Observatoire ARGA

Report on Sanctions and Compliance for 2025

GEOPOLITICS OF CRYPTOCURRENCIES AND THE DIGITAL ECONOMY

USDT Economy, Transnational Cyber Networks, and New Crime Nodes in Eurasia

Author:

Sergei Khrabrykh — President of ARGA, PhD

Organization: Observatoire ARGA – Sanctions and Compliance Division

Correspondence Address: 14 rue Jacques Laffitte, Bayonne, 64100

Contact: info@argaobservatory.org

Paris, 10 November 2025

Table of Contents

Executive Summary

Cryptocurrencies have ceased to be a marginal technological innovation and have transformed into a fundamental instrument of global politics and international security. Between 2020 and 2025, digital assets — especially USDT — created a parallel financial circuit that functions as a non-bank dollar system capable of bypassing SWIFT, sanctions lists, export controls, and banking regulation.

The USDT economy is becoming a global source of liquidity, accessible precisely where traditional banking infrastructure is constrained by sanctions, de-offshorisation, or political risk. Today it is used not only for payments and P2P settlements, but also as a substitute for offshore jurisdictions, correspondent accounts, exchange markets, and physical dollars.

Eurasia is the key geography where this system has developed its own geopolitical logic. Here, cryptocurrencies perform the functions of:

• bypassing sanctions and export controls,

• financing shadow trade and parallel import networks,

• sheltering assets during corporate conflicts and nationalisation campaigns,

• repatriating capital and cashing out digital assets,

• forming new criminal–economic alliances.

ARGA Observatory identifies the emergence of a new crypto-economic architecture in which digital assets underpin:

1. transnational shadow financial flows,
2. hybrid corridors linking the UAE, the Caucasus, Central Asia and Hong Kong,
3. a new elite of digital intermediaries — crypto-brokers and OTC dealers,
4. criminal and state-corporate digital cartels.

USDT and stablecoin finance are no longer a technological anomaly — they represent a new system of power and capital distribution that already competes with traditional institutions of the global economy. This report outlines the key risk nodes, the structure of cyber-financial networks, regulatory mechanisms, evolution scenarios, and strategic threats to international security in the 2025–2030 horizon.

1. Methodology

The report is built upon a multilayered research framework integrating technical blockchain analytics, financial intelligence, international law, OSINT investigation, and an empirical base of field observations. This structure makes it possible not only to map cryptocurrency flows, but also to identify the political, criminal and geo-economic factors that shape them.

1. On-chain analysis of the TRON, Ethereum, and BSC blockchains

The study employs graph-decomposition techniques, address clustering, flow-network mapping, and correlation analysis of liquidity movements. This enables the identification of:

• hidden brokerage centres and informal crypto hubs;

• transregional movements of USDT liquidity;

• transfers between criminal, corporate and state-affiliated wallets;

• recurring transactional routes (pattern recognition).

TRON has become the main transport layer of the Eurasian USDT economy, making its analytical decomposition a core component of the research.

2. Use of blockchain-intelligence platforms (Chainalysis, TRM, Crystal, Elliptic)

The following tools are applied:

• risk-score segmentation of addresses;

• attribution and threat-tagging of wallets (flagged entities);

• detection of mixer schemes and hop-routing patterns;

• analysis of USDT concentration in OTC pools.

The result is a model of the crypto-ecosystem not as a collection of transactions, but as an interconnected infrastructure network.

3. OSINT module: extraction of open-source intelligence

The analysis covers:

• media reports and investigative journalism;

• court archives;

• Eurasian corporate registries;

• Telegram networks of OTC exchangers;

• database leaks and dumps.

OSINT enables reconstruction of actor motivations, political context, and intermediary linkages. In crypto-geopolitics, facts and context carry equal analytical weight.

4. FININT (financial intelligence) layer

Using bank statements, correspondent-banking channels, SWIFT data, off-ramps and stablecoin-to-fiat conversions, the study reconstructs:

• cross-jurisdictional capital movements;

• schemes for cashing out USDT into fiat;

• the points at which digital capital becomes economically real.

This is the key layer that connects crypto-routes to the tangible economy.

