

**COMSATS University Islamabad,**



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

**SOFTWARE REQUIREMENTS SPECIFICATION**

**(SRS DOCUMENT)**

**for**

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

Version 1.0

***By***

**Shehryar 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 5](#_Toc88719448)

[1.1 Purpose 5](#_Toc88719449)

[1.2 Scope 6](#_Toc88719450)

[2 Overall description 6](#_Toc88719451)

[2.1 Product Perspective 6](#_Toc88719452)

[2.2 Operating Environment 6](#_Toc88719453)

[2.3 Design and Implementation constraints 6](#_Toc88719454)

[3 Requirement identifying technique 7](#_Toc88719455)

[3.1 Use Case Diagram 7](#_Toc88719456)

[3.2 Use Case Description 7](#_Toc88719457)

[Specific Requirements 8](#_Toc88719458)

[3.3 Functional Requirements 8](#_Toc88719459)

[3.4 REGISTRATION MODULE 9](#_Toc88719460)

[3.5 ADD ELECTION 9](#_Toc88719461)

[3.6 ADD STAFF 9](#_Toc88719462)

[3.7 VOTER REGISTRATION 9](#_Toc88719463)

[3.8 CANDIDATE SELECTION 9](#_Toc88719464)

[3.9 VOTE CALCULATOR 9](#_Toc88719465)

[3.10 GOVERNMENT SIDE MODULE 10](#_Toc88719466)

[4 NON-FUNCTIONAL Requirements 10](#_Toc88719467)

[5 Quality Attributes 10](#_Toc88719468)

[5.1 Usability 10](#_Toc88719469)

[5.2 Performance 11](#_Toc88719470)

[5.3 Security 11](#_Toc88719471)

[5.4 Portability: 11](#_Toc88719472)

[6 References 12](#_Toc88719473)

**Revision History**

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

# Application Evaluation History

|  |  |
| --- | --- |
| **Comments (by committee)**  \*Include the ones given at scope time both in doc | **Presentation** |
|  |  |
|  |  |

**Supervised by**

<Mr. Nasir Mehdi>

**Signature\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

# 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.

## Purpose

Because it’s online it is and decentralized it is impossible to temper data and it does not use manual counting methods, so it also overcomes the counting problem. All necessary computations are done by computer so did not take much time nor required much manpower (like in manual voting system). Unable to hack due to its blockchain technology

Our proposed cost-effective Online Voting system will replace the manual record-keeping system of voters, candidates; duty staff by polling the votes by a computerized system, which will reduce the chances of error occurrence, while counting, minimize time being consumed during counting, increase the security of votes being polled. No chances of voter rejection and easy management of records.

The system developed on the blockchain is decentralized a peer-to-peer network and does not need any third party, all nodes have equal authority, immutability that if data is saved on the blockchain cannot tamper. It provides transparency means that every node can view it publicly. To provide automation, Blockchain has smart contracts which are predefined rules in form of coding which tell that how, when, and where certain processes happened.

## 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 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.

# Overall description

## Product Perspective

The product is supposed to be open source, under the GNU General Public License. The product is Dapp (Web) based system implementing a peer-to-peer model. The Blockchain-based e-voting System provides a strong mechanism for citizens to cast their vote, government can register new voters and verify it.

The following are the main features that are included in the Blockchain-based E-voting System

* Manage Vote Record: Government can manage their Votes; citizens can view the voting details.
* User Authentication: Users access the Dapp using login credentials, and new users must have to register before login.
* Optimized Search: search is an optimized local search engine based on keywords.
* Complain Forum: Provides the user with a platform to complain about the issue to resolve.

## Operating Environment

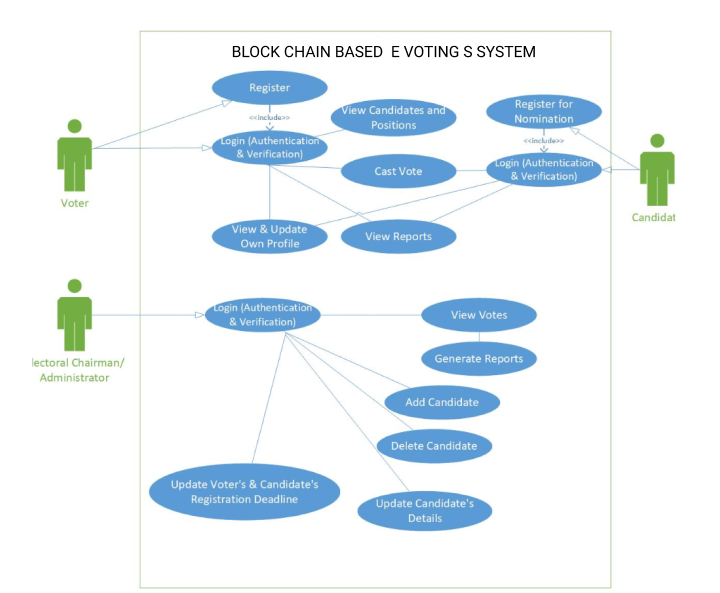
This Dapp will work on every operating system Windows (7,8,10), Linux, and Mac OS, and can be supported by any type and version of browsers installed in your operating system and browser must have Meta Mask extension added. Dapp also works on Android OS and IOS must have a browser with a Meta Mask extension. The operating system minimum has 4 GB RAM and needs good processing power to run the Dapp for better results.

