ÇANKAYA UNIVERSITY
FACULTY OF ENGINEERING
COMPUTER ENGINEERING DEPARTMENT

Project Report
Version 1

CENG 407
Innovative System Design and Development I

<P201810 >
BLOCKCHAIN CONSENSUS SIMULATOR

Canay TAŞAR
Hanife Hazel GÜLLER
M.Mustafa ERCAN
Yağmur Ebrar ÖZYURT

Advisor: Öğr.Gör.Dr.Faris Serdar TAŞEL

Table of Contents

Abstract **5**

Özet: **5**

Introduction **6**

Problem Statement 6

Background or Related Work 6

Solution Statement 6

Literature Search **7**

İntroduction 7

Blockchain Network 8

Blockchain Consensus Algorithms 9

POW (Proof of Work) 9

POS (Proof of Stake) 9

Simulation Systems 9

Software Requirements Specification **11**

Introduction 11

Purpose 11

Scope of Project 11

Glossary 11

Overview of Document 12

Overall Description 12

Product Perspective 12

Development Methodology 12

User Characteristics 13

3.2.3.1 .User 13

3.2.3.1.1 13

User must read and understand English language due to simulation system language is English. 13
Requirements Specification 13
External Interface Requirements 13
User interfaces 13
Hardware interfaces 14
Software interfaces 14
Communications interfaces 14
Functional Requirements 14
Performance Requirements 14
Software System Attributes 14
Portability 14
Performance 14
Usability 15
Adaptability 15
Scalability 15
Safety Requirement 15
Software Design Description **15**
Introduction 15
Purpose 15
Scope 15
Glossary 15
Overview of document 16
Architecture design 16
Simulation Design Approach 16
Class Diagram 17

Architecture Design of Simulation 18
Network Menu 18
Node Menu 18
Simulation Menu 19
Activity Diagram 19
Use Case Realization 20
Conclusions **24**
Acknowledgement **24**
References **24**

Abstract
Blockchain is a concept that has gained popularity thanks to bitcoin. The most important reason for this system to come forward is that it is fast and reliable. In short, the blockchain describes the combination of the combination of data blocks with mixed functions. This block chain system is kept in an independent database that makes it faster and safer. It has a network that computers have access to and use of the database. The name of this network is P2P (Peer to Peer) network. server is not. Chain holds information. The chain is associated with the corresponding block before and after it with private encryption. Therefore, if a block changes in the ring, it becomes incompatible with all the previous blocks. In addition, consensus algorithms are used to secure networks. Consensus mechanisms enable a transaction in the blockade to be valid and unchangeable across the network. All transactions are stored in the recording section of the network so that everyone can enter and see it, ensuring complete transparency. In the introduction section; What is Blockchain? How is the data kept? Why are you using the consensus algorithm? How do I create network structures? And how can we simulate this system? Detailed information about the given questions. In the last part of this study, information is given about simulation systems and application to simulation systems.

Key words:
Blockchain, P2P(Peer to Peer), Consensus mechanism, Transaction.

Özet:

Blockchain, bitcoin sayesinde popülerlik kazanmış bir kavramdır. Bu sistemin öne çıkmasının en önemli nedeni hızlı ve güvenilir olmasıdır. Kısacası, blockchain veri bloklarının karışık fonksiyonlarla kombinasyonunu açıklar. Bu blok zincir sistemi daha hızlı ve daha güvenli kılan bağımsız bir veritabanında tutulur. Bilgisayarların veritabanına erişimi olan ve kullanan bir ağa sahiptir. Bu ağın adı P2P (Eşler Arası) ağıdır. sunucu değildir. Zincir bilgileri tutar. Zincir özel şifreleme ile kendisinden önce ve sonra gelen block ile ilişkilidir. Bu nedenle, halka içinde bir block değişirse, kendinden önceki tüm bloklarla uyumsuz hale gelir. Böylece block içinde değişiklik yapıldığı çok kolay bir şekilde anlaşılır. Ayrıca konsensüs algoritmaları, ağların güvenliğini sağlamak için kullanılır. Konsensüs mekanizmaları transaction işleminin ağ üzerinde geçerli ve değiştirilemez olmasını sağlar. Tüm işlemler ağın kayıt bölümünde saklanır, böylece herkes girebilir, görebilir ve tam şeffaflık sağlanır. Giriş bölümünde; Blok zinciri nedir? Veriler nasıl tutulur? Neden konsensüs algoritmasını kullanıyoruz? Blok zinciri ağ yapılarını nasıl oluştururuz? Ve bu sistemi nasıl simüle edebiliriz? Verilen sorular hakkında detaylı bilgi. Bu çalışmanın son bölümünde, simülasyon sistemleri ve simülasyon sistemlerine uygulama hakkında bilgi verilmiştir.

Anahtar Kelimeler:
Blok zinciri, P2P, Konsensüs mekanizması, Transaction.

1. Introduction

1.1 Problem Statement

Consensus is needed to send money in the blockchain. People need to establish their own consensus for the approval process because of the problem of trust. The structure of this control also makes blockchain. We looked at the most popular consensus mechanisms of the POW and POS algorithms, and we found that none of them were absolutely perfect, but that each had power. Therefore, algorithms must be updated and completed continuously.

