DOI: 10.53477/1842-9904-23-11

SANCTIONS EVASION AND VIRTUAL ASSETS: IMPLICATIONS FOR NATIONAL SECURITY

Bogdan VACUSTA*

2022 was the year marking a significant increase in the use of virtual assets for illicit activities such as sanctions evasion. Most of the entities conducting these activities are linked to Russia, North Korea and Iran, which are subject to international sanctions imposed by the international community.

The paper presents key elements about the use of virtual assets in illicit activities by sanctioned entities and highlights the necessity to increase defence and intelligence resources for better data analysis on this type of entities. Analyzing data about virtual assets transactions requires strong collaboration between public and private organizations, with a focus on an intelligence-led approach, considering the growing links between cybercrime, money laundering, terrorist financing, special operations conducted by adversaries. In order to support this collaboration, it is essential to prioritize the education of decision-makers on the necessity to focus on technical data.

Keywords*: sanctions evasion; virtual assets; sanctioned entities; data analysis; blockchain; intelligence.*

Introduction

The Russian invasion of Ukraine and the subsequent sanctions imposed by the international community raised international awareness on the topic of *sanctions evasion*. Even though apparently there are no obvious indicators to identify a major risk towards national security, a closer look shows data about the use of virtual

**** Bogdan VACUSTA is a certified Blockchain/DLT Manager, by the Technical University of Munich, also a Counter Fraud Manager, accredited by the UK Counter Fraud Professional Accreditation Board, and a PhD Candidate for "Mihai Viteazul" National Intelligence Academy doctoral studies. E-mail: bogdan.vacusta@gmail.com***

assets in cybercrime, money laundering, illegal trade, conducted by entities linked to Russia, North Korea and Iran.

Blockchain is the underlying technology facilitating the transfer of value through virtual assets and has the potential to improve different legacy systems and procedures, mainly due to its transparent, permissiveness and distributed nature. However, virtual assets are only one major practical financial application on how blockchain technology can be deployed on a wider scale in the different sectors of activity. Essentially, transactions involving virtual assets have a pseudo-anonymous nature, contrary to common opinions that these are anonymous. The problem is that de-anonymizing them requires a lot of time and resources, which actually affects public confidence in cases of major incidents. The resources allocated from public money involve decisions across a wide range of decision-makers, who have not fully understood yet the technology, the data required to de-anonymize and the necessity to upgrade skills of existing workforce.

This paper provides examples on how virtual assets are used in illicit activities conducted by entities linked to Russia and their affiliates from North Korea and Iran, highlighting the need to improve intelligence gathering capabilities, data analysis and also the education of decision-makers so that regulation can be effective, based on technical data requirements.

A study published by the US Center for Strategic and International Studies (CSIS) provided details regarding the impact of sanctions evasion: "A current risk in today's trade ecosystem is that countries leverage virtual assets to circumvent US sanctions" (Reinsch, Palazzi, 2022). The study also provided examples on how Russia's affiliates, Iran and North Korea, used virtual assets:

- Iran legalized virtual assets payments to pay for imports;
- North Korea hacked into virtual assets wallets and laundered the stolen funds through financial institutions such as Virtual Assets Service Providers (VASPs);
- the North Korean state-sponsored hacking group Lazarus used obfuscation techniques to disguise the source and launder their approximately equivalent of 1 billion USD in virtual assets, obtained from their cyber-crimes since 2015.

The news agency Reuters published in November 2022 an article about Binance, a major VASP (who also has operations in Romania and a significant market share), on how they allowed Iranian firms trade 8 billion USD, even though there are sanctions in place to cut off Iran from the global financial system (Berwick, Wilson, Zamfir, 2022). Binance denied any wrong-doing, however the transactions have taken place. The question about avoiding such situations to occur again has the answer in the available blockchain analysis tools and the decisions to use these in an intelligence-led approach.

Chainalysis, one of the major private companies conducting blockchain analysis, mentioned in their *2023 Crypto Crime Report* that the share of all virtual

assets activity that are linked to illicit activity increased for the first time since 2019, from 0.12% in 2021 to 0.24% in 2022 (Figure no. 1). Overall, illicit transaction volume rose in 2022 for the second consecutive year, hitting an all-time high of 20.1 billion USD (Chainalysis, 2023).

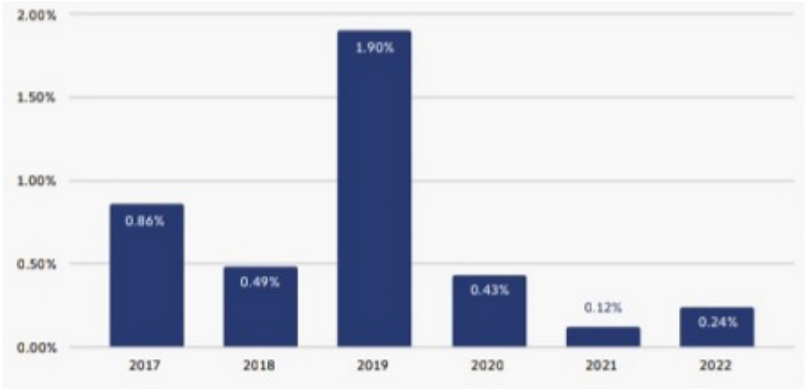

Figure no. 1: Illicit share of all cryptocurrency trading volume (Chainalysis 2023)

The report from Chainalysis mentioned that 44% of the overall illicit 20.1 billion USD came from "activity associated with sanctioned entities" (Figure no. 2), raising by a staggering figure of 10,012,224.34% from 2021 to 2022. The remaining 56% was related to stolen funds, ransomware, fraud, terrorism financing, and other illicit activities.

