TRM | CHIEF DISRUPTOR

Hidden Signals on the Blockchain

Why national security needs blockchain intelligence

TRMLABS.COM

INTRODUCTION

A new domain for threat finance

The battlefield is evolving. Nation-state adversaries and non-state actors are increasingly operating across a new attack surface: public blockchains. From sanctions evasion to ransomware, terrorist financing to strategic technology procurement, malicious actors are exploiting cryptocurrency to generate and move funds with speed, scale, and perceived impunity.

For the UK intelligence community, this presents a new imperative: **illuminate these financial flows before they become operational threats.** Blockchain intelligence — also known as BLOCKINT — is fast becoming a core component of national security toolkits.

Key definitions

What are blockchains?

Blockchains are decentralised, digital ledgers that record transactions across a distributed network of computers. Each transaction is bundled into a block, time-stamped, and linked cryptographically to the previous block — creating an immutable chain of data.

Unlike traditional databases managed by a central authority, blockchains operate peer-to-peer and are designed to be transparent, tamper-resistant, and globally accessible. This architecture enables cryptocurrencies such as bitcoin and stablecoins like USDT to function without banks or intermediaries.

There are different types of blockchains:

- **Public blockchains (e.g. Bitcoin, Ethereum, TRON):** Open to anyone, searchable by anyone
- **Private or permissioned blockchains:** Restricted to approved participants
- **Layer 2 and cross-chain networks:** Built to improve scalability or interoperability between blockchains

For national security and defence teams, blockchains are no longer a theoretical concern – they are an active battleground. Adversaries are already exploiting these networks to move funds in the form of cryptocurrency, obscure operations, and evade detection. **If you're not monitoring blockchain activity, you're missing critical signals – and risk leaving operational blind spots in your intelligence picture**. Yet this same infrastructure offers an intelligence advantage: its transparency can be leveraged to illuminate and disrupt illicit financial flows in ways traditional tools cannot.

What is blockchain intelligence?

Blockchain intelligence (BLOCKINT) is the fusion of blockchain data with off-chain context to generate insights into actors, entities, and activity patterns. Blockchain analytics organizes and visualizes raw on-chain data (transactions, addresses) for basic tracing; BLOCKINT builds on this by enriching it with off-chain intelligence.

Blockchain intelligence combines:

- Raw blockchain data (transactions, smart contract interactions)
- On-chain behaviour analysis (automated patterns, obfuscation tactics)
- Off-chain intelligence (open-source data, sanctions listings, regulatory filings, law enforcement records)

Together, this intelligence enables national security teams to identify, attribute, and act on adversarial financial activity. Crucially, the transparency and permanence of blockchain data offer enduring visibility into networks that traditional financial intelligence might overlook.

QUICK LINKS

The dynamic threat landscape

While the motivations for illicit actors and nation states to leverage crypto vary, their objective is consistent: use digital assets as part of a suite of tools to raise, move, or obscure funds. For UK national security teams, understanding these actors is essential.

In this section, we'll take a closer look at the activity of four primary global actors in the crypto space — including their on-chain behaviours (observed using BLOCKINT) and attack vectors:

1. North Korea
2. China
3. Russia
4. Iran

North Korea

North Korea-linked activity is dominated by large-scale theft and a continued shift toward operational compromise. **TRM attributes USD 1.92 billion in stolen crypto to DPRK-linked actors in 2025**, reflecting a mature capability set that targets the operational foundations of crypto services rather than smart contract code alone.

Hacks and exploits

The **February 2025 Bybit breach** was the defining event. TRM assesses that the incident was carried out by North Korean operatives, and the USD 1.46 billion theft accounted for 51% of all funds stolen in 2025. Across 2025, illicit actors stole USD 2.87 billion in nearly 150 hacks and exploits — but losses were highly concentrated: the top 10 incidents accounted for 81% of the annual total, and five events drove 70% of stolen value. This concentration suggests a threat environment where a small number of sophisticated actors can create outsized systemic impact.

