VIRTUAL ASSETS: HOLISTIC DATA ANALYSIS AS THE WAY FORWARD TO MITIGATE RISKS TO NATIONAL SECURITY AND FINANCIAL STABILITY

Bogdan VACUSTA
Blockchain Intelligence Professionals Association
bogdan.vacusta@blockchaintelligence.com

Abstract: Every day brings about a significant volume of data generated by financial entities, which makes it necessary that regulators, supervisors, and law enforcement bodies implement or enhance new capabilities for conducting data analysis and for mitigating risks linked to national security and financial stability. This paper presents the key elements of the challenges related to implementing a comprehensive approach regarding the transfer of virtual assets and highlights the necessity to improve resource management for a better monitoring, reporting and data analysis involving the entities associated with the transfer of virtual assets. Analyzing the data related to virtual asset transactions requires a strong collaboration between public and private organizations, with a focus on an intelligence-led approach, considering the increasing links between cyber security, money laundering, terrorism financing, sanctions evasion and state-sponsored illicit actions.
To support this collaboration, it is essential to cover the existing data gaps, harmonize data reporting standards and prioritize data analysis platforms which can map the links between traditional finance and virtual assets.
Keywords: Data, Virtual assets, Blockchain, Analysis, Finance, Intelligence.

INTRODUCTION

The amount of data created, captured, copied, and consumed globally is forecast to reach 180 zettabytes (one zettabyte contains 1,000,000,000,000,000,000,000 bytes, the basic unit in digital storage) in 2025, up from 64.2 zettabytes in 2020. Data involving financial transactions conducted through different national and international systems represent part of this huge amount of data, requiring constant data analysis to achieve specific objectives linked to financial stability, national security and to minimize risks linked to money laundering, terrorism financing, sanctions evasion or other illicit activities.

The last 10 years showed an increased impact of innovative technologies in the process of generating and managing data, one of these technologies being blockchain / distributed ledger technology. According to Oracle, blockchain is a ledger of decentralized data that is securely shared. Blockchain technology enables a group of selected participants to share data. Data is broken up into shared blocks that are chained together with unique identifiers in the form of cryptographic hashes. Blockchain provides data integrity with a single source of truth, eliminating data duplication and increasing security (Oracle, 2023). It facilitates the transfer of value in a decentralized manner, through assets known as "virtual assets," "crypto assets" or "cryptocurrencies," terms commonly used interchangeably, posing a significant challenge for traditional centralized systems and organizations.

As the main objective of this paper is risk management by improving data analysis capabilities, the terms "virtual assets" (VAs) and "virtual asset service providers" (VASPs) will be used throughout its content, according to comprehensive guidance on managing risks from the Financial Action Task Force (FATF), the international standard-setting body for anti-money laundering, countering the financing of terrorism and countering proliferation financing.

WHAT IS A VIRTUAL ASSET (VA) AND THE NECESSITY OF A HOLISTIC APPROACH

A virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes (Mazullo, Renz, Rubin, 2022). The most used VAs are mediums of exchange, for which generation or ownership records supported through a distributed ledger technology that relies on cryptography, such as a blockchain (US Presidency, 2022). Many popular VAs operate on public blockchains, where pseudonymous transaction information is viewable (FATF 2020).

The FATF definition of VASPs provides examples of specific financial activities and functions, it does not limit the definition to a particular kind of entity. Still, it considers how a person uses the VAs and for whose benefit. According to the FATF, if a person (natural or legal) is engaged as a business in any of the activities described below for or on behalf of another person, then that person is, by definition, a VASP, regardless of the technology used to facilitate these activities (FATF 2021a):

- exchange between VAs and fiat currencies
- exchange between one or more type of VAs
- transfer of VAs (to conduct a transaction on behalf of another natural or legal person that moves a VA from one VA address or account to another)
- safekeeping and/or administration of VAs or instruments enabling control over VAs (Gracey 2021)
- participation in and provision of financial services related to an issuer's offer and/or sale of a VA (Waghorn, 2021).

Most recently, as of July 2023, the 24-hour average trading volume of all VAs globally came to 29.2 billion USD. The global VAs market cap on 7 of August 2023 was 1.6 trillion USD, a huge increase since the end of 2013, when the global market cap was 1.21 billion USD (CoinMarketCap.com, 2023).

VAs represent only one major practical financial application on how blockchain technology can be deployed on a wider scale in different sectors of activity. Transactions involving VAs have a pseudo-anonymous nature, contrary to common opinion that they are anonymous. The challenge on de-anonymizing them has to do with data analysis across multiple public and confidential data sets, managed by different stakeholders or organizations, each having the duty of protecting customer personal data, this being the main reason why global efforts on the regulation and supervision of VAs have proven a tough objective to be achieved.

In the European Union, the European Parliament adopted in April 2023 the Markets in Crypto Assets (MiCA) Regulation, a dedicated and harmonized legislative framework for VAs, with its provisions to be fully applied from January 2025. The MiCA text is following in general lines the FATF recommendations on VAs, but the final text of MiCA excluded Decentralized Finance (DeFi - Decentralized Finance consists in technical programs running independently, in a fully decentralized manner without any intermediary, allowing financial products and services to be built as decentralized applications (dApps) on the Ethereum blockchain network), even the FATF guidance already mentioned that *"individuals or entities who control or influence over a DeFi arrangement would be captured as VASPs"* (FATF 2021a). According to MiCA, DeFi will be the subject of an interim report only in the first quarter of 2025 and a full report in the first quarter of 2027, which effectively means there will be no clear rules for DeFi in the next 5 years.

DeFi grew significantly in 2022 and early 2023, especially after the high-profile collapse of FTX, a centralized VASP, statistics showing a major DeFi trading volume in late 2022, with an increasing number of users choosing decentralized exchanges (DEXs) and decentralized applications (dApps) instead of centralized VASPs (Mandara, Hafeez. 2023).

DeFi's importance was highlighted by the Organization for Economic Co-operation and Development (OECD) in a special report issued in January 2022, which includes policy options for consideration by regulators and supervisors. The document from OECD mentions some of the characteristics of DeFi may be incompatible with existing regulatory frameworks involving financial intermediaries, requiring the redesign of the regulatory tools applicable in centralized settings in order to be made interoperable and compatible with decentralized structures. (OECD, 2022).

The OECD report recommends as a policy option to explore the availability of DeFi data and information, because *"good quality data improves the visibility and measurement of risks, preparing also any possible future policy intervention"* (OECD 2022).

Managing risks linked to VAs also requires DeFi data analysis, especially considering the increasing use of DeFi protocols in illicit activities.

The increasing use of DeFi for illicit activities and not having DeFi covered under MiCA leaves a huge data gap when it comes to data analysis involving VAs used for illicit activities.

