Comment in Response to the U.S. Department of the Treasury's Advanced Notice of Proposed Rulemaking on the Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS) Act Implementation

Darrell Duffie, Odunayo Olowookere, and Andreas Veneris

Stanford York University University of Toronto

November 1, 2025

Abstract: This comment recommends the delineation of criteria for a voluntary heightened standard for privacy in compliant decentralized payment systems. The comment also explains how this standard could be met by relatively decentralized stablecoin payment systems that support compliance with regulations governing sanctions, Know Your Customer (KYC), Anti-Money Laundering (AML), and Countering the Financing of Terrorism (CFT). This can be achieved by embedding privacy-preserving compliance mechanisms directly into a stablecoin's distributed ledger.

This comment is in response to the Advanced Notice of Proposed Rulemaking: Guiding and Establishing National Innovation for U.S. Stablecoins Act Implementation, posted by the Department of the Treasury on Sep 19, 2025. Duffie: Stanford Business School (duffie@stanford.edu); Olowookere: Osgoode Hall Law School, York University (odunayoolowookere@osgoode.yorku.ca); Veneris: Department of Electrical and Computer Engineering, Department of Computer Science and Munk School of Global Affairs & Public Policy, University of Toronto (veneris@eecg.toronto.edu). This comment is based in part on "A Note on Privacy and Compliance for Stablecoins," by Darrell Duffie, Odunayo Olowookere and Andreas Veneris, Research Note, Graduate School of Business, Stanford University, May, 2025.

1 Introduction

In payment systems, especially those using blockchain networks, legal compliance and user privacy are often viewed as competing forces.[1] In particular, stablecoin payments are widely perceived as essentially private, pseudonymous, and a challenge to regulate. This comment responds to Section IV of the Advanced Notice of Proposed Rulemaking (ANPRM), and suggests how stablecoin payment systems can have a high degree of privacy and yet be consistent with regulations governing sanctions, Know Your Customer (KYC), Anti-Money Laundering (AML), and Countering the Financing of Terrorism (CFT). This can be achieved by embedding privacy-preserving compliance mechanisms directly into the stablecoin's distributed ledger, which could be permissioned or permissionless. We also propose that Treasury consider the promulgation of a voluntary heightened standard for the privacy of compliant stablecoin-based payment systems.

Among the specific technologies described in the GENIUS Act raised in Treasury's prior Request for Comment (RFC),[2] our comment addresses digital identity verification within the context of blockchain technology and transaction monitoring. With respect to stablecoin payment arrangements, our comment is relevant to the following specific concerns listed in the prior RFC: (i) "improvements in the ability of financial institutions to detect illicit activity involving digital assets," (ii) "the amount and sensitivity of information that is collected or reviewed"; (iii) "privacy risk associated with the information that is collected or reviewed"; (iv) "operational challenges and efficiency considerations"; and (v) "effectiveness of the methods, techniques, or strategies at mitigating illicit finance."

These issues are especially relevant for permissionless blockchains which, without design improvements, can become avenues for illicit activity but also offer limited user privacy (Cointelegraph, 2025). To address these concerns, we recommend that the Treasury Department establishes a *heightened standard for privacy* in compliant decentralized payment systems. While meeting such a heightened standard would be voluntary, the standard could

[1] See Norbu et al. (2024); Van Valkenburgh (2019); Flood et al. (2013).

[2] The ANPRM requests comments on topics raised in the ANPRM and in the prior RFC, writing "Treasury will consider comments submitted in response to either the RFC or this ANPRM, so commenters need not, and should not, resubmit any RFC comments in response to this ANPRM. In addition to topics addressed in the RFC, Treasury now requests comment on the following topics relating to illicit finance."

encourage private-sector service providers to offer customers greater privacy, while supporting compliance with payment regulations, including those in the Bank Secrecy Act (BSA).

The main pillar of such a voluntary standard would be minimal collection, storage, and disclosure of confidential user data. For example, as part of this standard, when onboarding users, payment service providers should collect or verify the existence of the minimal information necessary for AML/CFT and sanctions compliance and retain these data no longer than necessary. This could be enabled by pseudonymous user credentials, which allow the portability of credentials across multiple platforms while disclosing the user's underlying identity only when legally required (Podda et al., 2025).

