A Major Project Final Report on

E-voting Based on Blockchain

Submitted in Partial Fulfillment of the Requirements for

the Degree of Bachelor's in Computer Engineering

under Pokhara University

Submitted by:

Baradan Mainali, 14308

Prazeen Mainali, 14328

Prakash Aryal, 14329

Rohit Shrestha, 14336

Sanjeev Maharjan, 14337

Under the supervision of

Er. Bhusan Thapa

Date:

08 DEC 2018

Department of Computer Engineering

NEPAL COLLEGE OF INFORMATION TECHNOLOGY

Balkumari, Lalitpur, Nepal.

Acknowledgement

We take this opportunity to express my deepest and sincere gratitude to our supervisor **ER. Bhusan Thapa**, Lecturer, Department of Computer Engineering for his insightful advice, motivating suggestions, invaluable guidance, help and support in successful completion of this project and also for his constant encouragement and advise through our bachelors programme.

We express our deep gratitude to our Department head **Er.Resha Deo**, Department of Computer Engineering for his regular support ,co-operation ,and co-ordination. The in-time facilities provided by the department throughout the Bachelor program are also equally acknowledgeable.

We would like to convey or thanks to our thanks to our principal **Niranjan Khakurel** and teaching and non-teaching staff of the Department of Computer Engineering, NCIT for their invaluable help and support throughout the period of Bachelor Degree. We are also grateful to all our classmate for their help, encouragement and invaluable suggestions.

Finally, yet more importantly, I would like to express my deep appreciation to our family members, friends, and all staffs and lecturers for their perpetual support and encouragement throughout the Bachelor's degree period.

Baradan Mainali-14308

Prajin Shrestha-14328

Prakash Aryal-14329

Rohit Shrestha-14336

Sanjeev Maharjan-14337

Abstract

In this document based on the blockchain technology, we propose a decentralized E-voting protocol, without the existence of a trusted third party. Furthermore, we provide several possible extensions and improvements that meet the requirements in some specific voting scenarios. This document describes the ongoing problems with the E-voting system used currently. Then to solve these problems, the project proposes a E-voting based on blockchain to follow the given objectives. Here we evaluate the potential of distributed ledger technologies, namely the process of an election and implementing a blockchain based application which improves the security and decreases the cost of election. Because of the properties such as transparency, decentralization, irreversibility, nonrepudiation, etc., blockchain is not only a fundamental technology of great interest in its own right, but also has large potential when integrated into many other areas. After developing this application, the Blockchain-based system will be secure, reliable, and anonymous, and will help increase the number of voters as well as the trust of people in the election.

Keywords: E-voting, Blockchain, Secure E-voting

Table of Contents

List of figures

1. Introduction

Electronic voting (e-voting), which uses electronic systems to aid casting and counting votes in an election. E-voting is used for a general election. In E-voting anonymity is an important factor to run a fearless election. Unfortunately guaranteeing anonymity also makes it harder to track election fraud and errors. Because of the properties such as transparency, decentralization, irreversibility, nonrepudiation, etc., blockchain is not only a fundamental technology of great interest in its own right, but also has large potential when integrated into many other areas.

1.1. Problem Statement

Traditional voting systems employ the use of papers which makes it non environment-friendly. Traditional voting system/paper voting system is time consuming, in paper voting system there is complexity of the documentation and records and it may consume a lot of time. Paper voting system takes a lot of manpower as well as it requires maximum budget to complete the election. As information technology evolves over time, the need for a better, faster, more convenient and secure electronic voting is essential requirement.

1.2. Objectives

E-voting based on blockchain is proposed with the following objectives in mind:

1. Use blockchain as a secure transaction database, to log votes and audit vote results
2. Shift E-voting slightly towards decentralization and minimize trust required on the organizers
3. Allow free, independent audits of the results

1.3. Significance of Study

The main purpose of e-voting is to support and enhance democratic process. Also, our project will be great helping hand for the beginning or

the new comers that are willing to work in the sector of e-voting as well as the reference that can be viewed thoroughly in advance in the future projects and get idea and support. It can also encourage government and official sectors to change the way of doing things in compliance with reliability and confidentiality. The shift towards technological workspace is great with the futuristic approach which can be greatly implemented in the sector of voting by the electronic mechanism. The study can also be super motivative for many individuals of different age groups. Our project would likely increase the voter turnout. Distrust and Insecurity felt due to centralization of traditional E-voting systems leads to low voters' turnout which is usually considered to be undesirable because only high voters' turnout is seen as evidence of the legitimacy of the election held. Low voter turnout may not be an acceptable reflection of the will of people. This project could create new potential for election systems. Since it is digital, it is easier to provide ballots in multiple languages, accommodate lengthy ballots, facilitate early and absentee voting, etc. Apart from this, voting provision for disabled people can be managed with ease.

