Crypto Money Laundering

Jiaying Jiang*

The crypto ecosystem has become a new frontier for money laundering, with criminals exploiting its anonymous and pseudonymous features. This Article explores how money laundering operates in the crypto space and highlights emerging trends. It then examines the existing legal and regulatory framework and argues that its core weakness lies in its reliance on trusted intermediaries. This approach conflicts with the philosophy that shaped the emergence of the crypto industry—one grounded in disintermediation and decentralized trust. To address this tension, this Article demystifies decentralization, showing that it is not a binary condition but instead exists on a spectrum. Across the dimensions of development, governance, and operation, some projects remain highly centralized despite adopting the label of "DeFi" or "decentralized." Arguably only Bitcoin has achieved near-total decentralization, and most others fall somewhere in between. Recognizing this dynamic is crucial for crafting effective regulatory responses. Finally, this Article proposes combining blockchain intelligence with a digital identity system to form a decentralized digital infrastructure that delineates the roles of public and private actors and distributes responsibilities among these stakeholders. Together, these technological tools and regulatory designs can strengthen the investigation, tracing, and seizure of illicit funds in the crypto space, while preserving a certain degree of decentralization that the industry values. This Article also reconceptualizes decentralization not merely as a technological design but as a regulatory strategy—one that shifts the anti-money laundering paradigm from centralized oversight to collective responsibility.

DOI: https://doi.org/10.15779/Z38833N19T

* Associate Professor of Law, University of Florida Levin College of Law. I am grateful to the following individuals who provided valuable insights and discussions that helped shape this article (listed in alphabetical order): Jussi Aittola, Sebastian Bode, Ben Buergi, Raul Carrillo, Sam Elfarra, Nick Furneaux, Tomas Haley, Linda Jeng, Benjamin Johnson, Lockhart Karl, Matthew Kim, Liat Shetret, Lev Menand, Alexandar Moser, Gal Sagie, Felix Shipkevich, Bjorn Wahlstrom, and Kai Wang. I would like to extend my sincere appreciation to the participants at the University of Florida Levin College of Law Junior Faculty Workshop, the Northeastern Junior Scholars Conference, the Financial Regulation

I.
INTRODUCTION

1Lbcfr7sAHTD9CgdQo3HTMTkV8LK4ZnX71

What information can you extract from this string of seemingly irrelevant letters and numbers? Probably nothing at first glance, right? In reality, this

Section of the 2025 Association of American Law Schools Annual Meeting, and the Blockchain and Fintech Program at Rutgers Center for Corporate Law and Governance for their thoughtful feedback. I would also like to thank my research assistants—Victor Dumitru, Seth Benjamin Garfield, and Sidney Thomas—for their invaluable support throughout the research and writing process.

alphanumeric string, known as a Bitcoin address, could be linked to a transaction worth millions of dollars stored on the Bitcoin blockchain. However, the identity of the person behind it is shrouded in mystery. This characteristic of Bitcoin—its pseudonymous nature—has made it a favored tool for those who want to obscure the flow of their wealth, especially for illicit activities like money laundering.

Many people view money laundering as an abstract, victimless crime. Unlike theft or fraud, where victims face immediate financial loss, the harm caused by money laundering is harder to trace and feels indirect. This disconnect reinforces the perception that money laundering is merely a technical offense affecting only institutions like banks or governments.[1] Moreover, its complexity—concealed behind layers of legal and financial transactions—makes it difficult for the public to see how it facilitates serious criminal activities.[2] As long as laundered funds re-enter the economy without obvious disruption, the link between money laundering and the harm it enables often goes unnoticed.

But make no mistake: without money laundering, organized crimes would collapse.[3] Laundering is the glue that holds the underworld together—without a way to wash their profits, criminals of many kinds simply cannot operate.[4] All of the following crimes depend on a system of moving and hiding money: human traffickers selling children into modern slavery; exploiters targeting vulnerable women—who could be anyone's mothers, daughters, sisters, or cousins—trapped in cycles of sexual abuse; drug dealers flooding nightclubs with dangerous substances; fraudsters siphoning life savings from our elderly relatives; and even terrorist organizations funneling money to finance violent attacks.[5] If criminals cannot launder and extract their ill-gotten gains, no one gets paid, and the criminal underworld falls apart.[6]

According to the United Nations, the estimated amount of money laundered annually is 2–5% of the global GDP or $800 billion to $2 trillion in current U.S.

1. *What Is Money Laundering & What Are the Penalties?*, DUGHI, HEWIT & DOMALEWSKI, P.C., https://www.dughihewit.com/what-is-money-laundering-and-what-are-the-penalties (last visited Oct. 28, 2024); *White-Collar Crime*, FED. BUREAU OF INVESTIGATION [FBI], https://www.fbi.gov/investigate/white-collar-crime (last visited Oct. 28, 2024); Mark Kersten, *Money Laundering Is Not a Victimless Crime*, GLOBE AND MAIL: OPINION (June 22, 2022), https://www.theglobeandmail.com/opinion/article-money-laundering-is-not-a-victimless-crime/.

2. *See* U.S. DEP'T OF THE TREASURY, 2024 NATIONAL MONEY LAUNDERING RISK ASSESSMENT 10–11, 31, 53, 56–57, 80, 93 (2024).

3. GEOFF WHITE, RINSED: FROM CARTELS TO CRYPTO: HOW THE TECH INDUSTRY WASHES MONEY FOR THE WORLD'S DEADLIEST CROOKS 2–5 (2024).

4. *Id.*

5. *Id.*; *see also Financial Crime Initiatives*, INT'L CRIM. POLICE ORG. [INTERPOL], https://www.interpol.int/en/Crimes/Financial-crime/Financial-crime-initiatives (last visited Sep. 29, 2025) ("Illicit financial flows underpin the vast majority of serious transnational criminal activity.").

6. WHITE, *supra* note 3, at 2–5.

dollars.[7] In recent years, criminals have increasingly turned to cryptocurrencies for money laundering due to their anonymity and pseudonymity features.[8] For instance, Darknet markets,[9] such as the now-defunct Silk Road,[10] used cryptocurrencies like Bitcoin for transactions involving illegal services and goods.[11] Cybercriminals often demand ransom payments in cryptocurrencies after encrypting victims' data.[12] Fraudulent Initial Coin Offerings (ICOs) and

7. United Nations Office on Drugs & Crime, Money Laundering, https://www.unodc.org/unodc/en/money-laundering/overview.html (last visited Oct. 27, 2024). Additionally, the FBI reports that "every year, more than $300 billon in concealed transactions is moved around the United States, according to a U.S. Department of the Treasury report on money laundering and terrorist financing threats." *Combating the Growing Money Laundering Threat: Specialized FBI Unit Focuses on Disrupting Professional Money Launderers*, FBI (Oct. 24, 2016), https://www.fbi.gov/news/stories/combating-the-growing-money-laundering-threat.

8. U.S. DEP'T OF JUST., REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE: CRYPTOCURRENCY ENFORCEMENT FRAMEWORK 1 (2020).

9. The three main layers of the internet are the surface, deep, and dark web. Varin Khera, *The Web Layers: Introduction to Surface, Deep and Darknet*, CYBER PROT. MAG. (Nov. 2, 2020), https://cyberprotection-magazine.com/the-web-layers-introduction-to-surface-deep-and-darknet. The surface web is the part of the intent most people use on a day-to-day basis and is indexed and accessed through search engines like Google. This makes up a very small portion of the entire internet's content. By contrast, the deep web makes up most of the internet's content and contains contents such as login forms requiring access credentials, fee-based content, and other things inaccessible to standard search engines. *Id.* The dark web is a subset of the deep web requiring specific software to access. Violeta Lyskoit, *Darknet Market: What You Should Know About Dark Web Marketplaces*, NORDVPN (Apr. 18, 2024), https://nordvpn.com/blog/darknet-market/?srsltid=AfmBOooS8s9U7izHXt6cfpO9p-7L_3AxDA7bScqjGsQTyldkMhzH4DBi. Darknet markets are online websites and marketplaces that run on the dark web. *Id.* Darknet markets tend to function as "unregulated virtual bazaars with a great deal of anonymity." U.S. DEP'T OF JUST., *supra* note 8, at 16. These markets allow participants to buy and sell illegal drugs, weapons, hacking services, and child sexual abuse materials. Cryptocurrencies provide critical payment infrastructure for these markets to function, and users may use these sites to launder money. In 2019, the DOJ announced that DeepDotWeb (DDW) websites received 8,155 Bitcoin in kickbacks from darknet marketplaces, valued at $8,414,173 adjusted for Bitcoin's trading value at the time of each transaction. *Id.* at 19–20.

10. The Silk Road processed millions of dollars of illicit transactions, and over 144,000 Bitcoin were seized when it was shut down. Press Release, U.S. Dep't of Just., Acting Manhattan U.S. Attorney Announces Forfeiture of $48 Million from Sale of Silk Road Bitcoins (Sep. 29, 2017), https://www.justice.gov/usao-sdny/pr/acting-manhattan-us-attorney-announces-forfeiture-48-million-sale-silk-road-bitcoins.

11. *See* FIN. ACTION TASK FORCE, VIRTUAL CURRENCIES: KEY DEFINITIONS AND POTENTIAL AML/CFT RISKS 11 (2014), https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf; U.S. DEP'T OF JUST., *supra* note 8, at 16–20; Sean Foley, Jonathan R. Karlsen & Tālis J. Putniš, *Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies?*, 32 REV. OF FIN. STUD. 1798, 1804 (2019); *see also* Investopedia Team, *What Was the Silk Road Online? History and Closure by the FBI*, INVESTOPEDIA (June 29, 2024), https://www.investopedia.com/terms/s/silk-road.asp.

12. U.S. DEP'T OF JUST., *supra* note 8, at 7. Ransomware is a type of malicious software that encrypts or blocks access to valuable data until the victim agrees to pay the perpetrator. Criminals may also demand payment after threatening to distribute confidential or embarrassing information (e.g., nude photos) or engage in "virtual kidnappings" where victims are misled into believing that a loved one was taken. U.S. DEP'T OF JUST., *supra* note 8, at 7; *see also* CHAINALYSIS, THE 2024 CRYPTO CRIME REPORT: THE LATEST TRENDS IN RANSOMWARE, SCAMS, HACKING, AND MORE 11 (2024), https://www.pensamientopenal.com.ar/system/files/Documento_Editado1686.pdf (finding that cryptocurrency ransomware payments exceeded $1 billion in 2023).

Ponzi schemes have also been prevalent in the crypto space.[13] Some criminals use crypto exchanges to wash their illicit gains.[14]

According to Chainalysis, a leading blockchain analysis company, illicit crypto volume is estimated to total $40 to $51.3 billion in 2024, a sharp increase from roughly $11 billion in 2020.[15] Whereas Chainalysis reports that less than 1% of blockchain transactions are associated with illicit activities, academia believes this share is 23%.[16] Among all illicit activities, money laundering is the predominant one.[17] Chainalysis estimates that the total amount of cryptocurrency laundered from 2021 to 2023 was approximately $18.3 billion, $31.5 billion, and $22.2 billion, respectively.[18] Centralized exchanges remained the primary destination for laundered funds, handling about 60% of these transactions.[19] At the same time, the share of illicit funds moving into decentralized finance (DeFi) protocols increased to 13%, reflecting a shift toward more complex laundering methods.[20]

This Article explores why money laundering remains so pervasive in the crypto space, why existing legal and regulatory frameworks have failed to effectively combat such crime, and whether a more effective approach could be implemented.

Part II explains the traditional three stages of money laundering—placement, layering, and integration—and explores how criminals exploit the crypto ecosystem at each stage due to its uniquely anonymous and pseudonymous nature. The crypto ecosystem is particularly useful to criminals during the second stage (layering), where they obscure the connection between illicit funds and their source. Criminals use techniques such as mixers, chain hopping, and nesting services to conceal the origins of illicit funds.[21] In recent years, criminals have exploited new crypto tools, from privacy coins to

13. U.S. DEP'T OF JUST., *supra* note 8, at 29–30, 32.

14. CHAINALYSIS, *supra* note 12, at 23–25; U.S. DEP'T OF JUST., *supra* note 8, at 13–15.

15. CHAINALYSIS, THE 2025 CRYPTO CRIME REPORT 2–4 (2025), https://go.chainalysis.com/2025-Crypto-Crime-Report.html.

16. *Id.* at 5 (estimating the shares of all crypto transaction volume associated with illicit activity from 2020 to 2024 are 0.7%, 0.12%, 0.31%, 0.61%, and 0.14%, respectively); Foley, *supra* note 11, at 1825. The wide disparity in estimates likely relates to differences in the underlying methodologies employed. Moreover, both may understate the true extent of money laundering due to availability bias—that is, these estimates fail to include illicit funds that were not captured or linked to illicit uses by law enforcement.

17. CHAINALYSIS, *supra* note 12, at 23–24.

18. *Id.*

19. *Id.* at 24.

20. *Id.*

21. ELLIPTIC, THE STATE OF CROSS-CHAIN CRIME 2025 8 (2025), https://www.elliptic.co/hubfs/The%20state%20of%20cross-chain%20crime%202025/The%20state%20of%20cross-chain%20crime%202025%20-%20FINAL.pdf; *Crypto Mixers and AML Compliance*, CHAINALYSIS (Aug. 23, 2022), https://www.chainalysis.com/blog/crypto-mixers/.

generative AI, which reflects both the expanding crypto ecosystem and the mounting challenges for law enforcement and regulators.

Part III explains why existing anti-money laundering (AML) laws have failed to effectively combat money laundering in the crypto space. A comprehensive review of the literature reveals several critiques, including definitional ambiguity, [22] high compliance and implementation costs, [23] disproportionate compliance burdens, [24] and an ineffective rule-based approach.[25]

This Article complements the existing literature and argues that a more fundamental issue lies at the heart of this failure: the inherent conflict of trust. The crypto industry is built on the concept of "trustless trust," [26] where decentralized protocols, rather than intermediaries, ensure the integrity of transactions and relationships. In contrast, current legal and regulatory frameworks attempt to bring the crypto industry back to an intermediary-based trust system, where financial institutions verify transaction relationships and process transactions.[27] As a result, there is an inherent conflict between the

22. PETER VAN VALKENBURGH, BROAD, AMBIGUOUS, OR DELEGATED: CONSTITUTIONAL INFIRMITIES OF THE BANK SECRECY ACT 2 (2023), https://www.coincenter.org/broad-ambiguous-or-delegated-constitutional-infirmities-of-the-bank-secrecy-act/ (arguing that the original category of "financial institutions" primarily consisted of insured banks, but over the years it has significantly expanded. The Bank Secrecy Act, however, "doesn't set much of a limit to what should and should not fit in the category.").

23. *See* Mengqi Sun, *Binance CEO Invests in Compliance to Move On from Past Mistakes*, WALL ST. J. (Sep. 20, 2024), https://www.wsj.com/articles/binance-ceo-invests-in-compliance-to-move-on-from-past-mistakes-6bc08d74; Ty Roush, *Judge Approves Binance's $4.3 Billion Settlement for Anti-Money Laundering, Sanctions Violations*, FORBES (Feb. 23, 2024), https://www.forbes.com/sites/tylerroush/2024/02/23/judge-approves-binances-43-billion-settlement-for-anti-money-laundering-sanctions-violations.

24. United States v. Conley, 833 F. Supp. 1121, 1149 (W.D. Pa. 1993); Jason Leopold, Anthony Cormier, John Templon, Tom Warren, Jeremy Singer-Vine, Scott Pham, Richard Holmes, Azeen Ghorayshi, Michael Sallah, Tanya Kozyreva & Emma Loop, *Dirty Money Pours Into the World's Most Powerful Banks*, BUZZFEED NEWS (Sep. 20, 2020), https://www.buzzfeednews.com/article/jasonleopold/fincen-files-financial-scandal-criminal-networks; BANK POL'Y INST., GETTING TO EFFECTIVENESS—REPORT ON U.S. FINANCIAL INSTITUTION RESOURCES DEVOTED TO BSA/AML & SANCTIONS COMPLIANCE 2 (Oct. 29, 2018), https://bpi.com/wp-content/uploads/2018/10/BPI-AML-Sanctions-Study-vF.pdf; Matthew Collin, *What the FinCEN Leaks Reveal About the Ongoing War on Dirty Money*, BROOKINGS (Sep. 25, 2020), https://www.brookings.edu/articles/what-the-fincen-leaks-reveal-about-the-ongoing-war-on-dirty-money.

25. QUANTEXA, HOW TO EFFECTIVELY TACKLE TRADE-BASED MONEY LAUNDERING 18 (2024), https://www.quantexa.com/resources/combat-trade-based-money-laundering/; Ronald F. Pol, *Anti-Money Laundering: The World's Least Effective Policy Experiment? Together, We Can Fix It*, 3 POL'Y DESIGN & PRAC. 73, 85 (2020).

26. Reid Hoffman, *The Future of the Bitcoin Ecosystem and "Trustless Trust"—Why I Invested in Blockstream*, LINKEDIN (Nov. 17, 2014), https://www.linkedin.com/pulse/20141117154558-1213-the-future-of-the-bitcoin-ecosystem-and-trustless-trust-why-i-invested-in-blockstream/; *see also* Kevin Werbach, *Trust, but Verify: Why the Blockchain Needs the Law*, 33 BERKELEY TECH. L.J. 487, 498 (2018) (Werbach attributes the phrase "trustless trust" to Reid Hoffman).

27. *See, e.g.*, Gary Gorton & Andrew Winton, *Financial Intermediation*, *in* 1 HANDBOOK OF THE ECONOMICS OF FINANCE 433, 433 (G.M. Constantinides, M. Harris & R. Stulz eds., 2003)

regulatory approach and the industry's core principles, rendering existing rules and regulations inadequate to address the realities of a trustless, decentralized crypto ecosystem.

To address this regulatory gap, regulators and law enforcement must first assess the degree of decentralization within the crypto industry across three dimensions: development, governance, and operation. Decentralization is not a binary concept; rather, it exists on a spectrum. At one end of the spectrum are systems that achieve maximum decentralization, with the Bitcoin network standing out as perhaps the only example. Most so-called decentralized projects occupy a middle ground on this spectrum, blending elements of centralization and decentralization to varying degrees. At the other end, there are projects that remain relatively centralized, even if they adopt the label of decentralization or aim to function peer-to-peer.

For decentralized and semi-decentralized projects, regulators and law enforcement should move away from the intermediary-based approach. Part IV proposes a decentralized digital infrastructure comprising two key elements: blockchain intelligence and a digital identity system. Blockchain intelligence leverages tamper-proof blockchain data and AI models to identify trends, assess risks, and detect anomalies. A digital identity system complements this by linking verified identities to blockchain transactions through a tiered approach: smaller transactions can remain anonymous or pseudonymous while larger ones require enhanced verification. Using Dock as a case study, this system shows how individuals can retain control of their identity and preserve privacy while mitigating money laundering risks.[28] Effective adoption requires collaboration among all stakeholders to determine tiered verification rules, licensing criteria, data access and reporting protocols, and the use of technology for privacy protection and interoperability.

For centralized projects, regulators and law enforcement can continue employing an intermediary-based approach but must gradually integrate blockchain intelligence and digital identity solutions at both the investigation and enforcement stages to align with modern AML needs.

("Financial intermediation is a pervasive feature of all of the world's economies."); Jai Massari & Christian Catalini, *DeFi, Disintermediation, and the Regulatory Path Ahead*, REGUL. REV. (May 10, 2021), https://www.theregreview.org/2021/05/10/massari-catalini-defi-disintermediation-regulatory-path-ahead/ ("U.S. financial regulation assumes the presence of intermediaries, and it applies regulation to intermediaries as a way to regulate financial markets and related activities comprehensively."); Tom C.W. Lin, *Infinite Financial Intermediation*, 50 WAKE FOREST L. REV. 643, 643 (2015) ("Intermediation is a fundamental fact of finance."); Carla L. Reyes, *Law's Detrimental Reliance on Intermediaries*, 92 GEO. WASH. L. REV. 1343, 1350 (2024) ("U.S. regulatory regimes demand, and even encourage, centralization that [blockchain] technology itself obviates.").

28. FIN. ACTION TASK FORCE, OPPORTUNITIES AND CHALLENGES OF NEW TECHNOLOGIES FOR AML/CFT 4 (2021), https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf.coredownload.pdf ("Technology can facilitate data collection, processing and analysis and help actors identify and manage money laundering and terrorist financing (ML/TF) risks more effectively and closer to real time.").

This Article makes contributions at both theoretical and practical levels. Theoretically, it offers a novel critique of the AML framework through the lens of trust, highlighting the fundamental misalignment between the regulatory assumptions and industry realities. Furthermore, by conceptualizing decentralization as a spectrum rather than a binary state, the Article advances the theoretical discourse on development, governance, and operation in decentralized systems, bridging the gap between the principles of decentralization and tailored regulatory interventions.

