NEUFUND

Security Tokens in Practice

PRESENTED BY
Marcin Rudolf
CTO at Neufund

neufund.org

WHAT IS SECURITY TOKEN?

A KIND OF TOKEN WITH SPECIFIC OFF-CHAIN SIDE EFFECTS

- Contrary to current DeFi trends that promulgate assets and financial mechanism as far isolated from off-chain as possible, **implementers of security tokens need to deal with off-chain side effects from the beginning**.
- **Off-chain side-effects are the (desired) consequences of owning a token on-chain**. In case of security token they are various rights investor's acquires via owning a token.
- **Off-chain side effect are legal in nature**. You need both legal proxies and proxies in the code to have working security token.

LEGALLY BINDING CONTRACTS

CODE AND LEGAL PROXIES

- Allows to bind a legal document to a smart contract, track the signing parties and provides a proof of entering into a contract with certain conditions (smart contract state) to all parties involved.
- A mixin class implementing IAgreement interface, mixed into contract that require a legal link: not only tokens, but also, for example, dividend distributing contract.
- Often you need a legal proxy that fill enforce off-chain rights in legal system. In case of equity tokens it's a Nominee Structure that enforces token holders rights as shareholders against issuing company. Other example is nEUR Token where holder rights are enforced against banking system by the token issuer.

NOTE ON HUMAN READABLE CODE

PARTIES MUST UNDERSTAND THE AGREEMENT - OTHERWISE IT'S INVALID

- We do not have any silver bullet solution that translates Solidity code into English. Instead we write legal document that represents code together with the code itself.
- Interestingly 90% of the legal work are just algorithms, the other 10% is a kind of metaprogramming which Solidity lacks (clauses like: what to do in case of fork? What is a bug fix and what is upgrade?)
- What is "on paper" takes precedence on what is in code. That is disincentive to write code that differs from what is legal document. Still some level of trust, as when you use regular smart contracts, is required.
- Example of such approach is tokenized Employee Stock Option Plan we use at Neufund from early 2017.

OFF-CHAIN EFFECTS - TOKEN HOLDER RIGHTS

WHAT COMES ON TOP OF OWNERSHIP

- By owning a token you have right to transfer it to someone else. That's covered by ERC-20.
- By owning a token you earn specific investor rights that are not transferable. In case of equity token you have rights to dividend and other proceeds and rights to information. In most cases you also have voting rights.
- Those rights are enforced on-chain by implementing snapshot token interface which provides past balances and a set of app-level smart contracts like Fee Disbursal which distributes payouts, dividends and exists proceeds.
- Off-chain they are enforced by token holder agreement attached to equity token, between token holder, nominee and issuer of the token. You can download a (real) one here or here.

COMPLIANCE - RESTRICTION OF RIGHTS

- **Due to regulatory compliance, various token holder rights are restricted**. For example there could be mandatory lock up period for newly issued tokens or KYC/AML verification requirement to exercise dividend rights.
- As regulators around the world have endless ideas on how to restrict those rights we refrained to code any of those into our tokens. **By default all our tokens are trustless**.
- Instead we introduced Token Controller Interface which each token observes. This allows to implement any control scheme: from fully trustless (NEU token) to heavily permissioned (nEUR token).
- Identity Registry app-level contract provides information on KYC/AML verifications which token controller may listen to, however other compliance schema may be implemented.

WORKING EXAMPLES

(LINKS TAKE YOU TO ETHERSCAN WITH MAINNET-DEPLOYED TOKENS)

- Equity Token is *legally binding contract* that allows for shareholder rights to be executed by any app understanding the snapshot token protocol. **It has a token controller which is simply a company/issuer of the token.** The token controller implements company governance and it is a legally binding contract as well
- nEUR Token is a *legally binding contract* that represent Euro which is off-chain asset. It does not need snapshot protocol, because it represents money where the only right that counts is a right to own so ERC-20 is enough. It however **has a token controller and a pretty restrictive one. Let's say it represents a bank and is responsible for checking KYC/AML verification and settling deposits and withdrawals.**
- NEU Token is the Neufund platform network token. It's legally binding but it's not a security. It also implements the snapshot token protocol, because **it pays you proceeds and gives access to the platform token portfolio**. It may also be used for voting on platform settings and for anything else which snapshot token apps might allow in the future. It however **does not have a token controller, because there is no entity controlling it** — it's a fully trustless token.

THANK YOU

Marcin Rudolf
EMAIL rudolfix@neufund.org