TOWARDS A GLOBAL ANTI-MONEY LAUNDERING LAW FOR CRYPTO-ASSETS

FRANCESCO PAOLO PATTI*

ABSTRACT

As crypto-assets continue to reshape global finance, they present both opportunities and challenges for financial regulation, particularly in anti-money laundering (AML) and countering the financing of terrorism (CFT) enforcement. While pseudonymity and decentralization have fueled concerns over illicit financial activities, blockchain technology itself offers unprecedented transparency and traceability, challenging the misconception that crypto-assets are inherently unregulated and untraceable.

The Financial Action Task Force (FATF) and international regulators have sought to extend AML/CFT frameworks to virtual asset service providers (VASPs) and even decentralized finance (DeFi) protocols. However, applying traditional compliance measures to DeFi raises critical concerns about privacy, innovation, and feasibility. While FATF and the International Organization of Securities Commissions (IOSCO) advocate for identifying "responsible persons" within DeFi arrangements, the enforcement of AML/CFT regulations in fully decentralized ecosystems remains highly problematic, costly, and potentially detrimental to innovation.

This Article argues that a globally coordinated AML/CFT approach is essential to mitigate illicit risks while preserving the transformative potential of blockchain technology. The most practical and effective approach is to focus regulatory oversight on VASPs, which serve as the primary fiat on/off ramps for crypto-assets, instead of expanding regulatory oversight on DeFi participants. Additionally, regulatory technology (RegTech) advancements—such as blockchain analytics, zero-knowledge proofs (ZKPs), and self-sovereign Identity (SSI)—offer privacy-preserving compliance solutions that could balance financial security and decentralization.

Achieving global harmonization in AML/CFT regulation for crypto-assets requires international cooperation, technological innovation, and regulatory adaptability. By fostering dialogue between policymakers, industry participants, and RegTech firms, a unified regulatory framework can emerge—one that effectively prevents financial crime without stifling technological progress in the evolving crypto-asset ecosystem.

---

* Professor of Law and Director of the Dual Degree Bocconi-King's College in Law of Technology and Automated Systems, Bocconi University, Milan, Italy; Council Member of the European Law Institute; Ph.D. Sapienza Università di Roma, Rome, Italy; LL.M. Westfälische Wilhelms-Universität Münster, Münster, Germany; J.D. Università degli Studi Roma Tre, Rome, Italy.

I. INTRODUCTION

The crypto-asset market is experiencing unprecedented growth and global adoption marked by increasing engagement from both retail participants and institutional actors, including major financial institutions and regulatory bodies across jurisdictions such as the United States, the European Union, and parts of Asia, solidifying its place in both mainstream finance and digital culture. Once considered a niche asset class, crypto has now reached key milestones with its total market capitalization surpassing USD 3.5 trillion, reflecting the increasing confidence of both retail and institutional investors.[1] The approval of Bitcoin[2] exchange-traded funds (ETFs) by the U.S. Securities and Exchange Commission (SEC) has opened the door for broader institutional participation,[3] while Ethereum's scaling solutions continue to

1. For current data on the crypto-asset market see *Today's Cryptocurrency Prices by Market Cap*, COINMARKETCAP, https://coinmarketcap.com/ (last visited May 22, 2025); *see also Cryptocurrency Prices, Charts, and Market Capitalizations*, COINGECKO, https://www.coingecko.com/ (last visited May 22, 2025).

2. *See generally* SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM, https://bitcoin.org/bitcoin.pdf; SAIFEDEAN AMMOUS, THE BITCOIN STANDARD: THE DECENTRALIZED ALTERNATIVE TO CENTRAL BANKING (2018) (claiming that Bitcoin with its decentralized, digital scarcity, could serve as a global monetary standard, akin to the role gold played in the past).

3. *See* Gary Gensler, *Statement on the Approval of Spot Bitcoin Exchange-Traded Products*, SEC (Jan. 10, 2024), https://www.sec.gov/news/statement/gensler-statement-spot-bitcoin-011023.

enhance blockchain efficiency.[4] Bitcoin, as the most prominent crypto-asset, has increasingly been considered a potential strategic reserve asset due to its decentralized, scarce, and non-sovereign nature.[5] The White House issued an executive order creating a Strategic Bitcoin Reserve and stating that government-owned Bitcoin transferred into it "shall not be sold and shall be maintained as reserve assets of the United States."[6] At the same time, the rise of so-called "meme coins,"[7] including $Trump, the meme coin owned by companies of U.S. President Donald Trump, showcases crypto's expanding influence in pop culture and speculative markets.[8] An important legislative development occurred with the enactment of the GENIUS Act in July 2025, which establishes, at the federal level, a regulatory framework for payment stablecoins.[9]

---

4. For more information about Ethereum's scaling mechanism see the post *Scaling*, ETHEREUM.ORG (Feb. 13, 2025), https://ethereum.org/en/developers/docs/scaling/.

5. *See* Pavel Ciaian et al., *The Economics of Bitcoin Price Formation*, 48 APPLIED ECON. 1799, 1799 (2016); Adam S. Hayes, *Bitcoin Price and its Marginal Cost of Production: Support for a fundamental Value*, 26 APPLIED ECON. LETTERS 554, 554 (2019); Murray A. Rudd & Dennis Porter, *A Supply and Demand Framework for Bitcoin Price Forecasting*, 18 J. RISK FINANCIAL MANAG. 66, 68 (2025).

6. Exec. Order No. 14233, 90 F.R. 11789 (Mar. 6, 2025). See also prior discussions among policymakers: Gertrude Chavez-Dreyfuss & Lisa Pauline Mattackal, *How would a U.S. bitcoin strategic reserve work?*, REUTERS (Dec. 17, 2024, at 15:22 ET), https://www.reuters.com/technology/how-would-us-bitcoin-strategic-reserve-work-2024-12-16/(reporting that Senator Cynthia Lummis proposed that the U.S. Treasury acquire up to 1 million bitcoins over five years to establish a strategic reserve). On the contrary, Christine Lagarde, President of the European Central Bank (ECB), has firmly rejected speculation about the ECB holding Bitcoin as a reserve asset. "Reserves must be liquid, secure, and safe," Lagarde stated, emphasizing that Bitcoin does not meet these criteria due to its high volatility and associated risks, including money laundering and illicit activities. *See* Pietro Cingari, *Lagarde hints at further ECB rate cuts, rules out Bitcoin reserves*, EURONEWS (30 Jan. 2025, at 16:35 GMT+1), https://www.euronews.com/business/2025/01/30/lagarde-hints-at-further-ecb-rate-cuts-rules-out-bitcoin-reserves.

7. For more information on "meme" coins see Division of Corporation Finance, *Staff Statement on Meme Coins*, SEC (Feb. 27, 2025), https://www.sec.gov/newsroom/speeches-statements/staff-statement-meme-coins.

8. Vicky Ge Huang, *$TRUMP Is Already Worth Billions. What to Know About the Meme Coin*, WALL ST. J. (Jan. 23, 2025, at 17:18 ET), https://www.wsj.com/finance/trump-meme-coin-crypto-explained-c881afff.

9. *See* Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act), Pub. L. No. 119-27, 139 Stat. 419 (2025) (codified at 12 U.S.C. §§ 5901-5916) (creating a comprehensive federal regime for "payment stablecoins," i.e., digital assets designed to maintain a stable value relative to a specified monetary unit—typically the U.S. dollar—backed by low-risk reserves such as cash or Treasury securities; the Act establishes licensing of permitted issuers, reserve and audit requirements, AML/CFT compliance, and consumer-protection and insolvency-priority rules). See also *Fact Sheet: President Donald J. Trump Signs GENIUS Act into Law*, WHITE HOUSE (July 18, 2025), https://www.whitehouse.gov/fact-sheets/2025/07/fact-sheet-president-donald-j-trump-signs-genius-act-into-law; *The GENIUS Act of 2025: Stablecoin Legislation Adopted in the U.S.*, LATHAM & WATKINS LLP (July 24, 2025), https://www.lw.com/en/insights/the-genius-act-of-2025-stablecoin-legislation-adopted-in-the-us.

Nonetheless, there remains a persistent concern and underlying fear regarding the illicit use of decentralized infrastructures and digital assets.[10] Due to the pseudonymous nature of blockchain transactions,[11] crypto-assets have often been associated with money laundering, illicit trade, and cybercrime, reinforcing a strong prejudice against their legitimacy.[12] This skepticism continues to be a major barrier to full institutional acceptance, as many traditional financial players, like banks and investment firms, remain cautious about integrating crypto into their operations.[13]

This skepticism is fueled by infamous cases of illicit activity tied to crypto-assets, such as the Silk Road and the operations of the North Korean Lazarus Group. Launched in 2011 by Ross Ulbricht, under the alias "Dread Pirate Roberts," Silk Road operated as a dark web marketplace, facilitating the anonymous sale of drugs, weapons, fake documents, and hacking services.[14] Using Bitcoin as its primary currency, the platform thrived until authorities infiltrated and shut it down in 2013, seizing

10. *See* Edgar G. Sanchez, *Crypto-Currencies: The 21st Century's Money Laundering and Tax Havens*, 28 U. FLA. J.L. & PUB. POL'Y 167, 180–187 (2017); Lerong Lu, *Bitcoin: Speculative Bubble, Financial Risk and Regulatory Response*, 33 BUTTERWORTHS J. INT'L BANKING & FIN. L. 178, 180 (2018).

11. Blockchain transactions are pseudonymous rather than fully anonymous because participants are identified on-chain only by their public key or wallet address, not by a civil identity. Each transaction is permanently linked to these cryptographic identifiers, creating a traceable history. When data is "pseudonymous", personal data can be attributed to a specific person with the use of additional information: see Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), art. 4(5) 2016 O.J. (L 119) 33 (defining "pseudonymization").

12. *See* Gail-Joon Ahn et al., *Ransomware and Cryptocurrency: Partners in Crime*, *in* CYBERCRIME THROUGH AN INTERDISCIPLINARY LENS 106, at 106–126 (Thomas Holt ed., 2016); *see generally* Daniel Dupuis & Kimberly Gleason, *Money laundering with Cryptocurrency: Open Doors and the Regulatory Dialectic*, 28 J. FIN. CRIME 60 (2020).

