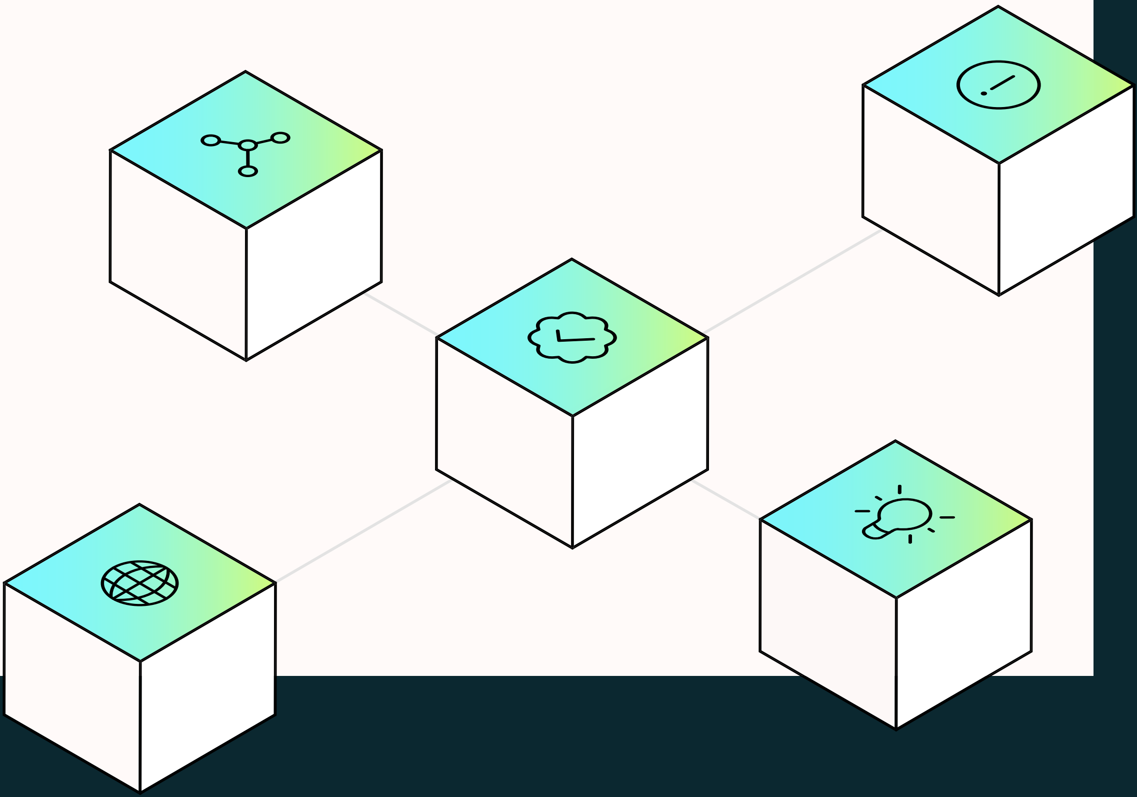
ELLIPTIC REPORT 2023

Sanctions Compliance in Cryptocurrencies

Using Blockchain Analysis to Mitigate Risk



ELLIPTIC

Sanctions Enforcement Ramping Up For the Crypto Space

Since Elliptic published the first version of this report in May 2019, sanctions activity impacting the crypto space has gone into overdrive.

In February 2022, the US, EU, UK and other countries imposed major financial and trade sanctions on Russia following its attack on Ukraine. While there has not been evidence of widespread sanctions evasion by Russia using crypto, there are indications that it is exploring avenues such as crypto mining to generate revenue. This led the US Treasury's Office of Foreign Assets Control (OFAC) to sanction the Russian mining service BitRiver in April 2022. Russian paramilitary groups fighting in Ukraine have also fundraised using crypto, as we've outlined in our separate "Crypto in Conflict" report.

Sanctions have been directed increasingly at mixing services such as Blender and Tornado Cash, which the US Treasury sanctioned last year for facilitating North Korean money laundering. Sanctions authorities in the US and UK have also been training their sights on the ransomware ecosystem in an effort to hit back at ransomware gangs.

Enforcement for crypto-related breaches of sanctions rules is also heating up, as was demonstrated by the seven-figure US Treasury settlement last year with the Bittrex crypto exchange for apparent violations of sanctions involving countries such as Iran.

Amid this rapidly evolving sanctions landscape, it is critical that cryptoasset businesses and financial institutions consider the impact on their compliance operations. They should also proactively take steps and immediately implement available compliance solutions to mitigate the significant risks involved.

Cryptoasset businesses and financial institutions must prepare for an ever-tightening sanctions compliance environment. Those that fail to take appropriate steps now could find themselves in regulators' crosshairs, risking large fines or penalties. Avoiding dealings with crypto addresses controlled by sanctioned entities and countries should be a top priority for any crypto business or financial institution.

How Elliptic Can Help

Compliance teams at cryptoasset businesses and financial institutions will need to be alert to potential sanctions evasion activity involving sanctions jurisdictions such as Russia, Iran and North Korea, as well as entities and individuals on sanctions lists, and they should take these risks seriously.

It is important to take steps proactively now to protect your team from potentially facilitating prohibited transactions or interacting with designated individuals or entities.
A first essential step is having access to wallet and transaction screening capabilities that can enable you to identify prohibited crypto addresses and counterparties.

Five Key Steps

In this report, we take a look at five key steps your team can take to navigate the emerging challenge of cryptocurrency sanctions compliance with success. These are:

1.

Deploying Effective Blockchain Monitoring Solutions and Leveraging Holistic Screening

Have you deployed blockchain monitoring solutions that rely on best-in-class data? Do you conduct pre-transaction wallet screening to prevent interactions with prohibited addresses? Can you identify sanctions risks involving cross-chain and cross-asset services?

2.

Managing Your Country Risk Exposure

Are you able to identify more subtle signs of sanctions risks, such as potential exposure to entities located in or near sanctioned jurisdictions?

3.

Knowing the Red Flags

In addition to geographical risk indicators, are your staff aware of red flags and suspicious indicators indicative of high-risk activity that may carry sanctions risks?

4.

Defining Your Investigative Strategy

Where risks have been identified, are you equipped to investigate potential sanctions breaches and report them to the appropriate authorities?

5.

Embedding a Comprehensive Risk Management Framework

Have you conducted a sanctions risk assessment to measure your overall level of risk exposure, and have you designed the processes and procedures necessary to mitigate that risk? Has your compliance team undergone the appropriate training needed to identify sanctions risks and ensure compliance?

→ 01.

Deploying Effective Blockchain Monitoring Solutions and Leveraging Holistic Screening

Avoiding exposure to sanctioned entities and individuals that use cryptocurrencies requires having the right technical solutions in place. Correctly utilizing the solutions we have developed at Elliptic – which rely on best-in-class data quality – can enable you to engage in efficient risk-based monitoring and to detect potential connections to sanctioned parties with confidence.

There are two essential components of blockchain analytics that any compliance team should have in place if it wants to be compliant with sanctions requirements:

- Pre-transaction wallet screening.
- Post-transaction screening to determine the ultimate source and destination of funds.

Screening destination crypto addresses prior to allowing customers to withdraw funds is critical to ensuring that you don't make funds available to a sanctioned person or jurisdiction. Monitoring fund flows on an ongoing basis is critical for identifying attempted sanctions evasion among your customers' transactions. Elliptic's data set contains crypto addresses belonging to individuals and entities on global sanctions lists, as well as information about exchanges and other entities using crypto in jurisdictions such as Iran, North Korea and Russia.

As the case study below demonstrates, screening customer wallets and transactions against these addresses can prevent a crypto business or financial institution from facilitating a prohibited transaction.

Case Study: OFAC Sanctions Tornado Cash

On August 8th 2022, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned Tornado Cash – a decentralized crypto mixer operating on a number of blockchains, including Ethereum. As Elliptic's research has shown, Tornado Cash has enabled criminals to launder more than $1.5 billion in criminal proceeds, including funds associated with North Korea's crypto-enabled sanctions evasion.

As part of the action, OFAC included 45 of Tornado Cash's cryptoasset addresses – in Ethereum and the USDC stablecoin – on its Specially Designated Nationals and Blocked Persons List (SDN List) to assist the private sector in complying.

Blockchain analytics solutions can assist in detecting addresses controlled by sanctioned parties. Elliptic's best-in-class data set enables us to identify other addresses controlled by sanctioned entities, in addition to those on the SDN List. This includes other addresses associated with Tornado Cash, which have not yet been added to the list.

By screening customer wallets and transactions using Elliptic's solutions, compliance teams can ensure comprehensive risk detection.

Additionally, the ability of our solutions to trace back through an infinite number of hops until we identify a sanctioned entity can enable compliance teams to identify other factors about a transaction that can enable a more informed view than less robust solutions.

For example, a compliance team might identify that the funds their customer received went from Tornado Cash to the customer's wallet through a large number of hops – or intermediary wallets – in a very short period of time. This is a common red flag we see in cases of money laundering related to cybercrime, and which may indicate elevated sanctions risks.

It is important when assessing sanctions risks not to draw a specific line when it comes to evaluating the number of hops. For example, a compliance team should not take a blanket approach that where there is sanctions exposure in a transaction, it will stop investigating if the exposure is more than five hops back in the transaction trail. As described in the scenario above, there may be risks of sanctions violations further back in the transaction trail that goes undetected using such an approach.

