgrade to TON's scalability. Block production involves collecting transactions, validating them, and then packaging them into blocks. This process requires nodes to store and continuously monitor the entire network state—the balances of all addresses within the TON blockchain.

TON plans to onboard 500 million Telegram users by 2028, utilizing sharding to ensure sufficient transaction execution times and low fees. Sharding divides the blockchain into multiple shard chains, where each additional shard chain doubles the throughput capacity. For example, two shard chains offer double the throughput, four shard chains quadruple it, and so forth.

Each shard chain will have its designated subset of validation nodes responsible for both block production and validation. To ensure security, these validation nodes must frequently rotate subsets. However, the challenge arises in that with random rotations, validation nodes would need to store the state of every shard, not just their own. Storing the state of 1 million accounts requires a powerful server, making it impractical to store the state of 500 million accounts in one location.

To solve this, the TON team has proposed separating validation and block production into two distinct roles: block production nodes will only store the state of their assigned shard chain and produce blocks, while validation nodes assigned to the same shard chain will only validate and sign blocks for a specific period. This division allows for an even distribution of load and risks, enabling TON to scale up to support billions of users.

Official documentation does not address staking rewards. While only validation nodes face risks during block validation, block production nodes should also receive rewards for storing state information and generating blocks.

Despite the increased complexity of the validation process, the Annual Percentage Yield (APY) for TON staking will not change, and the liquidity staking provided by Tonstakers will continue to yield high returns.

Sharding Guidelines and Tools

TON aims to be among the first blockchains to efficiently harness sharding technology, thanks to its outstanding development team. Centralized exchanges, payment systems, and even TON's services and applications will require specialized tools and documentation to implement sharding support, as this technology is still unfamiliar to many. Consequently, the TON development team plans to release these essential resources in the near future. Penalty Mechanism Optimization

Optimization of the Penalty Mechanism

The penalty mechanism is established to sanction underperforming validation nodes for issues such as missing blocks, frequent downtime, or attempts to insert fraudulent transactions into the blockchain.

Currently, TON employs a complaint mechanism to discipline misbehaving validation nodes. Any network participant can file a complaint with evidence to hold these nodes accountable.

The enhancement of the penalty mechanism will introduce a more effective system to detect and penalize misbehaving validation nodes, thus improving TON's robustness. This implementation will occur in stages: Initially, the liquid staking protocol will be shielded from the impacts of validation penalties, safeguarding users' rewards. Subsequently, penalties will be applied to the TON allocated by the liquid staking protocol, slightly decreasing the average annual percentage yield (APY).

Elector and Configuration Contract Updates

TON staking, liquid staking, and on-chain governance are facilitated through smart contracts. Tonstakers utilize these contracts to pool TON, supply it to validation nodes, and allocate rewards among users.

The updates to the elector and configuration contracts will allow users to vote on network proposals, thereby enhancing the openness of the network and increasing the value for each participant.

TON Stablecoin Toolkit

The Stablecoin Toolkit enables anyone to issue algorithmic stablecoins pegged to local fiat currencies, including the British pound, euro, and New Zealand dollar.

Considering TON's integration with Telegram, its built-in wallet, and the recent decision to share advertising revenue with channel owners, it is plausible that Telegram might introduce a native stablecoin payment feature within its built-in services.

Jetton Bridge

TON already features bridges to Ethereum and BNB Chain, enabling the transfer of \$TON and popular tokens like ETH, BNB, and USDC. The Jetton Bridge will further enhance this capability by allowing users to send TON tokens (such as tsTON) to other chains.

ETH, BNB, and BTC Bridge

Although third-party bridges are available, launching an official bridge to facilitate the integration of major cryptocurrencies like ETH, BNB, and BTC into TON seems logical, especially considering the potential for issuing them as additional currencies on the platform.

Additional Currencies

\$TON is the native token used for staking and paying Gas fees. Its code, including the function for transacting \$TON, is embedded within the TON protocol, and balances are stored in accounts.

Jettons, such as USDT and tsTON, are managed by third-party smart contracts and cannot substitute \$TON for paying fees or staking. User balances are held within these contracts.

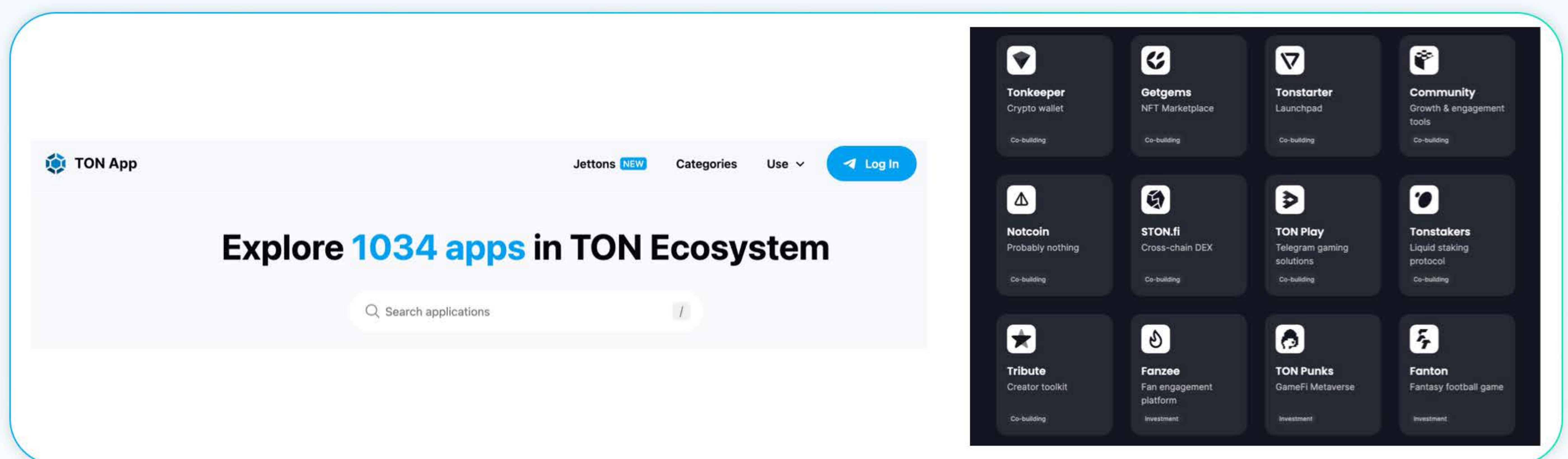
Additional currencies will enable TON users to create tokens similar to native tokens, with these also stored in user accounts. The key advantage of additional currencies over Jettons is that transactions will likely be 2–3 times cheaper, as they do not involve contract calls.

Issuing major tokens like bridged BTC and ETH, or a native USDT as additional currencies, will provide TON with a competitive advantage in managing these tokens and attract more new users to the platform. Looking to buy BTC, ETH, and BNB? TON will consolidate them all in one location.

3 Ecosystem Development

3.1 Overview

The TON Foundation's official website currently features nearly 1,000 applications, encompassing areas from decentralized finance (DeFi) to gaming, social media, and utility apps, illustrating the diversity and dynamism of the TON ecosystem. Through these projects, the TON Foundation not only underscores its leadership in blockchain technology but also its dedication to driving innovation and fostering ecosystem growth. These initiatives receive financial backing and technical guidance from the TON Foundation, offering developers essential resources and a platform to realize their creative and commercial aspirations on the TON blockchain. This holistic approach to support and investment has fueled the continual expansion of the TON ecosystem, drawing an increasing number of developers and users, and establishing a solid foundation for future advancements.



3.2 Key Metrics of the TON Ecosystem

As of July 27th, there are 383 validation nodes on the TON blockchain. Under the Proof-of-Stake (PoS) mechanism, over 590 million \$TON are staked across 29 countries.

