# ENDING THE CRYPTO TAX HAVEN

NOAM NOKED*

*There is growing global concern regarding the use of crypto for tax evasion and financial crimes. To address this problem, over sixty jurisdictions have recently committed to implement the Crypto-Asset Reporting Framework (CARF). CARF transposes the Common Reporting Standard (CRS)—designed for the traditional financial industry—onto the crypto industry. Under CARF, certain crypto intermediaries are treated like traditional financial institutions: they must identify and report crypto owners who are tax residents of other jurisdictions.*

*However, CARF is deeply flawed. This Article is the first to systematically analyze alarming loopholes and weaknesses that bad actors may exploit to avoid reporting. First, tax evaders may refrain from using compliant, in-scope intermediaries. The reliance on intermediaries was adopted by CRS for the traditional financial system, but this would have limited success where crypto owners can avoid such intermediaries. Second, as CARF is modeled after CRS, bad actors may circumvent reporting by exploiting loopholes inherited from CRS. Finally, bad actors may exploit vulnerabilities specific to CARF and the crypto industry.*

*As a result, this new international standard will likely fail to shut down the crypto tax haven. Moreover, compliant actors in the crypto industry will incur substantial costs when implementing this cumbersome standard. This Article proposes ways to address several of CARF's main shortcomings. It also suggests measures beyond CARF to enhance transparency and put an end to the crypto tax haven.*

---

* Associate Professor, Faculty of Law, The Chinese University of Hong Kong (noam.noked@cuhk.edu.hk). I thank Zachary Marcone, Omri Marian, Bob Michel, Paul Millen, Vincent Ooi, and Sarah Sonnenfeld for their helpful comments. This Article benefited from insightful feedback received at the Annual Conference of the Tax Research Network, the GREIT Lisbon Summer Course, the International Roundtable on Taxation and Tax Policy, and the UC Irvine Symposium on Taxation, and seminars of the International Fiscal Association Hong Kong Branch and the Hebrew University Faculty of Law. The work described in this article was fully supported by a grant from the Research Grants Council of the Hong Kong Special Administrative Region, China (Project No. CUHK 14609022).

TABLE OF CONTENTS

## Introduction

Crypto has been praised as revolutionary and criticized as a "super tax haven" that enables financial crime.[1] Larry Fink, the CEO of BlackRock—the world's largest asset management firm—described Bitcoin as an "index of money laundering" in 2017.[2] Yet in a remarkable change of tone, Fink recently stated that "crypto could revolutionize finance,"[3] and BlackRock is now working to expand public access to crypto.[4] This Dr. Jekyll and Mr. Hyde description of crypto is particularly intriguing considering that some of the innovative features of crypto—disintermediation, pseudonymity, tamper resistance, and autonomy—increase the risks it poses.[5] Moreover, mass adoption of crypto may increase the risk that crypto might be used for illicit purposes.[6]

Crypto emerged in a period when the United States and the international community increased efforts to curb tax evasion involving the traditional financial industry. Satoshi Nakamoto mined the genesis block of Bitcoin in January 2009.[7] Unrelatedly, a month later, the largest bank in Switzerland entered into a deferred prosecution agreement with the U.S. Department of Justice, under which it had to pay a hefty fine and disclose its U.S. account holders.[8] In April 2009, the G20 declared that "the era of bank secrecy is over."[9] Since then, the United States and other countries have significantly expanded their enforcement efforts against offshore tax evasion.[10] In 2010,

---

[1] *See* Omri Marian, *Are Cryptocurrencies 'Super' Tax Havens?*, 112 Mich. L. Rev. First Impressions 38, 42 (2013).

[2] Fred Imbert, *BlackRock CEO Larry Fink Calls Bitcoin an 'Index of Money Laundering*,' CNBC (Oct. 13, 2017, 2:32 PM), https://www.cnbc.com/2017/10/13/blackrock-ceo-larry-fink-calls-bitcoin-an-index-of-money-laundering.html [https://perma.cc/EU8H-ADXB].

[3] Billy Bambrough, *'Transcend' The U.S. Dollar: BlackRock CEO Issues 'Important' Crypto Prediction After Huge Week for the Bitcoin, Ethereum and XRP Price*, Forbes (July 16, 2023, 7:45 AM), https://www.forbes.com/sites/digital-assets/2023/07/16/transcend-the-us-dollar-blackrock-ceo-issues-important-crypto-prediction-after-huge-week-for-the-bitcoin-ethereum-and-xrp-price/?sh=4e018e601b11 [https://perma.cc/V3WF-LK27].

[4] *See BlackRock Files for Spot Ethereum ETF in Further Crypto Push*, Reuters (Nov. 17, 2023, 12:39 PM), https://www.reuters.com/business/finance/blackrock-woos-investors-ethereum-trust-further-crypto-push-2023-11-16/ [ https://perma.cc/V8TA-KG5N].

[5] *See* James Alm et al., *New Technologies and the Evolution of Tax Compliance*, 39 Va. Tax Rev. 287, 328–32 (2020).

[6] *See* Financial Action Task Force (FATF), *Virtual Assets and Virtual Asset Service Providers*, at 17 (Oct. 2021) [hereinafter FATF Guidance].

[7] *See* Julie Pinkerton, *The History of Bitcoin, the First Cryptocurrency*, U.S. News (Aug. 7, 2023), https://money.usnews.com/investing/articles/the-history-of-bitcoin [https://perma.cc/6EM6-4TNG].

[8] *See* U.S. Dep't of Just., *UBS Enters into Deferred Prosecution Agreement,* (Feb. 18, 2009), https://www.justice.gov/opa/pr/ubs-enters-deferred-prosecution-agreement [https://perma.cc/2ZB6-3NDW].

[9] G20, *London Summit: Leaders' Statement*, at 4 (Apr. 2, 2009), London Summit - Leaders' Statement (02/04/2009) - G7/G20 Documents Database (g7g20-documents.org) [https://perma.cc/HCR4-5R4T].

[10] *See* U.S. Dep't of Just., *Offshore Compliance Initiative*, https://www.justice.gov/tax/offshore-compliance-initiative (last visited Jan. 14, 2025) [https://perma.cc/N8Q5-RE2W].

U.S. Congress enacted the Foreign Account Tax Compliance Act (FATCA), which requires non-U.S. financial institutions (FIs) to identify U.S. persons holding financial accounts and report their account information to the Internal Revenue Service (IRS).[11]

In 2014, a few months after Vitalik Buterin published the Ethereum Whitepaper,[12] the Organisation for Economic Co-operation and Development (OECD) introduced the Common Reporting Standard (CRS).[13] CRS generally applies the FATCA information exchange model on a reciprocal, global basis,[14] and it was quickly adopted by more than a hundred jurisdictions globally. FATCA and CRS have facilitated "the largest exchange of tax information in history."[15] While FATCA and CRS have flaws, these information exchange standards make it riskier and costlier to evade tax by holding offshore financial assets.[16]

Crypto and traditional finance do not play by the same rules. While FATCA and CRS require FIs to report the financial assets they maintain for foreign tax residents, such reporting obligations do not generally apply to crypto assets.[17] Consequently, enhanced transparency for traditional financial assets makes the crypto tax haven more attractive. Part I discusses several technological features of crypto that make it a unique tax haven in addition to this regulatory arbitrage.

To address this problem, the OECD has recently published the Crypto-Asset Reporting Framework (CARF).[18] The European Union (EU) has

---

[11] Hiring Incentives to Restore Employment Act, Pub. L. No. 111-147, §§ 501-35, 124 Stat. 71, 97–115 (2010). The implementation of FATCA started in July 2014.

[12] *See* Vitalik Buterin, *Ethereum Whitepaper*, Ethereum (2014) https://ethereum.org/en/whitepaper/ [https://perma.cc/R8UU-4YRW].

[13] *See* Org. for Econ. Coop. and Dev. (OECD), Standard for Automatic Exchange of Financial Account Information in Tax Matters (2nd ed. 2017) [hereinafter CRS].

[14] *See id.* at 9–12.

[15] *Implementation of Tax Transparency Initiative Delivering Concrete and Impressive Results*, Targeted News Service (June 7, 2019), http://www.paolosoro.it/news/1575/Implementation-of-tax-transparency-initiative-delivering-concrete-and-impressive-results.html [https://perma.cc/P5C4-QL95].

[16] There is evidence indicating that there was a reduction in offshore tax evasion after the introduction of these reporting standards. *See, e.g.*, Lisa de Simone & Bridget Stomberg, *Has FATCA Succeeded In Reducing Tax Evasion Through Foreign Accounts?*, 39 Oxford Rev. Econ. Pol'y 550 (2023); Elisa Casi et al., *Cross-Border Tax Evasion After the Common Reporting Standard: Game Over?*, 190 J. Pub. Econ. 1, 11 (2020). For further analyses of weaknesses and loopholes in FATCA and CRS, see Menusch Khadjavi & Marjolein Vertelman, *Closing Pandora's Box: How to Improve the Common Reporting Standard* (Kiel Inst. World Econ., Working Paper No. 2223, May 2022); Noam Noked, *Tax Evasion and Incomplete Tax Transparency*, 7 Laws 31 (2018); Noam Noked, *FATCA, CRS, and the Wrong Choice of Who to Regulate*, 22 Fla. Tax Rev. 77 (2018); Noam Noked & Zachary Marcone, *International Response to the U.S. Tax Haven*, 48 Yale J. Int'l L. 177 (2023).

[17] The United States has adopted reporting requirements for domestic actors including digital-asset brokers and intermediaries. Pub. L. No. 117-58, 135 Stat. 429. However, these reporting obligations do not generally apply to non-U.S. intermediaries outside the United States.

[18] *See* OECD, *International Standards for Automatic Exchange of Information in Tax Matters: Crypto-Asset Reporting Framework and 2023 Update to the Common Reporting*

already adopted a directive requiring Member States to start implementing CARF in 2026, and the G20 has called for its swift implementation.[19] Over sixty jurisdictions have committed to implement CARF with information exchanges starting by 2027 or 2028.[20] In November 2023, forty-eight countries, including the United States, published a joint statement declaring that they "intend to work towards swiftly transposing the CARF into domestic law and activating exchange agreements in time for exchanges to commence by 2027."[21] Additional jurisdictions subsequently informed the OECD of their intention to implement CARF. To meet this timeline, countries will need to adopt domestic rules by the end of 2025 and start implementation in 2026.[22] Some jurisdictions are expected to carry out the first exchange in 2028, which means that they will need to enact the required legislation in 2026 and start implementation in 2027.[23] As of November 2024, forty-eight jurisdictions have signed the multilateral competent authority agreement for the automatic information exchange pursuant to CARF (CARF MCAA).[24]

With this international support, CARF is poised for widespread adoption. CARF is generally modeled after CRS.[25] As discussed in Part II, CARF treats certain intermediaries in the crypto industry like FIs: they must identify and report foreign tax residents who carry out crypto transactions. One scholar has recently predicted that CARF would be "especially effective in the digital financial market" because "tax reporting requirements are effective at combating money laundering and tax evasion in traditional financial markets, and thus will likely be effective at resolving parallel issues in the digital financial

---

*Standard* (June 8, 2023), https://www.oecd-ilibrary.org/taxation/international-standards-for-automatic-exchange-of-information-in-tax-matters_896d79d1-en [hereinafter CARF].

[19] G20, *New Delhi Leaders' Declaration*, at 27 (Sept. 9-10, 2023), https://www.mea.gov.in/Images/CPV/G20-New-Delhi-Leaders-Declaration.pdf [https://perma.cc/3T3K-KKCN]. *See infra* text accompanying note 92.

[20] OECD, *Global Forum Celebrates 15 Years of Progress and Extends Tax Transparency to the Crypto-Asset Sector* (Nov. 26, 2024), https://web-archive.oecd.org/tax/transparency/documents/global-forum-celebrates-15-years-of-progress-and-extends-tax-transparency-to-the-crypto-asset-sector.htm.

[21] U.S. Dep't of Treas., *Collective Engagement to Implement the Crypto-Asset Reporting Framework,* (Nov. 10, 2023), https://home.treasury.gov/news/press-releases/jy1895 [https://perma.cc/6M6R-PLA9]. It is uncertain at this stage what the Trump administration's position on CARF will be.

[22] OECD, *Joint Statement on the Implementation of the Crypto-Asset Reporting Framework*, https://www.oecd.org/tax/transparency/documents/CARF-signatories-joint-statement.pdf (last visited Jan. 15, 2025).

[23] *See, e.g.*, Government of the Hong Kong Special Administrative Region, *Press Release: Hong Kong Commits to Implementing Crypto-Asset Reporting Framework* (Dec. 13, 2024), https://www.info.gov.hk/gia/general/202412/13/P2024121300491.htm.

[24] OECD, *Signatories of the Multilateral Competent Authority Agreement on Automatic Exchange of Information Pursuant to the Crypto-Asset Reporting Framework: Status as of 26 November 2024*, https://www.oecd.org/content/dam/oecd/en/topics/policy-issues/tax-transparency-and-international-co-operation/carf-mcaa-signatories.pdf/_jcr_content/renditions/original./carf-mcaa-signatories.pdf.

[25] *See infra* Part II.

market."[26] As explained below, this Article makes the opposite prediction: CARF will likely fail to shut down the crypto tax haven.

This Article shows that CARF is deeply flawed. It is the first publication to systematically analyze alarming loopholes and weaknesses that bad actors may exploit to avoid reporting.[27] As discussed in Part III, there are three categories of such vulnerabilities. First, tax evaders may avoid using compliant, in-scope intermediaries. The reliance on intermediaries was adopted by CRS for the traditional financial system. However, this approach would have limited success where crypto owners can avoid such intermediaries. Tax evaders may avoid using intermediaries altogether.[28] They may use intermediaries that have no nexus to CARF-implementing jurisdictions.[29] In addition, they may use out-of-scope intermediaries, such as platforms over which no person has control or sufficient influence. The exclusion of such platforms from CARF's scope creates incentives for crypto projects to decentralize and for bad actors to use decentralized platforms. Alternatively, tax evaders may use noncompliant platforms.[30]

Second, as CARF is modeled after CRS, bad actors may circumvent reporting by exploiting vulnerabilities inherited from CRS itself. The "Active Entity" loophole, discussed in Part III, demonstrates how tax evaders may use private, closely held companies incorporated in tax havens to avoid CARF reporting. Such entities may declare (correctly or falsely) that they are Active Entities. The reporting of the beneficial owners of Active Entities is not required. As a result, bad actors may avoid reporting by exploiting this CRS-inherited loophole.[31]

Third, bad actors may exploit vulnerabilities specific to CARF and the crypto industry. The ability to remotely apply for accounts with many intermediaries may increase the likelihood that bad actors will open accounts by exploiting weaknesses and loopholes.[32] For instance, the limited human involvement and reliance on digitized due diligence procedures may reduce the ability to detect fraud and act based on actual knowledge or suspicion.[33] Additionally, the interactions between an intermediary and crypto owners may be limited to several transactions carried out over a short period, with few opportunities for intermediaries to detect fraud.[34] Finally, the anti-money-laundering

---

[26] Young Ran (Christine) Kim, *Tax Reporting as Regulation of Digital Financial Markets*, 80 WASH. & LEE L. REV. 1181, 1200 (2023).