13. *See* Andrew R. Chow, *The Significance of Jamie Dimon's Reluctant Bitcoin Surrender*, TIME (May 20, 2025), https://time.com/7287164/jpmorgan-chase-bitcoin-jamie-dimon (reporting that Jamie Dimon, longtime critic of Bitcoin and CEO of JPMorgan Chase, announced in May 2025 that the bank would permit clients to purchase Bitcoin, while reiterating concerns over its links to illicit activity).

14. *See generally* Paul Vigna, *Justice Department Seizes $1 Billion of Bitcoin Tied to Silk Road Website Agency says a hacker stole funds in 2012, 2013 from drug website, left untouched for years*, WALL ST. J. (Nov. 5, 2020), https://www.wsj.com/articles/justice-department-seizes-1-billion-of-bitcoin-tied-to-silk-road-website-11604612072; specifically on the role of Bitcoin, see JACK PARKIN, MONEY CODE SPACE: HIDDEN POWER IN BITCOIN, BLOCKCHAIN AND DECENTRALIZATION 40 (2020). For analysis of the judicial proceeding concerning Ulbricht, see also DANIEL T. STABILE ET AL., DIGITAL ASSETS AND BLOCKCHAIN TECHNOLOGY: U.S. LAW AND REGULATION 299–315 (2020).

144,000 BTC.[15] Ulbricht was convicted of money laundering, conspiracy, and drug trafficking, receiving a life sentence in 2015, marking a defining moment in the intersection of crypto-assets and cybercrime enforcement.[16]

Similarly, the Lazarus Group, a state-sponsored North Korean hacking collective, has exploited crypto-assets to finance illicit activities, including nuclear weapons programs.[17] The group has been linked to high-profile crypto heists, such as the USD 620 million Ronin Network hack,[18] the USD 280 million KuCoin hack,[19] and more recently the USD 1.5 billion Bybit hack,[20] using sophisticated money laundering techniques, mixers, and decentralized finance (DeFi) exploits to obfuscate stolen funds. Their activities have prompted global regulatory responses, reinforcing concerns that decentralized assets can be weaponized for cybercrime, sanctions evasion, and geopolitical threats.[21]

Given these significant risks, anti-money laundering (AML) and countering the financing of terrorism (CFT) law emerges as a crucial response to the challenges posed by the illicit use of crypto-assets and blockchains. Many believe that with strong regulatory frameworks, improved transaction monitoring, and international cooperation, policymakers and enforcement agencies can reduce the misuse of digital assets while still preserving

15. *Id.*

16. In January 2025, President Trump granted clemency to Ross Ulbricht. *See* Alexander Osipovich, *Crypto Industry Cheers Trump's Pardon of Silk Road Founder Ross Ulbricht*, WALL ST. J. (Jan. 22, 2025), https://www.wsj.com/livecoverage/stock-market-today-dow-sp500-nasdaq-live-01-22-2025/card/crypto-industry-cheers-trump-s-pardon-of-silk-road-founder-ross-ulbricht-TkQymCxRCyWua1QFz0oy.

17. *See* Kole Zellers, *Hacked! North Korea's Billion-Dollar Crypto Heisting Scheme*, 12 PENN ST. J.L. & INT'L AFF. 260, 264–268 (2024).

18. *See* Joe Tidy, *Ronin Network: What a $600m hack says about the state of crypto*, BBC (Mar. 30, 2022), https://www.bbc.com/news/technology-60933174; *see also* Paul Vigna, *U.S. Agency Links North Korea Crime Ring to $540 Million Axie Infinity Crypto Hack*, WALL ST. J. (Apr. 14, 2022), https://www.wsj.com/articles/u-s-agency-links-north-korea-crime-ring-to-540-million-axie-infinity-crypto-hack-11649966631.

19. *See* Michelle Nichols & Raphael Satter, *U.N. Experts Point Finger at North Korea for $281 million cyber theft, KuCoin likely victim*, REUTERS (Feb. 10, 2021), https://www.reuters.com/article/technology/un-experts-point-finger-at-north-korea-for-281-million-cyber-theft-kucoin-liidUSKBN2AA08T/.

20. *See* Justin McCurry, *North Korea behind $1.5bn hack of Crypto Exchange ByBit, says FBI*, THE GUARDIAN (Feb. 27, 2025), https://www.theguardian.com/world/2025/feb/27/north-korea-bybit-crypto-exchange-hack-fbi.

21. *See* EUR. SEC. AND MARKS. AUTH., DECENTRALISED FINANCE IN THE EU: DEVELOPMENTS AND RISKS 9 (2023), https://www.esma.europa.eu/sites/default/files/2023-10/ESMA50-2085271018-3349_TRV_Article_Decentralised_Finance_in_the_EU_Developments_and_Risks.pdf.

their legitimate financial and technological benefits.[22]

This Article contends that only through global coordination among states, involving the adoption of harmonized regulatory standards and cross-border enforcement mechanisms, can an effective and resilient framework for crypto-asset governance be established. Such coordination is imperative to address jurisdictional fragmentation, reduce regulatory arbitrage, and ensure a unified response to the misuse of digital assets. However, it is equally critical that this regulatory framework be designed in a manner that does not hinder the innovative potential of DeFi. The unique technological attributes of blockchain—including decentralization, immutability, transparency, cryptographic security, smart contract automation, and global accessibility—position the crypto-asset industry to address regulatory challenges proactively, while maintaining its capacity to drive financial innovation and inclusion.[23]

Part II of this Article will highlight the specific risks of illicit activities associated with blockchain and crypto-assets. Contrary to widespread belief, it will clarify that the very nature of blockchain technology provides effective tools for identifying and tracking user misconduct. Part III will examine regulatory interventions and ongoing challenges, while Part IV will outline a path forward for public blockchains and DeFi, aiming to safeguard innovation. Finally, Part V will conclude with a comprehensive assessment and a call for global coordination to ensure effective compliance among professional intermediaries operating in the crypto-asset sector.

II. True and False Assumptions on Crypto-assets and Blockchain

Blockchain technology and crypto-assets present both regulatory challenges and compliance opportunities in the context of AML/CFT. The first section of this discussion explores the risks associated with blockchain transactions, highlighting their pseudonymous nature, the role of privacy-enhancing assets, and the challenges posed by DeFi platforms and privacy-enhancing tools such as Tornado Cash. It also examines how weak enforcement in certain jurisdictions allows illicit actors to exploit regulatory gaps.

The second section demonstrates that blockchain technology is not inherently untraceable. On the contrary, blockchain analytics and

22. *See e.g.*, Rebecca Rettig, Michael Mosier & Katja Gilman, *Genuine DeFi as Critical Infrastructure: A Conceptual Framework for Combating Illicit Finance Activity in Decentralized Finance*, SSRN, Jan. 29, 2024, https://ssrn.com/abstract=4607332.

23. *See* Hadar Y. Jabotinsky, *The Network Effects of International Crypto and DLT Regulation*, 57 Vand. J. Transnat'l L. 1285, 1296-1301 (2024).

regulatory technology (RegTech) solutions have rapidly evolved to provide tools that help track financial flows, identify suspicious activity, and enhance AML/CFT compliance. By contrasting the risks and solutions, this discussion underscores how regulatory disparities remain the key issue in the fight against illicit financial activities in the blockchain ecosystem.

A. *The Dangers of Blockchain and Crypto-Assets from an AML/CFT Perspective*

Crypto-assets and blockchain technology pose significant challenges from an AML/CFT perspective due to their pseudonymous nature[24] that does not allow one to directly identify users, lack of centralized oversight, and capacity for cross-border and instantaneous transactions. Unlike traditional financial systems, blockchain transactions are recorded on a public ledger but do not require identity verification, making it difficult to trace ownership and assess risk with regard to potential links to illicit activities. For example, the ransom payment resulting from an extortion scheme could be instantly transferred to another continent using blockchain, through a system that makes it extremely difficult to trace the identities of the parties involved. This would be absolutely impossible with cash, the most commonly used payment method in illicit activities.

Also, the presence of privacy-enhancing crypto-assets such as Monero[25] and Zcash[26] poses specific risks.[27] Unlike Bitcoin, where all transactions are permanently recorded on a transparent blockchain, these crypto-assets implement advanced cryptographic techniques to ensure transactional privacy. Monero, launched in 2014, employs ring signatures, stealth addresses, and Ring Confidential Transactions (RingCT) to effectively obfuscate transaction origins, amounts, and recipient details, making

24. *See* Regulation 2016/679. art. 4(5) 2016 O.J. (L 119) 33.

25. *Monero Means Money*, MONERO, https://www.getmonero.org/ (last visited May 14, 2025).

26. *Zcash is encrypted electronic cash*, ZCASH, https://z.cash/ (last visited May 14, 2025).

27. *See* Alex Marthews & Catherine Tucker, *Blockchain and Identity Persistence, in* CRYPTOASSETS: LEGAL, REGULATORY, AND MONETARY PERSPECTIVES 243, 245 (Chris Brummer ed., 2019) (arguing that privacy coins "focus their efforts on obscuring the connection between a transaction on the blockchain and a particular, static digital identity"); Gioia Arnone, *Security and Privacy in the Digital Currency Space, in* NAVIGATING THE WORLD OF CRYPTOCURRENCIES, 63, 70–77 (2024) (exploring the regulatory and ethical dimensions of security and privacy in the crypto-assets space with reference to Monero and Zcash); ERIK SILFVERSTEN ET AL., EXPLORING THE USE OF ZCASH CRYPTOCURRENCY FOR ILLICIT OR CRIMINAL PURPOSES 34 (2020), https://www.rand.org/pubs/research_reports/RR4418.html (indicating that Zcash has only a minor presence on the dark web, indicating that Zcash is seen as a less attractive option to dark web users and is used less often compared to other cryptocurrencies, particularly Bitcoin and Monero).

fund movements virtually untraceable.[28] Similarly, Zcash, introduced in 2016, offers users the option of shielded transactions using zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge), allowing transaction validation without revealing sensitive details.[29] While Zcash provides users with the ability to choose between transparent and shielded transactions, Monero enforces privacy by default. These features, though serving a legitimate purpose in protecting financial data and ensuring confidentiality in sensitive transactions, raise concerns over their potential misuse for money laundering, ransomware payments, darknet transactions, and other illicit activities.[30]

Obfuscation tools like mixers and tumblers further complicate regulatory oversight by allowing users to anonymize transactions.[31] A known example is Tornado Cash, a privacy-focused protocol on the Ethereum (ETH) blockchain that allows users to make anonymous crypto-asset transactions.[32] Normally, when someone sends or receives ETH or other crypto-assets on the Ethereum blockchain, the transactions are recorded on the public blockchain,[33] making it possible to trace the flow of funds. To understand the problems with the anonymity provided by Tornado Cash, it is useful to outline the basic functioning of the protocol in three main steps. First, a user deposits crypto-assets into Tornado Cash's smart contract, which records the deposit without linking it to the sender's identity.[34] Second, the deposited funds are mixed with other users' deposits in a shared liquidity pool, making it difficult to determine the original source of any particular withdrawal.[35] Finally, the user can withdraw the same amount of crypto-assets to a different

28. *See Monero: All About the Top Privacy Coin*, CHAINALYSIS (May 4, 2023), https://www.chainalysis.com/blog/all-about-monero/; *The Rise of Monero: Traceability, Challenges, and Research Review*, TRM (Oct. 8, 2024), https://www.trmlabs.com/post/the-rise-of-monero-traceability-challenges-and-research-review.

