Observatoire ARGA

Report on Sanctions and Compliance for 2025

CRYPTO-FINANCIAL PLATFORMS IN “GREY” JURISDICTIONS

Unlicensed Fintech Hubs, Pseudo-Banking Structures, OTC Clusters and Transnational Risks to International Security

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, 27 November 2025

Table of Contents

Executive Summary

From 2020 to 2025, the crypto-financial infrastructure of Eurasia shifted from a fragmented, marginal-use ecosystem to a constellation of fully formed regional financial clusters. The most notable trend is the concentration of unlicensed crypto-platforms and OTC fintech operators in so-called grey jurisdictions, which now function simultaneously as payment gateways, regulatory-evasion channels, and transit hubs for cross-border financial flows.

Georgia, Kazakhstan, Kyrgyzstan, Lithuania, the UAE, Turkey, Montenegro, Northern Cyprus and parts of Eastern Europe have developed an infrastructure that functionally resembles a banking system—yet lacks the core elements of legal accountability: licensing, AML/KYC controls, financial reporting, and compliance oversight. Many platforms act as *shadow liquidity providers*, servicing both legal parallel-import operations and high-risk financial flows linked to sanctions evasion, money laundering, and criminal logistics.

A key shift is that cryptocurrencies have ceased to be merely investment instruments. In grey jurisdictions they operate as a full-scale transactional currency, forming their own payment ecosystem where:

• USDT functions as a digital dollar,

• OTC markets replace banks,

• P2P platforms serve as retail FX markets,

• cash-out operations are faster than traditional currency conversion,

• crypto liquidity pools act as credit providers.

As a result, a phenomenon of pseudo-banking crypto-economy has emerged: capital moves through dozens of jurisdictions without touching the banking sector, while fintech operators de facto perform the functions of settlement and clearing centers.

ARGA Observatory notes increasing integration of these platforms into high-risk sectors: corporate conflicts, export-control evasion, digital narco-economies, dual-use trade, and capital flight from authoritarian regimes. Parallel to this, the volume of transactions initiated by political elites and security structures is rising, transforming crypto-financial platforms into instruments of geo-economic leverage.

This report maps grey crypto jurisdictions, classifies unlicensed platforms, analyzes their architecture and their risk vectors for international financial systems, and proposes regulatory and security mechanisms.

1. Methodology

The report uses a multilayered methodology combining blockchain forensics, investigative analytics, and macro-economic assessment of shadow financial flows. The core of the research is the triangulation of digital transactions, regulatory data, and real-world OTC infrastructure across Eurasia.

The document relies on the following data sources and methods:

— analysis of 180 OTC clusters and unlicensed crypto-platforms in Georgia, Kazakhstan, Kyrgyzstan, Turkey, the UAE, Lithuania, Serbia, Montenegro, Northern Cyprus and Eastern Europe;

— examination of transaction structures on TRON, Bitcoin, Ethereum, TON, BSC, including wallet-behavior segmentation, routing patterns, and token-mixing cycles;

— OSINT investigations of Telegram exchanges, OTC chats, private swap pools, P2P platforms, crypto-pawnshops and fintech nodes operating without banking-type licenses;

— FININT reconstruction of laundering chains: *fake import → OTC offshore → cash-out → reintegration into real estate/corporate assets*;

— analysis of reports by FATF, EU AMLA, FinCEN, ESMA, Interpol Crypto-Crime Reports, including cases of sanctions evasion and re-export schemes;

— review of court materials involving parallel trading, crypto-financing, AML/KYC evasion and Interpol Abuse in economic cases;

— ARGA Observatory's own datasets (2022–2025) on crypto-escrow networks, pseudo-banking nodes, OTC concentration, and capital-flight pathways from authoritarian regimes.

The methodology integrates:

• technical blockchain tracing,

• legal AML/CFT assessment,

• geoeconomic mapping of fintech hubs,

• expert and insider interviews.

This allows not only to describe the phenomenon, but to model its risk architecture, identifying how grey crypto-platforms evolve into a parallel banking system operating beyond the reach of international legal oversight.

2. Introduction: Crypto-Fintech as the New Shadow Banking System

Between 2020 and 2025, the cryptocurrency sector in Eurasia ceased to be a domain of private transactions and experimentation — it evolved into a full-scale financial infrastructure, an alternative to traditional banking. At the intersection of sanctions pressure, dollar liquidity shortages, weak regulatory regimes and high capital mobility, new fintech ecosystems emerged that effectively *perform banking functions while remaining outside international AML/KYC frameworks*.

