T.C.
MARMARA UNIVERSITY
FACULTY OF ENGINEERING
COMPUTER ENGINEERING DEPARTMENT

CSE497 – Analysis and Design Document

CERTIFICATE VERIFICATION USING BLOCKCHAIN

Group Members

150114822 – Eren Ulaş
150114823 – Berk Karabacak

Supervised by

Assist. Prof. Ali Haydar Özer

1. Introduction

1.1. Problem Description and Motivation

According to a study made on 5,000 CVs by The Risk Advisory Group, 80% of the 5,000 screening cases sampled contained one or more CV discrepancies, and 38% of the cases analyzed related to inaccurate or falsified CVs of 25-32 years olds, and 57% of CV discrepancies relate to candidates' academic background [1].

Some people tend to make inaccurate statements on their resumes to get a job that asks for the requirements they may not have. They might claim holding a degree they don't have, or they might add some certificates to their resumes even though they don't have those certificates. It would be a long and a very inefficient process for human resources departments to verify the credentials of each applicant if some tools to reduce this overhead are not used. The system we will create can make it easier for human resources departments to verify the certificates that the applicant claims to hold.

On another perspective, our system can help refugees, too. According to UNHCR, there are 22.5 million refugees around the world [2]. Refugees who don't take their degrees with them cannot prove their expertise, and they might not get the job which they are capable enough to do. Our system will be available unless all the nodes are destroyed in its distributed network. It will be accessible all around the world and documents uploaded will be tamper-proof. Because of these features, refugees whose certificates exist in the system can prove their expertise, and employers can use our system to verify their certificates. As a result, it might get easier for refugees to have the job they deserve.

To overcome the issues mentioned above, our goal is to create a system that will make it easier to verify certificates. It will also provide a more convenient way to access, and share certificates while preserving their authenticity. To achieve our goal, we will implement a website which will allow the issuing institutions to issue certificates and it will also let employers and any other institutions to verify candidates' certificates. An Android application will be created which will allow certificate holders to access and share the certificates that are assigned to them.

1.2. Scope of the Project

1.2.1. Outcomes

1.2.1.1. Website

Each issuer will have a public private key pair which represents its identity. In order to issue a certificate into blockchain, issuer needs to

login using the website. Issuers need to upload a certificate in '.pdf' file type and they need to enter the public key of the certificate holder, too. Issuers will not be able to see the records of previous transactions. Log out functionality is also in the scope of this project.

Besides issuing certificates; companies, individuals, or institutions are able to verify certificates using website. Verification can be done in two ways, which are

- Entering hash string of a certificate
- Uploading a certificate file

After verification process is started, its result will be shown. If the certificate that is wanted to be verified is not in blockchain, then a simple warning box will be shown to user. If it exists in blockchain, then a new page consists of the pdf of certificate, its date of submission, and its authenticity status will be shown to user.

1.2.1.2. Android Application

Main purpose of our Android application is to let certificate holders access their certificates and share these certificates. Each certificate holder who wants access their certificates needs to login. In order to login to their accounts each user needs to enter its private key. After this step, all the certificates that are assigned to the user will be presented. Users can view or share their own certificates.

1.2.1.3. Blockchain

Blockchain part consists of the distributed decentralized database that we will create. Only the permitted issuers will be able to add new certificates to these database. Blockchain will be distributed among those permitted nodes and each of these nodes will have a local copy of the blockchain, and these copies will be in sync. All of them will have the same data. Viewing and verification rights will be public. When a new block containing a certificate is added to blockchain, it will be propagated to all nodes in order to achieve synchronization. Proof of work algorithm, and longest chain wins rules will be used to achieve consensus.

1.2.1.4. Server Applications

We will also create a software for the index servers. These index servers will maintain the nodes online status, and ip addresses. Each newly joined issuer will connect these index servers to retrieve the addresses of

other issuers' nodes, and it will form connections with them in order to create a distributed peer to peer network.

Another thing we're going to implement is the server application for issuer servers. This software will allow issuers to connect each other in order to form a distributed peer to peer network. It will also let issuer servers to synchronize their copy of blockchain with each other, propagate new blocks, verify a certificate, create new blocks, and add new blocks to blockchain.

1.2.2. Assumptions

- Certificate holders are assumed to have an Android device with a version 5.0 or higher.
- Issuers are assumed to use one of the browsers listed below:
  - Safari
  - Chrome
  - Opera
  - Edge
- Each certificate holder and issuer are assumed to have only one public-private key pair as their identification.
- When making verifications or accessing the certificates that are assigned using Android application, a random online node in the distributed network will be selected to achieve these operations on the blockchain.

1.2.3. Constraints

- Only the permitted issuers will be able to issue certificates.
- Right to verify a certificate will be public.
- Only pdf files are supported.

1.3. Definitions, acronyms, and abbreviations

- UNHCR: The UN Refugee Agency
- Hash Function: Function that takes an input and produces a unique value of fixed size.
- MB : MegaByte. A unit of information equal to one million or, strictly, 1,048,576 bytes.
- ECDSA: Elliptic Curve Digital Signature Algorithm is a variant of the widely used Digital Signature Algorithm which will be used to ensure that each certificate can only be issued by a permitted issuer.
- Blockchain: A blockchain is a decentralized and distributed digital ledger that is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the collusion of the network.

- Bitcoin : A type of digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank. It is the first cryptocurrency.
- Public Key : Cryptographic key that can be obtained and used by anyone to encrypt messages intended for a particular recipient, such that the encrypted messages can be deciphered only by using a second key that is known only to the recipient (the private key)
- Private Key : A private key is a bit of code that is paired with a public key to set off algorithms for text encryption and decryption.
- Cryptography : Method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.
- Android os : Linux-based platform for mobile phones.It is developed by Google and the Open Handset Alliance (OHA), a coalition of hardware, software and telecommunications companies.
- Transaction fee : Cost to complete a blockchain transaction.

2. Literature Survey

There are some similar projects done in this field.