29. *Privacy Coins 101: Anonymity-Enhanced Cryptocurrencies*, CHAINALYSIS (Apr. 18, 2023), https://www.chainalysis.com/blog/privacy-coins-anonymity-enhanced-cryptocurrencies/.

30. *See* Dupuis & Gleason, *supra* note 12, at 63-66.

31. *See* Usman W. Chohan, *The Cryptocurrency Tumblers: Risks, Legality and Oversight* 1, at 2-4 (Nov. 30, 2017), https://ssrn.com/abstract=3080361; Jan Zavřel et al., *Tumbling down the stairs: Exploiting a tumbler's attempt to hide with ordinary-looking transactions using wallet fingerprinting*, 52 FORENSIC SCI. INT'L: DIGIT. INVESTIGATION, 301869, 301869-70 (2025), https://doi.org/10.1016/j.fsidi.2025.301869.

32. *See* Matthias Nadler & Fabian Schär, *Tornado Cash and Blockchain Privacy: A Primer for Economists and Policymakers* 1, at 3-7, FED. RSRV. BANK OF ST. LOUIS REV. (2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4352337.

33. They can be seen and analyzed through a so-called block explorer. *See e.g. The Ethereum Blockchain Explorer*, ETHERSCAN, https://etherscan.io/ (last visited May 22, 2025).

34. *See* Nadler and Schär, *supra* note 31, at 127–28.

35. *Id.*

wallet address, effectively breaking the link between the sender and the receiver.[36] This process enhances privacy by obscuring transaction histories, making it harder for external parties to track financial movements. However, because of its ability to anonymize transactions, Tornado Cash became controversial, as evidenced by the U.S. Treasury sanctioning it for facilitating illicit financial flows. In particular, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) has sanctioned Tornado Cash for laundering over seven billion USD in cryptocurrency since 2019, including funds linked to North Korea's Lazarus Group and major cyber heists.[37] The Treasury asserts that Tornado Cash failed to implement effective controls to prevent illicit use, facilitating money laundering for cybercriminals despite public assurances to the contrary.[38]

DeFi platforms, designed for the conduct of peer-to-peer or system-to-system economic activities, operate without intermediaries.[39] This creates additional vulnerabilities by enabling anonymous lending, staking, and trading through smart contracts. In practice, holders of illicit assets are not merely able to transfer them globally with ease; they may also engage in complex trading strategies that generate additional profits. At the same time, non-fungible tokens (NFTs)[40] marketplaces have introduced novel money laundering risks through self-wash trading and high-value transactions with minimal regulatory scrutiny.[41] In

36. *Id.*

37. Press Release, U.S. Department of the Treasury, U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash (Aug. 8, 2022), https://home.treasury.gov/news/press-releases/jy0916.

38. *Id.*

39. *See* Fabian Schär, *Decentralized Finance: On Blockchain- and Smart Contract based Financial Markets*, 103 FED. RES. BANK OF ST. LOUIS Rev. 153, 153-55 (2021); *see also* Aaron Wright, *The Growth & Regulatory Challenges of Decentralized Finance*, 17 N.Y.U. J. L. & BUS. 686, 687–690 (2021); Justin Doop, *Decentralized Finance*, 6 GEO. L. TECH. REV. 373, 373–374 (2022); Vanessa V. Collao, *DeFi: A Framework of the Automated Financial System*, 26 TUL. J. TECH. & INTELL. PROP. 75, 91–108 (2024); Eric W. Hess, *Bridging Policy and Practice: A Pragmatic Approach to Decentralized Finance, Risk, and Regulation*, 128 PENN ST. L. REV. 347, 380–384. On the self-executing character of smart contracts and its legal implications, see generally Pietro Sirena & Francesco P. Patti, *Smart Contracts and Automation of Private Relationships, in* CONSTITUTIONAL CHALLENGES IN THE ALGORITHMIC SOCIETY 315, at 315–319 (Hans-W. Micklitz et al. eds., 2021).

40. NFTs differ fundamentally from traditional cryptocurrencies. Unlike Bitcoin or Ethereum, which are fungible and interchangeable at equal value, NFTs are unique digital assets, each possessing distinct characteristics that prevent them from being exchanged on a one-to-one basis. *See* Cathy Hackl, *Non-Fungible Tokens 101: A Primer On NFTs For Brands And Business Professionals*, FORBES (Feb. 28, 2021), https://www.forbes.com/sites/cathyhackl/2021/02/28/non-fungible-tokens-101-a-primer-on-nfts-for-brands–business-professionals/.

41. *See* Sofia Aizenman, *The Art World of Digital Assets: How Non-Fungible Tokens Create a Loophole in Anti-Money Laundering Regulations*, 44 CARDOZO L. REV. 1179, 1186-90, 1199-1200 (2023)

essence, the decentralized and permissionless nature of these markets enables access to financial services that facilitate the reuse and circulation of illicit funds.[42]

These risks are compounded by weak enforcement in certain jurisdictions, where offshore centralized exchanges and unregulated financial services provide opportunities for illicit actors to evade detection and launder funds outside the reach of stringent compliance measures. However, many countries—particularly in the Western world—have taken significant regulatory steps to strengthen oversight of cryptocurrency exchanges, recognizing their gatekeeper role in facilitating the conversion of crypto-assets into fiat currency and vice versa.[43] By tightening controls on these "fiat on- and off-ramping solutions," regulators aim to reduce the risk of illicit financial flows, enhance market transparency, and integrate crypto-assets more securely into the global financial system.[44]

Gaps still exist, particularly in jurisdictions that lack uniform regulation or where enforcement remains lax, allowing bad actors to exploit regulatory arbitrage and move illicit funds through less compliant platforms.[45] In other words, due to legislative advancements, off-ramping

(arguing that the digitalization of art transactions, particularly through NFTs, exacerbates money laundering risks, the authors highlight how the art world's long-standing secrecy is further intensified in the digital space, making it even more challenging to trace illicit transactions.).

42. *See* Caroline A. Crenshaw, *DeFi Risks, Regulations, and Opportunities*, 1 INT'L. J. BLOCKCHAIN L. 4, (2021); ANNE CHONE ET AL., DECENTRALISED FINANCE IN THE EU: DEVELOPMENTS AND RISKS 8 (2023) ("DeFi is especially vulnerable to scams and illicit activities, since virtually anyone can create or interact with DeFi protocols without the need to identify oneself and go through 'know your customer' checks. DeFi development has progressed to the point where templates allow for the creation of a token in a matter of minutes without any programming knowledge or experience. Malevolent people can use the technology to anonymously create malicious decentralised applications, which have no other purpose than to deprive users of their money"). DeFi platforms often grant a certain level of control to a select group of individuals operating behind the project through the use of so-called "admin keys": Max Parasol, *Enforcing Persistent "Smart Contracts": Admin Keys and the Myth of Decentralized Finance?*, 24 N. C. J. L. & TECH. 67, 102–112 (2023). *See* Jabotinsky, *supra* note 22, at 1297.

43. *See* Sarah Jane Hughes, *"Gatekeepers" Are Vital Participants in Anti-Money-Laundering Laws and Enforcement Regimes as Permission-less Blockchain-Based Transactions Pose Challenges to Current Means to "Follow the Money"*, IND. LEGAL STUDIES RESEARCH PAPER No. 408, 1, at 12 (2019), https://ssrn.com/abstract=3436098 (arguing that, while regulated gatekeepers may not eliminate the future need for new laws or enforcement tools, their current role in crypto markets helps reduce the urgency for immediate action and gives lawmakers time to assess developments before deciding on further regulation).

44. *See* Roee Sarel, Hadar Y. Jabotinsky & Israel Klein, *Globalize Me: Regulating Distributed Ledger Technology*, 56 VAND. L. REV. 435, 448 (2023).

45. On the risk of anti-money laundering related to centralized crypto-assets service providers, see Marco Dell'Erba, *Crypto-Trading Platforms as Exchanges*, 2024 MICH. ST. L. REV. 1, 37-42 (2024). *See also* Eric D. Chason, *Regulating Crypto Intermediaries*, 108 MARQ. L. REV. 187, 234–35 (2024).

significant amounts of illicit funds through a centralized exchange under the regulatory scrutiny of a European or a U.S. authority appears challenging. Still, the same activity may be more easily carried out in jurisdictions with weaker oversight, where stringent regulations and enforcement on and against crypto intermediaries are absent.[46]

B. *Compliance Tools Developed for Blockchain Technology*

Undeniably, several risks affect the operations of blockchain technology from an AML/CFT perspective. Nonetheless, there are several misconceptions regarding activities conducted over a blockchain network. Whereas cash transactions are entirely anonymous and leave no trace, crypto-asset transactions are permanently recorded on the blockchain, creating an immutable and publicly accessible ledger. While blockchain users' public addresses themselves are pseudonymous rather than directly linked to real-world identities,[47] the transparency of networks like Bitcoin or Ethereum allows for the tracking of transaction histories, wallet balances, and interactions between addresses. This means that, rather than enabling untraceable financial flows, blockchain technology actually provides a valuable source of transactional data. As a result, blockchain analytics tools have become essential in detecting and mitigating AML/CFT risks by mapping out transactional patterns and flagging suspicious behavior.[48]

---

46. *See High-Risk Jurisdictions Subject to a Call for Action - February 2024*, FINANCIAL ACTION TASK FORCE (FATF) (Feb. 23, 2024), https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Call-for-action-february-2024.html (listing the Democratic People's Republic of Korea (North Korea), Iran, and Myanmar as jurisdictions with serious strategic deficiencies in their anti-money laundering (AML) and counter-terrorist financing (CFT) regimes, subject to enhanced scrutiny and countermeasures); *Jurisdictions Under Increased Monitoring*, FATF, (Feb. 23, 2024), https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Increased-monitoring-february-2024.html (identifying jurisdictions actively working to improve AML/CFT frameworks but still facing significant challenges).

