protiviti®

Global Business Consulting

Crypto and the Travel Rule: What's Going On?

by Francesco Monini and Mattia Santi

June 2024

Face the Future with Confidence®

Table of Contents

Introduction

Cryptocurrency assets, along with their associated products and services, have undergone extensive growth in recent years. The rapid adoption of digital currencies raises questions about the future of the financial markets and the connection between crypto asset players and traditional financial services companies.

There are many, and varied, risks associated with cryptocurrency assets, including operational risk, financial integrity, risks associated with asset reserve management, and the potential impact of national currencies having to compete with, and potentially being replaced by, crypto.

The adoption of crypto assets also poses significant challenges for global regulators, who must navigate the complexities of a constantly evolving industry, both technologically and in terms of regulation.

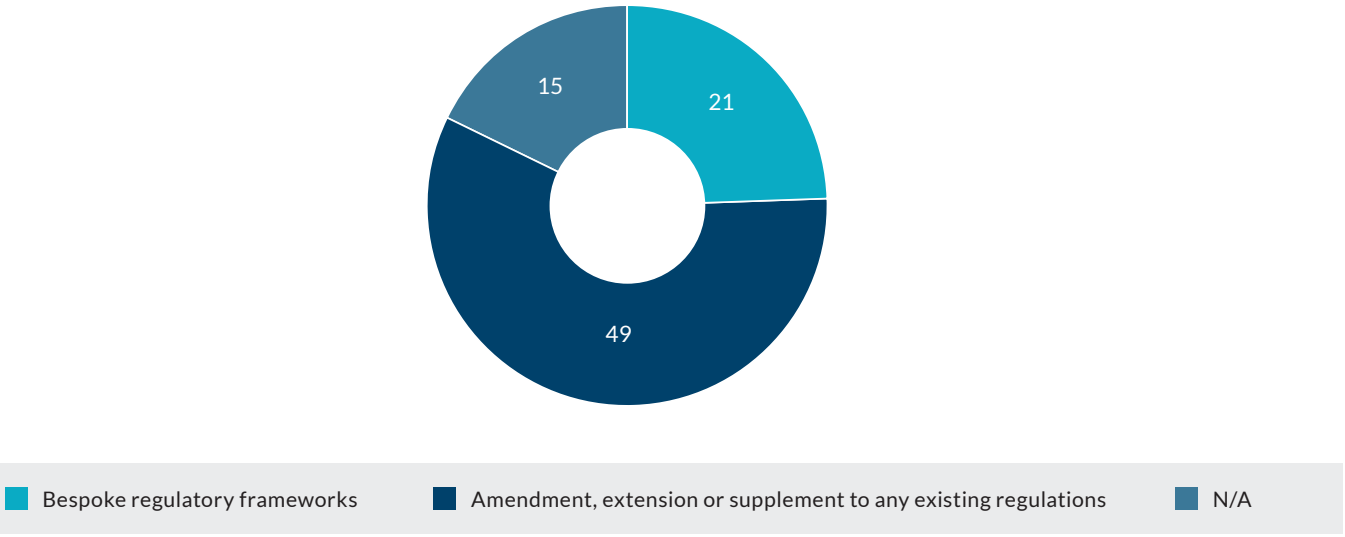
Identifying and managing these risks is a highly intricate and time-sensitive endeavor.

Key Regulatory Challenges

The substantial growth of crypto assets in recent years has created notable regulatory hurdles. In October 2022, the Financial Stability Board (FSB) published findings of a survey of 24 FSB member entities, including 23 national authorities and the European Commission, along with 24 non-member jurisdictions represented in the FSB's Regional Consultative Groups (RCGs).[1]

Fifteen FSB members and 10 RCG jurisdictions indicated they had implemented or had plans to enhance regulation in the crypto sector. Among the 70 cryptocurrency-related regulations issued by global supervisors, 49 are amendments to existing regulations, with only 21 being entirely new.

Regulatory or supervisory standards or guidance issued in each jurisdiction



Note: "N/A" reflects that the issued standard or guidance reported by respondents is not classified into either of the two categories.