According to OECD, pseudonymity, the lack of customer due diligence (CDD) and completion of other anti-money laundering / countering the financing of terrorism (AML/CFT) processes by most DeFi applications gives rise to risks of money laundering, terrorism financing, and other illicit use, facilitating misconduct. Participation in DeFi platforms only requires connection to a wallet, and some wallets do not require CDD or other AML/CFT controls for their opening (OECD 2022).

All activities involving DeFi transactions are publicly available and recorded on chain (not like centralized Virtual Asset Service Providers (VASPs)), but the key difference from centralized VASPs is that DeFi protocols do not allow the conversion of VAs into cash, which in theory may not help criminals to obscure the flow of funds and rapidly monetize their proceeds of crime. The increasing use of DeFi by illicit actors has to do with cutting

the flow of illicit funds (by conducting multiple conversions across different VAs, mixers or tumblers). This technology combines multiple transactions, distributing them among multiple wallets and other programmable applications, complicating data analysis. As a consequence, law enforcement investigations and legal procedures are delayed, which may affect public confidence and even impact financial stability.

In March 2023, The Bank of International Settlements (BIS) started Project Atlas (BIS 2023b), to gain insights into DeFi and VAs markets, by developing a data platform using off-chain data (from regulated entities and VASPs) and on-chain data (from public blockchains). Project Atlas will address the pressing need of the public sector to have data about capital flows in VAs, supporting policy makers to make informed decisions and enhance central banks' analytical and technical capabilities.

On 27 June 2023, FATF released its fourth annual report on VAs and VASPs, which highlights that risks posed by DeFi and peer-to-peer (P2P) transactions could increase, recommending the public sector to *"assess illicit finance risks of DeFi arrangements and the risks associated with unhosted wallets, including P2P transactions"* (FATF 2023c).

Managing risks involving the use of VAs requires multiple data sets (including DeFi, anonymous wallets and P2P transactions data, cyber-data), which actually means it is possible to identify the risks with a holistic, comprehensive approach, by referring to the whole, rather than part of it.

In practical terms for the VAs sector, such an integrated approach would also allow to identify the risks only by conducting a full analysis of data sets coming from public (on-chain data) and private sources (off-chain data).

There is a significant data gap in analyzing interactions between VAs and the traditional finance and banking sector, which also makes it difficult to manage risky or illicit actions involving the use of VAs in activities such as money laundering, cyber crime, terrorist financing, sanctions evasion, theft, fraud etc.

In a paper issued on 22nd August 2023, The Bank of International Settlements (BIS) mentioned a holistic approach on VAs "*would establish activity-based regulation that is enhanced and complemented by entity-based regulation"* (BIS 2023b).

FINANCIAL INSTITUTIONS AND THEIR EXPOSURE TO VIRTUAL ASSETS' RISKS

According to latest statistics from 2021 on non-cash payments from the European Central Bank (ECB), the total number of non-cash payments in the Eurozone increased by 12.5% to 114.2 billion Euro and total value increased by 18.6% to 197.0 trillion EUR. Card payments accounted for 49% of total number of non-cash payments, while credit transfers accounted for 22% and direct debits accounted for 20%. (ECB 2021).

Statistics from the ECB do not have any public data regarding the amount of VAs transactions processed by financial institutions (FIs), especially because there is no standardized approach to assess it across the financial and banking sector.

In May 2023, the European Systemic Risk Board (ESRB) pointed out this data gap in a report, considering there is limited information available to assess the exposure and impact of VAs. ESRB recommended as a policy option to improve processes on how data is assessed, monitored, reported, also encouraging work on standardized templates across competent authorities and financial institutions (ESRB 2023).

Any transaction with VAs involves interactions with the traditional finance and banking sector when fiat is converted into VAs or the other way round. These interactions usually involve payment institutions, with transfers being processed using bank account details, VAs wallets and addresses, IP addresses, device IDs and Merchant Category Codes for credit or debit card transactions. A Merchant Category Code (MCC) is a 4-digit number used to classify a business by the types of goods or services provided and a credit card company such as Visa or MasterCard assigns it when the business first starts accepting that card as a form of payment.

Research from CipherTrace show that "*8 out of 10 top banks in the USA unknowingly harbor illicit VAs transactions*", mainly because unregistered businesses such as VASPs use the payment networks to process funds (CipherTrace 2020).

Since 2018, Visa and MasterCard have reclassified the way transactions involving VAs are processed on their networks: these are now identified with the 6051 MCC code, but only if the compliance procedures of the FI are implemented with an elevated level of accuracy (Fathi 2021).

A growing number of FIs offer VAs products and services – such as custody and exchange services – and these financial institutions will consequently face direct exposure to multiple illicit activity typologies. However, the most important analysis to assess the VAs risks is linked to the indirect exposure of the FIs.

For example, a FI may have customers who use their fiat accounts to purchase VAs at VASPs located in other districts. In some cases, this might be readily detectable, for example, if the VASP's trading name is referenced on the payment's details or if the MCC 6051 is highlighted. In many instances, however, it may not be readily apparent. High-risk VASPs frequently rely on misleading legal names or other identifiers to mask their true purpose of business, obtain MCC for other type of commercial activity and sometimes operate through complex corporate structures. Without sufficient controls in place to detect this type of activity, the FI could face significant exposure to VAs-related risks (Carlisle 2021).

In 2017, FinCEN imposed a 110 million USD penalty on the VASP known as BTC-e, which was accused of facilitating more than 4 billion USD in VAs money laundering. BTC-e was taken down by US law enforcement and its founder Alexander Vinnik remained in US custody (FinCEN 2016). The key element about BTC-e is that it used the legal name Canton Business Corporation to receive fiat currency wire transfers from customers and operated through a series of shell companies registered in the British Virgin Islands and the Seychelles, among other locations - structures designed to prevent compliance officers from understanding its true purposes of business (Carlisle 2023).

FIs can also face indirect exposure to VAs-related risks through their correspondent relationships. Where a bank facilitates currency clearing or provides other services on behalf

of counterparty FIs, it may be exposed to risks where those FIs maintain relationships with VASPs or other VAs businesses (Elliptic 2023). The Wolfsberg Group recently addressed this type of exposure in February 2023, with the release of updated questionnaires on correspondent banking due diligence and financial crime compliance, creating the framework to obtain further information about internal policies and procedures (The Wolfsberg Group 2023a / 2023b).

CHALLENGES AND OPPORTUNITIES RELATED TO ACHIEVING A HOLISTIC APPROACH

This paper provides explanations about the data gaps in mapping the risks involving VAs and highlights the necessity to use all available data and analytical tools to achieve a holistic and integrated approach, allowing the faster identification of risky transactions across different FIs, reporting them to the FIU and initiating investigations once illicit activities have been identified.

MiCA is just a first regulatory step for VAs

On 25th of May 2023, the European Systemic Risk Board (ESRB) published a report on VAs and DeFi, considering systemic implications and policy options (European Systemic Risk Board 2023).