Rather, compliance teams should then evaluate a combination of factors – such as the exposure, proximity and velocity of a transaction involving a sanctioned entity – to make an informed decision about how to respond.

Using Elliptic Navigator – our transaction screening solution – cryptoasset exchanges and financial institutions can identify transactions with OFAC-sanctioned entities such as Tornado Cash and can take appropriate steps to block or report funds as required by OFAC.

It is also critical that any blockchain analytics capabilities that a compliance team uses enable them to detect risks involving cross-chain and cross-asset services. As Elliptic has outlined in our "State of Cross-chain Crime" report, illicit actors are now laundering billions of dollars worth of funds through services in the decentralized finance (DeFi) space.

Cross-chain crime has been made possible by recent developments in the decentralized finance (DeFi) space. Robust liquidity on decentralized exchanges (DEXs) is enabling more and more users to participate in the DeFi space. However, most DEXs do not apply anti-money laundering (AML) controls, and this allows criminals to swap assets rapidly through them as part of the money laundering process.

For example, using DEXs, criminals can readily exchange Ether for other assets – such as Tether, USDC and many more – that operate using Ethereum's ERC-20 protocol in an attempt to break the trail of traceability. In June 2022, North Korean cybercriminals did just that to launder the funds they stole after hacking a major DeFi service.

Another game changer has been the emergence of cross-chain bridges – services that allow a user to transfer assets seamlessly from one blockchain, such as Bitcoin, to another, such as Ethereum. Before the advent of bridges, crypto users could not move readily across blockchains to access DeFi services. But with bridges, DeFi services are able to thrive as part of an increasingly interwoven cross-chain ecosystem.

However, criminals have also identified that bridges offer an ideal method for laundering their ill-gotten crypto across blockchains. To date, one cross-chain bridge, the RenBridge – which allows users to move funds across Bitcoin, Ethereum and other blockchains – has processed more than $540 million in illicit transactions. This includes more than $153 million laundered by ransomware attackers, as well as $33.8 million which originated from the hack of the Liquid crypto exchange platform, and which has since been attributed to North Korean cybercriminals, who used RenBridge to try and hide their stolen Bitcoin.

As part of its efforts to disrupt the activity of threat actors, the US Treasury's Office of Foreign Assets Control has, since 2018, listed crypto addresses on its Specially Designated Nationals and Blocked Persons List (SDN List). To date, OFAC has listed more than 400 crypto addresses belonging to cybercriminals, money launderers, narcotics traffickers and their support networks.

Importantly, OFAC has clarified that the SDN List is non-exhaustive: that is, it expects US persons – such as crypto exchanges operating in the US, or operators of DeFi platform web interfaces who are US citizens – to avoid transactions not only with those crypto addresses that appear on the SDN List, but also with any other addresses that sanctioned entities control.

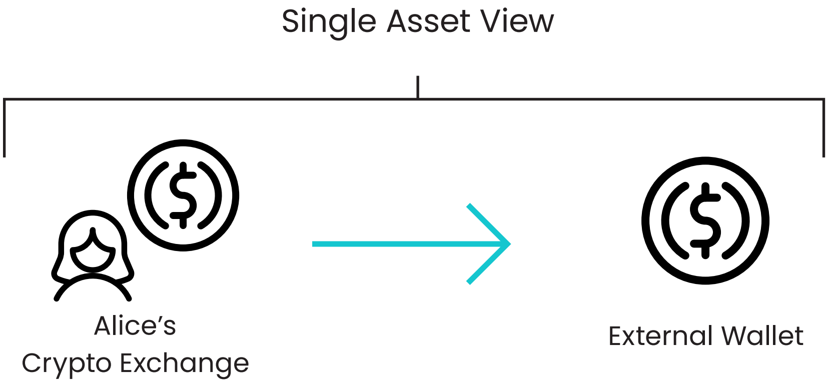
To surmount this challenge, compliance teams have relied on blockchain analytics capabilities to detect prohibited addresses. Through techniques such as "clustering", blockchain analytics capabilities make it possible to identify additional crypto addresses that a sanctioned entity controls, but which may not appear obvious to the average crypto user. Blockchain analytics have therefore become a critical component of sanctions compliance – an essential safeguard for anyone looking to comply with OFAC sanctions. In guidance for the crypto industry, both OFAC and the New York Department of Financial Services (NYDFS) have highlighted the role that blockchain analytics can play in sanctions compliance.

However, legacy blockchain analytics solutions face a limitation: they only enable compliance teams to screen against the OFAC list on a single-asset basis. A compliance team can use legacy blockchain analytics solutions to identify whether a particular address is connected to other addresses of the same asset that appears on the OFAC list, but they will not be able to identify instantly if that same wallet presents sanctions risks related to underlying cross-chain or cross-asset activity.

With illicit actors such as North Korea increasingly exploiting DEXs, bridges and other DeFi services to engage in sanctions evasion, the lack of programmatic holistic screening capabilities among most blockchain analytics solutions leaves compliance teams exposed to severe risks they may fail to detect.

To understand why, consider some examples.

Suppose a crypto exchange business has a customer named Alice. She has a USDC stablecoin account with the exchange, and periodically sends transactions to her external USDC wallet.

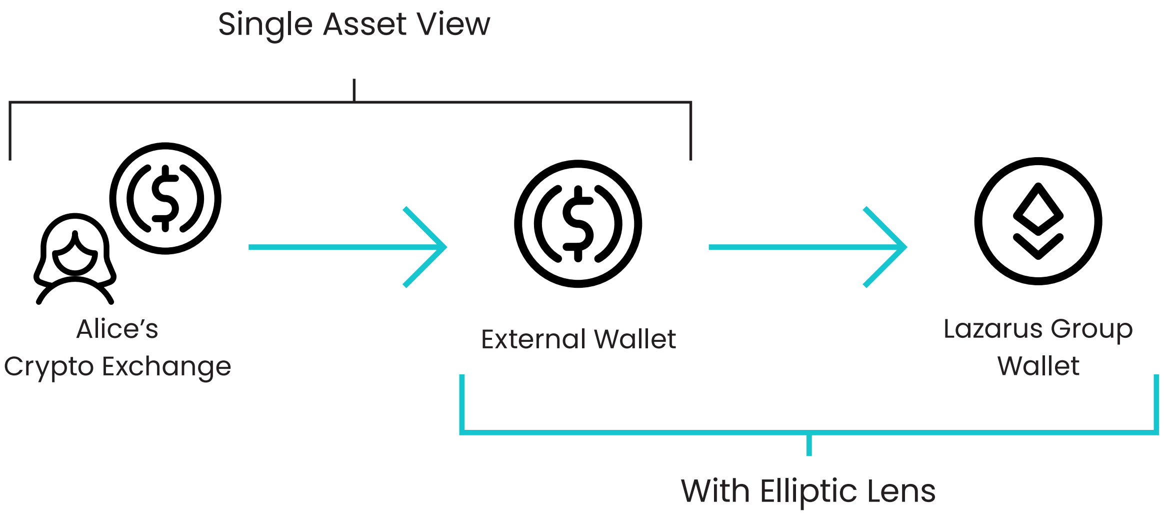


Using legacy blockchain analytics capabilities, the crypto exchange can screen Alice's external USDC address against the OFAC sanctions list to identify whether it is associated with any prohibited actors. If the legacy blockchain analytics solution does not identify any connection between the USDC address and other USDC addresses on the SDN List, it will assume that there are no sanctions risks present.

However, consider how the same scenario might play out using a blockchain analytics wallet screening capability – such as Elliptic Lens – that enables programmatic multi-asset risk detection.

In the same scenario, Alice's exchange could screen her external USDC address against the OFAC SDN List. However, where legacy blockchain analytics solutions only search for potential connections to other USDC addresses, Elliptic Lens enables Alice's exchange to check whether her USDC address may feature connections to addresses involving other assets that appear on the SDN List.

The implications of this enhanced screening are illustrated in the next diagram. By deploying Elliptic Lens, the exchange identifies that Alice's external USDC wallet is shared within an Ethereum account that includes an Ethereum address which OFAC listed on the SDN List for belonging to the Lazarus Group – a major North Korean cybercrime outfit.

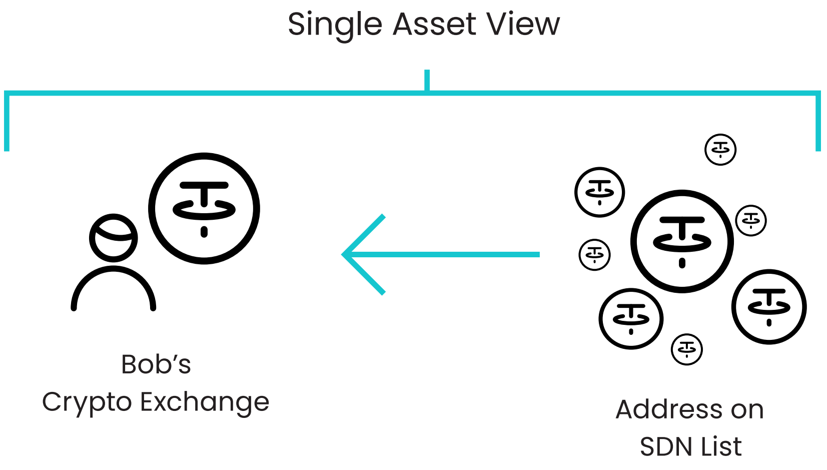


With legacy blockchain analytics, the exchange would have failed to detect these sanctions risks at the time of screening, and could only have identified its exposure to the OFAC-listed Ethereum address through painstaking investigative work.

