Crypto, Sanctions & Corporate Risk

IMPLICATIONS FOR MULTINATIONAL FIRMS

20763 Geopolitics for Business – Group Consulting 2

Crypto, Sanctions and Corporate Risk

Implications for Multinational Firms

Geopolitics of Bitcoin — Group Paper

Group Members:

Marialuisa Bertelli | 3161532
Camilla Bianco | 3165589
Matteo Buscaglia | 3180057
August Ehrenstein | 3387699
Akari Hase | 3295945
Lara Neise | 3387654
Francesco Rossetto | 3320071

Table of Contents

1. Introduction

For decades, economic sanctions have served as the West’s primary instrument when diplomatic efforts fail and military action is not pursued. The underlying logic is that isolating a country from the global financial system will generate sufficient economic pressure to induce a change in behavior. This depends on the assumption that international money moves through centralized, regulated channels where enforcement is possible. For most of the post-Cold War era, that assumption held. The United States, leveraging the dollar's reserve currency status and its control over institutions such as OFAC (Office of Foreign Assets Control), was able to turn financial interdependence into coercive power, what Farrell and Newman (2019; 2022) call "weaponized interdependence."

That assumption is now under serious pressure. The emergence of decentralized digital assets has opened alternative channels for moving value across borders without relying on traditional financial intermediaries. Early assessments tended to dismiss the threat, pointing to crypto markets' small scale, high volatility, and dependence on regulated exchanges (BAFFI-MINTS, 2022). The numbers have since told a different story. Sanctioned nations received $15.8 billion in cryptocurrency in 2024, representing 39% of all illicit digital asset transactions globally (Tsentsura, 2025). Russia, after the unprecedented financial blockade imposed following its 2022 invasion of Ukraine, built a state-supervised crypto settlement infrastructure in under two years, using Bitcoin, Ethereum, and USDT to route oil payments with China and India entirely outside the dollar system (Hirtenstein and Aizhu, 2025). Iran, drawing on decades of isolation, developed a parallel financial ecosystem rooted in large-scale Bitcoin mining and stablecoin-based trade finance, with estimated annual USDT volumes ranging from $6.2 to $12 billion (Sonmez, 2025). In both cases, what started as improvisation has hardened into deliberate, state-backed infrastructure.

The implications reach well beyond the governments directly involved. For multinational corporations, this shift fundamentally changes the compliance risk landscape. Exposure no longer comes primarily from direct dealings with listed entities, but through layered intermediary chains, alternative payment rails, and financial flows engineered to look legitimate at every individual step while ultimately serving sanctioned actors at the network level. Under IEEPA (International Emergency Economic Powers Act), strict liability applies regardless of intent: inadvertent facilitation through a commodity broker, a freight intermediary, or a non-bank payment processor can carry the same legal consequences as deliberate evasion (Wright, 2023). At the same time, regulatory responses remain uneven. Enforcement architecture has advanced significantly in the United States and Europe, yet implementation gaps, jurisdictional arbitrage, and the adaptive resilience of successor exchange networks continue to limit its reach (RUSI, 2025; FATF, 2025).

This report provides a comprehensive analysis of the intersection between cryptocurrency and sanctions risk. It examines how sanctioned states have turned crypto's theoretical potential into operational reality, assesses the corporate risk landscape across compliance, treasury, and supply chain dimensions, evaluates the current regulatory and enforcement outlook, and develops forward-looking scenarios and recommendations to support strategic decision-making in an increasingly fragmented financial environment.

2. Sanctions as Financial Coercion

2.1 The Architecture of Financial Sanctions

At their core, economic sanctions work as a tool of financial coercion by restricting access to the infrastructures that enable cross-border transactions. Sanctions mainly limit access to financial services, reserve currencies and payment systems that support the global economy, rather than physically stopping trade. The effectiveness of sanctions depends on control over essential nodes of the global financial system, especially dollar-dominated clearing and correspondent banking networks (U.S. Government Accountability Office [GAO], 2024).

The United States has the ability to freeze assets, restrict transactions, and impose secondary sanctions on third parties through the Office of Foreign Assets Control (OFAC), and therefore plays a central role. Because of the world's reliance on the dollar and U.S.-affiliated financial institutions, these policies go beyond U.S. control. At the multilateral level, the European Union uses coordinated regulatory tools to carry out its own restrictive measures, while the United Nations offers a legal basis for sanctions. However, responsibility for enforcement ultimately depends on financial intermediaries that convert legal restrictions into operational exclusion, such as banks, payment processors and clearing systems (OFAC, 2021; GAO, 2024).

Correspondent banking networks and messaging services like SWIFT are crucial for cross-border payments, as they enable secure communication between financial institutions. SWIFT complies with regulatory obligations and has the authority to disconnect sanctioned businesses as required, even if it does not impose sanctions on its own. Therefore, being cut off from these networks severely restricts a nation's capacity to transact internationally (GAO, 2024).

2.2 The Limits of the Model: Why Sanctions Depend on Centralized Finance

This logic draws from the concept of "weaponized interdependence", defined by recent literature, according to which states that control central nodes of global financial networks can leverage them for coercive purposes. Farrell and Newman (2019) argue that the global system's structure enables states to monitor and restrict the flows passing through the networks. As a consequence, economic interdependence becomes a source of geopolitical power.

From a theoretical perspective, there are multiple forms of sanctions, which range from comprehensive country-level restrictions to targeted measures against individuals, firms, or specific sectors. They generally become more effective when economic pressure is generated

through constraining access to liquidity, increasing transaction costs, and reducing the ability of targeted actors to engage in international trade. However, as Drezner (2011) notes, the success of sanctions ultimately depends on the ability to enforce them through control of financial channels and compliance mechanisms embedded within the global financial system.

There is therefore one key assumption this model relies on: most financial flows go through centralized and regulated intermediaries where enforcement is possible. Restricted access to these intermediaries means the success of economic pressure transmission. However, this reliance on centralized infrastructures also introduces structural weaknesses when alternative systems avoid these nodes (Farrell and Newman, 2022; GAO, 2024).

2.3 Crypto as a Structural Challenge

The previously mentioned assumption is increasingly challenged. Digital assets introduce alternative channels for transferring value without having to rely on traditional intermediaries. Cryptocurrencies can be transferred peer-to-peer, across borders, and without direct interaction with regulated financial institutions. According to the Financial Action Task Force (FATF, 2024), virtual assets enable transactions through unhosted wallets and decentralized platforms, reducing dependence on conventional banking systems and creating potential gaps in sanctions enforcement.

In 2022, it was mainly believed that cryptocurrencies posed only a limited threat to sanctions effectiveness. Bocconi University's BAFFI-MINTS research unit noted that crypto's claimed decentralization was "actually a myth," since most transactions passed through centralized exchanges subject to KYC/AML regulations (BAFFI-MINTS, 2022). This reflected official assessments emphasizing crypto markets' small size, high volatility and dependence on centralized exchanges. Moreover, the transparency of blockchain transactions was seen as a constraint on large-scale evasion (OFAC, 2021; FATF, 2024).

Recent developments suggest a more nuanced reality. Cryptocurrencies have not replaced traditional financial infrastructures, but their role as complementary channels has expanded. According to the GAO, increased adoption of digital assets and inconsistent global regulation have created opportunities for sanctioned actors to exploit gaps in oversight. Academic research further highlights that digital assets and decentralized finance can reshape cross-border payment dynamics by reducing reliance on traditional intermediaries (Auer, Cornelli, and Frost, 2022; IMF, 2024).

The main change comes from the creation of alternative pathways at the margins of the system. Sanctioned actors can combine conventional and crypto-based mechanisms to

maintain access to global markets. This hybridization makes sanctions less effective, as evasion becomes less expensive and enforcement more complex.

This has significant implications for multinational firms. Sanctions risk can now arise through complex intermediary chains and alternative payment mechanisms, not only through direct transactions with sanctioned entities. Companies must therefore navigate a system where compliance relies on both transaction architecture and counterparties (GAO, 2024).