Digital Certificates Project: "An incubation project by the Media Lab Learning Initiative and Learning Machine that builds an ecosystem for creating, sharing, and verifying blockchain-based educational certificates. Digital certificates are registered on the Bitcoin blockchain, cryptographically signed, and tamper proof." [3] Its development continues under Blockcerts initiative [4].

OriginStamp: "OriginStamp is a non-commercial trusted timestamping service that can be used free of charge and anonymously." [5] It allows us to anonymously timestamp information in a decentralized and tamper proof way using Bitcoin Blockchain. Once the user submits a file, its hash is created. Then, OriginStamp aggregates the created hashes and submits to the Bitcoin Blockchain and hashes stay there forever.

Stampd: "Stampd is a web application for the time stamping of documents on the decentralized public ledger of digital cryptocurrencies. Stampd's digital stamping on the blockchain proves that the document existed at that particular point of time. The user will be able to prove the document stamping by referring to the pertinent posting of the document's imprint (hash) on the publicly available bitcoin ledger (blockchain)." [6]

"University of Nicosia issues academic certificates whose authenticity can be verified through the Bitcoin blockchain. These certificates are being issued to students who successfully completed or participated in DFIN-511 Introduction to Digital Currency, which is the first university course offered on the topic of cryptocurrency." [7] Hashes of

the certificates are produced, and then they are put into Bitcoin blockchain. Verification can be done by searching the hash of a certificate on the authenticated index document provided by the university.

Besides the projects above, there are some widely used verification systems that are based on centralized networks. These document verification services use barcodes or QR codes to verify the authenticity of documents.

Some of the systems listed above are based on Bitcoin blockchain. They use Bitcoin blockchain to store the hashes of documents in a decentralized manner, and timestamp them. Because of the transaction fees, for the hashes put in the Bitcoin blockchain some amount of Bitcoin is needed to be paid. Our system will be based on a private blockchain so only the authorized issuers will be able to put their records on the blockchain and blockchain will be distributed only to those authenticated issuers. Since we are building our own private blockchain instead of using a cryptocurrency blockchain, there will be no need to pay some amount of money to put the records.

Since our system is not a centralized one, it will be available unless all the nodes are destroyed. Only the permitted issuers can edit or add certificates into blockchain, and each certificate that is added will be tamper-proof due to the nature of blockchain.

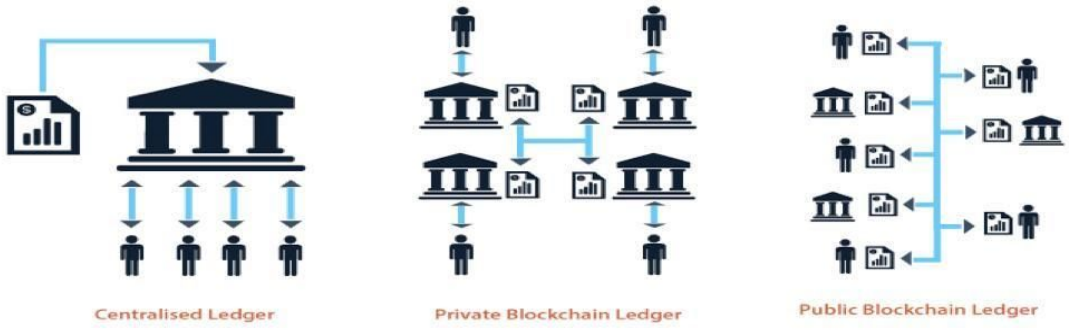

Figure 1: Comparison of centralized, private blockchain, and public blockchain ledgers [8]

Differences between centralized, private blockchain, and public blockchain ledger systems can be seen from the figure above. In a centralized system, control of the ledger belongs to only one institution and anyone who wants to interact with the ledger have to use the institution as an intermediary. In public blockchain ledger which has the same working principle as Bitcoin blockchain, the ledger is public which means that anyone can see the content of the ledger and interact with it. However, in private ledger systems which we are going to implement, ledger is controlled by a group of

permissioned intermediaries, and a person can interact with it using one of the intermediaries.

3. Project Requirements

3.1. Functional Requirements

3.1.1. Login System

3.1.1.1. Description

Website provides a login system for issuers and Android application provides a login system for certificate holders.

3.1.1.2. Inputs

Issuers or certificate holders can login by entering their private keys.

3.1.1.3. Processing

Public key that belongs to this private key is created, and searched in the table in index servers.

3.1.1.4. Outputs

If issuer exists, then a page for issuing certificates will be shown. Otherwise, a pop-up message that indicates the non existence of issuer will be shown.

If the certificate holder exists, then all of its certificates will be shown on Android application. Otherwise, an alert dialog will be shown.

3.1.1.5. Error/Data Handling

The length of private keys will be checked.

3.1.2. System for Issuing Certificates

3.1.2.1. Description

Website will provide a system for issuing certificates.

3.1.2.2. Inputs

Issuer will upload a certificate, and enter the public key of the recipient.

3.1.2.3. Processing

A request to issue the uploaded certificate will be redirected to issuer's server, and it will be encrypted using issuer's private key. After that, a block will be created using proof of work algorithm, and it will be added to blockchain. Finally, this block will be propagated to all nodes.

3.1.2.4. Outputs

A pop-up message that indicates the status of transaction will be shown.

3.1.2.5. Error/Data Handling

Format of uploaded file and recipient's public key will be checked. When a propagated block is received by other nodes, each node will check the validity of it.

3.1.3. Verification System

3.1.3.1. Description

Website will provide a verification system.

3.1.3.2. Inputs

User needs to upload the certificate to verify or enter the hash string of a certificate.

3.1.3.3. Processing

If user chooses to verify a certificate by uploading it, then its hash will be generated and then this hash will be searched in blockchain.

If user chooses to verify by entering the hash string of a certificate, then this hash string will be searched in blockchain.

3.1.3.4. Outputs

If document is found, then a page that consists of the certificate, its date of submission and authenticity status will be shown. Otherwise, a pop-up message which indicates the non existence of the certificate will be shown to user.

3.1.3.5. Error/Data Handling

Format of the uploaded file and length of the hash string will be checked.

3.1.4. Certificate Viewing and Sharing System

3.1.4.1. Description

Android application will provide a sharing and viewing system.