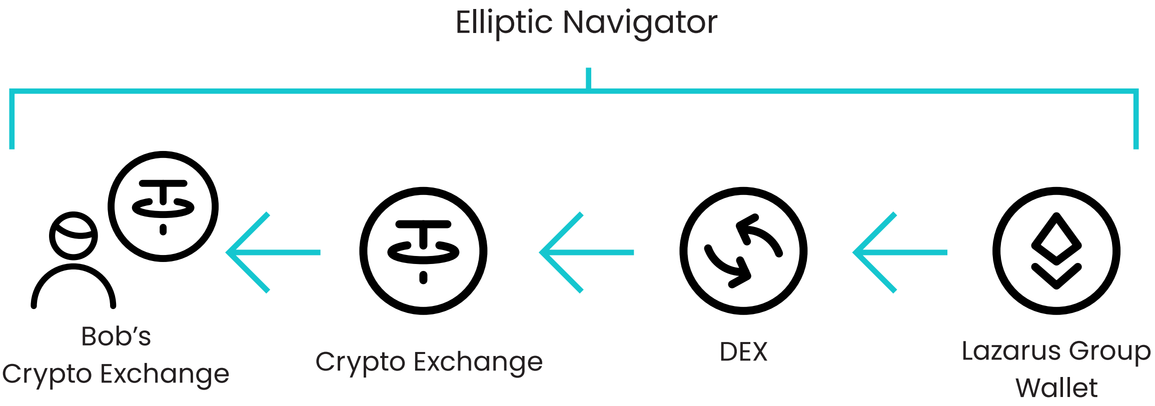
However, with Elliptic's unique Holistic Screening capabilities, the exchange is able to instantly obtain an accurate view of customer risk across multiple assets that ensures it can take appropriate steps to address the identified sanctions exposure. The result is the ability to undertake more effective risk management while retaining efficient and scalable compliance workflows.

Consider another example that shows how single-asset screening can fail to detect risks involving DEXs.

In this scenario illustrated below, the same crypto exchange has a customer named Bob, who deposits Tether into the exchange. Using legacy blockchain analytics, the exchange will only detect sanctions risks if the counterparty Tether address is linked to other Tether addresses on the SDN List.

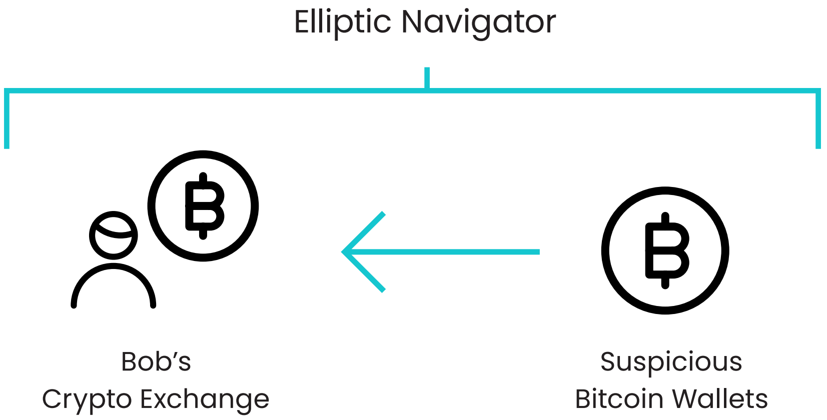


However, with Elliptic Navigator – our transaction screening solution – the exchange immediately identifies that the Tether Bob received can be traced back to a DEX, where it was swapped for Ether originating from a wallet belonging to the Lazarus Group. The impact of this enhanced ability to detect risks through cross-asset flows is illustrated below.



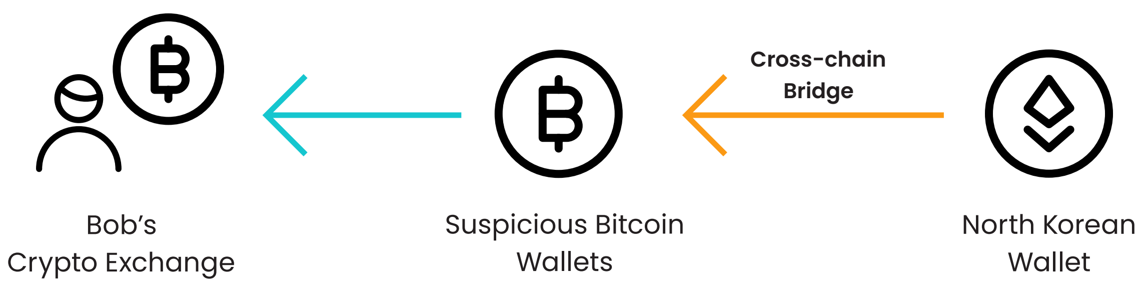
Let's consider a final scenario, one that demonstrates the importance of detecting sanctions risks amid cryptoasset flows across different blockchains.

In this case, Bob deposits some Bitcoin at the crypto exchange where he maintains his account. With single-asset screening, the exchange is limited to detecting risks associated with Bitcoin only, as illustrated in the next figure.



However, by relying upon a screening capability that deploys cross-chain tracing, the exchange identifies risks that would otherwise go undetected. In this case, as illustrated below, the exchange finds that the ultimate origin of funds is the same North Korean Ethereum wallet, which sent funds through a cross-chain bridge in order to transfer the funds over to the Bitcoin blockchain.

Cross-chain Tracing



In all of these scenarios, the outcome is the same: the crypto exchange can only engage in effective sanctions risk detection where it uses capabilities that enable a deeper view of risk across assets and blockchains.

At Elliptic, we have pioneered the next generation of blockchain analytics with our Holistic Screening capabilities, equipping compliance teams with the solutions they need to operate in a multi-asset world.

As sanctioned actors look to abuse DEXs and cross-chain bridges in an effort to circumvent OFAC restrictions, compliance teams can avoid exposing themselves to risks unnecessarily.

→ 02.

Managing Your Country Risk Exposure

Avoiding sanctions risk exposure is about more than just monitoring for connections to specific SDNs or other known illicit actors. A successful risk-mitigation strategy also involves detecting more subtle signs of risk, such as exposure to high-risk countries, or to regions that pose high risks of sanctions evasion activity.

> *"While large-scale sanctions evasion using [cryptocurrencies] by a government such as the Russian Federation is not necessarily practicable, sanctioned parties, illicit actors, and their related networks or facilitators may attempt to use [crypto] and anonymizing services to evade US sanctions and protect their assets around the globe [...]."*
>
> US Treasury's Financial Crimes Enforcement Network (FinCEN), March 2022[1]

For example, compliance teams need to be alert not only to interactions with individuals and entities on sanctions lists. They also need to be able to identify interactions with cryptocurrency exchanges, miners, and other services in countries such as North Korea, Iran, Cuba, Russia, Venezuela and other jurisdictions that are subject to broad financial and economic sanctions.

Since early 2022, sanctions concerns involving Russia's potential nexus with crypto have become particularly pronounced. For example, as Elliptic has previously shown, Russia-linked separatist groups – including those operating in the Donetsk, Luhansk, Kherson and Zaporizhzhia regions – have solicited Bitcoin donations worth nearly $5 million in support of their militant activities. After the announcement by the US, EU, and other jurisdictions of sanctions targeting those regions, Elliptic took steps to ensure our customers could screen cryptoasset wallets and transactions involving these groups in using our blockchain analytics solutions.

Our team undertook urgent assertions of these actors, adding cryptoasset wallets belonging to these groups to our data set, which enabled our customers to take proactive steps to identify potentially prohibited dealings. Using Elliptic's Configurable Risk Rules, compliance teams can set their monitoring arrangements to ensure they can detect entities located in these regions, in neighboring countries such as Belarus – or in Russia more broadly – as required by their sanctions compliance obligations.

What's more, compliance teams can leverage transaction and wallet screening to ensure the full implementation of pre-existing sanctions targeting Russian actors who use cryptoassets. OFAC has previously sanctioned Russian cybercriminal gangs, as well as Russia-linked individuals involved in hacking US elections.

[1] https://www.fincen.gov/sites/default/files/2022-03/FinCEN%20Alert%20Russian%20Sanctions%20Evasion%20FINAL%20508.pdf

Another essential component of sanctions compliance at this time is having the ability to identify digital asset exchange services in Russia that could potentially enable sanctions evasion. Cryptoasset businesses and financial institutions should take special care to apply enhanced due diligence to these transactions for signs of potential dealings with sanctioned individuals and entities in Russia.

Fortunately, solutions exist to empower compliance teams in these efforts. Elliptic Discovery is our database of comprehensive due diligence profiles on more than 1,000 virtual asset service providers (VASPs) located globally. Using Discovery – which already includes profiles of hundreds of exchanges located in Russia – compliance teams can proactively take steps to apply enhanced monitoring to any transactions involving them. They can even determine whether to continue business with them as restrictions increase.

