**BLOCKCHAIN BASED VOTING SYSTEM**

**SEMINAR REPORT**

***Submitted by***

**Siddham Singh Rao [RA2011027020105]**

**V Phanindra Varma [RA2011027020117]**

**Nishant Shandilya [RA2011027020112]**

Under the guidance of

**Mr.N.Sathish,AP/CSE**

**Mr.Thiruneelakandan.A,AP/CSE**

***In partial fulfillment for the award of the degree***

***of***

**BACHELOR OF TECHNOLOGY**

***in***

**COMPUTER SCIENCE AND ENGINEERING**

***of***

**FACULTY OF ENGINEERING AND TECHNOLOGY**

****

**SRM INSTITUTE OF SCIENCE AND TECHNOLOGY**

**RAMAPURAM CAMPUS, CHENNAI-600089**

**APRIL-2023**

# SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

(Deemed to be University Under Section 3 of UGC Act, 1956)

# BONAFIDE CERTIFICATE

Certified that the Seminar-II report titled “**BLOCKCHAIN BASED VOTING SYSTEM”** is the bonafide work of “**SIDDHAM SINGH RAO[RA2011027020105], V. PHANINDRA VARMA[RA2011027020117] AND NISHANT SHANDILYA[RA20110270112]**” submitted for the course 18CSP105L/SEMINAR – II. This report is a record of successful completion of the specified course evaluated based on literature reviews and the supervisor. No part of the Seminar Report has been submitted for any degree, diploma, title, or recognition before.

**SUPERVISOR SIGNATURE HOD SIGNATURE**

Mr.N.Sathish, Dr.K.Raja

Assistant Professor Head of Department

Dept. of Computer Science & Dept. of Computer Science & Engineering Engineering

SRM Ramapuram SRM Ramapuram

Submitted for the Viva Voce Examination held on ………………… at SRM Institute of Science and Technology, Ramapuram Campus, Chennai-600089.

**EXAMINER 1 EXAMINER 2**

**ABSTRACT**

Electronic voting systems have replaced paper-based systems, but even now, people doubt the voting system’s ability to secure the data and defend against any attacks. The blockchain-based system can ensure transparent and publicly verifiable elections in the country. If implemented successfully, voting can be done using a mobile application that is attached to a blockchain system. This project helps you to conduct voting at the national and organizational levels. You must ascertain certain things to let this project work. Firstly, the users’ details must be hidden in your application because of privacy issues. You must use an Ethereum address that works as the user’s identifier. Secondly, an individual must be able to submit only one vote, and only when they are eligible. The voting process must be transparent and all voting rules must be followed. No mistakes or fraud occurrences are accepted in such types of projects on blockchain. Blockchain-based systems can tackle the corruption observed in the voting process. This is because they provide a more transparent and straightforward platform for casting a vote. Mobile voting applications are also allowed to cast a vote. The blockchain is said to be an emerging, decentralized, and distributed technology that promises to enhance different aspects of many industries. Expanding e-voting into blockchain technology could be the solution to eliminate the present concerns in e-voting system There is no doubt that the ever-changing concept of the blockchain, which is the backbone of the famous cryptocurrency Bitcoin has triggered the start of a new era in the Internet and the online services. While most people focus only on bitcoin and other cryptocurrencies

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| CHAPTER  No. | TITLE | PAGE No. |
|  | ABSTRACT | iii |
|  | LIST OF FIGURES | v |
|  | LIST OF TABLES | vi |
| 1 | INTRODUCTION OF THE PROJECT | 1 |
| 2 | PROBLEM STATEMENT | 2 |
| 3 | SCOPE & OBJECTIVE | 3 |
| 4 | EXISTING SYSTEM | 4 |
| 5 | LITERATURE SURVEY | 5 |
| 6 | ARCHITECTURE | 10 |
| 7 | PROPOSED WORK & ALGORITHM | 11 |
| 8 | FUTURE SCOPE | 12 |
| 9 | DISADVANTAGES | 14 |
| 10 | CONCLUSION/REFRENCES | 15 |

**LIST OF FIGURES**

|  |  |  |
| --- | --- | --- |
| **Sl. No.** | **Name** | **Page No.** |
| 1 | Architecture | 9 |
| 2 | Global Market | 14 |

**LIST OF TABLES**

|  |  |  |
| --- | --- | --- |
| **Sl. No.** | **Name** | **Page No.** |
| 1 | Literature Survey | 6 |

**1.INTRODUCTION**

Elections are a fundamental pillar of a democratic system enabling the general public to express their views in the form of a vote. Due to their significance to our society, the election process should be transparent and reliable so as to ensure participants of its credibility. Within this context, the approach to voting has been an ever evolving domain. This evolution is primarily driven by the efforts to make the system secure, verifiable, and transparent. In view of its significance, continuous efforts have been made to improve overall efficiency and resilience of the voting system. Electronic voting or e-voting has a profound role in this. Since its first use as punched-card ballots in the 1960's, e-voting systems have achieved remarkable progress with its adoption using the internet technologies. However, e voting systems must adhere to specific benchmark parameters to facilitate its widespread adoption. These parameters include anonymity of the voter, integrity of the vote and non-repudiation among others. Blockchain is one of the emerging technologies with strong cryptographic foundations enabling applications to leverage these abilities to achieve resilient security solutions. A Blockchain resembles a data structure which maintains and shares all the transactions being executed through its genesis. It is primarily a distributed decentralized database that maintains a complete list of constantly germinating and growing data records secured from unauthorized manipulating, tampering and revision. Blockchain CORE Metadata, citation and similar papers at core.ac.uk Provided by UWL Repository allows every user to connect to the network, send new transactions to it, verify transactions and create new blocks.

