



**G B B C**  
DIGITAL  
FINANCE

2022 | GDF Report

# **CRYPTOASSETS AND SANCTIONS COMPLIANCE**

A PRIMER

---

## TABLE OF CONTENTS

3	<b>Chair's Foreword</b>
4	<b>Executive Summary</b>
6	<b>Sanctions Compliance and Cryptoassets</b>
	Current State of Regulatory and Legal Requirements
	United States
	European Union
	UK
	Other Requirements
	Sanctions Compliance Practices By the Industry
	Know Your Customer(KYC)/Customer Due Diligence (CDD) Practices
	Blockchain Analytics
	The Travel Rule
11	<b>Leveraging Transparency to Prevent Sanctions Evasion</b>
15	<b>Sanctions Evasion Risks</b>
	Cybercrime
	Mining
	Mixers
	High Risk VASPs
18	<b>Policy Recommendations</b>
21	<b>Report Contributors</b>



# Chair's Foreword



Lawrence Wintermeyer  
Chair  
GBBC Digital Finance

The Ukraine conflict has brought a globally unprecedented level of sanctions on Russia, and as part of this, put the cryptocurrency industry on the front lines on enforcing sanctions.

In March 2022, GDF convened the global crypto and digital assets community along with global policymakers in an Emergency Sanctions Summit to plan for and prepare the industry response to the sanctions imposed by agencies across the globe.

A key theme of the summit was overcoming the misconception of many, that the cryptocurrency ecosystem would be used to significantly avoid sanctions by Russian banks, institutions, and targeted individuals. Whilst the size of the cryptocurrency market and transparency of the ecosystem renders it unsuitable for large scale sanctions evasion, the industry has been vigilant in the enforcement of sanctions.

The GDF Sanctions Working Group was mobilized with the aim to engage with agencies on the industry's needs, as well as to communicate the ways in which the industry is well-equipped and has responded effectively to deal with sanctions evasion risks.

Our crypto market analysis members have worked to understand the full extent of crypto activity in Russia and have provided knowledge and education, analysis

and reports, and free sanctions screening tools to the industry. They have linked more than 15 million crypto addresses to criminal activity with a nexus in Russia.

The creation of this report is the first step, looking to outline the operational components of sanctions compliance in the crypto and digital asset market, and is designed to aid policymakers in better understanding that the cryptoassets industry has become part of the mainstream global financial system, and is responsible player and contributor, in a global sanctions framework that has proven its utility.

We thank David Carlisle, Elliptic, and Ari Redbord, TRM Labs, our working group co-chairs who lead the work in this report with some of our most active global members. You have gone above and beyond the call of duty in your outstanding contributions to our global community, and we are grateful.

As important, we have demonstrated another use case for the global crypto industry - we can organize ourselves, come together, and collaborate on a single outcome as required by agencies, just as we did in response to the Financial Action Task Force's Recommendation 16 implementation with the development of the InterVASP messaging standard (IVMS101).

The majority of players in the global crypto industry are staffed by responsible executives, employees, and shareholders, and have knowledgeable customers.

We are vigilant to further manipulation of the crypto ecosystem that we well understand, which is publicly open and transparent, and which we monitor and report on for all to see, and we are on guard to further strengthen the ecosystem as required. ■

# Executive Summary



**Ari Redbord**  
Head of Legal & Government Affairs  
TRM Labs  
Sanctions Working Group Co-Chair



**David Carlisle**  
VP of Policy and  
Regulatory Affairs  
Elliptic  
Sanctions Working Group Co-Chair

The Russian invasion of Ukraine has accelerated public policy discussions about the potential role of cryptoassets in facilitating sanctions evasion.

The Global Digital Finance (GDF) Sanctions Working Group has produced this report to facilitate an informed policy discussion about cryptoassets and sanctions. It provides an overview of existing legal and regulatory requirements affecting cryptoassets, describes sanctions compliance capabilities in the cryptoasset sector, and summarizes actions undertaken by the public and private sectors to disrupt potential sanctions evasion risks related to cryptoassets. Among its key observations are:

- **Existing legal and regulatory frameworks are generally sufficient to mitigate the risks of cryptoassets being abused for sanctions evasion. Frameworks should be reassessed periodically to ensure they remain fit for purpose.** No major overhauls of laws or regulatory frameworks are required to address the risks of sanctions evasion through crypto. Rather, emphasis should be placed on ensuring that existing frameworks are enforced effectively, and that public sector agencies are sufficiently resourced to address emerging risks and investigate potential cases of sanctions evasion involving cryptoassets.

- **The transparency of cryptoasset transactions acts as a powerful mitigant that limits their utility for sanctions evasion.** The open, public nature of cryptoasset blockchains ensures that transactions are transparent and traceable. Agencies responsible for sanctions enforcement can leverage this traceability to counter attempted circumvention. The traceability of cryptoassets also limits their utility for sanctions evasion because it exposes sanctioned actors to potential identification.
- **The cryptoasset industry has developed technical solutions that enable compliance with sanctions measures, though use of these solutions across the sector is uneven due in part to insufficient regulatory clarity and enforcement gaps.** Cryptoasset businesses can utilize available technology solutions to detect potential sanctions evasion and identify sanctioned counterparties in transactions. This includes the use of blockchain analytics capabilities to identify addresses belonging to sanctioned parties, or transactions involving entities in sanctioned jurisdictions. Solutions also exist for enabling compliance with the Travel Rule, which requires identification and sanctions screening of transaction beneficiaries and originators. Further adoption of these solutions across the industry can be facilitated through accelerated implementation of regulation and more robust regulatory guidance.

- **Where sanctions evasion risks do exist, these can be countered through focused efforts by public and private sector stakeholders.** Industry and the public sector have already demonstrated successes in disrupting attempted sanctions evasion through cryptoassets. These efforts can be enhanced by deepening public-private intelligence sharing, education, and communication partnerships.

In light of these observations, we make the following recommendations to policymakers:

- 1) **Agencies responsible for administering and enforcing sanctions should be provided with enhanced funding, resources, training, and access to crypto-specific investigative capabilities.** Agencies such as the US Treasury's Office of Foreign Assets Control (OFAC) and the UK's Office of Financial Sanctions Implementation (OFSI) are already taking important steps to apply sanctions to the cryptoasset space. To ensure these agencies can keep pace with developments related to cryptoassets, it is critical that they receive additional funding to enable them to hire and develop teams with sufficient knowledge of cryptoassets, and to acquire crypto-specific technical capabilities, such as blockchain analytics solutions. Countries should also pursue a "whole-of-government" approach to addressing sanctions evasion risks that leverages not just regulatory capacity, but also law enforcement and national security agencies as well.

**2) Governments should work with the cryptoasset industry to establish public-private partnerships to share intelligence, insights, and best practices on crypto and sanctions issues.** Successfully addressing crypto-asset related risks requires deep and ongoing collaboration between the public and private sector. Governments should work with the private sector to establish collaborative fora for sharing actionable intelligence related to sanctions evasion activity in crypto, leveraging the transparency of cryptoassets to engage in real-time disruption of sanctions evasion. Information sharing models related to cybersecurity may offer a promising model for these efforts. The public sector should also leverage regulatory sandboxes and “tech sprint” initiatives to identify opportunities alongside the private sector for enhancing responses to sanctions challenges.

