Bridging Identity Verification and Compliance with ERC-3643(T-rex standard)

Introduction

The private markets are known for their complex and often inefficient transaction processes. The traditional framework governing these markets is outdated, leading to a fragmented infrastructure. This results in significant liquidity discounts, making the buying and selling of private assets a cumbersome and time-consuming endeavor.The advent of blockchain technology, particularly the ERC-3643 standard, offers a promising solution. In this analysis, we dive into how ERC-3643 stands apart from other prevalent standards like ERC-20,ERC-721 and ERC-1400 in fostering seamless, compliant, and efficient transactions in private markets.

Traditional Private Market Challenges

- **Illiquidity**

The inherent illiquidity of private market assets is a significant obstacle for investors. Without an active market or willing buyers, realizing returns on investments becomes a daunting task.

- **Inefficiency and Fragmentation**

The current framework operates on outdated and fragmented infrastructure, making the buying and selling process of private assets inefficient. This inefficiency often leads to a substantial liquidity discount, discouraging transactions.

- **Tedious Transaction Processes**

Whether an investor is dealing with real estate, a stake in a private company, or a limited partner interest in a fund, the transaction process is arduous. It encompasses sourcing a buyer, negotiating sale terms, conducting due diligence, and finally transferring ownership. Each step is laden with bureaucratic hurdles, making the process lengthy and costly.

- **Time-Consuming Due Diligence**

Due diligence in private market transactions is notoriously time-consuming. It involves a meticulous review of financial statements, legal documents, and contracts, among other elements, and requires substantial document sharing and verification.

- **Lack of Transparency**

The traditional private market often lacks transparency, making it difficult for buyers and sellers to have full visibility into the transaction processes and asset values.

Alleviating Challenges with ERC-3643:

- **Sourcing a Buyer**

With ERC-3643, upon publishing assets on the blockchain network, they become accessible to a vast array of potential counterparties across multiple marketplaces, including centralized and decentralized exchanges. This standard also opens avenues for using securities as means for staking or collateralized loans, enriching the ecosystem with diverse transaction opportunities.

- **Negotiating Terms of the Sale**

ERC-3643 transforms this into a more market-driven process where supply and demand dynamics on trading platforms streamline the negotiations. Additionally, for peer-to-peer trading, on-chain or off-chain negotiations can swiftly reach agreements, enhancing the speed and ease of transactions.

- **Conducting Due Diligence**

With ERC-3643, a verifiable due diligence certificate embedded into the tokens is introduced. Smart contracts further verify counterparts' eligibility through verifiable credentials. This digital transformation not only streamlines the process but ensures a higher degree of compliance and efficiency.

- **Transfer of Ownership**

ERC-3643 enables instant transfer or swap of tokens if the payment method is token-based (like stablecoins, tokenized cash, or crypto). The smart contract ensures that transfers only occur when both investor and offering rules are met, unlocking the potential for peer-to-peer transfers, a feat unattainable in the traditional setup.

Bridging Identity Verification and Compliance with ERC3643 through ONCHAINID

Introduction

The integration of verifiable on-chain digital identities is pivotal in the evolving landscape of blockchain-based transactions, especially in the context of compliance with regulatory requirements. A significant stride in this direction is the interlinking of ERC3643 with ONCHAINID, an open-source self-sovereign identity smart contract. This synergy not only enhances the verification process but also streamlines compliance enforcement in real-time, on-chain, devoid of any intermediary intervention.

ONCHAINID Overview

ONCHAINID is a self-sovereign identity smart contract that empowers tokens and applications to ascertain the identities of individuals and organizations. This facilitates automated compliance enforcement and seamless access to digital assets on-chain, eliminating the need for intermediary oversight.

Integration with ERC3643

ERC3643 leverages ONCHAINID to ascertain if users comply with the predefined eligibility rules set by token issuers. Unlike conventional methods, ERC3643 links token ownership directly with users' ONCHAINID rather than mere wallet addresses. This integration fosters a more robust and precise identity verification mechanism.

