10 Traceability of crypto-asset transfers under the new EU AML/CFT regime: the crypto travel rule between challenges and open issues

Nadia Pocher

I. Introduction

In 2022, more than USD 31 billion flowed from illicit crypto-asset addresses to services such as crypto-asset exchanges.[1] The year after, the illicit crypto-asset flow amounted to about USD 22 billion, partially mirroring the overall drop in crypto-asset transaction volume following the 2022–23 Crypto Winter.[2] In this timeframe, the crash of Terra-Luna led to the bankruptcy of several leading actors in the decentralised finance space, as well as banks with significant crypto-asset exposures.[3] Following the collapse of the second largest crypto-asset exchange, FTX, in November 2022, the co-founder and former CEO Sam Bankman-Fried was found guilty of several counts of fraud and conspiracy.[4] Meanwhile, in February 2024, the US government fined the

1 Chainalysis, 'The Chainalysis 2024 Crypto Crime Report' (2024) 23 <https://go.chainalysis.com/crypto-crime-2024.html> accessed 10 November 2024.

2 ibid. Douglas W Arner and others, 'The Financialization of Crypto: Lessons from FTX and the Crypto Winter of 2022–2023' (2023) University of Hong Kong Faculty of Law Research Paper No. 2023/19 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4372516> accessed 10 November 2024.

3 A primary case is that of Silicon Valley Bank. Dirk A Zetzsche and others, 'Remaining Regulatory Challenges in Digital Finance and Crypto-assets after MICA' (Committee on Economic and Monetary Affairs (ECON), Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, May 2023) 31 <https://www.europarl.europa.eu/RegData/etudes/STUD/2023/740083/IPOL_STU(2023)740083_EN.pdf> accessed 10 November 2024.

4 Luc Cohen and Jody Godoy, 'Sam Bankman-Fried Convicted of Multi-billion Dollar FTX Fraud' (*Reuters,* New York, 3 November 2023) <https://www.reuters.com/legal/ftx-founder-sam-bankman-fried-thought-rules-did-not-apply-him-prosecutor-says-2023-11-02/> accessed 10 November 2024.

largest crypto-asset exchange, Binance, USD 4.3 billion for money laundering,[5] amidst other charges that included market manipulation.[6] The co-founder and former CEO Changpeng Zhao had to step down and pay a personal fine of USD 50 million.[7] As it becomes relatively common for crypto-asset exchanges to face charges for failure to comply with laws and regulations, this poses an existential concern for the framework to prevent the misuse of financial systems for purposes of money laundering and terrorist financing (AML/CFT).

The vulnerability of crypto-assets to financial turmoil is far from new. From the events of the Silk Road darknet marketplace and the Mt. Gox exchange in the 2010s, to the alleged involvement of Tornado Cash in the laundering of USD 1 billion in 2023,[8] the perception of crypto-assets as a means to achieve unaccountability in value transfers keeps generating concerns. Meanwhile, alongside advances in crypto-asset analytics, the techniques deployed to engage in illicit activities become increasingly sophisticated.[9] In 2023, USD 743.8 million were sent from illicit addresses primarily linked to ransomware attacks to cross-chain bridge protocols,[10] compared to only USD 312.2 million in 2022.[11] Further, not only has the crypto-asset space overall emerged as not as decentralised as advertised,[12] but this holds true also for illicit activities: in 2023, more than two-thirds of all illicit funds sent to off-ramping services (i.e., services that allow one to "cash out" crypto-assets) were sent to five services.[13]

5 Jonathan Stempel, 'Judge Approves Binance $4.3 Billion Guilty Plea as US Seeks to Modify Founder Zhao's Bond' (*Reuters,* New York, 23 February 2024) <https://www.reuters.com/technology/judge-approves-binance-43-billion-guilty-plea-us-seeks-modify-founder-zhaos-bond-2024-02-23/> accessed 10 November 2024.

6 U.S. Securities and Exchange Commission, 'SEC Files 13 Charges Against Binance Entities and Founder Changpeng Zhao' (SEC Press Release, Washington DC, 5 June 2023) <https://www.sec.gov/news/press-release/2023-101> accessed 10 November 2024.

7 Chris Prentice, David Lawder, and Jonathan Stempel, 'Binance's Zhao Pleads Guilty, Steps Down to Settle US Illicit Finance Probe' *Reuters* (New York, 22 November 2023) <https://www.reuters.com/markets/us/us-authorities-set-unveil-settlement-with-binance-source-2023-11-21/> accessed 10 November 2024.

8 Southern District of New York, 'Tornado Cash Founders Charged With Money Laundering and Sanctions Violations' (U.S. Attorney's Office Press Release, New York, 23 August 2023) <https://www.justice.gov/usao-sdny/pr/tornado-cash-founders-charged-money-laundering-and-sanctions-violations> accessed 10 November 2024.

9 Nadia Pocher and others, 'Detecting Anomalous Cryptocurrency Transactions: An AML/CFT Application of Machine Learning-Based Forensics' (2023) 33 Electronic Markets 37.

10 For more insights into cross-chain bridges: Sung-Shine Lee and others, 'SoK: Not Quite Water Under the Bridge: Review of Cross-Chain Bridge Hacks' (2023, IEEE International Conference on Blockchain and Cryptocurrency).

11 Chainalysis (n 1) 25, 32.

12 Tom Barbereau and others, 'Decentralised Finance's Timocratic Governance: The Distribution and Exercise of Tokenised Voting Rights' (2023) 73 Technology in Society.

13 Chainalysis (n 1) 26.

The international AML/CFT regime has long fought against the circulation of illicit money through transfers of funds, as it significantly threatens financial integrity and stability. Well before the advent of crypto-assets, strategies to "follow the money" have been deployed to constrain the activities of criminal groups by targeting their economic resources.[14] Various forensic techniques are deployed to monitor and investigate financial transactions, and constantly evolve to account for emerging technologies and decentralisation.[15] Despite the advancements in transaction analytics, however, one of the backbones of the efforts to ensure accountability in the financial space is that of securing the traceability of transactions.

This chapter explores the obligations laid out by the "(crypto) travel rule" both at an international and EU level, with specific reference to the new measures introduced by the EU AML Package. It does so by considering the broader expansion of the AML/CFT measures to the crypto-asset field, as well as pinpointing major challenges to their effective implementation.

II. Crypto-asset service providers and the AML/CFT framework

The measures to prevent and repress money laundering and terrorist financing comprise criminal sanctions as well as compliance duties qualified in several ways (e.g., civil, administrative) depending on the legal system. As a field where regulatory action often intertwines with the socio-economic context – for example, organised crime-related factors, tax crimes such as tax evasion, and fiscal policies – the fight against financial crime tends to be in the political limelight and exposed to territorial fragmentation. The gist of AML/CFT measures, however, tends towards global coherence in the form of compliance with the standards laid out by the Financial Action Task Force (FATF), an international organisation established in 1989. Although the FATF Standards, known as Recommendations, are instruments of soft law, participating jurisdictions are committed to transposing them into national law through individual regulatory and operational initiatives.[16] In this regard, the FATF cooperates closely with regional bodies and organisations such as the International Monetary Fund (IMF), the World Bank, and the United Nations (UN).[17]

14 William F Wechsler, 'Follow the Money' (2001) 80(4) Foreign Affairs 40.

15 Nick Furneaux, *Investigating Cryptocurrencies: Understanding, Extracting, and Analyzing Blockchain Evidence* (Wiley 2018); Pocher and others (n 9).