**3) Public sector agencies should provide the industry with more robust and forward-looking regulatory guidance on crypto-specific compliance challenges related to sanctions.** Certain technical features of cryptoassets present operational challenges when it comes to assessing the applicability of sanctions to certain transactions and scenarios. Addressing these challenges requires that sanctions agencies issue guidance specific to the cryptoasset industry that acknowledges these technical challenges. Sanctions agencies should also aim to provide specific guidance

on how to apply sanctions related to key components and developments within the cryptoasset ecosystem such as decentralized finance (DeFi), non-fungible tokens (NFTs), and cryptoasset mining.

**4) Sanctions enforcement agencies should establish dedicated points of contact at sanctions agencies responsible for liaising with the private sector on crypto-specific topics.** Given the highly technical nature of cryptoassets and related sanctions compliance issues, agencies responsible for sanctions enforcement should appoint appropriately skilled, dedicated points of contact responsible for liaising with the cryptoasset sector. This can enable a more fluid channel of communication and will assist public sector agencies in synthesising learnings and insights from the cryptoasset industry.

**5) Governments must work urgently to address the gaps in applying international standards on combating financial crime to cryptoassets.** Some jurisdictions have implemented legal and regulatory requirements for cryptoassets related to anti-money laundering, countering the financing of terrorism (AML/CFT), and sanctions; however, few jurisdictions are actively enforcing these requirements. A number of jurisdictions still have not implemented regulatory frameworks for cryptoassets. The failure of many jurisdictions to apply the Financial Action Task

Force’s (FATF) AML/CFT Standards to cryptoassets creates vulnerabilities in the international regime that sanctioned actors and countries can exploit, and disincentives the full, industry-wide adoption of sanctions compliance solutions. This is particularly true of continued gaps in implementation and enforcement of the Travel Rule. Closing these gaps - especially by addressing the “sunrise problem” of uneven Travel Rule implementation - is critical to ensuring that sanctioned actors cannot exploit cryptoassets successfully. ■

# Sanctions Compliance and Cryptoassets

## Current State of Regulatory and Legal Requirements

There is a common misconception that cryptoassets provide a ready-made avenue for sanctions evasion because they sit outside the regulatory and legal perimeter. In fact, sanctions authorities in many jurisdictions have ensured that relevant legal and regulatory requirements apply comprehensively to activity conducted in cryptoassets.

Consequently, authorities are equipped with the necessary enforcement powers to act against breaches of sanctions that may involve cryptoassets.

Below is a summary of key requirements and actions in select jurisdictions that illustrate the breadth of sanctions measures with which cryptoasset businesses, and individuals or entities transacting in cryptoassets, must currently comply.

### United States

In the US, economic and financial sanctions are implemented by the US Department of the Treasury's Office of Foreign Assets Control (OFAC). Since 2018, OFAC has taken numerous steps to clarify how sanctions apply to cryptoassets, and to disrupt the ability of sanctioned actors to leverage cryptoassets in evading restrictions.

In March 2018, [OFAC updated its Frequently Asked Questions](#) to clarify that all of the sanctions it implements apply to transactions in cryptoassets. This was followed in October 2021 by more extensive guidance that OFAC issued, [Sanctions Compliance For the Virtual Currency Industry](#). That guidance describes core components of a sanctions compliance framework OFAC expects of US businesses, and how these may be applied in the context of cryptoassets.

Similarly, OFAC has issued [guidance on how its sanctions apply](#) to transactions involving ransomware. This guidance - originally issued in October 2020 and subsequently updated in September 2021 - indicates that US persons effecting or facilitating ransomware payments, which are generally made using cryptoassets, may not do so where the payment would benefit a sanctioned person or otherwise violate existing sanctions measures.

Perhaps more significantly, OFAC has undertaken a number of actions to curtail the ability of sanctioned persons and countries to evade sanctions using cryptoassets.

To this end, [OFAC now routinely includes cryptoasset addresses](#) controlled by sanctioned entities and individuals as identifiers on its Specially Designated Nationals and Blocked Persons List (SDN List). US persons are prohibited from dealing with those addresses, or any other addresses belonging to SDNs.

For example, in April and May 2022, OFAC added several ethereum addresses to the SDN List belonging to the Lazarus Group, the North Korean cybercrime gang that has been involved in large thefts of cryptoassets, as well as a crypto mixing service, Blender.io, that facilitated the Lazarus Group's money laundering. (Part II of this report describes how these actions were used to disrupt North Korea's sanctions evasion activity in real time). Other actions OFAC has taken to expose the cryptoasset wallets of sanctioned actors include designations of Chinese fentanyl traffickers, Iranian cybercriminals, and Russia-linked cybercriminal actors and their support networks.

These OFAC actions not only curtail the ability of sanctioned actors to utilize their cryptoasset addresses; they also provide the private sector with essential information about sanctioned actors' cryptoasset wallets that enables more effective compliance. As described further below, the private sector can leverage this information from the OFAC SDN List to screen cryptoasset wallets and prevent prohibited transactions with them.

In addition to OFAC, the US Treasury's Financial Crimes Enforcement Network (FinCEN), which administers US anti-money laundering and countering the financing of terrorism (AML/CFT) requirements and is the US financial intelligence unit (FIU), has also acted to

address sanctions risks involving cryptoassets and provide the private sector with guidance to facilitate compliance.

In March 2022, [FinCEN issued an alert for financial institutions](#) and money service businesses warning of the risks of Russian sanctions evasion. In order to assist regulated businesses in detecting evasion, the alert sets out six red flags of potential sanctions evasion involving cryptoassets. The alert indicates that FinCEN expects regulated businesses to file suspicious activity reports (SARs) with FinCEN where they identify instances of suspected sanctions evasion involving cryptoassets.

Similarly, in May 2019, [FinCEN issued an advisory on illicit activity](#) involving convertible virtual currencies, which contains more than two dozen red flag indicators that cryptoasset businesses and other financial institutions can utilize to identify potentially suspicious activity related to sanctions evasion and other crimes.

## European Union

The EU imposes a broad range of sanctions through measures adopted by the Council of Europe and given effect by the European Commission. Following the Russian invasion of Ukraine, in March 2022 [the European Commission clarified](#) that EU sanctions adopted to date apply to transactions and activity in cryptoassets.

In April 2022, the [Commission adopted specific measures](#) aimed at restricting the ability of Russia to leverage crypto in sanctions evasion. Those measures

prohibit the provision of crypto wallet, account, and custody services to Russian nationals or entities incorporated in Russia, where the total value of cryptoassets exceeds €10,000.

## UK

In the UK, sanctions are administered by the Office of Foreign Sanctions Implementation (OFSI) at HM Treasury.

In March 2022, [OFSI issued a joint statement with the Financial Conduct Authority \(FCA\) and the Bank of England \(BoE\)](#) clarifying that existing UK sanctions apply to cryptoasset service providers and to transactions in cryptoassets. It states that, “Financial sanctions regulations do not differentiate between cryptoassets and other forms of assets. The use of cryptoassets to circumvent economic sanctions is a criminal offence under the Money Laundering Regulations 2017 and regulations made under the Sanctions and Anti-Money Laundering Act 2018.”

The UK government’s joint statement also includes a list of red flag indicators to assist the private sector in identifying sanctions evasion through cryptoassets.

