The Technology Behind the ERC1400 Protocol

Up until the rigorous involvement of regulators in the cryptocurrency industry and its regulation, ERC20 served as the token standard for a majority of crypto tokens on the Ethereum network. It helped build tokens as utilities, which did not require to adhere to complex laws as is needed for securities. However, with time, as regulators started demanding crypto tokens to abide by all regulations under the securities law, ERC20 failed to comply with the complexities. This stagnated the growth of the industry by preventing new startups to build over the old concept of crypto tokens while also making it tough for the existing ones to thrive.

A team of four blockchain developers and engineers, Stephane Gosselin, Adam Dossa, Pablo Ruiz and Fabian Vogelsteller proposed ERC1400 as the alternative for ERC20 token standard.

What is ERC1400?

ERC1400 is a standard deployed on the Ehtereum blockchain that would ensure that crypto tokens created over the network are compliant with regulations and qualify as securities. ERC1400 comprises of four different security token standards namely Core Security Token Standard (ERC1594), Partially Fungible Token Standard (ERC1410), Document Management Standard (ERC1643) and Controller Token Operation Standard (ERC1644). All these standards are together used while developing an ERC1400 token to give it all the functionalities that a traditional security asset would otherwise possess.

Some features that ERC1400 standard enforces on to crypto tokens include:

- The ability to inquire, validate, and justify transactions
- Forced transfers
- Ability to distribute token holdings and attach metadata to them
- Assessing transactions using both on-chain and off-chain data and authorization

While ERC1400 focuses on the creation of security tokens, it also makes it mandatory for all tokens built under this standard to be compatible with ERC777 and ERC20.

To understand the ERC1400 protocol better, let’s understand the concept of the four constituting tokens standards listed under it.

ERC1594: Core Security Token Standard

A utility token only has to follow the rules of a blockchain and use the data directly fed to the ledger. However, for a security token to function on the blockchain, it must also be able to

incorporate real-world/off-chain data input and authorizations. The ERC1594 standard acts a bridge for the passage of such data onto the blockchain.

Apart from checking the balance required for a transaction, ERC1594 also ensures several other off-chain factors before completing the transactions, such as KYC compliance of both the sender and the receiver and whether or not the tokens are subject to a lock-up period.

Using these functionalities, token issuers or exchanges can share the reason for the failure of a transaction with their users, which so far was not possible.

ERC1410: Partially Fungible Token Standard

ERC1410 allows for the creation of partially fungible tokens. They allow token owners to segregate their total holdings and attach a variety of metadata to each part, including vesting, time locks, and voting privileges. All the portions of the holdings thus specified is represented by a unique key and balance. This not only helps token owners stay more organized but also allows for functionalities such as vesting and lock-up to be implemented on a specific portion of the total holdings.

ERC1643: Document Management Standard

Securities are not as simple to use as utility tokens or cryptocurrencies as they were first developed. They come attached with a set of mandatory documentation regarding the asset. And as tokens created under the ERC1400 standard are securities, they need to comply with all such processes that traditional securities are subject to.

ERC1643 enables token issuers to attach all legal documents to the tokens before sharing them with peers. It also notifies token holders or any updates that are made to the documents in order to keep all involved parties on the same page.

ERC1644: Controller Token Operation Standard

So far, billions have been lost to hacks and thefts of crypto tokens. And once the tokens were lost, they were almost impossible to recover from the hackers' accounts. This was because no one other than the owner of the tokens exercised any control over the funds.

ERC1644 deems to change this by allowing regulators or other "controllers" of the tokens to force the reversal of a transaction in cases of frauds and thefts. This would also allow token holders to claim their tokens if they lose their private keys.

Final Words

Crypto tokens are usually simple to use, but with these added functionalities, they are becoming a somewhat complex asset class. However, it is happening for the good. ERC1400 facilitates the creation of securities as crypto tokens, which will bring institutional money into the crypto market and present individual investors with a more reliable mode of investment. As is very clear, governments too are more likely to accept security tokens as a legal form of asset over other crypto tokens.