3. How Sanctioned States Use Crypto

Crypto-assets create alternative channels that are only partly dependent on centralized infrastructures such as SWIFT, which can help actors circumvent dollar-dominated financial systems (Reinsch & Palazzi, 2022). In 2024, sanctioned nations received $15.8 billion in cryptocurrency, representing 39% of all illicit digital asset transactions globally. It shows how digital assets are increasingly used to sustain financial resilience under sanctions (Tsentsura, 2025).

At the micro level, sanctioned actors use transaction obfuscation techniques, including “virtual-to-virtual layering schemes” that make transfers easier, cheaper, and harder to trace (Pocher, 2025). However, these methods remain limited by liquidity constraints, blockchain traceability, and the need to eventually connect with regulated financial systems.

At the macro level, crypto use is becoming more institutionalized. FATF (2024) documents how state-affiliated actors have progressively moved from opportunistic evasion to deliberate, government-backed financial infrastructure, with central banks and state institutions assuming direct roles in digital asset strategy. As a result, crypto adoption is shifting from uncoordinated practices toward state-aligned infrastructures shaped by economic constraints.

Model 1: Crypto as trade settlement (Russia)

Russia represents a model in which crypto functions primarily as a trade settlement instrument. Due to its partial exclusion from the global financial system, Russia has explored the use of cryptocurrencies and stablecoins to facilitate cross-border payments, particularly in energy trade. Digital assets have been used in transactions with partners such as China and India, allowing Russian firms to bypass dollar-denominated channels (Hirtenstein & Aizhu, 2025). This shift reflects broader fragmentation in the global financial system, as geopolitical risk and sanctions pressures reduce reliance on traditional banking networks (Skinner, 2023). In response, Russia has institutionalized alternative mechanisms, including state-supervised crypto-based international payments, to reduce dependence on Western-controlled systems (Bryanski, 2024). However, these arrangements remain supplementary rather than substitutive. Their effectiveness is constrained by limited liquidity, price volatility, and continued exposure to broader economic conditions, which limit crypto’s reliability as a stable financial mechanism (Kuchkarov et al., 2025; Hodula, 2025).

Model 2: Crypto as energy conversion (Iran)

Iran illustrates a model in which crypto converts domestic resources into globally transferable value. Leveraging abundant subsidized energy, it has developed a large-scale Bitcoin mining sector, which means that excess oil and gas turn into digital assets (Wright, 2023). Low

production costs, which are around $1,320 per Bitcoin, further reinforce this strategy (More, 2025). In fact, the Iranian Central Bank has conditionally permitted mining under a regulated framework (Faghih et al., 2025). In this context, crypto has become a key component of Iran's sanctions response. Beyond production, it is also used in external payments, with stablecoins such as USDT facilitating imports, estimated at $6.2 to 12 billion annually, particularly through China, Turkey, and the UAE (Sonmez, 2025). This model allows Iran to bypass export constraints by embedding value creation within the crypto ecosystem. However, its effectiveness remains limited by regulatory ambiguity and reliance on external trading partners.

These two models are not merely theoretical. The following sections examine each in depth, tracing how Russia and Iran have built the legal frameworks, financial infrastructure, and operational mechanisms that turn these strategies into reality.

4. Russia's Financial Adaptation to Western Sanctions: A Case Study

4.1 Why Russia needed an alternative

Russia's engagement with alternative payment infrastructure is best understood as a structural response to progressive financial exclusion. The sanctioning coalition's measures, initiated following the 2014 annexation of Crimea through asset freezes, travel restrictions, and investment constraints, imposed estimated losses of around $50 billion (Wright, 2023) while proving insufficient to fracture the system, leaving Russia with reduced but functional access to global finance.

The post-2022 escalation operated on a qualitatively different scale. The simultaneous disconnection of major Russian banks from SWIFT, the immobilization of approximately $300 billion in sovereign reserves, and broad export controls on critical technologies (Wright, 2023) collectively removed the institutional foundations on which conventional cross-border settlement depends. The pressure extended beyond the sanctioning coalition itself. By 2023, financial institutions in China and Turkey, jurisdictions that had not formally adopted the measures, started declining Russian transactions in response to secondary-sanctions exposure risk, which extends U.S. restrictive measures to non-U.S. entities transacting with sanctioned parties (Hirtenstein and Aizhu, 2025). Russia's Central Bank acknowledged the resulting constraints as a significant structural challenge. It is against this background of effective payment channel closure that Russia has turned to cryptocurrency

4.2 How Moscow built the legal architecture

Russia's legislative response to financial exclusion followed a trajectory of rapid institutional reversal. The same Central Bank that had formally characterized digital assets as pyramid-like instruments in early 2022 (RAND, 2025) had, under the pressure of accelerating financial isolation, repositioned those same assets as a legitimate component of Russia's international payments architecture within two and a half years.

The simultaneous legalization of nationwide crypto mining and the creation of an Experimental Legal Regime granting the Central Bank authority over cross-border digital settlements, both enacted in a single July 2024 legislative session, established the twin foundations of state oversight and operational authorization. Fiscal legislation classifying digital currencies as taxable property further anchored this framework within the formal economy. The coherence of these moves suggests deliberate architectural design: a state seeking to bring crypto use under institutional control and deploy it as a strategic instrument.

The deployment of crypto custody services by Sberbank and the construction of dedicated international payment infrastructure at VTB, led by personnel drawn directly from the Central

Bank's digital currency division (RAND, 2025), point to coordinated capacity-building directed from the center. RAND (2025) further documents the involvement of Rosatom and Rostec, entities at the core of Russia's defense-industrial complex, in crypto-enabled procurement and payment schemes.

4.3 How the oil trade works

The operational mechanics of Russia's crypto-based energy settlement were brought into public documentation by Reuters in March 2025 (Hirtenstein and Aizhu, 2025; Moscow Times, 2025), confirming a practice whose architectural logic had been circulating in financial intelligence channels for months. The structure is deliberately layered: a Chinese buyer transfers yuan into an offshore intermediary account, which converts the funds into cryptocurrency before routing them through successive wallets until they are reconverted into rubles within Russia. At no point does a Western bank, SWIFT message, or dollar transfer touch the transaction. The result is a settlement mechanism that is functionally equivalent to conventional energy trade finance while remaining structurally invisible to the enforcement architecture designed to interdict it.

The scale and timing of this arrangement carry analytical weight beyond the operational detail. Individual trader volumes with China reached tens of millions of dollars monthly (The Block, 2025), while Russia's aggregate crypto inflows between July 2024 and June 2025 reached $379 billion, a 48% year-on-year increase, with transfers exceeding $10 million surging by 86%, a pattern consistent with institutional trade activity rather than retail speculation (DL News, 2025). The expiration of OFAC General License 8L, which closed the last remaining legal channel for conventional Russian energy settlements, reinforces the inference that crypto adoption was partly demand-driven by the progressive closure of alternatives.

Crypto remains one instrument among several rather than a wholesale replacement for conventional settlement. The Central Bank's own acknowledgment that the experimental regime was not developing as rapidly as anticipated in corridors where traditional methods remained available (Interfax, 2026) underscores its supplementary character.

4.4 The infrastructure underneath: A7A5 and the Garantex network

The crypto-oil settlement mechanism is best understood as the visible layer of a more extensive parallel financial infrastructure: a purpose-built stablecoin operating as the settlement core, and a resilient exchange network providing the conversion and liquidity functions that make the system operational.

The stablecoin dimension is anchored by A7A5, a ruble-pegged token issued by a Kyrgyz firm and it has processed $93.3 billion within its first twelve months. Chainalysis has described it

as a purpose-built settlement rail for sanctioned actors (Chainalysis, 2026a). Its integration with an “Instant Swapper” conversion service, routing funds into mainstream stablecoins with minimal verification and already responsible for $2.2 billion in transfers at the time of reporting (OFAC, 2025; Chainalysis, 2026a), illustrates how the architecture is engineered to dissolve the evidentiary trail at the point where it would otherwise become traceable.