3.1.4.2. Processing

When a certificate is selected on application, it will be shown to certificate holder along with its date of submission, and sender. If certificate holder chooses to share it, options to share it via social media or email will be shown to user.

3.2. Nonfunctional Requirements

- System should be able scale up to 100 institutions and each of them can issue 10.000 certificates per year.
- Maximum size for certificate data should not exceed 1 MB.
- Up to 100 users may access the certificate details at the same time.
- Blockchain will be available to users 99% of normal working hours.
- Timestamp of data must be recorded to the nearest second.
- Blockchain software can be licensed up to 30000 concurrent users.
- All comment fields will be spell checked.
- All certificates will be backed-up daily.

4. System Design

4.1. UML Use Case Diagram

Following diagram shows actions that can be done by each actor.

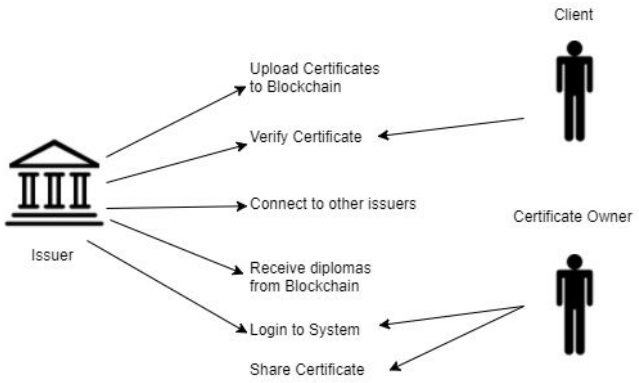

Figure 2: UML Use Case Diagram

4.2. UML Class Diagram

In this section, a class diagram which briefly shows the structure of our project is given.

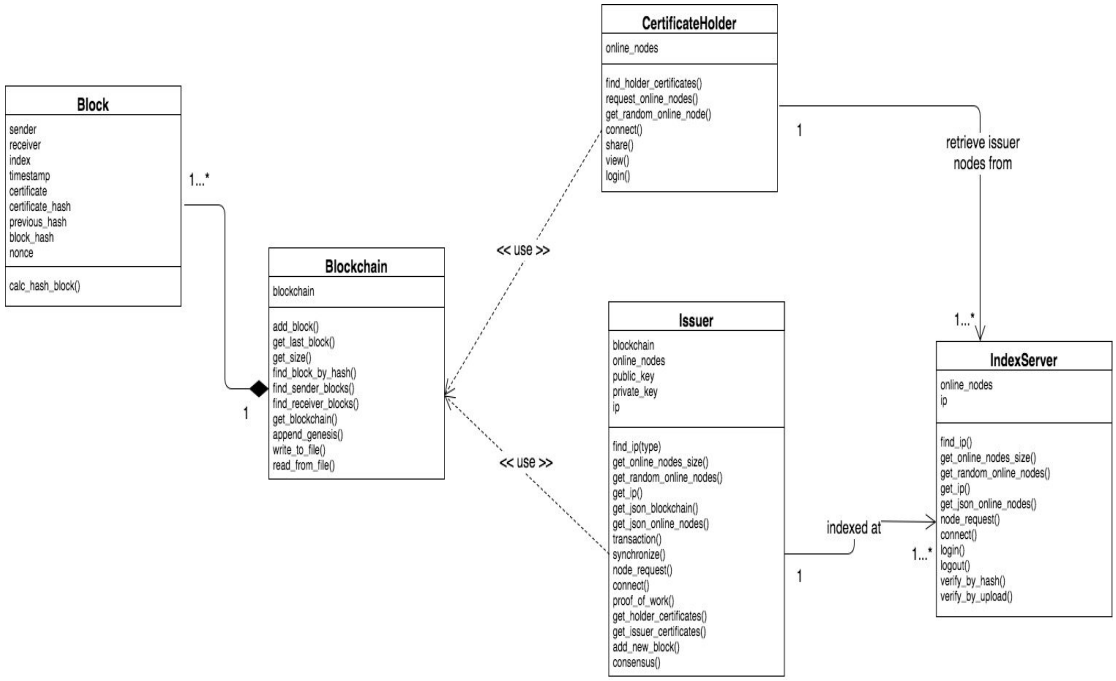

Figure 3: UML Class Diagram

- **Block:** Block class defines the block structure for our blockchain. It contains data that will be stored in each block and a method to calculate block's hash string using its own data will be implemented as well.
- **Blockchain:** This class mainly consists of the methods that will be used to achieve some operations on blockchain. Retrieving a block, adding a new block into blockchain, writing blockchain to a file and reading it are some of operations that can be done on blockchain.
- **Certificate Holder:** This represents the certificate holders. It will be implemented as a part of our Android application. Includes some methods which allow certificate holders to retrieve, share or view their certificates.
- **Issuer:** Issuer class represents the backend application that each issuer needs to use in order to issue certificates. It includes methods that allow it to retrieve certificates, adding new blocks, achieving consensus and synchronization.
- **IndexServer:** This is the representation of our index servers. It mainly consists of the methods that will allow them to keep track of the online nodes in network.

4.3. User Interface

4.3.1. Website

Screenshot below is a sample design we've created as our website's main page. In this page, an issuer can log in to issue certificates. Organizations or individuals can use this page to verify a certificate using its hash string or they can upload a document to check its authenticity.