1.2 Background or Related Work

Blockchain is a distributed database that contains a list of growing data records and records that are protected as encrypted. The passwords generated by the hash functions for each block are fixed length and unique for each block. The operation is issued for validation to the peer-to-peer network of computers running the block chain. Each node in the network contains a transaction that verifies whether the operation is valid.

1.3 Solution Statement

Our project aim is to model and simulate Blockchain for a real process or system to work within a certain period of time. We will examine how we connect the network. We will determine the connection of the nodes, the number of nodes and how much they are connected. We will determine which algorithms will work in network. We'll check the transaction fee range. The user will have features such as speeding up and stopping the simulation and slowing backwards or going backwards or forwards.

2. Literature Search

2.1 İntroduction

A pseudonymous software developer going by the name of Satoshi Nakamoto proposed bitcoin in 2008, as an electronic payment system based on mathematical proof [3].The aim here is to create a virtual currency that is not connected to any central authority through the internet.With this virtual currency, we can make all the monetary transactions that we perform with the currencies we use.Therefore, crypto coins are widely used today in many different areas.

Another popular virtual currency is the ethereum.Ethereum is an open platform that enables developers to build and deploy decentralized applications such as smart contracts and other complex legal and financial applications [1].

The blockchain can be thought of as an electronic mail system that enables the transfer of digital coins (bitcoin, ethereum etc.).Details on the subject are explained in the first part of the article.

There are blocks where data is held, and the first block is called "Genesis Block". This block is considered the beginning of the blockchain.

Each block in the block chain is connected cryptographically. They also use hash functions to provide this connection. Hash functions work as an inter-block validation mechanism. The Hash functions encrypt data in a way that's hard to predict, thus providing data security.

The blockchain has a scattered database. The communication between the nodes connected to this database is provided by the P2P (peer to peer) network. Details on the subject are explained in the second part of the article.

Blockchain operations are seen by everyone. This also makes the network vulnerable to attacks. Details on the subject are explained in the third part of the article.

2.2 Blockchain

The biggest reason why Blockchain technologies are more popular these days is the success of bitcoin. Blockchain, also known distributed ledger, is used in many different areas such as banking, real estate sector and education. İmportant steps are being taken to expand its use blockchain. In the past two years, leading financial institutions have taken a quick step and set a new direction to collect blockchain guides and evidence of concepts.

At the same time, they financed software competitions in cooperation with financial technologies, opened innovation labs, participated in the consortium and worked with regulatory institutions to lay the groundwork for blockchains.

Blockchain is a shared, trusted, public ledger of transactions that everyone can inspect but which no single user controls [2]. The lack of a central authority also creates a safer

environment between the sender and the receiver. Blockchain is a distributed database that has an ever-growing list of data records and maintains these records cryptographically [2].

The ledger is built using a linked list, or chain of blocks, where each block contains a certain number of transactions that were validated by the network in a given timespan [2].

Each block on the blockchain keeps information such as time, data, hash and previous hash.The blocks form a chain with the hash information. The hash information of the blocks has been created according to certain rules. According to these rules, passwords created with hash functions for each block should be fixed length and these passwords must be unique for each block.

The crypto-economic rulesets of the blockchain protocol (consensus layer) regulate the behavioral rulesets and incentive mechanism of all stakeholders in the network [2].

2.3 Blockchain Network

Architectures developed using P2P (peer to peer) networks and block chains contribute to cyber security.

1) A blockchain transactions starts by accepting to send data to one side. These data could be anything. But because the point of a blockchain is to create a permanent, verifiable record of exchange, the data usually represent some valuable asset. Common examples: units of a cryptocurrency or other financial tool; contracts, deeds or records of ownership.

2) The transaction is broadcast for verification to a peer to peer network of computers operating the blockchain. Every node on the network is furnished with a process for verifying whether the transaction is valid or not. (In a Bitcoin transaction, for example, the network would verify whether those paying actually have the amount of Bitcoins they say they do.) Once the network has reached a consensus, algorithms package up the validated transaction with other recent transactions into a block.

3) Software creates a “fingerprint” for the new block by hashing the data inside it, together with two other pieces of information: the fingerprint of the preceding block and a random number called a nonce.

4) Specific nodes called miners begin competing with one another for the right to add the new block to the blockchain. Their computers perform a tedious set of hash based calculations over and over again by trial and error, hoping to generate a solution that satisfies an arbitrary rule defined by the network. (On the Bitcoin blockchain, the miners are searching for solutions—or “hash values”—that have a particular number of zeros at the beginning.) Whoever is first to

complete this proof of work process and find the matching solution successfully “mines” that block, earning a financial reward.

5) The validated block is added to the blockchain with a digital fingerprint that also mathematically encodes the validated fingerprints of every block preceding it. These nested fingerprints make the blockchain increasingly secure with every new block that gets added because altering a single bit of information anywhere in the blockchain would drastically change not only the fingerprint of that particular block but every subsequent one in the chain as well.

2.4 Blockchain Consensus Algorithms

The blockchain consensus algorithms are speed, applications, and potential. These algorithms identify issues such as network security and environmental friendliness. In distributed architecture, they must provide a consensus between the blocks on each node to be the same. Proof of Work (POW) and Proof of Stake (POS) approaches are commonly used to provide consensus.

