CCT College Dublin

Assessment Cover Page

Module Title:	Distributed Digital Transactions
Assessment Title:	CA2 Individual
Lecturer Name:	Dr. Muhammad Iqbal
Student Full Name:	Xiaohui Weng
Student Number:	2020387
Assessment Due Date:	8th January 2023
Date of Submission:	8th January 2023

Declaration

By submitting this assessment, I confirm that I have read the CCT policy on Academic Misconduct and understand the implications of submitting work that is not my own or does not appropriately reference material taken from a third party or other source. I declare it to be my own work and that all material from third parties has been appropriately referenced. I further confirm that this work has not previously been submitted for assessment by myself or someone else in CCT College Dublin or any other higher education institution.

Catalog

Question 1

As far as we are aware, the main characteristics of Blockchain are peer-to-peer decentralized distributed ledger technology, which means that no third parties, not even the government, are involved. As a result, the transaction is more secure and less vulnerable to fraud. Additionally, it is a cryptographic technology. Therefore, it can be said that Blockchain technology is well suited for use in the financial sector. Just like our standard international exchange, letter of credit, equity registration, and stock exchange, Blockchain technology can be very valuable. In particular, when conducting transaction payments, Blockchain technology can directly bypass the third party to achieve fast payment, which can significantly reduce costs.

As we know that Bitcoin and Etherenum are public Blockchain networks where anyone can trade and invest.Bitcoin is an online currency, but Etherenum is intended for complex smart contract and decentralized applications. And Bitcoin is using the consensus protocol called proof of work(Pow), instead of this Etherenum is using proof of stake (PoS). Furthermore Etherenum is faster than Bitcoin with transactions. Last but not least, Etherenum's algorithm which is Ethash, instead of this that Bitcoin is using SHA-256.

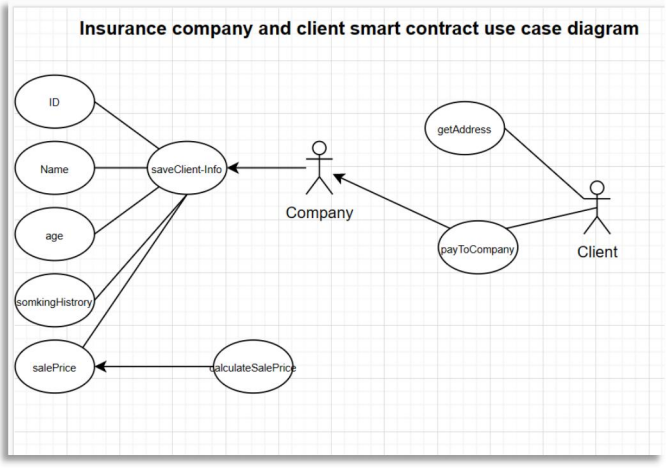
Question 2

Nowadays cryptocurrency and smart contracts become more and more important and popular in people's live. Therefore there are some pros and cons for governments and banks. As we know that cryptocurrency eliminates the third-party clearinghouse, thus, cut down the cost and time delay. All the transaction over cryptocurrency platforms, whether domestic or international, are equal. In addition, cryptocurrencies offer users a reliable means of money exchange outside the direct control of national or private banking systems. Banks' position is somewhat in jeopardy as a result. In other words, as cryptocurrencies gain popularity, the influence of governments will gradually decline. On the other hand, We are aware that the fact that nobody regulates cryptocurrencies. Without government oversight there are people who are using cryptocurrencies to launder money and so on for illegal activities.

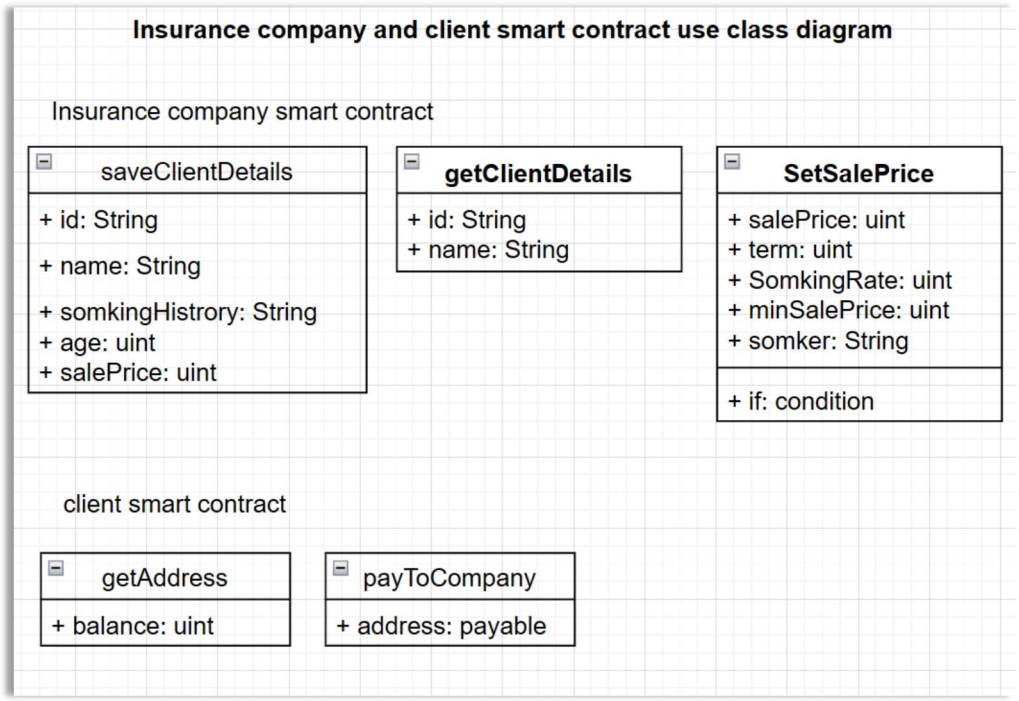
Question 3

There are 4 design principles when create a smart contract.

Firstly, define the contents of a smart contract and make a design specification.



Secondly, define user's stories by using UML diagram which include "use case diagram and class diagram" to represent the design.



Thirdly, defines the data assets, peer participants and their roles, rules to be enforced, and transactions to be recorded for the system which is designing

Finally,defines a contract diagram that specifies the name, data assets, functions, and rules for execution of functions and access to the data.(more detail,click here to check github smart contract code)

Question 4

1. As we know that there is not any such a law for Blockchain technology and unsupervised as well. Therefore nobody take the responsibility for the data in Blockchain.

2. Furthermore that data in Blockchain which cant be changed, but no one can make sure all data are true.

3. In addition in European Data Protection that claim everyone has right to be forgotten, but the immutable nature of Blockchain conflicts with this.

4. On other hand,Blockchain is distributed and decentralized management, which no need any third parties.

5. Blockchain does not require a trust system.

6. The block chain adopts one-way hash algorithm, and each newly created block advances in strict chronological order. The irreversibility of time leads to any attempt to invade and tamper with the data information in the block chain can be easily traced, resulting in rejection by other nodes, so as to limit relevant illegal behaviors.

Reference

1. Smart Contracts.Act 2000 (the Act). Dr. Muhammad Iqbal ..\Lecture 6 - Smart Contracts.pdf(Page9-14)