Tactically, theft patterns are driven by infrastructure attacks. While **code exploits** were the most frequent category (52 incidents), they accounted for USD 350 million (12.1%). By contrast, **infrastructure attacks** drove USD 2.2 billion (76%) across 45 incidents, averaging approximately USD 48.5 million per incident. This reflects a shift toward compromise of keys, wallet infrastructure, privileged access, and front-end or control-plane surfaces. In practice, this "move up the stack" widens the attack surface to include developer environments, signer isolation, and withdrawal governance.

The "Chinese laundromat"

In 2025, North Korea's post-theft activity increasingly relied on **Chinese-language laundering** intermediaries. DPRK operators continued to route stolen assets through "Chinese laundromat" networks of professionalised OTC brokers and underground intermediaries that absorb stolen assets and settle off-chain. These services enable subcontracted laundering, chain hopping, and fragmentation across chains and services — narrowing the interdiction window and complicating recovery.

China

Chinese-language escrow services, underground banking networks, and "guarantee" marketplaces operate as core settlement infrastructure for cross-border illicit finance. **TRM analysis shows that activity associated with Chinese-language escrow services and underground banking networks grew from approximately USD 123 million in 2020 to over USD 103 billion in 2025**, indicating that these services have shifted from niche facilitation into large-scale settlement layers.

Chinese-language escrow services and underground banking networks

These networks function as a trust mechanism and liquidity bridge. Escrow and guarantee marketplaces reduce counterparty risk through reputation systems and dispute resolution, enabling high-frequency stablecoin settlement in corridors where speed and reliability matter more than access to formal banking. They also bridge on-chain activity into off-chain cashout and reintegration via OTC brokers, money mule networks, and APAC-based casinos.

The market has historically been concentrated across several major players. TRM observed Chinese-language guarantee marketplaces on Telegram led by **Huione Pay** (approximately USD 73 billion), followed by **Haowang** (approximately USD 7.3 billion), **Xinbi** (approximately USD 5.9 billion), and **Tudou** (approximately USD 3 billion). This concentration makes the sector a recurring enforcement focus — but recent pressure has re-routed activity rather than eliminating demand.

2025 enforcement and platform actions reshaped, but did not remove, the escrow model:

- **May 2025:** FinCEN designated Huione Group as a foreign financial institution of primary money laundering concern under Section 311
- **Shortly after:** Telegram removed channels associated with Haowang Guarantee and Xinbi, disrupting visible hubs

- **Displacement:** Vendors and flows shifted toward Tudou — in a context where Tudou benefited from Huione's earlier 30% stake acquisition — and inflows rose to approximately USD 70 million per week (May – November 2025)
- **Late 2025:** After finalization of the Section 311 rule (effective November 17, 2025), Huione Pay inflows fell sharply to approximately USD 100 million per month by December 2025
- **Xinbi resilience:** After channel removal, Xinbi reportedly reappeared under the same Telegram ID and saw an approximately 90% increase in daily inflows, later promoting migration to a mirrored escrow service on a proprietary chat platform

This pattern supports an assessment that **enforcement changes the shape and venue of settlement**, while the escrow function persists as long as underlying demand persists. In operational terms, the most durable detection signals are behavioural rather than brand-based — including broker hubs, repeated counterparty patterns, short holding periods, and consistent off-ramp dependencies.

Sanctions evasion

These networks are also used as a vector for sanctions evasion. China-based suppliers sell restricted goods — including US-made electronics, dual-use components, and Common High Priority List (CHPL) items — to sanctioned buyers in Russia and Iran, using Russian or Hong Kong crypto brokers who employ escrow-backed crypto payment infrastructure. In several cases, sanctioned Russian exchanges received and sent funds to Chinese resellers that were in turn possibly using Hong Kong-based intermediaries to process the cryptocurrency transactions. The convergence of illicit trade, sanctions evasion, and global fraud typologies through a shared escrow-based financial infrastructure presents a complex challenge for enforcement.