## Other Requirements

Since the Russian invasion of Ukraine in February 2022, several other jurisdictions have implemented new measures, or have issued guidance, related to ensuring that sanctions measures apply to activity in cryptoassets. These include:

- **Switzerland:** In April 2022, Switzerland issued a prohibition on providing cryptoasset wallet, account, or custody services to Russian nationals or legal entities with a value of greater than CHF 10,000. This measure aligns to [similar EU measures](#) described above.
- **Japan:** In April 2022, Japan’s Diet [approved amendments](#) to the Foreign Exchange and Foreign Exchange Act to extend the scope of sanctions provisions targeting Russia to include activity in cryptoassets.
- **Singapore:** In March 2022, Singapore’s Ministry of Foreign Affairs [imposed various sanctions on Russia](#), including prohibiting financial institutions in Singapore from “entering into or facilitating any transactions in cryptocurrencies” designed to circumvent the sanctions.

## Sanctions Compliance Practices By the Industry

Cryptoasset businesses and financial institutions employ a number of controls to comply with the above measures. These involve a combination of compliance practices and systems employed across the financial sector historically, as well as newer, crypto-specific compliance systems and capabilities. These systems and controls enable the cryptoasset industry to remain resilient against attempted sanctions evasion.

This section provides an overview of key sanctions compliance practices utilized across the cryptoasset sector.

## Know Your Customer(KYC)/Customer Due Diligence (CDD) Practices

To ensure compliance with sanctions regulations, regulated businesses must take steps to determine if their customers are subject to sanctions or operate from sanctioned jurisdictions. These measures can include:

- *Identification and verification (ID&V)* - Cryptoasset businesses, like other regulated financial services providers, can take steps to verify the identity of their customers by collecting KYC information, such as government-issued identification documents. Cryptoasset business are well placed to leverage technology solutions to verify the authenticity of such documentation, and may also utilize other techniques, such as biometric identification to verify who their customers are.
- *Sanctions list screening* - Cryptoasset service providers also routinely use widely available sanctions list screening software to determine if a prospective customer appears on the OFAC SDN List or on other sanctions lists, or if an existing customer becomes the target of sanctions.

An example of cryptoasset businesses leveraging list screening capabilities to disrupt potential sanctions evasion [occurred in April 2022](#), when the cryptoasset exchange Binance announced that it had blocked numerous accounts of family members of senior Russian officials subject to sanctions. Similarly, in March 2022, the cryptoasset exchange [Coinbase announced that it had blocked](#)

[over 25,000 accounts](#) associated with Russian users that presented risks of illicit activity and sanctions evasion.

- *Geolocation* - As OFAC notes in its October 2021 guidance on virtual currencies, “One sanctions risk that members of the virtual currency industry face is from users located in sanctioned jurisdictions who try to access virtual currency products and services.”<sup>1</sup> A common technique employed by regulated cryptoasset businesses is to gather geolocation data in the form of Internet Protocol (IP) addresses that their customers use when logging on to their online accounts. A cryptoasset business can use this information to determine whether their customers may be operating from a sanctioned jurisdiction. Additionally, these techniques can enable cryptoasset businesses to identify activity that may be indicative of sanctions evasion, such as the use of Virtual Private Networks (VPNs) designed to obfuscate a customer’s location.

## Blockchain Analytics

In addition to the above capabilities, cryptoasset businesses routinely utilise solutions that have been specifically designed to identify risks related to crypto wallets and transactions. These capabilities are referred to as “blockchain analytics.”

Blockchain analytics involves leveraging data about cryptoasset wallets and transactions and attributing that blockchain-native data to real world actors. Because blockchains are visible public records of crypto

transactions, information about those transactions is readily available for analysis. Where this information can be attributed to actors such as cybercriminals, fraudsters, and sanctioned parties, it can enable regulated businesses to determine if their customers may be engaging in illicit or prohibited transactions. (In Part II below we provide further detail describing how the transparency of cryptoasset transactions can prevent sanctions evasion.)

Most cryptoasset businesses rely on software provided by third party vendors specialised in the development of blockchain analytics capabilities. There are several ways in which these capabilities can be deployed to enable compliance with sanctions requirements.

- *Wallet Screening* - As noted previously, OFAC has included on its SDN List cryptoassets belonging to sanctioned individuals and entities. Utilizing blockchain analytics software, cryptoasset business can screen wallets where their customers intend to send funds prior to executing transactions.

Where an address is identified as belonging to a sanctioned party, the business can prevent the transaction from being sent to that wallet.

- *Transaction Screening* - Cryptoasset businesses also utilize information from public sanctions lists to identify ongoing transactions involving sanctioned entities or individuals. By screening transactions, a cryptoasset business can identify if funds its customers sent or received include exposure to wallets belonging to entities or individuals on

<sup>1</sup>P.13 OFAC guidance





## The Travel Rule

Another core component of sanctions compliance is the application of the Travel Rule. The Travel Rule is a longstanding requirement aimed at enhancing transactional transparency by mandating that financial institutions obtain, hold, and securely transmit identifying information about payment originators and beneficiaries. Financial institutions must also screen this identifying information against applicable sanctions lists in order to prevent prohibited transactions.

In 2019, the Financial Action Task Force (FATF), the global standard setter for AML/CFT matters, [updated its Standards](#) to clarify that countries should require VASPs to comply with the Travel Rule. Under the FATF's guidelines, countries should ensure that VASPs gather and transmit the following information during the course of cryptoasset transfers<sup>2</sup> over USD/EUR 1,000:

- (a)** the name of the originator;
- (b)** the originator account number (or wallet address) where such an account is used to process the transaction;
- (c)** the originator's address, or national identity number, or customer identification number, or date and place of birth;
- (d)** the name of the beneficiary; and
- (e)** the beneficiary account number (or wallet address) where such an account is used to process the transaction.

Applying the Travel Rule for cryptoasset transfers presents certain technical challenges. First and foremost, the pseudonymous nature of cryptoassets makes it difficult in certain circumstances for a VASP to identify with certitude that a wallet belongs to another VASP that can receive the required originator and beneficiary information. Secondly, identifying information about originators and beneficiaries generally cannot be appended to transactions on decentralized cryptoasset blockchains but must be transmitted through a separate mechanism. Finally, the application of the Travel Rule to cryptoasset transfers has raised privacy concerns because it requires VASPs to retain substantial amounts of personal identifying information about customers and counterparties that, if compromised, can be associated with transactions on open, public blockchains.

Despite these challenges, the crypto industry has succeeded in creating numerous technical solutions that enable VASPs to comply with the Travel Rule. These include the [Travel Rule Universal Solution Technology \(TRUST\)](#), a solution developed by an alliance of US cryptoasset exchanges and custodians, as well as a number of open source protocols and proprietary compliance software.

Some VASPs have implemented Travel Rule solutions and are integrating these into their compliance processes. However, as the FATF has [highlighted in its reviews of the status of implementation](#) of its Standards, industry adoption of Travel Rule solutions remains incomplete. A key reason for this is what the FATF has termed the "sunrise problem" - the uneven

pace at which countries are transposing the Travel Rule into local law and regulation to align with the FATF Standards. Because not all jurisdictions have implemented the Travel Rule for VASPs, VASPs do not face the requirement to comply everywhere they operate, which disincentivizes compliance.

As noted in Part IV below, a key policy objective should be to ensure the full application of the FATF standards to VASPs in countries that have failed to do so. ■

<sup>2</sup>See FATF guidance, p. 57.