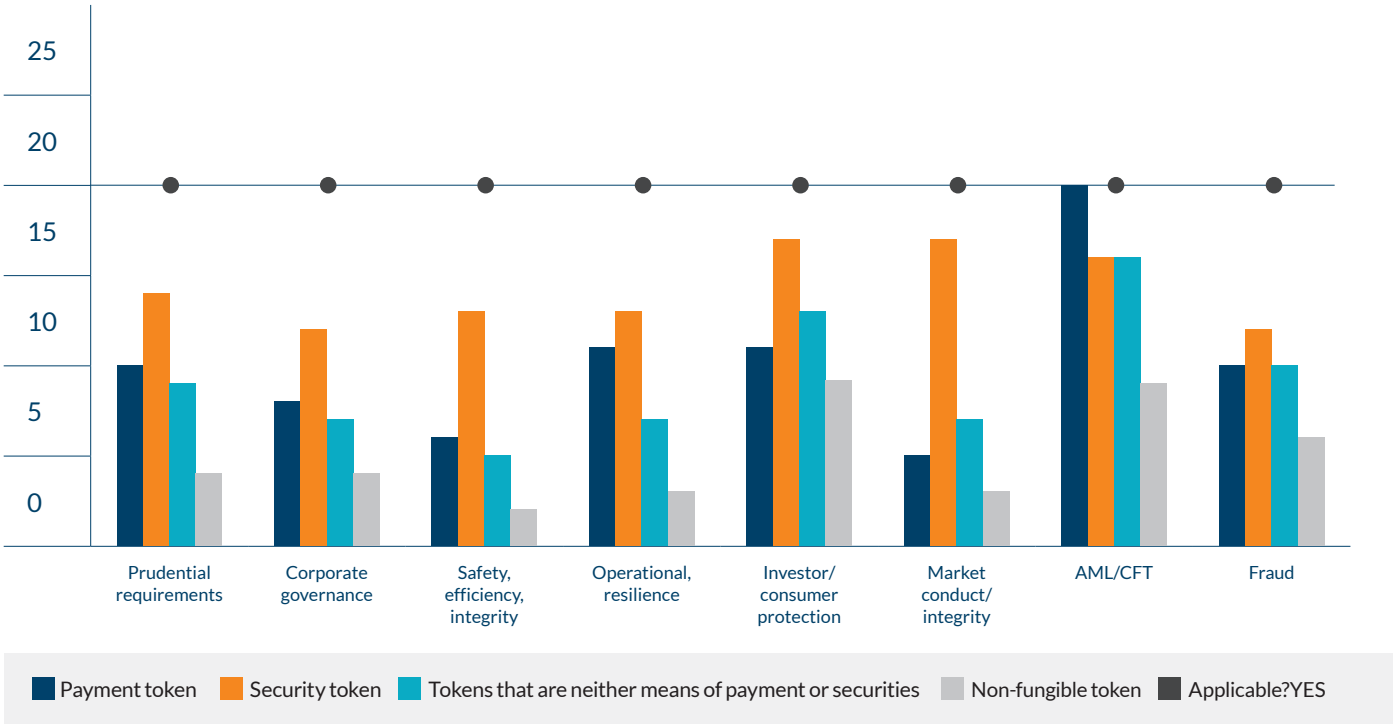
Source: FSB

Additionally, approximately one-third of survey respondents said they had introduced a definition for "crypto asset," with 13 jurisdictions establishing definitions for "security tokens" and "payment tokens."

Regarding the primary regulatory areas affecting crypto assets, the anti-money laundering/combating the financing of terrorism (AML/CFT) framework appears to receive the most coverage, followed by transparency issues and the protection of crypto-asset holders.

[1] FSB, Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets, 2022.

Applicable thematic regulation to different categories of crypto assets



Source: FSB

In assessing these survey results, clarity and consistency emerge as fundamental themes. In alignment with this, the FSB finalized its regulatory framework for crypto asset activities in July 2023. The framework includes high-level recommendations for regulating and supervising stablecoins and crypto assets more broadly. The FSB also enshrined the principle of "same activity, same risk, same regulation" within this framework to guide future standard-setting endeavors.[2]

Notably, the European Union has enacted new regulations, such as the transfer of funds regulation (TFR)[3] and the Markets in Crypto-Assets Regulation (MiCAR).[4] These regulations mark the first harmonized cross-border regulatory frameworks in the crypto-asset industry.

These significant strides not only demonstrate a commitment to tackling challenges but also aim to cultivate a favorable regulatory landscape that fosters innovation and security within the crypto ecosystem. In summary, the regulatory environment is evolving, presenting new opportunities for the industry while offering a clearer and more reliable framework for market participants.

[2] FSB, FSB Global Regulatory Framework for Crypto-Asset Activities — Umbrella public note to accompany final framework, 2023.

[3] EU, Regulation (EU) 2023/1113 of the European Parliament and of the Council of May 31, 2023 on information accompanying fund transfers and certain crypto-assets.

[4] EU, Regulation (EU) 2023/1114 of the European Parliament and of the Council of May 31, 2023 on markets in crypto-assets.

The Origins of the AML/CFT Crypto Framework

In the realm of combating financial crime, Virtual Asset Service Providers (VASPs) face a primary obligation: implementing the Travel Rule.

To gain insight into the current state of affairs, it's beneficial to take a step back to 1990 when the Financial Action Task Force (FATF) first introduced its 40 Recommendations to combat money laundering and terrorist financing. These recommendations underwent revisions in 1996 and gained endorsement from 130 countries, thereby establishing them as an international standard. Among them, Recommendation 16 proposed global standards for funds transfers, commonly referred to as the Travel Rule. It mandates that financial institutions identify both the sender and recipient of each transfer and provide accompanying data necessary for their identification.

Subsequently, in 2006 and 2015 the European Union adopted earlier versions of the TFR,[5] essentially the European counterpart to the Travel Rule. These measures aimed to harmonize the European approach and align legislation with Recommendation 16.

In 2019 and 2021, the FATF broadened the scope of Recommendation 16, extending the definition of financial institutions to include VASPs. This expansion led to the issuance of specific guidance,[6] prompting the European Union to enact a new fund transfer regulation in May 2023; this regulation mandates compliance with the Travel Rule for all European crypto operators, referred to as crypto asset service providers (CASPs), as defined by the TFR and MiCAR, by the end of 2024.

With the introduction of the new TFR, the European Banking Authority (EBA) was tasked with issuing guidelines to assist CASPs in implementing these standards, particularly in cases where originator or beneficiary information is lacking or incomplete. This includes operations involving decentralized finance (DeFi), such as transactions with self-hosted addresses on blockchain. In November 2023, the EBA initiated its first consultations on the Travel Rule Guidelines,[7] demonstrating Europe's commitment to the effective and harmonized implementation of the new regulation.