Russia

Russia-linked activity drives the majority of sanctions-associated crypto volume and is showing indicators of institutionalization: repeated use of stablecoins, professionalized intermediaries, and coordinated infrastructure that reduces dependence on USD-backed rails and more regulated venues. At the same time, A7's large-scale use of blockchain infrastructure — numbering at least in the tens of billions of USD in value — allows for a unique opportunity to track Russia's procurement networks, economic partners, and identify weaknesses and failings in Russia's ability to produce its own goods.

At the macro level, cryptocurrency associated with inflows to sanctioned entities and jurisdictions reached USD 93 billion in 2025. A large share was associated with Russia-linked actors, including USD 72 billion received by the **A7A5 token** and an additional USD 39 billion linked to **A7 addresses**. These figures measure different exposures and are not directly additive; there may be overlap where categories interact.

A7 addresses

A7 stands out as a centrally coordinated sanctions-evasion architecture tied to Russian state interests. Leaked internal documents reveal A7's direct connections to the Kremlin and a large cluster of cryptocurrency addresses. **This group shows at least USD 65 billion in direct A7-related volume**, with additional flows moving through intermediary wallets likely tied to A7 shell companies or foreign trade partners.

On-chain analysis showed over USD 10 billion in direct bidirectional exposure between A7 and sanctioned Russian exchanges like Garantex and Grinex, showing integration of Russian sanctions evasion-related entities' operations. A7 also shows exposure to IRGC, Hamas, financial intermediaries operating in Venezuela, and sanctioned entities HuiOne and BYEX — indicating overlap with other high-risk financial networks and state actors.

At the same time, A7 shows consistent use of central exchanges, through which it sends tens of millions in USDT at a time, daily. This exposure to central exchanges provides an opportunity for public and private sectors to cooperate and track Russian payment paths to answer what Russia's procurement needs are, what operations abroad it supports, who its partners are, and where its supply chain may be vulnerable for interdiction.

China-based intermediaries supported procurement and payment flows

A7-linked funds moved through intermediaries in jurisdictions across the globe, including China and Hong Kong-based entities. TRM has identified several Chinese counterparties operating with crypto intermediaries. One of these entities, an electronics reseller, is using a wallet run by a possible A7 subentity operating in China, or else a Chinese counterparty coordinating Russian sanctions evasion on the blockchain. This proves a strong level of cooperation between not just A7 and a mainland Chinese company, but between the Russian and Chinese states themselves.

A7A5 as internal settlement and apparent liquidity inflation

TRM observed that approximately 34% of A7A5's trading volume was likely inflated through wash trading patterns, including rapid circular transfers

consistent with automated behaviour. These patterns may represent fiat on- and off-ramps, or some kind of account-settling activity. Many of these transactions also occurred within the span of several minutes, making it also possible that this is an effort to inflate apparent liquidity to build confidence in a novel stablecoin for trade settlement.

On-chain analysis indicates that A7A5 was used disproportionately in transactions between A7, Garantex, and Kyrgyzstan-based entities likely within the same network — reinforcing the view that **A7A5 primarily functioned as an internal settlement mechanism within a broader sanctions evasion architecture**, rather than a globally competitive stablecoin.

Rebranding and continuity under enforcement pressure

Russia-linked crypto services responded to enforcement through rapid rebranding and reincorporation. Following the March 2025 operation against Russian government-connected Garantex, TRM uncovered a series of Kyrgyzstan-based entities that showed the same network fingerprint tied to Garantex. These Russia-linked platforms had nearly identical interfaces and wallet heuristics. Many of these entities were later sanctioned due to their connections to Russian sanctions evasion. One of them, Grinex, was initially used for the migration of Garantex-tied assets via A7A5.

Russian high-risk exchange ABCeX also launched a rebranded version of itself, AEXBit. ABCeX has been tied to Garantex via the latter's co-founder, Sergei Mendeleev, who supported the platform's launch. At the same time, Russia-connected payment system Cryptomus launched Heleket in what is likely an attempt to disassociate the platform from cybercrime users who have previously been identified as using Cryptomus. Cryptomus also received initial liquidity from Garantex.