# Leveraging Transparency to Prevent Sanctions Evasion

The nature of public blockchains enables unprecedented visibility on financial flows. As discussed extensively above, blockchain analytics, also known as “blockchain intelligence,” is the practice of organizing and analyzing on-chain data — by timestamp, currency, address, or the service used to conduct the transaction, for example — to map trends or patterns of activity, detect links to off-chain data points, or surface other attributes that might indicate risk. Blockchain intelligence takes the raw, accessible public blockchain data and layers it with threat intelligence. Blockchain intelligence allows law enforcement, regulators, and compliance professionals more visibility on real-time financial flows than they ever had before. The nature of the blockchain — the open and distributed ledger upon which tokens can be sent — means that each transaction is verified and logged in a shared, immutable record, along with the timestamp of the transaction and the addresses involved. This data from the public blockchain is accessible to anyone.

For example, when OFAC adds a cryptocurrency address to its SDN List, that address is tagged in a blockchain intelligence tool as being connected to sanctions. This allows a cryptocurrency exchange to flag any transactions involving that address, assess the risk, and take any action that may be required of them based on regulatory requirements. In addition, blockchain intelligence is used to trace and track the movements of funds to and from an address associated with sanctions or any other illicit activity

Txn Hash	Method	Block	Age	From	To	Value	Txn Fee
<a href="#">0x57d1c2d19d30c82f34...</a>	Transfer	(pending)	28 days 7 hrs ago	<a href="#">0xb84b2c205b27d56234...</a>	IN Ronin Bridge Exploiter	0.00001 Ether	(Pending)
<a href="#">0xa0427076e8a3ae2aca...</a>	Transfer	14709620	14 days 1 hr ago	Ronin Bridge Exploiter	OUT <a href="#">0x08723392ed15743cc3...</a>	12,595.3 Ether	0.00102454237
<a href="#">0xd578594dfc23e8ec14...</a>	Transfer	14703573	15 days 59 mins ago	Ronin Bridge Exploiter	OUT <a href="#">0x3e37627deaa754090f...</a>	23,528.8 Ether	0.001052676222
<a href="#">0xc215bba75bb84fb1e3...</a>	Transfer*	14667134	20 days 18 hrs ago	<a href="#">0x46d126be6902661d64...</a>	IN Ronin Bridge Exploiter	0.00001 Ether	0.00076296
<a href="#">0xb743785cf049b0577a...</a>	Transfer*	14667050	20 days 18 hrs ago	<a href="#">0x68af8805f64dcb82be...</a>	IN Ronin Bridge Exploiter	0.00001 Ether	0.00158032
<a href="#">0x06d514d941f75671fb...</a>	Transfer*	14666525	20 days 20 hrs ago	<a href="#">0x15b853f23a236023e5...</a>	IN Ronin Bridge Exploiter	0.0001 Ether	0.000675304
<a href="#">0xadee9d8ba4bed9247c...</a>	Transfer	14666112	20 days 22 hrs ago	Ronin Bridge Exploiter	OUT <a href="#">0xf7b31119c2682c88d88...</a>	25,127.5192 Ether	0.000963818887
<a href="#">0x1dc458bb6ad496f335...</a>	Transfer*	14646409	24 days 1 hr ago	<a href="#">0x34c5b753066d64f358...</a>	IN Ronin Bridge Exploiter	0 Ether	0.001214402039
<a href="#">0x9f6a19c9fed374450dc...</a>	Transfer	14645965	24 days 2 hrs ago	Ronin Bridge Exploiter	OUT <a href="#">0x35fb6f6db4fb05e6a4c...</a>	33,568.152 Ether	0.000606449276
<a href="#">0x47e885cb65ecb70fbb...</a>	Transfer*	14633590	26 days 54 mins ago	<a href="#">0x5a1a006a7a345dfa51...</a>	IN Ronin Bridge Exploiter	0 Ether	0.000601128

The above image shows transactions from the ethereum blockchain undertaken by the Lazarus Group using the ethereum address [0x098B716B8Aaf21512996dC57EB0615e2383E2f96](#). This information is open and available for anyone to view on the public ethereum blockchain as new transactions are conducted, in real time (Source: Etherscan)

to help investigators follow the money and, in certain circumstances, work to seize it.

For example, through a sanctions designation on April 14, 2022, the US Treasury Department announced that North Korea was behind the \$600 million Ronin bridge hack, the largest crypto hack to date. Specifically, OFAC released a list of entities associated with North Korean state-sponsored hacking gang, the Lazarus Group, including this crypto Ethereum address: [0x098B716B8Aaf21512996dC57EB0615e2383E2f96](#).

The FBI announced later the same day that it was, “able to confirm Lazarus Group and APT38, cyber actors associated with the DPRK, are responsible for the theft of \$620 million in Ethereum reported on March 29.”

On April 22, 2022, OFAC added three additional Ethereum addresses associated with the hack to its SDN list. The addresses designated by OFAC had interacted with the originally sanctioned address and at one point held roughly 50,000 of the stolen ETH (approximately \$100 million). The funds were moved

through Tornado Cash, the most popular mixing service on the Ethereum blockchain. (We explain the sanctions implications of mixing services in further detail in Part III below.)

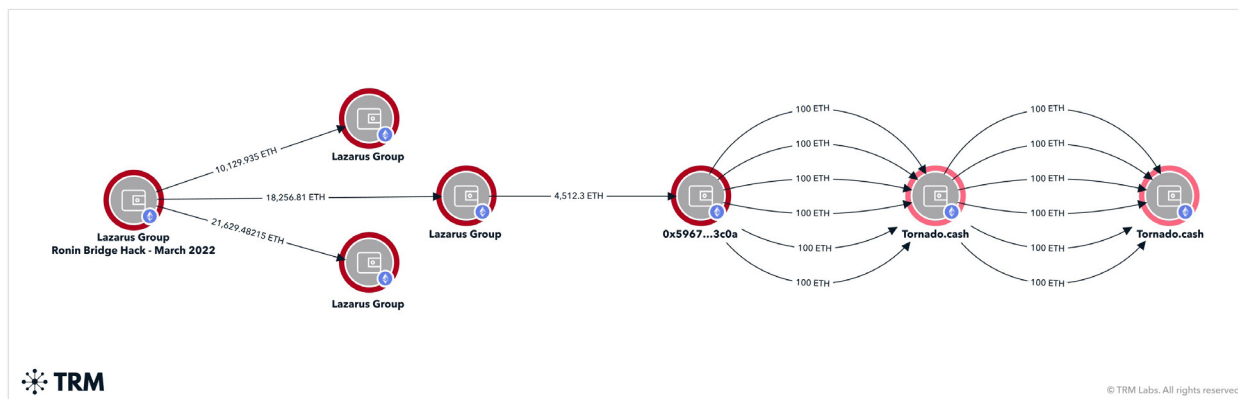
Then on May 6, 2022, OFAC sanctioned cryptocurrency mixer blender.io, another mixer that Lazarus Group used to obfuscate the flow of the Ronin proceeds. This was the first time the Treasury sanctioned a cryptocurrency mixer. According to Treasury’s press release, “Blender.io is a virtual currency mixer that operates on the Bitcoin blockchain and indiscriminately facilitates illicit transactions by obfuscating their origin, destination, and counterparties. Blender receives a variety of transactions and mixes them together before transmitting them to their ultimate destinations. While the purported purpose is to increase privacy, mixers like Blender are commonly used by illicit actors. Blender has helped transfer more than \$500 million worth of Bitcoin since its creation in 2017. Blender was used in the laundering process for North Korea’s Axie Infinity heist, processing over \$20.5 million in illicit proceeds.”

