A Note on Privacy and Compliance for Stablecoins

Darrell Duffie, Odunayo Olowookere, and Andreas Veneris
Stanford York University University of Toronto

May 8, 2025

Abstract: This note explains how modern 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 goal can be achieved by embedding privacy-preserving compliance mechanisms directly into the stablecoin's distributed ledger.

Keywords: Payment systems, blockchain, stablecoins, privacy, AML/CFT compliance.

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 and the Department of Computer Science, University of Toronto (veneris@eecg.toronto.edu). We are extremely grateful to Dan Awrey, Joe Grundfest, Gordon Liao, Tim Massad, Tony McLaughlin, Dinesh Shah, Rakesh Arora, Kelly Mathieson, Bill Nelson, Paige Paridon, Manoj Ramia, Don Wilson, and Pete Zimmerman for helpful reactions to an initial draft, and to Srisht Fateh Singh for his useful input on various technical items.

1 Introduction

In payment systems, particularly 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. In this note we explain 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. Before Alice can pay Bob, the 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 transaction are not exposed unless embedded algorithmic smart-contract compliance mechanisms flag their transaction as suspicious. In that case, the smart contracts can automatically send Suspicious Activity Reports (SARs) to the authorities.

This *compliance-by-design* approach embeds compliance mechanisms directly into the distributed ledger architecture to effectively balance privacy and regulatory transparency.[2] Once this approach is available, users may bifurcate into two different classes. In one class, most large corporations, banks, governments, other "establishment" users, and some individuals will insist that their stablecoin transactions data are not publicly revealed, even pseudonymously. The other class will consist of users who do not prioritize compliance (or wish to avoid 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 not be fully compliant with established AML/CFT and privacy regulatory frameworks.

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

[1] See Norbu et al. (2024); Van Valkenburgh (2019); Flood et al. (2013).
[2] See Pocher and Veneris (2022); Gross et al. (2022); Pauwels (2021).

2 Regulatory Challenges

The United States Congress is considering legislation that would attempt to integrate stablecoins into the conventional financial-compliance framework of the the Bank Secrecy Act.[3] The European Union's recent Markets in Crypto-Assets Regulation (MiCA) regulates stablecoins under a broader framework. Stablecoins that are said to lack MiCA compliance, such as Tether (USDT) and PayPal's PYUSD, face delisting from European exchanges.[4] The Hong Kong Monetary Authority published a consultation paper and a regulatory proposal for stablecoin issuers.[5] Crisanto et al. (2024) provides an overview of global stablecoin regulatory efforts.

While these efforts to regulate stablecoins are establishing some legal clarity, they have not yet effectively addressed the key sources of tension between compliance and privacy in existing decentralized systems. Traditional regulatory frameworks for sanctions, KYC, AML, and CFT 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).

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]

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 juris-

[3] See U.S. House Committee on Financial Services (2024) and Massad (2025) for an evaluation. The draft legislation includes the GENIUS Act 2025 (Senate; Scott, Hagerty, Lummis, Gillibrand) and the STABLE Act (House; Hill and Steil).

[4] See CoinDesk (2025).

[5] See Reuters (2025); Animoca Brands (2024).

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

dictions.[7]

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.[8]

Finally, DeFi stablecoins lack standardized methods for securely linking wallet addresses to verified identities, making it difficult to enforce KYC, AML, and CFT 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).

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. 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).

[7] See The Wall Street Journal (2024a); Draganidis (2022).
[8] See Cheng et al. (2019); Haller et al. (2016).

are ostensibly "decentralized," but actually address compliance with centralized methods for blacklisting non-compliant wallets and conducting off-chain KYC checks (OneSafe, 2024). These methods typically rely on external supervision tools and some form of centralized storage or control of user data. Moreover, compliance supervision is often retroactive.[9] These practices risk privacy and are exposed to regulatory arbitrage.[10]

As an alternative, a compliance-by-design stablecoin payment system that protects confidentiality except as required by law 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 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. Trans-

[9] See CoinSpeaker (2024); The Wall Street Journal (2024b).
[10] See Financial Stability Board (2021).

