Blockchain programming - Laboratory 03

Ometita Radu - Adrian

March 2022

1 Review of lecture and assignment

We will be expanding on some of the subjects introduced in the lecture and assignments.

1. Asymmetric cryptography.
2. The distinction between on-chain and off-chain code.
3. UTxO based blockchains vs account based blockchains.
4. Fungible and non-fungible tokens.

2 Questions

1. State variables are stored on the blockchain. since the blockchain is immutable, how can we change the value of a variable?
2. Since data stored on the blockchain is available to all nodes, isn't it dangerous to store sensitive information in state variables? Is the information stored in state variables encrypted?
3. How are stablecoins kept "stable"? Is it by using oracles to get off-chain data?
4. What is the best way to avoid writing vulnerable ERC20 contracts?

5. In the first lesson on cryptozombies it says that it is a convention to name function parameters with an underscore to differentiate between the global and local fields. Is this just a convention/recommendation or this is something that the compiler will enforce ? By this I mean that if we have a parameter without underscore will we get an error?

6. How can smart contracts be used to securely transfer sensitive files?

7. How can we improve blockchain implementations in order to make them eco-friendly?

8. Cum functioneaza mai exact proof of stacking? Daca utilizatorii pun monede la stacking, cu ce ajuta acest lucru reteaua? Nu inteleg exact ce se intampla, facand o paralela cu proof of work unde nodurile valideaza o tranzactie astfel oferind puterea de validare in schimbul profitului in moneda respectiva, aici nu inteleg exact modul in care depozitarea de monede ajuta reteaua.

9. Can blockchain only be used for cryptocurrency transfers or can be expanded to other areas?

3 Final assignment

Discussing ideas for your final assignment.