Week 1 - SC Dev Basics & ERC20

Created	@December 8, 2021 4:23 PM
Tags	

Objectives

- □ Learn how to setup a Smart Contract project from scratch with Hardhat.
- □ Learn all functions and be familiar with the ERC20 standard.
- □ Be exposed and familiar with some libraries from OpenZeppelin.
- □ Learn how to use modifiers and how it works.
- □ Learn how to write tests with typescript and run test coverage.
- □ Learn how to write deployment script and deploy on different networks.

Requirements

- Write a standard & simple ERC20 token contract without using any libraries for token (can use other libs like SafeMath, Ownable, etc).
    - Total supply of 1B tokens with decimals of 18.
    - Have a **mint** function to allow only the owner to mint more tokens, but the total supply can not be more than 1B tokens.
    - Have a **burn** function to burn from sender wallet.
    - Should have all necessary events and public getters.
- Write full coverage tests for the contract.
- Write a deployment script for the contract.

Resources and Tips

- Smart-contract beginner guide
- https://docs.soliditylang.org/en/v0.8.10/
- https://hardhat.org/
    - Check out the 3rd party plugins and play around with them (Eg. contract sizer, gas reporter)
- https://docs.openzeppelin.com/openzeppelin/
    - Try out the contracts wizard and read / understand the different contracts being used https://docs.openzeppelin.com/contracts/4.x/wizard
-
- Check out our dao_sc repo

  - Read some of the contracts, tests (TS files, JS files are outdated) and deployment scripts (hardhat tasks)
  - Try running coverage
- See bad ERC20 implementations
  - Understand how bZx got exploited due to a bad `transferFrom()` implementation https://bzx.network/blog/incident

Extra / Bonuses

- Check out this challenge and try to hack it: https://www.damnvulnerabledefi.xyz/challenges/1.html
- Try the warmup and lotteries sections of Capture The Ether
- Contract best practices: https://consensys.github.io/smart-contract-best-practices/
- Read Ethereum 101: https://secureum.substack.com/p/ethereum-101 to understand more about Ethereum basics
- Read more about ERC20 variants:
  - Fee on transfer:
    - WAV3: https://etherscan.deth.net/address/0x14c38e90a593b0bd5b7e9896a8ef4ae0a119d6ae#code
    - ZUKI: https://bscscan.deth.net/token/0xe81257d932280ae440b17afc5f07c8a110d21432#readContract
  - Rebase tokens https://dev.to/rajasekharguptha/what-is-rebase-in-crypto-explained-1nci
    - AMPL: https://etherscan.deth.net/address/0xd0e3f82ab04b983c05263cf3bf52481fbaa435b1#code
    - UPC: https://bscscan.deth.net/address/0x945fD7037986BD62d37c6934fc4F397BB0bD3cC8#code
  - BlackList tokens:
    - USDT: https://etherscan.deth.net/address/0xdac17f958d2ee523a2206206994597c13d831ec7#code
  - Crowdsales: https://docs.openzeppelin.com/contracts/2.x/crowdsales