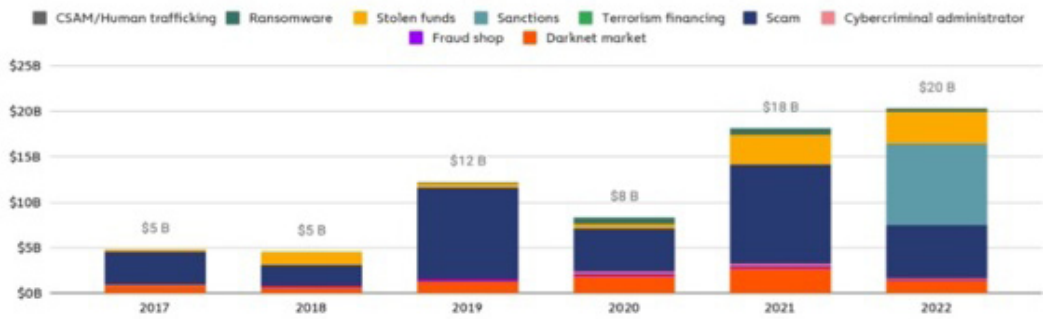

Figure no. 2: Total cryptocurrency value received by illicit addresses (Chainalysis 2023)

In order to assess the impact of sanctions evasion on a specific country level, further blockchain analysis data could be provided by companies such as Chainalysis, but these include proprietary data sets and methodologies which are subject to privacy and confidentiality requirements, this is why this paper only makes reference to data already in the public eye.

It is essential to underline that these are only estimates of illicit virtual assets activity, considering the transparency of most blockchain transactions and allow us to understand why sanctions evasion is becoming a major topic from professionals in finance, law enforcement, defence and intelligence agencies. In order to tackle the risks, improve the accuracy of data (so that we can work not only with estimates) and de-anonymize the illicit transactions, the work between the public sector and the private sector has become essential when it comes to virtual assets.

Companies from the private sector conducting blockchain analysis, such as Chainalysis, Elliptic, TRM Labs etc., can help initially by evaluating the risk of entities involved in virtual assets transactions, but they are not able to complete the cycle and fully de-anonymize the transactions and link specifically virtual assets addresses to individuals because that would imply intrusion into private lives. Only the organizations from the public sector such as defence and intelligence agencies, law enforcement, prosecution bodies can complete the cycle of de-anonymization when illicit activity is identified, by further exploring data sets and risk evaluations obtained from these blockchain analysis companies, cross-referencing these with internal data sets and conducting further intelligence gathering using special methods on risky entities, according to legal frameworks.

1. How Sanctions Evasion Can Be Enforced

The US Treasury's Office of Foreign Assets Control (OFAC) and similar agencies in other jurisdictions (G7, European Union, UK Treasury, Japan Ministry of Economy, Australia Department of Foreign Affairs etc.) implement sanctions through the targeting of individuals, groups, countries, considered threats to national or international security.

"The growing prevalence of virtual assets as a payment method… brings greater exposure to sanctions risk – such as the risk that a sanctioned person or a person in a jurisdiction subject to sanctions might be involved in a virtual currency transaction" warns OFAC in its *Sanctions compliance guidance for the virtual currency industry (*Office of Foreign Assets Control, 2023*)*. For example, in May 2017, North-Korean hackers known as the Lazarus Group, launched the WannaCry ransomware attack, which had damaging effect on individuals, businesses and other organizations, but allowed to generate funds for North Korea's government by requesting payments in virtual assets (US Treasury, 2019). This marked a link between cyber-crime and virtual assets, justifying OFAC to sanction the Lazarus Group by prohibiting US persons from making or facilitating payments to the group.

Traditionally, sanctions enforcement relied on the cooperation of mainstream financial institutions. With virtual assets at the intersection of cybercrime, finance and banking, technology, money laundering and financial crime enforcement, the

role of defence and intelligence agencies is becoming more and more critical to properly assess the problem by gathering intelligence using specific methods. The main challenge now is that the enforcement of sanctions evasion can be conducted by organizations like OFAC only if the approach is intelligence-led. Having reliable data also from international partners of the USA, which could be analyzed properly without waiting for a problem to have systemic implications, is essential. This can be achieved mainly by improving cooperation among authorities, public sector and it requires first a clear understanding of the problem and how it affects current roles, responsibilities and partnerships.

