From Stablecoins to 'Digital Bills of Exchange': Why Monitoring After Sanctions Implementation Is Critically Important

Dr Tetiana Dmytrenko - Founder and Chair of NGO 'Ukrainian Modern Digital Science', Chair of the Finance Committee of the Public Council of the Ministry of Finance of Ukraine, a member of the Public Council under the State Financial Monitoring Service (FIU) of Ukraine.

James Ramsden KC – Senior Partner at Astraea.

Dr Khrystyna Khanas – Associate at Astraea.

Introduction

When another package of sanctions against an aggressor country comes into force, it may seem that the financial flows of its regime are about to dry up. In reality, sanctions are not the finish line, but only the beginning of a new round of confrontation: sanctioned individuals and companies immediately look for loopholes to circumvent restrictions and often act faster than regulators can respond. A striking example is the rouble-pegged stablecoin A7A5, launched in Kyrgyzstan in early 2025, which facilitated the transfer of US$ 9.3 billion in Russian funds within just four months, despite Western sanctions. This laid bare the scale of the problem: without continuous monitoring after the sanctions are imposed, even the strictest bans can prove powerless in the face of creative approaches to financial circumvention.

We wrote about A7A5 and Grinex in our previous article with Alexandr Chernykh. In this article, we examine how the A7A5-Grinex scheme works, why it became possible, and what lessons can be learnt for effective sanctions control.

A7 'digital bills of exchange': a new tool for circumventing sanctions

In 2025, the financial company A7 introduced a product that appeared to be legal at first glance – the 'A7-Kyrgyzstan digital bill of exchange' – intended for international settlements. In fact, it implemented the A7A5 stablecoin, the rouble value of which was secured by bank deposits. The bill (debt obligation) provides the holder with A7A5 tokens, which are pegged to the Russian rouble at a 1:1 exchange rate and fully backed by the real funds. According to the intention of its developers, this instrument allows Russians to legally and conveniently transfer money abroad. When circulated, the 'digital bill of exchange' performs several functions at once: it can be exchanged for any currency in any country (the limit is up to the equivalent of US$ 10,000 in cash for export) and can be quickly converted back into cash or a bank account outside the Russian Federation. Its owners can store this asset in the form of tokens, exchange them for popular cryptocurrencies (USDT, BTC, ETH, etc.) and even spend them abroad using Mir (Russian national payment system) and Visa payment cards. Formally, this looks like a convenient service for travellers and businesses, but its real role is to serve as a bridge for Russian money to bypass financial sanctions.

The basis of this scheme is the A7A5 stablecoin, the world's first digital token pegged to the Russian rouble. It was officially launched in Kyrgyzstan in February 2025, positioning itself as a payment solution that would soften the blow of the Western sanctions on large cross-border payment transactions of the Russian Federation. The mechanism is simple and effective: Russian users buy A7A5 tokens on the Tron or Ethereum blockchain, then exchange them for the equivalent in Tether (USDT, a stablecoin pegged to the dollar). Once they have received the USDT, they can withdraw it in any country and currency they want — in effect, the money is transferred outside Russia, bypassing SWIFT and other traditional channels. Importantly, for every rouble spent on the purchase of A7A5, a real rouble is credited to an account with Promsvyazbank – a large Russian defence sector bank, which is sanctioned by the US, the UK and the European Union. Thus, A7A5 is completely dependent on Russian financial institutions that are subject to sanctions: the token's reserves are held in Promsvyazbank accounts, and 49% of A7 itself is owned by Promsvyazbank (other support came from the state-owned corporation VEB.RF – the State Corporation Bank for Development and Foreign Economic Affairs Vnesheconombank).

Moreover, as the Financial Times investigation revealed, the beneficiary of A7 is the notorious Moldovan oligarch Ilan Shor, who fled to Russia from criminal prosecution in his homeland. According to British sanctions lists, Ilan Shor was behind the creation of A7A5 and openly stated that he was building a "larger, differentiated and sufficiently invulnerable" payment system that would include alternative instruments – securities exchange, precious metals, etc. – all to avoid the regulatory control.