[27] For a critique concerning other aspects of CARF, see Christopher Ignatius Moylan, *OECD's Proposed Crypto-Asset Reporting Framework (CARF): A Critique* (2022), https://www.diva-portal.org/smash/get/diva2:1664824/FULLTEXT01.pdf [https://perma.cc/5GZU-AYQN].

[28] *See infra* Part III.A.1.

[29] *See infra* Part III.A.2.

[30] *See infra* Part III.A.3.

[31] *See infra* Part III.B.

[32] *See infra* Part III.C.1.

[33] *See infra* Part III.C.2.

[34] *See infra* Part III.C.3.

know-your-customer procedures (AML/KYC Procedures) implemented by some crypto intermediaries may not be as effective as those implemented by many traditional FIs.[35]

This analysis has important policy implications. This Article proposes ways to address several of CARF's major flaws.[36] It further suggests measures beyond CARF to enhance transparency and shut down the crypto tax haven.[37] It also considers the advantages, costs, and potential critiques of these proposals.[38]

Several amendments to CARF could improve its effectiveness substantially. First, the "Active Entity" loophole could be closed by requiring the reporting of controlling persons of private, closely held entities.[39] Second, standardized registration requirements and a publicly available search tool would help identify unregistered intermediaries. Harmonized disclosure requirements and a presumption of control that shifts the burden of proof to insiders where it is claimed that a platform is decentralized would reduce the risk of noncompliance among in-scope intermediaries.[40] Third, as some of the rules and guidance on key issues are either vague or inadequate, the OECD should consider providing additional guidance to prevent intermediaries from adopting the position that they are not required to comply with CARF.[41] Fourth, adopting mandatory disclosure rules would likely deter some actors from designing, marketing, or implementing CARF avoidance schemes, improve tax authorities' ability to detect such schemes, and enable intelligence gathering.[42] Finally, expanding CARF's scope to cover decentralized platforms should be considered because their exclusion may undermine CARF's effectiveness.[43]

Measures beyond CARF should also be considered. First, as CARF's effectiveness depends on effective AML/KYC Procedures, it is important to ensure that crypto intermediaries' compliance with these rules is on par with that of the traditional financial industry.[44] Second, eliminating some loopholes in CRS and FATCA (such as the non-reporting of withdrawals from depository accounts) would make using the crypto tax haven less attractive.[45] Third, CARF could be integrated with other regulations. In particular, this Article proposes a requirement that only CARF-compliant wallets be used for

---

[35] *See infra* Part III.C.4; *infra* note 207 for the definition of "AML/KYC Procedures."
[36] *See infra* Part IV.A.
[37] *See infra* Part IV.B.
[38] *See infra* Part IV.C.
[39] *See infra* Part IV.A.1.
[40] *See infra* Part IV.A.2.
[41] *See infra* Part IV.A.3.
[42] *See infra* Part IV.A.4.
[43] *See infra* Part IV.A.5.
[44] *See infra* Part IV.B.1.
[45] *See infra* Part IV.B.2.

transactions using crypto as a means of payment.[46] Finally, other measures to ensure tax compliance among crypto owners should be considered. Such measures include, among others, protocol-level tax reporting and ex-ante regulation of blockchain applications.[47]

This Article is organized as follows: Part I discusses the crypto tax haven and the lack of tax transparency concerning crypto assets. Part II provides an overview of CARF. Part III analyzes the weaknesses and loopholes that will likely undermine CARF's effectiveness. Part IV proposes ways to address the shortcomings of this new standard and shut down the crypto tax haven.

## I. The Crypto Tax Haven

The OECD, the EU, tax experts, and analysts have raised concerns about the risk that crypto might be used for tax evasion and other financial crimes.[48] The key features of crypto that make it a "super tax haven," as described by Omri Marian, are pseudonymity and disintermediation.[49] Pseudonymity is achieved because crypto owners are not identified by their names on the blockchain ledger.[50] No identifying information concerning crypto owners is required for creating a wallet or carrying out on-chain transactions. "This anonymity makes it hard for tax authorities to detect the identity of tax cheats who use blockchain to facilitate their illicit activity."[51]

Disintermediation is achieved because blockchain technology enables transferring crypto without financial intermediaries like banks or credit card companies.[52] "This presents a unique challenge to any tax system because modern tax enforcement relies heavily on reporting by financial intermediaries: empirical evidence demonstrates that tax-compliance rates are significantly increased when third-party reporting is involved."[53] As Marian noted,

---

[46] *See infra* Part IV.B.3.

[47] *See infra* Part IV.B.4.

[48] *See* sources cited *infra* in this Part.

[49] *See* Omri Marian, *A Conceptual Framework for the Regulation of Cryptocurrencies*, 82 U. Chi. L. Rev. Online 53, 56–57 (2015); Marian, *supra* note 1, at 42.

[50] *See* Marian, *supra* note 45, at 56–57 ("It should be noted, however, that most cryptocurrencies are not completely anonymous, but rather are pseudonymous.").

[51] Alm et al., *supra* note 5, at 330.

[52] *See id.* at 329.

[53] *Id.* The advantages of third-party reporting over self-reporting have been discussed and documented in the literature. *See, e.g.*, Bibek Adhikari, James Alm & Timothy F. Harris, *Information Reporting and Tax Compliance*, 110 AEA Papers & Proc. 162 (2020); Paul Carrillo, Dina Pomeranz & Monica Singhal, *Dodging the Taxman: Firm Misreporting and Limits to Tax Enforcement*, 9 Am. Econ. J.: Applied Econ. 144 (2017); Henrik Jacobsen Kleven, Claus Thustrup Kreiner & Emmanuel Saez, *Why Can Modern Governments Tax So Much? An Agency Model of Firms as Fiscal Intermediaries*, 83 Economica 219 (2016); Dina Pomeranz, *No Taxation Without Information: Deterrence and Self-Enforcement in the Value Added Tax*, 105 Am. Econ. Rev. 2539 (2015); Mark D. Phillips, *Individual Income Tax Compliance and Information Reporting: What do the U.S. Data Show?*, 67 Nat'l Tax J. 531 (2014); James Alm, *Measuring, Explaining, and Controlling Tax Evasion: Lessons from Theory, Experiments, and Field Studies*

"The combination of anonymity and the decentralization of financial dealings presents governments with formidable regulatory challenges."[54]

Other factors that create challenges for regulators and tax authorities are blockchain's tamper resistance and autonomy. The government and FIs cannot unwind immutable transactions on the blockchain, even if they involve tax evasion or other financial crimes.[55] The autonomous execution of smart contracts facilitated by blockchain creates challenges for governments to stop systems aimed at tax evasion or other financial crimes.[56]

---

(Tul. Econ. Working Paper No. 1213, 2012); Henrik Jacobsen Kleven et al., *Unwilling or Unable to Cheat? Evidence from a Tax Audit Experiment in Denmark*, 79 ECONOMETRICA 651 (2011); Leandra Lederman, *Reducing Information Gaps to Reduce the Tax Gap: When Is Information Reporting Warranted?*, 78 FORDHAM L. REV. 1733, 1738-39 (2010); Leandra Lederman, *Statutory Speed Bumps: The Roles Third Parties Play in Tax Compliance*, 60 STAN. L. REV. 695 (2007); James Alm, John A. Deskins & Michael McKee, *Third-Party Income Reporting and Income Tax Compliance* (Andrew Young Sch. Pol'y Stud. Rsch. Paper Series, Working Paper No. 06-35, 2006).

[54] Marian, *supra* note 49, at 57.

[55] Alm et al., *supra* note 5, at 331.

[56] *Id*. ("Thus, even when tax authorities identify a blockchain-based application aimed at tax evasion, there is nothing that a government can do short of shutting down the internet."). For further discussion about crypto, tax evasion and compliance challenges, including some of the issues discussed here, see Robby Houben & Alexander Snyers, *Cryptocurrencies and Blockchain: Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion,* EUROPEAN PARLIAMENT (2018); Thomas Slattery, *Taking a Bit Out of Crime: Bitcoin and Cross-Border Tax Evasion*, 39 BROOK. J. INT'L L. 829 (2014); Sarah Gruber, *Trust, Identity, and Disclosure: Are Bitcoin Exchanges the Next Virtual Havens for Money Laundering and Tax Evasion?*, 32 QUINNIPIAC L. REV. 135 (2013); James Alm, *Tax Evasion, Technology, and Inequality*, 22 ECON. GOV. 321 (2021); Alessio Faccia & Narcisa Roxana Mosteanu, *Tax Evasion, Information Systems and Blockchain*, 13 J. INFO. SYS. & OPERATIONS MGMT. 65 (2019); Ioana–Florina Coita, Laura–Camelia Filip & Eliza-Angelika Kicska, *Tax Evasion and Financial Fraud in the Current Digital Context*, 30 ANNALS U. ORADEA ECON. SCI. 187 (2021); Amy Q. Nguyen, *The Mysteries of NFT Taxation and the Problem of Crypto Asset Tax Evasion*, 25 SMU SCI. & TECH. L. REV. 323 (2022); Tom G. Meling, Magne Mogstad & Arnstein Vestre, *Crypto Tax Evasion*, NAT'L BUREAU OF ECON. RES. WORKING PAPER NO. 32865 (2024); Suet Yi Yan, *Cryptocurrency and Tax Evasion: Unraveling the Digital Knot for Global Governance*, 2ND INT'L CONF. ON MGMT. INNOVATION & ECON. DEV. (2024); Henrik Refstad Heidenstrøm & Victor Myren, *Prevention of Tax Evasion Through Crypto-Assets: An Economic and Legal Analysis* (2023); Pangi Suryadi & Azis Budianto, *Money Laundering and Tax Evasion Resulting from Cyber Crimes Through Digital Currency (Crypto Currency)*, 2ND INT'L CONF. ON L., SOC. SCI., ECON. & EDUC. (2022); Jori Grym, Jaakko Aspara & Veronica Liljander, *Studies on Moral Judgment and Cognition Involving Cryptocurrencies and Tax Evasion,* 44 IMAGINATION, COGNITION & PERSONALITY 66 (2024); Jori Grym et al., *A Crime by Any Other Name: Gender Differences in Moral Reasoning When Judging the Tax Evasion of Cryptocurrency Traders,* 14 BEHAV. SCI. 198 (2024); Edgar G. Sanchez, *Crypto-Currencies: The 21st Century's Money Laundering and Tax Havens*, 28 U. FLA. J.L. & PUB. POL'Y 167 (2017); Arvind Sabu, *Reframing Bitcoin and Tax Compliance,* 64 ST. LOUIS U. L.J. 181 (2019); Gamze Öz Yalaman & Hakan Yıldırım, *Cryptocurrency and Tax Regulation: Global Challenges for Tax Administration,* in BLOCKCHAIN ECONOMICS AND FINANCIAL MARKET INNOVATION: FINANCIAL INNOVATIONS IN THE DIGITAL AGE (2019); Vincent Ooi, *Report on the Challenges which Digital Assets Pose for Tax Systems with a Special Focus on Developing Countries* (March 2023), https://financing.desa.un.org/sites/default/files/2023-03/Report%20Challenges%20of%20Digital%20Assets%20for%20Tax%20Systems.pdf.

The OECD and the EU have expressed concerns about the rise of the crypto tax haven. The OECD noted, "The Crypto-Asset market, including both the Crypto-Assets offered, as well as the intermediaries involved, poses a significant risk that recent gains in global tax transparency will be gradually eroded …. Overall, the characteristics of the Crypto-Asset sector have reduced tax administrations' visibility on tax-relevant activities carried out within the sector, increasing the difficulty of verifying whether associated tax liabilities are appropriately reported and assessed."[57]

As noted, the crypto tax haven's attractiveness has increased because of the enhanced transparency with respect to the owners of traditional financial assets.[58] FATCA and CRS have made tax evasion through holding offshore financial assets less attractive. FATCA generally requires that non-U.S. FIs identify U.S. account holders and report them to the IRS.[59] FATCA's implementation started on July 1, 2014.[60] FATCA requires FIs to implement certain due diligence procedures to identify account holders who are U.S. persons.[61] The FIs must report such U.S. persons' personal information, financial account balances, and income to the IRS.[62] FIs that do not follow these requirements are generally penalized by a withholding tax of 30% on certain

---

[57] OECD, *Public Consultation Document: Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard*, at 4 (2022) https://www.oecd.org/tax/exchange-of-tax-information/crypto-asset-reporting-framework-and-amendments-to-the-common-reporting-standard.htm [https://perma.cc/7AJZ-N2Z6]. *See also* EU, *DAC8: Impact Assessment Report*, at 8 (2022) ("In particular, the emergence of alternative means of payment and investment, such as crypto-assets, which may pose new risks of tax evasion, are not covered.").

[58] *See supra* text accompanying note 17.

[59] For further background on FATCA, see WILLIAM H. BYRNES, LEXISNEXIS GUIDE TO FATCA AND CRS COMPLIANCE (Matthew Bender & Co., Inc. 2023); Niels Johannesen et al., *Taxing Hidden Wealth: The Consequences of US Enforcement Initiatives on Evasive Foreign Accounts*, 12 AM. ECON. J.: ECON. POL'Y 312 (2020); Yi-Hsin Wu, *Unwise Integration of the Foreign Account Tax Compliance Act into the Common Reporting Standard: Taking Taiwan as an Example*, 1 INT'L COMPAR., POL'Y & ETHICS L. REV. 565 (2017); Dean Smith, *The* Foreign Account Tax Compliance Act *(FATCA): An Introduction to the Potential Impact on Canadian Trusts and Estates*, 36 EST., TR. & PENSIONS J. 1 (2016); Taylor Denson, *Goodbye, Uncle Sam? How the Foreign Account Tax Compliance Act is Causing a Drastic Increase in the Number of Americans Renouncing Their Citizenship*, 52 HOUS. L. REV. 967 (2015); Bruce W. Bean & Abbey L. Wright, *The U.S. Foreign Account Tax Compliance Act: American Legal Imperialism?*, 21 ILSA J. INT'L & COMPAR. L. 333 (2015); Adrian Sawyer, *The Implications of the Multilateral Convention and the Foreign Account Tax Compliance Act: An Australasian Perspective*, 44 AUSTL. TAX REV. 1 (2015); Sunita Ahlawat & Howard Telson, *The Foreign Account Tax Compliance Act's Unintended Consequences*, 2 BANKING & FIN. REV. 137 (2015); Sean Deneault, *Foreign Account Tax Compliance Act: A Step in the Wrong Direction*, 24 IND. INT'L & COMPAR. L. REV. 729 (2014); Adrian Sawyer, *Comparing the Swiss and United Kingdom Cooperation Agreements with Their Respective Agreements Under the Foreign Account Tax Compliance Act*, 12 ELEC. J. TAX RSCH. 285 (2014); Richard Eccleston & Felicity Gray, *Foreign Accounts Tax Compliance Act and American Leadership in the Campaign against International Tax Evasion: Revolution or False Dawn?*, 5 GLOB. POL'Y 321 (2014).

[60] IRS Notice 2013-43, 2013-31 I.R.B. 113.8.

[61] Treas. Reg. § 1.1471-4 (2013); Rev. Proc. 2017-16, 2017-3 I.R.B. 501.