5. Monitoring of OTC Structures in the UAE, Georgia, Kazakhstan, Hong Kong, and Lithuania

Data were collected on:

• spreads, commissions, and liquidity;

• mechanisms for bypassing KYC;

• settlement methods used in grey and black liquidity pools;

• entities working with high-risk capital (sanctioned, shadow, and criminal assets).

The OTC market functions as the *informal interbank layer* of the USDT economy. Field analytics reveal processes that are not visible in blockchain data or court records.

6. Analysis of Criminal Cases and Investigations

Sources include:

• prosecution materials concerning operators of OTC / P2P networks;

• cases involving money laundering (AML), crypto-cash-outs, and sanctions evasion;

• court rulings related to the confiscation of digital assets.

This allows us to distinguish situations where cryptocurrency serves as a tool of crime from those where it is used as a mechanism for protecting capital from state pressure.

7. Regulatory Analysis (FATF, FinCEN, EU MiCA, Asian Regulators)

The regulatory dimension of the methodology covers:

• analysis of international AML standards and the Travel Rule;

• comparison of USDT regulation across the EU, the US, the UAE, and Hong Kong;

• assessment of the gap between formal legal frameworks and actual enforcement mechanisms.

Crypto-geopolitics is shaped not by technology but by regulatory asymmetry between jurisdictions.

8. Empirical Base: 163 Cases (2020–2025)

The case base includes instances of:

• capital flight into USDT;

• transit through OTC liquidity pools;

• sanctions hedging;

• crypto-raiding and digital pressure schemes.

Each case provides not only a documented fact but also data for constructing mathematically recurring patterns. Crypto-economics becomes predictable through a *critical mass of case studies*, not through isolated examples.

2. Introduction: The Digital Transformation of Global Crime and Finance

Cryptocurrencies, originally viewed as a technological innovation and a tool of economic liberalization, have over the past decade evolved into a fundamental component of the new global financial architecture. Their functional role is no longer limited to serving as an alternative to the banking system — they have become an infrastructure capable of substituting state monetary mechanisms and creating autonomous shadow markets of liquidity.

Today, cryptocurrencies simultaneously perform several systemic functions:

• a sanctions-evasion mechanism enabling transfers inaccessible within the banking system;

• an instrument of transnational criminal networks, facilitating supply routes for weapons, narcotics, illicit technologies, and digital services;

• a channel for capital flight and preservation, used by entrepreneurs and political elites under conditions of persecution;

• a tool of corporate warfare and economic coercion, enabling rapid movement of assets beyond the control of state institutions;

• a medium for cyber-extortion underpinning the ransomware economy;

• an alternative dollar system, in which USDT functions as a unit of account without any central-bank institution.

The key element of this transformation has been the USDT architecture — the world's largest tokenized-dollar network, operating without geographic boundaries, institutional sovereignty, or full regulatory accountability. Transaction volumes in USDT pools on TRON and Ethereum are comparable to the financial turnover of mid-sized banks and, in certain jurisdictions, exceed official foreign-exchange operations.

Thus, cryptocurrencies have ceased to be a technological experiment and have become a new form of global money, shifting economic power and financial control from states to a hybrid ecosystem of OTC markets, liquidity operators, mining centers, cybercriminal networks, and private crypto-corporations. In Eurasia, this process is unfolding particularly rapidly — the region is becoming

one of the key zones where the digital criminal economy and transnational financial flows shape a new map of power and influence.

3. The USDT Economy: A New Global Financial Infrastructure

Parallel to the traditional dollar system, an alternative settlement network based on tokenized liquidity — primarily USDT — has emerged. In terms of transaction volume, it is comparable to state-controlled currency segments of emerging economies, yet it operates outside any geographic, regulatory, or banking jurisdiction. USDT has become a new form of financial sub-sovereignty: a monetary system without a central issuer, regulator, correspondent-banking constraints, or borders for cross-border capital movement.

3.1. Liquidity Beyond State Control

USDT enables a mode of settlement that is:

• instant and irreversible,

• conducted between users anywhere in the world,

• inaccessible to state-driven transaction blocking,

• capable of moving large volumes of capital within a single operation.