According to ESRB report, MiCA left unaddressed the following challenges:

- not establishing requirements for FIs to report exposure to VAs;
- not applying standardized reporting requirements for all entities carrying out VAs activities (e.g. wallet providers, including exchanges/trading platforms that provide e-wallet services, are not required under MiCA to report any data pursuant to a standard template);
- not clarifying comprehensive reporting on linkages between trading platforms;
- not including any prohibitions for any combinations of services within the same entity/ group, expressly designed to mitigate cumulative prudential, reputational, or operational risks across an entity or group;
- not including prudential consolidation rules (e.g. those applicable to banks under the Capital Requirements Directive/Regulation (Directive 2013/36/EU and Regulation (EU) 575/2013));
- not including supplementary supervision arrangements (e.g. those applicable to financial conglomerates within the scope of Directive 2002/87/EC (the Financial Conglomerates Directive));
- not including powers for the supervisor to require a "push out" of specific business activities to a separate legal entity within the group (e.g. as per the power available to supervisors under Article 11(5) of the second Payment Services Directive (Directive (EU) 2015/2366).

ESRB proposes three areas of focus, listed in order of urgency and importance (European Systemic Risk Board 2023):

- Improve the EU's capacity to monitor potential contagion channels between the VA sector and the traditional financial sector, and within the VA sector;

- Carry out assessments of risks posed by VAs conglomerates and identify potential additional actions to mitigate observed risks;
- Promote EU-level knowledge exchange and monitoring of market developments, focusing on (a) operational resilience, (b) DeFi, and (c) VAs staking and lending.

ESRB highlights that "*the identification and quantification of risks to financial stability from the VAs sector is possible only with transparent, consistent, timely and trusted data on VA markets and their linkages with the financial sector (and, increasingly, within the VA sector).*"

Existing gaps in managing risks

On 26th of June 2021, The EU's European Court of Auditors (ECA) has issued a special report on EU efforts to fight money laundering in the banking sector. The report found "*institutional fragmentation and poor coordination at EU level when it came to actions to prevent money laundering and take action where risk is identified*." ECA mentioned the *"EU needs a stronger and more coherent oversight framework for combating money laundering because supervision still takes place at national level with an insufficient EU oversight framework."* (ECA, 2021)

In July 2021, the European Commission published an AML/CFT package consisting of 4 legislative proposals. One of these proposals was the recasting of Regulation (EU) 2015/847 ('The Transfer of Funds Regulation' or 'TFR') to extend its scope to transfers of VAs, in line with the FATF's standards. Article 30(b) amends Article 3(2) of Directive (EU) 2015/849 and highlights VASPs are now subject to the same ML/TF requirements and ML/TF supervision as credit and financial institutions. Consequently, any data gaps in managing ML/TF risks also relate to VASPs.

The European Banking Authority's included remarks on supervision: *"AML/CFT reviews have been conducted and the review teams found that "cooperation with FIUs was not always systematic and continued to be largely ineffective in most Member States, though several Competent Authorities (CAs) had started to take steps to address this"*. EBA highlights in its report the importance of supervisory cooperation and a holistic, joint approach to fighting financial crime: *"a coordinated, joint approach will be particularly important as the new institutional AML/CFT framework is set up."* (EBA 2022)

On 16 June 2023, EBA published its Report on money laundering and terrorist financing (ML/TF) risks associated with EU payment institutions. Its findings suggest that *"ML/TF risks in the sector may not be assessed and managed effectively by institutions and their supervisors."* (EBA 2023d).

The EBA's findings suggest that institutions do not manage ML/TF risk adequately. AML/CFT internal controls in payment institutions are often insufficient to prevent ML/TF and failure to manage ML/TF risks in the payment institutions sector can impact the integrity of the EU's financial system. The report highlights that those payments institutions having VASPs as institutional customers, facilitating trades with VAs, involve a higher ML/TF risk. (EBA 2023d).

The ESRB report from May 2023 highlighted the limited information available to assess the exposures and impact of VAs, making it necessary to improve processes on how data is assessed, monitored, reported, also encouraging the work on standardized templates across competent authorities and financial institutions (European Systemic Risk Board 2023).

The requirement to focus on a standard reporting format – including technical data – was also mentioned in a report published by the Egmont Group on "Fintech Cooperation and Associated Cybercrime Typologies and Risks" (Egmont Group of Financial Intelligence Units 2022). Such a standard reporting format is highly required to facilitate the collection of already available information by Financial Technology companies (FinTechs) such as VASPs and its use by regulators, supervisors, or law enforcement (Egmont Group of Financial Intelligence Units 2022).

The Bank of International Settlements (BIS) mentioned the data gaps as a significant issue in their recently issued paper focused on the financial stability risks related to VAs. According to BIS, "*the only way to truly monitor financial stability risks is by filling the data gaps that are necessary to understand the technology and the interconnections across the traditional and VAs markets*" (BIS 2023a). The ideal data set and metrics to monitor VAs markets should address the following risks: market risks, liquidity risks, credit risks, operational risks, bank disintermediation risks, capital flow risks.

Financial Intelligence Units (FIUs) and their journey to digital transformation

The FATF issued multiple recommendations, which are now an international standard to allow countries the implementation of a consistent framework of actions to combat money laundering and terrorist financing, as well as the financing of proliferation of weapons of mass destruction (FATF, 40 Recommendations).

Recommendation number 29 of FATF says *"countries should set up a FIU that serves as a national centre for the receipt and analysis of suspicious transaction reports and other information relevant to money laundering, associated predicate offences and terrorist financing, and for the dissemination of the results of that analysis"*. Recommendation 29 does not prejudge a country's choice for a particular FIU model considering there are different FIU models, but the FATF highlights the FIU "*should be operationally independent and autonomous, free from any undue political, government or industry influence or interference, which might compromise its operational independence".*

In a report from March 2023, the Financial Action Task Force (FATF) concluded the prevalent use of VAs by cyber criminals, because these assets offer decentralized, permissionless and fast cross border value transfer (FATF 2023b).

However, the traceability and immutability of the blockchain on which these VAs move offers unique opportunities to follow the trail, disrupt the financial flows of these proceeds of crime. To achieve this, it is essential to integrate data available on blockchains with operational intelligence and data sets reported by regulated sectors under different compliance obligations such as cyber security, money laundering, terrorist financing, sanctions evasion etc.

The EU Anti-Money Laundering Directive requires obliged entities to inform the FIU in the Member State where they are established if they know, suspect or have a reasonable suspicion that funds involved in a transaction are the proceeds of criminal activity or are related to financing of terrorism and by promptly responding to requests for additional information by the FIU. The information flows should also include feedback on and follow-up to the reporting. This feedback should be timely and cover the effectiveness of and the follow-up to reports. (European Commission 2019)

To ensure national security and financial stability, it is essential that FIUs receive quality information on transactions or attempted transactions involving the use of VAs linked to illicit activities.

