CENTEF | Center for Research of Terror Financing

Cryptographic Assets and Sanctions Evasion: Iran and Russia as Models of Decentralized Economies under Geopolitical Pressure

A Comparative Analysis of Alternative Financial Infrastructures, Terror Financing, and Implications for the Global Economic Order

Submitted for Publication: November 2025

Author: CENTEF Team

About CENTEF

CENTEF, the Center for Research of Terror Financing, is a global research institute dedicated to advancing the understanding of terror financing and its worldwide impact. CENTEF's mission is to generate research, disseminate knowledge, and serve as an industry hub to better understand and disrupt the financing of terrorist activities. An established 501(c)(3) organization, CENTEF has a presence in the United States, Israel, and Italy.

Abstract

As international sanctions intensify, states such as Iran and Russia increasingly leverage cryptographic assets to construct resilient, decentralized financial systems that bypass traditional economic restrictions. This comparative study examines the use of cryptocurrency mining, stablecoins (notably Tether/USDT), and blockchain-based infrastructures to advance trade, finance illicit networks, and challenge U.S. dollar hegemony. The research introduces two original frameworks: *Sanctioned Decentralized Economies*, describing parallel financial ecosystems under geopolitical pressure, and *Dual Identity*, capturing the coexistence of legitimate and illicit crypto uses. It further identifies the *Static Designation Gap*—the structural mismatch between static address-based sanctions and the dynamic nature of blockchain protocols—and proposes a cluster-level enforcement framework to close it. The findings highlight the erosion of sanctions' effectiveness and the rise of digital financial sovereignty, underscoring the need for coordinated regulatory and technological responses.

Executive Summary: Cryptographic Assets and Sanctions Evasion

Background and Research Question

Cryptographic assets are evolving into a strategic tool in geopolitical struggles, with sanctioned countries like Iran and Russia leveraging decentralized technologies to circumvent financial restrictions. This study asks: How do countries subject to state sanctions utilize cryptographic technologies to build alternative financial infrastructures, and what are the implications of this process for the international economic and regulatory order?

Methodology

The research is based on a comparative analysis of Iran and Russia, employing official reports and documents (Central Bank of Iran, Central Bank of Russia, U.S. Department of the Treasury), publications from research institutes, reports from crypto analysis firms, and media coverage. Qualitative analysis identified patterns of behavior and policy, while quantitative analysis assessed transaction volumes and the activity of national crypto infrastructures.

Key Findings

- Iran possesses a regulated mining industry (since 2019) that generates foreign currency, uses stablecoins (USDT) for foreign trade through exchanges like Nobitex, finances terrorist organizations with hundreds of millions of dollars (Houthis, Hezbollah, Hamas), and has developed blockchain infrastructure to support autonomous international trade.
- Russia has transitioned from a restrictive policy to controlled adoption, including the local development of a ruble-backed stablecoin (A7A5) and the promotion of international initiatives for alternative systems (e.g., BRICS Pay).

Systematic Theoretical Insights

- *Sanctioned Decentralized Economies* refers to a model that has parallel economic systems, ensuring financial sovereignty, exploiting regulatory gaps, and employing mechanisms for transaction obfuscation.
- *Dual Identity* refers to local regulation restricting civilian use due to concerns about undermining monetary sovereignty, while simultaneously developing and promoting governmental infrastructures for sanctions evasion.
- These concepts contribute new patterns of decentralized activity to the literature.

Strategic Implications

- **Economic:** Increased use of cryptographic assets in international trade and the promotion of initiatives like BRICS Pay may challenge dollar hegemony, though their current impact remains limited.
- **Security:** The use of cryptographic assets for sanctions evasion reduces sanction effectiveness and enables the financing of illicit activities.
- **Legal:** Regulatory arbitrage facilitates the use of cryptographic tools for sanctions evasion and complicates activity monitoring.

Policy Recommendations

- Establish AI-based forensics units for crypto analysis.
- Synchronize regulation internationally to prevent regulatory arbitrage.
- Implement a "Static Designation Gap" framework: A coordinated enforcement regime that shifts crypto-sanctions from static address designations to dynamic, cluster-level identification of sanctioned entities. The framework would include standardized clustering methodologies across analytics providers, a real-time cross-jurisdictional designation database, mandatory stablecoin issuer integration for automated cluster-level freezing, and defined compliance obligations for VASPs, while incorporating due-process safeguards and remediation procedures for false positives.

Limitations and Future Research

The research is limited by the inherent lack of transparency in illicit financing and the reliance on secondary sources. For future research, directions may include expanding the study to countries like Venezuela or North Korea and developing quantitative models.

Conclusion

The increasing use of cryptographic assets for sanctions evasion presents the potential to destabilize the global financial order. Understanding this dynamic is crucial for formulating a balanced policy response that considers enforcement, innovation, and liberal principles.

Section 1: Introduction

Context and Research Significance

Over the past decade, cryptographic assets have evolved into a central tool in geopolitical struggles. Countries under state sanctions, such as Iran and Russia, leverage blockchain technologies to maintain their foreign trade activities and construct alternative financial infrastructures. These technologies, which enable decentralized and hard-to-trace transactions, challenge the international financial system predicated on dollar hegemony and systems like SWIFT. This phenomenon raises critical questions regarding the effectiveness of sanctions as a policy instrument, the capacity to monitor decentralized financial activity, and its implications for the global economic and regulatory order. This research contributes to the literature on financial sovereignty and decentralized technologies[1] by examining the use of cryptographic assets for sanctions evasion, highlighting the nuances between countries operating under sanctions regimes.

Research Question

This study examines the question: How do countries subject to institutional sanctions utilize cryptographic technologies to build alternative financial infrastructures, and what are the implications of this process for the international economic and regulatory order? This question focuses on how countries like Iran and Russia leverage cryptographic assets to establish financial sovereignty, exploiting regulatory arbitrage and mechanisms for transaction obfuscation. It further discusses the impact of this activity on sanctions effectiveness, the financing of security bodies and terrorist organizations, and the global financial structure.

Methodology and Research Approach

The research employs a comparative approach, analyzing the case studies of Iran and Russia. The analysis integrates qualitative and quantitative methodologies. The qualitative analysis identifies patterns of behavior and policy, such as local regulatory restrictions alongside the development of governmental infrastructures for sanctions evasion. The quantitative analysis examines the scope and characteristics of activity using open-source information. Sources include official reports from the Central Bank of Iran, the Central Bank of Russia, and the U.S. Department of the Treasury, publications from research institutes, reports from crypto analysis firms (such as Chainalysis), and media reports. The study is largely limited by a lack of transparency in official data, particularly in Iran, and thus relies on secondary sources.

[1] https://delong.typepad.com/files/eichengreen-globalizing.pdf ; https://nsiteam.com/social/wp-content/uploads/2019/11/Farrell-and-Newman-2019-IS-Weaponised-interdependence.pdf

Findings

The research identifies similar patterns of activity with nuances between Iran and Russia; both operate with relative secrecy, although Russia has led with overt and detailed legislation. In Iran, since 2019, crypto usage includes a regulated mining industry, the use of stablecoins (USDT) via exchanges like Nobitex, and the financing of illicit activities (e.g., Hezbollah, Hamas, Houthis) totaling hundreds of millions of dollars. Concurrently, Iran is developing independent blockchain infrastructures like Kuknos and Project Borna to support autonomous international trade. In Russia, cryptographic regulation evolved from a restrictive policy (2022) to controlled adoption (2024), with local initiatives for developing a ruble-backed stablecoin (A7A5) and dominance in leading international initiatives such as BRICS Pay, an activity that Iran also expresses support for.

Theoretical and Practical Contribution

This research introduces two theoretical concepts, *Sanctioned Decentralized Economies*, which describes parallel economic systems, and *Dual Identity*, which highlights the tension between restrictive regulation and the development of governmental infrastructures. These concepts contribute to the literature by identifying new patterns in decentralized activity. Practically, the study offers policy recommendations, such as the establishment of AI-based forensics units, regulatory harmonization, and a framework for closing the *Static Designation Gap* through cluster-level enforcement and real-time designation infrastructure, while addressing technological and legal challenges.

Structure of the Research

The research is divided into three parts: (1) a review of Iranian activity characteristics, examining the use of crypto in trade and financing illicit activity; (2) a review of the development of Russian activity, focusing on controlled adoption and international initiatives; and (3) a discussion of the economic, security, and regulatory implications, alongside policy recommendations. This study aims to deepen the understanding of sanctions evasion in the digital era.

Section 2: The Cryptographic Asset Market in Iran: The Current Situation and Extent of Adoption

This section examines the extent of cryptographic asset adoption in Iran, the economic backdrop to this phenomenon, and the characteristics of activity within the local market. Iran stands out as one of the most active countries in the cryptographic asset arena. According to a recent 2025 survey by Arzdigital, approximately 41.9% of the adult population in the country (21.9 million people) is active in this market, making it the most popular investment channel in Iran. For comparison, the proportion of those active in the stock market stands at only 20.3%, while the gold and foreign exchange (FX) markets garner interest from about 16.1% of the population.[2] Based on estimates published in the third quarter of 2024, the volume of private cryptographic asset holdings in Iran is estimated to be between $30 billion and $50 billion.[3] This figure positions the sector as a significant component of the country's informal economy.

The Background to Increasing Cryptographic Asset Usage

The significant rise in the use of cryptographic assets in Iran is deeply rooted in the country's complex economic reality, characterized by international sanctions and macroeconomic instability:

- **Preservation of Asset Value:** Since the re-imposition of U.S. sanctions in 2018, the Iranian Rial has experienced a dramatic depreciation of approximately 90% of its value, accompanied by persistent inflation at an average annual rate of about 40%.[4] These developments significantly eroded public trust in the country's monetary stability, prompting a widespread shift to alternative financial channels. In this context, stablecoins, primarily USDT (Tether), have assumed a central role as an effective substitute for the U.S. dollar, access to which is limited.[5]
- **Access to International Markets and Foreign Currency:** The economic sanctions imposed on Iran severely and continuously restricts the country's, and its citizens', access to international markets and the global financial system. Within this reality, cryptographic assets offer a sanction-circumventing and cross-border

[2] https://cdn.arz.digital/ad-cnt/main/2025/03/Arzdigital-Annual-Report-1403-pdf.pdf

[3] https://www.eghtesadonline.com/fa/news/2024056

[4] https://www.chainalysis.com/blog/crypto-crime-sanctions-2025/

[5] https://iranblockchain.org/wp-content/uploads/2025/01/%D9%85%D9%82%D8%A7%D9%84%D9%87-%D8%A8%D8%B1%D8%B1%D8%B3%DB%8C_%D8%AA%D8%A7%D8%AB%DB%8C%D8%B1_%D8%B1%D9%85%D8%B2%D8%A7%D8%B1%D8%B2%D9%87%D8%A7_%D8%A8%D8%B1_%D9%82%DB%8C%D9%85%D8%AA_%D8%A7%D8%B1%D8%B2_%D8%AF%D8%B1_%DA%A9%D8%B4%D9%88%D8%B1.pdf

instrument, providing Iranians with relatively free access to trading platforms, financial services, and foreign currency, thereby connecting them indirectly but effectively to the international economic system.[6]

- **Search for New Investment Avenues:** A challenging economic reality, characterized by high inflation, erosion of local currency value, and a lack of investment opportunities in traditional markets, pushes large segments of the Iranian public to seek financial alternatives to improve their economic situation. Against this backdrop, cryptographic asset trading has become an accessible and popular investment channel, perceived as an effective alternative to traditional Iranian avenues (stock market, real estate, vehicles, FX).[7]
- **Capital Flight:** The lack of structural stability in Iran's economic policy, particularly the exchange rate volatility, persistent inflation, and severe restrictions on access to foreign currency, have exacerbated the phenomenon of capital flight from the country. Given this, cryptographic assets have become one of the primary means for transferring financial assets outside Iran's borders, circumventing formal financial oversight and regulatory systems. According to estimates published during 2024, the volume of capital flight from Iran via cryptographic assets amounted to approximately $4.18 billion–an increase of about 70% compared to the previous year.[8] This figure highlights the increasing use of cryptographic assets not merely as a means of private economic protection but as a tool with systemic potential to undermine the state's mechanisms of financial control.

