

**COMSATS University Islamabad,**



**COMSATS Road, off GT Road, Sahiwal, Pakistan**

**SOFTWARE DESIGN**

**DESCRIPTION**

**(SDD DOCUMENT)**

**for**

**< BLOCKCHAIN-BASED E-VOTING SYSTEM >**

Version 1.0

***By***

**Sheharyar Jamil** **CIIT/FA-BCS-017/SWL**

**Shahzaib Naeem** **CIIT/FA-BCS-042/SWL**

**Zubair Amin** **CIIT/FA-BCS-051/SWL**

***Supervisor***

***Mr. Nasir Mehdi***

***Bachelor of Science in Computer Science (2018-2022)***

Table of Contents

[1. Introduction 8](#_Toc68962871)

[2. Scope 8](#_Toc68962872)

[3. Design methodology and software process model 8](#_Toc68962873)

[3.1 Incremental Model 8](#_Toc68962874)

[3.2 Agile Model 9](#_Toc68962875)

[4. System overview 9](#_Toc68962876)

[5. Architectural design 9](#_Toc68962877)

[5.1 Process flow/Representation 11](#_Toc68962878)

[6. Design models 13](#_Toc68962879)

[7. Data design 16](#_Toc68962880)

[8. Data dictionary 16](#_Toc68962881)

[9. Algorithm & Implementation 16](#_Toc68962882)

[10. Human interface design 17](#_Toc68962883)

[10.1 Screen images 18](#_Toc68962884)

[10.2 Screen objects and actions 21](#_Toc68962885)

11. References……………………………………………………………………………………………..16

# 

# Table of Figures:

[Figure 1: Architecture Design of DApp using Ethereum Blockchain. 8](#_Toc89377974)

[Figure 2: Architecture Design System 9](#_Toc89377975)

[Figure 3: Flow Chart 10](#_Toc89377976)

[Figure 4: Sequence Diagram 11](#_Toc89377977)

[Figure 5: Class Diagram 12](#_Toc89377978)

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Date** | **Reason for changes** | **Version** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Application Evaluation History

|  |  |
| --- | --- |
| **Comments (by committee)**  \*Include the ones given at scope time both in doc and presentation | **Action taken** |
|  |  |
|  |  |

**Supervised by**

**<Mr. Nasir Mehdi >**

Signature\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Co-Supervised by**

**<Mr. Amir Ali>**

Signature\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# 1. Introduction

Blockchain is a vast technology in today's era and the system developed on the blockchain technology has a great impact to change the world industries working way. One efficient example is cryptocurrency in the form of Bitcoin BTC that takes over paper currency and now it is safe to use. Blockchain collects information together in blocks and each block has different transactions. To utilize the blockchain to develop a system for the electronic voting system that provides the facilities decentralized, secure, transparent, not changeable data and traceability. That is to empower and stable the Voting system. In an electronic voting system, a voter can cast the vote, that works on the blockchain (Ethereum) and smart contracts using Dapp. The presiding officer is the person who has access to the system to manage the record, view casting, verify the voting, and initiate the transfer and document validation and authenticity. It will reduce the time cost, payment cost, provide transparency, and keep the records secure. Once the voting is done all the data record in the blockchain and the hash is generated automatically, and it cannot change that is best for security purposes.

# 2. Scope

E-voting has a proper system in all developed countries and taking it to an advanced level that is secure and immutable. The Blockchain-based e-voting system provides the best solution for the current system problem. In the Future this system provides the traceability feature that checks the previous and current voter because of the blockchain. Every block connects with the previous block. It will resolve the conflicts and provide security that is not hackable, and minimize the scope of vote disputes, records are transparent that checked by the public and private keys. Records data in digital ledger for transactions or contracts. The use of blockchain technology serves as the basis for a more reliable, cheaper, and more efficient.

# 3. Design methodology and software process model

## **3.1 Incremental Model**

The waterfall model has many drawbacks in the development of any product, to overcome these drawbacks incremental model is used in the development phase of our project. In this model, the product is developed in increments and module-wise one after one, each module contains more functionalities than before. These smaller pieces are then built and delivered to the client in increments. Quick response from clients. Each module is smaller than compared to the whole module. This model is used in our project.

## **3.2 Agile Model**

When clients do not want changes in their product then the Agile model is useful. This method assists teams in responding to the unpredictability of constructing software. It uses incremental, iterative work sequences that are commonly known as sprints. The ability to create and respond to change to succeed in an uncertain and turbulent environment.

# 4. System overview

The system will save the time of the user and improve efficiency. All actions are performed step by step to use this system that provides consistency in the system. Users know in which state working on when the state change it notifies the user. The system is easy to use for users.