2. Methodology

2.1. Software Development Life Cycle

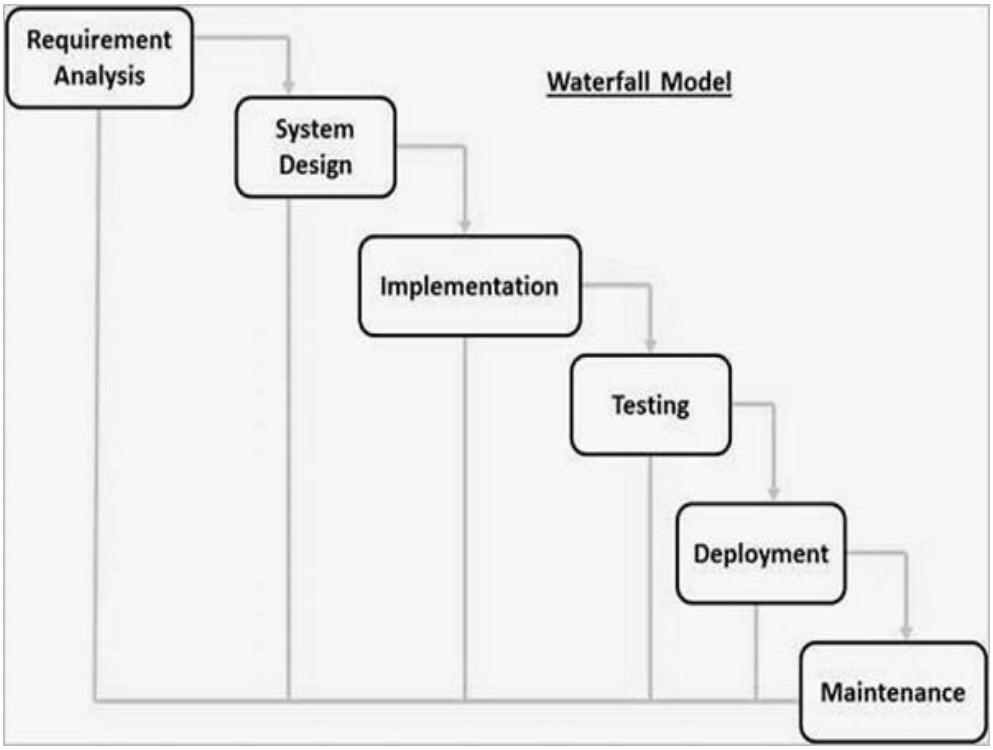

figure 2. 1 Waterfall model

(SDLC Waterfall Model, n.d.)

Requirement Gathering and analysis: All possible requirements of the system to be developed are captured in this phase and documented in a requirement specification document.

System Design: The requirement specifications from first phase are studied in this phase and the system design is prepared. This system design helps in specifying hardware and system requirements and helps in defining the overall system architecture.

Implementation: With inputs from the system design, the system is first developed in small programs called units, which are integrated in the next phase. Each unit is developed and tested for its functionality, which is referred to as Unit Testing.

Integration and Testing: All the units developed in the implementation phase are integrated into a system after testing of each unit. Post integration the entire system is tested for any faults and failures.

Deployment of system: Once the functional and non-functional testing is done; the product is deployed in the customer environment or released into the market.

Maintenance: There are some issues which come up in the client environment. To fix those issues, patches are released. Also, to enhance the product some better versions are released. Maintenance is done to deliver these changes in the customer environment.