47. On the pseudonymous character of public addresses recorded on blockchains, see Michèle Finck, *Blockchains and Data Protection in the European Union*, EUR. DATA PROTECTION L. REV. 17, 24 (2018) ("Public keys are a string of letters and numbers that allows for the pseudonymous identification of a natural or legal person for transactional or communication purposes"); Ammar Zafar, *Reconciling blockchain technology and data protection laws: regulatory challenges, technical solutions, and practical pathways*, 11 J. CYBERSECURITY 1, 13 (2025).

48. *See e.g.*, Jiajing Wu et al., *From Shadows to Light: Uncovering Money Laundering in Ethereum Transaction Graphs*, SSRN, Dec. 30, 2024, https://ssrn.com/abstract=5076472 (conducting an empirical analysis of money laundering patterns on Ethereum, comparing laundering accounts with regular accounts across three key aspects: transaction network topology, transaction temporal characteristics, and transaction amount characteristics).

Given the technological nature of blockchains and the capabilities of smart contracts, the technology itself offers innovative RegTech solutions that can significantly aid in mitigating AML risks. RegTech refers to the application of technology-driven compliance tools that streamline regulatory processes, enhance oversight, and improve financial crime detection and prevention.[49] Within the realm of blockchain and crypto-assets, RegTech solutions leverage real-time data analytics, automation, and machine learning algorithms to monitor transactions, detect suspicious activities, and ensure compliance with AML/CFT frameworks. One of the most prominent areas where blockchain technology assists in AML compliance is blockchain analytics, a field that has grown considerably with the rise of crypto-assets adoption and increased regulatory scrutiny. Several leading firms, such as Chainalysis,[50] TRM Labs,[51] and Elliptic,[52] have developed sophisticated blockchain forensic tools that allow regulators, law enforcement agencies, and financial institutions to trace the movement of crypto-assets across blockchain networks. These firms analyze on-chain transaction patterns, identify high-risk wallet addresses, and flag potential illicit financial flows linked to money laundering, terrorism financing, ransomware attacks, and other financial crimes. Their methodologies rely on tracking known illicit wallets, mapping out the movement of funds, and connecting blockchain transactions to real-world entities, allowing authorities to intervene, freeze assets, and disrupt criminal activities.[53]

Contrary to the widespread belief that crypto-assets offer complete anonymity, blockchain analytics firms have demonstrated that most crypto transactions are highly traceable due to the public and immutable

49. *See* LERONG LU, GLOBAL FINTECH REVOLUTION 67-72 (2024) (referring that popular applications of RegTech include compliance solutions relating to KYC, AML and CFT).

50. *See generally* CHAINALYSIS, https://www.chainalysis.com/ (last visited May 13, 2025).

51. *See generally* TRM, https://www.trmlabs.com/ (last visited May 13, 2025).

52. *See generally* ELLIPTIC, https://www.elliptic.co/ (last visited May 13, 2025).

53. In English common law, see Elena Vorotyntseva v. Money-4 Ltd. t/a Nebeus.Com [2018] EWHC (Ch) 2596 [10]-[13] (UK) (granting a freezing order over substantial holdings of Bitcoin and Ethereum due to a real risk of dissipation); AA v. Persons Unknown & Ors, Re Bitcoin, [2019] EWHC (Comm) 3556 [63] (UK) (holding that cryptocurrencies constitute property under English law, and granting a proprietary injunction and disclosure orders following a ransomware payment traced by a specialist blockchain analytics firm); Ion Science Ltd. v. Persons Unknown & Ors. [2020] (Comm) [1], [18] (UK) (granting a worldwide freezing order, a proprietary injunction, and a *Bankers Trust* order against cryptocurrency exchanges to preserve Bitcoin linked to an alleged ICO fraud and to compel disclosure of account information for the purpose of identifying the perpetrators).

nature of blockchain ledgers.[54] Every transaction on a public blockchain is recorded in a way that ensures data permanence and transparency, enabling forensic tools to reconstruct entire transactional histories and follow the flow of illicit funds across multiple wallet addresses.[55] Although users are not directly identified by their real names, blockchain transactions are linked to public addresses—alphanumeric strings that function as identifiers for wallets holding digital assets. This feature, as previously stated, makes blockchain pseudonymous rather than fully anonymous, meaning that while wallet addresses do not directly reveal a user's identity, they can still be associated with real-world individuals or entities through additional data points. One of the critical ways in which blockchain analytics firms de-anonymize transactions is by combining on-chain data with off-chain intelligence. By linking transactions to known crypto-assets' exchange addresses, darknet markets, or illicit actors, blockchain forensic tools help law enforcement agencies map out entire criminal networks operating within the crypto ecosystem.[56]

Furthermore, IP addresses, geolocation data, and behavioral analytics can be leveraged to associate a given public address with a specific individual. For instance, when a user interacts with a centralized crypto-asset exchange that enforces Know Your Customer (KYC) regulations, such as Binance,[57] Coinbase[58] or Kraken,[59] their personal information—including their identity documents and banking details—is collected. If this user later engages in suspicious activities, blockchain analytics firms can track and correlate their on-chain movements to these verified exchange accounts, effectively exposing their identity. Additionally, even in DeFi environments where KYC requirements are absent, other

54. *See* Sahil Dudani et al., *The Current State of Cryptocurrency Forensics*, 46 FORENSIC SCI. INT'L: DIGITAL INVESTIGATION (2023), https://doi.org/10.1016/j.fsidi.2023.301576; Hany F. Atlam et al., *Blockchain Forensics: a Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions*, 13 ELECTRONICS 3568, 3571-74 (2024) (providing a comprehensive investigation of the fundamental principles of blockchain forensics, exploring various techniques and applications for conducting digital forensic investigations in blockchain).

55. Shivani Jamwal et al., *A survey on Ethereum pseudonymity: Techniques, challenges, and future directions*, 232 J. NETWORK & COMP. APPLICATIONS 104019, 104021-22 (2024), https://www.sciencedirect.com/science/article/abs/pii/S1084804524001966.

56. Gurvais Grigg, *Law Enforcement in the Age of Cryptocurrency*, POLICE1 (Jan. 6, 2025), https://www.police1.com/investigations/law-enforcement-in-the-age-of-cryptocurrency.

57. *See How to Complete KYC on Binance: A Simple Guide*, BINANCE Square, https://www.binance.com/en/square/post/15917991332305 (last visited June 29, 2025).

58. *See Know-your-customer (KYC) verification*, COINBASE, https://www.coinbase.com/th/blog/know-your-customer-kyc-verification (last visited June 29, 2025).

59. *See Know Your Customer (KYC) Questionnaire*, KRAKEN SUPPORT, https://support.kraken.com/hc/en-us/articles/know-your-customer-kyc-questionnaire (last visited June 29, 2025).

identifiers—such as transaction timing, recurring interactions with centralized entities, and even metadata left behind in smart contract interactions—can contribute to re-identifying individuals behind pseudonymous addresses. The ability to trace illicit financial flows through blockchain analytics tools challenges the misconception that crypto-assets are untraceable tools for money laundering. In reality, the transparency and auditability of blockchain networks make them more traceable than many traditional financial systems—a stark contrast to cash-based transactions, which offer complete anonymity and are far more difficult to track. This aspect of blockchain presents a paradox in the regulatory debate: while decentralized technologies do introduce challenges to AML enforcement, they simultaneously provide powerful new tools for financial surveillance and compliance automation. By harnessing RegTech solutions and blockchain analytics, regulators and law enforcement agencies have an unprecedented ability to monitor, track, and intervene in illicit financial activities occurring within the crypto ecosystem.

In conclusion, it is incorrect to claim that blockchain avoids the identification of its users or the tracing of individuals operating within it due to the supposed anonymity of transactions. While the technology carries inherent risks related to the pseudonymization of addresses and the absence of traditional intermediaries, the industry has developed sophisticated blockchain analytics tools that enable the reconstruction of financial flows and the identification of individuals involved in illicit activities. These increasingly advanced countermeasures demonstrate that the application of RegTech solutions and appropriate investigative methodologies makes forensic investigations in the cryptocurrency sector not only possible but progressively more effective. The primary challenge lies in the inconsistent application of emerging AML/CFT regulations across different jurisdictions. This regulatory disparity allows many intermediaries to operate without adhering to best practices, creating gaps in oversight that can be exploited for money laundering activities due to inadequate compliance measures and weak enforcement mechanisms.

III. THE REGULATORY RESPONSE: THE DIFFICULTIES OF ADAPTING COMPLIANCE

Since the launch of Bitcoin in 2009,[60] blockchain technology has been framed as a disruptive force challenging traditional legal frameworks, encapsulated by the slogan "Code is Law."[61] The foundational vision was

60. Ciaian et al., *supra* note 5, at 1801.

61. *See* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 6 (1999) ("We can build, or architect, or code cyberspace to protect values that we believe are fundamental, or we can build,

to create a decentralized system, free from intermediaries and financial oversight, where transactions could be executed autonomously through cryptographic protocols and smart contracts.[62] Given this ethos of decentralization, it is unsurprising that blockchain technology presents inherent challenges in the realm of regulatory compliance. In the early years of Bitcoin and other blockchains, the absence of clear regulations, coupled with the legal uncertainty surrounding the classification of crypto-assets, facilitated transactions that operated outside financial controls.[63] However, as the crypto ecosystem evolved and intermediaries—particularly exchanges enabling the conversion of crypto-assets into fiat currency—became integral to the market, regulatory authorities extended existing AML/CFT frameworks, which traditionally applied to financial institutions, to these new digital actors.[64] In this context, the Financial Action Task Force (FATF) has played a pivotal role in shaping the AML/CFT regulatory framework for crypto-assets through its recommendations.