Practically, this Article offers specific strategies for addressing varying degrees of decentralization, distinguishing when to apply an intermediary-based framework and when to leverage decentralized solutions. It proposes and outlines the design of a digital infrastructure, providing a roadmap for lawmakers, regulators, law enforcement, and industry participants to adopt blockchain intelligence and establish a robust digital identity system.

Compared to the existing rule-based recordkeeping and reporting system, blockchain intelligence enables more effective investigation, tracing, and seizure of illicit assets. Meanwhile, the digital identity system directly addresses the core challenge of combating money laundering in the crypto space—the disconnect between blockchain transactions and their real-world actors. As crypto money laundering remains at the forefront of national and international regulatory debates, this Article delivers timely and pragmatic insights for shaping more effective and adaptive legal and regulatory responses.

The Article proceeds as follows: Part II explains traditional money laundering methods, explores how criminals exploit the crypto ecosystem, and identifies emerging trends. Part III reviews the existing AML legal framework and critiques its failures. It introduces a trust-based argument that the key failure lies in its reliance on trusted intermediaries, which conflicts with the decentralized and "trustless" nature of the crypto industry. Part IV conceptualizes decentralization as a spectrum and proposes decentralized digital infrastructure—integrating blockchain intelligence and digital identity systems—as a potential solution. Part V concludes.

II.
MONEY LAUNDERING THROUGH THE CRYPTO ECOSYSTEM

This Part explains money laundering in both traditional and cryptocurrency contexts. Section II.A introduces the traditional money laundering process, which typically involves three key steps: placement, layering, and integration. These steps explain how illicit funds are introduced into the financial system, concealed through various mechanisms, and eventually reintegrated into the economy as seemingly legitimate funds. Section II.B then explores how money laundering operates within the cryptocurrency ecosystem. While the process follows the same three stages, it employs various methods and tools adapted to the unique characteristics of cryptocurrencies—particularly their pseudonymity

and anonymity—which make them attractive to criminals. Finally, Section II.C analyzes emerging trends, offering insights into the increasing use of methods such as stablecoins, non-fungible tokens (NFTs), DeFi platforms, privacy coins, layer 2 solutions, and even generative AI for laundering funds.

A. Traditional Money Laundering

Money laundering is "the concealment of the existence, nature, or illegal source of illicit funds in such a manner that the funds appear legitimate if discovered."[29] Put differently, it is a way to "clean" money obtained illegally so that it appears to derive from a legitimate source.[30] It is important to distinguish money laundering from the criminal acts that produce these funds. For example, funds exchanged for drugs, child sexual abuse material, or terrorism become "illicit" because they are involved in illegal transactions. Money laundering—the process criminals engage in to obscure the source of these funds and make them appear legitimate—is a separate crime from the initial illegal act.[31] Criminals might be prosecuted for both the initial criminal act and money laundering, depending on the circumstances of the case.

Money laundering follows three key stages: placement, layering, and integration.[32] First, placement involves introducing illegally obtained money into the financial system.[33] This is often done through multiple deposits or investments to avoid detection.[34] Next, layering occurs as criminals attempt to obscure the connection between the funds and their illegal source, moving the money through a series of complex transactions.[35] Finally, integration takes place when the money appears to come from a legitimate source and is reintroduced to the economy, no longer requiring concealment.[36]

29. 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"*, 27 GEO. MASON L. REV. 1, 9 n.41 (2019). The UN Vienna 1988 Convention Article 3.1 describes money laundering as "the conversion or transfer of property, knowing that such property is derived from any offense(s), for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in such offense(s) to evade the legal consequences of his actions." United Nations Office on Drugs & Crime, *supra* note 7.

30. FBI, *supra* note 1.

31. I.R.S. IRM 9.5.5.1.1(5) (Dec. 18, 2024), https://www.irs.gov/irm/part9/irm_09-005-005 ("The same transaction cannot be both a money laundering offense and the underlying specified unlawful activity (SUA) that generated the funds being laundered.").

32. FBI*, supra* note 1.

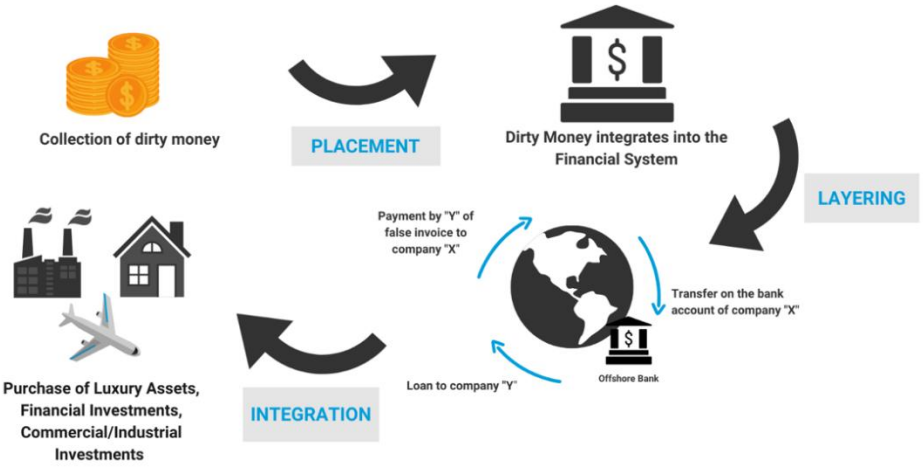
33. *Id.*

34. *Id.*

35. *Id.*

36. *Id.*

Figure 1: Money Laundering Cycle.[37]



To illustrate, consider a criminal organization that owns a legitimate restaurant. The laundering process might unfold as follows: placement happens when the organization deposits illegal funds into a bank by inflating the restaurant's reported cash sales. Then, layering occurs as the restaurant funnels the money into legitimate businesses—often through shell companies—to evade detection. This typically involves multiple transactions, accounts, and entities, further distancing the money from its illicit origin. Finally, integration occurs once the funds are "clean," and the criminal organization can use the funds to expand the restaurant business, purchase additional properties, or even make personal investments. At this point, the money is fully integrated into the financial system, with no clear link to its criminal origin.

Traditional money laundering techniques include smurfing, where criminals divide large sums of illicit cash into smaller deposits below the $10,000 reporting threshold and spread them across multiple "smurfs" and accounts to avoid detection.[38] Another tactic is the use of mules—individuals who knowingly or unknowingly move money through deposits, wire transfers, or currency exchanges, who are often recruited online or paid a fee to "clean" the funds.[39] Shell companies, which often lack assets, employees, physical offices,

37. United Nations Office on Drugs & Crime, *supra* note 7. MARY ALICE YOUNG, BANKING SECRECY AND OFFSHORE FINANCIAL CENTERS: MONEY LAUNDERING AND OFFSHORE BANKING 9, 11 (2012).

38. U.S. DEP'T OF THE TREASURY, *supra* note 2, at 30; *see* CHAINALYSIS, *supra* note 12, at 24; *see also What Is the Difference Between Smurfing and Structuring?*, SANCTION SCANNER (Sep. 24, 2024), https://www.sanctionscanner.com/blog/what-is-the-difference-between-smurfing-and-structuring-594#:~:text=Smurfing%20involves%20splitting%20large%20sums,amounts%20to%20avoid%20reporting%20requirements.

39. U.S. DEP'T OF THE TREASURY, *supra* note 2, at 27; *Money Mules*, FBI, https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/money-mules (last visited Oct. 27, 2024); *see, e.g.*, Margot Patrick, *Billions in Dirty Money Flies Under the Radar at World's Busiest Airports*, WALL ST. J. (Apr. 21, 2024),

or genuine business operations, also play a major role.[40] Though sometimes legitimate, they are frequently set up in weak-AML jurisdictions to mask illicit activity through trade, real estate, offshore accounts, or loans.[41] Criminals further exploit gambling and casinos by converting cash into chips, placing minimal-risk bets, and cashing out as checks or transfers, sometimes using junket accounts or colluding to inflate winnings.[42]

These techniques illustrate the creativity and adaptability of launderers in exploiting weaknesses in the traditional financial system. The next Section shows how similar strategies have migrated, and in some cases evolved, in the crypto space.

B. Money Laundering with Cryptocurrencies

Cryptocurrencies are digital currencies that utilize blockchain, consensus mechanisms, peer-to-peer networks, and cryptographic techniques to perform transactions.[43] Unlike traditional payment systems, which rely on centralized entities such as banks to verify and process transactions, cryptocurrencies operate on decentralized networks built on the blockchain.[44] The blockchain functions as a distributed ledger where transactions are recorded chronologically and immutably across a network of computers.[45] Each block in the chain contains a cryptographic hash of the previous block, a timestamp, and transaction data, ensuring the integrity and continuity of the ledger.[46] Consensus mechanisms enable participants in the distributed network to agree on the validity of transactions and the state of the blockchain.[47] This decentralized structure

---

https://www.wsj.com/business/airlines/heathrow-dubai-airports-billions-dirty-money-9f49cc7f ("Officials and industry groups said smuggling cash via airline is a relatively low risk for people hired to do the job . . . . Authorities believe [two hired smugglers in this story] transported $125 million, largely from July to October in 2020.").

40. U.S. DEP'T OF THE TREASURY, *supra* note 2, at 53; *see also* Emmanuel Agwu, *The Role of Shell Companies in Money Laundering & How to Combat Them*, SMILE ID (June 1, 2024), https://usesmileid.com/blog/shell-companies-in-money-laundering.

41. *See* Gabija Stankevičiūtė, *The Risks of Shell Companies in Money Laundering*, IDENFY (Mar. 29, 2024), https://www.idenfy.com/blog/shell-companies-money-laundering; *see also* Agwu, *supra* note 40.

42. U.S. DEP'T OF THE TREASURY, *supra* note 2, at 84; *see also* Institute for Financial Integrity, *Are Casinos Havens for Money Laundering?*, FINTEGRITY (Mar. 12, 2024), https://finintegrity.org/are-casinos-havens-for-money-laundering/.

43. SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM 1 (2008); ORG. FOR ECON. COOP. & DEV. [OECD], OECD BLOCKCHAIN PRIMER 3 (2019).

44. NAKAMOTO, *supra* note 43, at 2; OECD, *supra* note 43, at 4. This analysis focuses public permissionless blockchains, but it is important to note that blockchains come in different forms with various functionalities. The other three main types of blockchains are public permissioned, consortium, and private permissioned ("enterprise") blockchains. Additionally, blockchains have three "layers"—the protocol, networking, and applications layers—serving different purposes. *See* OECD, *supra* note 43, at 5 ("Table 1. The main types of blockchain segmented by permission model" contains a clear breakdown on blockchain types and layers).

45. OECD, *supra* note 43, at 4.

46. NAKAMOTO, *supra* note 43, at 1; OECD, *supra* note 43, at 4.

47. OECD, *supra* note 43, at 6.

eliminates the need for a central authority and allows for peer-to-peer transactions.[48]

One of the defining features of cryptocurrencies is their inherent anonymity and pseudonymity, which makes them particularly appealing for money laundering. Although every transaction is recorded on the blockchain and publicly visible, the identities of participants are concealed behind alphanumeric addresses rather than being linked to personal identifiers such as names.[49] Users can create and manage multiple addresses without revealing any personally identifiable information, adding an additional layer of privacy.[50] In traditional financial systems, intermediaries like banks require users to verify their identities, making it easier to track financial transactions.[51] By contrast, cryptocurrencies aim to operate without intermediaries, making it more difficult for authorities to trace the flow of funds and link transactions to real-world identities.[52]

Money laundering within the cryptocurrency ecosystem follows the same three-step process of placement, layering, and integration as traditional forms of money laundering.[53] However, the methods and tools used at each stage differ due to the unique characteristics of cryptocurrencies.

Placement in crypto usually involves converting illicit funds (often cash) into cryptocurrencies. Instead of depositing cash into banks, criminals can use crypto exchanges to convert cash into cryptocurrencies, often opting for exchanges with fewer AML and Know Your Customer (KYC) requirements.[54] They may also use Bitcoin ATMs to buy cryptocurrency with cash, as these kiosks allow customers to insert banknotes, buy cryptocurrency, and send it directly to a wallet without the need for an exchange or bank account.[55]

48. *Id.*; Nakamoto, *supra* note 43, at 4.

49. OECD, *supra* note 43, at 6.

50. *Id.*

51. *Id.*

52. *Id.*

53. U.N. OFF. ON DRUGS & CRIME, CASINOS, MONEY LAUNDERING, UNDERGROUND BANKING, AND TRANSNATIONAL ORGANIZED CRIME IN EAST AND SOUTHEAST ASIA: A HIDDEN AND ACCELERATING THREAT 6 (Jan. 2024), https://www.unodc.org/roseap/uploads/documents/Publications/2024/Casino_Underground_Banking_Report_2024.pdf ("Money laundering using cryptocurrencies follows the general pattern of placement-layering-integration.").

54. KYC is the legal and regulatory requirement that financial institutions must verify the identity of their clients before and during the course of a business relationship. For individual clients, financial institutions need to collect information such as legal name, date of birth, residential address, government-issued ID, etc. For institutional clients, information such as legal name, business address, incorporation documents, and tax identification number is necessary for verification. *See* U.S. DEP'T OF JUST., *supra* note 8, at 14.

55. TRM LABS, ILLICIT CRYPTO ECOSYSTEM REPORT: A COMPREHENSIVE GUIDE TO ILLICIT FINANCE RISK IN CRYPTO 36 (June 2023). Crypto ATMs have processed at least $160 million in illicit volumes between 2019 and 2024. TRM also determined that schemes involving multiple payments sent from different ATM companies, often located in different countries, to a single address, is indicative of money laundering. *Rate of Illicit Activity at Crypto ATMs Is Double That of Overall Crypto Industry*,

Additionally, criminals can engage in offline peer-to-peer exchanges, bypassing both exchanges and Bitcoin ATMs altogether.[56] The goal of placement in the cryptocurrency world remains the same: to inject illicit money into the system while avoiding scrutiny.[57]

Layering can be more sophisticated in crypto laundering due to the global and decentralized nature of cryptocurrencies. Criminals often employ various methods to obscure the digital footprint left on the blockchain, such as mixers (also known as tumblers), chain hopping, and nesting services.[58]

Mixers blend cryptocurrencies from various sources and release them at random intervals to destination addresses or wallets.[59] The mixer acts as a "communal washing machine" to obscure the owner of the cryptocurrency, its origin, and its destination.[60] Ultimately, the assets are returned to users in a randomized manner.[61]

Mixers can be classified into centralized and decentralized types. Private third parties operate centralized mixers.[62] The main risk with these mixers is that users can lose their funds if the operator shuts down or engages in theft.[63] Additionally, hackers often target centralized mixers due to the large sums of money they handle.[64] In contrast, decentralized mixers use open-source protocols to enable automatic, permissionless mixing.[65] Although they function similarly to centralized mixers, they eliminate the risks associated with a central authority.[66] Like other decentralized networks, decentralized mixers rely on a large user base.[67] As more people use the mixer, its effectiveness increases, and the chances of detection decrease.[68]

In 2022, the U.S. Office of Foreign Assets Control (OFAC) sanctioned Ethereum's most popular decentralized mixer, Tornado Cash.[69] Tornado Cash allowed users to send funds they wanted to mix and received a cryptographic

---

TRM LABS (Aug. 28, 2024), https://www.trmlabs.com/post/illicit-activity-involving-crypto-atms-is-double-that-of-overall-crypto-industry.

56. U.S. DEP'T OF JUST., *supra* note 8, at 37–39.

57. *Id.*

58. *See generally* ELLIPTIC, *supra* note 21; CHAINALYSIS, *supra* note 21.

59. CHAINALYSIS, *supra* note 21.

60. Jody Houton, *Crypto Mixer Money Laundering: Is the Risk Worth the Reward?*, IDNOW, https://www.idnow.io/blog/crypto-mixer-money-laundering-risk-reward/ (last visited Oct. 27, 2024).

61. *Id.*

62. Lipsa Das, *What Is a Bitcoin Mixer?*, LEDGER ACAD. (June 29, 2023), https://www.ledger.com/academy/topics/blockchain/what-is-a-bitcoin-mixer.

63. *Id.*

64. *Id.*

65. *Id.*

66. *Id.*

67. *Id.*

68. *Id.*

69. Chainalysis Team, *OFAC Sanctions Popular Ethereum Mixer Tornado Cash for Laundering Crypto Stolen by North Korea's Lazarus Group*, CHAINALYSIS (Aug. 8, 2022), https://www.chainalysis.com/blog/tornado-cash-ofac-designation-sanctions.

note in return.[70] This note enabled users to withdraw mixed funds to a new address by sending a transaction referencing the note.[71] OFAC sanctioned Tornado Cash after discovering its role in laundering over $455 million worth of cryptocurrency stolen by the Lazarus Group, a North Korea-affiliated hacking organization.[72] By the time it was sanctioned, Tornado Cash had processed over $7.6 billion worth of Ethereum, most of which originated from high-risk sources.[73]

Nesting services have also been frequently used for layering.[74] They can be understood by comparing them to correspondent banking, an arrangement where one bank (the correspondent) provides services such as international fund transfers and cash management to another bank (the respondent).[75] The respondent bank leverages this relationship to serve clients without opening branches abroad.[76] Similarly, in cryptocurrency, a "correspondent" exchange acts as an intermediary for a "respondent" exchange, allowing the respondent exchange to tap into the liquidity and trading services of the larger platform.[77]

Criminals exploit this setup by laundering money through smaller exchanges with weak AML/KYC protocols.[78] For example, a criminal might deposit illicit funds into a small exchange in a country with lax regulations. The smaller exchange then routes these funds through the larger exchange as part of its regular operations.[79] Because the larger exchange processes thousands of transactions, the criminal's funds are "nested" within a large pool of legitimate activity, making it difficult for the larger exchange to detect illegal transactions.[80]

In addition to exchange services, over-the-counter (OTC) broker services can also be exploited. To begin with, OTC brokers facilitate large, private

---

70. *Id.*

71. *Id.*

72. *Id.*; *see also* Van Loon v. Dep't of the Treasury, 122 F.4th 549 (5th Cir. 2024).

73. Chainalysis Team, *supra* note 69.

74. EUROPOL, CRYPTOCURRENCIES: TRACING THE EVOLUTION OF CRIMINAL FINANCES 8–9 (2021), https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf .

75. *FATF Glossary*, FATF, https://www.fatf-gafi.org/en/pages/fatf-glossary.html (last visited Sep. 29, 2025) ("Correspondent banking is the provision of banking services by one bank (the 'correspondent bank') to another bank (the 'respondent bank').").

76. Correspondent banking possesses money laundering risks because the correspondent bank relies on the respondent bank to conduct KYC diligence on its clients. A correspondent bank may unknowingly facilitate money laundering due to a respondent bank's weak KYC protocols. BANK FOR INT'L SETTLEMENTS, COMM. ON PAYMENTS AND MARKET INFRASTRUCTURES, CORRESPONDENT BANKING 9–10 (July 2016), https://www.bis.org/cpmi/publ/d147.pdf; Will Kenton, *Correspondent Bank: Definition and How It Works*, INVESTOPEDIA (May 2, 2023), https://www.investopedia.com/terms/c/correspondent-bank.asp#citation-2.

77. *What Are Nested Exchanges and Why Should You Avoid Them?*, BINANCE ACAD. (Dec. 3, 2021), https://academy.binance.com/en/articles/what-are-nested-exchanges-and-why-should-you-avoid-them.

78. *Id.*

79. EUROPOL, *supra* note 74, at 8.

80. *Id.*

transactions outside of exchange order books.[81] Unlike ordinary exchange trades, which are visible to all market participants, OTC transactions are negotiated directly between brokers and clients and remain opaque to outsiders.[82] These services conceal critical details such as the identities of the parties, the size of the transaction, and the negotiated price.[83] Next, to obtain liquidity, OTC brokers often route funds through major exchanges, embedding these transfers within the broader flow of legitimate trading activity.[84] As a result, illicit funds can be layered through OTC channels and exchanges in ways that make them difficult to detect, allowing launderers to obscure the origins of their assets before re-entering the financial system.[85]

Another way to obscure the connection between the funds and their illegal source in the layering stage is through chain hopping.[86] Chain hopping refers to a scenario where criminals rapidly exchange one cryptocurrency for another, often in rapid succession and across multiple exchanges.[87] This method is "frequently used by individuals who are laundering proceeds of virtual currency thefts," as it complicates the transaction trail by shifting it from one blockchain to another.[88] For example, a hacker who receives illicit Bitcoin from ransomware operations engages in chain hopping by exchanging the Bitcoin for Ethereum, then Ethereum for Tether, Tether for Solana, and so on. Similarly, criminals can transfer funds between multiple cryptocurrency wallets they control.[89] These wallets can be spread across various jurisdictions or held under pseudonyms, making tracking more difficult.