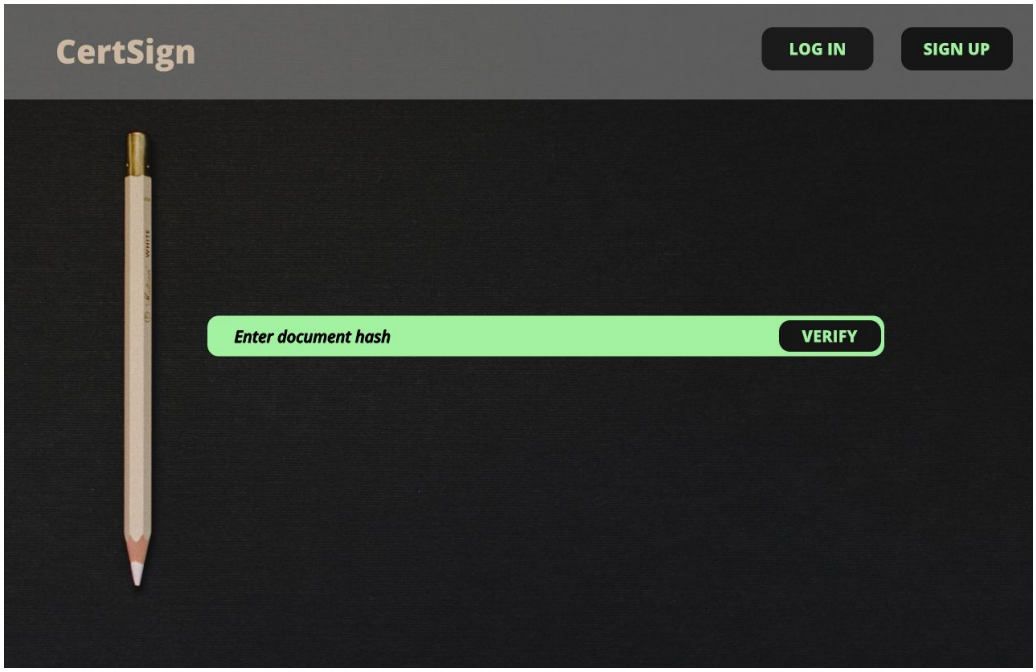

Figure 4: Sample Design for the Main Page of Website

Design below belongs to certificate issuing panel. Issuer can issue a certificate by giving certificate holder's public key and the certificate as input. Issuer can also log out in this panel.

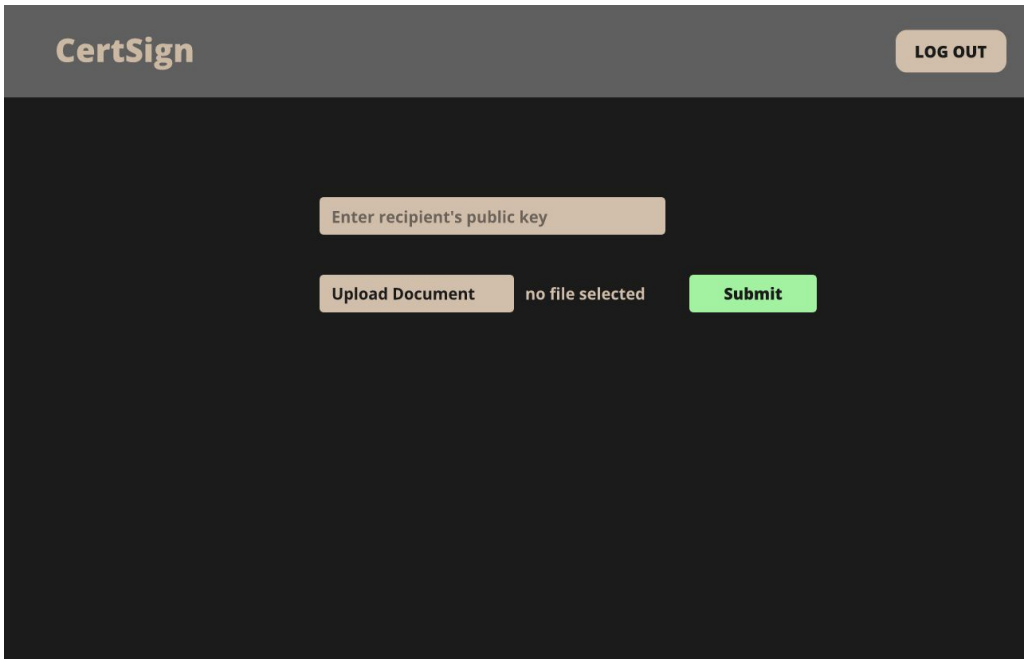

Figure 5: Sample Design for Certificate Issuing Page

Page design below shows the screen that will be shown to organizations and individuals, if the certificates they want to verify is verified successfully.

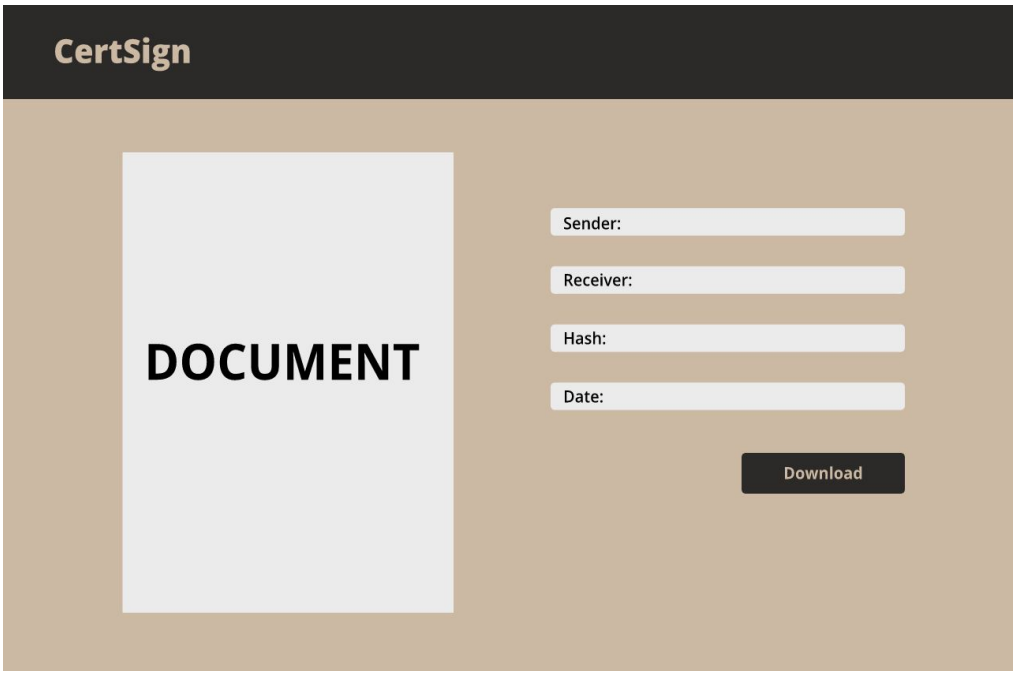

Figure 6: Sample Design for the Certificate Detail Page of Website

4.3.2. Android Application

Android application design samples are shown below. Sample on the left will be login screen of our application, and screen on the right will be shown to user after he/she logs in. In this screen, certificate holders are able to see all the certificates that are assigned to them, and they can view these documents and share them.