16 Iwona Karasek-Wojciechowicz, 'Reconciliation of Anti-Money Laundering Instruments and European Data Protection Requirements in Permissionless Blockchain Spaces' (2021) 7(1) Journal of Cybersecurity 2 <https://academic.oup.com/cybersecurity/article/doi/10.1093/cybsec/tyab004/6166133>.

17 FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations' (*FATF*, 2012) 8 <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html> accessed 10 November 2024.

The final goal of AML/CFT measures is to prevent criminals from enjoying the profit of illicit activities, thwarting their capacity to disguise the origin of funds and provide them with a legitimate appearance. For this reason, at the origins of the framework in the 1970s and 1980s, the focus was on proceeds of organised criminal activities with substantial returns – for example, trafficking in drugs and illegal firearms and corruption.[18] The crimes that generate proceeds whose laundering is considered by law as money laundering are known as "predicate offences", and they have broadened over time. According to FATF, money laundering must be interpreted to include the widest range of predicate offences.[19] In terms of money laundering activities – that is, what is done with the proceeds generated from the predicate offence – the EU AML Regulation refers to converting or transferring property derived from criminal activity, concealing or disguising qualities of said property (e.g., source, location, ownership), possessing or using said property, including any participation and attempt to facilitate these actions.[20]

A. The AML/CFT regime between FATF's standards and EU law

The FATF Recommendations require participating countries to establish authorities that regulate, monitor, supervise, and handle the licensing of various actors in different sectors, as well as impose disciplinary and financial sanctions.[21] The regimes established in different jurisdictions rely on a set of "regulated entities", also labelled "obliged entities", required to actively cooperate with the authorities, chiefly in terms of monitoring financial transactions and value exchanges.[22] Their selection is grounded on their (purported) oversight capacity, which is in practice often debated. The risk-based approach (RBA) sits at the core of the regime, and compliance and supervision measures are tuned to the principle of proportionality. To do so, regulated entities and authorities must consider risk factors identified by the FATF, such as the "red flag indicators", but also by the AML Regulation, national regulation, and supervisory authorities – that is, stricter if risk factors are higher and vice versa. The end goal is to draw the attention of competent authorities in case of suspicions of illicit

---

18 Liliya Gelemerova, 'On the Frontline against Money-Laundering: The Regulatory Minefield' (2009) 52(1) Crime, Law and Social Change 33, 34, 36.

19 FATF (n 17). FATF Recommendation 3.

20 The AML Regulation is Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing [2024] OJ L 2024/1624of 19.6.2024. Its Article 2(1) directly refers to the definition of money laundering as per Article 3(1–5) of Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law [2018] OJ L 284/22 of 12.11.2018.

21 FATF (n 17) 7. Recommendation 26; Carol R Goforth, 'Crypto Assets: A Fintech Forecast' (2021) 37 Banking & Finance Law Review 5, 10; Chris Brummer, *Soft Law and the Global Financial System: Rule Making in the 21st Century* (2nd edn, Cambridge University Press 2015) 88, 89.

22 For FATF, regulated entities encompass financial institutions and designated non-financial businesses and professions.

activities. At the receiving end, there are national Financial Intelligence Units (FIUs), who receive, assess, and share financial information (e.g., suspicious transaction reports, other data relevant for analysis) with other national authorities or other FIUs.

At the EU level, a key part of AML/CFT activities consists of incorporating FATF Standards into Union law, where EU law operates as a legalisation means whereby soft law is transformed into embedded rules.[23] From 1991 onwards, the EU has drafted legislation to harmonise Member States' responses in the AML/CFT sphere. The actions have so far taken the form of directives of minimum harmonisation, where considerable discretion is left to national transposition. The alternative of maximum harmonisation would be incompatible with the RBA.[24] Article 5 of the Treaty on European Union (TEU) requires EU actions to comply with subsidiarity and proportionality, and the inherent cross-border nature of AML/CFT problems makes it impossible to achieve results through individual Member State actions. It is in this context that, in 2021, the Commission put forward a set of proposals known as the "AML Package". The goal was not to transform the content of the framework, still anchored to the FATF's approaches and methods, but rather to ensure the implementation of the regime by overcoming national fragmentation originated by the transposition of directives, while narrowing the gap with the new Regulation (EU) 2023/1114 on Markets in Crypto-Assets, known as MiCA Regulation.[25]

The AML Package contained four legislative proposals that were adopted between 2023 and 2024. In the first place, the AML Regulation establishes an AML/CFT single rulebook. Although the regulation does not disrupt the regime in terms of content, as a regulation it is directly binding on Member States, individuals, and organisations in its entirety. The main changes include the expansion of regulated entities to crypto-asset service providers (CASPs), the clarification of risk indicators, the strengthening of measures to mitigate the misuse of bearer instruments, and the establishment of a limit to the use of cash for large transactions. Parallelly, the so-called Sixth AML Directive focusses on FIUs.[26]

---

23 Abraham Newman and David Bach, 'The European Union as Hardening Agent: Soft Law and the Diffusion of Global Financial Regulation' (2014) 21(3) Journal of European Public Policy 430, 430–432.

24 Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing' COM (2021) 420 final, 5. For EU requirements laid out by directives, with "minimum harmonisation" a directive sets minimum standards and Member States retain the right of setting higher ones, while with "maximum harmonisation" they cannot introduce stricter rules.

25 Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 [2023] OJ L 150/40 of 09.06.2023.

26 Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist

Further, the Regulation establishing the EU Anti-Money Laundering Authority (AMLA) introduces EU-level supervision of selected entities, assistance to financial supervisors, and coordination of information exchange.[27] As agreed in February 2024, AMLA will be located in Frankfurt, Germany.[28] The new Authority will adopt regulatory technical standards, guidelines, or recommendations for regulated entities, supervisors, or FIUs. Fourthly, Regulation (EU) 2023/1113 was adopted to recast Regulation (EU) 2015/847 – known as the Fund Transfer Regulation (FTR). The goal was to expand beyond wire transfer traceability obligations, according to which financial institutions and payment service providers (PSPs) exchange certain information. As outlined below, the new framework introduces the obligation to collect and share data on originators and beneficiaries of crypto-asset transfers.

B. The application to the crypto-asset space

Over the years, the AML/CFT regime was adjusted to the novel ways of transmitting value online. The FATF started to address crypto-asset risks in 2014–15, issuing background notions on virtual currencies,[29] and a first guidance.[30] These documents did not address crypto-assets comprehensively and focussed exclusively on the on- and off-ramps to the traditional financial system. In 2018, the FATF clarified the application of the Standards to virtual assets, and the amended Recommendation 15 included virtual asset service providers (VASPs) into the standards' scope. The development of new products, services, and providers led the FATF to specify in 2021 that the Standards apply "to both virtual-to-virtual and virtual-to-fiat transactions and interactions involving virtual assets".[31]

financing, amending Directive (EU) 2019/1937, and amending and repealing Directive (EU) 2015/849 [2024] OJ L, 2024/1640 of 19.6.2024.