The final stage of money laundering in the crypto world, the integration stage, involves converting laundered cryptocurrency into assets or fiat currency that can be used without suspicion.[90] Criminals can use crypto exchanges to convert laundered cryptocurrency back into fiat currency or stablecoins (such as USDC or USDT), which are pegged to fiat currency.[91] Criminals can also use

81. *Id.* at 9.

82. *What Are Crypto OTC Desks and How Do They Work?*, COINDESK (Jan. 11, 2024), https://www.coindesk.com/learn/what-are-crypto-otc-desks-and-how-do-they-work/.

83. *Id.*

84. EUROPOL, *supra* note 74, at 9.

85. *Id.*; *see also* SK Arora, *What Is OTC Crypto Trading, and How Does It Work?*, COINTELEGRAPH (Mar. 1, 2024), https://cointelegraph.com/explained/c.rypto-otc-trading.

86. U.S. DEP'T OF JUST., *supra* note 8, at 44.

87. *Id.*

88. *Id.*

89. *Money Laundering in Crypto: How Criminals Hide Their Tracks*, MERKLE SCI. (Nov. 21, 2024), https://www.merklescience.com/blog/money-laundering-in-crypto-how-criminals-hide-their-tracks.

90. *See* United Nations Office on Drugs & Crime, *supra* note 7 ("Integration (i.e. making the money available to the criminal from what seem to be legitimate sources).").

91. *What Is a Stablecoin?*, COINBASE, https://www.coinbase.com/learn/crypto-basics/what-is-a-stablecoin#:~:text=Stablecoins%20are%20a%20type%20of,more%20suitable%20for%20common%20transactions (last visited Oct. 27, 2024); Cryptopedia Staff, *What Are Stablecoins?*, GEMINI CRYPTOPEDIA (July 20, 2023), https://www.gemini.com/cryptopedia/what-are-stablecoins-how-do-they-work.

the "cleaned" cryptocurrency to purchase expensive assets such as real estate, luxury cars, and artwork (e.g., NFTs).[92] Some businesses and individuals now accept direct crypto payments, bypassing traditional banking systems.[93] They can also invest in legitimate businesses in cryptocurrency-friendly sectors such as tech startups or by funding crypto mining operations.[94] The ultimate goal of integration in both traditional and crypto laundering is to make the money appear as though it has come from a legitimate source.

C. Emerging Trends

In recent years, money laundering through cryptocurrency has evolved, with criminals increasingly turning to new methods such as stablecoins, NFTs, DeFi platforms, privacy coins, layer 2 solutions, and even generative AI to obscure the origins of illicit funds.[95] These new trends reflect the growth and diversification of the cryptocurrency ecosystem, as well as the challenges that law enforcement and regulators face in keeping pace.

Stablecoins**,** pegged to traditional assets like the U.S. dollar, have become a popular tool for money laundering due to their stability and ease of use.[96] Unlike more volatile cryptocurrencies like Bitcoin or Ethereum, stablecoins maintain a consistent value, making them ideal for transferring large sums of illicit funds without risking devaluation.[97] In 2024, stablecoins were involved in approximately 60% of all illicit cryptocurrency transactions, a significant increase from approximately 20% in 2020.[98] This trend contrasts with Bitcoin, which originally comprised most illicit cryptocurrency transaction volumes—accounting for approximately 75% of all cryptocurrency crime in 2020—but has seen a decline in recent years.[99] Between 2020 and 2024, Bitcoin's share of illicit

92. Chainalysis Team, *Crime and NFTs: Chainalysis Detects Significant Wash Trading and Some NFT Money Laundering in This Emerging Asset Class*, CHAINALYSIS (Feb. 2, 2022), https://www.chainalysis.com/blog/2022-crypto-crime-report-preview-nft-wash-trading-money-laundering.

93. *250+ Companies & Stores That Accept Cryptocurrency*, BITPAY, https://bitpay.com/directory/ (last visited Oct. 27, 2024).

94. Agent Gold, *How to Finance a Bitcoin Mining Operation in 2022*, HASHRATE INDEX (Mar. 17, 2022), https://hashrateindex.com/blog/how-to-finance-a-bitcoin-mining-setup-a-guide-for-retail-investors-and-institutions.

95. Nizan Geslevich Packin & Uri Volovelsky, *Digital Assets, Anti-Money Laundering and Counter-Financing of Terrorism: An Analysis of Evolving Regulations and Enforcement in the Era of NFTs*, *in* THE CAMBRIDGE HANDBOOK ON LAW AND POLICY FOR NFTS 18 (2023) ("[I]nstances of NFTs being used in money laundering and terrorist financing schemes have already been observed.").

96. COINBASE, *supra* note 91; Cryptopedia Staff, *supra* note 91; ELLIPTIC, ELLIPTIC TYPOLOGIES REPORT 2024: PREVENTING FINANCIAL CRIME IN CRYPTOASSETS 55 (2024); *see also* Yulia Guseva, Sangita Gazi & Douglas Eakeley, *On Innovation and the Coexistence of Stablecoins and Central Bank Digital Currencies*, 87 LAW & CONTEMP. PROBS. 91, 113–14 (2025) (highlighting the emergence of stablecoins posing a threat to the sovereignty of established currencies and challenging counter money laundering efforts).

97. ELLIPTIC, *supra* note 96, at 55.

98. CHAINALYSIS, *supra* note 15, at 6.

99. *Id.*

transaction volume dropped from 75% to 20%.[100] Criminals favor stablecoins in cross-border transactions, especially in jurisdictions with strict capital controls or sanctions.[101] Sanctioned entities and jurisdictions, in particular, accounted for $14.9 billion (61.5%) of illicit cryptocurrency transaction volume in 2023,[102] much of it through stablecoins.[103]

NFTs, which represent ownership of digital assets such as artwork, have also emerged as a tool for laundering money.[104] Criminals can exploit the lack of regulation in NFT marketplaces to engage in wash trading, artificially inflating the value of NFTs by buying and selling them among themselves.[105] This creates the appearance of legitimate profits from the sale of NFTs, which can then be cashed out as clean funds.[106] Although comprehensive data on the scale of money laundering through NFTs are still developing, there have been reports of illicit actors moving millions of dollars in cryptocurrency through NFT platforms, leveraging the anonymity provided by decentralized wallets.[107]

DeFi platforms, which operate without intermediaries and allow users to trade, borrow, and lend cryptocurrency directly, have become another avenue for money laundering.[108] In 2023, DeFi continued to receive illicit inflows as criminals took advantage of the relative lack of oversight and KYC

100. *Id.*
101. ELLIPTIC, *supra* note 96, at 63.
102. *Id.* at 8–9.
103. *Id.*
104. Chainalysis Team, *supra* note 92.
105. *Id.*
106. *Id.*
107. Although over $100 million of NFTs were publicly reported as stolen though scams between July 2021 and July 2022, approximately $8 million of illicit funds were laundered through NFT-based platforms between Q4 2017 to Q2 2022, or 0.02% of trading activity originated from known sources. Most of these illicit funds flowing into NFT services originated from thefts, scams, phishing, or Ponzi schemes. In contrast, illicit funds flowing from malware, dark web services, and criminal organization remained minimal, constituting $30,000 of inflows into NFT services. ELLIPTIC, NFTS AND FINANCIAL CRIME: MONEY LAUNDERING, MARKET MANIPULATION, SCAMS & SANCTIONS RISK IN NON-FUNGIBLE TOKENS 4, 70 (2022). In 2021, the U.S. Treasury sanctioned Chatex, a cryptoasset exchanged registered in Latvia, accused of laundering ransomware and darknet market proceeds. It was tied to SUEX, another Russian-based exchange that shared the same founder. One of the sanctioned addresses contained 42 NFTs worth approximately $531,600 in total. This was the first time that NFTs were involved in international sanctions due to their alleged use in laundering cybercrime proceeds. *Id.* at 71. In 2022, the "Frosties" scam NFT project boasted about upcoming metaverse capabilities and other features of NFT projects. After 8,888 NFTs were minted, the project shut down its social media servers and disabled its website, making $1.1 million in ETH. Over 94% of the proceeds were laundered through Tornado Cash, whereas the remainder was laundered through centralized exchanges. The DOJ ultimately arrested two perpetrators of this "rug pull," who were preparing launch another million-dollar rug pull scheme. ELLIPTIC, *supra* note 96, at 104–05.
108. *See* U.S. DEP'T OF THE TREASURY, ILLICIT FINANCE RISK ASSESSMENT OF DECENTRALIZED FINANCE 5, 16 (Apr. 2023), https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf. Three types of decentralized applications—decentralized exchanges, decentralized mixers, and cross-chain bridges—are used to launder funds on DeFi. ELLIPTIC, DEFI: RISK, REGULATION, AND THE RISE OF DECRIME 21 (2021).

requirements.[109] One of the most prominent methods used involves cross-chain bridges, which allow users to move cryptocurrency between blockchains, making it harder to track the flow of funds.[110] In 2023, $743.8 million in illicit value moved through cross-chain bridges, a sharp increase from previous years.[111] DeFi's growth as a platform for money laundering is closely tied to the rise of these bridges, which enable sophisticated criminals to obfuscate their transactions.[112]

Privacy coins such as Monero[113] and Zcash[114] have long been associated with money laundering and their use has steadily increased due to their ability to conceal transaction details.[115] These coins, which obscure the sender and receiver's identities, are favored by criminals seeking to operate under the radar.[116] The use of privacy coins for laundering purposes is heightened when criminals use them in tandem with decentralized exchanges (DEXs), mixing services, and digital wallets to further obscure the source of illicit funds.[117]

In parallel, layer 2 solutions further complicate AML efforts. Layer 2 solutions are protocols built on top of a base blockchain (layer 1, like Bitcoin or

109. CHAINALYSIS, *supra* note 12, at 7, 25. Although the percentage of total illicit funds received by DeFi protocols decreased relative to 2022, it remains significantly elevated from 2019, when less than 3% of laundered funds were sent to DeFi protocols. Today, over 10% of total illicit funds are sent to DeFi protocols.

110. ELLIPTIC, *supra* note 96, at 51. Cross-chain bridges allow for an asset on one blockchain to be represented as a token on another. For example, someone who owns Bitcoin and wants to conduct transactions with Ethereum-based Dapps cannot because the Bitcoin on the two blockchains are incompatible. Cross-chain bridges overcome this problem by allowing the Bitcoin to be represented as a token on Ethereum's blockchain. The user does not need to exchange their Bitcoin, surrender custody, or undergo KYC requirements, which would be required at a centralized exchange. *Id.*

111. CHAINALYSIS, *supra* note 12, at 32.

112. ELLIPTIC, *supra* note 96, at 51.

113. Monero transactions are confidential and untraceable. The sender, receiver, and amount of every transaction are hidden through Steal Addresses, Ring Signatures, and RingCT. What is Monero (XMR)? For more information on the complex technology underlying Monero, see *Moneropedia: Ring Signature*, MONERO, https://www.getmonero.org/resources/moneropedia/ringsignatures.html (last visited Oct. 27, 2024); Ronald L. Rivest, Adi Shamir & Yael Tauman, *How to Leak a Secret*, 2248 LECTURE NOTES IN COMPUT. SCI. 552 (2001); Peter Todd, *Stealth Addresses*, LINUX FOUND. (Jan. 6, 2014), https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2014-January/004020.html; Vitalik Buterin, *An Incomplete Guide to Stealth Addresses*, VITALIK.ETH (Jan. 20, 2023), https://vitalik.eth.limo/general/2023/01/20/stealth.html; Shafi Goldwasser, Silvio Micali & Charles Rackoff, *The Knowledge Complexity of Interactive Proof Systems*, 18 SOC'Y FOR INDUS. & APPLIED MATHEMATICS J. COMPUT. 186 (1989); Aleksander Berentsen, Jeremias Lenzi & Remo Nyffenegger, *An Introduction to Zero-Knowledge Proofs in Blockchains and Economics*, 105 FED. RSRV. BANK OF ST. LOUIS REV. 280 (2023).

114. Zcash uses zero-knowledge proofs to validate transactions without revealing any underlying information. However, they "selectively transparent" and do not anonymize every user by default. For more information on ZKPs, see how Monero transactions are confidential and untraceable: Petar Stoykov, *Demystifying Zero-Knowledge Proofs: The Future of Web3 Privacy*, CHAINSTACK (Aug. 18, 2023), https://chainstack.com/demystifying-zero-knowledge-proofs.

115. ELLIPTIC, *supra* note 96, at 64.

116. *Id.*

117. *Id.*

Ethereum) to improve scalability, transaction speed, and cost efficiency.[118] By enabling a series of smaller off-chain transactions, layer 2 solutions make fund flows less traceable.[119] Although exact figures are difficult to determine, the growing adoption has become a notable trend in crypto money laundering.[120]

Additionally, criminals have begun incorporating generative AI into their crypto money laundering practices. A dark web service, Only Fake, has been offering AI-generated fake IDs, enabling users to open accounts on financial services platforms while bypassing KYC procedures.[121] The Hydra marketplace, another dark web platform, utilized AI-driven algorithms to mix cryptocurrency transactions, effectively obfuscating the origin of funds.[122] AI-generated fake businesses and online marketplaces can also provide a cover for the movement of illicit funds. This growing trend highlights the increasing threat of generative AI in the hands of cybercriminals, making it more challenging for law

118. Blockchains is organized into layers, each with a specific role. Layer 1 forms the base protocol and manages essential functions such as transaction validation, consensus mechanisms and data storage. It focuses on decentralization, security and immutability. Bitcoin, Ethereum and Solana are the most well-known layer 1 blockchains. However, as blockchain adoption surged, significant limitations of layer 1 became apparent, such as scalability bottlenecks and high transaction costs. Layer 2 is built on top of layer 1 to address these limitations. Layer 2 solutions process transactions off-chain or through sidechains, lightening the load on layer 1. For example, the Lightning Network is a layer 2 solution for Bitcoin that facilitates faster and cheaper transactions. Layer 3 provides user-facing applications such as Uniswap (a decentralized exchange) and OpenSea (an NFT marketplace). *See* Rahul Nambiampurath, *A Beginner's Guide to Understanding the Layers of Blockchain Technology*, COINTELEGRAPH (Jan. 14, 2026), https://cointelegraph.com/learn/articles/a-beginners-guide-to-understanding-the-layers-of-blockchain-technology; Investopedia Team, *Lightning Network: What It is and How It Works*, INVESTOPEDIA (May 8, 2024), https://www.investopedia.com/terms/l/lightning-network.asp; Sankrit K., *What are Layer-2 Solutions? A Guide to L-2 Blockchains*, MOONPAY (Dec. 12, 2023), https://www.moonpay.com/learn/blockchain/what-are-layer-2-solutions.

119. Fred Kahn, *How Layer-2 Rollups Are Hiding Money Laundering from Crypto AML Teams*, FINCRIME CENT. (Sep. 29, 2025), https://fincrimecentral.com/growing-role-layer2-networks-in-aml-crypto/#why-rollups-and-layer-2-matter-for-money-laundering ("Layer-2 networks . . . operate on top of a base blockchain (layer-1) to batch or compress transactions off-chain, then submit compact proofs or summaries back to the base chain. Because of this architecture, many individual transfers are hidden from direct view on the base chain. Instead, only aggregated proofs or checkpoints are visible. That means much of the transaction detail is internal to the layer-2 environment or in off-chain data stores or rollup nodes. Criminal actors can exploit this by hiding more of their money movement from monitoring systems that only observe the base chain.").

120. *Chain Hopping: The Future of Crypto Money Laundering*, MERKLE SCI. (July 10, 2023), https://www.merklescience.com/blog/chain-hopping-the-future-of-crypto-money-laundering ("[C]ybercriminals are turning to layer 2 solutions such as side chains or state channels for cross-chain laundering.").

121. EUROPEAN UNION AGENCY FOR L. ENF'T COOP. [EUROPOL], INTERNET ORGANISED CRIME THREAT ASSESSMENT 10 (2024), https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf (detailing the increasing use of Stablecoins, ransomware, and noncompliant services in cryptocurrency money laundering, and finding an investment scam that uses traditional forms of ML—money mules, international bank accounts, cash movements, and underground banking—compared to peer-to-peer platforms, which use messaging applications).

122. Press Release, U.S. Dep't of Just., Justice Department Investigation Leads to Shutdown of Largest Online Darknet Marketplace (Apr. 5, 2022), https://www.justice.gov/opa/pr/justice-department-investigation-leads-shutdown-largest-online-darknet-marketplace.

enforcement agencies to detect and prevent money laundering in the crypto space.

Despite these new trends, centralized exchanges remain the primary destination for laundered cryptocurrencies.[123] In 2023, five major fiat off-ramping service providers—platforms that allow individuals to convert cryptocurrencies into fiat currencies such as USD, EUR, and other tangible assets—received 71.7% of all illicit funds sent to off-ramping services.[124] Additionally, money laundering activities tend to be concentrated among several deposit addresses.[125] For example, in 2023, the top 109 addresses, which received over $10 million each in illicit funds, accounted for a cumulative $3.4 billion.[126] This suggests that although criminals explore new avenues such as DeFi and NFTs, they continue relying heavily on centralized exchanges and key addresses to off-ramp their illicit gains.

These emerging trends highlight the increasing sophistication of money laundering in the crypto space. Criminals have moved beyond early methods, such as using Bitcoin for payments, and now exploit the full range of tools in the rapidly evolving crypto ecosystem. At the same time, existing laws have not kept pace with these developments, creating regulatory gaps that further hinder efforts to combat money laundering, as discussed in the next section.

III.
FAILURE OF EXISTING FRAMEWORK

This Part examines why the existing legal and regulatory framework has failed to effectively address money laundering in the crypto space. Section III.A begins by outlining the three major laws that form the current legal framework. Section III.B provides a comprehensive literature review, highlighting several reasons for its ineffectiveness. Section III.C presents a new explanation from the perspective of trust**,** arguing that the misalignment between the crypto industry's "trustless trust" nature and the existing legal framework's reliance on intermediary trust mechanisms fundamentally contributes to the ineffectiveness of compliance and enforcement against money laundering in the crypto space.

A. Existing Legal Framework

AML laws comprise the Bank Secrecy Act (BSA) of 1970 and its subsequent amendments that notably include the Uniting and Strengthening

123. CHAINALYSIS, *supra* note 12, at 25.

124. *Id.* at 26. The report does not state whether these are centralized exchanges. However, it is likely that at least one of these are considering centralized exchanges' dominance with regard to the destination for laundered cryptocurrency.

125. *Id.* at 27.

126. *Id.*

America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("Patriot Act") of 2001 and the AMLA Act of 2020.[127]

1. Bank Secrecy Act of 1970

The BSA stands as a cornerstone in U.S. AML legislation. Passed in 1970 to prevent banks from engaging in tax evasion, it also provided tools in fighting organized crime by mandating financial institutions to assist U.S. government agencies in detecting and preventing money laundering, primarily through recordkeeping and reporting.[128]

Financial institutions are required to retain records that are highly useful in criminal, tax, or regulatory investigations and proceedings.[129] This includes maintaining evidence of the identity of individuals engaging in transactions that must be recorded or reported under the BSA.[130] The Secretary of the Treasury prescribes the specific types of records to be retained, which may include microfilm or other reproductions of checks, drafts, or other instruments drawn on the bank, as well as records of each check, draft, or other instrument received for deposit or collection.[131] More recently, the Secretary of the Treasury was given authority to prescribe electronic or automated modes of recordkeeping.[132] Additionally, financial institutions must maintain records related to changes in ownership, control, and management.[133] The Secretary of the Treasury determines the retention period for these records, which generally should not exceed six years unless a longer period is deemed necessary for a particular type of record.[134]

Key requirements regarding making reports include (1) reporting transactions over $10,000 with a Currency Transaction Report (CTR),[135] (2) reporting financial interests in foreign accounts with Foreign Bank and Accounts Reports (FBARs),[136] and (3) filing reports of suspicious activity that might signify money laundering, tax evasion, or other criminal activities with a Suspicious Activity Report (SAR).[137]

---

127. 31 U.S.C. §§ 5311–5314; Pub. L. No. 107-56, 115 Stat. 272 (2001); Pub. L. No. 116-283, div. F, 134 Stat. 3388, 4547 (2021).

128. FIN. CRIMES ENF'T NETWORK [FINCEN], A REPORT TO CONGRESS IN ACCORDANCE WITH SECTION 357 OF THE USA PATRIOT ACT 8 (Apr. 26, 2002), https://www.fincen.gov/sites/default/files/shared/ReportToCongress357.PDF.

129. 12 U.S.C. § 1829b(a)(1)(A).

130. 12 U.S.C. § 1829b(e).

131. 12 U.S.C. § 1829b(d).

132. 12 U.S.C. § 1953(c).

133. 12 U.S.C. § 1952.

134. 12 U.S.C. § 1829b(g).