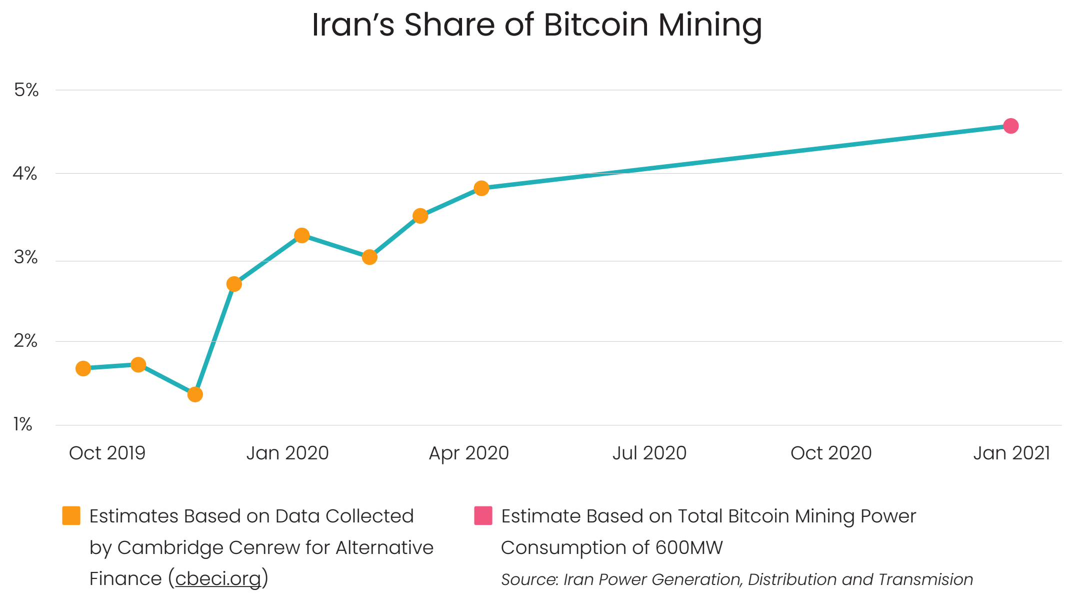
Crypto Mining in Sanctioned Countries

Cash-strapped countries under economic sanctions have looked to crypto mining as a source of potential revenue. Reports suggest North Korea may have mined Bitcoin and has engaged in crypto-jacking campaigns – hacking a computer and using it to mine crypto – to raise funds. Meanwhile, Venezuela has put in place a licensing framework for mining activity domestically, which ensures it can capture profits from miners.

Similarly, Iran's government has looked to benefit from hosting mining operations there. In July 2019, the country announced the roll-out of a licensing regime that requires miners to register and pay a fee to the government. Iran initially licensed more than 1,000 miners to operate there, but has shut down certain mining operations that have consumed excess electricity and caused power outages.

The prospect of cheap power for Bitcoin mining has attracted significant inward investment, particularly from China, which is a leader in the industry. Several Chinese businesses have been granted mining licenses and have established operations in the country. Elliptic estimates that Iran-based miners account for approximately 4.5% of all Bitcoin mining.

The electricity being used by miners in Iran would require the equivalent of approximately ten million barrels of crude oil each year to generate – around 4% of total Iranian oil exports. The Iranian state is therefore effectively selling its energy reserves on the global markets, using the Bitcoin mining process to bypass trade embargoes.



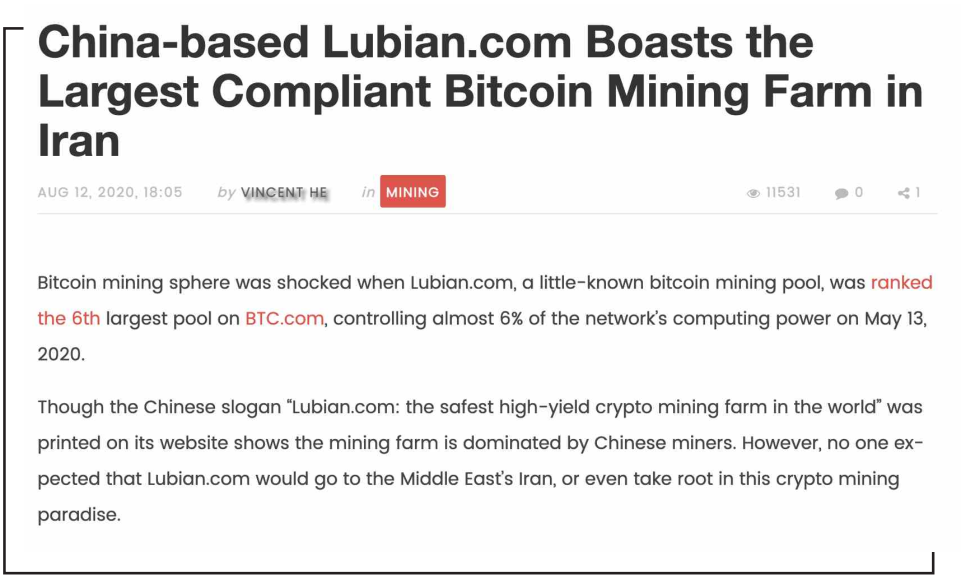
Source: *Elliptic*

Iran-based miners are paid directly in Bitcoin, which can then be used to pay for imports – allowing sanctions on payments through Iranian financial institutions to be circumvented. Many of those making the Bitcoin transactions and paying the fees to Iran-based miners will be located in the United States – the very country spearheading the sanctions. As the US government considers whether to lift some sanctions on Iran in exchange for a return to a nuclear deal, it will need to consider the role that Bitcoin mining plays in enabling Iran to monetize its natural resources and access financial services such as payments.

In the meantime, Iranian mining represents an acute risk for US financial institutions – particularly those that are beginning to offer Bitcoin services. If 4.5% of such mining is based in Iran, then there is a 4.5% chance that any Bitcoin transaction made will involve the sender paying a transaction fee to a Bitcoin miner in the country, potentially leading to sanctions violations.

There is also the risk of receiving Bitcoins earned by Iranian miners, who are looking to cash out or spend their cryptoassets. Crypto businesses and financial institutions outside Iran should be alert to transactions sent to or from Iran-based miners, as facilitating those transactions could result in sanctions violations.

Perhaps more attractive for Iran's cash-strapped regime than licensing domestic mining operations is providing mining licences to foreign companies, which bring much needed investment into Iran. The country has licensed Chinese mining pools – such as Lubian.com – to operate mining farms there.



China-based Lubian.com Boasts the Largest Compliant Bitcoin Mining Farm in Iran

AUG 12, 2020, 18:05 by VINCENT HE in MINING 11531 0 1

Bitcoin mining sphere was shocked when Lubian.com, a little-known bitcoin mining pool, was ranked the 6th largest pool on BTC.com, controlling almost 6% of the network's computing power on May 13, 2020.

Though the Chinese slogan "Lubian.com: the safest high-yield crypto mining farm in the world" was printed on its website shows the mining farm is dominated by Chinese miners. However, no one expected that Lubian.com would go to the Middle East's Iran, or even take root in this crypto mining paradise.

Source: *8BTC News website, August 12th 2020.*

In April 2022, OFAC issued sanctions against the Russian mining company BitRiver. The sanctions appear to have been pursued in response to statements from the Russian government – including President Vladimir Putin directly – suggesting that Russia may seek to leverage its vast energy reserves to mine Bitcoin and circumvent sanctions, potentially attempting to emulate the Iranian approach.

We expect that in 2023 OFAC will ramp up its efforts to target mining activity in sanctioned jurisdictions by designating further mining-related entities in countries such as Russia and Iran.

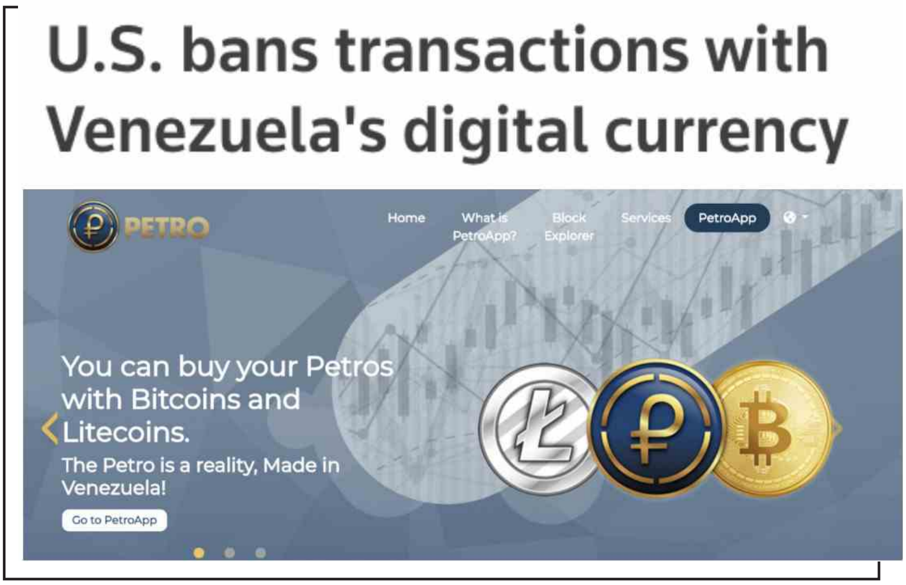
Compliance teams should be on the lookout for transactions that could expose them to mining activity in sanctioned countries. That includes having the capability to detect transactions received from miners operating in sanctioned countries, as well as ensuring you do not pay transaction fees to those miners. Elliptic's blockchain analytics solutions can assist in identifying these connections so you can block them.

Country-related sanctions risks can manifest in other ways. A United States Executive Order prohibits US persons from having dealings involving any Venezuelan government-backed cryptoassets – a response to Venezuela's launch of the Petro cryptocurrency in December 2017.

In May 2019, the US also blocked dealings in all property of the government of Venezuela. Eleven months earlier, the latter announced that it had approved 16 cryptocurrency exchanges domestically to handle the Petro. Among these are government-owned platforms, such as the PetroApp, which enables users to swap cryptoassets such as Bitcoin and Litecoin for Petros.

