TRT WORLD research centre

Digital Currencies' Evasion: Sanctions Enforcement and the Digital Battlefield

Şeymanur Yönt

(Hakan Nural - Anadolu Agency)

Digital currencies are popular tools of sanctions evasion. Therefore, effective sanctions enforcement requires a multifaceted approach that addresses both the structural complexities of digital currencies and the gaps in international cooperation. This policy outlook examines challenges arising from inherent characteristics of digital currencies and lack of universal compliance and enforcement in sanctions evasion and offers solutions to overcome such challenges to prevent sanctions evasion through digital currencies. Solutions include those technical and regulatory ones aimed at increasing compliance as well as the ones targeting other states', organisations', and private sectors' inclusion in the enforcement efforts.

Introduction

As sanctions have become more prevalent and sophisticated in recent years, so have sanctions evasion practices. Between 2000 and 2021, the U.S. significantly expanded its use of sanctions, with an increase of more than 933 per cent in response to various economic, foreign policy, and national security challenges. As a result of such expansion, targets have increasingly focused on finding ways to circumvent sanctions, minimising their economic and political impact and thereby undermining the effectiveness of sanctions regimes. In response, sanctioning parties have intensified efforts to close loopholes and enhance enforcement mechanisms to prevent evasion.

This has required addressing common sanctions evasion tactics, such as the use of intermediaries, engaging third-party companies or jurisdictions to obscure the true origin or destination of goods; false documentation, which involves misrepresenting the nature, value, or end recipient of transactions; and the exploitation of digital currencies to bypass conventional financial controls. From Russia's efforts to circumvent Western sanctions through the digital Ruble and Bitcoin mining to North Korea's extensive cyber-digital currency theft operations funding its weapons programs, digital assets have emerged as a critical tool for evasion. Iran, Venezuela, and various sanctioned entities have similarly turned to blockchain-based financial systems, decentralised exchanges, and privacy-enhancing technologies to conduct transactions beyond the reach of traditional enforcement mechanisms. Since digital currencies pose unique challenges for sanctions enforcement due to their decentralised nature, anonymity features, and global accessibility, developing effective regulatory measures to counter their misuse is increasingly important. This policy outlook examines challenges arising from inherent characteristics of digital currencies and lack of universal compliance and enforcement in sanctions evasion and offers solutions to overcome such challenges to prevent sanctions evasion through digital currencies. Solutions include those technical and regulatory ones aimed at increasing compliance as well as the ones targeting other states', organisations', and private sectors' inclusion in the enforcement efforts.

1. What is a Digital Currency?

Digital currency is a form of currency that exists only in digital or electronic form, without a physical counterpart like cash or coins. As an umbrella term, it covers many assets, from highly decentralised digital assets such as cryptocurrencies to centralised central bank digital currencies (CBDCs). Related to digital currencies, and also important for sanctions evasion, centralised and decentralised exchanges[1] serve as platforms for trading digital currencies, but they differ significantly in terms of regulation and their role in sanctions evasion. Centralised exchanges, such as Binance (where clients trade digital currencies through an intermediary), are heavily regulated and must adhere to laws such as Know Your Customer and Anti-Money Laundering regulations. This makes them less attractive to sanctioned entities seeking to avoid detection. Centralised exchanges typically handle well-established, regulated digital currencies like Bitcoin and Ethereum and centralised stablecoins like Tether, backed by fiat currencies.

In contrast, decentralised exchanges facilitate peer-to-peer transactions without intermediaries, using smart contracts on the blockchain, and are far less regulated. This lack of oversight makes decentralised exchanges appealing to those who bypass government monitoring, including sanctioned entities. Decentralised exchanges tend to support a wider range of digital currencies, including major cryptocurrencies like Ethereum and Bitcoin, as well as lesser-known or newer tokens that may not be listed on centralised platforms.

DIGITAL CURRENCIES			
Type	**Key Features**	**Examples**	**Centralisation**
Cryptocurrencies	Decentralised, blockchain-based, immutable ledger	Bitcoin (BTC), Ethereum (ETH)	Decentralised (varies by governance)
CBDCs	Government-issued, digital form of fiat currency	Digital Yuan (e-CNY), Digital Euro	Centralised
Stablecoins	Pegged to fiat or assets, reduces volatility	Tether (USDT), USD Coin (USDC)	Can be centralised or decentralised
Virtual Currencies	Used in specific platforms or games	V-Bucks (Fortnite), Robux (Roblox)	Centralised

[1] The concepts of centralisation and decentralisation apply to both digital assets and exchanges. A centralised digital currency is issued, controlled, and regulated by a central authority, such as a central bank (e.g., CBDCs) or a company managing a pegged asset (e.g., USDT). In contrast, a decentralised digital currency (e.g., Bitcoin) operates on a distributed network without a single controlling entity. Similarly, a centralised exchange (CEX) (e.g., Binance) is a platform managed by an intermediary that facilitates trading and typically requires user identification. A decentralised exchange (DEX) (e.g., Uniswap), on the other hand, enables peer-to-peer trading through smart contracts, allowing users to trade without relying on a central authority.