135. 31 C.F.R. §§ 1010.311, 1010.340 (including "each deposit, withdrawal, exchange of currency or other payment or transfer").

136. 31 C.F.R. § 1010.350(a).

137. 31 C.F.R. § 1010.540(c) (requiring that financial institutions file reports as laid out in the act to the appropriate federal agency if the financial institution knows or suspects "an individual, entity, or organization is involved in, or may be involved in terrorist activity or money laundering").

The U.S. Department of the Treasury created the Financial Crimes Enforcement Network (FinCEN) in 1990 and delegated much of its BSA responsibilities to it. FinCEN therefore monitors financial institutions' compliance with new laws and regulations, offers recommendations, conducts analysis, and gathers financial data related to compliance and financial crimes.[138]

2. Patriot Act of 2001

The Patriot Act of 2001,[139] enacted after the September 11 attacks as part of a government effort to tighten U.S. national security, strengthened AML laws by first expanding the definitional scope of financial institutions to include a variety of non-bank entities, such as credit unions, casinos, and what constitutes a "licensed sender of money."[140] Notably, the Patriot Act extended BSA-related duties to nonfinancial trades or businesses.[141]

Next, the law introduced additional requirements for financial institutions, including (1) the formal statutory requirement for all covered institutions to establish AML programs,[142] (2) enhanced due diligence procedures, particularly for accounts involving foreign individuals or entities,[143] (3) enhanced KYC requirements to verify and keep records of the identity of their clients,[144] and (4) increased requirements to share information between financial institutions about potential money laundering threats.[145]

---

138. *See* U.S. Dep't of the Treasury, Treas. Order. 105-08 (Apr. 25, 1990); *see also* U.S. Dep't of the Treasury, Treas. Order. 180-01 (Sep. 26, 2002) (solidifying FinCEN as a bureau of the Department of the Treasury).

139. Title III is the part of the Patriot Act dealing specifically with AML/CFT laws.

140. 31 U.S.C. § 5312(a)(2) (2001) (defining new institutions covered by these regulations and requirements).

141. 31 U.S.C. § 5312(a)(4) (2001). In contrast to financial institutions, nonfinancial trades or businesses could include retail stores, manufacturing companies, service providers, and other entities that engage in commercial activities but do not primarily deal with financial transactions or services. Nonfinancial trades or businesses are still subject to certain reporting obligations, especially when they engage in significant cash transactions.

142. 31 U.S.C. § 5318(h) (2018) (requiring financial institutions to establish anti-money laundering programs, including, at a minimum: (A) the development of internal policies, procedures, and controls; (B) the designation of a compliance officer; (C) an ongoing employee training program; and (D) an independent audit function to test programs).

143. 31 U.S.C. § 5318(i)(1) (2018) (requiring financial institutions to establish appropriate, specific, and, where necessary, enhanced due diligence policies, procedures, and controls that are reasonably designed to detect and report instances of money laundering if the financial institution establishes, maintains, administers, or manages a private banking account or a correspondent account in the United States for a non-United States person).

144. 31 U.S.C. § 5318(l)(2) (2018) (requiring financial institutions to, at a minimum, implement, and customers to comply with, reasonable procedures for (A) verifying the identity of any person seeking to open an account to the extent reasonable and practicable, (B) maintain records of the information used to verify a person's identity, including name, address, and other identifying information, and (C) consulting lists of known or suspected terrorists or terrorist organizations provided to the financial institution by any government agency to determine whether a person seeking to open an account appears on any such list).

145. 31 U.S.C. § 5311(5) (2021) (establishing appropriate frameworks for information sharing among financial institutions, their agents and service providers, their regulatory authorities, associations

The Patriot Act expanded the types of transactions that need to be recorded, including foreign transactions or transactions in foreign currency or coin.[146] It also offered legal liability protection to financial institutions, incentivizing more extensive recordkeeping and reporting without concern for liability.[147] Additionally, the Patriot Act allowed for greater sharing of information regarding such reports between federal intelligence agencies.[148] The law expanded the responsibilities of FinCEN to monitor financial institutions' compliance with the new laws and regulations, gather financial data related to compliance and financial crimes, and offer recommendations.[149]

In addition to FinCEN, the Patriot Act enabled the Office of Foreign Assets Control (OFAC) to impose sanctions. OFAC maintains a list of blocked or sanctioned persons (e.g., terrorists) and entities, which is frequently updated and available on their website as the Specially Designated Nationals (SDNs).[150] Institutions are required to check OFAC's list of SDNs before creating new accounts and facilitating transactions.[151]

3. AMLA of 2020

Congress enacted the AMLA as part of the National Defense Authorization Act for Fiscal Year 2021 to enhance and modernize AML laws. The AMLA authorizes enhanced information sharing among financial institutions and between financial institutions and the government.[152] Since its enactment, regulations have been adopted that require financial institutions to follow specific procedures for sharing information to identify and report activities that may involve terrorist activity or money laundering.[153] The AMLA also mandated

---

of financial institutions, the Department of the Treasury, and law enforcement authorities to identify, stop, and apprehend money launderers and those who finance terrorists).

146. 31 U.S.C. § 5331 (requiring the filing of a report from any who receives more than $10,000 in coins, domestic currency, or foreign currency in the course of their business, with such a report including the details of the transaction, as well as the identification information of both the individual transacted with/reported on and the filer of the report).

147. 31 U.S.C. § 5318(g)(3) (granting, generally, immunity from liability to individuals or institutions who, when making a voluntary disclosure of potentially illegal activity, may otherwise incur a legal liability as a result of such disclosure, either at the federal or state level).

148. 31 U.S.C. §§ 5318(g)(4)(B), 5319.

149. 31 U.S.C. § 310 (2018).

150. 31 C.F.R. Ch. V, App. A (2024); *Sanctions List Service*, OFF. OF FOREIGN ASSETS CONTROL, https://ofac.treasury.gov/sanctions-list-service (last visited Sep. 20, 2024).

151. 31 C.F.R. § 1028.210 (requiring credit card operators to check OFAC's list of SDNs); *see also* 31 U.S.C. § 5318.

152. 31 U.S.C. § 5318(g)(8) (granting financial institutions the right to share information with their international divisions, subsidiaries, and partners); 31 U.S.C. § 5318(g)(5)(D) (establishing streamlined and automated SAR reporting to the government).

153. 31 C.F.R. § 1010.540(b). First, financial institutions must submit a notice to FinCEN if they intend to share information. Second, before sharing information, financial institutions must verify that the other institution with which they intend to share information has also submitted the required notice to FinCEN. Third, the information received by a financial institution under this regulation must only be used for specific purposes: identifying and reporting on money laundering or terrorist activities,

the creation of a whistleblower program for reporting money laundering violations, the first of its kind within the AML legal framework.[154]

The AMLA again revised the statutory definitions of "financial agency," "financial institution," and "monetary instruments."[155] These amendments broadened the language to encompass a wider range of what can be regulated, including "value that substitutes for currency."[156] Often, cryptocurrency is not defined as a currency,[157] but this language allows for the regulation of currency substitutes such as cryptocurrency or other virtual currencies. Additionally, the Code of Federal Regulations (CFR) adopts the inclusive language of "value that substitutes for currency." For example, a "money transmitter" is defined as a person engaged in the "transmission of currency, funds, or other value that substitutes for currency to another location or person by any means," which encompasses virtual currencies.[158]

As a result of statutory and regulatory modernization by the AMLA, cryptocurrency is now under the purview of the existing recording and reporting strategy initially established by the BSA and later expanded by the Patriot Act. This includes the filing of SARs, CTRs, and FBARs for cryptocurrency transactions.

Table 1: 31 USC § 5312 Definitions Expansion

	(2) Financial Institution
BSA (1970–2001)	(A) an insured bank; (B) a commercial bank or trust company; (C) a private banker; (D) an agency or branch of a foreign bank in the United States; (E) an insured institution (under National Housing Act); (F) a thrift institution; (G) a broker or dealer registered with the SEC; (H) a broker or dealer in securities or commodities; (I) an investment banker or investment company;

determining whether to establish or maintain an account or engage in a transaction, or assisting in compliance with any requirement of the chapter.

154. Brett Wolf, *US Senate Passes Defense Bill with New Anti-Money Laundering Measures*, THOMSON REUTERS (Dec. 15, 2020), https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/defense-bill-anti-money-laundering/.

155. LIANA W. ROSEN & RENA S. MILLER, CONG. RSCH. SERV., R47255, THE FINANCIAL CRIMES ENFORCEMENT NETWORK (FINCEN): ANTI-MONEY LAUNDERING ACT OF 2020 IMPLEMENTATION AND BEYOND (Sep. 27, 2022), https://www.congress.gov/crs-product/R47255.

156. 31 U.S.C. § 5312(a)(1)–(3) (giving discretion to the Secretary of the Treasury to further define the term "value that substitutes for currency" for (a)(3)(A)–(C)).

157. *See, e.g.*, IRS Virtual Currency Guidance, I.R.S. Notice 2014-21, 2014-16 I.R.B. 938 (Mar. 25, 2014) (declaring that the IRS would treat virtual currencies as property, not currency).

158. 31 C.F.R. § 1010.100(ff)(5).

	(J) a currency exchange; (K) an issuer, redeemer, or cashier of travelers' checks, checks, money orders, or similar instruments; (L) an operator of a credit card system; (M) an insurance company; (N) a dealer in precious metals, stones, or jewels; (O) a pawnbroker; (P) a loan or finance company; (Q) a travel agency; (R) a licensed sender of money; (S) a telegraph company; (T) a business engaged in vehicle sales . . . ; (U) persons involved in real estate closings and settlements; (V) the United States Postal Service; (W) an agency of . . . government carrying out a duty or power of a business described in this paragraph; (X) any business or agency which engages in any activity which the Secretary of the Treasury determines, by regulation, to be an activity which is similar to, related to, or a substitute for any activity in which any business described in this paragraph is authorized to engage; (Y) any other business designated by the Secretary whose cash transactions have a high degree of usefulness in criminal, tax, or regulatory matters.
Patriot Act (2001–2021)	(E)[159] any credit union (R) a licensed sender of money or any other person who engages as a business in the transmission of funds, including any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system (X) casinos . . .
AMLA 2020	(J) a currency exchange or a business engaged in the exchange of currency, funds, or value that substitutes for currency or funds . . . [160]

159. Inserting entities into the list of financial institution shifted itemized lettering over time.
160. 31 U.S.C. § 5312(a)(2).

B. Existing Critiques

A comprehensive review of the literature reveals several factors that contribute to the ineffectiveness of AML laws in combating money laundering, including definitional ambiguity, excessive economic costs, disproportionate compliance burden, and an ineffective rule-based approach.

1. Definitional Ambiguity

AML laws suffer from broad and ambiguous definitions. The BSA, Patriot Act, AMLA, and the accompanying regulations categorize "financial institutions" to include licensed senders of money and money transmitters.[161] The statutory and regulatory definitions of these two terms are problematic as they could, in theory, apply to virtually anyone engaging in the transfer of funds, creating an overly expansive regulatory scope.[162] Such vagueness creates uncertainty and poses a risk of criminalizing ordinary business activities,[163] a problem that is especially acute in the crypto space. The vague and broad definitions impose unclear compliance requirements on multi-signature wallets, DeFi platforms, and governance tokens.[164]

For instance, a multi-signature wallet can both receive and send money,[165] and if cryptocurrency is deemed to constitute "money," the wallet may fall within the category of a "money transmitter." Yet the wallet setup requires multiple private keys to authorize a transaction.[166] Who, then, is the actual "money transmitter"? Each keyholder? Only the initiator of the transaction? Or the software provider? Regulators cannot easily assign responsibility, making enforcement fraught. If regulators interpret each participant as a potential "money transmitter," then developers, custodial service providers, or even individual keyholders could all be subject to licensing, recordkeeping, and reporting requirements. This imposes disproportionate liability risks on actors who are not engaged in traditional money-transmission businesses.

---

161. 31 U.S.C. § 5312(a)(2)(R) ("licensed sender of money or any other person who engages as a business in the transmission of . . . funds"); 31 C.F.R. § 1010.100(ff)(5) (defining "money transmitter" as "[a] person that provides money transmission services. The term 'money transmission services' means the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means.").

162. Valkenburgh, *supra* note 22, at 7–10 (using a plain reading approach results in a reading that is "broad verging on absurdity").

163. *Id.* at 8 (illustrating how a barber can be ensnared by recording and reporting regulations because a barber can be categorized as a money transmitter).

164. *Id.*

165. *What Is Multi-Signature (Multi-Sig)?*, COINBASE, https://www.coinbase.com/learn/wallet/what-is-a-multi-signature-multi-sig-wallet (last visited Oct. 26, 2025).

166. *Id.*

2. Excessive Economic Costs

Another downside of the broad and vague definitions is the significant compliance costs they trigger. Crypto businesses must retain legal expertise to interpret them and then build processes to comply. Because failure to comply can result in severe fines and penalties, they are forced to invest heavily in compliance programs to mitigate risks.[167] The fluid and fragmented international regulatory landscape further compounds these challenges, as crypto businesses must continuously adapt to new laws and regulations across multiple jurisdictions.

Additional costs arise because money transmitters involved in crypto transactions are often subject to greater regulatory scrutiny than traditional financial institutions.[168] Whereas traditional banks and payment companies generally are not required to trace an asset's complete transaction history to satisfy sanctions screening and AML monitoring (e.g., CTRs and SARs), money transmitters involved in crypto transactions are expected to monitor blockchain transactions beyond their direct users—tracing prior and subsequent owners of digital assets to ensure compliance.[169] When knowingly dealing with anonymity-enhanced cryptocurrencies, they must not only trace through different transactions including through mixers or privacy coins but also implement procedures to obtain and verify the identities of the originator and beneficiary.[170]

High compliance costs also arise from the requirement to identify links to sanctioned individuals, necessitating the use of advanced technologies to comply with the OFAC screening. Meeting this requirement typically involves adopting

167. 31 C.F.R. § 1022.210; *see also* Joseph Ibitola, *Overcoming the Hidden Costs of AML Compliance*, FLAGRIGHT (June 30, 2025), https://www.flagright.com/post/overcoming-the-hidden-costs-of-aml-compliance (suggesting that crypto firms have learned non-compliance is not an option as several have been fined or even had to shut operations. The crypto firms face dramatic hidden costs—many had to spin up compliance teams from scratch, hire expatriated AML officers, etc., at great cost).

168. CAROL GOFORTH & YULIA GUSEVA, REGULATION OF CRYPTOASSETS 80 (2d ed. 2022) (highlighting a proposed travel rule implementation that would disproportionately impact cryptocurrency transactions).

169. *See* FINCEN, GUIDANCE FIN-2019-G001: APPLICATION OF FINCEN'S REGULATIONS TO CERTAIN BUSINESS MODELS INVOLVING CONVERTIBLE VIRTUAL CURRENCIES 16 (May 9, 2019), https://www.fincen.gov/system/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf (explaining that money transmitters involved in crypto transactions need to track and monitor the transaction history of a crypto through blockchain to satisfy their BSA obligations.); *see also* U.S. Dep't of Treasury, Enforcement Release: OFAC Settles with Bittrex, Inc. for $24,280,829.20 Related to Apparent Violations of Multiple Sanctions Programs (Oct. 11, 2022), https://ofac.treasury.gov/media/928746/download?inline (The settlement notes that "[Bittrex] screened transactions only for hits against OFAC's [SDN List] and other lists but did not scrutinize customers or transactions for a nexus to sanctioned jurisdictions." In other words, law enforcement expects a "nexus" investigation, which would extend beyond immediate transactions and into previous and subsequent transactions that Bittrex had no control over).

170. FinCEN, *supra* note 169, at 21.

sophisticated third-party screening services or developing expensive compliance software, imposing a significant financial burden.[171]

3. Disproportionate Compliance Burden

The AML reporting requirements place a heavy compliance burden on financial institutions yet deliver minimal gains in disrupting illicit activity. Out of fear of noncompliance, financial institutions often submit excessive reports—a practice referred to as technical compliance—rather than pinpointing and addressing money laundering risks.[172] A 2018 study by the Bank Policy Institute found that 19 financial institutions reviewed 16 million alerts and filed over 5.2 million CTRs, yet only 0.44% warranted law enforcement review, with even fewer resulting in criminal convictions.[173] Another report suggested that, out of approximately 4.6 million SARs filed in FY 2023,[174] only about 13,000 cases—less than 0.3% of total SARs—involved either the Internal Revenue Service's criminal investigation or the FBI with some connections to SARs.[175] These results highlight the inefficiency of the current system.

These deficiencies also surface in the crypto space, where a heavy compliance load yields limited gains while creating inequitable and sometimes unintended consequences.[176] The Patriot Act and the AMLA extend compliance obligations beyond banks to crypto businesses, many of which lack the resources and infrastructure that traditional financial institutions have built over decades. Applying the same standards across both sectors disproportionately burdens crypto firms, since the rules were crafted with banks in mind.[177] Critics warn that

171. ELLIPTIC, SANCTIONS COMPLIANCE IN CRYPTOCURRENCIES: USING BLOCKCHAIN ANALYSIS TO MITIGATE RISK 6 (2024).

172. *Conley*, 833 F. Supp. at 1149 (recognizing technical compliance and relying on the testimony of David D. Queen, Acting Assistant Secretary for Enforcement and Operations, Department of the Treasury); *see also* Leopold et al., *supra* note 24 (noting that major banks comply with reporting requirements as a "get-out-of-jail-free card," but do not take action as evidenced by leaked SARs reports).

173. BANK POL'Y INST., *supra* note 24, at 2; *see also* Collin, *supra* note 24 (showing that leaked SARs were frequently submitted months after a suspicious transaction had taken place, and the same client would transact multiple times with seemingly no action by the SAR submitter).

174. FINCEN, YEAR IN REVIEW FOR FY2023 3, https://www.fincen.gov/system/files/shared/FinCEN_Infographic_Public_508FINAL_2024_June_7.pdf.

175. Peter D. Hardy & Siana Danch, *FinCEN Releases Year-in-Review for FY 2023: SARs, CTRs and Information Sharing*, BALLARD SPAHR LLP (June 10, 2024), https://www.moneylaunderingnews.com/2024/06/fincen-releases-year-in-review-for-fy-2023-sars-ctrs-and-information-sharing/.

176. Sun, *supra* note 23 (reporting that Binance spent $213M on compliance in 2023 and expanded to approximately 645 full-time compliance staff members—over 1,000 including contractors—alongside dual U.S. monitorships).

177. *See* Hughes, *supra* note 29, at 25 (arguing that the AML regulatory framework was designed for banks to leverage their important role as gatekeepers); *see also* Christina Parajon Skinner, *Coins, Cross-Border Payments, and Anti-Money Laundering Law*, 60 HARV. J. ON LEGIS. 301, 321 (2022) (extending a similar reliance on banks as special gatekeepers to sanctioning frameworks).

this approach not only strains less-equipped entities but also introduces cybersecurity risks, undermines consumer protection, and may even threaten national security as blockchain technology gains broader adoption.[178]

4. Ineffective Rule-Based Approach

A rule-based approach has proven ineffective in combating money laundering. This approach relies on predefined regulations and guidelines that dictate when financial activities should be recorded and reported to authorities. These approaches operate by setting fixed rules, such as transaction thresholds or patterns, to identify potentially suspicious behavior.[179] Despite longstanding use in the financial industry, these rules have not led to significant success.[180] According to Quantexa, a data analytics company, less than 1% of criminals laundering money globally are caught due to predominantly rule-based AML systems.[181] Most legacy AML systems rely on manually defined rules that money launderers can easily evade, resulting in a false-positive alert rate over 95%.[182] Of these alerts, 98% never lead to a suspicious activity report, forcing costly manual reviews that waste billions annually and divert attention from genuine illicit activity.[183]

The broader inefficacy of the existing AML framework further highlights the limitations of the rule-based approach. Some estimates suggest that this approach has a less than 0.1% impact on criminal finances globally.[184] Confusion over terms like "confiscation" and "forfeiture" further complicates assessment, but regardless of whether 99.9% or 99% of illicit funds remain in criminal hands, the outcome remains the same: serious crimes continue to be enabled and rewarded.[185] Even assuming a generous 1% recovery rate, much of this success comes from conventional law enforcement efforts—such as drug trafficking investigations uncovering laundered assets—rather than from AML regulations.[186]

178. Shlomit Azgad-Tromer, Joey Garcia & Eran Tromer, *The Case for On-Chain Privacy and Compliance*, 6 STAN. J. BLOCKCHAIN L. & POL'Y 265, 282 (2023).

179. *See, e.g.*, Fed. Fin. Insts. Examination Council, *BSA/AML Examination Manual: Assessing Compliance with BSA Regulatory Requirements*, FFIEC BSA/AML INFOBASE, https://bsaaml.ffiec.gov/manual/AssessingComplianceWithBSARegulatoryRequirements/04 (last visited Oct. 2, 2025) (describing transaction-monitoring systems that target specific transaction types to identify unusual activity).