Validators

Count of validators ⓘ
383

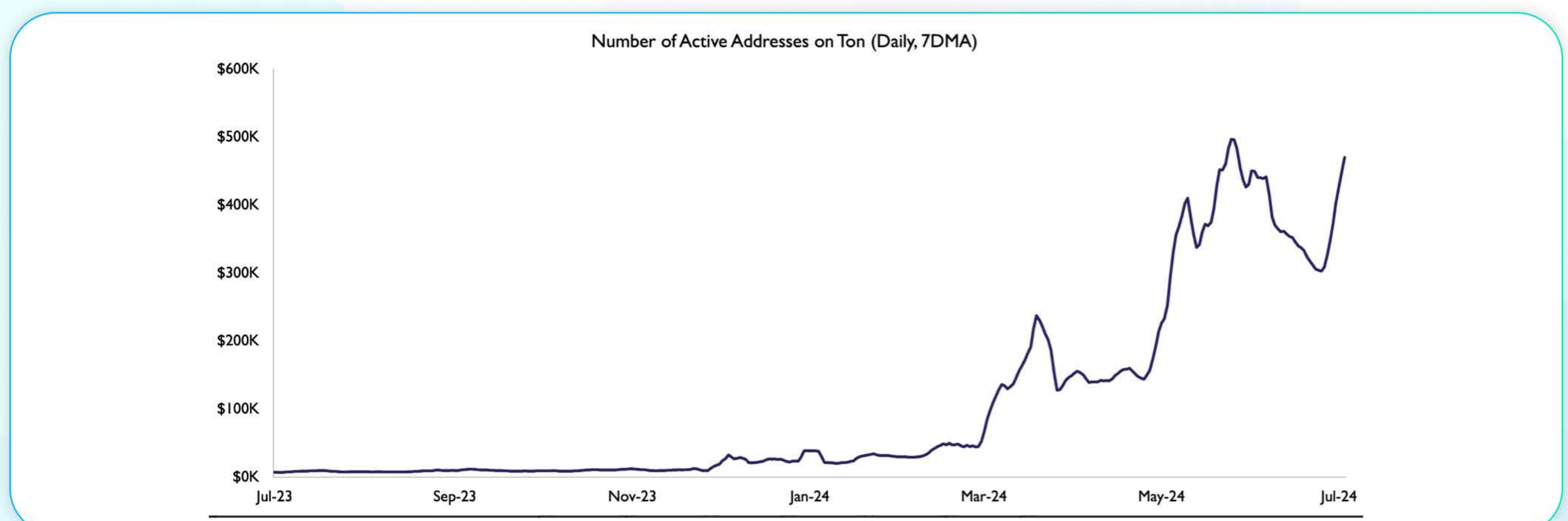
+6 ↗

Staked, TON ⓘ
598,610,551

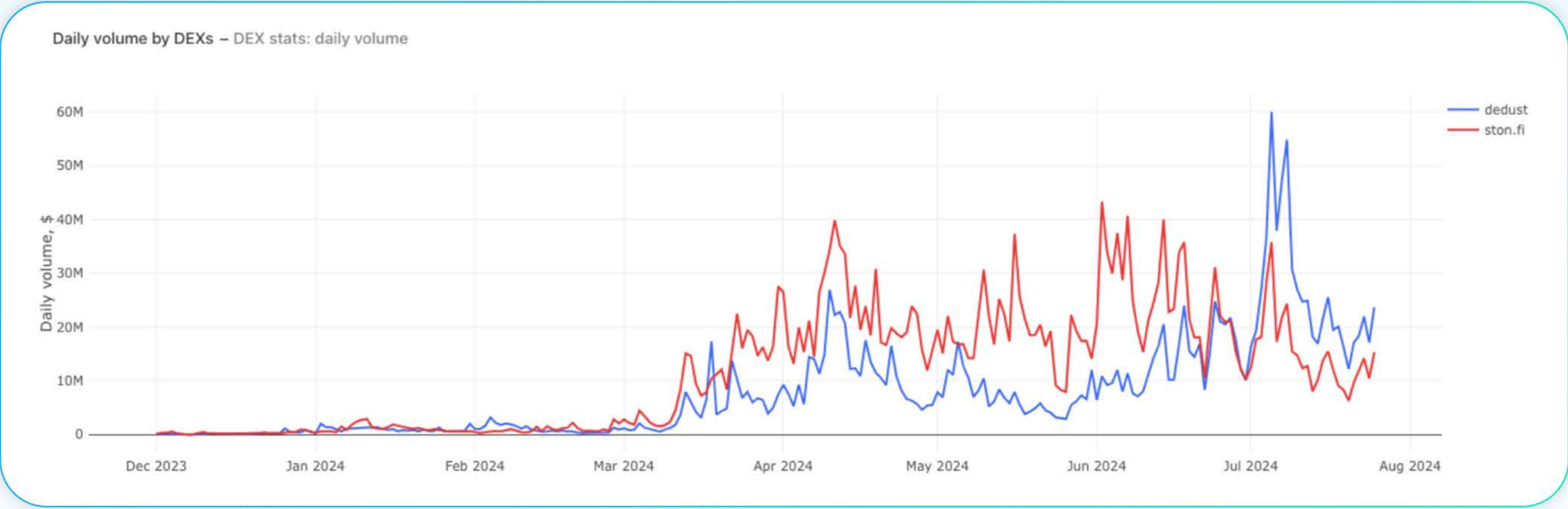
+2.02% ↗

Countries ⓘ
29

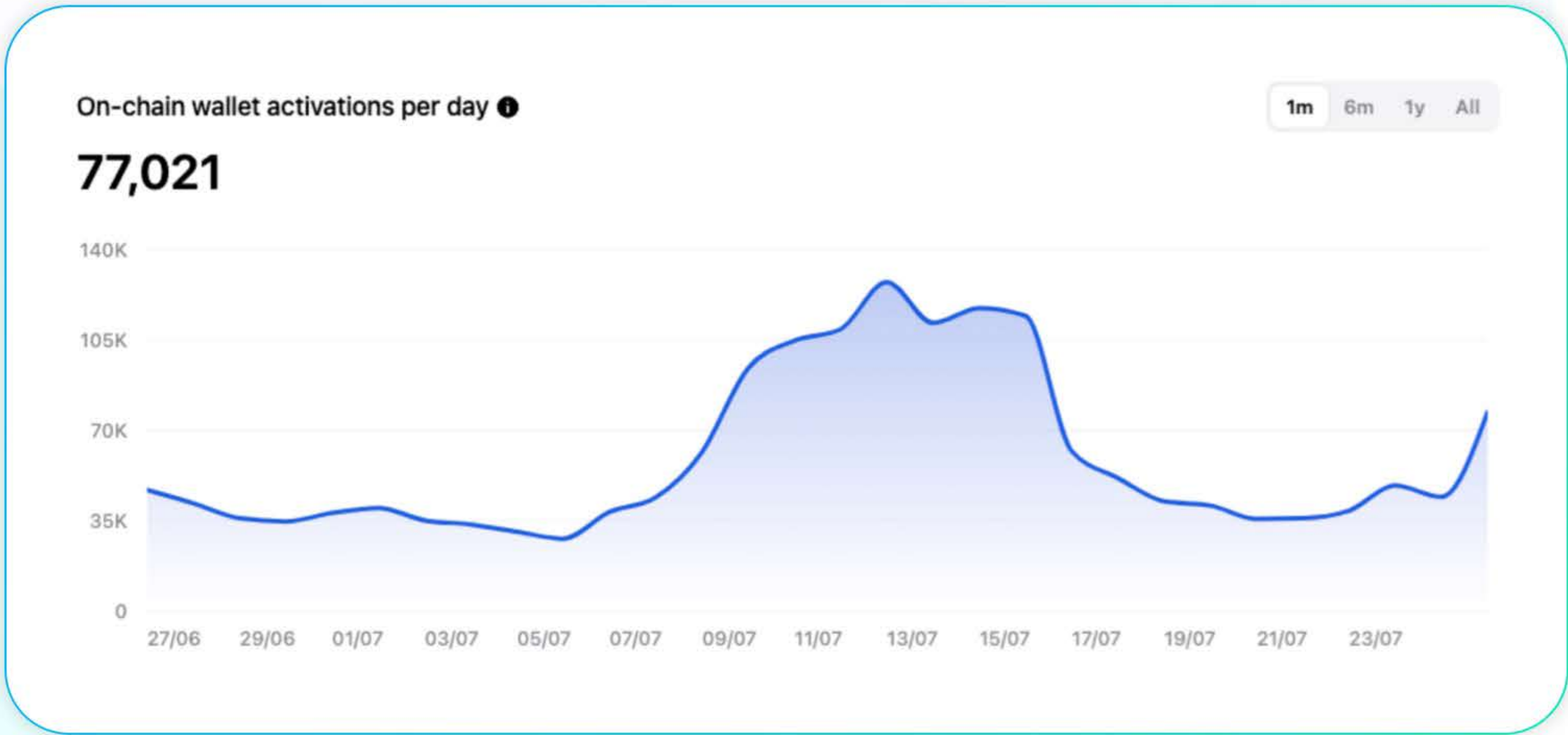
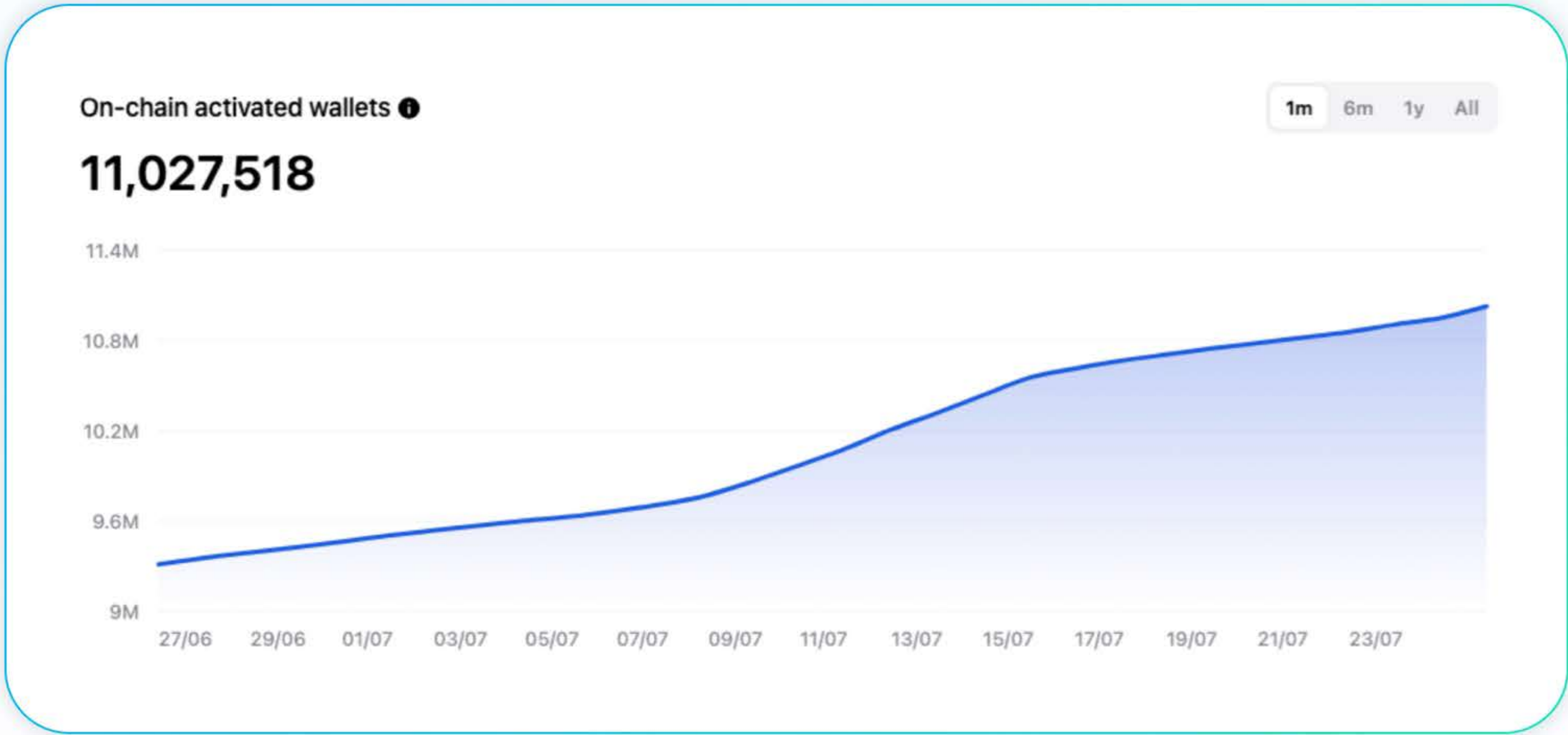
As of mid-July, the TON network boasts 373,000 daily active addresses, marking a year-over-year increase of 5,360%. This remarkable growth underscores the growing popularity and accelerated adoption of the TON blockchain among users.

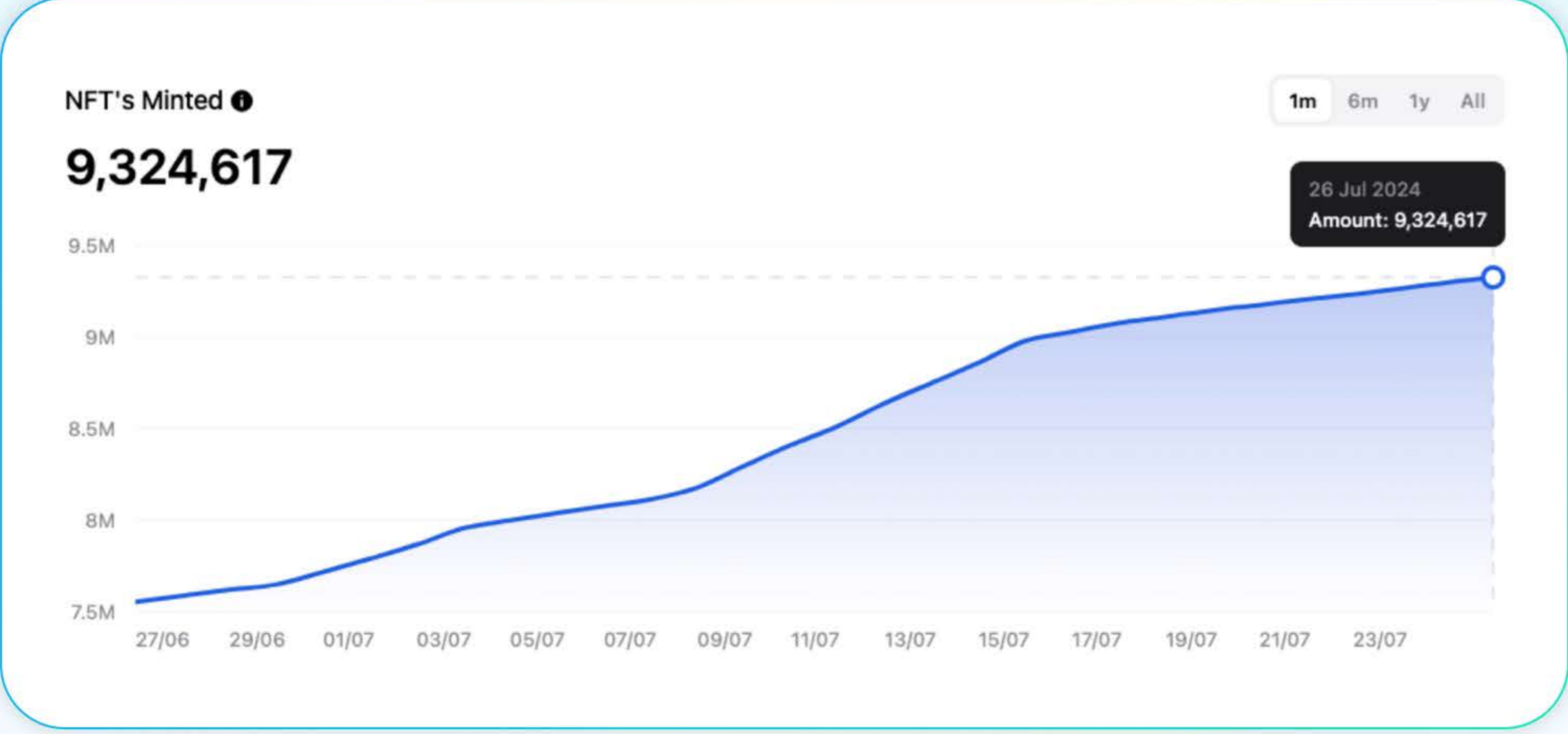


The DeFi ecosystem on the TON network is showing strong growth and a wide user base. Key metrics indicate that the number of unique users has reached 1,784,089, demonstrating active engagement with DeFi services on the TON network. Furthermore, the total value locked (TVL) has surged to \$706,307,873, a testament not only to users' trust and confidence in TON's DeFi ecosystem but also to its prominent role in the blockchain finance sector. The number of liquidity providers has increased to 26,297, further evidencing TON network's effectiveness in attracting investment and enhancing liquidity.