(Stringer - Anadolu Agency)

Digital currencies and their centralised or decentralised exchange offer several advantages, such as lower transaction costs, faster cross-border payments, and increased financial inclusion. However, some digital currencies' anonymity, borderless nature, and lack of centralised control have made them attractive to individuals and entities seeking to evade sanctions.

2. Methods of Sanctions Evasion Through Digital Currencies

Sanctions evasion using digital currencies can occur in various ways. One common method is using mixers or tumblers, which are services that obfuscate the trail of mostly decentralised digital currency transactions by mixing them with other transactions. This happens by mixing one account's coins with those of other accounts, ensuring that no one reveals the origin and destination of the digital assets. On the one hand, the process is used for legitimate reasons, such as ensuring transaction security by reducing the possibility for attackers to track transactions.

On the other hand, it is used for illegitimate motivations such as evading sanctions and money laundering, making it difficult for authorities to trace the flow of funds and identify the parties involved. For example, Bitcoin Fog, one of the most well-known mixers, was accused of laundering $400M in cryptocurrency, resulting in its operator being sentenced to 12 years and 6 months in prison in the U.S. Tornado Cash, another well-known mixer, was sanctioned by the U.S., being accused of laundering more than $7 billion worth of virtual currency. This amount includes over $455 million stolen by the Lazarus Group, a North Korean hacking group that is also sanctioned by the U.S., which seeks to support North Korea's economy, heavily impacted by international sanctions.

Another method of sanctions evasion through mostly decentralised digital currencies involves using privacy coins, such as Monero and Zcash, which employ advanced cryptographic techniques to enhance transaction privacy and anonymity. Monero utilises privacy-enhancing technologies to ensure anonymity, making tracing the sender, receiver, or transaction amount almost impossible. Zcash, on the other hand, encrypts transaction information, ensuring private peer-to-peer payments. The privacy features of these currencies make them particularly appealing to individuals seeking to evade sanctions.

Cybersecurity measures such as VPNs, Tor and proxy services, which obfuscate a user's location, are another method of sanctions evasion. For instance, a VPN can be used to conceal the actual location of an entity conducting a digital asset transaction, making it seem that the transaction does not involve a party from a sanctioned country. Other methods include using false identities, chain hopping, and peel chains. False identities involve using fake names, aliases,

or stolen personal information to hide the true identity of a party in a digital asset transaction. Chain hopping refers to rapidly converting one type of virtual currency into another across different blockchains, making it harder to track illicit funds and exploiting differences in regulatory oversight across blockchains. This happens through "chain hopping," where individuals first acquire a more traceable coin (such as Bitcoin) and then transfer it to a less transparent blockchain (such as Monero) to obscure their transactions. Finally, peel chains involve breaking down a large sum of virtual currency into smaller amounts and transferring them through multiple transactions to obscure their origin. Moreover, cross-chain bridges allow digital assets to be transferred between different blockchain networks and are particularly vulnerable to hacks. Hackers can manipulate these bridges by creating fraudulent transactions or exploiting weaknesses in their smart contract code. For instance, the Binance Smart Chain bridge was breached in a 2022 attack, where attackers fraudulently minted BNB tokens, leading to a loss of $570 million.