Characteristics of the Domestic Market: Trading Platforms and Activity Volumes

The domestic market in Iran is developed and includes numerous trading platforms, alongside extensive activity in the informal market:

- **Trading Platforms:** Over 100 cryptographic asset trading platforms operate in Iran. Nobitex is the largest and most central among them. As of 2023, it held a market share of approximately 87% of all official cryptographic trading activity, serving as a strategic hub connecting the Iranian market to international markets.[9] According to a Chainalysis report, assets totaling approximately $11 billion have flowed into Iran through Nobitex over the years, while the cumulative volume of the

[6] https://www.chainalysis.com/blog/crypto-crime-sanctions-2025/
[7] https://cdn.arz.digital/ad-cnt/main/2025/03/Arzdigital-Annual-Report-1403-pdf.pdf
[8] https://www.chainalysis.com/blog/crypto-crime-sanctions-2025/
[9] https://www.trmlabs.com/resources/blog/iran-crypto-economy

next ten largest exchanges combined amounted to only about $7.5 billion.[10] Beyond widespread use among citizens, there are significant indications that Nobitex also serves as a central platform for governmental and security activities in Iran. An analysis conducted by TRM Labs of the exchange's code, which was leaked by the pro-Israel hacking group Gonjeshke Darande (Predatory Sparrow) in June 2025, reportedly revealed patterns indicative of significant state-level use of this platform, a fact that reinforces the "Dual Identity" claim for the entire Iranian market.[11]

- **Trading Volumes:** According to official data, the daily trading volume between March 2024 and March 2025 across the ten largest cryptographic exchanges in Iran was approximately 1,524 billion Tomans, equivalent to about $31 million per day.[12] However, official estimates indicate that approximately 47% of the total market activity occurs on unlicensed trading platforms,[13] with some estimating the daily turnover at approximately $143 million.[14] This figure points to the existence of an extensive and unregulated parallel infrastructure, which constitutes a significant part of Iran's cryptographic economy.

The extensive usage, high trading volumes, and broad accessibility to cryptographic assets have created a dual challenge for the Iranian regime: How to enable beneficial and controlled use of these assets while mitigating the risks associated with free, anonymous, and unregulated use. The next section will examine how the state has attempted to formulate stable regulation in light of conflicting economic, political, and security interests.

[10] https://www.chainalysis.com/blog/nobitex-iranian-exchange-exploit-june-2025/; Other crypto exchanges operating in Iran - Wallex, Excoino, Aban Tether, Bit24.cash, Tetherland, Sarmayex, Ramzinex, Pooleno, Arzpaya, Efex, Exir

[11] https://www.trmlabs.com/resources/blog/inside-the-nobitex-hack-how-the-iran-israel-conflict-exposed-tehrans-grip-on-its-crypto-services

[12] https://cdn.arz.digital/ad-cnt/main/2025/03/Arzdigital-Annual-Report-1403-pdf.pdf

[13] https://arzdigital.com/blog/report-cbi-telecom-ministry-crypto-regulation/

[14] https://news.bitcoin.com/iranian-crypto-holdings-equal-a-third-of-national-gold-market/

Section 3: The Regulatory Journey: Iran's Winding Path

This section will analyze the evolution of Iranian regulation in the field of cryptographic assets, examining the stages of development from sweeping restrictions to strategic state adoption, and end with exploring recent measures tightening governmental oversight of citizen activity. The development of cryptographic asset market regulation in Iran has fluctuated between outright rejection and controlled adoption, as the state attempts to balance the need to ensure monetary control with efforts to utilize this domain as a means of confronting geopolitical constraints and economic sanctions.

Initial Approach: Prohibitions and Concerns (2017-2018)

Iran's initial policy towards cryptographic assets was characterized by a staunchly negative approach, formally justified by concerns regarding the criminal and security aspects inherent in this field. Between 2017 and 2018, the use, ownership, and trading of cryptographic assets were prohibited based on the perception that they could be used for money laundering, terror financing, and illegal transfers. As part of these concerns, the Central Bank of Iran (CBI) issued directives prohibiting all financial institutions–including banks, regulated exchanges, and financial centers–from engaging in any activity involving cryptographic assets. Furthermore, it was clarified that operating a blockchain-based payment network without explicit authorization would be considered a legal offense and incur legal sanctions. This phase marked the implementation of a prohibitive regulatory policy focused on restricting cryptographic activity in the local market.[15]

Controlled Recognition and Attempts at Regulation (2019): Crypto as a Tool for Sanctions Mitigation

The United States' withdrawal from the nuclear agreement in 2018 and the imposition of the "maximum pressure policy," which led to the Iranian financial system's disconnection from the international system, accelerated a paradigmatic shift in the state's approach to cryptographic activity, aiming to leverage the potential inherent in this domain for sanctions evasion. An institutional academic expression of this can be found in a comprehensive policy report published in 2019 by the Economic Research Group of the Institute for Strategic Studies (پژوهشکده تحقیقات راهبردی) in Tehran, titled "The Phenomenon of Cryptocurrencies: Risks, Opportunities, and Policy-Making." This report advocated for the controlled use of cryptographic assets for foreign trade purposes, while avoiding their adoption as a domestic means of payment, partly due to concerns about undermining the Rial's stability and increasing illicit financial activity. Furthermore, the report recommended the development of regional monetary mechanisms based on cryptographic assets, within which dedicated assets could be defined for trade among

[15] https://fiu.gov.ir/mizancrypto

partner countries, outside the SWIFT system. This move was defined as a potential foundation for establishing an alternative financial network. From an energy perspective, the report proposed institutionalizing and expanding cryptographic asset mining activities to increase state revenues.[16] The comprehensive recommendations in the report reflected a concerted effort to shift from a conservative mindset, which viewed this activity as a threat, to an applied geopolitical perspective that recognized crypto as a legitimate sovereign tool within the struggle against international restrictions.

Concurrently with the report's publication, the CBI issued an official regulatory framework designed to regulate cryptographic asset trading and mining activities, aiming to balance the preservation of sovereign economic interests with the protection of monetary stability.[17]

Within this framework, the CBI emphasized concerns about the detrimental macroeconomic impacts inherent in cryptographic activity–primarily undermining the state's ability to control currency policy and increasing local market volatility. To this end, the CBI distinguished between three types of cryptographic assets: a state-issued sovereign currency (Central Bank Digital Currency), such as Iran's Digital Rial; a regional currency for limited inter-state use; and a decentralized global currency, such as Bitcoin or USDT. While the first two gained legitimacy due to their inherent control characteristics, the use of decentralized assets was prohibited as a means of payment within the country's borders and permitted solely for activity within regulated trading platforms. Additionally, it was stipulated that every crypto trading platform would require explicit licensing and approval from the CBI. In the mining sector, the legal framework was defined such that this activity would be permissible under licensing from the Ministry of Industry, Mine and Trade (MIMT), subject to increased electricity tariffs. Furthermore, mining activity was conditioned upon the sale of its output to a dedicated mechanism designed to provide foreign currency to authorized importers. These steps marked the beginning of a dual regulation policy: on one hand, limiting the scope of cryptographic asset use among the general public; and on the other, controlled and targeted adoption of the technology by the state for strategic economic needs under sanctions conditions. This model aimed to enable authorities to retain regulatory control while harnessing the inherent potential of cryptographic assets as a geo-economic lever. This approach laid the groundwork for a crypto policy that supports state interests and would deepen in the coming years.

---

[16] https://csr.ir/files/fa/news/1398/6/6/1916_970.pdf

[17] https://iranblockchain.org/wp-content/uploads/2021/03/%D8%A7%D9%84%D8%B2%D8%A7%D9%85%D8%A7%D8%AA-%D9%88-%D8%B6%D9%88%D8%A7%D8%A8%D8%B7-%D8%AD%D9%88%D8%B2%D9%87-%D8%B1%D9%85%D8%B2%D8%A7%D8%B1%D8%B2.pdf

Permitting Import Activity via Cryptographic Assets (2022)

Following the economic sanctions imposed on Iran and the growing difficulties in accessing the international financial system, Iran became one of the first countries to regulate the use of cryptographic assets for foreign trade purposes. This activity was regulated during 2022 under CBI directives permitting the import of goods using cryptographic assets (this topic will be discussed in detail in Section 6).[18]

Regulatory Tightening and Increased Oversight (Late 2024 - Mid-2025)

Another significant regulatory development occurred in late December 2024, when the CBI took a series of dramatic regulatory steps. These measures aimed to restrict the general public's access to cryptographic asset trading in order to reduce its impact on monetary stability. These actions were taken against the backdrop of the increased use of assets like USDT as a dollar substitute, the depreciation of the Rial, and a sharp rise in speculative activity.[19]

As a first step, the CBI ordered a halt to Rial-denominated transactions (buying and selling) within cryptographic asset trading activities. After several weeks, the CBI permitted these transactions but mandated that they be conducted exclusively through a governmental API (Shaparak).[20] This move grants the government control and monitoring capabilities over all trading activity occurring in this market. Additionally, the CBI ordered an expansion of licensing requirements, obligating various platforms to meet significant capital requirements.[21]

In February 2025, Iran's Ministry of Culture issued a directive prohibiting all advertising promoting cryptographic asset activity, justifying it with "the economic risks inherent to the public in this activity."[22] In June 2025, following the breach of the Nobitex exchange, the CBI announced a restriction on the operating hours of licensed cryptographic asset exchanges, limiting them to between 10:00 and 20:00.[23]

---

[18] https://www.radiofarda.com/a/iran-to-use-cryptocurrency-to-imports/32008640.html
[19] https://www.specialeurasia.com/2025/02/05/crypto-iran-geopolitics/
[20] https://way2pay.ir/427938/
[21] https://www.aljazeera.com/news/2025/2/27/irans-government-hits-out-at-crypto-again-as-currency-freefalls
[22] https://www.etemadonline.com/%D8%A8%D8%AE%D8%B4-%D8%A7%D9%82%D8%AA%D8%B5%D8%A7%D8%AF%DB%8C-22/701303-%D8%B1%D9%85%D8%B2%D8%A7%D8%B1%D8%B2-%D9%88%D8%B2%D8%A7%D8%B1%D8%AA-%D8%A7%D8%B1%D8%B4%D8%A7%D8%AF-%D8%B3%D8%B1%D9%85%D8%A7%DB%8C%D9%87-%DA%AF%D8%B0%D8%A7%D8%B1%DB%8C
[23] https://cointelegraph.com/news/iran-crypto-curfew-nobitex-100m-hack

Iran's regulatory policy regarding cryptographic assets for its citizens reflects a clear trend of tightening and deepening oversight. This trend stems from increasing concerns over the loss of monetary sovereignty, capital flight, and the exacerbation of economic and social risks. The widespread and unregulated use of cryptographic assets among citizens is perceived by government officials as a potential threat to the Rial's status, the transparency of financial activity, and the state's ability to conduct effective monetary policy.

Considering these scenarios, the Central Bank of Iran is working to prevent the widening gap between the official financial system and decentralized systems, employing an unconventional array of regulatory tools. However, the reactive characteristics of this policy–sudden changes in direction and a lack of stability–diverts many transactions to unregulated channels, thereby weakening the state's own enforcement capacity.

The next section will focus on the dominance of USDT (Tether) in Iran, the implications of this widespread use for the local economy, and governmental oversight efforts to control its impacts.

Section 4: The Use of USDT (Tether) in Iran

The severe sanctions imposed on Iran has significantly curtailed its access to the global financial system. These restrictions, including blocked access to SWIFT, the freezing of state assets amounting to tens of billions of dollars, and sanctions on the Iranian banking system, including the Central Bank of Iran (CBI), have led to an increase in activity involving cryptographic assets generally, especially USDT. USDT effectively serves as a substitute for the U.S. dollar, access to which has been dramatically limited.[24]

The fact that USDT functions as a proxy for the U.S. dollar has led many Iranians to use it extensively, including for international trade and as a hedge against inflation and the sharp, continuous depreciation of the Rial. As such, USDT is perceived by the Iranian public as a tool for preserving value, similar to holding physical dollars or gold, with its use often serving as a hedging mechanism rather than a speculative investment.

A report by TRM Labs states that during 2022, the total volume of cryptographic asset activity flowing into Iranian exchanges approached $3 billion, where the TRON network accounted for approximately 65% of all incoming activity (around $1.95 billion), with this activity concentrated in two types of tokens: USDT and TRX, the latter primarily used for paying transaction fees on the network. While the report does not provide a precise breakdown between the two token types, it can be estimated that most of this activity was conducted in USDT. According to the report's authors, USDT's dominance stemmed primarily from its availability and stability in its TRC20 version, alongside significantly lower transaction fees compared to other blockchains also supporting USDT, such as Ethereum. USDT's status as a stablecoin pegged to the U.S. dollar made it particularly attractive in Iran's unstable economic environment.[25]

An Iranian article reviewing 2024 data indicates that, according to Iranian exchange figures, the annual volume of USDT used through official Iranian exchanges amounts to less than $5 billion out of a total annual trading volume of approximately $6 billion.[26] This volume of USDT activity constitutes about 80% of all cryptographic asset activity occurring on official platforms. It is noteworthy that official estimates suggest 47% of

[24] https://www.chainalysis.com/blog/crypto-crime-sanctions-2025

[25] https://www.trmlabs.com/resources/blog/iran-crypto-economy

[26] https://iranblockchain.org/wp-content/uploads/2025/01/%D9%85%D9%82%D8%A7%D9%84%D9%87-%D8%A8%D8%B1%D8%B1%D8%B3%DB%8C_%D8%AA%D8%A7%D8%AB%DB%8C%D8%B1_%D8%B1%D9%85%D8%B2%D8%A7%D8%B1%D8%B2%D9%87%D8%A7_%D8%A8%D8%B1_%D9%82%DB%8C%D9%85%D8%AA_%D8%A7%D8%B1%D8%B2_%D8%AF%D8%B1_%DA%A9%D8%B4%D9%88%D8%B1.pdf ; https://cdn.arz.digital/ad-cnt/main/2025/03/Arzdigital-Annual-Report-1403-pdf.pdf

cryptographic asset transactions in Iran are conducted on unlicensed platforms, which could imply that the actual volume of USDT activity is significantly higher.[27]

The substantial increase in USDT usage in Iran has raised growing concern among government officials, primarily the CBI, who have warned against its use as a mechanism for capital flight, money laundering, and undermining the Rial's exchange rate stability.[28]

In December 2024, against the backdrop of a sharp depreciation of the local currency and increasing public reliance on USDT as a dollar substitute, the CBI took a sudden step by imposing a sweeping ban on Rial-denominated transactions on local crypto trading platforms.

