

The Travel Rule and Unhosted Wallets: Regulation and Practical Implications

Applying the Financial Action Task Force (FATF) Travel Rule to unhosted wallets poses significant regulatory and technical challenges given their anonymous and decentralized nature. This document examines the legal and practical implications of implementing the Travel Rule across major jurisdictions, focusing on the European Union, Switzerland, and the United States. Using a qualitative, comparative approach grounded in primary and secondary legal sources, the research identifies differences in how AML obligations and identity verification are applied to users of unhosted wallets. European markets impose transaction requirements based on value, while Switzerland enforces a strict verification system that greatly restricts private wallets. In contrast, the United States does not require unhosted wallets to comply with the Travel Rule, emphasizing due diligence over mandatory reporting. The analysis shows that regulatory fragmentation hinders compliance, distorts market competition, and risks discouraging technological innovation. Meanwhile, debates about user privacy, pseudonymity, and financial surveillance remain central to regulatory tensions. The paper concludes that harmonized, risk-based frameworks are critical to balancing innovation and security without marginalizing self-hosted wallet users in the evolving crypto-assets landscape.

Keywords: Anti-money laundering, unhosted wallet, regulation, compliance, decentralization.

Introduction

Cryptoassets represent a new source of opportunity not only for the financial world but also for criminal enterprises. Their widespread adoption through decentralized platforms has raised concerns about financial crimes such as money laundering and terrorist financing, prompting national authorities to develop rules and directives to mitigate risks associated with emerging technologies.

In this context, the Financial Action Task Force (FATF) introduced the "Travel Rule", aimed at combating money laundering in virtual asset transfers, which requires virtual asset service providers (VASPs) to share personal information about both originators and beneficiaries.

The Travel Rule is one of the fundamental pillars for the creation of a global, effective and specific Anti-Money Laundering system (AML), particularly designed to counter cybercrime conducted through virtual currency services.

The Travel Rule derives its name from the principle that information regarding the beneficiary and the sender "travels" with the transaction itself and is kept by both actors involved.

By ensuring that all parties involved are aware of the inherent and potential risks of the transaction, the Travel Rule aims to mitigate vulnerabilities

1 connected with the transfers of a digital asset. Unlike traditional financial
2 systems, where an intermediary only sees a segment of the transaction flow and
3 rarely grasps its full dynamics, this framework enhances the capacity to detect
4 fraudulent schemes and strengthens overall risk management by ensuring that all
5 parties have a complete picture. In this landscape, it becomes crucial to
6 distinguish between the different tools through which digital assets are held.
7 Unhosted wallets, for instance, allow users to maintain full control of their
8 private keys, a structure that inherently amplifies confidentiality and reduces the
9 traceability of the wallet to its actual holder. In other cases, the management of
10 keys and transactions is delegated to an intermediary, as occurs in hosted wallets,
11 reintroducing a level of centralization, partly similar to the dynamics of
12 traditional financial services.

13 Extending the discipline of the Travel Rule to unhosted wallets raises
14 specific critical issues related to their decentralized structure and the difficulty
15 of definitively tracing them back to a holder, due to their anonymous and
16 pseudonymous nature. Precisely this opacity fuels, at the regulatory level, the
17 perception of a greater risk of money laundering, terrorist financing and other
18 illicit conduct, since such instruments can easily evade AML obligations.

19 The discussion of this topic is an opportunity to highlight the role of
20 unhosted wallets in the cryptocurrency landscape. Regulatory fragmentation is
21 largely justified by the perception that these private wallets pose risks for money
22 laundering, terrorist financing and other illegal activities, as they can easily
23 bypass AML regulations. Yet, despite the growing regulatory attention, there
24 remains no consensus on how and to what extent the Travel Rule can be
25 effectively applied to transactions involving unhosted wallets. The literature has
26 so far focused mainly on hosted environments, leaving the specific legal
27 implications, operational barriers and cross-jurisdictional inconsistencies
28 concerning private wallets largely unexplored. This paper addresses this gap by
29 examining the divergent regulatory solutions adopted in the European Union,
30 Switzerland and the United States.

31 From this perspective, the paper aims to understand to what extent the
32 Travel Rule can be applied to unhosted wallets without compromising
33 technological neutrality, privacy principles, and the functioning of decentralized
34 ecosystems. The paper aims to identify structural tensions in current regulatory
35 frameworks and outline the conditions under which consistent, risk-based
36 regulation of unhosted wallets can be achieved.

37 First, the paper develops a conceptual model of regulatory misalignment,
38 demonstrating that Travel Rule obligations were designed for systems with
39 custodial intermediaries that exercise control, perform KYC tasks, and act as
40 identifiable enforcement points.