2.4.1 POW (Proof of Work)

Bitcoin and Ethereum use proof-of-work (POW) consensus algorithm. POW is primarily a protocol to block cyber-attacks on the network. Usually used for comprehensive mining operations. POW, a consensus algorithm is used to access the same consensus. The solution to the problem in POW is easy to confirm but difficult to solve. In the case of POW algorithms, it is necessary to solve the problems of miners to add blocks to the chain. The problem is first to add the unblocking block to the chain. Significant detail, processing power and number of miners in the POW algorithm. In theory, this algorithm becomes safer as processor power and number of miners increase. To increase the potential in Proof of Work, mining is required. We can increase the number of devices we are mining, or we need to replace those devices with high performance devices.

2.4.2 POS (Proof of Stake)

Proof of Stake is the crypto money infrastructure algorithm. Pos is fast and efficient. PoS coins are produced at the beginning of the system and are sent to the wallets at certain intervals according to the investment made. In our pos electronic wallet we only need to keep the money. Pos is a way of accessing the distributed consensus. It makes less computations in pos studies, so it is less laborious and low cost. With pos, miners can control some of their money by placing them on the process block. If the cost of the coin you buy from the Proof Of Stake system goes down too much, your earnings rate will be reduced.

2.5 Simulation Systems

A simulation is to model and simulate the operation of a real process or system within a certain period of time. It is an animation that allows us to fully see the process in real life without risking our current performance. Simulation enables the generation of the artificial history of a system. It leads to the making of inferences by utilizing the produced system. Today, the

behavior of a developing and developing system is developed by developing a simulation model.This model makes a number of assumptions about the operation of the system.

Simulation is a unique approach to making confident, evidence-based decisions that will increase the efficiency and profitability of a product. So how does the simulation work ? Simulation is an effective technique to simulate an existing or proposed system (process). The simulating software allows us to create a visual representation of our process, similar to the flowchart. The activities and resources we add tell the simulation to imitate real life behavior.

So what can we simulate? Their simulations are often used to experiment in real life. The greatest benefit is to simulate any complex or costly process. These may include ambiguous, complex interactions, or product variants with random variability. Using simulation, we can quickly test our ideas about the product.

The application and design of the simulators is as complex as the simulated program. It has been a concerted effort to implement the latest developments in order to eliminate the increasing complexity. These efforts have led to simulators that are easy to maintain and develop.

The most important paradigm that is currently used to implement simulators is the generation-oriented paradigms. While we are building Blockchain Consensus Simulator, we are one of the object oriented paradigms. [4]

2.5.1 ADVANTAGES OF SIMULATION

Simulators have many advantages.If we take a look at these advantages, the systems we simulate most provide practical feedback to users. These simulated systems enable us to obtain information about the product and to determine the accuracy and efficiency. One of the main advantages of simulators is that they can provide practical feedback to users when designing real-world systems. Simulators are frequently used in teaching or demonstrating concepts. And this is seen as another effective benefit of simulators. Simulated systems dynamically display their behavior and relationships. Thus, the system is explained to the user in a meaningful way.

If we briefly summarize the main advantages of the simulation; Provides a virtual environment without building a system. The system helps users to find their behavior.

2.5.2 DISADVANTAGES OF SIMULATION

When designing a simulation, measuring how a system affects other system can be expensive to build the model. To be able to simulate a system, all factors on the system must know.

Without this information, we cannot create a simulation. Another disadvantage is that the results of some simulations can be complex and difficult to interpret. [5]

3. Software Requirements Specification

3.1 Introduction

3.1.1 Purpose

The purpose of this document is to test the behavior of a blockchain consensus simulator consensus algorithm and observe the main blockchain and fork, we have developed a decentralized blockchain network, which makes it possible to generate and simulate the transmission of transaction orders. This system can also be used to monitor the effects of blockchain based system applications.

3.1.2 Scope of Project

Nowadays, the software used for blockchain based systems is insufficient in many ways.For this reason, having an easy user interface has created the need for an application to modify the basic parameters to create a network and to observe the behavior of the consensus algorithm.

This project will benefit from the communication between block chains, it gives permit a reliable entry into the framework through a system. Then the user can access the process and enter the data to perform operations. during these operations, The PoW and PoS algorithms in the background control the security status, the network, and the transfer is completed safely.

3.1.3 Glossary

This subsection should provide the definitions of all terms, acronyms, and abbreviations required to properly interpret the SRS. This information may be provided by reference to one or more appendixes in the SRS or by reference to other documents. Example:

Table 1 Glossary of SRS

Term	Definition
Algorithm	is the one and only version of the truth. It keeps powerful adversaries from derailing the system and successfully forking the chain. The most widespread form of consensus algorithm is Bitcoin's Proof of Work and involves contributing power in the form of computing capacity measured as hash rate. The most common alternative to POW of Proof of Stake.
Cryptography	Cryptography is the encryption and decryption of data.

