The Shadow Crypto Economy Feeding Russia's War Machine

Gonzalo Saiz Erausquin

Research Fellow
Centre for Finance and Security at RUSI

About us

THE CENTRE FOR FINANCE AND SECURITY AT RUSI

The CFS was founded in 2014 to study security issues through a financial lens.

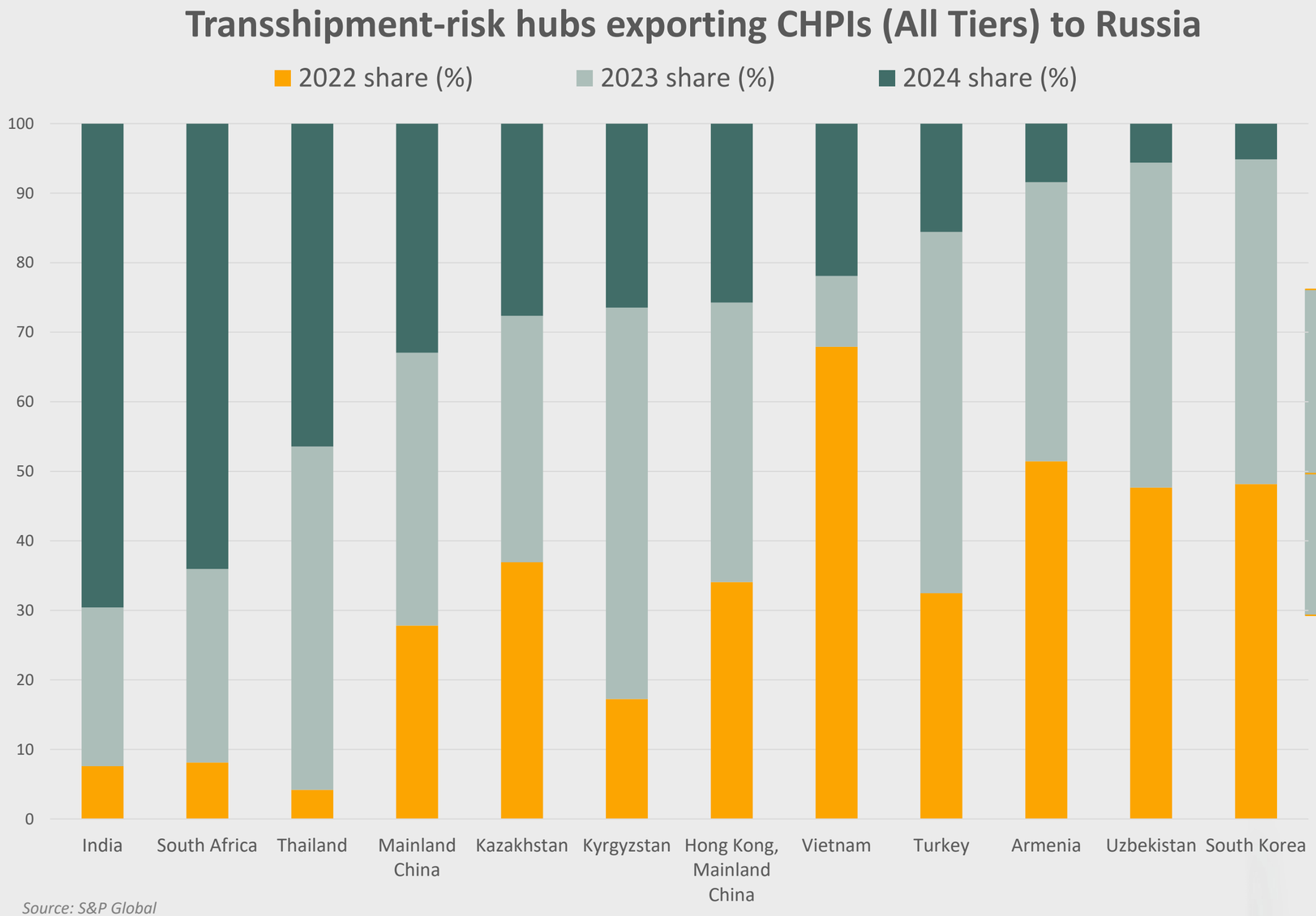
Our research focuses on the intersection of finance and security.