41 Second, the paper demonstrates that extending these obligations to self-
42 hosted wallets creates an enforcement vacuum, where compliance becomes
43 technically impossible or economically distortive, thus generating undesirable
44 outcomes such as regulatory arbitrage, market exclusion, and disproportionate
45 surveillance risks. This framework aims to go beyond simple descriptive

1 comparisons and provides an analytical explanation for the persistent regulatory
2 fragmentation affecting unhosted wallet transactions.

3 The paper is structured as follows. Following this Introduction, Section 2
4 reviews the existing literature on the application of the Travel Rule to crypto-
5 asset transfers. Section 3 sets out the comparative legal methodology. Section 4
6 presents the results of the comparative analysis, focusing on the different
7 approaches to identity verification, peer-to-peer transactions and the obligations
8 imposed on regulated intermediaries. Section 5 discusses the broader
9 implications of these regulatory divergences. Finally, Section 6 draws the main
10 conclusions and identifies possible directions for a more coherent and risk-based
11 regulatory framework.

12 13 14 **Literature Review**

15
16 The existing literature has largely examined the Travel Rule with reference
17 to hosted wallets, while only recently have studies begun to address its
18 implications for unhosted wallets. These contributions remain limited and
19 fragmented, leaving several regulatory specificities insufficiently explored.
20 Compliance challenges arise mainly from divergent national requirements, the
21 intrinsic difficulty of verifying information linked to unhosted wallets and
22 uneven enforcement mechanisms.

23 Unlike traditional transactions, accessible only to regulated intermediaries,
24 cryptocurrency transfers may occur through multiple channels, including peer-
25 to-peer transactions between two self-hosted wallets (paragraph 117 of the
26 Guidelines). This operational structure complicates the application of
27 Recommendation 16.

28 The FATF Guidelines have adapted the application of the Travel Rule for
29 transactions involving unhosted wallets, considering the lack of a financial
30 institution or entity capable of performing identity verification (paragraph 204
31 of the Guidelines). Therefore, when one of the counterparties uses a self-hosted
32 wallet, only the VASP involved is required to collect the relevant information,
33 as it is the sole entity subject to the Travel Rule.

34 Comparative analyses highlight significant discrepancies in how
35 jurisdictions have transposed the 2019 extensions of Recommendation 16 to
36 virtual assets. These divergences stem not merely from the content of domestic
37 rules, but from deeper structural inconsistencies in their design and enforcement.
38 While the FATF aims at regulatory harmonization, national approaches vary
39 considerably in terms of rigour, proportionality and operational feasibility.
40 Understanding these differences is essential to assess whether the current
41 regulatory landscape can realistically govern transactions involving self-hosted
42 wallets.

Methodology

To examine the application of the Travel Rule to unhosted wallets in different jurisdictions, the study takes a qualitative and comparative approach. The methodology is based on a collection of information through the analysis of official normative documents and regulations issued at national and international levels, with particular reference to the European Union, Switzerland and the United States, as well as relevant academic studies. The research is mainly based on primary legal sources, including national and supranational legislation (eg, MiCA, Bank Secrecy Act, FINMA regulations); soft law instruments such as FATF guidelines, which are one of the main reference sources for this framework, and authoritative secondary literature, including academic publications and technical reports. The analysis follows a model of documentary legal research, based on the interpretation and comparison of texts and regulatory frameworks between jurisdictions. The selection of sources was based on their normative value, relevance to the travel rule and topicality. Preference was given to legal texts and regulatory guidelines published or updated after 2019, when the FATF extended Recommendation 16 to virtual assets. Secondary literature was selected based on academic reliability, citation frequency and relevance to compliance challenges in decentralized finance. The benchmarking framework is organised in a matrix that contrasts key regulatory elements such as the treatment of peer-to-peer transactions, identity verification thresholds, obligations for virtual asset service providers (VASPs) and enforcement mechanisms. This structure allows the identification of divergences, compliance burdens and practical implications for actors operating in cross-border cryptographic environments. The choice of these countries is justified by the fact that the European Union has adopted a detailed regulatory framework for crypto-assets with the Markets in Crypto-Assets Regulation (MiCAR), influencing member states' policies; Switzerland has adopted an innovative regulatory ecosystem, and the US is a key player in global financial markets. So, they all represent normative reference models.

Subsequently, the analysis proceeds to a summary of the results, offering an overview of the different regulations and highlighting the main critical issues that arise in transactions involving unhosted wallets.

To ensure a consistent comparative assessment, the analysis adopts three legal analytical criteria: the degree of regulatory proportionality applied to unhosted wallet transactions; the feasibility of applying the travel rule in each jurisdiction, assessed through the presence of obligated parties and legal limitations; and, finally, the impact of each regulatory framework on innovation and the risk of regulatory arbitrage. By utilizing these criteria, the study can go beyond a descriptive comparison of statutory provisions.

