CERTIK
SKYNET

Skynet 2026 Stablecoin Threat Intelligence Report

Stablecoins have become critical settlement infrastructure and a growing frontier for financial threat activity.



Executive Summary

The global stablecoin market has matured into critical financial infrastructure, processing trillions of dollars in cross-border settlement annually. As institutional adoption has accelerated, so has the sophistication of threats targeting it, both from opportunistic attackers exploiting the technical and operational layers surrounding stablecoin infrastructure, and from state-adjacent actors deliberately constructing parallel systems to circumvent Western sanctions. This report examines both dimensions of that threat.

The first section documents emerging exploit trends across stablecoin-related infrastructure, including cross-chain bridges, custody systems, and DeFi composability. The second section provides a deep-dive case study on A7A5, a Russian-ruble-backed stablecoin that has become the most consequential example of state-sponsored sanctions evasion in the digital asset ecosystem to date. Together, they define the two defining stablecoin security challenges of 2026: attacks on interconnected financial infrastructure, and the deliberate weaponization of stablecoin architecture by sanctioned actors.

Key Insights

Stablecoin Infrastructure Exploits

- **Bridge and interoperability protocols remain the highest-value attack surface.**
  Bridge-related incidents in 2026 have so far totaled over $328 million in losses, with the Kelp DAO wallet compromise alone accounting for $291.3 million in April 2026.
- **Wallet compromise has overtaken code vulnerabilities as the dominant exploit vector.**
  Across the largest 2026 DeFi incidents, wallet compromise was responsible for the majority of losses by value, reflecting a shift toward targeting operational and custody security rather than on-chain logic.
- **The attack surface is expanding beyond DeFi.**
  As stablecoins integrate deeper into traditional financial systems, attackers are increasingly targeting compliance infrastructure, KYC providers, payment APIs, and sanctions screening systems. These attack patterns more closely resemble those seen in traditional financial crime than earlier crypto exploits.

A7A5: State-Sponsored Sanctions Evasion

- **Rapid, large-scale adoption.**
  Within one year of its January 2025 launch, A7A5 processed more than $110 billion in cumulative on-chain transactions and captured approximately 43% of the global non-USD stablecoin market.
- **Sanctioned ownership at every layer.**
  A7A5's issuer (Old Vector LLC), collateral bank (PSB), and transaction platform (Tokeon) are all under overlapping U.S., UK, and EU sanctions designations, creating a structurally circular arrangement with no independent reserve attestation.
- **AML exposure is significant and documented.**
  A7A5's parent ecosystem has direct exposure to ransomware proceeds linked to Conti, Black Basta, and LockBit, as well as DPRK-attributed funds including more than $30 million traced from the 2023 Horizon Bridge hack.

- **Unprecedented multi-jurisdictional enforcement.**
  A7A5 became the first cryptocurrency ever explicitly named in an EU transaction ban (19th sanctions package, effective November 25, 2025), followed by broader categorical prohibitions in the EU's 20th package (effective May 24, 2026), and parallel designations from OFAC and the UK's OFSI.
- **Enforcement has structural limits.**
  Despite multi-jurisdictional action, A7A5 holder counts grew continuously from approximately 13,000 to 29,000 between February 2025 and May 2026, with no observable inflection at any sanctions event. The user base is structurally non-Western and therefore largely insulated from Western enforcement pressure.
- **Active geographic expansion into regulatory blind spots.**
  Russia has invited African nations to join the A7 network, with offices established in Nigeria and Zimbabwe. No African jurisdiction has been formally engaged by OFAC, HM Treasury, or the EU on A7A5-related exposure, creating potential secondary-sanctions risk for Western-aligned banks in those markets.
- **Liquidity concentration remains a structural fragility.**
  The primary A7A5 trading venue, Grinex, was reportedly hacked for approximately $15 million in April 2026 and suspended operations. With no comparable alternative, this represents a significant single point of failure in the A7A5 ecosystem.

PART 1.

Stablecoin Infrastructure Exploit Trends

A number of important exploit trends have emerged around stablecoin infrastructure over the last 18–24 months, particularly involving bridges, interoperability protocols, custody systems, and payment infrastructure. As stablecoins have evolved into core settlement infrastructure rather than simply trading assets, attackers have increasingly shifted their focus toward the operational and infrastructural layers surrounding them.

Cross-Chain Bridges & Interoperability Protocols

One of the clearest trends has been the continued concentration of attacks against cross-chain bridges and interoperability protocols. Because stablecoin liquidity is fragmented across multiple blockchains and Layer 2 networks, bridges have become critical infrastructure for moving value between ecosystems. Exploits have frequently targeted:

- Weaknesses in validator systems and multisig controls
- Message verification logic and cross-chain messaging complexity
- Burn-and-mint settlement logic and oracle dependencies in interoperability layers
- Replay attacks and manipulation of liquidity routing middleware

Because interoperability layers increasingly aggregate liquidity across multiple ecosystems, a single exploit can expose large amounts of capital simultaneously across several chains. 2026 bridge incidents totaled over **$328 million in losses**, with the Kelp DAO wallet compromise alone accounting for **$291.3 million** in April.

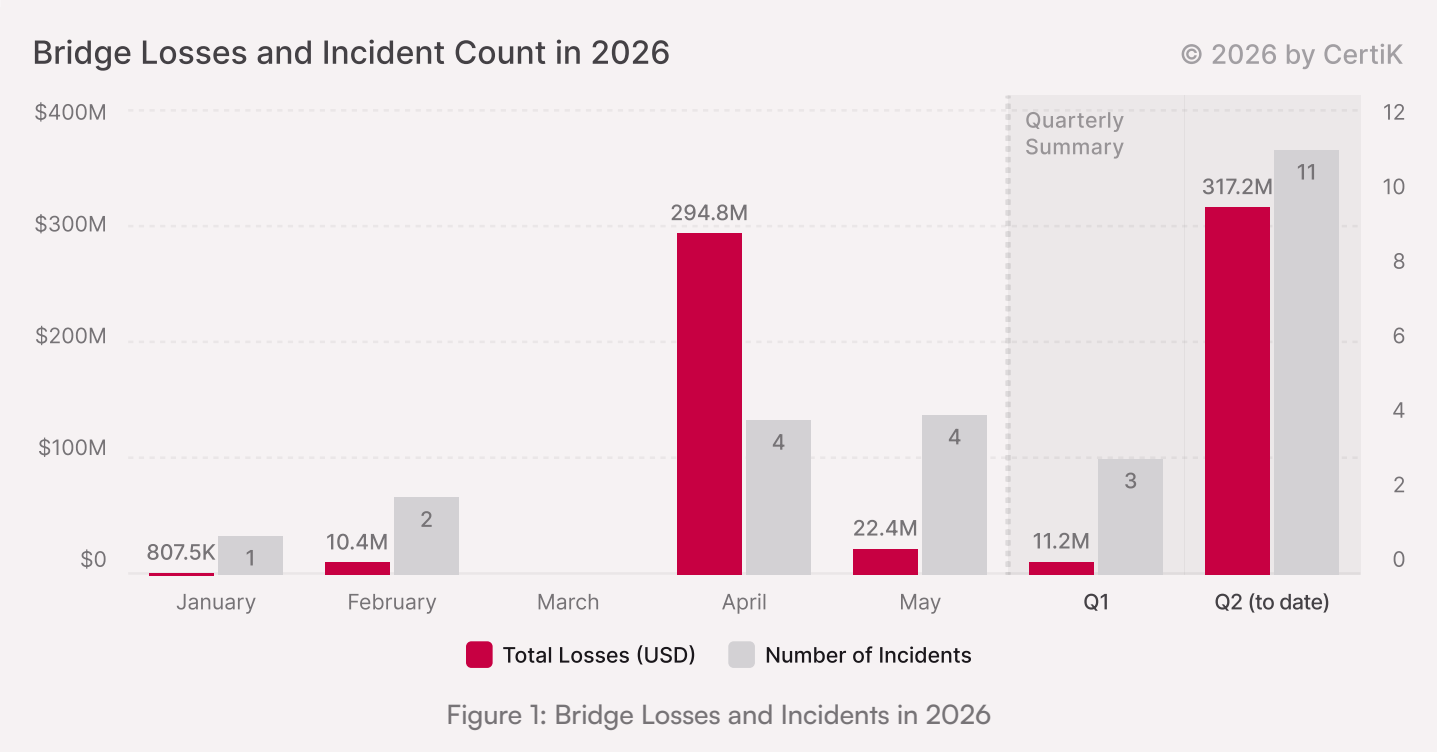


Figure 1: Bridge Losses and Incidents in 2026

Custody & Treasury Infrastructure

Attackers have also shifted toward exploiting weaknesses in stablecoin custody and treasury infrastructure rather than only attacking DeFi protocols directly. Institutional adoption has led to the growth of programmable treasury systems, custodial platforms, fiat on- and off-ramps, and automated settlement infrastructure. These systems introduce more centralized operational risks, including:

- Compromised private keys and insider threats
- API vulnerabilities and cloud infrastructure misconfigurations
- Weaknesses in access-control systems

As stablecoin infrastructure becomes more integrated with traditional financial systems, attackers are increasingly targeting operational security failures alongside on-chain vulnerabilities.