Unlike SWIFT, SEPA, or Fedwire, this system does not require correspondent banks, is not subject to sanctions filters, and enables economic operations that cannot be halted by administrative order. For states, this represents a loss of monopoly over currency operations.

3.2. Transit and “Soft Anonymity”

Cryptocurrency anonymity is not absolute, but it is operationally reproducible. Tracing is possible, yet costly; transaction atomization allows large sums to be split into dozens of micro-packets, breaking the link between sender and recipient.

USDT is characterized by a low evidentiary density: transactions are technically public, but identifying wallet owners requires external datasets — KYC trails, leaked databases, exchange logs, fintech metadata. In the grey zone where cryptocurrency intermediaries operate, this linkage is deliberately severed.

3.3. The Geocentric Role of TRON as Eurasia’s Crypto-Payment Corridor

Between 2023 and 2025, TRON became the de facto “economic backbone” of the USDT ecosystem. More than 70% of P2P transfers associated with shadow capital flows move through this network. The reasons are clear:

• minimal gas fees,

• high network throughput,

• weak institutional oversight,

• a mature OTC infrastructure across Eurasia and Asia.

Thus, TRON has effectively become the SWIFT analogue for the region's illicit settlements — cheap, fast, resistant to blocking, and optimized for high-velocity transfers.

3.4. OTC Markets as the Functional Equivalent of a Banking System

Alongside the USDT settlement network, an infrastructure has emerged that substitutes for the core functions of banks. OTC dealers serve as:

• cashiers of digital currencies,

• liquidity lenders,

• cross-border clearing nodes,

• back-office operators for grey imports and corporate conflicts.

The principal OTC hubs are now concentrated in:

Region	Function	Status
UAE (Dubai)	Central USDT↔Fiat exchange	Primary global liquidity market
Georgia (Tbilisi)	P2P transit, grey import	Regional hub for RU/ARM/KZ
Lithuania	Fiat off-ramp into the EU, corporate accounts	"Gateway to the European Union"
Kazakhstan	Import transit, cash-out operations	Node for parallel import
Hong Kong	Corporate crypto-circuits of China	Offshore USDT center for Asia

Taken together, this network functions as a new global settlement layer capable of competing with the banking infrastructure.

4. Geography of Eurasian Cryptocurrency Nodes

The shadow crypto-economy of Eurasia is forming as a distributed network of node-cities, each performing specialized functions—exchange, conversion, transit, cash-out, corporate clearing, or liquidity redistribution. These centers do not simply service crypto transactions; they constitute a new transit architecture of capital, parallel to the traditional banking system and partially replacing it.

4.1. UAE (Dubai, Abu Dhabi)

The UAE is the world's primary hub for USDT circulation, where liquidity flows in from Russia, Turkey, China, Central Asia, Pakistan, and Afghanistan.

A quasi-banking market has formed there, operating outside traditional regulation:

• the world's largest volume of off-exchange USDT→fiat deals,

• OTC desks linked to Russian, Georgian, Chinese and Pakistani criminal and corporate networks,

• services such as crypto-factoring, crypto-escrow, and layering-based settlement structures — analogues of banking products, but without KYC and transparency.

The UAE is the *heartland* of the USDT economy, where digital liquidity is transformed into dollars, gold, real estate, and commodity assets.

4.2. Georgia (Tbilisi, Batumi)

Georgia is Europe's primary "grey" crypto-node. It is not an EU member state, yet it is technologically integrated into the EU's financial space — making it an ideal platform for high-risk digital liquidity.

Key characteristics:

• hundreds of unlicensed OTC operators,

• simultaneous presence of "Russian," "Turkish," and "Arab" networks,

• liquidity supply for parallel imports, including defense-industry components,

• mass conversion of USDT→cash→bank accounts in the EU.

Tbilisi effectively serves as Europe's crypto-gateway, through which digital funds enter the EU banking system.

4.3. Lithuania — the digital gateway to the EU

Lithuania has become a registration hub for financial intermediary companies that formally hold European status but operate on flows from the CIS, the Caucasus, and Asia.

