Exercise: Request for Quotation

Exercise Description

- David is responsible for procurement in his company. His job includes requesting quotes from suppliers and place orders for required materials.
- As the company grew significantly in the last years, David struggles to keep up with the additional workload and shall be supported by an automated process that does most of the work for him.
- The companies ERP holds information about the kind and amount of materials for procurement.
- David wants to be able to start a bidding process by publishing a procurement and have his suppliers respond with their quotes and prices.
- Only white listed suppliers are allowed to respond to a bidding process.
- The suppliers respond with information in the form of:
    - Brisco can deliver 10 000 items within 60 days at a price of 0.10 cents per item
    - Lifephone can deliver 8 000 items within 45 days at a price of 0.12 cents per item
    - ...
- David wants to be able to retrieve this information from the contract to select the best supplier for his company.
- **Bonus 1:** David wants to be able to have the contract select the best/cheapest supplier for a given quantity and due date
- **Bonus 2:** Suppliers want to be able to respond to a bidding process with their own automated systems (smart contracts) that define which amounts can be delivered by a given date and the price they charge for a given amount ordered so that they can optimize their bidding process too.
- **Bonus 3:** (Probably REALLY difficult) David's company as well the suppliers have an interest in not publicly revealing the quotas and prices during the bidding process. Design the involved smart contracts in a way that they can decide on a "winner" with revealing as little information between the parties as possible.

Technical description / Implementation hints:

- David requires a smart contract that can initiate a bidding process for a procurement. The procurement is defined by an ID, the minimum required amount of materials and the type of materials.
- Multiple bidding processes shall be able to be run on the same contract concurrently.
- David shall be able to whitelist different suppliers for different bidding processes.
- Suppliers shall be able to provide multiple responses to the same bid, e.g. Brisco can also deliver only 1 000 items within 20 days at a price of 0.15 cent per item.
- Bidding processes need to be able to be closed so suppliers cannot provide new quotas and prices for that bid.
- **Bonus 1:** The smart contract needs to have a function that closes a bid by it's ID and returns the winner of that bidding process.
- **Bonus 2:** Instead of responding with a concrete bid a supplier shall also be able to provide a smart contract that can be queried for information. This smart contract needs to adhere to an interface that needs to have functions for the following queries:
    - How many items can be delivered by date T
    - If N items are requested by date T what is the price per item
    - How many items need to be requested to have a price P of an item by date T
- When a bid is closed, supplier contracts shall queried to retrieve information about conditions of sale and delivery and an algorithm shall select the best /cheapest for this bid.
- **Bonus 3:** The smart contracts need to be able to compare published quotas and prices and identifying orders (which publication has a earlier delivery date, higher amount, higher price, compared to each other) without revealing the concrete numbers. There are multiple possible ways to achieve this:
    - The contract could act as self sovereign identity
        - Introduction: https://bitsonblocks.net/2017/05/17/a-gentle-introduction-to-self-sovereign-identity/
    - By the use of zk-SNARKs
        - https://media.consensys.net/introduction-to-zksnarks-with-examples-3283b554fc3b
        - https://blog.ethereum.org/2016/12/05/zksnarks-in-a-nutshell/
        - https://z.cash/technology/zksnarks.html
        - As long as the involved smart contracts are only verifying the provided data and not providing proof, the EVM should be provide enough computing power to use zk-SNARKs.
    - By the use of encrypted query processing:
        - https://www.darkreading.com/risk/a-look-at-encrypted-query-processing/d/d-id/1138400
    - ...