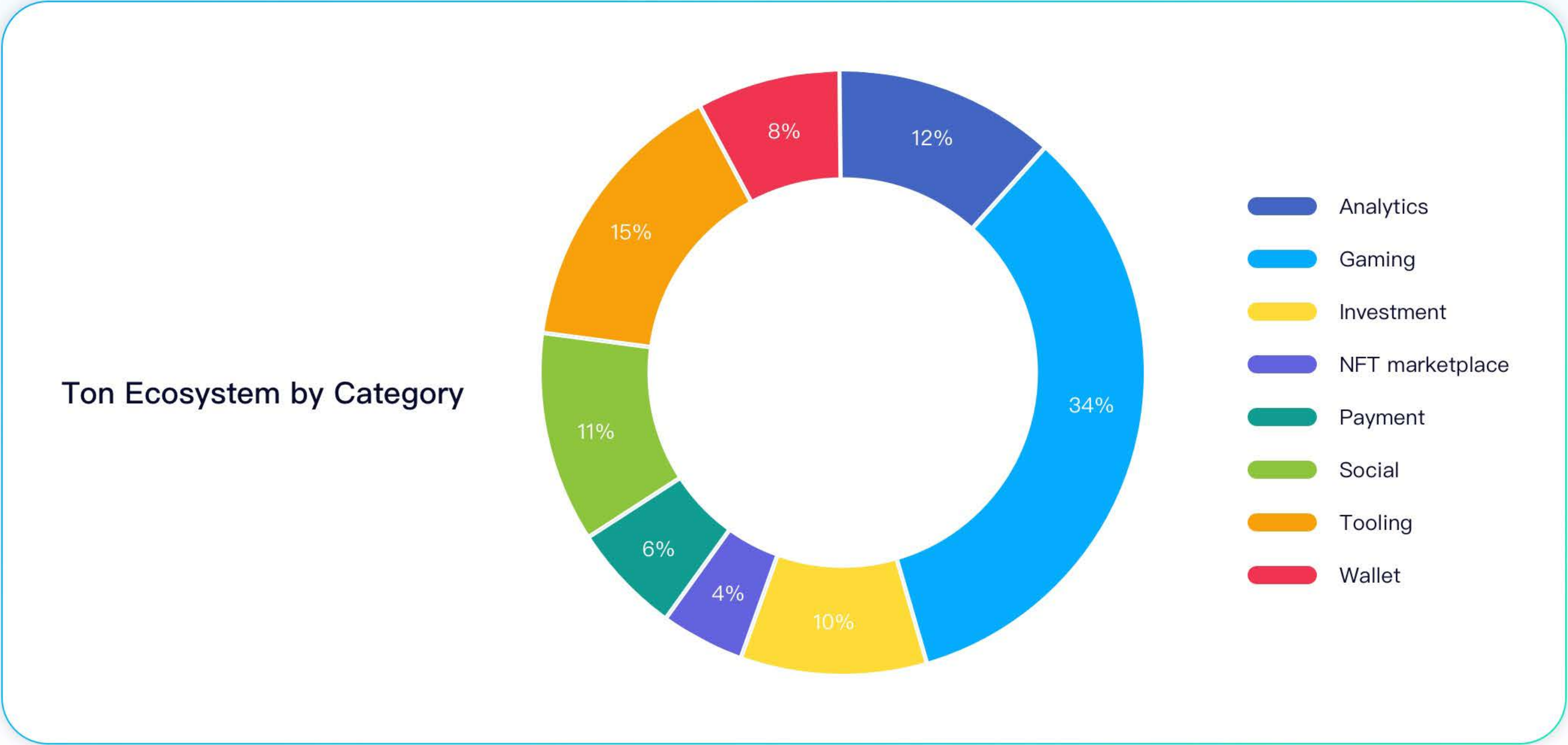


As of July 27th, the TON network has reached 11,027,518 active on-chain wallets, demonstrating its broad appeal and consistent growth in user base. Additionally, the daily activation of on-chain wallets has reached 77,021, signifying robust participation from both new and existing users. Moreover, the number of NFTs minted has climbed to 9,324,617, illustrating the vibrant development of the TON ecosystem in digital asset creation and transactions. Together, these metrics underscore the strong vitality of the TON network and its ever-expanding ecosystem within the blockchain industry.





According to statistics from The Block in mid-July, over half of the projects on TON are developed as bots on Telegram, underscoring the deep integration between TON and the social platform. This integration furnishes developers with a convenient development environment and access to a vast user base, making it an optimal platform for both project creation and promotion.



The primary categories of major projects within the TON ecosystem include gaming and investment (particularly various financial applications), showcasing the diverse interests of the community. Gaming projects harness TON's high-speed transaction processing and low fees to offer players a seamless gaming experience and a robust in-game economy. Meanwhile, investment projects utilize TON's decentralized features and security, attracting a large number of investors and developers of financial applications.

The continual expansion of the TON ecosystem not only underscores its technical prowess and potential as a platform but also its wide applicability across different application scenarios. As more developers and users join, TON is well-positioned to drive further innovations in blockchain technology and assume an increasingly vital role in the digital economy of the future.

3.3 How TON Becomes a Powerful Decentralized Gaming Platform

3.3.1 Key Reasons for Building Decentralized Games Based on TON

Developing decentralized games on the TON blockchain offers a range of advantages for businesses and developers, aiming to reshape the gaming industry's landscape.

Here are the key reasons why TON is emerging as the preferred platform for decentralized gaming:

Integration with Telegram

The integration of TON with Telegram offers developers access to over 900 million monthly active users, enabling games to be launched quickly and effortlessly directly on Telegram. This stands in stark contrast to traditional app stores, where users typically navigate multiple steps such as downloading and authorization. TON-based games on Telegram allow users to start playing instantly by simply opening a bot or via the Telegram app center.

Powerful User Acquisition and Retention Tools

By leveraging TON and Telegram, developers gain access to a suite of comprehensive tools designed to boost user retention and enhance the in-game experience. These tools include:

- **Telegram App Center:** A one-stop destination for apps, utilities, and games, all integrated within the Telegram ecosystem.
- **Telegram Advertising:** Enables targeted advertising campaigns across almost any Telegram channel, reaching millions of users.
- **In-Messenger Notifications:** Notifications sent directly within Telegram, which typically achieve higher engagement rates compared to traditional in-game push notifications.

These tools are specifically designed to foster active player engagement within the gaming environment, helping developers maintain a vibrant user community.

Fast and Efficient Blockchain

TON is renowned for its exceptional speed, capable of processing over 100,000 transactions per second while maintaining low transaction fees. These characteristics are vital for sustaining the performance and scalability of decentralized games, especially critical in managing high-throughput player interactions.

Diverse Monetization Opportunities

TON provides developers with a variety of monetization strategies, from in-app advertising and integrating tradable and sellable NFTs, to the creation of in-game economies that mirror real-world economic principles. These options open up multiple revenue streams for developers and bolster the financial viability of gaming projects.

Simple and Accessible

TON is a user-friendly and accessible blockchain, essential for widespread adoption in the gaming industry. For GameFi Web3 developers and players, TON offers a comprehensive suite of tools, making it the perfect choice for those looking to transition to the decentralized gaming world.

3.3.2 Use Cases of TON in Decentralized Gaming

The TON blockchain is rapidly developing into a dynamic decentralized gaming ecosystem. Here are some of the most popular examples that are shaping the TON gaming experience:

- Notcoin: A click-to-earn game where players earn tokens by clicking.
- Catizen: An airdrop-to-earn game where players breed cats to earn \$CATS tokens.
- Fanton Fantasy Football: A play-to-earn game where players manage a football team and earn rewards.

(1) Notcoin

Notcoin is a straightforward and engaging click-to-earn game that quickly became popular on Telegram, thanks to its easy-to-understand gameplay and enjoyable mechanics. Players earn tokens by clicking, and their achievements are recorded on a league leaderboard. They can also join Telegram channels and chat groups to complete various tasks and climb the rankings.

(2) Catizen

Catizen is a captivating airdrop-to-earn game that incorporates elements of the metaverse, GameFi, and AI. Players breed cats by dragging and dropping them together, enhancing their levels and earning \$CATS tokens. Additionally, players can fish to earn fish coins, which are used for various in-game enhancements and upgrades.

In Catizen, players can purchase items to speed up cat breeding, acquire new cats, and improve the overall experience. The game's store allows purchases with \$CATS and fish coins, which can be bought using TON.

As players collect more tokens, they progress through the leagues—from bronze to silver, gold, platinum, and diamond—reflecting their growing achievements.

