GEORGETOWN UNIVERSITY

Psaros Center for Financial Markets and Policy
McDONOUGH SCHOOL of BUSINESS

Considering Institutional DeFi Integration: How To Manage Illicit Finance Risk

Yaya J. Fanusie
Visiting Fellow

Saskia Seidel
Law and Policy Researcher

Georgetown University's Psaros Center for Financial Markets and Policy

McDonough School of Business

October 2025

I. Executive Summary

Decentralized Finance (DeFi) represents a fundamental shift in financial infrastructure, enabling many traditional financial services through autonomous smart contracts on permissionless blockchain networks. DeFi is growing and continuously innovating and there are signs that traditional finance is exploring strategic and technical benefits of decentralized architectures.

The regulatory landscape is rapidly evolving but is not accommodating this exploration—thus slowing down advances towards employing true permissionless DeFi. The European Union's Markets in Crypto-Assets (MiCA) regulation provides comprehensive frameworks for centralized crypto activities while explicitly excluding fully decentralized protocols. The United States has established robust anti-money laundering (AML)/counter-the financing of terrorism (CFT) frameworks for centralized activities through Financial Crimes Enforcement Network (FinCEN) guidance and recent stablecoin legislation, yet genuine DeFi protocols remain largely outside existing regulatory frameworks due to their intermediary-less structure.

This regulatory gap creates risks but also an opportunity for new approaches. While institutions are gaining clarity for centralized crypto operations, they lack formal guidance for DeFi integration. Meanwhile, illicit actors exploit DeFi's openness and privacy features. As regulatory clarity emerges for centralized markets, institutions are increasingly pressured by competitive and operational advantages to consider DeFi, making proactive compliance frameworks critical for these institutions that utilize DeFi.

Rather than requiring entirely new regulatory regimes, this paper identifies technology-native solutions that can achieve traditional AML/CFT objectives while preserving DeFi's core benefits. These approaches range from familiar centralized methods overlaid on DeFi protocols to innovative crypto-native tools that embed compliance directly into blockchain infrastructure.

Key recommendations include formally enabling regulatory flexibility to utilize blockchain-based compliance solutions, expanding financial institution pilots and case studies to experiment with DeFi integration, and ramping up software development of compliance-native blockchain infrastructure, all of which can help foster collaboration between regulators, institutions, and technology providers to establish best practices for compliant DeFi participation.

II. Understanding DeFi: Technology and Regulatory Context

A. What is DeFi?

DeFi refers to a technological ecosystem that replicates traditional financial services—trading, lending, borrowing, and asset management—through programmable smart contracts on permissionless blockchain networks.[1] Unlike traditional finance, which relies on centralized intermediaries like banks and broker-exchanges, DeFi systems operate through autonomous code that executes financial transactions without human intervention.

The defining characteristics of genuine DeFi include: permissionless access (anyone can participate without approval), non-custodial operation (users maintain control of their private keys), transparency (all transactions are publicly verifiable and auditable), programmability (simple and complex transactional processes can be automated by pre-written code)[2], and composability (applications designed for a particular blockchain protocol are seamlessly integrated with one another on that chain). Since DeFi is built on open-source code, developers can modify the code to build new projects—leading to DeFi's global nature and creating technical building blocks that can be combined to create increasingly sophisticated digital financial products.[3]

Importantly, while the term "DeFi" has been appropriated by many centralized services that merely use blockchain technology while maintaining traditional intermediary structures, this paper focuses on "genuine DeFi"—systems where no single entity exercises control.

CeFi vs. DeFi: Fundamental Operational Differences

While centralized finance (CeFi) entities and DeFi applications engage in many of the same activities, their approach is fundamentally different. Consider cryptocurrency trading as an example:

A centralized exchange (CEX) functions like traditional stock trading, requiring users to deposit funds into exchange-controlled accounts, undergo identity verification, and trade within the CEX's internal ledger system. Users must trust the CEX to safeguard their assets and execute trades fairly, though CEXs enable crypto-fiat trading and provide familiar regulatory oversight.[4]

In contrast, a decentralized exchange (DEX) operates through smart contracts where users trade directly from their own wallets. No entity controls user funds during the trading process. Prices are determined algorithmically through automated market makers (AMMs),[5] and all trading activity is recorded immutably on-chain. Users interact with decentralized software protocols

[1] "What is DeFi?" Crypto Council for Innovation*,* 18 July 2025, https://cryptoforinnovation.org/what-is-defi/.

[2] "Key Elements of an Effective DeFi Framework." Crypto Council for Innovation, 5 October 2023, https://cryptoforinnovation.org/key-elements-of-an-effective-defi-framework/.

[3] Ammori, Marvin. "Decentralized Finance: What It Is, Why It Matters." a16z crypto, 9 September 2024, https://a16zcrypto.com/posts/article/what-is-decentralized-finance/.

[4] "What is a Decentralized Exchange?" Crypto Council for Innovation, 18 July 2025, https://cryptoforinnovation.org/what-is-a-decentralized-exchange/.