This Part examines FATF's evolving role in shaping global AML/CFT standards, particularly as they apply to the crypto-asset sector. It first explores the challenges and unintended consequences of the risk-based approach introduced by FATF, including de-risking and institutional disparities. The discussion then turns to the extension of AML/CFT obligations to VASPs and the fragmented implementation of these standards across jurisdictions, highlighting ongoing regulatory arbitrage risks. The final section addresses the limits of current frameworks in regulating DeFi, raising critical questions about enforceability, innovation, and individual rights in permissionless blockchain environments.

---

or architect, or code cyberspace to allow those values to disappear"). As seen, the phrase "Code is law" originally described how computer code can function as a form of regulation, shaping user behavior in digital spaces much like legal rules do in the physical world. In the blockchain context, Code is Law has been adopted as a guiding principle by some proponents, reflecting the idea that smart contracts and decentralized protocols should operate autonomously, without interference from legal or regulatory authorities. *See also* Georgios Dimitropoulos, *The Law of Blockchain*, 95 WASH. L. REV. 1117, 1117 (2020) (arguing that blockchain operates based on its own rules and principles that have a law-like quality); Usha Rodrigues, *Law and the Blockchain*, 104 IOWA L. REV. 679, 708–13 (2019); PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE 2 (2018). On the origins of the blockchain, see also WILLIAM MAGNUSON, BLOCKCHAIN DEMOCRACY: TECHNOLOGY, LAW AND THE RULE OF THE CROWD 9–40 (2020).

62. *Id.*

63. *See* Heidimaria Manninen, *The Anti-money Laundering Challenges of FinTech and Cryptocurrencies*, NORDIC J. LEG. STUDIES 7, 13–15 (2023) (claiming that the current regulatory landscape has several weaknesses that can be attractive for those wishing to exploit them).

64. *See* Dupuis & Gleason, *supra* note 12, at 62. Within the European context, see Valentina Covolo, *The EU Response to Criminal Misuse of Cryptocurrencies: The Young, Already Outdated 5th Anti-Money Laundering Directive (Univ. of Luxembourg Law Working Paper No. 2019-015, 2020)*, SSRN, 1, at 7–11 Jan. 6, 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3503535.

A. *The Role of the Financial Action Task Force (FATF)*

Established in 1989 as an intergovernmental organization, FATF is responsible for setting global standards to combat money laundering, terrorist financing, and other financial crimes.[65] Its recommendations serve as the primary international benchmark for AML/CFT regulations, influencing the legal frameworks of national governments and financial institutions worldwide.[66] While it does not create binding law, its recommendations are widely adopted by over 200 jurisdictions that commit to aligning their domestic regulations with FATF's guidelines.[67] Countries that fail to comply with FATF's standards risk being placed on the "grey list" or "blacklist," which can severely impact their financial reputation and access to the global economy.[68] As a result, FATF has effectively become a regulatory enforcer in the crypto space, driving governments and industry participants to implement stricter AML/CFT measures.[69]

One of FATF's milestones has been the introduction of the mandatory risk-based approach in 2012.[70] Moving away from a strictly rule-based framework, the risk-based approach was designed to provide financial institutions with greater flexibility, allowing them to allocate

---

65. *See* Mark T. Nance, *The Regime that FATF Built: an Introduction to the Financial Action Task Force*, 69 CRIME L. SOC. CHANGE 109, 129 (2018); *see also* Leonardo Sergio Borlini, *The Financial Action Task Force: An Introduction*, *Bocconi Legal Studies Research Paper No. 3834449*, SSRN, Apr. 26, 2021, https://ssrn.com/abstract=3834449 (providing a primer on the history and purpose of FATF).

66. *See FATF Recommendations*, FATF, https://www.fatf-gafi.org/en/topics/fatf-recommendations.html#:~:text=The%20FATF%20Recommendations%20are%20the%20building%20blocks%20for%20an%20effective,as%20a%20tick%2Dbox%20exercise ("The FATF Recommendations provide a comprehensive framework of measures to help countries tackle illicit financial flows. These include a robust framework of laws, regulations and operational measures to ensure national authorities can take effective action to detect and disrupt financial flows that fuel crime and terrorism, and punish those responsible for illegal activity").

67. *See generally Countries*, FATF, https://www.fatf-gafi.org/en/countries.html (last visited Sept. 2, 2025).

68. *See* Guy Stessens, *The FATF 'Black List' of Non-Cooperative Countries or Territories*, 14 LEIDEN J. INT'L L. 199, 200–207 (2001).

69. *See* Inês Sofia de Oliveira, *The Governance of the Financial Action Task Force: An Analysis of Power and Influence throughout the Years*, 69 CRIME L. SOC. CHANGE 153, 153–172 (2018). With reference to one specific legal system, see generally Doron Goldbarsht, *Who's the Legislator Anyway? How the Fatf's Global Norms Reshape Australian Counter Terrorist Financing Laws*, 45 FED. L. REV. 127, 128–51 (2017) (examining the CTF regime in Australia, a decade after the FATF's first CTF Mutual Evaluation Report on Australia, and its "decisive influence").

70. *See* Louis de Koker & Doron Goldbarsht, *FATF's Risk-Based Approach: Has the Pendulum Swung too Far?*, *in* FINANCIAL CRIME AND THE LAW 247, 250–254 (Doron Goldbarsht & Louis de Koker eds., 2024).

resources proportionally to their specific risk exposure rather than following uniform compliance obligations.[71] This theoretical empowerment was expected to enhance efficiency, reduce unnecessary regulatory burdens, and ensure that compliance efforts targeted the most significant financial crime risks.[72] The described regulatory technique has created some problems, because many institutions—especially smaller financial entities and non-bank financial institutions—lack the necessary resources, expertise, or technological capabilities to conduct sophisticated financial crime risk assessments.[73] Unlike larger banks with dedicated compliance departments and access to advanced AML tools, smaller institutions often struggle to design, implement, and justify their risk models to regulators.[74] This results in a paradox: while the risk-based approach was intended to free institutions from rigid regulatory constraints, in practice, it has placed significant operational and financial burdens on startup blockchain businesses with limited resources because banks and other financial players have established a benchmark that is difficult to meet for young and innovative businesses.

Additionally, the risk-based approach has led to unintended consequences, particularly in the form of de-risking practices. Financial institutions seeking to mitigate regulatory and reputational risks have chosen to withdraw from high-risk markets, limit services to certain customer segments, or avoid transactions involving jurisdictions with weaker AML/CFT oversight.[75] This de-risking trend has disproportionately affected developing economies, correspondent banking relationships, and non-profit organizations, limiting their access to global financial services.[76] The result is a financial exclusion dilemma: while the AML/CFT framework aims to prevent illicit financial flows, de-risking measures inadvertently push transactions into less regulated, informal channels, thereby increasing the risk of financial crime rather than reducing it.

Regulators also face significant challenges in overseeing the risk-based approach, as compliance varies widely across institutions and jurisdictions. The lack of standardized methodologies for risk assessment has

71. *Id.*

72. *Id.*

73. *Id.*

74. *See, e.g.*, European Banking Authority [EBA], *Guidelines On policies and procedures in relation to compliance management and the role and responsibilities of the AML/CFT Compliance Officer under Article 8 and Chapter VI of Directive (EU) 2015/849*, EBA/GL/2022/05 (June 14, 2022). Compliance to these guidelines requires inter alia the appointment of senior management roles and the establishment of complex policies and procedures.

75. *See* de Koker & Goldbarsht, *supra* note 69, at 254.

76. *Id.*

made it sometimes difficult for regulators to evaluate institutions' compliance measures objectively, leading to inconsistent enforcement and regulatory uncertainty.[77]

These issues have been particularly pronounced in the crypto-asset sector, which has been regarded as high-risk from its inception due to its inherent characteristics.[78] Crypto-asset intermediaries operating in the sector have often struggled to keep up with the rapidly evolving regulatory compliance requirements and have frequently been isolated by established financial institutions such as banks and payment service providers. As crypto-assets gained wider adoption, the FATF was quick to recognize the risks associated with digital assets, particularly their potential use in illicit financial flows.[79] The classification of crypto-asset-related activities as high-risk from an AML/CFT perspective has further led banks and other traditional financial intermediaries to refrain from engaging with this emerging asset class.[80]

B. *The Extension of AML/CFT Recommendations to Virtual Asset Service Providers (VASPs)*

In October 2018, the FATF updated Recommendation 15 to extend AML/CFT requirements to crypto-assets and virtual asset service providers (VASPs):

> New technologies: Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks. To

77. *See* Peter Erian et al., *The Crypto Industry Does Not Hinder Law Enforcement*, ACAMS TODAY (Mar. 19, 2025), https://www.acamstoday.org/the-crypto-industry-does-not-hinder-law-enforcement/.

78. *See supra* Section II.A.

79. *See Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets*, FATF (Sept. 14, 2020), www.fatf-gafi.org/publications/fatfrecommendations/documents/Virtual-Assets-Red-Flag-Indicators.html.

80. *See* Pete Schroeder & Douglas Gillison, *U.S. Regulator Warned Banks on Crypto but Did Not Order Halt to Business*, REUTERS (Jan. 3, 2025), https://www.reuters.com/technology/us-regulator-was-cautious-crypto-did-not-tell-banks-choke-off-sector-documents-2025-01-03/.

> manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for AML/CFT purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations.[81]

Based on the above recommendation and the subsequent updates,[82] VASPs have to be fully included within the category of financial intermediaries and fulfill the most advanced compliance measures in the field of AML/CFT. In particular, FATF requires countries to treat crypto-assets as property or other corresponding value and apply relevant AML/CFT measures to VASPs.[83] Countries must assess money laundering, terrorist financing, and proliferation financing risks associated with crypto-assets and adopt a risk-based approach to mitigating these risks.[84] VASPs must be licensed or registered in their jurisdiction of establishment or business operations, and competent authorities should prevent criminals from holding ownership or management positions in VASPs.[85] Countries must ensure effective regulation, supervision, and compliance monitoring of VASPs, including imposing

81. THE FIN. ACTION TASK FORCE, INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION 17, (2025), https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf [hereinafter: FATF Recommendations].

