Name: Taoyue Xia (James) Date: 2021/08/16 Section: ST10701

**Total in points** (100 in total):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Professor’s Comments:**

1. **(a).** Oracles are third-party services that collect data from web services and write the data via a special Smart Contract to the blockchain.

**(b).** A synchronous oracle writes data to the smart contract once every fixed time. A asynchronous oracle only requests data from third-party service and write back to the Smart Contract when users request.

**(c). Advantages**:

* Enables data retrieval from external sources
* Either easy to use or live data
* Can be used for varying purposes (randomness, stock data, weather data, etc.)

**Disadvantages**:

* Costly in terms of gas consumption
* Dependence on a third party
  + In terms of data manipulation (Oracle owner can manipulate data)
  + In terms of availability (Oracle service could be offline such that Smart contract not functioning)

**(d).** . So it should update up to 13 blocks every day.

1. **(a).** This contract has the function of voting. Users can buy votes via the function **buyVotes()**. Then they can vote for their preferred candidates via the function **vote()**. Users can also redeem the amount of votes they don’t need via the function **payoutVotes()**. Finally, the owner of this contract can end the vote and collect the remaining balance.

**(b).** This contract has a bug in the function **payoutVotes()**. It first calls the transfer function, then it deduce the amount of votes of the msg.sender. However, a malicious user can construct a fallback function, and recall the payoutVotes() function many times until the gases are used.

**(c).** The **Pull over Push** idiom can be used to prevent this type of error.

**(d).** We just need to swap the position of the two sentences and then this type of bug can be fixed.



1. **(a).** web3.js is a collection of libraries that allow you to interact with a local or remote ethereum node using HTTP, IPC or WebSocket.

**(b).** Infura provides the tools and infrastructure that allow developers to easily take their blockchain application from testing to scaled deployment - with simple, reliable access to Ethereum and IPFS.

**(e).** We can issue a higher gas fee to speed up the execution.

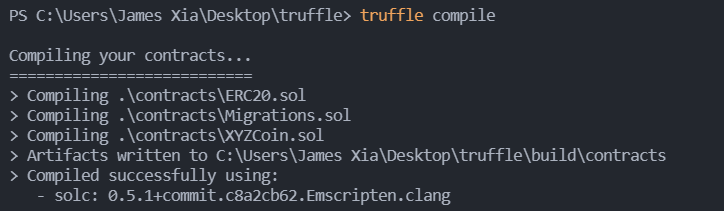
1. **(a).** Truffle creates folders with names “contract”, “migration” and “test”. Files in the “contract” folder denote for the different contracts written in solidity. The file in folder “migration” is used to deploy contracts. The file in folder “test” is used to test the functions in contracts whether they are running correctly.\

**(b).** see the file on github.

**(c).** see the file on github.

**(d).** The first mapping is used to map the address of users to their balances. The second mapping is used to map the address to the balance mapping, which indicates the amount the spender is able to withdraw from the owner.

**(e).** The compilation result is shown below.

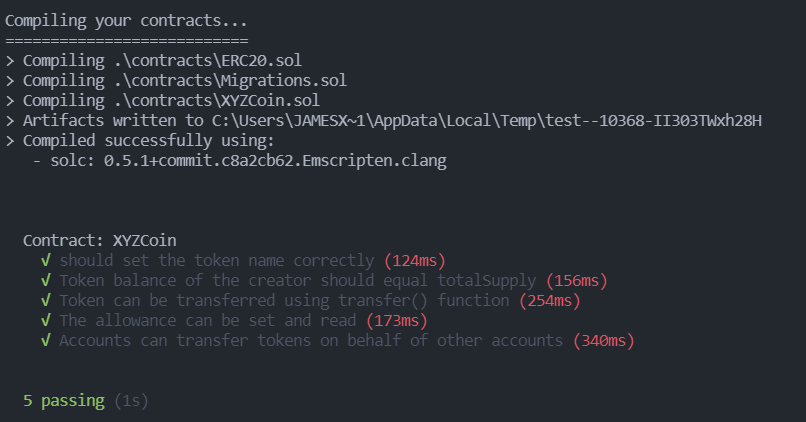


**(f).** Please see the files on github.

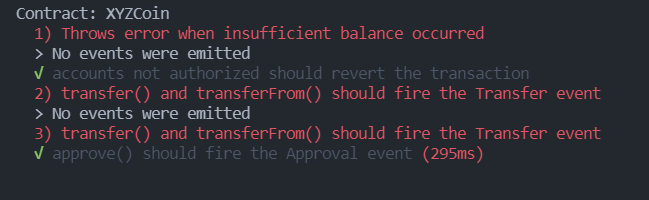
**(g).** The deployment figure is shown below:



**(e).** The test result are shown below:



**(i).**

****