[62] *See supra* note 61.

payments.[63] Since 2014, the U.S. government and many foreign governments have entered into intergovernmental agreements (IGAs), which provide rules on FATCA implementation by FIs in the relevant jurisdictions.[64] There are two categories of FATCA IGAs: Model 1 and Model 2.[65] These models require different reporting channels. Model 1 IGA provides that FIs must report the information to their domestic tax authority, which then transmits the information to the IRS.[66] Model 2 IGA requires that FIs report the information to the IRS directly.[67] Most IGAs follow Model 1.[68]

The OECD introduced CRS—a multilateral standard for the automatic exchange of information—in 2014.[69] Its implementation started in 2016.[70] One hundred seventeen jurisdictions exchanged information under CRS by 2024, and ten more have committed to do so by 2027.[71] The United States is the only developed economy and international financial center that does not

---

[63] I.R.C. §§ 1471(a), 1472(a); Treas. Reg. §§ 1.1471-2(a)(1), 1.1472-1(a)(2013).

[64] *See* U.S. Dep't of Treas., *Foreign Account Tax Compliance Act*, https://home.treasury.gov/policy-issues/tax-policy/foreign-account-tax-compliance-act [https://perma.cc/T9WK-GYE9] (last visited Jan. 15, 2025); Leopoldo Parada, *Intergovernmental Agreements and the Implementation of FATCA in Europe*, 7 World Tax J. 1 (2015); John S. Wisiackas, *Foreign Account Tax Compliance Act: What it Could Mean for the Future of Financial Privacy and International Law*, 31 Emory Int'l L. Rev. 583 (2017).

[65] *See* U.S. Dep't of Treas., *supra* note 64.

[66] The U.S. Treasury provides a general version of each type of IGA. For Model 1, see U.S. Dep't of Treas., *Model 1A IGA Reciprocal, Preexisting TIEA or DTC* (2014).

[67] *See* U.S. Dep't of Treas., *Model 2 IGA, Preexisting TIEA or DTC* (2014).

[68] *See* U.S. Dep't of Treas, *supra* note 64.

[69] For more background on CRS, see Eschrat Rahimi-Laridjani & Erika Hauser, *The New Global FATCA: An Overview of the OECD's Common Reporting Standard in Relation to FATCA*, 42 Int'l Tax J. 31 (2016); Hannes Arnold & Sophie Herdina, *Implications of Common Reporting Standard for Liechtenstein Foundations and Trusts: Taking Stock*, 25 Trusts & Trs. 682 (2019); Noam Noked, *Should the United States Adopt CRS?*, Mich. L. Rev. Online 118 (2019); Andres Knobel, *Statistics on Automatic Exchange of Banking Information and the Right to Hold Authorities (and Banks) to Account*, Tax Just. Network (June 21, 2019), https://taxjustice.net/2019/06/21/statistics-on-automatic-exchange-of-banking-information-and-the-right-to-hold-authorities-and-banks-to-account/ [https://perma.cc/6QV3-QX8D]; Xavier Oberson, International Exchange of Information in Tax Matters: Towards Global Transparency (2nd ed. 2018); David Russell AM QC, *Trusts and Foundations: Implications of Common Reporting Standard and Anti-money Laundering Legislation*, 24 Trusts & Trs. 493 (2018); Andres Knobel & Frederik Heitmüller, Citizenship and Residency by Investment Schemes: Potential to Avoid the Common Reporting Standard for Automatic Exchange of Information (Tax Justice Network eds., 2018); Daniel Ho, *Common Reporting Standard: An Unprecedented Time for Improving Tax Transparency in Hong Kong*, 44 Int'l Tax J. 63 (2018); Filippo Noseda, *EU National Challenges the Common Reporting Standard*, 24 Trusts & Trs. 985 (2018); Andres Knobel & Markus Meinzer, Automatic Exchange of Information: Opportunity for Developing Countries to Tackle Tax Evasion and Corruption (Tax Just. Network, eds., 2014).

[70] 49 jurisdictions started implementation in 2016 and conducted their first information exchanges in 2017. 51 jurisdictions started implementation in 2017 and conducted their information exchanges in 2018. *See* OECD, *Automatic Exchange of Information (AEOI): Status of Commitments as on 13 January 2025*, https://web-archive.oecd.org/tax/transparency/documents/aeoi-commitments.pdf [https://perma.cc/6Z84-X4WY].

[71] *See id.*

implement CRS or carry out a reciprocal information exchange under FATCA.[72] CRS generally follows the FATCA Model 1 IGA reporting framework by requiring that FIs report information to the domestic tax authority, which then transmits the information to the tax authority of the account holders' jurisdictions of tax residence.[73] By design, the CRS due diligence and reporting obligations are largely similar to those under FATCA.[74] While tax evaders may find ways to circumvent the reporting of their offshore financial assets, FATCA and CRS generally make it costlier and riskier to evade tax by holding offshore financial assets.[75]

FATCA and CRS "were not constructed with cryptocurrencies, or crypto assets, in mind."[76] It is unclear whether crypto exchanges and other crypto intermediaries fall within the FI definition.[77] Even where crypto intermediaries are classified as FIs, it is uncertain whether crypto assets are classified as reportable "financial assets" for FATCA and CRS purposes.[78] The OECD stated that crypto assets "will in most instances not fall within the scope of the CRS, which applies to traditional Financial Assets and Fiat Currencies held in accounts with Financial Institutions."[79] The OECD further noted that even if a crypto asset is considered a "financial asset" for CRS purposes, reporting under CRS can be avoided by holding the asset in the owner's cold wallet or in a crypto exchange that does not fall within the FI definition.[80]

Enhanced tax transparency for traditional financial assets, combined with the lack of similar transparency for crypto assets, heightens the appeal of using crypto for tax evasion and illicit activities. Future enhancements in tax transparency for non-crypto assets, such as the OECD's recent proposal to improve international tax transparency for foreign-owned real estate,[81] might further amplify the allure of crypto.

---

[72] *See* Rachel E. Brinson, *Is the United States Becoming the "New Switzerland"?: Why the United States' Failure to Adopt the OECD's Common Reporting Standard is Helping it Become a Tax Haven*, 23 N.C. Banking Inst. 231 (2019); Andres Knobel, The Role of the U.S. as a Tax Haven, Implications for Europe (Catherine Olier et al. eds., 2016); Nick Shaxson, *Panama Papers Help the World Wake Up to Tax Haven USA*, Tax Just. Network (Apr. 7, 2016); Lukas Hakelberg, The Hypocritical Hegemon: How the United States Shapes Global Rules Against Tax Evasion and Avoidance, 104 (2020); Noked & Marcone, *supra* note 16.

[73] *See* CRS, *supra* note 13, at 9–10.

[74] OECD, Standard for Automatic Exchange of Financial Information in Tax Matters: Implementation Handbook 22 (1st ed. 2015).

[75] *See supra* note 16.

[76] Katherine Baer, Ruud de Mooij, Shafik Hebous & Michael Keen, *Taxing Cryptocurrencies* 23 (International Monetary Fund Working Paper, WP/23/144, 2023).

[77] The FI definition generally includes depository institutions, custodial institutions, specified insurance companies, and investment entities. Treas. Reg. § 1.1471-5(e).

[78] *See* Eric D. Chason, *Crypto Assets and the Problem of Tax Classifications*, 100 Wash. U. L. Rev. 765, 793 (2023).

[79] CARF, *supra* note 18, at 11–12.

[80] *See id.* at 12.

[81] *See* OECD, *Enhancing International Tax Transparency on Real Estat*e (July 2023).

Furthermore, mass adoption of crypto and stablecoins may increase the attractiveness of using crypto for tax evasion and illicit purposes.[82] Stablecoins may be more attractive for persons who do not want to be exposed to the price volatility of other crypto assets.[83] Also, as noted by the Financial Action Task Force (FATF), criminals' ability to use crypto "as a means of exchange depends to a great extent on it being freely exchangeable and liquid, which mass-adoption could facilitate."[84] Therefore, the risk that crypto would be used for illicit purposes increases with mass adoption.[85]

## II. Crypto-Asset Reporting Framework

The OECD, with the G20's support, developed CARF "to ensure that recent gains in global tax transparency will not be gradually eroded."[86] In March 2022, the OECD published a consultation document introducing CARF to the public for the first time. Interested parties and members of the public were invited to send their comments to the OECD during a 5-week consultation. Coinbase, one of the world's largest crypto exchanges, stated in its response to the consultation that "this short period to provide comments is inadequate for a document that proposes to impose significant requirements on a developing market."[87]

After this consultation exercise, CARF was approved with minor changes by the OECD Committee on Fiscal Affairs in August 2022.[88] The CARF rules were published in October 2022 in a document containing both CARF and amendments to CRS.[89] CARF was later published in June 2023 with additional commentaries and a multilateral agreement for its implementation (i.e., the CARF MCAA).[90] In September 2023, the G20 declared, "We call for the swift implementation of [CARF] and amendments to the CRS. We ask the Global Forum on Transparency and Exchange of Information for Tax

---

[82] *See* FATF Guidance, *supra* note 6, at 17. In general, the FATF is an intergovernmental organization that develops international standards (referred to as the "FATF Recommendations") to curb money laundering and terrorist financing. Many countries have enacted laws implementing the FATF Recommendations by imposing obligations that require FIs and other parties to carry out AML/KYC Procedures and file disclosures with law enforcement bodies to report suspicious transactions and arrangements. *See* FATF, https://www.fatf-gafi.org/ [https://perma.cc/AN9B-PPM6] (last visited Jan. 14, 2025).

[83] *See* FATF, *supra* note 6, at 17.

[84] *See id.*

[85] *See id.*

[86] CARF, *supra* note 18, at 3.

[87] Coinbase Global, *Comments on the OECD Consultation Document: "Crypto-Asset Reporting Framework"* (Apr. 29, 2022).

[88] OECD, *Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard*, (Oct. 10., 2022), https://www.oecd.org/tax/exchange-of-tax-information/crypto-asset-reporting-framework-and-amendments-to-the-common-reporting-standard.htm.

[89] *See id.*

[90] *See* CARF, *supra* note 18, at 15.

Purposes . . . to identify an appropriate and coordinated timeline to commence exchanges by relevant jurisdictions, noting the aspiration of a significant number of these jurisdictions to start CARF exchanges by 2027."[91] The European Council approved in October 2023 a directive that adopts CARF (DAC8).[92] EU Member States will need to adopt legislation implementing CARF by the end of 2025, with implementation starting on January 1, 2026.[93] As noted, since November 2023, over sixty jurisdictions have committed to implement CARF with information exchanges commencing in 2027 or 2028, and forty-eight jurisdictions have signed the CARF MCAA by November 2024.[94]

The CARF rules cover the following: (i) which crypto assets are reportable; (ii) which intermediaries are subject to due diligence and reporting requirements; (iii) what information must be reported; and (iv) the prescribed due diligence procedures.[95] These rules are discussed below.[96]

### *A. In-Scope Crypto Assets*

The term "Crypto-Asset" is defined as "a digital representation of value that relies on a cryptographically secured distributed ledger or similar technology to validate and secure transactions."[97] This definition is broad by design, and it covers non-fungible tokens (NFTs) and other assets "that can be held and transferred in a decentralised manner, without the intervention of traditional financial intermediaries."[98]

CARF applies to Relevant Crypto-Assets. Relevant Crypto-Assets are Crypto-Assets that are not central bank digital currencies (CBDCs), certain e-money products, and Crypto-Assets that cannot be used for payment or investment purposes.[99] CBDCs and e-money products will be covered under

---

[91] G20, *supra* note 19, at 24.

[92] *See* Council Directive 2023/2226, 2023 O.J. (L2226) 1, 2.

[93] *Id.* art. 2(1).

[94] *See supra* text accompanying notes 20–24.

[95] CARF, *supra* note 18, at 12.

[96] For a critical discussion of CARF, see Paul Foster Millen & Peter A. Cotorceanu, *Old Tricks for New Dogs: The OECD's Cryptoasset Reporting Framework*, 112 Tax Notes Int'l 345 (Oct. 16, 2023); Peter A. Cotorceanu & Paul Foster Millen, *Old Tricks for New Dogs, Part II: The OECD's Cryptoasset Reporting Framework*, 114 Tax Notes Int'l 203 (Apr. 8, 2024); Paul Foster Millen & Peter A. Cotorceanu, *Old Tricks for New Dogs, Part III: Identifying Crypto Beneficial Owners*, 115 Tax Notes Int'l 2153 (Sept. 30, 2024); Peter A. Cotorceanu & Paul Foster Millen, *Old Tricks for New Dogs, Part IV: CARF's Reporting Obligations*, 116 Tax Notes Int'l 801 (Nov. 4, 2024); Paul Foster Millen & Peter A. Cotorceanu, *Old Tricks for New Dogs, Part V: CARF Enforcement and Compliance*, 116 Tax Notes Int'l 1517(Dec. 9, 2024). For further discussion of CARF, see also Jonathan Cutler, *CRS for Crypto: Demystifying the OECD's Proposed Crypto-Asset Reporting Framework*, 19 J. Tax'n Fin. Prods. 9 (2022); Xavier Oberson, *Exchange of Information on Crypto-Assets and Crypto-Currencies*, in International Exchange of Information in Tax Matters (2023).

[97] CARF, *supra* note 18, at 22.

[98] *Id.* at 13.

[99] *Id.* at 22.

CRS, and, therefore, they are excluded to avoid an overlap between CARF and CRS.[100] The exclusion for assets that "do not have the capacity of being used for payment or investment purposes" follows a similar exclusion under the FATF Recommendations.[101]

### *B. In-Scope Intermediaries*

CARF imposes due diligence and reporting obligations on Reporting Crypto-Asset Service Providers (RCASPs). An RCASP means "any individual or Entity[102] that, as a business, provides a service effectuating Exchange Transactions for or on behalf of customers, including by acting as a counterparty, or as an intermediary, to such Exchange Transactions, or by making available a trading platform."[103] Exchange Transactions mean any exchange between Relevant Crypto-Assets and fiat currencies (i.e., official currencies of a jurisdiction[104]) or between one or more Relevant Crypto-Assets.[105] In other words, Exchange Transactions include crypto-to-fiat, fiat-to-crypto, and crypto-to-crypto exchanges.

The Commentary notes, "The phrase 'as a business' excludes individuals or Entities who carry out a service on a very infrequent basis for non-commercial reasons."[106] The Commentary also states that investment funds that invest in Relevant Crypto-Assets and validation nodes are not RCASPs because they do not conduct a "service effectuating Exchange Transactions for or on behalf of customers."[107]

Persons acting as intermediaries or counterparties may be considered RCASPs. The Commentary provides the following examples for RCASPs: "dealers acting for their own account to buy and sell Relevant Crypto-Assets to customers; operators of Crypto-Asset [Automated Teller Machines] . . . ; Crypto-Asset exchanges that act as market makers and take a bid-ask spread as a transaction commission for their services; brokers in Relevant Crypto-Assets where they act on behalf of clients to complete orders to buy or sell an interest in Relevant Crypto-Assets; and individuals or Entities subscribing one or more Relevant Crypto-Assets."[108] "While the sole creation and issuance of a Relevant Crypto-Asset would not be considered a service effectuating Exchange Transactions as a counterparty or intermediary, the direct purchase of

---

[100] *Id.* at 13.
[101] *Id.*
[102] An "Entity" is defined as "a legal person or a legal arrangement, such as a corporation, partnership, trust, or foundation." *Id.* at 27.
[103] *Id.* at 22.
[104] *Id.* at 23.
[105] *Id.* at 22.
[106] *Id.* at 53.
[107] *Id.*
[108] *Id.* at 53–54.