82. *See* THE FIN. ACTION TASK FORCE, TARGETED UPDATE ON IMPLEMENTATION OF THE FATF STANDARDS ON VIRTUAL ASSETS/VASPS 7 (2024), https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2024-Targeted-Update-VA-VASP.pdf [hereinafter: FATF, 2024 Update on VASP standards] (Listing different acts and interventions:Recommendation 15 amended (2018); Adoption of Interpretive Note to R.15 (2019); Creation of the FATF Virtual Assets Contact Group (VACG) (2019); Initial guidance for regulators: A risk-based approach to VAs and VASPs (updated in 2021) (2019); 12 month review of the new FATF Standards: 1st 12-month review (2020); Report to the G20: FATF Report to the G20 on So-called Stablecoins (2020); Risk indicators: List of Red Flag Indicators of ML/TF through VAs (2020); Updated guidance for regulators (2021): Updated Guidance for a Risk-Based Approach to VA and VASPs (2021); 24 month review of the FATF Standards: 2nd 12-month review (2021); Report on R.15 compliance, with a particular focus on the "travel rule," and emerging VA risks: Targeted Update on Implementation of the FATF Standards on VA and VASPs (2022); Report on ransomware, with a focus on VA risks and trends: Countering Ransomware Financing (2023); Report on implementation of R.15: VAs: Targeted Update on Implementation of the FATF Standards (2023); Status of implementation of Recommendation 15 by FATF Members and Jurisdictions with Materially Important VASP Activity (2024)).

83. FATF Recommendations, *supra* note 80, at 79.

84. *Id.*

85. *Id.*

appropriate sanctions for non-compliance, such as license withdrawal or financial penalties.[86] Additionally, VASPs must adhere to preventive measures, such as customer due diligence (CDD) for transactions above 1,000 USD/EUR and ensuring the secure transmission of originator and beneficiary information in virtual asset transfers.[87] The latter, is the so-called "travel rule" encompassed in Recommendation 16:

> Countries should ensure that financial institutions include required and accurate originator information, and required beneficiary information, on wire transfers and related messages, and that the information remains with the wire transfer or related message throughout the payment chain. Countries should ensure that financial institutions monitor wire transfers for the purpose of detecting those which lack required originator and/or beneficiary information, and take appropriate measures. Countries should ensure that, in the context of processing wire transfers, financial institutions take freezing action and should prohibit conducting transactions with designated persons and entities, as per the obligations set out in the relevant United Nations Security Council resolutions, such as resolution 1267 (1999) and its successor resolutions, and resolution 1373 (2001), relating to the prevention and suppression of terrorism and terrorist financing.[88]

The implementation of the "travel rule" has been particularly challenging in the field of crypto-assets, especially in the case of the so-called "unhosted" or "self-hosted" wallets, a type of digital wallet that is hosted and controlled by the user, as opposed to being hosted by a third-party service, like a VASP.[89] VASPs interacting with self-hosted wallets should prove the ownership of the crypto-assets that are transferred from one user to the other, and this is particularly challenging due to the characteristics of blockchain technology.[90] Finally, especially with respect to a borderless technology as blockchain, regulatory authorities

86. *Id.* at 79-80.

87. *Id.* at 80.

88. *Id.* at 17-18.

89. *See Hosted vs. Unhosted Crypto Wallets: A Comprehensive Guide to Self-Custody*, SECUX (May 31, 2024), https://secuxtech.com/blogs/blog/hosted-vs-unhosted-crypto-wallets?srsltid=AfmBOooCsS7UDarYsdc91ho8duEvoE83PaigH4GN0e4B__Z1wKFo4kU8.

90. *See* Catarina Veloso, *A Deep Dive into Self-Hosted Wallet Transaction Requirements Under the EU TFR*, NOTABENE (July 22, 2024), https://notabene.id/post/a-deep-dive-into-self-hosted-wallet-transaction-requirements-under-the-eu-tfr.

must cooperate internationally to combat illicit financial activities involving virtual assets.[91]

C. *Regulatory Disparities: The Challenge of Arbitrage*

FATF recommendations have certainly improved compliance standards related to VASPs. Nonetheless, many disparities still exist at a global level. Some jurisdictions have quickly adapted their legal systems and implemented the new standards, while others have been left behind: implementing little to no new provisions in their legal systems. The EU stands as a global leader in the regulation of AML/CFT within the crypto-asset sector, having developed a comprehensive legal framework to mitigate financial crime risks. Recognizing the growing role of VASPs in the financial ecosystem, the EU has implemented a series of legislative measures to ensure that these entities are subject to the same stringent compliance obligations as traditional financial institutions. The cornerstone of the EU's regulatory efforts in this field is the Fifth Anti-Money Laundering Directive (AMLD5),[92] which, for the first time, explicitly brought VASPs within the scope of AML/CFT obligations by requiring registration, CDD procedures, and the reporting of suspicious transactions to the national financial units (FIUs). The directive mandates that crypto exchanges and wallet providers adhere to KYC requirements, thereby increasing transparency and preventing illicit financial flows.[93] Building on AMLD5, the Sixth Anti-Money Laundering Directive (AMLD6) further enhanced enforcement mechanisms by harmonizing definitions of financial crimes and strengthening criminal liability for money laundering offenses across Member States.[94]

The EU's regulatory framework has continued to evolve, culminating in the Markets in Crypto-Assets Regulation (MiCA)[95] and the Transfer

91. *See* FATF Recommendations, *supra* note 80, at 3.

92. Directive 2018/843 of the European Parliament and of the Council of 30 May 2018 Amending Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, and Amending Directives 2009/138/EC and 2013/36/EU; *See* Philipp Maume & Lars Haffke, *Anti-Money Laundering*, *in* THE LAW OF CRYPTO ASSETS 269, at 274–312 (Philipp Maume et al. eds., 2022).

93. *See* Maria Bergström, *The Global AML Regime and the EU AML Directives: Prevention and Control*, *in* THE PALGRAVE HANDBOOK OF CRIMINAL AND TERRORISM FINANCING LAW 33, 46-47 (Colin King et al. eds., 2018); Maume & Haffke, *supra* note 91, at 288–303.

94. Directive 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive (EU) 2019/1937, and amending and repealing Directive (EU) 2015/849, 2024 O.J. (L 1640).

95. Regulation 2023/1114 of the European Parliament and of the Council on markets in crypto-assets and amending Regulations (EU) No. 1093/2010 and (EU) No. 1095/2010 and

of Funds Regulation (TFR),[96] both of which aim to establish a harmonized approach to crypto-asset oversight. MiCA introduces a licensing regime for crypto-asset service providers (CASPs), ensuring prudential requirements, market integrity, and consumer protection across the EU.[97] Meanwhile, the TFR extends the "travel rule" to crypto transactions, requiring VASPs to collect and share information on the originators and beneficiaries of crypto-asset transfers, aligning with the FATF Recommendation 16.[98] Together, these measures place the EU at the forefront of global efforts to regulate digital assets in a way that balances innovation with security.

However, the implementation of AML/CFT standards remains inconsistent at the international level, creating vulnerabilities that can be exploited through regulatory arbitrage. Despite FATF's efforts, many countries have either failed to implement the guidelines or have adopted fragmented, inconsistent approaches. Some jurisdictions maintain lax regulatory environments, either by design or due to limited enforcement capacity, allowing crypto businesses to operate with minimal or no oversight. As of April 2024, the FATF has completed and published 130 mutual evaluations and follow-up reports assessing the implementation of Recommendation 15 on crypto-assets and VASPs.[99] The findings indicate that seventy-five percent of jurisdictions (97 out of 130) remain partially compliant or non-compliant, a figure unchanged from April 2023.[100] A major challenge is the lack of adequate risk assessments, with twenty-nine percent of jurisdictions failing to conduct any crypto asset risk assessment.[101] Additionally, more than a quarter (twenty-seven percent) of surveyed jurisdictions have not yet decided on how to regulate the VASP sector, while sixty percent opted to permit VASPs and fourteen percent

Directives 2013/36/EU and (EU) 2019/1937, recital (1), 2023 O.J. (L 150) 40, 40 [hereinafter MiCA].

96. Regulation 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 (Text with EEA relevance), 2023 O.J. (L 150).

97. *See generally* Philipp Maume, *The Regulation on Markets in Crypto-Assets (MiCAR): Landmark Codification, or First Step of Many, or Both?*, 20 EURO. CO. & FIN. L. REV. 242 (2023); *see also* Francesco P. Patti, *The European MiCA Regulation: A New Era for Initial Coin Offerings*, 55 GEO. J. INT'L L. 388, 395–398 (2024).

98. *See* European Banking Authority [EBA], *Guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfers under Regulation (EU) 2023/1113* ('Travel Rule Guidelines'), EBA/GL/2024/11 (July 4, 2024).

99. FATF, 2024 Update on VASP Standards, *supra* note 81, at 9.

100. *Id.* at 11.

101. *Id.*

chose prohibition, though prohibiting VASPs has proven difficult to implement effectively.[102]

A key issue remains the insufficient progress on the implementation of the "travel rule," which requires VASPs to collect and share information on crypto transactions.[103] Nearly one-third of surveyed jurisdictions (thirty percent) have not passed legislation enforcing the "travel rule," and even among those that have, supervision and enforcement remain low, with only twenty-six percent of jurisdictions issuing directives or taking enforcement actions.[104] Finally, according to FATF, crypto-assets continue to be exploited for illicit purposes, including the proliferation of weapons of mass destruction, money laundering, and terrorist financing.[105] In particular, market developments indicate a rise in illicit financial activity using stablecoins and DeFi protocols, alongside persistent cyber threats and hacking incidents.[106] As previously stated,[107] this divergence creates significant risks, as illicit actors can exploit gaps in global regulation by transacting through less stringent jurisdictions, undermining international AML/CFT efforts.

D. *What Remains Outside the Scope*

The FATF has established a legal framework that can be adopted and enforced by legal systems worldwide. A crucial first step in mitigating risks is the global promotion and implementation of these guidelines. While progress has been made in recent years and will likely continue, full international cooperation remains uncertain. A more fundamental regulatory challenge emerges in the context of fully on-chain transactions, whether simple peer-to-peer transfers that bypass VASPs or interactions with DeFi protocols through which users transact directly with smart contracts. In such cases, users never interface with regulated intermediaries such as VASPs, meaning that, at present, no effective gatekeeping or supervisory mechanism is in place to monitor or control these activities. Unlike traditional financial systems that rely on intermediaries for compliance enforcement, DeFi operates in a decentralized manner, making the application of AML/CFT regulations particularly challenging.[108]

---

102. *Id.* at 12-14.