Such a standard could be met with a *compliance-by-design* approach for stabelcoin payments. With this approach, before Alice can pay Bob, the underlying distributed ledger can require both to have blockchain-registered KYC certificates that protect their personally identifying information (PII). This ensures that Alice's and Bob's PII and transactions are not exposed unless embedded algorithmic compliance mechanisms flag their transaction as suspicious. In that case, Suspicious Activity Reports (SARs) can be automatically sent to the authorities. This compliance-by-design approach embeds compliance mechanisms directly into a stablecoin's distributed ledger architecture to effectively balance privacy and regulatory transparency.[3]

Once compliant stablecoin payment systems meeting a heightened standard of privacy are available, users may bifurcate into two classes. One class would include most large corporations, banks, governments, other "establishment" users, and some individuals who prefer that their stablecoin transactions data are not publicly revealed, even pseudonymously. The other class could consist of users who do not prioritize compliance and are not concerned about having their payments appear pseudonymously on publicly observable distributed ledgers. This class will likely continue to use stablecoin payment systems that expose information about their payments pseudonymously and may use or attempt to use stablecoins that are not compliant with the Genius Act, including with respect to AML/CFT. Stablecoin issuers and payment service providers might choose to compete for customers by opting for a high voluntary standard of privacy that is recognized by the

[3] See Pocher and Veneris (2022); Gross et al. (2022); Pauwels (2021).

Treasury Department and other regulators.

The remainder of this comment describes privacy-compliance tradeoffs in more detail and reviews technological advances that could enable the compliance-by-design approach that we have in mind.

2 Regulatory Challenges

The GENIUS Act brings stablecoin payment systems into the conventional compliance framework of the BSA.[4] While this provides greater legal clarity, there remain important sources of tension between compliance and privacy in existing decentralized payment systems. Traditional regulatory frameworks for sanctions, KYC, AML, and CFT intrinsically rely on centralized oversight. However, because many Decentralized Finance (DeFi) blockchain approaches are based on avoiding reliance on trusted third parties, the enforcement of legacy compliance rules has been fragmented and challenging (Hess, 2024). Stablecoin issuers such as Tether that are domiciled in more leniently regulated jurisdictions have obtained significant network scale advantages that inhibit the growth of stablecoins issued in more tightly regulated jurisdictions.[5]

In a DeFi setting, KYC is typically done at the fiat-currency on ramps and off ramps to the traditional financial system. However, when combined with sophisticated cryptographic tools like mixers, the cryptographically protected trail of transactions and user identities in a DeFi ecosystem complicates AML and CFT enforcement (U.S. Department of the Treasury, 2023). For example, the U.S. Fifth Circuit Court of Appeals recently found that existing US legislation does not give sufficient authority to the U.S. Treasury Department to stop the use of Tornado Cash for money laundering or other illegal purposes.[6]

Notably, DeFi stablecoins lack standardized methods for securely linking wallet addresses to verified identities, making it difficult to enforce KYC, AML, CFT, and sanctions across various platforms and protocols (IOSCO, 2023). Bad actors can use multiple wallets without meaningful oversight. In the world of crypto, it is often said that "You are what you know, not who you are" (Ledger, 2024).

[4] Crisanto et al. (2024) provides an overview of global stablecoin regulatory efforts.

[5] See The Wall Street Journal (2024a); Draganidis (2022).

[6] See Van (2024); Levy (2024) and the final ruling of the West Texas District Court.

Typical on-chain compliance mechanisms, such as blacklists and transaction monitoring, function *retroactively* and in some cases are not even enforced (Heimbach et al., 2023). In other words, illicit transactions can be executed before they are detected, despite the programmability and ledger transparency that are key features of decentralized systems.

Current on-chain compliance methods also have limited ability to prevent sophisticated money laundering tactics such as smurfing, layering, chain-hopping, mixing, and cross-chain laundering (U.S. Department of the Treasury, 2024). This is largely because current algorithmic compliance techniques are difficult and computationally costly to implement efficiently and proactively with decentralized smart contracts.[7] However, as described below, rapid ongoing advances in decentralized technology and automation through smart contracts has the potential to bring down

3 Balancing Privacy and Compliance

How can stablecoin payment systems effectively balance privacy and regulatory compliance?