We address two key pillars:

- Financial Crime Policy, including the FATF standards and AML/CFT/CPF policy developments.
- Sanctions and State Threats, including UN and unilateral regimes and the financial dimension of electoral interference.



Trade sanctions and the rise of circumvention



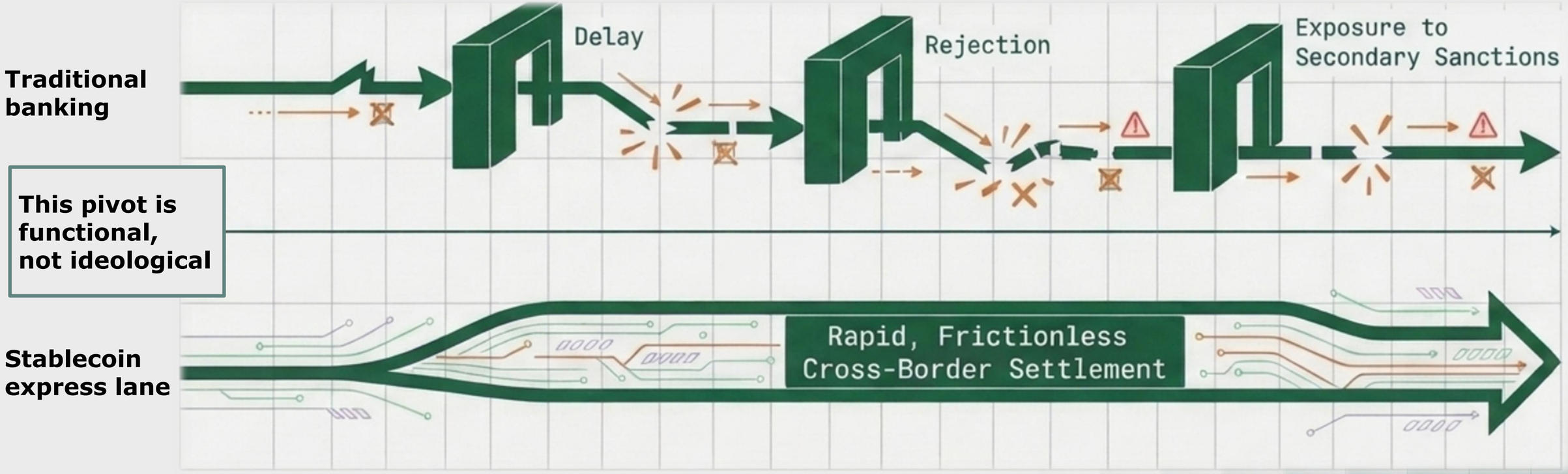
Source: S&P Global

Sourcing	Tier 1 flows are concentrated in Hong Kong and mainland China, with Thailand emerging as a new hub. Tier 4 flows are diversified across Central and Southeast Asia.
Impact	CHPI flows are highly sensitive to sanctions and require sophisticated evasion schemes and often centralised routing.

Crypto emerges as a financial lifeline

International banks, even in Russia-friendly jurisdictions, fear secondary sanctions, causing delays or outright rejections for Russia-linked trade.

Stablecoins like USDT provide rapid cross-border settlement without the need (and supervision) of correspondent banking relationships.



Garantex and Grinex

Garantex was responsible for **82% of all cryptocurrency volumes** associated with sanctioned entities worldwide and transacted over $96 billion.