[5] An automated market maker is a smart contract that creates a pool of liquidity for two types of tokens; as the trades occur, the pricing of the tokens updates by a mathematical formula. "What is an Automated Market Maker?" Uniswap Labs, 1 May 2025, https://blog.uniswap.org/what-is-an-automated-market-maker.

rather than corporate entities. DEXs essentially are peer-to-peer marketplaces where participants trade exclusively cryptocurrency tokens—not fiat—directly with each other.[6]

CeFi functions through databases requiring manual input and centrally managed accounts. DeFi represents a technological solution following entirely automated and autonomous processes where funds remain in users' self-custodial wallets. This fundamental difference means DeFi does not require identification or personal information from participants, making it pseudonymous and preventing the application of traditional AML/CFT tools like know-your-customer (KYC) and transaction monitoring.

B. Market Scale and Growth

The DeFi ecosystem has experienced explosive growth with total value locked (TVL) reaching over $100 billion at times[7] and maintaining substantial volumes even through market downturns.[8] Major DeFi protocols like Uniswap routinely handle the equivalent of more than $100 billion in monthly trading volume of crypto-assets, often exceeding many traditional CeFi exchanges.[9] This growth occurs entirely outside existing regulatory frameworks designed for intermediary-based systems.

C. Current Regulatory Landscape

Formalization of CeFi Markets

In the United States, the Treasury Department's FinCEN issued guidance in 2013 establishing robust AML/CFT frameworks for centralized crypto activities by classifying cryptocurrency exchanges as money services businesses.[10] This guidance was updated in 2019, with FinCEN addressing how the rise of certain crypto-asset business activities are covered under the Bank Secrecy Act (BSA), the set of laws governing U.S. AML/CFT regulations.[11] This updated guidance did not sufficiently address DeFi, which was relatively nascent in 2019, but the main interpretation was that truly decentralized entities that do not control user funds are outside the

[6] "What are decentralized exchanges, and how do DEXs work?" *Cointelegraph*, 10 August 2023, https://cointelegraph.com/learn/articles/what-are-decentralized-exchanges-and-how-do-dexs-work.

[7] "DeFi TVL reaches $100B as Bitcoin pumps sentiment." *Cointelegraph*, 9 March 2024, https://cointelegraph.com/news/defi-tvl-reaches-100b-bitcoin-pumps-sentiment.

[8] DeFi Total Value Locked Tracker, *The Block*, https://www.theblock.co/data/decentralized-finance/total-value-locked-tvl. Accessed 23 October 2025.

[9] DEX Volume by chain: Uniswap. *Defi Llama,* https://defillama.com/protocol/dexs/uniswap. Accessed 23 October 2025.

[10] Financial Crimes Enforcement Network. "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies." FIN-2013-G001. U.S. Department of the Treasury, 18 March 2013, https://www.fincen.gov/system/files/shared/FIN-2013-G001.pdf.

[11] Financial Crimes Enforcement Network. "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies." FIN-2019-G001. U.S. Department of the Treasury, 9 May 2019, https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

scope of BSA regulations. More recently, passage of the GENIUS Act formally extends the AML/CFT framework to stablecoin issuers, requiring them to operate as regulated financial institutions under BSA obligations.[12] DeFi entities are not regulated under the stablecoin framework.

The EU's MiCA regulation, which became fully operational at the end of 2024, establishes comprehensive regulatory frameworks for centralized crypto activities. MiCA brings crypto-asset issuers, exchanges, and service providers under formal supervision with robust AML/CFT requirements comparable to those for traditional financial services.

Importantly, Recital 22 of MiCA explicitly excludes fully decentralized protocols from its scope,[13] acknowledging the practical challenges of applying traditional financial regulation to autonomous code.[14] This creates a clear distinction between regulated CeFi activities and the unregulated DeFi space.[15]

The DeFi Regulatory Gap

Despite these policy advancements, genuine DeFi operates largely outside existing regulatory frameworks. The BSA's intermediary-focused approach cannot readily address systems where no intermediaries exist. Traditional AML/CFT obligations—customer identification, suspicious activity reporting, recordkeeping—presuppose the existence of regulated entities capable of performing these functions.

Financial regulators globally acknowledge this challenge. The Financial Action Task Force (FATF)'s 2025 Virtual Assets update reiterates the acknowledgment from previous reports that AML in the context of DeFi is challenging since DeFi protocols lack identifiable responsible parties to whom traditional obligations could attach.[16] The U.S. Treasury's 2023 DeFi Risk Assessment similarly noted that while some DeFi projects retain centralized control (making them subject to existing rules), others operate as genuinely decentralized infrastructure beyond traditional regulatory reach.[17]

[12] GENIUS Act U.S. Congress, 18 July 2025, https://www.congress.gov/bill/119th-congress/senate-bill/1582/text.

[13] European Commission. REGULATION (EU) 2023/1114 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937, https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng.