In other words, this is an entire shadow ecosystem designed to protect Russian money from the impact of sanctions. We wrote about the launch of the A7A5 stablecoin and the sanctions imposed by the US, the EU and the UK in our previous articles – 'Russia is one step ahead in the game of crypto 'whack a mole''; 'The crypto web of power: the story of A7A5, Grinex and Shor' and 'A7A5 in the crosshairs of the European Union: a new phase in the sanctions war.'

It is now obvious that the launch of the A7A5 token in Kyrgyzstan is not a coincidence, but a well-thought-out move. Kyrgyzstan has one of the most cryptocurrency-friendly laws in Central Asia. The token issuer (Old Vector LLC) was officially registered in this country, having obtained the necessary permission to issue tokens. It is A7-Kyrgyzstan that acts as the guarantor of A7A5.

Western analysts immediately sounded the alarm: according to the Centre for Information Resilience (CIR), this project is clearly aimed at "moving money across borders" and poses "a serious challenge to existing sanctions regimes." In other words, the Russian company A7 (together with its Kyrgyz subsidiaries) created A7A5 as a parallel payment system to circumvent international sanctions.

The token operates in a 'narrow ecosystem' of services related to the Russian Federation and is traded mainly on weekdays, i.e. it is focused on business transactions of Russian clients. It's also worth noting that by the end of July 2025, transactions worth over US$51 billion had been conducted through A7A5 – that is a colossal turnover for an instrument that had appeared just a few months earlier. In terms of the scale, this rouble stablecoin quickly became the world's largest stablecoins not pegged to the US dollar. In fact, A7A5 has become the Kremlin's 'shadow digital currency', a channel for financing which has long remained unnoticed by Western regulators.

Grinex Exchange: the successor to Garantex and the 'shadow exchanger' of the Russian crypto economy

Another important element of the scheme is the Grinex cryptocurrency exchange, also registered in Kyrgyzstan. It was founded in March 2025, just a few weeks after the US authorities shut down the previous Russian exchange, Garantex.

Since 2019, Garantex has been notorious for its dubious transactions (at least US$100 million, linked to money laundering by hackers and darknet markets, passed through it) and was sanctioned by the US in 2022. Despite this, Garantex continued to operate in the shadows until spring 2025, when law enforcement agencies finally seized its servers and infrastructure and brought charges against the exchange's management. The closure of Garantex prompted its organisers to implement 'plan B' – the launch of a new platform, Grinex, to which client funds and the liquidity of the old exchange were quietly transferred.

Global Ledger's (a blockchain analytics company) investigators traced a direct succession: before being shut down, Garantex transferred about 4.5 billion A7A5 tokens to Grinex wallets. The interface, marketing campaigns, and even the source code of the new exchange were suspiciously reminiscent of its predecessor. So it is not surprising that analysts call Grinex a 'clone' of Garantex, specifically created to serve the rouble stablecoin and Russian clients that are cut off from other markets.

According to the Financial Times, trading volumes on Grinex reached US$9.3 billion in January – April 2025 alone, with most transactions being conducted in A7A5 tokens. This rapid growth attracted the attention of the international community: has the Kyrgyz exchange become the main hub for circumventing Russian sanctions? These fears proved to be well-founded: Grinex, as it turned out, was closely linked not only to the creators of Garantex, but also to the entire A7 network of companies. Both the A7A5 stablecoin and the Grinex exchange were managed by the same people, who are closely connected to Russian financial structures.

It's worth mentioning that the state-owned Promsvyazbank is a co-owner of A7. The Kyrgyz company Old Vector LLC, the issuer of the A7A5 token, was also involved in the scheme. In August 2025, OFAC (US) and the British regulator OFSI simultaneously imposed sanctions against Grinex, Old Vector and related figures, recognising their role in facilitating the Russian crypto-evasion scheme. Several Kyrgyz banks and companies involved in this scheme were also sanctioned, including CJSC Tengricoin (operator of another exchange, Meer) and Altair Holding. The UK has explicitly stated that the A7A5 stablecoin 'pumped' US$9.3 billion in just four months and became a key element of the Kremlin's shadow finances.