Composability Risk Within DeFi

Another major exploit trend involves composability risk within DeFi integrations. Stablecoins are deeply embedded across lending protocols, liquidity pools, derivatives systems, and automated market makers, meaning vulnerabilities in one protocol can rapidly cascade into others.

Flash loan attacks, oracle manipulation, liquidity pool imbalances, and governance exploits have repeatedly been used to manipulate stablecoin pricing, collateral ratios, or redemption mechanisms. Because stablecoins often serve as base collateral throughout DeFi ecosystems, disruptions involving them can have systemic effects that spread rapidly across interconnected protocols.

Payment-Focused & Stablecoin-Specific Chains

The emergence of payment-focused and stablecoin-specific chains has also introduced new security concerns. Chains optimized for fast settlement and low-cost transfers sometimes prioritize throughput and user experience over decentralization or security hardening. This can create vulnerabilities around:

- Validator concentration
- Centralized sequencing infrastructure
- Weaker consensus assumptions

Networks heavily used for remittances and stablecoin transfers have become attractive targets for attackers seeking to exploit operational dependencies or infrastructure bottlenecks.

Compliance & Identity Infrastructure

Regulation and institutionalization are also reshaping exploit patterns. As regulated stablecoins become more integrated into mainstream payment systems, attackers are increasingly interested in targeting compliance and identity infrastructure surrounding them. This includes attacks against KYC providers, API integrations, sanctions screening systems, and payment orchestration platforms.

Rather than purely stealing on-chain funds, some attacks now aim to disrupt settlement processes, manipulate compliance workflows, or exploit weaknesses in the interaction between traditional financial systems and blockchain infrastructure.

Overall DeFi Incident Trend in 2026

The data below illustrates the acceleration of both incident volume and financial losses across the first half of 2026.

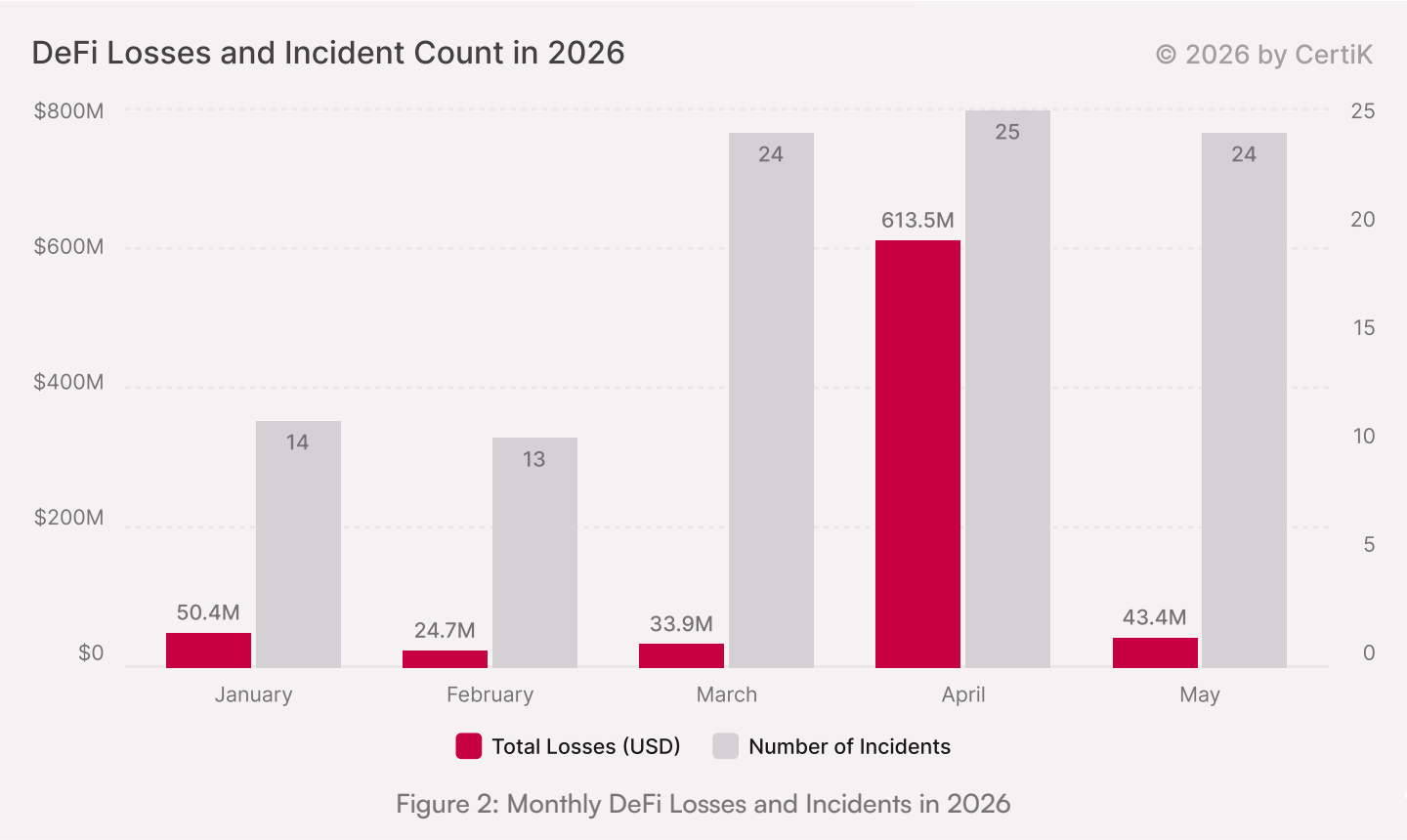


Figure 2: Monthly DeFi Losses and Incidents in 2026

Largest DeFi Incidents by Amount Lost

Incident	Date	Chain	Exploit Type	Amount Lost
Kelp DAO	Apr 18, 2026	Ethereum	Wallet Compromise	$291,328,075
Drift Protocol	Apr 1, 2026	Solana	Wallet Compromise	$285,278,414
Step Finance	Jan 31, 2026	Solana	Wallet Compromise	$27,325,461
Resolv	Mar 22, 2026	Ethereum	Wallet Compromise	$26,846,293
Rhea Finance	Apr 16, 2026	Near Intents	Price Manipulation	$18,474,150
Swapnet	Jan 25, 2026	BASE	Code Vulnerability	$13,337,243
Verus	May 17, 2026	Ethereum	Code Vulnerability	$11,523,563
YieldBlox	Feb 22, 2026	Stellar	Price Manipulation	$10,594,211
Thorchain	May 15, 2026	Multiple Chains	Code Vulnerability	$10,120,270
IoTeX	Feb 21, 2026	Ethereum	Wallet Compromise	$8,904,830
TrustedVolumes	May 7, 2026	Multiple Chains	Code Vulnerability	$6,575,197
Wasabi Protocol	Apr 30, 2026	Multiple Chains	Wallet Compromise	$5,568,618
Makina Finance	Jan 19, 2026	Ethereum	Price Manipulation	$4,243,039
Volo Protocol	Apr 22, 2026	Sui	Wallet Compromise	$3,425,865
StablR	May 24, 2026	Ethereum	Wallet Compromise	$3,425,346
Aperture Finance	Jan 25, 2026	Ethereum	Code Vulnerability	$3,229,451
TAC	May 11, 2026	Ton	Code Vulnerability	$2,875,917
Haveno	May 20, 2026	Monero	Code Vulnerability	$2,700,000
SolV	Mar 5, 2026	Ethereum	Code Vulnerability	$2,530,943
Hyperbridge	Apr 13, 2026	Ethereum	Code Vulnerability	$2,500,000

Bridge-Related Incidents in 2026

Incident	Date	Chain	Exploit Type	Amount Lost
Kelp DAO	Apr 18, 2026	Ethereum	Wallet Compromise	**$291,328,075**
Verus	May 17, 2026	Ethereum	Code Vulnerability	**$11,523,563**
Thorchain	May 15, 2026	Multiple Chains	Code Vulnerability	**$10,120,270**
IoTeX	Feb 21, 2026	Ethereum	Wallet Compromise	**$8,904,830**
Hyperbridge	Apr 13, 2026	Ethereum	Code Vulnerability	**$2,500,000**
CrossCurve	Feb 1, 2026	Multiple Chains	Code Vulnerability	**$1,479,255**
Gyroscope	Jan 31, 2026	Ethereum	Code Vulnerability	**$807,534**
Aethir	Apr 9, 2026	Multiple Chains	Wallet Compromise	**$652,926**
Adshares	May 15, 2026	Ethereum	Code Vulnerability	**$645,348**
Syndicate IO	Apr 29, 2026	Base	Wallet Compromise	**$313,234**

Overall, the broader trend is that stablecoin-related exploits are expanding beyond smart contract bugs and toward attacks on interconnected financial infrastructure. Bridges, interoperability layers, custody systems, payment APIs, and settlement orchestration mechanisms are increasingly becoming important components of the attack surface. As stablecoins continue evolving into internet-scale financial infrastructure, the associated security risks are beginning to resemble those seen in global payment networks and critical financial systems rather than the earlier, narrower risks associated with speculative crypto applications. Yet technical exploits represent only one dimension of the threat landscape.