The EC's report assessing the framework for cooperation between FIUs makes reference to another 2016 mapping report, which highlighted the lack of IT tools - a number of FIUs maintaining paper-based working procedures – which poses a difficulty for FIUs to effectively process and analyze information, due to the recent high volume of Suspicious Transaction Reports (STRs) received (European Commission, 2019).

A report published by the Egmont Group on "Fintech Cooperation and Associated Cybercrime Typologies and Risks" indicated: "*some of the FIUs could not analyze VAs related cases at all and over half of the FIUs had to rely on open-source intelligence information since their internal analytical software did not possess the capability to analyze such transactions"* (Egmont Group of Financial Intelligence Units 2022).

The designated Romanian FIU is the National Office for the Prevention and Control of Money Laundering (NOPCML-FIU).

A Council of Europe Moneyval report from July 2023 on Romania's measures to combat money laundering, terrorist financing, show the NOPCML-FIU's current analytical tools require improvements to enhance capabilities to conduct complex operational and strategic analysis (Moneyval 2023).

The report show paper-based working procedures are still operational, allowing potential errors in the analysis of STRs, which can impede the identification of suspicious activity (Moneyval 2023).

The report also mentions that the NOPCML-FIU does not have access to dedicated blockchain analytical tools, which would assist in supervisory activities and analyzing the suspicious transactions reports related to virtual assets transactions (Moneyval 2023).

NOPCML-FIU's 2021 report shows statistics regarding 8 total STRs submitted by VASPs in 2019 (2 STRs), 2020 (2 STRs) and 2021 (4 STRs). The 2021 report also highlights those banks and other financial institutions submitted more than 10.000 STRs each year.

NOPCML's 2022 report also shows more than 10.000 STRs submitted by banks, but the report no longer mentions how many STRs were submitted by VASPs. The only information available for VASPs is that there are 11 entities registered with NOPCML as VASPs and only for 2 of these VASPs, on-site supervision has been deployed due to their identified

high-risk activity. However, no sanction or warning has been imposed because of the on-site supervision. It is also unclear how the 2 VASPs' risk assessments were conducted since the Moneyval report mentions there is no access to blockchain analytical tools, and these tools are the most effective way to assess risk.

Not even the number of STRs from 2022 was not mentioned in the NOPCML's 2022 report, these details appear only partially in the Moneyval report: only 2 STRs submitted until the end of June 2022 (Moneyval 2023).

FATF's fourth annual report on VAs and VASPs highlights the challenge among many authorities with regard to conducting a sectoral risk assessment for VAs and VASPs as they may not know what information, data, or methodology to use (FATF 2023c).

The Moneyval report also mentions that the Romanian authorities will undertake a dedicated sectoral risk assessment to analyze the use of VAs and VASPs, but more details are not provided. (Moneyval 2023). The recommendations from FATF include the use of blockchain analytics tools to conduct such a risk assessment, but the Moneyval report mentions the NOPCML-FIU has no access to blockchain analytical tools. Consequently, it is unclear what methodology is used, what type of data is analyzed, and which entities are involved.

The limited amount of STRs submitted by VASPs to FIUs and the difficulties of the FIUs in obtaining and recording statistical information represent problems not only for Romania, these were highlighted by Moneyval in their Typologies report from July 2023 (Council of Europe, 2023). The report also mentions *"it is possible that the true abuse of VAs and VASPs could be identified from external financial institutions (FIs)."* (Moneyval 2023).

In the case of Romania, which has a significant volume of VAs transactions (iSense Solutions, 2023), it is probable that a percent of STRs involving VAs was in fact reported by banks, payment service providers, electronic money institutions or other regulated entities for other reasons such as money laundering, fraud, theft, terrorist financing etc. Without implementing blockchain analysis tools in their internal monitoring capabilities, regulated entities are not able to assess the interactions between fiat transactions and VAs in an effective way. Consequently, financial institutions are not able to identify suspicious transactions involving VAs and report them to the FIU, hence the limited number of STRs in Romania.

To put in context and understand the recommendation from Moneyval to enhance analytical tools and capabilities, it is useful to mention the results of such an improvement made by the United Kingdom's FIU (UKFIU), the National Crime Agency (NCA). On 24 January 2023, the NCA published their 2022 Suspicious Activity Report (SARs) Annual Report, which features statistics covering the years 2020, 2021 and 2022. The report mentions the reforms to their analytical and operational systems, which allowed an increase of VAs work stream (from approx. 80 a day in September 2021 to approx. 350 a day in 2022). According to the report., this is due to *"engagement with stakeholders and the use of more suitable keywords, resulting in a steady increase of SARs identified for review"* (National Crime Agency 2023).

The necessity to improve existing legacy systems to facilitate data analysis across multiple data sets has become essential to manage risks, requiring a digital transformation of the FIUs.

Such a transformation is now a priority, according to the Egmont Group (EG) and the FATF (Egmont Group of Financial Intelligence Units - FATF 2021).

The joint EG-FATF Digital Transformation Report recognizes that "*technology has immense potential to increase the efficiency of AML/CTF workflows and the effectiveness of efforts to combat serious crime. It also provides examples of how FIUs have incorporated different digital tools to assist their operational efforts. These tools range from automation to large datasets, big data, and advanced analytics such as artificial intelligence (AI) and machine learning. The increased capability of FIUs to fight financial crime following such technological uplifts cannot be underestimated, particularly regarding FinTech and VAs, where data underpins all financial activity"* (Egmont Group of Financial Intelligence Units - FATF 2021).

The use of blockchain analytics to assess VAs risks and exposure

The FATF 2021 Guidance for a risk-based approach provides solutions to manage the risks involving the use of VAs, one of these solutions is the use of blockchain analytics (FATF 2021b).

FATF highlighted that the blockchain analytics solutions provided by private companies have limitations. According to FATF, each blockchain analytics company "*has their own methods, resources, techniques, and data which they combine with the data taken from the blockchain. It takes considerable time, resources, expertise, and investment for companies to map real-world entities onto wallets. This is an ongoing challenge, as more wallets are easily created, new businesses and services are established, new virtual assets are released, and services operate over an increasing number of blockchains. Entities, including compliant VASPs, often change their addresses, which can also challenge the attribution process. Therefore, the work of each company is not equivalent, and it is not interchangeable, which makes it difficult to know what the 'right' numbers are for market metrics."* (FATF 2021b).

According to FATF, blockchain analytics can provide "*interesting insights into the use of virtual assets that are not available with traditional financial products and services. Moreover, blockchain analysis can be useful for investigative purposes to track identified illicit funds or attribute identities of wallet holders. Such tools can be of great potential benefit to law enforcement, FIUs, supervisors, VASPs and the broader private sector in fulfilling their AML/CFT obligations and combating illicit activity*" (FATF 2021b).