For both ABCex and Cryptomus, the initial on-chain indications of these rebranding operations date to roughly the same time as those of Garantex's. Collectively, these patterns are consistent with **rebranding as an operational tactic to preserve access to liquidity while insulating core operators from sanctions and legal exposure**. Given Garantex's connections to the Russian government and likely importance as a sanction evasion tool, these coordinated rebranding operations may have been centrally coordinated with the assistance of the Russian government.

Iran

Iran's crypto ecosystem remained resilient under sanctions and periods of acute disruption in 2025, with flows adapting rather than collapsing. **TRM observed approximately USD 11.4 billion in total crypto activity in Iran in 2024 and roughly USD 10 billion in 2025, including inbound and outbound flows**. The

modest year-over-year decline suggests persistent structural demand rather than speculative participation, though observed totals remain subject to upward revision as attribution of offshore intermediaries and broker-mediated settlement expands.

Two recent events illustrate how different shocks shaped participation:

12-day Iran-Israel conflict in June 2025

First, the 12-day Iran-Israel conflict (June 13 – June 24, 2025) served as a stress test. **During that period, Iran's crypto volume increased by approximately 35% while transaction counts fell by roughly 40%, and average transaction size rose by about 122% compared to the same period in 2024**. The combination of higher volume with fewer transactions is consistent with consolidation into fewer, larger transfers, which can reflect crisis-driven behaviour such as balance consolidation, capital movement, and risk mitigation.

Exchange-level dynamics reinforced this pattern. In the days preceding June 13, outflows from Nobitex surged by more than 150% week over week. Shortly after, the Israel-linked group Predatory Sparrow targeted Nobitex in an approximately USD 90 million hack, after which incoming transaction volumes dropped by more than 70% year over year. Nobitex resumed service in stages beginning in late June, aided in part by reserves held in bitcoin, including funds consolidated from previously dormant mining-linked wallets. More broadly, activity rerouted through intermediary wallets and offshore services rather than disappearing.

Domestic unrest

Second, domestic unrest had the opposite effect on broad participation. **Between December 28, 2025, and January 16, 2026, Iran's total crypto volume declined by roughly 60% year over year and transaction counts fell by approximately 63% compared to the same period in 2024–2025, in a context of near-total internet shutdowns and restrictions on digital services**. While significant value still moved on-chain, activity narrowed to a smaller set of higher-capacity actors able to operate through disruptions.

Illicit activity remained a stable share of observed Iranian flows. In 2025, illicit Iranian crypto volume totaled just over USD 580 million, representing approximately 5.9% of observed activity. In 2024, illicit activity was roughly USD 600 million, or approximately 5.1% of observed volume. Across both years, the activity was overwhelmingly concentrated in stablecoins, particularly USDT on TRON, likely reflecting liquidity, low transaction costs, and broker acceptance.

IRGC-aligned offshore exchange infrastructure

TRM analysis identified two UK-incorporated exchanges, **Zedcex and Zedxion**, that processed hundreds of millions of dollars in stablecoin transactions while

functioning as offshore infrastructure linked to Iran's Islamic Revolutionary Guard Corps (IRGC).

Between 2023 and 2025, IRGC-linked flows accounted for roughly USD 24 million in 2023 (about 60% of observed activity), rose to around USD 620 million in 2024 (nearly 90%), and declined to approximately USD 410 million in 2025 as non-IRGC activity increased. Across the period, TRM observed close to USD 1 billion in IRGC-associated transactions, primarily USDT on TRON. Corporate records reflected virtual office addresses, overlapping directors, and dormant filings despite the on-chain scale.

On-chain tracing connected Zedcex-attributed wallets to addresses designated by Israeli authorities as IRGC property and blocklisted by stablecoin issuers, as well as domestic Iranian exchanges and offshore intermediaries. In at least one instance, TRM observed transfers exceeding USD 10 million from Zedcex-linked infrastructure to a US-designated terrorist financier associated with the IRGC without intermediary routing.