So-called grey jurisdictions — Georgia, Kazakhstan, Kyrgyzstan, Lithuania, the UAE, Turkey and parts of the Balkans — have become key hubs where crypto-services transformed into *shadow settlement centers*, operating beyond the supervisory reach of the EU, the US and FATF. These zones have developed a parallel economic infrastructure that includes:

— unlicensed exchange nodes, capable of converting cryptocurrency into cash or bank transfers within minutes;

— large OTC pools, processing transactions from $50,000 to $50 million per day with no formal verification of funds' origin;

— fintech platforms without banking licenses, yet offering acquiring, P2P withdrawal, escrow storage and multi-currency conversion;

— digital pseudo-banks, providing asset custody, crypto-backed lending and cross-border capital outflows;

— distributed P2P networks, where user identification is often replaced by nominal operators and "financial brokers";

— crypto hubs linked to corporate, security and clan-based groups, making the system not only criminalized but politically instrumentalized.

Crypto-fintech has become a new form of banking *outside regulation*. It services not only classic criminal pipelines, but also:

• business structures attempting to bypass sanctions;

• political-corporate groups moving capital out of Eurasia;

• actors in corporate wars using crypto-transactions as leverage;

• parallel-import networks where cryptocurrency is embedded in supply-chain logistics;

• security and intelligence clusters operating in the grey zone.

The cryptocurrency market is no longer peripheral — it is an alternative infrastructure of global finance, where control is exercised not by states, but by algorithms, anonymity and distributed brokerage networks. This makes it not merely a financial instrument, but a new architecture of the global shadow economy — flexible, sanctions-resistant and largely inaccessible to traditional legal mechanisms.

3. Architecture of the "Grey" Cryptofinancial Ecosystem

ARGA Observatory notes that the shadow cryptofinancial system of Eurasia is not composed of chaotic channels, but of a *stable hierarchy* functioning as a parallel banking circuit. The ecosystem contains five interconnected layers which can substitute for one another when needed, making the system nearly immune to direct shutdown.

3.1. OTC Clusters — Core Settlement Nodes of Shadow Liquidity

The most concentrated form of "grey" crypto-banking is represented by large OTC centres in Georgia, the UAE (Dubai, Ajman), Kazakhstan (Almaty, Astana), Lithuania, and Turkey.

They perform bank-like functions *outside regulation*:

- daily turnover at some points reaches $5–80 million, rising even higher during sanctions bottlenecks;
- transactions require no KYC, no passport, no proof of funds — the only identifier may be a Telegram nickname;
- many OTC desks maintain direct links with criminal networks and brokers of the parallel-import economy.

These clusters manage liquidity, redistribute USDT balances, and ensure rapid fiat on/off-ramping. For sanction-sensitive operations, they function as financial "laundries" with banking speed but without banking rules.

3.2. High-Density P2P Platforms

P2P platforms form the *mass layer* of the cryptofinancial structure. Their core characteristics:

- tens of thousands of micro-transactions daily → extremely fast turnover;
- derivative crypto trading with USDT as the settlement unit;
- users can remain fully anonymous even when conducting large operations.

P2P activity ensures the system's resilience. Even if an OTC hub is shut down, flows disintegrate into hundreds of small routes, impossible to track without advanced crypto-intelligence. In this layer, traditional banking disappears → control shifts to algorithms

3.3. Shadow Fintech Companies — Next-Generation Pseudobanks

These entities constitute the core of unlicensed cryptoeconomics. Such companies:

- may outwardly resemble IT start-ups, yet operate as banks without licences;
- provide asset custody, lending, multi-currency conversion, escrow freezing, and large-volume crypto transit;
- rely on high-capacity corporate wallets shielding real beneficiaries.

Many are run by individuals with financial expertise or former compliance officers — making their operations professional, discreet and difficult to detect.

3.4. Offshore SPV Structures — The Veneer of Legality

Offshore SPV platforms (BVI, Belize, Seychelles, UAE Free Zones) provide:

- a legal façade for dark capital;
- tokenisation of illicit assets (commodities, real estate, corporate shares);
- interaction with foreign brokers and crypto-platforms in EU/SG/HK.