180. QUANTEXA, *How HSBC Uses Technology to Combat Crime | Fireside Chat Series*, (YouTube, Mar. 9, 2021), https://www.youtube.com/watch?v=JmnI2K6OVNg.

181. QUANTEXA, *supra* note 25, at 18.

182. *Google Cloud Launches AI-Powered Anti Money Laundering Product for Financial Institutions*, FINTECH FIN. NEWS (June 21, 2023), https://ffnews.com/newsarticle/fintech/google-cloud-launches-ai-powered-anti-money-laundering-product-for-financial-institutions/.

183. *Id.*

184. Pol, *supra* note 25, at 73, 85.

185. *Id.*

186. *Id.* at 88.

In the crypto space, where transactions can be pseudonymous, borderless, and highly dynamic, such rule-based controls are even less effective. They often fail to capture the complex typologies of the crypto industry because illicit actors employ methods that go far beyond the scenarios envisioned by traditional AML rules. As mentioned in Part I, money launderers may rapidly move crypto across multiple blockchains, use DEXs, or route funds through mixers or privacy coins. These strategies do not fit neatly within fixed thresholds or standardized customer identification rules, meaning that rule-based systems often miss genuinely suspicious activity.

C. A Critique from the Trust Perspective

All of these critiques highlight relevant factors contributing to the inefficiencies and ineffectiveness of the current framework in combating money laundering in the crypto space.[187] However, they seem to overlook a more fundamental issue at the heart of this failure: the inherent conflict of trust. The crypto industry emerged around the concept of "trustless trust,"[188] where cryptographic, decentralized protocols, rather than intermediaries, guarantee the integrity of transactions and relationships. In contrast, the existing legal framework attempts to bring the crypto industry back to an intermediary trust system, forcing it into a structure that undermines its core principles. This conflict between "trustless trust" and intermediary trust is a crucial reason why the current regulatory approach falls short.

1. Trust Architectures

Law professor Kevin Werbach outlines four distinct architectures of trust: peer-to-peer trust, Leviathan trust, intermediary trust, and "trustless trust."[189] Each trust architecture reflects various societal, technological, and institutional approaches to establishing reliability and accountability.

Peer-to-peer trust is established directly between individuals or groups.[190] It is grounded in personal relationships, reputation, and shared experiences within a network.[191] This form of trust arises naturally in human communities and is based on repeated interactions, social bonds, and knowledge of others' past behavior.[192] It is particularly common in smaller communities or informal

187. *See supra* Section III.B.

188. *See* Hoffman, *supra* note 26; *see also* Werbach, *supra* note 26 (Werbach attributes the phrase "trustless trust" to Reid Hoffman).

189. KEVIN WERBACH, THE BLOCKCHAIN AND THE NEW ARCHITECTURE OF TRUST 25–31 (Sandra Braman ed., 2018).

190. *Id.* at 26.

191. *Id.*

192. *Id.*

settings, where individuals know one another personally or can rely on community enforcement mechanisms, such as reputation.[193]

Leviathan trust is based on the idea of a powerful, centralized authority (often the government or a legal system) that enforces rules and provides security.[194] Named after Thomas Hobbes's notion of the "Leviathan,"[195] this model suggests that people can trust one another not necessarily because of personal bonds but because a strong central authority enforces laws and punishes violations.[196] The state's monopoly on force ensures order, resolves disputes, and maintains trust through the legal and regulatory frameworks it imposes.[197] In modern society, legal contracts, law enforcement, and government regulation are key mechanisms of Leviathan trust.[198]

Intermediary trust is established through third-party intermediaries—institutions or entities that facilitate trust between individuals or entities.[199] Banks, payment processors, and platforms like Airbnb or Uber are examples of intermediaries that foster trust by providing guarantees, verification, and dispute resolution mechanisms.[200] Intermediary trust is crucial in larger, more complex systems where individuals do not directly know or interact with one another but rely on trusted third parties to ensure smooth transactions and interactions.[201]

"Trustless trust," a term coined by venture capitalist Reid Hoffman, refers to the trust model enabled by blockchain technology.[202] In this model, trust shifts from intermediaries and authorities to technology that ensures transaction integrity.[203] Participants in the Bitcoin system do not need to know or trust one another; instead, cryptographic protocols and decentralized systems verify transactions, eliminating the need for a centralized oversight and ensuring their validity and security.[204] Hoffman emphasizes that Bitcoin's "trustless trust" architecture is especially noteworthy because it is open source, functioning as a public good without control by any single entity.[205]

To be clear, "trustless trust" does not mean that participants have no need for trust whatsoever. As Nick Szabo, a computer scientist and legal scholar, points out, "there is no such thing as a fully trustless institution or

193. *Id.* (referencing ELINOR OSTROM, GOVERNING THE COMMONS: THE EVOLUTION OF INSTITUTIONS FOR COLLECTIVE ACTION (1990) (Nobel prize-winning work on how fisheries produce stable self-governance surrounding a "Common Pool Resource" of fish)).

194. WERBACH, *supra* note 189, at 27.

195. THOMAS HOBBES, LEVIATHAN; OR, THE MATTER, FORME AND POWER OF A COMMONWEALTH, ECCLESIASTICALL AND CIVIL (1651).

196. WERBACH, *supra* note 189, at 27.

197. *Id.*

198. *Id.*

199. *Id.*

200. *Id.* at 28.

201. *Id.*

202. Hoffman, *supra* note 26.

203. WERBACH, *supra* note 189, at 29–30; *see also* Hoffman, *supra* note 26.

204. NAKAMOTO, *supra* note 43.

205. Hoffman, *supra* note 26.

technology."[206] When Satoshi Nakamoto wrote in the Bitcoin whitepaper about "a system for electronic transactions without relying on trust," he was referring to something much narrower.[207] He meant, in Bitcoin, electronic transactions can be verified as valid without a discrete trustworthy third party, such as a government or bank.[208] The Bitcoin network represents a significant shift in how financial trust is established.[209]

However, trust is not eliminated—it is simply reconstructed. Participants must still trust the developers who wrote the code and trust that the Bitcoin network will process transactions as intended. Blockchain does not remove trust; it reconstructs it in a decentralized form. As Arun Sundararajan of NYU noted, "[i]f you look back at history, every time there was a big expansion in the world's economic activity, it was generally induced by the creation of a new form of trust."[210] The blockchain vision treats trust as a public good rather than a source of private advantage.[211] Since the term "trustless trust" can be misleading, the following Sections will instead use the term decentralized trust to describe this new form of trust.

2. The Conflict with AML Laws

The cryptocurrency industry builds on the concept of decentralized trust, with Bitcoin being one of the earliest examples. Bitcoin employs a decentralized Proof of Work consensus mechanism, where miners solve complex mathematical problems to validate transactions.[212] This process ensures consensus across the network, preventing any single entity from controlling the ledger. Ethereum further advanced this concept by introducing smart contracts—self-executing agreements that automatically enforce terms based on code.[213] For instance, an Ethereum smart contract can manage an escrow arrangement, releasing funds automatically when specific conditions, such as delivery confirmation, are met.[214] This eliminates the need for trusted intermediaries like banks.

---

206. Nick Szabo, *Money, Blockchain, and Social Stability*, SATOSHI NAKAMOTO INST. (Feb. 9, 2017), https://nakamotoinstitute.org/library/money-blockchains-and-social-scalability/.

207. WERBACH, *supra* note 189, at 16.

208. *Id.*

209. *Id.*

210. Reinvent Team, *Will Crowd-Based Capitalism Replace Managerial Capitalism?*, MEDIUM (Aug. 18, 2016), https://medium.com/@Reinvent/will-crowd-based-capitalism-replace-managerial-capitalism-27a3b16394c7.

211. WERBACH, *supra* note 189, at 16.

212. Scott Nevil, *What Is Proof of Work (PoW) in Blockchain?*, INVESTOPEDIA (May 17, 2024), https://www.investopedia.com/terms/p/proof-work.asp.

213. Jean Chalopin & Robin Trehan, *Ethereum's Smart Contracts Explained*, DELTEC BANK, https://www.deltecbank.com/news-and-insights/ethereums-smart-contracts-explained/ (last visited Oct. 18, 2024).

214. Neel Kirit & Priya Sarkar, *Escrow Chain: Leveraging Ethereum Blockchain as Escrow in Real Estate*, 5 INT'L J. INNOVATIVE RSCH. COMPUT. & COMMC'N ENG'G 16237, 16242 (2017).

In recent years, the crypto market has witnessed decentralized trust take shape through a variety of products and services. DeFi platforms such as Uniswap, Aave, and Compound have facilitated peer-to-peer lending, borrowing, and trading without traditional intermediaries.[215] Decentralized autonomous organizations (DAOs) like MakerDAO use smart contracts for collective management.[216] MakerDAO issues the DAI stablecoin, governed by smart contracts and token holder votes, with decisions made collectively rather than by a centralized authority.[217] Projects like Polkadot aim to create interoperable ecosystems that enable secure interactions between different blockchains without intermediaries, further advancing the industry's vision of decentralized trust.[218]

However, the development of decentralized trust within the crypto industry is far from clear-cut. Over time, different industry participants have departed from Bitcoin's original decentralized vision. Some actors have capitalized on the popularity of the decentralized idea while building highly centralized products and services, such as centralized exchanges and fiat-backed stablecoin businesses.[219] Some try to build decentralized projects, but in practice, these projects often exhibit centralized and consolidated power capable of influencing their governance or operations.[220]

The development of decentralized trust in various forms and directions within the crypto industry represents a dynamic that the existing legal framework has failed to recognize. Current laws and regulations continue to rest on the assumption that there is always a centralized entity responsible for compliance. This assumption is evident in statutory text, regulatory interpretation, and enforcement actions.

For instance, the AMLA amended the BSA to include within the statutory definition of a "financial institution" any money transmitting business, or "any other person who engages as a business in the transmission of currency, funds, or value that substitutes for currency."[221] The language "person who engages as a business" presupposes a legally identifiable entity or individual conducting an organized business activity. FinCEN's 2019 Guidance reaffirmed this and added

215. Andry Alamsyah, Gede Natha Wijaya Kusuma & Dian Puteri Ramadhani, *A Review on Decentralized Finance Ecosystems*, 16 FUTURE INTERNET 1, 15–16, 18 (2024).

216. *Id.* at 14.

217. *Id.*

218. *See* Sandra Johnson, Peter Robinson & John Brainard, *Sidechains and Interoperability* 1 (Mar. 22, 2024), https://arxiv.org/pdf/1903.04077.

219. *See, e.g.*, Sirio Aramonte, Wenqian Huang & Andreas Schrimpf, *DeFi Risks and the Decentralisation Illusion*, BANK FOR INT'L SETTLEMENTS (Dec. 6, 2021), https://www.bis.org/publ/qtrpdf/r_qt2112b.htm?.

220. U.S. DEP'T OF THE TREASURY, *supra* note 108, at 1–2; OECD, WHY DECENTRALIZED FINANCE (DEFI) MATTERS AND THE POLICY IMPLICATIONS 11, 45 (Jan. 19, 2022), https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/01/why-decentralised-finance-defi-matters-and-the-policy-implications_5f54eead/109084ae-en.pdf.

221. 31 U.S.C. § 5312(a)(2).

that "when [decentralized applications] perform money transmission, the definition of money transmitter will apply to . . . owners/operators" under the BSA.[222] This interpretation shows FinCEN's assumption that there is an owner/operator to hold accountable. If none exists (e.g., in a decentralized protocol), the Guidance provides no clear path for enforcement. Another piece of evidence is that FinCEN and DOJ enforcement actions have consistently targeted corporate entities and their officers (e.g., BTC-e, BitMEX, and Binance).[223] This enforcement pattern confirms that regulators still conceptualize compliance as an organizational duty attached to identifiable entities and managers.

The assumption is increasingly at odds with the reality and dynamics of the crypto industry. As the industry continues to evolve and diversify, this assumption may hold true for certain centralized projects such as exchanges like Coinbase or Binance, which maintain extensive compliance teams and centralized corporate governance structures. However, the situation becomes far more complex when projects adopt decentralized structures that lack a clear point of accountability.

DEXs provide a case in point. It is challenging to identify entities or individuals who can or should assume the compliance burden. These platforms operate on the blockchain, using smart contracts to automate and manage trading activities. Initially, developers, sometimes anonymous or pseudonymous, set up the protocol, deploy smart contracts, and provide initial liquidity to launch the platform. Once the DEX is operational, governance often transitions to the community through a DAO, where token holders (anyone can be a token holder) vote on protocol changes such as fee structures, upgrades, or new trading pairs.[224]

Most DEXs employ an Automated Market Maker (AMM) model, where users, known as liquidity providers, deposit their assets into liquidity pools.[225] In exchange, they receive a share of the transaction fees generated when trades

222. FINCEN, APPLICATION OF FINCEN'S REGULATIONS TO CERTAIN BUSINESS MODELS INVOLVING CONVERTIBLE VIRTUAL CURRENCIES 18 (May 9, 2019), https://www.fincen.gov/system/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

223. *See, e.g.*, Press Release, U.S Dep't. of Just., Global Cryptocurrency Exchange BitMEX Fined $100 Million for Violating Bank Secrecy Act (Jan. 15, 2025), https://www.justice.gov/usao-sdny/pr/global-cryptocurrency-exchange-bitmex-fined-100-million-violating-bank-secrecy-act; *FinCEN Announces $100 Million Enforcement Action Against Unregistered Futures Commission Merchant BitMEX for Willful Violations of the Bank Secrecy Act*, FIN. CRIMES ENF'T NETWORK (Aug. 10, 2021), https://www.fincen.gov/news/news-releases/fincen-announces-100-million-enforcement-action-against-unregistered-futures; Press Release, U.S. Dep't of Just., Binance and CEO Plead Guilty to Federal Charges in $4 Billion Resolution (Nov. 21, 2023), https://www.justice.gov/archives/opa/pr/binance-and-ceo-plead-guilty-federal-charges-4b-resolution.

224. Alamsyah, *supra* note 215, at 13–14.

225. *Automated Market Makers*, XRP LEDGER (Dec. 31, 2024), https://xrpl.org/docs/concepts/tokens/decentralized-exchange/automated-market-makers.

occur within those pools.[226] Instead of trading directly with another individual, traders interact with these liquidity pools.[227] The AMM algorithm determines asset prices based on the token ratio in the pool, while smart contracts manage the pools and transactions autonomously, eliminating the need for a central authority.[228]

Despite the involvement of various parties—developers, token holders with voting rights, liquidity providers, and traders—none of them can or should serve as a traditional centralized entity or individual responsible for compliance. First, developers are not well-suited to comply with AML requirements, especially when they relinquish control by transferring governance to the community or a DAO after the platform's launch. It would be unreasonable to hold them accountable for compliance when they no longer manage the day-to-day operations or decision-making of the DEX. Moreover, money laundering typically occurs during ongoing transactions, not at the initial setup stage, so there is no direct link between such activities and the developers' original work.

Second, token holders are not a good fit for compliance either. They participate in governance by voting on key protocol changes, such as fee adjustments or feature upgrades. They form a distributed group of individuals and entities, often spread across different jurisdictions. Given their anonymous or pseudonymous nature, it is difficult to trace who is participating in governance. Furthermore, since governance decisions are made collectively and on a voluntary basis, some token holders may choose to vote while others may not. Even those who do vote might only do so once and disappear, unlike a corporate board that makes regular decisions. Their votes may have little connection to any money laundering activities occurring on the DEX, so it is impractical to hold any individual or entity accountable for compliance-related decisions.

Third, asking liquidity providers, traders, or users to bear compliance responsibilities would be unreasonable. Liquidity providers contribute assets to liquidity pools but have no control over the platform's governance or operations beyond their individual contributions. They are participants rather than managers, and their involvement is limited to earning transaction fees rather than overseeing compliance. Similarly, traders are users who interact with the platform but have no influence over its governance or management. They function as customers rather than stakeholders responsible for the exchange's operations. Holding them accountable for compliance would be unfair—just as it would be unreasonable to hold stock traders on the NASDAQ responsible for NASDAQ's compliance obligations. It is the entity operating the platform that should bear the compliance burden, not the users.

226. *Id.*
227. *Id.*
228. *Id.*

As a result, such decentralized arrangements fundamentally challenge the AML framework, which depends on clearly identifiable intermediaries to bear compliance obligations. The AML laws continue to operate within a paradigm of intermediary trust—an architecture designed for a world of banks and similar centralized financial institutions. This architecture is fundamentally incompatible with the philosophy that shaped the emergence of the crypto industry—one grounded in disintermediation and decentralization. This structural mismatch underscores a deeper tension: efforts to graft traditional compliance obligations onto decentralized networks risk undermining both the effectiveness of AML regulation and the broader trust reform the crypto industry seeks to achieve.

IV.
DECENTRALIZED DIGITAL INFRASTRUCTURE

As concluded in Part III, existing frameworks' heavy reliance on centralized intermediaries for compliance is a fundamental reason for the failure of regulation and enforcement against money laundering in the crypto space. This Part explores whether the intermediary-based approach remains applicable in a limited scope, how to gradually transition away from it in areas where it proves ineffective, and how to establish a better approach.

Section IV.A demystifies the dynamics of decentralization, arguing that it is not a binary concept but rather exists on a spectrum. Analyzing decentralization across three key dimensions—development, governance, and operation—it finds that some projects remain highly centralized, only one has achieved maximum decentralization, and many fall somewhere in between, blending elements of both centralization and decentralization to varying degrees. Section IV.B proposes a decentralized digital infrastructure to enable the latter two categories to combat money laundering in a somewhat decentralized environment, while arguing that an intermediary-based approach remains applicable to the first category—at least in the near future—but will require necessary adaptations over time.

A. Decentralization as a Spectrum

There is no universally agreed-upon definition of decentralization, and sometimes the term is misused.[229] Lawmakers, governments, think tanks, scholars, and the crypto industry each have their own interpretations.

In a proposed congressional bill, a blockchain system is considered decentralized if, over a 12-month period, no single person or entity has had control over its operation or restriction of its use, no single entity holds or

229. U.S. DEP'T OF THE TREASURY, *supra* note 108; Rebecca Rettig, Michael Mosier & Katja Gilman, *Genuine DeFi as Critical Infrastructure: A Conceptual Framework for Combating Illicit Finance Activity in Decentralized Finance* 13 (Feb. 2, 2024); OECD, *supra* note 220, at 9.

controls more than 20% of its digital assets, changes to the system's code must address maintenance or be agreed upon by decentralized governance, the assets have not been marketed as investments, and all new digital assets are distributed to end users.[230] The Department of the Treasury broadly refers to decentralized systems as "virtual asset protocols and services that purport to allow for some form of automated peer-to-peer transactions, often through the use of self-executing code known as 'smart contracts' based on blockchain technology."[231]

The OECD lists decentralized features such as a "non-custodial nature (i.e., no central authority or other intermediary gets access or control over participants' digital assets), community-driven governance (relying on participants for decision-making) and composability (i.e., components of DeFi are pieced together to create new products)."[232] Other scholars highlight that power in decentralized blockchain systems resides in specific and changing relationships among various actors rather than in fixed identities or roles.[233] According to law professor Christina Skinner, blockchain technology is decentralized when it operates without a central authority and manages the system through a "protocol"—a bundle of smart contracts that create and manage the coins, removing the need for intermediaries typically required in traditional financial systems.[234]

Some definitions narrow the scope to focus solely on decentralization in finance, thereby adopting the term DeFi. The Financial Stability Board defines DeFi as "an umbrella term commonly used to describe a variety of services in crypto asset markets that aim to replicate some functions of the traditional financial system while seemingly disintermediating their provision and decentralizing their governance."[235] Attorney Rebecca Rettig and others define "Genuine DeFi"[236] as a system of open-source software where users conduct financial transactions independently without intermediaries, maintain control over their assets via private keys, and complete all transactions on a permissionless blockchain network.[237] The CFTC has a functional definition of

230. Financial Innovation and Technology for the 21st Century Act, H.R. 4763, 118th Cong. (2023–2024), https://www.congress.gov/bill/118th-congress/house-bill/4763/text.

231. U.S. DEP'T OF THE TREASURY, *supra* note 108, at 1.

232. OECD, *supra* note 220, at 9.

233. Andrej Zwitter & Jilles Hazenberg, *Decentralized Network Governance: Blockchain Technology and the Future of Regulation*, 3 FRONTIERS IN BLOCKCHAIN art. 12 (2020).

234. Christina Parajon Skinner, *Coins, Cross-Border Payments, and Anti-Money Laundering Law*, 60 HARV. J. ON LEGIS. 302, 332 (2023).

