cct | College Dublin
Computing • IT • Business

CCT College Dublin Continuous Assessment

Module Title:	Distributed Digital Transactions
Assessment Title:	CA2
Lecturer Name:	Dr. Muhammad Iqbal
Student Full Name:	Leisly Alitzel Pino Duran
Student Number:	2020303
Assessment Due Date:	8th of January 2023
Date of Submission:	8th of 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.

Table of contents

Question 1

Briefly explain the purpose of Blockchain technology for crypto currency and its impact for different applications. Compare the characteristic difference between two cryptocurrencies, such as Bitcoin and Ethereum.

Blockchain technology provides cryptocurrencies with a high-security system that can prevent the same digital asset from being transferred twice or counterfeited. Blockchain technology works like an outstanding digital ledger of transactions where vast amounts of information can be recorded and stored. All of it is shared on the network and protected so that all the data it houses cannot be altered or deleted.

The security provided by these transactions has motivated several industries to apply Blockchain technology in the services they provide, for example:

Cloud storage: Cloud storage based on the Blockchain allows the creation of nodes in different geographical locations capable of withstanding any server's fall. This decentralization of information supports data integration, overcoming one of technology's most challenging challenges: data longevity. Companies like Microsoft and Amazon are developing Blockchain as a Service (BaaS), a cloud-based service that allows users to create their products using Blockchain technology.

Medical Services: Healthcare companies like Medicalchain are embracing this technology to help patients centralize their medical records.

Digital identities: The chain of blocks provides a uniquely secure and immutable system that is the optimal solution to the problem of identity theft.

Registration and data verification: Establishing a new, more secure registration method for users.

Supply chains: Blockchain technology as logistics management, food chains supervision, or production monitoring. In countries like the United Kingdom, 22% already use applications of this nature.

Automated security: The incorruptibility of the Blockchain allows the information that is required to be obtained without paying attention to security flaws that can lead to data theft. In addition, the surveillance system can use throughout the day without the possibility of the server going down.

Voting system: Some Nations consider the Blockchain as a new way of proposing democracy, obtaining a new framework for regulating the voting system from this application. The USA applied this technology in the state of Virginia.

The following table shows the comparison of the cryptocurrency ADA and XRP:

Features	Cardano ADA	Ripple XRP
Released	2015	2012
Founders	Charles Hoskinson	Ryan Fugger, Chris Larsen and Jed McCaleb
Purpose	DApps	Transactions
Scalability	Medium	High
Blockchain	Cardano	XRP Ledger
Supply	45 billion	100 billion
Consensus algorithm	Peer-of-Stake	XRPL Consensus
Decentralised network	High	High
Type	Layer 1	Layer 1
Smart Contracts	Yes	Yes
Transactions per second	270	1500
Mining Capability	No	No
Transaction speed	60 seconds	3-5 seconds
Scripting Language	Plutus	C++/JavaScript
Energy consumption	48,851 kWh	474,000 kWh
Market Cap Rank	9	6

Question 2

Describe the current status of cryptocurrency and smart contracts for the organizations. Discuss their effects on society, the moral and legal implications.

The creation of cryptocurrencies facilitated the movement of currencies within and outside the limits of countries that exercise greater control over capital, and banks cannot impose restrictions on their movement—becoming a facility to acquire stablecoins in the market and fostering innovation in the financial market, opening various possibilities for developing countries and paving the way for Smart contracts. This allowed companies not precisely in the financial sector to incorporate cryptocurrencies as a payment method, such as Starbucks, Norwegian, Microsoft, Bitrefill, Destinia, Shopify, and Moon, among others.

Smart contracts are computer programs stored on blocks executed when predetermined conditions are met. They are usually used to automate the execution of a deal so that all participants can be immediately sure of the result without the involvement of any intermediary or loss of time. They can also automate a workflow, activating the following action when the conditions are met and providing benefits such as speed, efficiency and precision in their programming, trust and transparency since there are no third parties, security in their encrypted transactions and at a low cost. . One example is Pharma Portal, developed by IBM Blockchain Transparent Supply is a Blockchain-based platform that tracks temperature-controlled pharmaceuticals through the supply chain to provide reliable and accurate data across multiple parties.

