Decentralized Voting System Using Blockchain

A SYNOPSIS

Submitted by

Yash Gupta (2019BTCS088)

Rishabh Verma (2019BTCS063)

Goutam Choudhary (2019BTCS032)

Bachelor of Technology

IN

Computer Science & Information Technology

TO

School of Computer Science and Information Technology

SYMBIOSIS UNIVERSITY OF APPLIED SCIENCES, INDORE

Under the guidance of

Dr. Indrajeet Kumar

Jan 2023

CONTENTS

Chapter 1

PROBLEM DEFINITION

1.1 Title of Project

Decentralized Voting System Using Blockchain.

1.2 Definition of Project

In a democratic country like India (which is the largest democracy in the world), Voting plays a major role in the selection of government officials as well as showing our opinion how the governing body to be formed. Time to time, researches are conducted in order to tackle the difficulties in the centralized voting system to make it more anonymous, reliable and secure while preventing any kind of frauding. Even though the use of e-voting through the electronic medium, we have to face well-known problems of maintenance and fraud. Currently, various researches are conducting in-order to make secure and reliable voting system while tackling issues of anonymity and security. Through Decentralized System, focus is drifting towards making Voting Process simple, secure and anonymity in the hand of the public. This paper presents a literature review on the papers and the techniques used to tackle voting challenges.

1.3 Economical Problems

1. **Transport_Cost** = Rental_Cost_of_Private_Vehicle.
2. **Resources _Cost** = Vehicle Cost + Diesel/Petrol Cost.
3. **Manpower _Cost** = All **Public + Private** Servants, Food Cost.
4. **Residence _Cost** = Men + Women
5. **Embedded_Cost** = Cost _of(EVMs **Rs. 17,000 per unit** , VVPATs Machines), Handling all documentscost of papers.

1.4 Managerial Problems

- Managing of workforce (for managing **900 million** people =¿ **1,035,918 polling** stations)
- Managing of EVMs **3.96 million** & VVPATs **1.74 million**

- Managing huge no. of polling stations 1,035,918
- Managing of Security forces (CRPFs, CISFs, State Police & other departments)

1.5 Expenditure Statistics of EVMs

Characterstics	EVM Details
Launched	1982, Kerala
Cost Per Unit	17,000
Max. No of Votes(in M3 EVMs)	2000 votes
Max. No. of Candidates(in M3 EVMs)	384
Min. No of EVMs used in 2019 Elections	39,60,000
Min. Expenditure used in 2019 Elections(in INR)	₹ 67,32,00,00,000.00

Chapter 2

OBJECTIVE

2.1 Objective of Project

The objective of project is to design a **Secure De-Centralized** E-Voting System implemented on the **public blockchain** using **Ethereum** as a framework & it's capable to provide Anonymity, Integrity, Security, Privacy, Fairness, Verifiability, Mobility.

1. Telematic Voting is Secure & has Legal validity.
    - **Invalidity of Decision**
    - **Illegal Activities**
2. Electronic Voting reduces the **mundane human effort** of preparing a Poll.
    - Huge Census demands huge resources.
3. Online Voting optimizes the voter experience.
    - **Vote from Anywhere, Anyplace, Anydevice**(min. Internet connection)
4. Digital Voting **saves** the **environment,** which results in good health, cost benefits.
    - Saves huge cost of batteries used in EVMs.
5. Huge Savings in finance.(Shown in earlier slide)
    - Cost of EVMs(**Rs. 17,000 per unit** , VVPATs Machines) [Figure **??**]

Chapter 3

SCOPE

3.1 Scope of Project

The scope of the final project is to research the possibility to design a decentralized e-voting system and implement a prototype as a proof of concept that assures transparency, privacy, correctness, and integrity.