Through this layer, funds undergo legal-wrapping — a formal whitening stage after which they become nearly indistinguishable from legitimate capital.

3.5. Links to Security and Corporate-Political Structures

The shadow cryptofinancial economy operates within, not outside, state and elite networks:

- crypto is used as a tool in corporate wars — for asset extraction, freezing and pressure;
- security agencies receive a share of transit flows and provide "cover";
- crypto-transactions fund cross-border operations: pressure campaigns, surveillance, buy-offs, and corporate raids.

Thus, "grey" cryptobanking is not merely a criminal environment — it has become a *technical backbone* for political-economic elites, offering them a way out of the sanctioned financial system.

4. Geography of Key Hubs

The geography of the unlicensed crypto-infrastructure in Eurasia did not emerge randomly — it aligns with zones of political neutrality, weak financial oversight, opaque corporate registries, and intense parallel-import flows. These territories function as *borderline banking ecosystems*, where crypto replaces SWIFT and OTC deals substitute traditional bank transactions.

4.1. Georgia (Tbilisi, Batumi)

Georgia has become the largest unlicensed cryptocurrency hub in Europe and Central Eurasia.

Key features:

- high concentration of OTC operators working through Telegram and closed chats;
- conversion available without KYC and without any AML obligations;
- stable channels for USDT → cash → goods;
- liquidity exported to Russia, Türkiye, the UAE, and the Caucasus;
- crypto-based logistics embedded in parallel import of electronics, auto parts, and equipment.

Tbilisi is the main settlement hub,

Batumi — the key cash-out and offshore-routing point.

According to ARGA Observatory, the daily capital flow through the Georgian OTC corridor is comparable to the banking turnover of a mid-sized European city.

4.2. Kazakhstan and Kyrgyzstan

These two countries function as a single crypto-transport corridor within the EAEU.

Role of the region:

- transit of USDT flows to and from Russia;
- a hotspot for P2P markets and small-size high-frequency transactions;
- registration of pseudo-FX fintech services offering "digital deposits";
- use of crypto payments for parallel import, procurement, and logistics.

Almaty — the main liquidity distributor.

Bishkek — a P2P hub where crypto is used as a *quasi-currency* in both retail and commercial transactions.

Here, cryptobanking is already integrated into everyday economic activity.

4.3. Lithuania

Lithuania is the most technologically developed yet most vulnerable crypto hub within the EU.

Characteristics:

- registration of fintech companies effectively operating as crypto platforms;
- EU jurisdiction → access to SEPA, banking infrastructure, and European markets;
- risky combination of pseudo-licenses and simplified entry for non-residents;
- active use as a conduit for transferring funds from the EAEU into Europe.

Lithuania is the only hub where "grey" cryptobanking can realistically masquerade as legitimate European fintech, increasing the risk of infiltration into the EU financial system.

4.4. UAE

The UAE is a global center of unlicensed crypto liquidity.

Compared to Georgia or the EAEU, the UAE hosts a far more complex corporate architecture:

- Dubai OTC markets — the largest conversion hubs in Eurasia;
- emergence of private digital banks offering custody, lending, and conversion;
- large transactions conducted without meaningful AML filters and masked via SPV structures;
- crypto converted into real estate, assets, and investment vehicles.

Dubai is the point where dark capital becomes white — unless intercepted by external intelligence or compliance scrutiny.

4.5. Türkiye

Türkiye is the main crypto and logistics bridge between Eurasia and the Middle East.

Key elements:

- major unregulated crypto exchanges and a dense P2P market;
- USDT transit along the Russia → UAE → EU route;
- weak oversight of OTC trading;
- corporate groups using crypto for procurement and import payments.

Istanbul — the center of large-scale settlements.

Antalya and Mersin — regional entry points for "digital-to-cash-to-goods" schemes.

5. Core Models of Shadow Crypto Operations

ARGA Observatory identifies five primary schemes most frequently used within the "grey" crypto-financial infrastructure in Eurasia. These schemes differ in anonymity levels, risk exposure, intermediary involvement, and blockchain-tracing complexity.

5.1. USDT → OTC → Fiat

The classic and most widespread digital-laundering model.

Mechanism:

- cryptocurrency (in 90% of cases USDT-TRC20) is sent to a cash-out point;
- the OTC operator converts it into cash without KYC or AML;
- funds are delivered physically or sent to local bank accounts;
- in several countries, the final step involves purchasing goods or logistical re-export.

