**Synopsis**

**on**

**Online Voting System using Blockchain**

**Submitted in the partial fulfillment of the**

**Degree of Bachelor of Technology**

**(Computer Science and Engineering)**

**Submitted by**

**Avdhesh Chaudhary (02315002719)**

**Amar Sinha (04415002719)**

**Chirag Aggarwal (04615002719)**

**Under the supervision of Mr. Vikrant Shokeen (Assistant Professor CSE)**



**Department of Computer Science and Engineering**

**Maharaja Surajmal Institute of TechnologyJanakpuri, New Delhi.**

**2019-23**

|  |  |
| --- | --- |
| **INDEX** |  |
| **1. Abstract** | **1** |
| **2. Introduction** | **2** |
| **3. Literature Survey** | **3** |
| **4. Objective** | **4** |
| **5. Research Methodology** | **5** |
| **6. Gantt Chart** | **6** |
| **7. References** | **8** |

# Abstract

In any democratic country, Voting is a fundamental right of any citizen that enables them to choose the leaders of tomorrow. It gives individuals in a community the facility to voice their opinion. It helps them to realize the importance of citizenship. Online voting systems are software platforms used to securely conduct votes and elections. As a digital platform, they eliminate the need to cast your votes using paper or having to gather in person. They also protect the integrity of your vote by preventing voters from being able to vote multiple times.

Electronic voting or e-voting has fundamental benefits over paper based systems such as increased efficiency and reduced errors. The electronic voting system tends to maximize user participation, by allowing them to vote from anywhere and from any device that has an internet connection. The blockchain is an emerging, decentralized, and distributed technology with strong cryptographic foundations that promises to improve different aspects of many industries. Expanding e-voting into blockchain technology could be the solution to alleviate the present concerns in e-voting. Here we propose a Blockchain based voting system that will limit the voting fraud and make the voting process simple, secure and efficient.

# Introduction

India is a democratic country and has a democratic country. As now all Indian citizen become a part of the growing digital India with a digital ID that is Aadhaar card. Voting schemes have evolved from counting hands in early days to systems that include paper, punch card and electronic voting machine.

The Existing System of Election is running manually. The Voter has to Visit to Booths to Vote a Candidate so there is wastage of Time. Due to this many people don’t go out to cast their vote which is one of the most important and Worrying factor. In democracy Each and every vote is important. This Traditional system can be replaced by a new online system which will limit the voting frauds and make the voting as well as counting more efficient and transparent.

# Proposed System:

The current voting system requires some improvement in it because of the issues mentioned above. This can be achieved by replacing the existing system by the new system which will limit the voting frauds and make the voting as well as counting more efficient.

- Online Election System would have user registration, user login and admin login.

- This Online Voting System will manage the Voter’s information by which voter can login and use his voting rights.

- At the time of registration voter will be asked for this: Full name, age, Aadhaar card no, mobile no. email id and after being verified will be given the access.

- At the time of requesting vote, voter will be asked to enter his Aadhaar id. Then voter will be authenticated, and he can give vote from one of the candidate from the list .Voters can vote for a Candidate only once per Election.

- The software system allows the user to login in to their profiles and upload all their details including their previous milestone onto the system. The admin can check each Candidate details.

- The software system also allows Voters to view a list of Candidates in their area. The admin has overall rights over the system and can moderate and delete any details not pertaining to Election Rules.

# Blockchain

Blockchain can help to implement a system that is immutable, transparent, and efficient and cannot be hacked into. The inability to change or delete information from blocks makes the blockchain the most effective technology for voting systems. Blockchain technology is supported by a distributed network consisting of variety of interconnected nodes. Each of these nodes have their own copy of the distributed ledger (information) that contains the total history of all transactions the network has processed. There is no centralized system that controls the network. If the majority of the nodes agree, then they accept a transaction. This network permits users to stay anonymous. A basic analysis of the blockchain technology (including sensible contracts) suggests that it is an appropriate basis for e-voting and furthermore, it might have the potential to form e-voting a lot of acceptable and reliable.

# Block

Every chain consists of multiple blocks and each block has three basic elements:

Data (i.e transactions), the hash of the previous block and the block hash value. Hash value is a unique value, identifying one block. It depends on the block’s content (data and previous block hash), so each block has its unique hash value, and it’s identifying this block only.

# Smart Contracts

Smart contracts are self-executing contracts which contain the terms and conditions of agreement between peers.

They are simply programs stored on a blockchain that run when predetermined conditions are met.

They typically are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary's involvement or time loss.

Smart contracts eradicate the need for a third-party intermediary of facilitator, essentially giving you full control of the agreement.