Garantex, the dominant exchange within this infrastructure, had processed $96 billion since 2019 and intermediated over 70% of crypto volumes involving sanctioned entities (TRM Labs, 2025). In March 2025, a multinational operation seized its domains and froze $26 million. The disruption lasted days, thanks to its successor, Grinex, which was created three months earlier. Customer account balances were migrated overnight, the A7A5 system was integrated, and business operations resumed without disruption. When OFAC sanctioned Grinex as well, new successors were already running across the UAE, Brazil, Thailand, and Hong Kong. Transparency International Russia documented the whole network operating through Telegram, with no crypto trace in Russian banking records (TI Russia, 2025; ICIJ, 2025), describing it as a “crypto hydra”. The EU's subsequent prohibition of all A7A5 transactions in its 19th sanctions package, the first instance of a specific cryptocurrency being banned under a sanctions regime (EU Council, 2025), reflects a regulatory acknowledgment of the architecture's systemic character.

4.5 What this means for companies

Russia's crypto infrastructure generates corporate exposure that operates below the threshold of conventional compliance controls. Because the architecture is designed so that each transactional step appears legitimate in isolation, liability under IEEPA attaches regardless of intent, and a commodity trader unknowingly touching the crypto-oil chain bears the same legal exposure as one acting deliberately (Wright, 2023). The same logic extends across sectors: TI Russia's undercover investigation documented the Exved network facilitating the purchase of microprocessors and telecommunications equipment from China and Taiwan for Russian importers through crypto-funded channels (TI Russia, 2025), while successor exchange networks were found exploiting compliance gaps at Bank of China, DBS, JP Morgan, and Deutsche Bank institutions in Hong Kong. In shipping, the convergence of the shadow fleet with crypto payment infrastructure, addressed jointly in the EU's 19th sanctions package (EU Council, 2025), further illustrates how exposure cuts across operational and financial dimensions simultaneously. The common thread is that sanctioned character becomes visible only at the level of the full chain, never at any single link within it.

5. Iran's Mining-Based Sanctions Evasion Strategy: A Case Study Analysis

In recent years, Iran has faced growing economic and political strain, driven by a combination of domestic instability and external pressure. These conditions have significantly weakened the national economy, contributing to a sharp decline in the value of the rial, losing around 90% of its value since 2018, alongside persistently high inflation rates ranging between 40% and 50%. According to Chainalysis, a blockchain analytics firm whose on-chain tracking data is used operationally by the U.S. Department of Justice and OFAC, these macroeconomic pressures have directly accelerated the adoption of cryptocurrency as an alternative financial channel in Iran *(*Chainalysis, 2025b*)*. Within this fragile environment, cryptocurrencies have taken on an increasingly important role, offering both an alternative channel for financial transactions under sanctions and a means for individuals to safeguard their assets in a volatile system (Boltuc, 2025).

The expansion of crypto usage in Iran, however, is not confined to private citizens. State-affiliated actors, most notably the Islamic Revolutionary Guard Corps (IRGC), have incorporated digital assets into their financial strategies, using them to support operations within the country and across regional networks (Chainalysis, 2026b).

5.1 Mining Regulations and Underground Economy

Iran's growing interest in cryptocurrencies dates to 2017, when international sanctions significantly restricted the country's access to global financial systems. Iran officially legalized cryptocurrency mining in 2019, recognizing that its surplus of oil and natural gas made Bitcoin mining an attractive opportunity for a sanctions-hit economy. The regulatory framework was designed to capture revenue while preserving state control. Miners were required to register, pay elevated electricity tariffs, and sell their digital assets directly to Iran's Central Bank (Boltuc, 2025). The high energy tariffs created an unstable financial environment for mining and pushed many to abandon legal operations for underground, unlicensed mining. Meanwhile, many operations linked to Iran's Islamic Revolutionary Guard Corps (IRGC) reportedly use electricity for free. The government has periodically attempted to rein in illegal mining, but the structural incentives sustaining the underground economy have proven more powerful than enforcement capacity (Boltuc, 2025).

The legalization attracted significant inward investments. According to Elliptic, a blockchain intelligence firm specializing in sanctions compliance, Chinese investors, leaders in this sector, established licensed operations, with at least one large facility in the Rafsanjan Special Economic Zone (Elliptic, 2021). Iran's global share of Bitcoin hash rate reached approximately 4.5% in 2021, though it declined to around 3.1% by 2024 as energy constraints and post-halving economics weighed on profitability (Elliptic, 2021; Chainalysis, 2025b).

5.2 The Central Bank with Blockchain Infrastructure and Stablecoin Strategy

The Central Bank of Iran (CBI) has assumed a crucial role in shaping the country's cryptocurrency ecosystem. Beyond mandating that licensed miners sell mined Bitcoin to the state, the CBI has developed domestic blockchain infrastructure as part of a broader strategy to operate outside dollar-denominated financial rails. Notable initiatives are the Borna blockchain platform, developed in partnership with Iranian firm Areatak, and the Kuknos Network, both designed to create a sovereign digital financial framework.

Stablecoins, particularly USDT (Tether), have become the CBI's preferred instrument for international settlement. Pegged to the dollar but transferable outside SWIFT, USDT enables Iran to conduct cross-border payments, accumulate dollar-equivalent reserves, and intervene in the rial's exchange rate without touching the US banking system (The Guardian, 2026). The CBI's stablecoin strategy was exposed in late 2025, when leaked documents posted by financier Babak Morteza Zanjani revealed that the Central Bank was using a broker to purchase stablecoins from currency deposits (Chainalysis, 2026b, 2026c)

5.3 The Dominant Force of the IRGC

The Islamic Revolutionary Guard Corps is not merely a military organization, it is a vertically integrated economic conglomerate with controlling interests across construction, logistics, telecommunications, energy, and now cryptocurrency. Its entry into crypto began as opportunistic evasion and has evolved into institutionalised financial infrastructure. In Q4 2025, IRGC-linked addresses accounted for over 50% of all value received by Iranian crypto entities, with more than $3 billion moved across the year to support regional militia networks, facilitate sanctioned oil sales, and procure dual-use military components (Chainalysis, 2026b).

The IRGC uses cryptocurrencies for strategic purposes. They facilitate proxy financing, enabling funds to be transferred directly to allied militia groups without relying on traditional banking systems. Second, cryptocurrencies are used for oil revenue conversion, allowing proceeds from illicit oil sales, often routed through front companies, to be transformed into digital assets and reintegrated into the financial system. Third, crypto funds support dual-use procurement, financing the acquisition of restricted technologies, weapons components, and military equipment (Asia Times, 2026).

5.4 Corporate Exposure

For multinational firms, the Iranian case presents a qualitatively different risk profile. Iran's evasion architecture is deliberately opaque, operating through layered intermediaries across multiple jurisdictions rather than through named legislative infrastructure. The sectors most

exposed to indirect facilitation risk are energy and petrochemicals, financial services and international logistics providers (Asia Times, 2026).

According to FinCEN, the U.S. Financial Crimes Enforcement Network, a bureau of the Treasury Department, Iranian shadow banking networks spanning the UAE, Hong Kong, Singapore, and Turkey, transacted approximately $4 billion through front oil companies alone, while technology procurement networks linked to Iran engaged in a further $413 million in transactions involving export-controlled goods (FinCEN, 2025). This is further corroborated by OFAC's own press releases, confirming that in 2025, OFAC sanctioned more than 875 persons, vessels, and aircraft tied to Iranian sanctions evasion, a figure that underlines both the scale of the enforcement campaign and the breadth of the commercial ecosystem it targets (Chainalysis, 2026a).

The Russia and Iran cases, while structurally different, converge on a common implication for multinational firms: sanctions risk is no longer confined to identifiable counterparties or regulated channels. The following section draws these threads together into a unified corporate risk framework.

6. Corporate Exposure and Risk Landscape

The Russia and Iran cases highlight a broader structural shift: the emergence of crypto-enabled financial networks that operate alongside, and at times outside, traditional regulatory frameworks. For multinational corporations, the resulting risk is less about direct interaction with sanctioned entities and more about indirect exposure embedded within complex transaction ecosystems.

6.1 Compliance and secondary sanctions: expanding the liability perimeter

Crypto-based settlement mechanisms weaken the effectiveness of traditional compliance controls by reducing reliance on regulated financial intermediaries. As a result, transactions can be executed across multiple layers without clear visibility on counterparties or beneficiaries.

