Journal of Economic Criminology 7 (2025) 100131

Contents lists available at ScienceDirect

Journal of Economic Criminology

journal homepage: www.journals.elsevier.com/journal-of-economic-criminology

# Who constitute the VASPs in DeFi? A case study on money laundering via cross-chain bridge from the 2022 harmony hack

Yuyun Ma

*School of Law and Politics, Cardiff University, CF10 3DY, United Kingdom*

## 1. Introduction

The decentralized nature[1] of DeFi has led to a 1964 % year-over-year increase in total value received from illicit addresses,[2] exacerbated by tools like privacy coins and mixers.[3] This poses significant challenges for anti-money laundering (AML) regulation.[4] Notably, there has been a decline in funds sent to mixers, with cross-chain bridges emerging as popular alternatives, reaching $743.8 million in 2023.[5] In response, the Financial Action Task Force (FATF) has published several interpretive notes and updated guidance on virtual asset service provider (VASPs).

In October 2018, the FATF adopted a new definition regarding VASPs and updated Recommendation 15.[6] The FATF also introduced Recommendations targeting DeFi, identifying 'creators, owners and operators or some other persons who maintain control or sufficient influence in the DeFi arrangements' as VASPs.[7] The Recommendations will also apply to VASPs 'regardless of the additional services that the platform potentially incorporates (such as a mixer or tumbler or other potential features for obfuscation)'.[8]

Albeit these efforts, jurisdictions are making limited progress in implementing these requirements on VASPs.[9] Challenges have arisen in a number of jurisdictions in identifying VASPs, and further guidance should be provided for registration and licensing.[10] According to the FATF's survey, 77 % of jurisdictions have not successfully identified any unregistered/unlicensed DeFi entities as VASPs.[11] FATF has acknowledged the challenges in identifying specific natural or legal persons responsible for VASP obligations in DeFi arrangements,[12] especially with the incorporation of obfuscation tools.

Existing literature on DeFi regulation primarily focuses on regulatory challenges,[13] compliance and risk management,[14] and comparison to traditional finance.[15] However, there is a gap regarding specific regulatory considerations for DeFi as VASPs under the FATF Recommendations. This article aims to address this gap by assessing the effectiveness of current regulatory approaches in mitigating money

*E-mail address:* MaY79@cardiff.ac.uk.

[1] Igor Makarov and Antoinette Schoar, 'Cryptocurrencies and Decentralized Finance (DeFi)' (2022) BIS Working Paper 12/2022, 1061 < https://www.bis.org/publ/work1061.htm > Accessed 28th April 2024

[2] Chainalysis, *The 2024 Crypto Crime Report: The latest trends in ransomware, scams, hacking, and more* (2024)

[3] United Nation, 'Money Laundering Through Cryptocurrencies' https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/launderingproceeds/moneylaundering.html Accessed 28th April 2024

[4] Igor Makarov and Antoinette Schoar, 'Cryptocurrencies and Decentralized Finance (DeFi)' (2022) BIS Working Paper 12/2022, 1061 < https://www.bis.org/publ/work1061.htm > Accessed 28th April 2024

[5] Chainalysis, *The 2024 Crypto Crime Report: The latest trends in ransomware, scams, hacking, and more* (2024)

[6] FATF, '12-Month Review of the Revisited FATF Standards on Virtual Assets/VASPS' (2020)

[7] FATF, 'Updated Guidance for a Risk-based Approach: Virtual Assets and Virtual Asset Service Providers' (2021)

[8] FATF, 'Updated Guidance for a Risk-based Approach: Virtual Assets and Virtual Asset Service Providers' (2021)

[9] FATF, 'Virtual Assets: Targeted \update on Implementation of the FATF Standards' (2023)

[10] FATF, '12-Month Review of the Revisited FATF Standards on Virtual Assets/VASPS' (2020)

[11] FATF, 'Virtual Assets: Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset' (2024)

[12] FATF, 'Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset' (2023)

[13] For example, Vladlena Benson et al. published a paper 'Dark Side of Decentralised Finance: A Call for Enhanced AML Regulation based on use Cases of Illicit Activities'. It offers valuable insight into the regulatory challenges presented by DeFi.