235. THE FINANCIAL STABILITY BOARD, THE FINANCIAL STABILITY RISKS OF DECENTRALISED FINANCE 1 (Feb. 16, 2023).

236. Katrin Schular, Ann Sofie Cloots & Fabian Schar, *On Defi and On-Chain CeFi: How (Not) to Regulate Decentralized Finance*, 10 J. FIN. REGUL. 213, 214 (2024) (introducing "Genuine DeFi").

237. Rettig et al., *supra* note 229, at 13–14; *see also* Linda Jeng, Christian Rome Lansang, Kristy Lam, Sean Lee & Tyler Peltekci, *Key Elements of an Effective DeFi Framework*, CRYPTO COUNCIL FOR INNOVATION 4 (Oct. 5, 2023) (similarly defining DeFi as "the ecosystem of applications and protocols enabled by blockchain technology to provide digital and open access to financial services without a single intermediary or small group of intermediaries controlling the system offering the

DeFi: "enterprises, projects, and ecosystems . . . characterized by highly automated financial networks that have no single point of failure, do not rely on a single source of information, and are not governed by a central authority that is capable of altering or censoring this information in order to perform tasks central to delivery of one or more financial services."[238]

None of these definitions are perfect. Some definitions emphasize the technical structure of decentralization, while others highlight the features that emerge from this technical framework. Certain interpretations focus on the goals or functions of decentralization. While these descriptions accurately capture specific aspects of decentralization, they fail to provide a holistic understanding. Others narrowly concentrate on the financial dimensions of decentralization, neglecting its potential to extend beyond finance into other sectors and serve broader societal and organizational objectives.

Inspired by the CFTC's dimensional analysis of DeFi,[239] this Article broadens the scope and examines decentralization across three dimensions: development, governance, and operation. First, development refers to who builds the project, which addresses the relationship between developers and projects.[240] Viewed on a spectrum, a small, close-knit team working together at a single firm to build proprietary software represents a high degree of centralized development.[241] In contrast, when a large number of otherwise independent developers collaborate on a project using open-source software and each focuses on different assignments, this arrangement reflects a high degree of decentralized development.

Second, governance refers to control or influence over a project after deployment. Projects that rely on automated decision-making processes and self-executing software exhibit a higher degree of decentralization.[242] In contrast, when human agents retain residual discretion over key decisions and operations,

financial service."); Iwa Salami, *Challenges and Approaches to Regulating Decentralized Finance*, 115 AM. J. INT'L L. 425, 425 (2021) (claiming that DeFi aims to create an open-source, permissionless, and transparent financial system that operates without any central authority.); Raphael Auer, Bernhard Haslhofer, Stefan Kitzler, Pietro Saggese & Fridhelm Victor, *The Technology of Decentralized Finance (DeFi)* (Bank for Int'l Settlements, Working Paper No. 1066, Jan. 2023) (describing Defi as "a competitive, contestable, composable and non-custodial financial ecosystem built on technology that does not require a central organization to operation and that has no safety net.").

238. COMMODITY FUTURES TRADING COMM'N [CFTC], REPORT OF THE SUBCOMM. ON DIGIT. ASSETS & BLOCKCHAIN TECH.: DECENTRALIZED FINANCE 20 (Jan. 8, 2024), https://www.cftc.gov/media/10106/TAC_DeFiReport010824/download.

239. *Id.* at 20–24. The CFTC focuses on decentralization specifically within the financial sector, addressing DeFi from five functional dimensions: access, development, governance, balance sheet, and operation. In addition to these functional aspects, the CFTC also considers key technological dimensions, including open-source software, smart contracts, distributed ledgers, decentralized applications (DApps), decentralized autonomous organizations (DAOs), and oracles.

240. *Id.* at 21.

241. *Id.*

242. *Id.* at 22.

decentralization diminishes.[243] Such residual rights may include the authority to determine products, services, or the underlying technical architecture, as well as the authority to override automated decisions or intervene during system malfunctions.[244] Taking governance of a DEX as an example, these rights may rest with a small group of core developers or be widely dispersed among token holders—often passive participants—who vote on matters such as protocol governance, financial management, community initiatives, and risk oversight.[245]

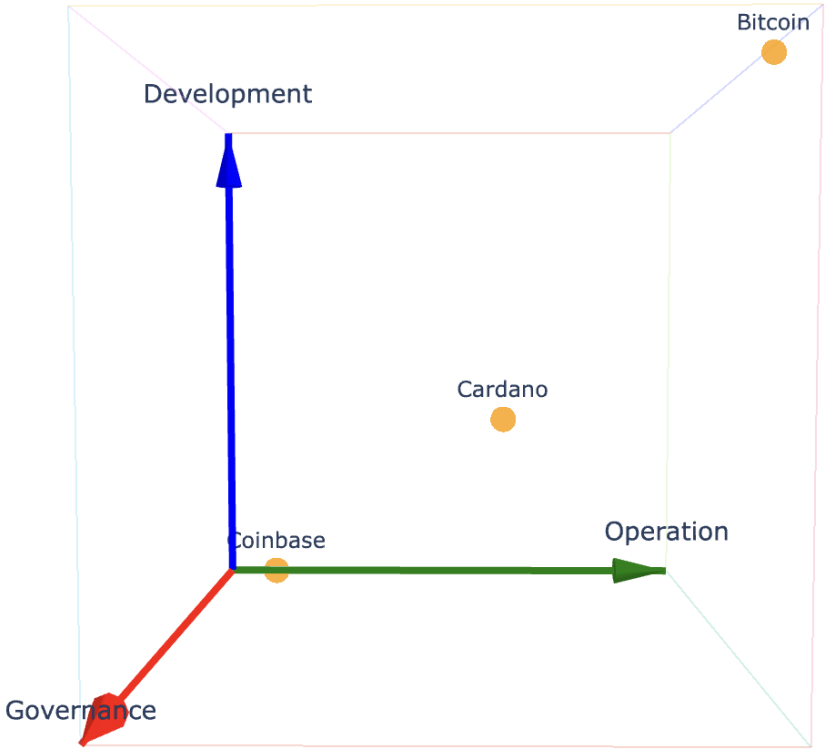
Third, operation refers to whether the project outsources critical functions or processes to third parties.[246] These functions and processes can theoretically include: software design, maintenance, and upgrades; transaction processing, validation, and recordkeeping; cybersecurity; and regulatory compliance.[247] Outsourcing these functions or processes to a single vendor would represent a relatively low degree of operational decentralization, whereas outsourcing many functions or processes to various vendors would represent a relatively high degree of operational decentralization.[248]

Examining blockchain projects through these three dimensions reveals that decentralization is not a binary concept but rather exists on a spectrum.[249] At one end are systems that, despite often being labeled as "decentralized" or "DeFi," remain highly centralized. For example, Coinbase is highly centralized across governance, development, and operations: it is managed by a corporate board and executive team, its codebase and infrastructure are proprietary, and all custodial and compliance functions are controlled internally.[250] At the other end of the spectrum are systems that achieve maximum decentralization, with the Bitcoin network standing out as perhaps the only example. Most so-called decentralized projects occupy a middle ground on this spectrum, blending

243. *Id.*
244. *Id.*
245. *Id.*
246. *Id.*
247. *Id.*
248. *Id.*
249. *Id.*; *see also* Agata Ferreira, *Decentralized Finance (DeFi): The Ultimate Regulatory Frontier?*, 19 CAP. MKTS. L.J. 242, 255 (2024); Zwitter, *supra* note 233, at 7 (describing power as fluid); Cheryl Saunders, *Constitutional Design: Options for Decentralizing Power*, *Policy Paper No. 2*, CONST. TRANSFORMATION NETWORK (Mar. 2018), https://law.unimelb.edu.au/__data/assets/pdf_file/0006/2698854/CTN-Policy-Paper-2-Decentralisation-Approaches-Feb-18.pdf; Kai Wang, *Regulating Cryptocurrency Non-Custodial Service Providers Through the Bank Secrecy Act*, 4 U. CHI. BUS. L. REV. 341 (2025).
250. *See* Coinbase Global, Inc., Registration Statement (Form S-1) (Feb. 25, 2021), https://www.sec.gov/Archives/edgar/data/1679788/000162828021003168/coinbaseglobalincs-1.htm (noting that Coinbase's trading, custody, and wallet infrastructures are proprietary, internally managed, and protected as trade secrets); Coinbase Global, Inc., Annual Report (Form 10-K) (Feb. 15, 2024) (describing Coinbase as a publicly listed Delaware corporation governed by a board of directors and executive officers that oversee operations, strategy, and risk management); Angela Walch, *Deconstructing 'Decentralization': Exploring the Core Claim of Crypto Systems*, *in* CRYPTOASSETS: LEGAL, REGULATORY, AND MONETARY PERSPECTIVES 39, 41–42 (Oxford Univ. Press 2019) (using Coinbase as an example of centralization and contrasting it with decentralized protocols).

elements of centralization and decentralization in varying degrees. Cardano is a good example of a semi-decentralized system: its consensus and network operations are distributed among numerous stake pool operators, yet its governance and core development remain largely directed by a few founding entities, including the Cardano Foundation, IOHK, and Emurgo.[251]

Figure 2: Three Dimensions for Analyzing Decentralization.



Considering these dimensions together provides a holistic framework for understanding how decentralization is conceived, implemented, and sustained across the crypto ecosystem. This multidimensional approach responds to a growing problem in both scholarship and industry discourse—the tendency to invoke decentralization as a marketing trope, treating any project built on

251. ORCADA.IO, https://orcada.io/resources (last visited Nov. 8, 2025) (stating that thousands of people's computers (nodes) cooperate to agree if a transaction is valid therefore Cardano is decentralized in this sense); *Cryptocurrencies and Blockchain*, TAX3 COMM. 41, https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf (last visited Nov. 8, 2025) ("The Cardano project currently has three main contributors that each have separate roles: the Cardano foundation, based in Switzerland, which aims to standardise, protect and promote the Cardano technology and eco-system; IOHK, a blockchain engineering company responsible for building the Cardano blockchain; and Emurgo, an entity responsible for the fostering of commercial applications being built upon the Cardano ecosystem.").

distributed ledgers as inherently decentralized—and instead exposes the structural and institutional forces that shape both the premise and the limits of decentralization in theory and in practice. Given this dynamic of decentralization, distinct regulatory approaches should be tailored to address money laundering concerns, as discussed in the following Section.

B. Toward Decentralized Digital Infrastructure

Addressing money laundering in the crypto space requires both a clear understanding of the decentralization spectrum and the development of short- and long-term solutions. For decentralized and semi-decentralized projects, regulators and law enforcement should move away from the intermediary-based approach. This Section proposes a decentralized digital infrastructure that leverages blockchain intelligence and a robust digital identity system to ensure effective investigation, tracing, and seizure of illicit proceeds. For centralized projects, the existing intermediary-based approach can continue but blockchain intelligence and digital identity solutions should gradually be integrated at both the investigation and enforcement stages to ensure alignment with modern AML needs.

The concept of decentralized digital infrastructure echoes the core ethos of the crypto industry—distributing power, trust, and responsibility across a network rather than concentrating them in a single authority. In the AML context, it implies that combating money laundering should not rest solely with a centralized entity, such as law enforcement or a financial intelligence unit. Instead, effective prevention and enforcement should arise from distributed collaboration among diverse stakeholders in the crypto ecosystem, including regulators, law enforcement agencies, product and service providers, developers, analytics firms and even users themselves. In this sense, decentralization becomes not merely a design principle but a regulatory strategy—one that shifts the paradigm from centralized oversight to collective responsibility.

1. Blockchain Intelligence

Blockchain intelligence comprises three key components: what, who and how. The "what" refers to the digital infrastructure—including the blockchain's data architecture and the AI models built on topic of it for analytics purposes—that form the foundation of this approach. The "who" addresses the allocation of responsibility, identifying which individuals or organizations in the decentralized and semi-decentralized systems should leverage the infrastructure and defining their specific roles. The "how" focuses on the implementation process, detailing the practical steps and oversight measures to operationalize blockchain intelligence.

a) What

First and foremost, on-chain data serves as the foundation of the digital infrastructure. On the blockchain, all transaction data is publicly recorded and timestamped, creating a comprehensive and auditable trail of activity.[252] The transparent and cryptographic nature of blockchain provides a single source of truth.[253] Importantly, blockchain allows everyone, including law enforcement agencies and industry participants, to access data instantly.[254] The combination of comprehensive, auditable data and free, real-time accessibility lays a robust foundation for further study, analysis, and actionable insights.

One argument is that even if on-chain transaction data is transparent, off-chain transactions will again become obscure, thereby undermining the effectiveness of blockchain data for money laundering insights.[255] This argument is flawed, as the term "off-chain" transaction is a misnomer.[256] Off-chain transactions typically refer to activities that occur outside of the blockchain.[257] Since these transactions are not recorded on the blockchain, they of course lack the transparency and traceability that on-chain transactions offer. Criminals

252. NAKAMOTO, *supra* note 43, at 4.

253. John Harms, *How Your Agency Can Use Data, Analytics, and AI to Modernize and Improve Investigations*, QUANTEXA 14 (2024).

254. *How Blockchain Data Can Be Leveraged by Law Enforcement Agencies*, MERKLE SCI., https://www.merklescience.com/how-blockchain-data-can-be-leveraged-by-law-enforcement-agencies (last visited Feb. 5, 2025).

255. *See* CHAINALYSIS TEAM, MONEY LAUNDERING AND CRYPTOCURRENCY: TRENDS AND NEW TECHNIQUES FOR DETECTION AND INVESTIGATION 3 (2024); Emily Ekshian, *On-Chain vs. Off-Chain Transaction*s, CRYPTO COUNCIL FOR INNOVATION (Aug. 5, 2025), https://cryptoforinnovation.org/on-chain-vs-off-chain-transactions; Syedur Rahman, *The Scale of Crypto's Involvement in Money Laundering*, RAHMAN RAVELLI (Feb. 16, 2024), https://www.rahmanravelli.co.uk/expertise/cryptocurrency/articles/the-scale-of-crypto-s-involvement-in-money-laundering/.

256. *Crypto Crime in Context Part II: Examining Approaches to Combat Illicit Activity: Hearing Before the Subcomm. on Digit. Assets, Fin. Tech., & Inclusion*, 118th Cong. (2023–24) (statement of Grant Rabenn, Director, Financial Crimes Legal, Coinbase) (Feb. 15, 2024), https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=409142; *Crime in Context: Breaking Down Illicit Activity in Digital Assets: Hearing Before the Subcomm. on Digit. Assets, Fin. Tech., & Inclusion*, 118th Cong. (2023–24) (statement of Jonathan Levin, Co-Founder & Chief Strategy Officer, Chainalysis) (Nov. 15, 2023), https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=409028.

257. A.B.A., DIGITAL AND DIGITIZED ASSETS: FEDERAL AND STATE JURISDICTIONAL ISSUES 34 (2019), https://marketingstorageragrs.blob.core.windows.net/webfiles/McLaughlin_50_State_virtual_currency_regulation_survey.pdf; *On-Chain vs. Off-Chain Cryptocurrency Transactions: What Is the Difference?*, COINBASE, https://www.coinbase.com/learn/tips-and-tutorials/onchain-vs-offchain-cryptocurrency-transactions-what-is-the-difference (last visited Feb. 6, 2025); The Investopedia Team, *Off-Chain Transactions: Benefits, Drawbacks, and Comparisons to On-Chain*, INVESTOPEDIA (Aug. 24, 2024), https://www.investopedia.com/terms/o/offchain-transactions-cryptocurrency.asp#:~:text=Off%2Dchain%20transactions%20refer%20to,contrasted%20with%20on%2Dchain%20transactions.

utilizing "off-chain" transactions for money laundering are merely restoring to traditional money laundering methods.[258]

Once comprehensive, transparent, and accurate transaction data is available,[259] another crucial part of the digital infrastructure involves utilizing advanced AI models to analyze this data. AI models can contribute by identifying unusual transaction patterns, analyzing user behaviors, uncovering hidden relationships, and providing real-time monitoring with instant alerts for suspicious activities.[260]

Many blockchain intelligence firms, such as TRM Labs, Chainanlysis, and Elliptic, are actively leveraging advanced AI models and analytics tools to combat money laundering in the crypto space.[261] For instance, Elliptic has developed deep learning models that uncover money laundering patterns and detect unknown illicit wallets. The data set labeled transactions as licit or illicit through a "heuristics-based reasoning process."[262] More specifically, accounts that use the same address multiple times and have more inputs are linked to legitimate activity because these repeated transactions make it easier to identify the entity associated with them.[263] Similarly, an account that gathers funds from

258. *Crypto Crime in Context Part II: Examining Approaches to Combat Illicit Activity: Hearing Before the Subcomm. on Digit. Assets, Fin. Tech., & Inclusion*, 118th Cong. (2023–24) (statement of Michael Mosier, Co-Founder and Partner, Arktouros) (Feb. 15, 2024), https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=409142.

259. *See* JEROME BRYSSINCK & KARL KEINZ KRUG, QUANTEXA FINANCIAL INVESTIGATION SOLUTION FOR MICROSOFT AZURE: HOW TO MANAGE ANALYTICS, PREVENTION, AND DETECTION FOR FINANCIAL CRIME 9–10 (2023).

260. *Id*. at 13–16; HARMS, *supra* note 253, at 12; QUANTEXA SYNEO, HOW TO BETTER UNDERSTAND YOUR CUSTOMERS USING CONTEXT: A GUIDE TO TRANSFORMING YOUR KYC PROCESSES ACROSS THE CUSTOMER LIFECYLE 10–11, 16 (2022). For instance, Quantexa's Contextual Decision Intelligence (CDI) uses AI and machine-learning to help traditional financial institutions in their KYC/AML detection and compliance efforts. *Id.* at 11. CDI allows organization to evaluate each customer and their financial crime risk throughout the customer lifecycle. *Id.* It connects multiple internal and external datasets to provide a single view of customers, showing relationships between people, organizations, and places by applying context-aware reasoning and AI. *Id.* at 12. Rather than focus on static variables, like geography, CDI uses dynamic variables like observed behavior to get a more complete understanding of customer behavior. *Id.* at 9. In place of manual processes, AI is used to streamline data organization and accurately create connections among a customer's network. *Id.*

261. *See* Mark Weber, Giacomo Domeniconi, Jie Chen, Daniel Karl I. Weidele, Claudio Bellei, Tom Robinson & Charles E. Leiserson, *Anti-Money Laundering in Bitcoin: Experimenting with Graph and Convolution Networks for Financial Forensics*, KDD '19 WORKSHOP ON ANOMALY DETECTION IN FIN. (Aug. 2019); Claudio Bellei, Muhua Xu, Ross Phillips, Tom Robinson, Mark Weber, Tim Kaler, Charles E. Leiserson, Arvind & Jie Chen, *The Shape of Money Laundering: Subgraph Representation Learning on the Blockchain with the Elliptic2 Dataset*, ARXIV (2024), https://arxiv.org/pdf/2404.19109; Chainalysis Team, *Introduction Cross-Chain Investigation in Reactor: Enhancing Crypto Tracing*, *Company News*, CHAINALYSIS (Mar. 9, 2022), https://www.chainalysis.com/blog/cross-chain-investigations/; *Detecting the Invisible: The Power of TRM Labs' Signatures™ in Blockchain Investigations*, *TRM Insights: Product Updates*, TRM LABS (May 16, 2024), https://www.trmlabs.com/post/detecting-the-invisible-the-power-of-trm-labs-signatures-tm-in-blockchain-investigations.

262. Weber et al., *supra* note 261.

263. *Id.*

multiple addresses into a single transaction, which makes it harder to maintain user anonymity, is likely to belong to a legitimate exchange.[264] Conversely, accounts that prefer transactions with fewer inputs make it harder to trace identities, which means they are more likely to be used for illicit activities.[265]

Another example is Elliptic's use of "subgraph representation learning" to analyze millions of cryptocurrency transactions, building on its heuristics-based reasoning process.[266] Instead of tracking specific illicit wallets, this method identifies broader networks based on transaction subgraphs.[267] Subgraph representation learning analyzes local structures within complex networks, enabling a machine learning model—developed in partnership with IBM—to detect transaction subgraphs indicative of laundered bitcoin rather than merely flagging transactions by known illicit actors.[268] This study identified 52 suspicious subgraphs, 14 of which were linked to money laundering cases.[269] This approach provides a more comprehensive view of transaction patterns, moving beyond isolated on-chain activities of individual wallets. Notably, the model identified illicit activity based purely on on-chain patterns, which previously required off-chain data, such as funds entering a regulated exchange.[270]

b) Who

The second component of blockchain intelligence concerns who should assume responsibility for implementing AML measures in decentralized or semi-decentralized systems. In short, responsibility should be distributed across three groups: (1) regulators and law enforcement agencies, (2) individuals or groups with influence over semi-decentralized projects, and (3) developers and technical contributors building and maintaining the protocols.