Relevant Crypto-Assets from an issuer, to resell and distribute such Relevant Crypto-Assets to customers would be considered effectuating an Exchange Transaction."[109]

A person is also considered an RCASP by "making available a trading platform" that provides a service effectuating Exchange Transactions for customers.[110] The Commentary notes that "[a] 'trading platform' includes any software program or application that allows users to effectuate (either partially or in their entirety) Exchange Transactions . . . . An individual or Entity that is making available a platform that solely includes a bulletin board functionality for posting buy, sell or conversion prices of Relevant Crypto-Assets would not be a Reporting Crypto-Asset Service Provider as it would not provide a service allowing users to effectuate Exchange Transactions. For the same reason, an individual or Entity that solely creates or sells software or an application is not a Reporting Crypto-Asset Service Provider, as long as it is not using such software or application for the provision of a service effectuating Exchange Transactions for or on behalf of customers."[111] Therefore, CARF only applies where the relevant platform effectuates exchange transactions *as a service*. Software that does not effectuate Exchange Transactions as a service is not within CARF's scope.

Moreover, CARF would only apply to a person making available a platform "to the extent it exercises control or sufficient influence over the platform, allowing it to comply with the due diligence and reporting obligations with respect to Exchange Transactions concluded on the platform."[112] This means that CARF will only apply if there is a person who controls or has sufficient influence over the platform.

CARF applies to an RCASP if it has a certain nexus to a CARF-implementing jurisdiction. Such a nexus includes the following: (i) the RCASP is a tax resident of the relevant jurisdiction; (ii) it is incorporated or organized under the laws of the relevant jurisdiction, and it has legal personality in the relevant jurisdiction or has tax filing obligations in that jurisdiction with respect to its income; (iii) it is managed from the relevant jurisdiction; or

---

[109] *Id.*

[110] *Id.* at 17.

[111] *Id.*

[112] *Id.* at 54. The Commentary notes, "Whether an individual or Entity exercises such control or sufficient influence should be assessed in a manner consistent with the 2012 FATF Recommendations (as amended in June 2019 with respect to virtual assets and virtual asset service providers) and related FATF guidance." *Id.* For information about AML/KYC Procedures, see generally FATF, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations (2023), https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf [https://perma.cc/7GUN-HXQ6]. For a list of participating countries, see FATF, *supra* note 82.

(iv) it has a regular place of business in the relevant jurisdiction.[113] If an RCASP is subject to CARF laws of two or more jurisdictions, it can follow the reporting and due diligence requirements of the jurisdiction with priority based on the hierarchy of these nexus rules,[114] and then it will not be required to follow these requirements in the other jurisdictions.

Importantly, wallets not associated with an RCASP are not within CARF's scope.[115] The details of a private wallet will be reported when there is a transfer from an RCASP to a private wallet, as noted below.

### *C. Reporting Requirements*

RCASPs are required to report "Relevant Transactions," which include Exchange Transactions and "Transfers" of Relevant Crypto-Assets.[116] A Transfer means "a transaction that moves a Relevant Crypto-Asset from or to the Crypto-Asset address or account of one Crypto-Asset User, other than one maintained by the Reporting Crypto-Asset Service Provider on behalf of the same Crypto-Asset User."[117] Transfers of crypto assets from an RCASP to external wallets are generally reportable, except transfers to wallets associated with other Virtual Asset Service Providers (VASPs) and FIs.[118]

---

[113] *See* CARF, *supra* note 18, at 17.

[114] The jurisdiction of tax residence has priority; the jurisdiction of incorporation or organization comes second; the jurisdiction with the place of management comes third; the jurisdiction with the place of business comes last. *Id.*

[115] For a general discussion on crypto wallets, see Crypto.com, *What Is a Crypto Wallet? A Beginner's Guide* (Apr. 24, 2024), https://crypto.com/en/university/crypto-wallets.

[116] *Id*. at 14.

[117] *Id.* at 22. A "Crypto-Asset User" generally means "an individual or Entity that is a customer of a Reporting Crypto-Asset Service Provider for purposes of carrying out Relevant Transactions." *Id.* at 23.

[118] *Id.* at 18–19. The FATF Recommendations apply to VASPs, which generally include RCASPs and some other service providers. VASP means "any natural or legal person who is not covered elsewhere under the Recommendations and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: (i) Exchange between virtual assets and fiat currencies; (ii) Exchange between one or more forms of virtual assets; (iii) Transfer of virtual assets; (iv) Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and (v) Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset." FATF, *supra* note 6, at 109. This definition is broader than the RCASP definition that only includes the activities described in (i) and (ii) above ("any individual or Entity that, as a business, provides a service effectuating Exchange Transactions for or on behalf of customers, including by acting as a counterparty, or as an intermediary, to such Exchange Transactions, or by making available a trading platform".). CARF, *supra* note 18, at 22. The term "virtual asset" means a "digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations." FATF, *supra* note 6, at 109.

The required reporting includes information about the Crypto-Asset Users and Controlling Persons[119] who are Reportable Persons,[120] the RCASP, and the Relevant Transactions. The required Reportable Persons' information includes the persons' name, address, jurisdiction of tax residence, tax identification number (TIN), and date and place of birth.[121] The RCASP's information includes its "name, address, and identifying number (if any)."[122] With respect to Relevant Transactions, CARF requires the reporting on an aggregate basis by type of transactions, distinguishing between outward and inward transactions, crypto-to-fiat and crypto-to-crypto transactions, and transfers.[123] The reporting should be done in fiat currency.[124] If fiat currencies were not used in

---

[119] Controlling Persons are "the natural persons who exercise control over an Entity. In the case of a trust, such term means the settlor(s), the trustee(s), the protector(s) (if any), the beneficiary(ies) or class(es) of beneficiaries, and any other natural person(s) exercising ultimate effective control over the trust, and in the case of a legal arrangement other than a trust, such term means persons in equivalent or similar positions. The term 'Controlling Persons' must be interpreted in a manner consistent with the 2012 Financial Action Task Force Recommendations, as updated in June 2019 pertaining to virtual asset service providers." CARF, *supra* note 18, at 23.

[120] Reportable Person means "an Entity or individual that is resident in a Reportable Jurisdiction under the tax laws of such jurisdiction, or an estate of a decedent that was a resident of a Reportable Jurisdiction. For this purpose, an Entity such as a partnership, limited liability partnership or similar legal arrangement that has no residence for tax purposes shall be treated as resident in the jurisdiction in which its place of effective management is situated," other than an Excluded Person. *See id.* Reportable Jurisdiction is defined as "any jurisdiction (a) with which an agreement or arrangement is in effect pursuant to which [Jurisdiction] is obligated to provide the information specified in Section II with respect to Reportable Persons resident in such jurisdiction, and (b) which is identified as such in a list published by [Jurisdiction]." *Id.*

[121] *Id.* at 18.

[122] *Id.*

[123] The Relevant Transactions' information includes the following: "for each type of Relevant Crypto-Asset with respect to which it has effectuated Relevant Transactions during the relevant calendar year or other appropriate reporting period: a) the full name of the type of Relevant Crypto-Asset; b) the aggregate gross amount paid, the aggregate number of units and the number of Relevant Transactions in respect of acquisitions against Fiat Currency; c) the aggregate gross amount received, the aggregate number of units and the number of Relevant Transactions in respect of disposals against Fiat Currency; d) the aggregate fair market value, the aggregate number of units and the number of Relevant Transactions in respect of acquisitions against other Relevant Crypto-Assets; e) the aggregate fair market value, the aggregate number of units and the number of Relevant Transactions in respect of disposals against other Relevant Crypto-Assets; f) the aggregate fair market value, the aggregate number of units and the number of Reportable Retail Payment Transactions; g) the aggregate fair market value, the aggregate number of units and the number of Relevant Transactions, and subdivided by Transfer type where known by the Reporting Crypto-Asset Service Provider, in respect of Transfers to the Reportable User not covered by subparagraphs A(3)(b) and (d); h) the aggregate fair market value, the aggregate number of units and the number of Relevant Transactions, and subdivided by Transfer type where known by the Reporting Crypto-Asset Service Provider, in respect of Transfers by the Reportable User not covered by subparagraphs A(3)(c), (e) and (f); and i) the aggregate fair market value, as well as the aggregate number of units in respect of Transfers by the Reportable Crypto-Asset User effectuated by the Reporting Crypto Asset Service Provider to wallet addresses not known by the Reporting Crypto-Asset Service Provider to be associated with a virtual asset service provider or financial institution." *Id.* at 18–19.

[124] *Id.* at 19.

the transaction, the reportable value should be based on the market value of the relevant asset at the time of the relevant transaction.[125]

CARF also applies to Reportable Retail Payment Transactions, which are transfers of crypto assets "in consideration of goods or services for a value exceeding USD 50,000."[126] There are situations where an RCASP "processes payments on behalf of a merchant accepting Relevant Crypto-Assets in payment for goods or services."[127] In these situations, in addition to reporting the merchant, the RCASP must "also treat the customer of the merchant as a Crypto-Asset User" and report him, but only if the RCASP is required to verify the customer's identity under the domestic AML laws.[128]

### *D. Due Diligence Requirements*

CARF's due diligence requirements are largely similar to CRS. The CARF Commentary notes that "[t]he due diligence requirements are designed to allow Reporting Crypto-Asset Service Providers to efficiently and reliably determine the identity and tax residence of their Individual and Entity Crypto-Asset Users, as well as of the natural persons controlling certain Entity Crypto-Asset Users."[129] "The due diligence procedures build on the self-certification-based process of the CRS, as well as existing AML/KYC obligations enshrined in the 2012 FATF Recommendations."[130]

The due diligence obligations with respect to individual users are as follows: RCASPs must obtain a self-certification when establishing the relationship with an individual user and within 12 months of the implementation of CARF in the relevant jurisdiction.[131] The self-certification must include the individual's first and last name, residence address, jurisdiction(s) of residence for tax purposes, TIN with respect to each Reportable Jurisdiction, and the individual's date of birth.[132] The RCASP must confirm "the reasonableness of such self-certification based on the information obtained by the Reporting Crypto-Asset Service Provider, including any documentation collected pursuant to AML/KYC Procedures" (hereinafter the "reasonableness test").[133] In addition, the RCASP cannot rely on a self-certification where it knows or has reason to know that it is unreliable or incorrect.[134] In such situations, the RCASP "must obtain a valid self-certification, or a reasonable explanation

---

[125] *Id.*
[126] *Id.* at 22.
[127] *Id*. at 14.
[128] *Id*. For the definition of "Crypto-Asset User," see *id.* at 23.
[129] *Id.* at 15.
[130] *Id.*
[131] *Id.* at 19.
[132] *Id.* at 20–21.
[133] *Id.* at 19.
[134] *Id.*

and, where appropriate, documentation supporting the validity of the original self-certification."[135]

The due diligence obligations for entity users are similar, with additional obligations that concern the Controlling Persons of entities other than Active Entities and Exempt Persons. RCASPs must obtain a self-certification when establishing a relationship with an entity user and within 12 months of the implementation of CARF in the relevant jurisdiction.[136] The entity's self-certification must include the entity's legal name, address, jurisdiction(s) of residence for tax purposes, the TIN with respect to each Reportable Jurisdiction, and the information required for individuals with respect to each Controlling Person of the entity unless it is an Active Entity[137] or an Excluded Person,[138] and "if applicable, information as to the criteria it meets to be treated as an Active Entity or Excluded Person."[139] The RCASP must apply the reasonableness test to self-certifications from entities.[140]

Where the entity is not an Active Entity or an Excluded Person, the RCASP must also determine whether the entity's Controlling Persons are Reportable Persons.[141] To determine the entity's Controlling Persons, an RCASP "may rely on information collected and maintained pursuant to AML/KYC Procedures, provided that such procedures are consistent with the 2012 FATF Recommendations (as updated in June 2019 pertaining to virtual asset service providers)."[142] "If the Reporting Crypto-Asset Service Provider is not legally required to apply AML/KYC Procedures that are consistent with the 2012 FATF Recommendations (as updated in June 2019 pertaining to virtual asset service providers), it must apply substantially similar procedures for the purposes of determining the Controlling Persons."[143] To determine whether a Controlling Person is a Reportable Person, the RCASP "must rely on a self-certification from the Entity Crypto-Asset User or such Controlling Person that allows the Reporting Crypto-Asset Service Provider to determine the Controlling Person's residence(s) for tax purposes" and apply the reasonableness test to such self-certification.[144]

---

[135] *Id.*
[136] *Id.* at 20.
[137] The definition of Active Entity is discussed below in Part III.2.
[138] CARF defines Excluded Person as "(a) an Entity the stock of which is regularly traded on one or more established securities markets; (b) any Entity that is a Related Entity of an Entity described in clause (a); (c) a Governmental Entity; (d) an International Organisation; (e) a Central Bank; or (f) a Financial Institution other than an Investment Entity described in Section IV E(5) (b)." CARF*, supra* note 18, at 24–25.
[139] *Id.* at 21.
[140] *See id.* at 20.
[141] *See id*. at 19–20.
[142] *Id.*
[143] *Id.*
[144] *Id.*

RCASPs may rely on third-party service providers to carry out their due diligence obligations.[145] They must "maintain all documentation and data for not less than five years after the end of the period within which the Reporting Crypto-Asset Service Provider must report the information required to be reported" under CARF.[146] RCASPs that are also FIs under CRS may rely on the CRS due diligence procedures instead of the due diligence requirements under CARF.[147]

## III. Loopholes and Weaknesses

This Part analyzes loopholes and weaknesses in CARF that bad actors may exploit to avoid CARF reporting. It identifies three categories of such vulnerabilities. Section A discusses strategies that involve avoiding interactions with in-scope, compliant RCASPs. Section B explores flaws inherited from CRS. Section C examines vulnerabilities specific to CARF and the crypto industry.