For corporates, this fundamentally expands the perimeter of liability. Exposure extends beyond direct counterparties to multi-step transaction chains. Sources of funds and ultimate beneficiaries may be obscured at the point of transaction. Compliance risk therefore shifts from a counterparty-screening exercise to a network exposure challenge, where firms must assess not only with whom they transact, but how transactions are structured end-to-end.

6.2 Proxy and indirect facilitation: systemic intermediary risk

Sanctions-affected systems increasingly rely on distributed intermediary networks, including trading companies, brokers, and offshore financial actors to facilitate transactions and obscure links to sanctioned entities. These intermediaries often operate within legitimate global markets, creating structural overlap between compliant and non-compliant flows.

For corporations, this generates three systemic risks. Shared intermediaries blur the line between compliant and sanctioned flows. Operational partners may enable restricted transactions without full visibility. And sanctions risk can materialize retroactively following new designations. Risk is therefore no longer confined to individual counterparties but embedded within interconnected commercial ecosystems.

6.3 Payment infrastructure fragmentation: treasury implications

The rise of alternative payment rails, including crypto assets, stablecoins, and non-Western financial infrastructures, is contributing to a fragmentation of global settlement systems. For corporate treasury functions, this creates a more complex operating environment. Multi-rail systems operate with divergent regulatory standards and transparency levels. Liquidity complexity increases, particularly where digital assets intersect with traditional balance sheets. And auditability is reduced, as certain transaction flows fall outside established

reporting frameworks. These alternative rails are not full substitutes for traditional systems but are increasingly used in specific corridors where conventional channels are constrained or high-risk.

6.4 Supply chain vulnerabilities: financial opacity meets dual-use trade

The convergence of crypto-based payments and global supply chains introduces heightened risk in sectors involving dual-use goods and sensitive technologies. Financial opacity can decouple the link between buyer, payer, and end-user, making it more difficult to verify the ultimate destination and use of goods.

This creates exposure across multiple points in the value chain: suppliers engaging with indirectly financed distributors, limited visibility over end-use and end-user compliance, and elevated exposure to export control violations, particularly in technology-intensive sectors. As a result, supply chain risk becomes increasingly financially mediated, rather than solely operational or geographic.

6.5 Implications for corporate risk management

Across these dimensions, the core shift is from linear to networked risk structures. Traditional compliance models, built on identifiable counterparties and regulated financial channels, are increasingly insufficient in an environment characterized by fragmentation, intermediation, and partial opacity.

Leading firms are beginning to adapt by extending due diligence from counterparties to transaction pathways, integrating crypto-related exposure into financial risk and treasury frameworks, and enhancing supply chain controls with greater visibility into financial as well as physical flows. In this context, the primary challenge is not deliberate non-compliance, but inadvertent exposure to systems designed to obscure the link between transactions and sanctioned actors.

The corporate risks outlined above do not exist in a regulatory vacuum. The following section examines how enforcement authorities are responding, where the gaps remain, and what trajectory the regulatory landscape is likely to follow.

7. Regulatory and Enforcement Outlook

Using cryptocurrency to evade sanctions has moved firmly into the center of regulatory concern. In the United States and Europe, regulators now apply the same rules to digital asset activity as any other financial activity. The harder problem is institutional. Sanctions were designed to identify and block persons, entities, and accounts, whereas contemporary evasion often operates through adaptive networks of successor exchanges, OTC brokers, self-hosted wallets, mule accounts, and third-country settlement channels. For multinational firms, the implication is that exposure is increasingly indirect and embedded in payment, trade, and treasury relationships rather than in obvious dealings with a listed crypto intermediary (OFAC, 2021; U.S. Department of the Treasury, 2022a; FATF, 2025a).

7.1 The Regulatory Architecture

Different jurisdictions are broadly moving in the same direction, though each through its own legal framework. OFAC said that sanctions apply to digital currency just as they do to cash, and Treasury has since moved from guidance to direct enforcement action against exchanges and services including Garantex, Tornado Cash, and Sinbad. FinCEN has reinforced this approach by proposing rules that treat deliberately obscured transaction structures as a systemic risk (OFAC, 2021; U.S. Department of the Treasury, 2022a, 2022b, 2023a, 2023b; FinCEN, 2023). In the EU, MiCA regulation provides the main supervisory framework for crypto markets, while a transfer-of-funds regulation and EBA guidance extend sanctions obligation to all crypto-asset service providers. ESMA has consequently stressed that no such providers should be considered low-risk for supervisory purposes (Council of the European Union, 2023; EBA, 2024a, 2024b; ESMA, 2026a, 2026b). Globally, FATF sets the standard through its rules on virtual assets and the Travel Rule, though its own 2024 and 2025 reviews acknowledge that implementation remains patchy across many jurisdictions (FATF, 2024; FATF, 2025a).

7.2 The Enforcement Gap

The core enforcement gap is therefore not a lack of legal authority but a mismatch between list-based enforcement and networked evasion. RUSI's 2025 roundtable report says that after an address or entity is designated, analytics tools may update and generate retrospective alerts, but there is often a lack of capacity to detect subsequent infrastructure changes. Three Garantex addresses were initially on the sanctions list, and the exchange continued operating for three years after designation, shifting through shell companies and new addresses until the disruption. In other words, the designation flagged the problem but did not dismantle the network behind it (RUSI, 2025; U.S. Department of Justice, 2025; U.S. Department of Treasury, 2025b). Transparency International Russia in Exile documents brokers willing to

swap cash rubles into the stablecoin USDT and move funds offshore, alongside markets for verified accounts and business entities that can be used to bypass customer due diligence. The critique is thus that crypto-based sanctions evasion depends on shell structures, nominee accounts, informal brokers, and poor beneficial-ownership visibility, not merely on blockchain pseudonymity (Transparency International Russia in Exile, 2023a, 2023b, 2024).

7.3 Evaluating Reform Proposals

Wright's (2023) three proposals expose exactly where current governance is thin. Her first proposal, a global KYC baseline that preserves pseudonymity vis-a-vis the public while making identity available to competent authorities, is broadly consistent with the direction of FATF and the EU. Yet as a universal solution it is politically and operationally unrealistic. FATF still reports wide implementation gaps, self-hosted wallets remain difficult to fold into ordinary customer-identification models, and a heavily centralised identity architecture would intensify privacy and civil-liberties objections (Wright, 2023; FATF, 2024; FATF, 2025a). Her second proposal is an internationally coordinated public-key directory. Rather than a universal identity ledger, the more feasible path is a dynamic, evidence-based registry or API for newly attributed sanctions-linked addresses and related entities. That is close to what RUSI participants recommended in 2025, while also warning that defective attribution could shift liability or create false confidence. Wright's third proposal, suggests the use of ethical hackers, which is best understood as a complementary cyber-resilience tool. It may help identify vulnerabilities and improve recovery readiness, but it cannot substitute for sanctions supervision as it does not solve the fundamental compliance failures (Wright, 2023; RUSI, 2025).

7.4 Private Analytics as Enforcement Infrastructure

In the current system blockchain analytics firms have become enforcement infrastructure. FATF explicitly acknowledges private analytics providers, and RUSI describes how such firms help attribute addresses, update risk tools after designations, and generate alerts that shape VASP reporting and law-enforcement follow-up. In practice, companies such as Chainalysis, TRM Labs, and Elliptic increasingly mediate how firms identify indirect exposure, including cross-chain and stablecoin-linked risks (FATF, 2025a; RUSI, 2025; Chainalysis, 2026b; TRM Labs, 2026; Elliptic, 2026). Yet this infrastructure raises governance questions. Attribution is probabilistic, coverage is uneven where mixers, bridges, OTC brokers, or unhosted wallets dominate, and proprietary methodologies concentrate substantial epistemic power in private vendors. More broadly, accountability in blockchain systems is inherently trade-off laden, and end users are often consumers rather than producers of accountability (Nabben and De Filippi, 2024). Regulators are moving toward greater traceability and data sharing, but the authorities

remain legally vulnerable when sanctions touch open-source infrastructure rather than clearly bounded intermediaries (U.S. Department of the Treasury, 2022b, 2025a).