Smart contracts present difficulties in verifying the parties' capacity and determining the jurisdiction in case of conflict; in this last point, the criterion is shared that later this matter can be resolved within the same Blockchain network by the nodes or pairs. Smart contracts are a sample of the changes that have been generated in the law as a result of globalization and technological advances, where the State has lost the regulatory monopoly, finding itself within the diversity of regulations which are outside the State, giving quick and effective responses to new situations that the State has been slow to understand and therefore to regulate.

For Smart contracts to be considered contracts from a legal point of view, they must meet the essential requirements of any contract under the legal doctrine. Significantly, consent marks the birth of the contract, which materializes with the typical manifestations of wills expressed by the parties. Courts establish as conditions of agreements:

1. A conspicuous notice of the terms of use for an online transaction
2. An express warning that continuing with the transaction would bind the party to the terms
3. An express acceptance by the user of the terms and conditions at the time of account creation

All these conditions protect the legal weak, which would be the consumer and his right to be informed.

Smart contracts are valid contracts based on the autonomy of the parties that establish their conditions in a virtual environment using Blockchain technology; they have the potential to continue developing, presenting challenges to the law. It may be that in the future, the mechanisms for resolving conflicts generated between the parties will be established within the same Blockchain technology, without the need to go to the state jurisdictional system; and not for this reason, they stop being contracts and found within the current complex legal order product of globalization, where not all the rules come from the State or are regulated by it. Except when there is a transfer of tangible properties of fundamental rights, to which legal systems establish formalities to produce legal effects, in which case, at most, a hybrid Smart contract can be used.

A hybrid Smart contract is when the parties can enter into a conventional contract and agree in it that specific obligations will be executed through a Smart contract on the Blockchain; in this way, once the established conditions are met, the contract will be self-executed, which will give greater security to the parties, and in case of disagreement, they may renegotiate and establish new clauses in the conventional contract.

