THE STABLECOIN BALANCING ACT

Darrell Duffie, Odunayo Olowookere, and Andreas Veneris

Fighting financial crime doesn't have to come at the cost of privacy

Legend has it that gangster Al Capone hid the illicit origins of his wealth by using laundromats as a front. Ever since, authorities have worked to track and seize "laundered" money from criminals and, more recently, terrorists.

These efforts are even trickier today because of digital assets such as stablecoins, which can be washed through many accounts beyond the reach of law enforcement. But the need to stop bad actors must not trammel the privacy rights of law-abiding people nor the efficient processing of billions of dollars in payments and transfers every day.

These goals may seem unreachable, but we argue that technology may actually make this objective feasible.

"Smart-compliant" payment systems that fight crime, protect privacy, and work efficiently are within reach. These systems can be built directly into the blockchains of stablecoins—digital assets pegged to traditional money.

How would this work in practice? Say Alice wants to pay Bob. Once she taps "send" in her phone app, previous verification of their identities is confirmed, the transaction is reviewed by a decentralized algorithm for suspicious activity, and the operation is completed—all on a blockchain. Flagged transactions would automatically be reported to law enforcement. The identities of Alice and Bob, however, could be unmasked only with a warrant or through another legal process.

With anticipated advances in technology, this compliance-by-design vision *could become* a practical *reality* for large-scale payment systems.

Illustration by Jasu Hu

Balancing privacy and transparency

New attempts at regulating blockchain-based finance do not resolve the fundamental tension between the protection of privacy and legal compliance. In payment systems, compliance and privacy are traditionally competing forces. Stablecoin payment systems exemplify this tension. But they may also offer a natural compromise since their decentralized and programmable architecture allows compliance mechanisms to be built in, and their pseudonymity helps keep privacy risks low.

This article explains how a "compliance-by-design" approach (Duffie, Olowookere, and Veneris 2025) could make it possible for decentralized stablecoin payment systems to protect privacy and enforce anti–money laundering (AML) and countering the financing of terrorism (CFT) regulations and sanctions. Compliance enforcement would take place as transactions occur, based on predefined criteria and risk indicators, instead of reactively, as is the case today. This approach is in line with the 2023 IMF–Financial Stability Board policy framework for crypto assets, which calls for compliance measures for stablecoin providers.

In such an environment, stablecoin users are likely to split into two groups. If institutions and individuals value both compliance and confidentiality, they are likely to select a compliance-by-design payment network. Others may continue using legacy approaches to stablecoin payments that are based on pseudonymity and relatively loose compliance constraints.

Before going deeper, let's define privacy interests in the context of stablecoin payments. For individuals, a major concern is the protection of personal information, including names, home addresses, and phone numbers. For corporations and institutions, privacy concerns may include transaction metadata—such as amounts, time stamps, patterns, and counterparties—which may be commercially sensitive. For businesses, maintaining confidentiality is not only strategically important, it is often also a legal requirement.

Compliance involves know-your-customer (KYC) standards and monitoring of payments for illegal activity. Currently, stablecoin providers delegate compliance tasks to centralized exchanges and other custodians that provide on-ramps and off-ramps for conversion between stablecoins and traditional currencies.

However, the ability to mint stablecoins and move them between multiple accounts with decentralized protocols, and the availability of "mixers" that obscure the trail of any single coin, makes it relatively easy to obscure transactions. Law enforcement has limited reach and is often reactive, triggered only after suspicious activity is detected. As a result, compliance with AML, CFT, and sanctions frameworks is relatively ineffective. Moreover, compliant users' privacy is limited because payments are publicly observable and transparently linked to the user's pseudonym.

Reconciling privacy standards with regulatory compliance calls for a model that better protects user data while reasonably enforcing the law. This requires a way to verify identities without exposing them.

Verification without exposure

In a compliance-by-design decentralized payment system, before Alice can pay Bob, both must have undergone identity verification by a licensed provider of such services (subsequently referred to as a credential issuer), as illustrated in Chart 1. Verification places Alice and Bob within the KYC perimeter of their chosen decentralized payment system. This verification is stored on the payment-system ledger as a "hashed" (cryptographically masked) certificate.

At this point, zero-knowledge proofs (ZKPs) come into play. These are cryptographic tools that can be implemented in a multiuser software platform, allowing a user to prove something without revealing what that something is. For example, a ZKP can establish which poker hand wins without revealing the cards of that player.