2.2. Gantt Chart

ID	Task Name	Start	Finish	Duration
1	Requirement Analysis	7/2/2018	7/30/2018	4.14w
2	Planning	8/1/2018	8/20/2018	2.86w
3	Designing	8/21/2018	9/10/2018	3w
4	Coding and implementation	9/11/2018	10/30/2018	7.14w
5	Tessting	11/1/2018	11/20/2018	2.86w
6	Documentation	11/23/2018	12/3/2018	1.57w

figure 2. 2 : Gantt Chart

3. Software Requirement Specifications

3.1. Generic voting principles

1. Only eligible persons vote
2. No person gets to vote more than once
3. The vote is secret
4. Each (correctly cast) vote gets counted
5. The voters trust that their vote is counted.

3.2. Voting System design criteria

Democratic: A system is considered to be "democratic" if only eligible voters are allowed to vote (eligibility) and if each eligible voter can only cast a single vote (reusability). An additional characteristic is that no one should be allowed to duplicate anyone else's vote.

Accuracy: Correctness of the system. Election systems should record the votes correctly. The announced result should match the actual outcome of the election.

Reliability: No reasonably sized coalition of voters or authorities (either benign or malicious) may disrupt the election. This includes allowing abstention of registered voters, without causing problems or allowing other entities to cast legitimate votes on their behalf, as well as preventing misbehavior of voters and authorities from invalidating the election outcome by claiming that some other actor of the system failed to properly execute its part.

Robustness implies that security should also be provided against external threats and attacks, e.g. denial of service attacks.

Integrity: Votes should not be able to be modified without detection.

Verifiability: Should be possible to verify that votes are correctly counted for in the final tally. Results can be find agree on the election result by comparing election data with other holders of election data or by checking whether an individual vote has been properly cast.

Auditability: There should be reliable and demonstrably authentic election records.

Secrecy: No one should be able to determine how or whom any individual voted.

Non-coercibility: Voters should not be able to prove how they voted. An incoercible scheme does not allow the voters to convince any other participant (e.g. a coercer) on what they have voted.

Fairness: Should ensure that no one can learn the outcome of the election before the announcement of the tally. Therefore, acts like influencing the decision of late voters by announcing an estimate, or provide a significant but unequal advantage (being the first to know) to specific people or groups, are prevented.

Flexibility: Equipment should allow for a variety of ballot question formats.

Convenience: Voters should be able to cast votes with minimal equipment and skills.

Certifiability: Systems should be testable against essential criteria.

Transparency: Voters should be able to possess a general understanding of the whole process.

Cost-effectiveness: Systems should be affordable and efficient.

4. Literature Study

(Wang)There has been a lot of work on remote e-voting protocols using cryptographic
tools. In some cases, a trusted third party is involved to make e-voting systems more easily implemented and controlled.

The first-ever electronic voting system was introduced in the early eighties by David Shaum. The system used a public key cryptography, which was used to cast votes and keep voters anonymous. To make sure there were no links between voters and ballots, the Blind Signature Theorem was used. Since the system was first introduced, many scholars have shown interest in the subject, and a lot of research has been done. Most of the research done on the field has focused on the Direct Recording Electronic System and the Internet Voting Systems. The first International Journal of Network system is used in polling stations instead of the paper ballot voting system, but the second system is meant to be mobile and allows voters to cast their votes from anywhere using any device Internet connection.

Estonia was the first country where citizens were able to cast their vote using only the Internet and an electronic national identification card. The ID card used in the elections was designed to run on an integrated circuit, a chip Java chip platform, and protected with 2048bit PIN.

In 2011 Norway used an electronic remote voting system for the country council elections. The system was developed by e-voting vendor Scytl, and was very similar to the Estonian electronic voting system. However, in 2014, the country has discontinued its I-Voting project due to security concerns. One of the main critics Norwegian I system faced was the fear of votes going public in case of a cyber-attack.

Zhao and Chan proposed a voting protocol in 2015, which introduces a reward/penalty scheme for correct or incorrect behaviors of voters. Although the protocol has some limitations, this is the first attempt to combine e-voting with blockchain (Zhao, 2015). Later in 2016, Lee, James, Ejeta and Kim proposed an e-voting protocol which involves a TTP into blockchain to preserve voters' choices. Very recently, using Bitcoin, there had been proposed another

e-voting protocol [1]. This protocol divides the organizer of elections into two different parts - the Authentication Server (AS) and the Token Distribution Server (TDS), to protect voters' privacy. However, there remain some problems in this protocol, for example, it is difficult to inspect these two parts' behaviors, and it limits the extension of the voting scheme.