(3) Fanton Fantasy Football

Fanton Fantasy Football is the first play-to-earn game integrated with Telegram. In this game, players assemble a team consisting of five football players: a goalkeeper, defender, midfielder, forward, and a substitute. Their real-life performance in actual football matches determines the points they accumulate in the game.

Players earn points for various on-field actions such as scoring goals, providing assists, making saves, and other pivotal contributions. The players accumulating the highest points stand a chance to win valuable rewards, including cryptocurrencies and NFTs, making every match thrilling and potentially lucrative.

TON's seamless integration with Telegram greatly simplifies the process of game publishing, making it easier than ever before. Coupled with its advanced tools for user acquisition and retention, TON enables developers to create engaging and profitable decentralized gaming experiences. However, it is crucial to also consider and address security risks when developing such projects.

4 TON Ecosystem Security Research

4.1 How to Develop Securely on TON

To ensure the security of smart contracts on TON, a series of security measures should be implemented. Below are some key security practices within the TON ecosystem:

(1) Access Control

When a contract contains critical logic or sensitive operations that should only be executed by specifically authorized users, it is crucial to implement robust access control. This prevents attackers from carrying out sensitive operations and causing significant damage.

Practices:

- Identify operations that need permission controls.
- Restrict access to operations requiring permissions by verifying the sender of the message.
- Regularly review and update access control policies to keep pace with changes in the contract's requirements.

Please refer to the following proposals:

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

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

(2) Message Input Validation

Inadequate validation or filtering of external inputs in smart contracts can allow malicious data entry by attackers, potentially leading to unsafe behaviors or vulnerabilities.

Practices

- Rigorously validate and filter all external inputs, which includes verifying data types, checking boundary conditions, and sanitizing user inputs.
- Consider all possible input scenarios, including edge cases and unexpected inputs.
- Regularly audit and test the input validation logic.

(3) Check Gas usage

In smart contracts, the sender typically pays the gas fees for internal messages, while the contract itself covers the gas costs for external messages. This necessitates careful management of gas usage, especially in external messages. Continuously testing the gas usage of contracts is crucial to ensure that everything functions as intended and to prevent vulnerabilities that could exhaust the contract's balance.

Practices:

- Monitor and optimize gas usage throughout the development process.
- Implement gas limits to prevent operations that consume excessive amounts of gas.
- Regularly test the contract's gas consumption under various scenarios.

(4) Timestamp Dependency

Some smart contracts rely on block timestamps to dictate their behavior. However, these timestamps can be manipulated by validators. For instance, validators may selectively include or exclude certain transactions, or they might adjust timestamps to achieve specific outcomes. Such manipulations can compromise the integrity of contract logic, introducing security risks.

Practices:

- Avoid relying directly on block timestamps for critical decision-making in contract logic.
- If timestamps are necessary, ensure they are applied in a manner that is reliable and less susceptible to manipulation.

- Implement time buffering mechanisms that allow for variations within a specified range, thus reducing dependence on precise timestamp values.
- Conduct regular reviews of contract logic to ensure it is not vulnerable to timestamp manipulation.

(5) Integer Overflow and Underflow

Integer overflow and underflow occur when the results of arithmetic operations exceed the storage capacity of a variable, leading to incorrect outcomes. These issues are common in operations like addition, subtraction, and multiplication. Without proper checks, they can lead to significant security vulnerabilities, such as miscalculating balances or unintended fund transfers.

Practices:

- Utilize safe math libraries for all integer operations to prevent overflow and underflow.
- Implement checks for overflow and underflow before and after each arithmetic operation.
- Conduct regular audits of contract code to ensure all integer operations are securely managed.

(6) Rounding Errors

Rounding errors are discrepancies in calculation outcomes caused by limitations in numerical precision or improper rounding techniques. These errors are especially critical in financial contexts or when dealing with high-precision values, where they can lead to financial losses or unfair allocations.

Practices:

- Utilize high-precision numerical libraries or fixed-point libraries for currency-related calculations.
- Conduct regular testing and verification of the numerical computation logic to ensure the accuracy aligns with expectations.
- Clearly define and consistently apply rounding methods in the code to maintain consistency.

(7) Denial of Service (DoS)

Denial of Service risks involve depleting a smart contract's computational resources or triggering error states, rendering the contract unable to execute properly or trapping it in infinite loops. Such situations can prevent legitimate users from interacting with the contract or even halt updates to the contract's state.

Practices:

- Limit loop counts or recursion depths to prevent long-running operations that can lead to DoS.
- Monitor remaining Gas before executing critical operations to avoid transaction failures due to insufficient Gas.
- Regularly review and optimize contract logic to ensure both efficiency and reliability.
- Implement event logs to document significant actions, aiding in troubleshooting and recovery efforts.

(8) Business Logic

Business logic vulnerabilities are design flaws or implementation errors within a smart contract's business processes that cause abnormal behavior under certain conditions. These vulnerabilities can be exploited by malicious actors, leading to financial losses, data tampering, or contract malfunctions. Unlike coding errors, business logic vulnerabilities typically arise from misunderstandings or incomplete implementations of business requirements.

Practices:

- Thoroughly understand and analyze business requirements to ensure the logic design is accurate.
- Conduct regular code audits and logic validations to promptly identify and address vulnerabilities.
- Develop comprehensive test cases that cover all conceivable business scenarios.

By adhering to these security practices, we can significantly enhance the security of smart contracts, minimize risks, and ensure the stable operation of contracts and the safety of user funds.

4.2 Review of Security Incidents in the TON Ecosystem

In 2024, multiple security incidents unfolded within the TON ecosystem, underscoring existing security challenges. Below, we provide a detailed description of several key incidents, analyzing their causes, impacts, and resolutions. Additionally, we inventory some of the more common security vulnerabilities observed during these events.

4.2.1 Common Attack Types

Throughout 2024, the TON ecosystem experienced several significant security incidents that adversely affected both projects and users, highlighting some inherent vulnerabilities in blockchain security. Below is a list of common attack types, along with their brief descriptions:

(1) Incorrect Input Validation

Input validation is the process of verifying the integrity, accuracy, and security of input data. Incorrect input validation occurs when smart contracts fail to adequately validate and sanitize user inputs, leaving them vulnerable to various types of attacks. Such vulnerabilities can be exploited to manipulate contract logic, inject malicious data, or cause unintended behaviors. Proper input validation ensures that contracts process only valid and intended data, thereby minimizing the risk of exploitation.

(2) Computation Errors

Computation errors occur when there are mistakes in executing certain calculations, resulting in unintended behaviors or vulnerabilities. These errors often stem from logical or programming errors in the smart contract code. Attackers can exploit these flaws to manipulate outcomes or gain undue advantages within the contract.

(3) Oracle/Price Manipulation

Price manipulation refers to scenarios where attackers artificially influence market prices to derive illicit profits. In the TON ecosystem, attackers may manipulate trading volumes or order books on decentralized exchanges (DEXs) to affect the prices of specific tokens, resulting in profits or triggering market panic. Additionally, attackers could tamper with the data reported by oracles, such as the prices of digital assets or other external information, leading smart contracts to make incorrect decisions.

(4) Weak Access Control

Weak access control occurs when a system fails to adequately restrict user access to resources or operations, thereby allowing unauthorized individuals to carry out sensitive actions. In the TON ecosystem, this vulnerability could enable unauthorized access to administrative interfaces, alteration of smart contract settings, or theft of user assets.

(5) Denial of Service (DoS) Attacks

Denial of Service (DoS) attacks drain the computational resources of a smart contract or trigger error conditions, rendering the contract unable to execute properly or causing it to loop indefinitely. This can inhibit legitimate users from interacting with the contract and might even prevent updates to the contract's state. In the TON ecosystem, attackers could exploit DoS vulnerabilities to maliciously lock up all assets, leading to direct financial losses for both project operators and users. Such actions not only disrupt the normal operation of projects but also undermine user trust.

(6) Phishing Attacks

Phishing attacks are a type of social engineering tactic where attackers impersonate trusted entities to trick users into divulging sensitive information, such as usernames, passwords, or private keys. In the TON ecosystem, these attackers might pose as official channels or partners, dispatching fraudulent emails or messages to coax users into clicking malicious links or surrendering personal details.

These incidents not only highlight the security challenges within the TON ecosystem but also emphasize the critical need for enhanced security measures and heightened user vigilance.