The following section examines a more structurally complex risk: the deliberate construction of stablecoin infrastructure by a sanctioned state actor, designed from the ground up to operate beyond the reach of Western enforcement.

PART 2.

A7A5: Anatomy of a Sanctioned Stablecoin

A7A5 is a Russian-ruble-backed stablecoin, which was issued in January 2025 by Old Vector LLC, a Kyrgyz entity acting on behalf of the Russian cross-border-settlement firm (A7 LLC). A7 LLC is co-owned by sanctioned Moldovan-Russian oligarch Ilan Shor and the sanctioned Russian state-owned defense-sector lender Promsvyazbank.

Within a year of launch, A7A5 processed **more than $110 billion** in cumulative on-chain transactions, and captured roughly 43% of the global non-USD stablecoin market. Following the March 2025 takedown of Garantex (later reborn as Grinex), it became the operational backbone of the Russian crypto economy.

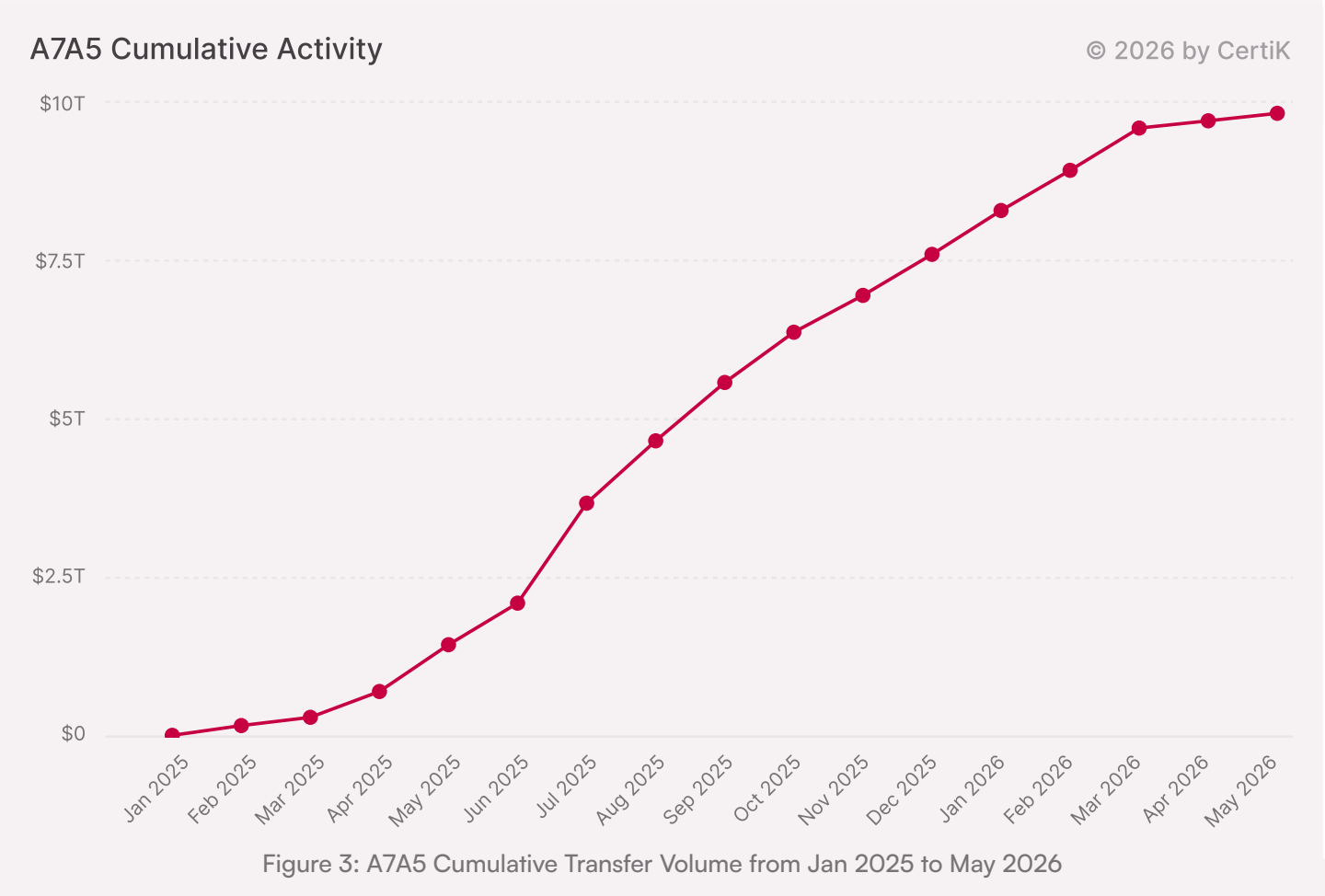


Figure 3: A7A5 Cumulative Transfer Volume from Jan 2025 to May 2026

Key findings

- The Russian Central Bank formally recognized A7A5 as a Digital Financial Asset (DFA) in October 2025.
- Approximately $11.2 billion in A7A5/RUB and $6.1 billion in A7A5/USDT trades have been recorded, primarily on Grinex (successor to Garantex).
- Garantex was a primary laundering venue for Conti, Black Basta, and LockBit, and for funds attributed to the DPRK, including more than $30 million stolen from Horizon Bridge in 2023.

Global Context

Russia's February 2022 invasion of Ukraine triggered one of the most extensive coordinated sanctions packages ever applied to a G20 economy. Multiple Russian banks were excluded from SWIFT, Visa, and Mastercard. By mid-2022 the practical capacity of major Russian financial institutions to settle in U.S. dollars or euros via correspondent banking had collapsed.

In this environment, Tether's USDT became, by default, the preferred non-ruble settlement asset for Russian commercial actors and exchanges. USDT offered global reach, deep on-chain liquidity (especially on Tron), and apparent stability against the volatile ruble. The vulnerability of this dependency became apparent in March 2025: in coordination with the U.S. Secret Service's seizure of the Garantex domain, Tether froze approximately $26-28 million in USDT held by Garantex-controlled wallets.