[5] The reference is to Regulation (EC) No. 1781/2006 of the European Parliament and of the Council of November 15, 2006 on information on the payer accompanying transfers of funds and Regulation (EU) 2015/847 of the European Parliament and of the Council of May 20, 2015 on information accompanying transfers of funds.

[6] FATF, Updated Guidance for a Risk-Based Approach — Virtual Assets and Virtual Asset Service Providers, 2021.

[7] EBA, EBA/CP/2023/35 — Consultation Paper — 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'), 2023.

Going Deeper: The Travel Rule

The Travel Rule, as outlined by the FATF, emphasizes the collection of vital information such as the originator's name and physical address (or other unique identifiers like national identity numbers, customer identification numbers or dates of birth), as well as the beneficiary's name and the account numbers of both parties involved in the transaction (i.e., the blockchain address in a crypto-asset transfer).

Data requirements for ordering and beneficiary VASPs in the Travel Rule

	VASP ordering	VASP beneficiary
Ordering data	• Required, i.e., submitting the necessary data to a beneficiary VASP is mandatory • Accurate, i.e., the ordering VASP needs to verify the accuracy as part of its customer due diligence (CDD) process	• Required, i.e., the beneficiary VASP needs to obtain the necessary data from the ordering VASP • Data accuracy is not required. The beneficiary VASP may assume that data has been verified by the ordering VASP
Beneficiary data	• Required, i.e., submitting the necessary data to the beneficiary VASP is mandatory • Data accuracy is not required, but the ordering VASP must monitor the data to confirm no suspicions arise	• Required, i.e., the beneficiary VASP needs to obtain the necessary data from the ordering VASP • Accurate, i.e., the beneficiary VASP must have verified the necessary data and needs to confirm if the received data is consistent
Actions required	• Obtain the necessary information from the originator and retain a record • Screen to confirm that the beneficiary is not a sanctioned name • Monitor transactions and report when they raise a suspicion	• Obtain the necessary information from the ordering VASP and retain a record • Screen to confirm that the originator is not a sanctioned name • Monitor transaction and report when it raises a suspicion

For traditional banking and financial institutions,[8] compliance with the Travel Rule is essential when engaging in crypto-related services, including custody or management of crypto-asset transfers between or from other VASPs. As previously mentioned, the Travel Rule aims to align AML/CFT standards related to crypto assets with those already established for fiat transactions.

Addressing the Travel Rule poses challenges that can be categorized into three main areas:

- **Timing differences in implementation ("sunrise issue")**
  Regulatory adoption occurs at varying times across different jurisdictions, leading to the "sunrise issue." This discrepancy in timing can result in arbitrage, compliance complexity, uncertainty and high compliance costs when operating cross-border.
- **Hybrid approaches across jurisdictions**
  Divergent and sometimes inconsistent approaches taken by different jurisdictions in implementing the Travel Rule create another obstacle. These differences may involve defining a de minimis threshold, addressing privacy concerns and managing DeFi-related transactions.
- **Definition of the technological solution**
  Selecting a suitable technology solution, or a combination of multiple solutions, to ensure compliance with FATF requirements and local regulations poses the third challenge. Choosing an effective technological approach is crucial to navigating the complexities of the Travel Rule successfully.

In this ever-evolving landscape, addressing the challenges of the Travel Rule demands not only a profound understanding of regulations, but also flexibility and technological innovation to adapt to the rapid changes in the crypto ecosystem overall.

[8] It should be noted that for these operators, the Travel Rule doesn't seem new, given that they are already subject to the previous Regulations (EC) No. 1781/2006 and (EU) 2015/847.

A Closer Look: The Sunrise Issue

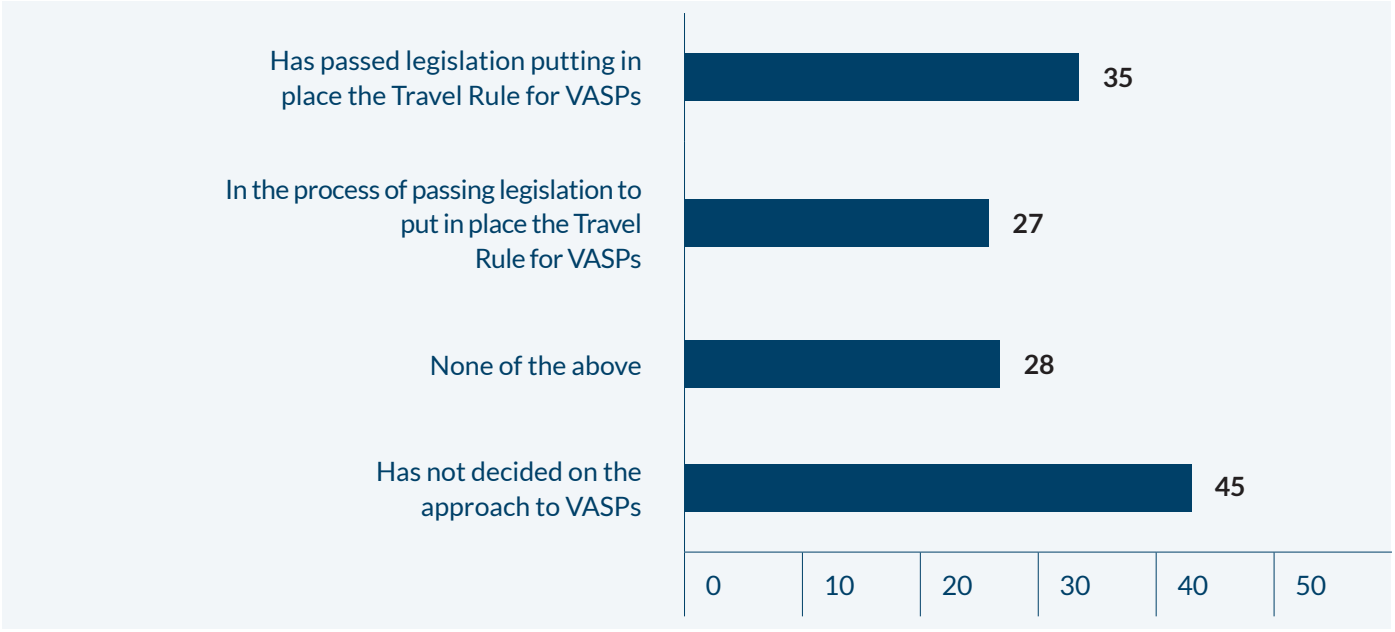
As previously mentioned, one of the foremost challenges within the crypto ecosystem is regulatory in nature. This challenge is particularly evident in the implementation of the Travel Rule, where we observe varying timelines across countries, often accompanied by transitional periods.