The performance of the system is very good. It performs all the tasks very correctly and provides all the results quickly and accurately. When the contract between the member and the government RPC is on a peer-to-peer network that needs processing power to run the contract. The system provides a good response time to the user.

The Dapp should run on every machine, Windows, Mac OS, Linux, Mobile phone. and can be supported by any type and version of browsers installed in your operating system and the browser must have Meta Mask extension added. Dapp also works on Android OS and IOS must have a browser with a Meta Mask extension. The operating system minimum has 4 GB RAM and needs good processing power to run the Dapp for better results.

# 5. Architectural design

The structure of the system explains its core components, their relationships, and how they deal with each other. Blockchain Software architecture and design include several factors such as business logic, Ethereum Blockchain, Dapp, and the design of the system. In Architecture, nonfunctional decisions are cast and separated by the functional requirements. In Design, functional requirements are accomplished. The government module is very important. It is a major module in this module government have all rights to manage the votes and their results. Anyone can visit the main page related to the system and can get information and knowledge about our system that how to use the system and how anyone can get their self-registered. A combination of the modules makes up the system. We can use flowcharts to represent and illustrate the architecture.

Diagram

Description automatically generated­­­­

Figure 1: Architecture Design of Dapp using Ethereum Blockchain.

The **server** stores data that cannot be stored in the blockchain and performs business computations. A picture containing diagram

Description automatically generated

Figure 2: Architecture Design System

## **5.1 Process flow/Representation**

## 

**Flow Chart**

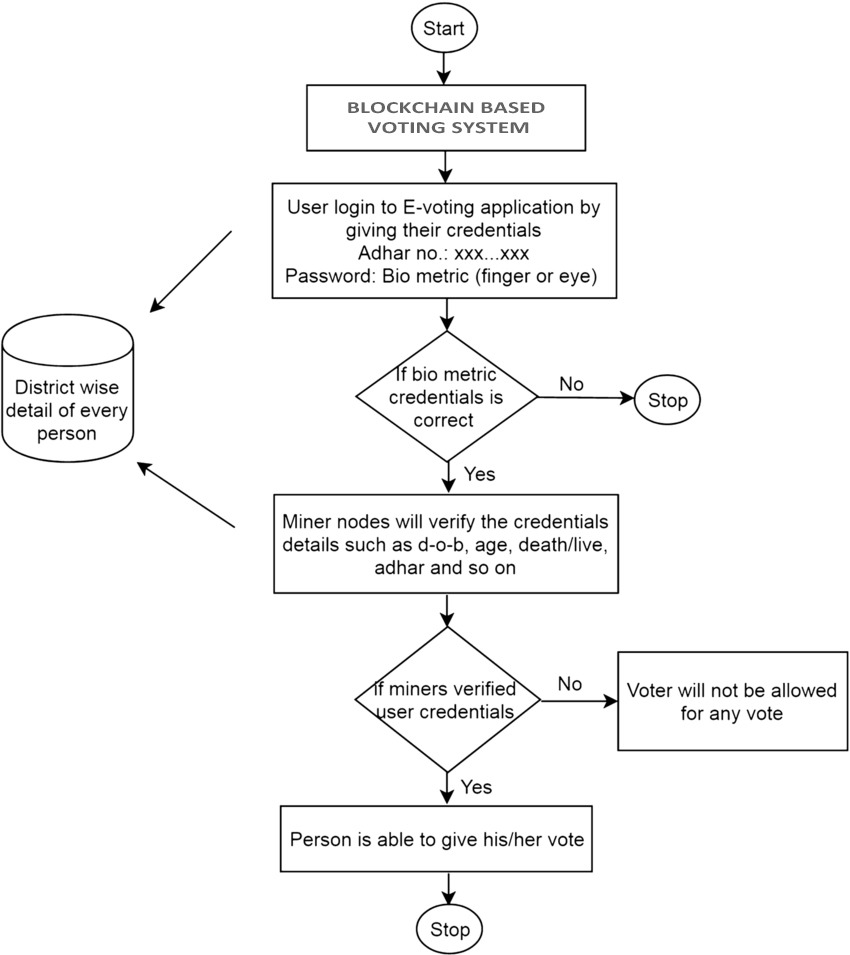


Figure 3: Flow Chart

# 6. Design models

**Sequence Diagram**

This sequence diagram shows that how the Dapp will work, tasks after tasks sequence-wise. It gives a complete description of the working of our Dapp.