While there are myriad examples of law enforcement and regulators using blockchain intelligence tools to trace transactions and build investigations - from Lazarus Group to cybercriminals, terrorist financier to fraudsters - the idea of a regulators and law enforcement agencies using blockchain intelligence to impose sanctions in real time is new. This type of action relies on the unique nature of an open blockchain and the visibility it provides.

A recent judicial opinion is consistent with law enforcements and regulators’ unique ability to trace

Txn Hash	Method	Block	Age	From	To	Value	Txn Fee
0x1553288924a808fa81...	Deposit	14722592	12 days 1 hr ago	0x99b6843f8410ee696b...	OUT Tornado.Cash: Router	100 Ether	0.047157252
0xef72cb93dba46dfa03...	Deposit	14722574	12 days 1 hr ago	0x99b6843f8410ee696b...	OUT Tornado.Cash: Router	100 Ether	0.047157252
0x939f566cae5d4d2c00...	Deposit	14722555	12 days 1 hr ago	0x99b6843f8410ee696b...	OUT Tornado.Cash: Router	100 Ether	0.05021244
0xc8e7b3158544b21299...	Deposit	14722540	12 days 1 hr ago	0x99b6843f8410ee696b...	OUT Tornado.Cash: Router	100 Ether	0.053939924
0xfed01fe2595072d1f8b...	Deposit	14722524	12 days 1 hr ago	0x99b6843f8410ee696b...	OUT Tornado.Cash: Router	100 Ether	0.05056942
0xdbaa1d579bae87333b...	Deposit	14722486	12 days 1 hr ago	0x99b6843f8410ee696b...	OUT Tornado.Cash: Router	100 Ether	0.039536092
0xe5049bce801b95339f...	Deposit	14722450	12 days 1 hr ago	0x99b6843f8410ee696b...	OUT Tornado.Cash: Router	100 Ether	0.049931208
0x339bad50805cc3c620...	Deposit	14722429	12 days 1 hr ago	0x99b6843f8410ee696b...	OUT Tornado.Cash: Router	100 Ether	0.057005528
0xd054b25bc277551729...	Deposit	14722410	12 days 1 hr ago	0x99b6843f8410ee696b...	OUT Tornado.Cash: Router	100 Ether	0.063800988
0x3781da3ad5de98cc08...	Deposit	14722395	12 days 1 hr ago	0x99b6843f8410ee696b...	OUT Tornado.Cash: Router	100 Ether	0.0462326

The above image shows transactions on the ethereum blockchain that ultimately originated from OFAC-listed addresses belonging to the Lazarus Group and were sent to the Tornado Cash mixing service. (Source: Etherscan) The image below shows how this same transactional activity can be represented visually using blockchain analytics, which demonstrates the flow of funds from the Lazarus Group to the Tornado mixer. (Source: TRM Labs)



Transactions 0			
Fee	0.00000646 BTC (2.084 sat/B - 0.708 sat/WU - 310 bytes) (2.821 sat/vByte - 229 virtual bytes)		-24.21823000 BTC
Hash	629cb62bee02e3206fb3580fcd85e7a130f1d4a858a2db22b19933c0609ffd73		2022-03-30 12:28
	3K35dyL85fR9ht7UgzPfd1gLRXQtNTqE3	24.21823000 BTC →	325iCITPLKqo3U5YLkX3VjGWwrrAkWPuTVZ bc1q7ukgmtrqssp5mr8a95kdxn8443rxaf72kitu9e 3KAQti8TBDMVjQv9PApFvVJDsEfINB3w27 3A2dDCSox3MjVbAqYg6Rr1gipjGSTXEKga
			17.42339744 BTC 0.00352937 BTC 4.63339150 BTC 2.15790523 BTC
Fee	0.00013506 BTC (2.807 sat/B - 1.506 sat/WU - 4811 bytes) (6.024 sat/vByte - 2242 virtual bytes)		+24.21823000 BTC
Hash	4534ece6505de39f0f842d40eb0f3ec9ffa27e1ecf630015d9caeb268f297a6		2022-03-29 05:12
	bc1qvhw8s4n4j2zfcnwey540ymq92fkfyvgze3gmxg bc1qvhw8s4n4j2zfcnwey540ymq92fkfyvgze3gmxg bc1qvhw8s4n4j2zfcnwey540ymq92fkfyvgze3gmxg bc1qvhw8s4n4j2zfcnwey540ymq92fkfyvgze3gmxg	2.67926581 BTC → 3.70010680 BTC 3.12493514 BTC 2.80770098 BTC	3K35dyL85fR9ht7UgzPfd1gLRXQtNTqE3 bc1q4afkmgw8p8jmr9dke04edqztrmp45zdxjxcct2y
			24.21823000 BTC 63.73654400 BTC

The image shows transactions on the bitcoin blockchain undertaken by blender.io using the bitcoin address 3K35dyL85fR9ht7UgzPfd1gLRXQtNTqE3, which OFAC included on the SDN List. The blockchain shows the time, date, and value of each transaction with this address, as well as the addresses that transacted with it. Investigators and compliance staff can utilize this data from the bitcoin blockchain to identify potential transactions with blender in real-time. (Source: Blockchain.com)

and track transactions in crypto to investigate sanctions evasion. The memorandum opinion, written by Federal Magistrate Judge Zia Faruqui of the United States District Court for the District of Columbia who has written a number of opinions on the use and reliability of blockchain intelligence tools, highlights the use of blockchain analytics to investigate sanctions evasion. Specifically, the government alleges in a criminal complaint that an unnamed defendant operated a payments platform based in a sanctioned jurisdiction. The operation of the payments platform, involved “establishing a U.S.-based front company to facilitate the purchase of domains, using U.S. financial accounts to conduct financial services, and transferring virtual currency to accounts associated with platform.”

The payments platform advertised its services as designed to evade U.S. sanctions, including through purportedly untraceable virtual currency transactions. The defendant also opened accounts with a U.S.-based crypto exchange from which s/he bought and sold bitcoin. The defendant used these accounts to transmit over \$10 million worth of bitcoin between the United States and sanctioned country for the payments platform’s customers.

The opinion, littered with great pop culture references throughout, begins by adopting OFAC’s recent guidance that “sanctions compliance obligations apply equally to transactions involving virtual currencies and those involving traditional fiat currencies,” before



The image above illustrates how blockchain intelligence can be used to investigate funds flows related to sanctions evasion. It shows the the Lazarus Group (whose bitcoin wallets are represented by the red circle) sending funds to blender.io (whose bitcoin wallets are represented by the blue circle), the bitcoin mixing service sanctioned by OFAC. (Source: TRM Labs)

delving into the use of blockchain analytics. Judge Faruqui writes, "Appearing to rely on this perceived anonymity, defendant did not hide the payments platform's illegal activity. Defendant proudly stated the payments platform could circumvent U.S. sanctions by facilitating payments via bitcoin." The opinion continues, "Yet by following the (virtual) money, the government established by probable cause that defendant was operating the Payments Platform. Law enforcement synthesized subpoena returns from virtual currency exchanges, email search warrant returns, banking information, and shell company registration information to reliably dox defendant."

The District Court for the District of Columbia is one of the first to find that blockchain analytics are reliable for

a finding of probable cause in support of a search or arrest warrant. As courts continue to see cases on the use of blockchain analytics to mitigate sanctions and other illicit finance risk, we are likely to see a developing body of case law. ■

# Sanctions Evasion Risks

As highlighted throughout this report, certain technical features of cryptoassets, as well as robust existing regulatory frameworks and compliance practices, make large-scale systematic sanctions evasion challenging and often impractical.