Regarding this issue, the FATF, in its 2023 annual update on the implementation of the Travel Rule,[9] reported limited progress. It noted that 54 percent of participants (73 out of 135 jurisdictions), up to that point, had not taken any action to implement the Travel Rule.

The FATF's update noted that while 35 jurisdictions had enacted specific regulations to ensure implementation, 27 others were in the process of adopting regulations. The FATF also highlighted some developments, primarily related to the enactment of the TFR at the European level, which increased the number of jurisdictions with specific regulations in this area to 58.

Consistent with the 2022 report, the FATF also revealed in 2023 that only 21 percent of jurisdictions (13 out of 62 respondents) indicated they had issued recommendations or findings or taken action against VASPs for failing to align with Travel Rule requirements.

• • • Implementation of the Travel Rule

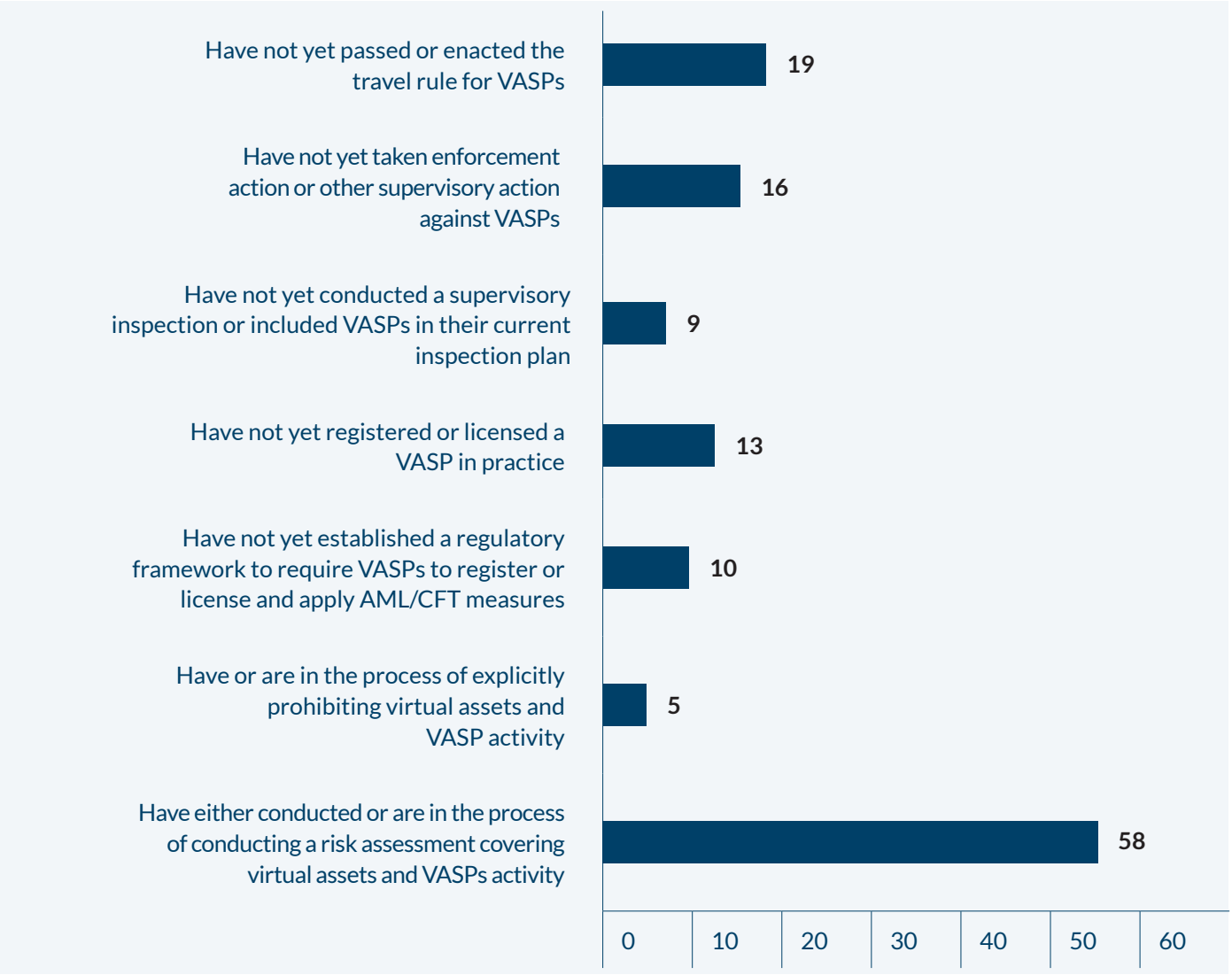


Source: FATF

[9] FATF, Targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers, 2023.

On March 28, 2024, the FATF released a report detailing the implementation status of FATF standards concerning crypto assets and VASPs across 58 jurisdictions deemed particularly relevant to these activities. This list comprises 38 FATF member countries and an additional 20 jurisdictions identified due to their significant trading volumes.[10]

Key highlights of the FATF report



Source: FATF

In addition to the aforementioned findings, the report evaluates each jurisdiction's compliance with Recommendation 15, providing ratings and the year of assessment. Notably, the Bahamas stands out as the only country on the list deemed fully compliant, based on an assessment conducted in 2022.