Results

In the European Union, the regulatory framework applicable to crypto-assets relies on two complementary pillars: Markets in Crypto-assets Regulation (MiCAR), which establishes authorization and supervisory requirements for crypto-asset service providers (CASPs) and the European Fund Transfer Regulation (TFR, Reg. 2023/1113/EU), which specifically extends the application of the Travel Rule to crypto-asset transfers. Thus, while MiCAR governs who may operate as a CASP and under what conditions, the TFR regulates the information that must accompany digital asset transfers, including those involving CASPs.

Under this regime, all transactions between CASPs must include the information required by law, irrespective of the transfer amount; however, according to the TFR, it does not apply to transfers between unhosted wallets, unless a CASP is involved. In this situation, for transactions above the 1,000 euros threshold to and from private wallets, CASPs must verify and confirm that the client controls the wallet, whereas below that threshold, they are still required to collect basic identifying information. The European approach is, therefore, more stringent than the FATF Guidelines, as it requires data collection even for sub-threshold transfers.

Switzerland represents one of the strictest regulatory environments in this field. FINMA, the Swiss financial market supervisory authority, was among the first authorities to implement the FATF guidelines rigorously and to issue detailed rules on the Travel Rule's application. Swiss regulation mandates anti-money laundering controls, including Travel Rule requirements, for all transfers above CHF 1,000. The practical consequence is a de facto ban on transactions involving unhosted wallets whenever identity verification cannot be achieved. Proof-of-ownership is the mechanism used to satisfy verification obligations, typically through systems such as Satoshi Test or Address Ownership Proof of Protocol (AOPP). The latter is a tool that enables users to demonstrate control over a self-hosted wallet (also known as an unhosted, private, non-custodial wallet) "in an easy, fast and private way".

Under US legislation, FinCEN (Financial Crimes Enforcement Network) has extended the requirements of the KYC regulation and recordkeeping to VASPs for transactions above 3,000 USD, mirroring the threshold applicable under the Bank Secrecy Act (BSA) to banks and non-bank financial institutions. Concerning unhosted wallets, FinCEN clarified that individuals using a self-hosted wallet for their own purposes do not qualify as money transmitters and are therefore outside the scope of BSA obligations applicable to financial institutions. As stated in the Federal Register, "when a person conducts a transaction solely on their own behalf, including through a non-custodial wallet, they are not a money transmitter and are not subject to BSA requirements".

From this perspective, the following table provides a comparative overview of the main international approaches to crypto-asset regulation, with particular attention to the implementation of the Travel Rule.

Table 1. Comparison of regulatory approaches. Analysis of unhosted wallet transactions

CRITERION	EU (MICAR + TFR)	SWITZERLAND (FINMA)	USA (FINCEN)	FATF GUIDELINES
Transaction between an obliged entity (VASP/CASP) and an unhosted wallet	Yes, with identity verification required above € 1000	No, unless proof of ownership is provided	Yes, no mandatory reporting for unhosted wallets, but CDD applies	Yes, the Travel Rule applies, but enforcement depends on national implementation
P2P transaction (unhosted to unhosted)	Not covered by the Travel Rule	No	No	Left to national discretion
Objective of the regulation	Balance transparency and GDPR compliance	Strict anti-money laundering enforcement	Prevent illicit activities	Ensure traceability while allowing flexibility for national regulators
Sanctions for non-compliance	High penalties for non-compliant CASPs	Strict limitation on unverifiable transactions	Fines and restrictions for unregistered VASPs	Varies by national regulation

Source: Author's elaboration (2025).

The table provides an overview of four different regulations governing the transfer of funds and their impact on unhosted wallets. The first row lists the relevant regulatory frameworks and authorities: FATF, European Union, Switzerland and the United States.

In the vertical columns, specific regulatory criteria are analyzed: first, it is verified whether the regulation applies to transactions involving at least one unhosted wallet or if it also includes transactions exclusively between non-custodial (P2P) wallets. Next, we examine the objectives pursued by the different jurisdictions through the implementation of the Travel Rule, highlighting the balance between security, transparency and privacy protection. Finally, the possible provision of penalties for non-compliance is analysed, with a comparison between the measures taken in the different legal systems.

The comparison clearly shows that regulators adopt different approaches to the use of unhosted wallets.

The approach of different states to peer-to-peer (P2P) transactions is heterogeneous, adapting to the intrinsic risks of this type of operation.

By contrast, transactions between an obliged entity (VASP/CASP) and an unhosted wallet show a different degree of intervention, based on the regulatory framework adopted by individual states and the objective that they intend to achieve through their legislation. The difference in the application of the Travel Rule lies in the fact that the presence of at least one obliged entity allows for a control point of the transaction, entrusting this entity with the task of collecting information and, in some jurisdictions, even verification.