1.1. A closer look on illicit activity

Data obtained from blockchain analysis companies allows to understand better the flow of illicit transactions, decide accordingly where resources should be allocated with priority and what should be the role of public sector organizations in order to achieve de-anonymization of transactions involving entities linked to illicit activity, such as sanctions evasion.

According to Chainalysis crime report, there are different entities used in various combinations by criminals who are processing illicit virtual assets transactions, the biggest volumes in recent years involving two types of entities: Centralized VASPs and Decentralised Finance (DeFi) protocols (Chainalysis, 2023).

Centralized VASPs, mostly controlled by legal entities, were the biggest recipient of illicit virtual assets, because this is the easiest way to convert virtual assets into cash. It may be surprising because internal transactions of a VASP are not available publicly available (theoretically facilitating obfuscation) and most of these VASPs are regulated, with compliance measures in place to report illicit activity to financial intelligence units once detected, but this is what data shows. However, it is important to note that transaction data can be further obtained from most of the regulated VASPs by law enforcement, defence and intelligence agencies, using legal framework, once illegal activity has been detected.

In May 2023, OFAC imposed sanctions on Huriya Private, a company based in the United Arab Emirates. According to the US Department of the Treasury: "Since Russia's full-scale invasion of Ukraine in 2022, Huriya began working quickly to move Russian assets into structures protecting them from sanctions. Huriya also helped high-net-worth Russian Federation nationals procure non-Russian passports under assumed names to avoid financial scrutiny and sanctions." (Office of Foreign Assets Control, 2023)

The governments of Iran and Russia have reportedly been working on a gold-backed virtual asset to be utilized for cross-border payments, which could be an attempt by the two governments to avoid the impact of international sanctions.

Iranian and Russian VASPs also have significant transactions, which requires close monitoring by the defence and intelligence agencies to assess transaction flows involving illicit counterparties or operations. (Kuznetsov, 2023)

As example, TRM Labs, a blockchain analysis company, conducted research on Iran's virtual assets transactions and their findings show sanctioned entities sent less than 2 million USD to Iranian VASPs in 2022 and that Iranians are using Virtual Private Networks (VPNs) to obfuscate their location and fake identity documents (IDs) to bypass the compliance systems of international VASPs (TRM Labs Insights. 2023). In January 2023, Iran's government launched_the National Task Force on Virtual Assets (Financial Tribune, 2023), which should enhance coordination between government institutions on virtual assets-related matters, with meetings of the members taking place twice a month (Central Bank of Iran, intelligence agencies, energy, industry, mining and trade).

A critical element, relevant for data analysis, is the increasing use of DeFi protocols in illicit activities (Figure no. 3), which are technical programs running independently, without obvious link to regulated legal entities.

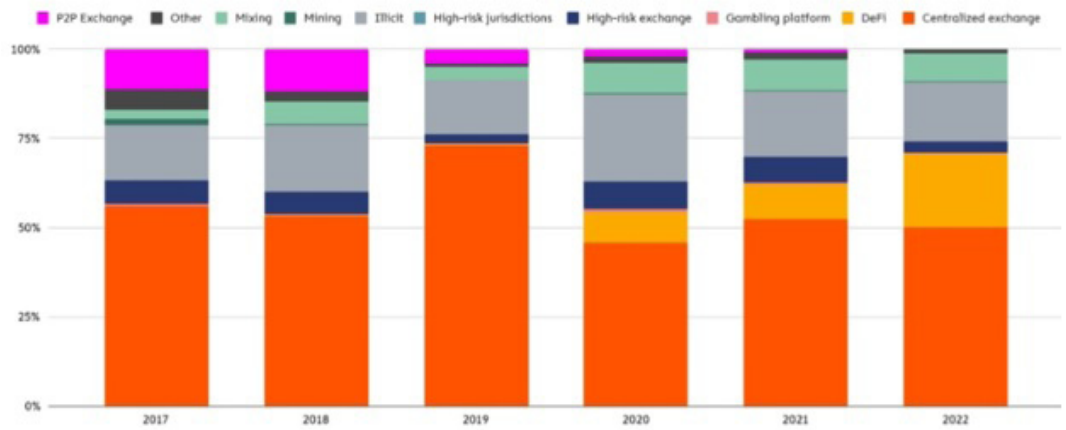

Figure no. 3: Destination of funds leaving illicit wallets
(Chainalysis 2023)

The increasing use of DeFi for illicit activities and not having DeFi regulated under the recently published Markets in Crypto-Assets Regulation in the European Union (Quarta, 2022), leaves a huge data gap when it comes to data analysis involving virtual assets used for illicit activities such as sanctions evasion. In practical terms, law enforcement, intelligence agencies can no longer submit to DeFi protocols a formal request for information as they can do with centralized VASPs, therefore requiring a new methodology for intelligence gathering, data analysis and risk assessments.

All activity involving DeFi is recorded on-chain (unlike centralized VASPs) and DeFi protocols don't allow for the conversion of virtual assets into cash, which in theory may not help criminals to obscure the flow of funds and rapidly monetize their proceeds of crime. But the benefits for criminals with the increasing use of DeFi have to do with cutting the flow of illicit funds (by conducting multiple conversions across different virtual assets, mixers or tumblers and other programmable applications), complicating investigations and delaying legal procedures, which may ultimately affect public confidence and even impact financial stability.