[10] FATF, Status of implementation of Recommendation 15 by FATF Members and Jurisdictions with Materially Important VASP Activity, 2024.

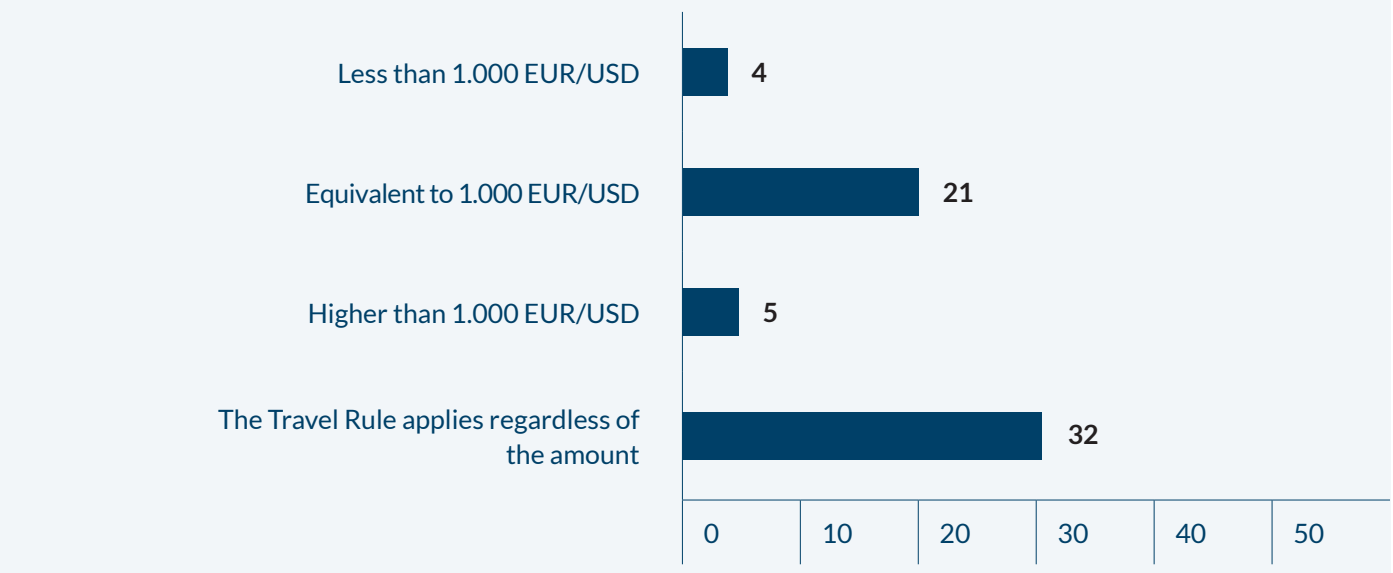
Hybrid Approaches

In the context of approaches to the Travel Rule, one of the primary divergences pertains to the application of varying de minimis thresholds. It is crucial to recall that the FATF Recommendations stipulate a threshold of USD/EUR 1.000 for the implementation of the Travel Rule.

According to the FATF's July 2023 report, of the 62 jurisdictions that expressed a stance on the de minimis threshold, 32 percent indicated that they had already implemented or intended to introduce a de minimis threshold set at USD/EUR 1.000. Meanwhile, 58 percent planned to introduce a lower threshold or EUR 0 threshold, and 8 percent aim to implement a higher threshold than the one proposed by the FATF.

For instance, in the United States, the threshold is set at USD 3.000, while the TFR establishes a Europe-wide threshold of EUR 0. Similarly, Canada has also established a threshold of 0 CAD 0.

Threshold approach to Travel Rule implementation



Source: FATF

These differences in de minimis thresholds underscore the variety of approaches taken globally, with some jurisdictions adhering to the FATF Recommendations while others preferring to adjust these thresholds according to their own requirements and regulatory environments. The definition and implementation of these thresholds are crucial aspects in the harmonization of international practices under the Travel Rule.