These connections were largely uncovered thanks to the monitoring of blockchain transactions. Global Ledger's analysts began tracking the movement of funds between Garantex wallets and new Grinex wallets in the spring of 2025. They identified 312 crypto wallets associated with the Grinex exchange, many of which previously belonged to Garantex. Interestingly, after OFAC imposed sanctions on Grinex in August 2025, most of the known wallets ceased activity — but at least four addresses continued to function, holding a significant amount of tokens. This means that even after sanctions, part of the infrastructure remained in the shadows and did not immediately fall under the sanctions lists. Such loopholes arise because sanctioned individuals prepare backup routes and new legal 'faces' for their businesses in advance. In the case of Grinex, the founders claimed that it was an 'independent' Kyrgyz company and denied any connection with Garantex or A7A5. However, evidence on the blockchain (shared IP addresses of websites, simultaneous registration of companies, transfers of huge sums between wallets) refuted these claims. Ilan Shor – already identified as the architect behind A7A5 – was also found by RFE/RL journalists to be likely personally involved in the scheme — it was through a network of companies from Moscow to Bishkek that he was able to control both A7A5 and Grinex. Despite being under sanctions and even convicted in absentia in the EU and the US, Ilan Shor was still able to play the role of the 'gray cardinal' of the project.

Unfortunately, the Kyrgyz authorities have been evasive and unresponsive to the journalists' enquiries. The body responsible for supervising digital assets in Kyrgyzstan confirmed only that Grinex was registered on its register, but stated that it was 'still investigating' whether this was the same exchange that the international press was writing about. The Kyrgyz ministries of finance and economy stated that crypto exchanges were not within their jurisdiction.

This bureaucratic silence is causing concern among the Western partners. Experts warn that the lack of transparency creates ideal conditions for illegal activity, and Kyrgyzstan risks becoming a favourite ‘haven’ for those seeking to circumvent international controls. Simply put, if, after sanctions are imposed, there is no control over where the money of sanctioned individuals is moving, they will always find new ways – through a third country, a new crypto exchange or a front company.

Blockchain analytics: when transactions speak louder than words

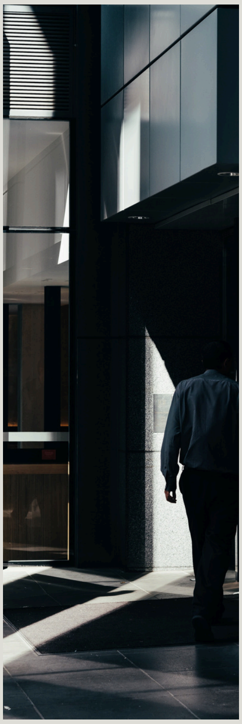
Despite the complexity of schemes such as A7A5-Grinex, international investigators have a powerful ally: blockchain’s transparency. Every cryptocurrency transaction leaves a trace in a public ledger, and with the right tools, even the most convoluted routes can be traced. In the case of A7A5, this was proven beyond doubt. Most of the token's transactions took place on the Tron network, which is popular among Russian users due to its low fees and speed. At the same time, Tron has an open ledger, and analysts were able to piece together a detailed picture of the movement of billions through this chain. In particular, Global Ledger’s specialists used their own blockchain analytics software to find that the liquidity of the stablecoin was largely created artificially: there were only three large Ethereum wallets endlessly ‘shuffling’ A7A5 and USDT among themselves, creating thousands of transactions without the inflow of new money. This practice is known as wash trading — inflating fictitious trading volumes to create the illusion of high demand. Another tactic was discovered on Tron: a number of interconnected wallets regularly ‘dumped’ the A7A5 they received, exchanging it for USDT through the project's smart contract. Moreover, the USDT came from a specific pool of addresses, which were replenished from more than 15 different exchanges, including those licenced in the EU. In other words, the organisers of the scheme used the global crypto infrastructure to feed the rouble stablecoin with dollar liquidity, masking these injections as ordinary transactions.

Monitoring social media also yielded some interesting clues: on the official A7A5 Telegram channels, announcements of large token sales often appeared simultaneously with regular injections of USDT into the liquidity pool. It looked like a planned campaign to attract buyers — as if to say, “Look, we have a lot of USDT for exchange again, hurry up and buy A7A5”. In some cases, analysts noticed that ‘big buyers’ began to withdraw USDT literally a minute before the public announcement — clearly acting on insider information. Taken together, these observations indicate that the entire environment surrounding A7A5 was manually controlled and not truly market-driven. The main goal was to ensure the functioning of a ‘transit channel’ for money, rather than to create a popular mass asset.