Ethereum	Ethereum is an open software platform based on blockchain technology that enables developers to write smart contracts and build and deploy decentralized applications.
Hash function	A function that maps data of an arbitrary size. Used to create a “digital ID” or “digital thumbprint” of an input string.
P2P (Peer to Peer)	Denoting or relating to computer networks in which each computer can act as a server for the others, allowing shared access to files and peripherals without the need for a central server
Proof of Stake (POS)	A consensus algorithm that chooses the owner of a new block based on the wealth they have or (Stake). There is not a block reward so the forgers take the transaction fee.
Proof of Work (POW)	A consensus algorithm which requires a user to “mine” or solve a complex mathematical puzzle in order to verify a transaction. “Miners” are rewarded with Cryptocurrencies based on computational power.

3.1.4 Overview of Document

The second part of the document shows the functions of our system and the usage status of each function. Requirement Specification chapter is written for software developers and explained details of the functionality of the blockchain simulation system.

3.2 Overall Description

3.2.1 Product Perspective

The purpose of the blockchain consensus simulation is to simulate the operations on the block chain structure. User is not authorized to change the system after logging in.The administrator is also responsible for the transfer manipulations in the system. This project is a desktop application developed using java language.

3.2.2 Development Methodology

For developing the project, we have planned to use Scrum which is an agile software development methodology. The Scrum method offers us a simple but flexible management phase, rather than specifying the steps that need to be followed in detail in the project when developing a project [6]. Particularly, it is possible to change this process while splinters are moving. Scrum is also divided into sprints to complete the time required for the main work to be done. There are tasks for team members in the split. At the end of each splint, the necessary

tests are carried out. This allows us to reduce the errors that may occur during the development of the software. For these reasons we decided to develop our project with Scrum which is an agile software development methodology. We have created a Scrum Board to complete the tasks defined in the project. So that we have made the distribution of tasks and the need to complete the time we have divided the splints. After each period is completed, necessary tests are performed.

3.2.3 User Characteristics

3.2.3.1 .User

3.2.3.1.1

User must read and understand English language due to simulation system language is English.

3.2.3.1.2

User must know how to use a computer.

3.3 Requirements Specification

3.3.1 External Interface Requirements

The user interface will be worked on Windows. The blockchain consensus simulation work with java language. So requires necessary drivers installed within the operating system in PC. There are no external software interface requirements. There are no external communications interface requirements.

3.3.1.1 User interfaces

The user will see the Create random network, delete network, add node, and select node options in the interface when the program opens.If you want to be a network, click Create random network button.To create a network, it must select one of the POW or POS algorithms.Then, the number of nodes, the number of edge, and the percentage of connections between them must indicate.

If the user wants to add a node to the network, the user must click the add node button.After the user has added the node, add the node.If the user is using the PoW algorithm, the hashrate value must be entered, if the PoS algorithm is using the stack value must be entered.If the user wants to add or set transaction, the user must click the enter transaction and set transaction buttons.

If the user wants to delete the network, click the Delete network button.

If the user wants to select the node, click the select node button. The user can perform delete edge, delete node, change hashrate or delete and add transaction operations through this node.

The user can stop the simulation, play, rewind and forward.

3.3.1.2 Hardware interfaces

No hardware interfaces needed to run this software.

3.3.1.3 Software interfaces

Software presented in this SRS only needs an Windows Operating System.

3.3.1.4 Communications interfaces

There is not an internet connection is required to run this software.

3.3.2 Functional Requirements

- ➔ The user must create a network using the POW and POS algorithms.
- ➔ The user can delete an existing network.
- ➔ The user can stop or play the simulation.
- ➔ The user can add or delete node and edge.

3.3.3 Performance Requirements

The simulation system should run smoothly without any delay. Therefore, the features of the user's computer affect the speed of the system.

1. GPU: 2.30 Ghz

2. CPU: Intel i5-6200U / Intel Core or better

3. RAM: 4 GB or more

4. Operating system: Windows 7, Windows 8.1 or later, Windows 10

3.3.4 Software System Attributes

3.3.4.1 Portability

Blockchain consensus simulator is designed for using Java Language. This project system is running on all computers with windows operating system.

3.3.4.2 Performance

With the application developed in this project, using the tools in the system can quickly create the system and test the system it creates.

3.3.4.3 Usability

In this system, which has a simple interface, the user can see the results of the changes he made in the system as a message.

3.3.4.4 Adaptability

This system is no adaptability requirement.

3.3.4.5 Scalability

This system is no scalability requirement.

3.3.5 Safety Requirement

This system is no safety requirement.

4. Software Design Description

4.1 Introduction

4.1.1 Purpose

The purpose of this document is to test the behavior of a blockchain consensus simulator consensus algorithm, to examine Pow Pos algorithms closely, processing speeds and observe the main blockchain and fork, we have developed a decentralized blockchain network, which makes it possible to generate and simulate the transmission of transaction orders. This system can also be used to monitor the effects of blockchain based system applications.

4.1.2 Scope

Nowadays, the software used for blockchain based systems is insufficient in many ways. For this reason, having an easy user interface has created the need for an application to modify the basic parameters to create a network and to observe the behavior of the consensus algorithm.

With this project, we will simulate the blockchain consensus, the POW and POS algorithms used, and how the mining process takes place. We will use the Java language and GUI (Graphical User Interface) to simulate our simulation. The GUI is an interface for visual communication between the program and the user. The Java programming language uses AWT and Swing libraries for GUI. The swing library has all the tools you need to write portable applications that are easy to use. We plan to use the swing libraries for our project.