Regulators and law enforcement agencies remain critical actors in AML enforcement but must adapt their roles to decentralized contexts. Regulators set the legal parameters and compliance expectations for the industry and should design rules that encourage the responsible use of blockchain analytics tools to improve transparency and oversight. Law enforcement agencies translate this regulatory framework into practice by detecting, investigating, and deterring money laundering, ensuring that enforcement mechanism remain effective even in a more decentralized environment.

Individuals or groups with influence—such as foundations or protocol governance teams—occupy a position between centralized and decentralized

264. *Id.*
265. *Id.*
266. Bellei et al., *supra* note 261.
267. *Id.*
268. *Id.*
269. *Id.*
270. *Id.*

systems. They possess both the technical capacity and institutional authority to implement compliance mechanisms within their networks. For instance, the Tron blockchain is somewhat decentralized, but the Tron foundation, based in Singapore, plays a vital role in ecosystem development and decision-making.[271] Similarly, Cardano Foundation and Solana Foundation retain distinct strategic and technical roles and financial oversight for their Cardano and Solana blockchains.[272]

Developers and technical contributors shape the technological foundations of blockchain ecosystem. Their designs and coding decisions determine how traceability, accountability, and monitoring can occur within decentralized systems, positioning them as key actors in embedding compliance into the system's very architecture.

c) How

The third component concerns how these groups can implement their respective responsibilities in a somewhat decentralized environment. The methods differ depending on the actor and the degrees of decentralization.

Regulators should issue interpretive guidance, technical standards, or rules that explicitly recognize blockchain analytics as a legitimate compliance tool. They can promote interoperability by requiring exchanges and service providers to maintain data formats compatible with analytic technologies and to share relevant information with supervisory bodies, subject to appropriate privacy safeguards. Law enforcement agencies can complement these initiatives by developing internal expertise, forming joint task forces with analytics firms, and coordinating cross-border investigations to operationalize the intelligence gathered under these regulatory frameworks.

Individuals or groups with influence over semi-decentralized projects can operationalize compliance by embedding monitoring and risk management within governance structures. These actors may procure blockchain intelligence services, build internal analytic tools, or implement automated protocols that flag and review suspicious transactions. For example, while the Tron network operates with a degree of decentralization, the TRON Foundation maintains decision-making power to procure and deploy blockchain analytics tools to proactively identify and mitigate suspicious transactions.[273]

---

271. *See* Xangle, *What Is Tron?*, XANGLE PORTAL (Aug. 27, 2021), https://xangle.io/en/research/detail/335.

272. *See Cardano Governance*, CARDANO FOUND., https://cardanofoundation.org/governance (last visited Oct. 27, 2025); *DAOs and Governance*, SOLANA, https://solana.com/developers/dao (last visited Oct. 27, 2025).

273. *TRON and Google Cloud: A Dynamic Partnership for Blockchain Data on Big Query*, TRON DAO (Sep. 23, 2023), https://trondao.org/blog/2023/09/25/tron-and-google-cloud-a-dynamic-partnership-for-blockchain-data-on-big-query/ ("The recent inclusion of TRON into Google Cloud's BigQuery public datasets marks a pivotal point . . . . With the vast amount of data TRON processes, its addition brings a wealth of information, enabling users to analyze on-chain transaction histories

At the more decentralized end of the spectrum, developers and early-stage technical contributors should assume greater responsibility for embedding compliance and accountability mechanisms into a system's design and protocol architecture. Preventive features—such as smart contracts that temporarily pause questionable transactions, trigger alerts, or grant conditional data access to authorized investigative entities—can enhance transparency without centralizing control. In fully decentralized networks, governance mechanisms may allow token holders to vote on allocating treasury resources to fund blockchain analytics tools or independent audits, ensuring that AML measures arise from decentralized consensus rather than top-down enforcement.

d) Benefits

One of the greatest advantages of blockchain intelligence is that blockchain's inherent transparency enables faster and more effective identification of suspicious activities. This transparency also facilitates targeted and coordinated responses to combat money laundering.[274] Unlike traditional banking systems, where only centralized intermediaries such as banks have direct access to their consumer data and investigations require lengthy bureaucratic processes to obtain records, blockchain provides everyone with instantaneous access to transactional information.[275]

Moreover, AI models can analyze blockchain data in real time, delivering timely insights that enhance the efficiency and accuracy of detecting and addressing money laundering. This arrangement overcomes a critical limitation of existing rule-based AML systems, which rely on predefined thresholds and delayed reporting, often resulting in high false positive rates and delayed enforcement actions. By embedding AML safeguards at the protocol level, enforcement becomes proactive rather than reactive. Automated AML mechanisms integrated directly into blockchain infrastructure enable the identification and prevention of illicit activities before they escalate. This not only reduces the compliance burden on entities or individuals manually monitoring transactions but also fosters a more self-regulating ecosystem.

Another key benefit of blockchain intelligence is its alignment with blockchain's "trustless" philosophy and somewhat decentralized nature. Instead of relying on an intermediary model that identifies a single trusted entity to

seamlessly."); TRON DAO, https://trondao.org ("In December 2021, TRON became TRON DAO, a community-governed, decentralized, autonomous organization.") (last visited Nov. 8, 2025).

274. *See Crypto Crime in Context Part II: Examining Approaches to Combat Illicit Activity: Hearing Before the H. Comm. on Fin. Servs., Subcomm on Digital Assets, Fin. Tech. & Inclusion*, 118th Cong. (2023–24), https://www.congress.gov/118/meeting/house/116861/witnesses/HHRG-118-BA21-Wstate-RedbordA-20240215.pdf (written testimony of Ari Redboard, at 3).

275. *See Crypto Crime in Context Part II: Examining Approaches to Combat Illicit Activity: Hearing Before the H. Comm. on Fin. Servs., Subcomm on Digital Assets, Fin. Tech. & Inclusion*, 118th Cong. (2023–24) https://docs.house.gov/meetings/BA/BA21/20240215/116861/HHRG-118-BA21-Wstate-RabennG-20240215.pdf (written testimony of Grant Rabenn, at 3).

manually submit reports to law enforcement, this method leverages readily available data and intelligence. It distributes responsibilities more evenly among stakeholders, alleviating the burden on a single entity. This distributed approach also enhances the scalability of AML measures in a decentralized environment.

By integrating responsibilities into governance mechanisms, blockchain intelligence empowers token holders to actively participate in AML efforts, reinforcing the decentralized ethos. It shifts the paradigm from centralized, intermediary-based compliance to a collaborative, data-driven framework that enhances transparency and accountability without compromising the principles of decentralization.

e) Limitations

The adoption of blockchain intelligence also comes with technical, governance, and operational challenges or limitations. One major technical challenge is that criminals deliberately obfuscate the movement of illicit funds using methods such as mixers, chain hopping, and asset hopping, which significantly complicate investigation and tracing efforts.[276] By 2022, Elliptic had identified over $4.1 billion in illicit or high-risk cryptocurrency laundered through these techniques.[277] Such activities are facilitated by DEXs, cross-chain bridges, and coin-swap services.[278]

Fortunately, some commercial tools have developed capabilities to trace transactions through mixers, across multiple blockchains, and between different crypto assets. For example, Elliptic Lens, a wallet screening solution, helps businesses detect whether their customers intend to withdraw funds to blacklisted mixing services, enabling them to block such transactions before they occur.[279] Additionally, Elliptic's Holistic Screening offers multi-asset screening, cross-asset tracing, and cross-chain tracking.[280] Similarly, Chainalysis Reactor can trace transactions even when bad actors use mixers, privacy coins, or cross-

276. ELLIPTIC, FOLLOWING THE MONEY IN A CROSS-CHAIN WORLD: A LAW ENFORCEMENT SUPPLEMENT TO ELLIPTIC'S CROSS-CHAIN CRIME REPORT ON THE FUTURE OF CRYPTO CRIME AND MONEY LAUNDERING 2 (2022).

277. *Id.*

278. *Id.*

279. David Carlisle, *Crypto Mixers and Privacy Protocols: The Sanctions Compliance Implications*, ELLIPTIC (Mar. 1, 2023), https://www.elliptic.co/blog/analysis/crypto-mixers-and-privacy-protocols-the-sanctions-compliance-implications. Elliptic Navigator can identify when users indirectly interreacted with mixers by leveraging their AI and machine-learning capabilities. Elliptic Investigator, a multi-asset crypto forensics tool, helps investigators visualize complex transactions involving mixers. For more information, see *Crypto Transaction Monitoring with Elliptic Navigator*, *Platform*, ELLIPTIC, https://www.elliptic.co/platform/navigator (last visited Feb. 6, 2025); *Blockchain Forensics with Elliptic Investigator*, ELLIPTIC, https://www.elliptic.co/platform/investigator (last visited Feb. 6, 2025).

280. *Next-Generation Blockchain Analytics for Efficient Cross-Chain Compliance*, ELLIPTIC (Aug. 10, 2022), https://www.elliptic.co/blog/next-generation-blockchain-analytics-for-efficient-cross-chain-compliance.

chain swaps to obfuscate their activities.[281] TRM Labs' Signature can flag transactions associated with high-risk behavior such as the use of mixers, privacy wallets, cross-chain swaps and bridging mechanisms.[282]

The next challenge is the high cost of blockchain intelligence tools and services, which limits access for law enforcement and industry participants. With limited resources and knowledge gaps, they often rely on firms like TRM Labs, whose services can cost between €33,272 and €475,795 annually.[283] U.S. law enforcement agencies have spent millions on Chainalysis and Elliptic tools and services,[284] which can be a heavy burden for smaller jurisdictions with limited resources. Costs extend beyond tracing tools to attribution databases containing critical information on money laundering patterns, illicit funds, and addresses.[285] Companies often offer tiered pricing, charging higher fees for more

281. CHAINALYSIS TEAM, *supra* note 255.

282. Signatures leverage advanced machine learning to automatically uncover suspicious patterns across multiple transactions. They can help law enforcement detect and track complex transactions through mixers and across chains. TRM LABS, *supra* note 261; *Signatures®: Proactively Detect Suspicious Activity with Advanced Blockchain Pattern Recognition*, TRM LABS, https://www.trmlabs.com/blockchain-intelligence-platform/forensics/signatures#:~:text=Powered%20by%20advanced%20machine%20learning,investigative%20angle%20is%20left%20unconsidered (last visited Feb. 6, 2025).

283. TRM Labs posted some of its pricing data on the Digital Marketplace on GOV.UK Digital Marketplace, a searchable database that displays approved suppliers for public sector organization. For their "Cloud Software—Saas" license called "Forensics Premium," TRM Labs charges an annual fee of €33,272 per user. Alternatively, their "Cloud Software—API" named "BLOCKINT API" costs €41,591.66 annually. *TRM Forensics Premium*, *Lot 2: Cloud Software*, GOV.UK DIGIT. MARKETPLACE, https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/205548500859141 (last visited Feb. 6, 2025); *Pricing: TRM Forensics Premium*, TRM LABS, https://assets.applytosupply.digitalmarketplace.service.gov.uk/g-cloud-14/documents/721706/205548500859141-pricing-document-2024-05-02-1629.pdf (last visited Feb. 6, 2025). For their "Cloud Support Services—Training," TRM Labs charges an annual fee between €256,198 and €475,795 for "Augmented Investigative Support" or an hourly rate ranging from €292 to €375 for "cryptocurrency investigations." *Pricing: TRM Professional Services*, TRM LABS, https://assets.applytosupply.digitalmarketplace.service.gov.uk/g-cloud-14/documents/721706/375422714108266-pricing-document-2024-05-02-1621.pdf (last visited Feb. 6, 2025).

284. Blockchain analytic firms have various pricing models that reflect their unique products and business plans. Pricing depends on contract duration, subscription levels, and other factors. For example, Chainalysis has a silver, gold, and platinum risk and compliance solutions. *Chainalysis Product Guide*, CHAINALYSIS, https://www.chainalysis.com/productguide/ (last visited Feb. 6, 2025). In 2020, the Treasury Department awarded Chainalysis a $1.3 million contract, of which $625,000 was paid. *Treasury Contract Awarded to Chainalysis Inc.*, USA SPENDING, https://www.usaspending.gov/award/CONT_AWD_2032H820C00041_2050_-NONE-_-NONE- (last visited Feb. 6, 2025). In 2018, the DOJ awarded and paid Elliptic $75,000. *DOJ Contract Awarded to Elliptic Inc., USA Spending*, USA SPENDING, https://www.usaspending.gov/award/CONT_AWD_15F06719P0000313_1549_-NONE-_-NONE- (last visited Feb. 6, 2025).

285. *See* Thomas R. Alber, *Blockchain Tracing Software: Tools, Costs, Algorithms, and Alternatives for Investigators*, LINKEDIN (Sep. 27, 2024), https://www.linkedin.com/pulse/blockchain-tracing-software-tools-costs-algorithms-thomas-r-alber-05ejf/; *see also supra* notes 283–284.

comprehensive datasets.[286] Even if discovery and tracing efforts are successful, freezing and recovering illicit funds can incur further significant expenses.[287]

To address this challenge, the industry could establish a consortium dedicated to identifying suspicious addresses and funds and releasing the database to the public in a timely manner. The consortium could also provide seizure tools and strategies to support projects with limited resources in combating money laundering. Public-private partnerships could help establish such organizations as a public good. These partnerships could also play a role in educating law enforcement agencies, bridging knowledge gaps, and helping them digest, structure, and analyze vast amounts of data.

Another challenge for blockchain intelligence lies in motivating decentralized network participants—such as token holders, entities with influence over semi-decentralized projects, and developers—to assume responsibilities for AML efforts. While a network that facilitates peer-to-peer transactions with minimal criminal activity could theoretically attract more users, not all participants are willing to prioritize long-term benefits over short-term gains. Without clear incentives, they may lack the motivation to invest resources or effort into implementing AML measures.

To address this, future research and experimentation should focus on developing effective incentive structures. For example, introducing token-based incentives or rewards for participants who actively support and vote for AML measures could encourage broader engagement. Additionally, implementing staking mechanisms that reward participants for contributing to AML efforts can align their financial interests with the network's security and compliance goals. In the long run, as the industry matures, standardized practices or regulations may be introduced to complement early incentive-based strategies, fostering a more robust and compliant ecosystem.

2. Digital Identity

Addressing money laundering in the crypto space requires both short-term and long-term solutions. Blockchain intelligence represents a pragmatic and immediately actionable approach that can be adjusted and adopted. Digital identity, by contrast, offers a longer-term and more structural solution, one that complements blockchain intelligence but requires deeper institutional coordination and systemic reform to implement effectively.

Identity refers to the distinguishing character or personality of an individual, entity, or object.[288] It represents the holistic concept of "who" or "what" someone or something is. Identity can be recognized, verified, or

286. *Id.*
287. *Id.*
288. *Identity*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/identity (last visited Oct. 29, 2024).

differentiated through specific pieces of information known as identifiers.[289] Identity is multidimensional, which includes all aspects that make someone or something unique, while identifiers are functional, which provide a means to reference or authenticate someone or something. For example, someone's identity as a British citizen can be referenced or authenticated by their British passport (i.e, the identifier).

Digital identity is the representation of someone or something online.[290] Similar identifiers such as names, dates of birth, email addresses, passport numbers, and social security numbers can be used to authenticate individuals or entities, establish trust, and access services online.[291] Digital identity systems can be broadly classified into centralized and decentralized models—two distinct approaches to managing and verifying identities online.[292]

A centralized digital identity system is managed by a single authority or entity (e.g., government or company).[293] This authority or entity issues, manages, and verifies users' digital identities, and it controls a centralized database that stores identity-related data.[294] Examples include the Social Security Administration managing citizens' social security numbers, Meta managing users' social media accounts, and Bank of America managing users' account credentials.

A decentralized digital identity system distributes control across multiple entities or the users themselves, often leveraging technologies like blockchain.[295] Examples include self-sovereign identity (SSI) systems such as those using decentralized identifiers (DIDs) standards.[296] SSI is a decentralized digital identity model where individuals have full control over their own personal information and digital identifiers, with minimal reliance on centralized authorities, and can selectively disclose specific identifiers without revealing

289. *Identifier*, COLLINS ENGLISH DICTIONARY, https://www.collinsdictionary.com/us/dictionary/english/identifier#google_vignette (last visited Jan. 30, 2025).

290. Onfido, *What Is Digital Identity?*, ONFIDO BLOG (May 17, 2023), https://onfido.com/blog/digital-identity.

291. *Id.*

292. *See* Lauren Hendrickson, *Centralized vs. Decentralized Identity Management*, IDENTITY.COM (Oct. 7, 2024), https://www.identity.com/centralized-vs-decentralized-identity-management.

293. *Comparing Centralized Versus Decentralized Approaches for Privacy-Preserving Digital Identity*, IEEE DIGIT. PRIV., https://digitalprivacy.ieee.org/publications/topics/comparing-centralized-versus-decentralized-approaches-for-privacy-preserving-digital-identity (last visited Jan. 30, 2025).

294. *Id.*

295. *Digital Identity: A Beginner's Guide 2025*, DOCK (Dec. 2, 2025), https://www.dock.io/post/digital-identity.

296. *Id.* SSI enables users to selectively disclose specific identity information, enhancing privacy while reducing intermediary reliance. The core of these systems is DIDs, which are cryptographically verifiable identifiers. DIDs can be anchored on-chain to ensure tamper resistance which allows users to authenticate and verify identity credentials.

their entire identity.[297] The backbone of SSI is DIDs, which are unique, cryptographically secure identifiers that are independent of any central authority.[298]

This Article proposes the adoption of an SSI system to combat money laundering in the crypto space. The core idea is that anyone conducting transactions on the blockchain must first be vetted, creating a link between verified identities and blockchain transactions. An SSI system directly addresses the root of the money laundering problem in the crypto world: the disconnect between blockchain transactions and the individuals behind them. By linking crypto transactions or digital wallets to verified identities, the SSI system closes this critical gap. In cases of suspicious activity, regulators or law enforcement can trace transactions back to verified individuals or entities, enabling effective investigation and enforcement. Furthermore, the blockchain-based SSI system ensures that verifiable credentials and transaction logs are tamper-proof, significantly enhancing forensic capabilities.[299]

Critics, particularly within the crypto community, may resist linking identities to transactions, citing privacy concerns and the importance of anonymity or pseudonymity.[300] However, SSI systems can be designed with privacy preservation features.[301] They can leverage advanced technologies such as zero-knowledge proofs (ZKPs), allowing verification of information without disclosing sensitive details.[302] For example, a user could prove they meet certain regulatory requirements without revealing unnecessary personal information. By sharing only what is essential, SSI reduces the risk of identity theft and data misuse while making compliance far less intrusive for users.

Below is a case study using Dock[303] to illustrate how a decentralized digital identity system can allow users to retain control of their digital identity and preserve privacy while combating money laundering. Dock is a Substrate-based blockchain platform that facilitates the creation, issuance, and verification of

297. *Benefits of Using Digital Identity with Blockchain*, SOLULAB, https://www.solulab.com/benefits-of-using-digital-identity-with-blockchain/ (last visited Jan. 30, 2025).

298. *Decentralized Identifiers (DIDs): The Ultimate Beginner's Guide 2025*, DOCK (Oct. 16, 2025), https://www.dock.io/post/decentralized-identifiers.

299. Rahul Nambiampurath, *What Is Digital Identity Management, and Why Is It Important?*, COINTELEGRAPH (Jan. 14, 2026), https://cointelegraph.com/learn/what-is-digital-identity-management.

300. *See generally Blockchain-Based Digital Identity: Benefits, Risks, and Implementation Challenges*, FIN. MAGNATES, https://www.financemagnates.com/cryptocurrency/education-centre/blockchain-based-digital-identity-benefits-risks-and-implementation-challenges/ (last visited Feb. 6, 2025). This critique is about digital identity as a whole but is applicable in the cryptocurrency space.

301. *See* Nambiampurath, *supra* note 299.

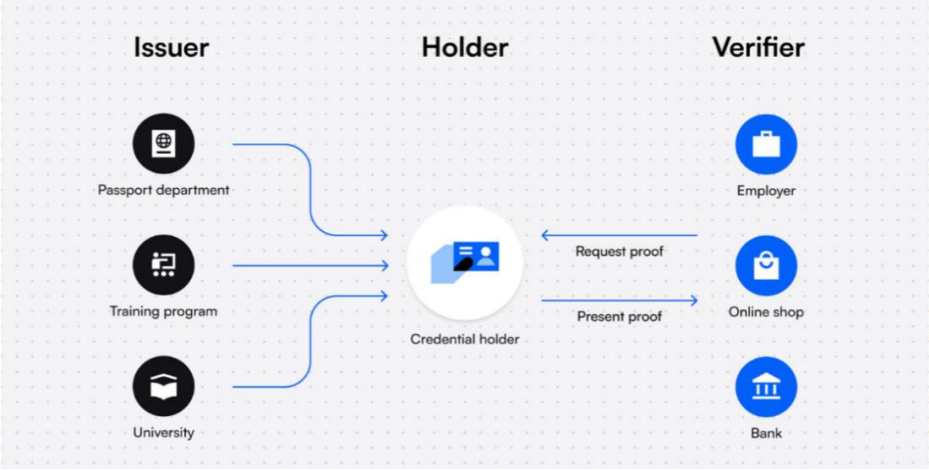
302. Kurt Hemecker, *Digital Identity: Solving the Privacy Problem with Zero Knowledge Proofs*, MINA PROTOCOL (May 2, 2024), https://minaprotocol.com/blog/digital-identity-in-web3-with-zero-knowledge-proofs-zk.