It is not a coincidence that A7A5 transactions took place mainly on working days and hours according to Moscow time, as if they were bank transfers rather than round-the-clock cryptocurrency transactions. User support for the token was also provided only during the working hours of the Moscow offices, and it was possible to buy the token for cash directly at the Grinex office in Moscow (located in the Moscow City skyscraper, where the Garantex office was previously located). These facts, established by journalists and blockchain analysts, shed light on the true nature of A7A5: it is not so much an innovative financial product as a cleverly disguised 'transit channel' for Russian money.

It should be noted that after the sanctions were imposed, the financial company A7 slightly changed its approach to the circulation of the A7A5 stablecoin. In addition to issuing the 'A7 digital promissory note' - which significantly complicates transactions with the A7A5 stablecoin by exchanging it for fiat paper financial instruments such as cash and the so-called 'A7 promissory note' – UMDS experts, using the AMLbot PRO blockchain analysis software, tracked almost all transactions related to A7A5 and 'A7 digital promissory notes' on the Tron network and identified characteristic patterns of fund movements. In addition, they detected the replacement of A7A5's simulated liquidity with real collateral, i.e., the actual injection of large sums of money. The peak times of transaction activity also changed, indicating the development of new regions of activity.

'A7 digital bill': a new level of obfuscation of money transit



If the A7A5 stablecoin became the main 'digital pipeline' for circumventing sanctions, the 'A7 digital bill of exchange' became its shadow partner – a versatile paper-digital tool designed to add another layer of opacity to cross-border schemes. Formally, it is positioned as a classic simple or interest-bearing promissory note, but with modern elements: it can be purchased at branches of 'A7 Finansy' in Russia, transferred to a counterparty through endorsement and used to pay for international contracts or settlements in any currency (USD, EUR, CNY, AED) — as openly stated in A7's presentation materials. Thanks to this instrument, the company has been able to convert easily traceable transactions in roubles into paper bills of exchange, which are subsequently recorded in the accounts as ordinary corporate payments rather than cryptocurrency or financial transfers by sanctioned banks.

The bills are mainly issued by Russian structures within the A7 group, but their key feature is that they are subsequently 'cashed' abroad. The recipient can redeem the bill of exchange at A7 partner entities outside the Russian Federation (including in Dubai, Kyrgyzstan, Kazakhstan or Turkey), where they are paid the equivalent in USDT or foreign currency cash. Thus, the rouble amount is officially removed from Russian jurisdiction in the form of a bill of exchange and is redeemed through the A7 infrastructure as digital assets or cash. This mechanism allows the true nature of the transaction to be concealed: in accounting, it is a 'bill of exchange as a financial investment' or 'payment of obligations', but in reality, it is a transfer of money abroad and the issuance of convertible currency to the client, which cannot then be directly linked to its Russian origin.

Due to the ability to transfer a bill of exchange via endorsement in the form of a QR code, the instrument is ideal for concealing its origins. The chain of bill of exchange owners is not recorded in a centralised ledger, and thus, in effect, creates 'anonymous circulation' of debt obligations, which can be exchanged between Russian and foreign companies without leaving any digital traces. When the bill of exchange is finally presented for redemption at one of the A7 points abroad, the transaction looks like the legal fulfilment of debt obligations, although in reality it is the final stage of a hidden transit of funds.

Exactly that construction – paper bill of exchange → transfer to a third party → repayment in USDT/cash — creates a new 'gray area' for regulators. Unlike stablecoins, the movement of bills of exchange is virtually impossible to track automatically, and their circulation is not subject to the same AML/KYC rules that apply to digital assets. In some cases, a 'digital bill of exchange' is used as an intermediate instrument: the buyer first receives the bill of exchange, and then employees of the A7 subsidiary convert it into a digital A7A5, which is immediately exchanged for USDT on Grinex or another affiliated exchange. Thus, the bill of exchange allows paper, bank and cryptocurrency transactions to be mixed in a single path, which significantly complicates the entire chain of tracking.