3.2 Future Scope of Project

- **Security Trust Enhancement**

  In Voting Protocol

  Using Best Practices for Creating Smart Contracts

  Regression of Auditing Test must be performed

- Integrating **5G-SMS** Services

- Privacy of Data Transmission

  Data Confidentiality & Neutrality

  Dishonest of Auditiong from the Organizer & Inspectors

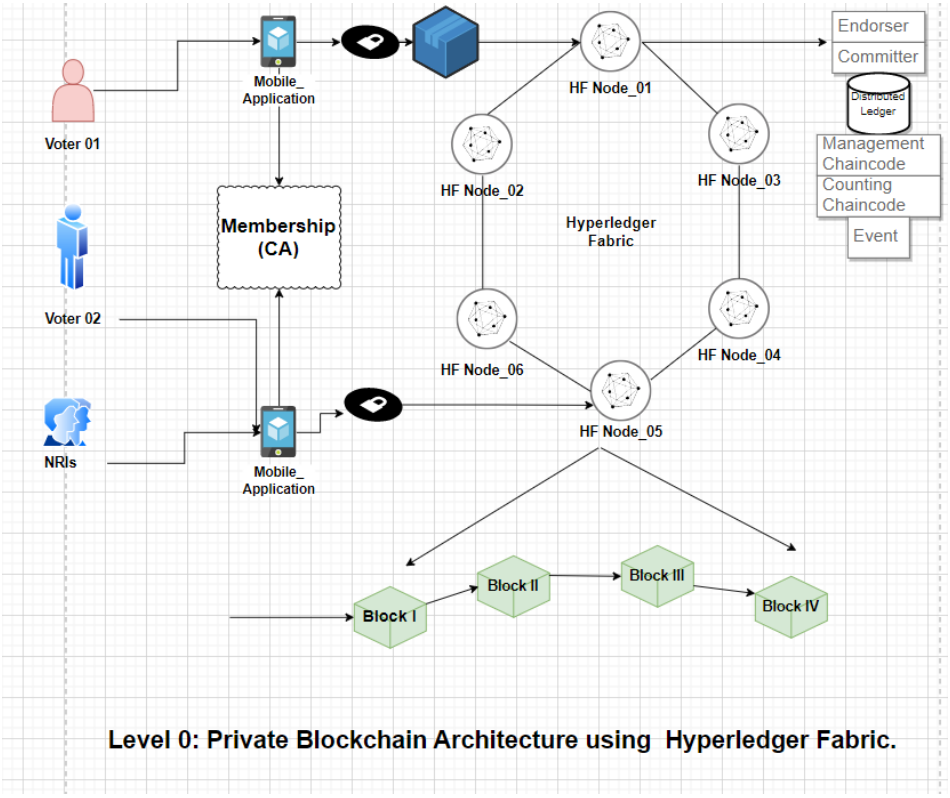

Figure 3.1: Scope

Chapter 4

LITERATURE REVIEW

In this section, we introduce study done by few researchers. This article gives an overall view of Blockchain technology and its potential to contribute to the development of the future by proposing several directions for further research. This paper proposed the effects of industrial revolution 4.0 to the society were robots will replace humans completely in the work force. This paper explains the basic operation of blockchain technology that is peer-to-peer decentralized ledger which provides a method to record and distribute information publicly on peer-t-peer systems of computers through crypto protocol.

This paper also describes the advantages of blockchain such as it is arranged rationally that allows user to execute quick insurance requests that can be valuate immediately using AI and Blockchain decentralization helps it become less likely to be attacked. It gives role of blockchain in technological revolution 4.0 and also within the society. Blockchain can help in faster insurance and payments, it can make travelling easier by helping the travel insurance agencies to automate payment which saves a great amount of time, helps in protecting corporate identities, in banking sectors, internet security, supply chain management, helps government to alleviate bureaucracy, increase safety and transparency in government activities and many more.

This paper investigates Bitcoin cryptocurrency application and blockchain technology that enables existence of digital currency. This paper also highlights requirements and benefits related to security, database and network. This paper gives the understanding of Bitcoin as it is a peer-to-peer electronic cash system. The word bitcoin denotes three different objects: blockchain platform, digital currency and protocol that runs over this platform to define how transactions are moved. This paper describes the characteristics of blockchain where the distributed ledger is structured into two main network types: permission less network such as bitcoin where anyone can join the network without previous permission.