Each block is assigned a cryptographic hash (which may also be treated as a fingerprint of the block) that remains valid as long as the data in the block is not altered. If any changes are made in the block, the cryptographic hash would change immediately indicating the change in the data which may be due to a malicious activity. Therefore, due to its strong foundations in cryptography, blockchain has been increasingly used to mitigate against unauthorized transactions across various domains.

Bitcoin remains the most distinguished application of blockchain however researchers are keen to explore the use of blockchain technology to facilitate applications across different domains leveraging benefits such as non-repudiation, integrity and anonymity.

In this paper, we explore the use of blockchain to facilitate e-voting applications with the ability to assure voter anonymity, vote integrity and end-to verification. We believe e-voting can leverage fundamental blockchain features such as self-cryptographic validation structure among transactions (through hashes) and public availability of distributed ledger of records.

The blockchain technology can play a key role in the domain of electronic voting due to the inherent nature of preserving anonymity, maintaining decentralized and publicly distributed ledger of transactions across all the nodes. This makes blockchain technology very efficient to deal with the threat of utilizing a voting token more than once and the attempt to influence the transparency of the result. The focus of our research is to investigate the key issues such as voter anonymity, vote confidentiality and end-to-end verification. These challenges form the foundation of an efficient voting system preserving the integrity of the voting process.

In this paper, we present our efforts to explore the use of the blockchain technology to seek solutions to these challenges. Our system is based on the Prêt à Voter approach and uses an open source blockchain platform, Multichain as the underlying technology to develop our system. In order to protect the anonymity and integrity of a vote, the system generates strong cryptographic hash for each vote transaction based on information specific to a voter. This hash is also communicated to the voter using encrypted channels to facilitate verification.

Extensive research has been done on electronic voting systems that enable voters to vote at their convenience using a mobile phone, computer, or any other electronic device. Still, none of these technologies have been incorporated on a larger scale due to inherent security threats/concerns that these systems might pose to the integrity of the voting process.

In this paper, we discuss the electronic voting system using blockchain, a secure and robust system that ensures anonymity of the voter, transparency, and robust functioning. Blockchain- The blockchain is a digital platform for digital assets.

It consists of a continuously growing list of records known as blocks that are linked and secured using cryptography. Major usage of Blockchain has been in all cryptocurrency transactions, mainly Bitcoin. However, they are increasingly being used in several other applications because of their inherent resistance to modification to the transaction/block/whole distributed ledger.

Blockchain technology offers a decentralized node for online voting or electronic voting. Recently distributed ledger technologies such as blockchain were used to produce electronic voting systems mainly because of their end-to-end verification advantages.

Blockchain is an appealing alternative to conventional electronic voting systems with features such as decentralization, non-repudiation, and security protection. It is used to hold both boardrooms and public voting.

**PROBLEM STATEMENT**

Whether talking about traditional paper-based voting, voting via digital voting machines, or an online voting system, several conditions need to be satisfied:

* Eligibility: Only legitimate voters should be able to take part in voting;
* Reusability: Each voter can vote only once;
* Privacy: No one except the voter can obtain information about the voter’s choice;
* Fairness: No one can obtain intermediate voting results;
* Soundness: Invalid ballots should be detected and not taken into account during tallying;
* Completeness: All valid ballots should be tallied correctly.

Below is a brief overview of the solutions for satisfying these properties in online voting systems.

#### 4.1. Eligibility

The solution to the issue of eligibility is rather apparent. To take part in online voting, voters need to identify themselves using a recognized identification system. The identifiers of all legitimate voters need to be added to the list of participants. But there are threats: Firstly, all modifications made to the participation list need to be checked so that no illegitimate voters can be added, and secondly, the identification system should be both trusted and secure so that a voter’s account cannot be stolen or used by an intruder. Building such an identification system is a complex task. However, because this sort of system is necessary for a wide range of other contexts, especially related to digital government services, researchers believe it is best to use an existing identification system, and the question of creating one is beyond the scope of work.

#### 4.2. Un-reusability.

At first glance, implementing un-reusability may seem straightforward—when a voter casts their vote, all that needs to be done is to place a mark in the participation list and not allow them to vote a second time. But privacy needs to be taken into consideration; thus, providing both un-reusability and voter anonymity is tricky. Moreover, it may be necessary to allow the voter to re-vote, making the task even more complex. A brief overview of un-reusability techniques will be provided below in conjunction with the outline on implementing privacy.

#### 4.3. Privacy

#### Privacy in the context of online voting means that no one except the voter knows how a participant has voted. Achieving this property mainly relies on one (or more) of the following techniques: blind signatures, homomorphic encryption, and mix-networks. Blind signature is a method of signing data when the signer does not know what they are signing. It is achieved by using a blinding function so that blinding and signing functions are commutative–Blind (Sign(message)) = Sign(Blind(message)). The requester blinds (applies blinding function to) their message and sends it for signing. After obtaining a signature for a blinded message, they use their knowledge of blinding parameters to derive a signature for an unblinded message. Blind signatures mathematically prevent anyone except the requester from linking a blinded message and a corresponding signature pair with an unblinded one.

#### The voting scheme proposed by Fujioka, Okamoto, and Otha in 1992 uses a blind signature: An eligible voter stores his ballot and sends it to the validator. The validator verifies that the voter is allowed to participate, signs the blinded ballot, and returns it to the voter. The voter then derives a signature for the unblinded vote and sends it to the tallier, and the tallier verifies the validator’s signature before accepting the ballot.

#### Many online voting protocols have evolved from this scheme, improving usability (in the original method, the voter had to wait till the end of the election and send a ballot decryption key), allowing re-voting, or implementing coercion resistance. This information logically corresponds to the receiving of a ballot by the voter, so it should be verified that only eligible voters receive signatures from the signer. It should also be verifiable that accounts of voters who are permitted to vote but have not taken part in voting are not utilized by an intruder. To truly break the link between voter and ballot, the ballot and the signature need to be sent through an anonymous channel.