27 Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010 [2024] OJ L, 2024/1620 of 19.6.2024.

28 European Commission, 'Commission Welcomes the Selection of Frankfurt as the Seat for the Authority for Anti-Money Laundering and Countering the Financing of Terrorism' (European Commission Press Release, Brussels, 22 February 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_972> accessed 10 November 2024.

29 FATF, 'Virtual Currencies – Key Definitions and Potential AML/CFT Risks' (FATF Report, June 2014) <https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> accessed 10 November 2024.

30 FATF, 'Guidance for a Risk-Based Approach: Virtual Currencies' (June 2015) <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-RBA-Virtual-Currencies.pdf.coredownload.inline.pdf> accessed 10 November 2024.

31 FATF, 'Virtual Assets and Virtual Asset Service Providers - Updated Guidance for a Risk-Based Approach' (October 2021) 7, 8 <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html> accessed 10 November 2024; Goforth (n 21) 10.

The most recent FATF definition of 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", excluding "digital representation of fiat currencies, securities, and other financial assets that are already covered elsewhere in the FATF Recommendations".[32] VASPs, in turn, comprise natural or legal persons that as a business conduct – for or on behalf of another natural or legal person – one or more activities among: exchange between virtual assets and fiat currencies, between one or more virtual assets, transfer of virtual assets from one address or account to another, safekeeping or administration of virtual assets or instruments enabling control over them, provision of financial services related to an offer and/or sale of virtual assets.[33] In 2019, the FATF adopted the Interpretative Note to Recommendation 15 to clarify the application of the RBA to virtual asset activities and issued the first related comprehensive Guidance.[34] This was revised in 2021, also concerning risks in peer-to-peer transactions and the "travel rule" implementation.[35] Meanwhile, after a surge in ransomware attacks,[36] the FATF published the "Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing", with a section on anonymity.[37] In 2024, the FATF issued an overview of the status of implementation of Recommendation 15, including its member jurisdictions but also those with significant VASP activities.[38] The report further accounts for the implementation of the crypto travel rule, at least in the form of draft legislation.[39]

Within the previous EU framework, Article 2(1)(g) and (h) of the AML Directive included fiat-to-crypto exchanges and custodian wallet providers.[40] Yet, the AML

32 FATF (n 31) 109; FATF (n 17).

33 FATF (n 31) 109.

34 FATF, 'Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers' (June 2019) <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html> accessed 10 November 2024; FATF (n 17); Goforth (n 21) 11; FATF (n 31) 4, 8.

35 FATF (n 31) 5, 6.

36 ibid 10.

37 FATF, 'Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing' (September 2020) <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf> accessed 10 November 2024.

38 FATF, 'Status of Implementation of Recommendation 15 by FATF Members and Jurisdictions with Materially Important VASP Activity' (March 2024) <https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/VACG-Table-Jurisdictions-2024.pdf> accessed 10 November 2024.

39 ibid 10.

40 The term "AML Directive" refers to the last consolidated version of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC [2015] OJ L 141/73 of 05.06.2015 (Fourth AML Directive), as amended by Directive (EU) 2018/843 of the European

Regulation broadens the scope of application of the regime from virtual currencies to crypto-assets and refers to the MiCA Regulation for the definitions. As per Article 3(1)(5) of the MiCA Regulation, a crypto-asset is "a digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology".[41] A crypto-asset service provider (CASP) provides services such as custody and administration, trading, exchange (for funds or other crypto-assets), execution (or reception and transmission) of orders, placing, advice, portfolio management, and transfer services.[42] The provision of advice is the only case that does not fall within the scope of the AML Regulation.

III. The obligation to ensure traceability of fund flows

The traceability of money flows is crucial to prevent, detect, and investigate money laundering and terrorist financing.[43] As per FATF Recommendation 16 on "wire transfers",[44] financial institutions must "include required and accurate originator information, and required beneficiary information, on wire transfers and related messages". They must also ensure that such information remains with the transfer throughout the payment chain. This is the so-called "travel rule", which is designed to detect any attempt to move illicit funds by making sure to trace the relevant transactions and collect the necessary information to hold the perpetrators accountable. In practice, a set of data must accompany the funds throughout the payment chain. This is achieved through a duty on some regulated entities to collect and share certain information on originators and beneficiaries of all wire transfers and to make it available to the authorities – for example, FIUs and law enforcement agencies.[45] Further,

Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU [2018] OJ L 156/43 of 19.06.2018 (Fifth AML Directive). The AML Directive was repealed by Directive (EU) 2024/1640 (n 26).

41 The definition of crypto-assets in the MiCA Regulation corresponds to the definition of virtual assets set out in the revised FATF Recommendations. Further, the list of crypto-asset services and crypto-asset service providers covered in the MiCA Regulation encompasses the virtual asset service providers identified as such by FATF.

42 Regulation (EU) 2023/1114 (n 26) Article 3(1)(15–16).

43 Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 [2023] OJ L 150/1 of 09.06.2023, Recital 16.

44 A "wire transfer" is any electronic transaction on the originator's behalf through a financial institution to make funds available to a beneficiary at a beneficiary financial institution. Glossary of FATF Recommendation 16.

45 The originator is the "account holder who allows the wire transfer from that account, or where there is no account, the natural or legal person that places the order with the ordering financial institution to perform the wire transfer". The beneficiary is the "natural or legal person or legal arrangement who is identified by the originator as the receiver of the requested wire transfer". Glossary of FATF Recommendation 16.

they must monitor the transfers to detect the absence of this required information and take appropriate measures, as well as take freezing actions and prohibit transactions with sanctioned persons or entities.[46]

The Interpretative Note to FATF Recommendation 16 lays out different rules imposed on ordering, intermediary, and beneficiary financial institutions and money or value transfer services (MVTSs).[47] The travel rule was implemented in the EU in 2015, when the adoption of the Fourth AML Directive was accompanied by that of Regulation (EU) 2015/847 on information accompanying transfers of funds (FTR) sent or received by a PSP or intermediary PSP established in the Union.[48] Within that regime, funds are defined as "banknotes and coins, scriptural money and electronic money",[49] and "transfer of funds" refers to transactions performed by electronic means, including credit transfers, direct debits, money remittances, and transfers via payment cards, e-money, and mobile phones.[50]

Recommendation 16 and its Interpretative Note are undergoing a revision process that includes a public consultation. FATF, 'Public Consultation on Recommendation 16 on Payment Transparency' (*FATF*, 26 February 2024) <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/R16-public-consultation-Feb24.html> accessed 10 November 2024.

46 FATF (n 17) FATF Recommendation 16.

47 MVTS are "financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs". This can involve intermediaries and any new payment methods – e.g., hawala, hundi, fei-chen. ibid 132.

48 Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 [2015] OJ L 141/1 of 05.06.2015, Article 2(1); Article 2(4) excludes PSP-to-PSP fund transfers from the regime.