At the level of individuals, "privacy" refers primarily to the protection of Personally Identifiable Information (PII), such as full names, home addresses, telephone numbers, and government-issued identifiers. For corporations and other institutional users, privacy priorities also include the confidentiality of transaction data such as payment amounts, time stamps, payment patterns, and counterparties (Chaum, 1985). Exposing such proprietary payment information can compromise a firm's competitive advantages and other strategic interests. In business sectors for which confidentiality is essential to meeting duties to clients or jurisdiction-specific data rules, maintaining privacy is also a baseline legal requirement.

The two largest stablecoin issuers, Tether (USDT) and Circle (USDC). are ostensibly "decentralized," but practically, they address compliance with traditional centralized methods such as by blacklisting non-compliant wallets and by conducting off-chain KYC checks (OneSafe, 2024). These methods are similar to legacy compliance operations. They involve extensive data collection and storage, often more than is strictly necessary, with compliance

[7] See Cheng et al. (2019); Haller et al. (2016).

monitoring occurring only retroactively[8] Over-collection, centralization, and ex-post supervision heighten privacy risks and leave gaps for regulatory arbitrage.[9]

Beyond these typical privacy risks, AML/CFT compliance in cross-border payments is further complicated by frameworks for data protection, privacy, and regulation that are not consistent across various jurisdictions. As the Financial Stability Board observes, fragmented supervision, divergent regulatory approaches, and stringent privacy regimes restrict or delay the exchange of customer and transaction data, making oversight of crypto-asset activities inconsistent and often incoherent (Cointelegraph, 2025). A central theme of our Comment is that a heightened standard of privacy for tasks involving *identification* and *credentialization* could reconcile the privacy inherent in stablecoin payments with the transparency required for compliance. To support regulatory interoperability without compromising user privacy, a heightened privacy standard should also remain compatible with diverse jurisdictional privacy frameworks (as ISO 20022-style messaging does).

We therefore believe it would be beneficial for Treasury to recommend a voluntary heightened standard for privacy in compliant decentralized payment systems. This standard would strike a much-needed balance between compliance and privacy by encouraging the design of systems in which regulatory assurances are embedded directly into decentralized payment processes. This approach ought not to be limited to any particular technology or architecture but should instead define functional outcomes that promote both verifiable compliance and strong user privacy protections. This also has the potential to create a *common benchmark* for regulated entities to compete "upward" by voluntary adoption of the standard.

In the context of stablecoin payments, the standard could be based on the following key principles:

- Limited data collection: personal information should be collected only once at the point of onboarding by accredited entities. This reduces unnecessary data exposure and duplication.

- Credentialization and encryption: sensitive user data should be encrypted and represented as verifiable credentials that permit compliance checks without the need to reveal underlying PII.

[8] See CoinSpeaker (2024); The Wall Street Journal (2024b).

[9] See Financial Stability Board (2021).

- Real-time ID verification: credential validity should be verified at the time of each transaction. This ensures *proactive* compliance.

- Lawful data disclosure: decryption or identity revelation should occur only through due legal process. This would maintain accountability and user trust – we touch upon this in a later section of the document.

- Accredited oversight: credential issuers and intermediaries should operate under clear accreditation and audit frameworks that ensure the integrity and revocability of credentials when necessary.

These principles are consistent with the AML/CFT obligations of the BSA, which requires financial services firms to maintain programs *reasonably designed* to ensure compliance, but to also include internal controls for detecting and reporting suspicious transactions. The BSA also mandates the development of a Customer Identification Program (CIP) that is sufficient to form a *reasonable belief* of each customer's true identity.[10] In the context of stablecoin payments, as envisioned under the GENIUS Act and the BSA, these provisions suggest that while PII must still be collected during onboarding, the subsequent usage, storage, and transmission of this information should be minimized through credentialization and encryption without weakening AML/CFT oversight. Under this prism, our proposed solution indeed provides a foundation for a compliance-by-design stablecoin payment system that protects confidentiality except as required by the law.

Consistent with this approach, a compliance-by-design stablecoin payment system could be based on a framework that contains the following two basic design elements.