4.1.3 Glossary

Example glossary for SDD.

Table 2 Glossary of SDD

Term	Definition
BLOCK DIAGRAM	The type of schema which the components in the system are displayed in blocks
SDD	Software Design Document.
UML DIAGRAM	It is a modelling language which is used in Software Engineering.
POW	A proof of work is a piece of data which is difficult (costly, time-consuming) to produce but easy for others to verify and which satisfies certain requirements. Producing a proof of work can be a random process with low probability so that a lot of trial and error is required on average before a valid proof of work is generated.
POS	Proof of Stake is one of the commonly used consensus protocols within blockchain technology.

4.1.4 Overview of document

This document describes the software design we will use for blockchain consensus simulation. In the architectural design section, we showed the whole structure of the system and how it was installed.

4.2 Architecture design

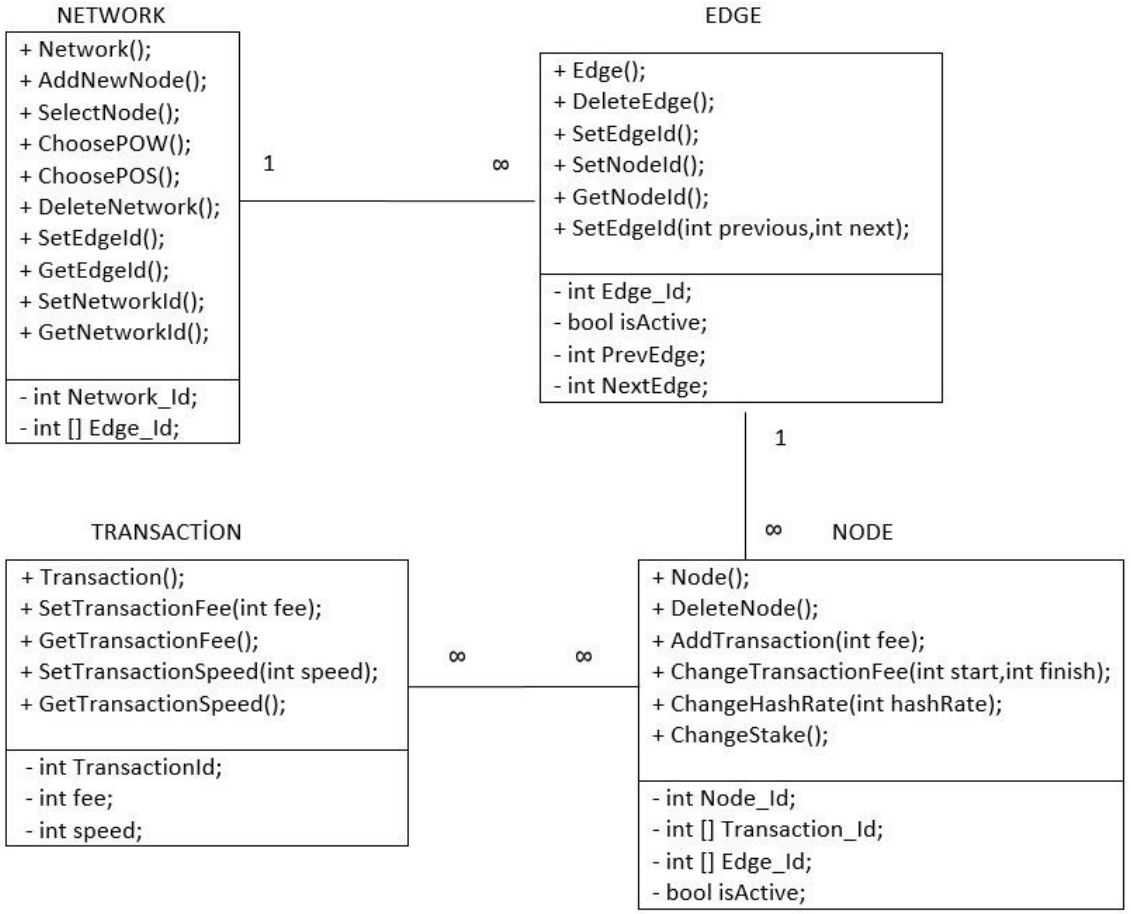
4.2.1 Simulation Design Approach

For developing the project, we have planned to use Scrum which is an agile software development methodology. The Scrum method offers us a simple but flexible management phase, rather than specifying the steps that need to be followed in detail in the project when developing a project.[6]Particularly, it is possible to change this process while splinters are moving. Scrum is also divided into sprints to complete the time required for the main work to be done.There are tasks for team members in the split.At the end of each splint, the necessary tests are carried out. This allows us to reduce the errors that may occur during the development of the software.For these reasons we decided to develop our project with Scrum which is an agile software development methodology.. We have created a Scrum Board to complete the

tasks defined in the project.So that we have made the distribution of tasks and the need to complete the time we have divided the splints.After each period is completed, necessary tests are performed. Considering all these steps, Scrum was chosen as the most suitable methodology for the project.

4.2.1.1 Class Diagram

This class diagram shows the functions required for the blockchain consensus simulation.



4.3 Architecture Design of Simulation

4.3.1 Network Menu

Summary: This system is used by user. The user can create random network , select pow or pos algorithm, add a new node, select node and delete network.