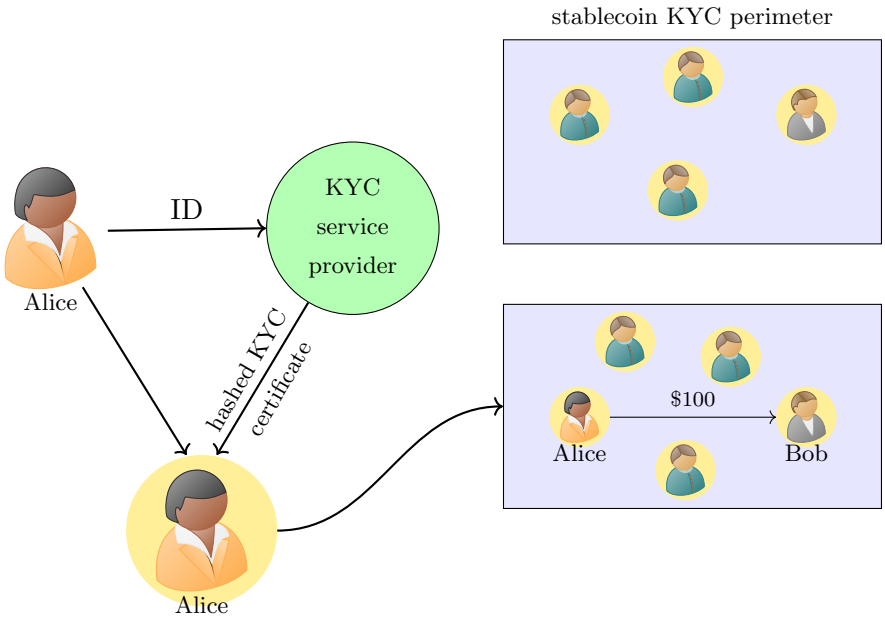

Figure 1: Alice can join the blue-shaded stablecoin KYC perimeter only after she obtains a hashed (cryptographically signed) KYC certificate from an authorized service provider, to whom she has provided necessary identity-proving documentation. Once Alice gets her KYC certificate, indicated by the addition 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).

actions 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 drivers 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 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 com-

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

[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.

pliance 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 Note. 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 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

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

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 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

[14] See Digital Asset (2025).

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 notable tensions between privacy and regulatory compliance. This note posits a compliance-by-design approach that embeds privacy-preserving compliance mechanisms directly into the stablecoin's distributed ledger, with a privacy-preserving KYC perimeter based on zero-knowledge proofs, and with AML checks and reports executed automatically by ledger-embedded smart contracts.

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.

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. Hence, we anticipate that new developments will soon 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] However, as these systems evolve, it is important to acknowledge their challenges that come with them. In particular, ZKPs arrive with trade-offs: they can obscure systemic risks, introduce layers of complexity in auditing, and depend heavily on the reliability of external oracles (Duley et al., 2023). These vulnerabilities merit closer investigation.

We expect that decentralized private-sector blockchain compliance methods will evolve so as to attract a broad subset of users by meeting official-sector compliance standards while protecting user privacy for legal payments. Ultimately, as history has shown with the mass adoption of internet applications over past decades, many users will gravitate to systems that effectively balance privacy and regulatory compliance.

[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).

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.

Animoca Brands. Standard Chartered, Animoca Brands, and HKT Establish Joint Venture to Issue HKD-backed Stablecoin, 2024. Accessed: 2025-04-25.

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

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

CoinDesk. Crypto.com Will Suspend Tether, PayPal Stablecoin Services in Europe Due to MiCA, 2025. Accessed: 2025-01-25.

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

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.

Timothy Massad. Testimony before the U.S. House Committee on Financial Services, February 2025. Accessed: 2025-04-25.

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.

Reuters. AnchorX Receives Approval to Issue CNH-Pegged Stablecoins in Kazakhstan, February 2025. Accessed: 2025-02-24.

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.

U.S. House Committee on Financial Services. Hearing: Oversight of Stablecoins: Identifying Risks and Ensuring Stability, 2024. Accessed: 2025-01-20.

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

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