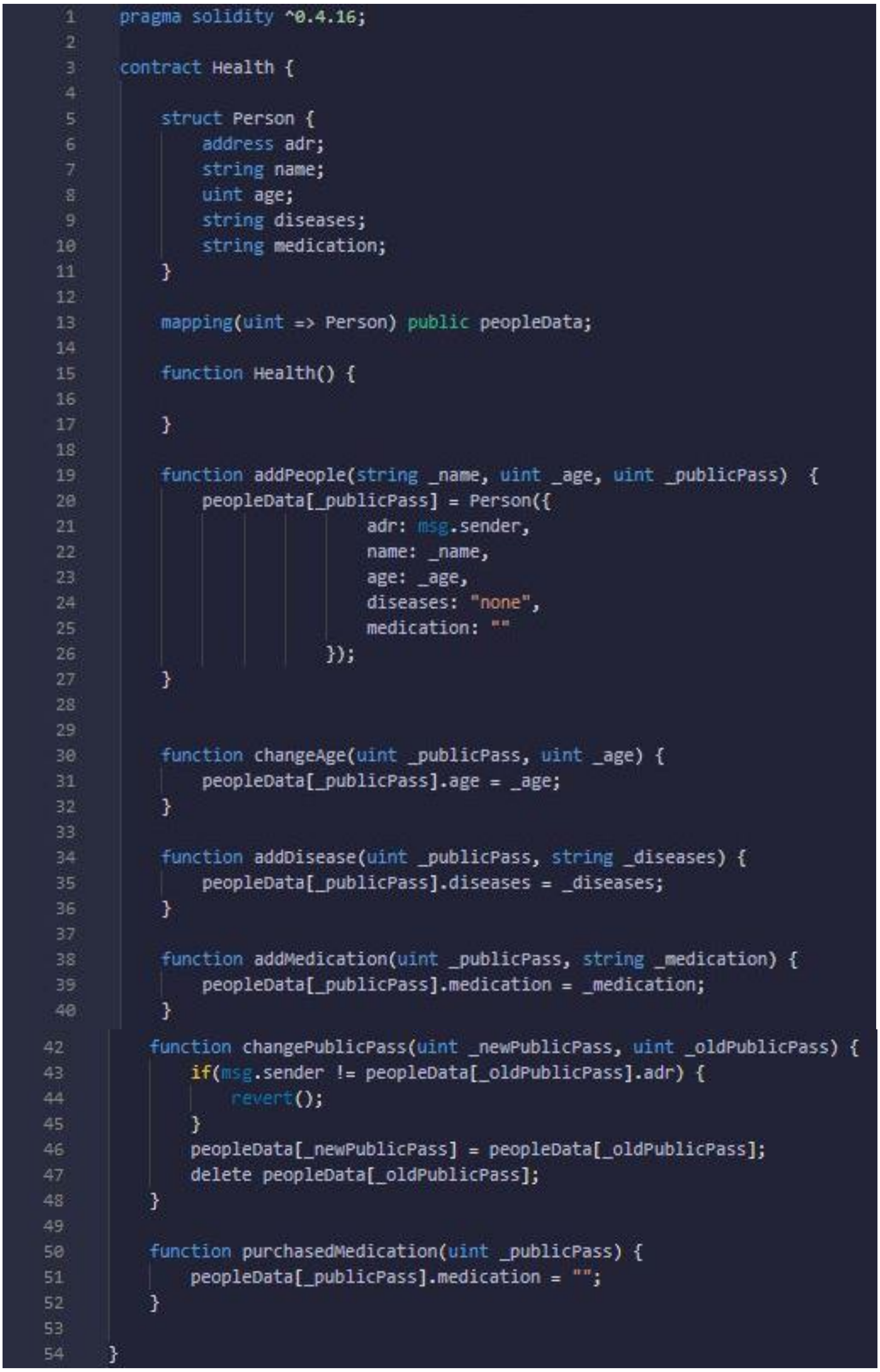
Question 3

Explain the design principles behind the smart contract. Consider a smart contract between the insurance company and the client or a similar scenario. Design and write the code using Solidity programming language or any other programming language.

To design a smart contract it is necessary:

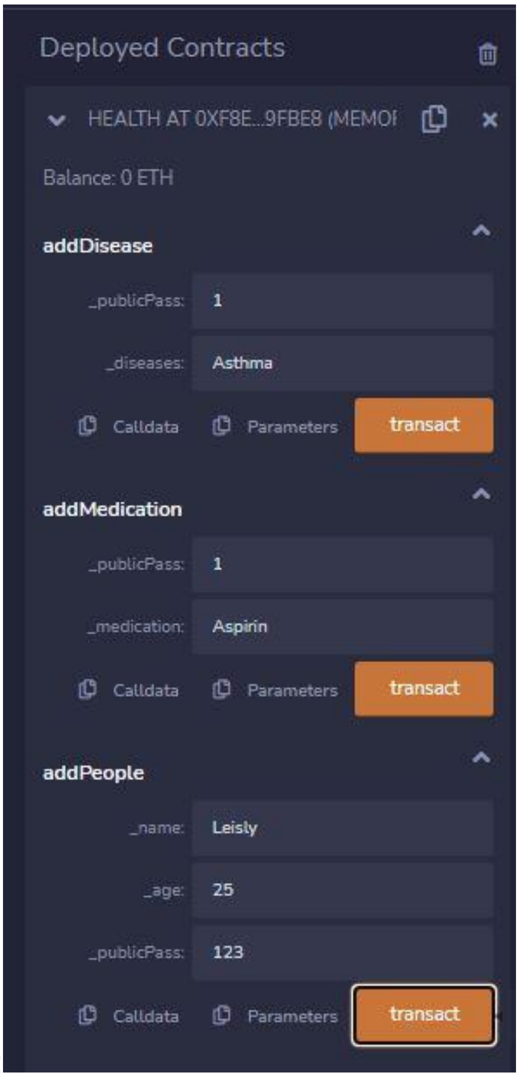
- **Identify Agreement:** Multiple parties identify the cooperative opportunity and desired outcomes and agreements could include business processes, asset swaps, etc.
- **Set conditions:** Smart contracts could be initiated by parties themselves or when certain conditions are met like financial market indices, events like GPS locations, etc.
- **Code business logic:** A computer program is written that will be executed automatically when the conditional parameters are met.
- **Encryption and Blockchain technology:** Encryption provides secure authentication and transfer of messages between parties relating to smart contracts.
- **Execution and processing:** In Blockchain iteration, whenever consensus is reached between the parties regarding authentication and verification then the code is executed and the outcomes are memorialized for compliance and verification.
- **Network updates:** After smart contracts are executed, all the nodes on the network update their ledger to reflect the new state. Once the record is posted and verified on the Blockchain network, it cannot be modified, it is in append mode only.