**Benefits of E-voting system over the current system:**

**1. Increasing the level of participation**

The Internet voting system tends to maximize user participation, by allowing them to vote from anywhereand from any devicethat has an internet connection.

**2. Security**

By considering the importance of the e-voting system is implemented using “Blockchain”.

**3. Efficiency**

The reductionin organizational and implementation costssignificantly increases the efficiency of election management compared to traditional paper voting, for example.

**4. Precision**

The electronic vote eliminates errors in manual count, which brings with it an accurate and quick publication of results, with receipt of vote for each vote cast

# Literature Survey

Currently increasing digital technology helped many people lives. In contrast to the electoral system, there are many conventional uses of paper in its implementation. The aspect of security and transparency is a threat from still widespread election with the conventional system .Block chain technology is one of solutions, because it embraces a decentralized system and the entire database are owned by many users.

There is no doubt that the revolutionary concept of the blockchain, which is the underlying technology behind the famous cryptocurrency Bit coin and its successors, is triggering the start of a new era in the Internet and the online services. In this work, we have implemented and tested a sample e-voting application as a smart contract for the Ethereum network using the Ethereum wallets and the Solidity language.

E-voting is a potential solution to the lack of interest in voting amongst the young tech savvy population. For e-voting to become more open, transparent, and independently auditable, a potential solution would be base it on block chain technology. Block chain technology has a lot of promise; however, in its current state it might not reach its full potential.

# Objective

The main objective of our project is to develop online voting system using blockchain.

**Objectives Pointwise:**

1. Improve on the shortcomings of I-voting system, that is Internet Voting system. In Internet voting system, the major issue is the centralized nature of the Internet i.e. somewhere all votes will have to be stored and if that is hacked or changed the whole voting system fails.
2. Improve on existing blockchain based models for voting system, as seen in some African countries where decentralized voting system is implemented.
3. Provide a secure platform for voting.
4. Develop a generalized voting system i.e. not only limited to election based voting but can also be extended to voting in institutions.

# Research Methodology

For our proposed plan of work we are considering two modules that are to be completed

in three phases. Two modules are as follows:

1. Front-end for the application

2. Back-end using Solidity to implement Blockchain.

**Ethereum:**

For developing E-voting using Blockchain we will be using Ethereum - a popular platform for creating distributed Blockchain applications that support smart contracts.

**Solidity:**

Solidity is a contract-oriented, high level language for implementing Smart contracts. It is statically typed, support inheritance, libraries and complex user-defined types among other features.

**Metamask:**

For performing any transaction on the blockchain we require an account which will have unique account address. This can be created using the Metamask chrome extension.