## Design and Implementation constraints

This system is provisioned to be built on the React framework which is highly flexible. For data storage, it uses Blockchain to store the data, that use personal blockchain Ganache and Test Network, and for document storage that will use IPFS. The challenges in developing the product include deploying the Dapp on Ethereum Main net. The Dapp will be running 24 hours a day.

# Requirement identifying technique

## Use Case Diagram



## Use Case Description

The table below indicates a comprehensive use case template filled in with an example drawn from the BLOCHAIN BASED E-Voting SYSTEM.

|  |  |
| --- | --- |
| **Use Case ID:** | BLRS-1 |
| **Use Case Name:** | BLOCKCHAIN-BASED E-VOTING SYSTEM |
| **Actors:** | Primary Actors: Citizen,  Secondary Actor: Government |
| **Description:** | A Citizen can access the Blockchain-based e-voting System by login credentials and acting as a vote caster.  Smart Contract that makes a contract between the voter and government, transfer initiate, and voter data automatically deduces and update.  Government can access Dapp by their login credentials. And able to register new members, view voter history, manage the votes. |
| **Trigger:** | A Citizen registers himself for casting the vote. After getting registered, can accept or reject the registration request based on age. If the government accepts then the user is eligible to cast vote.  A Citizen search for candidates to cast the vote  Government checks and verifies the record of the user and the candidates as well. |
| **Preconditions:** | PRE-1. All users, candidates, and Government are logged into Blockchain-based E-Voting System to use it.  PRE-2. Both member and candidate must be registered for proper usage of Dapp and casting of votes into accounts.  PRE-3. Government must verify the voter data and register. |
| **Postconditions:** | POST-1. For registration of new voters and casting vote.  POST-2. For. the registration of the new candidate.  POST-3. Government must verify the vote. |
| **Normal Flow:** | Voter must log in for profile and view the total number of votes, view candidates.  Select the candidate to whom he wanted to vote |
| **Alternative Flows:** | Government can register the new member's details.  If any person has special issues, then he may proceed by using biometric and by a barcode reader. |
| **Exceptions:** | Dapp provides the facility to verify the voter, contract between candidate and government, automatically. |
| **Assumptions:** | Assume that one hundred transfer land each day. The system makes the record on daily basis. |
|  |  |

# Specific Requirements

## Functional Requirements

This system will have the following modules:

* **Module 1: Registration Module**
* **Module 2: Add Election**
* **Module 3: Add staff**
* **Module 4: Voter Registration**
* **Module 5: Candidate Selection**
* **Module 6: Vote Calculator**
* **Module 7: Government Side**

All the modules of Blockchain-based Dapp.

## REGISTRATION MODULE

* The user will log in using his account.
* In this system, registration is applied to all users.
* The government also acts as the user to cast the vote.
* Each user creates an account and gets a unique private number for casting vote.

## ADD ELECTION

* A user can add his election id and username.
* The user has the option to add and clear the data.
* And the user can display all his necessary information.

## ADD STAFF

* Users can enter their staff id, name, and designation.
* The senior designated member can view the record of other members.
* The staff member sends the request to the Government by using the Dapp (Distributed App).
* The senior member can view the request and be able to accept and reject the request of the voter.
* If the Government accepts then the piece of code called smart contract self-execute and checks the condition, then approval is sent to the member of staff.
* The staff member confirms the request and approval will send to the member.

## VOTER REGISTRATION

* The voter can register himself by giving his information.
* The voter must be at an age of 18.
* The one candidate can have a specific number that helps him in casting the vote.

## CANDIDATE SELECTION

* This option is for the government who want to check details about the members.
* They can view the history of the casted vote by entering the ID of that member.
* Also, the officials can check the list of votes by a particular user by entering the address key corresponding to the account of that user.

## VOTE CALCULATOR

* This option is public available to all users.
* The vote counter is easily accessible to all users.
* It is very beneficial for all people that they can easily see the results on time.

## GOVERNMENT SIDE MODULE

This module will be used by Government only.

**Table 6 Show the functional requirement template.**

|  |  |  |
| --- | --- | --- |
| **Identifier** |  | Government Side |
|  |  |  |
| **Title** |  | Manage Votes |
|  |  |  |
| **Requirement** |  |  |
|  |  |  |
|  |  |  |
|  |  | Government must verify the results and ensure that no anomalies in the record. Also, register new members with detail. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| **Source** |  | From both citizens and candidates. |
|  |  |  |
| **Rationale** |  | To verify the votes to avoid any tampering. |
|  |  |  |
| **Business Rule** | **(If** | The citizen must be eighteen years old, and he must be Pakistani |
| **required)** |  |  |
|  |  |  |
| **Dependencies** |  | Both citizens and candidates |
|  |  |  |
| **Priority** |  | Medium |
|  |  |  |

# NON-FUNCTIONAL Requirements

Non-Functional Requirements are the requirements that specify criteria that can be used to judge the operation of the system. Those constraints under which the system will be operated are called non-functional requirements. Each request should be processed depending on Ethereum Blockchain. The site should load in 3 seconds when the number of simultaneous users is greater than 10000. The system uses the ERC20 token. Land deed document stored on IPFS.

# Quality Attributes

## Usability

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.

## Performance

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 government the 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.

## Security

All the data inside the system and the system itself will be protected against malware attacks or unauthorized access. Each user has their login credentials to access the system. Datastore in the blockchain that is impossible to hack because of data store in the form of transaction in a block, each block connected with the previous block with the encrypted hash value. If anyone tries to change the data, then other nodes validate it if the data change, then the transaction is failed automatically by the system.

## Portability:

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.

# 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