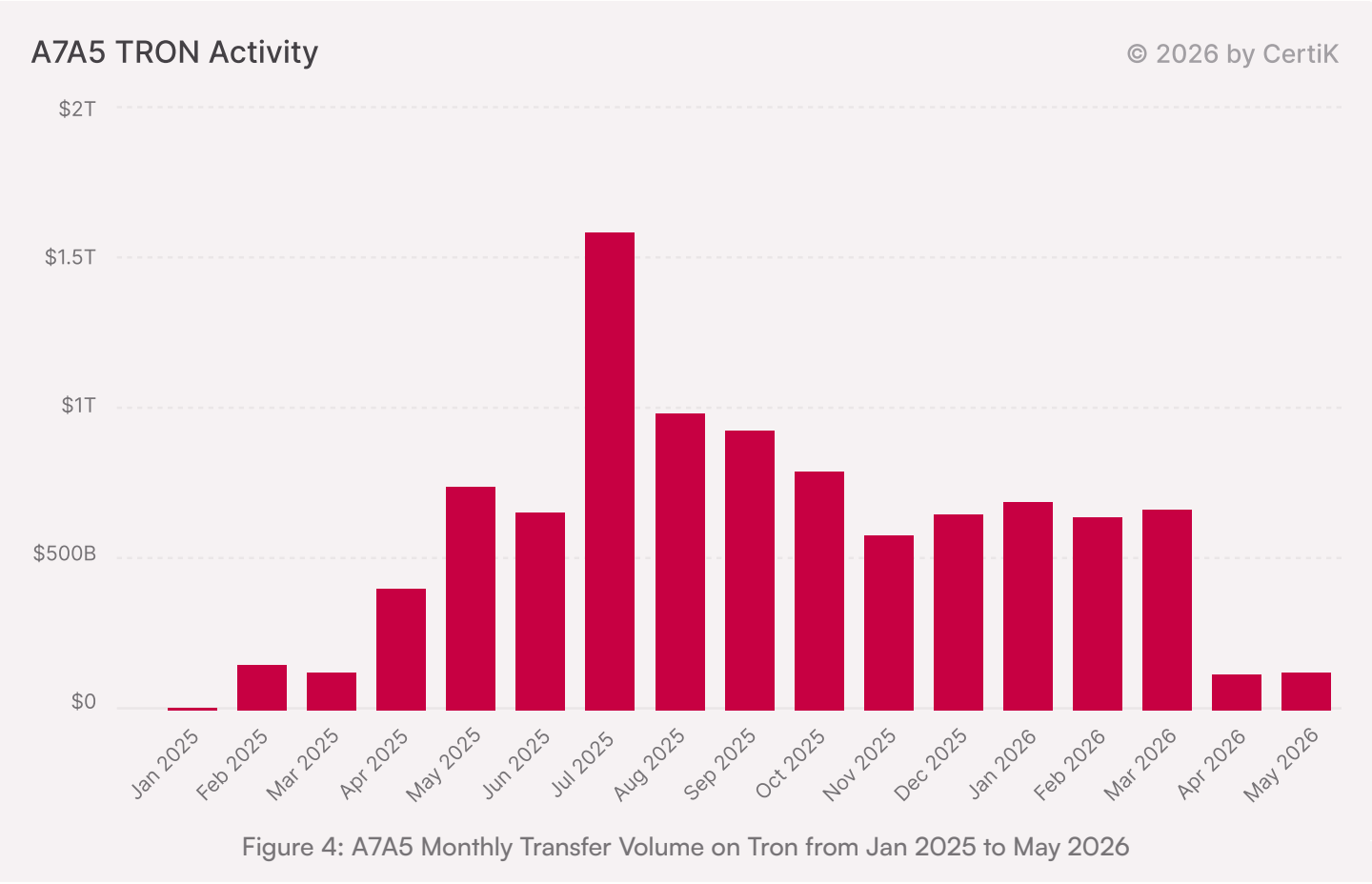


Figure 4: A7A5 Monthly Transfer Volume on Tron from Jan 2025 to May 2026

A7A5 is the Russian institutional response to that demonstration. Its design philosophy is to replicate the technical architecture of USDT (centralized mint, blacklist, freeze and destroy capabilities), but locate the issuer, collateral, and compliance authority outside Western enforcement reach.

Creation and launch of A7A5

A7 LLC was registered in Russia in October 2024 as a cross-border-settlement service for Russian businesses constrained by Western sanctions.

On January 28, 2025, A7 and PSB jointly announced the launch of A7A5. A first issuance of 1.5 million A7A5 tokens was minted. The token was nominally issued by Old Vector LLC, a Kyrgyz company.

At launch, A7A5 was almost immediately listed on Garantex. The CEO of A7, speaking at the St. Petersburg International Economic Forum on June 19, 2025, framed A7A5 as one component of a broader payment infrastructure.

Actors and Ownership Structure

Ilan Mironovich Shor is the majority owner (51%) of A7 LLC and the public face of the A7A5 project. He is a Moldovan-born businessman and former member of the Moldovan parliament. In 2017, he was convicted by a Moldovan court in connection with the 2014 theft of approximately $1 billion from three Moldovan banks. He fled Moldova in 2019 and was sentenced in absentia in 2023 to fifteen years in prison. Shor has subsequently obtained Russian citizenship and resides in Moscow.

Promsvyazbank (PSB) is a Russian state-owned bank that has functioned as the primary financial institution servicing the Russian defense-industrial complex. The bank owns 49% of A7 LLC, holds the ruble collateral that backs the token, and owns the Tokeon platform that processes its transactions.

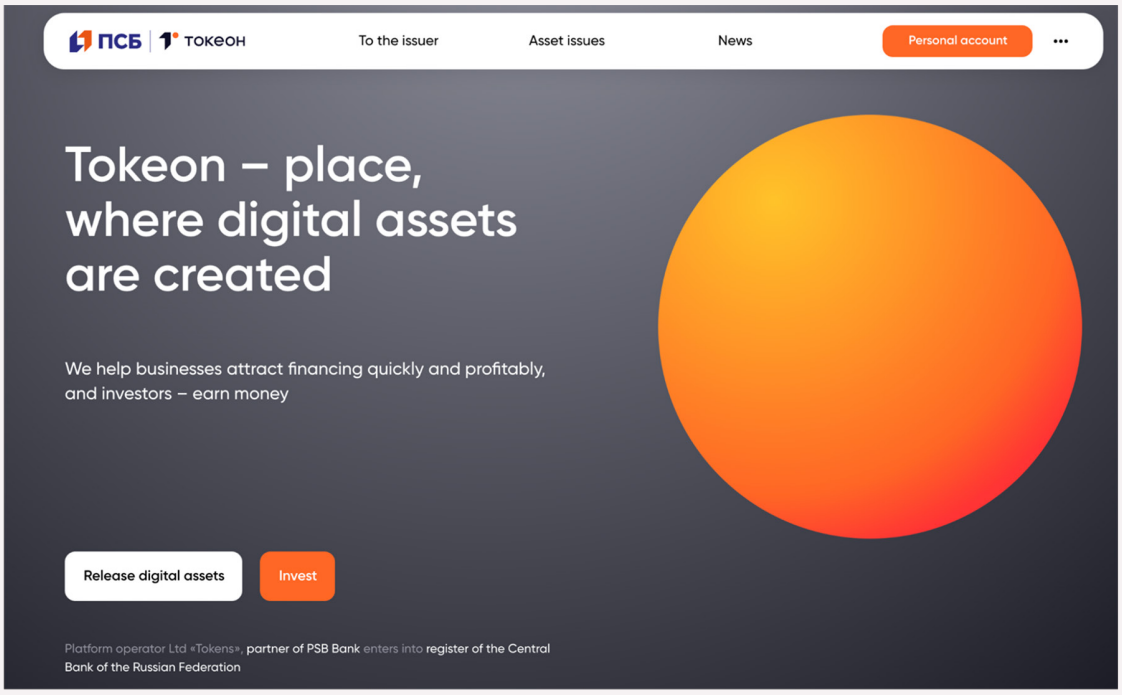


Figure 5: Tokeon platform

A7 LLC is the central operating entity. It styles itself as a cross-border payment platform offering Russian businesses a turnkey solution for international settlement in the absence of traditional correspondent banking.

Old Vector LLC is the Kyrgyz entity that nominally issues A7A5. OFAC designated Old Vector in August 2025 for "working with Garantex and others in the creation of the A7A5 token" and for facilitating the distribution of compensation to Garantex customers in the wake of the March 2025 takedown.