Why it works:

- USDT does not require banking confirmation of source of funds;
- OTC exchangers are not obliged to report data to regulators;
- withdrawal can occur in batches of 5,000–500,000 USD without any identification.

This is the main cash-out mechanism for shadow capital — from corporate conflicts to narcotics networks.

5.2. Off-chain Trading

Transactions that do not fully appear on the blockchain.

Application:

- final settlements are executed not via on-chain transfers but through internal platform balances (ledger-to-ledger);
- operators maintain only internal ledgers, which are not public and can be erased;
- the buyer ultimately receives an asset, goods, or fiat with no trace in public registries.

Problem:

- even digital forensics cannot reconstruct the full transaction trail;
- evidentiary value in international courts drops sharply.

5.3. Token-layering

A multi-stage method for blurring the digital trail.

How it works:

- funds pass through 5–15 intermediary wallets, sometimes hundreds;
- blockchain bridges (cross-chain swaps) are used;

- mixers, smart-routing, and automated micro-splitting of transfers.

Purpose:

- maximum loss of traceability;
- preventing linkage between the origin and the destination wallet.

Example: 1,000,000 USDT → split into 400 × 2,500 USD transactions → OTC market → fiat → SPV.

5.4. "Cold" Corporate Wallets

Long-term liquidity storage with delayed withdrawal.

Usage:

- funds accumulate in cold wallets, inaccessible online;
- keys distributed among several holders or protected via multi-sig;
- withdrawal occurs only after preparation steps:

1. setting up an offshore SPV (BVI / Belize / UAE),
2. registering a purchasing entity,
3. acquiring an asset or routing through OTC.

The objective is accumulating capital without risk of immediate detection.

5.5. Conversion into Compliant Assets

The final stage of laundering — full legalization.

Types of assets:

- real estate in the UAE, Türkiye, Georgia, Spain, Cyprus;
- premium vehicles later resold;
- offshore SPVs used to inject capital into businesses.

Key feature:

- once converted into a compliant asset, the origin of funds no longer appears crypto-criminal;
- the asset can serve as collateral, corporate property, or part of an investment portfolio.

This converts "digital money of unknown origin" → into legally recognized structures.

6. Case Studies

Case 1 — The Georgian OTC Corridor (Anonymized Case)

Turnover: ~70 million USD per month

Scheme: USDT → OTC → EUR → physical and corporate conversion

A route documented across several independent sources involved dozens of private OTC operators in Tbilisi and Batumi. The main flow consisted of USDT-TRC20 arriving into exchangers' hot wallets, where the funds were fragmented, passed through short concealment chains, and then converted into euros and dollars. Intermediaries linked to two fintech groups participated, providing guaranteed liquidity and exchange rates below the banking market.

A typical cycle functioned as follows:

1. incoming USDT batches of 200,000–900,000 USD;
2. local conversion into cash EUR / USD;
3. further transfers into the EU through bank channels — labeled as "payment for equipment," "IT services," or "logistics";
4. placement of funds in accounts of companies registered in Czechia / Poland / Slovakia.

Notable feature: the active role of brokers who acted not only as exchange points but also as gateways into Western payment systems. The system operated for at least 19 months, ensuring high-speed liquidity with minimal regulatory footprint.

Case 2 — Lithuanian Fintech Shell

Structure: a registered "financial company" → corporate wallets → equipment import chain

The case is based on the analysis of a company that formally held the status of a payment service provider (PSP) but in practice functioned as a high-risk crypto hub. The entity controlled several corporate wallets (USDT / ERC-20) through which client funds — primarily belonging to non-residents — circulated.

Mechanism:

1. registration of a fintech company in Lithuania under a PSP regime;
2. activation of corporate wallets and P2P withdrawal channels;
3. cooperation with EU logistics providers to import equipment (telecom, electronics, servers);
4. resale of goods to third countries for cash or USDT.

As a result, cryptocurrency was transformed into high-liquidity physical goods, which were later converted back into fiat across the EAEU states, Türkiye, and the UAE. The financial trail became blurred: the blockchain segment was split from the material extraction of value.

Case 3 — UAE Digital Pseudo-Banking Center

Scheme: USDT → AED → EUR via Asian brokers

ARGA Observatory identifies a cluster of several dozen exchange centers in Dubai and Sharjah operating as "digital banks" — receiving large volumes of cryptocurrency, including USDT, USDC, and BTC, and performing rapid cash-outs into dirhams.