To carry out the example of a smart contract, take the idea of medical insurance where the patient, disease and medication records are kept. This could help keep track of the record of the people who contract the service and each person's background. The following code was designed in Solidity:



```
pragma solidity ^0.4.16;

contract Health {

    struct Person {
        address adr;
        string name;
        uint age;
        string diseases;
        string medication;
    }

    mapping(uint => Person) public peopleData;

    function Health() {

    }

    function addPeople(string _name, uint _age, uint _publicPass)  {
        peopleData[_publicPass] = Person({
                        adr: msg.sender,
                        name: _name,
                        age: _age,
                        diseases: "none",
                        medication: ""
                    });
    }


    function changeAge(uint _publicPass, uint _age) {
        peopleData[_publicPass].age = _age;
    }

    function addDisease(uint _publicPass, string _diseases) {
        peopleData[_publicPass].diseases = _diseases;
    }

    function addMedication(uint _publicPass, string _medication) {
        peopleData[_publicPass].medication = _medication;
    }
    function changePublicPass(uint _newPublicPass, uint _oldPublicPass) {
        if(msg.sender != peopleData[_oldPublicPass].adr) {
            revert();
        }
        peopleData[_newPublicPass] = peopleData[_oldPublicPass];
        delete peopleData[_oldPublicPass];
    }

    function purchasedMedication(uint _publicPass) {
        peopleData[_publicPass].medication = "";
    }

}
```

The Smart contract was executed and connected in Ganache:



Balance: 0 ETH

addDisease

_publicPass: 1

_diseases: Asthma

addMedication

_publicPass: 1

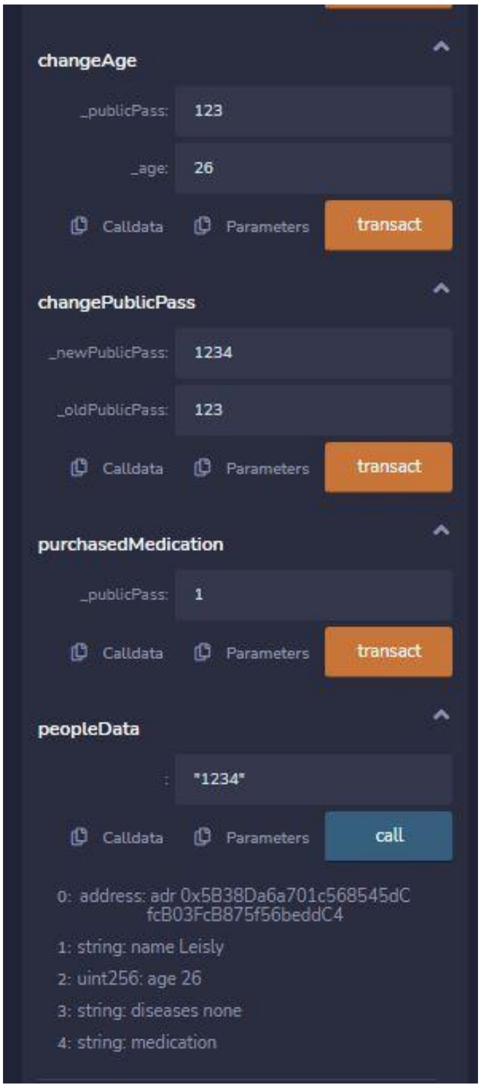
_medication: Aspirin

addPeople

_name: Leisly

_age: 25

_publicPass: 123



changeAge

_publicPass: 123

_age: 26

changePublicPass

_newPublicPass: 1234

_oldPublicPass: 123

purchasedMedication

_publicPass: 1

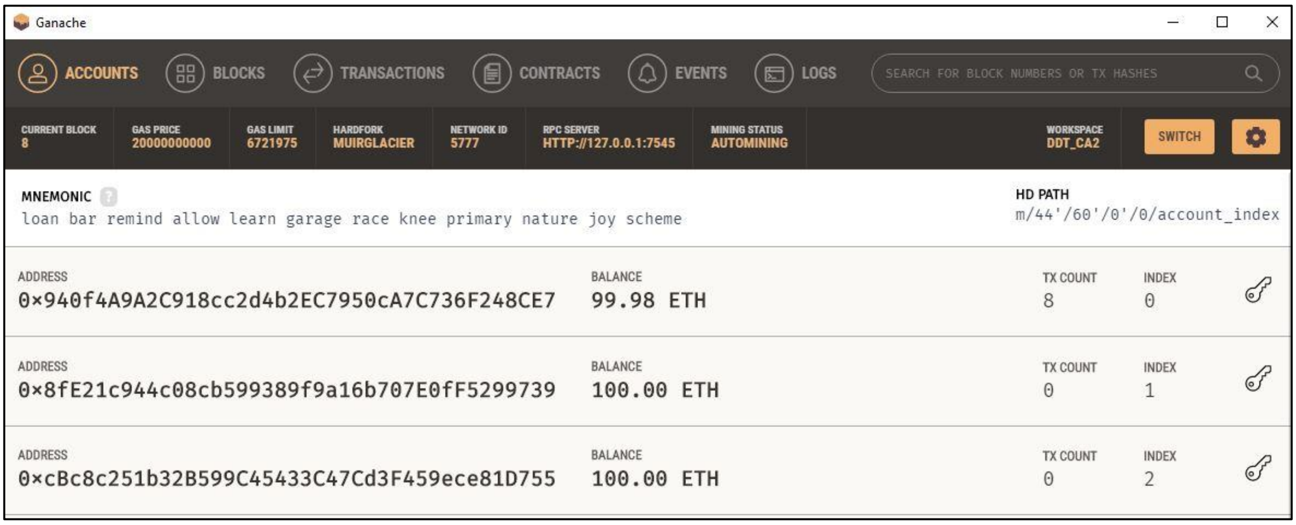
peopleData

: "1234"

```
0: address: adr 0x5B38Da6a701c568545dC
            fcB03FcB875f56beddC4
1: string: name Leisly
2: uint256: age 26
3: string: diseases none
4: string: medication
```

:

Ganache shows the interaction and creation of each block:

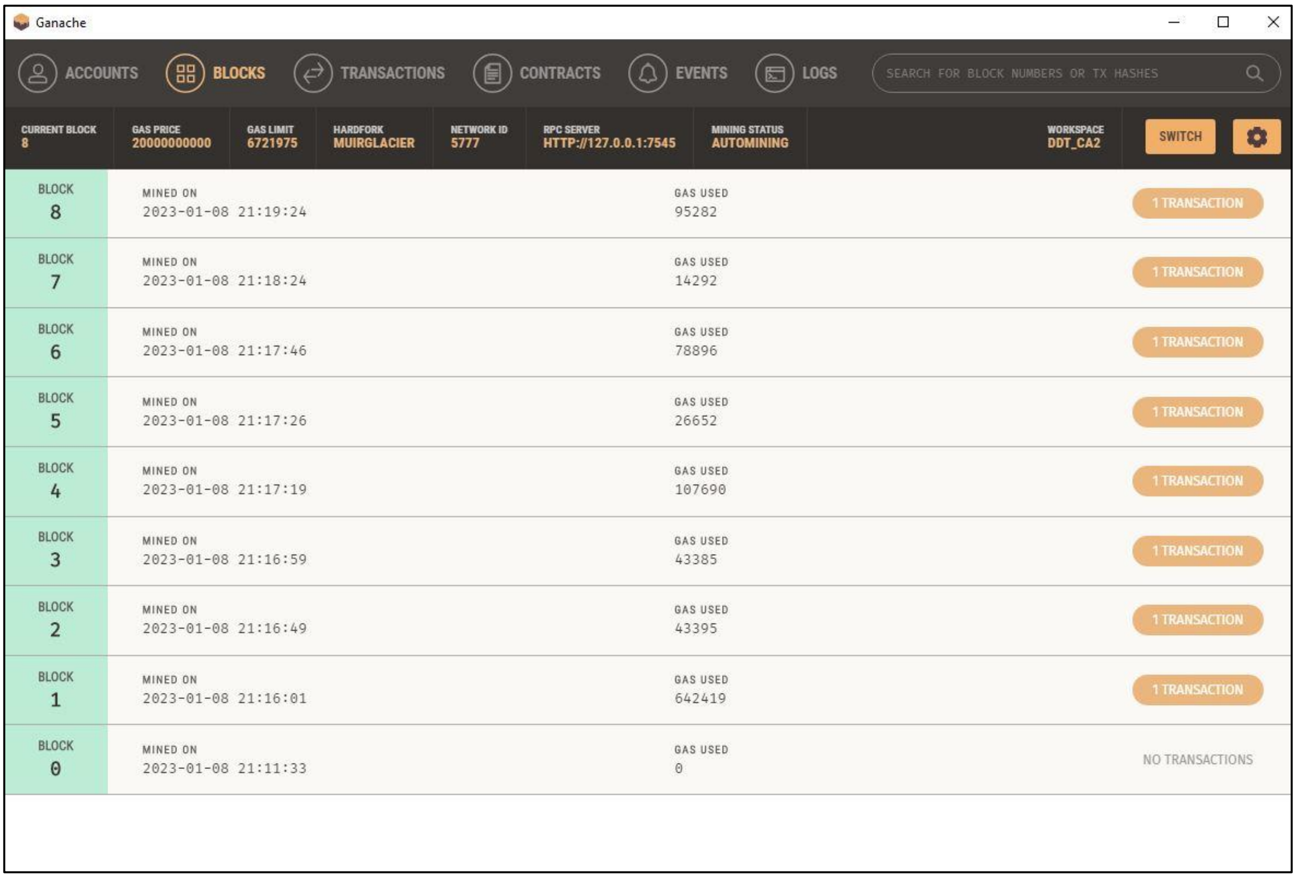


CURRENT BLOCK 8 | GAS PRICE 20000000000 | GAS LIMIT 6721975 | HARDFORK MUIRGLACIER | NETWORK ID 5777 | RPC SERVER HTTP://127.0.0.1:7545 | MINING STATUS AUTOMINING | WORKSPACE DDT_CA2

MNEMONIC
loan bar remind allow learn garage race knee primary nature joy scheme

HD PATH
m/44'/60'/0'/0/account_index

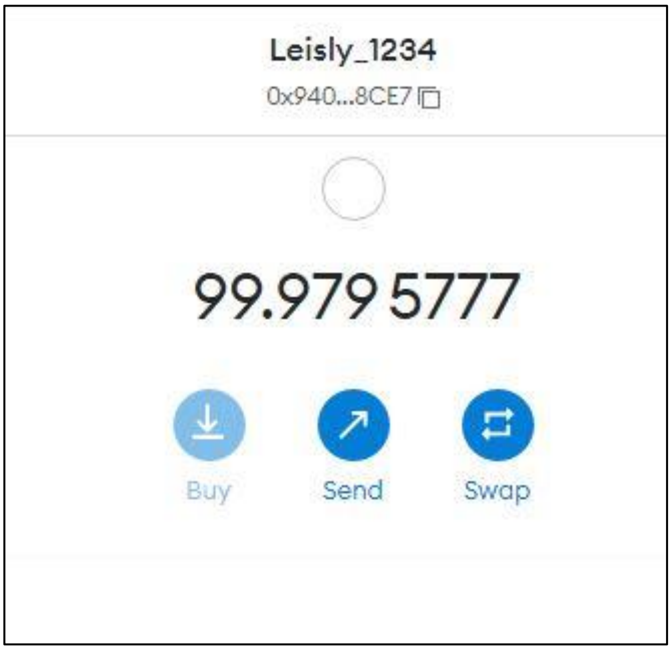
ADDRESS	BALANCE	TX COUNT	INDEX
0×940f4A9A2C918cc2d4b2EC7950cA7C736F248CE7	99.98 ETH	8	0
0×8fE21c944c08cb599389f9a16b707E0fF5299739	100.00 ETH	0	1
0×cBc8c251b32B599C45433C47Cd3F459ece81D755	100.00 ETH	0	2



CURRENT BLOCK	GAS PRICE	GAS LIMIT	HARDFORK	NETWORK ID	RPC SERVER	MINING STATUS	WORKSPACE
8	20000000000	6721975	MUIRGLACIER	5777	HTTP://127.0.0.1:7545	AUTOMINING	DDT_CA2