[14] For example, Suzana Mesquita de Borba Maranhão Moreno and Jean-Marc Seigneur published a paper 'Enabling KYC and AML Verification in DeFi Services'. It proposes an approach to comply with KYC/AML regulations supporting self-hosted wallets, empowering users to voluntarily comply by selecting the most suitable compliance analysis provider when participating in regulated use cases and to take more informed decisions considering the intrinsic risks of their own transactions.

[15] For example, Katrin Schuler et al. published a paper 'On DeFi and On-Chain CeFi: How (Not) to Regulate Decentralized Finance'. It analyses blockchain-based financial infrastructure and provides policymakers and regulators with a tool to identify the differences between truly independent, neutral infrastructure and fake decentralization.

https://doi.org/10.1016/j.jeconc.2025.100131
Received 22 August 2024; Received in revised form 2 February 2025; Accepted 5 February 2025

laundering risks associated with DeFi, particularly cross-chain bridges. By analyzing specific natural or legal persons responsible for VASP obligations within DeFi arrangements, this study contributes to the literature on DeFi regulation.

## 2. Method

This study employed the case study method to evaluate the effectiveness of FATF's Recommendations in mitigating money laundering risks associated with DeFi. Specifically, this study applied FATF's DeFi-relevant recommendations to identify who constitutes the VASPs in two cross-chain bridge protocols involved in the 2022 Harmony Hack money laundering case. By focusing on these specific instances, the research aims to provide detailed insights into the practical application and challenges of FATF's guidelines within the DeFi ecosystem.

## 3. Results

This study highlights the challenges in identifying legal and natural persons as VASPs for bridge protocols 1 and 2 due to limited information and vagueness in FATF Recommendations. While the Recommendations are non-binding and broadly explanatory,[16] ensuring correctness, clarity, and understandability is essential. Issues identified are summarized below.

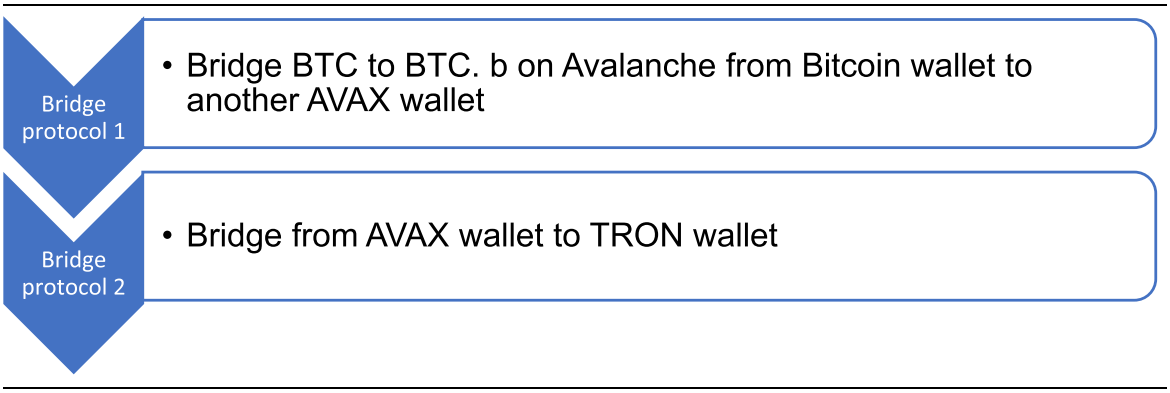
Firstly, FATF's oversight of complex organizational structures renders the Recommendations impractical. VASP identification should align with the business scope of the corresponding legal or natural persons. The oversight of DeFi platforms comprising multiple subsidiaries with varied business activities complicates VASP identification. If the Avalanche and Defiway bridges operate under a single legal entity, it may not be classified as a VASP. Additionally, when multiple VASPs exist within a platform incorporating obfuscation tools, determining VASP obligations may result in excessive punishment during legal enforcement.

