Essay – Lab 5 – Florin-George Bărcan

We start the 5th chapter with some information regarding tokens. Tokens are contracts that follow some common rules, i.e., implements a set of functions that all other contracts share between them, most known being transferFrom(address \_from, address \_to, uint256 tokenId) and balanceOf(address \_owner).

We are given an example. We build a token and we make it capable of interacting with an ERC20 token. Since all ERC20 tokens share the set functions with the same name, that won’t stop us if we desire to interact with the other ERC20 tokens. In our case, trading 0.111 ETH worth of zombies is not going to make any sense or worth. That’s why we are introduce to a new standard, ERC721. This standard assumes each token is unique and not divisible, thus it is not interchangeable. We can trade whole units, each with a unique ID.

What’s also great about the ERC721 standard is that if we or somebody wants to communicate with this contract, it will do so easily because of the set of functions with the same name, without entering our contract and checking which function X approves function Y for a transfer. We are also not allowed to have modifiers or functions with the same name that we inherit from a token standard. It can completely mess up the whole structure.

Later we get to use the SafeMath library in order to prevent overflows and underflows, like in uint256 where if we add 1 to 11111111 in turns into 00000000, or if we subtract 1 from 0, we get 255.