#### Homomorphic encryption is a form of encryption that allows mathematical operations to be performed on encrypted data without decryption, for example, the addition

#### Enc(a) + Enc(b) = Enc (a + b); In the context of online voting, additive homomorphic encryption allows us to calculate the sum of all the voters’ choices before decryption.

#### It is worth mentioning here that multiplicative homomorphic encryption can generally be used as an additive. For example, if we have choices x and y and multiplicative homomorphic encryption, we can select a value g and encrypt exponentiation: Enc(gx) × Enc(gy) = Enc (g (x + y)).

#### Homomorphic encryption can be used to obtain various properties necessary in an online voting system; Using homomorphic encryption for privacy implies that decryption is performed by several authorities so that no one can obtain the decryption key; In contrast to the blind signature scheme, no anonymous channel between voters and the system is needed. In a decryption mix network, each mixing server has its key, and the voter encrypts their choice like an onion so that each server will unwrap its layer of decryption.

#### 4.4. Fairness

Fairness in terms of no one obtaining intermediate results is achieved straightforwardly: Voters encrypt their choices before sending, and those choices are decrypted at the end of the voting process. The critical thing to remember here is that if someone owns a decryption key with access to encrypted decisions, they can obtain intermediate results. This problem is solved by distributing the key among several keyholders. A system where all the key holders are required for decryption is unreliable—if one of the key holders does not participate, decryption cannot be performed. Therefore, threshold schemes are used whereby a specific number of key holders are required to perform decryption. There are two main approaches for distributing the key: secret sharing, where a trusted dealer divides the generated key into parts and distributes them among key holders (e.g., Shamir’s Secret Sharing protocol); and distributed key generation, where no trusted dealer is needed, and all parties contribute to the calculation of the key (for example, Pedersen’s Distributed Key Generation protocol).

#### 4.5. Soundness and Completeness

On the face of it, the completeness and soundness properties seem relatively straightforward, but realizing them can be problematic depending on the protocol. Thus, we need to prove that the encrypted data meets the properties of a valid ballot without compromising any information that can help determine how the vote was cast. More specifically, range proofs demonstrate that a specific value belongs to a particular set in such cases.  
The properties described above are the bare minimum for any voting solution. A voting system needs to be fully verifiable to earn this trust, I. Everyone involved can ensure that the system complies with the stated properties. and universal, when everyone can prove that the system as a whole works precisely. This entails the inputs and outputs of the voting protocol stages being published and proof of correct execution. For example, mix-networks rely on proof of correct shuffling (a type of zero-knowledge proof), while proof of correct decryption is also used in mix-networks and threshold decryption. However, online voting makes extensive use of cryptography, and the more complex the cryptography, the more obscure it is for most system users. It may take a considerable amount of time to study the protocol and even more to identify any vulnerabilities or backdoors, and even if the entire system is carefully researched, there is no guarantee that the same code is used in real-time.  
Finally are problems associated with coercion and vote-buying. Online voting brings these problems to the next level: As ballots are cast remotely from an uncontrolled environment, coercers and vote buyers can operate on a large scale.

That is why one of the desired properties of an online voting system is coercion resistance. Both kinds of malefactors—coercers and vote buyers—demand proof of how a voter voted. That is why many types of coercion resistance voting schemes introduce the concept of receipt-freeness.  
The voter cannot create a receipt that proves how they voted. The approaches to implementing receipt-freeness generally rely on a trusted party—either a system or device that hides the unique parameters used to form a ballot from the voter, so the voter cannot prove that a particular ballot belongs to them. The reverse side of this approach is that if a voter claims that their vote is recorded or tallied incorrectly, they simply cannot prove it due to a lack of evidence.  
An overview of technologies used to meet the necessary properties of online voting systems and analysis deliberately considered the properties separately. For example, as noted for the blind signature, there is a risk that non-eligible voters will vote, receipt-freeness contradicts verifiability, a more complex protocol can dramatically reduce usability, etc.