A KYC perimeter:
As illustrated in Figure 1, in order to gain access to a compliance-by-design stablecoin ledger, Alice must first undergo KYC verification by a recognized authority, such as a regulated payment service provider. Upon successful verification, Alice receives a hashed KYC certificate that is stored on the same decentralized ledger that records stablecoin payment records. This brings Alice within the "KYC perimeter," allowing her to transact with other similarly KYC-ed users while keeping her PII private. Zero Knowledge Proofs (ZKPs) enable Alice to prove that she is KYC-compliant without

[10] See 31 U.S.C. § 5318(h)(1); 31 U.S.C. § 5318(l); 31 C.F.R. § 1020.220(a)(2).

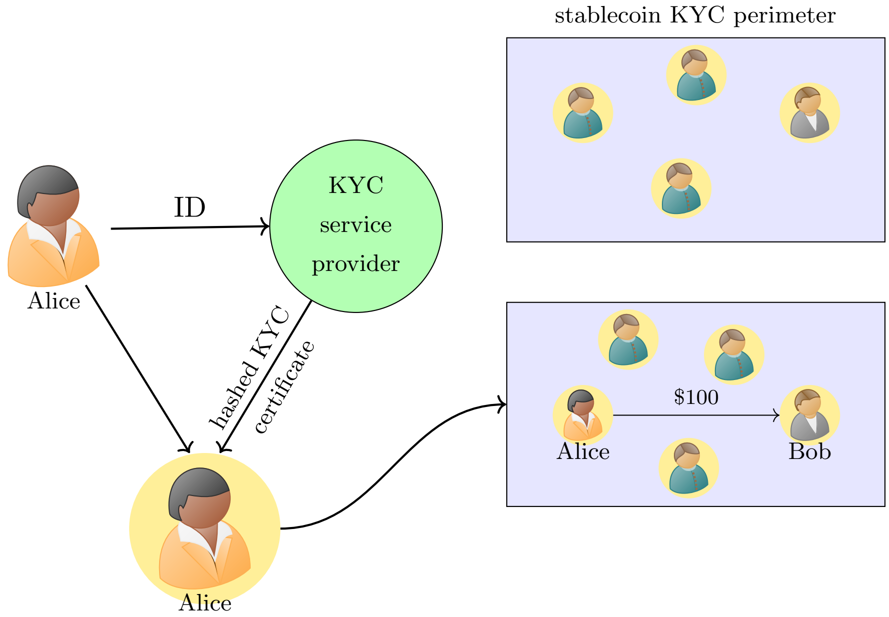

Figure 1: Alice can join the blue-shaded stablecoin KYC perimeter only after she obtains a hashed (cryptographically signed) KYC certificate from an authorized service provider, to whom she has provided necessary identity-proving documentation. Once Alice gets her KYC certificate, indicated by the addition of a gold background to her icon, she can join the KYC perimeter and pay Bob $100. Her KYC certificate is a zero-knowledge-proof that her identity has been verified; the certificate itself does not reveal her identity or its documentation with personally identifying information (PII).

revealing any of her private data. That is, both her PII and her transaction data remain inaccessible except as necessary to comply with regulation and law enforcement. For instance, the Financial Action Task Force (FATF) Travel Rule mandates that under certain conditions, a payee's Virtual Asset Service Provider (VASP) must receive specific identity information about the payor.

Embedded smart-contract suspicious activity reports:
In a compliance-by-design stablecoin payment system, AML, CFT, sanctions rules, and other payment regulations can be supervised by smart contracts that are embedded in the decentralized ledger on which payments are made. These smart contracts can classify transactions using algorithmic risk assessments and, when necessary, produce SARs for the relevant authorities.

These risk classifications could include:

- Whitelisted Transactions: These transactions involve verified, low-risk amounts and counterparties, requiring no additional scrutiny. Transactions in this category can proceed without triggering compliance checks by the smart contracts.
- Flagged Transactions: For transactions that trip risk indicators such as unusual payment patterns or large amounts, smart contracts can automatically generate SARs for review by the relevant authorities.
- Blacklisted Transactions: Transactions that involve sanctioned entities or known illicit actors, or violate established regulatory payment thresholds, can be automatically blocked. Smart contracts can generate alerts for the relevant authorities.