But Here in this paper, we integrate the blockchain paradigm into e-voting procedure and come up with a feasible and general e-voting protocol without a TTP, which provides a secure and flexible voting mechanism, satisfies almost all of the main requirements for an e-voting system and weakens the power of the election organizer.

5. Scope and Limitations

The scope and limitations of blockchain based voting system are as follows:

Scope:

1. This project will provide a usable E-voting system for small scale election by communities, associations or small organizations
2. Voters have the opportunity to vote quickly and conveniently
3. Votes can be counted in real time system.
4. E-voting is more accurate.
5. Within a day voting will be completed.

Limitations:

1. Susceptibility to fraud.
2. Difficult to implement in rural areas
3. Coercion is not attainable. It will require much more focus and we feel like t

6. Tools and Techniques

6.1. Blockchain

The blockchain protocol is a means of logging and verifying records that is transparent and distributed among users. Usually, votes are recorded, managed, counted and checked by a central authority. Using this would empower voters to do these tasks themselves, by allowing them to hold a copy of the voting record. The historic record could then not be changed because other voters would see that the record differs from theirs. Illegitimate votes could not be added, because other voters would be able to scrutinize whether votes were compatible with the rules (perhaps because they have already been counted, or are not associated with a valid voter record). BEV would shift power and trust away from central actors, such as electoral authorities, and foster the development of a tech-enabled community consensus. One way of developing BEV systems for e-voting is to create a new, bespoke system, designed to reflect the specific characteristics of the election and electorate. A second approach that may be cheaper and easier is to 'piggyback', running the election on a more established blockchain, such as that used by the virtual currency, bitcoin. Given that the security of a blockchain ledger relies upon the breadth of its user base, this piggyback approach may also be more secure for elections with a small number of voters. Blockchain experts are discussing a new generation of 'techno-democratic systems', and we can already see the emergence of virtual equivalents of national administrations, based upon blockchain technology. However, in the near term, BEV's strongest potential may be in organizational rather than national contexts. Indeed, they have been used for the internal elections of political parties, and shareholder votes in Estonia. Taking the concept, a step further, BEV could be combined with smart contracts, to automatically act under certain agreed conditions. Here, for example, election results could trigger the automatic implementation of manifesto promises, investment choices or other organizational decisions.

6.2. Ethereum

(Wood, 2014)Ethereum is a decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third-party interference. These apps run on a custom built blockchain, an enormously powerful shared global infrastructure that can move value around and represent the ownership of property. Smart Contracts for the Ethereum can be written in solidity.

6.3. Blind Signature

(Camenisch, 1994)It is a form of digital signature in which the content of a message is disguised (blinded) before it is signed. The resulting blind signature can be publicly verified against the original, unblinded message in the manner of a regular digital signature. Blind signatures are typically employed in privacy-related protocols where the signer and message author are different parties.