1 In this perspective, the approach of the FATF, which is then reflected in all
2 other states, emphasizes traceability and transparency of transactions. The FATF
3 guidelines aim to balance innovation with the prevention of illegal activities.
4 While not excluding the use of unhosted wallets or peer-to-peer (P2P)
5 transactions, the FATF, at paragraph 204, leaves it up to states to modulate the
6 use of such tools, such as the Travel Rule, based on the risk they entail.

7 In other words, a "technology-neutral" approach is adopted, strongly
8 anchored on a risk assessment. This regulatory flexibility allows each state to
9 decide how far it wants to integrate these instruments into its legal framework
10 (paragraph 52)

11 In recent years, the FATF has consistently directed and urged Member
12 States to adopt measures aimed at verifying users' identities, highlighting that
13 these do not represent a goal, but rather a starting point for more effective
14 regulation (paragraphs 3 and 160).

15 However, the need to leave out unhosted wallets was also justified by the
16 impossibility, partly technical, of reporting or collecting information on
17 unhosted wallets, as they are not managed by regulated entities, and may offer a
18 high degree of pseudonymity. The neutral and technology-independent nature of
19 this discipline has led to the natural consequence that the Travel Rule was not
20 specifically designed for the use of wallets, whatever they may be, leading to
21 significant privacy concerns. Rather, its application in the cryptocurrency sector
22 stems from an analogue extension of the regulations already existing in the
23 traditional financial system.

24 The European Union, through its regulations on fund transfers, also aims to
25 include non-custodial wallets in the regulatory scope. The adoption of this
26 specific discipline, which also involves unhosted wallets, is inspired by the goal
27 of delineating a uniform regulatory landscape among states. Precisely for this
28 reason, the European strategy deriving from TFR and MICAR prefers
29 traceability and introduces thresholds and obligations. From this perspective, the
30 CASP involved in the transaction always collects, verifies and stores
31 information, regardless of whether the transaction involves a custodial or non-
32 custodial wallet. Furthermore, regardless of whether the unhosted wallet belongs
33 to the sender or the beneficiary, if the transaction exceeds 1,000 euros and
34 appears suspicious, the service provider must inform the competent authorities.
35 This is because transactions involving private wallets represent a "red flag" for
36 AML authorities. This approach increases investigative capacity and intra-EU
37 regulatory consistency but raises practical questions about the proportionality of
38 interference in personal data protection rights (GDPR). This development by the
39 EU involves a shift from a risk-based model with transaction thresholds to a
40 more prohibitionist approach, with far-reaching implications for the future use
41 of unhosted wallets in the European market. In this context, the EU model seems
42 to prioritise traceability at the cost of expanding compliance burdens for CASPs
43 and narrowing the functional space for self-hosted wallets.

44 By contrast, Switzerland takes an even more restrictive approach: unhosted
45 wallets are practically banned or subject to very strict limits. The table shows
46 that there is no general ban on "hybrid" transactions, but clearly, the

1 impossibility of verification automatically leads to their exclusion in practice.
 2 As a result, P2P transactions are also severely restricted to prevent the misuse of
 3 cryptocurrencies. As can be seen, the Swiss strategy is among the most rigorous.
 4 While strong ex ante control of transactions involving unhosted wallets allows
 5 effective repressive action, it also entails a risk of high exclusion from the world
 6 financial circuit, with negative repercussions in terms of innovation. This strict
 7 interpretation of the Travel Rule turns the identity verification requirement into
 8 a ban on transactions involving unhosted wallets.

9 The US (Bank Secrecy Act) model does not impose a real reporting
 10 obligation for transactions with unhosted wallets but still requires the application
 11 of Customer Due Diligence (CDD). It reflects a more permissive and innovation-
 12 oriented regulatory philosophy. This means that VASPs must collect information
 13 about their clients, although they are not required to report transactions with
 14 private wallets. The American approach places greater emphasis on customer
 15 control and verification, rather than imposing direct reporting obligations or
 16 rigid thresholds. From this perspective, the aim is to balance innovation and
 17 supervision, leaving a certain margin of discretion. However, this flexibility
 18 creates regulatory gaps that could be exploited for illicit activities.

21 Discussion

23 Comparative analysis of the EU, Switzerland and the US reveals that
 24 divergent Travel Rule implementations do not simply reflect different regulatory
 25 choices but generate systematic incentives and structural distortion in the way
 26 actors interact with unhosted wallets. These dynamics emerge from a deeper
 27 regulatory misalignment: the Travel Rule is designed for environments with
 28 verifiable intermediaries, while unhosted wallets operate in an architecture with
 29 no application points, no KYC anchor and no custodial supervision.

