Fintech and Cryptocurrencies

Take Home Exam 2019

Instructions

- This exam follows the honor code. You are not allowed to work together with other students and all answers must be in your own words. Copy-pasting from online (or other) sources is not permitted.
- Answer all questions including all sub-questions.
- There are 100 points in total and each question has a clearly indicated number of points. There are 10 bonus points, which do not count against the total of points.
- All answers must be complete English sentences, no unnecessary abbreviations (commonly used abbreviations such as ICO are acceptable, provided you explain them in a separate section of your answers for which there is no word limit). I can deduct points for grammar and spelling errors.
- You must submit your code using a public github repository. When you submit your solutions, include the link to the github repository. Make sure you commit answers to individual sub-questions separately. Please place each project that you develop in Q2.1 - Q2.3 in a subfolder within your github repository.

Part 1: Theoretical Questions

Question 1.1 [6p]

Give an example of a company that you think will disrupt its target market in the next 5 years. Analyze the company's target market and explain very carefully why you consider it as potentially being disruptive. Your example should NOT be a company that has already been classified as disruptive by news agencies or discussed in class.

Question 1.2 [6p]

Give an example of a blockchain company that does not need a blockchain. Explain why the blockchain is unnecessary for their application and does not add any value.

Question 1.3 [6p]

Explain the concept of an ICO. Give an example of an ICO that failed. Analyze why this ICO probably failed by citing dodgy parts from the whitepaper and explain why these parts are dodgy.

Question 1.4 [6p]

While Proof of Work consumes a lot of electricity, Proof of Stake also is not perfect. Explain how Libra, as an example of a Proof of Stake protocol, works and what its advantages and disadvantages over Proof of Work are.

Question 1.5 [6p]

Which regulatory obstacles will you face when you want to commercialize your group project? Please explain why.

Part 2: Practical Questions

As you have probably already noticed, Co is obsessed with sneakers. Since he wears them every day, he is certain he knows what good sneakers are. This is why he designed his own pair:

Each pair is personalized, the buyer can choose the name at the back and the image on the side (of course, Co chose the unicorn). Also, the public key of the buyer is engraved into the sole.

Question 2.1 [40p]

Since all of these pairs of shoes are unique and a piece of art, why not create a smart contract to keep a digital twin of them?

Tasks

1. Create a truffle project
2. Write a smart contract called `CoShoe` that holds non-fungible tokens:
    a. Each shoe is a struct called `Shoe` comprised of:
        i. `owner` (address)
        ii. `name` (string)
        iii. `image` (string: url to the image)
        iv. `sold` (bool)
    b. Define a state variable called `price` and set it to 0.5 Ether, converted to Wei.
    c. Define a state variable called `shoesSold` that holds the number of shoes that have already been sold. Set it to 0.
    d. Define a public array called `shoes` that holds instances of `Shoe`
    e. Implement a `constructor` that mints 100 `CoShoe` tokens. The `owner` of each token is the address deploying the contract, `name` and `image` are empty strings (`""`), and `sold` is equal to `false`. Add the instances of `Shoe` to the array `shoes`.
    f. Implement a function called `buyShoe` that
        i. Takes the input parameters `name`, `image`
        ii. Checks that there is still a pair of shoes left that has not been sold yet, otherwise it throws an error
        iii. Checks that the value that is attached to the function call equal the `price`, otherwise it throws an error
        iv. Transfers the ownership of a `Shoe` to the caller of the function by setting `owner` within the `Shoe` struct, setting `name` and `image` to the input variables, and changing `sold` to `true`
        v. Don't forget to update `soldShoes`
    g. Implement a function called `checkPurchases` that
        i. returns an array of bools that are set to true if the equivalent index in `shoes` belongs to caller of this function
        Example: `[true, false, false, false, false, true, false, false, …]`
        ii. Remember to implement it in a gas saving manor
3. Test the following functionalities:
    a. 100 tokens are minted on deployment
    b. `buyShoe` correctly transfers ownership, sets the name and the image, sets sold, and updates `soldShoes` count
    c. `buyShoe` reverts if the price is not equal to 0.5 ether
    d. `checkPurchases` returns the correct number of `true`s
4. Compile your contract
5. Include a `2_deploy_contract.js` in the migrations folder
6. Deploy your contract to a network of your choice (this can be an emulated network)

7. In addition to submitting on github, please hand in a complete zip file including the truffle project.

Question 2.2 [30p]

Instead of starting a kickstarter campaign, Co wants to use a token bonding curve to sell his shoes.