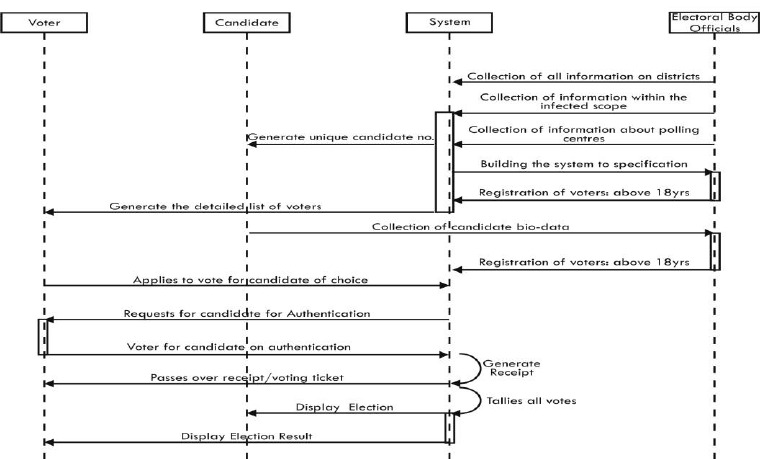


Figure 4: Sequence Diagram

**Class Diagram**

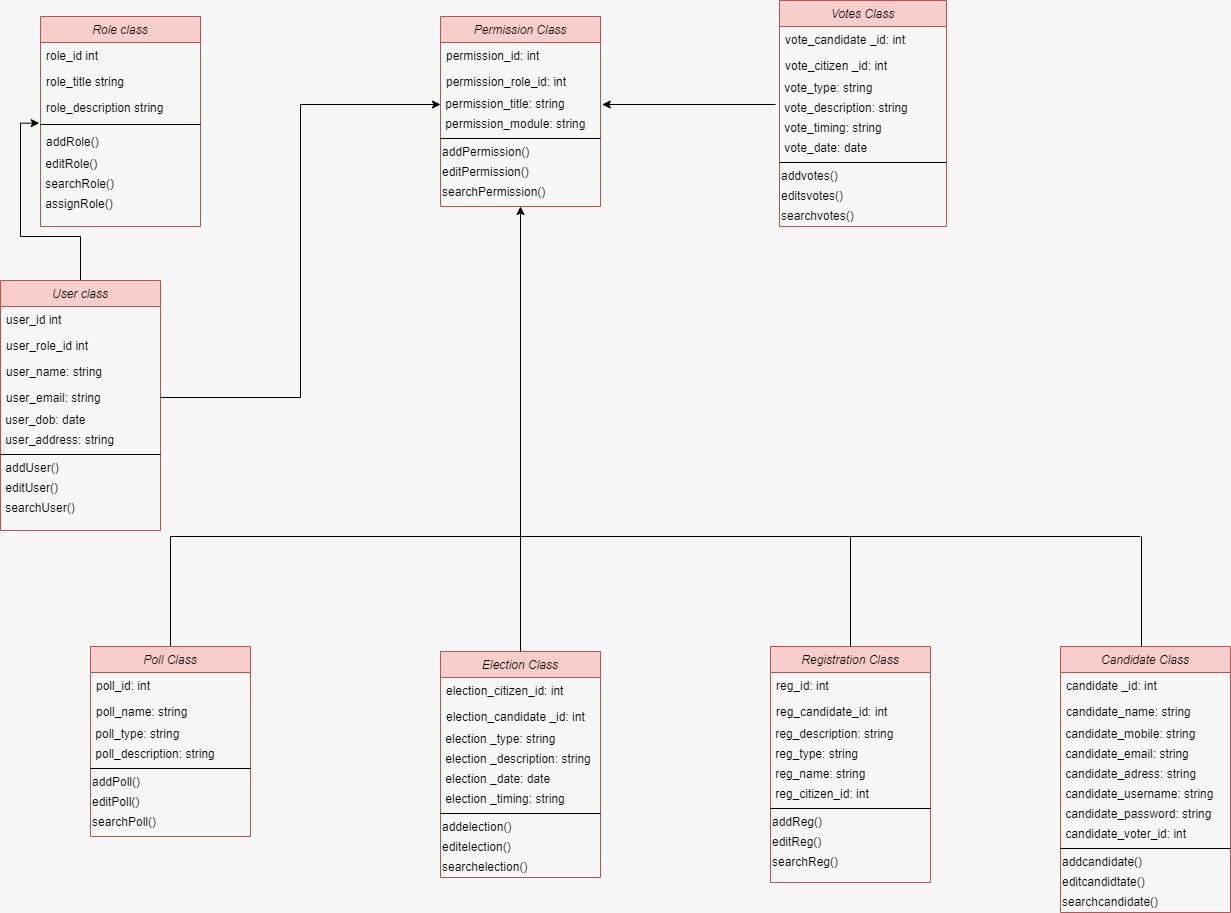
****

Figure 5: Class Diagram

**Data Flow Diagram**

This diagram represents the flow of data or process of the system. It gives complete information about the outputs and generated after providing the user’s inputs of each module and process itself**.**