S.No.	Authors	Paper Title	Journal	Conclusion	Methodology Used
1	K. Dhinakaran, P. M. Britto Hrudaya Raj, and D. Vinod	**A Secure Electronic Voting System Using Blockchain Technology**	Information Management and Machine Intelligence. Lecture Notes in Networks and Systems, vol 166. Springer. (2023) doi: 10.1007/978-981-15-9689-6_34	In this paper, we concluded that 1. Electoral Voting System is the best way to cast your vote by saving **huge resources**; 2. We can ensure that the voting process is **more secure**. 3. For **reliability & zero fault tolerance** of the system, as the **Nodes grew**, the time for the system was also raised in simulation to make it work. 4. Recording the voting result using hash values makes the system more secure.	They proposed a blockchain structure in which a Node consists of: 1. Voter_ID {4 bytes} 2. Timestamp {4 bytes} 3. Signature {32 bytes} 4. Hash of previous block data {20 bytes} 5. Data Structure used: **Merkel Tree {20 bytes}** 6. With respect to **System Design** the system continued sequence even **if {(initial node)** ***lower*** **(next node)}:** **counter time++** 7. Then dimensions needed for the **Recording Process ∝ Number Nodes.**
2	A. M. Al-madani, A. T. Gaikwad, V. Mahale and Z. A. T. Ahmed,	**De-Centralized E-voting system based on Smart Contract by using Blockchain Technology**	International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing. (2022) doi: 10.1109/ICSIDEMPC49020.2020.9299581.	In this paper, 1. Developed a Voting Application in a Decentralized Method with a Smart Contract based on **Ethereum Blockchain** technology as a network & decentralized database all in one for storage voter accounts, votes and candidate details. 2. **Voter's Point of View**: **1 VOTE == 1 PERSON == 0% DUPLICACY** 3. Problems with **Centralized Voting System (CVS)** a. To overcome limitations b. Security Issues using Blockchain technology.	They proposed 4-Tier Architecture Design: - **Level 1: Authentication Web Page** 1. Created a webpage which contains Authentication {using **Aadhar Card**} **Level 2: Authentication with DB** 2. Used Mongo DB as Government Identity Verification Service. **Level 3: Smart Contract Creation** 3. Created **Smart Contract includes {District, List Candidates}** **Level 4: POA Network Deployment** 4. Deploy a **POA Network**. It has **3 sub-modules:** - **a. Government** {Boot Node, Node1, Node2} **b. Origin** {Boot Node, Node1, Node2} **c. HR** {Boot Node, Node1, Node2}
3	F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa and G. Hjálmtýsson,	**Blockchain-Based E-Voting System**	IEEE 11th International Conference on Cloud Computing. (2022) pp. 983-986, doi: 10.1109/CLOUD.2018.00151.	In this paper, 1. We analysed the Traditional Voting System. 2. Benefits of Implementing a blockchain-based E-Voting system using various blockchain-based tools 3. Found using a Case study of the Manual Voting Process. 4. Also studied about comparison between the traditional voting system in use and the electronic voting system based on the blockchain.	They created **3-Tier Architecture** Design: - A. **Level 1:** End User (HOME PAGE), Cast a Vote B. **Level 2:** Candidate Management, Voter Management, Result, View Ledgers C. **Level 3:** Logout

Figure 4.1: Literature Review Table

Chapter 5

PROPOSED METHODOLOGY

Algorithmic Steps :

1. Voter need to enter his/her credentials in order to vote.
2. All data is then encrypted and stored as a transaction.
3. This transaction is then broadcasted to every node in network, which in turn is then verified.
4. Network approves transaction, it is stored in a block and added to chain.
5. Block is added into chain, it stays there forever and can't be updated.
6. Users can now see results and also trace back transaction if they want.

Framework : Used in our project are

- GitHub
- NPM, NodeJS
- Ethereum.js
- Gnache-Truffle
- MetaMask Account

Chapter 6

EXPECTED OUTCOMES

- All **Tier-I** & **Tier-II** cities can easily vote using this application.
- Application can be used from any device having (**Android 5.x+, WebGUI**)
- Improves Voter Engagement
- Using **SHA512** bits encryption as **CA**.
- Providing access to **NRIs**.
- Centralized Web Portal for event management.
  - Create Event
  - Voting Event
  - Deploy Smart Contract in **.sol**
- **Application Security Analysis**
  - **Voter's Privacy:** Provides full-proof anonymity.
  - Ballot Manipulation & Forgery is unimaginable to happen.
  - Network Attack Resistant
  - Ballot Collision
- **Authentication Facilities**
  - **Scalability Issue:** Layer I issues are solved as much as poosible.
  - Low Authentication Efficiency

  Storage Overload: Bitcoin's block size is limited to **1 MB**, but this small amount of data is enough to store over **2000 transactions**.