Affected project types include Launchpads, Staking platforms, Decentralized Exchanges (DEXs), Lending platforms, and Gaming platforms, among others. These attacks have exposed vulnerabilities within these projects and presented formidable challenges to the overall security of the ecosystem. Below, we provide a detailed review of specific security incidents and a rundown of the vulnerabilities identified.

4.2.2 Security Vulnerability Review

1. Attack on Staking Contract of a Protocol Leading to Significant Token Loss

Date: May 22, 2024

Loss Amount: Not specified

Root Cause: Misconfiguration of Parameters

Description:

In the wake of a celebratory staking event within the TON ecosystem, a protocol's staking contract fell victim to a hacking incident due to a misconfiguration of its parameters. This breach resulted in the theft of a significant number of tokens. Immediately following the incident, the project team halted the functionality for withdrawing staking rewards and allocated a substantial sum of \$USDT to repurchase the 307,264 lost tokens.

Post-attack, the project team swiftly reached out to TonBit for an audit. TonBit demonstrated their proficiency by quickly mobilizing a team of security experts who conducted an exhaustive and meticulous audit of the project's core code. TonBit's experts identified six low-risk issues and engaged in comprehensive discussions with the project team. With their rich experience and technical expertise, TonBit not only provided targeted solutions but also helped the team quickly rectify all identified issues, thus restoring the security and stability of the contract.

```
/// 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();
}
```

Issues related to the configuration found by TonBit audit:

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.

Solution: modify parameter configuration

2. Exploitation of Wallet to Display Controllable Comment Information to Mislead Users

Date: May 10, 2024
Loss Amount: 22,000 TON
Root Cause: Misleading comment information displayed during wallet transactions

Description:

In the TON ecosystem, while it is possible to add comments to transfer messages, the UI design of certain wallets poses a risk of misleading users. Hackers exploited this vulnerability by manipulating the comment content in transfer messages, presenting false information during transactions. This deceptive practice led users to make erroneous decisions, resulting in significant financial losses.

Solution:

To mitigate this issue, wallet applications should include conspicuous warnings when displaying comments, alerting users that the content may not be reliable. Additionally, wallet development teams need to enhance the UI design to ensure that transaction information is displayed transparently and reliably. Users should also cultivate a heightened awareness of suspicious transaction information.

Further Measures:

TonBit recommends that wallet developers implement a multi-layer verification mechanism for displaying transaction comments, such as verifying the source of the comment to confirm its authenticity. Furthermore, regular educational initiatives should be conducted to equip users with the necessary skills to recognize and guard against potential fraud. By integrating technological safeguards with user education, the frequency of such security incidents can be effectively minimized.

3. BookPad used a smart contract with a backdoor to siphon funds and then absconded with the money

Date: April 15, 2024
Loss Amount: 74,424 TON
Root Cause: BookPad implemented a backdoor in a non-open-source smart contract to illicitly siphon user funds.

Description:

BookPad launched a non-open-source smart contract embedded with a backdoor as part of a presale campaign. After accumulating sufficient funds, they exploited this backdoor to extract the funds and subsequently absconded with the money.

Solution:

To avert similar frauds in the future, investors are advised to thoroughly research any project before committing funds, prioritizing those that are open-source and have undergone stringent security audits. This approach can significantly mitigate the risk of falling victim to fraudulent schemes.

TonBit suggests users pay particular attention to the following points:

- **Open-Source Status of Project:** Ensure that the smart contract code is open-source. This allows independent security experts to review it, identifying hidden vulnerabilities or malicious code.
- **Security Audit:** Opt for projects that have undergone rigorous reviews by reputable security auditing firms. Such audits can detect and rectify potential vulnerabilities in contracts, offering additional safeguards.
- **Background Investigation:** Conduct thorough research on the project's background, including the reputation and historical performance of the team members. Projects characterized by high transparency and reputable teams are generally more trustworthy.
- **Community Feedback:** Monitor community feedback regarding the project, engage in discussions, and assess the project's reputation and potential risks.

Further Measures:

TonBit advocates for the implementation of stricter regulatory and review mechanisms within the TON ecosystem. This includes conducting qualification reviews of new projects to ensure they comply with established security standards. Moreover, the creation of a public contract code repository, where only vetted contracts are permissible for use, would greatly reduce the risk of theft of user funds and bolster the overall security and trustworthiness of the TON ecosystem.

4. Hackers forge phishing links to steal funds

Date: April 26, 2024
Loss Amount: Not specified
Root Cause: Phishing attack by hackers

Description:

Hackers created a counterfeit NFT project and a fake official Tether (USDT) website. Users who visited this fraudulent site were duped into entering sensitive information and transferring their USDT to the hackers' accounts. This deceptive scheme successfully misled many users, jeopardizing their funds.

Solution:

To avoid similar phishing attacks, users should take the following measures to verify the authenticity of domain names when visiting unfamiliar websites:

- **Check the Domain:** Ensure the domain name is spelled correctly and be cautious of characters that may look similar but are used in deceptive domains.
- **Obtain Links from Official Channels:** Always retrieve domain links from trusted sources, such as official social media, apps, and announcements, to avoid navigating to websites through unreliable sources.
- **Check Security Certificates:** Ensure the website's SSL/TLS certificate is valid. The browser should display a secure lock icon in the address bar. Clicking this icon will provide details to verify that the certificate is issued by a reputable authority and is associated with the correct domain.
- **Use Security Tools:** Employ browser security plugins and anti-phishing tools to identify and block fraudulent websites. Use reputable online services like VirusTotal or PhishTank to assess the legitimacy of websites.
- **Education and Awareness:** Regularly participate in cybersecurity education to stay informed about the latest phishing tactics and preventive measures. Users should be particularly cautious with new NFT projects and cryptocurrency platforms and should scrutinize any unverified information.

Further Measures:

TonBit suggests implementing additional security education and preventive measures within the TON ecosystem. This includes disseminating safety tips and guidelines through official channels to help users recognize and ward off phishing attempts. Strengthening the vetting process for new projects and websites to confirm their legitimacy and security will create a safer environment for all users.

5. Hackers impersonate the project team on Telegram to commit fraud

Date: February 4, 2024

Loss Amount: Not specified

Root Cause: Hackers impersonated the Ton_fish project team, posting fraudulent airdrop information on Telegram to deceive users.

Description:

Hackers posed as members of the Ton_fish project team and disseminated false airdrop announcements in Telegram groups to lure users into participating. They employed sophisticated social engineering tactics and used accounts that closely mimicked official ones, gaining trust by replicating the official account names, profile pictures, and posting styles. Victims who interacted based on this misleading information were potentially redirected to phishing sites or induced to transfer funds directly to hacker-controlled accounts, leading to financial losses.

Solution:

To prevent similar fraudulent activities, users engaging with Telegram or other social platforms should adopt the following security measures:

- **Verify Information Through Multiple Channels:** Always confirm the authenticity of any information through several official channels such as official websites, social media accounts, and announcements, rather than relying solely on one source.
- **Check Account Authenticity:** Scrutinize the details of accounts posting information, paying attention to the account's creation date, content history, and level of interactions. Genuine accounts typically have a longstanding presence and a substantial follower base, unlike fraudulent accounts.
- **Avoid Clicking Unknown Links:** Exercise caution with unfamiliar or suspicious links. Use security-enhanced browser extensions or online tools to assess link safety.
- **Confirm Directly with Official Sources:** For any suspicious information, directly contact the project team using officially provided communication channels to avoid misinformation through unreliable third-party channels.
- **Increase Security Awareness:** Regularly participate in cybersecurity education to stay informed about the latest phishing tactics and preventive strategies, especially when dealing with cryptocurrency and blockchain-related activities.
- **Enable Two-Factor Authentication:** Enhance account security by enabling two-factor authentication on social platforms like Telegram to provide an additional layer of security.

4.3 How TON Ecosystem Projects Conduct Security

As the TON ecosystem expands, the number and complexity of associated security issues also increase. To safeguard these projects, conducting thorough security audits is essential.

General Steps for a Security Audit:

1. Initial assessment

Understand the project background and requirements, confirm the audit scope and version, familiarize with the protocol architecture, and develop a detailed audit strategy.

2. Automated Inspection

Use static and dynamic analysis tools to conduct comprehensive testing of the project code to find problems that may damage contract functionality or security.

3. Manual Auditing

A team of security experts will examine each line of code in detail, identify potential errors and vulnerabilities, and maintain close communication with the project, and provide regular feedback on issues.