### *A. Avoiding Compliant In-Scope Intermediaries*

#### 1. Avoiding Intermediaries Altogether

As noted, one of the innovations of crypto is disintermediation, which means less reliance on intermediaries compared to the traditional financial industry.[148] One way to avoid CARF reporting would be to avoid intermediaries altogether. For example, a person who sells assets or provides services in exchange for crypto holds crypto without exchanging it and then transfers it to other persons (e.g., as a payment for goods and services) would not need to use intermediaries. As Marian noted, "FATCA-like solutions, namely, targeting intermediaries that facilitate Bitcoin trading and exchange, may be appropriate, but it is not clear to what extent . . . ."[149] "It might be possible for tax authorities to regulate such intermediaries in the same manner in which they regulate financial intermediaries under the FATCA regime."[150] However, "[a]ny transaction made solely in Bitcoins, meaning with no exchange to real currencies, avoids such regulation."[151] "Theoretically, if Bitcoin becomes

---

[145] *Id.* at 21.
[146] *Id.*
[147] *Id.*
[148] *See supra* text accompanying notes 52–53.
[149] Marian, *supra* note 1, at 46.
[150] *Id.*
[151] *Id.*

widely accepted so as to enable taxpayers to 'live on it,' taxpayers could live their lives using only Bitcoins, without ever reporting income."[152]

Thus, the effectiveness of CARF will diminish with the increase in the use of crypto assets as a means of payment. Stablecoins may accelerate the mass adoption of crypto. The FATF notes:

> Stablecoins can have characteristics which could overcome factors which have held back the widespread adoption of [virtual assets] as a means of payment. By maintaining a stable value, stablecoins are designed to overcome the price volatility issues often associated with many [virtual assets]. Reduction of volatility could encourage their widespread use as a means of payment or transferring funds, particularly where they are sponsored by large technology, telecommunications, or financial firms that could offer global payment arrangements.[153]

If crypto becomes a widely accepted means of payment (a trend that may accelerate as a result of regulation), tax evaders would have little need to use intermediaries, including RCASPs.[154]

### 2. Using Out-of-Scope Intermediaries

Tax evaders may avoid reporting by using RCASPs that have no nexus to CARF-implementing jurisdictions. As noted, an RCASP is subject to CARF only if it has a certain nexus to a CARF-implementing jurisdiction.[155] Thus, an RCASP that has no nexus to CARF-implementing jurisdictions is not subject to CARF. Notably, the viability of this CARF avoidance strategy will depend on CARF's international adoption.[156]

In addition, CARF creates an incentive for exchanges and decentralized finance (DeFi) projects to adopt a decentralized platform structure where no person has control, thereby avoiding CARF. As noted, CARF only applies to a person making available a platform "to the extent it exercises control or sufficient influence over the platform, allowing it to comply with the due diligence and reporting obligations with respect to Exchange Transactions concluded on the platform."[157] In other words, CARF will only apply if a person controls or

---

[152] *Id*.

[153] FATF, *supra* note 6, at 17.

[154] *See id*.

[155] *See supra* text accompanying note 107.

[156] *Cf.* Noked & Marcone, *supra* note 16, at 191–201 (discussing how the United States' non-participation in CRS undermines the effectiveness of that standard).

[157] CARF, *supra* note 18, at 54. The Commentary notes, "Whether an individual or Entity exercises such control or sufficient influence should be assessed in a manner consistent with the 2012 FATF Recommendations (as amended in June 2019 with respect to virtual assets and virtual asset service providers) and related FATF guidance." *Id*.

has sufficient influence over the platform. The CARF Commentary refers to the FATF Recommendations and guidance on determining whether a person has control or sufficient influence.[158]

The FATF guidance notes that "[a] DeFi application (i.e., the software program) is not a VASP under the FATF standards, as the Standards do not apply to underlying software or technology."[159] However, this exclusion only applies where the DeFi arrangement is truly decentralized without persons with control or sufficient influence. "This is the case, even if other parties play a role in the service or portions of the process are automated . . . [f]or example, there may be 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 this is exercised through a smart contract or, in some cases, voting protocols."[160] The FATF guidance leaves it to countries to consider other factors, including "whether any party profits from the service or has the ability to set or change parameters to identify the owner/operator of a DeFi arrangement."[161]

The FATF guidance calls on countries to investigate whether projects that claim to be decentralized are indeed decentralized: "It seems quite common for DeFi arrangements to call themselves decentralized when they actually include a person with control or sufficient influence, and jurisdictions should apply the VASP definition without respect to self-description."[162] Countries should evaluate the facts and circumstances of each arrangement without relying on marketing terms or self-proclaimed decentralization.[163]

The FATF guidance acknowledges that there may be situations where no person with control or sufficient influence can be identified. "Where 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."[164] While the FATF notes that countries should monitor for money laundering risks that emerge in such situations,[165]

---

[158] *See id.*
[159] FATF, *supra* note 6, at 27.
[160] *Id*.
[161] *Id*.
[162] *Id*.
[163] *Id*.
[164] *Id.* at 28.
[165] *Id*. ("Countries should monitor for the emergence of risks posed by DeFi services and arrangements in such situations, including by engaging with representatives from their DeFi community. Countries should consider, where appropriate, any mitigating actions, where DeFi services operating in this manner are known to them. Such actions may be taken before the launch of the service or during the course of the DeFi services being offered, as necessary. As an example, where no VASP is identified, countries may consider the option of requiring that a regulated VASP be involved in activities related to the DeFi arrangement in line with the country's RBA or other mitigants. Countries could also consider the ML/TF risks and potential mitigating actions in relation to P2P as set out in this Guidance.").

there is no required reporting under CARF where no person with control or sufficient influence can be identified.[166]

Importantly, the terms "control" and "sufficient influence" in this context are undefined. It appears that there is no specified ownership percentage (in voting rights or value) to be considered as having control or sufficient influence. The meaning of these terms appears functional: A person has control or sufficient influence for CARF purposes only if the control or influence can cause the platform "to comply with the due diligence and reporting obligations" of the platform.[167]

Also, it is unclear how to apply these rules and guidance where two or more persons acting together may have control or sufficient influence. For example, assume that two founders create a platform; any change in the platform can be done only with the consent of both founders, so no single person acting alone has control or sufficient influence over the platform. This could potentially be achieved by a governance mechanism or the technical requirements of the software. If the relationship between the founders is a partnership, then the partnership itself could be viewed as having control or sufficient influence, and thus, it can be considered an RCASP.[168] However, it is uncertain whether this would be the case where there is no express or implied partnership agreement. The question of whether this relationship constitutes a partnership would likely be determined under domestic laws, which may vary across jurisdictions. Also, if there is a partnership with control or sufficient influence, it is unclear whether the obligation would be imposed on both founders. Each one of them cannot ensure that the platform complies with CARF without the other founder's consent. It is uncertain whether both are required to act together to ensure the platform's compliance with its CARF obligations.

Similarly, it is unclear how to determine whether a Distributed Autonomous Organization (DAO) has sufficient influence or control.[169] The DAO itself may be considered an "Entity" for CARF purposes as a partnership or another legal arrangement.[170] However, if there is no person who controls the DAO, it is unclear how it would be able to comply with the applicable

---

[166] *See supra* text accompanying note 157.

[167] CARF, *supra* note 18, at 54. The Commentary notes, "Whether an individual or Entity exercises such control or sufficient influence should be assessed in a manner consistent with the 2012 FATF Recommendations (as amended in June 2019 with respect to virtual assets and virtual asset service providers) and related FATF guidance." *Id.*

[168] As noted, "Entity" means "a legal person or a legal arrangement, such as a corporation, partnership, trust, or foundation." *Id.* at 27.

[169] For further discussion on DAOs, see generally Lu Liu et al., *From Technology to Society: An Overview of Blockchain-Based DAO*, 2 IEEE Open J. Comp. Soc. 204 (2021); Youssef El Faqir et al., *An Overview of Decentralized Autonomous Organizations on the Blockchain*, *in* OpenSym '20: Proceedings of the 16th Int'l Symposium on Open Collaboration (Gregorio Robles, Klaas-Jan Stol & Xiaofeng Wang eds., 2020), https://doi.org/10.1145/3412569.3412579 [https://perma.cc/4CW5-JC7E]; Muhammad Izhar Mehar et al., *Understanding a Revolutionary and Flawed Grand Experiment in Blockchain: The DAO Attack*, 21 J. Cases Info. Tech. 19 (2019).

[170] CARF, *supra* note 18, at 27.

requirements. It is unclear whether we should look through such arrangements to identify one person with control or sufficient influence over the platform. If no such person can be identified, it is unclear whether the DAO members are all required to ensure the relevant platform's compliance. Moreover, the rules and guidance concerning "control" and "sufficient influence" do not appear to include constructive ownership, which could open the door to abuse by splitting ownership rights and powers among family members and related parties.

Where founders and other insiders have control at the initial stages of creating a platform, they could potentially ensure that no person has control in later stages. The FATF guidance provides that owners and operators who meet the VASP definition "should undertake ML/TF risk assessments prior to the launch or use of the software or platform and take appropriate measures to manage and mitigate these risks in an ongoing and forward-looking manner."[171] This may suggest an ex-ante approach to the regulation of decentralized arrangements: The persons with control or sufficient influence over a platform should ensure, before launching the platform, that it will comply with the applicable regulatory requirements in the future.[172] However, the FATF Recommendations and guidance fall short of stating whether these persons must ensure that the platform will comply with the applicable regulatory requirements even when it becomes decentralized. For example, assume that before the launch of a platform, the founders have control over the relevant software, but they design it such that it will become decentralized upon or after its launch. It is unclear whether the founders must ensure compliance with the applicable regulatory requirements even after the platform becomes decentralized.

What control-avoidance techniques might the platforms use? The first control-avoidance technique would be to design a platform where noncompliance with CARF is an immutable feature of the platform. If it is technically impossible for any person to change the platform to ensure compliance, then no person would be considered as having control or sufficient influence under the functional interpretation of these terms. Whether CARF and the FATF Recommendations and guidance prohibit this approach is unclear.

Another control-avoidance technique would be creating a governance structure or technical features where no single person can change the platform to ensure compliance with CARF. Under this approach, making such changes may be technically possible but subject to the approval of at least two persons. The individuals owning and operating the platform will not enter into legal arrangements such as partnerships that would have control or sufficient influence at the legal arrangement level. Even if such a legal arrangement exists, it is unclear

---

[171] FATF, *supra* note 6, at 27.

[172] For a discussion of proactive ex-ante regulation of blockchain platforms before they are launched, see Omri Marian, *Blockchain Havens and the Need for Their Internationally-Coordinated Regulation*, 20 N.C. J.L. & Tech. 529, 566–67 (2019).

whether the obligations apply to the members of such a legal arrangement if no single person has control or sufficient influence over the legal arrangement.

Finally, CARF-avoidance techniques could exploit the fact that CARF only applies to services conducted as a business. CARF does not apply to where a person "solely creates or sells software or an application" if the software or application is not used to provide a service of "effectuating Exchange Transactions for or on behalf of customers."[173] Therefore, CARF only applies where the platform effectuates Exchange Transactions *as a service* for customers. This implies that selling software *as a product* (without any related services) would not be within CARF's scope, even if that software effectuates Exchange Transactions. Also, a person is an RCASP if he provides such services *as a business*. It is unclear whether this requirement is satisfied in cases of platforms that effectuate Exchange Transactions without charging any fees or generating revenue from other sources.[174] While it may be possible to avoid the RCASP definition by avoiding providing services or by providing services but not as a business, these options may not be commercially viable.

The crypto industry has already taken note that CARF would encourage decentralization. For example, Coin Bureau, a YouTube channel with over 2.6 million subscribers, noted in late 2022: "The CARF could do some serious damage to the crypto industry."[175] "Now the caveat is that most of this damage is to centralized elements of the crypto industry, which could be bullish for decentralized alternatives such as [decentralized exchanges]."[176]

For example, Bisq is an exchange that aims to achieve decentralization that would make it immune to regulation. According to the Bisq website:

> The Bisq network is organized as a DAO. The Bisq DAO's purpose is to make the Bisq's governance model as decentralized and censorship-resistant as the Bisq network itself. The Bisq founders realized that decentralized software—no matter how technically robust—is no good if it's still controlled by a single entity. All the software's technical strength would be worthless if the whole project could be ruined by attacking the single entity that runs it. Thus the need for decentralizing the resources in charge of running Bisq itself. These resources cannot be organized in the form of a company, a nonprofit, or any other traditional organization because a single entity would be a single point of failure.[177]

---

[173] CARF, *supra* note 18, at 54.

[174] This may be the case where the persons involved in the platform's operations do it voluntarily.

[175] Coin Bureau, *What's Coming in 2023: The OECD's Crypto Tax Plans!!*, YouTube (Dec. 18, 2022), https://www.youtube.com/watch?v=mMxZ5wrSdAs [https://perma.cc/2BK5-ARV3].

[176] *Id.*

[177] *Decentralized autonomous organization*, Bisq Wiki, https://bisq.wiki/Decentralized_autonomous_organization (Apr. 28, 2021).

Bisq has been highlighting the fact that it does not collect the users' personal data, unlike centralized exchanges.[178]

Bisq is not alone. Many other platforms do not require user information through AML/KYC Procedures.[179] If CARF does not apply to Bisq and other platforms because no person has control or sufficient influence over them, bad actors will likely flock to these platforms.

### 3. Using In-Scope, Noncompliant Intermediaries

If an RCASP does not comply with CARF, the relevant jurisdictions may be unable to identify the RCASP and its noncompliance.[180] The challenges in detecting noncompliance may emanate from difficulties in identifying RCASPs. Even where RCASPs are identified, they may not have an apparent nexus to any jurisdiction.

The difficulty in identifying RCASPs may arise from the pseudonymity of crypto. Assume that there is a person with control or sufficient influence over a platform through governance tokens, but that person's identity and location remain unknown. That person would be considered an RCASP, but if he fails to comply, the authorities in the relevant jurisdictions may not be able to identify him as an RCASP subject to their laws.

The difficulty of identifying persons in control was raised by STEP in their submission in response to the OECD's public consultation on CARF.[181] STEP illustrated this point by using Curve—a decentralized exchange—as an example:

Take, for instance, the Curve DeFi protocol:

1. The protocol itself is not a VASP (FATF 67)
2. The decentralised autonomous organisation (DAO) is not a registered corporate body with legal personality. The Curve DAO token (CRV) can be used to vote on proposals for amendments to the operation of the Curve protocol and it may be that under the law of England and Wales (if and to the extent that the law of that jurisdiction governs the position) the CRV holder are partners.

---

[178] *See, e.g.*, Bisq (@bisq_network), X (June 9, 2023, 7:51 PM), http://tinyurl.com/mvb34c4m.

[179] For example, the website kycnot.me provides a list of dozens of crypto platforms that do not implement AML/KYC Procedures.

[180] *See* Bob Michel, *Are FTX and the "Other 'Bad Apples' Spoiling the Low-Hanging Fruit Approach of the OECD's Crypto-Asset Reporting Framework (CARF)?* 3 (Jan. 18, 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4328576 ("The question arises as to what happens in case there is no identifiable link to a commercial entity operating the DEX.").

[181] STEP is the Society of Trust and Estate Practitioners, an international professional body with members in the trust, private client, and wealth management industries. *See About STEP*, https://www.step.org/about-step (last visited Jan. 15, 2025).

> 3. CRV tokens can be used to vote on proposals for amendments to the operation of the Curve protocol, providing exchange and automated market making services. Owners of CRV tokens are, however, pseudonymous so that they cannot be directly identified as Reporting Crypto-Asset Service Providers…
> 4. It may be impossible to enforce (or punish any failure) any such requirements imposed on the CRV token holders (if identifiable).
> 5. The creators of the Curve protocol are within the definition of Reporting Crypto-Asset Service Providers and can be identified. They can at present have no direct knowledge of Crypto-Asset Users involved in their system, nor any other Reporting Crypto-Asset Service Providers.[182]

In this example, assume that the DAO is considered to be an RCASP because it is a partnership (i.e., an Entity for CARF purposes) with control or sufficient influence over the protocol. However, as noted by STEP, it is unclear how enforcement actions can be taken against the DAO, especially if its members are pseudonymous. If one person controls or sufficiently influences the DAO, he would be considered as an RCASP, but it would be hard to identify him due to the pseudonymity of the DAO's governance tokens.

Even if we can identify an RCASP, relevant jurisdictions may not identify that the RCASP has a nexus to them. As noted, the CARF laws of a country apply to an RCASP if it has a nexus to the jurisdiction.[183] If an RCASP is subject to CARF laws of two or more jurisdictions, it can follow the reporting and due diligence requirements of the jurisdiction with priority based on the hierarchy of the nexus rules,[184] and then it will not be required to follow these requirements in the other jurisdictions.