49 By reference to Article 4(15) of Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC, and 2006/48/EC and repealing Directive 97/5/EC [2007] OJ L 319 of 05.12.2007 (PSD) replaced by Article 4(25) of Directive 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC, and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [2015] OJ L 337/35 of 23.12.2015 (PSD2). The definition of "funds" refers to Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit, and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC [2009] OJ L 267/7 of 10.10.2009 (EMD2), where e-money is "electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions as defined in point 5 of Article 4 of PSD, and which is accepted by a natural or legal person other than the electronic money issuer" (Article 2(2)).

50 Regulation (EU) 2015/847 (n 50) Article 3(9).

A. The crypto travel rule

The crypto travel rule expands the scope of obligations for information sharing to the crypto-asset space. In 2018, the revision of the Interpretative Note to FATF Recommendation 15 on "new technologies" addressed the application of FATF Recommendation 16 to virtual asset transfers. Countries were asked to introduce new rules for financial institutions and VASPs, whereby (i) originators obtain and hold required and accurate originator information and required beneficiary information on virtual asset transfers, submit it (directly or indirectly – that is, not necessarily attached to the transfer) to the beneficiary (if any) immediately and securely, and on request make it available to the competent authorities; (ii) beneficiaries obtain and hold required originator information and required and accurate beneficiary information on transfers of virtual assets, and on request make it available to the competent authorities. The scope of application of other rules laid out by FATF Recommendation 16 was extended accordingly – for example, data monitoring, freezing actions, prohibiting transactions with designated persons.[51]

Consistently, the EU AML Package included a proposal to recast the FTR and introduce the crypto travel rule. The new regime was adopted as Regulation (EU) 2023/1113 and establishes the obligation to collect and make accessible specific data on originators and beneficiaries of crypto-asset transfers to the authorities.[52] In doing so, the reform explicitly targets crypto-asset anonymity, as "the global reach, the speed at which transactions can be carried out and the possible anonymity offered by their transfer, particularly expose crypto assets to the risk of criminal misuse against jurisdictions".[53] The regime applies to those transfers of crypto-assets, including by means of crypto-ATMs,[54] where the CASP of the originator or beneficiary, or the intermediary CASP,[55] has its registered office in the EU.[56]

A transfer of crypto-assets is defined as any transaction that aims to move crypto-assets from one distributed ledger address, crypto-asset account, or other storage device to another one.[57] It is carried out by at least one CASP on behalf of an originator or a beneficiary, regardless of whether the originator and beneficiary are the

51 FATF (n 17) Revised Interpretative Note to FATF Recommendation 15.

52 Article 3(14) and (15) of Regulation (EU) 2023/1113 (n 45) refer to MiCA's definition of crypto-assets and CASPs, respectively. In the United Kingdom, the crypto travel rule was enacted in the new Part 7A of The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (SI 2017/692). Part 7A was inserted by SI 2022/860.

53 Regulation (EU) 2023/1113 (n 45).

54 A crypto-ATM is a physical or online electronic terminal enabling CASPs to transfer crypto-assets; ibid, Article 3(17).

55 Intermediary CASPs are those CASPs (other than that of the originator or beneficiary) that receive and transmit crypto-asset transfers on behalf of the CASP of the originator or of the beneficiary, or of another intermediary CASP. ibid, Article 3(16).

56 ibid, Article 2(1).

57 ibid, Article 3(10).

same person and whether the CASPs of the originator and the beneficiary are the same one.[58] All regulated entities that offer crypto-asset services within the meaning defined above, such as banks, fall within the scope of application of the crypto travel rule.[59] The regime does not apply when both the originator and beneficiary are CASPs acting on their own behalf. Likewise, as further discussed below, it does not apply to person-to-person transfers without the involvement of a CASP.[60] In line with the RBA, the original version of the recast proposal distinguished between crypto-asset transfers of more than EUR 1,000 – that is, individual transfers exceeding the threshold or multiple transfers seemingly linked – and those below this threshold. The latter were subject to a more lenient regime. This approach was rejected during the legislative process, and crypto-asset transfers are now subject to the same requirements regardless of their amount and their domestic or cross-border features. This is not only due to their borderless nature, but also to the fact that they facilitate the structuring of large transactions into smaller transfers, in a context where calculating linked transactions is disrupted by high volatility.[61]

Hence, no matter the transferred value, the CASP of the originator is required to: (i) obtain and hold for five years accurate – that is, verified for accuracy – information on the *payer*: name, distributed ledger address and/or crypto-asset account number, address, official ID number, customer ID number or date and place of birth, current Legal Entity Identifier (LEI) or equivalent (if applicable);[62] (ii) obtain and hold for five years certain accurate information on the *beneficiary*: name and distributed ledger address and/or crypto-asset account number, current LEI or equivalent (if applicable);[63] (iii) securely submit *all of the above* to the beneficiary entity in advance of, simultaneously, or concurrently with the transfer.[64] The CASP of the beneficiary is required to: (i) monitor that the required data is included in the transfer or follows it; (ii) before making the assets available to the payee, verify the accuracy of the data using reliable and independent sources.[65] The intermediary CASP is required to ensure all data is relayed with the transfer and to comply with data retention obligations.[66]

58 ibid, Article 3(10).

59 Regulation (EU) 2023/1114 (n 25), Articles 59 and 60.

60 Regulation (EU) 2023/1113 (n 45), Article 2(4).

61 ibid, Recitals 27 and 30.

62 ibid, Article 14(1). Article 14(6–7) provides criteria for accuracy verification. Data retention duties are laid out by Article 26. The LEI is "a unique alphanumeric reference code based on ISO 17442 standard assigned to a legal entity" (Article 3(23)).

63 ibid, Article 14(2).

64 As per ibid. Article 14(4), the data as per Article 14(1–2) does not need to be attached directly to or included in the transfer. Further, as per Article 15(1), in case of a batch file transfer from one originator, Article 14(1) shall not apply to the individual transfers, provided the batch file contains the information as per Article 14(1–3), verified as per Article 14(5–6), and the individual transfers contain the originator distributed ledger address, crypto-asset account number, or individual identifier.

65 ibid, Article 16(1) and (3).

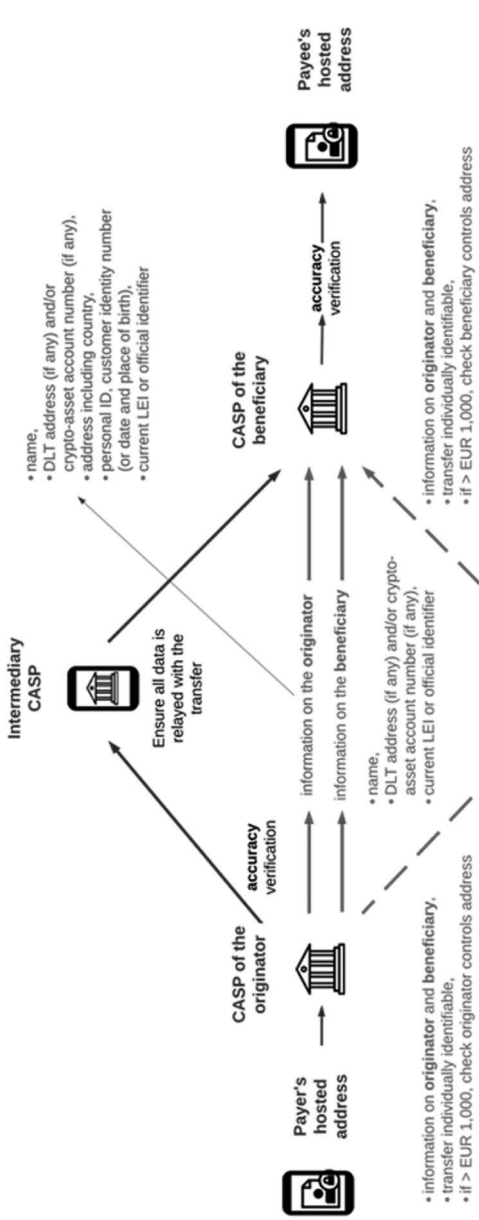
66 ibid, Article 19.

