The Naive Depositer Contract

Overview

This contract is made to be the less complex that a contract can be. No complex structures nor external libraries are used. Code is a bit ugly since it is not factorized : it is done this way on purpose : it's a pattern. Like real-life contracts, the more informations (even redudent) it gives, the more security it is for all the parties involved.

This contract includes :

- A KYC oracle mechanism
- A deposit mechanism bound to the KYC Oracle
- A withdraw mechanism with requieres 2 of 3 parties to agree on withdrawal

The KYC Oracle feature

The KYC Oracle feature is an interface (found in the `kyc_oracle.sol` file) that is built so the automated oracle can whitelist an user.

When a user calls a method on the contract that rely on the `onlyKycCleared` modifier, the action will be performed only if the sending address has been cleared by the oracle.

Contract construction

When the contract is deployed, the following parameters must be passed :

- `oracleAddress` : the address used by the Oracle to whitelist users.
- `legal` : the address of a neutral legal officer.
- `projectOwner` : the address of a legal representative of the company beind the ICO project.

NB : The Chaineum address is the msg.sender address, since Chaineum will be the one deploying the contract.

Setting the destination wallet

`destinationWallet` is the wallet that will receive the funds. Can be a smart-contract itself (for multisig). Chaineum can change the destination wallet, but it will reset all votes for wath.

The Deposit feature

The contract can receive funds, but the `onlyKycCleared` modifier is applied to the default method requiring the sender address to be whitelisted to transfer funds.

The Withdraw feature

To withdraw funds parties must agree. This contract is designed this way : if 2 of 3 parties agree, all the funds holds by the contract are transfered to the `destinationWallet` (passed when constructed).

To signify its agreement, each party has its own method to call :

- `chaineumVote()`
- `legalVote()`
- `projectOwnerVote()`

Each method will toggle the flag for this user. All the flags are cleared when a withdraw is done.