DTB Assignment 1

Team: Tripple

- Tathagato Roy (*2019111020*)
- Snehal Kumar (*2019101003*)
- Rutvij Menavlikar (*2019111032*)

Programming Logic

The smart contract `Market` contains a struct of item listings and its details. Each listing contains the item details required, the seller and buyer address and its current state. For every change in the struct caused by the fuction calls, an event is emitted, updating the states of the listings as required. The transactions follow a procedure based on trust to ensure the validity and atomicity of the transaction:

1. A buyer selects a valid active listing to purchase and sends a request to buy.
2. To request a purchase, the buyer must submit a deposit of 2 time the item price and the seller is notified.
3. The seller then confirms the deposited amount and sends an encrypted hash key for the item. This ensures the security of transaction such that it is not leaked to any other person.
4. The item is then delivered to the buyer after which they are refunded the additional deposited amount, and the seller gets the asking price of the item.

Making a Listing

- The method `createListings` takes input the price, name and description of the item and it assigns it a unique id, stores the unique seller id for it and sets it's status to indicate that the item is available.
- Then it emits 2 events.
  - `ListingCreated`
  - `ListingChanged` to indicate its creation.

Viewing Listings

- The method `fetchactivelistings` goes through all the listings created, stores all listings whose item's status is available and returns them.

Buying an Item

- The method `requestBuy` takes input as the listing unique id of the item to be bought and checks if it is a valid listing id and if the item is available.
- Then it emits an event `PurchaseRequested`
- Then the method `sellItem` takes input listing id and the unique string to be assigned to the item.
- Then it emits an event `encryptedKey`

Delivery

- The method `confirmDelivery` is responsible for ensuring the delivery of the sold item by the seller. It checks the existence of valid listing Id, and proceeds to transfer 3*item_price to the seller and item_price to the buyer. This ensures the security and completeness of the transaction after which the state of the listing and active listings are updated.

Encryption

- We need off-chain Encryption to secure pass the item string securely without anyone having access to it.This encryption can be done inside the Truffle develop console.
- We will use the library `EthCrypto`

Installation

```
npm install eth-crypto --save
```

Import

```
const EthCrypto = require('eth-crypto');
```

Workflow

- The buyer would send his public key to the contract when requesting to buy from the contract any given item.
- The public key can be generated using private key using the function `EthCrypto.publicKeyByPrivateKey()`
- The Seller can see the logs of the event `PurchaseRequested` to find the public key using the following piece of code:

```
await M.getPastEvents( 'PurchaseRequested', { fromBlock: 0, toBlock:
'latest' } )
```

- The Seller will then use the public key to encrypt the item string using the function `EthCrypto.encryptWithPublicKey()` and then generate the string of the cyphertext using `EthCrypto.cypher.stringify()`.
- The Seller can then send the encrypted final string to Blockchain using `sellItem()`.
- The Buyer can obtain the final encrypted string from the logs of the event `encryptedKey` using the following code:

```
await M.getPastEvents( 'encryptedKey', { fromBlock: 0, toBlock: 'latest' }
)
```

- The Buyer will then generate the cypher text from the obtained string using `EthCrypto.cypher.parse()`
- The cyphertext can then be decrypted using the buyers public key by the function `EthCrypto.decryptWithPrivateKey()` and the item string is obtained by the buyer.

Transactions

- The buyer and the seller must escrow two times of the listing price to the contract.The buyer will send the money when he/she makes a request to buy and the seller when he/she sends the item.This is done to ensure trust and motivate the parties to act fairly.
- The seller will get 3 times the listing price (initial deposit + listing price) and buyer will get the listing price (initial deposit -listing price) after the purchase is confirmed by the buyer.

Modifiers

- Several modifiers are used to ensure the valid actions are taken during execution of a function. They are:
    - Checking whether a listing is valid
    - Checking the valid state of the item listing
    - Checking whether the buyer/seller are eligible to execute a particular method
    - Checking if the string of the item has length less than or equal to 50.