7. Business Process Model

7.1. Registration process

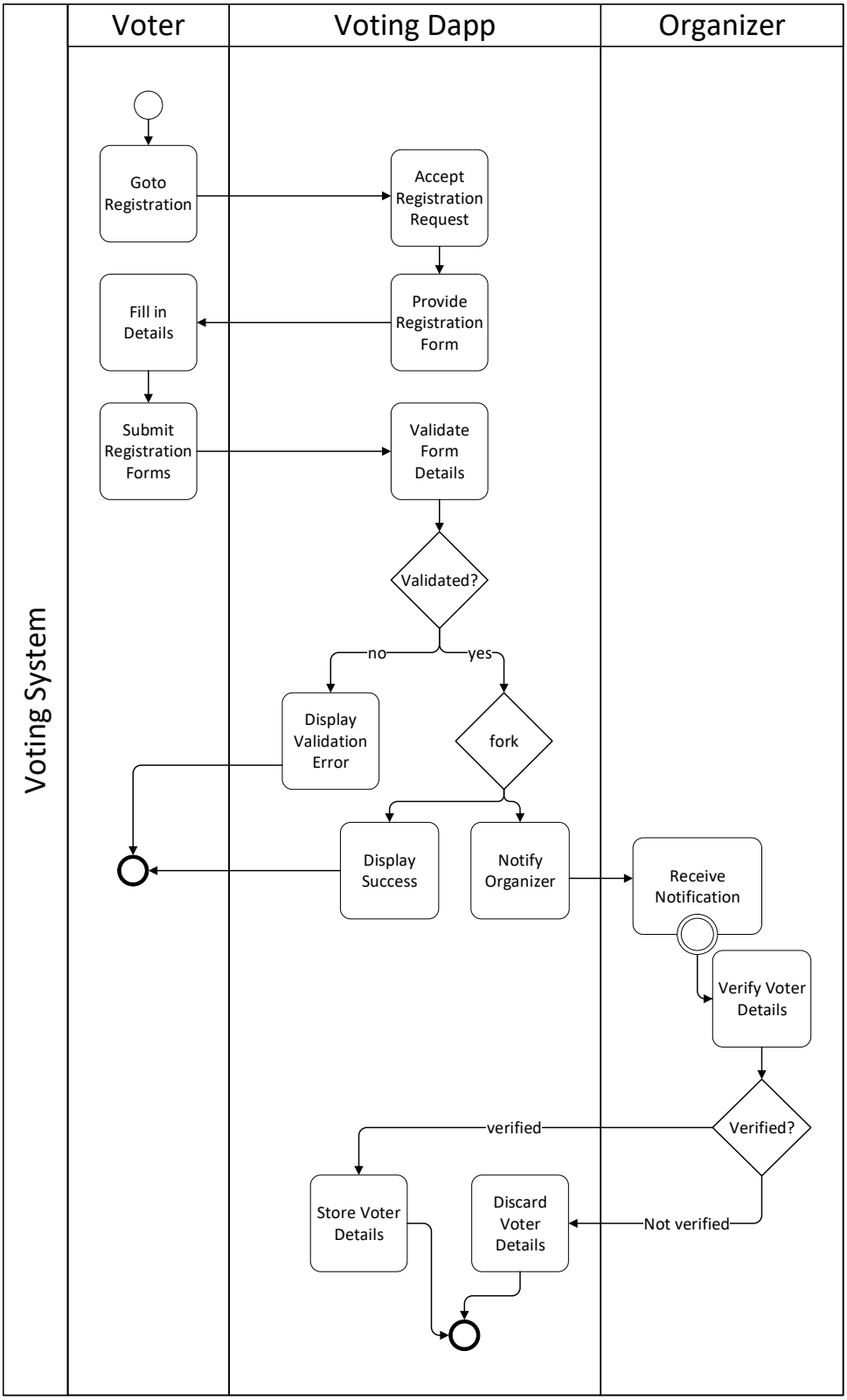

figure 7. 1 Registration Process

7.2. Voting Process

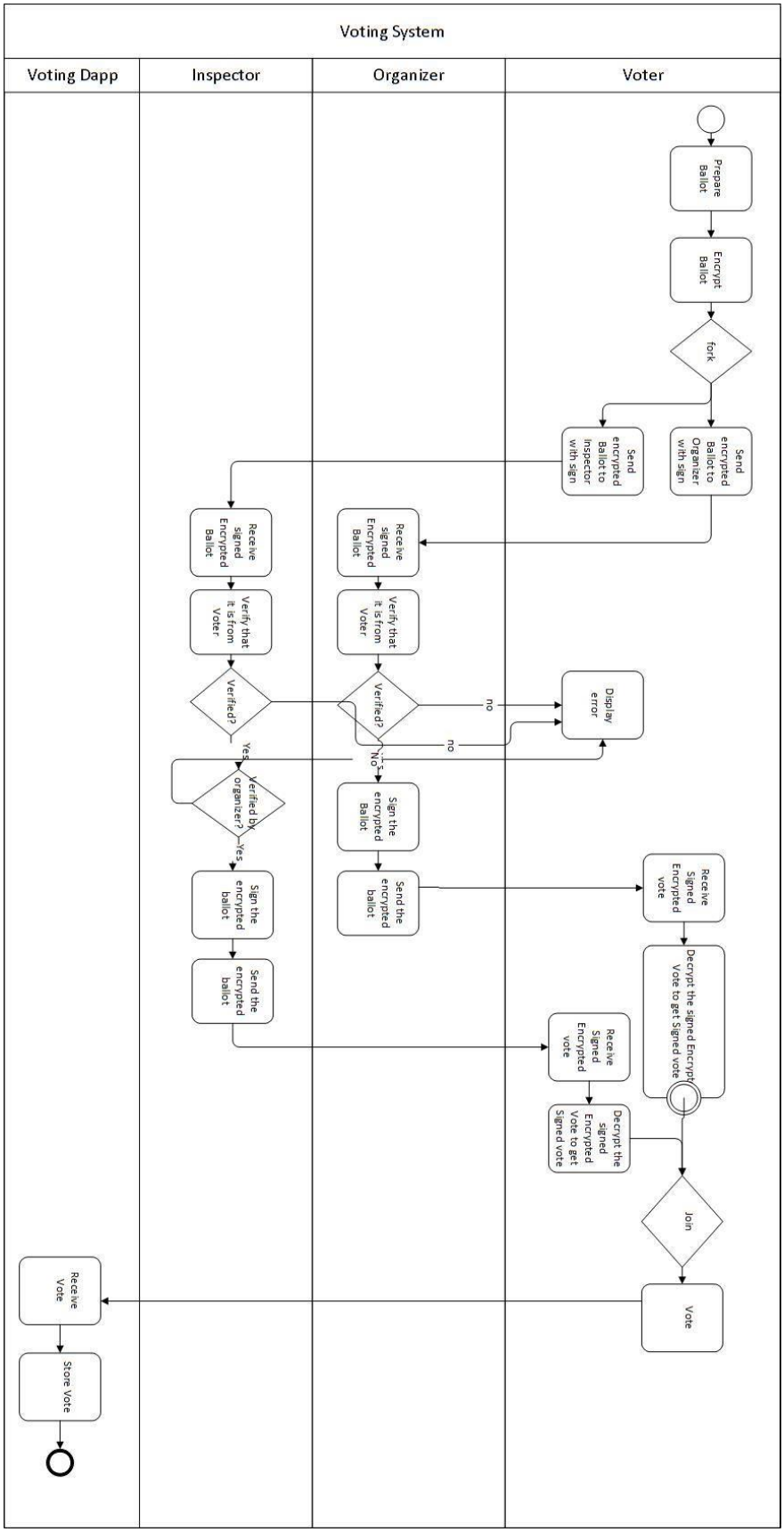

figure 7. 2 : Voting Process

8. Use-case diagram

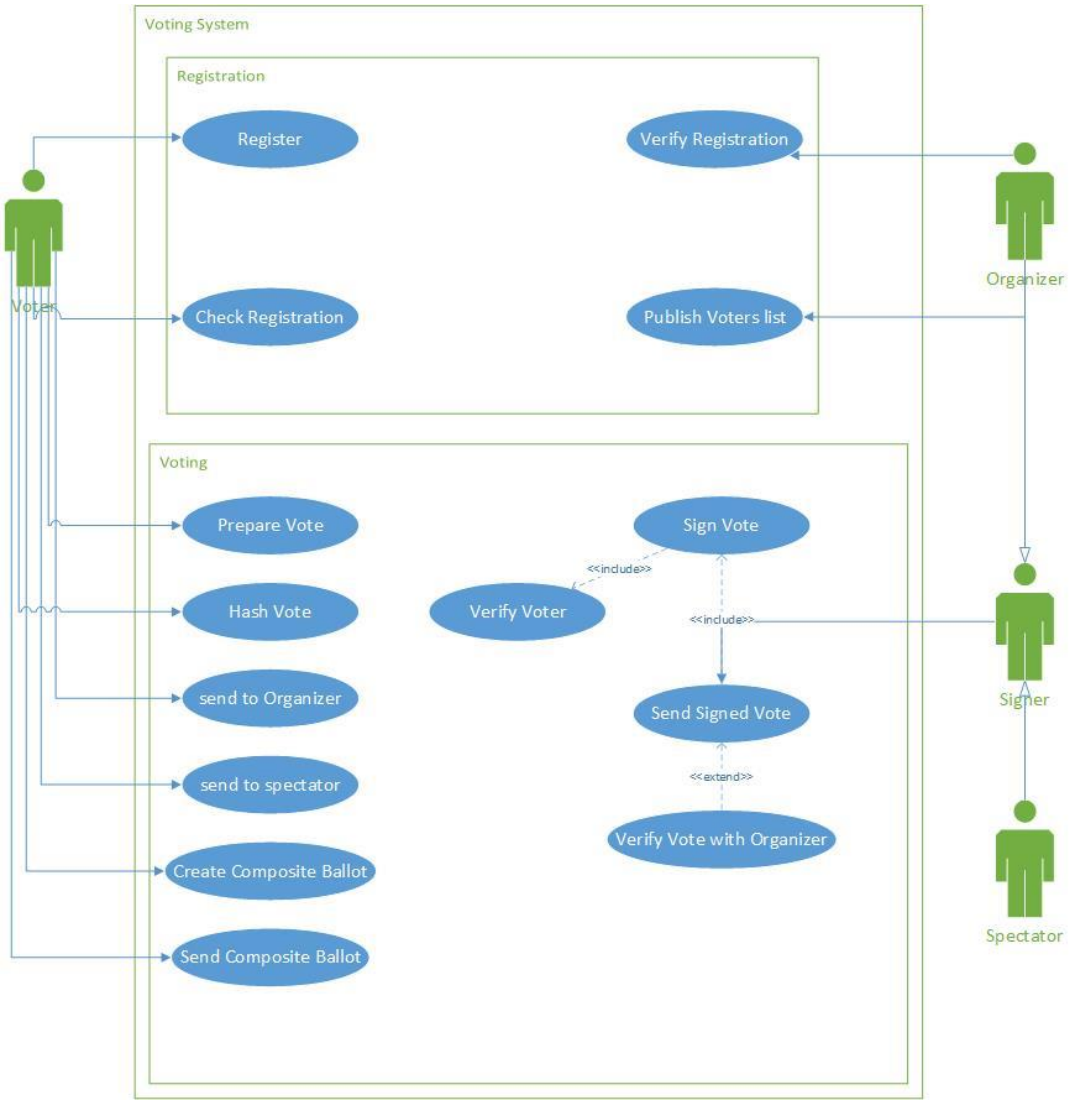

figure 8. 1 : Use Case Diagram

Conclusion

Using blind signature and blockchain, we proposed an e-voting protocol, which introduces a lot of desirable properties from blockchain.This paper describes how to define and implement a new e-voting system concept. This system is called Crypto-voting and it is based on permissioned blockchain technology., In this technology and there is a use of tool known as Smart Contracts. This document focuses on the potential of the blockchain technology. We described how it is possible to implement Crypto-voting system using blockchains. The