30 From this perspective, the different implementation of the Travel Rule also
 31 implies that, while regulatory flexibility would allow individual jurisdictions to
 32 adopt preventive and control measures proportionate to their regulatory and
 33 financial context, regulatory fragmentation hinders and discourages the use of
 34 unhosted wallets, as differences in requirements between jurisdictions create
 35 uncertainty for users and for VASPs themselves.

36 For example, in transactions involving different jurisdictions, there are
 37 problems with the fact that, for instance, not all countries have a structured
 38 verification system like Switzerland. One example is the experience in the UK,
 39 where VASPs face many practical difficulties in identifying information to be
 40 included in transactions and even if the client can provide it, there is no guarantee
 41 that it will be reliable.

42 These regulatory differences also generate a mechanism of discrimination
 43 between non-custodial and custodial wallets: in transactions involving the
 44 former, an intermediary could incur higher costs than those required for a
 45 custodial wallet, especially in cases where additional requirements are applied
 46 compared to those proposed by the FATF. As the European Parliament stated in

2023, all this has the natural consequence of discouraging interaction with private or non-custodial wallets, precisely to avoid legal risks and incur suspicious transactions. Indeed, starting in 2027, the regulatory landscape will change significantly. The recently adopted anti-money laundering regulation (Regulation 2024/1624/EU) will prohibit obliged entities (including CASPs) from maintaining commercial relationships involving anonymous wallets, also prohibiting the provision of services relating to coins that improve privacy.

In contrast, supporters of decentralization point out that unhosted wallets are an essential pillar of the blockchain philosophy, as they allow users to retain full control over their funds without having to rely on third parties. Some have argued that these wallets promote social and economic dynamics, precisely because they do not require intermediaries to function, thus embodying the essence of decentralized technology.

The difficulty in regulating them poses a significant compliance challenge. This is precisely why the authorities have focused on hosted wallets and operators that facilitate users' interactions. Supporters of private wallets, however, dispute the authorities' claims regarding the risks and regulatory complexity of unhosted wallets, arguing that such arguments could lead to unjustified stigmatization and erroneous or unfounded conclusions about their use and purpose.

The anonymity of unhosted wallets is often cited as one of the main risks in implementing anti-money laundering and fraud regulations. Indeed, the presence of tools that conceal the origin and destination of operations makes it difficult to trace flows, hindering the detection of suspicious activities and the application of appropriate customer verification procedures.

Yet, this is an intrinsic feature of the blockchain: what distinguishes private wallets is not so much anonymity but the use of pseudonyms, which represent the first level of privacy protection for the user. The level of protection diminishes once the user interacts with a regulated intermediary, increasing the risk of data collection and potential unlawful use. Thus, the use of unhosted wallets does not substantially change the situation nor introduce any additional risks compared to other digital tools on the market.

However, the absence of a central authority involves a trade-off between privacy and traceability: while these wallets guarantee data confidentiality, they reduce the ability to monitor and track transactions. Cryptocurrency transactions remain public but pseudonymized, which still allows authorities to track financial flows. This is particularly useful in custodial-to-non-custodial wallet transactions, where the KYC data of the custodial provider can be linked to on-chain transactions.

The debate between control and privacy protection remains open and continues to influence regulatory strategies aimed at collecting information on cryptocurrency users. Supporters of private wallets also argue that the risk associated with these transactions is often overestimated: advanced tools, such as blockchain analytics solutions, can still effectively trace information without compromising the security of the system. (Elliptic, 2022). Furthermore, restricting the use of anonymity or privacy coins projects could push users towards less regulated platforms or more permissive jurisdictions, complicating

oversight. The experience of ICOs and DeFi protocols relocating to countries such as Singapore after the U.S. crackdown has shown that a similar trend could also emerge for decentralised and privacy-centric projects.

Finally, self-hosted wallets also pose an arbitrage risk. By maintaining full control without intermediaries and operating outside the supervision of obligated entities, some users may exploit market discrepancies for economic gain, potentially undermining the regulatory consistency efforts promoted by the FATF.

In conclusion, these practical implications show that the core difficulty in regulating unhosted wallets does not lie in their technical features, but in the structural misalignment between regulatory objectives and the decentralised nature of the instruments. The regulatory framework thus outlined results in an uneven and sometimes inconsistent application of the travel rule, resulting in uneven compliance burdens and a high rate of regulatory uncertainty, without this resulting in an actual increase in the levels of traceability of operations. The result is an overall inefficient structure, in which the regulatory effort appears not proportionate to the real risk surface. From this perspective, it is preferable to avoid merely analogical extensions of models designed for hosted wallets to unhosted wallets, instead developing regulatory frameworks that reflect their specific technical and functional characteristics.