Actor: User

Precondition: User must run the program.

Basic Sequence:

1.The user can create a random network. To do this, it has to select one of the POW or POS algorithms.

2. The user can add node or edge to create a network.

3. The user can choose to make changes to the node.

4. The user has to choose which of the POW or POS algorithms to use on the network.

5. The user can delete the entire network.

Exception: None.

Post Conditions: None

Priority: High

4.3.2 Node Menu

Summary: This system is used by user. The user can delete node, add transaction, change transaction fee, set transaction speed, change hash rate and change stake.

Actor: User

Precondition: User must create edge successfully.

Basic Sequence:

1. The user can delete the node.

2. The user can change the node's hashrate.

3. The user can add transaction. To do this, you must enter transaction fee.

4. The user can delete the edge to which the node is attached.

5. The user must enter hashrate for the POW algorithm or stake for the POS algorithm.

6. The user must enter the fee range of the transactions.

7. The user can enter or change the production speed of transactions.

Exception: None

Post Conditions: None

Priority: Medium

4.3.3 Simulation Menu

Summary: This system is used by user. The user can see next step, previous step, play all and stop simulation.

Actor: User

Precondition: User must create system successfully.

Basic Sequence:

1. The user can forward simulation to 1 ms.

2. The user simulation can be reduced to 1 ms.

3. The user can play the simulation.

4. The user can stop the simulation.

Exception: None

Post Conditions: None

Priority: Medium

4.4 Activity Diagram

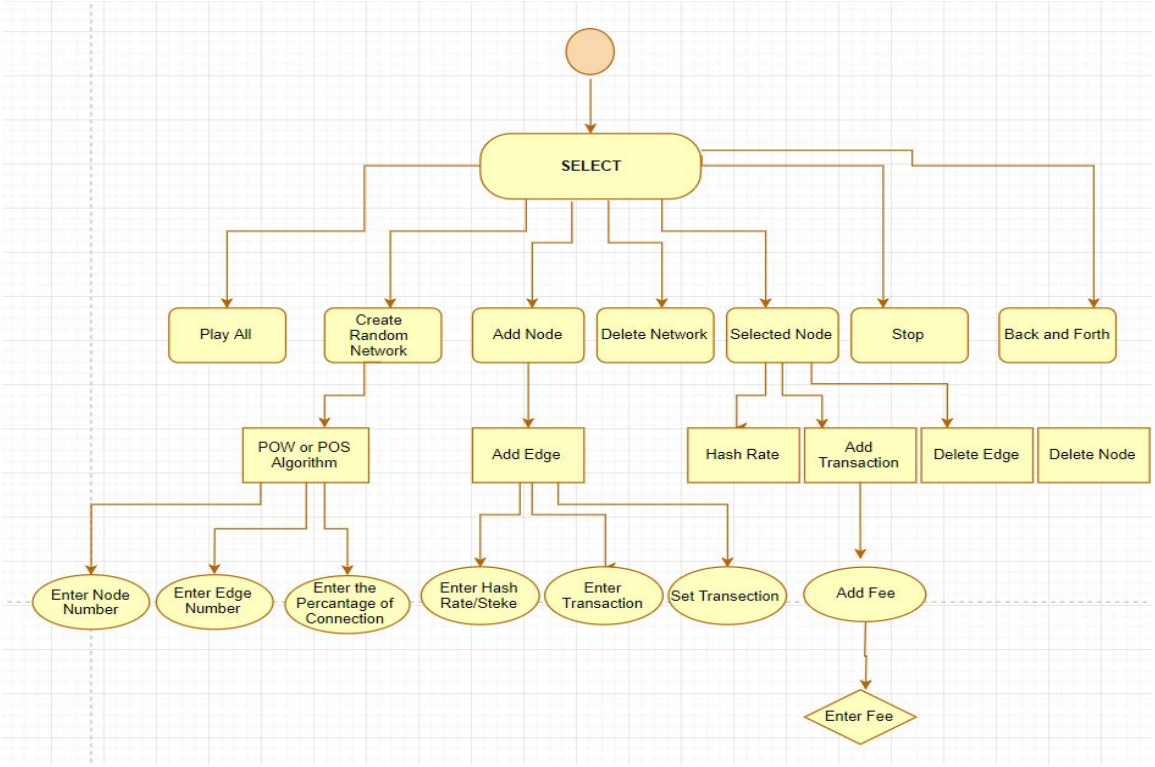
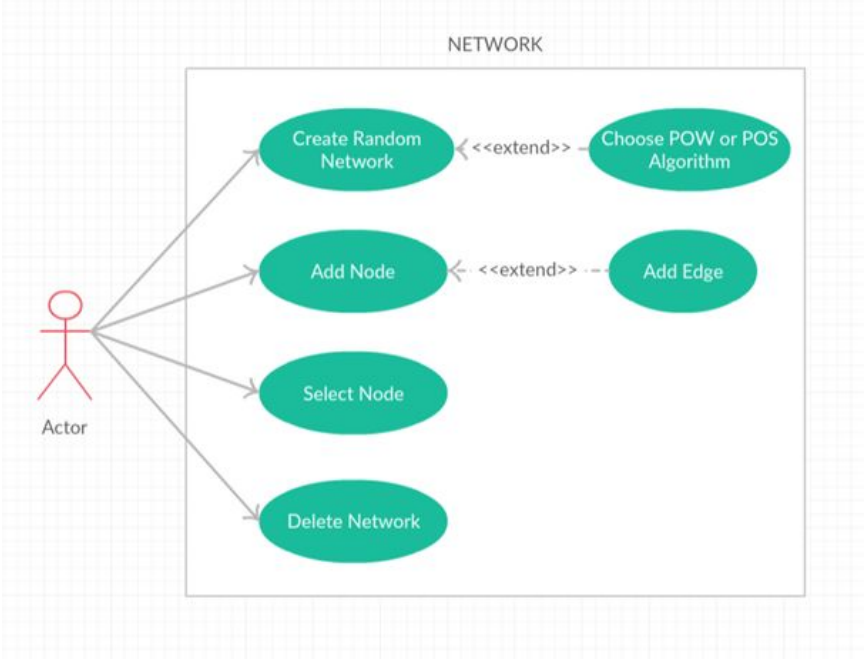