North Korea-linked hackers such as Lazarus Group have deployed multiple hacks over the last few years, in 2022 they stole approx. 1.7 billion USD worth of virtual assets (Figure no. 4). To put this into context, the total value of North Korea's goods exports in 2020 was 142 million USD (The Observatory of Economic Complexity, 2022), this is why many professionals mention that the North Korean government is using the cash obtained from the conversion of stolen virtual assets to fund its nuclear weapons programs (Jin Kang, 2022).

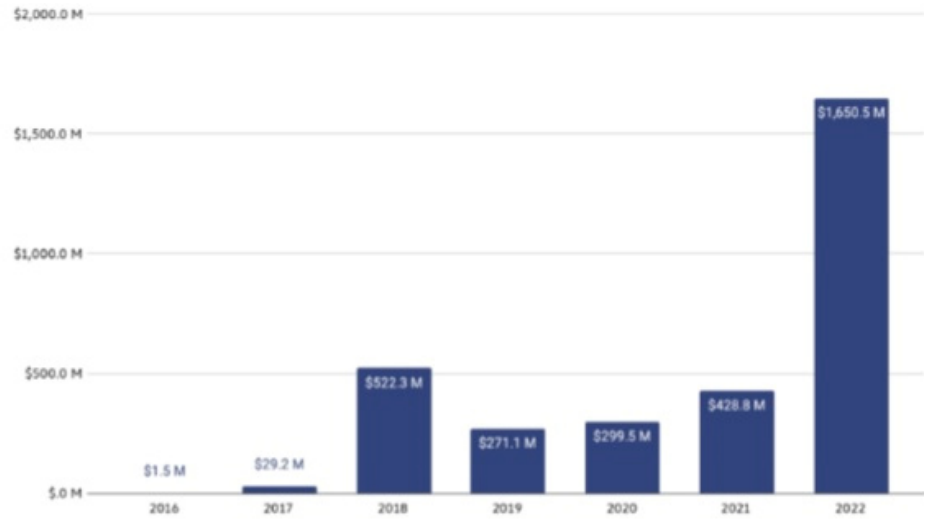

Figure no. 4: Yearly total cryptocurrency stolen by North Korea-linked hackers (Chainalysis 2023)

The Chainalysis report also underlines that 1.1 billion USD of the total 1.7 billion USD, was stolen in hacks of DeFi protocols. After stealing the virtual assets, the North Korea-linked hackers usually sent these assets to other DeFi protocols, mainly because DeFi hacks often resulted in obtaining illiquid virtual assets that aren't listed at centralized VASPs. What hackers usually did by the use of DeFi was to convert those illiquid assets into other virtual assets which have better liquidity. Hackers also sent large sums to mixers, which allow to cut the transaction flow and the origin of funds.

Overall, data from Chainalysis shows that over 40% of illicit virtual assets move first to intermediary services such as mixers or DeFi protocols, with most of those funds coming from high-risk virtual assets addresses such as those linked to sanctions evasion, cyber-crime, money laundering, terrorism financing etc. (Chainalysis, 2023). As a consequence, putting more resources into data analysis involving DeFi transactions and the interactions of criminal entities with DeFi protocols seems reasonable, the key is to build an extensible argumentation so that decision-makers can act accordingly.

1.2. Current trend: Going from individual sanctions to protocol-based sanctions requiring more technical data

The first case involving virtual assets sanctions dates from 2018, when OFAC designated two Iranian nationals associated with the SamSam ransomware strain and included their virtual assets addresses on the Specially Designated Nationals and Blocked Persons (SDN) List entries (US Treasury, 2018).

After 2018, only virtual assets addresses which belong to individuals were included on the SDN List as sanctions identifiers (an average of four addresses per designation in 2019 and nine in 2020). However, in 2021 the designations were extended by also including addresses linked to entities, not only to individuals. The digital currency addresses on the SDN List included their unique alphanumeric identifier (up to 256 characters) while also identifying the blockchain / distributed ledger to which the address corresponds (Office of Foreign Assets Control, 2023).

Overall, the average number of addresses per sanctioned entity reached 35 by 2022, with some designations containing more than 100 virtual assets addresses as identifiers. To have a clearer image, this is a short list of the individuals and entities with virtual assets links sanctioned by US Treasury's OFAC in 2022, along with the reason why these were included on the SDN List:

- Lazarus Group - hacking/theft on behalf of North Korean government;
- Ahmad Khatibi Aghada, Amir Hossein Nikaeen Ravari - ransomware;
- Alex Adrianus Martinus Peijnenburg, Matthew Simon Grimm - drug trafficking;
- Hydra Marketplace - darknet market and money laundering;
- Garantex, Blender.io, Tornado Cash - money laundering;
- Task Force Rusich - Russian paramilitary group in Ukraine.