2019
Garantex is founded

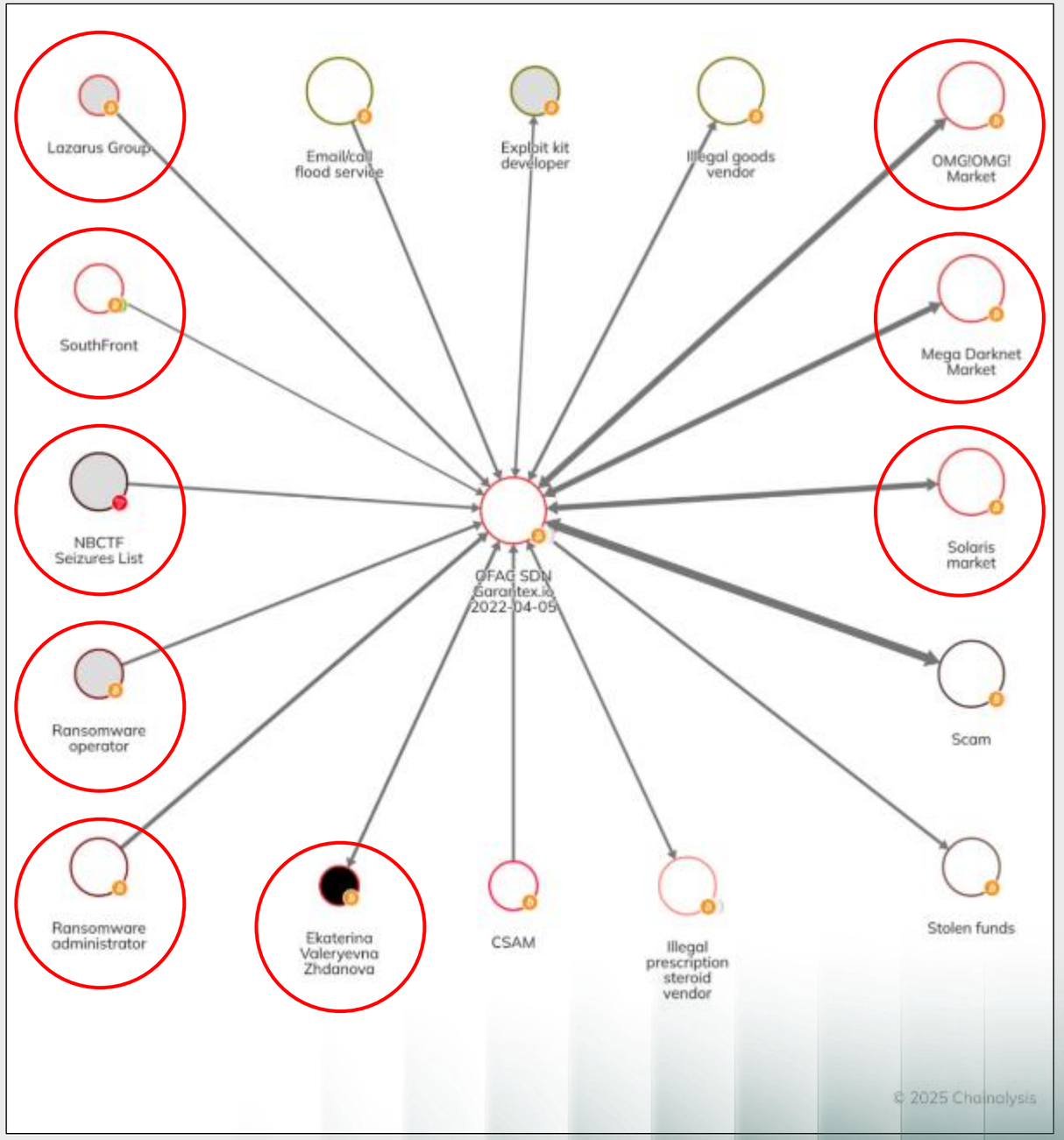
2022
Founder raided in Moscow

Apr 2022
OFAC sanctions Garantex

Dec 2024
Grinex domain launched

Mar 2025
Multinational takedown

Mar 2025
Relaunches as Grinex



© 2025 Chainalysis

A7 and A7A5

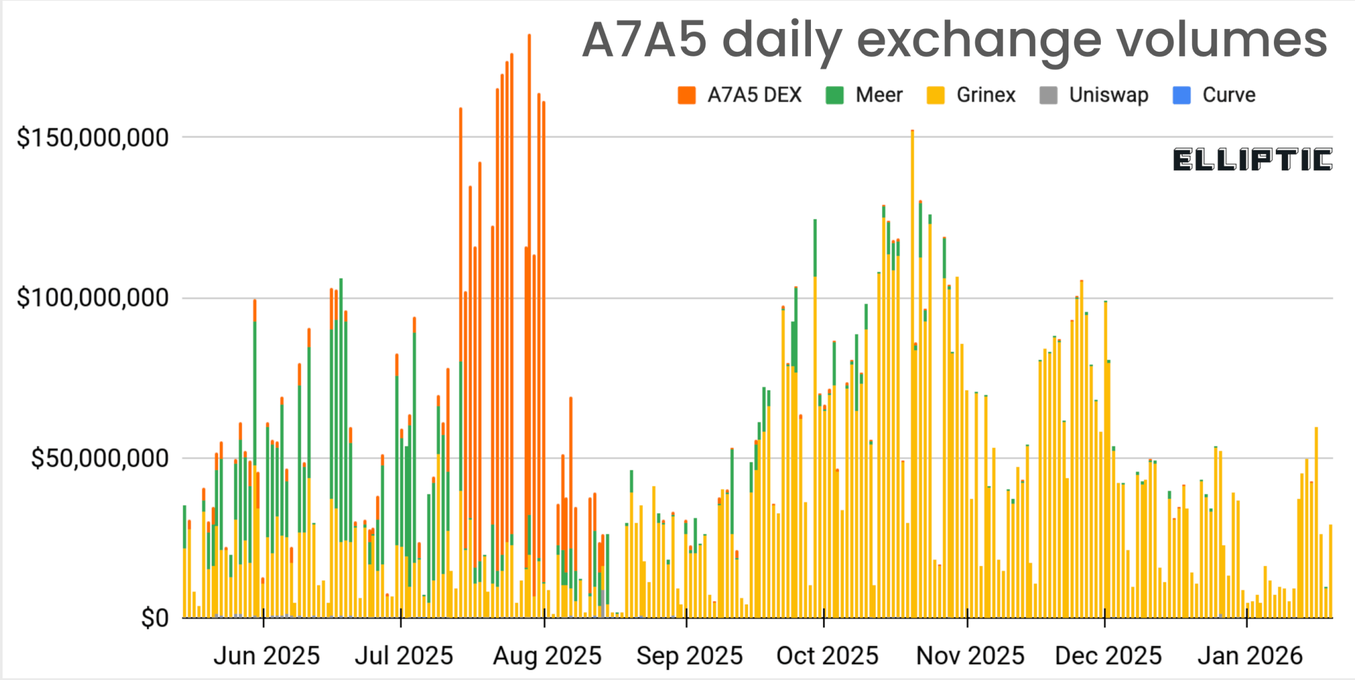
A7 is a Russian company established in Oct 2024
Majority owned by Ilan Shor (Moldovan fugitive), minority by Promsvyazbank (PSB)
Stated purpose is to facilitate cross-border transfers for Russian clients. Estimated around $90bn in annual flows.

A7 launched rouble-backed stablecoin A7A5
Launched via Kyrgyz shell company, Old Vector
Claims a 1:1 backing by Ruble deposits, held at PSB

Step 1 A Russian firm pays roubles to A7.