This measure, which was described in detail in Section 3, reflected, among other things, the state's severe reaction to USDT's deep penetration into the local market, illustrating the familiar pattern of an unstable regulatory policy—reactive, sometimes extreme, and subject to market pressures and geo-economic shocks.

Subsequently, the CBI implemented a series of additional measures, including examining the possibility of blocking USDT trading in the event of a sharp daily increase (over 4%) in the dollar's exchange rate.[29] According to the CBI, these steps were intended to curb the speculative nature of USDT trading and prevent its influence on volatility in the unofficial foreign exchange market.

Criticism against the growing use of USDT is based, in part, on the systematic discrepancy between the asset's price on local trading platforms and the dollar's exchange rate in the free market—a gap ranging from 5% to 10%. This disparity creates market distortions that could intensify pressure on the Rial's exchange rate and deepen its depreciation trend, a fact that even led the CBI to impose temporary restrictions on the use of Rial for purchasing cryptographic assets. Conversely, some observers point to the government's own policies, which seek to control exchange rates and stem capital outflow, as indirectly contributing to the increased demand for stable assets and creating structural distortions in the local crypto market. Another explanation for the price

---

[27] https://arzdigital.com/blog/report-cbi-telecom-ministry-crypto-regulation/

[28] https://crystalintelligence.com/investigations/beyond-the-headlines-of-irans-crypto-usage/ , https://mihanblockchain.com/capital-flight-crypto-iran/ , https://caspianpost.com/iran/iran-shuts-down-crypto-payment-services-as-rial-hits-record-low , https://iranblockchain.org/wp-content/uploads/2025/01/%D9%85%D9%82%D8%A7%D9%84%D9%87-%D8%A8%D8%B1%D8%B1%D8%B3%DB%8C_%D8%AA%D8%A7%D8%AB%DB%8C%D8%B1_%D8%B1%D9%85%D8%B2%D8%A7%D8%B1%D8%B2%D9%87%D8%A7_%D8%A8%D8%B1_%D9%82%DB%8C%D9%85%D8%AA_%D8%A7%D8%B1%D8%B2_%D8%AF%D8%B1_%DA%A9%D8%B4%D9%88%D8%B1.pdf

[29] https://www.aljazeera.com/news/2025/2/27/irans-government-hits-out-at-crypto-again-as-currency-freefalls

discrepancies argues that Iranian investors' restricted access to international trading platforms has led to increased reliance on local intermediaries—a process involving significant brokerage costs, reflected in a consistent premium on USDT's price relative to the dollar's exchange rate.[30]

However, some parties reject this claim, noting that despite USDT's dominant weight in the local cryptographic market, its relative share of Iran's total foreign exchange market—estimated at over $300 billion annually—remains negligible. Accordingly, it is argued that USDT's direct impact on the Rial's exchange rate is marginal, if any, and that it is directly influenced by the dollar's rate in Iran's free market, acting more as an immediate indicator of the exchange rate than as an influencing factor.[31]

A significant counter-argument can be raised against this claim: Comparing USDT's activity volume to the entire foreign exchange market may be misleading, as a substantial portion of Iran's FX trade occurs at subsidized rates determined by the government for essential imports.[32] In such a reality, even a relatively small market segment—as long as it operates in unregulated markets—can influence the dollar's exchange rate in the free market.

The Central Bank of Iran's struggle with the increasing use of USDT illustrates the limitations of centralized monetary policy in a rapidly changing financial reality. Faced with extensive economic sanctions, continuous depreciation, and double-digit inflation, there is a clear trend of financial activity shifting outside the formal system—adopting stable assets, primarily USDT, as a substitute for the U.S. dollar and for value preservation. The authorities' response, which includes regulatory restrictions and attempts to mitigate USDT's influence on the exchange rate, reflects growing concern over losing control of the unofficial foreign exchange market. This phenomenon highlights the strategic challenge confronting policymakers in Iran: how to balance the needs of macroeconomic

---

[30] https://ramzinex.com/blog/tether-price-difference-to-dollar/,
https://www.chainalysis.com/blog/crypto-crime-sanctions-2025/
https://crystalintelligence.com/investigations/beyond-the-headlines-of-irans-crypto-usage/
https://www.aljazeera.com/news/2025/2/27/irans-government-hits-out-at-crypto-again-as-currency-freefalls https://www.specialeurasia.com/2025/02/05/crypto-iran-geopolitics/
https://utotimes.com/impact-of-fundamentals-on-usdtirt-march-26-2025/

[31] https://iranblockchain.org/wp-content/uploads/2025/01/%D9%85%D9%82%D8%A7%D9%84%D9%87-%D8%A8%D8%B1%D8%B1%D8%B3%DB%8C_%D8%AA%D8%A7%D8%AB%DB%8C%D8%B1_%D8%B1%D9%85%D8%B2%D8%A7%D8%B1%D8%B2%D9%87%D8%A7_%D8%A8%D8%B1_%D9%82%DB%8C%D9%85%D8%AA_%D8%A7%D8%B1%D8%B2_%D8%AF%D8%B1_%DA%A9%D8%B4%D9%88%D8%B1.pdf

[32] World Bank. (2024). Iran Economic Monitor: Sustaining Growth Amid Rising Geopolitical Tensions (Spring 2024
https://openknowledge.worldbank.org/server/api/core/bitstreams/e7c79f03-32de-4c2a-ac67-38b2f0883589/content

stability with the growing dynamic of using decentralized financial tools, which are often perceived by the public not as speculative investment vehicles, but as functional solutions in a reality of persistent economic uncertainty.

Following a series of USDT wallet freezes and particularly after the Nobitex exchange breach, recommendations have been observed on Iranian websites to switch to DAI as an alternative to USDT.[33] DAI is a stablecoin designed to maintain a nominal value of $1. Unlike USDT, this asset is predominantly backed by cryptographic assets, and its operations are managed by smart contract-based mechanisms on the Ethereum network, developed by MakerDAO. These mechanisms provide relative anonymity due to their decentralized nature.[34]

Beyond the use of cryptographic assets as a means of trade and protection against depreciation and inflation, the Iranian government identified the economic potential inherent in digital currency mining activities as early as 2019. The next section will examine the cryptographic asset mining industry in Iran, with an emphasis on Bitcoin mining, and discuss the potential revenues and the associated energy and political challenges of this activity.

[33] https://wallex.ir/blog/dai-vs-tehter/;
https://www.eghtesadonline.com/fa/news/2075095/%D8%AC
[34] https://www.osl.com/hk-en/academy/article/what-is-dai-dai-a-decentralized-stablecoin

Section 5: Cryptographic Asset Mining in Iran

This section will survey Iran's cryptographic asset mining industry, examine its regulatory framework, assess its relative share in the global market, and evaluate its potential revenues. Furthermore, this section discusses the impact of mining activity on the national electricity infrastructure, the involvement of foreign investors, and in particular, the engagement of Iranian security bodies in this field.

Iranian Regulation in the Mining Sector: Overview

In 2019, cryptographic asset mining was officially recognized as a legal industry in Iran.[35] This move made Iran one of the first countries to strategically integrate cryptographic assets into its national economy. This development stemmed from an acknowledgment of the economic potential inherent in this activity, given the international sanctions imposed on the country. The adopted regulatory framework included a formal licensing requirement for operators, the establishment of dedicated electricity tariffs higher than the subsidized rates prevalent in many sectors, a prohibition on the domestic use of mined assets, and a mandate for selling cryptographic assets to institutional bodies responsible for allocating foreign currency to authorized importers.[36]

Iran's Share in the International Market: Estimates and Scope

The lack of transparency in Iran's mining data makes it challenging to determine its relative share of the blockchain network's global computing power (hashrate),[37] which in turn complicates the calculation of its potential revenues from this activity. This difficulty is reflected in the wide range of estimates regarding the quantity of Bitcoin mined in Iran over the years, which vary from 60,000 Bitcoin units, representing a current value of approximately $7.2 billion, to 200,000 units, representing a current value of approximately $24 billion.[38]

In 2021, mining activity in Iran was estimated at 4% to 8% of the global hashrate, a figure that positioned it as the fifth-largest miner globally after China, the U.S., Russia, and Malaysia.[39] Reports referencing a 2019 study by the Iranian Presidential Centre for

[35] https://www.aljazeera.com/economy/2019/8/5/irans-government-recognises-cryptocurrency-mining-with-caveat
[36] https://cdn.arz.digital/ad-cnt/main/2019/01/IT-Reg-Cryptocurrency-0.0.pdf
[37] Hashrate is the total computational power being used to mine and process transactions on a Bitcoin blockchain network.
[38] https://decrypt.co/327381/how-much-bitcoin-iran-mined-complicated
[39] https://www.babelstreet.jp/blog/iran-counts-on-bitcoin-to-evade-sanctions

Strategic Studies estimate that the potential revenue from cryptographic asset mining in that year stood at approximately $700 million.[40]

An estimate by Elliptic, based on 2020 data from the Cambridge Centre for Alternative Finance[41] and supported by a January 2021 statement from the Iranian Electricity Company, assessed Iran's share at approximately 4.5% of global computing power. This granted Iran a mining potential of around 19,500 Bitcoin units during that year, with a total value of approximately $1 billion.[42]

A 2022 estimate projected Iran's share of the global hashrate had decreased to 3.1%, an assessment that remains valid to date.[43] Based on these estimates, Iran's potential mining revenues for 2024 amount to approximately $435 million.[44]

Iranian Mining Activity During the Conflict and Its Impact on the Global Hashrate

During the period of conflict between Iran, Israel, and the U.S., the global blockchain network experienced a drastic decrease of approximately 15% in its total computing power (hashrate). This decline sparked extensive debate regarding whether it could be attributed to kinetic damage to mining sites operating in Iran, the Iranian government's decision to disconnect from the internet, the bi-weekly update of the system's difficulty level, the severe heatwave that affected the U.S. at the time,[45,46] or some combination of these factors

Direct indication of a link between the security escalation and the decrease in the global blockchain network's hashrate can be found in electricity consumption data released after the conflict. According to official reports, during the 12 days of confrontation between Iran, Israel, and the United States, there was a decrease of approximately 2,400 megawatts in the daily electricity demand in the country. A senior official at the Iranian Electricity Company (Tavanir) attributed this decline to the cessation of operations by approximately 900,000 crypto miners—a figure that, if accurate, indicates a dramatic surge in the scope

[40] Official Report: Iran Could Use Cryptocurrencies to Avoid Sanctions
[41] https://ccaf.io/cbnsi/cbeci/mining_map
[42] https://www.elliptic.co/blog/how-iran-uses-bitcoin-mining-to-evade-sanctions
[43] https://crystalintelligence.com/investigations/beyond-the-headlines-of-irans-crypto-usage/; https://www.ainvest.com/news/iran-bitcoin-mining-surge-driven-95-cheaper-electricity-2506/
[44] https://news.bitcoin.com/bitcoin-mining-revenue-in-2024-a-year-of-change-and-challenges; https://www.khabaronline.ir/news/1519097; https://www.elliptic.co/blog/how-iran-uses-bitcoin-mining-to-evade-sanctions; https://www.reuters.com/technology/iran-uses-crypto-mining-lessen-impact-sanctions-study-finds-2021-05-21/
[45] https://medium.com/coinmonks/the-bitcoin-mystery-that-exposed-irans-secret-crypto-empire-d8ee2cceae5e
[46] https://blocksbridge.substack.com/p/bitcoin-hashrate-misconception

of the country's mining industry compared to previous estimates.[47] For comparison, Tavanir's CEO estimated in 2021 that all mining activity in Iran consumed only between 500 and 600 megawatts, with about half of this consumption attributed to illegal activities.[48] However, some parties express skepticism regarding the direct contribution of miners to the decrease in electricity demand, cautioning that, given the significant lack of governmental transparency concerning the scope of active mining industry, it is difficult to establish an accurate estimate of its relative contribution to the decline in electricity demand.[49]

Insights published by Chainalysis confirmed that a decrease in Iranian mining volume was indeed detected throughout the conflict period, with the most significant drop occurring around June 19th, which coincided with two events: the Nobitex breach and the government's decision to disconnect internet access.[50]

According to the company's assessment, since these events preceded the U.S. attack on the Fordow site, this indicates that the disruption was likely due to connectivity issues rather than direct military action impacting significant mining sites. The company further notes that despite some recovery following the restoration of internet access, Iranian mining volumes remain lower than in the past.