Additionally, cryptoasset markets lack the scale, liquidity, and interconnectedness with the mainstream financial sector necessary to enable sanctioned nation states such as Russia, Iran, and North Korea to circumvent the overwhelming sanctions they face at a macro scale. As a point of comparison, the total assets held by the Russian banking sector total approximately \$1.4 trillion, whereas the total market capitalization of all cryptoassets in May 2022 was approximately \$1.2 trillion. Cryptoassets simply cannot sustain the economies or financial activity of sanctioned nation-states at scale.

Nonetheless, there are sanctions evasion risks associated with certain types of cryptoasset activity, and a number of high-profile cases underscore how these risks are evolving. This section describes these risks, as well as efforts underway across the public and private sectors to identify and deter them using existing legal authorities.

## Cybercrime

Cybercrime is one method that sanctioned nation states and actors have employed to access cryptoassets and transfer funds outside the banking sector.

North Korea's cybercriminal activity involving cryptoassets is well documented. In particular, a number of large cybercriminal hacks of cryptoasset exchanges and other platforms have been perpetrated by the Lazarus Group, North Korea's cybercriminal group. Reporting suggests that North Korea steals cryptoassets and then converts the funds to fiat currencies to launder them through the Chinese banking system, potentially to fund its weapons proliferation activities. Credible estimates suggest that North Korea has succeeded in stealing approximately \$1 billion in cryptoassets.

The US government has taken several actions to disrupt North Korea's cryptoasset theft. In March 2020, OFAC sanctioned two Chinese nationals who assisted the Lazarus Group in laundering more than \$250 million in funds stolen from cryptoasset exchanges and included their cryptoasset addresses on the SDN List. These same individuals were [indicted by the US Department of Justice in March 2020](#) as well.

As described above, OFAC has since undertaken several additional actions to list cryptoassets belonging to the Lazarus Group and associated with the theft of more than \$540 million in cryptoassets from the Ronin Bridge, a decentralized finance (DeFi) application. Cryptoasset businesses can use this information to block transactions undertaken by the Lazarus Group. In April 2022, [the cryptoasset exchange Binance](#)

stated that it had frozen more than \$5 million worth of cryptoassets associated with the Ronin Bridge hack.

OFAC has also taken a number of actions to target ransomware perpetrators and their support networks. The 2017 WannaCry ransomware attack has been attributed to the OFAC-sanctioned Lazarus Group. OFAC has also [sanctioned the Iran-based facilitators of the SamSam ransomware attack](#), as well as [Russia-based ransomware gangs](#) and their facilitation networks, and has included their cryptoasset addresses on the SDN List.

## Mining

Another category of activity that can present sanctions risk is cryptoasset mining. Mining refers to the process of validating cryptoasset transactions. Miners supply computing power to facilitate transactions on behalf of other cryptoasset users and are in turn rewarded with cryptoassets for providing this service to the network. Mining therefore offers a way to generate revenue in the form of cryptoasset rewards.

Mining bitcoin is a computationally intensive process and requires access to significant energy resources, which are abundant in some sanctioned jurisdictions. Some sanctioned nation states have looked to crypto mining as a potential source of revenue in the face of sanctions. Most notably, Iran has established a licensing framework for bitcoin mining domestically.

In return for allowing miners to use Iran's energy reserves, the Central Bank of Iran (CBI) collects a portion of the bitcoin rewards generated. Blockchain analytics firm Elliptic estimates that the scale of mining in Iran could generate as much as \$1 billion in revenues for the Iranian government. This enables Iran to monetize energy resources it struggles to export in the face of sanctions.

The Russian government has publicly expressed interest in establishing a similar framework for bitcoin mining. In January 2022, Russian President Vladimir Putin stated that Russia has a competitive advantage in bitcoin mining owing to its vast energy resources. In March 2022, Russia's deputy energy minister called for the government to expedite the roll out of a legal framework to allow the government to oversee and regulate mining, much like Iran.

In response, OFAC has taken preemptive action to prevent Russia from leveraging crypto mining in the face of sanctions. In April 2022, OFAC sanctioned BitRiver, a bitcoin mining firm based in Russia, in an effort to prevent Russia from leveraging its energy reserves to mine cryptoassets and generate revenue in the face of sanctions. Consequently, US persons are prohibited not only from transacting with BitRiver, but also from providing it with bitcoin mining equipment or other goods and services.

## Mixers

One method some sanctioned actors have used to conceal their cryptoasset activity is the use of crypto mixers. Mixers are a form of privacy-enhancing

technology that combines users' cryptoassets and provides them with new coins whose original provenance can no longer be discerned. Consequently, mixers enable illicit actors to obfuscate their original source of funds, which can frustrate efforts to investigate them.

As described in Part II of this report, the Lazarus Group has relied on mixers as part of North Korea's efforts to launder its ill-gotten cryptoassets. In April and May 2022, the Lazarus Group utilized numerous mixing services to launder funds it stole from its hack of the Ronin Bridge. In response, OFAC on May 6, 2022 issued sanctions on Blender.io, one of the mixing services the Lazarus Group used to launder as much as \$20.5 million from the hack. As a result of this action, cryptoasset businesses and financial institutions must ensure that they do not facilitate transactions with Blender.io, hindering the ability of actors such as the Lazarus Group to cash out the proceeds of their crimes.

Blockchain analytics can also play a role more broadly in enabling cryptoasset business and financial institutions in identifying red flags associated with mixers that may prevent attempted sanctions evasion. While mixers can succeed in obfuscating a user's ultimate source or destination of funds, activity involving mixers is nonetheless detectable. Owing to the transparent nature of the blockchain, analytics software can identify where funds have been sent to or from a mixer, even if the complete funds trail is broken.

Consequently, regulated businesses that use blockchain analytics capabilities in their compliance operations to

identify when their customers send funds to, or receive funds from, a mixer - and they may use this information to take appropriate action, such as notifying law enforcement and filing SARs where they have concerns that illicit activity such as sanctions evasion may be at hand.

## High Risk VASPs

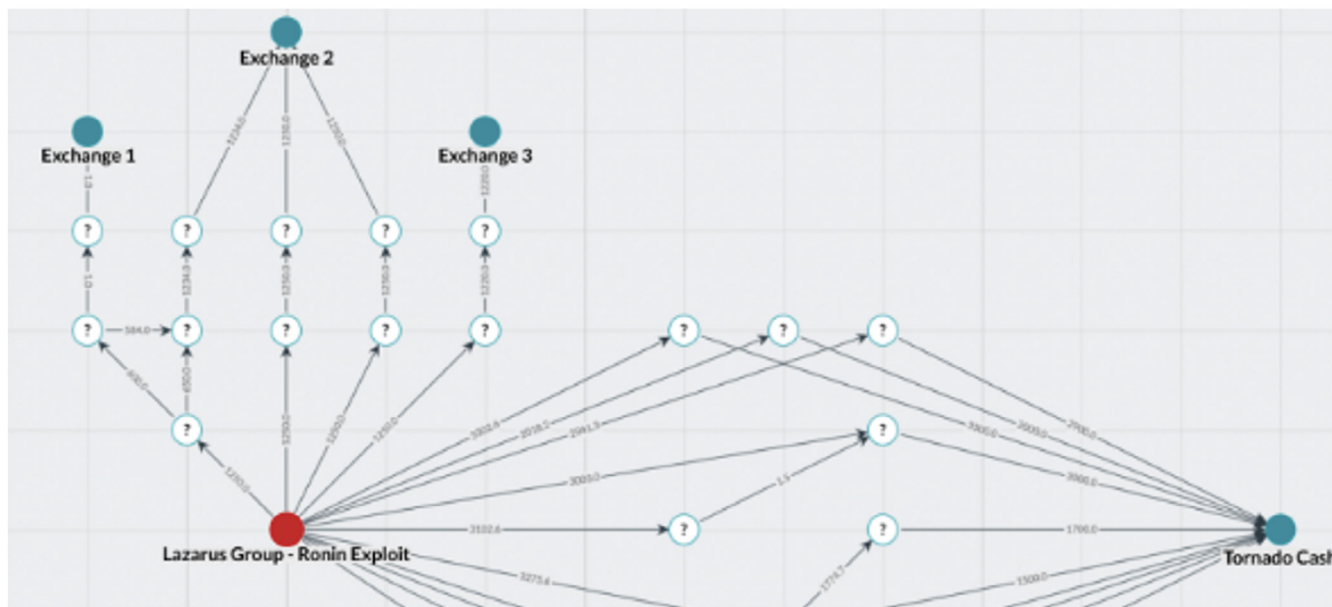
As discussed elsewhere in this report, VASPs in many major financial centers today face extensive regulatory requirements and undertake efforts to comply with these measures. However, in many parts of the world, VASPs are subject to insufficient regulation, or are not regulated at all.