7.5 The Trajectory Ahead

In the future, four trends will likely define the coming years. More actions against OTC brokers, successor exchanges, and stablecoin-linked settlement rails. Public authorities and private analytics firms will share intelligence more systematically. Greater scrutiny of indirect and pre-designation exposure and continued regulatory arbitrage through under-resourced jurisdictions. For multinationals, that means sanctions compliance must move beyond list screening toward network-sensitive due diligence across counterparties, payment routes, treasury operations, and third-country intermediaries (Massad, 2019; U.S. Department of the Treasury, 2025b; RUSI, 2025).

8. Strategic Scenarios and Corporate Recommendations

To move beyond tactical, country-specific evasion methods, the future intersection of sanctions, digital assets, and corporate risk is best understood through a structural model. The strategic environment facing multinational firms depends on the interaction of two conditions: the degree of fragmentation of the international monetary system and the degree of fragmentation of global governance over sanctions, compliance, and financial regulation. Monetary fragmentation refers to the extent to which cross-border settlement remains concentrated in dollar-centered, bank-intermediated channels or disperses across regional payment systems, local-currency arrangements, stablecoins, and other digital rails. Governance fragmentation refers to whether sanctions enforcement and supervisory expectations remain relatively coordinated across major jurisdictions or become increasingly uneven, contested, and politically differentiated. Framed in this way, the issue is not whether crypto replaces traditional finance. It does not. The more plausible development is hybridization: sanctioned and high-risk actors combine conventional and crypto-based infrastructures to route value around the central nodes on which sanctions historically depend. The weakening of sanctions effectiveness should therefore be understood less as technological substitution than as a problem of changing network architecture (Farrell & Newman, 2019; FATF, 2024; GAO, 2024; Kim et al., 2024).

Table 1:

Variable	Definition	Low value	High value
Monetary fragmentation	Degree to which cross-border settlement disperses away from dollar-centered, bank-intermediated channels into regional payment systems, local-currency arrangements, stablecoins, and crypto-adjacent rails	Cross-border payments remain concentrated in traditional banking, correspondent networks, and dollar-based settlement	Cross-border payments are spread across multiple parallel rails with uneven transparency and interoperability
Governance fragmentation	Degree to which sanctions enforcement, financial regulation, and compliance expectations remain coordinated across major authorities	Sanctions governance remains relatively convergent across major regulators and market gatekeepers	Sanctions governance becomes uneven, contested, and jurisdictionally differentiated, creating rival or partially incompatible compliance spaces

Source: Author's framework based on Farrell and Newman (2019), FATF (2024), GAO (2024), IMF (2024), OFAC (2021, 2022), U.S. Department of the Treasury (2023), and Regulation (EU) 2023/1114 (2023).

8.1 Scenario One: Reinforced Hierarchy

Where both forms of fragmentation remain limited, the likely outcome is reinforced hierarchy**.** In that world, the traditional financial core continues to dominate and the principal sanctioning jurisdictions converge around common expectations for traceability, compliance, and secondary-sanctions enforcement. Crypto does not disappear, but it is progressively pulled back into a denser supervisory framework. OFAC guidance, FATF standards, EU supervisory rules under MiCA, and the growing use of blockchain analytics together point toward a tighter regulatory ecology around virtual-asset exposure (FATF, 2024; OFAC, 2021, 2022; Regulation (EU) 2023/1114, 2023). This is the scenario in which sanctions governance most closely resembles the classic model of financial coercion updated for a digitizing system: power still flows from control over central nodes, but regulators become more capable of monitoring hybrid payment pathways that pass partly outside traditional banking channels.

For multinational firms, reinforced hierarchy would not reduce risk. It would make risk more data-intensive, more retrospective, and less forgiving. Exposure would increasingly arise through brokers, freight forwarders, offshore distributors, OTC facilitators, non-bank payment processors, and treasury arrangements involving stablecoins or virtual-asset service providers. The central compliance challenge would be the widening gap between traditional list-based screening and the networked character of contemporary evasion. A firm may avoid direct dealings with a designated party yet still facilitate a prohibited transaction through a high-risk chain of intermediaries. In such an environment, compliance failure becomes less a matter of missing a name on a sanctions list and more a matter of failing to understand transaction architecture end to end (GAO, 2024; OFAC, 2021, 2022).

8.2 Scenario Two: Managed Multipolarity

A different dynamic appears once monetary fragmentation increases while governance fragmentation remains comparatively low. That produces managed multipolarity. Here the international system becomes more plural in its payment infrastructures, yet leading regulators still preserve a meaningful degree of coordination. Alternative rails proliferate because they are useful, politically attractive, and in some corridors faster or more resilient than legacy banking channels, but they do not fully displace conventional finance. Instead, multinational firms confront a layered settlement environment in which traditional banking coexists with regional mechanisms, local-currency arrangements, and selective crypto use. IMF analysis suggests that digital money may alter cross-border payments and reserve dynamics, while FATF materials show how uneven implementation can still coexist with partial regulatory convergence (FATF, 2024; Kim et al., 2024).

The defining feature of this scenario is path dependency. Once states and firms have invested in alternative infrastructures under sanctions pressure, those infrastructures are unlikely to disappear simply because tensions ease or selected sanctions are relaxed. Hybridization persists because it serves strategic and commercial purposes beyond sanctions evasion alone. For firms, legal permissibility and operational normality therefore diverge. A transaction may again be lawful, while the surrounding payment environment remains dependent on the intermediary structures, workarounds, and data asymmetries built during the sanctions period. The managerial challenge in this setting is not simple de-risking, but operating across mixed payment ecologies without assuming a return to pre-sanctions normality. Treasury, compliance, and strategy teams must distinguish between the formal reopening of a corridor and the actual governance quality of that corridor (Farrell & Newman, 2019; Kim et al., 2024).

8.3 Scenario Three: Systemic Bifurcation

The most severe friction emerges when both monetary fragmentation and governance fragmentation become high, pushing the system toward systemic bifurcation**.** This does not imply the disappearance of the dollar. The more plausible outcome is the consolidation of partially rival monetary and regulatory spaces: parallel settlement infrastructures, different transparency standards, competing compliance expectations, and diverging notions of legitimate financial governance. Crypto-related rails matter here not in isolation, but as one component of a broader process of geo-financial decoupling. Stablecoins, regional payment systems, state-linked alternatives, OTC broker networks, and non-Western settlement channels all contribute to reducing dependence on the nodes through which sanctions have historically operated (Farrell & Newman, 2019; FATF, 2024; Kim et al., 2024).

For multinational firms, systemic bifurcation transforms sanctions risk from a specialist legal issue into a problem of corporate strategy and organizational design. The question is no longer only whether a transaction is permitted, but under which monetary-governance ecology the transaction takes place. Treasury architecture, legal entity structure, ERP systems, liquidity buffers, banking relationships, procurement protocols, and market-entry decisions all become conditioned by fragmentation at the level of both money and governance. This is also the scenario in which the limits of current enforcement become most visible. As the previous section argued, sanctions systems are still built largely around identifying and blocking persons, entities, and accounts, whereas crypto-enabled evasion increasingly operates through adaptive networks of successor exchanges, OTC brokers, mixers, mule accounts, self-hosted wallets, and third-country intermediaries. The more fragmented the monetary system becomes, the sharper this mismatch grows between list-

based enforcement and networked evasion (GAO, 2024; Royal United Services Institute [RUSI], 2025; U.S. Department of the Treasury, 2023).

One additional scenario deserves brief mention. A situation of low monetary fragmentation but high governance fragmentation would describe contested centralization: political disagreement rises faster than infrastructural diversification. This is better understood as a transitional condition than as a stable equilibrium. If governance becomes more contested while the payment system remains centralized, affected actors have strong incentives to build or deepen alternative rails, pushing the system over time toward managed multipolarity or systemic bifurcation. In theoretical terms, this follows directly from the logic of weaponized interdependence: once chokepoints are used coercively, actors have reasons to invest in escape routes from those chokepoints (Farrell & Newman, 2019).

Table 2:

	Low governance fragmentation	**High governance fragmentation**
Low monetary fragmentation	Scenario 1: Reinforced Hierarchy. A still-centralized monetary order combined with coordinated enforcement and dense supervisory reach.	Transitional case: Contested Centralization. Political disagreement rises, but the underlying payment system remains largely centralized. Usually unstable over time.
High monetary fragmentation	Scenario 2: Managed Multipolarity. Alternative payment rails persist and expand, but major regulators retain partial coordination and shared compliance expectations.	Scenario 3: Systemic Bifurcation. Parallel payment ecosystems and fragmented governance produce partially rival monetary-regulatory spaces.