In fact, the A7 group has built a hybrid mechanism for the transit of sanctioned funds, where fiat bills of exchange are used as a legal front, and final payments are made in digital currencies or cash outside Russia. That is why 'A7 digital bills of exchange' are becoming the next level of threat after A7A5: unlike the Tron blockchain, their circulation is not transparent, they easily cross borders and allow sanctions to be avoided not only technically, but also legally. In combination with A7A5 crypto channels, they form a synchronised system for circumventing sanctions, which international regulators need to take into account when assessing risks and planning new sanctions packages.

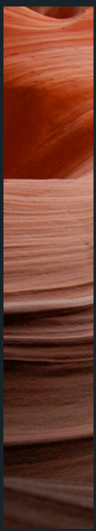
These revelations were made possible due to vigilant monitoring after the sanctions were imposed. Initially, neither A7A5 nor Grinex were on the sanctions lists, as they were simply unknown. Only after independent researchers (FT, CIR, Global Ledger) published the results of their investigations did Western governments make changes.

In October 2025, the EU imposed a direct ban on any transactions with the A7A5 stablecoin as part of its 19th sanctions package. As noted, the UK and the US had already imposed sanctions on the organisers of the scheme. However, by that time, significant amounts had already passed through the system. Moreover, A7A5 operators anticipated the blow and prepared in advance: after the US sanctions against Grinex in August 2025, the stablecoin administrators quickly carried out a technical operation to sever the link between the token and the sanctioned exchange. They used a special smart contract function (the destroyBlackFunds command) to destroy the old tokens in two wallets linked to Grinex, which held 33.8 billion A7A5 (worth approximately US$405 million, or more than 80% of all tokens). Immediately after that, the exact same amount of new A7A5 was issued in another wallet. This 'trick' effectively broke the direct chain of transactions leading to the Grinex exchange, making it harder to track the token's links to the sanctioned platform. The Financial Times notes that the activity of the new wallet (through which A7A5 now circulates) completely replicates the typical behaviour of the old ones – transactions take place at the same times and in the same mode. This is further proof that all roads lead to the same hands, but the puppeteers have skilfully intertwined them as soon as the old schemes began to 'burn'.

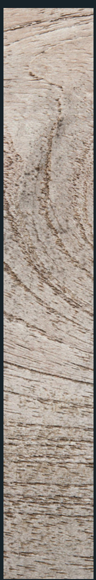
Thus, modern monitoring technologies — from analytical platforms such as Global Ledger, AMLbot PRO and Chainanalysis — allow even the most complex multi-step combinations of money laundering or transfer of sanctioned funds to be exposed. However, this is not enough if the response to such exposures is delayed. The A7A5 story clearly shows that sanctions alone do not guarantee success if there is no ongoing post-sanction monitoring.

Recommendations: how to prevent sanctions from being circumvented and increase their effectiveness

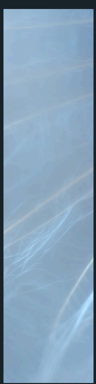
Based on the case described above, several key conclusions and recommendations can be formulated regarding the monitoring of sanctions regimes:



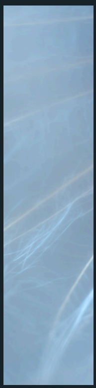
Continuous monitoring of sanctioned entities: Sanctions should be viewed not as a one-off action, but as a process. Once a person or company has been added to the sanctions list, their activities must be continuously monitored. Which counterparties continue to work with them? Have any new affiliated structures have been created? Have related projects suddenly appeared in other jurisdictions (as was the case with Garantex's move to Kyrgyzstan under the guise of Grinex)? Monitoring can be carried out through analysis of open data, journalistic investigations, and intergovernmental information exchange. It is important to establish international cooperation, as sanctioned assets can easily ‘migrate’ across borders.