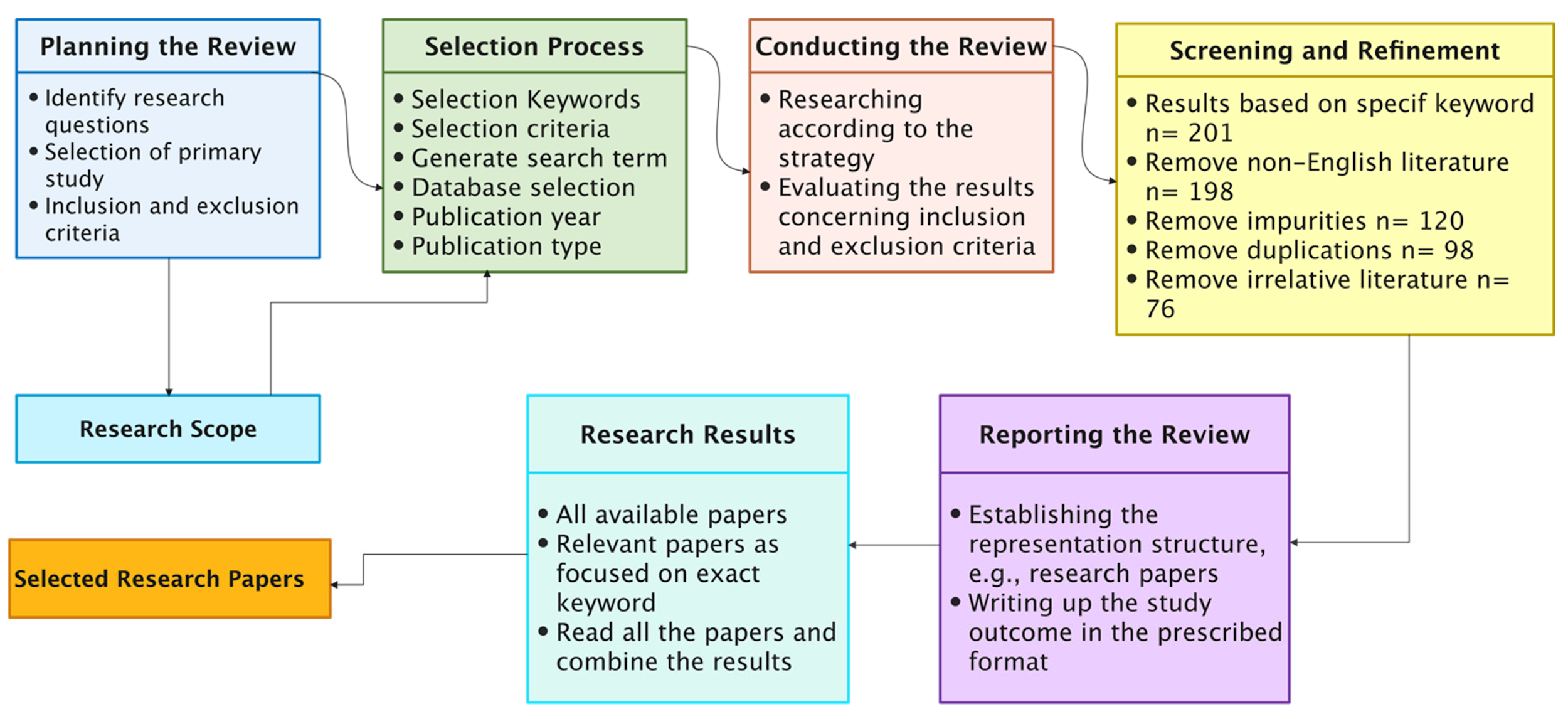
Furthermore, the fundamental principles of developing the solution, but many additional aspects must be considered in a real-world system like security and reliability of the communication protocols, system deployment procedure, access to system components. At present, no protocol satisfies all the desired properties and, therefore, no 100% truly robust online voting system exists. Traditional voting systems have several limitations, including concerns about security, transparency, and tampering. Additionally, the manual process of conducting elections can be time-consuming, labor-intensive, and costly. These limitations make it difficult to ensure that every vote is counted accurately and that the results of the election are reliable.

A blockchain-based voting system can help address these limitations by providing a secure, transparent, and tamper-proof platform for conducting elections.

However, the implementation of such a system requires addressing several challenges, including the scalability of the blockchain network, the management of user identities and authentication, and the integration of the system with existing voting infrastructure.

Therefore, the problem statement for a blockchain-based voting system is to design a secure, transparent, and scalable platform that can enable reliable and efficient voting while ensuring the privacy and anonymity of voters. The system must address the challenges related to scalability, identity management, and integration with existing voting infrastructure while meeting the legal and regulatory requirements of the jurisdiction in which it is implemented.

1. **SCOPE AND OBJECTIVE**



***Scope:***

The scope of a blockchain-based voting system is to provide a secure, transparent, and tamper-proof platform for conducting elections. The system should ensure the privacy and anonymity of voters while enabling reliable and efficient voting. The system must also address the challenges related to scalability, identity management, and integration with existing voting infrastructure.

***Objective:***

The objective of a blockchain-based voting system is to provide a reliable and efficient platform for conducting elections that can ensure the accuracy and integrity of the voting process. The system should enable secure and transparent voting while maintaining the privacy and anonymity of voters. The system must also comply with legal and regulatory requirements while providing a user-friendly and accessible interface for voters. The specific objectives of a blockchain-based voting system may include:

Ensuring the security and transparency of the voting process through the use of blockchain technology.

Providing a tamper-proof platform that can ensure the accuracy and integrity of the voting process.

Enabling efficient and reliable voting while maintaining the privacy and anonymity of voters.

Addressing the challenges related to scalability, identity management, and integration with existing voting infrastructure.

Complying with legal and regulatory requirements in the jurisdiction where the system is implemented.

Providing a user-friendly and accessible interface for voters to cast their votes.

Overall, the objective of a blockchain-based voting system is to provide a secure and reliable platform for conducting elections that can ensure the accuracy and integrity of the voting process while maintaining the privacy and anonymity of voters.



1. **EXISTING SYSTEM**

We surveyed existing methods of creating smart interactive mirror systems. Smart Mirrors are developed mostly for the purpose to display time, date, and weather forecast. Some also contain To-Do lists, traffic information, and notifications.

Later, it got upgraded with a music player and voice recognition. Thus, it can be personalized as per the requirements. Similar projects and products to our smart mirror project span a wide range of capabilities and applications.

There were much more projects than finished items. Some of the blame can be attributed to the fact that the smart home is still a developing market with production costs that keep the gadgets out of reach of the average user.

The fact that there were more projects demonstrates that there is a need to create a smart mirror that is more affordable and functional. Although a company's real products delivered on characteristics, they were either still in development or were already too expensive to be deemed a potential rival.

Several attempts have been made to add specific capabilities to mirrors, including both commercial and research-based approaches. However, due to the high amount of space required, such systems are typically infeasible to build. There are several existing blockchain-based voting systems that have been developed and implemented in various jurisdictions. Some of these systems include:

Voatz: Voatz is a mobile-based blockchain voting platform that has been used in various elections, including the 2018 West Virginia primary election. The platform uses blockchain technology to secure the voting process and ensure the anonymity of voters.

Horizon State: Horizon State is another blockchain-based voting platform that has been used in several elections, including the 2018 Fijian elections. The platform uses blockchain technology to ensure the security and transparency of the voting process.

Agora: Agora is a blockchain-based voting platform that was used in the Sierra Leone presidential elections in 2018. The platform uses blockchain technology to provide a transparent and secure voting process.

Follow My Vote: Follow My Vote is a blockchain-based voting platform that has been developed to enable secure and transparent voting. The platform uses blockchain technology to ensure that votes are recorded accurately and can be audited for accuracy.