[14] IBIT. However, Article 142 of MiCA also mandates that the European Commission publish a report on DeFi, evaluating its unique regulatory challenges and proposing potential frameworks for supervision. This forthcoming report is expected to play a significant role in shaping the EU's future approach to DeFi oversight.

[15] "Demystifying DeFi in MiCAR." PwC Legal, 8 October 2024, https://legal.pwc.de/en/news/articles/demystifying-defi-in-micar.

[16] "Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs." FATF, 26 June 2025, https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2025-Targeted-Upate-VA-VASPs.pdf.coredownload.pdf.

[17] "Illicit Finance Risk Assessment of Decentralized Finance." U.S. Department of the Treasury, April 2023, https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf.

III. The DeFi Integration Imperative: Market Forces Driving Institutional Adoption

A. Regulatory Clarity as Catalyst

The formalization of centralized crypto regulatory frameworks has removed primary barriers to institutional participation. MiCA's comprehensive approach brings crypto-asset issuers, exchanges, and service providers under formal supervision with robust AML/CFT requirements comparable to traditional financial services. This regulatory certainty has already driven significant institutional adoption across EU markets.

In the U.S., the trajectory appears similarly promising. The current administration's supportive stance toward digital assets, combined with bipartisan congressional momentum behind comprehensive market structure regulation, signals imminent increased regulatory clarity for centralized crypto markets. Provisions in the GENIUS Act even allow U.S. banks to use stablecoins for interbank settlement, a highly unlikely—if not impossible—prospect before the legislation was enacted. In October 2025, the Federal Reserve Board of Governors held a payments innovation conference hosting many of the companies building stablecoin and DeFi infrastructure. Fed Governor Christopher Waller gave opening remarks welcoming "new entrants from the DeFi world" to the mainstream payment ecosystem and explained that the DeFi industry would no longer be treated with suspicion by the Federal Reserve.[18] This new regulatory environment is enabling new potential bridges between traditional finance and blockchain infrastructure.

This regulatory progress naturally directs institutional attention toward DeFi's compelling value propositions. As institutions become comfortable with basic crypto operations within established regulatory frameworks, they inevitably encounter DeFi's operational advantages: continuous global markets, enhanced liquidity dynamics, programmable compliance capabilities, and unprecedented transparency.[19]

B. Institutional Momentum and Infrastructure Development

Major financial institutions demonstrate clear movement beyond simple crypto custody toward sophisticated blockchain integration. BlackRock's tokenized fund offerings, including the BUIDL fund representing over $1 billion in tokenized treasury securities,[20] prove institutional appetite for blockchain-native financial instruments. JPMorgan's Onyx platform—including its

[18] Federal Reserve Board. "Embracing New Technologies and Players in Payments." Governor Christopher J. Waller, 21 October 2025, https://www.federalreserve.gov/newsevents/speech/waller20251021a.htm.

[19] SEC. "Remarks at the Crypto Task Force Roundtable on Decentralized Finance." Chairman Paul S. Atkins, 9 June 2025, https://www.sec.gov/newsroom/speeches-statements/atkins-remarks-defi-roundtable-060925.

[20] "BlackRock's BUIDL first to cross $1 billion mark, making it the largest tokenized fund tracking onchain Treasuries." *The Block*, 13 March 2025, https://www.theblock.co/post/346237/blackrocks-buidl-first-to-cross-1-billion-mark-making-it-the-largest-tokenized-fund-tracking-onchain-treasuries.

JPM Coin stablecoin—is a private blockchain network enabling institutional payments. JPM Coin has been reported to process about $1 billion in transactions daily,[21] demonstrating that major banks can effectively deploy and operate blockchain infrastructure at scale, even if still in closed environments.[22]

The stablecoin ecosystem particularly illustrates institutional readiness for DeFi integration. Stablecoins—well before the recent regulatory advancement—have been very popular on DeFi platforms as a way to counter the price volatility of other types of crypto-assets. Regulated stablecoins would provide price stability necessary for mainstream financial applications while retaining blockchain technology's programmability and efficiency benefits. Major banks have announced plans to issue regulated stablecoins, signaling institutional confidence in this compliance pathway.[23]

Payment infrastructure companies have similarly embraced stablecoin technology. PayPal has embedded stablecoin functionality directly into its payment systems: PayPal USD (PYUSD) launched in August 2023 as a fully backed ERC-20 stablecoin used for peer-to-peer transfers, merchant payments, and even its first commercial business payment via SAP's Digital Currency Hub.[24] This integration exemplifies how payment infrastructure providers can operationalize blockchain-native assets within legacy networks. Established payment giants are actively integrating stablecoin capabilities: Visa has piloted USDC settlement—including on Solana rail—and Mastercard has partnered with Circle and Paxos to enable merchant stablecoin acceptance.[25]

[21] "JPMorgan Says JPM Coin Now Handles $1 billion Transactions Daily." *Bloomberg*, 26 October 2023, https://www.bloomberg.com/news/articles/2023-10-26/jpmorgan-says-jpm-coin-now-handles-1-billion-transactions-daily?embedded-checkout=true.