Crypto exchanges outside Venezuela therefore need to be alert to potential connections to these exchanges, such as customers who may frequently utilize them, in order to mitigate their sanctions risk exposure.

Elliptic's blockchain monitoring solutions can enable you to detect this activity. Our configurable country-specific risk rules allow you to monitor for both direct and indirect transactional connections to entities located in countries such as Russia, Iran and Venezuela.



U.S. bans transactions with Venezuela's digital currency

You can buy your Petros with Bitcoins and Litecoins.

The Petro is a reality, Made in Venezuela!

Source: *https://petroapp.petro.gob.ve.*

Our best-in-class data sets and configurable transaction risk rules can also allow you to identify connections to entities in third countries that present sanctions-evasion risks, as described in the case study below.

Elliptic's monitoring solutions can prove especially successful in managing geographical risk exposure when combined with other control measures. For example, to detect if their customers are operating from or near a sanctioned jurisdiction, business we work with often also monitor geolocational indicators, such as:

- Their customers' IP addresses.

- Email addresses.

- Phone numbers.

- Other indicators.

Third Country Sanctions Evasion Risk

Sanctioned actors frequently target third countries as go-betweens to move funds and avoid scrutiny. Iranian sanctions evaders have frequently looked to countries such as Turkey, Lebanon and the UAE to avoid US scrutiny.

Both Iran and North Korea have also utilized financial institutions in countries such as China, Malaysia, Singapore and elsewhere to elude both US and international restrictions.

Blockchain analysis of OFAC-listed crypto addresses indicates that sanctioned Iranian individuals have engaged in transactions with entities in third countries such as Turkey and various nations in Southeast Asia.

This activity suggests exchanges in these third countries need to be alert to the risks of sanctions-related activity. And exchanges located elsewhere in the world need to be alert to activity involving third country exchanges that could be high risk, where such activity appears in conjunction with other sanctions-related red flags.

→ 03.

Knowing the Red Flags

Because sanctioned individuals and entities go to great lengths to conceal their activity, it is essential that you know what red flags to look out for. Red flags of potential sanctions-related activity can involve both transactional behaviors, as well as a range of other qualitative indicators.

Normally, several red flags will appear in tandem that should alert your compliance teams to sanctions risks, prompting them to take a closer look.

In March 2022, following the Russian invasion of Ukraine, the US Treasury's Financial Crimes Enforcement Network (FinCEN) issued an alert warning of potential crypto-related red flags related to sanctions evasion, including:

- A customer of an exchange or financial institution engages in transactions with addresses on the OFAC SDN List.
- A customer engages in transactions with a crypto exchange located in a high-risk jurisdiction.
- A customer's transactions involve the use of mixing or obfuscating services.

Below, we outline a number of additional sanctions-related red flags that can be indicators of sanctions-related activity.

Cryptocurrency and Sanctions Risks: Key Red Flags

- A customer attempts to log-on to an exchange using IP addresses, email addresses, phone numbers, or other identifying indicators registered in a sanctioned jurisdiction.
- A customer is identified as being associated with advertisements for cryptocurrency brokerage activity on P2P trading sites available to users in sanctioned jurisdictions.
- A customer engages in indirect transactions – ie. transactions separated by more than one hop – with exchanges in sanctioned jurisdictions with a frequency that can't be logically explained; a customer sends funds to a cryptocurrency address that forms part of "cluster" of addresses (or wallet) associated with an OFAC-listed address, but that has not itself been identified by OFAC.
- A customer frequently engages in transactions through or with entities in countries known to be associated with sanctions evasion activity, with no clear purpose or rationale for the activity in question.
- A customer sends funds to a cryptocurrency address that forms part of a "cluster" of addresses (or wallet) associated with an OFAC-listed address, but that has not itself been identified by OFAC.

- A customer frequently engages in transactions through or with entities in countries known to be associated with sanctions evasion activity, with no clear purpose or rationale for the activity in question.

- A customer sends or receives funds to or from a miner in a sanctioned jurisdiction, or a mining pool located in a country such as China, but with operations in a sanctioned jurisdiction.

- A customer frequently sends/receives funds to/from exchange services that do not require KYC information and are located in high-risk jurisdictions. At Elliptic, we conduct ongoing research into these and other red flag indicators of sanctions-related typologies and can assist your compliance teams in understanding how to identify them.

In addition to knowing what key red flags of sanctions evasion to spot, it’s important to be aware of emerging issues and typologies impacting the crypto space. Some emerging issues that impact sanctions risk include:

- **Privacy Coins:** Elliptic’s research indicates that illicit actors – especially darkweb markets – are increasingly looking to privacy coins like Monero as a way to evade the traceability of other cryptoassets. OFAC has included Monero, Dash, Verge and Zcash addresses belonging to sanctioned cybercriminals on its SDN List – suggesting that privacy coins could prove attractive to sanctioned actors as well.

- **Privacy Wallets:** the use of privacy wallets such as Wasabi Wallet as an alternative to centralized mixers has grown significantly among illicit actors. Privacy wallets are less vulnerable to law enforcement disruption than centralized mixing services, and criminals look to them increasingly as a way to obfuscate funds flows in Bitcoin.

- **Coinswap Services:** illicit actors are moving away from using large fiat-to-crypto exchange platforms. Since the introduction of comprehensive guidance from the Financial Action Task Force (FATF) in June 2019, large exchanges have implemented AML and KYC measures that are deterring criminals. Elliptic’s research indicates that threat actors are increasingly using coinswap services to launder funds. Coinswap services are crypto-to-crypto exchange platforms that generally do not collect KYC information and that are often located in high risk money laundering jurisdictions. Elliptic’s separate briefing note on coinswap services highlights that many of these services are based in Russia, and we have identified instances of sanctioned actors using these services.

- **DEXs:** decentralized exchanges (DEXs) and other apps in decentralized finance (DeFi) are among the most exciting innovations in the crypto space. However, because they are unregulated and do not gather KYC information from users, there are concerns that they could become a haven for crypto laundering. North Korea’s Lazarus Group has been linked to the hack of a crypto exchange in Singapore, KuCoin, from which it stole cryptoassets worth $280 million. Some of the funds were laundered through DEXs – an indication that North Korea is capable of exploiting DeFi technology.

Chinese Money Launderers Move Crypto For North Korea

On March 2nd 2020, the US government unveiled details of a major money laundering operation that facilitated North Korea's movement of ill-gotten crypto.

The case reveals the complexity of emerging sanctions evasion techniques using crypto. According to the US Department of Justice (DoJ), two Chinese nationals – Tian YinYin and Li Jaidong – laundered more than $100 million for the Lazarus Group.

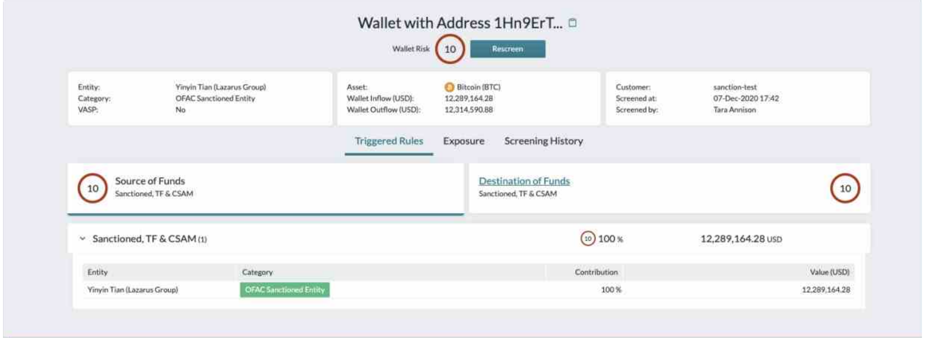
The US indictments against them indicate that YinYin and Jaidong used more than 113 crypto addresses as part of their laundering scheme. On the day the DoJ announced criminal charges against them, OFAC also put YinYin and Jaidong on the SDN List, and included 20 of their Bitcoin addresses on the list as well.

YinYin and Jaidong engaged in complex money laundering techniques to conceal funds derived from hacks of crypto exchanges the Lazarus Group had carried out. After hacking exchanges – including a single hack in April 2018 that reaped $91 million worth of cryptocurrencies – the Lazarus Group turned over the funds to YinYin and Jaidong.

The pair then laundered the funds using techniques including:

- Repeatedly moving funds through a large number of new Bitcoin addresses, an attempt at obfuscation known as "chain-peeling".
- Layering the funds through several different exchanges, sometimes making hundreds of small deposits into a single account.
- Cashing out the funds they had sent to exchanges by converting them into fiat currency and withdrawing them to numerous Chinese bank accounts through thousands of transactions.
- Using Bitcoin to purchase $1.4 million worth of Apple iTunes gift cards they could use to further launder the funds.

With access to blockchain analytics solutions such as Elliptic Lens, compliance teams can screen addresses known to belong to these North Korea-linked criminals and avoid interaction with them.



Wallet with Address 1Hn9ErT...