Votem: Votem is a blockchain-based voting platform that has been used in various elections, including the Rock and Roll Hall of Fame Fan Vote. The platform uses blockchain technology to ensure the security and transparency of the voting process.

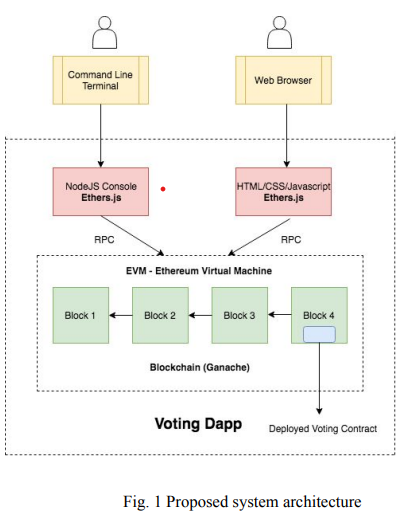
These existing blockchain-based voting systems demonstrate the potential of blockchain technology to provide a secure, transparent, and tamper-proof platform for conducting elections.

However, each system has its own unique features and capabilities, and the design and implementation of a blockchain-based voting system will depend on the specific requirements and constraints of the jurisdiction in which it is implemented.

1. **LITERATURE SURVEY**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sl. No.** | **Journal Name** | **Year of Publishing** | **Paper Title** | **Author** | **Description** |
| 1. | Decentralized E-voting portal using blockchain | 2019 | At Institute of Electrical and Electronics | Kriti Patidar | voters authentication can be done using  private key cryptography that has to be provided to  voters prior to the election process. |
| 2. | SUNY Genesso | 2018 | Advanced communications and computing analysis | Dr jain | Their intention does not seem to be to create a commercial smart mirror to sell to consumers, but rather they unveiled all the details on how to build one and made all the code publicly available at a GitHub repository. |
| 3. | Cosmos | 2012 | Masters India | Krisna Adiputra | suggests that there must be an public,  private key infrastructure, the electoral commission  (or another election manager) generates a key-pair for  the election (PE; SE) which later is used for encrypting  and decrypting messages of voters |
| 4. | Research GATE | 2017 | Multi-user smart mirror syst | Friðrik Þ.  Hjálmarsson | use 6 digit pin for voter  that voter can use for voter authentication, Each  individual is identified and authenticated by the  system by presenting an electronic ID from Auokenni  and the corresponding 6-digit PIN in the voting booth.  Without supervision |
| 5. | AADHAR Database system | 2016 | UIDAI | Roopak | unique solution of using  Aadhar database for voter information. The proposed  framework is an electronic voting system using virtual  ID which is provided by the UIDAI which is unique. |
| 6. | Research by Mrunal Patankhar | 2016 | Euthereum | Prof Mrunal Patankhar | Verifying voter identity from various angles is always  a challenge; some works have tried the biometric  solutions, such as facial comparison, fingerprint, Iris  and retinal scan but this can be biased and easily  gamed or stolen |
| 7. | Research by Jetir.org | 2015 | Protect voters | Trivedi | propose an  electronic voting system based on smart contracts to  protect voters’ privacy. The test results suggested that  the system can effectively reduce the cost of using  smart contracts to vote, and protect the privacy of  voters with practicability. |
| 8. | Studocu | 2016 | Ballot | C. S Narayan | propose a concrete construction of a  blockchain based self-tallying voting protocol in  decentralized IoT, and prove that it satisfies fairness,  dispute freeness, and maximal ballot secrecy. In this  system they formalize the system model of self-  tallying voting systems based on blockchain in  decentralized IoT |
| 9. | Published at IEEE Conference publication | 2016 | Smart Mirror for Smart Life | Published at IEEE Conference publication | Describes about the monitoring and controlling of home based devices with the mirror. |
| 10. | Research by Yannan Li,  Willy  Susilo | 2019 | Association of Computing Machinery | Yannan Li,  Willy  Susilo | Verifying voter identity from various angles is always  a challenge; some works have tried the biometric  solutions, such as facial comparison, fingerprint, Iris  and retinal scan but this can be biased and easily  gamed or stolen. However, we think that one way to  protect the stolen biometrics data is by using a  complex algorithms that are hard to crack. It can be  hashed using any hashing algorithm instead of saving  the biometric information as binary data and then  stored as a reference string |

1. **ARCHITECTURE**



1. **PROPOSED WORK**

For our architectural design we tried to create a system that does not entirely replace the current voting system but rather integrates itself within the current system which we are using today. We decided to do this because most people are familiarized with the current system and the introduction of a new system can create confusion as well as disinterest. System Architecture The system architecture is given in Figure 1. Each block is described in this Section. Fig. 1 Proposed system architecture the first step of our design is the registration process, verifying a voter is essential in establishing security within the system. Making sure that someone’s identity isn’t being misused for fraudulent purposes is important, especially when voting is considered because every vote matters. To allow users to register to vote our proposed service utilizes Recognition devices & valid identity card number to cross check whether the user is present in the database or not /whether he is eligible to vote or not. After that a unique hash address is given to voter using which he can cast a vote. Each hash is supplied with Ethers by which he can cast vote once. During the voting day the voter will visit the polling booth he/she will undergo a verification process and then using the address given to him he/she will cast a vote then he will be automatically logged out. The voters will also get live status of voting. 3.2 Requirement Analysis The implementation detail is given in this section. The entire system is divided into two sub-system a registration system & a voting system. Registration System: A voting registration System is developed using Html/CSS front-end and SQL back-end which contains the user's personal details already stored for e.g.: One can consider this as an Aadhar database. A biometric device would be used for validation purpose. If the user is a valid user, then he/she is handed a hash code /address which is used as a credential for login into the voting machine. Voting System: The voting system can be considered as a replacement for EVM. It is a decentralized app with a front-end in Bootstrap or Html and a Blockchain in back-end. The smart contract is written in solidity language. The candidate’s name with symbol of candidate is mentioned in smart-contract. A smart contract is the actual logic piece of entire voting system. Each change made in a blockchain is called a Transaction. Transaction is the way by which the external world interacts with the Ethereum network. Transaction is used when we wish to modify or update the state stored in the Ethereum network. Each Transaction requires a transaction fee or service charge. Within an Ethereum network circulates a native currency: ether. Ether is mainly used as the transaction fee or service charge also Electronic copy available at: https://ssrn.com/abstract=3648870 called gas fee. In this project we are using Ganache-CLI. These speeds up the process of setting up a private network and transactions are mined almost immediately. MetaMask is a bridge that allows you to visit the distributed web of tomorrow in your browser today. It allows you to run Ethereum d-apps right in your browser without running a full Ethereum node.