Typical operational logic:

1. large USDT tranches arrive into hot wallets;
2. funds are cashed out in AED with no KYC checks;
3. subsequent transfers are routed to Europe through Asian brokers (Hong Kong, Singapore);

4. final EUR amounts are credited to corporate accounts of import companies, often incorporated for single-use transactions.

Key indicator: persistent links to brokerage structures that provide the “bridging layer” connecting crypto, offshore entities, and Eurozone corporate accounts. The scheme is used for capital flight, sanctions evasion, and financing of shadow imports.

7. International Risks

1. Infiltration of Criminal Networks into EU Payment Systems

The ecosystem of unlicensed fintech platforms creates a parallel channel for introducing funds into the European financial sector. OTC clusters in Georgia, Lithuania, the UAE and Kazakhstan enable opaque movement of large USDT/fiat volumes, eroding the effectiveness of AML filters.

When banking gateways become interconnected with shadow crypto channels, compliance systems lose the ability to identify the true source of funds.

This poses a direct threat to the financial sovereignty of the EU, as criminal transactions become indistinguishable from legitimate payments, and anonymous capital gains systemic access to European markets, real estate and corporate structures.

2. Use of Crypto to Evade Sanctions

Grey jurisdictions already allow crypto flows to be integrated with foreign-trade operations, supply-chain financing, offshore SPVs and parallel-import routes.

The absence of centralized regulation for OTC markets turns cryptocurrency into a sanctions-evasion mechanism, regardless of the political will of states.

Where sanctions violations once required cooperation from banks and intermediaries, now the trajectory can be routed through a handful of USDT wallets and P2P aggregators, remaining fully invisible to classical AML systems.

This leads to destabilization of EU/US sanctions regimes and weakens international law through technological adaptation of the market.

3. Economic Pressure on Businesses through Digital Schemes

Unlicensed crypto-financial infrastructures are used not only by criminal groups but also by private corporate clans.

USDT → OTC → Fiat mechanisms allow actors to create leverage in corporate conflicts — to withdraw assets, finance hostile takeovers, pay for PR attacks, or conduct digital harassment against competitors.

Thus, cryptocurrency becomes not only a financial rail but an instrument of coercive influence in corporate warfare and business governance.

4. Blurring of Boundaries Between the State and Criminal Actors

In several jurisdictions, unlicensed crypto platforms have become intertwined with security structures and politico-economic elites.

OTC exchangers are used as services for:

• funding special operations,

• moving officials' assets offshore,

• paying for covert logistics,

• supporting extraterritorial activity.

This leads to the formation of hybrid economies, where government policy and criminal capital operate along the same financial routes.

Under such conditions, traditional law-enforcement mechanisms lose effectiveness because the object of legal control fractures into decentralized nodes.

5. Threat to International Financial Institutions

As digital "grey banks" and OTC hubs begin to function as parallel payment systems, the banking sector loses its monopoly over settlement infrastructure.

USDT becomes a currency outside regulation:

— not issued by a state,

— not controlled by a central bank,

— not dependent on monetary policy.

This creates a global risk of parallel dollarization, in which crypto liquidity replaces banking liquidity, and institutional regulators lose control over balances, money supply, and cross-border capital flows.

8. Forecast 2025–2027

1. Growth of Highly-Tuned OTC Networks

As regulatory pressure increases, traditional unlicensed exchangers will evolve into multi-layered decentralized structures with distributed responsibility.

Operational models will shift from open trading to closed, point-to-point channels accessible only through trusted intermediaries and crypto-guarantors.

"Second-generation OTC clusters" will emerge, functioning as anonymous fintech complexes hidden inside P2P markets, mixers, DAO-like structures and closed Telegram infrastructures.

2. OTC Regulation at the EU and U.S. Level

Within the next two years, the first attempt at systematic international regulation of OTC markets is expected.

The EU and the U.S. will develop:

– cross-border AML registries,

– reporting requirements for OTC operators,

– jurisdictional risk indices,

– restrictions on operating fintech exchangers without licenses.

Tighter oversight will push part of the OTC ecosystem out of the compliant environment, while simultaneously incentivizing a deeper shift of such services into the grey underground layer.