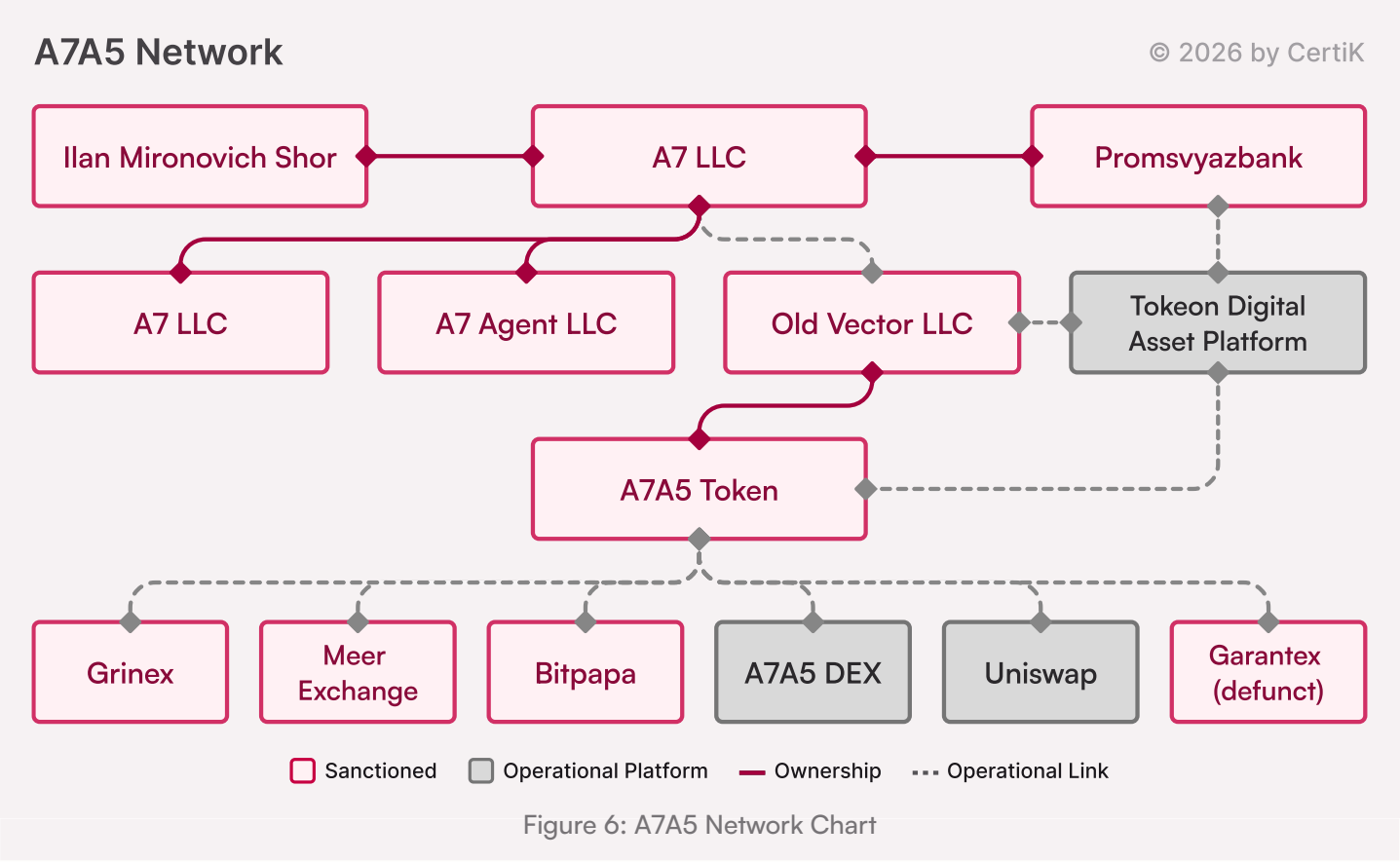


Figure 6: A7A5 Network Chart

Technical Architecture

Smart Contract Address

Asset	Chain	Address
A7A5	Ethereum	0×6fA0BE17e4beA2fCfA22ef89BF8ac9aab0AB0fc9
A7A5	Tron	TLeVfrdym8RoJreJ23dAGyfJDygRtiWKBZ
wA7A5 (wrapped)	Ethereum	0×0d57436f2d39c0664c6f0f2e349229483f87ea38

Note: as of the date of this report, OFAC has not designated any of the above contract addresses on the SDN list.

A7A5 is deployed on Ethereum and Tron. A wrapped version (wA7A5) is available on Ethereum. Approximately 99% of supply circulates on Tron. The contract is a near-direct lineage of the Tether USDT contract, with three privileged roles: owner, compliance, and accountant. Key functions include:

- `addBlackList / removeBlackList:`
  Administrative blacklisting of wallet addresses.
- `destroyBlackFunds(user):`
  Permanently destroys the balance of a blacklisted address. Destroyed amount logged on-chain as `dirtyShares`.
- `issue / burn:`
  Mint and burn controlled by the owner.
- `pause / unpause:`
  Emergency suspension of all transfers.
- `distributeInterest(int256):`
  Rebasing function executed by the accountant role (see yield mechanism below).

Each A7A5 token is claimed to be backed 1:1 by ruble deposits held at PSB under the custodianship of Old Vector LLC. No independent audit or reserve attestation has been published. The arrangement is structurally circular: issuer, collateral bank, operator, and retail distributor are all under common ownership and overlapping sanctions designations. Transactions are processed through Tokeon, a PSB-owned digital asset platform.

Digital Promissory Notes

Beyond the on-chain token, A7 has developed a hybrid instrument it markets as “Digital Promissory Notes.” Holders can exchange a physical paper note for local cash via a Telegram bot, convert it back into A7A5, or redeem it for rubles directly. This component of the system is significant for three reasons:

- It extends the network into physical-cash distribution, which is a meaningful capability in jurisdictions with weak banking infrastructure or where the recipient cannot or will not interact directly with sanctioned crypto rails.
- It materially complicates the on-chain investigation because once value has moved into the paper-note layer it leaves the public ledger entirely until the next conversion event.
- The hybrid model is functionally analogous to “trade-based money laundering” infrastructures that have historically supported sanctions evasion via shell companies and falsified invoices.

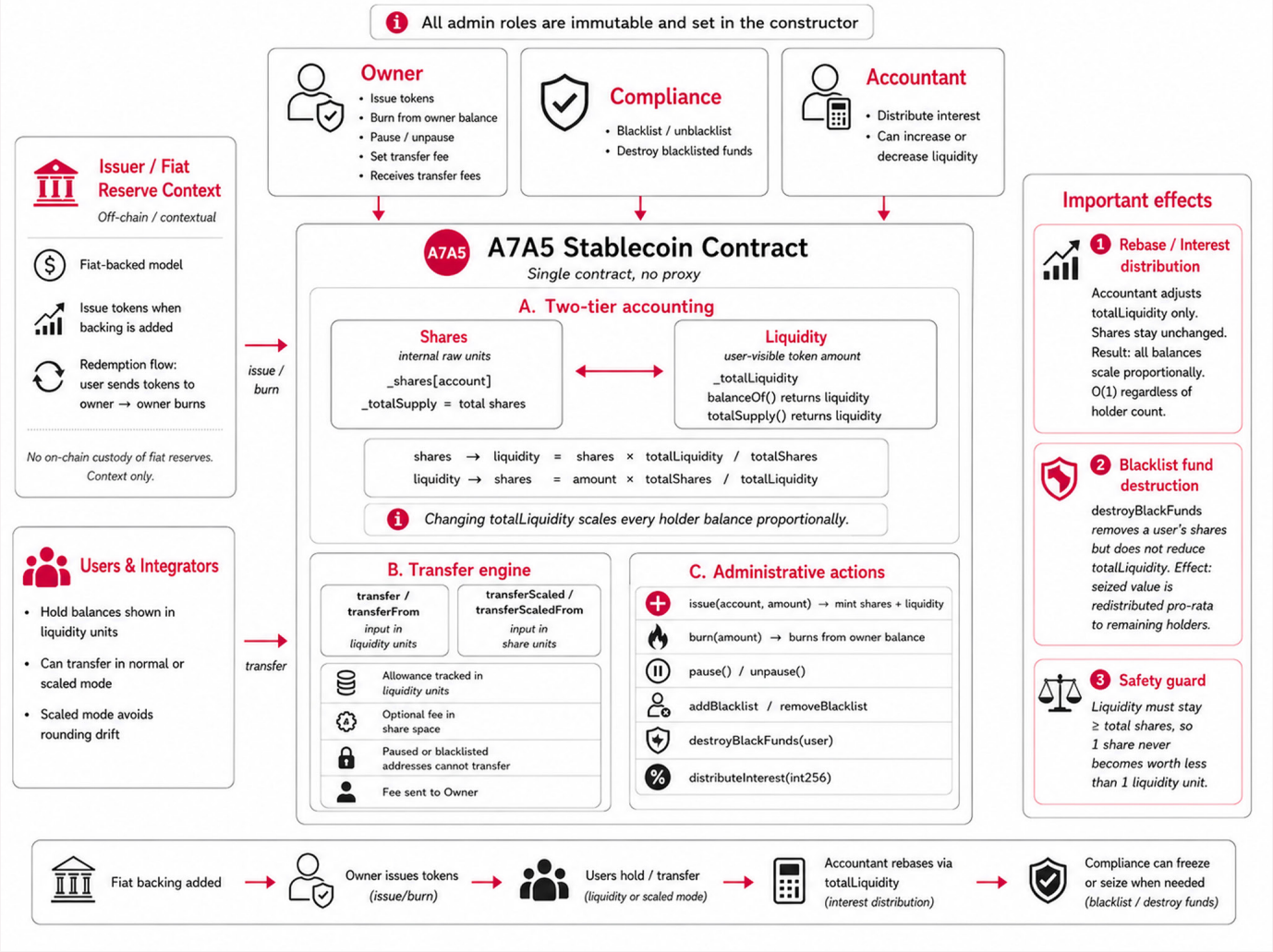


Figure 7: How A7A5 works

On-Chain Analysis

The Tron transfer-volume curve is the most informative artifact in the entire A7A5 dataset. December 25, 2025 is the highest single-day volume, approximately 135 billion tokens, or USD 1.7 billion. The date falls 30 days after the EU 19th-package effective date (November 25, 2025) and 6 days before Russia's long New Year banking closure. A plausible reading is a year-end settlement push by Russian commercial actors clearing cross-border invoices before the institutional shutdown, possibly compounded by a second `destroyBlackFunds()` reset against EU-identified wallets following the end of the 19th-package wind-down period.