The Token

Issuance: A fungible token called “CO”

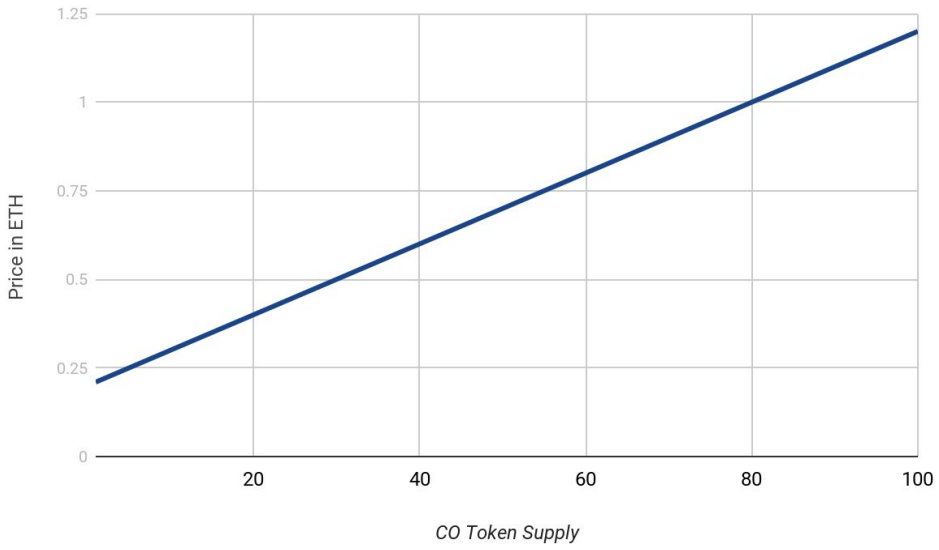
Supply: 100, this is the number of shoes Co wants to produce

The Bond

Collateral: ETH, CO tokens are bought in ETH

The Traded Asset or Objective: The shoes, 1 pair cost one “CO”

The Curve



Curve function: $f(x) = 0.01x + 0.2\,,\ x \in \mathbb{N}$

Pricing: static pricing

Specialty

Only Co is allowed to sell tokens back to the curve.

Tasks

1. Create a truffle project
2. Write a smart contract to issue CO tokens:
    a. Make the contract “ownable”
    b. Implement the ERC20 functionalities
    c. Implement a `buyPrice` function that calculates the price for the purchase of `n` CO tokens based on the curve defined above.

    d. Implement a `sellPrice` function that calculates the price for the sale of `n` CO tokens based on the curve defined above.
    e. Implement a `mint` function that creates tokens if the correct current price is transferred to the contract. The price is determined by the `buyPrice` function.
    f. Implement a `burn` function that can only be called by the `owner` (i.e., only the `owner` can sell tokens back to the curve and withdraw the funds). The price is determined by the `sellPrice` function.
    g. Implement a `destroy` function that destructs the contract (see `selfdestruct`). This function can only be called by the `owner` and it can only be called if all CO tokens belong to the `owner`.
3. Test the following functions:
    a. `mint`
    b. `burn`
    c. `destroy`
4. Compile your contract
5. Include a `2_deploy_contract.js` in the migrations folder
6. Deploy your contract to a network of your choice (this can be an emulated network)
7. In addition to submitting on github, please hand in a complete zip file including the truffle project.

Bonus Question 2.3 [10p]

Update your contracts from Question 2.1 (CoShoe) and 2.2 (CoToken) such that they interact with each other. For this, move them into a new truffe project, i.e. a truffle project that includes both contracts.

Updates in CoShoe:

1. `CoShoe` needs to know about `CoToken`
2. The `price` does not have to be defined because it is 1 CO.
3. The `buyShoe` function does not accept Ether. Instead, it checks on the `CoToken` contract if the address calling this function owns a CO token.
4. If the address calling the `buyShoe` function owns a CO token, it triggers the `transferFrom` function in the `CoToken` contract and transfers the token to the `owner` of the `CoToken` contract. Make sure that the function call reverts if the CoTokens could not be transferred.

Updates in CoToken:

1. You may have to make the `owner` public in order to retrieve the recipient address for the `transferFrom` function.

Deploy the updated version of you contracts to a network of you choice. In addition to submitting on github, please hand in a complete zip file including the truffle project.