Likewise, ZKPs can allow users of a decentralized payment system to demonstrate know-your-customer compliance without revealing their personal data. It works by ensuring that each transaction that users initiate includes a ZKP proof of their eligibility to be inside the KYC perimeter of the payment system—without revealing their identity or any other underlying personal information.

This approach could be used in any decentralized payment system, in particular a system based on stablecoins. In principle, the same approach could be applied to decentralized payment systems based on central bank digital currencies and other digital representations of money.

Privacy is preserved unless specific risk indicators, such as unusual transaction patterns, transfers exceeding designated thresholds, or links to known high-risk wallets, are detected. Smart contracts embedded in the ledger monitor for these red flags. Smart contracts are automated software modules that enforce agreements on the ledger network without needing a middleman. When sufficiently suspicious activity is detected, the smart contracts generate suspicious activity reports (SARs) that are forwarded to regulatory authorities. Access by the authorities to underlying sensitive user data beyond that point follows a legal process that

depends on the jurisdiction, potentially involving court applications and procedures for warrants or administrative subpoenas.

This model enables layered detection and oversight. White-listed transactions (routine transfers between known parties) proceed seamlessly. Flagged transactions may be delayed or trigger automated SARs, and high-risk transfers involving known offenders may be blocked. These responses are enforced through smart contracts that can be dynamically updated to reflect evolving regulatory priorities, special cases, and insights obtained from the statistical analysis of payment patterns.

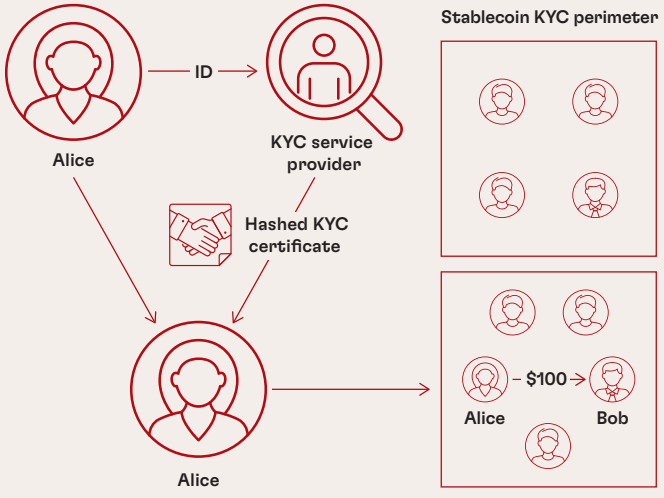
The KYC credential maintained by issuers secures databases of validated user credentials and allows them to be updated or revoked when compromised. If Alice's legal status changes—for example, as a result of a sanction—her compliance proof would fail and her transactions within the KYC perimeter would be blocked.

The stablecoin payment system we have described replaces time-consuming "off-chain" manual reactive reviews—common practice today—with proactive real-time "on-chain" algorithmic supervision. By leveraging smart contracts to apply compliance rules as transactions occur, this framework taps directly into the strengths of blockchain systems.

CHART 1

KYC for stablecoins

Alice joins the KYC perimeter after obtaining a hashed certificate from an authorized service provider.



SOURCE: Duffie, Olowookere, and Veneris 2025.
NOTE: ID = identification; KYC = know your customer.

Implementation

The KYC perimeter could be implemented using zero-knowledge KYCs (zkKYCs) (Pauwels 2021), which combine zero-knowledge proofs with selective disclosure. For example, Alice can prove that she meets specific identity checks (like being over 18) without revealing her age. Under this approach, a government agency or authorized financial institution issues Alice a verifiable credential derived from her official or government-issued identity documentation. A cryptographically protected version of this credential is stored in each user's private digital wallet.

During a transaction, a zkKYC token generated from this credential is embedded on-chain. This token proves KYC compliance without revealing user identities, and the underlying credentials remain securely off-chain with the credential issuer. For payments by natural persons, such as peer-to-peer or customer-to-business payments, identity spoofing can be mitigated by anchoring verifiable credentials to standardized legal documents such as passports or driver's licenses.

For example, when Alice initiates a payment to Bob, her wallet generates a zkKYC token that cryptographically proves that Alice has a verifiable credential. The token confirms that Alice has undergone KYC certification and belongs within the KYC perimeter. The token also indicates whether Alice is an individual or an institution and confirms the transaction amount, wallet thresholds, and other relevant data. This token need not reveal Alice's identity or transaction details to Bob or any third party unless Alice agrees, or unless a SAR is triggered and a legal basis for disclosure is established.