Wallet Risk 10

Entity: Yinyin Tian (Lazarus Group)
Category: OFAC Sanctioned Entity
VASP: No

Asset: Bitcoin (BTC)
Wallet Inflow (USD): 12,289,164.28
Wallet Outflow (USD): 12,314,590.88

Customer: sanction-test
Screened at: 07-Dec-2020 17:42
Screened by: Tara Annison

10 Source of Funds
Sanctioned, TF & CSAM

Destination of Funds
Sanctioned, TF & CSAM 10

Sanctioned, TF & CSAM (1) 10 100 % 12,289,164.28 USD

Entity	Category	Contribution	Value (USD)
Yinyin Tian (Lazarus Group)	OFAC Sanctioned Entity	100 %	12,289,164.28

Source: Elliptic

Blender is Back: North Korea Leverages Alternatives to Sanctioned Mixers

Cryptoasset mixers and other privacy-enhancing technologies – such as privacy wallets – are a long-standing feature of the crypto space.

Because the open and transparent nature of the blockchain makes crypto transactions readily traceable, crypto innovators have for most of crypto's history sought ways to enhance privacy. This has included developing cryptoasset mixers and privacy wallets, which are services that seek to obfuscate the origin of funds on the blockchain.

This desire for enhanced confidentiality in crypto certainly includes legitimate aims. Individuals may wish to enhance the privacy of their transactions if earning a salary in crypto, donating to charity, or undertaking other activities where confidentiality is both desirable and legitimate.

Unfortunately, privacy-enhancing technologies in the crypto space have also been routinely abused by criminal actors seeking to evade detection from law enforcement agencies and regulated businesses. While in some cases the developers of these services have legitimate aims and even condemn users who abuse them for illicit purposes, some of the platforms have wittingly provided their obfuscating capabilities directly to criminal actors.

Cryptoasset exchanges and financial institutions frequently rely on blockchain analytics capabilities to identify if their customers' transactions involve the use of mixers and other obfuscating services. Where that is the case, regulated businesses can manage risks appropriately, including by performing enhanced due diligence or reporting suspicious activity where warranted.

Since early 2022, OFAC has begun imposing sanctions on mixing services that have facilitated illicit activity.

In May that year, OFAC sanctioned Blender – a mixing service that was used to launder Bitcoin by North Korea's Lazarus Group – a sanctioned cybercrime organization.

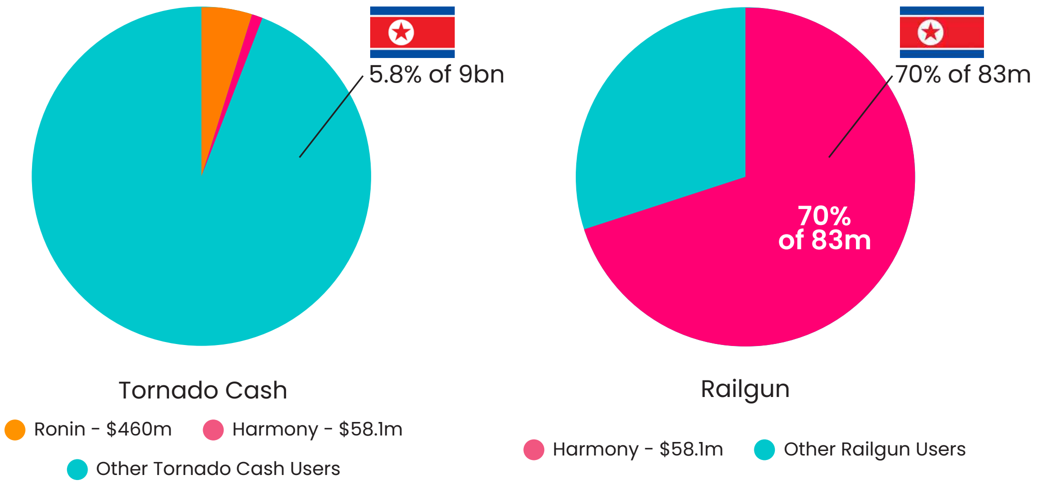
Analysis of the blockchain indicates that the Lazarus Group laundered Bitcoin worth more than $20.5 million through Blender following the March 2022 hack of the Ronin Bridge, a decentralized finance (DeFi) service related to the *Axie Infinity* blockchain-based gaming platform, which resulted in the theft of more than $540 million on cryptoassets.

By imposing sanctions on Blender, OFAC prohibited US persons – including US crypto exchanges – from processing transactions with the mixer, which shut down around the time of the sanctions.

In August 2022, OFAC took aim at another mixer, this time sanctioning the Tornado Cash mixer, which operates on Ethereum and other blockchains. As with Blender, OFAC targeted Tornado Cash because the Lazarus Group had used it to launder funds from the *Axie Infinity* hack and other cybercrime incidents.

Ellptic's research indicates that the Lazarus Group laundered more than $518 million through Tornado Cash, which constituted approximately 5.8% of the total $9 billion in funds mixed through it.

Proportion of Funds DeFi obfuscating Services
Have Received From North Korean Hacks



In February 2023, Elliptic identified that the Lazarus Group had also sent Bitcoin totalling more than $100 million through the Sinbad mixer, a new service that was established in October 2022.

In researching Sinbad, Elliptic determined that the new service appeared to be acting as a replacement for Blender following the OFAC sanctions. Analysis of Bitcoin transactions indicated that Sinbad's activity was closely tied to Blender's through common transactions, and showed that a disproportionate number of transactions for such a new mixing service appeared to be related to facilitating transactions with the Lazarus Group.

Cryptoasset businesses and financial institutions therefore face a range of sanctions risks when it comes to mixers and other privacy-enhancing services.

It is important to note that the OFAC actions mentioned above only apply to the specifically named mixers and do not prevent transactions with all mixers and privacy protocols. Compliance teams need not assume that every single transaction involving mixers or other privacy-enhancing services is illicit or related to sanctioned activity. Customers may very well attempt to use mixing services for legitimate reasons.

However, in addition to the risks that they could face from engaging in direct transactions with sanctions services like Blender and Tornado Cash, crypto exchanges and financial institutions should be alert to other signs of sanctions risks involving similar services.

For example, compliance teams should be especially alert to signs of transactions involving the Sinbad and Railgun services, given the high probability that funds from them could relate to the Lazarus Group.

Other sanctions-related red flags and risk indicators that compliance teams should be alert to include:

- A customer whose transactions involve interactions with mixers or other obfuscating services has also engaged in transactions with entities located in sanctioned jurisdictions, or that are on the OFAC Specially Designated Nationals and Blocked Persons (SDN) List.

- A customer's transactions show frequent and significant exposure to mixers that the customer is unable or unwilling to explain, particularly where the exposure to mixers occurs in proximity to major instances of cybertheft or other crimes.

- A customer who receives a large inbound transfer from a mixing service immediately attempts to swap the funds into another cryptoasset and move it off the platform in a short period of time (an indicator of "chain-hopping" typologies of money laundering).

- A customer who transacts frequently with mixers or other similar services presents other sanctions risks, such as logging on to their account from high risk or sanctioned jurisdictions.

Cryptoasset exchanges and financial institutions should take proactive steps to identify and manage the sanctions-related risks involving mixing and other obfuscating services. They can accomplish this by using blockchain analytics solutions – such as those offered by Elliptic – at various stages of the compliance journey.

First, using a wallet screening solution such as Elliptic Lens, businesses can identify if their customers intend to withdraw funds to a blacklisted mixing service such Blender, or an ostensibly related service such as Sinbad, and can block those transactions from taking place – ensuring adherence to sanctions requirements.

Second, compliance teams can utilize transaction screening software such as Elliptic Navigator to identify where they have customers who have interacted with mixers indirectly. It is common that illicit actors such as the Lazarus Group will send funds through numerous intermediary wallets (or "hops") before or after passing funds through a mixer – a technique known as a "peeling chain" designed to try to further obfuscate the origin of funds.

Using Elliptic's exposure-based tracing methodology that leverages Holistic Screening, compliance teams can identify exposure to sanctioned or high-risk mixers even where related funds have passed through numerous hops, or have been swapped across different assets or blockchains, ensuring that they can identify and address indirect sanctions risk exposure.

Finally, compliance teams should be equipped with capabilities to conduct in-depth investigations into suspected sanctions breaches involving mixers and other obfuscating services. Using Elliptic Investigator – our multi-asset crypto forensics tool – analysts can map the flow of funds to visualize complex transactions involving mixers, helping them to determine whether sanctions evasion may be taking place.

→ 04.

Defining Your Investigative Strategy

If your compliance team identifies red flags that may suggest you have sanctions exposure, it will be necessary to dig deeper. You need to have in place an investigations strategy that allows you to look in depth at customer activity and exhaustively scrutinize it.

This is especially important in sanctions-related cases, where even indirect and seemingly remote connections between customers and sanctioned parties can carry severe regulatory consequences. A well-designed investigative strategy includes:

- ensuring that all relevant staff are skilled in conducting cryptocurrency investigations;
- having documented investigative procedures and recordkeeping policies in place;
- leveraging crypto forensic analysis software – like Elliptic Investigator – to map the flow of funds related to suspected sanctions cases;
- having in place internal escalation processes for raising alerts where positive hits have been identified; and
- clearly documenting investigation findings in final reports that can be shared with relevant regulatory bodies, law enforcement or other relevant stakeholders.

Elliptic's Investigator software can equip you with the blockchain analytics capability to investigate complex sanctions-related cases, as described in the case study below.

The $100 Million Horizon Hack: Following the Trail Through Tornado Cash to North Korea

On the morning of June 24th 2022, over $100 million in cryptoassets was stolen from Horizon Bridge – a service that allows assets to be transferred between the Harmony blockchain and other blockchains.