Secondly, distinguishing between owners/operators and other influential parties in DeFi arrangements requires clarification. Ambiguity surrounds the definitions of ownership, management, and governance rights conferred by tokens. While Defiway lacks identified individuals with control or influence, the absence does not negate the existence of owner/operators. Clarification is needed on the parameters defining control and significant influence. Moreover, if ownership, management, and token governance rights are justified, owners/operators may not be identical to other influential parties. Exploring the distinction between owners as responsibility bearers and operators as obligation conductors could offer a practical and cost-effective solution. Additionally, FATF oversimplifies the complexity of the decentralization of DeFi arrangements by putting more emphasis on centralized elements and deeming that centralized operations may be regarded as VASPs.[17] How the decentralized elements operate should be further explored.

## 4. Discussion

### 4.1. Case introduction and FATF's relevant definition as a VASP

The 2022 Harmony hack involved the theft of approximately US $103.7 million worth of Ethereum and various tokens in 12 transactions. The stolen funds were laundered through a complex process, including fragmentation and transacting through Tornado Cash and Railgun,[18] before being converted and withdrawn on the Bitcoin blockchain. Subsequently, they were transferred cross-chain to Avalanche and bridged to the TRON blockchain.[19] This layering[20] process[21] utilized mixers, privacy services, intermediary addresses, cross-chain transfers, and Ethereum contracts to obscure the funds' origins.[22] The list below shows the detailed content regarding the two cross-chain bridges employed in 2022 Harmony hack money laundering:




(Chainalysis'; 2024 Crypto Crime Report)

Cross-chain interoperability has become a crucial aspect and an additional layer of complexity in DeFi[23]. Hiding illicit money via cross-chain bridges refers to transferring digital assets from one blockchain to

[16] FATF, 'Updated Guidance for a Risk-based Approach: Virtual Assets and Virtual Asset Service Providers' (2021)

[17] FATF, 'Virtual Assets: Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset' (2024)

[18] Big Investigations, 'Harmony's Horizon Bridge Exploit: A Crypto Money Laundering Case Study' (23 March 2023) < https://blockchaingroup.io/harmonys-horizon-bridge-exploit-a-crypto-money-laundering-case-study/ > Accessed 28th April 2024

[19] Chainalysis, The 2024 Crypto Crime Report: The latest trends in ransomware, scams, hacking, and more (2024).

[20] Nicholas Ryder et al., 'The United Kingdom, Organised Crime, and Money Laundering' in Dan Jasinski et al. (eds), Organised Crime, Financial Crime, and Criminal Justice (Routledge 2023).

[21] Big Investigations, 'Harmony's Horizon Bridge Exploit: A Crypto Money Laundering Case Study' (23 March 2023) < https://blockchaingroup.io/harmonys-horizon-bridge-exploit-a-crypto-money-laundering-case-study/ > accessed 28th April 2024.

[22] Raphael Auer et al., 'The Technology of Decentralized Finance (DeFi)' (2023) BIS Working Papers 1/2023, 1066 < https://www.bis.org/publ/work1066.htm > accessed 28th April 2024.

[23] Vladlena Benson et al., 'Dark Side of Decentralized Finance: A Call for Enhanced AML Regulation Based on Use Cases of Illicit Activities' (2023) 32 (1) Journal of Financial Regulation and Compliance < https://www.emerald.com/insight/content/doi/10.1108/JFRC-04-2023-0065/full/html > accessed 28th April 2024.

another, intending to hide the origin or destination of the funds.[24] There has been a significant increase in the volume of funds sent to blockchain bridges from addresses associated with stolen funds, reaching $743.8 million in cryptocurrency from illicit addresses in 2023, up from just $312.2 million in 2022. Accordingly, there is an urgent need to study the current regulations addressing the challenges posed by cross-chain bridge money laundering. The investigation in Part 4.2 will focus on the two cross-chain bridges employed in the 2022 Harmony hack money laundering, as mentioned above.