4 Implementation

The first element of the compliance-by-design framework, the KYC perimeter, could be implemented using recently proposed methodologies such as zkKYCs (Pauwels, 2021). This approach relies on a government agency or an authorized financial services firm to issue cryptographically protected verifiable credentials. The credential issuer stores user PII securely. Rather than embedding credentials into an on-chain token, users would maintain an encrypted version of their credentials in their private digital wallets. Attempts to avoid compliance by using multiple identities could potentially be blocked by anchoring verifiable credentials with standardized legal documents. (For individuals, these could be passports or driver's licenses.) Maintaining the integrity of the system over time requires a mechanism for revoking outdated or compromised credentials. For example, credential issuers could periodically publish Merkle trees[11] of current valid KYC certificates.

When a user initiates a payment, the user's wallet generates a zkKYC token that cryptographically proves the existence of the user's verifiable credentials, thus ensuring that the user has undergone a KYC check and belongs within the KYC perimeter. The zkKYC token also contains the transaction amount, the individual versus corporate status of the originating

[11] A Merkle tree is compact form of cryptographically signed records (Merkle, 1988).

wallet, and other necessary transaction data. Cryptography ensures that the token does not reveal the identity of the user or the transaction data to any third party, unless a SAR is triggered and a subsequent legal foundation for piercing the user's privacy is established.

Implementation of the second element of the compliance-by-design approach relies on ledger-embedded smart contracts to automatically generate SARs without unduly invading the privacy of compliant users. For this, a decentralized smart contract can analyze the encrypted information contained in zkKYC tokens for a match with specified SAR criteria. When the criteria are met, the smart contract can automatically generate a SAR. This introduces computational costs,[12] which might be covered in a compliance-as-a-service business model. For instance, regulated payment service providers could license and maintain compliance smart contracts. Users could allow some access to their payment data in exchange for compliance services, among other rewards. This approach might resemble some practices in the financial sector today, with the attendant privacy and other consumer-protection risks to be managed by regulation.

An approach would also be needed to determine whether an automated SAR meets the prima-facie legal standard for an enforcement authority to directly uncover the user's PII and transactions data, or the circumstances under which the SAR is the basis for the enforcement authority to seek or obtain a court order or warrant that permits the authority to uncover these private data. Addressing this complex legal question is beyond the goal of this Comment. Courts generally require a reasonable basis of suspicion, even for automated reporting systems, to justify further legal enforcement action.

With the approach taken by Pauwels (2021), a SAR would automatically reveal the underlying transaction data to the relevant enforcement authority, although without revealing user PII. To go further and obtain the PII, the authority would need to meet a threshold of sufficient evidence that the transactions are actually non-compliant. In that case, the authority could require the issuer of verifiable credentials to reveal the user's PII. It remains to determine probable-cause standards that would allow the authorities to obtain a warrant for this purpose. In the U.S., heavy use of SARs has

[12] Costs would include "gas" costs and the costs of decentralized computational storage demands that scale with the complexity of the underlying encoded compliance rules.

raised concerns over violations of 4th-Amendment constitutional privacy rights (Van Valkenburgh, 2019).

With the current state of decentralized programmable systems, the proposed smart-contract approach can efficiently handle only simple SAR criteria such as payment amounts exceeding a threshold and certain sequences of payments that signal surfing or layering.[13] In the last section of this note, we discuss opportunities to research and develop more complex forensic AML algorithms that might be able to handle the volume of transactions needed for a large and efficient payment system.

5 Other Approaches

For applications involving the settlement of financial transactions, among other settings that involve transfers of tokenized assets within closely defined groups, a broad KYC perimeter may lack the necessary ability to control the sharing of information. Canton Networks addresses this by allowing groups of market participants to establish controlled information sharing sub-networks in which[14]

> *"only parties permissioned to see data are in possession of it. Not only is this critical for participants in capital markets, but it also allows for regulators to be provisioned with a node that enables them to see transactions in real time—for example, transactions over ten thousand dollars–enabling more efficient and effective regulation. And transaction validation is always only between the parties to the transaction; there is never any need to rely on potentially unknown third parties and potentially uncertain consensus mechanisms for transaction validation (which could challenge transaction finality)"*

Taking another approach, Notabene (2024) achieves compliance with FATF's Travel Rule by facilitating secure identity sharing between Virtual Asset Service Providers (VASPs). Whereas a compliance-by-design approach integrates hashed KYC attestations directly on-chain, Notabene

[13] See Financial Crimes Enforcement Network (2024); Financial Action Task Force (2023).