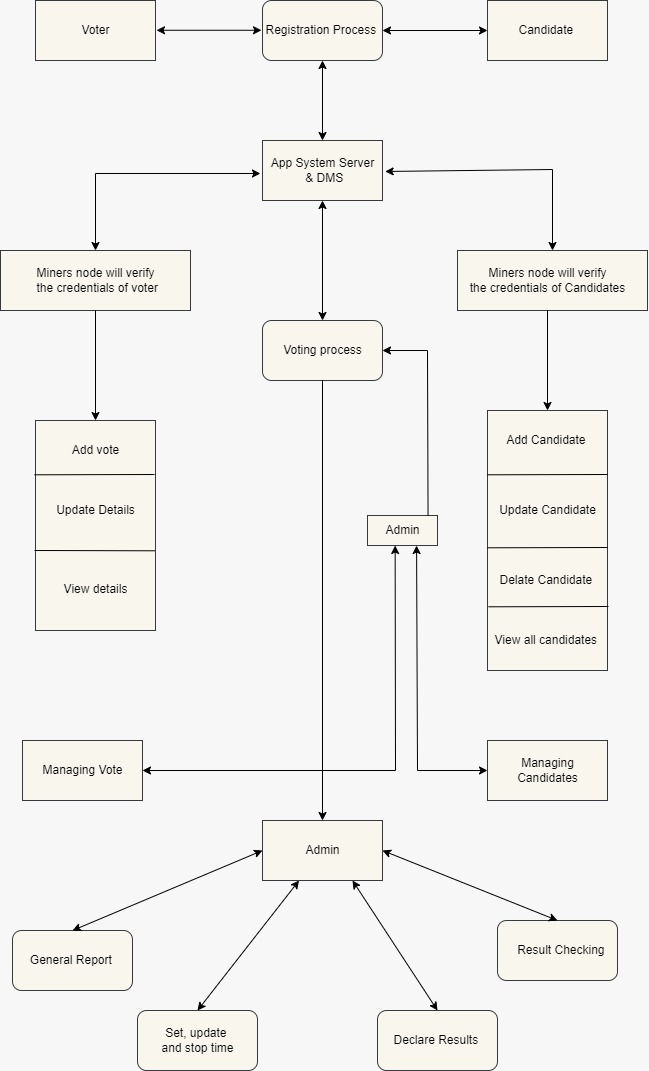
**LEVEL 1: **

Figure 6: DFD Level 1

# 7. Data design

In the Blockchain, data is designed in such a way that is secure and immutable. During the data design process, smart contracts are specified along with the required and provided rules for the data. Each transaction is stored in a block; every block relates to the previous block with a hash value that makes a chain of the blocks. Data is stored on the blockchain in the form of contracts and transactions. For Ethereum (the most popular blockchain for Dapps), the library Web3.js is used to communicate with the blockchain. The way this works is that it uses something called the JSON-RPC protocol to query the blockchain. Government and Citizens act as a user to each other on a peer-to-peer network, everyone has the same authority. Government registers the new members and candidates for storing and sharing data in a distributed file system. For testing, developing purposes, the Ganache is a personal blockchain that will be used in the system. Government can verify the vote, register new members, and view election results.

# 8. Data dictionary

* Blockchain-based E-voting system - BEVS
* Decentralized Application - DApp
* Smart Contracts - SC
* Data Flow Diagram - DFD
* Distributed Ledger -DL
* Entity Relationship Diagram - ERD
* Graphic User Interface - GUI
* Procedural description language - PDL
* State Transition Diagram - STD
* Unified Modeling Language - UML

# 9. Algorithm & Implementation

* Smart Contracts are programs stored on the blockchain it automates the execution of an agreement.
* All transactions are stored on the blockchain; each block has different transactions. Each block connects with the previous block by encrypted hash. It provides security to the blockchain.
* The voter must have to register to Dapp.
* Dapp has optimized search functionality, users can search the candidate’s name to cast vote.
* Users can check the results.
* Dapp automatically counts the votes.
* Government can register the candidates for voting.
* Also, view record history and votes cast by the people.
* All the events happened in the form of transactions that will be stored on the blockchain without third-party involvement.
* Blockchain makes Dapp secure, transparent, immutable, and verifiable.
* Also, trace back to check the history of previous owners.