Upon request, all the information must be shared with the authorities. The dynamics of these exchanges are depicted in Figure 10.1.

For some transfers, a "distributed ledger address" – defined as "an alphanumeric code that identifies an address on a network using distributed ledger technology or similar technology where crypto-assets can be sent or received" – and/or a "crypto-asset account number" – that is, the number of an account held by a CASP "in the name of one or more natural or legal persons which can be used for the execution of transfers of crypto-assets" – may not exist.[67] Accordingly, in terms of data to collect, reference to a "distributed ledger address" is limited to cases in which the transfer is "registered on a network using distributed ledger technology or similar technology", and reference to an "account number" is limited to cases in which "such an account exists and is used to process the transaction".[68] When this is not the case, the originating CASP must ensure the transfer is accompanied by a "unique transaction identifier" that allows traceability of the transfer back to the originator and the beneficiary.[69]

It is prohibited for originating CASPs to execute any transfer before they can ensure full compliance with the above, and beneficiary CASPs must establish procedures to apply when the required data is lacking – that is, to decide whether to execute, reject, or suspend the transfer, and to determine follow-up actions.[70] Notably, if the beneficiary or intermediary CASP becomes aware of missing or incomplete information, they must either reject the transfer or ask for the information before making the crypto-assets available to the beneficiary or before transmitting the transfer.[71] If a CASP repeatedly fails to provide the required data, the beneficiary or intermediary CASP must (a) take actions such as issuing warnings or setting deadlines before proceeding to reject the transfer, or restricting or terminating the business relationship with the CASP; (b) reject directly any future transfers from the CASP or restrict and terminate the business relationship with it;[72] (c) consider the missing/incomplete data when deciding on the suspiciousness of the transfer or related transactions to report them accordingly.[73] Intermediary CASPs that become aware of missing/incomplete information can decide whether to reject the transfer and return the transferred crypto-assets or to ask for the required data.[74]

67 ibid, Article 3(18) and (19).
68 ibid, Article 14(1)(b).
69 ibid, Articles 14(3) and 3(12); The "unique transaction identifier" is defined as a combination of letters, numbers, or symbols determined by a CASP, which permits the traceability of the transfer of crypto-assets back to the originator and the beneficiary.
70 ibid, Article 17(1).
71 ibid, Articles 17(1) and 21(1).
72 ibid, Articles 17(2) and 21.
73 ibid, Articles 18 and 22(2); suspicious transaction reports are to be submitted to the authorities as per the AML Regulation.
74 ibid, Article 21.



Source: Elaboration of the author.

Figure 10.1 Information exchange as per the crypto travel rule under Regulation (EU) 1113/2023

B. Anonymity-related risks and self-hosted addresses

Some crypto-asset transfers present high-risk factors for money laundering, terrorist financing, and other criminal activities, especially when they are related to "products, transactions, or technologies designed to enhance anonymity, including privacy wallets, mixers, or tumblers".[75] In compliance with the RBA, this must be taken into consideration by regulated entities. Accordingly, the European Banking Authority (EBA) is expected to clarify the risk factors to be considered by CASPs to ensure the traceability of these transfers, such as in the case of transactions with non-Union counterparties that are not regulated, registered, or licenced anywhere, or with self-hosted addresses. In particular, the EBA is expected to issue guidelines specifying which enhanced due diligence measures should be applied to mitigate such risks – for example, the adoption of analytics tools to detect the origin or destination of crypto-assets.[76] Another example of a high-risk use case is that of transfers through "crypto-ATMs", as they allow users to perform transfers by depositing cash, often without customer identification and verification. Due to the possibility of using cash of unknown origin, they are deemed an ideal vehicle for illicit activities.[77]

Because the AML/CFT framework is fundamentally intermediary-based, it is not surprising that the recast of the FTR does not apply to "person-to-person transfers",[78] defined as transfers of crypto-assets without the use or involvement of any CASP.[79] This is also depicted at the bottom of Figure 10.1. One of the key points introduced by Regulation (EU) 2023/1113, however, explicitly covers the regime applicable to transfers involving self-hosted wallets, using the term "self-hosted addresses", defined as distributed ledger addresses not linked to a CASP nor to a similar entity established outside the EU.[80] Self-hosted wallets are also known as unhosted, private, non-custodial, or self-custody wallets. This means users are the sole holders of their private keys, and thus have full control of their crypto-assets. The alternative is keeping them in a third-party wallet offered by a provider of custody services such as a crypto-asset exchange.[81] Indeed, the crypto travel rule applies to crypto-asset transfers to or from a self-hosted address, if a CASP is involved. Acknowledging the complexity of this regulatory endeavour, the recast provided for further evaluation to be performed by the Commission.[82]

---

75 ibid, Recital 69.

76 ibid, Recital 17.

77 ibid, Recital 25.

78 ibid, Article 2(4).

79 ibid, Article 3(13).

80 ibid, Article 3(20).

81 Nadia Pocher, 'Self-Hosted Wallets: The Elephant in the Crypto Room?' *(KU Leuven CiTiP Blog*, 11 March 2021) <https://www.law.kuleuven.be/citip/blog/self-hosted-wallets/> accessed 10 November 2024.

82 Regulation (EU) 2023/1113 (n 45), Recital 38. As per Recital 58, considering the high risks associated with self-hosted addresses and corresponding complexities (e.g., verification of ownership data), by 1 July 2026, the Commission will assess the need for additional risk mitigation measures, including possible restrictions. The Commission

Meanwhile, Regulation (EU) 2023/1113 already provides important specifications concerning self-hosted addresses in the form of specific duties placed on originating and beneficiary CASPs. As per Articles 14(5) and 16(2), in the case of transfers of crypto-assets made to or from a self-hosted address, the CASP of the originator and of the beneficiary, respectively, must obtain and hold the information mentioned above and ensure the crypto-asset transfer can be individually identified. In addition, in the case of transfer of more than EUR 1,000 to or from a self-hosted address, the CASP of the originator and of the beneficiary must take adequate measures to verify that the address is owned or controlled by the originator or beneficiary, respectively. As clarified in the recitals, the CASP usually collects this information from its client, considering the lack of counterparties. In this respect, the verification of the accuracy of the information provided by the clients can be challenging. The industry has been relying on several general methods to collect proof of ownership of self-hosted addresses, including visual proof (the user sends the CASP a screenshot of the wallet displaying the withdrawal address), the Satoshi test (the user sends a trivial amount to the CASP, thereby proving control of the address), and manual signing (the user must sign a message using the key associated with the specific address, thereby proving control).[83] Further, proprietary solutions have emerged for holders of self-hosted addresses to reliably provide their status within transaction monitoring and/or know your customer (KYC) applications already in use by the service provider – for example, the Address Ownership Proof Protocol (AOPP).[84]

Besides the risk mitigation and verification measures, when the entity becomes aware that the provided information is inaccurate or encounters suspicious patterns, it must perform enhanced due diligence and, if needed, submit a suspicious transaction report to the authorities.[85] In this context, one should not forget that the use of self-hosted wallets to move crypto-asset funds across borders is listed among the FATF's red flags concerning anonymity,[86] and thereby frequently requires close scrutiny.