4. Preliminary Audit Report

The auditor drafts a preliminary audit report summarizing code defects and other issues and provides feedback to the project team. The project team confirms the audit issues, makes modifications to valid issues, and notifies the auditor of the re-audit.

5. Final Audit Report

Submit a detailed audit report with findings and recommendations for fixes. Communicate with the project team to ensure that all issues are effectively addressed.

6. Continuous Monitoring and Support

Provide continuous security monitoring on the chain to identify and respond to emerging security issues in a timely manner. Conduct regular security reviews to maintain the long-term security of the project.

TonBit’s Expertise:

TonBit fields a team of blockchain security specialists and seasoned developers who bring deep technical knowledge and extensive hands-on experience to each project. With years of practice in blockchain security, they are proficient in identifying and mitigating potential security risks, ensuring robust protection for projects within the TON ecosystem.

Audit Activities

	Planning		Audit				Reporting
Portfolio Selection	Audit Scoping	Analysis	Code Review > Verification		Initial Report	Iteration	Close-out
		Protocol Analysis	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 How Users Can Stay Safe on TON and Telegram

As the TON and Telegram ecosystems continue to rapidly expand, now boasting over 38 million active accounts, the heightened attention has also brought about increased risks. With scammers and malicious actors targeting newcomers, it is crucial for all users, even those in seemingly secure environments, to remain vigilant and informed about potential risks. Below, we detail some of the most prevalent scams and provide guidance on how to protect oneself.

5.1 Common Scams

1. **Fake Friends:** Scammers impersonate friends or family members, urgently requesting funds. Always verify their identity.
2. **Phishing Websites:** Fake websites mimic legitimate ones to steal login credentials. Double-check URLs and avoid clicking on unknown links.
3. **Investment Scams:** These scams that promise high returns without evidence are prevalent in the cryptocurrency space. Conducting in-depth research, and if it sounds too good to be true, it probably is.
4. **Fake Surveys:** Scammers offer rewards for survey participation to steal personal information. Avoid providing details to unknown surveyors.
5. **Fake Job Offers:** Enticing job ads request personal information, payment or download an APP. Verify through official channels.
6. **Classified Ad Scams:** Fraudulent ads direct you to fake Telegram bots to steal information.
7. **Pump and Dump:** Groups manipulate cryptocurrency prices for profit, leading to losses for others. Always research and verify investment advice.
8. **Romance Scams:** In online relationships, scammers ask for money or personal information. Be wary of financial requests from people met online.

5.2 Beware of Toncoin Pyramid Schemes

Unfortunately, Telegram's support for the TON blockchain has attracted some scammers who attempt to exploit unsuspecting users. Here's a detailed breakdown of this scam:

1. **Setup:** Scammers send links to an "exclusive money-making scheme" that appears to come from a friend or contact. They direct users to join an unofficial Telegram bot, falsely claiming it's for storing cryptocurrency.
2. **Investment:** Users are instructed to purchase Toncoin through legitimate channels (like wallets, P2P markets, or cryptocurrency exchanges), which adds a layer of false "credibility". Once purchased, users are told to transfer their Toncoin to the scam bot.
3. **Accelerator:** Victims are pressured to buy an "accelerator" through a separate bot, with fees ranging from 5 to 500 Toncoin. At this stage, users lose their cryptocurrency.
4. **Recruitment:** Scammers promote a referral program, encouraging users to create private Telegram groups and invite friends. They promise a fixed payment of 25 TON per referral and a commission based on the accelerator purchases of those referred.

In reality, this is a classic pyramid scheme. The scammers profit while others lose their investments.

5.3 How to Avoid Online Scams

To protect yourself from online scams and ensure the security of your Telegram account, follow these basic steps:

1. **Enable Two-Step Verification on Telegram:** Go to "Settings > Privacy and Security > Two-Step Verification" to add an extra layer of protection to your account.
2. **Verify Contacts:** Be cautious of unsolicited messages, especially those asking for personal information or money. Confirm the sender's identity through other means.
3. **Regularly Check Telegram Account Activity:** Go to "Settings > Devices > Active Sessions" to check if there are any unknown devices or sessions on your account.
4. **Report Suspicious Activity:** If you encounter a scam, report it to Telegram.
5. **Avoid Get-Rich-Quick Schemes:** Be skeptical of these schemes, even if recommended by friends or family, as they may also be victims.
6. **Don't Transfer Cryptocurrency to Unknown Wallets:** Always verify the recipient's identity before transferring cryptocurrency to avoid being scammed.

Staying safe on TON and Telegram requires vigilance and awareness. By recognizing common scams and following these security tips, you can protect your assets and personal information. Always verify sources, be skeptical of offers that seem too good to be true, and only conduct transactions through official channels. Staying informed and cautious will allow you to enjoy the benefits of TON and Telegram without falling victim to fraud!

6 Summary of TON Ecosystem Development

The rationale for choosing TON is deeply rooted in the inherent strengths of Telegram's ecosystem. Deploying your Web3 project on TON leverages Telegram's extensive user base, which boasts over 700 million monthly active users. This integration offers a fertile environment for the growth and prosperity of decentralized applications, akin to the supportive platforms provided by Apple's App Store and Steam for developers.

To grasp the importance of this integration, consider the analogy of symbiotic relationships in nature—whether it's the mutualism between clownfish and sea anemones or the parasitic relationships of viruses. These relationships are crucial for shaping the Earth's biodiversity and are pivotal drivers of evolution. Similarly, in technology and Web3, symbiotic relationships between different stakeholders are essential for thriving ecosystems. Networking and collaboration enable entities within these relationships to enhance their survival capabilities, achieving far more collectively than they could individually.

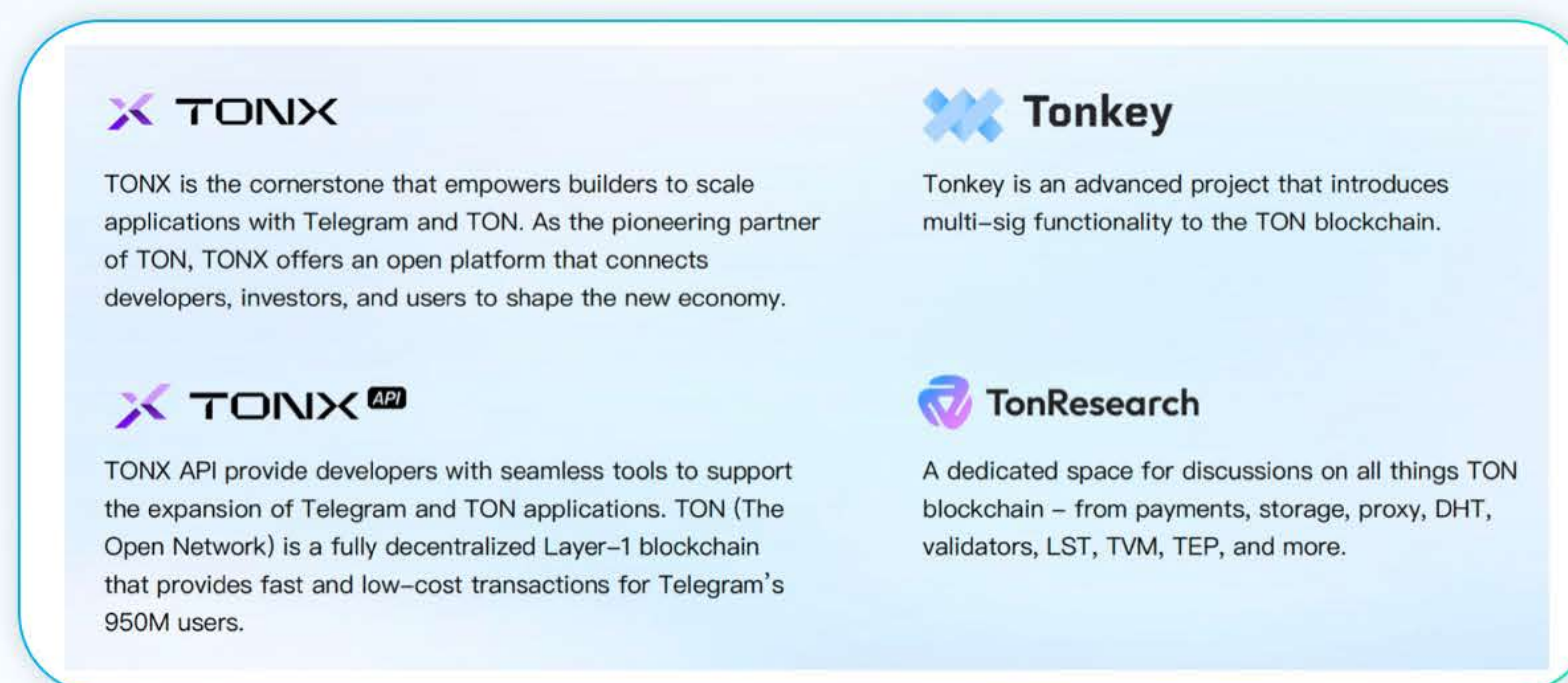
Such symbiotic relationships within technology foster collaboration and create synergies that benefit all participants, driving progress and innovation in the Web3 domain.