[22] While most institutional blockchain initiatives today remain permissioned and centrally governed, they are explicitly inspired by the operational advantages of DeFi—continuous settlement, composability, and programmability. Notable pilots include JPMorgan's 2022 MAS Project Guardian transaction on Polygon, Société Générale's use of MakerDAO for refinancing tokenized debt, and the launch of Aave Arc's permissioned DeFi pools. These illustrate that traditional finance is strategically exploring decentralized architectures, even if full-scale integration with permissionless DeFi remains nascent.

[23] "Bank of America Plans To Launch Stablecoin Once U.S. Legislation is Passed, CEO Says." *Yahoo Finance*, 27 February 2025, https://finance.yahoo.com/news/bank-america-plans-launch-stablecoin-081305207.html.

[24] "PayPal's stablecoin opens door for crypto adoption in traditional finance." *Cointelegraph*, 17 August 2023, https://cointelegraph.com/news/paypal-stablecoin-crypto-adoption.

[25] "Mastercard Adds Stablecoin Settlement Support for Merchants." *Bloomberg*, 28 April 2025, https://www.bloomberg.com/news/articles/2025-04-28/mastercard-adds-stablecoin-settlement-support-for-merchants
.

III. Current Illicit Finance Landscape in DeFi

A. Evolving Threat Patterns

DeFi's illicit finance landscape reflects sophisticated adaptation to the digital asset ecosystem by actors seeking to expand their resources beyond traditional financial channels. TRM Labs' 2025 analysis shows North Korea accounted for approximately 35% of all stolen cryptocurrency funds in 2024, approaching $800 million in total theft.[26] These operations average nearly five times larger than those of other criminal actors, demonstrating state-level exploitation of DeFi infrastructure.

Criminal actors increasingly exploit DeFi's cross-chain infrastructure, using decentralized bridges and multiple blockchain networks to obscure transaction trails. The movement of stolen funds from initial theft to final disposition often occurs within hours, especially through ecosystems like TRON that offer fast confirmation times and low transaction fees. This speed makes traditional law enforcement interdiction extremely difficult.

Criminals leverage stablecoins' stability, transaction efficiency, and abundant liquidity while pairing them with anonymity-enhancing tools, including mixers, bridges, and cross-chain transactions.

B. Secondary Market Vulnerabilities

The stablecoin ecosystem's structure creates particular compliance challenges. Stablecoins are available through a variety of trading environments. While primary markets—where stablecoin issuers provide tokens to institutional customers—operate under established AML/CFT frameworks, secondary markets present significant vulnerabilities. Primary market institutional customers provide the stablecoins they acquire to retail users who can trade directly with anyone outside regulated channels. Outside the United States, in places with high demand for U.S. dollar price stability, many users acquire USD stablecoins through over-the-counter (OTC) crypto brokers operating with minimal KYC procedures, often in jurisdictions lacking robust virtual asset regulation.

This creates what industry analysis describes as "gray markets" that proliferate in countries not implementing FATF's virtual asset guidance.[27] Circle has previously noted that, although exact figures are difficult to obtain, the OTC market often sees 2 to 3 times the daily trading volume of

[26] "2025 Crypto Crime Report." TRM Labs, 9 February 2025, https://cdn.prod.website-files.com/6082dc5b670562507b3587b4/6823baf9045160ea474b3f7a_TRM_2025%20Crypto%20Crime%20Report.pdf.

[27] Fanusie, Yaya J., and Terry, Isabella. "Stablecoin Markets and Mitigating Illicit Finance." Georgetown University Center for Financial Markets and Policy, July 2025, https://finpolicy.georgetown.edu/wp-content/uploads/2025/07/Stablecoin-Markets-and-Mitigating-Illicit-Finance.pdf.

traditional exchanges, highlighting the massive, largely opaque transaction flow outside of regulated venues.[28]

The technical ease of stablecoin transfers compounds these challenges. Unlike traditional banking systems requiring multiple verification steps, stablecoins can transfer between users on blockchain networks with minimal friction. When combined with decentralized exchanges that operate without centralized intermediaries, this creates pathways for illicit actors to access stablecoins outside regulatory oversight.

IV. Centralized Overlay Methods

Regulated institutions exploring how to engage with DeFi have several options to consider. The most familiar approach involves layering traditional AML/CFT procedures onto DeFi protocols. This includes implementing KYC verification requirements, transaction whitelisting, and sanctions screening before users can access DeFi functions. Companies like Fireblocks have developed institutional DeFi services using this model, creating “gated” versions of DeFi protocols accessible only to verified participants.[29]

While this approach provides regulatory comfort to financial institutions by maintaining familiar oversight mechanisms, it faces significant limitations. Adding the exact same compliance mechanisms from traditional finance eliminates many of DeFi’s core benefits—24/7 access, permissionless participation, and the reliance on programmability. The approach essentially creates “CeFi on top of DeFi,” potentially negating the technological advantages that would make DeFi’s operational efficiency attractive to institutions in the first place.