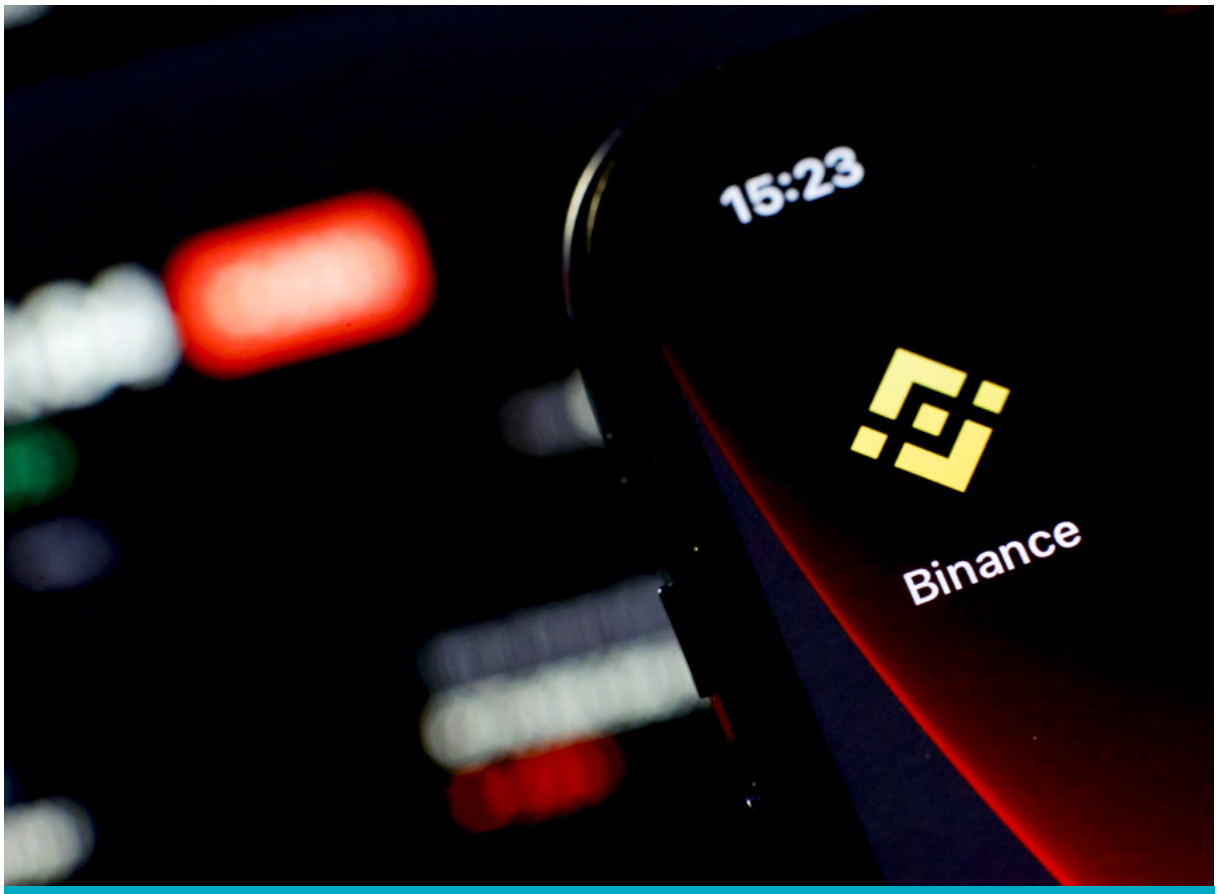
These methods are widely employed by sanctioned entities, including Russia and Iran, to bypass restrictions and sustain access to global financial networks. Their strategic use of digital assets enables them to circumvent traditional monitoring mechanisms, complicating enforcement efforts.

3. How Do Targets of Sanctions Use Digital Currencies to Evade Sanctions?

Targets of sanctions can use digital currencies to evade sanctions in many ways, including conducting business through payments in digital currencies and hacking cryptocurrency wallets to make revenue. Among those targets, countries that are heavily hit by sanctions are the ones that usually refer to sanctions evasion through digital currencies. Those countries include Iran, Venezuela, North Korea, and Russia.

3.1. Iran

Several sanctions target Iran due to its nuclear activities. Sanctions on Iran include those adopted by the E.U. on "serious human rights violations", resulting in asset freezes. More significantly, both the UN and the E.U. imposed asset freezes and restrictions such as embargo on dual-used goods about the "non-proliferation of weapons of mass destruction". The United States, too, has imposed comprehensive sanctions on Iran, targeting various sectors, in-



(Sefa Karacan - Anadolu Agency)

cluding finance, oil exports, trade, and individuals associated with terrorism and weapons development. Sanctions have significantly impacted Iran's economy, particularly by isolating it from the international financial system and reducing its oil revenues.

As a means to evade these sanctions, Iran referred to digital currencies. In June 2018, Iranian officials announced that they were working on establishing a national digital currency, which would enable seamless money transfers both within the country and internationally. In line with that, Iran permitted cryptocurrencies and smart contracts to pay for imported goods, avoiding using the dollar and circumventing sanctions. As a result, since 2018, approximately $7.8 billion has been transferred between Binance and Nobitex, Iran's largest cryptocurrency exchange. The use of digital currencies was also aimed at enabling bilateral trade between Iran and other sanctioned nations, such as Russia. Iran and Russia formalised a cryptocurrency cooperation agreement in November 2018 that aligned with this objective. Meanwhile, Tehran leverages its excess oil to generate electricity for Bitcoin mining hubs, using the sector as a source of revenue. In 2020, Iran accounted for approximately 4.5% of global Bitcoin mining, generating an estimated $1 billion in annual revenue.