# 10. Human interface design

There will be a user-friendly and responsive GUI. A Citizen can register to use the Dapp. The citizen can cast the vote after adding his special key and it is easy to cast the vote even a layperson can use it easily.

## **10.1 Screen imagesC:\Users\zubai\AppData\Local\Microsoft\Windows\INetCache\Content.Word\WhatsApp Image 2021-11-22 at 1.41.29 AM (1).jpeg**

**Figure 8: Graphical user interface, website

Description automatically generated**

Figure 9: ****

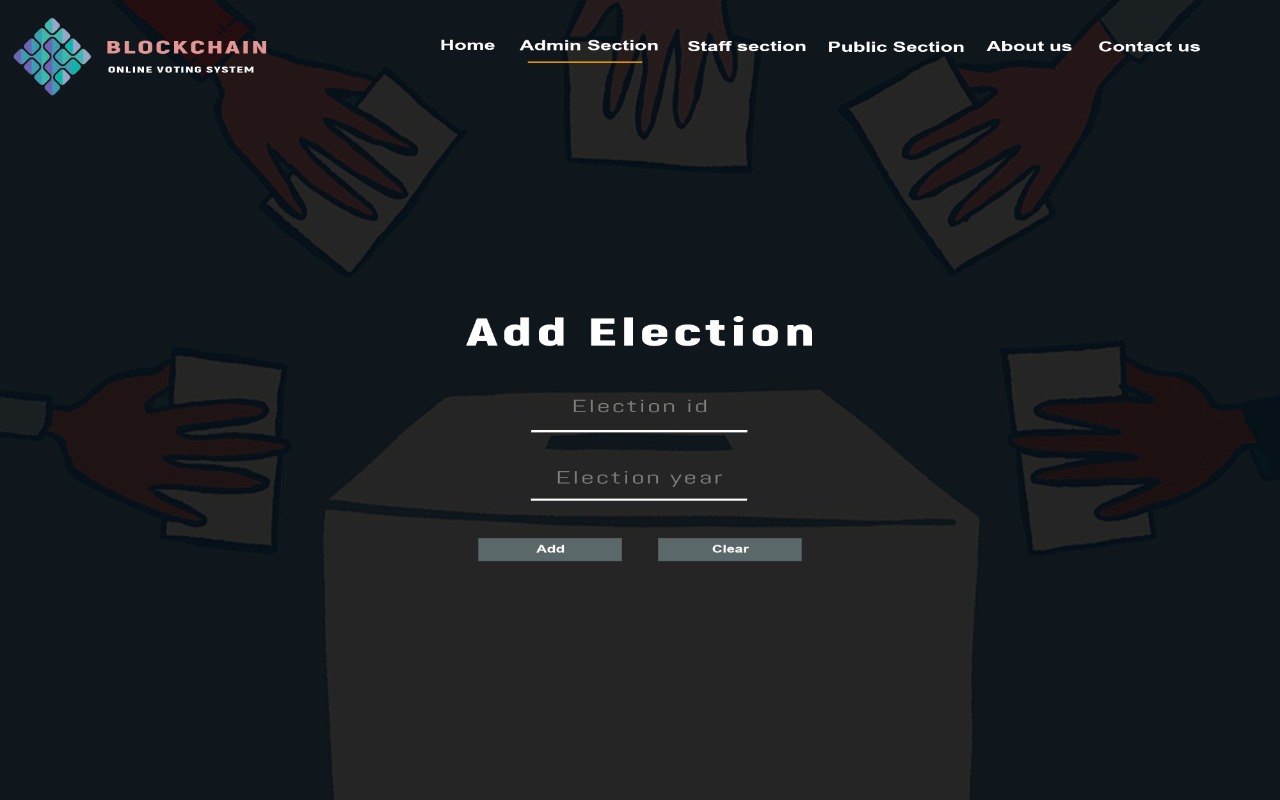


Figure 10:



Figure 11:

## **10.2 Screen objects and actions**

Screen objects containing the government side and citizen side. On the Government side, it will register voters, add election and record history, verify the member, and view cast votes. On the Citizen side, users can view candidates that are available for elections. With authentication, the user can view the see the results.

**References:**

* Analysis of an Electronic Voting System in Various Countries

Mr. Sanjay Kumar1

Department of Computer Engineering, M. M. University,

Mullana (Ambala) 133207, India

* Analysis of an Electronic Voting System in Pakistan

Ghafoor, Ahmed