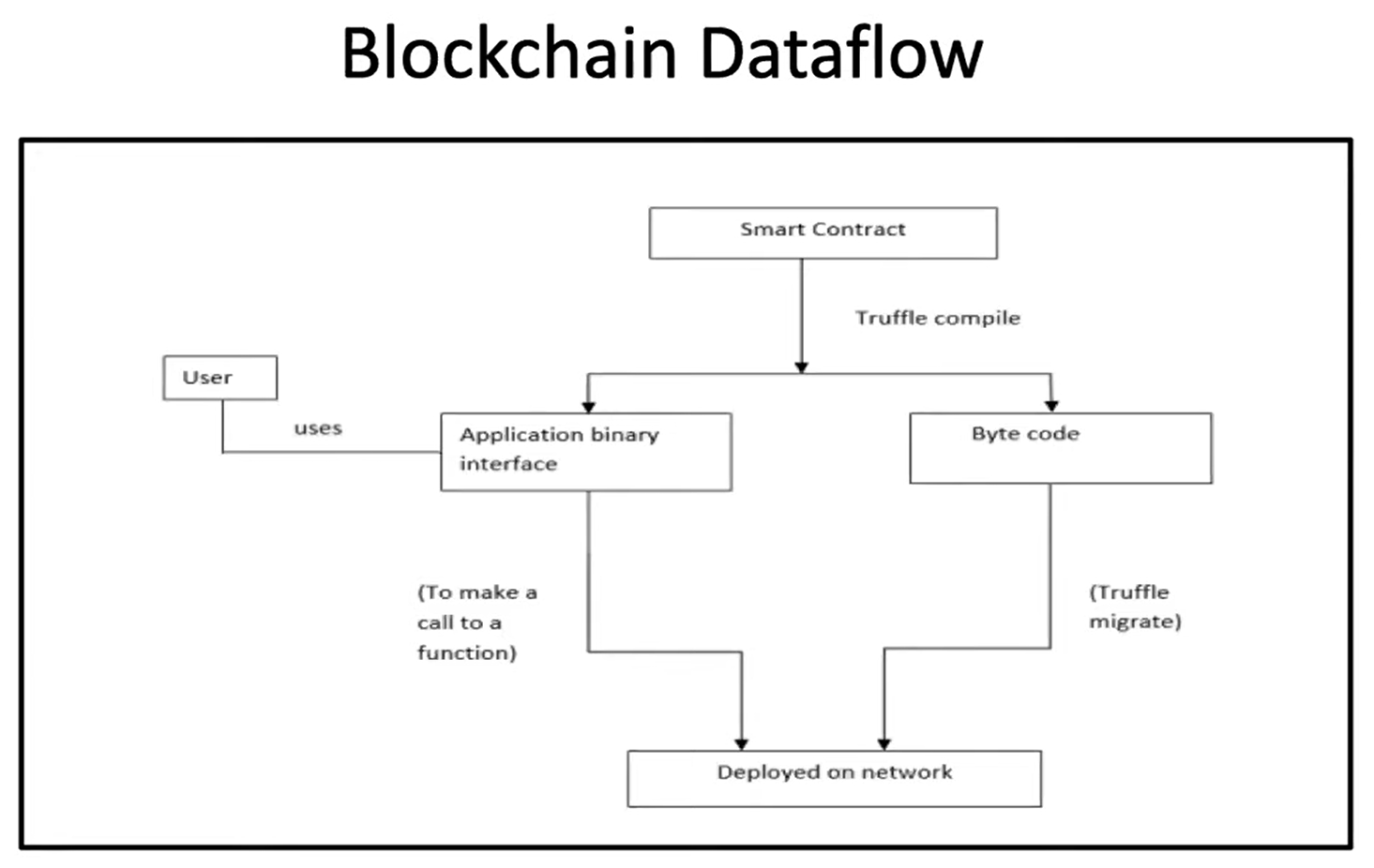
**Ganache:**

Since working with the main Ethereum network costs actual money for transactions, we are using a local RPC “Ganache”. Ganache is a rapid Ethereum and distributed application development. It can be used across the entire development cycle, enabling us to develop, deploy, and test out dApps in a safe and deterministic environment.

**Truffle:**

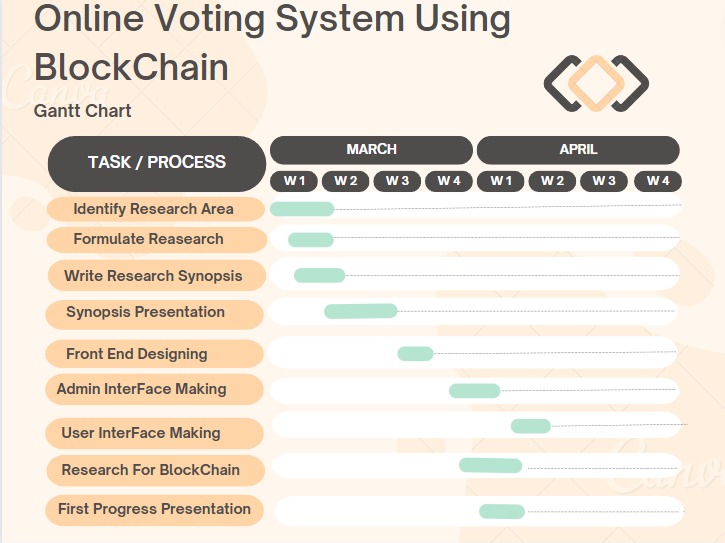
To interact with our compiled smart contract in a hassle-free manner we use Truffle suite. Truffle is the most popular framework for Ethereum which makes lots of work easier.

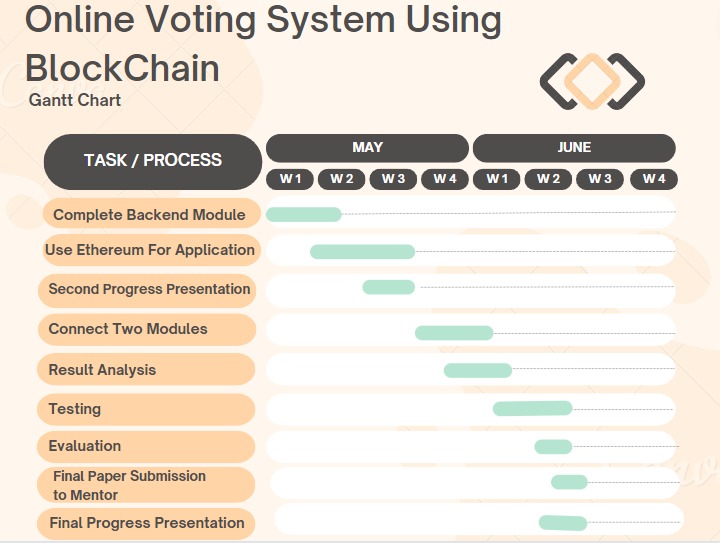
**Proposed Model:**



We will have a smart contract and then the truffle compiler will convert it into two components: Application binary interface and byte code. Byte code is the actual machine code that will be deployed over the network. Application binary interface is the interface which we will use to make a function call to the deployed code on the network.