Further exploration of the disparities between the Travel Rule governed by the FATF and the TFR reveals some notable differences, despite their overall alignment.

First, the TFR distinguishes between crypto-asset transfers involving blockchain (or distributed ledger technology, DLT) and those that do not. In the former case, it is necessary to collect the DLT address (i.e., the alphanumeric code on the blockchain from/to which the crypto-assets are transmitted), while in the latter case, the crypto-asset account held by the VASP is required.

Specifically, the TFR mandates the transmission of a more comprehensive array of data regarding the originator, encompassing the address (including the country name), the personal identification document number and the customer identification number. While the FATF does not mandate the inclusion of all these details, it stipulates the presence of at least one of the following: a physical address, a national identity number, a customer identification number, or the date and place of birth.

FATF and TFR requirements comparative analysis

FATF			Correlation	TFR		
Name	●	●	Y	Name	●	●
Account number (wallet on blockchain)	●	●	Unclear	Address on DLT OR	●	●
				Crypto asset account (if transfer did not occur on blockchain)	●	●
Geographic address OR	●		Y	Address (including country)	●	
ID number OR	●		Y	ID number	●	
Date and place of birth	●		Y	Date and place of birth*	●	
LEI**	●		Y	LEI or equivalent**	●	

● Originator ● Beneficiary * Only required in rare cases * * If available

The TFR further specifies that in the (rare) instance where the name, blockchain address or account number, physical address and identification document number are insufficient to identify the originator, the VASP should also collect and transmit date and place of birth information.

In contrast, the FATF does not provide detailed use cases for geographic addresses, unlike the EBA Guidelines under consultation, which clarify that if the originator is:[11]

- an individual, the place of habitual residence should be shared.
- a vulnerable person, the address from other available documentation should also be shared.
- a legal entity, the address of the registered office should be shared.

Similarly, the EBA Guidelines under consultation state that in the case of bundled crypto-asset transfers, it is mandatory to transmit information on all originators unless there are technical limitations preventing the transmission of such data. In contrast, the FATF does not provide corresponding guidance on this scenario.

Regarding transfers to/from DeFi, i.e. self-hosted addresses, the FATF emphasizes the importance of obtaining and transmitting accurate beneficiary information, acknowledging that the methods of obtaining this information may vary among jurisdictions.

On this issue, the TFR and the EBA Guidelines in consultation introduce additional arrangements, such as:

- Using blockchain analytics tools, third-party data providers, etc., to identify transactions involving DeFi in real-time before executing the transfer by the originator's VASP and before crediting the funds by the beneficiary's VASP, as well as verifying the information received from the originator through such tools;
- For crypto-asset transfers exceeding EUR 1.000, verifying the ownership of the self-hosted address (e.g., through the use of the aforementioned tools, signing the transaction with the private key pair in both the account and the wallet, etc.).

In practical terms, this implies that if a person (who has an account with a VASP) intends to transfer EUR 1.000 to another person (e.g., his brother with a self-hosted address), the transferring person's VASP must verify the identity of the recipient and demonstrate the ownership and control of their DeFi address.

As previously mentioned, the technical methods for conducting such analyses are not exhaustively defined, and the EBA provides only some guidance.[12]

It is essential to recognise that one method does not preclude others. A VASP can offer its users one, multiple or all of the available methods.

[11] The EBA Guidelines in consultation also specify the order of priority for providing the address as follows: i) full country name; ii) postal code; iii) city; iv) state; v) province; vi) municipality; vii) street name; viii) building number; ix) building name. It's important to note that a post office box or virtual address is not considered a valid type of address and will not comply with the requirements of the TFR.

[12] On this matter, it's worth noting that the EBA Guidelines under consultation don't mandate a combined use of these methods, even in high-risk scenarios.

The technical modalities currently most widely used

	Visual proof	Satoshi test	Manual signing	AOPP
Overview	• The customer is requested to capture a screenshot of his DeFi wallet/address displaying the withdrawal address • After uploading the screenshot to the VASP platform, the DeFi address is cross-referenced with the one provided by the client for approval • If the address depicted in the screenshot corresponds to the withdrawal address provided, the VASP can approve the transaction	• The client initiates a prearranged transaction between his DeFi address and the VASP before the intended transfer • The VASP sets criteria including a minimum amount, a timeframe, and a destination address • The customer transfers the specified amount to the provided address within the designated time frame • Upon successful verification of the transaction, the customer verifies the DeFi address	• The VASP requests the client to sign a designated message using his private key • After copying the message to their DeFi wallet and signing it with their private key, the VASP can verify the signature against the message and public key, confirming the client's control over the DeFi address	• Address Ownership Proof Protocol (AOPP) is an automated variant of Manual Signing for VASP and user
Pros	• Easiest wallet verification methods to be performed by customers as they are familiar with screenshots and video tools • Compatible with all DeFi wallets	• Offers greater security compared to Visual Proof	• Provides secure proof of control through encryption	• Provides secure proof of control through encryption • Offers automated processes on both the client-side and VASP, ensuring a user-friendly experience
Cons	• Vulnerable to tampering and counterfeiting • May require time-consuming and manual audits by the VASP, depending on the implementation of the solution	• It tends to be slower and more costly for users due to transaction fees on the blockchain	• Not universally supported by all DeFi wallets • Requires more complex tasks, which may be challenging for the average user	• Not universally supported by all DeFi wallets

The Technological Solutions

Choosing the right tool or integrated solution for monitoring crypto-asset transactions requires careful consideration.