An examination of the graph provided by Chainalysis reveals that while the peak decline occurred on the 19th of the month, the downward trend began as early as June 16th, in the midst of Israeli attacks, including on the nuclear facilities in Natanz and Esfahan.

This seemingly precludes that the decrease in mining volume originated solely from the internet disconnection. Furthermore, Chainalysis' assertion that mining volumes remained lower than in the past even after internet access was restored could suggest the possibility that at least part of the decline is attributable to kinetic damage to mining farms.

In this context, some point to the potential for an infrastructural link between nuclear facilities and cryptographic asset mining activity. The operation of nuclear facilities, particularly uranium enrichment systems, requires high levels of stability and continuous electricity supply, partly to maintain the functionality of centrifuges. This characteristic could make nuclear sites locations with suitable energy infrastructure for operating large-scale mining farms. Rajat Ahlawat, a researcher at Crystal Intelligence, addressed this

[47] https://www.tasnimnews.com/fa/news/1404/04/07/3343958

[48] https://financialtribune.com/articles/business-and-markets/107075/cryptomining-suspended-for-2-weeks-to-save-power

[49] https://fararu-com.translate.goog/fa/news/885604

[50] https://www.linkedin.com/posts/chainalysis_iranian-bitcoin-mining-rates-have-remained-activity-7345798273078554624-v2Xq

possibility, noting that a nuclear facility, such as Fordow, could have sufficient electricity infrastructure to power mining farms, though he emphasized that there is no specific evidence indicating the existence of such mining activity at Fordow.[51]

Although there are no conclusive findings on this matter, the mere establishment of mining farms near sensitive infrastructures sparks debate among many who identify the possibility of proactive regime actions aimed at securing a stable and secure source of income outside the global financial system.

Impact of Mining on the National Energy Balance

Although the Iranian government views cryptographic asset mining as an alternative and effective source of income in light of economic sanctions, this activity is accompanied by severe structural challenges—foremost among them, the growing burden on the national electricity grid. One of the central issues concerns the high rate of illegal use of subsidized electricity infrastructure for mining purposes, including unauthorized connections to public institutions, religious buildings, and, according to some claims, security facilities. This phenomenon has been identified by authorities as one of the primary causes of persistent energy shortages and frequent, widespread power outages across the country.[52] In 2021, then-Iranian President Hassan Rouhani estimated that 85% of the country's mining activity was conducted illegally—an assessment that led him to order a temporary suspension of all activity in the sector for four months, with the aim of reducing its negative impact on the energy sector.[53] Superficially, this directive raises questions: Given the President's declaration about the dominant share of illegal mining (85%), it is doubtful whether these actors would choose to comply with such a directive.

Although attempts have been made in recent years to regulate mining activity, including setting targeted electricity tariffs for this industry, a senior official at the national electricity company (Tavanir) recently estimated that over 50% of active miners in Iran are currently located in industrial zones benefiting from subsidized electricity tariffs—a situation that continues to fuel tension between the state's need to generate crypto revenues and the demands for reliability and stability in the energy system.[54]

---

[51] https://decrypt.co/327381/how-much-bitcoin-iran-mined-complicated

[52] https://www.ncr-iran.org/en/publications/special-reports/bitcoin-mining-in-iran-irgc-operations-and-the-power-grid-crisis/

[53] https://www.reuters.com/technology/iran-uses-crypto-mining-lessen-impact-sanctions-study-finds-2021-05-21/

[54] https://www.iranjib.ir/shownews/133093

Foreign Investments in Mining

Subsidized electricity tariffs in Iran have, over the years, created an economic incentive that attracted foreign players to the Bitcoin mining sector—particularly companies from China. A prominent example of this is the establishment of Iran's largest mining farm by the Chinese company RHY, which began operations in late 2017 with a declared capacity of approximately 175 megawatts. This facility was strategically located near a power plant in the Rafsanjan region of southeastern Iran, a location that ensured direct, cheap, and reliable access to energy supply.[55] At the time of its establishment, this project became one of the largest mining ventures globally, and it is claimed to be operated in partnership with the "Iran-China Development Investment Company." Evidence supporting this partnership claim can be found in a November 2018 report by this company, in which it officially declared its entry into cryptographic asset mining activities.[56]

Despite this significant foreign presence, there are consistent reports claiming that the Iranian government implements a deliberate concealment policy regarding the extent of Chinese involvement in the sector. This policy is reflected in the publication of partial or contradictory information concerning the number of foreign-owned mining facilities and the special electricity tariffs they receive. This conduct may indicate Tehran's desire to balance its aspiration to generate revenues from mining with concerns about public and political criticism regarding the granting of extensive benefits to external actors. Furthermore, alongside the Chinese partnership, activity licenses have also been reported for miners from Turkey and other countries, illustrating Iran's attractiveness to foreign investors in the mining sector.[57]

---

[55] https://www.babelstreet.jp/blog/iran-counts-on-bitcoin-to-evade-sanctions ; https://www.ncr-iran.org/en/publications/special-reports/bitcoin-mining-in-iran-irgc-operations-and-the-power-grid-crisis/

[56] https://virgool.io/@epsi1on/rafsanjan-miner-farm-1-gmpziiyskl5g ; https://radis.org/%D_8%B_%D9%8A%D9%86%D9%8A-%D9%87%D8%A7-%D9%88-%D8%B3%D9%BE%D8%A7%D9%87-%D9%BE%D8%A7%D8%B3%D8%AF%D8%A7%D8%B1%D8%A7%D9%86-%D8%A8%D9%87-%D9%87%D8%AF%D9%81-%D8%A7%D8%B3%D8%AA%D8%AE%D8%B1%D8%A7%D8%AC-%D8%A8/; https://rasmio.com/company/14006645955/Direct/https://rasmio.com/News/15082249/

[57] https://observers.rfi.fr/fa/%DA%AF%D8%B2%D8%A7%D8%B1%D8%B4-%D9%87%D8%A7%DB%8C-%D8%AA%D8%AD%D9%82%DB%8C%D9%82%DB%8C/20210203-%D9%85%D8%B2%D8%A7%D8%B1%D8%B9-%D8%A8%DB%8C%D8%AA-%DA%A9%D9%88%DB%8C%D9%86%DB%8C-%DA%A9%D9%87-%D8%B4%D8%B1%DA%A9%D8%AA-%D9%87%D8%A7%DB%8C-%DA%86%DB%8C%D9%86%DB%8C-%D9%88-%D9%85%D9%82%D8%A7%D9%85%D8%A7%D8%AA-%D8%A7%DB%8C%D8%B1%D8%A7%D9%86%DB%8C-%D8%B3%D8%B9%DB%8C-

Involvement of Security Bodies in Mining Activities

Against the backdrop of continuous sanctions and the rising demand for alternative funding sources, a picture is emerging suggesting that governmental bodies in Iran, including the Islamic Revolutionary Guard Corps (IRGC), play a central role in the country's cryptographic asset mining sector. An assessment published in 2021 posited that over half of Iran's active mining power—approximately 100,000 out of 180,000 devices—is under the direct or indirect ownership of state-affiliated entities.[58] If these estimates indeed reflect reality, it points to extensive institutional control over national cryptographic infrastructures, a fact that may also explain the prevailing lack of transparency regarding this area of activity.

Further reinforcement for this assessment can be found in an analysis by TRM Labs, which found that wallets associated with mining activity in Iran began flowing Bitcoin into Nobitex for the first time after the breach, emphasizing that these flows were critical for the exchange's resumption of activity. Following this finding, the report's authors note that, in their estimation, Iran continues to use Bitcoin mining as part of a strategic approach to generating revenue and circumventing sanctions.[59]

Moreover, estimates published in recent years, primarily by Iranian opposition figures and independent sources, contend that entities identified with the IRGC are involved in mining activities, including through collaborations with foreign companies—mainly Chinese—to establish industrial-scale mining farms, including the one operating in Rafsanjan.[60] Support for this possibility can be found in reports concerning legislation passed by the Iranian parliament in 2022 that granted security bodies the authority to establish independent electricity generation infrastructures, a move that serves as a significant incentive for entering the mining sector.[61] If this information is accurate, it represents a structural change enabling security bodies to operate large-scale mining farms without effective oversight from enforcement authorities.

Another illustration of the potential involvement of security bodies in mining activity can be found in an event reported in 2021, describing a violent confrontation between IRGC

%D8%AF%D8%B1-%D9%BE%D9%86%D9%87%D8%A7%D9%86-%DA%A9%D8%B1%D8%AF%D9%86-%D8%A2%D9%86%D9%87%D8%A7-%D8%AF%D8%A7%D8%B1%D9%86%D8%AF

[58] https://www.bbc.com/persian/iran-features-55666032

[59] https://www.trmlabs.com/resources/blog/inside-the-nobitex-hack-how-the-iran-israel-conflict-exposed-tehrans-grip-on-its-crypto-services

[60] https://www.ncr-iran.org/en/publications/special-reports/bitcoin-mining-in-iran-irgc-operations-and-the-power-grid-crisis/

[61] https://enghelabe-eslami.de/69355/

units and Ministry of Energy personnel who sought to shut down an unlicensed mining facility.[62]

However, it is important to clarify that a significant portion of the information regarding the extent of the IRGC's direct involvement in the sector is based on sources that cannot be fully independently verified, and sometimes originates from opposition figures and regime dissidents.

In conclusion, Iran's crypto mining industry has evolved over the past decade from a marginal industry into an official significant sector. This development is characterized by a unique combination of governmental regulation, economic incentives, concealment, and, likely direct involvement of state and security bodies. This combination, which brings together formal recognition of the technology with covert practices, demonstrates the potential for using cryptographic assets as an essential strategic component in Iran's sanctioned economy.

Beyond leveraging crypto mining as a strategic revenue source, Iran also utilizes cryptographic assets to address foreign trade restrictions. The next section will examine the official uses of digital assets by state institutions as a tool for sanctions evasion, with an emphasis on financing goods imports, and will analyze the regulation, implementation, and challenges involved in this activity.

[62] https://www.meforum.org/mef-observer/how-irans-cryptocurrency-gamble-empowers-the-revolutionary-guards-and-drains-the-state ; https://www.dw.com/fa-ir/a-57653344

Section 6: Use of Cryptographic Assets for Goods Import and Development of Blockchain Platforms for International Trade

The economic sanctions imposed on Iran and the increasing difficulties in accessing the international financial system have led Iran to become one of the first countries to regulate the use of cryptographic assets for foreign trade purposes. This activity was formalized in 2022 through Central Bank of Iran (CBI) directives allowing for the import of goods using cryptographic assets.[63]

The CBI's directives regulated the use of these assets for import, while prohibiting their use as an internal means of payment. The rules further stipulate that only authorized entities, including licensed miners and non-oil exporters, are permitted to provide their cryptographic assets for import payments. It was also determined that the permitted quantity of assets for import activity would require approval from the Ministry of Industry, Mine and Trade (MIMT) in cooperation with the CBI. Additionally, cryptographic assets permitted for import use would be officially designated in a list of assets approved and published by the CBI. Furthermore, it was stipulated that import activity would only be allowed on exchanges that receive formal accreditation for this purpose. Estimates at the time of the directives' publication suggested that import activities would be carried out through the governmental import management system–ntsw.ir–in conjunction with a declaration on the customs website (epl.irica.gov.ir).[64]

In August 2022, Iran reported its first import transaction executed using cryptographic assets. According to publications, this involved a vehicle import deal totaling $10 million.[65] Deputy Minister of Industry, Alireza Peyman Pak, tweeted about this inaugural import transaction, noting that by September, the use of cryptographic assets and smart contracts would be widespread in foreign trade with target countries.[66]

Later reports claimed that the Deputy Minister announced Iran was developing a platform to provide Iranian traders with access to cryptographic assets originating from trade activities with Member States of the Eurasian Economic Union (EAEU) (Russia, Belarus, Armenia, Kazakhstan, and Kyrgyzstan). The same report stated that the Minister of Industry, Seyyed Reza Fatemi Amin, indicated that the approval of government

[63] https://www.radiofarda.com/a/iran-to-use-cryptocurrency-to-imports/32008640.html
[64] https://tajeroon.com/digital-currency-import-guide/;
https://www.heyvalaw.com/web/articles/view/3793/
[65] https://arzdigital.com/blog/iran-makes-first-import-order-using-cryptocurrency/
[66] https://borna.news/fa/news/1361888/

regulations concerning cryptographic assets would allow any importer to use Bitcoin instead of dollars and euros.[67]

One of the primary challenges in assessing the effectiveness and scope of Iran's policy in this area pertains to the absence of official data. Nevertheless, there is a potentially interpretable reference from the CBI, indicating that crypto-related transactions amounted to approximately $197.6 million in the second quarter of the fiscal year (likely referring to the Iranian year 1402). This figure, significantly lower than the total volume of funds that flowed into Iranian exchanges during the same year (approximately $3 billion), may suggest that it refers to specific aspects of governmental crypto activity, whether the volume of mining managed by state entities, or the extent of imports financed through these means.[68]

It is important to emphasize that the lack of transparency supports the possibility that this is intended to obscure its scope from the international community, aiming to reduce the risk of secondary sanctions being imposed on entities that might cooperate with this sanction-circumventing trade infrastructure.