Tronscan recorded an A7A5 transfer volume of 102,711,127,053 tokens on May 14, 2026. The spike is isolated and falls exactly ten days before the EU 20th-sanctions-package crypto provisions enter into force on May 24, 2026.

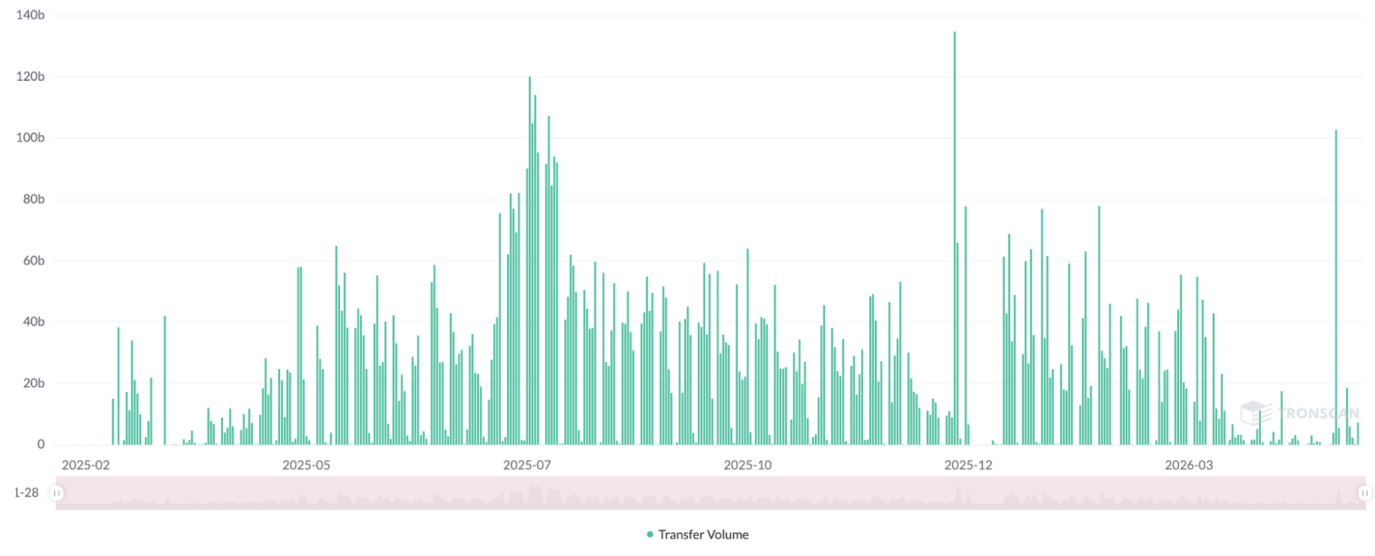


Figure 8: A7A5 transfer volume on TRON

Ethereum carries only ~1% of A7A5 supply which makes every spike high-signal. After the initial launch peak in May 2025, activity stays at a low baseline (under 100 tx/day). Spikes on May 5 and 11 fall at 19 and 13 days before the EU 20th-package effective date.

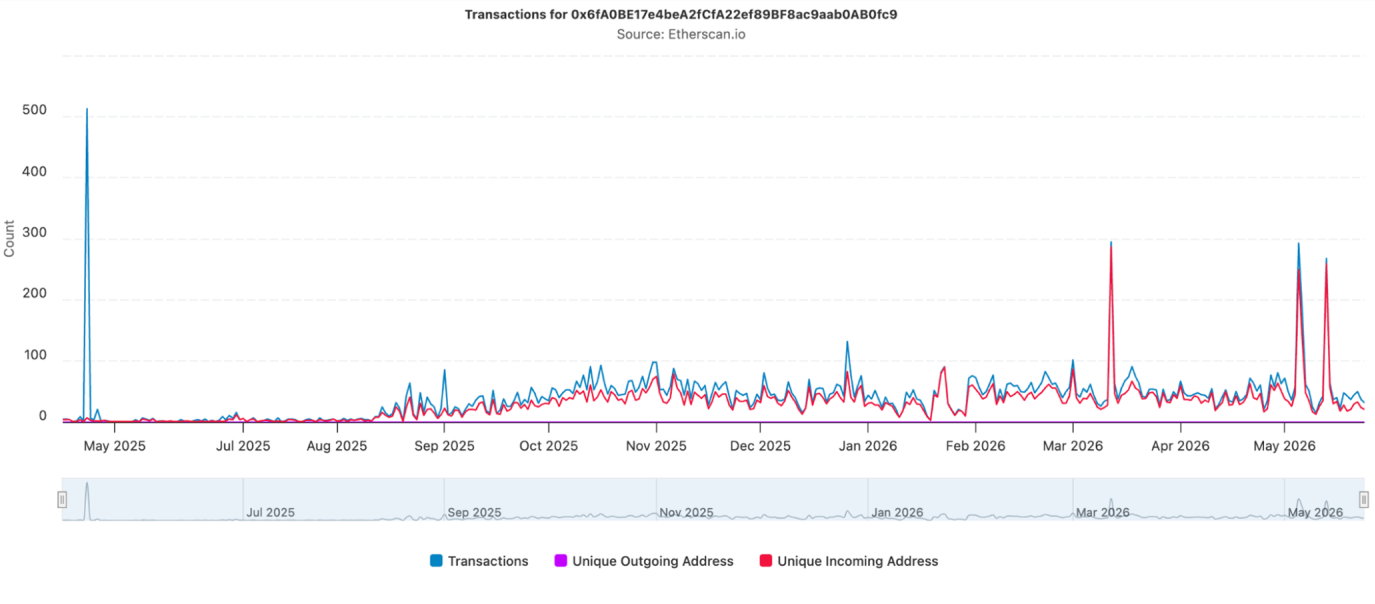


Figure 9: A7A5 transactions on ETH

If the volume curve reflects the activity of existing users, the holder curve reflects the new ones. The data are particularly interesting.

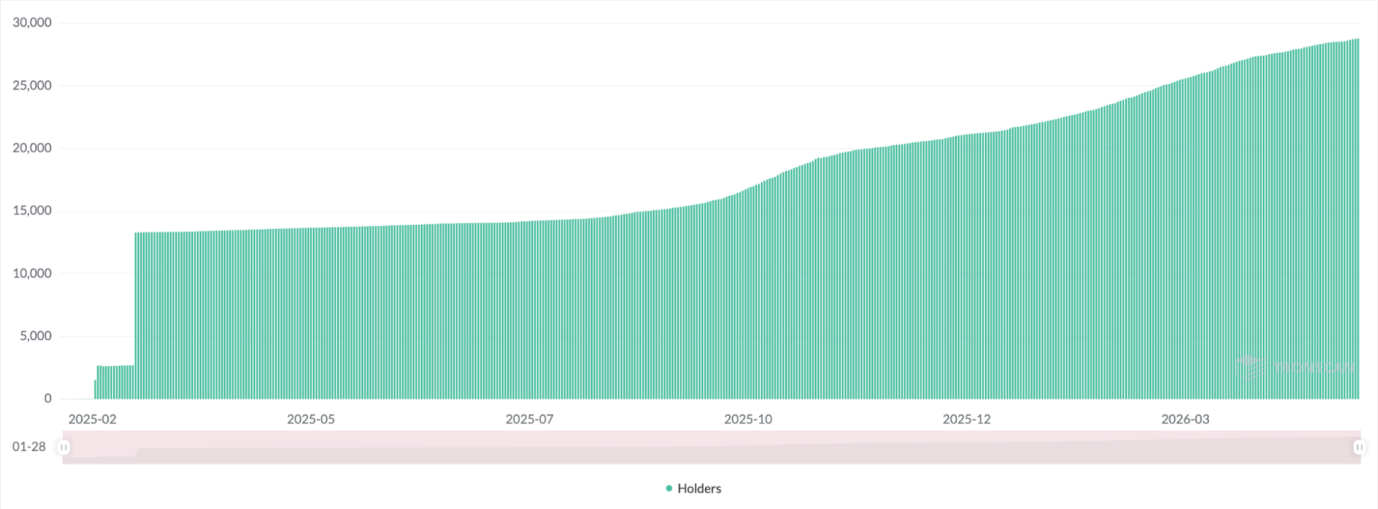


Figure 10: A7A5 holders on TRON

We can observe a continuous growth, **with no inflection at any sanctions event.** From February 2025, the curve grows in an almost perfectly linear trajectory from ~13,000 to ~29,000 holders by May 2026. The curve is monotone increasing throughout. It seems holders are not responsive to sanctions. Here are some possible explanations:

- **Yield retention.** The rebasing mechanism makes A7A5 economically rational to hold even when trading is restricted.
- **Captive demand.** The user population is structurally non-Western, consisting largely of Russian, Kyrgyzstani, Belarusian, and other regional users. Western sanctions do not generate exit pressure for this cohort.