3.2. Venezuela

Venezuela has been subject to severe sanctions primarily imposed by the United States, targeting the country's oil industry, government officials, and financial transactions. These sanctions aim to pressure the government to restore democratic processes and address human rights abuses. The U.S., in particular, has frozen Venezuelan assets, restricted access to international financial markets, and prohibited transactions with state-owned enterprises, including the national oil company, PDVSA. These measures have severely constrained Venezuela's economy, reducing the government's ability to generate revenue.

In response, the Venezuelan government has turned to digital currencies as an alternative to circumvent these economic restrictions. In December 2017, Venezuelan President Nicolás Maduro revealed plans to introduce a new digital currency, the "petro," backed by oil reserves and other commodities. He emphasised that the petro was intended to help Venezuela circumvent U.S. sanctions and generate new financial resources for the government, combating the currency devaluation. This move is intended to facilitate international trade and financial transactions outside the purview of U.S. sanctions.

3.3. North Korea

Since 2006, the U.S. and the UN have imposed extensive sanctions on North Korea, targeting key sectors of its economy to restrict funding for its nuclear weapons programme. These sanctions prohibit the export of luxury goods, chemicals, coal, and other natural resources that Pyongyang has historically used to generate revenue for the regime. Over the years, restrictions have tightened, including measures against North Korea's access to international banking systems, trade partnerships, and financial transactions. The sanctions also extended to individuals and entities involved in weapons proliferation, cybercrime, and illicit trade. Despite these efforts, North Korea has developed sophisticated methods to bypass these restrictions and continue financing its nuclear and military activities.

One of the most effective ways North Korea evades sanctions is through digital currencies. The regime has increasingly relied on cybercrime, particularly hacking cryptocurrency exchanges and wallets, to generate illicit funds. The Lazarus Group, a state-sponsored hacking collective, has been responsible for major cyberattacks, stealing billions in digital assets. An example is the WannaCry attack, where cybercriminals, suspected to be Lazarus Group, globally encrypted users' computers and demanded payment in Bitcoin to restore access. Reports indicate several Bitcoin wallets linked to the attack have since been emptied. To conceal the origins of these stolen funds, North Korea launders them through cryptocurrency mixing services like Tornado Cash, which blends different transactions to make tracing nearly impossible. In addition to cyber theft, North Korea has engaged in large-scale bitcoin mining, allowing it to acquire digital assets outside the reach of traditional financial regulations. These methods have enabled Pyongyang to circumvent sanctions and sustain its economy despite international pressure.

3.4. Russia

Russia, facing international sanctions primarily due to its annexation of Crimea and its invasion of Ukraine, has encountered extensive economic restrictions imposed by the United States, the European Union, and other nations. These sanctions target Russia's financial, energy, and defence sectors to curtail its ability to raise capital and access international markets. Measures include asset freezes, travel bans on individuals, restrictions on Russian state-owned enterprises, and prohibitions on technology transfers to the energy sector. The sanctions have significantly impacted Russia's economy, leading to a decrease in foreign investment, a depreciation of the rubble, and challenges accessing Western financial systems.

In response to these sanctions, Russia has increasingly turned to digital currencies to circumvent economic restrictions and sustain its financial systems. Cryptocurrencies allow Russian entities to bypass traditional financial systems, facilitating international trade and investment despite regulatory constraints. Moreover, Russia has explored the development of its own digital currency, the digital rubble, to further insulate its economy from international sanctions and reduce dependency on Western financial infrastructure. By leveraging the pseudonymous nature

of digital currencies, Russia can conduct transactions that are harder to trace back to the state or sanctioned entities. In September 2022, Russian hackers introduced advanced ransomware techniques capable of concealing transfer details from the blockchain, making transaction tracking more difficult. Another challenge in tracing transactions that enable Russia to circumvent sanctions is using non-custodial wallets, which interact solely through encrypted aliases of payers, leaving the wallets "beyond the reach of the authorities".

Moreover, Russia usually ranks amongst the first five largest Bitcoin mining nations. This growth is facilitated by the country's abundant natural resources, particularly in the energy sector. Notably, gas-powered mining hubs are gaining prominence. For instance, Gazpromneft, a state-owned energy giant Gazprom subsidiary, has partnered with BitRiver, a leading Bitcoin mining service provider, to supply flare gas for cryptocurrency mining operations. This collaboration enables Russia to monetise its energy resources by converting otherwise wasted flare gas into electricity for mining activities. Consequently, Bitcoin mining contributes to national revenue through taxation, licensing fees, and state-run initiatives, providing an alternative means of generating income outside the traditional financial system and reducing reliance on foreign banks or payment networks. Acknowledging this, the Kremlin implemented new legislation in November 2024, creating a regulatory framework for cryptocurrency mining. This framework enables the validation of blockchain transactions, facilitating international payments using digital assets.