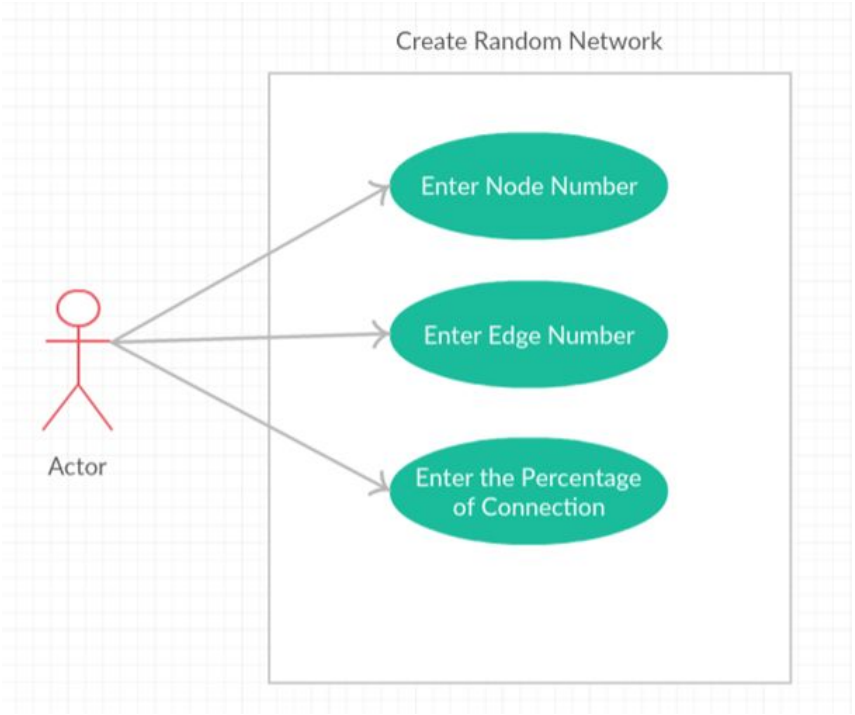
Figure F

The Figure F, shows that how the scenario generation works as an activity diagram.When the user open to the simulation, she/he sees that the main page of the simulation.