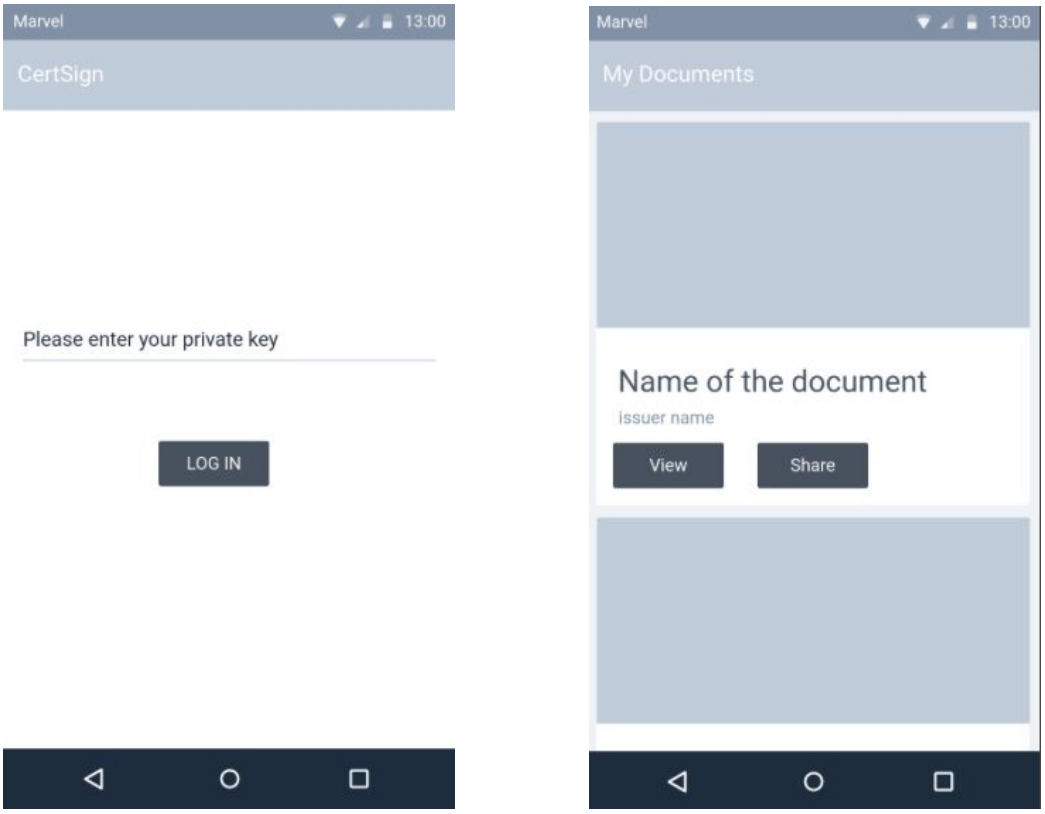

Figure 7: Sample Designs for Android Application's Login and Main Screens

4.4. Test Plan

These test cases describes the testing approach and overall framework that will drive the testing of the project. Plan below will address multiple risk cases.

Risk	Uploading file greater than limit size
Probability	Medium
Impact	Low
Test	Upload file with excessive size and observe outputs
Time	January - 2018

Risk	Non-availability of nodes
Probability	High
Impact	Medium
Test	Make one of the nodes offline and observer result
Time	January - 2018

Risk	Not enough resources on server, too much request to servers
Probability	Medium
Impact	Medium
Test	Send frequent requests to one of the servers and observer how it handles traffic
Time	February - 2018

Risk	Data loss in one of the servers
Probability	Low
Impact	High
Test	Delete part of blockchain in one server
Time	February - 2018

Risk	Sign in with wrong credentials
Probability	High
Impact	Low
Test	Enter wrong credentials, and observe rejection status
Time	February - 2018

Risk	Install Android app to phones older than Android OS 4.0
Probability	Medium
Impact	Low
Test	Observer how mobile app runs on old phones
Time	March - 2018

5. Software Architecture

5.1. Data Flow

Diagram below shows the data flow of our system.