IV. Techno-legal challenges and open issues

Even if the scope of AML/CFT measures has expanded over time to include (a part of) the crypto-asset space, the underlying approach remains largely intermediary-based and relies on the cooperation of regulated entities. There was no major alteration of the fundamentals of the regime to tailor it to crypto-asset specificities. On the one

will assess the effectiveness and proportionality of the mechanisms to verify the accuracy of the ownership information.

83 21 Analytics, 'Self-Hosted Wallet Verification Methods: An Overview' (*21 Analytics,* 30 March 2023) <https://www.21analytics.ch/blog/unhosted-wallet-verification-methods-an-overview/> accessed 10 November 2024.

84 21 Analytics, 'AOPP Explained' (*21 Analytics*) <https://www.21analytics.ch/what-is-aopp/> accessed 10 November 2024.

85 Regulation (EU) 2023/1113 (n 45), Recitals 39 and 45.

86 FATF (n 37) 10.

hand, risk-based procedures and policies were adapted to the crypto-asset space, and most jurisdictions made considerable progress in responding to emerging risks. On the other hand, these efforts still appear insufficient to address comprehensively the problems associated with the crypto-asset sphere without thrusting significant burdens on the industry. Compliance with the crypto travel rule is one of the most topical examples.[87] The controversy comprises technical issues interwoven with policy decisions and business incentives, mirroring the tension between the increasing sophistication of the crypto-asset space (including related misuses for criminal purposes) and the needs of an AML/CFT regime that is inherently intermediary-based and explicitly not applicable to person-to-person transfers that are not linked to any activity of a service provider.

Increasingly, crypto-asset regulation aligns with the principle of "same activities, same risks, same rules".[88] Accordingly, activities involving crypto-assets are expected to receive regulatory treatment that resembles in its rationale the one targeting traditional financial assets. With regard to risks of anonymity, for instance, the regulatory approach resembles the one applicable to physical cash and bearer instruments, currently subject to a series of monitoring and restrictive rules. A primary example is the introduction of an EU-wide limitation of EUR 10,000 for large cash payments in exchange for goods or services, which applies to transactions carried out in a single operation and to several operations that are seemingly linked and does not apply to payments between natural persons not acting in a professional capacity.[89] However, the specifics of the crypto-asset space bring about their share of challenges when subject to functionally similar compliance requirements – for example, difficulty in identifying linked transactions.[90] This emphasises the importance of implementation measures such as the EBA's "Travel Rule Guidelines", currently subject to a consultation procedure.[91] The role of the EBA in this field will be increasingly shared with, and later transferred to, the AMLA.

At the time of writing, at least four problematic angles have emerged on a general level: the impact of the rule on self-hosted to hosted wallet transactions and the legitimacy of restrictions; the challenge of linking crypto-asset activities to the respective actors, at least in terms of attribution to real-world identities to be identified as originators

87 Goforth (n 21) 11.

88 Regulation (EU) 2023/1114 (n 25), Recital 9. The approach resembles that of the United States Securities and Exchange Commission in applying functional tests to define crypto-asset exchanges and apply securities law (e.g., Howey test). FATF (n 38).

89 Regulation (EU) 2024/1624 (n 20), Article 80(1) and (4).

90 ibid, Recital 160.

91 EBA, 'Consultation Paper on the Draught Guidelines on Preventing the Abuse of Funds and Certain Crypto-Assets Transfers for Money Laundering and Terrorist Financing Purposes under Regulation (EU) 2023/1113 ("The Travel Rule Guidelines")' (*EBA*, 2023) <https://www.eba.europa.eu/publications-and-media/press-releases/eba-consults-guidelines-preventing-abuse-funds-and-certain> accessed 10 November 2024.

and beneficiaries; the absence of global standards and technical solutions to underpin affordable compliance; and compliance with data protection requirements.

A. The challenge of attribution

The first two issues can be interpreted as a challenge of attribution of crypto-asset activities, under the perspectives of who is to be (and can be) regulated under the AML/CFT scheme – for example, entities that qualify as CASPs – but also who the real-world identities involved in the transaction as payer/originator and payee/beneficiary are. In other words, both viewpoints relate to accountability. The third problem is denounced by the industry, and it is an underlying issue that assumes a regulated entity is identified but lacks a Regulatory Technology (RegTech) solution to comply with the requirements.[92]

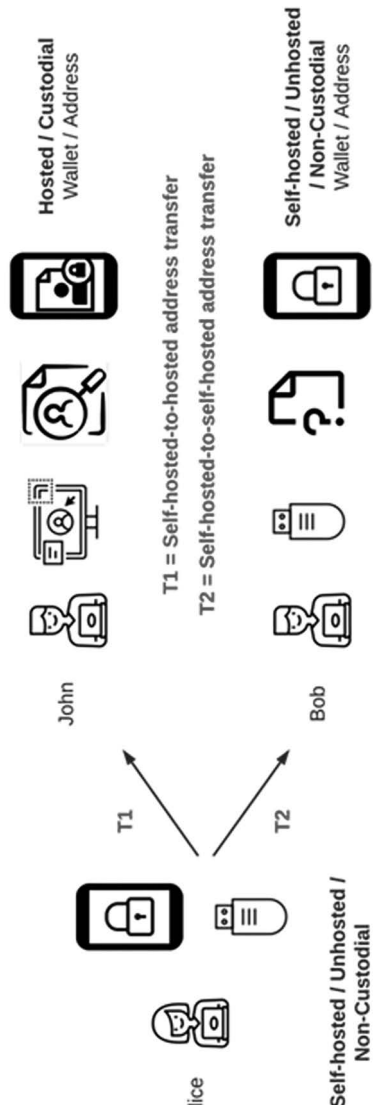
As the AML/CFT regime is traditionally based on the role of intermediaries in the detection of suspicious transactions, also the revision of the FTR pivots on CASPs. In the crypto-asset sphere, however, this approach fails to comprehensively account for its technical and structural peculiarities.[93] Focussing on self-hosted wallet/address activities, the two noteworthy scenarios, depicted in Figure 10.2, generate a two-fold issue of regulatory compliance. On the one hand, in the case of self-hosted to self-hosted wallet transactions, the fact that there is no regulated entity involved eludes the crypto travel rule and cash-related restrictions. While this encouraged regulators to consider restrictions, in terms of bans or often threshold limits, the issue generated a heated debate. Questions of legitimacy arose, and advocacy groups argue that it could give way to total surveillance – at odds with fundamental liberties such as privacy and autonomy, and with financial inclusion. It could also possibly generate a displacement of a considerable portion of activities towards unsupervised areas.[94] On the other hand, in the case of self-hosted to hosted wallet transfers, when regulated entities receive a transfer, they are required to obtain originator data but have no (regulated) counterparty entity to interact with, and are required to put a series of risk mitigation measures in place. Hence, self-hosted wallet holders could eventually be unable to transact with regulated PSPs if they are unable or unwilling to provide the necessary information. This would also be the case if the PSP adopts a de-risking approach and refuses to accept any transaction to/from self-hosted wallets in light of their real or perceived risk.