Some RCASPs may avoid creating an observable nexus to any jurisdiction. For example, assume an RCASP is organized as a partnership in a tax haven jurisdiction where it does not have tax residency, legal personality, or tax filing obligations. The jurisdiction where it is managed may not be able to identify this nexus if the RCASP is not compliant. The RCASP may avoid creating an easily identifiable place of business. The platform will have an internet website containing no information concerning nexus to any jurisdiction. How can the affected jurisdictions identify RCASPs subject to their CARF laws?

---

[182] STEP, *STEP Scoping Document Response: OECD Crypto-Asset Reporting Framework and amendments to the Common Reporting Standard* (Apr. 29, 2022).

[183] *See supra* text accompanying note 113; CARF, *supra* note 18, at 17.

[184] The jurisdiction of tax residence has priority; the jurisdiction of incorporation or organization comes second; the jurisdiction with the place of management comes third; the jurisdiction with the place of business comes last. *Id.*

The OECD acknowledges the potential challenge in identifying RCASPs with a nexus to the relevant jurisdictions.[185] Instead of providing a harmonized solution as part of the CARF framework, the OECD noted that countries should address this challenge by adopting mechanisms, which may include existing regulatory frameworks (such as registration requirements under AML rules or financial regulation) or new mechanisms.[186] Such new mechanisms may include a requirement for RCASPs to register with a domestic registry.[187] It is unclear how a registration requirement would resolve this problem where noncompliant RCASPs fail to register. The OECD also suggests that governments consider using market research portals, anonymous tip lines, and domestic reporting requirements for Crypto-Asset Users to identify RCASPs with nexus to the jurisdiction.[188]

### *B. Flaws Inherited from CRS*

CARF is largely based on CRS.[189] Fortunately, it did not inherit two loopholes that exist in CRS. The first one is the "shell bank" loophole.[190] The second one is the non-reporting of withdrawal of funds from depository accounts.[191] However, some other loopholes and weaknesses were inherited from CRS.

---

[185] *Id.* at 64.

[186] *Id.* at 65.

[187] *Id.*

[188] *Id.*

[189] In particular, the due diligence obligations and the reporting framework (i.e., reporting from the RCASPs to the domestic tax authority, which then transmits the information to the Crypto-Asset Users' jurisdictions of tax residence) are largely similar to CRS.

[190] *See* Noam Noked & Zachary Marcone, *Closing the "Shell Bank" Loophole*, 64 VA. J. INT'L L. 119 (2023). Tax evaders may avoid FATCA and CRS reporting by holding financial accounts through private, closely held, tax haven companies that certify that they are FIs. This is the result of the FATCA and CRS overly broad FI definition that classifies as an FI any entity managed by another FI if 50% or more of its gross income is from investing in financial assets (such entities are referred to as "managed" investment entities). CARF closes this loophole in the following manner: RCASPs must identify and report the Controlling Persons of entities that are not Excluded Persons or Active Entities. CARF, *supra* note 18, at 20. The Excluded Person definition provides that a "managed" investment entity is not an Excluded Person. All other types of FIs are included in the Excluded Person definition. *Id*. at 24–25 ("The term 'Excluded Person' means (a) an Entity the stock of which is regularly traded on one or more established securities markets; (b) any Entity that is a Related Entity of an Entity described in clause (a); (c) a Governmental Entity; (d) an International Organisation; (e) a Central Bank; or (f) a Financial Institution other than an Investment Entity described in Section IV E(5)(b)."). CARF Section IV E(5)(b) described "managed" investment entities ("the gross income of which is primarily attributable to investing, reinvesting, or trading in Financial Assets or Relevant Crypto-Assets, if the Entity is managed by another Entity that is a Depository Institution, a Custodial Institution, a Specified Insurance Company, or an Investment Entity described in subparagraph E(5)(a)."). *Id.* at 25. The result is that RCASPs must generally report their Controlling Persons, assuming that these entities do not certify that they are Active Entities or Excluded Persons as further discussed below.

[191] *See* Noam Noked, *Tax Evasion and Incomplete Tax Transparency*, 7 LAWS 31, at 7–8 (2018). Under FATCA and CRS, fund withdrawals from depository accounts are generally not subject to reporting. The reporting is of the account balance on 31 December of the relevant year and the income paid or credited to the account during the year. This may enable the avoidance of

The "Active Entity" loophole, discussed in detail below, demonstrates how a loophole inherited from CRS may undermine CARF's effectiveness.

In general, similar to CRS, CARF does not require RCASPs to identify and report the Controlling Persons of Active Entities.[192] There are several categories of Active Entities: Active businesses,[193] holding companies of non-financial subsidiaries,[194] start-up entities,[195] non-financial entities in liquidation,[196] group financing entities of non-financial groups,[197] and non-profit entities.[198]

The "Active Entity" loophole refers to the avoidance of CARF reporting of the beneficial owners by setting up offshore entities that will certify (correctly or falsely) that they are Active Entities. These are the key steps that a tax evader may follow under the "Active Entity" loophole:[199]

1. Incorporate a shell company (the "Company") in an offshore jurisdiction such as the British Virgin Islands (BVI).

---

FATCA and CRS reporting by emptying financial accounts in FIs before year end. CARF closes this loophole by requiring reporting of Reportable Transactions including withdrawals.

[192] *See* CARF, *supra* note 18, at 20 ("With respect to an Entity Crypto-Asset User, other than an Excluded Person, the Reporting Crypto-Asset Service Provider must determine whether it has one or more Controlling Persons who are Reportable Persons, unless it determines that the Entity Crypto-Asset User is an Active Entity, based on a self-certification from the Entity Crypto-Asset User.").

[193] An Entity is an Active Entity under this category where "less than 50% of the Entity's gross income for the preceding calendar year or other appropriate reporting period is passive income and less than 50% of the assets held by the Entity during the preceding calendar year or other appropriate reporting period are assets that produce or are held for the production of passive income." *Id.* at 24.

[194] An Entity is an Active Entity under this category where "substantially all of the activities of the Entity consist of holding (in whole or in part) the outstanding stock of, or providing financing and services to, one or more subsidiaries that engage in trades or businesses other than the business of a Financial Institution, except that an Entity does not qualify for this status if the Entity functions (or holds itself out) as an investment fund, such as a private equity fund, venture capital fund, leveraged buyout fund, or any investment vehicle whose purpose is to acquire or fund companies and then hold interests in those companies as capital assets for investment purposes." *Id.* at 24.

[195] An Entity is an Active Entity under this category where "the Entity is not yet operating a business and has no prior operating history, but is investing capital into assets with the intent to operate a business other than that of a Financial Institution, provided that the Entity does not qualify for this exception after the date that is 24 months after the date of the initial organisation of the Entity." *Id.*

[196] An Entity is an Active Entity under this category where "the Entity was not a Financial Institution in the past five years, and is in the process of liquidating its assets or is reorganising with the intent to continue or recommence operations in a business other than that of a Financial Institution." *Id.*

[197] An Entity is an Active Entity under this category where "the Entity primarily engages in financing and hedging transactions with, or for, Related Entities that are not Financial Institutions and does not provide financing or hedging services to any Entity that is not a Related Entity, provided that the group of any such Related Entities is primarily engaged in a business other than that of a Financial Institution." *Id.*

[198] *Id.*

[199] This list is similar to a list of steps under the "shell bank" loophole, as published by the U.S. Senate Committee on Finance's report on the "shell bank" loophole. *See* S. COMM. ON FINANCE, THE SHELL BANK LOOPHOLE 18 (2022) [hereinafter Finance Committee Report].

2. The Company will open an account with a crypto exchange (an RCASP) and certify that it is an Active Entity under the "start-up entity" category:[200]
   a. The Company was organized within 24 months.
   b. The Company is not yet operating a business and has no prior operating history.
   c. It is required that the Company "is investing capital into assets with the intent to operate a business other than that of a Financial Institution." This would not be the case where a tax evader uses an entity to avoid CARF reporting, but the RCASP may not be able to find out if the Company lies about its intentions concerning future activities.
4. Use the Company for Reportable Transactions for 24 months.
5. Repeat the above step with a new offshore company after 24 months.

As a result of these actions, the Company's Controlling Persons will not be reported if the RCASP accepts this self-certification. There will be reporting of the Company and its Reportable Transactions to its offshore jurisdiction (e.g., BVI), which is unlikely to be interested in that information because no tax would apply to the Company in that offshore jurisdiction.

Other categories susceptible to abuse may include the "active business" and "holding company" categories.[201] Notably, banks and other FIs implementing FATCA and CRS usually closely scrutinize claims of entities (especially offshore entities) that claim that they are active non-financial entities. It is unclear whether RCASPs would apply a similar level of scrutiny. Moreover, as discussed in the next section, the risk of this type of abuse is likely higher in the crypto industry because of weaknesses specific to CARF and the crypto industry. In addition to the "Active Entity" loophole, tax evaders may use other loopholes inherited from CRS to circumvent CARF reporting.[202]

### *C. Vulnerabilities Specific to CARF and the Crypto Industry*

Several factors specific to CARF and the crypto industry increase the risk of abuse compared to banks and other traditional FIs.

---

[200] For the requirements under this category, see *supra* note 195.

[201] *See* definitions in *supra* notes 193–94.

[202] For further discussion on loopholes and weaknesses in CRS, see the sources cited in *supra* note 16.

1. Remote Account Opening and Interactions

The communications between RCASPs and their clients, including in the onboarding process, are typically conducted remotely through the Internet. This enables tax evaders to approach many RCASPs in various jurisdictions at no or low cost. In contrast, many banks and other FIs require in-person meetings, provision of original documents or certified copies, and other requirements that make opening an account more costly and time-consuming.

It is generally desirable to lower transaction costs and costs of financial services. Nonetheless, the ability to approach multiple RCASPs online at a low cost may increase the risks of tax evasion and financial crimes. The likelihood of successfully opening an account using fraud and loopholes such as the "Active Entity" loophole may increase with the number of attempts to open accounts with different RCASPs. As a result, the ability to try to open accounts remotely with many RCASPs at a low cost appears to increase the risk of abuse in the context of CARF.

2. Little Human Involvement

Currently, many RCASPs apply due diligence procedures using software with no or little human involvement.[203] Also, after an account with an RCASP is opened, there is little or no human monitoring or communication with the users, even high-value users who carry out large transactions. In contrast, FI employees are usually involved in onboarding procedures, especially for high-net-worth clients, to whom banks frequently assign relationship managers who know and keep ongoing communications with the clients. CRS requires that relationship managers be asked for their actual knowledge with respect to certain accounts.[204]

It is unclear whether RCASPs' digitized due diligence procedures and assessment of self-certifications would be able to detect false certifications concerning an individual's tax residency or an entity's activities and intentions.[205]

---

[203] *See* Katherine A. Lemire, *Cryptocurrency and anti-money laundering enforcement*, Reuters (Sept. 26, 2022, 11:06 AM), available at https://www.reuters.com/legal/transactional/cryptocurrency-anti-money-laundering-enforcement-2022-09-26/ [https://perma.cc/Q4AL-EZN3 ] (discussing software compliance solutions for crypto); Leigh Cuen, *Most Crypto Exchanges Still Don't Have Clear KYC Policies: Report*, CoinDesk (May 27, 2019), https://www.coindesk.com/markets/2019/03/27/most-crypto-exchanges-still-dont-have-clear-kyc-policies-report/ [https://perma.cc/G5NC-69SX] (describing findings that only a minority of crypto exchanges had in-house compliance staff with AML experience).

[204] *See* CRS, *supra* note 13, at 35.

[205] However, improvements in digitized processes and artificial intelligence (AI) may result in better performance than humans. For further discussion of an AI for anti-money laundering, see, e.g., Jingguang Han, Yuyun Huang, Sha Liu & Kieran Towey, *Artificial Intelligence for Anti-Money Laundering: A Review and Extension*, 2 Digital Fin. 221 (2020); Rashid Alhajeri & Abdulrahman Alhashem, *Using Artificial Intelligence to Combat Money Laundering*,

Also, similar to FATCA and CRS, CARF prohibits RCASPs from relying on information where they know or have reason to know that the information is incorrect or unreliable.[206] However, this requirement to act on actual knowledge may have little effect in the context of RCASPs, where their employees have no interactions with the users.

### 3. Relationships Limited to Exchange Transactions

Unlike traditional financial assets, crypto owners do not need the RCASPs to maintain their crypto assets—many use RCASPs for Exchange Transactions and then transfer the crypto assets to their private wallets. As a result, the interactions with RCASPs can be limited to Exchange Transactions: A user can open an account with an RCASP, carry out transactions, withdraw the tokens on the same day or within days, and close the account or leave it with a zero balance. The crypto owner may use the same or a different RCASP for more transactions later. In contrast, many people have multi-year-long relationships with their banks and other FIs that maintain their financial assets.

The relationships between RCASPs and crypto owners likely provide fewer opportunities for RCASPs to detect fraud or otherwise learn that an account is reportable. For example, identifying changes in circumstances is more likely when there is a longer relationship with the relevant person. When a bank account holder moves to a different country, the holder may update the bank about their new address and phone number. The bank would then be able to detect a change in circumstances that may cause the account to become reportable. Even if the relevant person does not update the bank, the relationship manager who maintains the bank's relationship with that person may know they have moved to a reportable jurisdiction. These opportunities to detect changes in circumstances appear much more limited in the crypto context, where there may not be any long-term relationship with clients.

---

15 INTELLIGENT INFO. MANAG'T 284 (2023); Ana P. Martins & Miguel A. Brito, *Fraud Detection and Anti-Money Laundering Applying Machine Learning Techniques in Cryptocurrency Transactional Graphs* (2023) (Master's dissertation, University of Minho). This question is outside the scope of this Article.

[206] *See* CARF, *supra* note 18, § III B(3) ("If at any point there is a change of circumstances with respect to an Entity Crypto-Asset User or its Controlling Persons that causes the Reporting Crypto-Asset Service Provider to know, or have reason to know, that the original self-certification is incorrect or unreliable, the Reporting Crypto-Asset Service Provider cannot rely on the original self-certification and must obtain a valid self-certification, or a reasonable explanation and, where appropriate, documentation supporting the validity of the original self-certification."); *id.* at 20 ("If at any point there is a change of circumstances with respect to an Individual Crypto-Asset User that causes the Reporting Crypto-Asset Service Provider to know, or have reason to know, that the original self-certification is incorrect or unreliable, the Reporting Crypto-Asset Service Provider cannot rely on the original self-certification and must obtain a valid self-certification, or a reasonable explanation and, where appropriate, documentation supporting the validity of the original self-certification.").

4. Quality of AML/KYC Procedures

CARF's effectiveness depends on the quality and effectiveness of the AML/KYC Procedures.[207] An RCASP must confirm the reasonableness of a self-certification "based on the information obtained by the Reporting Crypto-Asset Service Provider, including any documentation collected pursuant to AML/KYC Procedures."[208] Identifying Controlling Persons of entities is also based on "information collected and maintained pursuant to AML/KYC Procedures."[209] Moreover, CARF provides that if the RCASP is not required to apply AML/KYC Procedures consistent with the FATF Recommendations, it "must apply substantially similar procedures for the purposes of determining the Controlling Persons."[210] This latter rule means that if a jurisdiction does not require RCASPs to implement AML/KYC Procedures under its AML laws, the RCASPs would still need to implement such procedures under CARF.