103. *See id.* at 18–20.

104. *Id.* at 19.

105. *See id.* 26–27.

106. *See id.* at 27.

107. *See supra* Section II.A.

108. *See, e.g.*, U.S. DEP'T OF THE TREASURY, ILLICIT FINANCE RISK ASSESSMENT OF DECENTRALIZED FINANCE 16-30 (2023), https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf.

In this regard, the FATF's regulatory approach has focused on establishing criteria to determine whether a DeFi protocol is genuinely permissionless and decentralized or whether it falls under the control of a specific group of individuals.[109] In its 2021 updated guidance,[110] the FATF emphasized that DeFi services often involve a central entity with some degree of control or influence.[111] This can include activities such as creating and launching crypto-assets, developing service functionalities and user interfaces, holding administrative "keys" for accounts, or collecting fees.[112] In such cases, DeFi services may fall under the FATF definition of a VASP and therefore be subject to AML/CFT obligations.

The International Organization of Securities Commissions (IOSCO) has taken this one step further by emphasizing that DeFi arrangements are not beyond regulatory reach simply because they claim to be decentralized.[113] Instead of accepting decentralization as an automatic exemption from oversight, IOSCO asserts that regulators should identify the individuals or entities ("responsible persons") that exert control or significant influence over financial products, services, or activities within a DeFi ecosystem.[114] According to IOSCO, responsible persons can be natural persons, groups, decentralized autonomous organizations (DAOs),[115] or entities that control or significantly influence a DeFi product, service, or activity. They may include developers, token holders, DAOs, foundations, venture capital firms, and other stakeholders who have governance rights, financial control, or influence over protocol decisions.[116]

---

109. THE FIN. ACTION TASK FORCE, UPDATED GUIDANCE FOR A RISK-BASED APPROACH TO VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS 27-28 (2021), https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf.

110. *Id.*

111. *Id.* at 26–30.

112. *Id.*

113. *See generally* International Organization of Securities Commissions [IOSCO], *Final Report with Policy Recommendations for Decentralized Finance (DeFi)*, FR/14/2023 (Dec. 2023), https://www.iosco.org/library/pubdocs/pdf/ioscopd754.pdf.

114. *See* International Organization of Securities Commissions [IOSCO], *Final Report with Policy Recommendations for Decentralized Finance (DeFi)*, at 21-24, FR/14/2023 (Dec. 2023), https://www.iosco.org/library/pubdocs/pdf/ioscopd754.pdf.

115. *See id.* On DAOs: *See generally* Aaron Wright, *The Rise of Decentralized Autonomous Organizations: Opportunities and Challenges*, STAN. J. BLOCKCHAIN L. & POL'Y 1, 7 (2021); Yucheng Weng, *Uncertainty about the Legal Status of DAOs*, COLUM. BUS. L. REV. ONLINE (2022), https://journals.library.columbia.edu/index.php/CBLR/announcement/view/564; Joseph Lee & Rougang Li, *Law and Regulation for Decentralised Autonomous Organisations (DAOs), in* WEB3 GOVERNANCE. LAW AND POLICY 72, 86–88 (Joseph Lee & Jyh-An Lee eds., 2025) (identifying major legal issues surrounding DAOs).

116. *See* International Organization of Securities Commissions [IOSCO], *Final Report with Policy Recommendations for Decentralized Finance (DeFi)*, at 21-24, FR/14/2023 (Dec. 2023), https://

This approach might detect extreme situations where certain actors take advantage of the technology to hide centralized business activities. But it cannot be accepted as a general regulatory framework for crypto-assets compliance in the public and permissionless blockchain space where operations are automated through smart contracts. In these cases, complying with traditional AML/CFT rules is not a viable option, given that users freely decide to interact with protocols through self-hosted digital wallets.[117] In a phase in which the development of the technology is still in its infancy, an overly strict approach would be detrimental for innovation, especially due to the enormous compliance costs associated with customer due diligence. In addition, based on a first assessment conducted by FATF, the enforcement of AML/CFT compliance in DeFi appears difficult to execute (if not impossible), given the difficulty of identifying the "responsible persons" and their locations.[118] Finally, it would tremendously harm fundamental freedoms, such as privacy and self-determination, given that persons would be obliged to disclose their financial activities beyond the scope of the application of existing legal rules.

IV. New Technologies for Compliance and Privacy Protection

To preserve the innovative nature of DeFi and uphold individuals' freedom to engage with public and permissionless blockchains, it is advisable not to extend existing AML/CFT regulations to the operation of DeFi protocols. Instead, regulatory efforts should focus on VASPs, which play a crucial gatekeeping role in facilitating the exchange between crypto-assets and fiat currencies. Additionally, the development of technological tools to enhance VASPs' compliance strategies can further mitigate risks and improve the detection of illicit activities, ensuring a balanced approach between regulation and innovation in the DeFi ecosystem.

This part of the article critically assesses the limitations of extending VASP-oriented compliance mechanisms to decentralized protocols, with a focus on privacy risks and practical enforcement challenges. Finally, it outlines emerging privacy-preserving technologies—such as

www.iosco.org/library/pubdocs/pdf/ioscopd754.pdf. On so-called decentralized exchanges, see also Syren Johnstone, Rethinking the Regulation of Cryptoassets: Cryptographic Consensus Technology and the New Prospect 169 (2021) (referring that "many DEX are not completely decentralized, and there will be often a non-insignificant element of centralized control over the deployed code ant its use. This results in a degree of permissioning being to specific participants for specific purposes, including access to the system [. . .] that may provide for editorial rights over recorded entries").

117. The above feature of DeFi is paramount of the Web3 industry: see Lee & Li, *supra* note 14, at 74–75.

118. FATF, 2024 Update on VASP Standards supra note 81, at 28–30.

zero-knowledge proofs and self-sovereign identity—that offer a path toward regulatory compliance without compromising decentralization or user autonomy.

A. *Safeguarding Privacy Protection*

The FATF's recommendations and updates have established a robust framework for AML/CFT compliance among VASPs in the crypto-asset sector.[119] However, expanding the scope of these regulations to DeFi protocols would not only stifle innovation but also introduce significant risks for users. A longstanding point of contention in this context is the tension between privacy rights and AML/CFT compliance. Regulators worldwide have imposed cash transaction thresholds, increasingly pushing individuals toward traceable payment systems—a shift that has broadened state surveillance over financial activities.[120]

In the blockchain ecosystem, AML/CFT compliance presents distinct challenges. Measures aimed at tracking and identifying financial transactions often conflict with privacy protections, which are particularly crucial in decentralized networks where transactions and holdings are stored on a distributed ledger and users operate without financial intermediaries.[121] While blockchain wallets are pseudonymous, linking an identity to a wallet address exposes users to heightened risks. Once personal information is revealed, individuals holding crypto-assets in self-hosted wallets may become vulnerable to coercion or exploitation, as they could be forced to transfer their assets to malicious actors. A terrible recent example is the kidnapping and torture of Ledger co-founder David Balland and his wife.[122] The case, where perpetrators demanded a ransom in crypto-assets, demonstrates how individuals publicly linked to digital assets can become

119. *See* Dirk Zetzsche & Jannik Woxholth, *AML/CTF Legislation on Cryptoassets, in* THE EU LAW ON CRYPTO-ASSETS 217, 217-218 (Dirk Zetzsche ed., 2025).

120. Within the European context, see, e.g., *EU Initiative for a Restriction on Payments in Cash EU Initiative for a Restriction on Payments in Cash*, ECORYS (Feb. 8, 2019), https://www.ecorys.com/case-studies/eu-initiative-for-a-restriction-on-payments-in-cash/.

121. See the clear explanation in JUSTIN WALES, THE CRYPTO LEGAL HANDBOOK: A GUIDE TO THE LAWS OF CRYPTO, WEB3, AND THE DECENTRALIZED WORLD 109 (1st ed. 2024) ("The range of financial activities achievable through DeFi without intermediaries is extensive. DeFi applications are typically accessed by connecting a user's in-browser digital wallet to a decentralized application or dApp. Because these applications enable direct interaction through a smart contract protocol, they require users to "sign" transaction commands before any activities are authorized.").

122. *Seven held in France for kidnapping and torture of crypto figure*, LE MONDE (Jan. 25, 2025 at 14:46 GMT+2), https://www.lemonde.fr/en/pixels/article/2025/01/25/seven-arrested-in-france-for-kidnapping-and-torture-of-crypto-co-founder_6737412_13.html.

targets for violent coercion. It confirms the dangers of unveiling user identities in the crypto space, particularly for those managing or holding significant assets in self-hosted wallets.

In conclusion, concerns about mass surveillance and the potential erosion of individual privacy rights suggest that, at this stage, AML/CFT compliance should not be imposed on DeFi protocols. At the present stage, stakeholders and regulators should foster a collaborative approach with industry participants in order to create technological solutions for compliance that are capable of preserving the rights and freedoms of blockchain users.

B. *VASP as Gatekeeper*

Given the limited real-world use of crypto-assets as a medium of exchange at this stage of technological development, AML/CFT controls should primarily focus on fiat on/off ramps—the points where users convert crypto to fiat and vice versa. This approach ensures that regulatory oversight is concentrated on centralized exchanges and other entry and exit points, rather than imposing compliance obligations on decentralized, non-custodial interactions. Risk-based compliance strategies implemented by VASPs already include on-chain screening tools to assess the risk level of wallets interacting with their services.[123] For example, digital wallets that have interacted with mixers, tumblers, or known illicit actors are typically flagged as indicators of "high-risk" transactions, potentially prompting the obliged entity to file a suspicious transaction report with the relevant authority.[124] Additionally, the "travel rule" mandates the identification of senders and recipients involved in transactions with VASPs.[125] Rather than introducing overly broad restrictions that could stifle innovation, regulatory efforts should focus on enhancing AML/CFT frameworks by integrating blockchain-based compliance tools into existing protocols. A collaborative approach between RegTech firms, crypto exchanges, policymakers, and law enforcement is essential to

123. *See* Liat Shetret, *Practical implementation of FATF Recommendation 15 for VASPs: Leveraging on-chain analytics for crypto compliance*, ELLIPTIC (Apr. 9, 2024), https://www.elliptic.co/blog/practical-implementation-of-fatf-recommendation-15-for-vasps-leveraging-on-chain-analytics-for-crypto-compliance.