Consequently, there are VASPs in some jurisdictions that do not comply with any AML/CFT or sanctions requirements. These VASPs frequently do not collect KYC information of users, allowing users to trade cryptoassets anonymously. In some cases, they may even be knowingly facilitating illicit activity.

High risk VASPs may operate from sanctioned jurisdictions, or may facilitate transactions with sanctioned jurisdictions. Blockchain analytics firms such as Elliptic and TRM Labs have identified several hundred VASPs operating in, or servicing the Russian market. Some of these exchanges have been prolific in facilitating large volumes of money laundering activity on behalf of Russia-based illicit actors.

Requisite legal authorities already exist to enable action against these high risk VASPs. OFAC has to date taken three major actions targeting Russia-linked VASPs:





The image illustrates the Lazarus Group sending funds to Tornado Cash, an ethereum mixing service. The image demonstrates that investigators can leverage information from open public blockchains to identify sanctions-related activity involving mixing services, and can subsequently report this information to relevant authorities or enforcement agencies. (Source: Elliptic)

- September 2021: OFAC sanctioned SUEX, a Czech-registered exchange service
- November 2021: OFAC sanctioned Chatex, a Latvia-registered exchange service
- April 2022: OFAC sanctioned Garantex, an Estonian-registered exchange service

While located outside of Russia, these three exchange businesses existed for one purpose: to assist Russia-based criminals in laundering their illegally obtained cryptoassets. Collectively, SUEX, Chatex, and Garantex enabled ransomware gangs, darknet market vendors

of narcotics, and other illicit actors based in Russia to launder hundreds of millions of dollars worth of bitcoin.

OFAC's sanctions prohibit US cryptoasset exchange services and financial institutions from facilitating transactions with these high risk VASPs - ensuring that they cannot access necessary financial services from US-based businesses in support of their activity.

In the case of Russia, without access to the global financial system, Russia will need to find alternatives. If Russia does turn to crypto to evade sanctions, Russian actors will need on ramps to obtain cryptocurrency and off ramps in order to convert crypto into more usable traditional currencies. According to TRM, Russia has

over 340 total VASPs, Ukraine 170, Estonia 360, and Belarus 10, which could be used by Russians to evade sanctions. These VASPs overwhelmingly do not apply AML/CFT or KYC measures and can be easily exploited by sanctioned actors. Compliant VASPs worldwide will need to have the compliance controls in place described in Part I of this paper to mitigate the risk of facilitating transactions with VASPs used by Russia, or sanctioned Russian individuals and entities, to evade sanctions. ■

# Policy Recommendations

In this section we provide several recommendations for policymakers. If implemented successfully, these actions can enable the public and private sectors to continue mounting effective responses and will ensure that the risks of cryptoassets facilitating sanctions evasion are minimized.

## Recommendation 1:

**Agencies responsible for administering and enforcing sanctions should be provided with enhanced funding, resources, training, and access to crypto-specific investigative capabilities.**

As described throughout this report, there is already a robust legal and regulatory framework in place in many jurisdictions that ensures sanctions apply to cryptoasset transactions and business activities. Additionally, agencies and bodies such as OFAC, OFSI, the European Commission, and others, have taken important steps to ensure that the cryptoasset sector understands its obligations to comply with sanctions measures, and can do so effectively.

However, ensuring the effective ongoing application of sanctions to cryptoassets will require that agencies responsible for sanctions implementation and enforcements have access to adequate funds and resources. The rapid evolution of cryptoassets, and the specific technical issues they present, places pressure on public sector agencies to keep pace, and demands

that sanctions enforcement agencies have access to skill sets and tools specific to cryptoassets.

To this end, it is essential that agencies responsible for sanctions administration and enforcement receive enhanced funding that will ensure they are equipped to surmount these challenges. This should include funding to enable them not only to recruit additional staff who can specialize in cryptoasset-related matters and carry out investigations, but also to provide staff with additional technical training and education on cryptosets.

Additionally, sanctions enforcement agencies should have access to blockchain analytics capabilities to ensure they can adequately identify, monitor, and respond to sanctions evasion risks involving cryptoassets. Staff should be trained on how to use these bespoke systems and leverage them in the course of sanctions evasion investigations.

Lastly, countries should also pursue a “whole-of-government approach to addressing sanctions evasion risks that leverages not just regulatory capacity, but also law enforcement and national security agencies that can be brought to bear in building an understanding of emerging sanctions evasion risks related to crypto.

## Recommendation 2:

**Governments should work with the cryptoasset industry to establish public-private partnerships to share intelligence, insights, and best practices on crypto and sanctions issues.**

The effective implementation of sanctions demands close collaboration between the public and private sector. The establishment of public-private partnerships (PPPs) dedicated to the nexus between sanctions and cryptoassets should be a priority.

PPPs can take several forms with specific objectives. Firstly, intelligence sharing PPPs can assist the public and private sector in detecting both specific threats and emerging risks related to sanctions and cryptoassets. To this end, governments and the cryptoasset industry should explore the creation of PPPs that leverage the transparency offered by blockchains to provide real-time insights about sanctions evasion. This could include, for example, mechanisms outside of existing suspicious activity reporting (SAR) regimes that allow cryptoasset businesses to undertake rapid reporting addresses associated with suspected sanctions evasion that can be disseminated to government agencies and industry peers in real time.

Several PPP financial intelligence sharing initiatives exist in other parts of the financial sector that may

offer a model for information sharing on sanctions and cryptoassets. For example, the [UK's Joint Money Laundering Steering Group \(JMLIT\)](#), an initiative of the UK's National Economic Crime Centre (NECC) serves as an official forum for major UK financial institutions to share intelligence collectively, and with law enforcement agencies, aimed at disrupting specific financial crime threats. A more private-sector driven initiative launched in the US was the formation of the Financial Services Information and Analysis Center (FS-ISAC). FS-ISAC serves as a global intelligence sharing community on cyber security threats impacting financial institutions. Financial institution members of FS-ISAC can share information with one another about cyber security risks, and FS-ISAC also facilitates information sharing about these industry identified threats with the public sector.

Similar initiatives could allow the cryptoasset industry to share information on emerging sanctions evasion threats with the public sector more fluidly.