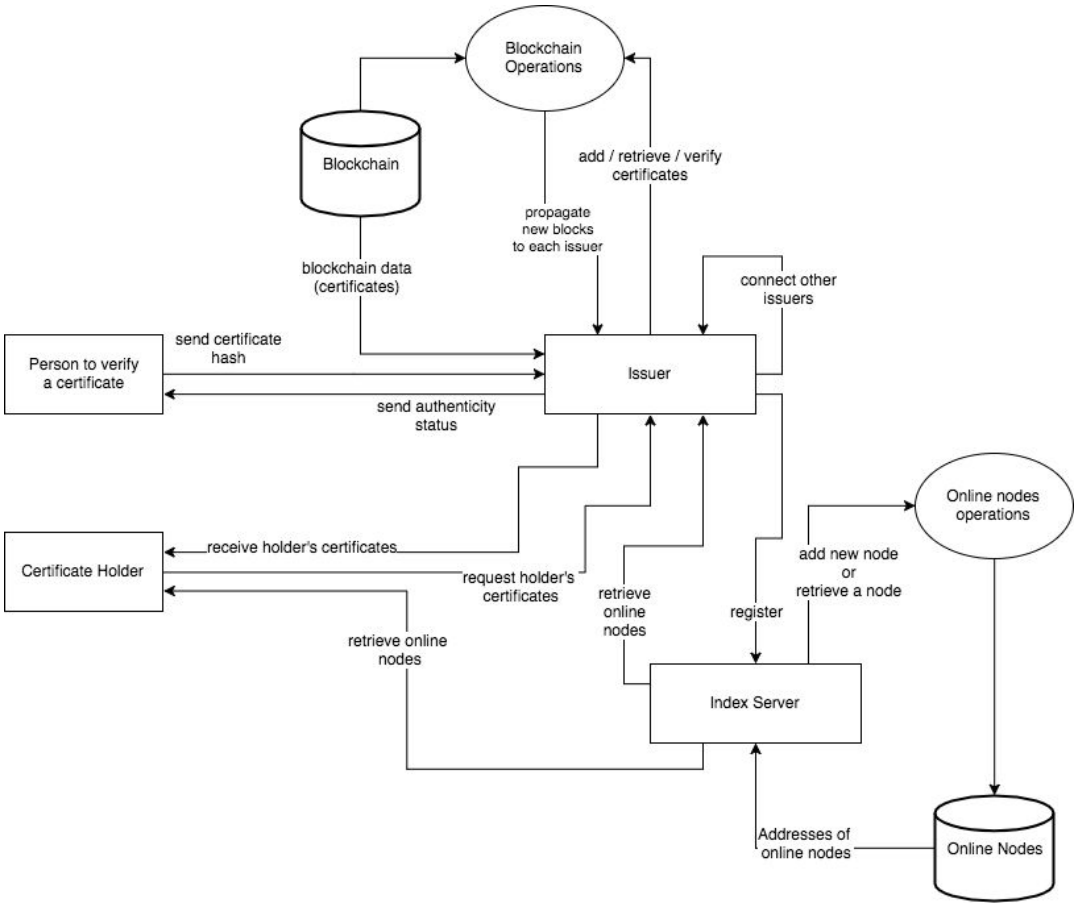

Figure 8: Data Flow Diagram

5.2. Control Flow

Diagram below shows the control flow for various parts of our system. Each one of these diagrams shows the actions done to accomplish a task.

5.2.1. Control Flow Diagram for a New Issuer Joining the Network

Diagram below shows the control flow that will be encountered when a new issuer joins the network.

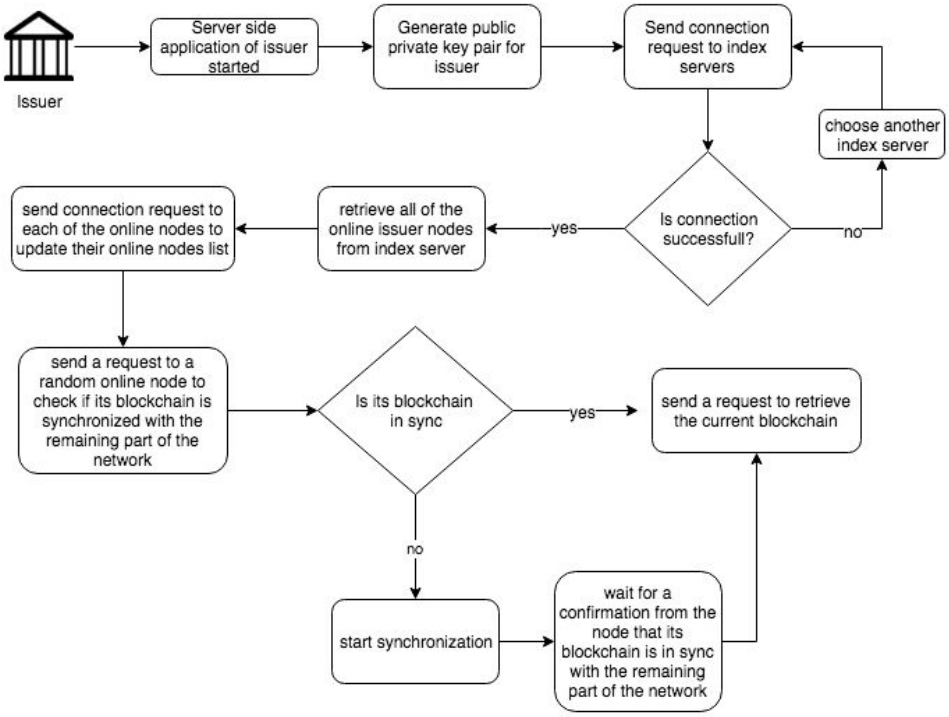

Figure 9: Control Flow Diagram for a New Issuer Joining the Network

5.2.2. Control Flow Diagram of Index Servers

Diagram below shows the control flow of index servers.

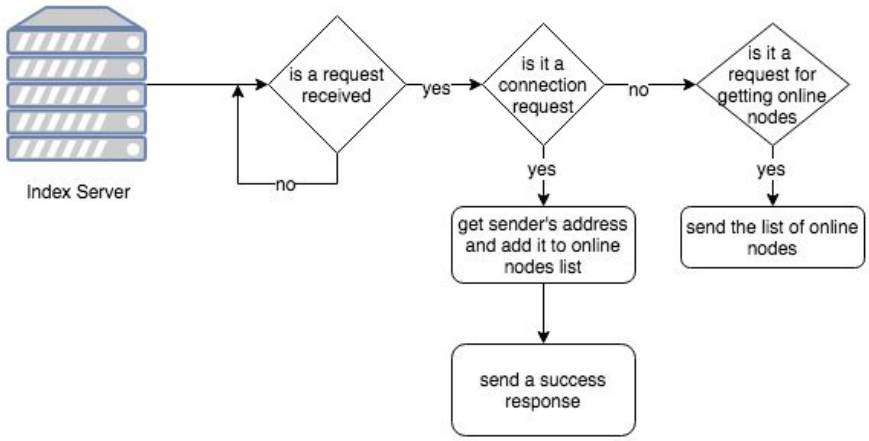

Figure 13: Control Flow Diagram of Index Servers

5.2.3. Control Flow Diagram of the Addition of a New Block Into Blockchain

Diagram below shows the control flow that will be encountered when a new block is added into blockchain as a result of issuing a certificate.