While Russia advocates using digital currencies, as did the Governor of the Central Bank of the Russian Federation, sanctioning authorities try to thwart such a strategy. The United States particularly states that Russia-related sanctions extend to virtual currencies, prohibiting its citizens from facilitating transactions, including digital currency dealings, that would be illegal if conducted within the U.S. This includes transactions involving Russia's Central Bank, National Wealth Fund, or Ministry of Finance. Additionally, U.S. financial institutions cannot process virtual currency transactions linked to foreign banks subject to sanctions under Executive Order 14024. Non-U.S. persons are also restricted from aiding U.S. sanctions violations or engaging in activities designed to evade them. E.O. 14024 further allows sanctions on those using digital or physical assets to circumvent restrictions, reinforcing efforts to prevent Russia from bypassing sanctions through cryptocurrency.

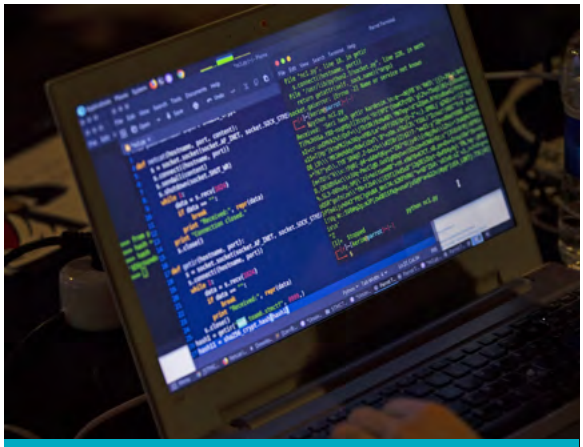
These practices demonstrate that digital currencies have become a frequent tool for sanctions evasion, making their regulation a priority. However, several challenges hinder effective prevention efforts.

4. Challenges in Addressing Sanctions Evasion Through Digital Currencies

There are two main types of challenges: one arises from the inherent characteristics and functioning of digital currencies, which enable anonymity, pseudonymity, and decentralised transactions that are difficult to regulate. The other involves the complexities of persuading third states and private entities to enforce or comply with sanctions, particularly when they have no direct obligation or economic incentive to do so, making the prevention of sanctions evasion a far more complex and fragmented endeavour.

4.1. Challenges Arising from Inherent Characteristics of Digital Currencies

While preventing sanctions evasion through digital currencies is crucial for maintaining the effectiveness of sanctions, enforcement efforts are complicated by challenges stemming from the inherent characteristics of digital currencies. First, the anonymity and pseudonymity of certain digital currency transactions make it difficult for authorities to trace and identify illicit activities. While blockchain technology provides a transparent and immutable ledger of transactions, the identities behind wallet addresses may remain obscured. Although transaction traceability is possible through blockchain analysis and forensic tools, factors such as using privacy coins, mixers, VPN use, and complex transaction patterns can make tracking funds significantly more challenging, ultimately facilitating sanctions evasion.



(Muhammed Selim Korkutata- Anadolu Agency)

In that regard, decentralised currencies, especially cryptocurrencies, create substantial challenges for sanctions enforcement due to their inherent anonymity and pseudonymity. These features, combined with decentralised exchanges and noncustodial wallets, make it difficult for authorities to trace and identify illicit activities. Unlike custodial wallets, which are subject to regulatory oversight, noncustodial wallets enable peer-to-peer transfers that leave limited identifiable information on the blockchain. This lack of traceability, coupled with the encrypted nature of transactions and the absence of third-party oversight, makes it significantly harder to track ownership and detect sanctions evasion, facilitating illicit activities while evading regulatory scrutiny.

Second, certain digital currencies' global and decentralised nature complicates regulatory efforts. Certain digital currency transactions can occur across borders without intermediaries, making it challenging for any jurisdiction to exercise control. For example, the cryptocurrency Tether has been utilised to facilitate large cross-border transactions without traditional banking oversight, making it challenging for authorities to monitor and regulate such activities. Moreover, the regulatory landscape for digital currencies varies widely between countries, with some adopting stringent regulations while others have more permissive approaches. For example, while the European Union subjects crypto-asset service providers to strict regulations under the Markets in Crypto-Assets Regulation (MiCA), some countries, such as the United Arab Emirates, have adopted more flexible regulations to promote the digital asset sector by establishing special free zones for crypto companies. Similarly, in some jurisdictions with weaker regulatory frameworks, enforcement becomes even more challenging. For instance, countries with limited anti-money laundering and know-your-customer requirements for crypto exchanges create loopholes that enable illicit financial activities to go undetected. This regulatory disparity allows individuals and entities to move digital assets across borders with minimal oversight, undermining international sanctions enforcement.