**Gantt Chart**

****

****

**References**

[1] Madise, Ü. Madise and T. Martens, “E-voting in Estonia 2005. The first practice of country-wide

binding Internet voting in the world.”,Electronic voting, 2nd International Workshop, Bregenz,

Austria,(2006) August 2-4.

[2] J. Gerlach and U. Grasser, “Three Case Studies from Switzerland: E-voting”, Berkman Center

Research Publication, (2009).

[3] I. S. G. Stenerud and C. Bull, “When reality comes knocking Norwegian experiences with verifiable

electronic voting”, Electronic Voting. Vol. 205. (2012), pp. 21-33.

[4] C. Meter and A. Schneider and M. Mauve, “Tor is not enough: Coercion in Remote Electronic

Voting Systems. arXiv preprint. (2017).

[5] D. L. Chaum, “Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms”,

Communication of the ACM. Vol. 24(2). (1981), pp. 84-90.

[6] T. ElGamal, “A public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms”,

IEEE Trans. Info. Theory. Vol. 31. (1985), pp. 469-472.

[7] S. Ibrahim and M. Kamat and M. Salleh and S. R. A. Aziz, “Secure E-Voting with Blind Signature”,

Proceeding of the 4th National Conference of Communication Technology, Johor, Malaysia, (2003)

January 14-15.

[8] J. Jan and Y. Chen and Y. Lin, “The Design of Protocol for e-Voting on the Internet”, Proceedings

IEEE 35th Annual 2001 International Carnahan Conference on Security Technology, London,

England, (2001) October 16-19.

[9] D. L. Dill and A.D. Rubin, “E-Voting Security”, Security and Privacy Magazine, Vol. 2(1). (2004),

pp. 22-23.

[10] D. Evans and N. Paul, “Election Security: Perception and Reality”. IEEE Privacy Magazine, vol.

2(1). (2004), pp. 2-9.

International Journal of Network Security & Its Applications (IJNSA) Vol.9, No.3, May 2017

9

[11] Trueb Baltic, “Estonian Electronic ID – Card Application Specification Prerequisites to the Smart

Card Differentiation to previous Version of EstEID Card Application.” http://www.id.ee/public/TBSPEC-EstEID-Chip-App-v3\_5-20140327.pdf

[12] Cybernetica. “Internet Voting Solution.” https://cyber.ee/uploads/2013/03/cyber\_ivoting\_NEW2\_A4

\_web.pdf.

[13] D. Springall, T. Finkenauer, Z. Durumeric, J. Kitcat, H. Hursti, M. MacAlpine, and J. A. Halderman,

“Security Analysis of the Estonian Internet Voting System.” Proceedings of the 2014 ACM SIGSAC

Conference on Computer and Communications Security. (2014), pp. 703-715.

[14] Ministry of Local Government and Modernisation. “Internet Voting Pilot to be Discontinued.”

https://www.regjeringen.no/en/aktuelt/Internet-voting-pilot-to-be-discontinued/id764300/

[15] J. A. Halderman, and V. Teague, “The New South Wales iVote System: Security Failures and

Verifications Flaws in a Live Online Election.” International Conference on E-Voting and Identity.

(2015), pp. 35-53.

[16] S. Wolchok, E. Wustrow, D. Isabel, J. A. Halderman, “Attacking the Washington, DC Internet

Voting System.” International Conference on Financial Cryptography and Data Security (2012), pp.

114-128.

[17] National Institute of Standards and Technology, “Federal Information Processing Standards

Publication”, (2012).

[18] S. Nakamoto, “A Peer-to-Peer Electronic Cash System”, (2008).

[19] F. Reid and M. Harrigan, “An Analysis of Anonymity in the Bitcoin System”, Security and Privacy

in Social Networks. (2013), pp. 1-27.

[20] S. Raval, “Decentralized Applications: Harnessing Bitcoin’s Blockchain Technology.” O’Reilly

Media, Inc. Sebastopol, California (2016).