The FATF has acknowledged significant progress in recent years in the development and adoption of technology solutions in this area. However, further improvements are necessary to ensure that these solutions are comprehensive, interoperable and adaptable to national requirements.

Currently, supporting solutions in the market can be broadly categorized into two main groups:

- **Blockchain analytics tools**
  These tools analyze and monitor blockchain data, wallets, DeFi addresses and related transactions. Their primary aim is to mitigate the risks associated with money laundering, terrorist financing, and violations or circumventions of international sanctions.
- **Travel Rule protocols**
  These tools and protocols are designed to facilitate the transmission of originator and beneficiary data in compliance with the Travel Rule.

The synergistic integration of both categories of tools enables a holistic approach to monitoring crypto-asset transactions, effectively addressing both financial crime risk management and Travel Rule-specific challenges.

[11] The EBA Guidelines in consultation also specify the order of priority for providing the address as follows: i) full country name; ii) postal code; iii) city; iv) state; v) province; vi) municipality; vii) street name; viii) building number; ix) building name. It's important to note that a post office box or virtual address is not considered a valid type of address and will not comply with the requirements of the TFR.

[12] On this matter, it's worth noting that the EBA Guidelines under consultation don't mandate a combined use of these methods, even in high-risk scenarios.

The Blockchain Analytics Tool

The blockchain operates on a principle of pseudonymity rather than anonymity.

While the identity of the crypto-asset holder behind a specific transaction, wallet or DeFi address may remain unknown, every movement on the blockchain is meticulously recorded. Transaction data such as the amount, time, currency, DeFi wallet/address of sender and recipient, along with other elements involved in the wallet/address DeFi (current balance, entries, exits, etc.), are all traceable and visible to anyone on a public blockchain.

Blockchain analytics tools leverage this wealth of available data to track transactions, cluster DeFi wallets/addresses (i.e., associate DeFi wallets/addresses that appear to be controlled by the same individual within the same cluster), link clusters to the real-world entities behind them, categorize the services offered by each cluster by assigning specific risk levels, and identify direct and indirect exposure between two or more clusters.[13]

Numerous tools are currently available, including but not limited to free options like Etherscan and Blockchain.com to licensed solutions such as Chainalysis, TRM Labs and Elliptic, among others.[14]

[13] Direct exposure pertains to funds transferred directly from one entity to another without intermediaries. In contrast, indirect exposure occurs when two clusters interact through a third party. Direct exposure signifies a robust connection between clusters. Conversely, with indirect exposure a detailed analysis of how the clusters are linked is required to assess their connection.

[14] Furthermore, the efficacy of these tools has been validated by a U.S. District Court in the District of Columbia, which issued an order regarding the admissibility of blockchain investigation results obtained through blockchain analytics tools in court. This ruling, dated February 29, 2024, could have substantial ramifications for forthcoming cases involving cryptocurrency transactions and digital currency-related crimes by establishing a precedent concerning the potential admissibility of evidence from such software. Specifically, the court focused on Chainalysis' solution, Reactor, which operates using three levels of heuristics (a heuristic refers to a computational function or technique used to solve problems or make decisions based on available information). These techniques are employed to clusterize addresses on the blockchain by identifying patterns or characteristics in the data suggesting they are controlled by the same entity. The first heuristic is based on the co-spending feature, wherein multiple input addresses on the blockchain are utilised in a single transaction. This heuristic posits that multiple addresses funding a single transaction are controlled by a single entity, as sharing private keys among different entities is highly improbable. The second heuristic observes and tracks specific behaviors and patterns unique to individual entities on the blockchain, facilitating the clustering of addresses based on these patterns. The third heuristic utilises off-chain information obtained from sources such as court documents, social media, and open-source intelligence activities. Additionally, the court underscored the extensive utilisation of Reactor since 2016 in various investigations, attesting to its high reliability based on real-world application. Reactor's clustering techniques have also been widely validated in court through subpoenas issued to VASPs. Witnesses described a systematic process wherein Chainalysis completes the clustering process with data/information provided by VASPs in response to subpoenas, thus validating Reactor's accuracy. The U.S. government, during a closed-door session, further clarified that it had conducted an exhaustive examination of numerous clustered addresses on the blockchain by Chainalysis, affirming Reactor's reliability at a level of 99.91%. Finally, the court emphasized the extensive adoption of blockchain analytics solutions, such as Reactor, in both the public and private sectors, citing Chainalysis as the industry standard. For further details, refer to UNITED STATES v. STERLINGOV (2024), Criminal Action No. 21-399 (RDM), Decided: February 29, 2024.

Travel Rule Protocols

Since the inception of the Travel Rule, several protocols have emerged to facilitate compliant and secure information exchange between VASPs. Among the notable commercial solutions are Sygna Protocol, VerifyVASP, TRISA, Shyft, and TRUST. Additionally, the Travel Rule Protocol (TRP), an open-source protocol developed in 2020 by a private consortium including ING, Standard Chartered and BitGO, has gained significant traction.