FATF's fourth annual report on VAs and VASPs highlights the challenge among many districts related to conducting a national risk assessment for VAs and VASPs as they may not know what information, data, or methodology to use (FATF, June 2023).

Moneyval's report from July 2023 recommends the use of blockchain analytics tools to follow the trail of VAs, considering transaction data recorded on the blockchain is immutable. However, the report mentions that a major challenge to implement such a recommendation is the lack of knowledge and expertise on how to handle VA analysis (Moneyval 2023, 28).

On 12 June 2023, EBA published its 2022 Annual Report, which mentions the completion of its public procurement aimed at obtaining access to VAs and blockchain analytics data service providers. The tender included two distinct services: blockchain analytics services (allowing

to monitor and track financial crime and other risks related to specific tokens, VASPs, wallets or transactions) and data on VAs markets (allowing to understand broader market dynamics, including that linked to specific tokens, distributed ledger technology networks or service providers). As a result of the tender, EBA will be able to overcome any limitations of the data reported by issuers under MiCA and improve the framework and resources needed for its future supervisory tasks (EBA 2023a).

In addition, data on VAs markets and blockchain analytics services can be useful for the EBA's monitoring of risks to consumers, assessment of ML/TF risks, impact assessment accompanying the EBA's policy mandates under MiCA, and any other assessments of VAs markets and their interconnectedness with the banking and payments sectors (EBA 2023a; 7).

On 29th of March 2023, the EBA issued a consultation paper on amending Guidelines EBA/GL/2021/16 on the characteristics of a risk-based approach to AML/CFT supervision. The paper recommends the use of advanced analytics tools such as blockchain analytics and *"in some instances, competent authorities should consider whether the combination of two or more tools may be more effective*." It also mentioned that *"competent authorities should identify the ML/TF risks based on information from a variety of sources"* (EBA 2023c; 16).

Data analysis focused on capacity building

Capacity building in blockchain analytics is critical, and it should be prioritized at a national level to develop a skilled workforce and foster public-private partnerships.

A recent report by FATF on ransomware highlighted the importance of such specialized capabilities, especially in the public sector (Financial Action Task Force 2023a):

"Competent authorities should use and adapt, as necessary, traditional law enforcement techniques as well as virtual asset-specific techniques, to conduct ransomware-related money laundering investigations. Competent authorities should have the necessary specialized skills and expertise for successful financial investigations relating to ransomware. This includes development, access and training relating to blockchain analytics and monitoring tools."

Moneyval's report from July 2023 recommends the use of blockchain analytics tools to follow the trail of VAs, considering transaction data recorded on the blockchain is immutable. However, the report mentions that a major challenge to implement such a recommendation is the lack of knowledge and expertise on how to handle VA analysis (Moneyval 2023).

The necessity to focus on capacity building would create the conditions to improve private-public partnerships, creating an opportunity to focus on how each stakeholder can maximize their contribution while also benefiting from a holistic approach.

Increasing expertise and fostering a community of blockchain analytics professionals would create the conditions to improve the amount and quality of data in a coordinated and consistent manner, allowing better monitoring, reporting and information sharing in a privacy-controlled environment about emerging typologies, identified red flags, enhancing awareness and knowledge on risks associated with VAs.

MAXIMISING THE USE OF AVAILABLE DATA AND TECHNOLOGIES

A holistic approach to mitigate risks involving VAs requires the support of decision-makers who need to understand the available technologies and the type of technical data required for analysis, in order to support effective policies, regulations and procedures.

The way forward from the Bank of International Settlements

The Bank of International Settlements (BIS) mentioned the reliability of data provided by commercial data vendors and blockchain analytics companies needs to be addressed by national authorities, in order to manage the risks, recommending these potential paths forward (BIS 2023a):

- establishing a shared data repository where key information such as VA-related activity and exposures of FIs, among others, would be stored (the repository could collect information at a level of granularity that allows for further analysis to identify concrete use cases and to differentiate domestic from cross-border flows)
- defining the type and scope of data needed for effective monitoring of VA markets developments, with an emphasis on the identification of critical connections points with FIs and core market infrastructures
- defining the additional disclosure and reporting required for effective monitoring of regulated entities exposures
- development of a commonly accepted taxonomy of VAs as well as of VA-related activities and associated providers
- improving the accuracy and representativeness of VA ecosystem surveys and developing of standards
- improving the monitoring of financial stability risks, including risk catalysts, collaborating with private data vendors, as well as blockchain analysis companies and academia.

The way forward from the European Banking Authority (EBA)

On 31st of May 2023, the EBA issued a consultation paper on customer due diligence and the factors that credit and FIs should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849. (EBA 2023b).

The revised ML/TF Risk Factors Guidelines are related to FIs and the AML/CFT competent authorities (CAs) supervising those firms. With the Article 30(b) of the recasting of Regulation (EU) 2015/847 and the amendment of Article 3 of Directive (EU) 2015/849, VASPs are now included in the FIs definition and, de facto, included in the revised ML/TF Risk Factors Guidelines.

The paper from EBA is relevant to consider the type of data, which will be necessary to be monitored and reported by FIs and analyzed by regulators and supervisors, when assessing risky or illicit activities involving VAs (EBA 2023b):

- products or services offered by VASPs by using privacy-enhancing features or with a higher degree of anonymity (mixers or tumblers, obfuscated ledger technology, Internet Protocol (IP) anonymizers, ring signatures, stealth addresses, ring confidential transactions, atomic swaps, non-interactive zero-knowledge proofs, privacy coins);
- IP addresses associated with the dark web markets or other similar platforms known for using anonymous communication (encrypted emails, Virtual Private Networks (VPNs));
- self-hosted addresses on decentralized platforms, which involve the use of mixers, tumblers and other privacy enhancing technologies that may obfuscate the financial history associated with the distributed ledger address and the source of funds for the transaction;
- bridges used to change VAs to privacy coins;
- P2P VAs exchange platforms;
- VAs decentralized or distributed application, which is not controlled or influenced by a legal or natural person (often referred to as "decentralized finance" (DeFi));
- VAs' ATMs or other hardware that involves the use of cash or electronic money, that benefits from exemptions under Article 12 of Directive (EU) 2015/849 or that does not fall within the regulatory and supervisory regime in the EU;
- device IDs or IP addresses used in VAs transactions by multiple customers in various jurisdictions without reasonable explanations.

The way forward from the Egmont Group of FIUs

Egmont Group is a global organization facilitating the exchange of information, knowledge, and cooperation amongst member FIUs and has overall goal of strengthening information-sharing mechanisms to combat money laundering, terrorist financing, and associated predicate crimes.