---

92 Doron Goldbarsht and Louis De Koker, 'From Paper Money to Digital Assets: Financial Technology and the Risks of Criminal Abuse' in Doron Goldbarsht and Louis De Koker (eds), *Financial Technology and the Law: Combating Financial Crime* (Springer International Publishing 2022) 309.

93 Valentina Covolo, 'The EU Response to Criminal Misuse of Cryptocurrencies: The Young, Already Outdated 5th Anti-Money Laundering Directive' (2020) 28 European Journal of Crime, Criminal Law and Criminal Justice 217, 247.

94 Miller Whitehouse-Levine and Lindsey Kelleher, 'Self-Hosted Wallets and the Future of Free Societies. A Guide for Policymakers' (*Blockchain Association*, November 2020) <https://theblockchainassociation.org/wp-content/uploads/2020/11/Self-Hosted-Wallets-and-the-Future-of-Free-Societies.pdf> accessed 10 November 2024.



Source: Elaboration of the author.

Figure 10.2 Depiction of self-hosted-to-hosted and self-hosted-to-self-hosted address transfers

Meanwhile, decentralised finance shows that even if the development of innovative services is influenced by regulation, part of the crypto-asset space is still leveraging technology to stay outside the border of compliance. These new schemes generate a challenge of attributing activities to a regulatable entity. The crypto travel rule is a prime example of how AML/CFT regulation is still dependent on the model of centralised exchanges (CEXs) and has not captured decentralised exchanges (DEXs) yet.[95] In this context, doubts have arisen about the nature of peer-to-peer trading platforms and DEXs, as – strictly speaking – these entities do not provide a service of exchange or conversion. Indeed, peer-to-peer exchanges provide users with a marketplace, handled by software, that aids in the connection between prospective buyers and sellers.[96] The scope of the issue narrows when considering the understanding of CASP provided by the MiCA Regulation. Indeed, this includes as a "crypto-asset service" also the operation of a trading platform defined as a multilateral system bringing together or facilitating "the bringing together of multiple third-party purchasing and selling interests in crypto-assets, in the system and in accordance with its rules, in a way that results in a contract, either by exchanging crypto-assets for funds or by the exchange of crypto-assets for other crypto-assets",[97] the execution of orders on behalf of third parties, placing activities, and order reception and transmission on behalf of third parties. But even when a peer-to-peer platform falls within the scope of a given AML/CFT framework, it is often problematic to identify the entity.[98] It is worth mentioning that not only is the share of crypto-asset activity performed through DEXs not trivial, but the CEX-centric nature of compliance can generate a substantial shift of liquidity to DEXs.[99] While the definition of the MiCA Regulation can mitigate the formal exclusion from the regime, it cannot solve the technical conundrum that makes it hard to thrust cooperation duties on them. This is highly problematic in consideration of the overall increase in decentralised finance (DeFi) laundering-related misuse starting from 2021,[100] while data reveal the preferred choice of malware operators to receive

95 Syren Johnstone, *Rethinking the Regulation of Cryptoassets: Cryptographic Consensus Technology and the New Prospect* (Edward Elgar Publishing 2021) 125.

96 Covolo (n 95) 235–236.

97 Regulation (EU) 2023/1114 (n 25), Article 3(1)(16) and (18).

98 Jai Massari and Christian Catalini, 'DeFi, Disintermediation, and the Regulatory Path Ahead' (*The Regulatory Review,* 10 May 2021) <https://www.theregreview.org/2021/05/10/massari-catalini-defi-disintermediation-regulatory-path-ahead/> accessed 10 November 2024.

99 Johnstone (n 97) 125; Massari and Catalini (n 100).

100 The Spartan Protocol hack is a prime example of the use of DeFi for laundering. After over 300 million USD worth of crypto-assets was stolen, the hackers converted the funds into anyETH and anyBTC (Ethereum and Bitcoin composites built on separate blockchains to the originals), then swapped some anyBTC for Bitcoin. Two chain-hopping protocols were used to convert funds into Ethereum and renBTC, then sent to a DEX and swapped for new Ethereum and wrapped Ethereum. The use of these platforms makes investigations significantly more complex. The funds were lastly sent to Tornado Cash; Chainalysis, 'The 2022 Crypto Crime Report' (2022) 7, 12 <https://go.chainalysis.com/2022-Crypto-Crime-Report.html> accessed 09 April 2024.

payments on self-hosted addresses, with the second choice being to receive them to addresses hosted by high-risk exchanges with low or non-existent compliance.[101]

B. The challenge of interoperability

While it is not easy to mitigate the risk of abuses without displacing illicit activities to peer-to-peer transfers, one wonders whether restricting self-hosted wallets unduly affects the freedom of economic activity, and/or whether the degree of enforceability of such limitations should bear any weight in the relevant policy-making.[102] Indeed, under the current regime, it seems impossible to enforce restrictions outside the scope of regulatable entities,[103] while CASPs denounce the lack of affordable compliance tools, and experts outline that the application of compliance requirements is overburdening the industry. For the purposes of technology neutrality, Regulation (EU) 2023/1113 does not require CASPs to make use of a specific technology to exchange the information. The EU co-legislators explicitly welcome as critical "standard-setting initiatives involving or led by the crypto-asset industry" to design interoperable solutions based on international or EU standards.[104]

Ever since the crypto-asset space started familiarising with the crypto travel rule, the industry has indeed commenced an exploration of various compliance technology solutions and RegTech tools. Relevant protocols are typically built to enable the secure exchange of originator and beneficiary information, and most of the solutions are commercial – for example, TRISA, VerifyVASP.[105] One open-source protocol emerged with the Travel Rule Protocol (TRP), developed in mid-2020 by an industry working group and merged with the OpenVASP association in late 2021. TRP is fully decentralised and free of charge.[106] However, overall, crypto travel rule compliance solutions have shown limited use. Unlike what happens for fiat money with the Society for Worldwide Interbank Financial Telecommunications (SWIFT), which serves as a dominant secure messaging network for financial institutions to exchange information about financial transactions and has become the industry syntax standard,[107]

---

101 ibid, 61, 74.

102 Pocher (n 83).

103 Nadia Pocher, 'Crypto-Wallets and the New EU AML Package: Where Are the Battle Lines Drawn?' (*KU Leuven CiTiP Blog*, 28 May 2023) <https://lirias.kuleuven.be/4070348?limo=0> accessed 10 November 2024.