Market evidence suggests limited institutional appetite for heavily restricted DeFi access. The relative scarcity of such services compared to growing DeFi volumes indicates institutions prefer approaches that might preserve more of DeFi’s native benefits while maintaining compliance aims.

[28] “Crypto OTC Markets See Up to 3x as Much Volume as Regular Exchanges, “Anecdotal Evidence” Suggests, Fintech Circle Claims.” *Crowdfund Insider*, 22 January 2021, https://www.crowdfundinsider.com/2021/01/171480-crypto-otc-markets-see-up-to-3x-as-much-volume-as-regular-exchanges-anecdotal-evidence-suggests-fintech-circle-claims.

[29] Sarbhai, Sagar, Kaj Burchardi, Douglas Hsu, Bihao Song, Adam Hart, and Stefan Wang. "Revolutionizing Cross-Border Transactions with Permissioned DeFi." White paper. Fireblocks and Boston Consulting Group, January 2024. https://www.fireblocks.com/wp-content/uploads/2024/01/FB-Permissioned-DeFi-WP-2024.pdf and Varun Paul, Oren Goldberg, and Amp Burapachaisri, "Permissioned and Permissionless Blockchains in Tomorrow's Financial System," Fireblocks, 30 April 2025, https://www.fireblocks.com/wp-content/uploads/2025/05/Whitepaper_Permissionless_4.30.pdf.

V. Blockchain-Based Risk Management Approaches

Rather than attempting to retrofit traditional financial regulation onto intermediary-less systems, emerging solutions embed compliance capabilities directly into DeFi infrastructure. These approaches range from centralized actors using blockchain-based tools to manually manage interactions with DeFi protocols to innovative crypto-native tools that maintain a more decentralized operational architecture while still supporting AML/CFT compliance goals.

Manual Use of Decentralized Tools

A. Blockchain Analytics

Modern blockchain analytics represent perhaps the most mature blockchain-based compliance tool available, offering capabilities that exceed traditional financial surveillance systems in many respects. Unlike traditional banking, where transaction flows are opaque across institutional boundaries, blockchain analytics provides comprehensive, real-time visibility into global transaction patterns.

Blockchain analytics software began as monitoring tools providing attribution of wallet addresses and pattern recognition to better track and understand transaction flows. These tools have evolved in the past few years, with several platforms including Chainalysis, TRM Labs, and Elliptic, offering sophisticated analytic capabilities to institutions that will want to use them as they manage DeFi interactions:

Real-time Risk Scoring: Advanced algorithms analyze transaction patterns, wallet behaviors, and network effects to assign dynamic risk scores. These systems identify suspicious activity as it occurs rather than post-transaction analysis.

Cross-chain Intelligence: Platforms track assets across multiple blockchain networks, providing comprehensive visibility as funds move between different DeFi protocols. This capability proves crucial as sophisticated actors increasingly use cross-chain bridges to obscure transaction trails.

Entity Clustering and Attribution: Analytics platforms can often identify real-world entities behind blockchain addresses, enabling institutions to understand actual counterparties in DeFi transactions. This includes clustering analysis that groups related addresses under common control.

Predictive Threat Detection: Machine learning models identify anomalous transaction patterns indicating money laundering, sanctions evasion, or other illicit activity. These systems learn from historical data to detect emerging threats before they become widespread.

Industry Collaboration: The blockchain analytics ecosystem has developed sophisticated information-sharing mechanisms, enhancing collective security. Major platforms collaborate to share threat intelligence, creating network effects benefiting all participants, such as ChainAbuse.[30] This collaborative approach proved particularly effective against organized illicit finance networks.

Integration with DeFi Infrastructure: Blockchain analytics tools increasingly integrate directly with DeFi protocols through APIs and smart contract hooks, giving interested financial institutions a tool to help manage risk throughout transaction lifecycles. Using blockchain analytics can support pre-transaction screening, real-time monitoring, automated blocking systems, and dynamic policy updates.

Challenges: No formal industry-wide standards exist for blockchain analysis software. Firms' analytic methodologies differ widely, causing discrepancies in wallet attribution between various proprietary tools. Heavy competition within the blockchain analysis sector may have kept companies from developing any sort of industry standard for methodology and performance. If blockchain analysis tools are to be a reliable tool for institutional DeFi integration, the industry will need to develop objective standards to evaluate and even certify tools.

B. Decentralized Identity & Credentials

Decentralized identity solutions involve confirming an individual's identity or attributes through a verification process and then creating a mathematical cryptographic proof attached to a blockchain token. This allows for a decentralized ID or credential that users could hold in digital wallets and present to enable transactions. Decentralized ID tools can be used not just for blockchain transactions but as a form of compliance check for traditional finance or even non-financial use cases where credentials must be presented to gain access to a specific system or environment. Blockchain-based tokens that prove verified credentials or attributes are sometimes called attestation tokens.[31] Government agencies are in the midst of significant R&D and piloting with decentralized identity and credentials, such as the State of California for its mobile driver licenses program,[32] as well as the U.S. Department of Homeland Security, which is

[30] "Think You May Have Fallen for a Crypto Scam?" Chainabuse, accessed 25 October 2025, https://help.chainabuse.com.