Despite the variety of protocols available, a primary challenge identified by the FATF and European regulations is the lack of interoperability among them. Unlike fiat transactions, which utilise SWIFT as the dominant network for exchanging financial information, a comparable global standard for exchanging information between VASPs has yet to emerge for crypto asset transactions. This lack of interoperability among the various Travel Rule protocols impedes efficient data utilisation and the broader adoption of Travel Rule requirements.[15]

In this regard, the current state of Travel Rule protocols can be likened to social messaging platforms: while one can exchange messages, audio and media within a platform, cross-platform communication remains a challenge.

To mitigate these limitations, both the FATF and the EBA Guidelines in consultation acknowledge the existing constraints of these solutions, including potential technical limitations that could impede the transmission of originator and beneficiary information. Consequently, European regulations will not introduce a transitional regime until 2025, ensuring the possibility of utilising infrastructure or services that may not fully meet all information transmission requirements.

[15] At least the crypto industry reached consensus over a single data messaging format for all Travel Rule protocols: the InterVASP Messaging Standard (IVMS 101), which establishes a universal common language for the communication of required originator and beneficiary information between VASPs.

Conclusions

The evolution of legislation often struggles to keep pace with the rapid advancements in the market, particularly in the realm of technology. In this context, the pressing need for a unified global vision becomes evident, especially in defining regulatory frameworks capable of addressing issues of global significance, such as those pertaining to crypto assets.

The Travel Rule stands as a prominent example of the complexities inherent in regulating crypto assets.

The absence of regulation in certain jurisdictions, juxtaposed with the increasing regulatory scrutiny specific to crypto assets in others, engenders legal uncertainty and disparate standards. Consequently, industry stakeholders are compelled to undertake additional compliance efforts to navigate the diverse regulatory landscape.

Furthermore, while current technological solutions demonstrate efficacy in addressing transaction monitoring challenges on the blockchain, achieving greater alignment and interoperability among these solutions is imperative. Such efforts are necessary to streamline processes and overcome existing limitations, facilitating more efficient compliance mechanisms.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and its independent and locally owned member firms provide clients with consulting and managed solutions in finance, technology, operations, data, digital, legal, HR, risk and internal audit through a network of more than 90 offices in over 25 countries.

Named to the *Fortune* 100 Best Companies to Work For® list for 10 consecutive years, Protiviti has served more than 80 percent of *Fortune* 100 and nearly 80 percent of *Fortune* 500 companies. The firm also works with government agencies and smaller, growing companies, including those looking to go public. Protiviti is a wholly owned subsidiary of Robert Half Inc. (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

About Our Financial Crime Practice

Protiviti's Financial Crime practice specialises in helping financial institutions satisfy their regulatory obligations and reduce their financial crime risk exposure using a combination of anti-money laundering/combating the financing of terrorism and sanctions risk assessment, control enhancement, and change capability to deliver effective operational risk and compliance frameworks. Our team of specialists assists organisations with protecting their brand and reputation by proactively advising on their vulnerability to financial crime, fraud and corruption, professional misconduct, and other financial business risk issues.

Authors

Francesco Monini
Managing Director
francesco.monini@protiviti.it

Mattia Simoncini
Director
mattia.simoncini@protiviti.it

Mattia Santi
Manager
mattia.santi@protiviti.it

THE AMERICAS

UNITED STATES
Alexandria, VA
Atlanta, GA
Austin, TX
Baltimore, MD
Boston, MA
Charlotte, NC
Chicago, IL
Cincinnati, OH
Cleveland, OH
Columbus, OH
Dallas, TX
Denver, CO
Ft. Lauderdale, FL
Houston, TX
Indianapolis, IN
Irvine, CA
Kansas City, KS
Los Angeles, CA
Milwaukee, WI
Minneapolis, MN
Nashville, TN
New York, NY
Orlando, FL
Philadelphia, PA
Phoenix, AZ
Pittsburgh, PA
Portland, OR
Richmond, VA
Sacramento, CA
Salt Lake City, UT
San Francisco, CA
San Jose, CA
Seattle, WA
Stamford, CT
St. Louis, MO
Tampa, FL
Washington, D.C.
Winchester, VA
Woodbridge, NJ

ARGENTINA*
Buenos Aires

BRAZIL*
Belo Horizonte*
Rio de Janeiro
São Paulo

CANADA
Toronto

CHILE*
Santiago

COLOMBIA*
Bogota

MEXICO*
Mexico City

PERU*
Lima

VENEZUELA*
Caracas

EUROPE, MIDDLE EAST & AFRICA

BULGARIA
Sofia

FRANCE
Paris

GERMANY
Berlin
Dusseldorf
Frankfurt
Munich

ITALY
Milan
Rome
Turin

THE NETHERLANDS
Amsterdam

SWITZERLAND
Zurich

UNITED KINGDOM
Birmingham
Bristol
Leeds
London
Manchester
Milton Keynes
Swindon

BAHRAIN*
Manama

KUWAIT*
Kuwait City

OMAN*
Muscat

QATAR*
Doha

SAUDI ARABIA*
Riyadh

UNITED ARAB EMIRATES*
Abu Dhabi
Dubai

EGYPT*
Cairo

SOUTH AFRICA *
Durban
Johannesburg

ASIA-PACIFIC

AUSTRALIA
Brisbane
Canberra
Melbourne
Sydney

CHINA
Beijing
Hong Kong
Shanghai
Shenzhen

INDIA*
Bengaluru
Chennai
Hyderabad
Kolkata
Mumbai
New Delhi

JAPAN
Osaka
Tokyo

SINGAPORE
Singapore

*MEMBER FIRM

protiviti®