Development of National Blockchain Infrastructures

Alongside the use of cryptographic assets, there are reports that Iran is developing its own blockchain platforms and cryptographic assets. The development of these systems may indicate a readiness to use them for international trade under sanctions restrictions. Reports detail two major projects in this area: the Kuknos network and Project Borna.

The Kuknos network is an initiative by leading Iranian banks (Mellat, Melli, Pasargad, Parsian), to offer a range of services including a gold-backed cryptographic asset,PayMon (PMN), where each token equals 0.001 grams of 24-carat gold, a digital wallet, an NFT platform, and a decentralized exchange (DEX) infrastructure. Its technological infrastructure, operational model, and legal considerations underscore an intention and capacity to operate in the international arena and support global asset trading on the network. It is crucial to note that PMN cannot be used as a means of payment itself, but only for fee payments or for assessing the value of other tokens operating on this network.[69] As of the Iranian year 1402 (March 21, 2023 – March 19, 2024), one million tokens of the currency had been issued and are traded on Iranian

[67] https://www.radiofarda.com/a/iran-to-use-cryptocurrency-to-imports/32008640.html

[68] https://www.trmlabs.com/resources/blog/iran-crypto-economy ; https://financialtribune.com/articles/business-and-markets/116953/renewed-majlis-call-for-reforming-crypto-rules https://financialtribune.com/articles/business-and-markets/116953/renewed-majlis-call-for-reforming-crypto-rules

[69] https://kuknos.ir/wp-content/uploads/2022/06/KUKNOS-Network-and-Paymon-Token-Whitepaper-v2.0.pdf

exchanges.[70] It is worth noting that this platform may support the Deputy Minister of Industry's statements that Iran is developing a platform to allow Iranian traders access to cryptographic assets originating from trade activity with Member States of the Eurasian Economic Union (EAEU).[71]

Project Borna is led by the CBI and is intended to serve as a central blockchain infrastructure for the Iranian banking and financial system, emphasizing its suitability for international activity. The flagship project of this system is the "Digital Rial" (Central Bank Digital Currency—CBDC), which is reportedly in its pilot phase.[72] This project's suitability for the international environment may support the Iranian effort to build independent financial systems to enable it to circumvent international restrictions and conduct foreign trade efficiently.

Alongside the development of these local platforms, there are reports of advanced discussions between Iran and Russia concerning the development of a new gold-backed stablecoin, intended to serve as a means of payment in cross-border trade between the two countries. This initiative, if it materializes, would constitute another layer in Iran's and Russia's efforts to build an independent financial infrastructure that enables them to circumvent international sanctions and expand their economic cooperation.[73]

These projects illustrate Iran's strategic approach to creating cryptographic financial solutions that will strengthen its economic independence and enable the continuation of essential trade activities.

In summary, the policy of using cryptographic assets for import and developing cryptographic infrastructures demonstrates how Iran seeks to harness decentralized and unregulated technology to create a sanction-circumventing foreign trade channel. This represents one of the world's most prominent cases of regulated governmental integration of cryptographic assets to bolster economic sovereignty under conditions of international financial isolation. Beyond these economic and civilian objectives, and in light of urgent funding needs enforced by sanctions, there is also increasing involvement of Iranian security bodies in the crypto domain. The next section will address the security uses of cryptographic assets, with an emphasis on sanction-circumventing oil activities, arms procurement, and the financing of terrorist organization activities.

---

[70] https://www.iranicard.ir/blog/crypto/iranian-cryprocurrency/

[71] https://www.radiofarda.com/a/iran-to-use-cryptocurrency-to-imports/32008640.html

[72] https://www.trmlabs.com/resources/blog/iran-crypto-economy, https://cbdctracker.hrf.org/currency/iran

[73] https://cointelegraph.com/news/iran-and-russia-want-to-issue-new-stablecoin-backed-by-gold ; https://www.trmlabs.com/resources/blog/iran-crypto-economy

Section 7: Financing Security Forces' Budgets through Cryptographic Assets

This section will analyze the strategic use of cryptographic assets by Iranian security bodies, with an emphasis on the Islamic Revolutionary Guard Corps (IRGC) and the Quds Force. Within this framework, we will review sanctions designations by the U.S. Department of the Treasury (OFAC) and Israel's National Bureau for Counter Terror Financing (NBCTF)[74] which provide concrete examples of the extensive use of cryptographic assets by these entities for arms procurement, terrorist financing, and extortion through ransomware attacks. Furthermore, this section delves into the Nobitex case, which appears to be a state infrastructure also utilized by security bodies for sanctions evasion and financing terror activities.

The Security Forces' Oil Budget

A 2025 report from the Majlis Research Center, the research arm of the Iranian Parliament, analyzing the budget bill for the Iranian year 1404 (corresponding to March 2025 - March 2026), indicates that oil allocations for the armed forces will amount to 550,000 barrels per day during this year. This quantity represents approximately 30% of the total oil designated for export (1.8 million barrels), with an estimated value of $12.4 billion.[75]

This funding mechanism evolved in response to economic pressures and sanctions imposed on Iran, which hindered its ability to acquire the foreign currency necessary for its security forces for arms and arms component procurement, as well as for financing the activities of terrorist organizations operating under their patronage.

These commercial activities are conducted by the security bodies through a network of shell companies,[76] shadow banking,[77] and clandestine maritime transfers, enabling them to sell oil, mostly to China.[78]

---

[74] National Bureau for Counter Terror Financing

[75] https://report.mrc.ir/article_10440.html

[76] https://home.treasury.gov/news/press-releases/sb0159 ; https://home.treasury.gov/news/press-releases/sb0191

[77] https://home.treasury.gov/news/press-releases/sb0159

[78] https://www.eia.gov/international/content/analysis/special_topics/SHIP_Act/SHIP-Act_2025.pdf

Sanctions Evasion and Terrorist Financing through Cryptographic Assets: Examples from U.S. Department of the Treasury (OFAC) Designations and Israel's National Bureau for Counter Terror Financing (NBCTF)

Growing evidence of the extensive use of cryptographic assets, particularly USDT, by Iranian security bodies can be found in a series of recent designations by the U.S. Department of the Treasury (OFAC) and Israel's NBCTF:

On March 26, 2024, OFAC exposed a large-scale financial network operated by Tawfiq Muhammad Sa'id al-Law, a Syrian-Lebanese currency exchanger operating from Beirut, who plays a central role in the financial infrastructure of the Quds Force. In his activities, al-Law provided financial services to Iranian-backed terrorist organizations by operating digital wallets used to receive proceeds from the sale of Iranian oil in USDT, which were then transferred to known terrorist entities linked to Hezbollah.[79] This designation followed a previous action by Israel's NBCTF, which, in June 2023, seized $1.7 million in cryptographic assets identified with al-Law.[80] An analysis by TRM Labs of one of the wallets found that it was involved in over a thousand transactions totaling tens of millions of dollars, most of which were in USDT.[81]

On December 19, 2024, OFAC revealed an extensive financial network through which hundreds of millions of dollars in digital assets flowed between financial networks controlled by the Quds Force and Iranian-backed terrorist organizations, including the Houthis in Yemen, Hezbollah in Lebanon, and entities linked to Hamas.[82] The central figure exposed in the report, Sa'id al-Jamal, acted as the primary finance facilitator for the Houthi network and was identified as directly subservient to the IRGC's Quds Force. Al-Jamal managed a complex network of shell companies, oil tankers, and informal banking infrastructures, used for selling Quds Force oil, the proceeds of which were stored in five digital wallet addresses. Analysis of these addresses showed that over $178 million, mostly in USDT, flowed through them over a one-year period.[83]

On April 2, 2025, OFAC uncovered an extensive financial and logistical network operating on behalf of the Houthis in coordination with Iran's Quds Force, through which arms and goods procurement transactions were conducted using cryptographic assets. The

[79] https://home.treasury.gov/news/press-releases/jy2209

[80] https://nbctf.mod.gov.il/en/pages/28062023EN.aspx; https://www.chainalysis.com/blog/israel-nbctf-hezbollah-iran-quds-crypto-seizure/

[81] https://www.trmlabs.com/resources/blog/us-treasury-sanctions-terrorist-financier-for-providing-crypto-related-services-to-hezbollah

[82] https://ofac.treasury.gov/recent-actions/20241219; https://home.treasury.gov/news/press-releases/jy2757

[83] https://www.chainalysis.com/blog/ofac-highlights-hundreds-of-millions-of-dollars-in-cryptocurrency-transactions-related-to-irgc-connected-houthi-financier-said-al-jamal/

network included, among others, brothers Sohrab and Hushang Ghairat, Afghan citizens operating from Russia under the direction of Sa'id al-Jamal—a key figure in the financing apparatus of numerous Iranian proxies, particularly the Houthis. The report points to eight crypto addresses (six private wallets and two addresses at centralized services) through which nearly $1 billion was transferred. A significant portion of the activity was conducted through the Russian Garantex exchange, which had previously been sanctioned. Additionally, these wallets were found to have processed approximately $2.5 million linked to addresses designated by Israel's NBCTF as involved in Hamas financing.[84]

On September 1, 2025, the Israeli Minister of Defense signed an order authorizing the seizure and forfeiture of assets held in 187 cryptocurrency wallets that belonged to, or were used in connection with, activities of the Iranian Revolutionary Guard Corps (IRGC).[85] As part of this operation, 1.5 million USDT were frozen in these wallets at the time of the seizure.[86]

An analysis conducted by the company Elliptic of the transactions carried out through these wallets found that the total volume of activity amounted to approximately 1.5 billion USD. However, the company noted that it is not possible to determine that the entire amount was used by the IRGC, as some of the wallets may have served as infrastructure for providing cryptocurrency services to multiple clients.[87]

On September 11, 2025, the U.S. Department of Justice (District of Massachusetts) filed a request for the forfeiture of approximately 580,000 USDT stored in a digital wallet allegedly controlled by Mohammad Abedini, the owner of San'at Danesh Rahpooyan Aflak Co. (SDRA)—an Iranian company that manufactures navigation modules used in the IRGC's military drone program.[88]

On September 14, 2022, OFAC exposed an IRGC-affiliated infrastructure responsible for a long series of cyber and ransomware attacks carried out against entities in the U.S. and worldwide, including municipalities and healthcare institutions.[89] In 2022, this group led two extensive ransomware attacks on governmental services in Albania, an action that

[84] https://home.treasury.gov/news/press-releases/sb0068 ; https://www.chainalysis.com/blog/ofac-sanctions-houthi-network-crypto-money-laundering-russia-april-2025/
[85] https://nbctf.mod.gov.il/he/Announcements/Documents/%d7%a6%d7%aa%2043-25.pdf
[86] https://www.elliptic.co/blog/israel-links-crypto-wallets-handling-billions-to-irans-revolutionary-guard
[87] https://www.elliptic.co/blog/israel-links-crypto-wallets-handling-billions-to-irans-revolutionary-guard
[88] https://www.justice.gov/usao-ma/pr/united-states-seeks-civil-forfeiture-cryptocurrency-associated-iranian-national-mohammad
[89] https://home.treasury.gov/news/press-releases/jy0948

led to the severance of diplomatic relations between the countries.[90] The OFAC report included details of seven digital wallets owned by two members of the infrastructure, Ahmad Khatibi Aghda and Amir Hossein Nikaeen Ravari.[91] An analysis by Chainalysis of six of these wallets supported the possibility that they were involved in ransomware attacks that yielded approximately $230,000, which was ultimately funneled to the Iranian Nobitex exchange.[92]

The Nobitex Case: Exposure to the Regime's Obfuscation Mechanisms

On June 19, 2025, a hacking group identified as Gonjeshke Darande (Predatory Sparrow), issued a statement claiming responsibility for a breach of Nobitex, Iran's largest and most central crypto exchange, in which they asserted digital assets worth approximately $90 million were destroyed. The hackers claimed the operation's objective was to disrupt the crypto infrastructure serving the regime and the IRGC.[93] Shortly after the breach was announced, the attackers leaked technical documents related to the exchange's operations, including the full source code, infrastructure documentation, and R&D on privacy.[94]

A Chainalysis analysis indicated that the stolen assets were transferred to burner addresses in a manner that precludes technical recovery, a move that supports the attackers' claims that the breach's purpose was not financial gain.[95]

