Beyond Detection: A Privacy-Preserving Framework for Proactive Digital-Asset Compliance

Response to Treasury RFC on Innovative Methods to Detect Illicit Activity Involving Digital Assets, Question 6: Other Innovative Technologies

Joss Duff, Lehigh University (jod323@lehigh.edu)
Henry F. Korth, Lehigh University (hfk2@lehigh.edu)
Lab: https://blockchain.cse.lehigh.edu/

Much of the RFC addresses detection of illicit actions. We would like to bring attention to technology that enables law-abiding entities to be able to prove compliance in an efficient and transparent manner. This not only creates broad public confidence in those entities but also allows enforcement efforts to be targeted towards those entities that cannot or will not demonstrate compliance. Here, we shall summarize a novel and highly promising approach under development at Lehigh University that fundamentally shifts the compliance paradigm from reactive detection to proactive verification. This technology applies broadly to blockchain transactions, but is particularly applicable in stablecoin systems where users have some reasonable expectation of privacy yet there is also a compelling need to ensure regulatory compliance.

Privacy and Compliance Problem

Stablecoin payment systems are public by default because transactions on a layer-1 (L1) blockchain are indeed public. Wallet addresses can be tied to corporations or individuals relatively easily. Participants in a transaction learn each-others' addresses and can then not only see all past transactions by their business partner, but also monitor all future ones. For a consumer, this means that sharing the cost of a take-out meal with a neighbor results in full financial disclosure. Such a lack of privacy is clearly unacceptable and, without mitigation, would limit the appeal of stablecoin payment systems despite their many advantages.

Current approaches to blockchain compliance face an inherent contradiction: privacy requires that only the individual knows certain information, while compliance traditionally requires revealing information to prove compliance criteria. This tension has led to two unsatisfactory outcomes:

1. Privacy systems without compliance attract illicit actors and face legal challenges
2. Compliance systems without privacy expose all transaction histories publicly, making them unacceptable for consumer and commercial adoption

The GENIUS Act's passage has positioned the United States to lead in stablecoin regulation. However, without privacy protections comparable to traditional banking, stablecoin adoption will remain limited despite clear advantages in transaction speed and cost. Our framework resolves this by enabling both privacy and compliance simultaneously.

Enabling Proactive Compliance: A Privacy-Preserving Framework for Digital Asset Regulation

We propose an open framework where regulatory bodies publish compliance requirements, applications require users to prove they meet those requirements, and users generate cryptographic proofs demonstrating compliance, all without revealing private information. Users who don't meet the compliance requirements are unable to interact with the compliant application.

Components:

1. Regulators publish compliance definitions as logical rules over blockchain data (e.g., "address not on sanction list," "funds from KYC'd exchange," "no transaction structuring patterns")

2. Applications select relevant compliance definitions based on their regulatory obligations.

3. Users generate Zero Knowledge proofs[1], demonstrating they meet requirements without revealing transaction histories, balances, or counterparties

4. Applications verify proofs on-chain before allowing transactions, preventing non-compliant activity cryptographically rather than detecting it afterward

Compliance definitions

Regulators construct definitions of compliance over on-chain data using a human readable syntax that can be compiled into a Zero Knowledge circuit. Regulators then publish this definition to a public repository or database and sign it for authenticity.

We refer to the building blocks of compliance definitions as "constraints". Each constraint is a logical statement over on-chain or regulator provided data. For example, a sanctions list constraint: $C\_sanction = (sender(txn) \notin A, B\_current)$. That is read as: "The sender of this transaction does not exist in the sanction list A, evaluated at the current block". The sanction list A is provided by the regulatory authority and can be updated frequently.

[1] Zero Knowledge proofs are a cryptographic technique that allows one party (the "prover") to prove correct execution of a computation to another party (the "verifier"), without revealing the entire computation or any private inputs.

Compliance definitions will not be written as raw logic constraints like above. We are working on a human readable intermediary syntax that complies down into constraints.

This constraint system allows us to rigorously prove the soundness of a compliance definition and also intelligently minimize the amount of computation necessary to generate a Zero Knowledge proof of a compliance definition.

Our framework accounts for not only frequent updates of compliance variables, like sanctions lists, but it also allows for updates to the required constraints for any compliance definition. This accounts for regulations changing over time.

Concrete Example

The three requirements listed are for example purposes only. This framework does not have an upper limit of compliance requirements in a definition, and compliance definitions can be constructed over any on-chain data.

A U.S.-based stablecoin issuer requires users prove they:

1. Are not on OFAC sanctions lists
2. Completed KYC with an approved exchange
3. Have not structured transactions to evade reporting requirements

Users generate a single Zero Knowledge proof satisfying all three constraints. The stablecoin contract verifies this proof on-chain in constant time (regardless of constraint complexity) without learning the user's transaction history, balance, or counterparties. The proof is mathematically irrefutable yet reveals nothing beyond compliance with the specified requirements.

Costs

When using SNARK Zero Knowledge proof systems, *verification* of a proof has constant on-chain computational cost regardless of compliance definition complexity. This cost is paid by users on their first interaction with the protocol to ensure compliance. Those submitting a transaction bear the computational cost of constructing the needed proofs. Separate from user cost is the effort needed for the careful construction of compliance definitions over on-chain data, and designing applications that integrate a requirement that a valid Zero Knowledge proof be submitted by their users.

The application requirement is a one time development/deployment cost. After the change to require proofs is made, it is guaranteed that all future users of the application are compliant. The compliance-definition author, often a regulatory body or blockchain-analytics company, has the ongoing responsibility of updating the compliance definition to ensure it accurately reflects current regulatory requirements, such as updating sanctions lists or adding new constraints.

Open Framework Approach

The distinguishing feature of our proposal relative to other work in this space is that it defines an open framework for use by players in a competitive ecosystem. It is not a new blockchain. We are not proposing to operate our own payment system. Rather, we are creating a framework for established and new-entrant financial providers to take advantage of the power of the emerging stablecoin ecosystem by leveraging the features of our framework. This openness is not only a feature applicable to service providers. Our framework is unique in its provision of a standard means for regulators to publish requirements openly in a way that enables proof of compliance. Regulation based on constraints and proofs is valuable not only to service providers but also to regulators and to users. Regulators can check compliance by verification of proofs, which is much more efficient than having to evaluate full execution histories. Users can show transparently that they are in compliance without having to reveal private data.

Because compliance constraints pertain to transactions and transaction histories and not to specific proprietary features of a particular blockchain, our framework enables interoperability across platforms that use our framework. This facilitates a competitive stablecoin ecosystem in which each member of the ecosystem shares a common foundation of privacy and compliance guarantees.