Its Information Exchange Working Group released in July 2022 a report on "Fintech Cooperation and Associated Cybercrime Typologies and Risks", based on the results of a survey conducted between March 2020 and June 2020, with the participation of 41 FIUs. In this project, VASPs were mentioned by FIUs as a category of *"FinTech entity providing financial services, enabling payments or transfers of value by using new or emerging technologies."*

Acccording to the report, "*the customer's digital fingerprint is an essential element of the information received from FinTech entities and provides avenues for further FIU analysis. This includes the IP addresses from which the connections were made, the device identifiers and geolocation data. Technical information received from FinTech entities may include specific details on unique device identification numbers such as International Mobile Station*

Equipment Identity (IMEI), International Mobile Subscriber Identity (IMSI) or Security Element Identifier (SEID) numbers and media access control (MAC) addresses".

Other information includes digital photo selfies (picture of the customer), client identification data, files related to voice or video identification, detailed transaction communications, source of funds/wealth, economic activity, purpose of the account; expected amount and frequency of transactions, associated entities and entity structure charts.

A report by the FinTech FinCrime Exchange (FFE) in partnership with the Royal United Services Institute (RUSI), Regulatory DataCorp (RDC) and leaders from 16 FinTech entities reveals that FinTech entities (including VASPs) hold data not routinely requested by law enforcement or FIUs, including geolocation data, login behavior, and device information (FFE, 2021).

According to EG's report on FinTech, "*the technological nature of VASPs products and services also presents opportunities to gather, collect and rely on new information, enabling FIUs to broaden the scope of their intelligence picture*."

The report from EG mentions the following elements as a non-exhaustive list of new data that can be incorporated into the analysis of FIUs: VAs wallets/addresses and associated blockchain records, various identification numbers, including IMEI, IMSI or SEID numbers, as well as MAC addresses, login behaviour and IP data, geolocation data, identification (e.g. authentication cookies) and information stored on devices.

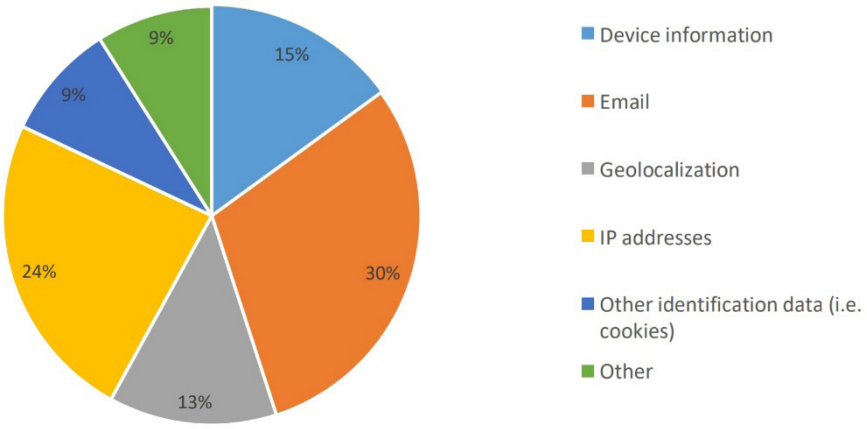

Figure 1. The information currently processed digitally by 41 FIUs
(Egmont Group 2022)

To conduct complex analysis regarding VAs transactions, EG recommends analytical tools such as network analysis and graphical tools, blockchain analytics, domain analysis tools, commercial databases and threat feeds, open source and social media, programming tools for determining trends and extracting critical information from transactional data and geographical analysis tools.

Cross-referencing data sets held by FIUs with results obtained from these analytical tools would allow the FIU to obtain information including the owner of a specific VAs wallet, when the

wallet was used, the transactions of the wallet with specific entities, pattern analysis, interactions with other Fis and risks associated with a wallet and its exposure to high-risk entities.

The International Monetary Fund (IMF) also highlighted in their FinTech notes from 2021 "*the necessity to adjust FIUs' existing practices, to ensure appropriate receipt and analysis of financial intelligence specific to VAs transactions*" (wallet account information, transaction hash and information on the originator and the recipient, login information, mobile device information etc.) (Schwarz et al. 2021).

The importance of geolocation data

In November 2022, The European Banking Authority (EBA) published its guidelines on remote customer onboarding, which highlighted the importance of identifying the location of the customers: *"Credit and financial institutions should apply controls to address associated risks, including risks associated with automatic capture of data such as the obfuscation of the location of the customer's device spoofed Internet Protocol (IP) addresses or services such as Virtual Private Networks (VPNs)"* (EBA 2022)

The problem of IP spoofing was also addressed by FATF in its Guidance for a risk-based approach to VAs and VASPs and the Guidance on digital identity (FATF 2020). FATF distinguished IP addresses as an identity attribute separated from geolocation data, considering geolocation as an example of dynamic, digital customer data sources that enable regulated entities to capture essential authentication information. To combat illicit activities, FATF indicates that no single data type is sufficient trustworthy for identity verification and authentication (FATF 2020).

The need for financial institutions with exposure to VAs to include geolocation data analysis in their compliance programs was highlighted by the U.S. Department of the Treasury's Office on Foreign Assets Control (OFAC). In this regard, BitPay AC and BitGo received financial sanctions from OFAC, even though internal compliance systems performed IP address analysis and blocked addresses associated with authorities subject to international sanctions (U.S. Department of the Treasury 2020). OFAC has highlighted the obligations of FIs such as VASPs to use systems allowing identification of customers' true location, given the widespread use of anonymization tools such as VPNs (U.S. Department of the Treasury 2021).

Maximizing the use of the "Ma3tch" technology

Article 56(2) of the EU Anti-Money Laundering Directive obliges FIUs to *"cooperate in the application of state-of-the-art technologies"* allowing them *"to match their data with that of other FIUs in an anonymous way by ensuring full protection of personal data with the aim of detecting subjects of the FIU's interests in other Member States and identifying their proceeds and funds"*. This provision was meant to maximize the use of the "Ma3tch" technology, which was developed in 2014 with the support of Europol.

The use of blockchain analytical tools by FIUs could be linked to existing data analysis capabilities such as "Ma3tch", because their core principles are similar (data-matching across multiple data sets), but a technological upgrade and an operational reform are necessary to reach their full potential and allow a better engagement of FIUs with regulators, supervisors and law enforcement (European Commission 2019).

CONCLUSIONS

Building a comprehensive institutional architecture to assess the risks posed by VAs to national security and financial stability is a major challenge for national authorities. Such an architecture should include public and private organisations and must consider data analysis as a priority, based on the capacity of all the entities in the financial, banking and technology sector to contribute to the overall risk assessment.

Reporting transactions with VAs linked to risky or illicit activities (cyber events, money laundering, terrorism financing, sanctions evasion, proliferation of weapons of mass destruction etc.) is difficult now, considering there is no standardized approach across public and private organisations. However, by using standardized methods and through the mandatory implementation of rules, data gaps can be gradually covered.