first records voters and voting procedures, the second counts vote and provides voting results. This approach emphasizes the importance of anonymization of the network consensus nodes. Smart contracts will be responsible for managing voting procedures and results. Our system increases the efficiency of the validation phase and of the assignment of the candidate's vote. Using blind signature and blockchain, we proposed an e-voting protocol, which introduces a lot of desirable properties from blockchain.

Further Works

In this section, we discuss some possible further improvements when applying the e-voting protocol in special elections and scenarios.

In our protocol, the communication through the blockchain network may divulge voters' IP addresses, which may lead to the exposure of connections between voters and ballots via network analysis. To enhance voters' privacy, we recommend voters to use anonymity services like proxies or TOR [26], with which voters can hide their IP addresses.

Corruption may happen if the organizer and inspector conspire together, since both of their signatures are components of a valid ballot. To avoid this kind of dishonest behaviors, we can introduce more inspectors such that the corruption cost is greatly increased.

Bibliography

Ambler, S. W. (2010). *The Agile System development.* Mexico: Youth Publications.

Camenisch. (1994). *Blind signatures based on the discrete logarithm problems.*

SDLC Waterfall Model. (n.d.). Retrieved from https://www.tutorialspoint.com

Wang, Y. L. (n.d.). *1043.* Shenzhen, China: Southern University of Science and Technology.

Wood. (2014). *Ethereum.*

Zhao, Z. C. (2015). *How to vote privately using bitcoin.* In Qing, S., Okamoto.