Key features of the node:

• licensing of crypto EMI/VASP entities with minimal requirements until 2023–2024,

• creation of "fin-travel structures" that inject USDT into the EU banking system (crypto-to-fiat injection),

• a market of pseudo-banking services using API-banking and external payment rails.

Lithuania acts as the entry point for high-risk digital flows into the European Union, enabling numerous asset-laundering schemes.

4.4. Kazakhstan and Kyrgyzstan — the EAEU crypto-logistics corridor

Central Asia functions as a transit corridor between China, Russia, and the Middle East.

Why the region is critically important:

• integration into the EAEU allows concealment of goods' origin,

• an active market of shadow exchangers and P2P dealers,

• cryptocurrency settlements are used for parallel import of electronics, machinery, and aircraft components,

• USDT → cash USD → industrial procurement → re-export → Russia.

Kazakhstan is the payment node for imports; Kyrgyzstan is the fintech platform for micro-flows servicing the retail segment of grey logistics.

4.5. Hong Kong and Southeast Asia

Hong Kong is the central point for cryptocurrency operations of Chinese corporate capital. It enables:

• capital outflow from China via USDT with subsequent fiat conversion,

• operation of off-ramp brokers for the purchase of microchips, electronics, and SaaS services,

• crypto-fintech bridges into Africa — a rapidly growing market for crypto-remittances.

Singapore, Malaysia, and Indonesia form a secondary layer: less public OTC markets where liquidity is redistributed among Silk Road networks, Middle Eastern actors, and Russian-Chinese clusters.

5. Actors of Crypto-Geopolitics

The cryptocurrency infrastructure of Eurasia is not chaotic or fragmented — on the contrary, it is governed by a stable system of actors who perform complementary functions. Within the USDT sector, power structures, criminal networks, fintech intermediaries, and corporate groups occupy distinct roles, forming a hybrid space where economics, politics, and crime no longer exist separately. Below are the key groups shaping the evolution of the digital shadow economy in 2020–2025.

5.1. State and Quasi-State Groups

This category includes security services, financial regulators, customs elites, and state-adjacent business formations. Their motivation is not ideological but pragmatic — to control capital and circumvent external regulation.

• cryptocurrencies are used as a sanctions-evasion tool, enabling international settlements without SWIFT or banking compliance;

• state structures supervise or "protect" specific OTC operators, gaining access to liquidity and transaction data;

• crypto-channels are used to finance government procurement and “sensitive imports,” especially under restrictions on Western technologies and equipment;

• in several jurisdictions, a dual policy is observed: official anti-crypto regulation coexists with the unofficial use of USDT for foreign trade operations.

Thus, the state does not eliminate the crypto market — under sanctions pressure, it is becoming one of its major beneficiaries.

5.2. Criminal Groups

Organized crime has become one of the most active users of the USDT economy. Their involvement is driven by the fact that cryptocurrencies enable capital movement without cash transport, banking risks, or physical seizure.

• USDT is used to launder proceeds from corruption, drug trafficking, extortion, grey supplies, and illegal exports;

• ransomware networks, digital PMCs, hacker groups, and Darknet marketplaces operate predominantly in crypto;

• criminal capital is increasingly intertwined with political actors and security groups, creating a stable ecosystem of mutual protection and resource exchange;

• criminal networks now occupy a niche equivalent to a banking sector — but without regulation, parity, AML control, or legal boundaries.

Criminal groups are not an external threat but an embedded component of the new crypto-architecture.

5.3. OTC Brokers and Shadow Bankers

OTC operators function as “digital cashiers.” They handle the largest volumes of USDT liquidity, enabling cash-out, cash-in, off-ramp, and cross-ramp conversions.

• P2P brokers exchange crypto for cash, bank transfers, and e-money without leaving traces in formal reporting;

• cross-mixing of flows is used, where dozens of clients’ funds are pooled, fragmented, and redistributed to the point where tracing becomes nearly impossible;

• OTC markets enable custodial-free operations that bypass exchanges and licensed services, making transaction blocking extremely difficult;

• many OTC desks operate under the protection of state structures or security groups, effectively becoming a crypto-banking system outside regulatory oversight.