Chainalysis and Elliptic reports, in this context, noted that Nobitex has for years served as a strategic platform for circumventing U.S. sanctions by the IRGC, and is identified by financial users in their regional proxies, including Hamas, Palestinian Islamic Jihad, and the Houthis in Yemen.[96]

[90] https://mcclain.house.gov/_cache/files/3/d/3d4e9480-81ce-4c23-8492-abf1e8ee85df/703BE2708834B0FCBA56D3B03A73324C.condeming-iranian-cyberattack-on-albania10.7.pdf
[91] https://ofac.treasury.gov/recent-actions/20220914
[92] https://www.chainalysis.com/blog/ofac-sanctions-iran-september-2022/
[93] https://www.nbcnews.com/world/middle-east/hackers-attack-irans-largest-crypto-exchange-destroying-90-million-rcna213920
[94] https://www.mitrade.com/au/insights/news/live-news/article-3-901581-20250619
[95] https://www.chainalysis.com/blog/nobitex-iranian-exchange-exploit-june-2025/
[96] https://www.elliptic.co/blog/iranian-crypto-exchange-nobitex-hacked-pro-israel-group

In this regard, it is worth noting that in an interview with Amir Hossein Rad, one of Nobitex's founders,[97] he stated that one of the platform's inherent advantages for the Iranian economy is its ability to be used for sanctions evasion.[98]

An investigation published following the Nobitex attack by an Iranian blogger named Nariman Gharib reportedly revealed an infrastructure used to transfer $800 million in USDT belonging to Iranian security bodies through Nobitex. This infrastructure, he claimed, was managed by an individual named Shahram Zakeri, who operated on the exchange via a dedicated (VIP) track exempt from Know Your Customer (KYC) checks, with his activity conducted without document verification, source of funds authentication, or any record of his activity, contrary to the standard procedures applicable to regular clients. This preferential treatment, according to Gharib, points to cooperation between Nobitex and Iranian security entities, positioning the exchange as an active partner in large-scale money laundering for these bodies.[99]

An analysis conducted by TRM Labs of the exchange's code and leaked documents supports, at least in part, Nariman Gharib's findings, providing extensive insight into the unique characteristics of this trading platform, which strengthens the assessment that it is used by state entities on a significant scale.

TRM Labs' investigation findings indicated that Nobitex developed unique mechanisms to maintain the confidentiality of certain clients' activities. These mechanisms include tools for encryption, mixing, and user identity camouflage, designed to enable evasion of monitoring by Western enforcement and compliance bodies and advanced blockchain analytics tools. This determination is supported by internal documentation attesting to an official strategy seeking to develop dedicated tools to elude monitoring by global compliance bodies, with an emphasis on the U.S. Financial Crimes Enforcement Network (FinCEN).

Similar to Gharib's claim, the TRM report also identified special operational paths within the system for preferred users (VIPs), intended to grant sensitive entities—likely including security bodies—exemption from identity and tracking checks. As part of obscuring such transactions, the platform supported over 25 blockchain networks, including TRON, Ethereum, Solana, and TON, which allowed specific users to transact through them, an action that complicates enforcement and compliance in identifying suspicious activity patterns.

---

[97] Nobitex's founders reportedly include Amir Hossein Rad, Amir Ali Akbari, Seyed Mohammad Ali Aghamir, and Mohammad Aghamir.

[98] https://shanbemag.com/interview-with-amir-hossein-rad-nobitex/

[99] https://blog.narimangharib.com/posts/2025%2F06%2F1750718297586?lang=fa&s=08

In conclusion, the report's authors note that the modularity of the source code allows for rapid replication of the system—including the trading engine and obfuscation capabilities—raising concerns about the dissemination of this architecture to other sanctioned countries and entities, aimed at evading international compliance bodies.[100]

It thus appears that the Nobitex breach provided a rare glimpse into an operational structure designed to circumvent the international economic system using blockchain technologies.

Crypto as a Strategic Pillar in Iranian Security

These findings illustrate the process of integrating cryptographic assets into Iran's security financing apparatus, where they no longer play a purely technical role but constitute an essential pillar of an alternative financing strategy. This strategy enables cross-border operations, obfuscation of user identities, and avoidance of the international financial oversight system—thereby providing Iranian security bodies with considerable operational and economic flexibility.

[100] https://www.trmlabs.com/resources/blog/inside-the-nobitex-breach-what-the-leaked-source-code-reveals-about-irans-crypto-infrastructure

Section 8: The Russian Case

The expanded use of cryptographic assets by sanctioned countries is not unique to Iran. Russia, which, similarly to Iran, initially expressed reservations about this domain, has since 2022 begun to formulate a more overt policy in response to the economic sanctions imposed following its invasion of Ukraine. Like Iran, Russia is also developing decentralized financial mechanisms designed to circumvent trade restrictions, maintain capital flow, and strengthen economic sovereignty.

Both countries exhibit a complex approach: on one hand, recognizing the strategic potential of cryptographic technologies for geo-economic purposes; on the other, harboring concerns about undermining sovereign control and losing monetary authority. These responses have manifested in a dual policy: combining stringent regulation with selective adoption of decentralized infrastructures under supervision.

This section will examine Russian policy, its regulatory and legislative efforts, and initiatives for developing asset-backed currencies—with a concise comparison to Iran to identify a shared pattern of action by isolated states turning to decentralized solutions as a component in reshaping the global financial order.

Timeline

August 2020: A law was enacted regulating the legal status of various types of digital assets, including decentralized cryptographic assets (Цифровая валюта / Криптовалюта). This law recognized their status as property but prohibited their use as a means of payment for goods, works, or services within the Russian Federation.[101]

January 2022: The Central Bank of Russia published a public consultation paper titled "Cryptocurrencies: Trends, Risks, Measures."[102] In this paper, released approximately one month before the outbreak of the war with Ukraine, the Central Bank called for a sweeping ban on most activities related to cryptographic assets, including stablecoins. This was despite Russia's prominent position in the global crypto arena, both in terms of adoption among its population and its relative share in global mining.[103] Notwithstanding this popularity, the Russian Central Bank proposed prohibiting the use of cryptographic assets as a means of payment, imposing a ban on the issuance, organization, and trading of cryptographic assets by exchanges and P2P platforms in Russia, and even called for a complete ban on crypto mining within its territory. The justifications for this policy centered on four areas: protecting investors from speculative assets, the use of cryptographic assets in criminal activity, undermining the ability to conduct monetary

[101] https://base.garant.ru/74451466/
[102] https://cbr.ru/Content/Document/File/132241/Consultation_Paper_20012022.pdf
[103] https://www.chainalysis.com/blog/eastern-europe-cryptocurrency-market-2020/

policy, and high energy costs posing a risk to electricity supply for residential, social infrastructures, and industrial facilities, alongside environmental damage.[104]

February 2022: Russia initiates war with Ukraine, leading to the imposition of extensive sanctions.

April 2022: The U.S. Department of the Treasury (OFAC) imposes sanctions on Garantex, an exchange operating from Russia, for assisting criminal actors operating on the Darknet.[105]

May 2022: The UK imposes sanctions on Garantex for supporting and assisting Russia in sanctions evasion.[106]

May 2022: The VEB Institute of Research and Expertise (Институт исследований и экспертизы ВЭБ) publishes a series of recommendations for confronting international sanctions. Within this framework, it suggests exploring the opening of sister or affiliated crypto exchanges in Commonwealth of Independent States (CIS) countries not under sanctions (Armenia, Kazakhstan, Kyrgyzstan), or in free economic zones in the United Arab Emirates and Oman. It also proposes issuing a gold-backed stablecoin, named "Gold Ruble," primarily for settling international transactions. Additionally, it suggests developing an international clearing system for national central bank digital currencies (CBDCs) with friendly countries, based on distributed ledger technologies.[107]

August 2022: Against the backdrop of international sanctions, Russian Prime Minister Mikhail Mishustin clarified that "serious fine-tuning" of the Russian financial system was required to ensure continuity and flexibility in international trade mechanisms. In this statement, he emphasized the need to develop and activate digital assets to ensure continuity in payment mechanisms for Russia's foreign trade activities, noting digital assets as a "safe alternative for all parties" that can guarantee payment continuity within this activity.[108]

---

[104] https://cbr.ru/Content/Document/File/132241/Consultation_Paper_20012022.pdf

[105] https://home.treasury.gov/news/press-releases/jy0701 ; https://www.trmlabs.com/resources/blog/eu-includes-crypto-exchange-garantex-in-16th-sanctions-package-on-russia

[106] https://assets.publishing.service.gov.uk/media/6419b742d3bf7f7ff9a35d0b/Notice_Russia_210323.pdf

[107] https://d-russia.ru/wp-content/uploads/2022/06/inst_deb_xltr.pdf

[108] https://www.rbc.ru/finances/30/08/2022/630df51a9a7947e33f312664

November 2022: A draft law is submitted to the Russian Parliament (Duma) seeking to regulate mining activity in Russia. It establishes a licensing requirement while prohibiting the use of mined assets within Russia.[109]

February 2024: The Russian Central Bank continues to exercise caution regarding the use of cryptographic assets, with Deputy Head of the Central Bank, Olga Polyakova, noting that investing in cryptocurrencies carries significant risks and that the Central Bank does not view them as a means of payment within Russia.[110]

February 2024: The Russian Parliament adopts legislation regulating international trade activity through the use of digital rights (цифровые права).[111] Among the possible associated rights for these assets are monetary rights, participation rights, and conversion rights. Furthermore, these rights may be backed by assets such as cash, metals, and real estate, making these assets similar to stablecoins.[112] This legislation aims to facilitate Russian international trade activities, which have been affected by the imposed sanctions. Within this framework, the Central Bank was granted authority to regulate these transactions. Additionally, the law obliges issuers of these rights to provide the Central Bank with information on beneficiaries and to maintain a dedicated database detailing all transactions.[113]

March 2024: The Russian Ministry of Energy presented a draft governmental decree aimed at reducing electricity consumption volumes stemming from cryptographic asset mining. This proposal comes against the backdrop of Russia being the world's second-largest country in terms of cryptographic asset mining volume, a fact that has led to a growing burden on the national electricity system. The proposed measures included authorities to limit miners' ability to connect to the electricity grid in areas identified as sensitive to mining, increasing their service costs by 5–10 times, and restricting electricity supply to miners in case of grid overload.[114]

March 2024: The U.S. Department of the Treasury (OFAC) sanctioned a large number of entities (15) for their involvement in assisting Russia in sanctions circumvention. The activities of the designated entities included operating blockchain-based services, virtual

[109] http://duma.gov.ru/news/55775/
[110] https://www.rbc.ru/crypto/news/65cdb0319a79475200c7b679
[111] https://tass.ru/ekonomika/20094257 ; https://www.rbc.ru/crypto/news/65e840eb9a79478b24d4eaed
[112] https://cbr.ru/Content/Document/File/162005/analytical_report_10072024.pdf
[113] https://tass.ru/ekonomika/20094257 ; https://www.rbc.ru/crypto/news/65e840eb9a79478b24d4eaed
[114] https://www.rbc.ru/crypto/news/65fd73469a79478e52628601

currency payment services, and technology procurement to enable Russia to evade sanctions,[115]

July 2024: The Russian Central Bank publishes a report titled: *Stablecoins: Experience of Use and Regulation. Analytical Report.*[116] The report provides an overview of various aspects of stablecoins, including their uses and regulatory implications, with an emphasis on issues of financial stability, monetary sovereignty, and technological risks. It reiterates the existing prohibition on the use of these assets as a means of payment in Russia. However, the report identifies the inherent advantage of using stablecoins as a tool for cross-border financial activity. In this context, it points to the existing legal framework regarding the use of digital rights (цифровые права) that possess similar stable characteristics, enabling their use in international trade transactions.[117]

July 2024: The Parliament approves, in its third reading, the law regulating mining activity[118] and the law authorizing the Central Bank to establish an experimental legal regime to permit foreign trade transactions using cryptographic assets for a limited period of up to three years.[119]

October 2024: Elvira Nabiullina, Head of the Central Bank, announced that the first transactions within Russian foreign trade activity, to be conducted using digital assets under governmental regulation, are expected to commence by the end of 2024, as part of a three-year experimental regulatory environment. The objective of this initiative is to assess the feasibility of integrating cryptographic assets into Russia's foreign trade mechanisms, especially given the escalating sanctions. This report noted that the Minister of Finance claimed the legalization of mining would allow the use of mined output for foreign trade activities. It also mentioned that the Mining Association estimated at the beginning of the year that the value of mined output that could be used for foreign trade activities amounted to roughly 240 billion Rubles.[120] A few months later, the Minister of Finance confirmed that foreign trade transactions are indeed being conducted, with Russia using Bitcoin and other digital currencies.[121] Later reports in Western media support this statement by the Minister of Finance, noting that Russia uses a variety of cryptographic assets in its oil trade activities with China and India. These same sources