**Detailed Description of the Layered Approach**

The proposed e-voting system architecture is presented in Fig. 1 and has been divided into several layers to achieve modular design. These layers are described below; the User Interaction and Front-end Security layer is responsible for interacting with a voter (to support vote casting functions) and the administrator (to support functions pertaining to administering the election process). It encapsulates two key functions i.e., authentication and authorization of the users (voters and administrators) to ensure that the access to the system is restricted to legitimate users in accordance with the predefined access control policies. Several different methods can be applied to achieve this function ranging from basic username/password to more advanced such as fingerprinting or iris recognition. Therefore, these are rendered specific to individual implementation of the proposed architecture. Overall, this layer serves as the first point of contact with the users and is responsible for validating user credentials as governed by the system-specific policies.

**Access Control Management layer** is envisaged to facilitate layer 1 and layer 3 by providing services required for these layers to achieve their expected functions. These services include roles definition, their respective access control policies and voting transaction definitions. The role definition and management provide core support for the access control functions implemented by layer 1 whereas the voting transaction definitions support the blockchain based transaction mapping and mining performed at layer 3. Overall, this layer enables a coherent function of the proposed system by providing the foundations required by individual layers. **e-Voting Transaction Management layer** is the core layer of the architecture where the transaction for e voting constructed at Role Management / Transactions layer is mapped onto the blockchain transaction to be mined. This mapped transaction also contains the credentials provided by a voter at layer 1 for authentication. An example of such data can be the fingerprint of the voter. This data is then used to create the cryptographic hash and contributes towards creating the transaction ID. The verification of such credentials is envisioned to be achieved at User Interaction and Front-end Security layer (layer 1). Several virtual instances of nodes are involved in the process of mining to get this transaction to finally enter into the chain.

**Ledger Synchronization layer** synchronizes Multichain ledger with the local application specific database using one of the existing database technologies. Votes cast are recorded in the data tables at the backend of the database. Voters are able to track their votes using the unique identifier provided to them as soon as their vote is mined and added into the blockchain ledger. The security considerations of the votes are based on block-chain technology using cryptographic hashes to secure end-to-end communication. Voting results are also stored in the application’s database with the view to facilitate auditing and any further operations at a later stage.

**The Voting Process**:

We now describe a typical interaction of a user with the proposed scheme based on our current implementation of the system. Typically, a voter logs into the system by providing his/her thumb impression. I

f the match is found, the voter is then presented with a list of available candidates with the option to cast a vote against them. On the contrary, if the match is unsuccessful, any further access would be denied.

This function is achieved using appropriate implementation of the authentication mechanism (fingerprinting in this case) and predefined role-based access control management.

Furthermore, it is also envisioned that a voter is assigned to their specific constituency and this information is used to develop the list of candidates that a voter can vote for.

The assignment of voters to a constituency is rendered an offline process and therefore out of scope of this research.

After a successful vote-cast, it is mined by multiple miners for validation following which valid and verified votes are added into public ledger. The security considerations of the votes are based on blockchain technology using cryptographic hashes to secure end-to-end verification. T

o this end, a successful vote cast is considered as a transaction within the blockchain of the voting application. Therefore, a vote cast is added as a new block (after successful mining) in the blockchain as well as being recorded in data tables at the backend of the database.

The system ensures only one-person, one-vote (democracy) property of voting systems.

This is achieved by using the voter’s unique thumbprint, which is matched at the beginning of every voting attempt to prevent double voting.

A transaction is generated as soon as the vote is mined by the miners which is unique for each vote. If the vote is found malicious it is rejected by miners.

After the validation process, a notification is immediately sent to the voter through message or an email providing the above defined transaction id by which the user can track his/her vote into the ledger.

Although this functions as a notification to the voter, it does not enable any user to extract the information about how a specific voter voted thereby achieving privacy of a voter.

It is important here to note that cryptographic hash for a voter is the unique hash of the voter by which the voter is known in the blockchain. This property facilitates achieving verifiability of the overall voting process.

Furthermore, this id is hidden and no one can view it even a system operator cannot view this hash therefore achieving privacy of individual voters

1. **FUTURE SCOPE**

Many issues with electronic voting can be solved using blockchain technology, which makes electronic voting more cost-effective, pleasant, and safe than any other network. Over time, research has highlighted specific problems, such as the need for further work on blockchain-based electronic voting and that blockchain-based electronic voting schemes have significant technical challenges.

#### Scalability and Processing Overheads:

For a small number of users, blockchain works well. However, when the network is utilized for large-scale elections, the number of users increases, resulting in a higher cost and time consumption for consuming the transaction. Scalability problems are exacerbated by the growing number of nodes in the blockchain network. In the election situation, the system’s scalability is already a significant issue. An electronic voting integration will further impact the system’s scalability based on blockchain.