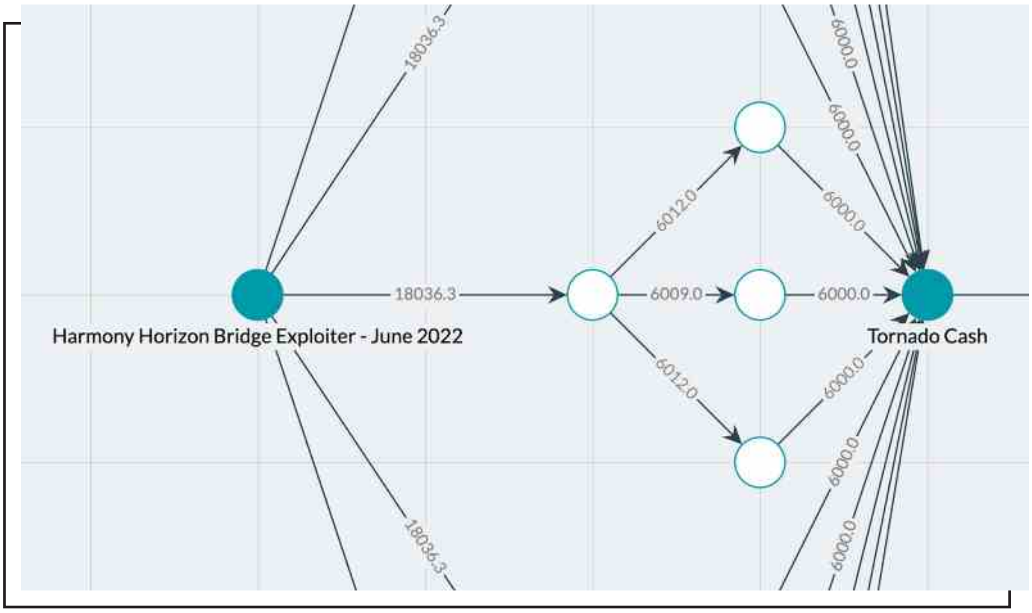
The stolen cryptoassets included Ether (ETH), Tether (USDT), Wrapped Bitcoin (WBTC) and BNB. The thief immediately used Uniswap – a decentralized exchange (DEX) – to convert the Ethereum-based assets into a total of 85,837 ETH. This is a common laundering technique used to avoid seizure of stolen assets.

Our analysis of the hack and the subsequent laundering of the stolen cryptoassets also indicated that it was consistent with activities of the Lazarus Group – a cybercrime group with strong links to North Korea.

The regularity of the deposits into Tornado Cash over extended periods of time after the hack suggested that an automated process was used. We have observed very similar programmatic laundering of funds stolen from the Ronin Bridge, which has been attributed to Lazarus, as well as a number of other attacks linked to the group.

The theft was perpetrated by compromising the cryptographic keys of a multi-signature wallet – likely through a social engineering attack on Harmony team members. Such techniques have frequently been used by the Lazarus Group. In January 2023, the FBI formally attributed the Harmony hack to the Lazarus Group.

Using our Elliptic Investigator software, we were able to map the flow of funds from the Harmony Hack to Tornado Cash, and onwards through the blockchain to cryptocurrency exchange services. Using these same capabilities, investigators can map out the funds trail related to cases of sanctions evasion.



The image above from Elliptic investigator shows the flow of funds from the Lazarus Group's crypto wallets associated with the $100 million hack of the Harmony Horizon Bridge. The arrows indicated where funds have been sent thrxough other wallets (indicated by the white circles) before being sent through Tornado Cash.

→ 05.

Defining Your Investigative Strategy

The steps outlined above are essential, but they can only excel where they are supported by a comprehensive compliance framework for managing sanctions risks holistically.

A comprehensive sanctions compliance risk management framework includes:

- **Risk Assessment:** conducting an enterprise-wide risk assessment to determine the extent of potential sanctions-risk exposure across customer, product and market segments.

- **Systems Configuration:** utilizing effective sanctions list screening solutions and ensuring those are calibrated for effective monitoring for hits against OFAC and other sanctions lists.

- **Sanctions Training:** having training programs in place to ensure that key members of staff understand sanctions obligations, risks and appropriate responses.

- **Policies and Procedures:** developing policies and procedures that clearly define staff responsibilities and set out well-defined prohibited activities. Below, we outline some specific steps you can take to address two of the components above: systems configuration and sanctions training.

OFAC and FinCEN Penalize Bittrex For Sanctions Monitoring Lapses

On October 11th 2022, the United States Department of the Treasury undertook one of its most significant enforcement actions yet impacting the crypto industry.

In a coordinated statement, OFAC and FinCEN announced civil monetary penalties totalling $24 million and $29 million, respectively, on the US cryptoasset exchange Bittrex.

The OFAC and FinCEN settlements relate to ongoing sanctions and anti-money laundering (AML) violations at Bittrex between 2014 and 2018. These violations had also been highlighted in a cease and desist letter that the New York Department of Financial Services (NYDFS) issued to the exchange in April 2019.

Since then, Bittrex has taken a number of steps to enhance its AML program and remediate the identified historical deficiencies. As part of the settlement, FinCEN agreed to credit the company $24 million, because some of its findings related to the same underlying conduct that OFAC had identified. Consequently, Bittrex will pay a total of $29 million to settle the violations, despite the total value of the penalties having been assessed at $53 million.

The OFAC settlement represents the most significant US enforcement action to date for sanctions violations related to crypto activity – and by a large margin. Previously, OFAC had levied penalties on BitGo and Bitpay for $98,830 and $507,375, respectively, related to sanctions violations. The Bittrex settlement is therefore nearly 40 times larger than OFAC's two previous crypto-related penalties combined.

The FinCEN settlement with Bittrex is not its largest related to AML violations in the crypto space. The agency had previously entered into settlements with BTC-e and BitMex in excess of $100 million each. Nonetheless, FinCEN's settlement with Bittrex contains important lessons for compliance teams operating in the crypto space.

The OFAC settlement highlights a number of sanctions compliance deficiencies, including the fundamental absence of a sanctions compliance program at Bittrex from March 2014 to December 2015. Importantly, the settlement also describes a number of sanctions screening lapses that ultimately led Bittrex to process more than 100,000 transactions totalling more than $263 million involving sanctioned jurisdictions – even after it implemented sanctions screening software in 2016.

Notably, the settlement points out that the scope of the screening capability deployed was insufficient for detecting many sanctions risks. It notes that: "Until October 2017, the vendor screened transactions only for hits against OFAC's List of Specially Designated Nationals and Blocked Persons (the SDN List) and other lists but did not scrutinize customers or transactions for a nexus to sanctioned jurisdictions."

This is a critical point for any crypto compliance team.

OFAC has noted in previously issued guidance that it expects US persons to avoid all dealings with cryptoasset wallets controlled by sanctioned parties, or associated with persons in sanctioned jurisdictions – even if OFAC has not included their wallets on the SDN List.

In FAQs on its website, the agency notes that: "OFAC's digital currency address listings are not likely to be exhaustive. Parties who identify digital currency identifiers or wallets that they believe are owned by, or otherwise associated with, an SDN and hold such property should take the necessary steps to block the relevant digital currency [...]."

Having access to a blockchain analytics capability that is underpinned by robust data is essential to achieving effective sanctions screening for any crypto compliance team.

Users of Elliptic Lens – our crypto wallet screening solution – can identify not only addresses that are exact matches to the more than 300 addresses that OFAC has included on the SDN List; our industry-leading data set enables compliance teams to identify additional addresses controlled by sanctioned individuals and entities. For example, we have identified several hundred thousand crypto addresses belonging to sanctioned Russian actors in addition to those included on the OFAC SDN List.

Similarly, our dataset includes information on entities that are located in sanctioned jurisdictions, but which do not necessarily appear on the OFAC SDN List. This includes virtual asset service providers (VASPs) and other entities located in jurisdictions subject to sanctions, such as Iran, Syria, Venezuela and the Donetsk and Luhansk regions of Russian-occupied Ukraine. By screening wallets and transactions using our blockchain analytics solutions, compliance teams can identify and block activity involving these and other sanctioned jurisdictions.

Additionally, our sanctions screening capabilities enable compliance teams to identify and manage sanctions risks that many other blockchain analytics capabilities fail to detect. Our Holistic Screening capabilities enable compliance teams to identify risks associated with crypto wallets and transactions, even where funds have passed through cross-chain services.

For example, if a compliance team screens an Ethereum address using our Holistic Screening functionality, they can identify if the funds in question had first been swapped for other assets – such as Tether – at a decentralized exchange (DEX) or other decentralized finance (DeFI) service by a sanctioned actor such as North Korea's Lazarus Group.

By enabling our customers to detect exposure to cross-chain sanctions risks with real-time screening, Elliptic's blockchain analytics solutions ensure that crypto exchanges are equipped with the comprehensive insights needed to satisfy regulators of comprehensive sanctions compliance.

Beyond sanctions screening, the US Treasury actions also point to the importance of having a well-tuned and effective transaction monitoring capability.

The FinCEN settlement indicates that in 2016 Bittrex had not implemented automated transaction monitoring capabilities despite processing more than 11,000 transactions per day. Instead, the company relied on highly manual transaction review processes, which proved ineffective, preventing Bittrex from identifying high risk and suspicious activity related to transactions it facilitated related to darknet markets and ransomware. In fact, the company filed no suspicious activity reports (SARs) with FincEN between 2014 and May 2017, and filed only one SAR between May and November 2017.

The FinCEN settlement also notes that even once Bittrex had established company policies for identifying certain risks – such as geographical ones – in transactions, its monitoring program remained deficient, and it continued to process transactions with sanctioned and high-risk jurisdictions.

