Verified Token Standard

Enabling the brightline controls required for Security Tokens

## Abstract

Security Tokens will require an interoperable specification for controlled transfer of tokens outside of exchanges. Token Issuers will benefit from incorporating Verification Registries on-chain as an extension of existing standards (i.e. ERC20). Identity Providers, Exchanges, and Investor Portals can expand their services to include Verification Registries of Accredited Investors.

## Background

ERC20 has been the first killer app of the Ethereum network. It lead to the concept of a ‘utility token’ a scarce digital asset representing future access to software not yet built, enabling a new type of financial exposure to the success of a software project previously unavailable in the marketplace. This financial exposure relied on rapid adoption of the ‘utility token’ and not the revenue or profits of the project, creating a new regulatory framework not yet fully explored.

The combination of a new funding model and a gap in the regulatory framework has created a proliferation of different utility tokens, and many billion dollars raised in their cause. Which has come with clear benefits and also downside costs.

The benefits: the funding model of utility tokens compared to traditional funding sources has resulted in - 10X improvement in availability of capital & 1000X improvement in time to liquidity.

Costs: most of these projects will fail, the concept of a ‘utility token’ is currently untested and for the most part only compatible with a small niche of different types of software and almost all of that software require a massive network effects and a winner takes approach to the problem space.

This has lead to a new wave of entrepreneur who would like to put aside the idea of a ‘utility token’ but continue with the funding model of a token, even if that would require additional regulatory scrutiny of who can own & buy tokens. Which may mean a move away from the current permissless model of the first generation of token standards like ERC20 and ERC721.

## Problem

The ecosystem cannot solely rely on the continuation of novel ideas for utility tokens, to continue the reap the benefits of a token capital raising model. The ecosystem is looking to evolve to tokens that are financially exposed to the revenue and profits of the underlying project. Which changes the current regulatory treatment and puts restrictions on who and under what circumstances people could buy such tokens.

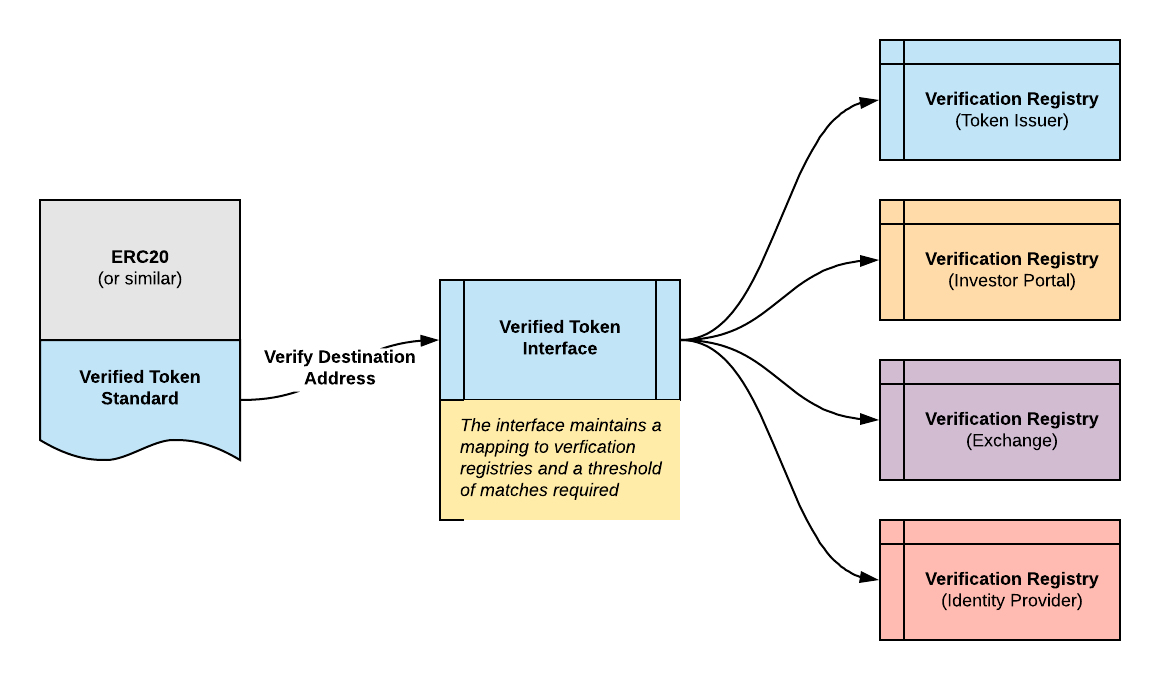
There needs to be a specification that can supplement the current ecosystem of tokens (ERC20, ERC223, ERC721) that enables a Token Issuers to ensure that their tokens is only transferred to holders who comply with their local & global regulatory requirements

## Key Requirements

* The specification must restrict tokens being transferred to parties that do not meet the regulatory brightlines required by the token issuer to be compliant.
* The specification must allow for the ability to update the restrictions placed on the token and need to be flexible and powerful to manage inevitable regulatory changes.
* The specification must allow token to continue to operate in a decentralised ecosystem.
* The specification must not overly restrict the possible features of the token itself, thus it needs to be simple and modular to enable additional features to be added in the future such as dividends share splits etc.

## Our Approach

Our approach is to create a specification to supplement the current generation of tokens (like ERC20), so the Token Issuer can maintain a level of control over who can receive the tokens and regulatory bodies can be satisfied that the transfers are restricted to only those deemed compliant (i.e. Accredited Investors).



This control will be enabled by allowing the Token Issuer to choose specific on-chain Verification Registries, which are queried every time a “transfer” or “transferFrom” is executed and only if the destination address is verified in multiple registries will the transfer complete.

We envision these on-chain registries would be federated in nature and maintained by different organisations, likely starting with the original Token Issuer themselves, then KYC/EV Identity Providers, Exchanges, Financial Institutions and even Regulators (should they wish to participate). Initially the verification registry may only hold information about a token holder’s Accredited Investor status, but could evolve to also hold information about your Net Wealth, Citizenship status or any other information required by future regulatory bodies.

The verification contract is modular in design to allow flexibility as regulations evolve, token issuers will be able to adopt different registries as well as require new or different brightlines to be checked on each transfer.

## Challenges

### Personally Identifiable Information

Information related to the eligibility of a particular public addresses’ ability to receive different tokens in different regulatory environments will be discoverable on the blockchain. Although in some cases this information may already be inferred through transaction analysis - i.e. The transfer of a security token will always infer information about that sender.

*Following the approach of ERC780 we expect all claims in a Verification Registry to be encrypted to ensure that the only public attributes are the ‘issuer’ address and the ‘subject’ address.*

### Infrastructure

As our proposal is only an extension to the current generation of token standards, we would expect all of the current exchanges and wallets to be compatible with this extension. Although they would require enhancements to be able to describe to the user why a particular transfer has failed.

*We expect this could be remedied in the first instance by a “Block Explorer” like website that can indicate the eligibility/ineligibility of a particular public address to receive specific tokens.*

### Third Party Data Integrity

At first, token issuers may only rely on the original KYC information that they have gathered from their token holders during the initial token distribution to restrict the transfers of their tokens. As they look to broaden the the possible holders of their token they may should adopt other identity providers, in which case they will have to rely on the integrity of their Verification Registries.

*Token Issuers should retain control over the ability to add/remove Verification Registries from their Verified Token Interface. The removal of a ‘corrupted’ registry will ensure that future transfers of tokens (or dividend payment splits) will only be completed to addresses within the ‘trustworthy’ registries.*