Source: Author's framework based on Farrell and Newman (2019), FATF (2024), GAO (2024), IMF (2024), OFAC (2021, 2022), U.S. Department of the Treasury (2023), and Regulation (EU) 2023/1114 (2023).

8.4 Corporate Recommendations

The corporate response to these scenarios should begin with a redesign of sanctions compliance around network visibility rather than formal counterparties alone. Enhanced due diligence needs to extend routinely to beneficial ownership, intermediary chains, payment-route design, wallet exposure where relevant, and the role of third-country service providers. That is particularly important because the growing use of blockchain analytics does not eliminate uncertainty; it redistributes it. Private analytics firms increasingly function as quasi-enforcement infrastructure by supplying address attribution, transaction alerts, and risk signals, yet attribution remains probabilistic and coverage is uneven where OTC brokers, mixers, bridges, or self-hosted wallets dominate (FATF, 2024; RUSI, 2025). Corporate compliance therefore cannot be outsourced to a vendor dashboard. It has to be

embedded in internal judgment, escalation procedures, and corridor-specific commercial intelligence.

Alongside that shift, treasury and trade-finance teams should conduct corridor-level payment-channel assessments covering convertibility, transparency, freezing risk, reliance on fragile banking relationships, potential stablecoin exposure, and fallback options if a bank, exchange, or intermediary is designated. Static screening is no longer sufficient. Firms need transaction-pattern monitoring capable of flagging unexplained stablecoin settlement, abrupt fiat-to-crypto conversion, sudden shifts in settlement geography, or newly inserted intermediaries. Procurement and logistics functions should likewise move from tier-one screening to transaction-chain mapping, especially in sectors exposed to dual-use goods, energy trading, commodities, advanced manufacturing, and shipping. The broader point is that liability increasingly attaches not only to who the firm deals with, but to how value moves through the chain.

These operational adjustments require governance changes inside the firm. Internal escalation protocols should connect legal, compliance, finance, treasury, procurement, logistics, and corporate strategy, with regular board-level review of high-risk geographies and business lines. Scenario planning should not be treated as an abstract compliance exercise, but as part of the corporate operating model. Firms need to test not only enforcement shocks, but also the persistence of hybrid payment systems after partial normalization and the organizational implications of deeper monetary-governance bifurcation (FATF, 2024; OFAC, 2021; Regulation (EU) 2023/1114, 2023; U.S. Department of the Treasury, 2023).

Ultimately, crypto-related sanctions risk is best understood as a manifestation of a broader structural transformation in the political economy of international business. What matters is not simply the existence of digital assets, but the interaction between the fragmentation of money and the fragmentation of governance. As those two conditions intensify, the relevant corporate question is no longer only whether a transaction is formally permissible, but whether the firm possesses the institutional capacity to operate across a more plural, contested, and strategically differentiated financial order (Farrell & Newman, 2019; FATF, 2024; GAO, 2024; Kim et al., 2024).

Table 3:

Scenario	Structural logic	Main corporate risk	Strategic corporate response
Reinforced Hierarchy	Traditional financial core remains dominant; governance remains coordinated	Retrospective enforcement, secondary-sanctions exposure, indirect facilitation through intermediaries, reliance on imperfect attribution tools	Upgrade from list-screening to network-sensitive compliance; strengthen transaction monitoring, beneficial-ownership analysis, and intermediary due diligence
Managed Multipolarity	Payment infrastructures diversify, but governance remains partly coordinated	Hybrid settlement risk, uneven auditability, persistence of sanctions-era workarounds, false assumptions of normalization	Build corridor-by-corridor payment assessments; distinguish legal permissibility from operational normality; monitor persistent alternative rails
Systemic Bifurcation	Monetary and governance fragmentation reinforce each other	Strategic exposure across treasury, entity structure, procurement, banking, liquidity management, and market access	Integrate sanctions risk into corporate strategy, treasury design, subsidiary structure, ERP architecture, and board oversight
Contested Centralization	Governance fragments faster than payment infrastructure	Regulatory uncertainty within still-centralized channels	Treat as a transition signal and prepare for migration toward Scenarios 2 or 3

Source: Author's framework based on Farrell and Newman (2019), FATF (2024), GAO (2024), IMF (2024), OFAC (2021, 2022), U.S. Department of the Treasury (2023), and Regulation (EU) 2023/1114 (2023).

9. Conclusion

The evolution of crypto-enabled financial networks marks a structural shift in the global risk environment. What was once a peripheral compliance issue is rapidly becoming a core strategic consideration, reshaping how value is transferred, obscured, and controlled across borders.

Three findings deserve emphasis. First, crypto-based sanctions evasion has ceased to be opportunistic. In Russia, the state legislated for it, built the banking infrastructure, and deployed a purpose-built stablecoin that processed $93 billion in under twelve months. In Iran, the IRGC alone moved over $3 billion through crypto channels in a single year, while the Central Bank quietly constructed a stablecoin-based reserve management strategy. Second, enforcement, while advancing rapidly in the United States and Europe, faces a structural mismatch: list-based designation cannot keep pace with networks that regenerate across jurisdictions within days. The Garantex-Grinex-Exved succession, described by investigators as a “crypto hydra,” illustrates the limits of current tools. Third, the corporate risk frontier has moved. Liability now attaches not to who a firm transacts with, but to how value moves through the chain, a shift that demands network-level visibility rather than counterparty-level screening.

Accordingly, Russian oil being settled in Bitcoin without a single dollar changing hands is no longer an isolated event. It is the visible surface of an infrastructure this analysis has mapped in detail: state-supervised legal frameworks, purpose-built stablecoins, successor exchange networks that regenerate faster than regulators can designate them, and a parallel financial architecture that its users say they would retain even if sanctions were lifted.

Ultimately, the strategic significance of crypto-related sanctions risk lies not in the existence of digital assets alone, but in the wider fragmentation of money, governance, and enforcement across the international system. As shown, multinational firms may face very different operating conditions depending on whether the emerging order tends toward reinforced hierarchy, managed multipolarity, or systemic bifurcation. In all three cases, however, the central corporate challenge is the same: sanctions risk can no longer be managed through narrow list-based screening or isolated legal review. It now requires visibility across transaction architectures, payment corridors, intermediary chains, and governance environments. Firms that respond by redesigning compliance around network exposure, strengthening corridor-level treasury assessment, integrating procurement and logistics into sanctions oversight, and embedding scenario planning into board-level decision-making will be better positioned to preserve resilience, market access, and strategic flexibility. Firms that fail to make these adjustments risk not only regulatory breaches, but a deeper loss of operational control in a more plural, contested, and politically differentiated financial order.

References

ASIA TIMES. (2026). "Iran drives $104 billion surge in sanctions-busting crypto flows". *Asia Times.* DOI: https://asiatimes.com/2026/03/iran-drives-104b-surge-in-sanctions-busting-crypto-flows/

AUER, R., CORNELLI, G., and FROST, J. (2022). "Rise of central bank digital currencies". *BIS Working Papers,* No. 1004. Bank for International Settlements.