Third, the rapid pace of innovation in the digital currency space outpaces regulatory frameworks. New technologies and platforms, such as decentralised finance and non-fungible tokens (NFTs), continue to emerge, creating new opportunities for sanctions evasion. For instance, NFTs can obscure asset transfers by disguising them as digital artwork or collectables, further complicating enforcement efforts. An example involves wash trading with NFTs to move funds between sanctioned entities. In this scheme, a sanctioned individual or entity can create an NFT and sell it to a collaborator (or even themselves using a different wallet) for an inflated price, disguising the transfer of funds as a legitimate sale. Because NFT transactions occur on decentralised marketplaces with minimal oversight, it becomes difficult for regulators to determine whether the transaction reflects a genuine purchase or a method of circumventing sanctions. Therefore, regulators must constantly adapt and update their strategies to keep up with these developments.

In addition, the vulnerability of digital currencies to cyberattacks, particularly blockchain networks and crypto-asset service providers, helps facilitate illicit money transfers and, therefore, sanctions evasion. For example, blockchains can be compromised if attackers gain control of 51% of a network's computational power (hash rate), allowing them to validate fraudulent transactions or reverse completed ones, effectively double-spending digital assets. These and other inherent characteristics emerge as key issues that must be addressed to prevent sanctions evasion.

4.2. Challenges Arising from the Lack of Universal Compliance and Enforcement

While tackling challenges inherent to digital currencies is essential, ensuring comprehensive enforcement and preventing sanctions evasion is equally important. One significant challenge stems from the business practices of digital currency providers. Given that the widespread use of digital assets translates into higher transaction volumes and, consequently, greater profits, these entities have little financial incentive to implement strict measures against sanctions evasion. Many digital asset service providers, particularly those operating in loosely regulated jurisdictions, may prioritise user growth and market expansion over compliance with international sanctions frameworks. For example, in the sanctions imposed on Binance, communications revealed that although Binance had sanctions compliance procedures in place, it had been reluctant to enforce them and had overlooked certain situations. In internal discussions, Binance's then Chief Compliance Officer (CCO) explained in a chat message to a Binance employee that the company's stance was "not to openly do business with Iran due to sanctions" as it impacted their banking relationships. However, he acknowledged that the platform continued to support Iranian customers, albeit in a "non-open" manner. This is understandable, as most digital currency platforms' primary aim is profit.

A further challenge lies in persuading other countries to enforce compliance with sanctions by which they are not formally bound. Unlike anti-money laundering efforts, which are supported by a strong global framework of cooperation and information-sharing due to their clear criminal nature, sanctions enforcement is far more fragmented. Sanctions are often driven by specific states or organisations' foreign policy and national security priorities rather than a universally recognised legal obligation. As a result, many countries have little incentive to participate in

enforcement mechanisms or align their regulatory frameworks with sanctions they do not impose. While cross-border cooperation does exist, it is largely reactive—focusing on punitive measures such as asset seizures—rather than fostering proactive regulatory alignment or preventive controls. This limits the effectiveness of sanctions as an enforcement tool and underscores the need for stronger international agreements to bridge these gaps. This situation, coupled with the lack of incentives for the private sector to comply, presents a major challenge that needs to be addressed.

5. Strategic Responses to Mitigate Sanctions Evasion

Strategic responses are essential for addressing the evolving landscape of financial regulations and enforcement while preserving confidence in financial markets. Furthermore, it is particularly important to maintain the reliability of digital currencies, as they offer a significant advantage in terms of accessibility, especially for developing countries. These strategies encompass a multifaceted approach involving technological advancements, regulatory cooperation, and adaptive policy frameworks. By leveraging advanced analytics and blockchain forensics, authorities and businesses can enhance their capabilities in tracking and identifying illicit transactions. International collaboration and information sharing among regulatory bodies are essential to harmonise efforts and ensure a cohesive response to digital currencies' global and decentralised nature. Additionally, continuous updates to regulatory frameworks are necessary to keep pace with rapid technological innovations in the digital currency space, thereby closing potential loopholes that could be exploited for sanctions evasion. While doing so, policymakers must regulate all evolving forms of evasion instead of fighting only their current form.