Conclusions

Regulatory heterogeneity raises questions about the future of the cryptocurrency industry in the EU and whether companies would prefer to move their operations to more accommodating jurisdictions. This has the natural consequence that the application of the Travel Rule and, in general, the anti-money laundering legislation could lead to a transfer of companies to countries with more favourable regulations, thereby reducing compliance costs. Therefore, there is a need for empirical research that explores how regulatory divergence between jurisdictions affects market innovation, startup location and technology development, especially in blockchain applications that preserve privacy. Future studies could investigate real-world compliance costs and operational frictions faced by VASPs when dealing with transactions involving unhosted wallets, particularly in cross-border scenarios. Interviews with compliance officials or surveys of cryptocurrency exchanges could provide valuable data.

The fact that unhosted wallets represent a blind spot in regulation is a significant limitation to the progress of a fully decentralized financial ecosystem. In this perspective, it is necessary to ask whether, since self-hosted P2P wallets represent one of the clearest expressions of the disintermediated architecture underlying crypto-assets, we should compromise this opportunity and what could happen if we decide to preserve it. The regulatory framework on unhosted wallets remains, unfortunately, very controversial. A deeper investigation into how the FATF guidelines are interpreted and transformed into binding rules by different jurisdictions would help to clarify the mechanisms of diffusion and

1 resistance of soft law. Comparative studies on regulatory convergence in the
2 cryptographic space are particularly relevant.

3 Regardless of whether these wallets are used to carry out illegal activities,
4 there is no way to enforce the rules set by the AML discipline against unhosted
5 wallets. Experts seem to argue that one of the most immediate and paradoxical
6 consequences could be to refuse the use of custodial wallets and adopt unhosted
7 wallets, avoiding having to distinguish between users who can and cannot make
8 transactions, for example because they fail to complete the verification process
9 or because the transactions have been delayed in processing by intermediaries.

10 Overall, the analysis shows that the regulatory debate over unhosted wallets
11 is still framed within categories that belong to an intermediary financial system.
12 If supervisory regimes continue to assume the presence of a controllable entity,
13 the regulation of unhosted wallets will remain conceptually misaligned with the
14 architecture of decentralized networks. The main challenge is therefore not the
15 absence of compliance tools, but the persistence of a regulatory logic that
16 presupposes centralization even though decentralization is a feature, not a flaw.
17 A coherent regulatory framework must instead start from the technical reality of
18 self-hosted wallets and design obligations compatible with it, rather than
19 adapting decentralized tools to models designed for custodial infrastructures.

20 In conclusion, this work suggests that to address fragmentation, it is
21 necessary to adopt a multilevel strategy based on: the adoption of a uniform
22 threshold to reduce regulatory arbitrage; the use of protocols such as Zero
23 Knowledge Proof or proof of ownership; and the creation of regulatory
24 sandboxes to test innovative compliance models. The purpose of this strategy is
25 to reconcile AML goals with innovation and privacy, while promoting a more
26 competitive and resilient crypto ecosystem.

27 28 29 **References**

- 30
31 Barbera, V. (2023) 'La Travel Rule Regulation e regolamentazione degli unhosted wallet', in
32 Furnari, S.L. (ed.) *La Finanza Decentralizzata. Cripto-attività, protocolli, questioni*
33 *giuridiche aperte*. pp. 261–265.
34 Barczentewicz, M. (2022), 'Regulatory compliance for crypto by relying on on-ramping
35 services. Available at: <https://ssrn.com/abstract=4068101>
36 Barbereau, T. and Bodó, B., (2023), 'Beyond financial regulation of crypto-asset wallet
37 software: In search of secondary liability. Interdisciplinary Centre for Security,
38 Reliability and Trust (SnT), University of Luxembourg and Institute for Information Law
39 (IViR), University of Amsterdam.
40 Beleuz Neagu, S., (2022) 'A Sharp Turn Towards Crypto-Surveillance: Analyzing
41 Implications of the EU's Revised Transfer of Funds Regulation', *European Union*
42 *Law Working Papers*, no. 64, pp. 1-68.
43 Caribbean Financial Action Task Force (2024). 'FATF Recommendation 16: Wire
44 Transfers'. Available at: [https://cfatf-gafic.org/index.php/documents/fatf-40r/382-](https://cfatf-gafic.org/index.php/documents/fatf-40r/382-fatf-recommendation-16-wire-transfers)
45 [fatf-recommendation-16-wire-transfers](https://cfatf-gafic.org/index.php/documents/fatf-40r/382-fatf-recommendation-16-wire-transfers) (Accessed: 14 December 2024).
46 Crystal Intelligence (2022). *The Travel Rule: hosted vs unhosted crypto wallets*, Crystal
47 Blockchain. Available at: [https://crystalintelligence.com/crypto-regulations/the-](https://crystalintelligence.com/crypto-regulations/the-travel-rule-hosted-vs-unhosted-crypto-wallets/)
48 [travel-rule-hosted-vs-unhosted-crypto-wallets/](https://crystalintelligence.com/crypto-regulations/the-travel-rule-hosted-vs-unhosted-crypto-wallets/) (Accessed: 14 December 2024).