104 Regulation (EU) 2023/1113 (n 45) Recital 50.

105 Magdalena Boškić, 'How RegTech Tools Enable Regulatory Compliance for Cryptoassets: A Case Study for Cryptoasset Transaction Monitoring' (2023) 8(2) Journal of Digital Banking 176, 184; For a brief overview of travel rule solutions: Chaehyeon Lee and others, 'Design of Blockchain-Based Travel Rule Compliance System' (*IEEE*, 2022) <https://arxiv.org/abs/2204.13508> accessed 10 November 2024.

106 Boškić (n 107) 184. OpenVASP Association, 'What Is the Travel Rule Protocol (TRP)?' (*OpenVASP*, 1 May 2022) <https://www.openvasp.org/blog/what-is-the-travel-rule-protocol-trp> accessed 10 November 2024.

107 Susan V Scott and Markos Zachariadis, *The Society for Worldwide Interbank Financial Telecommunication (SWIFT)* (Routledge 2013).

in the crypto-asset space there is no equivalent global standard for the exchange of information.[108] The different protocols under development are also not interoperable, except for the consensus reached regarding a single data messaging format – the InterVASP Messaging Standard (IVMS 101) – which established a common language for communication. The lack of unified compliance technology solutions is challenging according to the FATF.[109]

Further, the problem of (affordable) compliance is worsened by the divergent approaches across jurisdictions, both in the implementation of the crypto travel rule and in the specific requirements (e.g., de minimis threshold). The different pace of implementation of the crypto travel rule across jurisdictions causes both an unlevel playing field and difficulties for the entities that must comply earlier than their counterparts, known as the "sunrise issue".[110]

C. The challenge of data protection

While the regime to be applied to transfers involving self-hosted addresses generates one of the key controversies surrounding the FTR recast, another topical aspect concerns the interplay between the travel rule and data protection. Indeed, issues arise in terms of data protection and compliance with the General Data Protection Regulation (EU) 2016/679 (GDPR). The processing of personal data under the new FTR is subject to the GDPR and can be performed exclusively for AML/CFT prevention purposes, with specific prohibition of any commercial exploitation.[111] AML/CFT purposes are deemed an important public interest ground, but the transfer of personal data to a third country must be performed in accordance with Chapter V of the GDPR, which lays out rules for the transfers of personal data to third countries or international organisations. PSPs and CASPs that operate in multiple jurisdictions, with branches or subsidiaries outside the EU, should not be prevented from sharing data about suspicious transactions within their organisation, but they must apply adequate safeguards and have appropriate technical and organisational measures in place to protect personal data against accidental loss, alteration, or unauthorised disclosure or access.[112]

However, crypto-assets are inherently cross-border, and they can be transferred to a provider that is registered in a jurisdiction with different rules on data protection and its enforcement, or even to one that is not registered in a jurisdiction. In the first case, the CASP of the originator should assess the ability of the CASP of the beneficiary to receive and retain the data in compliance with the GDPR. Yet, the European Data

108 Boškić (n 107) 185.

109 ibid; FATF, 'Second 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers' (July 2021) <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Second-12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf> accessed 10 November 2024.

110 Boškić (n 107) 179.

111 Regulation (EU) 2023/1113 (n 45) Article 25(1–2).

112 ibid, Recital 19.

Protection Board (EDPB), in consultation with the EBA, will issue guidelines on the practical implementation of data protection requirements for transfers of personal data to third countries in the context of transfers of crypto-assets. For those situations in which personal data cannot be sent because the requirements of the GDPR cannot be fulfilled, the EBA is expected to provide guidelines on the procedures to follow to assess whether to execute, reject, or suspend the transfer.[113]

For a travel rule system to comply with the GDPR, overarching requirements are those laid out by Article 25 of the GDPR regarding "privacy by design" and "privacy by default". They relate, respectively, to ensuring data protection through technology design and to processing personal data only when necessary for a specific purpose and in a transparent fashion vis-à-vis the individuals involved.[114] The debate underlines the need to design the interplay between the AML/CFT sphere and privacy and data protection safeguards in the regulatory framework. Likewise, the specific crypto travel rule context requires appropriate design of RegTech/compliance technology solutions, able to embed the presence of various regulatory requirements such as AML/CFT and data protection.[115]

V. Conclusions

In recent years, the obligation to ensure the traceability of crypto-asset transfers has emerged as a key measure to prevent, detect, and investigate money laundering and terrorist financing. At a global level, this has been at the core of the FATF Recommendations since 2018. In the EU, the crypto travel rule was introduced by Regulation (EU) 2023/1113. The efforts to fight the lack of accountability in the crypto-asset space respond directly to the exposure and permeability of the traditional financial system to crypto-asset-related risks, showcased by the Crypto Winter 2022–23. At the same time, the application of traceability requirements poses major challenges for AML/CFT regulated entities involved in crypto-asset transfers. This occurrence is a primary example of the difficulty of applying an intermediary-based framework to the crypto-asset sphere, where the regime designed for self-hosted wallets arguably falls short in accounting for the difficulty of collecting the necessary information and, perhaps most importantly, verifying it according to the required accuracy and reliability.

---

113 ibid, Recital 34.

114 Ross P Buckley, Douglas W Arner, and Dirk A Zetzsche, *FinTech: Finance, Technology and Regulation* (Cambridge University Press 2023) 154.

115 Nadia Pocher and Andreas Veneris, 'Privacy and Transparency in CBDCs: A Regulation-by-Design AML/CFT Scheme' (2022) 19(2) IEEE Transactions on Network and Service Management 1776; Panagiotis Michalopoulos and others, 'Compliance Design Options for Offline CBDCs: Balancing Privacy and AML/CFT' (2024) IEEE International Conference on Blockchain and Cryptocurrency (ICBC).

The crypto travel rule debate also testifies to the importance of carefully assessing how to implement the "same activities, same risk, same rules" principle when the activities are performed in a context that features a range of stakeholders who differ starkly from the traditional financial system. At the EU level, much remains to be seen after the adoption of the implementing measures, guidelines, and risk assessments required from various actors by the new Regulation (EU) 2023/1113. These will foreseeably continue to rely on industry standardisation initiatives, usually privately led. One can speculate that a key point will be the start of the activities of AMLA, the new EU-level supervisor. Hopefully, the new institutional set-up will enable a stronger EU effort in leading the development of effective crypto travel rule solutions based on sound techno-legal collaboration. This will be crucial to efficiently handle the need to concurrently ensure data protection safeguards as required by the GDPR.

Acknowledgement

Parts of this chapter build upon research originally conducted for the author's doctoral thesis: Nadia Pocher, 'Distributed Ledger Technologies Between Anonymity and Transparency: AML/CFT Regulation of Cryptocurrency Ecosystems in the EU' (PhD Thesis, Katholieke Universiteit Leuven, Alma Mater Studiorum Università di Bologna 2023). The additional research for this book chapter was funded by the Luxembourg National Research Fund (FNR), grant reference NCER22/IS/16570468/NCER-FT [CryptoReg], as well as by FNR-PayPal, PEARL grant reference 13342933/Gilbert Fridgen. For open access purposes, and in fulfilment of the obligations arising from the grant agreement, the author applied a Creative Commons Attribution 4.0 International (CC BY 4.0) licence to any Author Accepted Manuscript version arising from this submission.