Elucidates different metrics or properties inherent to all blockchain frameworks and presents a comparative analysis of some blockchain-based platforms such as Bitcoin, Ethereum, Hyperledger Fabric, Litecoin, Ripple, Dogecoin, Peercoin, etc. One way to enhance blockchain scaling would be to parallelize them, which is called sharing. In a conventional blockchain network, transactions and blocks are verified by all the participating nodes. In order to enable high concurrency in data, the data should be horizontally partitioned into parts, each known as a shard.

#### User Identity:

As a username, blockchain utilizes pseudonyms. This strategy does not provide complete privacy and secrecy. Because the transactions are public, the user’s identity may be discovered by examining and analyzing them. The blockchain’s functionality is not well suited to national elections.

#### Transactional Privacy:

In blockchain technology, transactional anonymity and privacy are difficult to accomplish. However, transactional secrecy and anonymity are required in an election system due to the presence of the transactions involved. For this purpose, a third-party authority required but not centralized, this third-party authority should check and balance on privacy.

#### Energy Efficiency:

Blockchain incorporates energy-intensive processes such as protocols, consensus, peer-to-peer communication, and asymmetrical encryption. Appropriate energy-efficient consensus methods are a need for blockchain-based electronic voting. Researchers suggested modifications to current peer-to-peer protocols to make them more energy-efficient.

#### Immatureness:

Blockchain is a revolutionary technology that symbolizes a complete shift to a decentralized network. It has the potential to revolutionize businesses in terms of strategy, structure, processes, and culture. The current implementation of blockchain is not without flaws. The technology is presently useless, and there is little public or professional understanding about it, making it impossible to evaluate its future potential. All present technical issues in blockchain adoption are usually caused by the technology’s immaturity.

#### Acceptableness:

While blockchain excels at delivering accuracy and security, people’s confidence and trust are critical components of effective blockchain electronic voting. The intricacy of blockchain may make it difficult for people to accept blockchain-based electronic voting, and it can be a significant barrier to ultimately adopting blockchain-based electronic voting in general public acceptance. A big marketing campaign is needed for this purpose to provide awareness to people about the benefits of blockchain voting systems, so that it will be easy for them to accept this new technology.

#### Political Leaders’ Resistance:

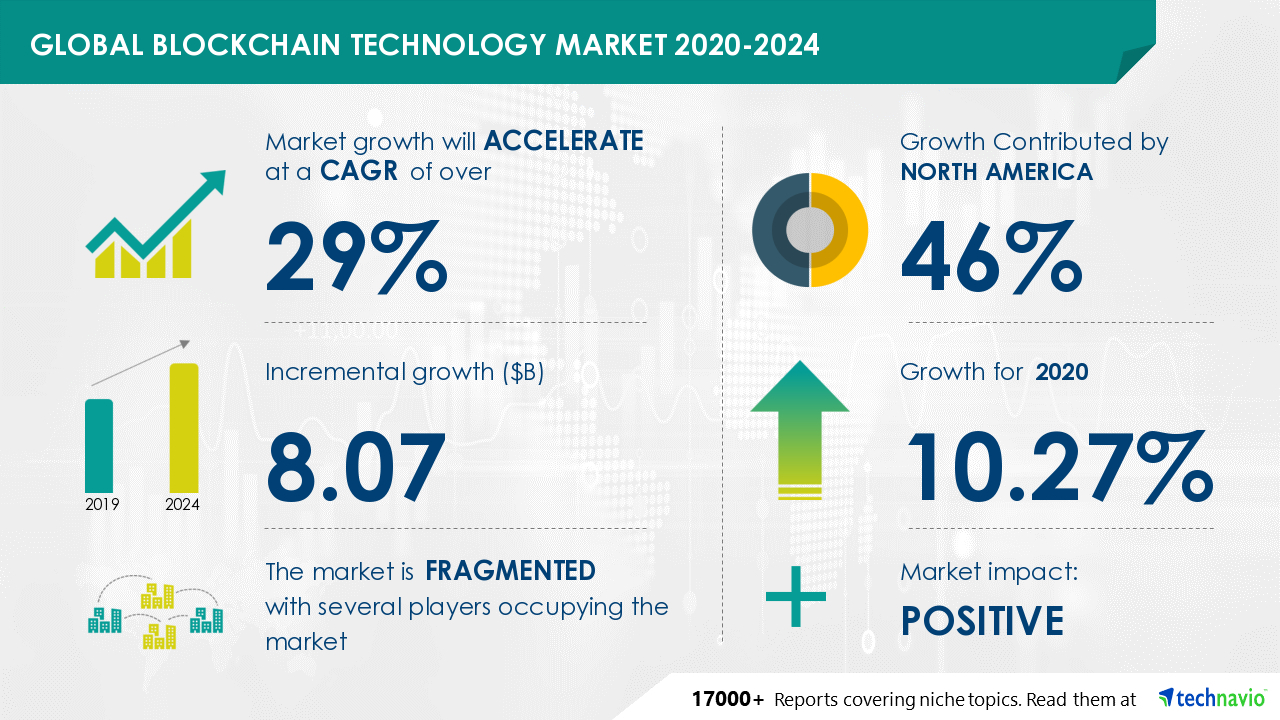
Central authorities, such as election authorities and government agencies, will be shifted away from electronic voting based on blockchain. As a result, political leaders who have profited from the existing election process are likely to oppose the technology because blockchain will empower social resistance through decentralized autonomous organizations.

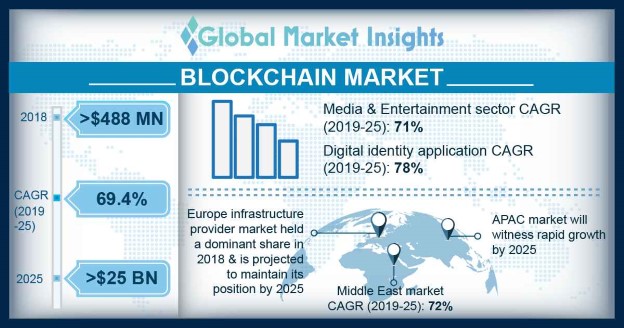
In continuation of this work, we are focused on improving the resistance of blockchain technology to the ‘double spending’ problem which will translate as ‘double voting’ for e-voting systems.