BLOCK	MINED ON	GAS USED	
8	2023-01-08 21:19:24	95282	1 TRANSACTION
7	2023-01-08 21:18:24	14292	1 TRANSACTION
6	2023-01-08 21:17:46	78896	1 TRANSACTION
5	2023-01-08 21:17:26	26652	1 TRANSACTION
4	2023-01-08 21:17:19	107690	1 TRANSACTION
3	2023-01-08 21:16:59	43385	1 TRANSACTION
2	2023-01-08 21:16:49	43395	1 TRANSACTION
1	2023-01-08 21:16:01	642419	1 TRANSACTION
0	2023-01-08 21:11:33	0	NO TRANSACTIONS

Through MetaMask, the account balance is checked for each interaction that was made:


Leisly_1234

0x940...8CE7

99.979 5777

Question 4

Explain the regulatory and ethical challenges that the Blockchain technology is experiencing currently. Discuss the advantages and disadvantages of Blockchain technology.

Deploying Blockchain technology presents significant economic and business challenges and, above all, sustainability. Since its applications are transversal, so are its challenges. The World Economic Forum defines the following challenges of Blockchain technology:

- **Challenges at the adoption level:** The low confidence of the general public in the system, its difficulties of use and the lack of knowledge make it difficult, for the moment, to implement it on a large scale.
- **Technological barriers:** Such as difficulties of scale or limitations to handle large volumes of transactions.
- **Cybersecurity risks:** Although it is a distributed and encrypted database, it still has some vulnerabilities to solve (such as those presented by authentication systems).
- **Legal and regulatory challenges:** The absence of legal frameworks is practically total. Added to this is the difficulty of deploying a global system on a planet with many different national and regional regulations.
- **Energy challenges:** One of the most talked about challenges lately. Blockchain validation processes require a large number of computational processes and are very energy intensive. Only the Bitcoin system currently consumes 0.35% of global energy. Alternatively, what is the same: all the energy that a small country like Austria needs.

Like any new technological tool that arises in accounting and transactions, it must be studied by auditors to understand its operation and carry out an analysis that allows concluding on the security of the transactions recorded in said tool.

However, implementing Blockchain is not an obstacle for the auditor but rather a new challenge of learning and adaptation. If a technological tool of the magnitude of Blockchain is well developed and implemented, it will make the auditor's work more efficient since it would eliminate the risk of manipulation of a transaction.

The Blockchain and Smart Contracts application will improve various controls, such as inventory control, payments, and cash flows, and reduce internal fraud risks.

The origin of Blockchain was looking for an opportunity to avoid the supervision of governments and regulators on economic activities. Decentralization and immutability, characteristics that time and facts have called into question from an ethical perspective, whether all those organizations born in Blockchain respond under all circumstances or if those who use this technology are responsible when the promises stipulated in a contract do not are met.

There are also jurisdictional challenges; Blockchains are global, and the laws of one country or state do not apply universally. Some challenges seem insurmountable, and it is convenient to have ethical rules adapted to this new technology.

BLOCKCHAIN	
Advantages	**Disadvantages**
Decentralization: This is the main characteristic of Blockchain technology and the decisive point around that to authenticate transactions or operations, and no other instance is required to act as an intermediary, reducing transaction validation times.	**High implementation costs:** Just as this technology represents low costs for users, unfortunately, it also implies high implementation costs for companies, which delays its adoption and implementation on a massive scale.
Network distribution: This point provides, at the same time, several benefits since, by having this distributed network, in the first instance, nobody owns the network, causing different users to have multiple copies of the same information at all times. Also, this characteristic makes it resistant and resilient to any failure since the fact that a node fails does not imply general failures in the network. In the same way, having a distributed	**Inefficiency:** Having several network users validate the same operations is inefficient since only one will receive the prize derived from this mining process. Said process, and for the same reason of many users doing precisely the same thing, also implies a considerable waste of energy and technology that is not very friendly to the environment.
	Private keys: Excessive security can also be an Achilles heel in private keys, as

network means that there are practically no errors because the information has to be verified by many participants in this network. Misinformation or malicious information within the Blockchain becomes practically impossible.	documented on many occasions. Losing them makes it almost impossible to recover these keys, causing a problem mainly for all those crypto security holders.
Low costs for users: The decentralized nature of the Blockchain allows for the validation of person-to-person transactions quickly and securely. Eliminating the need for an intermediary reduces costs for users.	**Storage:** As the number of users grows, the number of operations that will be integrated into the blocks that must be saved will also grow, so the space required will also have to increase within the miners' computers, eventually exceeding the capacity of hard drives.
	Unemployment: The lack of need for intermediaries will mean that, as Blockchain technology is adopted and implemented, all these intermediation sectors for validating payments and processes will necessarily be reduced to the point of disappearing. With this, the required jobs will disappear for it.