BAFFI-MINTS. (2022). "Cryptocurrencies: a way to evade sanctions?". *BAFFI-MINTS Newsletter,* Issue 0. Bocconi University. DOI: https://baffi.unibocconi.eu/research-units/mints-alternative-monies/newsletter/issue-0/cryptocurrencies-way-evade-sanctions

BOLTUC, S. (2025). "Crypto under control: The geopolitical drivers of Iran's new regulation". *SpecialEurasia.* DOI: https://www.specialeurasia.com/2025/02/05/crypto-iran-geopolitics/

BRYANSKI, G. (2024). "Russia to allow crypto payments in international trade to counter sanctions". *Reuters.* DOI: https://www.reuters.com/technology/russia-launch-international-payments-crypto-before-end-2024-2024-07-30/

CHAINALYSIS. (2025a). "OFAC sanctions Iranian shadow crypto banking network". *Chainalysis.* DOI: https://www.chainalysis.com/blog/ofac-sanctions-iranian-shadow-crypto-banking-network-september-2025/

CHAINALYSIS. (2025b). "Crypto crime and sanctions 2025". *Chainalysis.* DOI: https://www.chainalysis.com/blog/crypto-crime-sanctions-2025/

CHAINALYSIS. (2026a). "Crypto Crime Report Introduction". *Chainalysis.* DOI: https://www.chainalysis.com/blog/2026-crypto-crime-report-introduction/

CHAINALYSIS. (2026b). "Crypto sanctions 2026: Iran's $3 billion+ proxy network". *Chainalysis.* DOI: https://www.chainalysis.com/blog/crypto-sanctions-2026/

CHAINALYSIS. (2026c). "Iranian crypto activity amid geopolitical tensions 2026". *Chainalysis.* DOI: https://www.chainalysis.com/blog/iranian-crypto-activity-geopolitical-tensions-2026/

CNBC. (2024). "Russia legalizes cryptocurrency mining amid push for non-dollar payments". *CNBC.* DOI: https://www.cnbc.com/2024/07/30/russia-legalizes-cryptocurrency-mining.html

COINDESK. (2026). "Iran conflict throws the regime's $7.8 billion crypto ecosystem and Bitcoin mining network into spotlight". *CoinDesk.* DOI: https://www.coindesk.com/business/2026/02/28/iran-conflict-throws-the-regime-s-usd7-8-billion-crypto-ecosystem-and-bitcoin-mining-network-into-spotlight

COUNCIL OF THE EUROPEAN UNION. (2023). "Digital finance: Agreement on European crypto-assets regulation (MiCA) and transfer of funds rules". *Consilium.* DOI: https://www.consilium.europa.eu/en/press/press-releases/2023/05/16/anti-money-laundering-council-adopts-rules-which-will-make-crypto-asset-transfers-traceable/

DL NEWS. (2025). "Russia received $379 billion in crypto inflows as sanctions push digital payments". *DL News.* DOI: *https://www.dlnews.com/articles/regulation/war-pushes-russians-toward-defi-study-shows/*

DREZNER, D. W. (2011). "Sanctions sometimes smart: Targeted sanctions in theory and practice". *International Studies Review,* vol. 13, pp. 96–108.

ELLIPTIC. (2026). "Elliptic's 2026 regulatory and policy outlook: Sanctions enforcement will intensify". *Elliptic.* DOI: https://www.elliptic.co/blog/elliptics-2026-regulatory-and-policy-outlook-sanctions-enforcement-will-intensify

ELLIPTIC. (2021). "How Iran uses Bitcoin mining to evade sanctions". *Elliptic.* DOI: https://www.elliptic.co/blog/how-iran-uses-bitcoin-mining-to-evade-sanctions

EU COUNCIL. (2025). "Council adopts 19th package of sanctions against Russia". *Council of the European Union.* DOI: https://www.consilium.europa.eu/en/press/press-releases/2025/10/23/19th-package-of-sanctions-against-russia-eu-targets-russian-energy-third-country-banks-and-crypto-providers/

EUROPEAN BANKING AUTHORITY (EBA). (2024a). "Guidelines on information accompanying transfers of funds and certain crypto-assets under Regulation (EU) 2023/1113". *European Banking Authority.* DOI: https://www.eba.europa.eu/publications-and-media/press-releases/eba-issues-travel-rule-guidance-tackle-money-laundering-and-terrorist-financing-transfers-funds-and

EUROPEAN BANKING AUTHORITY (EBA). (2024b). "Final report on guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures under Regulation (EU) 2023/1113". *European Banking Authority.* DOI: https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/anti-money-laundering-and-countering-financing-terrorism/guidelines-internal-policies-procedures-and-controls-ensure-implementation-union-and-national

EUROPEAN SECURITIES AND MARKETS AUTHORITY (ESMA). (2026a). "MiCA register". *ESMA.* DOI: https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica

EUROPEAN SECURITIES AND MARKETS AUTHORITY (ESMA). (2026b). "Supervisory briefing on authorisation of crypto-asset service providers under MiCA". *ESMA.* DOI:

https://www.esma.europa.eu/sites/default/files/2025-01/ESMA75-453128700-1263_Supervisory_Briefing_on_Authorisation_of_CASPs.pdf

FAGHIH, A., BARZEGARZADEH, A., and SAFAEI, M. (2025). "A Comparative Analysis of Legislative Criminal Policies in Iran and the United Kingdom in Addressing Cryptocurrency-Related Financial Crimes". *Legal Studies in Digital Age,* vol. 4, pp. 1–10.

FARRELL, H., and NEWMAN, A. L. (2019). "Weaponized interdependence: How global economic networks shape state coercion". *International Security,* vol. 44, pp. 42–79. DOI: 10.1162/ISEC_a_00351

FARRELL, H., and NEWMAN, A. L. (2022). "Underground Empire: How America Weaponized the World Economy". *Henry Holt and Company.*

FINANCIAL ACTION TASK FORCE (FATF). (2024). "Targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers". *FATF.* DOI: https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2024-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf

FINANCIAL ACTION TASK FORCE (FATF). (2025a). "Targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers". *FATF.* DOI: https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2025-Targeted-Upate-VA-VASPs.pdf.coredownload.pdf

FINANCIAL ACTION TASK FORCE. (2025b). "FATF updates standards on Recommendation 16 on payment transparency". *FATF.*

FINANCIAL CRIMES ENFORCEMENT NETWORK (FinCEN). (2023). "Notice of proposed rulemaking: Convertible virtual currency mixing as a class of transactions of primary money laundering concern". *FinCEN.gov.* DOI: https://www.fincen.gov/news/news-releases/fincen-proposes-new-regulation-enhance-transparency-convertible-virtual-currency

FINANCIAL CRIMES ENFORCEMENT NETWORK (FinCEN). (2025). "FinCEN identifies $9 billion in Iranian shadow banking activity". *FinCEN.* DOI: https://www.fincen.gov/news/news-releases/fincen-identifies-9-billion-iranian-shadow-banking-activity-2024.

HIRTENSTEIN, A., and AIZHU, C. (2025). "Russia leans on cryptocurrencies for oil trade, sources say". *Reuters.* DOI: https://www.reuters.com/business/energy/russia-leans-cryptocurrencies-oil-trade-sources-say-2025-03-14/

HODULA, M. (2025). "Retail crypto investors when facing financial constraints: Evidence from energy shocks and the use and downloads of crypto trading apps". *Energy Economics,* vol. 144, pp. 108338. DOI: https://doi.org/10.1016/j.eneco.2025.108338

ICIJ. (2025). "Garantex investigation: How a sanctioned crypto exchange kept operating". *International Consortium of Investigative Journalists.* DOI: https://www.icij.org/news/2025/09/cryptocurrency-exchange-garantex-lives-on-despite-sanctions-new-report-unveils/#:~:text=%E2%80%9COur%20findings%20show%20that%20Garantex,and%20Telegram%2Dbased%20workflows.%E2%80%9D

IMF. (2024). "Digital money and cross-border payments". *International Monetary Fund.*

INTERFAX. (2026). "Central Bank deputy governor on experimental crypto regime progress". *Interfax.*

KIM, S., MIKSJUK, A., SURYAKUMAR, N., TULADHAR, A., VELCULESCU, D., WU, Y., ZUNIGA, J., and HALLMARK, N. (2024). "Digital money, cross-border payments, international reserves, and the global financial safety net: Preliminary considerations". *IMF Notes,* No. 2024/001. International Monetary Fund. DOI: 10.5089/9798400253478.068

KUCHKAROV, T., MAMADIYAROV, Z., KHAKIMOV, Z., SABIROVA, O., MATMURODOV, K., RAIMBOYEVA, M., and UMAROVA, S. (2025). "Energy-Related Uncertainty and Crypto-Currency Environmental Attention: Time-Varying Perspective". *International Journal of Energy Economics and Policy,* vol. 15, pp. 614–626. DOI: https://doi.org/10.32479/ijeep.20784