[14] See Digital Asset (2025).

functions externally as an off-chain compliance network that enables VASPs to exchange verified identity information in a privacy-preserving manner. Notabene currently provides this service for Tether's USDT.

A related approach is ERC-3643, an Ethereum Improvement Proposal that meets the ERC 20 standard for Ethereum-compatible security tokens and tokenized assets (Tokeny, 2023). Although not designed exclusively for stablecoin payments, ERC-3643 builds in mechanisms by which a decentralized validator can control token transfers and require users to have an on-chain ID provided by a third-party authority. A key difference with a compliance-by-design approach is that ERC-3643 assigns AML and identity checks to proof-of-stake Ethereum validators. Historically, this approach has proven to be more centralized than initially advertised. In practice, ER-3643 compliance standards have not always been maintained by system validators (Heimbach et al., 2023). Further, the external trusted authorities that conduct off-chain KYC for the ERC-3643 standard are not necessarily regulated by official-sector agencies. A further key distinction is that a compliance-by-design framework uses ZKPs to protect the confidentiality of PII and transaction details unless on-the-fly embedded smart-contract compliance checks trigger a SAR. By contrast, ERC-3643 relies on KYC permissions provided by validators and does not address the protection of user PII and transactions data.

The HAL Privatbank approach developed by Gross et al. (2022) creates "privacy pools" that are protected by ZKPs. Once users of HAL Privatbank are KYC-ed, validators are able to process their cryptographically protected transactions without access to their information. As with our compliance-by-design approach, HAL Privatbank maintains the confidentiality of PII and payments while preserving regulatory compliance. HAL Privatbank users and their wallets are affiliated with the institution that issued their KYC-cleared wallets. Without anchoring KYCs on a common documentary standard, users could therefore create different wallets with different institutions, potentially leading to a fragmented compliance environment that could frustrate AML efforts. With HAL Privatbank, as with ERC-3643, AML compliance checks are done cryptographically by validators rather than "on the fly" by ledger-resident smart contracts. While this implies that HAL Privatbank could conduct more complex AML analysis than our compliance-by-design approach, it seems to rely heavily—as with ERC-3643—on the intentions of the system validators rather than embedded software that runs automatically.

6 Conclusions and Directions

The emergence of stablecoin payment systems has raised crtical tensions between privacy and regulatory compliance. This Comment suggests the delineation of criteria for a voluntary officially endorsed heightened standard of privacy for compliant decentralized payment systems. We also explain how such a standard might be met with a compliance-by-design approach that embeds privacy-preserving compliance mechanisms directly into the architecture of decentralized payment systems. A privacy-preserving KYC perimeter can be based on zero-knowledge KYC proofs that are embedded directly into the distributed ledger, along with automated AML-CFT-sanctions compliance checks.

Among the disadvantages of the compliance-by-design approach that we have outlined is the potential for fragmentation across digital infrastructure. A compliance-by-design KYC perimeter places a frictional envelope between authorized users and others. In order to interact within the KYC perimeter and also with the rest of the digital world, Alice would need to operate on multiple ledgers that may have limited interoperability. For example, to trade financial assets or to convert her stablecoins to other currencies, Alice would need to conduct an extra step. These sorts of frictions could perhaps be addressed by regulated cross-ledger service providers that rely on portable digital credentials.

Another concern is the limited practical computational capacity implied by current smart-contract methodologies. Over the past decade, applied cryptography has evolved to accommodate many of the premises of blockchain technology. We anticipate technology developments that will make more complex compliance techniques computationally feasible at scale while preserving identity privacy and payment confidentiality. Research may harness multi-party computation to this purpose. By distributing data, multiple actors, including smart contracts and system validators, can share the burden of generating complex SARs without the need to access the full underlying ledger of transactions. To that end, advances in data handling in decentralized networks, such as sharding and distributed cryptographic file sharing, are also expected to assist in supervising a broader range of

AML-CFT standards.[15] Threshold decryption and statistical methods such as k-anonymity could reduce the risk of linking anonymized data to identities.[16] Although these techniques currently involve significant computational burdens, on-going technical advances may soon make them practical for large-scale payment-system settings. Finally, hardware-based secure environments are also expected to improve the scalability of privacy-preserving smart-contract computation and enable more sophisticated SAR generation.[17] Among other challenges, ZKPs can expose users to manipulation risk, add to the complexity of auditing, and depend heavily on the reliability of external oracles (Duley et al., 2023).