References

Advantages and disadvantages of the Blockchain | BBVA Switzerland [online]. BBVA.CH. [Accessed January 1, 2023]. Available at: https://www.bbva.ch/noticia/ventajas-y-desventajas-del-blockchain/

Anatomy of a Smart Contract - Blockchain Expo [online]. Blockchain Expo. [Accessed January 1, 2023]. Available at: https://www.blockchain-expo.com/2017/02/blockchain/anatomy-smart-contract/

Castrovilli, M., (2022). How bad is the current state of cryptocurrencies? An on-chain analyst explains [online]. Cointelegraph. [Accessed January 1, 2023]. Available at: https://es.cointelegraph.com/news/how-bad-is-the-current-state-of-crypto-on-chain-analyst-explains

Cryptocurrencies and blockchain in adolescence [online]. SciELO - Scientific Electronic Library Online. [Accessed January 5, 2023]. Available at: http://www.scielo.edu.uy/scielo.php?script=sci_arttext&amp;pid=S2393-61932022000100117

Design Considerations For Blockchain Smart Contracts [online]. HCLTech: Supercharging Progress | Digital, Engineering and Cloud. [Accessed January 5, 2023]. Available at: https://www.hcltech.com/blogs/design-considerations-blockchain-smart-contracts#:~:text=13%20key%20design%20principles%20for%20smart%20contracts&amp;text=This%20includes: ,upgrade,%20bug%20fixes%20and%20improvement

EOS vs. Cardano - Detailed Comparison of These Two Crypto! [online]. Blockhunters.io - We secure your blockchain code! [Accessed January 1, 2023]. Available at: https://blockhunters.io/eos-vs-cardano-detailed-comparison-of-these-two-crypto-titans/

Franco Degiovanangelo - fdegiovanangelo@bdo.com.uy, (2021). Blockchain Audit [online]. Welcome to BDO Uruguay - BDO. [Accessed January 2, 2023]. Available at: https://www.bdo.com.uy/es-uy/publicaciones/publicaciones/tecnologia-blockchain-un-nuevo-desafio-para-la-auditoria

Santander, (2021). What are cryptocurrencies and how do they work? [online]. Santander Corporate Website. [Accessed January 1, 2023]. Available at: https://www.santander.com/es/stories/guia-para-saber-que-son-las-criptomonedas#:~:text=Las%20criptomonedas%20funcionan%20mediante%20el,occasions%20o% 20that%20is%20falsified.

Smart Contract Design Patterns Explained | Hedera [online]. Hedera. [Accessed January 5, 2023]. Available at: https://hedera.com/learning/smart-contracts/smart-contract-design-patterns

Smart Contract Patterns - Blockchain Patterns [online]. Blockchain Patterns. [Accessed January 8, 2023]. Available at: https://research.csiro.au/blockchainpatterns/general-patterns/contract-structural-patterns/#:~:text=Smart%20contracts%20are%20programs%20running,impact%20on%20its%20execution%20cost .

Smart Contracts and legal analysis [online]. Occam Digital Agency - Inbound Marketing Madrid. [Accessed January 8, 2023]. Available at: https://www.occamagenciadigital.com/blog/smart-contracts-y-el-analisis-juridico

Smart Contracts in Blockchain - GeeksforGeeks [online]. GeeksforGeeks. [Accessed January 2, 2023]. Available at: https://www.geeksforgeeks.org/smart-contracts-in-blockchain/

The 3 areas of greatest impact of the Blockchain [online]. Zoho Blog. [Accessed January 8, 2023]. Available at: https://www.zoho.com/blog/es-xl/opinion/las-3-areas-de-mayor-impacto-del-blockchain.html

What are smart contracts on the blockchain? | IBM [online]. IBM - Deutschland | IBM. [Accessed January 8, 2023]. Available at: https://www.ibm.com/es-es/topics/smart-contracts

What is ADA: Characteristics and Opinions of Cardano [2023] [online]. No Commissions: The most honest Comparator on the market. [Accessed January 5, 2023]. Available at: https://sincomisiones.org/trading/ada-cardano