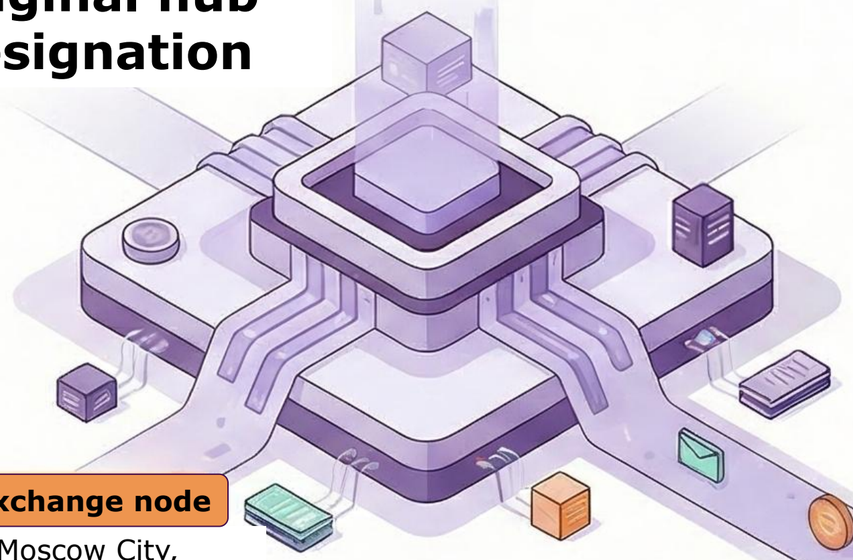
Step 2 Old Vector issues the equivalent in A7A5 tokens.

Step 3 A firm uses A7A5 on specialised exchanges to buy Western-linked stablecoins or pay foreign suppliers.



Russia’s crypto ecosystem

The original hub pre-designation



The central exchange node

Operated from Moscow City, specialising in high-volume rouble-to-stablecoin conversion for international trade.

$26 million frozen

International enforcement seized domains and funds, temporarily disrupting the primary rouble-to-crypto pipeline.

Designated infrastructure

Sanctioned by the US, EU and UK for facilitating illicit transactions and military-linked procurement.

Fragmentation and reconstitution

Infrastructure and personnel migrated to successor platforms like Grinex to preserve liquidity and service continuity.

Feeding the war machine

These networks facilitated payments for drone developers like KB Vostok to acquire critical military components.

The adaptive successor and continued procurement

Functional survival

Successor entities operate at a smaller, closed scale to avoid the visibility of the sanctioned nodes.

Mainstream exposure

The UK sanctioned entities linked to the A7 network, including the major global exchange HTX (formerly Huobi), alongside EXMO Exchange, Rapira Group, and Bitpapa.

HTX reportedly channelled $1.5 billion for Russia, allegedly through direct flows to sanctioned exchanges and the facilitation of cash-outs for A7.

GOV·UK

UK Sanctions List

HUOBI GLOBAL S.A.

< Back

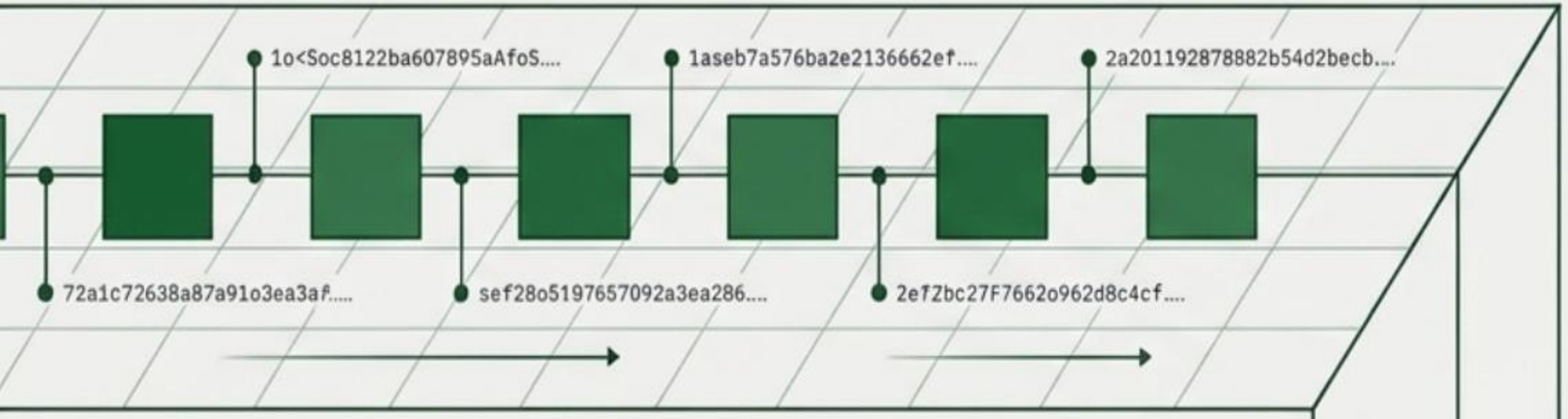
Designation | Names | Addresses | Entity | Download