These actors are the “engine of circulation” — without them, the crypto-economy simply would not function.

5.4. Fintech Intermediaries

Fintech companies act as infrastructural integrators. They connect crypto turnover with the banking system, create bridges between USDT and fiat, and provide the transactional layer for grey financial flows.

• fintech platforms occupy a quasi-compliance niche, establishing corporate shells, trust structures, API-banking gateways, and “legally cleaned” transaction channels;

• their operations make it possible to legalize cryptocurrency through corporate wallets, digital exchangers, EMI licenses, and cross-ledger-transfer schemes;

• they create an infrastructure of pseudo-security, where transactions appear legitimate but in reality serve to withdraw funds, evade sanctions, and “mask transparency.”

Fintech intermediaries are the technological layer of crypto-geopolitics.

5.5. Corporate Group

Large businesses use cryptocurrencies not only to circumvent regulation, but also to solve internal strategic objectives.

• USDT becomes a financing tool for parallel imports, especially in sectors with restricted access to European and U.S. equipment;

• corporate networks use cryptocurrencies to withdraw assets, create reserve funds, and distribute dividends outside banking control;

• a widespread “digitalization of capital” is taking place: companies convert working capital into crypto-liquidity to protect it from nationalization, asset freezes, and corporate attacks.

Cryptocurrency is becoming a new form of corporate sovereignty.

6. Case Studies

Case 1 — USDT Chain for Bypassing Export Controls (UAE → Armenia → Russia)

The mechanism relies on using cryptocurrency as a payment channel for importing sanctioned goods. The route involves purchasing electronics, machinery, chips, and telecom components through proxy companies in the UAE. Payments to the supplier are made in USDT, allowing avoidance of banking AML monitoring, SWIFT tracing, and End-User Verification checks.

The goods are then re-exported to Armenia, where their origin and destination are altered through document repackaging — certificates, invoices, export declarations. From Yerevan, the goods move to Russia as third-country products, while payment is processed via an OTC transfer through an offshore broker desk on TRON.

Conclusion:

This mechanism enables the acquisition of dual-use products without sanctions-related blocking and without involving banks. It is a classic model of the shadow import circuit of 2022–2025.

Case 2 — A Digital Criminal Hub (Asia → Eurasia → EU)

In this case, money laundering operates through a transregional crypto-relay.

The initial funds originate from cybercrime: phishing attacks, Ponzi schemes, compromised corporate emails, Telegram botnets. The generated flow is converted into USDT and moved into the Eurasian zone, where OTC structures perform mixing, cross-ledger routing, and pseudobanking (unlicensed digital quasi-banking).

Funds are fragmented into hundreds of transactions of 4–20,000 USDT, pass through TRON nodes, and are transferred to broker wallets in Kazakhstan, Kyrgyzstan, and Georgia.

The final stage is cash-out in the EU via Lithuanian EMI entities, P2P platforms, and transactions through shell e-commerce stores. The end result appears as euros on accounts of EU individuals with no documentary ties to the original crime.

Conclusion:

This case demonstrates how the Eurasian region becomes a "wash layer" between Asian cybercrime and the European financial system.

Case 3 — A Corporate Conflict "Digitized" into Crypto (CIS → OTC → State Pressure)

A corporate dispute between two beneficiary groups transforms into a digital financial crisis. The company's assets are converted into cryptocurrency via OTC operators, then moved through TRON–USDT–BSC chains, temporarily placing liquidity outside the reach of opponents.

The initiating side transfers funds abroad, hides ownership through multilayer wallet structures, and then uses liquidity access as leverage. In response, opponents initiate a criminal case, involve security agencies, and file Interpol notices targeting executives.

The actual goal is not prosecution but coercion to return the digital capital and share of corporate control.

Conclusion:

Cryptocurrency transforms a corporate conflict into an extraterritorial phase and shifts the balance of power — the party controlling USDT liquidity controls the conflict itself.