Moreover, the FATF Recommendations stipulate that financial services provided by DeFi must align with the businesses listed under the VASP definition. Marketing terms or self-identification as DeFi are not decisive, nor is the specific technology involved in determining VASP status for owners or operators.[25] The determination of DeFi status should adhere to FATF's definition. Furthermore, AML regulations encompass covered VA activities and VASPs, regardless of additional services like mixers or tumblers for transaction obfuscation.[26] This means that even if platforms offer such features, AML regulations still apply. The list[27] below outlines the process for identifying VASPs regulated by FATF and aids in identifying VASP conducted in Part 4.2.

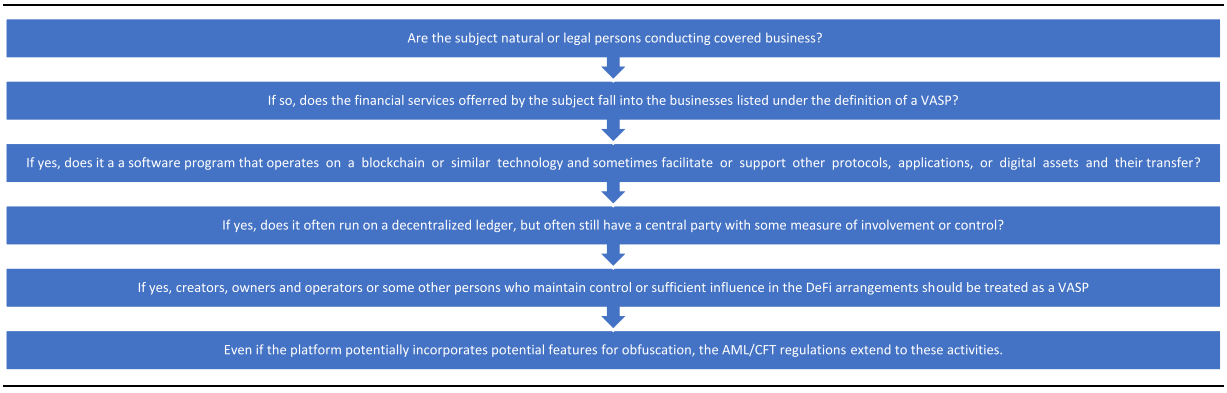
| | |
|---|---|
| Creators | The creation of software applications does not make the creator a VASP, unless it conducts the covered business mentioned in the definition of VASP[a]. |
| Distinguish owners/operators and some other persons who maintain control or sufficient influence in the DeFi arrangements | • Via their relationship to the activities being undertaken. These relationships include control or sufficient influence over assets or over aspects of the service's protocol, and the existence of an ongoing business relationship between themselves and users even if through a smart contract or in some cases voting protocols[b].<br>• Judging 'whether any party profits from the service or can set or change parameters[c].<br>• If it has not been possible to identify a legal or natural person with control or sufficient influence over a DeFi arrangement, there may not be a central owner/operator that meets the definition of a VASP[d]. |

aFATF, 'Updated Guidance for a Risk-based Approach: Virtual Assets and Virtual Asset Service Providers' (2021).

bFATF, 'Updated Guidance for a Risk-based Approach: Virtual Assets and Virtual Asset Service Providers' (2021).

cFATF, 'Updated Guidance for a Risk-based Approach: Virtual Assets and Virtual Asset Service Providers' (2021).

dFATF, 'Updated Guidance for a Risk-based Approach: Virtual Assets and Virtual Asset Service Providers' (2021)




The challenge is to identify specific natural or legal persons responsible for VASP obligations in DeFi arrangements. Namely, the regulation of "creators, owners, and operators, or some other persons who maintain control or sufficient influence in the DeFi arrangements"[28] as VASPs should be clarified in application. The form below lists the relevant FATF Recommendations regarding creators, owners, and operators, or some other persons who maintain control or sufficient influence in the DeFi arrangements. These recommendations will also be applied to the case investigation and analysis in Part 4.2.