Designation

Last updated 07 July 2026

Regime Name	The Russia (Sanctions) (EU Exit) Regulations 2019
Date Designated	26 May 2026
Designation Source	UK
Unique ID	RUS3619
OFSI Group ID	
UN Reference Number	
Sanctions Imposed	Asset freeze, Director Disqualification Sanction, Internet Services Sanctions: see "Other Information" | Correspondent Banking Sanctions and processing payments, Trust Services Sanctions
Other Information	Internet Services Sanctions: When an individual or entity is designated for the purposes of this measure, social media services, internet access services and application stores must take reasonable steps to prevent users in the UK from accessing content, sites or applications provided by designated individuals or entities. Correspondent banking relationships and processing payments: Where this prohibition applies, UK credit or financial institutions are prohibited from establishing or continuing a correspondent banking relationship with a designated person, and from processing payments to, from or via a designated person. The measures will also apply to credit or financial institutions "owned or controlled" by the designated person (as set out in the regulations).
UK Statement Of Reasons	The Secretary of State considers that there are reasonable grounds to suspect that HUOBI GLOBAL SA is or has been involved in obtaining a benefit from or supporting the Government of Russia by providing financial services, or making available funds, economic resources, goods or technology, to a person, namely A7 LIMITED LIABILITY COMPANY, which is carrying on business in a sector of strategic significance to the Government of Russia.The Secretary of State considers that there are reasonable grounds to suspect that HUOBI GLOBAL SA has been involved in obtaining a benefit from or supporting the Government of Russia by providing financial services, or making available funds, economic resources, goods or technology, to a person, namely GARANTEX Europe OU, which is carrying on business in a sector of strategic significance to the Government of Russia.

Cashdesks and on-chain tracing limits



Important note:
Drops in measured crypto crime frequently reflect a loss of visibility into OTC operations, not an actual contraction in illicit procurement activity.

Blockchain ledgers are public, but attribution is opaque.

Over-The-Counter (OTC) cashdesks rely on thousands of rotating addresses, in-person trust networks, and physical couriers.

They convert Russian funds into procurement-ready stablecoins entirely off-chain.



Enhance responses from detection to disruption



Active attribution

Move beyond on-chain analytics. Deploy HUMINT, controlled probing, and physical surveillance to expose opaque OTC networks.



Target bridging assets

Force stablecoin issuers like USDT to freeze wallets linked to Russian evasion and exchanges to prevent access to high-risk tokens.



Designate networks

Target successor entities like Grinex and map the wallets of dual-use goods vendors, integrating trade and financial enforcement.

THANK YOU!

GET IN TOUCH

Gonzalo Saiz Erausquin
Research Fellow
CFS At RUSI

Gonzalo.Saiz@rusi.org

FOLLOW OUR WORK

RESEARCH AND SOCIAL MEDIA

Visit our CFS website
Subscribe to our SIFMANet Sanctions Newsletter
Follow us on LinkedIn and X