[115] https://home.treasury.gov/news/press-releases/jy2204

[116] Стейблкойны: опыт использования и регулирования. Аналитический доклад https://cbr.ru/Content/Document/File/162005/analytical_report_10072024.pdf

[117] https://cbr.ru/Content/Document/File/162005/analytical_report_10072024.pdf

[118] https://www.pnp.ru/economics/v-rossii-uzakonyat-mayning-kriptovalyut.html

[119] https://www.pnp.ru/economics/v-rossii-ustanovyat-pravila-ispolzovaniya-kriptovalyut.html

[120] https://www.rbc.ru/crypto/news/6710ccff9a794737949f07d5

[121] https://www.reuters.com/markets/currencies/russia-is-using-bitcoin-foreign-trade-finance-minister-says-2024-12-25/

indicate that while this constitutes a small share of total trade activity, this share is growing.[122]

October 2024: During a BRICS organization conference held in Kazan, Russia emphasized the need to strengthen BRICS' role in the international monetary system, expand interbank cooperation, and increase the use of national currencies in mutual trade, calling for concrete steps to establish a new international payment system.[123] At this conference, the "BRICS Pay" payment system was unveiled,[124] intended to serve the organization's member countries, utilizing blockchain technology and cryptographic assets, including central bank digital currencies (CBDCs) and BRICS Chain, a currency to be issued by the organization's member companies.[125]

February 2025: The European Union imposes sanctions on Garantex for providing financial services to Russian banks subject to European sanctions.[126]

June 2025: A report by the CIR Institute reveals a complex financial infrastructure that, according to the report's authors, is designed to enable Russia to circumvent the international sanctions regime imposed upon it.[127] Central to this activity are Ilan Mironovich Shor, a Moldovan politician and businessman sanctioned for his involvement in attempts to sway elections for the Russian government,[128] and the Russian Promsvyazbank (PSB), a state-owned bank sanctioned for its ties and services to Russia's military-industrial sector.[129]

The report indicates that these entities founded the A7 company in October 2024, with the stated goal of facilitating cross-border financial transfers for Russian clients in light of the sanctions imposed on Russia. In January 2025, these entities launched a ruble-backed stablecoin called A7A5 in Kyrgyzstan. The ruble backing is provided by deposits in this currency held at PSB. The primary purpose of A7A5 is to create a reliable "fiat gateway" that enables quick and inexpensive deposit and withdrawal of money to and

[122] https://www.reuters.com/business/energy/russia-leans-cryptocurrencies-oil-trade-sources-say-2025-03-14/
[123] https://neweconomy.expert/publications/255834/
[124] https://www.iuemag.com/inspi-news/inspi-writes/everything-you-need-to-know-about-brics-pay/
[125] https://www.coinbase.com/en-nl/price/brics-chain
[126] https://www.consilium.europa.eu/en/press/press-releases/2025/02/24/16th-package-of-sanctions-on-russia-s-war-of-aggression-against-ukraine-eu-lists-additional-48-individuals-and-35-entities/
[127] https://www.info-res.org/app/uploads/2025/06/A7A5-Report-June-2025-Final-Draft-1.pdf
[128] https://home.treasury.gov/news/press-releases/jy1049
[129] https://home.treasury.gov/news/press-releases/jy0602

from the crypto system, with easy conversion from Rubles to other cryptographic assets like USDT.

Initially, the token was listed for trading on the Garantex exchange, which is subject to U.S., British, and European sanctions. In March, U.S. law enforcement authorities froze Garantex assets totaling $26 million.[130] Shortly after this action, Garantex transferred large amounts of liquidity to A7A5 wallets on its platform, followed by a “burning and re-minting” process of over 4.5 billion A7A5 tokens. Upon completion of the process, Garantex transferred the new tokens to Grinex, a new exchange operating from Kyrgyzstan.

Throughout the months preceding this exposure, Russian government officials expressed support for the project, including by participating in conferences promoted by A7, while refraining from officially sponsoring it, and at times presenting it as a Kyrgyz project.[131]

In May 2025, the UK imposed sanctions on A7 due to its ties to the Russian government and its war in Ukraine.[132]

According to an August 2025 report by Chainalysis, this token processed a transaction volume exceeding $51.17 billion, with $1.47 billion of that processed through a decentralized exchange (DEX) and converted into dollar stablecoins, thereby creating a financial channel enabling sanctioned Russian banks to operate in global crypto markets.[133]

An examination of Russian policy in the cryptographic asset domain, as detailed above, illustrates how, similar to Iran, countries subject to external economic pressure are working to build alternative financial mechanisms through decentralized technologies. Russia, like Iran, employs controlled use of digital assets for sanctions evasion, attempting to balance state control with the adoption of innovative financial tools. In both countries, a recurring pattern is evident: selective regulation, a dual approach to public exposure to crypto, and the implementation of national initiatives to develop cryptographic infrastructures designed for foreign trade.

However, Russia operates within a different global framework—both in terms of economic scale, its network of international partnerships (such as BRICS), and the degree of public

---

[130] https://www.justice.gov/opa/pr/garantex-cryptocurrency-exchange-disrupted-international-operation

[131] https://ria.ru/20250618/a7-2023689316.html , https://iz.ru/1957719/video/razvitie-transgranichnykh-perevodov-obsudili-na-moskovskom-finansovom-forume

[132] https://search-uk-sanctions-list.service.gov.uk/designations/RUS2718/Entity?utm_content=&utm_medium=email&utm_name=&utm_source=govdelivery

[133] https://www.chainalysis.com/blog/charts-in-review-august-2025/

visibility of its actions. While Iran tends to act cautiously and secretly, Russia positions crypto as a declared policy tool with relatively high public visibility.

Furthermore, leading platforms in these countries have demonstrated a rapid recovery capability following significant events. For instance, the Iranian Nobitex exchange managed to resume operations shortly after a cyberattack caused tens of millions of dollars in damages;[134] Similarly, Russia's Garantex demonstrated impressive operational flexibility after U.S. authorities froze $26 million in its assets—a step that led to the relocation of its operations to the Kyrgyz Grinex. This exchange itself was recently designated as prohibited by the U.S. Department of the Treasury (OFAC) and the British HM Treasury.[135] The similarity between these cases points to a broader trend of moving from an "adaptation under sanctions" approach towards the active shaping of alternative financial infrastructures. This process, often referred to as the "whack-a-mole phenomenon" in regulatory reports, underscores the need for an advanced and coordinated regulatory approach to reduce the ability of states to circumvent sanctions through successor exchanges.

[134] https://www.trmlabs.com/resources/blog/inside-the-nobitex-hack-how-the-iran-israel-conflict-exposed-tehrans-grip-on-its-crypto-services

[135] https://home.treasury.gov/news/press-releases/sb0225 , https://www.gov.uk/government/news/uk-targets-sanctions-circumvention-and-crypto-networks-exploited-by-russia

Section 9: Summary and Discussion

The use of cryptographic assets by countries subject to international sanctions is evolving into a strategic activity. Decentralized technologies, primarily stablecoins, have become a central means of circumventing the international financial system, thereby eroding the effectiveness of traditional sanctions regimes. This research examines the systematic and extensive ways in which countries like Iran and Russia utilize cryptographic assets and discusses the economic, regulatory, and security implications of these trends. This section summarizes the research findings, discusses theoretical and practical implications, points out key limitations, and proposes directions for future research. Policy recommendations will be presented separately in Section 10.

Key Findings

The Iranian Case

- **Mining as a National Industry:** Iran regulated the crypto mining sector as early as 2019 with the aim of generating revenues and injecting foreign currency to be used for foreign trade activities.[136] However, pressure on electricity infrastructures led to the imposition of restrictions.[137]
- **Use of USDT and Local Exchanges:** Stablecoins, primarily USDT, have become a central component of Iranian trade activity.[138] This activity has largely been conducted through local exchanges like Nobitex, with state-level operations carried out under a veil of secrecy and obfuscation.[139]
- **Secrecy and Security Activity:** Iran maintains a compartmentalized approach to activity in this domain. According to official American and Israeli sources, and companies conducting blockchain activity analysis, Iran uses cryptographic assets both for financing the operations of security bodies and for funding terrorist organizations such as Hezbollah, the Houthis, and Hamas.[140]

---

[136] https://iranblockchain.org/wp-content/uploads/2021/03/%D8%A7%D9%84%D8%B2%D8%A7%D9%85%D8%A7%D8%AA-%D9%88-%D8%B6%D9%88%D8%A7%D8%A8%D8%B7-%D8%AD%D9%88%D8%B2%D9%87-%D8%B1%D9%85%D8%B2%D8%A7%D8%B1%D8%B2.pdf

[137] https://www.reuters.com/technology/iran-uses-crypto-mining-lessen-impact-sanctions-study-finds-2021-05-21/

[138] https://www.chainalysis.com/blog/crypto-crime-sanctions-2025/ ; https://tajeroon.com/digital-currency-import-guide/; https://www.heyvalaw.com/web/articles/view/3793/

[139] https://www.chainalysis.com/blog/nobitex-iranian-exchange-exploit-june-2025/; https://www.trmlabs.com/resources/blog/inside-the-nobitex-hack-how-the-iran-israel-conflict-exposed-tehrans-grip-on-its-crypto-services

[140] https://home.treasury.gov/news/press-releases/jy2209 ; https://nbctf.mod.gov.il/en/pages/28062023EN.aspx; https://www.chainalysis.com/blog/israel-

The Russian Case

- **Shift from Reservation to Overt Adoption:** The Russian Central Bank's fundamental policy remains reserved regarding the regulation of cryptographic activity in the Russian economy.[141] Nevertheless, in light of the sanctions imposed on it, Russia adopted an experimental regime in 2024 that permits controlled use of cryptographic assets for foreign trade transactions.[142] This trend was also examined in a recent RAND study, which focused on Russia's adaptation to using cryptocurrencies in light of sanctions restrictions. RAND's findings illuminate the practical aspects of Russian policy, while this research adds a comparative dimension, examining parallel trends and similar developments in Iran, alongside a discussion of broader implications for the stablecoin market and proposals for international policy.[143]
- **Development of Alternative Infrastructures:** The Russian state-owned bank, Promsvyazbank (PSB), issued a ruble-backed stablecoin, A7A5, intended to serve as a "fiat gateway" for sanctions evasion.[144] As detailed in Section 8, this activity illustrates the Russian strategy for preserving economic sovereignty. According to a Chainalysis report, the token processed $51.17 billion in transaction volume, with $1.47 billion of that processed through a decentralized exchange (DEX) and converted into dollar stablecoins, thereby creating access to global crypto markets. This activity, concentrated during business days (Monday-Friday), reflects commercial use aimed at enabling sanctions circumvention.[145]
- **International Frameworks:** Russia is promoting alternatives to traditional payment systems and the dominance of the U.S. dollar in the international arena (BRICS Pay, BRICS Chain, Central Bank Digital Currencies–CBDCs), with a

nbctf-hezbollah-iran-quds-crypto-seizure/ ; https://www.trmlabs.com/resources/blog/us-treasury-sanctions-terrorist-financier-for-providing-crypto-related-services-to-hezbollah ; https://ofac.treasury.gov/recent-actions/20241219; https://home.treasury.gov/news/press-releases/jy2757 ; https://www.chainalysis.com/blog/ofac-highlights-hundreds-of-millions-of-dollars-in-cryptocurrency-transactions-related-to-irgc-connected-houthi-financier-said-al-jamal/ ; https://home.treasury.gov/news/press-releases/sb0068 ; https://www.chainalysis.com/blog/ofac-sanctions-houthi-network-crypto-money-laundering-russia-april-2025/

[141] https://cbr.ru/Content/Document/File/132241/Consultation_Paper_20012022.pdf

[142] https://tass.ru/ekonomika/20094257 ; https://www.rbc.ru/crypto/news/65e840eb9a79478b24d4eaed ; https://www.pnp.ru/economics/v-rossii-ustanovyat-pravila-ispolzovaniya-kriptovalyut.html

[143] https://www.rand.org/pubs/commentary/2025/08/russias-use-of-crypto-schemes.html

[144] https://www.info-res.org/app/uploads/2025/06/A7A5-Report-June-2025-Final-Draft-1.pdf

[145] https://www.chainalysis.com/blog/charts-in-review-august-2025/

declared aim to challenge dollar hegemony and build an alternative monetary order.[146]

Common Characteristics and Comparison Use of Stablecoins

Both countries show a preference for stable-value assets for international trade, seeking to avoid volatility.[147]

- **Dual Regulation:** Both use a combination of restrictive regulation and controlled governmental adoption, distinguishing between public and private uses.[148]
- **Differing Approaches to Disclosure:** While Iran operates with a low profile, Russia operates within a declared legal framework as part of an overt effort to build an alternative financial infrastructure to the existing one.[149]

Sanctioned Decentralized Economies

The research proposes a model to explain the emerging dynamic:

- **Decentralized Financial Sovereignty:** Cryptographic assets enable countries direct access to international trade while reducing dependence on traditional banking systems.
- **Global Oversight Gaps:** The lack of regulatory uniformity creates gaps that states exploit for systematic evasion of enforcement mechanisms.

