Aristotle University of Thessaloniki

Data & Web Science MSc Program

Decentralized Technologies Course

Assignment 2, 2021 - Ethereum

For this assignment you will need to implement a smart contract in Solidity, using the Ethereum blockchain.

The smart contract's purpose is to facilitate donations to different charities. When a user wants to send some funds to a destination address, instead of sending them directly to that address, they will use the smart contract. A part of the funds will be sent to the charity the user specified, while the rest will go to the destination address.

In order to accomplish that you will need to code a contract that when deployed, will accept a list of charities at creation time, specified by their respective addresses.

For facilitating the transfer of funds, you will code two different variations of the same method. The users that would want to donate, will then make their payments by sending funds to these methods.

In the first variation, the method that facilitates the payments, will accept a destination address, as well as the index number of the charity (0 is the index for the first charity, 1 for the second etc). The method should redirect 10% of the funds to the selected charity, while transferring the rest to the destination address. The contract should make appropriate checks if the user that originated the transfer has sufficient funds and if the charity index number that is provided is a valid one.

In the second variation, the method will additionally accept a value for the donated amount (in wei). In addition to the checks that the previous variation performs, in this case, it should also check that the donated amount is within acceptable limits; a donation has to be at least 1% of the total transferred amount, while it cannot exceed half of the total transferred amount.

The contract should keep track of the total amount raised by all donations (in wei) and towards any charity, collectively, and provide means for any interested party to access that information. So, for example, if one donation of 2 ether has been made to charity A and

another donation of 3 ether was made to charity B, the contract should report that 5 ether was donated in total.

The contract should also keep track of who is the person that made the highest donation, identified by their address, along with the amount they donated. This information should be available with a single call to one method in the contract. It should also be available only to the user that deployed the contract.

When a donation has been made through the contract, an event transmitting the address of the donor and the amount donated, should be emitted.

You will also have to provide some means to destroy the contract and render it unusable. This functionality should be available only to the user that deployed the contract.

Notes:

- Use method overloading for providing two different variations of the same method that facilitates the transfer of funds.
- Use a modifier to restrict access to functionality.
- The addresses of the charities should not be publicly available.
- Your submissions should include only the .sol file with the smart contract.
- Comment your code detailing your design choices.
- Submit only the .sol source code file inside a compressed archive (.zip, .tar.gz etc)