### 4.2. Investigation and analysis: who qualify as VASPs?

#### 4.2.1. The bridge protocol 1

The investigation into the Avalanche platform reveals that the Avalanche Bridge facilitates the activities in question.[29] The FATF recommends applying AML regulations to covered VA activities and VASPs, regardless of additional services such as mixer or tumbler that the platform may incorporate.[30] However, this recommendation does not consider the complicated corporate structure typically designed by technology companies. Corporate groups generally mitigate risk by establishing subsidiaries, each operating independently within its own legal framework.[31] Under this model, multiple subsidiaries may qualify as VASPs. If the bridge is run by a sole subsidiary, determining which VASP assumes the VASP obligation becomes crucial.

[24] Chainalysis, The 2024 Crypto Crime Report: The latest trends in ransomware, scams, hacking, and more (2024).

[25] FATF, 'Updated Guidance for a Risk-based Approach: Virtual Assets and Virtual Asset Service Providers' (2021)

[26] FATF, 'Guidance for a Risk-based approach: Virtual Assets and Virtual Asset Service Providers' (2019)

[27] This list is summarized from FATF's recommendation 'Updated Guidance for a Risk-based Approach: Virtual Assets and Virtual Asset Service Providers' (2021)

[28] FATF, 'Updated Guidance for a Risk-based Approach: Virtual Assets and Virtual Asset Service Providers' (2021).

[29] According to the Avalanche website, the conversion of BTC on Bitcoin into BTC.b on Avalanche is only possible through Core extension, Core mobile (iOS and Android), and Core web. The Avalanche Bridge facilitated the bridging and swapping of BTC to BTC.b using trusted technology.

[30] FATF, 'Guidance for a Risk-based approach: Virtual Assets and Virtual Asset Service Providers' (2019)

[31] Sharon Belenzon *et al.*, 'Managing risk in corporate groups: Limited liability, asset partitioning, and risk compartmentalization' (2023) 44 (12) Strategic Management Journal https://onlinelibrary.wiley.com/doi/full/10.1002/smj.3531 Accessed 28 April 2024

In this case, AVA Labs and its affiliates are recognized as the creators[32] and developers[33] of Avalanche, with Avalanche (BVI) Inc. holding the Avalanche wallet.[34] This suggests that the Avalanche Bridge may be operated by a sole subsidiary. If this is the case, AVA Labs, its affiliates, and the Avalanche (BVI) Inc. could be regarded as VASPs and fall under AML regulations. the Avalanche whitepaper outlines governance parameters,[35] indicating that AVA Labs and its affiliates likely exert significant influence over the ecosystem. That means that the three entities should share the VASP obligations.

However, this investigation was unable to obtain the internal decision-making model and corporate structure. It is likely that various resources are highly overlapping among different companies under the same parent company. In this situation, the effectiveness of legal enforcement - determining who should share the ultimate obligation while avoiding excessive punishment and ensuring proportionality - should be taken into account. Although the FATF's recommendation merely provides general guidance to different jurisdictions, with further application to be detailed by those jurisdictions, the points identified in this case could still be considered by the FATF and jurisdictions to further refine the identification of VASPs.

#### *4.2.2. The bridge protocol 2*

Further investigation reveals that Avalanche and TRON do not directly facilitate a bridge service between their blockchains. Instead, third-party service providers like Defiway enable the cross-chain bridge of USDT from Avalanche to the TRON blockchain. Delving into Defiway's organizational structure poses challenges compared to Avalanche's. For example, Defiway operates four decentralized products, each is a blockchain startup requiring decisions for growth and development.[36] However, it remains unclear whether these startups constitute legal entities, potentially exempting the Defiway bridge from FATF's VASP definition.

Moreover, Defiway employs a highly automated decentralized governance model, granting DEFI token holders decision-making authority over utilities, fees, products, and network choices.

The FATF has recognized that some 'DeFi arrangements are decentralized in name only and there are persons, entities or centralized elements that may be subject to the FATF requirements as VASPs in many cases'.[37] However, the FATF's recognition is oversimplified and does not distinguish the detailed tasks assigned to DeFi token holders' decision-making authority and the centralized operational processes.