In essence, developers benefit from the vast user network of a major social platform like Telegram without compromising on incentives or value, building a robust future for their decentralized applications. This integration provides an ideal setting for the decentralized world to flourish, highlighting why TON is a strategic choice for developers looking to deploy projects on an open network.

7 About TonBit

TonBit is a sub-brand of BitsLab, a Web3 blockchain security audit company, focused on security auditing and analysis within the TON ecosystem. As a professional and experienced team, TonBit is dedicated to ensuring the security and reliability of the TON ecosystem, providing high-level protection for developers and users alike.

1. Early Participants in the TON Ecosystem: Since 2021, TonBit members have been deeply involved in the TON ecosystem, initiating projects such as TONX, TONX API, TonKey, and Ton Research. These initiatives, including TonX Studio and TonFura, demonstrate TonBit's commitment to developing and enhancing the TON platform.



2. Comprehensive Auditing Services: TonBit offers a full spectrum of security audit services, including smart contract audits, protocol safety assessments, and code vulnerability checks. These comprehensive audits ensure the security of projects at all stages, helping to prevent potential attacks and mitigating risks.

Advantages of TonBit

1. Efficient Audit Process:

TonBit employs advanced audit tools and automation technology, allowing for the rapid and efficient completion of security audits. While maintaining high audit quality, this significantly reduces audit time, saving valuable development cycles for projects.

2. Customized Solutions:

TonBit provides customized security solutions based on the specific needs of each project. From early-stage design assessments to post-launch security monitoring, TonBit safeguards the entire life cycle of a project.

3. Continuous Monitoring and Support:

TonBit not only offers one-time audit services but also provides ongoing security monitoring and technical support. Through real-time monitoring and regular reviews, TonBit swiftly identifies and resolves emerging security issues, ensuring the long-term security of projects.

TonBit Protects the Entire TON Ecosystem Through

1. Preventive Audits:

Before project launch, TonBit conducts comprehensive security audits to identify and fix potential security vulnerabilities in advance, ensuring the project's security upon release.

2. Real-Time Monitoring:

TonBit offers 24/7 security monitoring services, continuously monitoring project operations to detect and respond to security threats promptly, ensuring smooth project performance.

3. Security Response:

When security issues are detected, TonBit responds quickly, providing emergency handling solutions to help project teams resolve issues swiftly and minimize the impact of security incidents.

4. Community Collaboration:

TonBit actively participates in the TON community's security initiatives, sharing security knowledge and best practices with community members to collectively enhance the security level of the entire ecosystem.

TonBit is committed to providing comprehensive security protection for the TON ecosystem, helping projects achieve higher security standards and gain user trust. As a guardian of the security of the TON ecosystem, TonBit is dedicated to the development of blockchain technology.

Contact US



www.tonbit.xyz



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



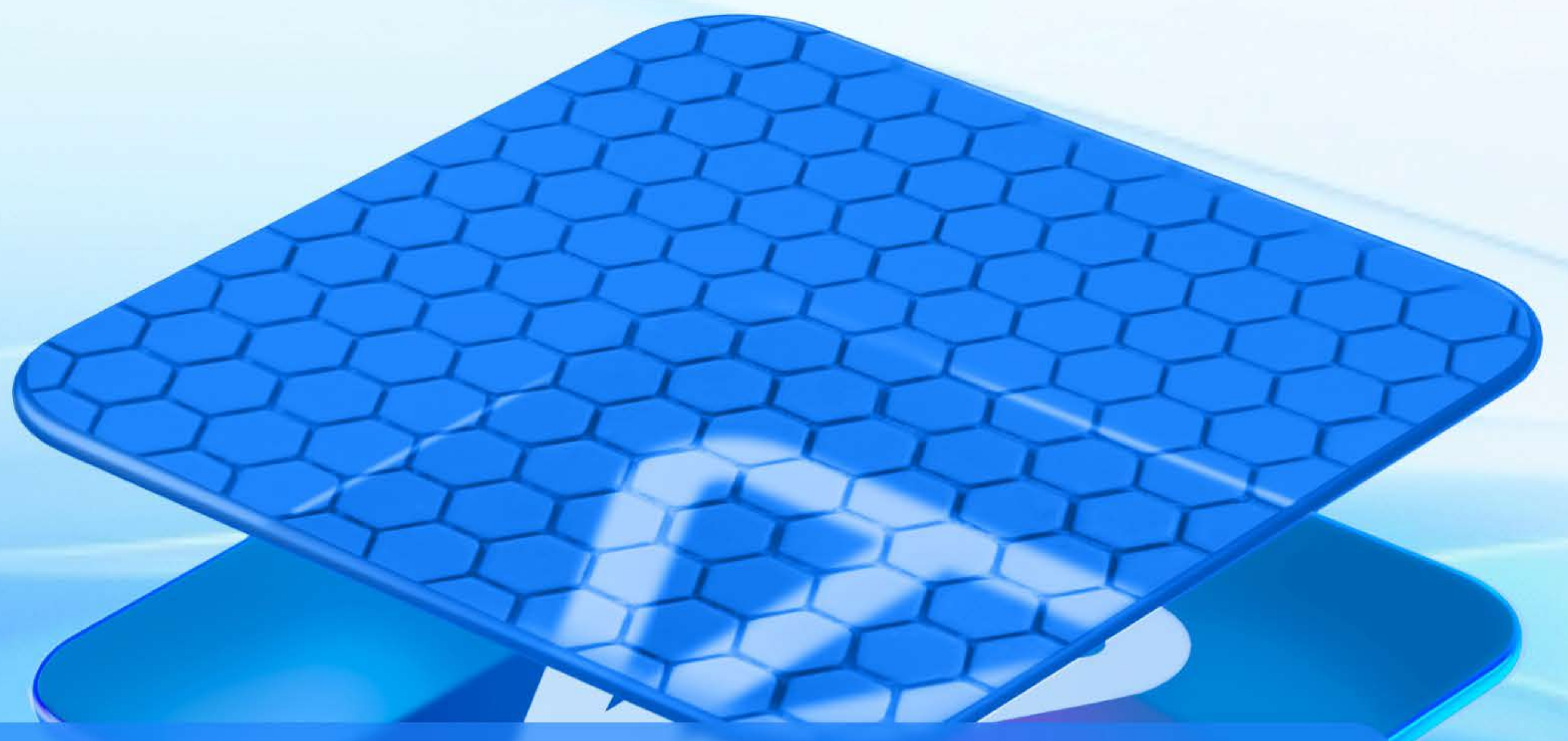
[@paul_li2024](https://t.me/paul_li2024)



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



contact@bitslab.xyz



Disclaimer: This report is for informational purposes only and does not constitute any form of investment advice, recommendation, or guarantee. Readers should conduct their own independent research and analysis before making any investment decisions.

Data Accuracy: The data in this report has been made as accurate and up-to-date as possible. However, due to the rapid changes in the market, some data may have changed after the report was published.

Report Limitations: Due to limitations in information availability, this report may not cover all security incidents and market changes. Readers should consider other sources to form a comprehensive judgment.

Copyright Notice: The content of this report is protected by copyright. Unauthorized copying, reproduction, or use for commercial purposes is prohibited without permission.

Security Advisory: Users should increase their security awareness, regularly update security software and preventive measures, and avoid becoming victims of cyber attacks and scams.

References: In addition to data from the official TON Foundation, this report also references multiple other sources.
<https://blog.ton.org/>
<https://x.com/DegenonTON/status/1783738318850789494>
<https://x.com/DegenonTON/status/1779729268953813381>
<https://x.com/realScamSniffer/status/1788749945459318868>