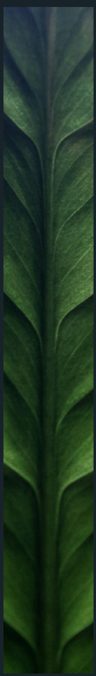
Analysis of next steps after the imposition of sanctions: Each sanction triggers a reaction from its targets. Therefore, it is worth predicting and tracking the next moves of those subject to sanctions. For example, as we previously wrote, after Russian banks were blocked from SWIFT, they rushed to develop cryptocurrency channels; after Garantex was banned, Grinex appeared; after some assets were frozen, oligarchs quickly re-registered them to relatives or front men. Analytical centres and special services must monitor such trends in real time in order to stop them promptly. To do this, they use OSINT intelligence, blockchain analytics (as in the example with the Tron network) and close cooperation with private analytical companies that already have experience in this field (AMLbot PRO, Global Ledger, Crystal Intelligence, Chainalysis, etc.).



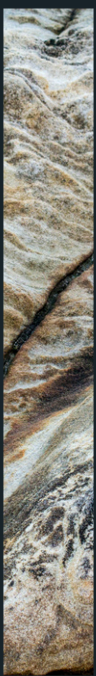
Identification and neutralisation of new circumvention schemes: Sanctions pressure inevitably leads to innovation in sanctions evasion. This may be the release of new financial products (stablecoins, ‘digital promissory notes’, surrogate currencies), the use of third countries and their financial systems (such as banks and exchanges in countries friendly to the Russian Federation), or a transition to barter and non-financial methods (barter, cryptocurrency payments for raw materials, exchange through gold reserves, etc.).



The task of the sanctioning authorities is to constantly brainstorm and model possible loopholes in order to stay ahead of the perpetrators. Regulators must closely monitor the emergence of suspicious projects, such as A7A5, and promptly include them (and their beneficiaries) in sanctions lists as soon as the true nature of such projects becomes clear. Financial intelligence data and insider information from industry informants are also useful, as market participants themselves often report suspicious innovations.



Use of modern analytical tools: The experience with A7A5 has shown that even a complex network of transactions can be untangled if you have access to technological solutions. Platforms such as AMLbot PRO, Global Ledger, Crystal Intelligence, Chainalysis, Elliptic and others are capable of automatically tracking the movement of funds on blockchains, signalling the appearance of ‘dirty’ funds and establishing links between wallets and services. The implementation of such monitoring tools in financial investigations is a prerequisite for success. Banks and exchanges must also connect such tools to detect attempts to circumvent sanctions through their platforms in real time. This also applies to traditional financial counterparties: for example, they should check transactions with countries that may resell sanctioned goods more carefully and track abnormal delivery routes (to detect schemes for re-exporting sanctioned goods through third countries) etc.



Assessing the effectiveness of existing sanctions: It is extremely important to regularly reflect on and assess the real impact of sanctions and respond promptly if it turns out to be less than expected. Monitoring the financial indicators of sanctioned entities (income, assets, expenses), the state of their business empires and changes in the lifestyle of oligarchs all helps to determine whether the sanctions have had a significant impact. If it turns out that, for example, a sanctioned company continues to conduct international operations through subsidiaries or that the aggressor country still purchases critical goods (chips, technology) in significant volumes, then there is a loophole somewhere. Regular audits of sanctions regimes should lead to policy adjustments: closing identified schemes, expanding lists, strengthening export controls, and putting pressure on intermediary countries. Sanctions are a dynamic tool, and their flexibility and adaptability determine their success no less than their initial severity.

Conclusion

The case of the Kyrgyz stablecoin, A7A5, and the Grinex exchange is a wake-up call: the international community and regulators must not let their guard down and lose vigilance after sanctions are imposed. On the contrary, this is the moment to begin careful monitoring and analytical work to identify the next steps of the sanctioned players. The Kremlin's financial network has demonstrated high flexibility and technological savvy, but the international community is not standing still either. The public nature of blockchains, investigations by journalists and analysts, and coordination between countries are all becoming new weapons in the sanctions war. For sanctions to be effective, they must always be treated with the principle of 'trust but verify.' Once restrictions are in place, steps must be taken to ensure that they are not circumvented; if a new scheme is found, immediate action should be taken to stay ahead of the curve. Only then can sanctions pressure truly achieve its goal: depriving the aggressor of the resources to continue the war and forcing it to change.

info@astraea-group.com

0208 092 8411

Astraea Group Ltd
7 Down Street, London, W1J 7AJ

SRA No. 806283