Asset Tokenization & Smart-Contract Compliance

KYC/AML retaining DeFi

Pattas Panagiotis-MFT2510

Principles of Financial Technology
University of Piraues

January 21, 2026

Main Subjects of the Presentation

1. What is asset tokenization and why it matters
2. Compliance risks associated with the process(legal, operational)
3. How to mitigate risks and retain the DeFi characteristic (KYC,AML,Zero-Knowledge Proofs)

1) What is Asset Tokenization?

- Creating and recording an Asset (tangible or intangible) -or a claim on it- into a digital token by using a programmable ledger(e.g Blockchain platform).These tokens are primarly created through a type of Initial Coin Offering, referred as Security Token Offering (STO).
- These newly created Tokens can represent:
  - **Ownership** (e.g., shares, funds, real estate fractions)
  - **Claims/rights** (e.g., debt instruments, revenue rights)
- Difference between the Tokenization and conventional systems:
  - **Proof of Value** : Tokens provide evidence or verifications that an asset has a certain value or uniqueness.
  - **Proof of Ownership** : There is an establishment of unambiguous ownership of the asset
  - **Proof of Transaction** : Once the token is on the programmable ledger and is being traded on the market there is always a verifiable record to provide the transactions history and evidence of settlements.

What is Asset Tokenization -Cont'd

- Types of Tokens :
  - **Native Tokens** : Are issued and exist entirely on on-chain.Their value depends on the network/protocol itself and they don't need to have references to the off-chain counterparts.Well implementation can lead to minimal operational burdens and liquidity risks; in contrast technology and governance risks also increase as the asset can exhibit bearer like characteristics.
  - **Backed Tokens** : Are on-chain token representations of off-chain real world assets (RWAs) or claims/ownerships.This can accelerate asset mobility on the markets via the non-stop on chain trading and settlements.
- Core Token Attributes:
  1. **Asset Definition** : Clear declaration of the underlying asset's type.
  2. **Embedded Legal Rights**: Holds details about legal & economic entitlements of the owner.
  3. **Provenance** : Transparent,auditable record of the token's origin,transaction history etc.
  4. **Ownership Status**
  5. **Permission Controls**: Through Smart Contracts(SC) there are sets of predetermined rules,permissions on the usage of the token.
  6. **Compliance Rules**: Again via SC there can be the encoding of regulatory & compliance requirements in the token's body.

Value and Benefits of Tokenization in Financial Markets

- **Operational Efficiency/Automation:** Due to the structure of Smart Contracts procedures like issuance,settlement,corporate actions,reporting etc. are being automated.Hence,they are faster with less operational costs and intermediaries.
- **Transparency & Auditability:** Their programmability alongside with the Shared System of Record via the cryptographic Proof of State can provide Information Symmetry and Immutability thus leading to a more precise auditing and visibility of the transcactions record.
- **Composability:** Multi-asset operations interact with on-chain lending,collateral and primitives.This enhances Collateral Mobility,Multi-Asset Coordination and Asset Fungibility.
- **Asset Fractionalization:** Any asset can be splitted into smaller units with this resulting into lowering the trading barries and providing better liquidation to more hard movable,complex assets by softening down their administrative burdens.

2) Compliance Problems & Dangers

Core Mechanism of the Problems and Dangers

Todays, Regulated finance needs **identity, monitoring, and accountability**
Tokenization of Assets via Smart Contracts on blockchain platforms are mainly **pseudonymous** and highly transferable.

- **Smart Contract/Operational Risk:** Programmable difficulties such as bugs,network failures/bottlenecks,high-risks of tampering with the platforms,hacking accounts etc. can lead to freezing or drainage of these tokenized assets and a reduced sense of security.
- **Legal/Rights Uncertainty:** The token's dual structure of asset representation can cause risks and fraudelent actions like the divergence of underlying assets and tokens, with this resulting in states of unclear enforceability on how to protect investors and cases of underminding of the whole tokenization procedure.

Compliance Problems & Dangers - Cont;d

- **Market and Systemic Risk:** The improved liquidation provided via tokenization's fragmentation,the leveraging through the DeFi's and the ability of non-stop transfers can lead to uncontrolled runs and highly amplify contagious situations during financial stress periods.
- **Illicit Finance/Sanctions Exposure :** The nature of DeFi embedded in the tokens with the help of the fast and borderless trading provided by blockchains, encourages the involvement of risky counterparties with intentions like money-laundering or fraudulent/scam transfers, creating regulatories and compliance risks affecting the reputation of the whole system.

Key takeaway: Pseudonymity is the main compliance/regulation fault line in tokenized markets.So there is an absolute need of robust design that will add verifiable, privacy-preserving KYC/AML controls where needed **without "killing" DeFi's permissionless composability and openness.**

3) KYC/AML Without "Killing" DeFi: The Design Goal

Goal

Reduce illicit finance and frauds originated from total pseudonimity **while preserving DeFi**.

Fast-noted Key Concepts

Use a global Common Standard Permissioned Token, Use of Add-on compliance Smart Contracts, Use of Attestations/Claims, New Proof Protocols/Whitepapers.