MASSAD, T. G. (2019). "It's time to strengthen the regulation of crypto-assets". *Brookings Institution.* DOI: https://www.brookings.edu/articles/its-time-to-strengthen-the-regulation-of-crypto-assets/

MORE, D. (2025). "Bitcoin mining costs $1,300 in Iran, but a whopping $306,000 in Italy". *The Economic Times.* DOI: https://economictimes.indiatimes.com/news/international/us/bitcoin-mining-costs-1300-in-iran-but-a-whopping-306000-in-italy-heres-the-full-list/articleshow/123656866.cms

MOSCOW TIMES. (2025). "Russia turns to crypto for oil trade as sanctions bite". *The Moscow Times.* DOI: https://www.themoscowtimes.com/2025/03/14/russia-using-crypto-in-chinese-and-indian-oil-trade-reuters-a88370

NABBEN, K., and DE FILIPPI, P. (2024). "Accountability protocols? On-chain dynamics in blockchain governance". *Internet Policy Review,* vol. 13. DOI: https://policyreview.info/pdf/policyreview-2024-4-1807.pdf

OFAC. (2025). "Treasury targets Russian sanctions evasion infrastructure, redesignates Garantex, and identifies successor entities". *U.S. Department of the Treasury.* DOI: https://home.treasury.gov/news/press-releases/sb0225

OFFICE OF FOREIGN ASSETS CONTROL (OFAC). (2021). "Sanctions compliance guidance for the virtual currency industry". *U.S. Department of the Treasury.* DOI: https://ofac.treasury.gov/recent-actions/20211015

OFFICE OF FOREIGN ASSETS CONTROL. (2022). "Do the prohibitions of Executive Order 14024 and other Russia-related sanctions extend to virtual currency?". *U.S. Department of the Treasury.*

OFFICE OF FOREIGN ASSETS CONTROL. (2024a). "Russia-related designations". *U.S. Department of the Treasury.*

OFFICE OF FOREIGN ASSETS CONTROL. (2024b). "Russia-related designations; cyber-related designation". *U.S. Department of the Treasury.*

OFFICE OF FOREIGN ASSETS CONTROL. (2024c). "Russia-related designations; publication of Russia-related determination; issuance of Russia-related general licenses and frequently asked questions". *U.S. Department of the Treasury.*

POCHER, N. (2025). "Obfuscation and traceability". *Law, Governance and Technology Series,* pp. 95–134. DOI: https://doi.org/10.1007/978-3-031-94698-1_4

RAND. (2025). "Russia's use of crypto schemes". *RAND Europe.* DOI: https://www.rand.org/pubs/commentary/2025/08/russias-use-of-crypto-schemes.html

REGULATION (EU) 2023/1114 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937. (2023). *Official Journal of the European Union,* L 150, 40.

REINSCH, W. A., and PALAZZI, A. L. (2022). "Cryptocurrencies and U.S. sanctions evasion: Implications for Russia". *Center for Strategic and International Studies.* DOI: https://www.csis.org/analysis/cryptocurrencies-and-us-sanctions-evasion-implications-russia

ROYAL UNITED SERVICES INSTITUTE (RUSI). (2025). "Sanctions in the Virtual Asset Industry: SIFMANet Roundtable Report". *RUSI.* DOI: https://static.rusi.org/virtual-asset-sanctions-roundtable-conference-report-march-2025.pdf

SKINNER, C. P. (2023). "Coins, cross-border payments, and anti-money laundering law". *Harvard Journal on Legislation,* vol. 60, pp. 285.

SONMEZ, O. (2025). "Iran's USDT and Stablecoin-Based Sanctions Evasion: An Empirical Analysis of Digital Dollar Exploitation for International Trade Finance". *SSRN,* No. 6362678.

SPECIALEURASIA. (2025). "Crypto and Iran: Geopolitics of digital finance". *SpecialEurasia.*

THE BLOCK. (2025). "Russian oil companies settling trades with China using Bitcoin and USDT". *The Block.*

THE GUARDIAN. (2026). "Iran central bank cryptocurrency Tether". *The Guardian.* DOI: https://www.theguardian.com/world/2026/jan/21/iran-central-bank-cryptocurrency-tether-nigel-farage

TI RUSSIA. (2025). "Crypto Laundromat". *Transparency International Russia in Exile.* DOI: https://cryptolaundromat.ti-russia.org/

TRANSPARENCY INTERNATIONAL RUSSIA IN EXILE. (2023a). "From Moscow-City with Crypto". *Transparency International Russia in Exile.* DOI: https://ti-russia.org/en/wp-content/uploads/sites/2/2025/09/from_moscow_city_with_crypto.pdf

TRANSPARENCY INTERNATIONAL RUSSIA IN EXILE. (2023b). "Money mule accounts for sale: The black market behind crypto-to-fiat conversion". *Transparency International Russia in Exile.* DOI: https://ti-russia.org/en/2023/10/31/ti-russia-presents-its-study-of-the-market-of-crypto-to-fiat-money-mules/

TRANSPARENCY INTERNATIONAL RUSSIA IN EXILE. (2024). "Unraveling the Web". *Transparency International Russia in Exile.* DOI: https://ti-russia.org/en/2024/08/09/unraveling-the-web/

TRM LABS. (2025). "Garantex network analysis: $96 billion in processed volume". *TRM Labs.*

TRM LABS. (2026). "2026 Crypto Crime Report Key Insights: TRM identifies record USD 158 billion in illicit crypto flows in 2025, reversing a multi-year decline". *TRM Labs.* DOI: https://www.trmlabs.com/resources/blog/2026-crypto-crime-report-key-insights-trm-identifies-record-usd-158-billion-in-illicit-crypto-flows-in-2025-reversing-a-multi-year-decline

TSENTSURA, K. (2025). "Crypto Under Sanctions: How restricted nations are adopting Bitcoin and stablecoins". *Yellow.com.* DOI: https://yellow.com/research/crypto-under-sanctions-how-restricted-nations-are-adopting-bitcoin-and-stablecoins

U.S. DEPARTMENT OF JUSTICE. (2025). "Garantex cryptocurrency exchange disrupted in international operation". *Department of Justice.* DOI: https://www.justice.gov/opa/pr/garantex-cryptocurrency-exchange-disrupted-international-operation

U.S. DEPARTMENT OF THE TREASURY. (2022a). "Treasury sanctions Russia-based Hydra, world's largest darknet market, and ransomware-enabling virtual currency exchange Garantex". *U.S. Department of the Treasury.* DOI: https://home.treasury.gov/news/press-releases/jy0701

U.S. DEPARTMENT OF THE TREASURY. (2022b). "U.S. Treasury sanctions notorious virtual currency mixer Tornado Cash". *U.S. Department of the Treasury.* DOI: https://home.treasury.gov/news/press-releases/jy0916

U.S. DEPARTMENT OF THE TREASURY. (2023a). "Illicit Finance Risk Assessment of Decentralized Finance". *U.S. Department of the Treasury.* DOI: https://home.treasury.gov/news/press-releases/jy1391

U.S. DEPARTMENT OF THE TREASURY. (2023b). "Treasury targets Sinbad.io virtual currency mixer as a tool of the DPRK". *U.S. Department of the Treasury.* DOI: https://home.treasury.gov/news/press-releases/jy1933

U.S. DEPARTMENT OF THE TREASURY. (2025a). "Treasury removes sanctions against Tornado Cash". *U.S. Department of the Treasury.* DOI: https://home.treasury.gov/news/press-releases/sb0057

U.S. DEPARTMENT OF THE TREASURY. (2025b). "Treasury targets Russian sanctions evasion infrastructure, redesignates Garantex, and identifies successor entities". *U.S. Department of the Treasury.* DOI: https://home.treasury.gov/news/press-releases/sb0225

U.S. GOVERNMENT ACCOUNTABILITY OFFICE. (2024). "Economic sanctions: Agency efforts help mitigate some of the risks posed by digital assets". *GAO,* No. GAO-24-106178.

WRIGHT, S. (2023). "The evolution of sanctions evasion: How cryptocurrency is the new game in evading sanction and how to stop it". *International Journal of Law, Ethics, and Technology,* vol. 3. DOI: https://ijlet.org/wp-content/uploads/2025/01/IJLET-3.1.pdf