[31] "Comment on FinCEN Proposal of Special Measure Regarding CVC Mixing." Crypto Council for Innovation, 22 January 2024, https://cryptoforinnovation.org/wp-content/uploads/2024/01/Crypto-Council-for-Innovation-Comment-on-FinCEN-Proposal-of-Special-Measure-Regarding-Convertible-Virtual-Currency-Mixing-Docket-No-FINCEN-2023-0016.pdf .

[32] "California DMV Open Source Mobile Wallet Awarded Gartner 2023 Eye on Innovation." SpruceID, 12 December 2023, https://blog.spruceid.com/state-of-california-department-of-motor-vehicles-open-source-mobile-wallet-for-decentralized-digital-credentials-named-by-gartner-as-2023-innovation-award-winner/.

exploring privacy-enhancing tech for passport travel and citizenship verification.[33] If such tokens became predominant on DeFi platforms, it would help mitigate many of the risks from permissionless activity. Decentralized credentials also have the cybersecurity benefit of minimizing private data leaks and hacks because personal documents and biometric records do not need to be uploaded to every institution that must verify a customer or user's identity. Also, they counter criminals' use of fake documents since, for practical purposes, cryptographic proofs can not be forged.

Implementation Challenges: Although decentralized identity appears to be a much more efficient and effective way of managing customer identity, regulated financial institutions will be hesitant to rely on such technology if financial supervisors and examiners do not approve of such methods. The KYC procedures, which are required through the Bank Secrecy Act, do not currently make provisions for such credentials. There are indications that financial regulators in the U.S. are becoming more open to allowing alternative ways of verifying identity, but these moves are quite elementary. For example, in mid-2025, U.S. regulators published an exemption allowing banks to use third parties to provide tax ID numbers of customers instead of the customer having to provide the information directly.[34] However, this exemption still requires the bank to collect the data and would not allow for a decentralized cryptographic proof framework for verifying that a user has a legitimate tax ID.

Programmable Compliance Methods

A. Pre-transaction Computation

Pre-transaction computation—embedding compliance controls in smart contracts within DeFi platforms—represents perhaps the most advanced decentralized approach currently in production. Paxos's implementation of USDL on Uniswap V4 (a DEX), developed in cooperation with blockchain software provider Predicate, provides a concrete demonstration of institutional-grade compliance in live DeFi environments, according to the joint white paper released by Paxos and Predicate.[35]

The Paxos case study shows smart contracts could be used to generate "policies" that govern transactions before they occur. This system employs Uniswap V4's "hook" functionality to

[33] "Homeland Security Mobilizes New York Startup for Privacy-Centric and Globally Interoperable Digital Wallets and Verifiers." DHS, Science and Technology, https://www.dhs.gov/science-and-technology/spruceid. Accessed 25 October 2025.
[34] Exemption Order, 27 June 2025, https://www.fincen.gov/system/files/2025-06/CIP-TIN-Exemption-Order-final508.pdf.
[35] "Risk Management Framework for Institutional Liquidity on Uniswap V4." Predicate, 18 June 2025, https://predicate.io/blog/risk-management-framework-for-institutional-liquidity-on-uniswap-v4.

create gated pools where regulated stablecoins can only be traded by verified participants. Before any transaction executes, the compliance infrastructure verifies multiple criteria:

- Sender and recipient identity verification status
- Real-time sanctions screening against Office of Foreign Assets Control (OFAC) lists
- Transaction risk scoring based on behavioral analysis
- Jurisdictional compliance requirements
- Dynamic policy updates reflecting emerging threats

According to the white paper, if any compliance check fails, the transaction automatically reverts before execution. This reportedly creates deterministic compliance, where prohibited transactions cannot occur regardless of user intent. This approach embeds compliance guarantees into transactional infrastructure more directly than found in traditional finance, where checks often occur post-transaction, requiring manual investigation and potential clawbacks.

Systems like the one piloted by Paxos and Predicate for Uniswap transactions also provide unprecedented transparency for regulators. In blockchain-based programmable compliance infrastructure, all compliance decisions are recorded on-chain with immutable audit trails, enabling real-time regulatory oversight rather than periodic reporting. This approach aims for institutional-grade performance, processing transactions in milliseconds while maintaining comprehensive risk screening.

Scalability and Adoption: The Paxos implementation demonstrates that institutional-grade compliance can potentially operate at DeFi scale without performance degradation. Other stablecoin issuers are developing similar approaches, suggesting industry convergence around programmable compliance architectures.

Challenges: A chicken-or-egg scenario exists. Programmable compliance is a nascent approach that would require significant testing before widespread deployment by financial institutions interested in accessing DeFi infrastructure. However, a lack of clarity on financial supervisors' acceptance of these tools may deter many institutions from investing in such pilots. Also, although the Paxos case study is a significant proof-of-concept, there is a huge range of illicit finance risks that need to be incorporated into programmable compliance in order to satisfy all AML/CFT compliance goals. Many risks would not be addressed by binary inputs such as presence on a sanctions list or the possession of a verified identity. Accounting for a wider array of risks would require much more complicated policy programming.