Common Token Standards

We start by introducing the T-REX token.This is an institutional grade security token standard. that provides a library of interfaces for the management and compliant transfer of security tokens, using an automated onchain validator system leveraging onchain identities for eligibility checks. The standard has the following interfaces:

- Token
- Identity Registry
- Identity Registry Storage
- Compliance
- Trusted Issuers Registry
- Claim Topics Registry

This proposed standard must always have the requirements that: It's an ERC-20–compatible(easy to plug in ETHEREUM platform),identity-linked "compliance token" that supports regulator-defined rules plus pre-checks, recovery, freeze/pause, mint/burn, role-based controls (agent/owner), forced transfers, and batch operations.So the token can be able to handle most of the risks discussed previously.

ERC-3643 & ERC-1400 Token

In example two tokens capable of fulfilling most of these prerequisites are the ERC-3643 and the ERC-1400.
ERC-3643 is an Ethereum token built for regulated assets; It has an **Identity Registry** so transfers only succeed if the sender/receiver wallets are verified and eligible.So it is **KYC'd token basically on its Edges**. Moreover it is designed to work in conjunction with an on-chain Identity System,thus ensuring compliance with legal and regulatory requirements for the trading of security tokens.
While the ERC-1400 token is also a standard that supports security-token needs (controlled issuance/redemption, transfer restrictions, transparency hooks) allowing for enhanced document management and investor protection.
Key Takeways: **ERC-3643 and ERC-1400 let compliance live at the "edges"** of regulated assets—by enforcing **identity-based transfer rules** (who can hold/receive) **without changing the underlying blockchain—so DeFi** can stay permissionless for open assets while regulated tokens interact through KYC-gated pathways.

KYC-AML as Separate Smart Contracts.

Key Concept

Based on the previous ERC-3643/1400, we see the need of treating KYC/AML as modular external smart contracts that operate at the edges of the token,hence constructing regulated assets that are compliance-safe while keeping DeFi's core permissionless composability intact.

- So instead of hardcoding rules inside the token forever, we can use KYC/AML systems and any other necessary eligibility rule in a **separate contract that will work as an add-on "extension" for the primary contract only during the transfering process**.This technique will make **any new regulatory/compliance rule easily implemented inside the system without redeploying the whole token**.

Retaining DeFi with ZK Proofs (ZK-KYC / ZK-AML)

Idea

Use **zero-knowledge proofs** to verify compliance *without revealing identity or personal data.*

- Zero-Knowledge Proof(**ZKP**) is a **cryptographic method where someone proves, if a statement is true(e.g I passed KYC procedure), without the need of him revealing the underlying personal data.**
- First users will complete a KYC/AML procedure based **off-chain** with a verifier and then receive a **verifiable credential** e.g a distinct "key".
- Then for the On-chain part, investors will submit a **ZK proof** that they are truly **eligible** (KYC passed, not sanctioned, allowed jurisdiction) **without disclosing** key personal informations like name/address/ID.
- After that Smart Contracts will verify the proof and allow interaction with **regulated pools/tokens** only when valid.

Retaining DeFi with ZK Proofs (ZK-KYC / ZK-AML): cont'd

- The Results of embedding such a Proof of Identity will be that: **Compliance is satisfied at the edges** while DeFi stays **permissionless and composable** for open assets.

Key takeaway: ZKP basically will transform the "show me who you are" into "prove you meet the rules" identity,hence keeping privacy and DeFi usability.

Summary

- **Tokenization** is an extreme usefull procedure that makes financial assets programmable thus resulting in improved efficiency,liquidation and market access especially for more tradional hard liquidated assets.
- But as any innovative advancement it holds main challenges.The major one is it's **pseudonymity along with the high transferability**, which create compliance, legal, and operational risks.
- Therefore is the need for a robust path to tackle that main difficulty.The answer lies in the aspect of a more **modular "edge compliance"** tokens: Examples like ERC-3643 / ERC-1400 can enforce eligibility-based transfers for regulated tokens without changing the base blockchain.

Summary: cont'd

- So the important regulation systems(identity + policy modules) like **KYC/AML must be as separate smart contracts** so new rules can be updated on-chain without redeploying the token and destroying the whole ledger.
- Last in order for the whole architecture to **maintain its DeFi character** there is the necessity of **ZK proofs**: Users can *prove* they meet compliance rules without revealing identity, keeping privacy and composability .

Final takeaway: Compliance should be *programmable and privacy-preserving at the edges*—so regulated assets are safe to use, while DeFi remains open for permissionless innovation.

References

- World Economic Forum — Asset Tokenization in Financial Markets: The Next Generation of Value Exchange
  Insight Report May 2025
- Financial Stability Board(FSB): The Financial Stability Implications of Tokenisation
  22 October 2024
- ERC-3643: T-REX - Token for Regulated EXchanges
  An institutional grade security token contract that provides interfaces for the management and compliant transfer of security tokens.
  Authors : Joachim Lebrun,Tony Malghem,Kevin Thizy, Luc Falempin,Adam Boudjemaa.
- Privacy-Protecting Regulatory Solutions Using Zero-Knowledge Proofs
  Authors: Joseph Burleson, Michele Korver, and Dan Boneh