7. Global Risks

7.1. The Emergence of a Parallel Dollar System (the USDT-Statehood Effect)

The growing circulation of USDT and other stablecoins is effectively creating an alternative global monetary architecture that is not subordinated to national central banks or international regulators.

This system displays features of a self-standing monetary continent:

• its own liquidity,

• exchange hubs,

• mechanisms of cross-border settlement,

• a pseudo-banking infrastructure of OTC dealers.

In the long term, it reduces the role of the classical dollar as an instrument of capital-flow control, weakens the monetary sovereignty of states, and creates a new level of global dependence on private issuers of digital currencies.

7.2. Consolidation of Digital Crime and Its Transformation into an Economic Sector

The cryptocurrency sector creates conditions in which cybercrime ceases to be marginal and becomes a stable economic model.

Ransomware, phishing networks, darknet marketplaces, crypto-laundering, and RaaS (Ransomware-as-a-Service) form a durable financial ecosystem with:

• its own pricing for criminal services,

• an investment system for fraud operations,

• mechanisms of "insurance" and capital recovery within illicit networks.

In Eurasia, this system feeds parallel imports, smuggling, and corporate wars, turning digital crime into a real macroeconomic factor.

7.3. Growing Complexity of AML Monitoring and Sanctions Enforcement (Regulatory Asymmetry)

Traditional anti-money-laundering methods — KYC, SWIFT tracing, banking compliance algorithms — lose effectiveness when transactions occur in an environment with no sending bank, no receiving bank, and no single regulator.

TRON-based flows, mixing services, chain-splitting, and P2P exchanges create zones of monitoring blindness.

This produces a regulatory paradox: tightening control pushes more activity into the crypto sector, while state monitoring becomes slower and more expensive than the speed at which digital assets move.

7.4. Geopoliticization of Cryptocurrencies and the Battle for Digital Sovereignty

Cryptocurrencies are becoming not just financial but geopolitical resources.

The UAE, Turkey, Hong Kong, Kazakhstan, and Singapore are no longer merely trading venues — they are influence hubs comparable to offshore financial centers of the 20th century.

A new form of foreign policy is emerging: control over digital assets becomes analogous to controlling oil, gas transit, or maritime choke points.

This leads to:

• the formation of digital alliances,

• competition between states for crypto-hub status,

• rising risks of sanctions blockades directed not at countries but at infrastructural nodes of the blockchain economy.

7.5. Growth of Interpol Abuse and the Criminalization of Digital Conflicts

As USDT flows expand, corporate wars, asset disputes, and political confrontations increasingly acquire a cryptocurrency dimension.

Police and security agencies use Interpol requests as a tool of pressure not only on individuals but also on their digital assets — demanding disclosure of private keys, wallet access, or repatriation of funds.

A new category of criminal proceedings emerges — **crypto-extradition cases**, where cryptocurrency becomes the object of investigation, seizure, and negotiation.

This significantly increases the risk of institutional degradation of Interpol and creates the danger of internationally criminalized persecution disguised as AML enforcement.

8. Forecast 2025–2027

8.1. Strengthening of Global Regulation of Digital Assets

Over the next two years, the digital economy will enter a phase of regulatory standardization.

The MiCA (EU), FinCEN (USA), and FATF frameworks will gradually converge, forming a multi-layered system requiring:

• mandatory identification of transaction participants,

• registration of crypto-service providers,

• integration of USDT flows into the classical AML circuit.

International reporting protocols comparable to traditional banking-compliance are likely to emerge.

This will push the informal crypto market into narrower niches and significantly increase the cost of anonymity.

8.2. Sanctions and Regulatory Strikes Against OTC Markets in the UAE, Georgia, and Kazakhstan

The largest cryptocurrency hubs in Eurasia will face systemic pressure: Washington, Brussels, and London are already considering secondary sanctions targeting OTC platforms involved in sanctions evasion, parallel imports, and laundering of financial flows.

Regulators are likely to introduce:

• licensing mechanisms for OTC operators,

• registries of high-risk brokers.

As a result, crypto flows may shift toward less controlled regions — Africa, Latin America, and Southeast Asia.