---

[146] https://neweconomy.expert/publications/255834/ ; https://www.iuemag.com/inspi-news/inspi-writes/everything-you-need-to-know-about-brics-pay/ ; https://www.coinbase.com/en-nl/price/brics-chain

[147] https://www.info-res.org/app/uploads/2025/06/A7A5-Report-June-2025-Final-Draft-1.pdf ; https://www.trmlabs.com/resources/blog/iran-crypto-economy ; https://iranblockchain.org/wp-content/uploads/2025/01/%D9%85%D9%82%D8%A7%D9%84%D9%87-%D8%A8%D8%B1%D8%B1%D8%B3%DB%8C_%D8%AA%D8%A7%D8%AB%DB%8C%D8%B1_%D8%B1%D9%85%D8%B2%D8%A7%D8%B1%D8%B2%D9%87%D8%A7_%D8%A8%D8%B1_%D9%82%DB%8C%D9%85%D8%AA_%D8%A7%D8%B1%D8%B2_%D8%AF%D8%B1_%DA%A9%D8%B4%D9%88%D8%B1.pdf ; https://cdn.arz.digital/ad-cnt/main/2025/03/Arzdigital-Annual-Report-1403-pdf.pdf

[148] https://iranblockchain.org/wp-content/uploads/2021/03/%D8%A7%D9%84%D8%B2%D8%A7%D9%85%D8%A7%D8%AA-%D9%88-%D8%B6%D9%88%D8%A7%D8%B5%D8%B7-%D8%AD%D9%88%D8%B2%D9%87-%D8%B1%D9%85%D8%B2%D8%A7%D8%B1%D8%B2.pdf ; https://www.pnp.ru/economics/v-rossii-uzakonyat-mayning-kriptovalyut.html ; https://www.pnp.ru/economics/v-rossii-ustanovyat-pravila-ispolzovaniya-kriptovalyut.html

[149] https://www.pnp.ru/economics/v-rossii-uzakonyat-mayning-kriptovalyut.html ; https://www.pnp.ru/economics/v-rossii-ustanovyat-pravila-ispolzovaniya-kriptovalyut.html ; https://www.trmlabs.com/resources/blog/inside-the-nobitex-hack-how-the-iran-israel-conflict-exposed-tehrans-grip-on-its-crypto-services

- **Secrecy:** The use of advanced tools that allow for obfuscation of activity and maintenance of confidentiality.

Implications

Economic Implications

- **Undermining Dollar Hegemony:** Initiatives like A7A5 and BRICS indicate signal a clear trend towards seeking an alternative to American financial dominance.
- **Changing Trade Patterns:** In Iran and Russia, some energy transactions (e.g., with China and India) are conducted in crypto—a move that indicates a potential shift in dollar-based international trade patterns.

Regulatory Implications

- **Challenge for Financial Regulators:** Decentralized exchanges, the use of mixers, and the transfer of activity between countries make monitoring and enforcement difficult.
- **Regulatory Gaps Between Countries:** Russia's overt approach versus Iran's clandestine approach highlights the need for uniform international regulation for cryptographic assets, particularly for stablecoins and the activities of Virtual Asset Service Providers (VASPs).
- **Recent Events Illustrate the Difficulty of Targeted Enforcement:** The Garantex exchange, which was central to Russian crypto activity, transferred significant liquidity to Grinex in Kyrgyzstan after its assets worth tens of millions of dollars were frozen. Shortly thereafter, Grinex itself was designated as a prohibited entity by the U.S. Department of the Treasury (OFAC) and the British HM Treasury. This sequence illustrates the "whack-a-mole phenomenon," where the closure of one venue leads to the almost immediate emergence of an alternative, underscoring the need for a coordinated and systemic regulatory approach.

Security Implications

- **Financing Illicit Activity:** The use of decentralized assets by states and terrorist actors complicates financial intelligence gathering and challenges the existing global order.

Research Contribution

This research provides a new theoretical framework for understanding the interplay between financial technology and international sanctions.

- **A New Theoretical Model:** "Sanctioned Decentralized Economies," as a conceptualization of the operating methods of isolated states.

- **"Dual Identity:"** Local regulation restricting civilian use due to concerns about undermining monetary sovereignty, while simultaneously developing and promoting governmental infrastructures for sanctions evasion.
- **Rich Empirical Documentation:** Based on official materials, up-to-date research reports, and Persian and Russian sources (machine translation).

Limitations and Future Research Directions

Main Limitations

- **Lack of Transparency:** Crypto activity in Iran and Russia is conducted with relative secrecy, making it difficult to assess the phenomenon's full extent.
- **Reliance on Secondary Sources:** Much information comes from commercial analytics firms' reports or journalistic sources.
- **Translation Challenges:** Materials in Persian and Russian required machine translation, which could impact the accuracy of content understanding.

Future Research Directions

- **Comparison to Additional Cases:** Venezuela, North Korea—diverse uses of cryptographic techniques for sanctions evasion.
- **Empirical Examination of the Phenomenon's Scope:** Development of an economic model to assess the phenomenon's extent and direction of development.
- **Obfuscation Technologies (Mixers, Chain Hopping):** Their impact on international enforcement.
- **Examination of Regulatory Bodies' Responses:** Such as the Financial Action Task Force (FATF), OFAC, and the European Union—policy, legislation, and implementation.

Conclusion

The increasing use of cryptographic assets by sanctioned countries is no longer a marginal phenomenon but a calculated strategic move with the structural potential to destabilize the global financial order. Iran and Russia, each in their own way, have developed creative mechanisms for sanctions evasion, utilizing decentralized technologies to create an extra-banking economy. Understanding this dynamic is crucial for formulating a coordinated state and international response to the era of decentralized finance. Section 10 will propose practical directions for shaping this policy.

Section 10: Policy Recommendations

The use of cryptographic assets for sanctions evasion, with a focus on Iran and Russia, has exposed the limitations of sanctions regimes in the cryptographic era. The research findings (Sections 2–9) demonstrate that decentralized technologies enable the management of a "Sanctioned Decentralized Economy," exploiting regulatory gaps in the crypto market for sanctions circumvention and terrorist financing. This Section offers recommendations for improving state capabilities, fostering cooperation with the FinTech industry, advocating for uniform regulation, and closing the Static Designation Gap through cluster-level enforcement and real-time cross-jurisdictional designation infrastructure.

Policy Recommendations

Improving State Capabilities: Personnel and Tools

The increasing sophistication of the crypto industry necessitates strengthening the personnel and technological tools of Western enforcement agencies, which currently rely on commercial tools with limited analytical capabilities.

- **Establishment of Dedicated Units:** Units such as the Virtual Assets Unit operating within the FBI, comprising blockchain experts and financial intelligence specialists for real-time monitoring of suspicious activity.[150]
- **Development of Governmental Analytical Tools:** Development and implementation of AI-based tools for identifying obfuscation patterns (e.g., the use of mixers or Chain Hopping) and detecting anomalous transactions.[151]
- **Personnel Training:** International training programs in collaboration with academic institutions and FinTech companies for blockchain forensics.[152]

Cooperation with the FinTech Industry

FinTech companies (such as Chainalysis, TRM Labs) develop advanced blockchain analytical tools, but generally, cooperation with governments is limited to unilateral reporting. A bidirectional cooperation model, similar to that existing in the cybersecurity domain (CISA)[153], should be adopted.

- **Joint Forums:** Establishment of international forums for governments and FinTech companies to analyze trends and courses of action.

[150] https://www.trmlabs.com/resources/trm-talks/trm-talks-how-the-fbi-tracks-and-seizes-illicit-crypto-with-the-virtual-assets-unit-chief-patrick-wyman
[151] https://www.mdpi.com/2079-9292/13/17/3568
[152] https://www.mdpi.com/2079-9292/13/17/3568
[153] https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative

- **Incentives for FinTech Companies:** Research grants for developing tools to analyze sophisticated cryptographic activity.[154]
- **Regulation of Data Sharing:** Legal protocols for data sharing, adapted to GDPR standards.[155]

Uniform Regulation to Prevent Regulatory Arbitrage

- **Regulatory Harmonization:** Promotion of a common legislative framework to reduce regulatory arbitrage.[156] Regulatory discrepancies enable regulatory arbitrage (see the Garantex case) and enhance the use of crypto for sanctions evasion and terrorist financing.
- **Mandatory Licensing and Registration of VASPs:** Requiring jurisdictions subject to Financial Action Task Force (FATF) guidelines to implement mandatory licensing and registration for Virtual Asset Service Providers (VASPs), including full Know Your Customer (KYC), suspicious transaction reporting (STR), and implementation of the "Travel Rule."[157]
- **Secondary Sanctions:** Expansion of the scope of sanctions on VASPs in countries that do not comply with international standards and a systematic prohibition of engagement with them.

The Static Designation Gap in Crypto-Sanctions Enforcement

Crypto-sanctions enforcement relies on public designation of specific blockchain addresses by agencies such as OFAC and NBCTF. These designations are ingested by commercial analytics firms (Chainalysis, Elliptic, TRM Labs) and integrated into VASP compliance screening. However, this architecture suffers from a structural mismatch: Designations are static identifiers applied to a dynamic system. Two failure modes render them insufficient:

- **Fund migration upon publication:** Generating a new blockchain address is instantaneous, free, and requires no registration. By the time a designation is published, funds have often already moved. In the September 2025 IRGC wallet seizure, only $1.5 million was frozen across 187 wallets despite $1.5 billion in historical volume—a 0.1% capture rate.

[154] https://www.darpa.mil/about/offices/contracts-management

[155] https://www.mdpi.com/2079-9292/13/17/3568

[156] https://www.csis.org/analysis/stabilizing-us-financial-leadership-why-congress-must-get-stablecoin-regulation-right

[157] https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html ; https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html ; https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html

- **Protocol-level address generation:** Bitcoin wallets generate new addresses per transaction by default. On Ethereum and TRON—which dominate Iranian sanctions-evasion activity—creating new accounts is instant and free. A sanctioned entity's operational capacity is not meaningfully degraded by the loss of a single address.

The Analytics Gap

The bridge between a designated address and the broader cluster of addresses controlled by the same entity is provided by commercial analytics firms using proprietary heuristics. However, each firm applies different clustering methodologies, confidence thresholds, and taint-propagation models. One VASP may block a transaction that another clears for the same funds. No public initiative currently exists to standardize this methodology—neither FATF nor any designating authority has published binding standards for cluster identification or designation propagation.

Proposed Measures

- **Cluster-level designation:** Designating authorities should target entity clusters, not individual addresses. FATF should develop a binding minimum standard for cluster identification heuristics, with defined confidence thresholds. Analytics firms would apply this as a baseline floor while retaining proprietary methods above it.
- **Real-time designation infrastructure:** A centralized, API-accessible designation database providing real-time feeds to VASPs, replacing periodic SDN list updates. This should include a provisional designation mechanism to act before fund migration is complete.
- **Cross-jurisdictional mutual recognition:** Automatic recognition of crypto-specific designations between participating jurisdictions within 24 hours, with a shared intelligence channel for pre-designation coordination to synchronize timing and minimize the migration window.
- **Stablecoin issuer integration:** Centralized stablecoin issuers (Tether, Circle) retain administrative freeze capabilities over their token contracts. They should be required to connect to the designation database and implement automated cluster-level freezing—leveraging a unique enforcement lever that does not exist for native protocol tokens.

Limitations

This framework operates primarily at centralized chokepoints (VASPs, stablecoin issuers) and cannot reach fully decentralized protocols or privacy-preserving chains. Standardized heuristics carry false-positive risk requiring defined remediation procedures. Effectiveness depends on adoption breadth—non-participating jurisdictions will continue to provide refuge, as the Garantex-to-Grinex migration to Kyrgyzstan demonstrated. Nevertheless, the framework addresses the most exploitable gap in current enforcement:

The mismatch between the speed at which sanctioned actors move funds and the speed at which the system can respond.

Conclusion

Sanctions evasion through cryptographic assets represents a complex interstate challenge requiring a multi-dimensional and coordinated response. The recommendations proposed in this research—strengthening state capabilities, deepening cooperation with the FinTech industry, international regulatory harmonization, and closing the *Static Designation Gap* through cluster-level enforcement and real-time designation infrastructure—offer an improved framework for confronting the changing technological reality. Implementing these recommendations requires significant investment in resources, expert personnel, and close international cooperation. However, the cost of inaction could be significantly higher than the cost of implementation. The success of the proposed framework is contingent on the international community's ability to adopt a coordinated, dynamic, and sustained approach, while maintaining a delicate balance between enforcement effectiveness and the preservation of individual rights and the promotion of technological innovation. Ultimately, the struggle against sanctions evasion in the cryptographic era is not merely a technological challenge but also a test of the ability of democratic governance institutions to adapt to an evolving digital reality while upholding their guiding values and principles.