From the above list, there are two entities which require special attention when it comes to data analysis of virtual assets transactions: Blender.io and Tornado Cash. These are mixers, a frequent method to cut the flow of transactions, working by taking in virtual assets from multiple users, mixing it all together, and sending each user an amount equivalent to what they put in. The result is that each user's virtual assets can now only be traced back to the mixer, rather than to its original source, unless special intelligence and blockchain analysis techniques are employed.

International organizations such as the Financial Action Task Force (FATF) and the US Treasury's Financial Crimes Enforcement Network (FinCEN) have warned that the frequent use of mixers is a red flag and requires careful monitoring and reporting (Financial Action Task Force, 2020 and Elliptic, 2022).

Analysis conducted by the Elliptic blockchain analysis company indicates that North Korea's Lazarus Group laundered virtual assets worth more than 20.5 million USD through Blender.io following the hack of the Ronin Bridge (DeFi service), which resulted in more than 540 million USD of virtual assets as proceeds of crime (Elliptic, 2022). However, sanctioning Blender.io and Tornado Cash did not stop North Korea from progressing further money laundering for their proceeds of crime, but it forced these state-sponsored hackers to find and use alternative mixers, in order to circumvent the sanctions.

Research from Elliptic also indicates that in January 2023, the Lazarus Group sent approximately 58 million USD through another privacy-enhancing service known as Railgun (Elliptic, 2023), which Elliptic had previously identified as an alternative to Tornado Cash (Elliptic, 2022). Elliptic also identified that the Lazarus Group sent virtual assets of more than 100 million USD using another mixer, Sinbad, a DeFi service that was established in October 2022 which appeared to be acting as a replacement for Blender.io following the OFAC sanctions (Elliptic, 2023).

In January 2023, FinCEN designated Bizlatzo, a VASP registered in Hong Kong (under the control of Russians and operating worldwide), as a primary money laundering concern, for failing to "effectively implement policies and procedures designed to combat money laundering and illicit finance" pursuant to Combating Russian Money Laundering Act (Financial Crimes Enforcement Network, 2023). Later, The U.S. Justice Department charged Bitzlato with money laundering (US Attorney's Office, 2023), and competent authorities from Europe reported having seized control of virtual assets wallets containing more than 19 million USD in virtual assets, as part of enforcement actions against Bitzlato (Europol, 2023).

Bitzlato allowed its users to process transactions without minimal identification, becoming a preferred method for using criminal proceeds and funds intended for use in criminal activity. According to US Attorney's Office, Bitzlato's largest counterparty in cryptocurrency transactions was Hydra Market, an anonymous, illicit online marketplace for narcotics, stolen financial information, fraudulent identification documents, and money laundering services that was the largest and longest running darknet market in the world. Hydra Market users exchanged more than $700 million in cryptocurrency with Bitzlato, also received more than $15 million in ransomware proceeds (US Attorney's Office. 2023).

In February 2023, OFAC also undertook a coordinated, joint action alongside the UK's Office of Financial Sanctions Implementation (OFSI) to target ransomware perpetrators (National Crime Agency, 2023). OFAC and the OFSI both sanctioned

seven Russian nationals associated with multiple cyber-attacks. It is important to note that neither OFAC nor OFSI did not include virtual assets addresses belonging to the individuals on their sanctions lists, but the blockchain analysis tool from Elliptic, a private company, identified 53 addresses belonging to six of the seven sanctioned cybercriminals (Elliptic, 2023).

It is the best course of action to avoid designations of individuals on the sanctions list without technical data such as the February 2023's OFAC and OFSI joint action focused on Russians involved in cyber-attacks, which had limited impact on an operational level because virtual assets addresses were not included. In that specific case, the inclusion of the addresses on the list would have had a positive impact by allowing financial institutions to track & monitor those addresses in an effective manner and reporting to competent authorities any counterparty sanctions exposure, mixers or IPs involved, transaction hashes etc.

These examples show the topic of sanctions comes at the intersection of multiple illicit activities and present an obvious obstacle: identifying virtual assets addresses and gathering data linked to transactions of these addresses with other entities in the DeFi space, where there are no centralized entities, which could be approached by law enforcement under legal gateway. Without clearly mentioning the virtual assets addresses, the efficiency of any investigation will be severely impacted.

1.3. Intelligence gathering focused on cross-referencing multiple data sets (geolocation, counterparties receiving / sending funds, mixers etc.)

On 15th of October 2021, OFAC published the "Sanctions Compliance Guidance for the Virtual Currency Industry," which provides best practices to combat the use of virtual assets by sanctioned persons or jurisdictions and highlights its application for VASPs the same as it is done for traditional financial institutions (Office of Foreign Assets Control, 2021). The guidance underlines the use of geolocation tools to prevent IP addresses from sanctioned countries (by using data from multiple sources - IP addresses, Wi-Fi triangulation, GPS signals) and the requirement to implement blockchain analysis monitoring and reporting tools which can identify transactions involving virtual assets addresses associated with sanctioned individuals and entities listed on the Specially Designated Nationals (SDN) list.