This serves as an important reminder about the need for compliance teams to deploy transaction monitoring capabilities that ensure efficient and effective screening, so that a business can reliably identify suspicious activity as it scales without having to manage large numbers of false positives.

Elliptic Navigator is our transactions screening solution used by many of the largest crypto exchanges in the world to detect suspicious transactions. Using Elliptic's configurable risk scoring features, compliance teams can establish the monitoring parameters they need in Navigator to align with their business model and risk appetite. This enables them to detect high risk transactions involving cybercrime, darknet markets, fraudsters and other illicit actors with both accuracy and efficiency.

Configuring Your Sanctions Screening Solutions

It's critical to ensure that any sanctions screening solutions your compliance team uses are configured to ensure airtight compliance. This means ensuring solutions can screen against sanctions lists maintained in any countries where you operate.

Elliptic's solutions are underpinned by a robust data set that includes individuals and entities that appear on global sanctions lists such as:

- The OFAC SDN List
- The UN Security Council Consolidated List
- The EU Consolidated Financial Sanctions List
- The UK HM Treasury Consolidated Sanctions List
- The Japan Ministry of Economy, Trade and Industry Sanctions List
- The Consolidated Canadian Autonomous Sanctions List
- The Australia Department of Foreign Affairs and Trade Sanctions List.

Elliptic's solutions also feature configurable risk rules that enable compliance teams to set thresholds for screening addresses and transactions against these lists – ensuring screening parameters are aligned to your requirements and risk appetite.

> *“When virtual currency firms fail to implement effective sanctions compliance controls, including screening customers located in sanctioned jurisdictions, they can become a vehicle for illicit actors that threaten US national security. Virtual currency exchanges operating worldwide should understand both who – and where – their customers are. OFAC will continue to hold accountable firms, in the virtual currency industry and elsewhere, whose failure to implement appropriate controls leads to sanctions violations.”*

Andrea Gacki, Director of OFAC, October 2021[8]

Up-skilling Compliance Teams With Sanctions Training

In guidance issued in May 2019, OFAC highlighted training as a fundamental component of sanctions compliance. According to the agency: “An adequate training program, tailored to an entity’s risk profile and all appropriate employees and stakeholders, is critical to the success of [a sanctions compliance program].”

OFAC highlights that this requires having training that is comprehensive, up-to-date, and easily accessible.

At Elliptic, we’ve developed a comprehensive suite of crypto compliance training and certification offerings. Our Elliptic Learn training solutions include both online courses and live instructor-led training that can be tailored to meet the sanctions-related learning requirements of compliance teams. You’ll also be able to demonstrate to regulators and internal stakeholders that you’re committed to continuous, relevant and auditable education.

Managing the Risks of Ransomware Payments

On September 21st 2021, OFAC issued an updated advisory outlining sanctions risks from facilitating ransomware payments. OFAC used the advisory to warn the private sector of risks associated with processing ransomware payments.

According to the agency, US financial institutions and other businesses that facilitate payments for ransomware may violate sanctions where those ransomware campaigns involve sanctioned individuals or countries.

The notice outlines several ransomware campaigns – such as Cryptolocker, SamSam, and WannaCry – associated with sanctioned individuals and jurisdictions. OFAC's ransomware advisory underscores why it is critical that cryptoasset businesses and financial institutions develop a comprehensive sanctions risk management framework.

The notice states that "the sanctions compliance programs of these companies should account for the risk that a ransomware payment may involve an SDN or blocked person, or a comprehensively embargoed jurisdiction". Any cryptoasset business or financial institution should undertake a risk assessment to understand the scale of risk it faces from potentially facilitating ransomware payments. This should be supported by clear risk appetite statements that define for staff whether it is permitted to facilitate those payments.

Since the time of the ransomware advisory, OFAC has taken a number of sanctions actions to ramp up pressure on ransomware gangs and their support networks. Across late 2021 and early 2022, the agency sanctioned three crypto exchanges registered in Eastern Europe - SUEX, Chatex and Garantex - for facilitating hundreds of millions of dollars in transactions on behalf of Russia-based ransomware gangs.

In April 2022, OFAC also announced sanctions against the Hydra dark web market, a Russian dark web market that US and German authorities managed to dismantle. Hydra had provided a forum for ransomware attackers to buy services, including money laundering services.

In February 2023, OFAC and the UK's Office of Financial Sanctions Implementation (OFSI) jointly imposed sanctions on seven members of a Russian cybercriminal gang affiliated with the Conti and Ryuk ransomware campaigns. Elliptic's research subsequently identified 53 crypto addresses associated with these cybercriminals.

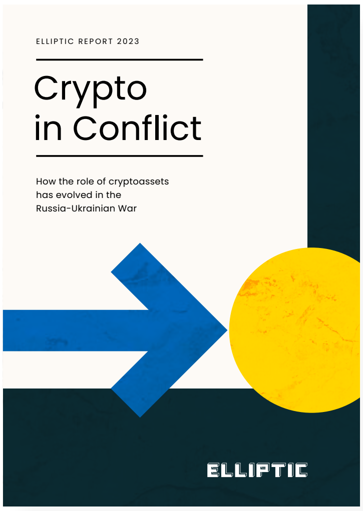
Elliptics solutions enable businesses to screen for payments to ransomware attackers and their support networks so that they can prevent exposure to these sanctioned parties.

Summary

Sanctions compliance is by no means a simple task. A rapidly evolving threat landscape and increasing scrutiny from regulators makes it all but certain that the sanctions-related challenges facing the crypto industry will only grow in complexity over time.

But if the industry is to continue its impressive growth, compliance officers must face these challenges head-on and navigate them successfully. Failure to do so can result in significant penalties and regulatory censure that businesses can't afford to face. By focusing on achieving the objectives outlined in this report, cryptocurrency compliance officers can ensure their sanctions compliance process is as smooth as possible. At Elliptic, we're here to assist. Contact us to learn more.

Other Reports by Elliptic


ELLIPTIC REPORT 2023

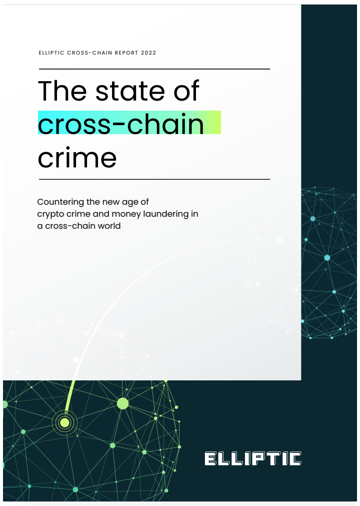
Crypto in Conflict

How the role of cryptoassets has evolved in the Russia-Ukrainian War

ELLIPTIC

Crypto in Conflict

Since Russia's full-scale invasion of Ukraine in February 2022, both sides have used blockchain technology to support their respective efforts, harnessing core developments in the crypto ecosystem to aid their fundraising.
Using our internal proprietary data, Elliptic has conducted in-depth analysis into the use of cryptoassets on both sides of the war – ranging from humanitarian causes to sanctioned groups suspected of war crimes.


ELLIPTIC CROSS-CHAIN REPORT 2022

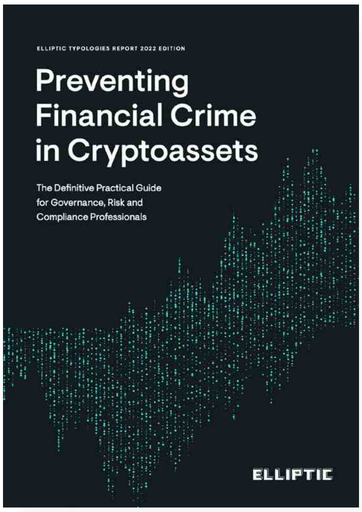
The state of cross-chain crime

Countering the new age of crypto crime and money laundering in a cross-chain world

ELLIPTIC

The State of Cross-chain Crime

Blockchains have become increasingly interconnected as new technologies remove many of the barriers to the free flow of capital between cryptoassets. However they are also being abused for money laundering by the likes of ransomware groups and hackers.
In this report we take a deep-dive into the new frontier of crypto laundering, exploring the criminal typologies through case studies and blockchain analytics.


ELLIPTIC TYPOLOGIES REPORT 2022 EDITION

Preventing Financial Crime in Cryptoassets

The Definitive Practical Guide for Governance, Risk and Compliance Professionals

ELLIPTIC

Preventing Financial Crime in Cryptoassets: Typologies Report 2022

This report is designed to equip governance, risk and compliance professionals with the knowledge and insights needed to proactively and practically:

- Identify specific money laundering and terrorist financing risks
- Develop anti-money laundering and counter terrorist financing (AML/CTF) governance systems
- Evolve the controls in place to manage risk to business, customers, and society.

About Elliptic

Elliptic is the global leader in cryptoasset risk management for crypto businesses, governments, and financial institutions worldwide. Recognized as a WEF Technology Pioneer and backed by investors including J.P. Morgan, Wells Fargo Strategic Capital, SBI Group, and Santander Innoventures, Elliptic has assessed risk on transactions worth several trillion dollars, uncovering activities related to money laundering, terrorist fundraising, fraud, and other financial crimes. Elliptic is headquartered in London with offices in New York, Singapore, and Tokyo.

ELLIPTIC

London • Tokyo • New York • Singapore

Connect on LinkedIn

Follow us on Twitter

✉ Contact us at hello@elliptic.co