Furthermore, although token allocation involves various entities, including developers and the treasury, the exact quantities are uncertain, complicating the identification of a specific individual with control or influence over Defiway. The FATF Recommendation stipulates that if a legal or natural person with control or sufficient influence cannot be identified, there may not be a central owner/operator.[38] This raises an issue, as under the traditional corporate model, granting DeFi token holders decision-making power equates to owners delegating authority while retaining ownership. However, decision-making is limited to specific areas, suggesting that owners/operators may still exist. Additionally, exploring the distinction between owners as responsibility bearers and operators as obligation conductors could offer a practical and cost-effective solution. Operators, responsible for DeFi protocol management and regulatory compliance, such as KYC,[39] could assume VASP obligations.

## 5. Conclusion

The decentralized nature of DeFi has introduced novel challenges for AML regulation, particularly concerning VASPs involved in cross-chain bridge businesses. Despite efforts by the FATF to regulate DeFi, pinpointing challenges in identifying specific natural or legal persons responsible for VASP obligations within DeFi arrangements remain elusive. The FATF has surveyed the application of FATF's recommendations on VASP identification and highlighted challenges in this area, but further guidance on improvements is scarce.

Through the case study of analyzing two cross-chain bridges transfers in money laundering from the 2022 Harmony hack, the article highlights significant shortcomings and ambiguities in current regulatory frameworks. The investigation reveals that identifying VASPs remains complex due to the intricate organizational structures and governance models prevalent in the ecosystem. When multiple VASPs exist within a platform incorporating obfuscation tools, determining VASP obligations is likely to result in disproportionate punishment in legal enforcement.

Furthermore, the article underscores the need for clarity and refinement in FATF regulations concerning the distinction between owners/operators and other persons with control or influence, as well as clarifying who shares the VASP obligation in situations where owners/operators or other influential parties are involved. Specifically, in decentralized DeFi arrangements involving centralized operational model, the FATF's recognition that DeFi arrangements are decentralized in name only and that centralized elements may be regarded as VASPs[40] is oversimplified. The operation of the decentralized elements operate should be deeply explored.

## CRediT authorship contribution statement

**Yuyun Ma:** Writing – review & editing, Writing – original draft.

## Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

[32] JD Alois, 'Ava Labs, Creator of Avalanche, Partners with Amazon Web Services (AWS)' (January 11, 2023) https://www.crowdfundinsider.com/2023/01/201002-ava-labs-creator-of-avalanche-partners-with-amazon-web-services-aws/ Accessed 28 April 2024

[33] Herman Hayes, 'What is the Avalanche (AVAX) Core Wallet? What is Ava Labs?' (2 May 2023) http:////bitkan.com/learn/what-is-the-avalanche-avax-core-wallet-what-is-ava-labs-12933 Accessed 28 April 2024

[34] Avalanche, 'Avalanche Wallet Terms of Use' (22 September 2020) < http://www.avax.network/avalanche-wallet-terms-of-use > Accessed 28 April 2024

[35] The Avalanche whitepaper specifies that only a predetermined number of parameters can be modified via governance. While Avalanche retains the ability to alter parameters, its impact is restricted, and it is highly probable that AVA Labs and its affiliates own and operate the Avalanche ecosystem.

[36] Defiway, 'Defiway Whitepaper' https://defiway.com/whitepaper-defi-token Accessed 28 April 2024

[37] FATF, 'Virtual Assets: Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset' (2024)

[38] FATF, 'Updated Guidance for a Risk-based Approach: Virtual Assets and Virtual Asset Service Providers' (2021)

[39] Nicholas Ryder et al., 'The United Kingdom, Organised Crime, and Money Laundering' in Dan Jasinski et al. (eds), *Organised Crime, Financial Crime, and Criminal Justice* (Routledge 2023)

[40] FATF, 'Virtual Assets: Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset' (2024)

## Acknowledgements

I would like to express our sincere gratitude to Dr. Nicholas Ryder for his invaluable contributions throughout the course of this research. His expertise and guidance have been instrumental in the development and completion of this article. We also thank our families and colleagues for their unwavering support and encouragement.

## Reference

Chainalysis, The 2024 Crypto Crime Report: The Latest Trends in Ransomware, Scams, Hacking, and More (2024).