Blockchain analysis tools developed by different companies allow collecting and analyzing on-chain data, based on timeline, hashes (unique identifiers), type of blockchain, wallet addresses, VASP and tracing their links to risky entities involved in illicit activity, based on threat intelligence indicators. This kind of output allows financial institutions, intelligence agencies and regulators to follow the financial flow of virtual assets, almost in real time. The nature of blockchains — transparent, permissionless, distributed - allows each transaction to be verified and logged in

a shared, immutable record, along with the time stamp of the transaction and the addresses involved.

In practical terms, adding a virtual assets address to the OFAC's SDN list is followed shortly by marking that address in the blockchain analysis tools developed by Chainalysis, Elliptic, TRM Labs as being connected to a sanctioned entity. Marking it allows later a financial institution, for example, to quickly identify any transactions involving that address, assess the risk, report it to the financial intelligence units or OFAC if it is suspicious or take any other action according to legal requirements. In addition, intelligence and law enforcement professionals can use a blockchain analysis tool to trace and track the movements of virtual assets (to and from an address associated with a reported suspicious address), to build an investigation based on prior intelligence or on the report initially reported by the financial institution to the financial intelligence units or OFAC.

One major challenge in virtual assets is that there is not a single comprehensive list of all virtual assets addresses controlled by sanctioned entities. Having no single list, there is an ongoing need for information about entities involved in transfer of virtual assets by using blockchain technology. The use of blockchain intelligence can partially capture this type of necessary information. The results can turn just a few virtual assets addresses in an OFAC designation into hundreds or thousands other addresses. In the case of Hydra, the darknet market, OFAC included more than 100 virtual assets addresses as identifiers in its designation. However, data from Chainalysis indicates more than 6 million addresses affiliated with Hydra, which are available for monitoring and data analysis (Coindesk, 2023).

Blockchain analytics companies such as Chainalysis are constantly using new data sets which allow them to map better the risk of entities and the links across blockchains. However, it is possible to have undiscovered entities facilitating illicit transactions because there is not enough information available or multiple services are used, which allow obfuscation of funds or location, to avoid detection.

When a traditional financial institution identifies a sanctions exposure, they can block/reject funds and report to OFAC. The limits have to do with the fact that the transaction details are only available to that financial institution, the correspondent institution involved in the transaction, and the regulators which received the report from the financial institution. The significant difference in virtual assets, compared with traditional finance, is that the transaction data is publicly available for everyone on the blockchain – and this is highly relevant when it comes to risk assessments and regulatory reporting.

Information about transactions involving virtual assets can be obtained from a variety of sources, but the path from data and information to intelligence requires cross-reference across multiple technical data sets. These data sets are currently under the control of different public authorities (defence, national security, intelligence,

finance intelligence units, tax data, cyber security operations) or under the control of the regulated financial institutions. Technical data sets held by public authorities also need to be matched across data held by regulated financial institutions such as VASPs, regarding counterparty exposure of their clients, obtained by screening transactions on a risk-based approach.

Historically, financial institutions have solely focused on performing sanction checks on their customers during the onboarding process. Now, only a limited number of financial institutions currently use blockchain analytics (to screen and identify sanctioned virtual assets addresses) or various geolocation tools to uncover if any customers are in sanctioned jurisdictions (device IDs, IP and GPS location, etc.). By encouraging the use of blockchain analytics to assess counterparty exposure and the use of mixers, financial institutions would be in a position to obtain a significant bigger volume of data about suspicious transactions linked to cybercrime, money laundering, terrorism financing etc.

In order to increase the use of blockchain analytics across financial institutions, law enforcement, and intelligence agencies, it is important that decision-makers understand the benefits of using these tools, but also their limits, considering they can only capture part of the overall transactions if data sets are not cross-referenced between public and private entities.

2. Why it is critical to inform decision-makers based on technical data

Traditionally, intelligence agencies have a responsibility to inform decision-makers and recommend a course of action once emerging threats or risks become apparent. In order to have the best course of action to manage the threats or risks involving the use of virtual assets, it is useful to ensure that the intelligence provided to decision-makers also includes minimal technical data which is specifically linked to blockchain technology.

The transfer of value across blockchains is already affecting current working practices and the risks associated with virtual assets in areas such as sanctions evasion cannot be ignored. The sooner more actions are implemented to increase internal capabilities, the better the outcome in terms of data analysis and managing the risks.

Many decision-makers actively participate in national or international working groups linked to cyber-crime, money laundering, terrorism financing, whose work end up often in policies and regulatory frameworks. Such frameworks should include the necessity to focus on data analysis and common reporting mechanisms as the key to achieve a coordinated approach. A recent report published in May 2023 by the European Systemic Risk Board highlighted there is limited information available to assess the exposures and impact of virtual assets, recommending as a policy option to improve processes on how data is assessed, monitored, reported,

also encouraging to work on standardized templates across competent authorities and financial institutions (European Systemic Risk Board, 2023).

Educating decision-makers on blockchain would allow them to understand why it is crucial to focus on tehnical data for a practical outcome, by including technical data in:

- the Early Warning Systems (EWS) linked to red flags on cyber-crime, money laundering, fraud etc.;
- the national risk assessments;
- new specific legislation drafted or updated;
- the global sanctions list (OFAC SDN List; UN Security Council and EU Consolidated 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).