Currently, the effectiveness of RCASPs' AML/KYC procedures is debatable compared to those of banks and other traditional FIs in jurisdictions adhering to the FATF Recommendations.[211] If the AML/KYC Procedures are not implemented effectively, it would be easier for tax evaders to avoid reporting under CARF—they may be able to hide their reportable status or exploit weaknesses such as the "Active Entity" loophole.

Consider the factors discussed above in the context of the "Active Entity" loophole: A tax evader who owns and controls a newly incorporated tax haven company can approach dozens of RCASPs to open an account for the company. The account opening will require submitting forms, certifications, and documents electronically. The AML/KYC Procedures implemented by some RCASPs may not be as effective as those implemented by banks and other FIs. They will likely involve limited or no interaction with any RCASP employee. If one RCASP accepts the company's self-certification as an Active Entity, the tax evader will use the account to carry out Exchange Transactions and withdraw the crypto to his private wallet. He will probably have no interaction or ongoing relationship with any RCASP employee. If the RCASP later requires the company to provide more information about its Controlling Persons, the company will neither respond nor use the RCASP again. Instead, it will try to open new accounts with other RCASPs.

---

[207] CARF defines "AML/KYC Procedures" as "the customer due diligence procedures of a Reporting Crypto-Asset Service Provider pursuant to the anti-money laundering or similar requirements to which such Reporting Crypto-Asset Service Provider is subject." *Id.* at 27.

[208] *Id.* at 19–20.

[209] *Id.*

[210] *Id.*

[211] *See, e.g.*, Lemire, *supra* note 203.

## IV. Potential Policy Responses

Bad actors might exploit the vulnerabilities and loopholes detailed in Part III to evade CARF reporting. Concurrently, RCASPs will incur significant compliance costs when implementing this complex tax information reporting standard. Thus, CARF may raise costs for compliant parties without effectively detecting or deterring bad actors. How can policymakers address this problem? What actions can be taken to reduce crypto-related opportunities for tax evasion and financial crime?

As discussed below, some of CARF's flaws can be addressed through amendments to CARF. The discussion in Section A below outlines several changes to CARF that policymakers should consider. Other vulnerabilities may be addressed through regulation outside CARF, as detailed in Section B. Section C considers the advantages and critiques of the proposed policy responses.

### *A. Amendments to CARF*

#### 1. Closing the "Active Entity" Loophole

Private, closely held companies organized in tax havens are most likely to exploit this loophole.[212] To address the "Active Entity" loophole, CARF could provide that all Controlling Persons of any private, closely held entity must be reported. This means excluding closely held entities from the exception for Active Entities and Excluded Persons from the requirement to report their Controlling Persons.

Notably, RCASPs in jurisdictions that implement AML/KYC Procedures are generally required to identify the entity's beneficial owners for AML/KYC purposes.[213] Thus, the additional compliance cost of requiring the reporting of such a Controlling Person is not expected to be substantial.

Requiring the reporting of Controlling Persons of private, closely held entities would make it harder for tax evaders to circumvent reporting by holding accounts through entities.[214] CARF follows this approach for "shell banks" by excluding "managed" investment entities from the Excluded Person's definition.[215] A similar approach could close the "Active Entity" loophole.[216]

---

[212] Similar entities may be used for the "shell bank" loophole. *See* Noked & Marcone, *supra* note 190, at 122.

[213] *See* FATF, *supra* note 112, at 67–68, which require the identification of the beneficial owners of entities, including persons with "controlling ownership interest," which may be based on an ownership threshold such as 25%.

[214] *See* Noked & Marcone, *supra* note 190, at 147–60 (proposing a similar solution to the "shell bank" loophole in CRS).

[215] *See id*.

[216] This would also address the potential use of a status as an Excluded Person to avoid reporting.

2. Reducing Noncompliance Among In-Scope RCASPs.

As noted, jurisdictions may not be aware of any noncompliance because platforms available online may not indentify any RCASP with an apparent nexus to any jurisdiction. In addition, persons with control or sufficient influence over platforms may be hard to identify. Disclosure requirements, as detailed below, could reduce noncompliance. The OECD stated that countries should try to address these challenges but did not propose an international, harmonized solution as part of CARF. The OECD's approach is problematic for two reasons. First, some countries may not be sufficiently incentivized to adopt effective mechanisms, especially where these countries have little interest in curbing noncompliance that harms other jurisdictions. Second, uncoordinated efforts of different tax authorities might be ineffective and wasteful because each tax authority would need to independently investigate the identity and compliance status of RCASPs that may not have an apparent nexus to any jurisdiction. Coordinated measures, such as the proposed legal measures described below, could be more effective and cost-efficient if implemented globally as part of CARF.

*Registration requirements and a publicly available search tool*. It is possible to identify noncompliant RCASPs by first identifying the compliant ones. This Article proposes to follow FATCA's approach for registration and a publicly searchable list of compliant parties. Under FATCA, in-scope FIs are required to register with the IRS and receive a unique identifying number, referred to as a Global Intermediary Identification Number (GIIN).[217] The IRS website provides a publicly searchable list of all the FIs registered by the IRS, their jurisdictions, and their GIINs.[218] As of June 2023, around 440,000 FIs have registered with the IRS.[219]

Similar to the FATCA portal on the IRS website, the OECD could set up a CARF portal on a dedicated website that RCASPs would use to register. Each registered FI would be assigned a unique number, similar to FATCA's GIIN. The CARF portal would include a search tool with the name,[220] the jurisdictions that the RCASP has a nexus to and the nature of this nexus, the jurisdiction where the RCASP reports, the name of the platform under the RCASP's control or sufficient influence, and the identification number of each RCASP.

---

[217] Treas. Reg. § 1.1471-1(b)(57) (2013). Alternatively, FIs can be "sponsored" by other entities that have registered with the IRS and obtained their own special "sponsor" GIINs. Treas. Reg. § 1.1471-4(d)(2)(ii)(C) (2013).

[218] *See* IRS, *FATCA Foreign Financial Institution (FFI) List Search and Download Tool*, https://apps.irs.gov/app/fatcaFfiList/flu.jsf [https://perma.cc/M2F2-425H] (last visited Jan. 14, 2025).

[219] *See id.* for the FFI List.

[220] Where the RCASP is an individual, privacy concerns may support that his or her identifying information will not be publicly available. It is possible to limit this information to governments with nexus to the relevant individual (e.g., jurisdictions of tax residency).

Tax authorities could use this information to monitor RCASPs' compliance with CARF. Moreover, the OECD, tax authorities, and others could use this list to identify those RCASPs and platforms that are not registered and investigate if such nonregistration is the result of noncompliance.

*Disclosure requirements.* In addition to registration requirements, it is possible to require all intermediaries and platforms that effectuate crypto exchanges to disclose the identity of any intermediary that meets the RCASP definition with respect to the relevant Exchange Transactions and the jurisdiction to which the RCASP has nexus. If no RCASP is identified, the platform would need to disclose information to establish that there is no person with control or sufficient influence over the platform. This would require disclosing information about the platform's founders, its governance, who has powers over the protocol, etc. It is also possible to require the identity and the jurisdictions of professional advisers who gave legal or tax opinions that CARF reporting is not required by any party. In addition, the platform would need to provide information on its nexus to jurisdictions, including the jurisdictions of its founders, managers, employees, and independent contractors involved in the operation of the platform.

The disclosure requirements could be standardized in a "CARF Disclosure Paper" with specific fields and required information. Many centralized exchanges, decentralized exchanges, and other DeFi projects have websites that include information (including whitepapers and technical information) on the relevant platform or project.[221] The CARF Disclosure Paper should be featured on that website. Alternatively, if there are privacy or data protection concerns that prevent public disclosure, it is possible to restrict access to this information to government authorities.[222] The disclosure requirements could be initially imposed on the founders of a platform that effectuates exchanges and RCASPs. If there is no identified RCASP or founder, the persons with the power to maintain the platform's website (or the persons who instruct other people on the website maintenance) may be required to make these disclosures. In case of noncompliance with the disclosure requirements, the persons subject to the disclosure requirements could face penalties where they reside. If the relevant platform has its own governance token, CARF-compliant exchanges would need to receive and feature the relevant CARF Disclosure Paper before listing that token for trading.

---

[221] *See, e.g.*, Decentralized Exchanges, https://defiprime.com/exchanges (last visited Jan. 14, 2025) [https://perma.cc/3MYB-5VL8].

[222] *Cf.* Solvej Krause, *Who Should Have Access to Beneficial Ownership Registries?*, World Bank (Jan. 26, 2023) [https://perma.cc/CD8Q-ZNAX] (discussing the ruling of the European Court of Justice that struck down public access for beneficial ownership information collected in registries in the EU, while allowing access to governments and other parties with a legitimate interest).

*Presumption of control.* As noted, there is a concern that platforms that present themselves as decentralized are actually controlled or influenced by some insiders.[223] CARF could adopt a rebuttable presumption under which the founders and operators are deemed to have control or sufficient influence over the platform. This presumption would shift the burden of proof concerning decentralization to the founders and operators of the platforms by requiring them to establish that no person has control or sufficient influence over the platforms.[224] If they fail to do so, their founders, operators, and other insiders could be subject to penalties for noncompliance in the jurisdictions they have a nexus to. This means that the individuals and entities involved in crypto projects could be penalized if they adopt an opaque structure that disguises who controls and influences the relevant platforms.

*Other regulatory requirements*. More extensive regulatory requirements can also be considered. The EU has recently adopted a comprehensive regulatory framework—the Markets in Crypto-Assets (MiCA) regulation—that requires regulatory authorization and presence in the EU as a condition for market access.[225] Under MiCA, a person must obtain regulatory authorization in order to provide crypto-asset services within the EU.[226] The service provider must have a registered office in the EU where it should carry out at least part of the services.[227] The service provider's place of effective management must be in the EU, and it must have at least one director who is a resident of an EU Member State.[228] However, MiCA has two important carve-outs that could undermine this regulation's effectiveness in the context of CARF. First, the regulatory requirements under MiCA do not apply where an EU client "initiates at its own exclusive initiative the provision of a crypto-asset service or activity by a third-country firm to that client."[229] This means that RCASPs outside the EU are not required to comply with the EU regulatory framework where EU clients request them to provide the services at the clients' exclusive initiative. Bad actors may approach, at their own initiative, non-EU RCASPs that do not comply with CARF. Second, MiCA does not apply "[w]here crypto-asset services are provided in a fully decentralised manner without any intermediary."[230] While MiCA in its current form may not prevent bad actors from using non-EU RCASPs that do not comply with CARF, this regulatory

---

[223] *See supra* text accompanying note 162.

[224] It is possible to require the disclosure of the relevant information in the CARF Disclosure Paper.

[225] Regulation (EU) 2023/1114.

[226] *Id*. at Art. 59(1)(a).

[227] *Id*. at Art. 59(2).

[228] *Id*.

[229] *Id*. at Art. 61(1); Recital 75 ("Where a third-country firm provides crypto-asset services on the own initiative of a person established in the Union, the crypto-asset services should not be deemed to be provided in the Union.").

[230] *Id*. at Recital 22.

framework could be expanded to impose additional requirements on non-EU parties that provide services to EU clients.

### 3. Addressing Vague or Inadequate Rules

As noted, some of CARF's rules and guidance are vague or lacking.[231] For example, the terms "control" and "sufficient influence" are vague under the current guidance. The application of these rules to partnerships, DAOs, and other arrangements is uncertain. Moreover, the rules and guidance concerning "control" and "sufficient influence" do not appear to include constructive ownership. More challenges involving vague and lacking rules and guidance will likely arise when CARF implementation begins.

The main concern involving vague and lacking rules is that persons with control or sufficient influence may rely on this legal ambiguity to adopt a position that they should not be considered to be RCASPs. Tax authorities may face challenges fighting such positions in courts. To address this risk, the OECD should first identify the rules and guidance that are vague or incomplete. It should then provide further rules and guidance to reduce legal ambiguity and uncertainty.

### 4. Introducing CARF Mandatory Disclosure Rules

Mandatory disclosure rules (MDRs) could be imposed on any person involved in CARF avoidance. Such CARF MDRs could be structured like the CRS MDRs.[232] The CRS MDRs were published by the OECD in 2018 to ensure that taxpayers and their advisers do not circumvent CRS reporting.[233] CRS MDRs list hallmarks to identify two types of schemes: CRS Avoidance Arrangements and Opaque Offshore Structures.[234] A CRS Avoidance Arrangement is generally an arrangement "for which it is reasonable to conclude that it is designed to circumvent or is marketed as, or has the effect of, circumventing CRS Legislation or exploiting an absence thereof."[235] An "opaque offshore structure" is generally an asset-holding structure that allows an individual to be a beneficial owner of certain passive vehicles while disguising this ownership or creating the appearance that the individual is not a beneficial owner.[236]

---

[231] *See supra* Part III.A.2.

[232] OECD, *Model Mandatory Disclosure Rules for CRS Avoidance and Opaque Offshore Structures*, at 14, 24 (Mar. 9, 2018) [hereinafter CRS MDRs], https://www.oecd.org/en/topics/tax-transparency-and-international-co-operation.html [https://perma.cc/R9VM-TJ3F].

[233] *See id.* at 9.

[234] *See id.* at Rules 1.1, 1.2.

[235] *See id.* at Rule 1.1.

[236] *See id.* at Rule 1.2.

Countries that implement CRS MDRs require that these schemes be reported by a broad range of intermediaries, including those who design, market, or implement the reportable schemes, and including persons who are "reasonably . . . expected to know the 'arrangement' or 'structure' is a CRS Avoidance Arrangement or an Opaque Offshore Structure."[237] CRS MDRs include a system of information exchange across jurisdictions.[238]

CARF MDRs could be modeled after CRS MDRs. The reportable schemes could include CARF Avoidance Arrangements that are designed to circumvent or are marketed as, or have the effect of, circumventing CARF reporting or exploiting an absence thereof. Also, CARF MDRs could include Opaque Control Structures designed to allow a person to exercise control or sufficient influence over a platform while disguising the identity of such a person or creating the appearance that the person does not have control or sufficient influence. Similar to other MDRs, the CARF MDRs would likely deter some actors from designing, marketing, or implementing reportable schemes, improve tax authorities' ability to detect these schemes, and enable intelligence gathering.[239]

### 5. Expanding CARF to Decentralized Platforms, Wallet Providers, and Products

The proposals above remain within the existing CARF framework, which only applies to centralized intermediaries—RCASPs and platforms subject to RCASPs' control or sufficient influence. However, as noted in Part III, the exclusion of decentralized platforms would create strong incentives for projects to decentralize and for bad actors to use decentralized platforms. Ensuring full compliance with CARF in its current scope would only increase these incentives. As Bob Michel noted:

> When the CARF was designed in 2021, its future effectiveness was arguably gauged on the assumption that private wallets and decentralized applications would remain marginal phenomena. The crypto winter of 2022 has drastically altered this baseline.

---

[237] *See id.* at Rules 1.3, 2.1. "Relevant services" mean "providing assistance or advice with respect to the design, marketing, implementation or organisation of that Arrangement or Structure." *Id.* at Rule 1.4(g).