Although blockchain technology achieves significant success in detection of malleable change in a transaction, successful demonstration of such events have been achieved which motivates us to investigate it further.

To this end, we believe an effective model to establish trustworthy provenance for e-voting systems will be crucial to achieve an end-to-end verifiable e-voting scheme. The work to achieve this is underway in the form of an additional provenance layer to aid the existing blockchain based infrastructure.

**GLOBAL MARKET**

****



1. **DISADVANTAGES**

Technical challenges: Implementing a secure and reliable blockchain-based voting system can be technically challenging, and it requires a lot of research and development.

1. Lack of regulation: There is currently a lack of regulation and standardization for blockchain-based voting systems, which can lead to confusion and mistrust among voters and election officials.
2. Voter anonymity: Some blockchain-based voting systems can compromise voter anonymity, which can be a concern for individuals who are concerned about their personal safety or who live in countries with a history of political repression.
3. Voter education: Blockchain-based voting systems can be difficult for some voters to understand and use, which can lead to confusion and mistrust.
4. Accessibility: Blockchain-based voting systems can be less accessible for individuals who are not tech-savvy or who lack internet access.
5. Complexity: Blockchain-based voting systems are complex and require a significant amount of technical expertise to design, implement, and maintain.
6. Scalability: The scalability of blockchain-based voting systems is a challenge. As the number of users and transactions increase, the system may become slower and less efficient.
7. Security: While blockchain technology is generally considered secure, blockchain-based voting systems are still vulnerable to hacking, malware, and other forms of cyberattacks.
8. Lack of standards: There is currently a lack of standards for blockchain-based voting systems, which can result in interoperability issues and difficulties in integrating different systems.
9. Legal and regulatory issues: Blockchain-based voting systems must comply with legal and regulatory requirements, which can be complex and vary depending on the jurisdiction. Failure to comply with these requirements could result in legal and financial penalties.
10. Limited accessibility: One major disadvantage of blockchain-based voting systems is their limited accessibility. Not everyone has the technical know-how or resources to access and use blockchain technology effectively.
11. Security risks: While blockchain technology is inherently secure, blockchain-based voting systems are still vulnerable to security risks, such as hacking, cyberattacks, and insider threats. If a blockchain-based voting system is compromised, it could result in tampering with or manipulating the election results.
12. Technical issues: Like any other technology, blockchain-based voting systems can experience technical issues, such as software bugs, system crashes, or hardware failures. These issues could disrupt the voting process and cause delays or errors in the election results.
13. **CONCLUSION**

As a conclusion, we introduced a blockchain-based electronic voting system that utilizes smart contracts to enable secure and cost-efficient elections while guaranteeing voters privacy. We have shown that the blockchain technology offers a new possibility to overcome the limitations and adoption barriers of electronic voting systems which ensures the election security and integrity and lays the ground for transparency.

Using an Ethereum private blockchain, it is possible to send hundreds of transactions per second onto the blockchain, utilizing every aspect of the smart contract to ease the load on the blockchain.

For countries of greater size, some additional measures would be needed to support greater throughput of transactions per second. The transparency of the block-chain enables more auditing and understanding of elections.

These attributes are some of the requirements of a voting system. These characteristics come from decentralized networks, and can bring more democratic processes to elections, especially to direct election systems.

For e-voting to become more open, transparent, and independently auditable, a potential solution would be to base it on blockchain technology. This project explores the potential of blockchain technology and its usefulness in the e-voting scheme. The blockchain will be publicly verifiable and distributed in a way that no one will be able to corrupt it.

REFERENCES

[1] Adida, B.; ‘Helios (2008). Web-based open-audit voting, in Proceedings of the 17th Conference on

[2] Security Symposium, ser. SS'08. Berkeley, CA, USA: USENIX Association, 2008, pp. 335{348.

[3] Adida B. and Rivest, R. L. (2006). Scratch & vote: Self-contained paper-based cryptographic voting, in

[4] Proceedings of the 5th ACM Workshop on Privacy in Electronic Society, ser. WPES '06. New York, NY, USA: ACM, 2006, pp. 29-40.

[5] Bell, S., Benaloh, J., Byrne, M. D., Debeauvoir, D., Eakin, B., Kortum, P., McBurnett, N., Pereira, O.,

[6] Stark, P. B., Wallach, D. S., Fisher, G., Montoya, J., Parker, M. and Winn, M. (2013). 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.: USENIX Association, 2013.

[7] Bohli, J. M., Muller-Quade, J. and Rohrich, S. (2007). Bingo voting: Secure and coercion- free voting using a trusted random number generator, in Proceedings of the 1st International Conference on E-voting and Identity, ser. VOTE-ID'07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 111-124.

[8] Chaum, D., Essex, A., Carback, R., Clark, J., Popoveniuc, SSherman, A. and Vora, P. (2008) Scantegrity: End-to-end voter-verifiable optical- scan voting, IEEE Security Privacy, vol. 6, no. 3, pp. 40-46, May 2008.

[9] Chaum, D. (2004) Secret-ballot receipts: True voter-verifiable elections, IEEE Security Privacy, vol. 2, no. 1, pp. 38{47, Jan 2004.

[10] Chaum, D. (1981) Untraceable electronic mail, return addresses, and digital pseudonym’, Commun.

[11] ACM, vol. 24, no. 2, pp. 84{90, Feb. 1981.

[12] Chaum, D., Ryan, P. Y. A. and Schneider, P. Y. A. (2005). A practical voter-verifiable election scheme, in Proceedings of the 10th European Conference on Research in Computer Security, ser. ESORICS 05.Berlin, Heidelberg: Springer-Verlag, 2005, pp. 118- 139.