Once the technical details are included in the above, regulated financial institutions can proceed accordingly, adapting their internal monitoring systems to capture transactions linked to sanctions evasion while also identifying more easily the entities or individuals involved in operations which may affect the national security. Consequently, any suspicious transactions or transfer of value involving virtual assets can easily be reported to the competent authority (financial intelligence units, cyber-security agencies etc.).

In many instances, a financial institution may have exposure to sanctions evasion that is not easy to identify, by processing transactions for VASPs and their customers that apparently do not have any obvious connection to virtual assets. Without the right tools such as blockchain analytics and sufficient controls in place to detect this type of activity, the financial institution could face significant exposure to virtual assets-related risks.

Managing the risks to the national security arising from the use of virtual assets in illicit actions requires the education of decision-makers, providing them with practical elements so that these can end-up in formal policies, procedures and regulations, which allow financial institutions to have legitimacy in capturing later the useful information for law enforcement, intelligence or defence agencies.

Conclusions

Sanctions evasion involving the use of virtual assets has become a problem affecting national security after the Russian invasion in Ukraine and especially because of the data gap concerning the risks coming from jurisdictions such as Russia, North Korea, Iran, which are involved in illicit activities to support their foreign policy. Covering the data gap requires the use of blockchain analysis data sets

provided by private companies and cross-referencing these with data sets which are under control of public authorities, while also using special defence and intelligence methods to de-anonymize illicit transactions.

A coordinated approach on a national and international level requires the support of decision-makers who need to understand the type of technical data required for analysis, in order to support effective policies, regulations and procedures. Having effectiveness in decisions aimed to tackle the use of virtual assets for sanctions evasion or other illicit activities would also allow defence and intelligence agencies to utilize blockchain technology aimed at compromising their enemies' ability to do so.

In order to ensure coordination and effectiveness of data analysis, it is essential for competent authorities to prioritise setting up a holistic data analysis platform regarding the use of virtual assets for illicit purposes, using consistent and relevant technical criteria, maximising results by using encryption, while also ensuring consistency of relevant data sets.

The national data analysis platform should be managed by a designated competent authority and would require updating the legal framework, having the objective to identify suspicious activity, monitor risky transactions, safeguard national security and financial stability.

Capacity building in blockchain analytics is essential and efforts should be made by all competent authorities to foster the development of relevant expertise and create a community of professionals in this field.

A national data analysis platform built through capacity building would also allow a pro-active approach being implemented, allowing to assess better the interactions between traditional finance and virtual assets, the risks towards financial stability, while also marking transactions used for illegal activities which will be there forever — no public or private entity could erase them from the blockchain.

BIBLIOGRAPHY:

Berwick, Angus & Wilson, Tom. 2022. *"Crypto exchange Bincance helped Iranian firms trade $8 billion despite sanctions"*, Reuters. November 7, 2022. Accessed June 3, 2023. https://www.reuters.com/business/finance/exclusive-crypto-exchange-binance-helped-iranian-firms-trade-8-billion-despite-2022-11-04

Chainalysis. *"2023 crypto crime trends"*. January 12, 2023. Accessed May 26, 2023. https://blog.chainalysis.com/reports/2023-crypto-crime-report-introduction

Coindesk. 2023. *"Darknet revenues fall after Hydra's shutdown: Chainalysis"*. February 9, 2023. Accessed June 1, 2023. https://markets.businessinsider.com/news/currencies/darknet-revenues-fell-after-hydras-shutdown-chainalysis-1032083033

Elliptic. 2022. *"Examining the FinCEN's crypto asset red flags"*. March 14, 2022. Accessed May 18, 2023. https://www.elliptic.co/blog/examining-the-fincens-

cryptasset-fincen-red-flags?__hstc=267712218.8d1967e3515191c1013500ac7e18de8e.1663668682938.1678455236447.1678790367630.51&__hssc=267712218.1.1678790367630&__hsfp=1520624391

Elliptic. 2022. *"North Korea's Lazarus group identified as explorers behind 4540 million Ronin Bridge theft"*. April 14, 2022. Accessed May 28, 2023. https://hub.elliptic.co/analysis/north-korea-s-lazarus-group-identified-as-exploiters-behind-540-million-ronin-bridge-theft.

Elliptic. 2022. *"Tornado Cash alternatives Briefing note"*. Accessed June 2, 2023. https://hub.elliptic.co/reports/tornado-cash-alternatives-briefing-note

Elliptic. 2023. *"Crypto Mixers and Privacy Protocols: the Sanctions Compliance Implications"*. January 3, 2023. Accessed June 5, 2023. https://hub.elliptic.co/analysis/crypto-mixers-and-privacy-protocols-the-sanctions-compliance-implications/

Elliptic. 2023. *"Has a sanctioned Bitcoin mixer been resurrected to aid North Korea's Lazarus group?"*. February 13, 2023. Accessed May 26, 2023. https://hub.elliptic.co/analysis/has-a-sanctioned-bitcoin-mixer-been-resurrected-to-aid-north-korea-s-lazarus-group