B. Privacy Pools

Privacy Pools[36] represent a sophisticated approach to reconciling financial privacy with regulatory compliance. The framework enables users to prove their funds do not originate from illicit sources without revealing complete transaction histories through what is referred to as zero-knowledge cryptographic proofs (ZKPs).

The system operates through “association sets”—cryptographically defined groups of addresses that users can prove membership in or exclusion from. When transacting, users generate proofs demonstrating their funds derive from “clean” association sets that exclude known illicit addresses. This creates powerful compliance capabilities while preserving legitimate privacy needs.

For financial institutions, Privacy Pools could enable compliant DeFi participation while maintaining customer privacy. Banks could define association sets excluding sanctioned addresses, darknet market outputs, and other high-risk sources. Customers could then engage in DeFi activities while cryptographically proving compliance with institutional risk standards.

Using privacy pools also enables dynamic risk management. As new threats emerge, association sets can be updated in real-time, automatically excluding newly identified illicit actors without requiring protocol-level changes. Different jurisdictions could maintain different association set standards, enabling customized compliance across regulatory environments.

Implementation Challenges: Privacy Pools face significant adoption barriers. The system requires broad participation to achieve effective network effects—if most users do not participate, privacy guarantees weaken substantially. Technical complexity also creates barriers for average users, potentially limiting adoption to sophisticated institutions.

C. Token Extensions

Solana's Token Extensions Program[37] is a form of programmable compliance that embeds protocol-level compliance functionality directly into blockchain environments. Rather than layering compliance programming on top of the transaction logic of DeFi services, such as with Predicate policies, Token Extensions allow developers to build regulatory-friendly features into the foundational token architecture itself.[38]

[36] Buterin, Vitalik et. al, “Blockchain Privacy and Regulatory Compliance: Towards a Practical Equilibrium.” 9 September 2023, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4563364.

[37] "Token Extensions," Solana, accessed 26 October 2025, https://solana.com/solutions/token-extensions.

[38] Comparable compliance-token standards, such as Ethereum's ERC-3643, are also under development, showing the potential for cross-chain embedded compliance.

The compliance aims are similar to pre-transaction computation, although the rules are set by the team developing and issuing a new token. The program provides modular compliance tools that token issuers can combine to meet specific regulatory requirements. For example, according to Solana's case study document, the program offers the following features:

Transfer Hooks: Enable custom compliance logic to execute automatically with every token transfer. These hooks perform compliance checks before transactions settle, enabling preventive rather than reactive oversight. Implementation examples include real-time sanctions screening, transaction-size monitoring, and recipient validation.

Confidential Transfers: Address institutional privacy needs while enabling regulatory oversight. The system uses advanced cryptographic protocols to hide transfer amounts while preserving transparency for designated auditors. Users can configure accounts for confidential transfers while maintaining complete auditability for authorized parties.

Permanent Delegates: Enable designated authorities to maintain oversight capabilities over token accounts even in decentralized environments. This provides institutional-grade control mechanisms, including unlimited privileges to burn or transfer tokens when necessary for regulatory compliance.

The Token Extension approach attempts to resolve fundamental tensions between regulatory requirements and blockchain openness through programmable selectivity. Rather than requiring entire protocols to become permissioned, Token Extensions enable granular control over specific functionalities while preserving open access for compliant participants.

Benefits for Institutional Deployment: In the Solana ecosystem, Token Extensions may provide advantages including reduced development time through proven, audited components, universal compatibility across Solana applications, and precise implementation of specific regulatory requirements rather than broad, potentially inadequate solutions.

Implementation Challenges: Token Extensions are building blocks and their capabilities still need to be deployed by development teams who find it attractive (and also profitable) to issue tokens and build compliant decentralized infrastructure. Broad implementation would require clear demand signals from both regulators and communities of users that these configurations are acceptable for their purposes. This is another form of the chicken-or-egg challenge, particularly without regulatory clarity.

VI. Recommendations

A. For Financial Regulators: Enabling Innovation Within Regulatory Boundaries

Key Actions:

1. **Develop Blockchain Analytics Standards:** Building on recent initiatives, including the Basel Institute's blockchain analytics conference,[39] regulators should establish standardized approaches to transaction monitoring and risk assessment in DeFi environments. This includes certification programs for analytics providers and standardized risk scoring methodologies.
2. **Publish Guidance on Blockchain-based Compliance Tools:** Issue clear regulatory guidance stating that financial supervisors will consider innovative compliance approaches, including decentralized identity solutions and programmable compliance when evaluating institutional risk management programs. This guidance should specify acceptable implementation standards and audit requirements.
3. **Establish Risk Thresholds:** Define clear contamination thresholds (e.g., 0.5% illicit exposure) that institutions can use to assess DeFi protocol suitability. These thresholds should be based on empirical analysis of traditional financial system risk levels and updated regularly based on threat intelligence.
4. **Invest in Regulatory Infrastructure:** Develop government blockchain analytics capabilities enabling real-time oversight of DeFi activities. This includes training programs for regulatory staff and the acquisition of professional-grade analytics tools.
5. **Create Regulatory Sandboxes:** Establish safe harbor provisions enabling supervised experimentation with technology-native compliance approaches. These programs should include clear success metrics and pathways to full regulatory approval.