A holistic approach to mitigate risks involving VAs requires the support of decision-makers who need to understand the available technologies and the type of technical data required for analysis, to support effective policies, regulations, and procedures. Effectiveness in decisions aimed to monitor and report relevant data sets would also ensure a better coordination and overall data analysis.

A clear line between VAs risks to national security and financial stability can no longer be drawn as data required for one of these areas is also relevant for the other one. Using consistent and relevant technical criteria can speed up the overall risk assessment, while ensuring standardisation across multiple types of organisations, maximizing technical capacity for monitoring, reporting and analysis.

REFERECENCE LIST

Bank of International Settlements (BIS). 2023a. *Financial stability risks from cryptoassets in emerging market economies.* https://www.bis.org/publ/bppdf/bispap138.pdf [Accessed 23rd August 2023].

Bank of International Settlements (BIS). 2023b. *Project Atlas: Mapping the world of decentralised finance*. https://www.bis.org/about/bisih/topics/suptech_regtech/atlas.htm [Accessed 11th August 2023].

Carlisle, D. 2021. *The importance of knowing your VASP in AML Compliance*. https://www.elliptic.co/blog/the-importance-of-knowing-your-vasp-in-aml-compliance [Accessed 4th July 2023].

Carlisle, D. 2023. *Why banks need to prioritize crypto due diligence and monitoring*. https://www.elliptic.co/blog/analysis/why-banks-need-to-prioritize-crypto-due-diligence-and-monitoring [Accessed 14th August 2023].

Chainalysis. 2021. *Infrastructure Investment Act Expands Tax Reporting Obligations for Cryptocurrency Exchanges and Others.* https://blog.chainalysis.com/reports/infrastructure-investment-act-tax-reporting-obligations-cryptocurrency/ [Accessed 4th August 2023].

Ciphertrace. 2020. *CipherTrace Armada – Virtual Asset Risk Mitigation for Financial Institutions.* https://ciphertrace.com/wp-content/uploads/2020/05/CipherTrace-Armada-Virtual-Asset-Risk-Mitigation-for-Financial-Institutions-051320.pdf [Accessed 14th May 2023].

Coinmarketcap.com. 2023. *Global Live Cryptocurrency Charts & Market Data*. https://coinmarketcap.com/charts/ [Accessed 30th July 2023].

Council of Europe. 2023. *Money laundering and Terrorist Financing Risks in the World of Virtual Assets*. https://rm.coe.int/moneyval-2023-12-vasp-typologies-report/1680abdec4 [Accessed 28th July 2023].

Council of Europe. 2023. *Mutual evaluation report of Romania. Anti-money laundering and counter-terrorist financing measures.* https://www.fatf-gafi.org/en/publications/Mutualevaluations/MER-Romania-2023.html [Accessed 29th July 2023].

Egmont Group of Financial Intelligence units, Financial Action Task Force (FATF). 2021. *Publication of the Joint EG-FATF Digital Transformation Report*. https://egmontgroup.org/news/publication-of-the-joint-eg-fatf-digital-transformation-report/
[Accessed 26th July 2023].

Egmont Group of Financial Intelligence Units Publications. 2022. *Fintech Cooperation and Associated Cybercrime Typologies and Risks.* https://egmontgroup.org/resource_type/publications/ [Accessed 6th April 2023].

Elliptic. 2023. *The Top Ten Latest Crypto Crime Typologies*. *Elliptic Typologies Report 2023.* https://hub.elliptic.co/analysis/the-top-ten-latest-crypto-crime-typologies/ [Accessed 12th August 2023].

European Banking Authority (EBA). 2023a. *Annual Report 2022*. https://www.eba.europa.eu/sites/default/documents/files/document_library/About%20Us/Annual%20Reports/2022/1056351/EBA%202022%20Annual%20Report.pdf [Accessed 14th August 2023].

European Banking Authority (EBA). 2023b. *Consultation Paper - Guidelines amending Guidelines EBA/2021/02 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849.* https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Consultations/2023/Consultation%20on%20revised%20Guidelines%20on%20money%20laundering%20and%20terrorist%20financing%20%28ML-TF%29%20risk%20factors/1055913/Consultation%20paper%20on%20amending%20Guidelines%20on%20ML%20FT%20risk%20factors.pdf [Accessed 18th June 2023].

European Banking Authority (EBA). 2023c. *Consultation Paper - Guidelines amending Guidelines EBA/GL/2021/16 on the characteristics of a risk-based approach to anti-money laundering and terrorist financing supervision, and the steps to be taken when conducting supervision on a risk-sensitive basis under Article 48(10) of Directive (EU) 2015/849 (The Risk-Based Supervision Guidelines)*. https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Consultations/2023/Consultation%20on%20draft%20Guidelines%20amending%20Risk%20Based%20Supervision%20Guidelines/1054077/CP%20on%20Guidelines%20amending%20Risk%20Based%20Supervision%20Guidelines.pdf [Accessed 14th May 2023].

European Banking Authority (EBA). 2023d. *EBA Report on ML/TF risks associated with payment institutions*. https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2023/1056453/Report%20on%20ML%20TF%20risks%20associated%20with%20payment%20institutions.pdf [Accessed 2nd August 2023].

European Banking Authority (EBA). 2022. Final Report - *Guidelines on the use of Remote Customer Onboarding Solutions under Article 13(1) of Directive (EU) 2015/849*. https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2022/EBA-GL-2022-15%20GL%20on%20remote%20customer%20onboarding/1043884/Guidelines%20on%20the%20use%20of%20Remote%20Customer%20Onboarding%20Solutions.pdf [Accessed 18th August 2023].

European Central Bank (ECB). 2022. *Payments statistics: 2021*. https://www.ecb.europa.eu/press/pr/stats/paysec/html/ecb.pis2021~956efe1ee6.en.html [Accessed 2nd August 2023].

European Commission. 2019. *Report from the Commission to the European Parliament and the Council assessing the framework for cooperation between Financial Intelligence Units*. https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52019DC0371 [Accessed 7th August 2023].

European Court of Auditors (ECA). 2021. *Special Report - EU efforts to fight money laundering in the banking sector are fragmented and implementation is insufficien*t. https://www.eca.europa.eu/Lists/ECADocuments/SR21_13/SR_AML_EN.pdf [Accessed 26th July 2023].

European Supervisory Authority (ESA). 2022. "*Joint European Supervisory Authority response to the European Commission's February 2021 Call for Advice on digital finance and related issues: regulation and supervision of more fragmented or non-integrated value chains, platforms and bundling of various financial services, and risks of groups combining different activities*". https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2022/1026595/ESA%202022%2001%20ESA%20Final%20Report%20on%20Digital%20Finance.pdf [Accessed 4th August 2023].

European Systemic Risk Board (ESRB). 2023. *ESRB publishes report on cryptos and decentralised finance.*

Systemic implications and policy options. https://www.esrb.europa.eu/news/pr/date/2023/html/esrb.pr230525~c74fa66621.en.html [Accessed 14th August 2023].

