Public Blockchains FSS 2024
Prof. Dr. Markus Strohmaier, Dr. Stefano Balietti

Home Assignment 03: ERC(ensor)-20

Points: 10

1 Main Task

ERC-20 contracts create fungible tokens on the Ethereum blockchain. Even if the Ethereum blockchain is decentralized, the creator of a contract may still keep "centralized" power over the ERC-20 tokens and unilaterally make changes, such as increasing the circulating supply or even censor transactions. Your task is to create an ERC-20 token that allows its creator to block transactions to and from blacklisted addresses. Use of Open Zeppelin is allowed.

Open Zeppelin Doc: `ERC-20`
Files: `Template`, `Testing Script`
Validator Contract: 0xc4b72e5999E2634f4b835599cE0CBA6bE5Ad3155

Specifications

a) Deploy your ERC-20 contract.
   1. Mint $N > 10$ tokens for the contract owner and 10 tokens for the validator. *(2 points)*
   2. Give the validator an allowance over the tokens of the owner equal to token currently held by owner. *(2 points)*

b) Handle blacklisting.*(1 points)*
   1. Implement the blacklist function: `blacklistAddress(address adrs)`.
   2. Blacklistings are stored in `mapping(address => bool) isBlacklisted`.
   3. Only owner and validator can blacklist an address.

c) Allow for removal of an address from the blacklist. *(1 points)*
   1. Implement the unblacklist function: `unblacklistAddress(address adrs)`.
   2. Mapping `isBlacklisted` is updated accordingly.

3. Only owner and validator can unblacklist an address.

d) Transactions to/from blacklisted addresses are reverted. *(2 points)*

e) Emit the event `Blacklisted(adrs)` when an address is blacklisted and the event `UnBlacklisted(adrs)` when an address is removed from the blacklist. *(2 Points, checked off-chain, assigned later)*