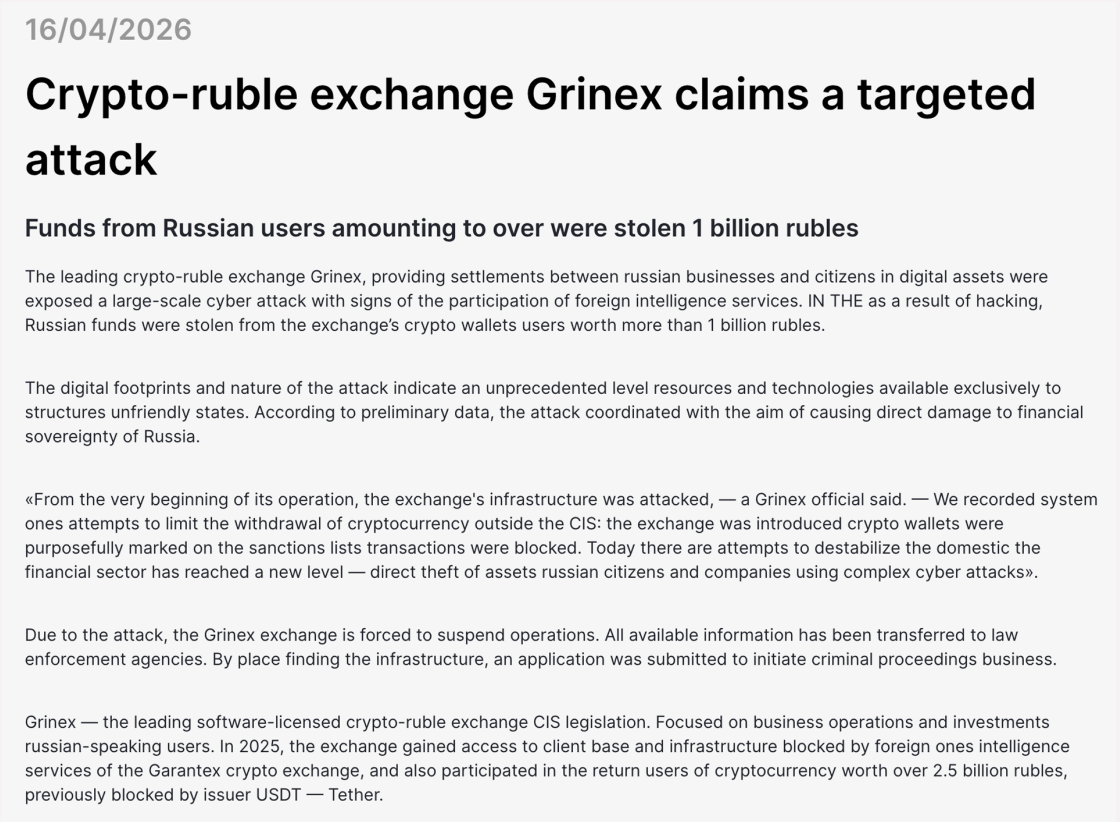
Use Cases

A7A5 operates as a sanctions-resilient settlement medium. Four use-case clusters are observable from on-chain activity, public statements, and venue-level data.

1. **Cross-border settlement for sanctioned Russian commercial actors.** A7 LLC sells A7A5 to Russian businesses cut off from correspondent banking. The token is the settlement medium for trade with counterparties in Kyrgyzstan, the UAE, and Central Asia willing to accept ruble-denominated digital assets.
2. **Garantex and Grinex liquidity bridge.** Following the March 6, 2025 Garantex takedown and Tether's freeze of approximately $28 million held in its wallets, successor exchange Grinex relisted A7A5 within weeks and credited Garantex customers with A7A5 in amounts equivalent to their frozen USDT. A7A5 then served as the bridge back to USDT via a dedicated DEX. Approximately $11.2 billion in A7A5/RUB and $6.1 billion in A7A5/USDT pair activity have been recorded, primarily on Grinex. On April 16, 2026, the exchange announced it had been hacked for approximately $15 million.

The exchange attributed the attack to “foreign intelligence services” and suspended operations. The incident has two direct implications:

- First, with Grinex suspended, the primary A7A5/USDT and A7A5/RUB liquidity is offline. No comparable alternative exists at scale.
- Second, the attack demonstrates that even a network designed to be sanctions-resistant remains vulnerable to cyber operations. The concentration of A7A5 liquidity in a single sanctioned exchange is a structural fragility.



16/04/2026

Crypto-ruble exchange Grinex claims a targeted attack

Funds from Russian users amounting to over were stolen 1 billion rubles

The leading crypto-ruble exchange Grinex, providing settlements between russian businesses and citizens in digital assets were exposed a large-scale cyber attack with signs of the participation of foreign intelligence services. IN THE as a result of hacking, Russian funds were stolen from the exchange’s crypto wallets users worth more than 1 billion rubles.

The digital footprints and nature of the attack indicate an unprecedented level resources and technologies available exclusively to structures unfriendly states. According to preliminary data, the attack coordinated with the aim of causing direct damage to financial sovereignty of Russia.

«From the very beginning of its operation, the exchange's infrastructure was attacked, — a Grinex official said. — We recorded system ones attempts to limit the withdrawal of cryptocurrency outside the CIS: the exchange was introduced crypto wallets were purposefully marked on the sanctions lists transactions were blocked. Today there are attempts to destabilize the domestic the financial sector has reached a new level — direct theft of assets russian citizens and companies using complex cyber attacks».

Due to the attack, the Grinex exchange is forced to suspend operations. All available information has been transferred to law enforcement agencies. By place finding the infrastructure, an application was submitted to initiate criminal proceedings business.

Grinex — the leading software-licensed crypto-ruble exchange CIS legislation. Focused on business operations and investments russian-speaking users. In 2025, the exchange gained access to client base and infrastructure blocked by foreign ones intelligence services of the Garantex crypto exchange, and also participated in the return users of cryptocurrency worth over 2.5 billion rubles, previously blocked by issuer USDT — Tether.

Figure 11: Grinex homepage message, which has been machine-translated from Russian into English

3. **Yield-bearing settlement balance.** The rebasing mechanism (50% of Promsvyazbank deposit interest passed to holders via _totalLiquidity adjustments) makes A7A5 attractive to hold rather than to transact with. Neither USDT nor USDC passes reserve income to holders. The design retains liquidity in-system and reduces the issuer’s effective cost of capital.
4. **Adjacent laundering exposure.** A7A5’s parent ecosystem has documented exposure to ransomware proceeds linked to Conti, Black Basta, and LockBit, and to DPRK-attributed funds including more than $30 million traced from the 2023 Horizon Bridge hack. No public evidence shows that A7A5 itself has been the issuance vehicle for these flows, but the venue overlap means a meaningful share of A7A5 activity touches wallets with prior illicit-flow exposure.

International Regulatory Response

A7A5 has been the subject of the most coordinated multi-jurisdictional sanctions response ever applied to a specific stablecoin. The actions to date establish a graduated enforcement model that distinguishes between targeting issuer entities, the token itself, and the surrounding crypto-asset service provider infrastructure.

Sanctions Response by Enforcement Layer

Layer	Target	Instrument	Observable effect
Entity layer	Old Vector, A7 LLC, A71, A7 Agent, Grinex, named individuals	OFAC SDN, UK OFSI, EU restrictive measures	Asset freeze, U.S.-person prohibition. Issuer retains operational capability via destroyBlackFunds reset.
Token layer	A7A5 named explicitly	EU 19th package (Annex LIII, Reg. 833/2014), effective Nov 25, 2025	Transaction prohibition for EU persons. First instance globally of named cryptocurrency placed under explicit transaction ban.
Infrastructure layer	All CASPs in Russia; Belarusian crypto providers	EU 20th package, Art. 5b, effective May 24, 2026	Categorical ban independent of entity designation. Targets the operational pattern rather than specific platforms, neutralizing the rebrand strategy.

Western Enforcement Timeline

United States: OFAC (August 14, 2025). The U.S. Treasury's Office of Foreign Assets Control designated Old Vector LLC (the Kyrgyz issuer of record), the Grinex exchange (successor to Garantex), and individuals tied to the A7 network. The designation explicitly identified A7A5 as a ruble-backed digital asset and placed the issuance and trading infrastructure within the SDN framework.