3. Migration of Criminal Networks to the TON Infrastructure

Increasing pressure on TRON/USDT will inevitably accelerate the transition to alternative technologies — primarily TON, tightly integrated with Telegram marketplaces.

We can expect the emergence of TON-banks, TON-laundering modules and TON-exchangers disguised as bots and API services.

TON may become the new operational currency system of the shadow market because it enables:

– transactions directly within the Telegram ecosystem,

– reduced auditability of financial traces,

– integration of payments with chat-bots and marketplace logic.

4. Pressure on “Grey” Jurisdictions

Georgia, Lithuania, Kazakhstan, Kyrgyzstan, the UAE and Turkey will face increasing international pressure aimed at:

– improving transparency of exchange platforms,

– licensing OTC operators,

– eliminating corporate–security-service influence,

– establishing data-sharing with the EU/U.S.

Some countries will adopt adaptive strategies — gradual legalization and formalization of the crypto sector.

Others will choose a confrontational model, relying on economic benefits derived from shadow liquidity.

As a result, the global map of crypto hubs may shift toward Africa, Asia and Latin America.

5. Creation of a Global Registry of Crypto Intermediaries

A launch of an international system for monitoring crypto intermediaries is likely, integrating:

– AML data,

– sanctions lists,

– information on intermediaries and beneficial owners,

– links to high-risk jurisdictions.

Such a registry may become a crypto-equivalent of Interpol, where transaction traces and participant identification are performed automatically through risk-analytics.

Its emergence would mark a turning point — the transition to Smart-Regulation 2.0, in which regulatory systems do not merely react to violations but anticipate them.

9. ARGA Observatory Recommendations

For international bodies and supranational regulators

The international system requires a unified tool for assessing and monitoring crypto-risks — a global crypto-risk index, capable of classifying jurisdictions, OTC clusters and platforms in real time as *low-*, *medium-*, or *high-risk* zones.

Such an index must account not only for transaction volume, but also for:

– the presence of unlicensed operators,

– the scale of P2P trading outside KYC/AML,

– the activity of Binance-like shadow brokers,

– links to offshore entities and corporate SPVs,

– involvement in sanctions evasion and parallel import schemes.

In parallel, a dedicated international monitoring regime is needed for shadow fintech structures, including digital pseudo-banks, OTC intermediaries, Telegram-based infrastructures and corporate wallets.

The Travel Rule must be expanded to apply not only to licensed exchanges, but also to OTC operators, fintech wallets, off-chain platforms and TON marketplaces — otherwise the rule loses its effectiveness.

For the EU, United States and United Kingdom

A core priority for the coming years is the regulation of OTC operators on par with exchanges and crypto-service providers, including mandatory licensing, registration, reporting and KYC monitoring.

Without this, the global AML framework will remain fragmented.

A targeted sanctions regime against pseudo-banks — companies and individuals operating digital clearing without licenses, converting USDT→fiat, performing token-layering and multisystem routing via Lithuania, Turkey, the UAE, Georgia and Kazakhstan — should be introduced.

Such a regime must include:

– account closures,

– blocking of corporate wallets,

– prohibition from operating in the fintech sector,

– extraterritorial liability for intermediaries.

This would significantly reduce crypto-laundering capabilities and restrict grey-market routes used for parallel import schemes.

For academic institutions and research centers

ARGA Observatory recommends the systematic development of crypto-criminology as an independent research field. This requires:

– building databases of OTC operators,

– tracing USDT→Fiat→Offshore routes,

– documenting cases of parallel import and crypto-financing,

– developing methodologies for analyzing multi-chain transactions,

– studying the migration of narcotic, corporate and corruption networks to TON/TRON infrastructures.

Academic analysis must incorporate not only legal frameworks but also market behavioral patterns — transaction velocity, network density, activity clusters and capabilities for automated risk-scoring.

10. Conclusion

Crypto-financial platforms in *"grey"* jurisdictions have ceased to be a peripheral element of the digital economy and have effectively transformed into an alternative banking circuit, partially autonomous from state regulation and international financial mechanisms. This system operates

with significant capital volumes, enables anonymous transactions, supports parallel import schemes, corporate conflicts, grey financial flows and transnational shadow networks.

In several regions (Georgia, the UAE, Kazakhstan, Lithuania, Turkey), crypto-OTC clusters have become more than exchange infrastructure — they now function as settlement centers that can compete with lightly regulated traditional banks in both transaction speed and liquidity.