- 1 Crypto Regulations (2022) ‘The Travel Rule: Hosted vs Unhosted Crypto Wallets’.
- 2 Available at: [https://www.cryptoregulations.com/the-travel-rule-hosted-vs-unhost](https://www.cryptoregulations.com/the-travel-rule-hosted-vs-unhosted-wallets)
- 3 [ed-wallets](https://www.cryptoregulations.com/the-travel-rule-hosted-vs-unhosted-wallets) (Accessed: 14 December 2024).
- 4 Crypto Valley Journal (2024) ‘Unhosted Wallets Regulations: Crypto Exchanges and
- 5 Banks Should Know’. Available at: [https://cryptovalleyjournal.com/focus/legal-an](https://cryptovalleyjournal.com/focus/legal-and-compliance/unhosted-wallets-regulations-crypto-exchanges-and-banks-should-know/)
- 6 [d-compliance/unhosted-wallets-regulations-crypto-exchanges-and-banks-should-](https://cryptovalleyjournal.com/focus/legal-and-compliance/unhosted-wallets-regulations-crypto-exchanges-and-banks-should-know/)
- 7 [know/](https://cryptovalleyjournal.com/focus/legal-and-compliance/unhosted-wallets-regulations-crypto-exchanges-and-banks-should-know/) (Accessed: 14 December 2024).
- 8 European Crypto Initiative (2025) The AML Handbook. A guide for crypto activities.
- 9 Available at: <https://www.fscmauritius.org/en/aml/amlcft/aml-cft-handbook>
- 10 European Parliament (2023) Resolution of 20 April 2023 on the regulation of crypto-
- 11 assets. Available at: [https://www.europarl.europa.eu/doceo/document/TA-9-2023-](https://www.europarl.europa.eu/doceo/document/TA-9-2023-0118_IT.html)
- 12 [0118_IT.html](https://www.europarl.europa.eu/doceo/document/TA-9-2023-0118_IT.html) (Accessed: 14 December 2024).
- 13 European Parliament (2024) Report on the Proposal for a Regulation of the European
- 14 Parliament and of the Council on Information Accompanying Transfers of Funds
- 15 and Certain Crypto-assets. Available at: <https://www.europarl.europa.eu> (Accessed: 14
- 16 December 2024).
- 17 Financial Action Task Force (2016) Guidance for a Risk-based approach for Money or
- 18 value transfer services, FATF, Paris.
- 19 Financial Action Task Force (2019) Guidance for a Risk-Based Approach to Virtual
- 20 Assets and Virtual Asset Service Providers.
- 21 Financial Action Task Force (2020) FATF Report: Virtual Assets Red Flag Indicators of
- 22 Money Laundering and Terrorist Financing, September, p. 13. Available at:
- 23 [https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-](https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf)
- 24 [Red-Flag-Indicators.pdf](https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf).
- 25 Financial Action Task Force (2021). Updated Guidance for a Risk-Based Approach to
- 26 Virtual Assets and Virtual Asset Service Providers, October, p. 65. Available
- 27 at: [https://www.fatfgafi.org/publications/fatfrecommendations/documents/guidanc](https://www.fatfgafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html)
- 28 [e-rba-virtual-assets-2021.html](https://www.fatfgafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html).
- 29 FinCEN (2019) Application of FinCEN’s Regulations to Certain Business Models
- 30 Involving Convertible Virtual Currencies. Available at: [https://www.fincen.gov/](https://www.fincen.gov/sites/default/files/2019)
- 31 [sites/default/files/2019](https://www.fincen.gov/sites/default/files/2019) (Accessed: 14 December 2024).
- 32 FINMA (2019). FINMA guidance: stringent approach to combating money laundering
- 33 on the blockchain. [online] 26 agosto. Available at: [https://www.finma.ch/en/news](https://www.finma.ch/en/news/2019/08/20190826-mm-kryptogwg/)
- 34 [/2019/08/20190826-mm-kryptogwg/](https://www.finma.ch/en/news/2019/08/20190826-mm-kryptogwg/).
- 35 Franza, E. (2024) ‘La regolamentazione dei cripto-asset: MiCA, un primo passo’, *Diritto*
- 36 *Bancario*. Available at: [https://www.dirittobancario.it/art/la-regolamentazione-dei-](https://www.dirittobancario.it/art/la-regolamentazione-dei-cripto-asset-mica-un-primo-passo/)
- 37 [cripto-asset-mica-un-primo-passo/](https://www.dirittobancario.it/art/la-regolamentazione-dei-cripto-asset-mica-un-primo-passo/).
- 38 Gandolfi, L. (2024) ‘Cripto-asset e intermediari vigilati: una guida per progettare e
- 39 presentare un piano AML volto a mitigare efficacemente i rischi’, in Annunziata, F. and
- 40 Varani, D. (eds.) *Criptoattività. Antiriciclaggio e gestione dei rischi aziendali*. pp. 51ss.
- 41 Lazar, R.E. (2025) ‘Impact of Regulation 2023/1114 on the Maturity of the Crypto-
- 42 assets Market in the European Union’, *Athens Journal of Law*, 11(3), pp. 323-336.
- 43 Ledger SAS (2024) ‘Response to the European Banking Authority’s consultation paper
- 44 on its Guidelines on preventing the abuse of funds and certain crypto-assets
- 45 transfers for money laundering and terrorist financing (ML/TF) purposes under
- 46 Regulation 2023/1113, Paris. Available at: [https://www.eba.europa.eu/eba-respo](https://www.eba.europa.eu/eba-response/73591?destination=/publications-and-media/events/consultation-guidelines-preventing-abuse-funds-and-certain-crypto)
- 47 [nse/73591?destination=/publications-and-media/events/consultation-guidelines-](https://www.eba.europa.eu/eba-response/73591?destination=/publications-and-media/events/consultation-guidelines-preventing-abuse-funds-and-certain-crypto)
- 48 [preventing-abuse-funds-and-certain-crypto](https://www.eba.europa.eu/eba-response/73591?destination=/publications-and-media/events/consultation-guidelines-preventing-abuse-funds-and-certain-crypto).
- 49 Lee, C., Kang, C., Choi, W., Lee, J., Cha, M., Woo, J. and Hong, J.W.K. (2022) ‘Design of
- 50 blockchain-based Travel Rule compliance system. Proceedings of the 2022 IEEE
- 51 International Conference [online]. IEEE. Available at: <https://doi.org/10.1109>.