Automated compliance enforcement relies on ledger-embedded smart contracts that analyze encrypted information contained in zkKYC tokens for a match with specified SAR criteria. If a match is found, the contract automatically generates a SAR, allowing enforcement without significantly compromising the privacy of compliant users.

Technological and systemic challenges

Compliance by design offers a promising path forward but is not a silver bullet. The approach we have outlined involves a significant computational burden for a large-scale modern payment system. Smart contracts must be capable of interpreting complex and evolving regulations at a throughput rate that allows close-to-real-time payments. Going instead for a very simplistic approach could generate many false-positive and false-negative compli-

"Stablecoins hold significant promise for improving financial inclusion and the efficiency of payment systems. But they need to reach a much better balance between privacy and compliance."

ance checks, overwhelming enforcement authorities with noise and risking exploitation by bad actors.

Another challenge is the computational cost of privacy-preserving mechanisms, risking delays during peak-payment periods. Compliance-by-design payment systems may also add frictional costs and delays to moving funds between different payment systems.

One solution to the computational burden problem would be to allow regulated providers to license and manage smart contracts, providing compliance as a service. With this setup, users could grant limited access to their payment data in exchange for compliance services and other benefits, mirroring how privacy and consumer risk are managed by private firms today.

Further, as applied cryptography remains a fast-evolving field, new zero-knowledge-proof implementation promises to be faster. And new techniques, like multiparty computation, may help with the computational burden of administering smart contracts.

The road ahead

The compliance-by-design model presented here relies on sound governance. Establishing a trusted ecosystem of credential issuers is critical. Credential issuers and smart contract operators must be carefully licensed and must operate transparently and with accountability. Governments, banks, and certified financial technology firms could be the trusted nodes that anchor users to the compliance perimeter. Trusted credential issuers must follow uniform standards for KYC verification, and their verification should be interoperable across multiple ledgers. As with conventional payment systems, system-wide compliance quality hinges on the least rigorous credential issuers.

Laws may need to be adapted or applied in new ways. What justifies triggering a SAR? Under what conditions may authorities unmask a user's identity? Different jurisdictions would likely set distinct due-process thresholds. One country might require only administrative subpoenas while another demands judicial warrants.

Effective cross-border enforcement of compliance relies on cross-jurisdictional cooperation, as is true of conventional correspondent banking today. For example, Project Mandala is a proposal by the Bank for International Settlements for a compliance-by-design approach to coordinating compliance checks by banks and other financial institutions involved in cross-border payments. Analogous to the stablecoin compliance-by-design approach we have described, Project Mandala uses zero-knowledge proofs to establish the validity of a bank's compliance statement without the need to share that bank's compliance-related data with other banks involved in the payment.

We do not propose that stablecoin payment systems be required to adopt a compliance-by-design approach. In fact, even if some countries were to impose this approach as a regulatory requirement, it would be challenging to block domestic access to alternative offshore stablecoin systems that do not take this approach to privacy and compliance.

Stablecoins hold significant promise for improving financial inclusion and the efficiency of payment systems—and making life harder on modern-day Al Capones. But they need to reach a much better balance between privacy and compliance. The compliance-by-design approach we have outlined is one way to do that. F&D

DARRELL DUFFIE *is the Adams Distinguished Professor of Management and professor of finance at Stanford University's Graduate School of Business.* **ODUNAYO OLOWOOKERE** *is a doctoral student at York University's Osgoode Hall Law School.* **ANDREAS VENERIS** *is a professor at the University of Toronto's Department of Electrical and Computer Engineering and the Munk School of Global Affairs and Public Policy.*

REFERENCES

Bank for International Settlements. 2024. "Project Mandala: Streamlining Cross-Border Transaction Compliance". Basel.

Duffie, D., O. Olowookere, and A. Veneris. 2025. "A Note on Privacy and Compliance for Stablecoins." SSRN Working Paper. https://dx.doi.org/10.2139/ssrn.5242230.

International Monetary Fund–Financial Stability Board. 2023. "IMF-FSB Synthesis Paper: Policies for Crypto-Assets." Basel.

Pauwels, P. 2021. "zkKYC: A Solution Concept for KYC without Knowing Your Customer—Leveraging Self-Sovereign Identity and Zero-Knowledge Proofs." IACR Cryptology ePrint Archive.