303. *See Verifiable Credentials for Companies*, DOCK, https://www.dock.io/verifiable-credentials-company (last visited Jan. 30, 2025).

digital identifiers and cryptographically signed Verifiable Credentials.[304] These credentials serve as secure digital versions of traditional paper and digital credentials, enabling individuals to verify their identities.[305]

The Verifiable Credentials ecosystem consists of three key participants: issuer, holder, and verifier, as outlined in the chart below.[306] The issuer is an entity, like a government or educational institution, that issues and cryptographically signs a verifiable credential to guarantee its authenticity.[307] The holder is an individual who receives and stores the credential in a secure digital wallet and can share it when needed.[308] The verifier is a person, such as an employer or service provider, that requests and verifies the credential to authenticate identity or qualification.[309]

Figure 3: Three Participants in the Verifiable Credentials Ecosystem.[310]



Dock offers a range of products to facilitate credential issuance and verification.[311] More specifically, Dock Certs Web App is the no-code platform that enables organizations to (1) create and manage digital identities and verifiable credentials, (2) create verification templates and requests to credential holders via QR codes, and (3) integrate digital identity and verifiable credential functionalities into their systems via API access.[312]

Below are steps of how Dock's Digital Identity Verification System works:

304. *See* DOCK, *supra* note 295.
305. *Id.*
306. *Id.*
307. *Id.*
308. *Id.*
309. *Id.*
310. *Id.*
311. *Id.*
312. *Id.*

1. The issuer creates a Verifiable Credential containing specific information about a person or organization. The issuer then cryptographically signs the credential to guarantee its authenticity.[313]

2. The holder stores the credential in their digital wallet (e.g., Dock Wallet) or identity management system.[314]

3. A verifier sends a verification request through a QR code to credential holders to confirm some information such as their name, professional license, and age.[315]

4. The credential holder gives explicit permission to share the necessary credential information from their digital wallet to the verifier.[316]

5. When the verifier checks the credential, Dock's system uses DIDs to check the cryptographic signature on the credential to confirm that it belongs to the correct issuer and has not been tampered with.[317]

6. Once the verifier is satisfied with the authenticity and validity of the credential, they can accept it as proof of the user's identity or qualifications.[318]

In this process, a key element that allows users to retain control of their identity is the use of DIDs. A DID is a globally unique identifier composed of a string of letters and numbers, such as did:dock:5Gl3xbSoufGoWenfllNb5, that contains details such as the public key and verification information.[319] Unlike traditional identifiers, DIDs are not tied to centralized registries or authorities. Instead, they are stored on the blockchain, ensuring user control over their identities. Holders can create as many DIDs as they want for different purposes, such as creating one DID for university credentials and another for work credentials.[320]

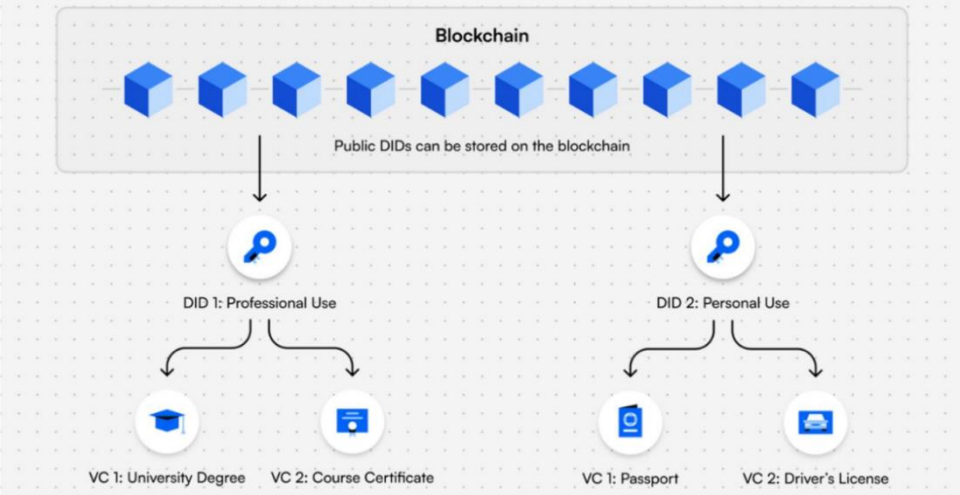
Each DID is associated with a cryptographic key pair: a public key, which is recorded on the blockchain, and a private key, which is securely held by the holder in the digital wallet. The public key acts like a digital signature that others can use to verify the authenticity of a credential or identity claim. The private key, on the other hand, remains confidential and is used to sign transactions, proving ownership and control over the DID.[321]

For example, when a holder presents a verifiable credential (such as a digital diploma), the verifier checks the signature using the public key stored on the blockchain. If the signature matches, it confirms that the credential was

313. *Id.*
314. *Id.*
315. *Id.*
316. *Id.*
317. *Id.*
318. *Id.*
319. *See Digital Identity: Beginner's Guide 2025*, *supra* note 295.
320. *Id.*
321. Mary Lacity & Erran Carmel, *Self-Sovereign Identity and Verifiable Credentials in Your Digital Wallet*, 21 MIS Q. EXEC. 241, 243 (Sep. 2022) ("Each DID is controlled by a public-private key pair. The DID private key is stored in an SSI digital wallet.").

issued by the correct entity and has not been tampered with. However, the verifier does not gain access to the user's private key or any sensitive data, preserving privacy and security.

Figure 4: How Decentralized Identity Works.[322]



In addition to helping users retain control of their digital identity while preserving privacy, a decentralized digital identity system can help combat money laundering by linking digital identities to blockchain transactions—one of the biggest challenges in AML compliance and enforcement. Such a system must be carefully designed, both technologically and institutionally, to balance AML goals, user autonomy, and the principles of decentralization.

First, lawmakers and regulators should establish clear, risk-based thresholds for when identity verification is necessary. At the federal level, Congress can direct the Treasury Department, or more specifically, FinCEN, to determine such thresholds more precisely. For example, transactions under $1,000 do not need identity verification and transactions between $1,000 and $10,000 would require standard authentication (e.g., a driver's license). Transactions over $10,000 would require enhanced verification (e.g., biometric authentication and additional identity proofs).

Next, regulators and law enforcement should collaborate with digital identity providers to define licensing criteria and industry standards, ensuring data protection, interoperability, and privacy in line with global frameworks such as W3C Verifiable Credentials and Decentralized Identifiers.[323] They should

322. *Id.*

323. Manu Sporny, Dave Longley, David Chadwick & Ivan Herman, *World Wide Web Consortium, Verifiable Credentials Data Model 2.0*, WORLD WIDE WEB CONSORTIUM [W3C] (May 15, 2025), https://www.w3.org/TR/vc-data-model/. The W3C Decentralized Identifier Standard is a framework for self-sovereign identity that allows users to create and control DID's without relying on centralized intermediaries. It enables interoperability through a DID document, which contains public

also work with decentralized and semi-decentralized projects to incorporate digital identity into their operation. Smart contracts could be programmed to enforce identity verification thresholds, requiring identity proofs for high-value or suspicious transactions while allowing lower standards for small, routine transactions. Digital identity can be integrated with blockchain analytics tools and AI models to analyze money laundering threats, support investigations, and enhance enforcement efforts.

Lastly, all stakeholders must collaborate to establish clear rules on when and how to unmask identities in cases of suspected money laundering. This includes defining methods for law enforcement to access identity data without violating user privacy and developing frameworks for reporting suspicious activity while maintaining decentralization principles.

Decentralized digital identity systems offer a transformative solution to combating money laundering in the crypto space. However, implementing such a system is inherently a long-term, resource-intensive, and challenging endeavor. SSI and DID systems require a fundamental shift in how regulators or law enforcement approach identity verification and AML compliance. Current frameworks are predominantly centralized, relying on financial institutions to perform KYC checks and report suspicious activity. Moving from centralized to decentralized identity models may face pushback from governments or regulators due to perceived risks or philosophical differences.

The structural and cultural changes may also face resistance from privacy-conscious crypto users. Despite assurances of privacy, the idea of sharing identity credentials, even selectively, can provoke skepticism. Users may fear that these systems could lead to increased surveillance or misuse of their data. Widespread education and training would be required to ensure users understand the pros and cons of the systems. Decentralized identity systems often require users to make nuanced decisions about what information to share and with whom. This level of autonomy, while empowering, can be overwhelming for some users.

Successful adoption of a decentralized digital identity also requires overcoming technological barriers. Implementing SSI and DIDs at scale requires significant investment in blockchain technology, cryptographic protocols, and secure digital wallets. SSI and DID systems must also be interoperable across different blockchain networks, platforms, and applications. The adoption of standards, such as the W3C's DID specification, is critical but not yet universal.[324] For users, managing cryptographic keys, digital wallets, and verifiable credentials requires a certain level of technical knowledge. Users unfamiliar with these concepts may struggle to adopt and effectively use these

keys and verification methods. The standard supports privacy measures by eliminating the need for personally identifiable information and through supporting verified credentials.

324. *Id.*

systems. Overcoming these challenges involves gradual implementation and testing, making this a multi-year, phased project.

3. Scope of Intermediary-Based Approach

While the crypto industry was founded on the idea of decentralization, many projects remain highly centralized in their development, governance, and operation in practice.[325] Centralized exchanges and stablecoin issuers exemplify this centralization. Centralized exchanges function much like traditional financial institutions, acting as intermediaries that not only facilitate cryptocurrency trading but also provide custody, staking, margin trading, lending, on-ramp, and off-ramp services.[326]

These exchanges are typically developed and maintained by a single entity or a closely controlled corporate team, rather than an open-source, community-driven process.[327] They rely on proprietary software that is neither transparent nor publicly auditable.[328]

Governance is fully controlled by a central entity, often the funding company or a corporate board.[329] Users or token holders usually have little to say in decision-making processes.[330] This includes critical aspects such as fee structures, listing policies, and compliance measures.[331] The leadership has the authority to delist assets, freeze accounts, or change policies without community input.[332]

---

325. *Supra* Section III.C.

326. Marco Dell'Erba, *Crypto-Trading Platforms as Exchanges*, 2024 MICH. ST. L. REV. 1, 33–34 (2023).

327. *Id.*

328. *See, e.g.*, Sandro Psaila, *Building Trust in Crypto Exchanges*, DELOITTE (Apr. 28, 2021), https://www.deloitte.com/mt/en/services/audit-assurance/perspectives/mt-building-trust-in-crypto-exchanges.html (offering private cybersecurity solutions for crypto exchange software); *cf.* Press Release, Gate.io, Gate.io Makes Its Proof of Reserves Audit Solution Open-Source, Works with Global Exchanges to Safeguard User Assets (Nov. 10, 2022), https://cryptoslate.com/press-releases/gate-io-makes-its-proof-of-reserves-audit-solution-open-source-works-with-global-exchanges-to-safeguard-user-assets/ (marketing an open-source audit as a selling point that makes Gate.io stand out as an exchanger).

329. *See, e.g.*, *Binance Board of Directors*, BINANCE (Jan. 2025), https://www.binance.com/en/about; *Our Executive Team*, COINBASE (Jan. 2025), https://www.coinbase.com/about.

330. Oliver Ethan, *The Pros and Cons of Investing in a Centralized Crypto Exchange*, NASSCOM (Mar. 21, 2024), https://community.nasscom.in/communities/fintech/pros-and-cons-investing-centralized-crypto-exchange.

331. Alexander Shishkanov, *How Do Crypto Exchanges Make Money?—An In-Depth Look*, B2BROKER (Nov. 11, 2024), https://b2broker.com/news/how-do-crypto-exchanges-make-money-an-in-depth-look.

332. *See, e.g.*, *Poloniex Delisting Policy*, POLONIEX, https://support.poloniex.com/hc/en-us/articles/360040013693-Poloniex-Delisting-Policy (last visited Oct. 27, 2025); blogtienso, *Why Your Binance Account Might Be Frozen and How to Avoid It*, BINANCE (Jan. 3, 2025), https://www.binance.com/en/square/post/18420338108202; *see also* Jonnie Emsley, *EOS Block Producers Violate Constitution, Freeze 7 Suspect Accounts*, CRYPTOSLATE (June 19, 2018), https://cryptoslate.com/eos-block-producers-violate-constitution-freeze-7-suspect-accounts (although

Operationally, centralized exchanges typically retain full control over critical functions and processes rather than outsourcing them to third parties.[333] They employ in-house teams to implement leadership decisions on services and products, maintain their software infrastructure, and process transactions internally using proprietary matching engines and centralized databases.[334] When executing transactions off-chain, these exchanges have the discretion to modify records, halt trading, or even reverse transactions.[335] Additionally, they can directly manage compliance requirements.[336]

Similarly, stablecoin issuers such as Tether, Ripple, and Circle exhibit a high degree of centralization. They develop and control the update of software, unilaterally determine issuance and redemption policies, and retain the authority to freeze or blacklist funds.[337] Operationally, they manage reserves through traditional financial institutions, oversee transactions, and enforce compliance regulations.[338]

For these highly centralized projects, the intermediary-based approach remains applicable, at least in the short term, to combat money laundering. Regulators and law enforcement can still mandate compliance with KYC and AML requirements, primarily because identifying responsible parties—usually the entities themselves—is straightforward. These entities typically have in-house teams dedicated to managing compliance; alternatively, leadership can choose to outsource compliance requirements to external firms. If they fail to meet these obligations, law enforcement can hold them accountable just as they would with traditional financial institutions.

Changes to the intermediary-based approach can be made in the investigation and enforcement stages. Regulators and law enforcement can shift to using blockchain intelligence by collecting information not only from these centralized entities through their reporting documents but also directly from the blockchain network. By leveraging blockchain analytics and AI models, authorities can enhance their ability to detect suspicious activities and trace illicit transactions.

---

not an exchange, a small group of decision makers froze accounts in direct opposition to the EOS blockchain protocol constitution).

333. While exchanges don't explicitly publicize their operational structures in detail, we can glean information from various sources to understand their approach to in-house teams versus outsourcing. *See How to Get Job in Binance and Earn Passive Income of $10000 Every Month*, BINANCE (Nov. 10, 2024), https://www.binance.com/en/square/post/16049417273641 (advertising multiple in-house positions for software development, cybersecurity, marketing, compliance, and finance).

334. *Id.*

335. *See, e.g.*, Binance France Live, *#Binance will delist and halt trading of all Spot trading pairs with the following token(s) on 2024/12/10 03:00 (UTC)*, BINANCE SQUARE (Nov. 29, 2024), https://www.binance.com/en/square/post/16898401292641.

336. Sun, *supra* note 23.

337. Shishkanov, *supra* note 331.

338. Shashank Agrawal, *Proof of Reserves Grant*, COINBASE (Nov. 9, 2023), https://www.coinbase.com/blog/proof-of-reserves-grant.

A few federal agencies, including the FBI**,** FinCEN, and IRS, have already been leveraging blockchain analytics and AI models to investigate money laundering and track and seize laundered cryptocurrency.[339] However, the scope of their use remains limited. These tools should be adopted by all relevant agencies, including state law enforcement. To ensure effective implementation, governments and legislative bodies should provide additional funding, specialized training, and subject matter experts. Expanding these resources will enable law enforcement to keep pace with evolving crypto-related money laundering tactics, improve cross-agency coordination, and strengthen AML enforcement at both the federal and state levels**.**

Similarly, to comply with AML laws, these responsible entities, such as exchanges and stablecoin issuers, can leverage blockchain intelligence and AI models to enhance monitoring, detect suspicious activities, and ensure regulatory compliance. The function of these tools to combat money laundering remains the same regardless of whether a project is centralized, semi-centralized, or decentralized. The key difference lies in who has the authority to implement and utilize them.

In centralized projects, leadership can easily decide to adopt blockchain intelligence and AI-driven compliance tools, ensuring that AML measures are enforced at the institutional level. Unlike semi-decentralized or decentralized projects, where decision-making is more distributed and often relies on community voting or influence from key stakeholders, centralized entities can be legally mandated to implement these tools. Failure to meet such a mandate should result in penalties.

Additionally, decentralized digital identity can provide significant benefits to centralized projects in combating money laundering. Since centralized projects are legally mandated to conduct KYC, they must verify user identities. [340] Traditional KYC processes require users to submit personal documents, which are then stored in centralized databases, making them vulnerable to hacks and data breaches.[341] A decentralized digital identity system allows users to verify their identity once, eliminating the need for centralized storage of personally identifiable information. Instead of repeatedly providing

339. *See, e.g.*, Press Release, U.S. Dep't of the Treasury, U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash (Aug. 8, 2022), https://home.treasury.gov/news/press-releases/jy0916 (finding a mixer after tracking interactions with another sanctioned mixer); Press Release, U.S. Dep't of Just., Justice Department Seizes Over $112M in Funds Linked to Cryptocurrency Investment Schemes (Apr. 3, 2023), https://www.justice.gov/archives/opa/pr/justice-department-seizes-over-112m-funds-linked-cryptocurrency-investment-schemes.

340. As discussed in Part II, many centralized projects now fall under the term "money transmitter" and are subject to the same laws as traditional financial institutions including KYC requirements. *See Implementing KYC/AML in Crypto Exchanges*, OPENWARE (Aug. 22, 2024), https://www.openware.com/news/articles/implementing-kycaml-in-crypto-exchanges.

341. *Id.*

sensitive data, users can cryptographically verify their identity without exposing personal details, reducing identity theft risks and enhancing privacy.

A decentralized digital identity system, if implemented well, can also help centralized entities automate and streamline AML compliance. By integrating decentralized identity solutions with AML compliance systems, centralized projects can automate identity verification and flag high-risk users before transactions occur. These systems can be linked to blockchain analytics and AI-driven behavioral monitoring models, allowing centralized entities to monitor transactions in real time, assess risk levels based on users' transaction histories, and detect unusual activity more efficiently.

Legislators, policymakers, and regulators must adopt a phased approach to implementing decentralized digital infrastructure. While some measures can be implemented immediately, others require long-term vision, strategic planning, and sustained efforts. Currently, many blockchain intelligence tools are already available on the market.[342] Law enforcement agencies and industry players can immediately leverage these tools, or be mandated to adopt them, to enhance AML enforcement and compliance, ensuring a more effective response to illicit activities in the crypto space.

However, a comprehensive decentralized identity framework has yet to be developed, making it a long-term objective that requires policy advancements, technological innovation, and industry collaboration. Large-scale projects like this face numerous challenges, including interoperability concerns, regulatory uncertainties, and the need for broad industry coordination to ensure successful implementation.

V.
CONCLUSION

This Article examines how criminals exploit the crypto ecosystem for money laundering and explains why the existing legal and regulatory framework fails to effectively combat illicit financial activities in this space. More importantly, it proposes a decentralized digital infrastructure that integrates blockchain intelligence alongside a digital identity system. It further outlines the roles and responsibilities of various stakeholders within the crypto industry and emphasizes the need for cross-sector collaboration and phased adoption, ensuring that the AML regime balances innovation and regulatory compliance. In doing so, it reconceptualizes decentralization not merely as a technological design choice but as a regulatory strategy—one that shifts from centralized oversight to shared responsibility in both preventing and combating money laundering.

342. *See, e.g.*, *Blockchain Intelligence*, CHAINALYSIS, https://www.chainalysis.com/blockchain-intelligence/ (last visited Oct. 2, 2025); *Blockchain Intelligence Platform*, TRM LABS, https://www.trmlabs.com/ (last visited Oct. 2, 2025); *Blockchain Analytics & Crypto Compliance Solutions*, ELLIPTIC, https://www.elliptic.co/ (last visited Oct. 2, 2025).

This Article contributes to understanding why the existing AML framework is ineffective and proposes novel solutions. However, it does not address all aspects of this complex issue. Future research can delve deeper into the theory of decentralization and explore incentive mechanisms that encourage stakeholders in decentralized ecosystems to assume greater AML responsibilities. Additionally, further collaboration with technical experts is needed to design and optimize blockchain intelligence tools for more effective applications. Efforts should also focus on creating a robust, interoperable digital identity system that balances privacy, user autonomy, and AML objectives. Continued interdisciplinary efforts will be essential in shaping a decentralized yet compliant ecosystem.