CONCLUSION

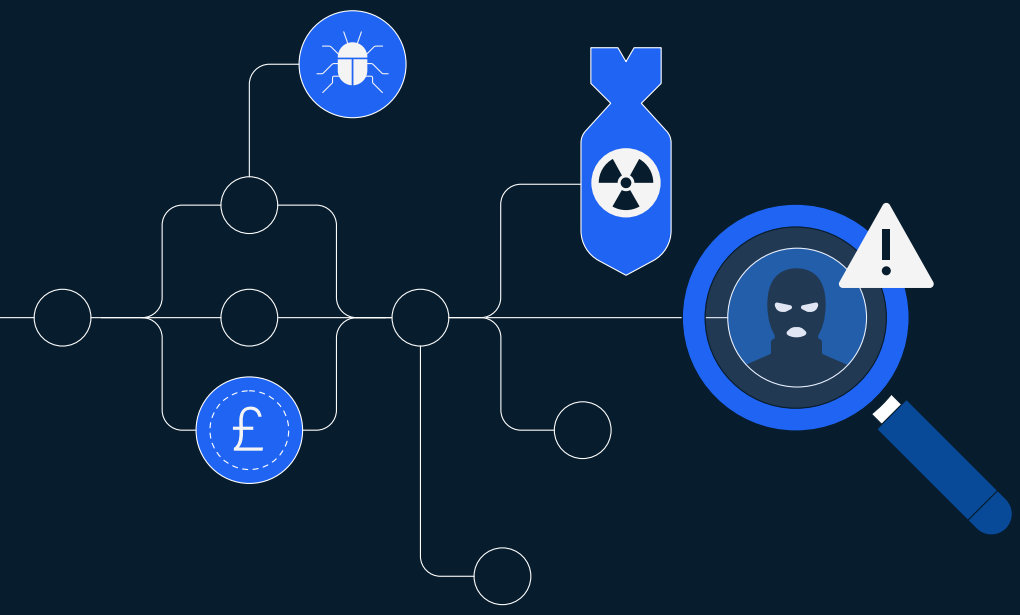
Mission advantage through blockchain intelligence

Public blockchains are enduring sources of structured, transparent, and time-stamped data. When combined with advanced analytics and threat intelligence, this data offers a powerful tool to counter adversarial finance.

BLOCKINT enables national security teams to:

- Detect early indicators of adversarial operations
- Attribute activity with speed and confidence
- Support sanctions, prosecutions, and disruption campaigns

For UK national security stakeholders, BLOCKINT is a critical input to the intelligence and targeting cycles of tomorrow. The breadth and depth of selectors inherent within blockchain data unlocks a unique ability to pivot between wider datasets, using BLOCKINT as the central plane. This is what enables analysts to not only drive intelligence understanding, but actively enable operational impact.



About TRM Labs

TRM Labs provides blockchain analytics solutions to help law enforcement and national security agencies, financial institutions, and cryptocurrency businesses detect, investigate, and disrupt crypto-related fraud and financial crime. TRM's blockchain intelligence platform includes solutions to trace the source and destination of funds, identify illicit activity, build cases, and construct an operating picture of threats. TRM is trusted by leading agencies and businesses worldwide who rely on TRM to enable a safer, more secure crypto ecosystem.

TRM is based in San Francisco, CA, and is hiring across engineering, product, sales, and data science.

To learn more, visit www.trmlabs.com

About Chief Disruptor

Since 2005, our membership community for business and tech leaders has brought together innovators, change-makers, and disruptive thinkers to share expertise, strategies and actionable insights.

Organisations need nimble, purposeful leadership that grasps the opportunities and proactively manages the threats of disruption. Our purpose is to cut through the hype and enable our members to leverage these disruptive trends and technologies through our member-led reports, content, and cross-sector activities.

Chief Disruptor Defence was formed in 2020 as a direct result of the demand from our vibrant and rapidly expanding network of Defence members. It delivers a wide range of defence and security focussed activities to help enable our MOD members drive innovation and disruption.