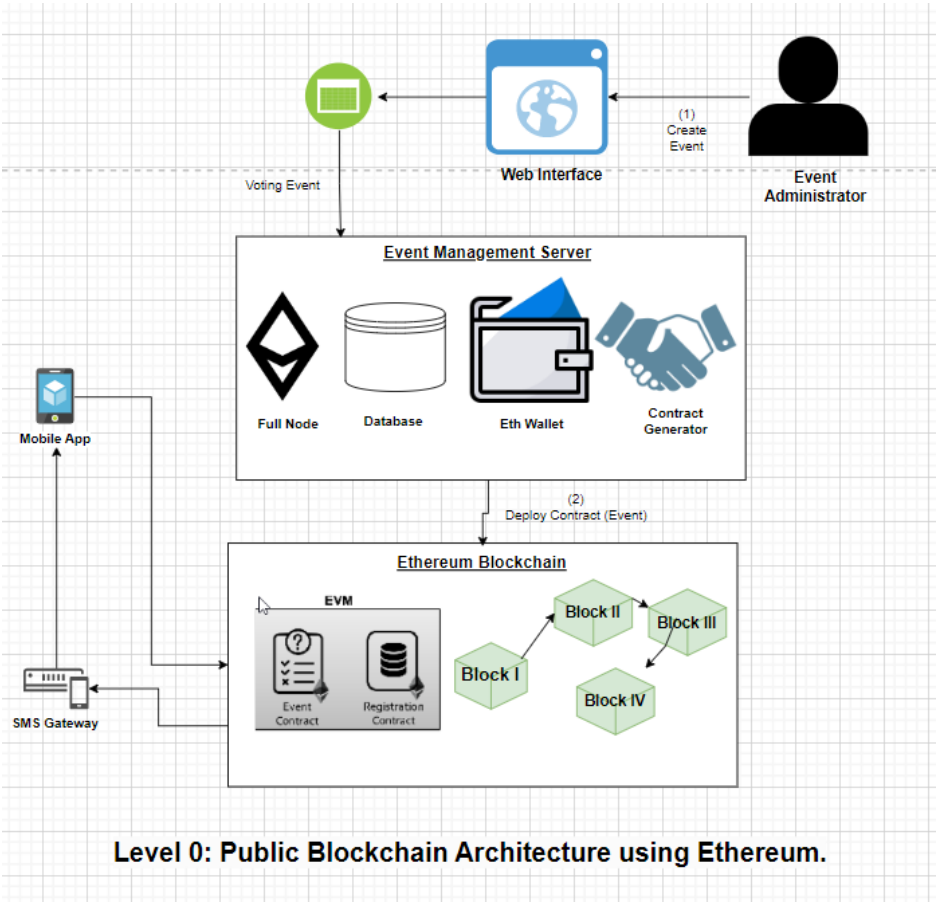

Figure 6.1: Architecture using Ethereum

Chapter 7

FACILITIES REQUIRED

7.1 Functional Requirements

1. **Software Requirements**

   OS: Ubuntu 20.04 LTS.

   IDE: Visual Studio Code.

   Developement Suite: Ganache-Truffle Suite.

   Database: MongoDB

2. **Hardware Requirements**

   Processor: Intel(R) Core(TM) i7-9750H CPU@2.60GHz

   HD: Minimum 15 GB of HDD.

   RAM: Minimum 12 GB of RAM.