Fathi, A. 2021. *Russia to block crypto transactions under MCC code 6051*. https://theindustryspread.com/russia-to-block-crypto-transactions-under-mcc-code-6051/ [Accessed 24th July 2023].

Financial Action Task Force (FATF). 2020. *Guidance on Digital ID*. https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Digital-identity-guidance.html#:~:text=The%20FATF%20has%20developed%20guidance%20that%20will%20help,secure%20to%20identify%20individuals%20in%20the%20financial%20sector [Accessed 19th July 2023].

Financial Action Task Force (FATF). 2021a. *Second 12-Month Review of Revised FATF Standards - Virtual Assets and VASPs*. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Second-12-month-review-virtual-assets-vasps.html [Accessed 4th August 2023].

Financial Action Task Force (FATF). 2021b. *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.* https://www.fatf-gafi.org/en/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html [Accessed 5th August 2023].

Financial Action Task Force (FATF). 2023a. *FATF Recommendations*. https://www.fatf-gafi.org/en/topics/fatf-recommendations.html [Accessed 7th August 2023].

Financial Action Task Force (FATF). 2023b *FATF Report - Countering Ransomware Financing*. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Countering-Ransomware-Financing.pdf.coredownload.pdf [Accessed 14th May 2023].

Financial Action Task Force (FATF). 2023c. *Virtual Assets: Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html [Accessed 18th July 2023].

Financial Crimes Enforcement Network (FinCEN). 2016. *Press release: FinCEN Issues Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime*. https://www.fincen.gov/news/news-releases/fincen-issues-advisory-financial-institutions-cyber-events-and-cyber-enabled [Accessed 18th June 2023].

FinTech FinCrime Exchange (FFE). 2021. FinTechs and Law Enforcement Partnerships. https://fintrail.com/news/2020/10/5/fintech-and-law-enforcement-partnerships [Accessed 16th June 2023].

ISense Solutions. 2023. *Studiu iSense Solutions: Ce cred românii despre criptomonede.* https://www.isensesolutions.ro/studiu-isense-solutions-ce-cred-romanii-despre-criptomonede/ [Accessed 14th July 2023].

Gracey, M. 2021. *What is a Virtual Asset Service Provider (VASP)?.* https://www.yugatech.com/guides/what-is-a-virtual-asset-service-provider-vasp-bsp/ [Accessed 14th July 2023].

Mandara, D. & Hafeez, B. 2023. *Hedge funds see bullish trends in DeFi even as Fed rate risk looms.* https://www.dlnews.com/articles/defi/hedge-funds-see-bullish-trends-in-defi-even-as-fed-rate-risk-looms/ [Accessed 18th July 2023].

Mazullo, N., Renz, K. & Rubin, A. 2022. *Understanding the risks and red flags of virtual assets*. https://www.crowe.com/insights/fincrime-in-context/understanding-the-risks-and-red-flags-of-virtual-assets [Accessed 8th August 2023].

National Crime Agency (NCA) 2023. *Suspicious Activity Report (SARs) Annual Report 2022.* https://nationalcrimeagency.gov.uk/news/suspicious-activity-report-sars-annual-report-2022 [Accessed 14th April 2023].

National Office for the Prevention and Control of Money Laundering (NOPCML-FIU). 2023. *Activity report 2022*. https://www.onpcsb.ro/uploads/articole/attachments/6474b0828e101273841000.pdf [Accessed 14th July 2023].

National Office for the Prevention and Control of Money Laundering (NOPCML-FIU). 2022. *Activity report 2021*. https://www.onpcsb.ro/pdf/Raport%20activitate%202021.pdf [Accessed 14th July 2023].

Organization for Economic Co-operation and Development (OECD). 2022. *Why Decentralised Finance (DeFi) Matters and the Policy Implications*. https://www.oecd-ilibrary.org/finance-and-investment/why-decentralised-finance-defi-matters-and-the-policy-implications_109084ae-en [Accessed 14th August 2023].

Oracle. 2023. *What is Blockchain?* https://www.oracle.com/middleeast/blockchain/what-is-blockchain/ [Accessed 12th August 2023].

Schwarz, N., Chen, K., Poh, K., Jackson, G., Kao, K. & Markevych, M. 2021. *FinTech Notes - Virtual Assets*

and Anti-Money Laundering and Combating the Financing of Terrorism (1): Some Legal and Practical Considerations. Washington, D.C., International Monetary Fund. https://www.elibrary.imf.org/view/journals/063/2021/002/063.2021.issue-002-en.xml [Accessed August 14th, 2023].

Biden, J.R. 2022. *Executive Order 14067 - Ensuring Responsible Development of Digital Assets*. https://www.presidency.ucsb.edu/documents/executive-order-14067-ensuring-responsible-development-digital-assets [Accessed 12th August 2023].

U.S. Department of the Treasury. 2020. *Press release: Settlement Agreement between the U.S. Department of the Treasury's Office of Foreign Assets Control and BitGo, Inc.* https://ofac.treasury.gov/recent-actions/20201230_33 [Accessed 18th May 2023].

U.S. Department of the Treasury. 2021. *Press release: Settlement Agreement between the U.S. Department of the Treasury's Office of Foreign Assets Control and BitPay, Inc.* https://ofac.treasury.gov/recent-actions/20210218 [Accessed 19th May 2023].

Waghorn, T. 2021. *New AML Registration Requirements for Virtual Asset Service Providers*. https://hayes-solicitors.ie/News/New-AML-Registration-Requirements-for-Virtual-Asset-Service-Providers [Accessed 12th August 2023].

Wolfsberg Group. 2023a. *Correspondent Banking Due Diligence Questionnaire (CBDDQ) Guidance*. https://db.wolfsberg-group.org/assets/1869c58a-7b5e-4750-ae67-519badeab82d/CBDDQ%20Guidance%20v2.0.pdf [Accessed 18th July 2023].

Wolfsberg Group. 2023b. *Financial Crime Compliance Questionnaire (FCCQ V1.2)*. https://db.wolfsberg-group.org/assets/8f28b4be-5808-485f-aba0-ff79ebce8294/FCCQ%20v1.2.pdf [Accessed 18th July 2023].

Bogdan VACUSTA is currently the chairman of the Blockchain Intelligence Professional Association (BIPA), the first EU initiative to facilitate the development of standards and good practice in blockchain intelligence. He is also a strategy consultant on virtual assets within a finance & banking regulator in the EU, with over 20 years' experience of investigations, compliance and audit. He is an Accredited Counter Fraud Specialist, Accredited Counter Fraud Manager, Certified DLT & Blockchain Manager, Certified Virtual Assets investigator & compliance specialist, and holds ICA Diplomas in Anti Money Laundering and Financial Crime Prevention.