Distributing Trust & Blockchains

Assignment 1: Smart Contract - A Modern Way

The following text describes the required packages, the steps to run the code, and the logic behind the desired functionalities.

Required Packages

You need to have NodeJS and Truffle installed. Instructions are present in the links attached.

On the terminal, type

```
npm install package.json
```

Steps to Run

On the terminal, type

```
truffle develop
```

In the truffle console,

```
deploy
let instance = await AModernWay.deployed();
```

After creating the instance, you can interact with the smart contract by calling the available functions.

How are we storing an Item?

We are storing an item using a struct. The struct contains various information such as the unique Item ID, it's name, description, asking price, the address of the seller, the status of the item (if it's still available, in transit or already sold), etc.

Making a Listing

The seller needs to call the `addNewItem` function and pass the name, description and the asking price of the item he wants to sell.

We have an array of items where we keep on adding the items as multiple sellers keep calling this function. The seller address is captured using `msg.sender`.

Viewing Listings

If a buyer wants to view all the available items, then he can call the 'viewItems' function. It returns a string where in each line, it contains the information such as the name, description and the price of the item.

> Note: The `uint2str()` function that was already present was outdated and hence we used the code from here to convert a uint into a string.

Buying an Item

To buy an item, a buyer has to call the function `buyItem` and pass the item ID of the item he wants to buy and also his public key. The buyer also has to pay the asking price using `{value: <asking_price>}` when calling the buy function.

The money gets transferred to the contract and the buyer will get the item once the seller delivers it. Following the delivery, the money will be transferred from the contract to the seller.

Delivery

A seller can deliver an item by calling the `deliverItem` function. First of all, he needs to get the public key of the buyer using the `getPublicKey` function. Then he has to encrypt the item string using the public key of the buyer and then pass it as an argument when calling the delivery function.

The encrypted string get's delivered to the buyer and then the contract transfers the money from the contract balance to the seller.

The item's status is also changed from In transit to Sold.

How are we keeping the string secret?

The code and all the state changes resultant of function executions, can be traced by anyone looking at the blockchain. Hence, we were expected to come up with a mechanism through which seller can provide the string to the buyer while keeping it a secret from other users.

So, we use the `eth-crypto` package. First, we create an identity for every buyer (the private keys are different from the ones provided by truffle).

Then, the seller will encrypt the item string using the public key of the buyer, offchain i.e. other users won't be able to trace it because it is not on the blockchain.

The seller delivers the encrypted string using the smart contract and the buyer can retrieve it using the smart contract.

The buyer can decrypt the encrypted string using his private key. This will also be executed offcain.

> An example has also been provided in the `script.js` file present in the folder.

Additional Information

- All relevant code has been properly explained with Doxygen Comments.
- A few sample test cases have been provided too. They are present as a markdown file `tests.md` in the folder. Alternatively, you can also access them as an html page using the file `tests.html`.

Group 1

- Manish (2018101073)
- Akshat Goyal (2018101075)
- Tanish Lad (2018114005)