[238] *See* OECD, *International Exchange Framework for Mandatory Disclosure Rules on CRS Avoidance Arrangements and Opaque Offshore Structures* (2018), available at https://www.oecd.org/en/publications/international-exchange-framework-for-mandatory-disclosure-rules-on-crs-avoidance-arrangements-and-opaque-offshore-structures_1cf5402b-en.html [https://perma.cc/W3WX-LYBT].

[239] *See* OECD, *Mandatory Disclosure Rules: Action 12*, at 25–26 (2015); Noam Noked & Zachary Marcone, *Targeting Tax Avoidance Enablers*, 13 UC Irvine L. Rev. 1355 (2023); Noam Noked, Zachary Marcone & Alison Tsang, *The Expansion and Internationalization of Mandatory Disclosure Rules*, 13 Colum. J. Tax L. 122 (2022).

> The high-profile CASP bankruptcies have drawn more crypto-users than ever to venture into private wallets and decentralized exchanges, and thus outside the reach of the CARF. The pull towards these technologies will only get stronger once the CARF enters into force . . . . One cannot but harbour the impression that the CARF attempts to catch a new reality with proven but outdated tools.[240]

Policymakers should reconsider the exclusion of decentralized platforms because it may undermine CARF's effectiveness.

The OECD has already stated that it "stands ready to proceed with future amendments to the CARF," emphasizing that "particular attention will be given to the development of DeFi."[241] These statements indicate that the OECD is aware of the potential problems and incentives that CARF's limited scope will likely cause. It is unclear why the OECD has chosen not to address these problems preemptively.

The application of CARF to decentralized platforms would need to include measures to deter the design and introduction of CARF-noncompliant platforms. Such measures could include a prohibition that would carry penalties for founders and other parties that introduce such platforms.[242] In addition to measures that focus on ex-ante prevention and deterrence, there should be some ex-post measures to address CARF-noncompliant platforms. Such measures could prevent access to websites of noncompliant platforms, prohibition of the marketing of these platforms, ban the trade of noncompliant actors' tokens on compliant platforms, and similar measures. As noted, reporting obligations under CARF MDRs should apply to any person providing assistance or advice with respect to the design, marketing, or implementation of these schemes.

### *B. Measures Beyond CARF*

This Article focuses on CARF because it is the international community's main tool against the crypto tax haven.[243] Improvements to CARF could remedy some of its major flaws, as discussed above. Nonetheless, in addition to considering ways to improve CARF, it is important to consider measures beyond CARF to improve transparency and reduce tax evasion and financial crime involving crypto.

---

[240] Michel, *supra* note 180, at 5.

[241] CARF, *supra* note 18, at 12.

[242] *See* Marian, *supra* note 172, at 566–67 (discussing ex-ante regulation of blockchain projects).

[243] Similarly, FATCA and CRS are the main tools against offshore tax evasion involving the traditional financial industry.

### 1. Ensuring Effective Implementation of AML Laws

CARF's effectiveness depends on the quality and effectiveness of the AML/KYC Procedures.[244] If the AML/KYC Procedures are ineffective, tax evaders may not be identified as Reportable Persons because they may not be identified as Controlling Persons, or they may exploit other weaknesses. Thus, ensuring that RCASPs and platforms implement AML/KYC Procedures effectively would improve CARF's effectiveness. In addition, CARF "outsourced" the determination of "control" or "sufficient influence" to the FATF Recommendations and guidance.[245] As long as CARF continues to rely on the FATF for this determination, it is essential to update the FATF Recommendations and guidance to address the vagueness in the current guidance.

### 2. Closing Loopholes in CRS and FATCA

Eliminating some loopholes in CRS and FATCA would make using the crypto tax haven less attractive. For example, CRS and FATCA do not require the reporting of fund deposits and withdrawals to and from depository accounts—only balances at the end of the calendar year and certain types of income should be reported.[246] This means that no CRS or FATCA reporting would generally be required when a tax evader receives cash in his bank account and withdraws or transfers the cash from the account before the end of the year.[247] If CRS and FATCA were to close this loophole by requiring the reporting of aggregate deposits and withdrawals, similar to CARF, the withdrawal of cash from a bank for the purchase of crypto would be reportable. Thus, ensuring that CRS and FATCA facilitate the reporting of fiat-to-crypto transactions makes such transactions less likely to be used for tax evasion.

### 3. Integrating CARF and Regulation Outside CARF

The application of CARF to wallets could be done in conjunction with regulation outside of CARF concerning the use of crypto as a means of payment. For example, it is possible to require merchants to accept payments only from CARF-compliant wallets. This would require setting up an

---

[244] *See supra* Part III.C.4.

[245] CARF, *supra* note 18, at 54 ("Whether an individual or Entity exercises such control or sufficient influence should be assessed in a manner consistent with the 2012 FATF Recommendations (as amended in June 2019 with respect to virtual assets and virtual asset service providers) and related FATF guidance."). Similarly, the term Controlling Person "must be interpreted in a manner consistent with" the FATF Recommendations and guidance. CARF, *supra* note 18, at 23.

[246] *See* Noked, *supra* note 191.

[247] In contrast, CARF eliminates this loophole by requiring the reporting of such transfers. *See* reporting requirements in *supra* note 123.

administratively easy way for merchants to identify which wallet addresses are CARF-compliant.[248] Under this approach, not all wallets will be subject to CARF—compliance with CARF will only be required where the crypto owner would like to use crypto as a means of payment.

#### 4. Other Measures to Increase Transparency and Ensure Tax Compliance

Analysts and scholars have raised additional proposals beyond CARF to ensure tax compliance among crypto owners. Bob Michel noted that "protocol level tax reporting (as in restricting blockchain validation to crypto-asset transactions that are confirmed to be reported for tax purposes) could be the future of comprehensive crypto tax reporting."[249] Manoj Viswanathan proposed scrutinizing blockchain's entry and exit points.[250] Omri Marian proposed to impose a tax on transactions where crypto is used as a means of payment unless the crypto owner agrees to be identified by merchants.[251] He also proposed regulating blockchain applications ex-ante before they are released.[252] For example, ex-ante regulation of programmers, financiers, and ICO issuers can address the challenges in regulating decentralized networks.[253] While these proposals are outside the scope of this Article, the international response to the crypto tax haven should consider these policy options.

### *C. Advantages and Critiques*

The starting point of the discussion in this Article is that CARF will likely become a widely adopted international standard, similar to CRS, which has been implemented by over one hundred seventeen jurisdictions.[254] This is a reasonable prediction, considering that CARF was adopted by the OECD with the support of the G20. Over sixty jurisdictions have recently committed to implementing it, and the EU has already adopted a directive requiring

---

[248] *Cf.* Marian, *A Conceptual Framework for the Regulation of Cryptocurrencies*, *supra* note 49, at 65.

[249] Michel, *supra* note 180, at 6.

[250] *See* Manoj Viswanathan, *Tax Compliance in a Decentralizing Economy*, 34 GA. STATE U. L. REV. 283, 327 (2018).

[251] *Cf.* Marian, *A Conceptual Framework for the Regulation of Cryptocurrencies*, *supra* note 49, at 65 ("Merchants that accept cryptocurrencies as a form of payment would be required to collect a special cryptocurrency-transaction tax based on a percentage of the gross value of any cryptocurrency payment and remit such tax to the IRS. This gross tax would be waived, however, if the consumer were identified by the merchant or by an approved third-party provider that cleared cryptocurrency payments for the merchant. The consumer would effectively be in a position to elect between avoiding the tax by disclosing his or her identity and paying the gross tax to maintain his or her anonymity.").

[252] *See* Marian, *supra* note 172, at 566–67.

[253] *See id.*

[254] *See* OECD, *supra* note 70.

Member States to implement CARF starting in 2026.[255] Recalcitrant countries may face naming, shaming, and blacklisting by the EU, following the EU's policy to blacklist third countries if they do not adopt certain tax transparency standards or amend their tax systems as required by the EU.[256] The EU Member States impose tax and non-tax penalties on blacklisted jurisdictions.[257] By blacklisting and threatening to blacklist jurisdictions, the EU has pressured jurisdictions to implement tax reforms such as CRS and other changes.[258] The EU may adopt a similar approach to ensure a wide implementation of CARF.

Therefore, the relevant policy question for most countries is not whether they should adopt CARF—most countries will adopt it, either voluntarily or under international or EU pressure.[259] The policy question, which is the focus of this Article, is whether CARF would be effective in curbing the use of crypto for tax evasion and financial crime.[260] This Article shows that CARF suffers from substantial weaknesses and loopholes that will likely undermine its effectiveness. The proposed amendments to CARF and measures beyond CARF have the potential to address the crypto tax haven more effectively. This would have societal benefits and potential benefits to compliant actors in the crypto industry.[261] As CARF's basic structure is unlikely to change, the

---

[255] *See supra* text accompanying notes 20–24.

[256] *See generally* Council of the European Union, *Council Conclusions on the Criteria for and Process Leading to the Establishment of the EU List of Non-Cooperative Jurisdictions for Tax Purposes*, 2016 O.J. (C 461) 2; Council of the European Union, *EU list of non-cooperative jurisdictions for tax purposes* (Oct. 17, 2023); Giuseppe Melis & Alessio Persiani, *The EU Blacklist: A Step Forward but Still Much to Do*, EC Tax Rev. 2019-5 (2019); Aija Rusina, *Name and Shame? Evidence from the European Union Tax Haven Blacklist*, 27 Int'l Tax & Pub. Fin. 1364 (2020).

[257] *See* Rusina, *supra* note 256, at 1369–71.

[258] *See, e.g.*, Alexander Özkan, *Cayman Islands Removed from EU Tax Blacklist*, PwC (Oct. 9, 2020) ("Cayman Islands was removed from the EU list after it adopted new reforms to its framework on Collective Investment Funds in September 2020."). While the EU successfully used blacklisting to pressure sizable economies such as South Korea to change their tax laws, it failed to use the blacklisting threat against the United States. *See* Noked & Marcone, *supra* note 16, at 202–03.

[259] Some developing countries that do not host substantial crypto activities may not be required to adopt CARF. In the context of CRS, the countries that have not yet committed to implementing CRS are the following developing countries: Algeria, Angola, Belarus, Benin, Bosnia and Herzegovina, Botswana, Burkina Faso, Cabo Verde, Cambodia, Chad, Congo (Republic of the), Côte d'Ivoire, Djibouti, Dominican Republic, Egypt, El Salvador, Eswatini, Fiji, Gabon, Guatemala, Guinea, Guyana, Haiti, Honduras, Lesotho, Liberia, Madagascar, Mali, Mauritania, Namibia, Niger, North Macedonia, Palau, Philippines, Serbia, Sierra Leone, Tanzania, Togo, Uzbekistan, Vietnam, Zambia, and Zimbabwe. *See* OECD, *supra* note 69. None of these countries is an established financial center where tax evaders are likely to hold funds. It is likely that CARF implementation would follow a similar approach of exempting such jurisdictions.

[260] The regulation proposed in this Article aims to ensure that crypto does not create more tax evasion risk than other asset classes, such as financial assets in the traditional financial industry. This approach follows Marian, *supra* note 49, at 59 ("Regulating cryptocurrencies is not intended to reduce the current level of criminal activity but rather ensure that cryptocurrencies do not increase criminal activity.").

[261] For example, if governments enact measures that effectively reduce the risk of the use of crypto for illicit purposes, they may be more open to allowing mass adoption of crypto as a means of payment, which could benefit compliant crypto businesses.

proposed amendments do not change the basic design of CARF, including the balance it makes between privacy and transparency.[262] Notably, a similar balance has been made in the context of the traditional financial industry, which requires reporting offshore financial assets to the relevant tax authorities.

The proposed amendments to CARF and other measures may increase the compliance costs of affected parties. For example, parties required to file disclosures under CARF MDRs will incur costs related to these disclosures. Notably, compliant actors in the crypto industry will incur substantial costs implementing CARF. Despite incurring these costs, this Article contends that the societal benefits from CARF in its current form will likely be limited. This is because bad actors may be able to continue using crypto for tax evasion and other illicit purposes. As a result, CARF will fail to shut down the crypto tax haven despite imposing substantial compliance costs on compliant actors. The proposed measures would be desirable from a societal perspective if the additional costs are lower than the societal benefits of reducing the use of crypto for illicit purposes.

Moreover, most of the proposed amendments would not cause substantial additional costs for compliant actors. As noted with respect to the proposal concerning the "Active Entity" loophole, compliant RCASPs should have information about the Controlling Persons of private, closely held entities; reporting them would not result in substantial costs. CARF MDRs, registration, and disclosure requirements are unlikely to cause significant costs for compliant RCASPs. In contrast, by design, the measures proposed in this Article would increase costs and risks for noncompliant actors.

## Conclusion

This Article offers two contributions. First, it analyzes vulnerabilities that bad actors might exploit to avoid CARF reporting, delving into how tax evaders could bypass compliant in-scope intermediaries, utilize flaws inherited from CRS, and take advantage of vulnerabilities unique to CARF and the crypto sector. Second, the Article explores policy solutions to these challenges. It proposes amendments to CARF and additional regulatory measures to shut down the crypto tax haven.

The experience with FATCA and CRS should urge policymakers to address CARF's flaws preemptively. For example, a loophole in FATCA and CRS was used to circumvent reporting in the largest individual tax evasion

[262] Advocates of privacy and anonymity of crypto may object to proposals that would improve tax transparency, including proposals to improve CARF's effectiveness. However, as noted, this Article does not engage in the debate on the trade-off that CARF makes between privacy and tax transparency. The main question addressed here is how CARF can be improved to achieve its aims to increase tax transparency and curb the illicit use of crypto.

case in U.S. history.[263] Senator Ron Wyden, the Chairman of the U.S. Senate Committee on Finance that investigated the loophole, said, "[i]t doesn't take a rocket scientist to see how this loophole leads to billions in tax evasion."[264] This loophole could be closed by amending the relevant legal rules in FATCA and CRS.[265] However, despite high-profile investigations by Congress and the Department of Justice, this loophole in FATCA and CRS has not been resolved.[266] This experience suggests that flaws may be hard to rectify after countries have adopted an international standard into their laws and when implementation has started.[267]

CARF is the first international step towards ending the crypto tax haven. The OECD already noted that it "stands ready to proceed with future amendments to the CARF, in case this is needed to ensure adequate tax reporting with respect to Relevant Crypto-Assets, as well as sufficient global coverage of the CARF."[268] This Article calls on the OECD to expedite this process by addressing weaknesses and closing loopholes before bad actors start exploiting them.

---

[263] *See* Finance Committee Report, *supra* note 199, at 3, for its investigation into the "shell bank" loophole. As noted in Noked & Marcone, *supra* note 190, this loophole is not available under CARF. However, as discussed in Part III, bad actors can exploit other loopholes to circumvent CARF reporting.

[264] U.S. Senate Comm. on Fin., *Wyden Investigation Uncovers Major Loophole in Offshore Account Reporting* (Aug. 24, 2022), https://www.finance.senate.gov/chairmans-news/wyden-investigation-uncovers-major-loophole-in-offshore-account-reporting [https://perma.cc/7WBS-NU8A].

[265] *See* Noked & Marcone, *supra* note 190, at 127–40.

[266] *See id*.

[267] *See* Noked, *supra* note 16, at 119.

[268] CARF, *supra* note 18, at 12.