Rationale: In many cases, blockchain-based compliance support tools can achieve regulatory objectives more effectively than traditional methods in decentralized environments. Clear regulatory parameters enable innovation within boundaries while public infrastructure reduces adoption barriers. Experimentation programs inform evidence-based policy development while maintaining appropriate oversight.

B. For Financial Institutions: Strategic Preparation for DeFi Integration

Undertake DeFi Integration Case studies and Pilots: Financial institutions interested in accessing the benefits of DeFi functionality should participate in pilots involving blockchain-based compliance tools. The above technologies serve as an option set of approaches and tools that financial institutions may consider for DeFi integration pilots. There is not one

[39] "An approach to anti-money laundering compliance for cryptoassets." BIS Bulletin, 13 August 2025, https://www.bis.org/publ/bisbull111.pdf.

singular risk management methodology for interacting with DeFi, or even with CeFi.[40] Pilots should be determined by the precise type of DeFi service or activity engaged, the jurisdiction in which the regulated institution operates, and the assessed risks of the DeFi protocol itself. Rather than blanket prohibition or unrestricted access, institutions should consider nuanced approaches to integration that deploy and evaluate proofs-of-concept using the illicit finance risk management features mentioned above.

C. For Technology Providers: Building Compliance-Native Infrastructure

Develop Permissionless Blockchain Infrastructure with Intrinsic Compliance Optionality: The most popular Layer 1 (L1) blockchain protocols, Bitcoin and Ethereum, as well as almost all others, do not have intrinsic support for AML/CFT compliance in their architectures. The tools listed above can help to provide an environment more hospitable to financial institutions. However, blockchain developers can still build chains from the ground up that enable compliance functions. For example, some recent L1 blockchain networks are attempting to resolve the tensions between permissionless activity, private transactions, and illicit finance risk management by developing blockchains built on zero-knowledge proofs in order to enable compliant architectures more easily on their ecosystems. For example, the Aleo network–which is a privacy blockchain where transactions are confidential by default–has partnered with Predicate to establish a risk management architecture that can verify that funds from cross-chain bridges meet specific regulatory and security criteria before entering the Aleo network.[41]

VII. Conclusion: Toward Compliant DeFi Integration

The convergence of regulatory clarity in centralized crypto markets with DeFi's compelling operational advantages creates a unique moment for collaborative solution development. Traditional approaches attempting to retrofit intermediary-based regulation onto intermediary-less systems face fundamental limitations. However, blockchain-based solutions can support regulatory objectives while preserving DeFi's core benefits.

The path forward requires recognition that compliance in decentralized systems demands new approaches rather than forcing existing frameworks onto incompatible technologies. Advanced blockchain analytics, decentralized credentials, and programmable compliance, such as pre-transaction computation, privacy pools, and token extensions, demonstrate that sophisticated risk management is possible in DeFi environments.

[40] "Crypto Illicit Finance Risk Management Guide" Crypto Council for Innovation*,* 9 May 2024, https://cryptoforinnovation.org/crypto-illicit-finance-risk-management-guide/.

[41] "Aleo launches secure bridge framework with Predicate." Aleo, 19 February 2025, https://aleo.org/post/aleo-launches-secure-bridge-framework-with-predicate/.

Success depends on collaborative development across regulatory, institutional, and technological stakeholders. Regulators must provide clear guidance enabling innovation within appropriate boundaries. Financial institutions must invest in capability development and engage constructively in standard-setting processes. Technology providers must prioritize compliance integration and regulatory engagement.

The alternative—allowing DeFi to develop entirely outside regulatory frameworks—risks creating parallel financial systems beyond traditional oversight. Early action to develop compliance-compatible DeFi integration pathways can channel innovation toward positive outcomes while maintaining financial system integrity.

The technology exists today to enable compliant institutional DeFi participation. What remains is the collaborative will to implement these solutions at the scale and sophistication necessary to bridge traditional finance and decentralized infrastructure. The institutions and jurisdictions that act decisively in this window will shape the future of global financial infrastructure.

This moment represents more than technological innovation—it represents an opportunity to build more transparent, efficient, and inclusive financial systems while maintaining the oversight necessary to protect against illicit finance. The question is not whether institutional DeFi integration will occur, but whether it will develop through proactive collaboration or reactive regulatory response. The former path offers far better outcomes for all stakeholders involved.

Acknowledgements: The authors would like to thank Rashan Colbert for his helpful feedback on this paper and Téa Anderson, Maude Ashra, and David Vandivier for their review and edits.