Chapter 8

TIMELINE

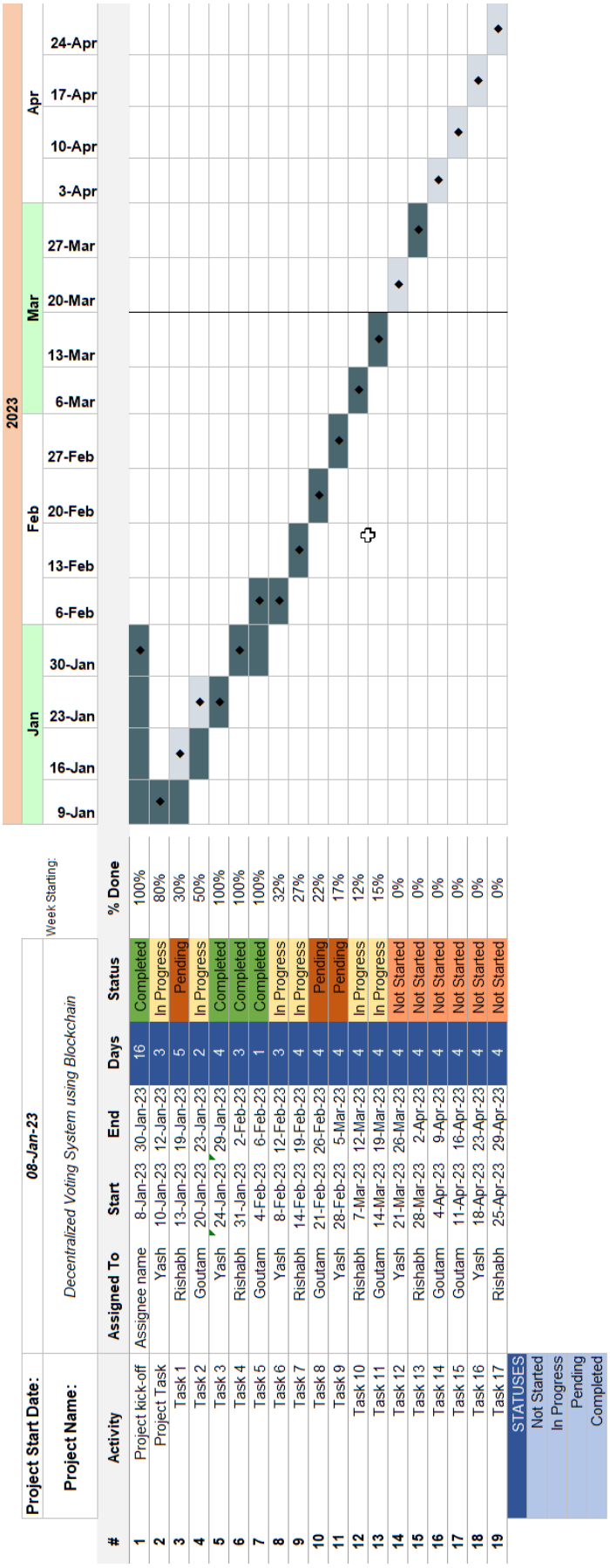

Figure 8.1: Timeline Gantt Chart

Chapter 9

TEAM

We are a team of **3** members.

1. **Yash Gupta (088)** Contributing as
   - Team Leader
   - **Backend Tech Stack**
     - Ganache-Truffle Suite,
     - Ethereum.js
     - **Database:** MongoDB
2. **Rishabh Verma (063)** Contributing in
   - **Building Front End**
     - React JS Library,
     - SCSS
   - **Documentation**
     - LaTeX
3. **Goutam Choudhary (032)** Contributing in
   - Documentation Printing
   - Project Resources Investor
   - Project SpotBoy

Bibliography

[1] Ben Adida and Ronald L Rivest. Scratch & vote: self-contained paper-based cryptographic voting. In *Proceedings of the 5th ACM workshop on Privacy in electronic society*, pages 29–40, 2006.

[2] Ali Mansour Al-madani and Ashok T Gaikwad. Iot data security via blockchain technology and service-centric networking. In *2020 International Conference on Inventive Computation Technologies (ICICT)*, pages 17–21. IEEE, 2020.

[3] Ali Mansour Al-Madani, Ashok T Gaikwad, Vivek Mahale, and Zeyad AT Ahmed. Decentralized e-voting system based on smart contract by using blockchain technology. In *2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC)*, pages 176–180. IEEE, 2020.

[4] Ahmed Ben Ayed. A conceptual secure blockchain-based electronic voting system. *International Journal of Network Security & Its Applications*, 9(3):01–09, 2017.

[5] Susan Bell, Josh Benaloh, Michael D. Byrne, Dana Debeauvoir, Bryce Eakin, Philip Kortum, Neal McBurnett, Olivier Pereira, Philip B. Stark, Dan S. Wallach, Gail Fisher, Julian Montoya, Michelle Parker, and Michael Winn. STAR-Vote: A secure, transparent, auditable, and reliable voting system. In *2013 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 13)*, Washington, D.C., August 2013. USENIX Association.

[6] Jens-Matthias Bohli, Jörn Müller-Quade, and Stefan Röhrich. Bingo voting: Secure and coercion-free voting using a trusted random number generator. In *E-Voting and Identity: First International Conference, VOTE-ID 2007, Bochum, Germany, October 4-5, 2007, Revised Selected Papers 1*, pages 111–124. Springer, 2007.

[7] Umut Can Çabuk, Eylul Adiguzel, and Enis Karaarslan. A survey on feasibility and suitability of blockchain techniques for the e-voting systems. *arXiv preprint arXiv:2002.07175*, 2020.