124. *See* Nadia Pocher, *Traceability of Crypto-Asset Transfers under the New EU AML/CFT Regime: the Crypto Travel Rule between Challenges and Open Issues, in* A RESEARCH AGENDA FOR FINANCIAL LAW AND REGULATION 197, 210 (Joseph Lee & Aline Darbellay eds., 2025).

125. *See* THE FIN. ACTION TASK FORCE, Virtual Assets: Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers 5, 8-18 (2025), https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2025-Targeted-Upate-VA-VASPs.pdf.coredownload.pdf.

strengthen AML/CFT compliance, improve financial transparency, and mitigate illicit risks while preserving the transformative potential of DeFi. Industry and regulators should work together to develop and encourage the adoption of RegTech solutions that safeguard user privacy while ensuring compliance.

One potential avenue for privacy-preserving compliance is the use of zero-knowledge proofs (zk-proofs). These cryptographic techniques allow one party to prove the truth of a statement without revealing underlying data.[126] In the AML/CFT context, zk-proofs could enable wallets to demonstrate compliance (e.g., verifying that a user is not sanctioned) without exposing sensitive financial information.[127] A recent paper by the Bank of Italy examines the potential of self-sovereign identity (SSI) as a digital identity framework that grants users full control over their personal information while enhancing privacy protections.[128] The SSI model would enable individuals to prove specific attributes on a blockchain without revealing sensitive personal data.[129] For instance, a user can demonstrate that they are legally of age without disclosing their exact date of birth by utilizing zk-proofs.[130] The discussed system would operate through a structured framework involving three key participants: the issuer, who provides a cryptographically signed verifiable credential to the user; the holder, who stores the credential in a secure digital wallet and generates a zk-proof when verification is

126. *See* Marthews & Tucker, *supra* note 26, at 257 (pointing to "facts about ourselves whose creation, management, distribution, and reuse is wholly under our control").

127. *See* T. Craig & J. Wright, *How crypto's zero-knowledge proofs could hit the regulation-privacy 'sweet spot'*, DL NEWS (Feb. 15, 2023), https://www.dlnews.com/articles/defi/how-cryptos-zero-knowledge-proofs-could-hit-the-regulation-privacy-sweet-spot/; Zoltan Vardai, *Regulators are cracking down on financial privacy, but ZK-proofs can help*, COINTELEGRAPH (May 14, 2024), https://cointelegraph.com/news/crypto-privacy-zero-knowledge-proofs-protocols.

128. Romina Gabbiadini et al., *Riciclaggio e blockchain: si può seguire la traccia nel mondo cripto?* [*Money Laundering and Blockchain: Can you Follow the Trail in the Crypto World?*], 893 QUESTIONI DI ECONOMIA E FINANZA (OCCASIONAL PAPERS), November 2024, at 21, https://www.bancaditalia.it/pubblicazioni/qef/2024-0893/index.html; *see also* Iswarya Konasani, *Decentralized Identity: Revolutionizing KYC/AML in Financial Services*, 16 INT'L J. INFO. TECH. & MGMT. INFO. SYS. 951, 952–65 (2025);

129. *Id.* at 21–22. On SSI. *See generally* Linda Weigl, Tom Barbereau & Gilbert Fridgen, *The Construction of Self-Sovereign Identity: Extending the Interpretive Flexibility of Technology Towards Institutions*, 40(4) GOV'T INFO. Q. 2023, https://doi.org/10.1016/j.giq.2023.101873.

130. *See* Vladimir Popov et al., *Blockchain Privacy and Self-regulatory Compliance: Methods and Applications*, SSRN, Apr. 16, 2024, http://dx.doi.org/10.2139/ssrn.4787693 (taking as examples three privacy-preserving protocols (Hinkal, RAILGUN, and zkBob)); Nicolin Decker, *Zero-Knowledge Proofs: Cryptographic Model for Financial Compliance and Global Banking Security*, SSRN, Apr. 17, 2025, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5170068.

required; and the verifier, who assesses the authenticity of the credential by ensuring that it was legitimately issued and remains untampered.[131]

Incorporating SSI into DeFi would enable users to prove their eligibility for financial services while preserving their privacy. By submitting zk-proofs to smart contracts, individuals could verify attributes such as their age, residency, political exposure, or compliance with national and international sanctions lists without exposing unnecessary personal details.[132] This would allow DeFi protocols to implement compliance measures without relying on centralized intermediaries, maintaining the decentralized nature of blockchain-based finance. Until now, despite their theoretical potential, zk-proof-based solutions face technical complexities, regulatory uncertainty, and industry resistance due to concerns that added compliance layers may compromise decentralization. Nonetheless, the technologies are still in their infancy, and it might be worth continuing their development. A strong endorsement by international organizations like FATF could definitely move things in the correct direction.

Another emerging compliance mechanism in DeFi is sanctions screening tools integrated at the front-end (e.g., website interfaces) of DeFi platforms. These tools help prevent wallets linked to sanctioned entities from interacting with protocols. However, given that DeFi operates on open blockchain networks, users can bypass such restrictions by accessing alternative interfaces or interacting directly with smart contracts, making these measures only partially effective.[133] FATF recognizes the emergence of these new technologies but has yet to provide explicit endorsement or clear guidance on their adoption.[134] Moving forward, the regulatory landscape must strike a delicate balance between ensuring compliance and preserving innovation, leveraging privacy-enhancing technologies to mitigate risk while respecting the fundamental principles of decentralization.

---

131. *See generally* PRIVADO.ID, https://www.privado.id/ (last visited Apr. 30, 2025)

132. *See* Lu Zhou et al., *Leveraging Zero Knowledge Proofs for Blockchain-based Identity Sharing: A Survey of Advancements, Challenges and Opportunities*, 80 J. INFO. SEC. & APPS. (2024) (conducting a survey of the existing literature, with a particular focus on the assimilation of ZKP technology into blockchain for the secure sharing of user identities).

133. *See* Bogdan Adamyk et al., *Risk Management in DeFi: Analyses of the Innovative Tools and Platforms for Tracking DeFi Transactions*, 18 J. RISK & FIN. MGMT. 1, 53–63 (2025) (referring to AI-powered anomaly detection systems can detect unusual real-time transaction patterns in detecting fraud, money laundering, or market manipulation).

134. See FATF, 2024 Update on VASP Standards, *supra* note 81, at 29 (reporting that only one jurisdiction has initiated a pilot project to create and test a technological solution for embedded supervision of DeFi activity).

V. CONCLUSION

The discussion has demonstrated that crypto-assets are neither inherently illicit nor untraceable. While pseudonymity and privacy-enhancing technologies pose challenges for regulators, blockchain technology itself offers powerful compliance tools.[135] Blockchain analytics firms have developed sophisticated forensic techniques that enable regulators and law enforcement agencies to track financial flows, identify high-risk wallets, and disrupt illicit activity.[136] Contrary to common misconceptions, crypto transactions are often more traceable than cash, as they are recorded permanently on public blockchains, allowing for detailed transactional analysis.[137]

The uneven implementation of FATF's AML/CFT recommendations has significant consequences for financial crime prevention in the crypto-asset sector. While some jurisdictions, such as the European Union, have introduced comprehensive regulatory frameworks, others have been slow to adapt, creating gaps that illicit actors can exploit.[138] The lack of universal compliance standards allows bad actors to leverage regulatory arbitrage, moving illicit funds through jurisdictions with weaker enforcement.[139] As the crypto industry continues to expand, stronger international coordination is necessary to close these gaps and ensure a consistent, effective approach to AML/CFT enforcement worldwide.

A critical challenge remains the regulation of DeFi. Unlike centralized exchanges, DeFi protocols operate without intermediaries, making traditional AML/CFT compliance measures difficult to enforce.[140] FATF and IOSCO have sought to identify responsible persons within DeFi arrangements, arguing that developers, DAOs, and governance token holders may exert control or influence over financial activities and should therefore be subject to regulation. While this approach may address cases where centralized elements exist within DeFi, it is not a universal solution.[141] Applying conventional AML/CFT rules to fully decentralized, permissionless blockchains risks undermining innovation, creating excessive compliance costs, and infringing on privacy rights.[142]

135. *See supra* Section II.B.
136. *Id.*
137. *Id.*
138. *See supra* Section III.C.
139. *Id.*
140. *See supra* Section III.D.
141. *Id.*
142. *Id.*

A more pragmatic approach would focus regulatory oversight on VASPs, which act as key gatekeepers for converting crypto to fiat. VASPs already implement risk-based compliance strategies, including on-chain screening tools and adherence to the "travel rule," making them the most practical focal point for AML enforcement.[143] At the same time, technological advancements such as zk-proofs and SSI frameworks present privacy-preserving solutions that could enable compliance without excessive disclosure of personal data. However, these technologies are still in their infancy, and their regulatory acceptance remains uncertain.[144] A clear endorsement by FATF and other global regulatory bodies could encourage further development and adoption.

Moving forward, regulators must balance AML/CFT enforcement with the need to preserve innovation and privacy. Overly restrictive measures could stifle technological advancements and push financial activities into less regulated spaces, counteracting the very objectives of AML compliance. Instead, a collaborative approach between regulators, industry participants, and RegTech firms should be pursued to develop solutions that ensure security, maintain financial integrity, and uphold fundamental freedoms in the evolving crypto-asset ecosystem. Achieving a globally coordinated AML/CFT framework for crypto-assets requires international regulatory alignment, standardization of compliance measures, and enhanced cross-border cooperation. Global financial institutions, policymakers, and blockchain industry leaders must work together to establish harmonized regulatory frameworks that address risks without imposing unnecessary barriers to innovation. By fostering dialogue, sharing best practices, and leveraging RegTech advancements, the global community can move toward a unified regulatory landscape that both mitigates financial crime and supports the long-term growth of the crypto-asset economy.

143. *See supra* Section IV.A.

144. *See supra* Section IV.B.