8.3. Decentralization of Crypto-Crime and the Formation of a New Shadow Core

Reduced anonymity in major Eurasian hubs will trigger geographic displacement of criminal networks.

The most likely destinations include Nigeria, Tanzania, South Africa, Kenya, Pakistan, the Philippines, and Vietnam — regions characterized by:

• weak regulation,

• high P2P transaction volumes,

• strong transnational diasporas.

Digital crime will become more distributed, resilient, and less vulnerable to sanctions-based enforcement mechanisms.

8.4. The Emergence of a "Digital Iron Curtain" — A Split of the Crypto-Economy into Two Blocs

The global crypto-infrastructure is likely to divide into two technological spheres, reminiscent of the Cold War's financial system:

• a **controlled block** (EU–USA–Japan–South Korea),

• an **uncontrolled block** (Eurasia–Middle East–Southeast Asia–Africa).

The first will be dominated by fully identified providers, smart-reporting mechanisms, and rigorous regulatory KYC.

The second will rely on USDT flows, OTC markets, shadow liquidity, and high-opacity crypto-brokers.

A “digital border” will emerge between them — a structural analogue of **SWIFT vs. MIR**.

8.5. Integration of Crypto-Assets into International Law and Judicial Practice

International institutions (UN, FATF, ICSID, Interpol CCF) will begin forming dedicated legal standards for working with crypto-assets — from evidentiary rules to norms governing seizure, extradition, and restitution of digital funds.

Cryptocurrencies will become part of investment disputes, and corporate conflicts will increasingly be treated as digital disputes, where the object of prosecution is not a company but a cluster of wallets.

This will lead to the emergence of a new field of law: **International Crypto Litigation**.

9. ARGA Observatory Recommendations

9.1. For International Organizations and Intergovernmental Regulators (FATF, UNODC, OECD, INTERPOL, EUROPOL)

A global registry of cryptocurrency intermediaries and OTC operators must be created, functioning similarly to OFAC/EU sanctions lists.

Such a registry should include:

• risk parameters,

• jurisdiction,

• legal status,

• associated wallets,

• history of suspicious transactions.

Another key measure is the development of multilateral crypto-information exchange mechanisms, analogous to the SWIFT KYC Registry but applicable to USDT/USDC/DeFi operations.

This would enable the formation of a cross-border “operational map” of digital flows and significantly improve tracking of illicit routes.

It is essential to integrate **crypto-intelligence (CRPTINT)** as a mandatory component of international law enforcement.

INTERPOL, FATF, and UNODC should incorporate on-chain analytics, wallet clustering, and DeFi monitoring into standards for investigations and risk assessment.

9.2. For Regulators in the EU, USA, UK, Japan, and South Korea

A transition to a strengthened AML/KYC regime for OTC markets is required, including:

• mandatory licensing,

• disclosure of ultimate beneficial owners,

• automatic reporting of transactions above established thresholds.

Special attention should be given to high-risk jurisdictions (UAE, Georgia, Kazakhstan, Hong Kong, Kyrgyzstan), where cryptocurrency turnover is used to circumvent export controls and investigations.

It is recommended to introduce sanctions lists for crypto-operators, analogous to OFAC sectoral lists, with the ability to impose secondary sanctions on platforms servicing criminal flows, parallel imports, and crypto-laundering schemes.

Such measures would create a systemic pressure tool against illegitimate crypto-networks and strengthen the resilience of the global financial architecture.

9.3. For Academic Institutions, Research Centers, and Digital Criminology Labs

A long-term data repository on Eurasian crypto-criminal networks must be developed, including:

• on-chain clusters,

• OTC routes,

• P2P bridges,

• affiliated digital brokers.

This data corpus would serve as a foundation for independent expert analysis and international investigations.

Another priority is the development of a new discipline — crypto-criminology — positioned at the intersection of cryptography, financial analytics, criminology, international law, and geopolitics.

This field will enable risk modelling, forecasting of flow structures, and the creation of strategic recommendations for security institutions.

There is also a need for systematic research on the impact of cryptocurrencies on global security architecture, including:

• the emerging inter-bloc split of digital economies,

• threats to dollar stability,

• evolution of shadow markets,

• transformation of the role of international financial organizations.