A full-scale ecosystem has emerged that is capable of:

• accumulating large volumes of funds outside AML/KYC oversight,

• enabling cross-border settlements circumventing sanctions and export controls,

• supporting digital logistics for goods and services,

• serving as an instrument of economic coercion and corporate warfare,

• masking the origin of capital through multi-layered transactions and SPV structures.

Within this paradigm, cryptocurrencies are only one component. More significant is the rise of shadow pseudo-banks — fintech nodes that provide clearing, escrow storage, off-chain transactions, token-layering and conversion of funds into traditional assets. These mechanisms allow financial flows to remain operational even under sanctions pressure, banking restrictions and law-enforcement actions. As a result, the crypto-infrastructure becomes resistant to traditional tools of control, increasing the burden on international regulators and global financial security.

The ARGA Observatory report establishes an analytical framework for assessing this phenomenon and underscores the need for a new global regulatory model capable of accounting for the digital decentralization of markets, the extraterritorial nature of transactions, and the rapid emergence of unlicensed operators.

In the coming years, a central challenge will be the synchronization of AML policy, export-control mechanisms, sanctions regimes and crypto-regulation. Without such integration, the global economic system will face expanding grey flows, the proliferation of parallel jurisdictions and a gradual erosion of state financial governance.

Crypto-financial hubs in “grey” zones are not an anomaly — they represent a new reality of the world economy, requiring a strategic response grounded in data, transactional models and international coordination. The ARGA Observatory provides an analytical basis for designing such an architecture and developing tools to prevent financial risks, money laundering and the digital criminalization of markets.

Sources

1. FATF, Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, Paris, 28 October 2021, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html.
2. FATF, Targeted Update on Implementation of the FATF Standarts on Virtual Assets and Virtual Asset Service Providers, 2025, https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2025-Targeted-Upate-VA-VASPs.pdf.coredownload.pdf.

3. FinCEN, Notice on the Use of Convertible Virtual Currency Kiosks for Scam Payments and Other Illicit Activity, August 4, 2025, https://www.fincen.gov/system/files/2025-08/FinCEN-Notice-CVCKIOSK.pdf.
4. EBA, Report on tackling ML/TF risks on crypto-asset services through supervision, October 2025, https://www.eba.europa.eu/sites/default/files/2025-10/6a64efb9-98e9-4e90-a5c5-2704a8ca8ef9/Report%20on%20tackling%20ML%20TF%20risks%20in%20crypto-asset%20services%20through%20supervision.pdf.
5. ESMA, Markets in Crypto-Assets Regulation (MiCA), https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica.
6. OFAC, Sanctions Compliance Guidance for the Virtual Currency Industry, October 2021, https://ofac.treasury.gov/media/913571/download?inline.
7. ICIJ, The Coin Laundry, Scilla Alecci, Hunt for missing millions unmasks one crypto exchange hidden inside another, November 20, 2025, https://www.icij.org/investigations/coin-laundry/hunt-for-missing-millions-unmasks-one-crypto-exchange-hidden-inside-another/.
8. CSIS, William Alan Reinsch and Andrea Leonard Palazzi, Cryptocurrencies and U.S. Sanctions Evasion : Implications for Russia, December 20, 2022, https://www.csis.org/analysis/cryptocurrencies-and-us-sanctions-evasion-implications-russia.
9. TRMLabs, Illicit Crypto Ecosystem Report, June 2023, https://www.trmlabs.com/resources/reports/the-illicit-crypto-ecosystem-report-2022.
10. OCCRP, Inci Sayki, Elliptic : Over $4 Billion in Illicit Crypto Laundered via Cross-Chain Technologies, October 7, 2022, https://www.occrp.org/en/news/elliptic-over-4-billion-in-illicit-crypto-laundered-via-cross-chain-technologies?gad_source=1&gad_campaignid=22567027894&gbraid=0AAAADO79RdD-rCOja8ygctf_JTAubuGo&gclid=Cj0KCQiAiqDJBhCXARIsABk2kSkMcUL_O9oWWJV8J1WxJKtAtmSgb2RGyS2PNQUdYmuCrdjo34oWI9oaAkdmEALw_wcB.
11. IFM, The Crypto Ecosystem and Financial Stability Challenges, Chapter 2, October 2021, https://www.imf.org/-/media/files/publications/gfsr/2021/october/english/ch2.pdf.