Elliptic. 2023. *"Ransomware and sactions. Using holistic screening to ensure compliance"*. March 21, 2023. Accessed May 12, 2023. https://hub.elliptic.co/analysis/ransomware-and-sanctions-using-holistic-screening-to-ensure-compliance/

European Systemic Risk Board. 2023. *"Crypto-assets and descentralised finance. Systemic implications and policy options"*. Accessed May 28, 2023. https://www.esrb.europa.eu/news/pr/date/2023/html/esrb.pr230525~c74fa66621.en.html

Europol. 2023. Press release*: "Bitzlato: senior management arrested"*. January 23, 2023. Accessed June 8, 2023. https://www.europol.europa.eu/media-press/newsroom/news/bitzlato-senior-management-arrested

Financial Action Task Force. 2020. *"Virtual assets. Red flags indicators of money laundering and terrorist financing"*. Accessed April 27, 2023. https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf

Financial Crimes Enforcement Network. 2023. Press release: *"FinCEN identifies virtual currency exchange Bitzlato as a prime money laundering concern in connection with Russian illicit finance"*. January 18, 2023. Accessed June 8, 2023. https://www.fincen.gov/news/news-releases/fincen-identifies-virtual-currency-exchange-bitzlato-primary-money-laundering

Financial Tribune. 2023. *"Iran Gov't forms crypto task force"*. January 16, 2023. Accessed June 4, 2023. https://financialtribune.com/articles/business-and-markets/116878/iran-gov-t-forms-crypto-taskforce

Jin Kang, James. 2022. *"North Korea's nuclear program is funded by stolen cryptocurrency"*. November 30, 2022. Accessed June 4, 2023. https://theconversation.com/north-koreas-nuclear-program-is-funded-by-stolen-cryptocurrency-could-it-collapse-now-that-ftx-has-195559

Kuznetsov, Mikhail. 2023. *"Russia and Iran began working on a common stablecoin on gold"*. January 16, 2023. Accessed June 4, 2023. https://www.vedomosti.ru/economics/articles/2023/01/16/959100-rossiya-i-iran-nachali-prorabotku-obschego-steiblkoina

National Crime Agency. 2023. Press release*: "Ransomware criminals sanctioned in joint US/UK crackdown on internation cyber crime"*. February 9, 2023. Accessed May 20, 2023. https://www.nationalcrimeagency.gov.uk/news/ransomware-criminals-sanctioned-in-joint-uk-us-crackdown-on-international-cyber-crime

Office of Foreign Assets Control. 2023. *"Publication of sanctions compliance guidance for the virtual currency industry and updated faqs"*. October 15, 2021. Accessed May 27, 2023. https://ofac.treasury.gov/recent-actions/20211015

Office of Foreign Assets Control. 2023. *"Questions on virtual currency"*. Accessed June 14, 2023. Accessed May 27, 2023. https://ofac.treasury.gov/faqs/topic/1626

Office of Foreign Assets Control. 2023. *"Russia-related Designations"*. May 19, 2023. Accessed May 27, 2023. https://ofac.treasury.gov/recent-actions/20230519

Quarta, Luciano. 2022. *"DeFi and MiCA: another missed opportunity"*. October 13, 2022. Accessed May 27, 2023. https://en.cryptonomist.ch/2022/10/13/defi-mica-another-missed-opportunity

Reinsch, William Alan & Palazzi, Andrea L. 2022. "*Cryptocurrencies and U.S. Sanctions Evasion: Implication for Russia*". December 22, 2022. Accessed May 8, 2023. https://www.csis.org/analysis/cryptocurrencies-and-us-sanctions-evasion-implications-russia

The Observatory of Economic Complexity. 2022. *"North Korea – country overview"*. Accessed June 4, 2023. https://oec.world/en/profile/country/prk

TRM Labs Insights. 2023. *"Iran's crypto economy"*. April 17, 2023. Accessed June 4, 2023. https://www.trmlabs.com/post/iran-crypto-economy

US Attorney's Office. 2023. Press release: *"Founder and majority owner of Bitzlato, a cryptocurrency exchange, charged with unlicensed money transmitting"*. January 18, 2023. Accessed June 8, 2023. https://www.justice.gov/usao-edny/pr/founder-and-majority-owner-bitzlato-cryptocurrency-exchange-charged-unlicensed-money

US Treasury. 2018. Press release*: "Treasury designated Iran-based financial facilitators of malicious cyber activity and for the first time identifies associated digital currency addresses"*. November 28, 2018. Accessed June 4, 2023. https://home.treasury.gov/news/press-releases/sm556

US Treasury. 2019. Press release: *"Treasury sanctions North-Korean state-sponsored malicious cyber groups"*. September 13, 2019. Accessed June 4, 2023. https://home.treasury.gov/news/press-releases/sm774

Zamfir, Claudiu. 2022. *"Șeful Binance a venit la București: România e o piață importantă"*. September 19, 2022. Accessed March 12, 2023. https://www.startupcafe.ro/afaceri/seful-binance-bucuresti-romania-piata-importanta.htm