We expect that decentralized private-sector blockchain compliance methods will evolve so as to attract a broad subset of users. This can be supported by voluntary official-sector compliance standards for user privacy. Ultimately, as history has shown with the mass adoption of internet applications over past decades, including this of peer-to-peer computation, many users will gravitate to systems that effectively balance privacy and regulatory compliance.

References

Van Loon, et al. v. Department of the Treasury, et al. *United States Court of Appeals for the Fifth Circuit*, 2024. Accessed: 2025-02-20.

Aleo. What is Aleo? The Privacy-First Blockchain. Online, 2024. URL `https://aleo.org/post/what-is-aleo-the-privacy-first-blockchain/`. Accessed: 2025-02-25.

Dan Boneh and Victor Shoup. *A Graduate Course in Applied Cryptography*. January 2023. Available online.

David Chaum. Security Without Identification: Transaction Systems to Make Big Brother Obsolete. *Communications of the ACM*, 28(10):1030–1044, 1985. doi: 10.1145/4372.4373. Accessed: 2025-06-12.

Raymond Cheng, Fan Zhang, Jernej Kos, Warren He, Nicholas Hynes, Noah Johnson, Ari Juels, Andrew Miller, and Dawn Song. Ekiden: A Platform

[15] See Nansen.ai (2024); ZachXBT (2024).

[16] See Boneh and Shoup (2023); Smart (2023); Ozdemir and Boneh (2022).

[17] See Aleo (2024); Cheng et al. (2019).

for Confidentiality-Preserving, Trustworthy, and Performant Smart Contracts. In *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 185–200. IEEE, 2019. doi: 10.1109/EuroSP.2019.00021. URL https://arxiv.org/pdf/1804.05141. Accessed: 2025-02-25.

CoinSpeaker. T3 Financial Crime Unit Freezes $100M Tether in Global Anti-Money Laundering Operation, 2024. Accessed: 2025-01-22.

Cointelegraph. Privacy Concerns Continue to Hinder Crypto Regulation, Says Financial Stability Board, 2025. Accessed: 2025-10-17.

Cointelegraph. Stablecoin or CBDC? Tether's Latest Freeze Adds Fuel to Decentralization Debate, July 2025. Accessed: 2025-08-29.

Juan Carlos Crisanto, Johannes Ehrentraud, and Denise Garcia Ocampo. Supervising Cryptoassets: Addressing Risks, Enhancing Resilience, 2024. URL https://www.bis.org/fsi/publ/insights57.pdf. Accessed: 2025-02-25.

Digital Asset. Letter to SEC Crypto Task Force, 2025.

Stelios Draganidis. Jurisdictional Arbitrage: Combatting an Inevitable By-Product of Cryptoasset Regulation. *Journal of Financial Regulation and Compliance*, 31(2):170–185, 2022. doi: 10.1108/jfrc-02-2022-0013.

Chanelle Duley, Leonardo Gambacorta, Rodney Garratt, and Priscilla Koo Wilkens. The Oracle Problem and the Future of DeFi, September 2023. URL https://www.bis.org/publ/bisbull76.pdf. BIS Bulletin No. 76, Accessed: 2025-04-24.

Financial Action Task Force. Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, 2023. Accessed: 2025-02-25.

Financial Crimes Enforcement Network. Money Services Business (MSB) Compliance Guide, 2024. Accessed: 2025-02-25.

Financial Stability Board. Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements: Final Report and High-Level Recommendations, 2021. Accessed: 2025-02-22.

Mark Flood, Jonathan Katz, Stephen Ong, and Adam Smith. Cryptography and the Economics of Supervisory Information: Balancing Transparency and Confidentiality. Working Paper 13-12, Federal Reserve Bank of Cleveland, September 2013. Accessed: 2025-01-22.

Jonas Gross, Johannes Sedlmeir, and Simon Seiter. How to Design a Compliant, Privacy-Preserving Fiat Stablecoin via Zero-Knowledge Proofs. Technical report, HAL Privatbank,, 2022. Accessed: 2025-01-20.