United Kingdom: FCDO and OFSI (August 20, 2025). The UK Foreign, Commonwealth, and Development Office, in coordination with HM Treasury's Office of Financial Sanctions Implementation, issued designations against Grinex LLC, CJSC TENGRICOIN, Old Vector LLC, OJSC Capital Bank of Central Asia, and Altair Holding SA. Three individuals were also designated. The UK action focused on the entity and individual layer, rather than naming the token directly.

European Union: 19th and 20th Sanctions Packages (October 23, 2025 and April 23, 2026). The EU's 19th package became the first sanctions instrument anywhere to place an explicit transaction ban on a named cryptocurrency: Annex LIII of Regulation 833/2014 was amended to list A7A5 specifically, prohibiting EU persons from engaging in any transaction involving the token, effective November 25, 2025. The package also designated the developer of A7A5 and the operator of the primary trading platform. The 20th package (effective May 24, 2026) widened the perimeter from specific designated entities to broader categorical bans: RUBx (the Rostec-issued ruble stablecoin) and the Russian central bank digital ruble were added to Annex LIII alongside A7A5, and a new Article 5bb of Regulation 833 introduced a blanket prohibition on transactions with crypto-asset service providers established in Russia, with mirror measures extended to Belarusian crypto providers and the Belarusian digital ruble. Rather than chasing specific platforms, which routinely rebrand, the EU is now sanctioning the operational pattern itself.

Uniswap protocol-level blocklist (November 2025). Following the EU designation, Uniswap added A7A5 (and its wrapper wA7A5) to its frontend blocklist, removing the token from the leading decentralized exchange interface. The underlying smart contracts remained accessible, but the practical effect was to remove A7A5 from the most common DeFi access path.



Figure 12: Regulatory Response chart

Russian Domestic Recognition

In parallel with Western enforcement, the Russian Central Bank formally recognized A7A5 as a Digital Financial Asset under Russia's domestic DFA framework in October 2025. This recognition created a domestic legal status for the token within Russia, enabling integration with the Tokeon platform (PSB-owned) and with regulated Russian institutional users. The contrast is structurally significant: A7A5 is simultaneously a sanctioned object in the West and a legitimized financial instrument in Russia.

The Singapore Paradox

A7A5 was a sponsor of the Token2049 conference in Singapore in late 2025. Singaporean sanctions on Russian entities are scoped to licensed financial institutions only. Singapore therefore did not block the participation. The episode illustrates the gap between the U.S., UK, and EU enforcement perimeter and the broader Asian regulatory landscape.

The African Vector: A Regulatory Blind Spot

At the Russia-Africa Partnership Forum in Cairo, Lavrov invited all African nations to join A7, the same network designated by the U.S., UK, and EU as a sanctions-evasion instrument. The African expansion exposes a structural gap in the current enforcement architecture. A7 has established offices in Nigeria and Zimbabwe, with Togo potentially next. The operational significance lies less in current footprint than in institutional framing. PSB Deputy Chairman Dorofeev visited Madagascar in January 2026 for discussions with its new military government, stating his ambition to establish a financial "corridor" in southern Africa. A7A5's African corridor is being activated in direct parallel with Russia's military deployments, creating a financial rail for arms transfers that bypasses Western correspondent banking entirely. Nigeria, Zimbabwe, Togo and Madagascar all maintain banking relationships with Western-aligned institutions, meaning their banks acquire potential secondary-sanctions exposure simply by processing flows from A7-linked local fronts such as Pilot Finance Limited in Lagos. No African jurisdiction has to date been formally engaged by OFAC, HM Treasury, or the EU on A7A5-related exposure. That absence is the most actionable gap in the current international response.

Conclusion

The stablecoin threat landscape in 2026 is defined by two converging forces. The first is the continued evolution of opportunistic attacks on interconnected financial infrastructure, including bridges, custody systems, payment APIs, and settlement layers, which together accounted for hundreds of millions in losses in the first half of the year alone. The second is the deliberate weaponization of stablecoin architecture by state-adjacent actors operating outside Western enforcement reach. Understanding either force in isolation understates the overall risk.

A7A5 is a proof of concept. Its design demonstrates that a state-adjacent actor, operating under comprehensive Western sanctions, can construct a stablecoin that processes over $110 billion in transactions within its first year, achieves formal domestic legal recognition, and sustains continuous holder growth despite coordinated international enforcement. The broader implication for the digital asset industry is significant: the tools of compliant stablecoin infrastructure, including centralized minting, reserve backing, and on-chain compliance controls, can be mirrored and deployed entirely outside Western enforcement reach.

The international response to A7A5 has been genuinely unprecedented. The EU's decision in its 19th sanctions package to name a specific cryptocurrency in a transaction ban was a regulatory first, and the 20th package's shift toward categorical bans on crypto-asset service providers established in Russia represents a meaningful strategic evolution, moving from chasing individual platforms that routinely rebrand to sanctioning the operational pattern itself. However, the on-chain data makes clear that these measures have contained rather than dismantled the network. As long as the underlying user base of Russian commercial actors, Kyrgyz and Central Asian counterparties, and an expanding African corridor operates outside the enforcement perimeter, holder growth and settlement volumes are unlikely to reverse materially.

The African expansion is the most urgent unresolved risk. A7 has established offices in Nigeria and Zimbabwe, with Togo potentially next, and Russia's outreach at the Russia-Africa Partnership Forum has framed the network in explicitly institutional terms. Banks in these jurisdictions maintaining correspondent relationships with Western-aligned institutions risk acquiring secondary-sanctions exposure through local A7-linked entities, yet no African regulator has been formally engaged on this exposure. Closing this gap requires coordinated outreach by OFAC, HM Treasury, and the EU to regulators in at-risk jurisdictions, combined with private-sector guidance for correspondent banks on identifying A7-linked transaction patterns.

Best Practices for Compliance and Risk Teams

- **Treat ruble-pegged stablecoins as high-risk by default.**
  Any token with ruble collateral, Russian issuer relationships, or PSB involvement should trigger enhanced due diligence regardless of the issuing entity's stated jurisdiction.
- **Monitor for venue migration.**
  The Garantex-to-Grinex rebrand illustrates that sanctioned infrastructure routinely reconstitutes under new names. Compliance programs should track behavioral and on-chain continuity, not just entity names.
- **Screen for A7A5 contract addresses explicitly.**
  As of this report, OFAC has not added A7A5's Ethereum or Tron contract addresses to the SDN list. Firms should add these addresses to internal screening lists proactively: Ethereum (`0×6fA0BE17e4beA2fCfA22ef89BF8ac9aab0AB0fc9`) and Tron (`TLeVfrdym8RoJreJ23dAGyfJDygRtiWKBZ`).

- **Assess correspondent banking exposure in A7A5-active jurisdictions.**
  Institutions with correspondent relationships in Nigeria, Zimbabwe, Kyrgyzstan, and the UAE should review whether local counterparties have exposure to A7-linked entities such as Pilot Finance Limited.
- **Account for the paper-note layer in investigations.**
  A7's Digital Promissory Note hybrid instrument removes value from the public ledger entirely until the next conversion event, creating a gap analogous to trade-based money laundering. On-chain analysis alone is insufficient to trace the full transaction lifecycle.
- **Prioritize security hardening for bridge and interoperability infrastructure.**
  Given that bridge-related incidents accounted for the majority of stablecoin-adjacent losses in 2026, firms should conduct regular independent audits of cross-chain messaging logic, validator systems, and multisig controls.
- **Treat wallet compromise as an operational risk.**
  The dominance of wallet compromise as an exploit vector in 2026 reflects failures in access control, key management, and insider threat detection rather than on-chain code alone. Security programs should reflect this accordingly.

CERTIK

Company Overview

CertiK is the largest Web3 security services provider, founded in 2017 and headquartered in New York. The company supports the secure adoption of blockchain technology by financial institutions, enterprises, and regulated crypto businesses.

Spanning the full digital asset lifecycle, CertiK provides security and compliance services including DLT infrastructure assessments, custody architecture reviews, penetration testing, code audits, formal verification, and compliance-focused security engagements.

CertiK also works with regulators and financial institutions across multiple jurisdictions, contributing to policy development and regulatory consultation efforts.

5,100+
Clients Served

180,000+
Vulnerabilities Detected

$600B+
Market Cap Assessed

70%+ of the Top 500 CoinMarketCap Projects Audited

Trusted Across Leading Ecosystems

BNB Chain · Bitcoin · TON · Cosmos · Cardano · Aptos · Algorand · Sui · Kaia · ZKPs

Elevate Your Web3 Journey

certik.com | bd@certik.com