5.1. Enhancing Regulatory Frameworks

Regulatory frameworks on sanctions evasion do not differentiate between digital and fiat currencies. However, certain characteristics of digital currencies—such as their pseudonymity, decentralised nature, and rapid cross-border transferability—require specific regulatory measures to address associated risks effectively. Effective regulation includes developing comprehensive frameworks that address anti-money laundering and counter-terrorist financing requirements. For instance, according to U.S. Treasury officials, robust anti-money laundering measures are fundamental to establishing effective controls that detect and prevent illicit activities, including sanctions evasion. Strong anti-money laundering protections include comprehensive customer due diligence, transaction monitoring, suspicious activity reporting, and strict regulatory oversight to ensure compliance with financial laws. Accordingly, regulators should require digital currency exchanges and service providers to enforce stringent know-your-customer and customer due diligence measures to verify user identities. In line with this, businesses and entities operating in the digital currency sector should

(Mustafa Çiftçi - Anadolu Agency)

be obligated to implement policies and procedures to: restrict access from IP addresses associated with sanctioned countries or regions, suspend accounts held by users from these restricted areas, designate a compliance officer with authority to oversee sanctions compliance; regularly conduct user screenings to confirm they are not from prohibited regions including utilising screening tools equipped with fuzzy logic, which can identify common name variations or misspellings, such as alternate spellings for sanctioned location (Krimea instead of Crimea etc.); increase cybersecurity measures to prevent thefts; and provide compliance training for relevant personnel.

Sanctioned entities' profit-making through data mining should be another focus area for regulators. To prevent their ability to process large-scale data operations, regulators should restrict their access to cloud computing services and high-performance computing infrastructure, as well as strengthen export controls on useful AI tools, advanced chips, and data processing technologies. Moreover, ensuring multinational tech firms comply with strict due diligence requirements, including geofencing, API usage monitoring, and customer vetting, can also help limit indirect support for sanctioned entities. Lastly, monitoring blockchain-based data monetisation and decentralised marketplaces is necessary because these emerging technologies offer new ways to circumvent traditional financial restrictions.

Meanwhile, the timing and quality of strong regulatory frameworks are crucial, too. At this point, it is important for digital currencies to implement sanctions evasion-related policies and procedures well before they begin operations, conducting risk assessments that also evaluate company touchpoints in advance. OFAC has stated that "it is never too soon to evaluate potential sanctions risks", which includes digital currency companies in the beta testing phase of their operations. A regulatory requirement could be envisaged to encourage businesses to act in this direction to ensure that

5.2 Use of AI and Machine Learning

AI and machine learning are critical in preventing sanctions evasion in digital currencies, enabling real-time detection of illicit transactions and improving compliance measures. Their advanced algorithms can analyse high amounts of blockchain transaction data to identify suspicious patterns, such as mixer services and fast asset transfers between wallets linked to sanctioned entities. Machine learning models improve traditional risk-scoring methods by adapting to evolving evasion tactics, such as the use of privacy coins and decentralised exchanges. AI-powered tools also improve know your customer and anti-money laundering processes by verifying identities, detecting fraud, and flagging inconsistencies in transaction histories. Additionally, natural language processing can monitor online forums, darknet markets, and social media for discussions on sanctions circumvention strategies, providing regulators with actionable intelligence to prevent such practices. AI and machine learning significantly hamper the ability of illicit actors to exploit digital currencies for sanctions evasion through automating compliance checks and strengthening enforcement. Accordingly, states and organisations may provide training and incentives to make companies adopt such solutions.

5.3 Improving Central Bank Digital Currencies

In order to effectively prevent sanctions evasion with digital currencies, CBDCs must adopt programmable compliance measures which enforce restrictions at the transaction level, automatically blocking transfers involving sanctioned entities or jurisdictions. By obliging businesses and financial institutions to use CBDC-based settlement systems in large-scale transactions, governments can limit the role of unregulated digital assets in sanctions evasion, reducing opportunities for illicit fund conversions. Moreover, integrating CBDCs with AI-driven blockchain analytics can enhance real-time monitoring and detecting obfuscation techniques like layering and mixing. Governments should establish interoperable CBDC frameworks with standardised compliance protocols to close regulatory loopholes, ensuring that sanctioned actors cannot exploit jurisdictional inconsistencies. Through such advancements, CBDCs can serve as a highly controlled and traceable alternative to private cryptocurrencies, significantly curbing their use for sanctions evasion.