Armin Haller, Adrian Paschke, and Axel Polleres. Rule-Based Compliance Checking of Financial Transactions. In *Proceedings of the 10th International Web Rule Symposium (RuleML 2016)*. Springer, 2016. Accessed: 2025-02-22.

Lioba Heimbach, Lucianna Kiffer, Christof Ferreira Torres, and Roger Wattenhofer. Ethereum's Proposer-Builder Separation: Promises and Realities. *arXiv preprint arXiv:2305.19037*, 2023. Accessed: 2025-02-21.

Eric W. Hess. Bridging Policy and Practice: A Pragmatic Approach to Decentralized Finance, Risk, and Regulation. *Penn State Law Review*, 128(2):347–431, 2024. Accessed: 2025-02-20.

IOSCO. Policy Recommendations for Decentralized Finance (DeFi), 2023. Accessed: 2025-02-20.

Ledger. Not Your Keys, Not Your Coins: Why It Matters, 2024. Accessed: 2025-01-20.

Steven A. Levy. Van Loon v. Department of the Treasury – A Decision with Important Implications for Bitcoin. *Yale Journal on Regulation*, 2024. Accessed: 2025-02-20.

Ralph C. Merkle. A digital signature based on a conventional encryption function. In Carl Pomerance, editor, *Advances in Cryptology — CRYPTO '87*, pages 369–378, Berlin, Heidelberg, 1988. Springer Berlin Heidelberg. ISBN 978-3-540-48184-3.

Nansen.ai. Blockchain Analytics: The Ultimate Tool to Understanding Crypto, 2024. Accessed: 2025-01-22.

Tenzin Norbu, Jae Young Park, Kin Wai Wong, and Hao Cui. Factors Affecting Trust and Acceptance for Blockchain Adoption in Digital Payment Systems: A Systematic Review. *Future Internet*, 16(3):106, 2024. doi: 10.3390/fi16030106. Accessed: 2025-01-25.

Notabene. The State of Crypto Travel Rule Compliance Report 2024, 2024. Accessed: 2025-02-21.

OneSafe. Tether vs USDC: Transparency and Compliance Challenges, 2024. Accessed: 2025-02-20.

Ali Ozdemir and Dan Boneh. Experimenting with Collaborative zk-SNARKs: Zero-Knowledge Proofs for Distributed Secrets. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 4291–4308. USENIX Association, August 2022. Available online.

Pieter Pauwels. zkKYC: A Solution Concept for KYC Without Knowing Your Customer, Leveraging Self-Sovereign Identity and Zero-Knowledge Proofs. Cryptology ePrint Archive, Paper 2021/907, 2021.

Nadia Pocher and Andreas Veneris. Privacy and Transparency in CBDCs: A Regulation-by-Design AML/CFT Scheme. *IEEE Transactions on Network and Service Management*, 19(2):1776–1788, 2022. doi: 10.1109/TNSM.2021.3136984. Accessed: 2025-01-25.

Emanuela Podda, Pol Hölzmer, Alexandre Amard, Johannes Sedlmeir, and Gilbert Fridgen. The impact of zero-knowledge proofs on data minimisation compliance of digital identity wallets. *Internet Policy Review*, 14(3), 2025. doi: 10.14763/2025.3.2019.

Nigel P. Smart. Practical and efficient fhe-based mpc. In *19th IMA International Conference on Cryptography and Coding*, pages 263–283, December 2023.

The Wall Street Journal. Who Is Giancarlo Devasini? The Secretive Billionaire Behind Tether and the Rivalry with Circle's Jeremy Allaire, 2024a. Accessed: 2025-02-24.

The Wall Street Journal. Federal Investigators Probe Cryptocurrency Firm Tether, 2024b. Accessed: 2025-01-20.

Solutions Tokeny. ERC-3643 Whitepaper: T-REX Standard v4. Technical report, Tokeny Solutions, 2023. Accessed: 2025-01-22.

U.S. Department of the Treasury. Illicit Finance Risk Assessment. Technical report, US Treasury Department, Washington DC, April, 2023.

U.S. Department of the Treasury. 2024 National Money Laundering Risk Assessment, 2024. Accessed: 2025-01-22.

Peter Van Valkenburgh. Electronic Cash, Decentralized Exchange, and the Constitution. Coin Center, March, 2019.

ZachXBT. Warpcast Profile - ZachXBT, 2024. Accessed: 2025-01-21.