[8] R Aroul Canessane, N Srinivasan, Abinash Beuria, Ashwini Singh, and B Muthu Kumar. Decentralised applications using ethereum blockchain. In *2019 Fifth International Conference on Science Technology Engineering and Mathematics (ICONSTEM)*, volume 1, pages 75–79. IEEE, 2019.

[9] David Chaum. Secret-ballot receipts: True voter-verifiable elections. *IEEE security & privacy*, 2(1):38–47, 2004.

[10] David Chaum, Aleks Essex, Richard Carback, Jeremy Clark, Stefan Popoveniuc, Alan Sherman, and Poorvi Vora. Scantegrity: End-to-end voter-verifiable optical-scan voting. *IEEE Security & Privacy*, 6(3):40–46, 2008.

[11] David Chaum, Peter YA Ryan, and Steve Schneider. A practical voter-verifiable election scheme. In *Computer Security–ESORICS 2005: 10th European Symposium on Research in Computer Security, Milan, Italy, September 12-14, 2005. Proceedings 10*, pages 118–139. Springer, 2005.

[12] David L Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2):84–90, 1981.

[13] David L Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2):84–90, 1981.

[14] K Dhinakaran, PM Britto Hrudaya Raj, and D Vinod. A secure electronic voting system using blockchain technology. In *Proceedings of the Second International Conference on Information Management and Machine Intelligence: ICIMMI 2020*, pages 307–313. Springer, 2021.

[15] M Erdenebileg. e-voting anwendung auf ethereum plattform als smart contract. *Fachhochschule Campus Wien*, 2019.

[16] Rifa Hanifatunnisa and Budi Rahardjo. Blockchain based e-voting recording system design. In *2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)*, pages 1–6. IEEE, 2017.

[17] Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson, Mohammad Hamdaqa, and Gísli Hjálmtýsson. Blockchain-based e-voting system. In *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, pages 983–986, 2018.

[18] Dalia Khader, Ben Smyth, Peter Ryan, and Feng Hao. A fair and robust voting system by broadcast. *Lecture Notes in Informatics*, pages 285–299, 2012.

[19] Dalia Khader, Ben Smyth, Peter Ryan, and Feng Hao. A fair and robust voting system by broadcast. *Lecture Notes in Informatics*, pages 285–299, 2012.

[20] Christian Killer, Bruno Rodrigues, Raphael Matile, Eder Scheid, and Burkhard Stiller. Design and implementation of cast-as-intended verifiability for a blockchain-based voting system. In *Proceedings of the 35th Annual ACM Symposium on Applied Computing*, pages 286–293, 2020.

[21] Basit Shahzad and Jon Crowcroft. Trustworthy electronic voting using adjusted blockchain technology. *IEEE Access*, 7:24477–24488, 2019.

[22] Shreyas Tandon, Niharika Singh, Shivani Porwal, Ashish Kumar Maurya, et al. E-matdaan: A blockchain based decentralized e-voting system. In *2022 IEEE Students Conference on Engineering and Systems (SCES)*, pages 1–6. IEEE, 2022.

[23] Mohammed Tawfik, Ali Almadani, and Alhasan A Alharbi. A review: the risks and weakness security on the iot. *IOSR Journal of Computer Engineering (IOSR-JCE)*, 2017.

[24] Deshan Wattegama, Pasindu S Silva, Chamika R Jayathilake, Kalana Elapatha, Kavinga Abeywardena, and N Kuruwitaarachchi. "isay": Blockchain-based intelligent polling system for legislative assistance. *International Journal of Advanced Computer Science and Applications*, 12(1), 2021.

[25] Jingyu Zhang, Siqi Zhong, Tian Wang, Han-Chieh Chao, and Jin Wang. Blockchain-based systems and applications: a survey. *Journal of Internet Technology*, 21(1):1–14, 2020.

[26] Wenbin Zhang, Yuan Yuan, Yanyan Hu, Shaohua Huang, Shengjiao Cao, Anuj Chopra, and Sheng Huang. A privacy-preserving voting protocol on blockchain. In *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, pages 401–408. IEEE, 2018.

[27] Yuxian Zhang, Yi Li, Li Fang, Ping Chen, and Xinghua Dong. Privacy-protected electronic voting system based on blockchin and trusted execution environment. In *2019 IEEE 5th International Conference on Computer and Communications (ICCC)*, pages 1252–1257. IEEE, 2019.