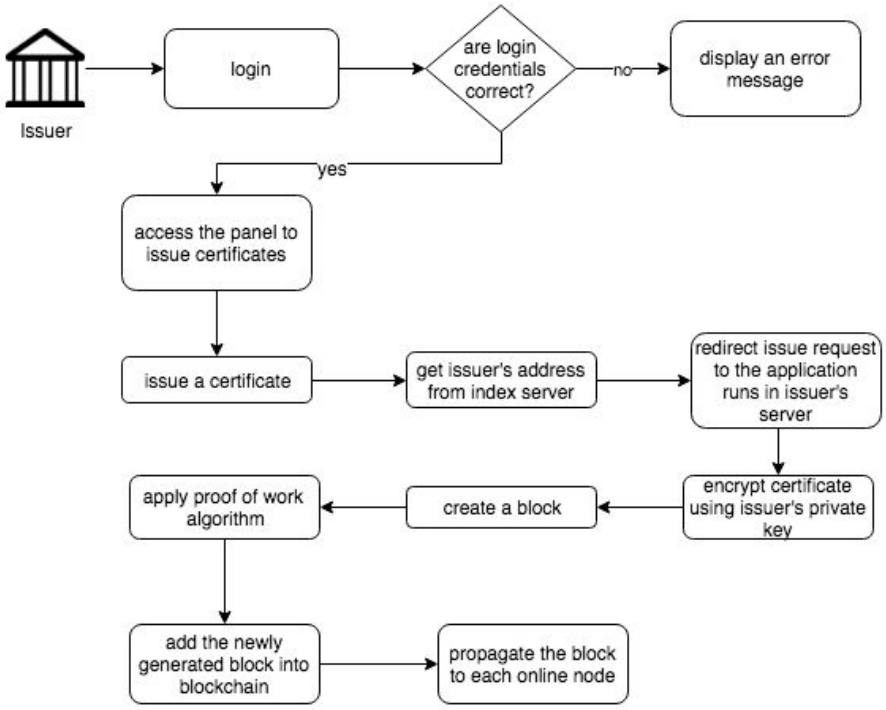

Figure 10: Control Flow Diagram of the Addition of a New Block

5.2.4. Control Flow Diagram of the Verification Process

Diagram below shows the control flow on a verification event.

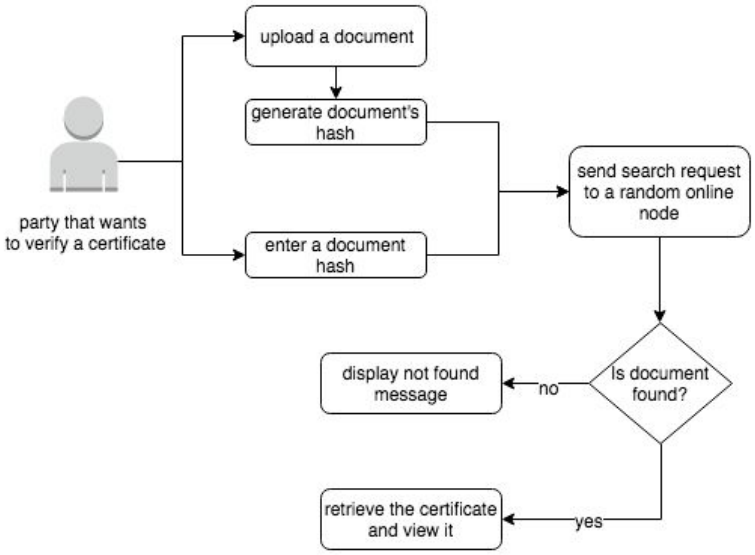

Figure 11: Control Flow Diagram of the Verification Process

5.2.5. Control Flow Diagram for a Certificate Holder Using Android Application

Diagram below shows the control flow of certificate holder's Android application usage.

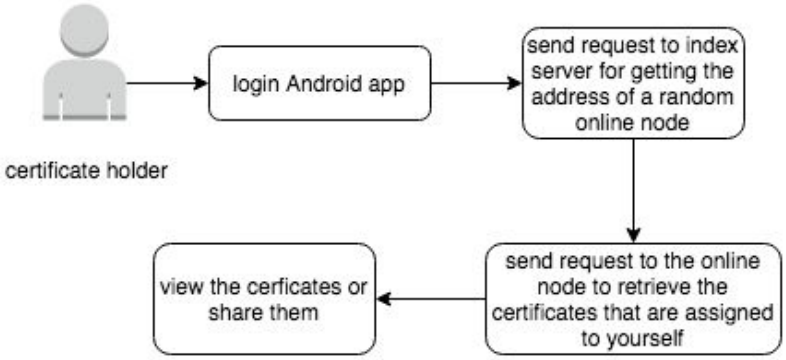

Figure 12: Control Flow Diagram for a Certificate Holder Using Android Application

5.2.6. Control Flow Diagram of Index Servers

Diagram below shows the control flow of index servers.

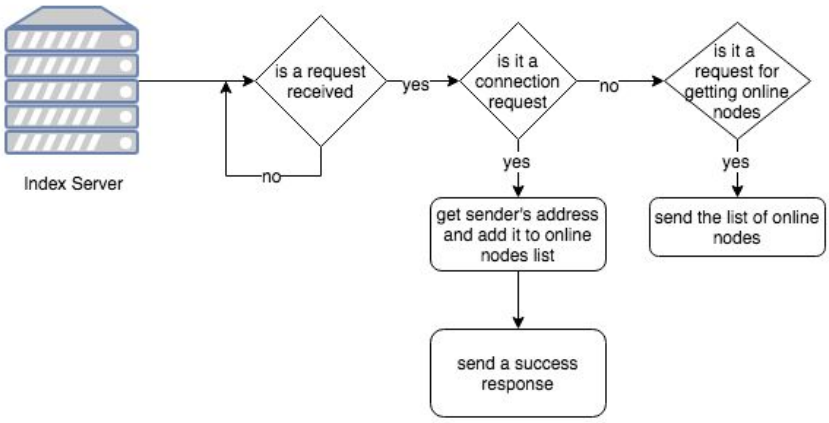

Figure 13: Control Flow Diagram of Index Servers

5.3. Modular Design

System consists of 3 parts and these are:

- **User Interface / Frontend:** This is the part that issuers interact in order to issue a certificate. Organizations or individuals who want to verify a certificate also uses this part.
- **Backend:** This the part that our index servers, issuer servers and api's lies. Index servers are used to keep track of the online issuer servers. Our system also contains an application for the issuer servers which will be used to create and interact with the distributed database(blockchain), and all of these parts are connected to each other with our API.