- 1 KPMG (2024). The Travel Rule - Transfer of Crypto Assets in Germany and the European
2 Union. KPMG AG Wirtschaftsprüfungsgesellschaft, April, p. 2. Available at: [https://](https://www.recht.bund.de)
3 www.recht.bund.de.
- 4 Ragha, M. and Ballon Ossio, D.(2021), '*Unravelling the Travel Rule: AML requirements*
5 *for cryptoasset businesses*', Butterworths Journal of International Banking and
6 Financial Law, December 2021, pp. 784–786.
- 7 Sicignano, G.J. (2021) 'Money Laundering using Cryptocurrency: The Case of Bitcoin!',
8 Athens Journal of Law, 7 (2), pp. 253-264.
- 9 Soana, G. (2024) 'The Anti-money laundering compliance duties: same old, same old?',
10 in The Anti-money Laundering Regulation of Crypto Assets in Europe. Milano,
11 Italy: Wolters Kluwer Italia, p. 212.
- 12 Takei, Y. and Shudo, K. (2024) 'FATF Travel Rule's Technical Challenges and Solution
13 Taxonomy', Proceedings of [conference or journal, if known], Mercari, Inc. and
14 Tokyo Institute of Technology / Kyoto University, pp. 1-16.
- 15 TLP Advisors. (2025, 2 giugno). EU vs. Crypto Anonymity: What You Need to Know.
16 Tech Law & Policy. Available at: [https://techlawpolicy.com/2025/06/eu-vs-crypto-](https://techlawpolicy.com/2025/06/eu-vs-crypto-anonymity-what-you-need-to-know/)
17 [anonymity-what-you-need-to-know/](https://techlawpolicy.com/2025/06/eu-vs-crypto-anonymity-what-you-need-to-know/).
- 18 U.S. Department of the Treasury (2020) Requirements for Certain Transactions Involving
19 Certain Convertible Virtual Currency or Digital Assets—FAQs, 18 December.
20 Available at: <https://home.treasury.gov/system/files/136/2020-12-18-FAQs.pdf>
- 21 U.S. Federal Register (2020) Requirements for Certain Transactions Involving Virtual
22 Currency or Digital Assets, 85 Fed. Reg. 83840. Available at: [https://www.federal](https://www.federalregister.gov/documents/2020/12/23/2020-28437)
23 [register.gov/documents/2020/12/23/2020-28437](https://www.federalregister.gov/documents/2020/12/23/2020-28437).
- 24 21Analytics, (2024) 'Address Ownership Proof of Protocol (AOPP)'. Available at:
25 <https://aopp.group/>.
- 26 21Analytics (2023) 'European Union's Travel Rule: Embracing technology for the
27 Transfer of Funds Regulation'. EYGM Limited, pp. 1-9. Available at: [https://www.](https://www.21analytics.ch/eu-travel-rule-tfr-ey/)
28 [21analytics.ch/eu-travel-rule-tfr-ey/](https://www.21analytics.ch/eu-travel-rule-tfr-ey/).