Secondly, PPPs can enable stakeholders to identify opportunities for enhancing sanctions enforcement and compliance. For example, sanctions agencies could establish regulatory sandbox frameworks that allow industry to test new innovations for enabling sanctions compliance in a controlled environment with input from regulators. Similarly, governments could launch sanctions-focused “tech sprints” or “regulatory sprints” that bring the public and private sector together to discuss new and innovative approaches for enhancing regulatory approaches.

There are already examples of crypto-focused “sprints” initiated by regulators that could offer a model for sanctions-specific fora. In March 2021, the New York Department of Financial Services (NYDFS) organized a tech sprint on designing a digital regulatory reporting framework for virtual currency companies. The sprint brought members of the cryptoasset industry together with regulators, law enforcement, and other public sector representatives to explore potential [technical solutions for enhancing regulatory reporting of cryptoasset activity](#).

Similarly, in May 2022, the UK's FCA organized a [CryptoSprint](#). The initiative brought representatives from the cryptoasset industry, financial institutions, and the FCA together to explore options for enhancing and evolving the UK's regulatory response to cryptoassets.

OFAC and other agencies responsible for sanctions enforcement should initiate sprint events aimed at improving coordination with the private sector on cryptoasset-related issues.

Additionally, the public and private sectors should identify opportunities for ongoing educational exchanges related to cryptoassets. This could include cross-sector training initiatives in which the private sector educates the public sector about key compliance challenges, emerging technological developments, and other matters, while the public sector educates the private sector about emerging issues of concern or areas of investigative focus related to sanctions.

One existing initiative that has undertaken this type of educational activity more broadly is the [Blockchain Alliance](#), a collective of cryptoasset industry firms who work collectively to educate the public sector on emerging challenges related to security and financial crime issues. Similar initiatives focused on sanctions risks and compliance challenges can foster a deep, ongoing dialogue between industry and relevant public sector agencies.

### **Recommendation 3:**

**Public sector agencies should provide the industry with more robust and forward-looking regulatory guidance on crypto-specific compliance challenges related to sanctions.**

As noted above, OFAC and other public sector bodies have provided helpful guidance to the private sector explaining how sanctions apply in the context of cryptoasset activity. However, the cryptoasset sector requires more specific and forward looking guidance to ensure that key challenges are addressed effectively, and that the industry understands how to comply with sanctions measures in light of rapidly evolving features of the technology.

For example, a common challenge encountered in the cryptoasset space relates to how to assess the relevance of “hops” in cryptoasset transactions for sanctions purposes (“hops” refers to the transfer of a cryptoasset through numerous intermediary wallets before arriving at its final destination - activity which is visible to any observer viewing transactions from the blockchain). That is, where a cryptoasset business

is in receipt of funds that may have been tainted from a previous association with a sanctioned actor, it is often not clear how that business should treat those funds if they have previously passed through numerous wallets. There is currently no regulatory guidance that addresses this specific technical challenge, which has no direct parallel in the traditional financial sector. Guidance from OFAC and other relevant regulatory bodies on how to apply sanctions compliance principles in the context of hops would provide the cryptoasset industry with an important understanding of how to deploy compliance resources efficiently and effectively to manage sanctions risks.

Similarly, there are specific sanctions challenges associated with cryptoasset mining - such as the implications of handling cryptoassets mined by a sanctioned actor - that warrant clarification in officially issued guidance.

Additionally, sanctions agencies should provide guidance related to the emergence of new innovations in the cryptoasset space. This includes explaining how sanctions can apply in the context of decentralized finance (DeFi), non-fungible tokens (NFTs), stablecoins, and other industry-specific developments.

#### **Recommendation 4:**

**Sanctions enforcement agencies should establish dedicated points of contact at sanctions agencies responsible for liaising with the private sector on crypto-specific topics.**

Periodic public-private initiatives and sector specific guidance are important. However, ongoing and permanent interaction between regulatory and enforcement with the cryptoasset industry on sanctions-specific topics is critical to ensuring that the industry can continue to maintain high standards of sanctions compliance.

To that end, sanctions authorities such as OFAC and OFSI should appoint dedicated specialist points of contact who can act as points of ongoing liaison with the private sector on cryptoasset-related topics.

Appointing dedicated POCs for industry liaison will also ensure that those agencies benefit from ongoing information and insights from the cryptoasset sector. This will better equip those agencies to identify opportunities to issue sector-specific guidance as described above and to address emerging challenges in a timely and targeted fashion.

#### **Recommendation 5:**

**Governments must work urgently to address the gaps in applying international standards on combating financial crime to cryptoassets.**

As described throughout this report, a significant source of sanctions evasion risk derives from the ability of sanctioned actors to use VASPs that do not apply AML/CFT or sanctions controls. These VASPs overwhelmingly operate from jurisdictions that have failed to implement the FATF's Standards as relates to VASPs. The FATF itself has highlighted the scale of the gap in the implementation of its Standards

related to the sector, and the consequences of these failures of implementation. In its July 2021 [review of the implementation of its Standards](#) related to virtual assets and VASPs, the FATF noted that "These gaps in implementation mean that there is not yet a global regime to prevent the misuse of virtual assets and VASPs for money laundering or terrorist financing."

The US, UK, EU, Japan, and other countries should continue to work through the Virtual Asset Contact Group (VACG) at the FATF to press for accelerated implementation of the FATF Standards to close these gaps. Similarly, Singapore, as the incoming president of the FATF, should prioritize the rapid implementation of the FATF Standards globally as a key pillar of ensuring that sanctioned actors cannot leverage high risk VASPs or jurisdictions to undermine international sanctions efforts. This should include encouraging countries to ensure effective enforcement of regulatory requirements, as well as concrete steps to address the "sunrise problem" of uneven implementation of the Travel Rule globally.

Regulatory agencies globally can assist the private sector by publishing guidance on risks associated with high risk VASPs, and appropriate mitigation strategies. OFAC and other sanctions authorities should also identify opportunities to leverage existing legal frameworks to impose sanctions on additional high risk VASPs - similar to those already undertaken against certain Russia-linked VASPs, as described in Part III of this report - known to facilitate sanctions evasion activity. ■

# Report Contributors



**Liat Shetret**  
Director of Regulatory Affairs  
& Compliance Policy  
**Solidus Labs**



**Elizabeth Boison**  
Partner  
**Hogan Lovells**



**Chris Ford**  
Head of Government Affairs — EMEA  
**R3**

**José Manuel**  
Tassara de León



**Malcolm Wright**  
Founder  
**InnoFi Advisory**



**Angel Niño Torres**  
Head of Compliance  
**Coinbag**



**Carol R. Van Cleef**  
CEO  
**Luminous Group**



**Manish Garg**  
CEO  
**Banksly**



**Mark D. Young**  
Strategic Advisor  
**ConsenSys**



**G B B C**  
DIGITAL  
FINANCE




**HEADQUARTERED AT:**

GBBC Digital Finance  
128 City Road  
London  
EC1V 2NX  
United Kingdom

**CONTACT US:**

**e:** [hello@gdf.io](mailto:hello@gdf.io)  
**w:** [www.gdf.io](http://www.gdf.io)

**FOLLOW US:**

 [@GlobalDigitalFi](https://twitter.com/GlobalDigitalFi)  
 [Global Digital Finance](https://www.linkedin.com/company/global-digital-finance)  
 [@GlobalDigitalFinance](https://medium.com/@GlobalDigitalFinance)