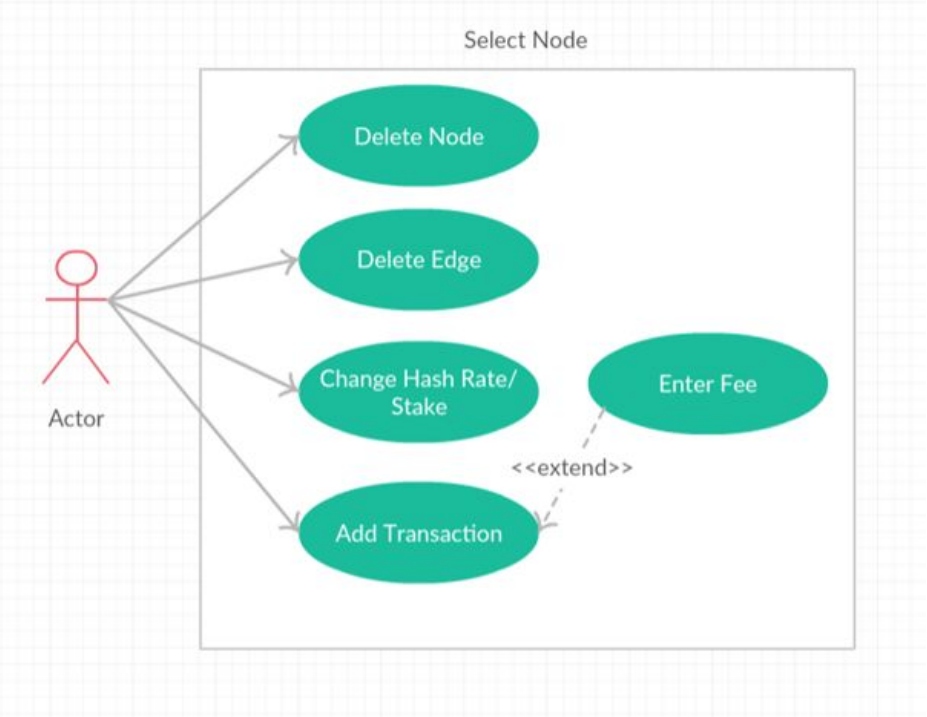
4.5 Use Case Realization



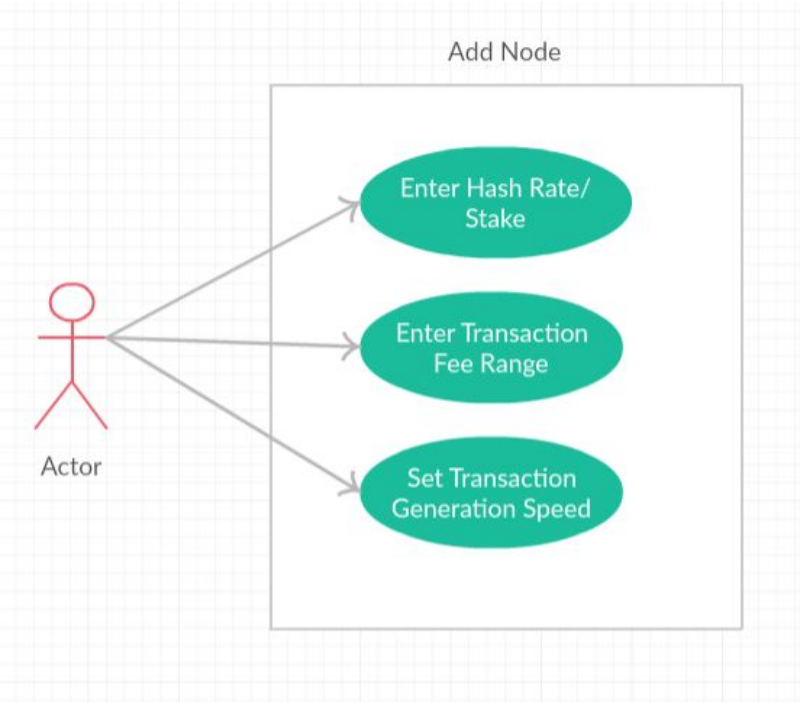
1. The user can create a random network.
2. The user can add node or edge to create a network.
3. The user can choose to make changes to the node.
4. The user has to choose which of the POW or POS algorithms to use on the network.
5. The user can delete the entire network.



1. The user must enter the number of nodes on the network.
2. The user must enter the number of edge on the network.
3. The user must enter the connection percentage. The system communicates between the edge and nodes according to the percentage entered.



1. The user can delete the node.
2. The user can change the node's hashrate.
3. The user can add transaction. To do this, you must enter transaction fee.
4. The user can delete the edge to which the node is attached.



1. The user must enter hashrate for the POW algorithm or stake for the POS algorithm.
2. The user must enter the fee range of the transactions.
3. The user can enter or change the production speed of transactions.

5. Conclusions

In this CENG 407 project, we talk about the blockchain consensus simulator. Based on the preliminary findings within this Literature review , our aim is to model and simulate Blockchain to work within a certain time period of a real process or system. Blockchain is a shared, trusted, public ledger of transactions, that everyone can inspect but which no single user controls.Blockchain, also known as the distributed book, is used in many different fields such as banking, real estate and education. A blockchain consensus mechanism is a fault-tolerant mechanism that is used in computer and blockchain systems to achieve the necessary agreement on a single data value or a single state of the network among distributed processes or multi-agent systems. We have examined the most popular consensus mechanisms POW and POS algorithms and we find out that none of them is absolutely perfect but they each have their strengths.That's why algorithms are being continuously updated and complemented. Sometimes the approaches from even different consensuses mix together forming hybrids.

Acknowledgement

We would like to thank Dr. Faris Serdar TAŞEL for all his feedbacks and efforts which are beneficial to improve our project.

References

[1] M. S. Paul, "Hyperledger - Chapter 1 | Blockchain Foundation – The Startup – Medium," Medium, 23-Apr-2018. [Online]. Available: https://medium.com/swlh/hyperledger-chapter-1-foundation-7ad5bd94d452. [Accessed: 08-Nov-2018].

[2] Ethos, "What is Ethereum ETH? What is the Ethereum Blockchain?," Ethos, 24-Oct-2018. [Online]. Available: https://www.ethos.io/what-is-ethereum/. [Accessed: 30-Oct-2018].

[3] N. Acheson, "What is bitcoin?," CoinDesk, 29-Jan-2018. [Online]. Available: https://www.coindesk.com/information/what-is-bitcoin/. [Accessed: 30-Oct-2018].

[4] Introduction. [Online]. Available: http://web.cs.mun.ca/~donald/msc/node4.html. [Accessed: 07-Nov-2018].

[5] GCSE Bitesize: Advantages and disadvantages of simulation," BBC. [Online]. Available: http://www.bbc.co.uk/schools/gcsebitesize/ict/modelling/1computersimulationrev3.shtml. [Accessed: 07-Nov-2018].

[6]ACMSoftware.(2018).ScrumNedir?.[online]Availableat: http://www.acm-software.com/scrum/[Accessed 23 Nov. 2018].