5.4 Use of International Regulatory Sandboxes

International regulatory sandboxes provide a controlled environment for governments and financial regulators to test and refine measures aimed at preventing sanctions evasion in digital currencies. These sandboxes enable the deployment of advanced blockchain analytics, AI-driven transaction monitoring, and cross-border data-sharing frameworks to detect and prevent illicit financial flows. For example, regulators can collaborate with cryptocurrency exchanges to trial real-time compliance tools that flag suspicious transactions linked to sanctioned entities. Additionally, pilot programs within these sandboxes allow authorities to assess the effectiveness of new know-your-customer and anti-money laundering standards tailored for decentralised finance platforms. By fostering cooperation among financial institutions, technology providers, and law enforcement agencies, international regulatory sandboxes help refine enforcement mechanisms before full-scale implementation, ensuring that compliance measures remain effective without stifling innovation in digital asset markets.

5.5. Strengthening International Cooperation

Given the borderless nature of digital currencies and inconsistent enforcement activities sanctioned targets take advantage of, international cooperation is crucial. Therefore, countries should collaborate to share information, intelligence, and best practices regarding digital currency regulation and enforcement. Organisations such as the Financial Action Task Force (FATF) can play a pivotal role in facilitating this cooperation and establishing global standards. Indeed, it is crucial for this cooperation to materialise as a multinational agreement. Without an international regulatory framework, the interaction of national laws often leads to a system that is both over-inclusive and under-inclusive when it comes to investigations and prosecutions. An international framework would prevent individuals using cryptocurrency for illicit purposes from slipping through the cracks and evading legal action while addressing the unpredictability of enforcement mechanisms, which can sometimes result in double punishments across different jurisdictions.

However, as much as international cooperation is important, it is difficult. For instance, achieving alignment between the E.U. and the U.S. policies on digital currencies is crucial, but there are already tensions due to differing views on digital regulatory policies. While the E.U. has implemented more comprehensive frameworks, such as the Markets in Crypto-Assets (MiCA) regulation, the U.S. has a more fragmented regulatory environment, with agencies like the SEC and CFTC playing differing roles in overseeing digital currencies. Moreover, it is difficult to regulate certain digital currencies at the international level due to their decentralised nature. These can create challenges for firms conducting transatlantic commerce, as they may face conflicting compliance requirements, hindering cross-border crypto transactions and investments. To address these discrepancies, the E.U., the U.S., and all sanctioning parties should collaborate to establish targeted regulations that facilitate cooperation in tackling crime and sanctions evasion rather than pursuing a broad international framework. This could include initiatives such as collaboration to enhance technical capacities or information sharing. Given the approach of the new U.S. administration towards international agreements, this objective is likely to be more attainable.

Finally, each country and organisation have different priorities and sanctions frameworks. As a result, a target sanctioned by one country may not be included in another's sanctions list, thereby reducing the incentive to prevent evasion within a specific sanctions programme. At this point, the common ground that could bring states together lies in their business interests, especially when considering secondary sanctions. Therefore, while creating an international framework for targeted sanctions might be achievable, establishing forums that promote open communication and increased transparency might be the more straightforward approach to preventing sanctions evasion. These platforms would facilitate cooperation and help align efforts to tackle the issue more effectively.

5.6. Engaging with the Digital Currency Industry

Policymakers should actively collaborate with stakeholders in the digital currency sector, including exchanges, wallet providers, and blockchain developers, to adopt a risk-based approach to combating sanctions evasion. Engaging industry players early in the regulatory process allows authorities to gain insights into emerging trends and technologies, enabling them to design more effective enforcement mechanisms while fostering responsible innovation. U.S. Treasury officials emphasise that regulators and investigators must continuously adapt to the evolving tactics used by illicit actors. Strengthening cooperation between regulators and the digital currency industry while ensuring the continued advancement of compliance tools will be critical in reducing the use of digital assets for sanctions evasion.

Moreover, engaging in the digital currency industry will help address the industry's lack of incentives to comply with sanctions over the profit it will make through evading sanctions. For example, regulations could assign oversight responsibilities to specific state agencies and even allow access to account information for designated state institutions. This would ensure more robust enforcement of compliance measures, providing authorities with the necessary tools to monitor transactions, detect illicit activity, and hold companies accountable for failing to adhere to sanctions and regulatory frameworks.

Conclusion

Sanctions evasion through digital currencies presents a complex and evolving challenge that requires a coordinated and adaptive response. Effective enforcement is crucial not only to uphold the integrity of sanctions regimes but also to prevent illicit actors, including terrorist organisations, rogue states, and criminal networks, from exploiting digital assets to finance unlawful activities. Policymakers can mitigate the risks associated with this illicit activity by enhancing regulatory frameworks, strengthening international cooperation, leveraging technology and data analytics, and engaging with the digital currency industry. As digital currencies grow in popularity and influence, governments and international bodies must remain vigilant and proactive in addressing their threats to global security and stability.