10. Conclusion

Cryptocurrencies have ceased to be a technological experiment and have become an autonomous architecture of global power and capital distribution. Instead of remaining a peripheral innovation tool, digital assets have evolved into a second financial circuit of the world economy—non-state, unregulated, yet increasingly systemic. The USDT economy now functions as an alternative dollar-based settlement system, enabling billions of dollars to move across jurisdictions faster than state control mechanisms can operate.

In Eurasia, the cryptosphere has become the point where the interests of states, criminal organizations, corporations, and networks of digital intermediaries intersect. Blockchain transactions play the role of diplomacy, while OTC markets perform the functions of banking infrastructure—replacing SWIFT, national regulators, and intergovernmental mechanisms. Sanctions evasion, capital flight, parallel imports, shadow logistics, and cybercrime are integrated into a unified digital ecosystem in which money moves faster than the law can register violations.

The growth of the USDT sector shows that the world is entering a phase in which the financial system no longer belongs to the state. Transnational P2P structures and TRON payment chains create a space where monetary sovereignty becomes conditional. This threatens the traditional banking order—not only in terms of AML risks, but also in relation to monetary control, tax administration, and sanctions enforcement. Cryptocurrencies are forming a new class of power: power over liquidity outside the national legal system.

At the same time, the crypto ecosystem gives rise to a new configuration of criminality. Whereas in the 20th century criminal networks were territorial, today they are distributed, decentralized, and anonymous. Cybercrime no longer requires physical space: digital narcotics networks, financial pyramids, extortion rings, OTC banking brokers operate as a global corporation independent of borders, jurisdictions, legal currencies, or physical oversight. The strengthening of such systems inevitably leads to the emergence of a parallel security market, parallel justice, and a parallel economy in which legal order is replaced by the algorithmic logic of blockchain.

The ARGA Observatory's report demonstrates that crypto is already geopolitics, and control over digital liquidity is becoming the equivalent of controlling oil, gas, and the military-industrial complex of the past century. States, research centers, and global regulators are not merely observers of this transformation—they must intervene. If the international system fails to adapt in time, the balance of power will be determined not by central banks, but by networks of digital intermediaries that control the routing of illicit transactions.

The era of digital economy requires a new governance architecture—one in which blockchain analytics, crypto law, sanctions monitoring, and criminological science are integrated into a unified discipline. Building such a discipline is one of the key tasks of the coming years.

Sources

1. Chainalysis, 2024 Crypto Crime Trends, January 18, 2024, https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/.
2. TRM Labs, 2024 Crypto Adoption and Illicit Exposure Report, December 6, 2024, https://www.trmlabs.com/reports-and-whitepapers/2024-crypto-adoption-and-illicit-exposure-report.

3. FATF, Virtual Assets : Targeted Update on Implementation of the FATF Standarts on Virtual Assets and Virtual Assets Service Providers, Paris, 27 June 2019, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html.
4. FATF, High-Risk Jurisdictions subject to a Call for Action, Paris, 24 October 2025, https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Call-for-action-october-2025.html.
5. BIS, Tokenisation in the context of money and other assets : concepts and implications for central banks, 21 October 2024, https://www.bis.org/cpmi/publ/d225.htm.
6. UNODC, Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia : A Shifting Threat Landscape, October 2024, https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf.
7. BIS, Rashad Ahmed and Inaki Aldasaro, Stablecoins and safe asset prices, No 1270, 28 May 2025, https://www.bis.org/publ/work1270.htm.
8. TraCCC, Yylia Krylova, Dubai : A Global Hub for Illicit Trade and Sanctions Evasion, May 2023, https://traccc.gmu.edu/wp-content/uploads/2024/11/Dubai-report-Updated.pdf.
9. Binance, TRC-20-USDT Issuance Surpasses 78.7 Billion Tokens : The Rise and Risks of the TRON Network, https://www.binance.com/en/square/post/25426948660049.
10. BIS, III. The next-generation monetaryand financial system, 24 June 2025, https://www.bis.org/publ/arpdf/ar2025e3.htm.