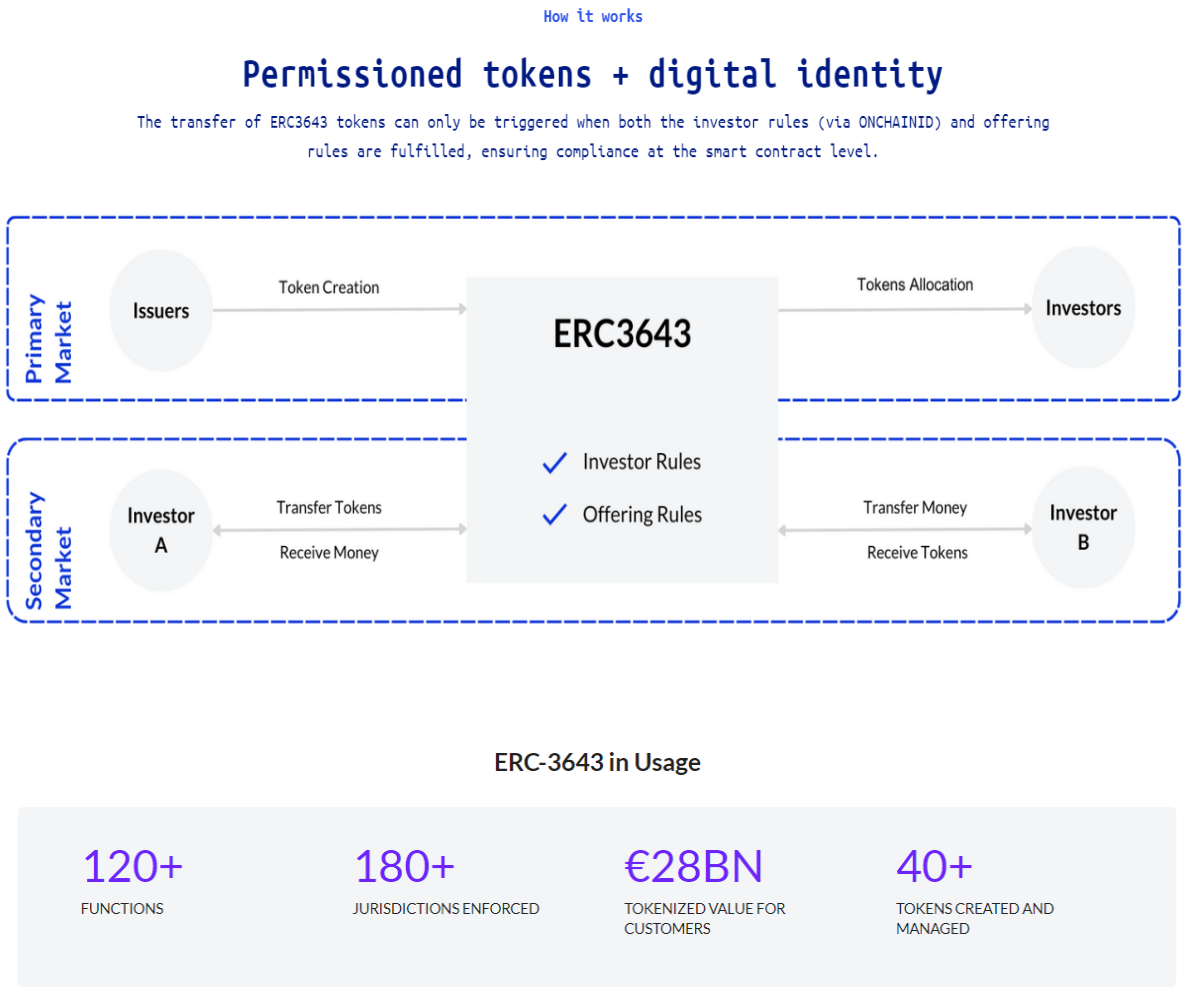
Eligibility Verification

The verification of eligibility rules is conducted through credentials issued by a trusted identifier, chosen by the token issuers. For instance, a KYC provider, dubbed as ABC, could be designated to scrutinize users' eligibility.
Post verification by KYC provider ABC off-chain, a hashed or anonymous credential is issued as a testament to the user fulfilling the required eligibility criterion. The ERC3643 token that the user engages with then corroborates this on-chain proof (credentials), adjudicating the user's permissions.

Real-Time Compliance Enforcement:

The on-chain evidence is intrinsically linked with the acquired security, enabling the embedded rules within the smart contract to be automatically executed or declined based on compliance.
Scenario Illustration:

Consider three investors: Investor A and Investor B have completed the necessary KYC/AML and other onboarding requisites, while Investor C has not.
Scenario 1: Investor A attempts to sell to Investor C on a public blockchain. However, the transaction is declined due to Investor C's non-verification, as per the smart contract's configuration.
Scenario 2: Investor A endeavors to sell security X to Investor B on a public blockchain. The transaction is authorized and executed seamlessly as both investors adhere to the smart contract's guidelines, showcasing the efficacy and real-time compliance enforcement enabled by the integration of ERC3643 and ONCHAINID.



Comparing with Other Standards

	ERC-20	ERC-721	ERC-3643
Interoperability Tokens can interact with any applications on the same network, such as exchanges and DeFi protocols.	✓	✓	✓
On-chain compliance Tokens are permissioned. They can only be transferred when both investor and offering rules are met.	✗	✗	✓
Guarantee of ownership Tokens are recoverable as they are linked with on-chain identity, instead of wallets.	✗	✗	✓
Auditable registry Who owns what is tracked by identity, so the blockchain can be used as an auditable registry.	✗	✗	✓

FEATURE	ERC-3643	ERC-1400
Open source smart contracts	✓	✓
Manage share classes	✓	✓
Audited by an external party	✓	✓
Validate transfers onchain	✓	✗
Block or unblock tokens	✓	✗
Tokens recovery process	✓	✗
Immutable cap table	✓	✗
Permission management with multiple agents	✓	✗
Stakeholders identity management	✓	✗
Perform batch functions	✓	✗
Partially fungible tokens (not compatible with decentralized exchanges)	✗	✓

Conclusion

leveraging the ERC3643 standard facilitates a robust, compliant, and efficient on-chain ecosystem for financially regulated institutions. By utilizing ERC3643 alongside ONCHAINID, institutions can ensure adherence to regulatory mandates, accurate identity verification, and automated compliance. The seamless transition of assets on-chain not only enhances liquidity but also streamlines transactions, due diligence, and ownership transfer processes. Moreover, the integration of smart contract functionality fosters a secure, transparent, and automated environment for asset management and transactions, aligning with the stringent demands of financial regulations.