- **Mobile Application:** This part contains a mobile application that the certificate holders will use to access their certificates. It interacts with issuer and index servers via our API.

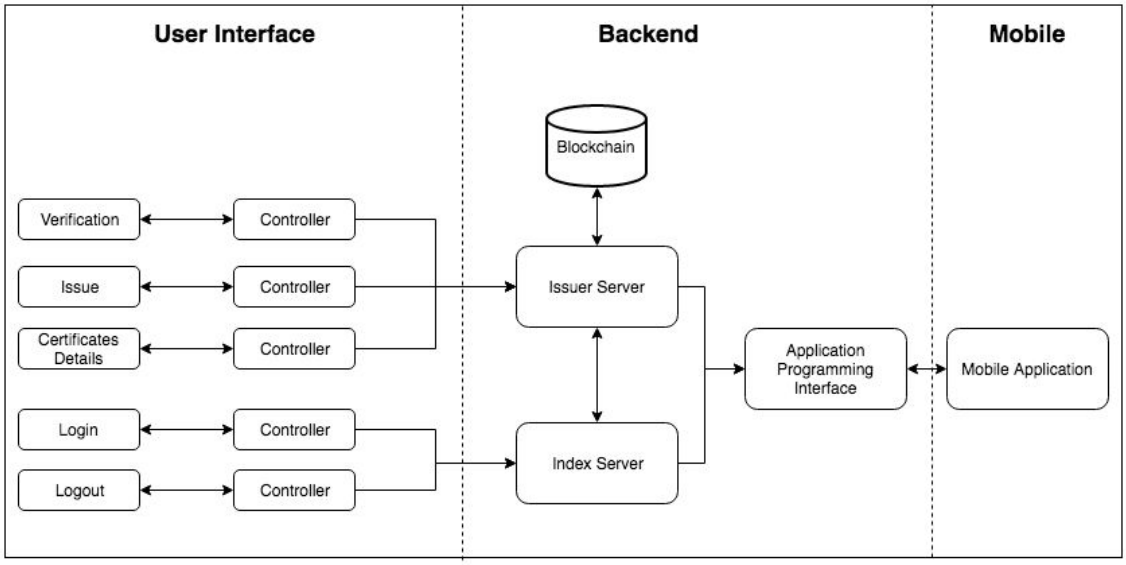

Figure 14: Modular Design

6. Tasks Accomplished

6.1. Current State of the Project

Tasks below are accomplished during this semester:

- We've finished our research and developed a high level structure of our system.
- We've examined some tools that can help us in case of a failure.
- A basic blockchain is implemented. Certificates can be added to and retrieved from blockchain. Verification of the certificates can be done, as well. However, all these operations are done on a central server.
- A simple web interface that will allow to add certificates into blockchain is developed.

6.2. Task Log

- **First Month**

  We planned how should we approach to solve the problem.We decided to use blockchain as a solution. We made plans to use GitHub during our project development. Also had meetings with our advisor Assist. Prof. Ali Haydar Ozer, he suggested some improvements on our project.

- **Second Month**

  We examined similar projects on topic and discussed what our difference will be. Also we made some plans on how to implement this project with institutions such as universities. We contacted with several universities and discussed their feedbacks.

- **Third Month - Building Basic Blockchain**

  This month we have examined how blockchain works and looked at sample blockchain codes. We have decided programming languages and frameworks for the project. After finishing basic coding for the blockchain we started making simple tests.

- **Fourth Month**

  This month we made some tests on blockchain and compared its performance to standard SQL databases. At the meetings with our advisor we have received positive feedbacks. Also we made plans for risk analysis in case we fail at some part of our project we decided to use existing blockchain frameworks.

6.3. Task Plan with Milestones

	January	February	March	April	May
Task 1					
Task 2					
Task 3					
Task 4					
Task 5					

- **Task 1:** In our current blockchain implementation, all the additions of new data and verifications are done on a central server. During this task, our aim is to convert it into a decentralized and a distributed network.
- **Task 2:** Web interface will be made more user friendly, and some other functionalities such as verification of a document, and login of an issuer will be added.
- **Task 3:** Android application will be implemented during this period.
- **Task 4:** Final and complete version of our project will be tested with multiple issuers and certificate owners.
- **Task 5:** Project thesis and presentation will be prepared during this period.

7. References

[1] – The Risk Advisory Group, CV Lies 2017 on July 24, 2017 [Online] Available: https://www.riskadvisory.com/news/cv-lies-on-the-increase.php (Date of Access: 17 October 2017)

[2] – The UN Refugee Agency, Figures at a Glance [Online] Available: http://www.unhcr.org/figures-at-a-glance.html (Date of Access: 17 October 2017)

[3] – Digital Certificates Project [Online] Available: http://certificates.media.mit.edu (Date of Access: 07 October 2017)

[4] – Blockcerts [Online] Available: https://www.blockcerts.org/ (Date of Access: 07 October 2017)

[5] – OriginStamp [Online] Available: https://app.originstamp.org/about (Date of Access: 10 October 2017)

[6] – Stampd [Online] Available: https://stampd.io/about-document-blockchain-stamping/ (Date of Access: 17 October 2017)

[7] – University of Nicosia, Academic Certificates on the Blockchain (up to Mar 2017) [Online] Available: https://digitalcurrency.unic.ac.cy/free-introductory-mooc/self-verifiable-certificates-on-the-bitcoin-blockchain/academic-certificates-on-the-blockchain/ (Date of Access: 15 October 2017)

[8] – The Social Epistemology Review and Reply Collective [Online] Available: https://socialepistemologydotcom.files.wordpress.com/2017/05/sandstrom_blockchain_3.jpg (Date of Access: 17 October 2017)