VOTING SYSTEM BASED ON BLOCKCHAIN TECHNOLOGY

A Project Report

Submitted in partial fulfilment of the
requirements for the award of the Degree of

BACHELOR OF SCIENCE (INFORMATION TECHNOLOGY)

By

BHIMESH BASAVARAJ PATIL

Seat Number: 3021303

Under the esteemed guidance of

Mrs. Pushpa Mahapatro

Assistant Professor, Department of Information Technology

DEPARTMENT OF INFORMATION TECHNOLOGY

VIDYALANKAR SCHOOL OF INFORMATION TECHNOLOGY

(Affiliated to University of Mumbai)

MUMBAI, 400 037

MAHARASHTRA

2018 – 2019

VIDYALANKAR SCHOOL OF INFORMATION TECHNOLOGY

(Affiliated to University of Mumbai)

MUMBAI-MAHARASHTRA-400037

DEPARTMENT OF INFORMATION TECHNOLOGY

VSIT | Vidyalankar School of Information Technology

CERTIFICATE

This is to certify that the project entitled, **"Voting System Based on Blockchain Technology."** is bonafide work of **BHIMESH BASAVARAJ PATIL** bearing Seat No: 3021303 submitted in partial fulfilment of the requirements for the award of degree of BACHELOR OF SCIENCE in INFORMATION TECHNOLOGY from University of Mumbai.

Internal Guide **Coordinator**

Internal Examiner **External Examiner**

Date: **College Seal** **Principal**

ABSTRACT

Electronic voting or e-voting has been used in varying forms since 1970s with fundamental benefits over paper-based systems such as increased efficiency and reduced errors. Notwithstanding, there remain difficulties to accomplishing broad reception of such frameworks particularly concerning working on their strength against expected shortcomings. Blockchain is a problematic innovation of the current period and vows to work on the general strength of e-casting a voting framework.

This paper presents a work to use the advantages of blockchain, for example, cryptographic establishments and straightforwardness to accomplish a powerful plan for e-casting a voting. The proposed plot adjusts to the key prerequisites for e-casting a voting conspires and accomplishes start to finish undeniable nature. The paper presents subtleties of the proposed e-casting a voting conspire alongside its execution utilizing the Multichain stage. The paper presents an inside and out assessment of the plan which effectively shows its viability to accomplish a start to finish undeniable e-casting a voting plot.

Keywords: Blockchain, Ethereum, smart contracts, electoral system, Bitcoin system, e-voting, security, privacy.

ACKNOWLEDGEMENT

We would like to express our special thanks and gratitude to ur project guide **Mrs. Pushpa Mahapatro** for guiding us to do the project work on time and giving us all support and guidance, which made complete our project duly. We are extremely thankful to her for providing such nice support and guidance.

We are also thankful for and fortunate enough to get constant encouragement, support, and guidance from the teachers of information Technology who helped us in successfully completing our project work.

DECLARATION

I hereby declare that the project entitled, **Secure Digital Voting System Based on Blockchain Technology** done at Vidyalankar School of Information Technology, has not been in any case duplicated to submit to any other universities for the award of any degree. To the best of my knowledge other than me, no one has submitted to any other university.

The project is done in partial fulfillment of the requirements for the award of degree of **BACHELOR OF SCIENCE (INFORMATION TECHNOLOGY)** to be submitted as final semester project as part of our curriculum.

Name and Signature of the Student

Table of Contents

List of Figures

Introduction

Elections are a crucial component of a democratic society because they allow the general population to express their opinions through voting. Because of their importance to our public, the political decision interaction ought to be straightforward and solid to guarantee members of its validity. Inside this specific situation, the way to deal with casting a voting has been an always developing area. This advancement is fundamentally determined by the endeavours to make the framework secure, certain, and straightforward. Because of its importance, ceaseless endeavours have been made to work on the general effectiveness and flexibility of the democratic framework. Electronic democratic or e-casting a voting plays a significant part in this. Since its first use as punched-card polling forms during the 1960s, e-casting a voting framework have accomplished momentous advancement with their adaption utilizing the web advances (Goble et al, 2015). Nonetheless, e-casting a voting framework should stick to explicit benchmark boundaries to work with their broad reception. These boundaries incorporate obscurity of the elector, respectability of the vote and non-renouncement among others.

Blockchain is one of the arising advancements with solid cryptographic establishments empowering applications to use these capacities to accomplish tough security arrangements. A Blockchain looks like the information structure that keeps up with and shares every one of the exchanges being executed through its beginning. It is basically a circulated decentralized information base that keeps a total rundown of continually developing and developing information records got from unapproved controlling, altering and amendment. Blockchain permits each client to associate with the organization, send new exchanges to it, confirm exchanges, and make new squares (Rosenfeld, 2017; Kadam et al, 2015; Nakamoto, 2009). Each square is allotted a cryptographic hash (which may likewise be treated as a unique mark of the square) that stays substantial if the information in the square isn't adjusted. If any progressions are made in the square, the cryptographic hash would change quickly showing the adjustment of the information which might be because of malignant action. Thusly, because of its solid establishments in cryptography, blockchain has been progressively used to relieve unapproved exchanges across different areas (Nakamoto, 2009; Kraft, 2015; Narayanan et al, 2015).

Bitcoin stays the most recognized utilization of blockchain anyway specialists are quick to investigate the utilization of blockchain innovation to work with applications across various areas utilizing advantages like non-disavowal, trustworthiness, and secrecy. In this paper, we investigate the utilization of blockchain to work with e-casting a voting application with the capacity to guarantee citizen obscurity, vote trustworthiness and end-to check. We accept e-casting a voting can use essential blockchain provisions, for example, rack cryptographic approval structure among exchanges (through hashes) and public accessibility of conveyed record of records. Blockchain innovation can assume a critical part in electronic democratic because of the intrinsic idea of protecting secrecy, keeping a decentralized and freely appropriated record of exchanges across every one of the hubs. This makes blockchain innovation exceptionally proficient to manage the danger of using a democratic token more than once and the endeavour to impact the straightforwardness of the outcome.

The focal point of our examination is to research the central questions like elector obscurity, vote privacy and start to finish check. These difficulties structure the establishment of a proficient democratic framework safeguarding the uprightness of the democratic interaction. In this paper, we present our endeavours to investigate the utilization of blockchain innovation to look for answers for these difficulties. Specifically, our framework depends on the Prêt à Voter approach (Ryan, 2008) and utilizes an open source blockchain stage, (Multichain, 2017) as the hidden innovation to foster our framework. To secure the obscurity and uprightness of a vote, the framework produces a solid cryptographic hash for each vote exchange dependent on data explicit to a citizen. This hash is likewise conveyed to the citizen utilizing scrambled channels to work with confirmation. The framework, subsequently, adjusts with the major prerequisites of an e-casting a voting framework as recognized by (Rura et al, 2016). More conversation around this is introduced in segment 2.

The remainder of the paper is coordinated as follows: the following segment presents the prerequisites for an e-casting a voting framework as recognized by (Rura et al, 2016) and clarifies how our proposed framework satisfies them. Segment 3 presents the best in class concerning e-casting a voting and how we add to it followed by a nitty gritty portrayal of the framework plan in segment 4. Area 5 presents the execution of our proposed framework with Multichain and UI alongside an assessment of the framework featuring how it accomplishes the prerequisites introduced in segment 2. Area 6 closes the paper by recognizing current advancement and plans for additional work.

Proposed System

The proposed system involves a client server architecture integrated with a block chain system. The minimum requirements needed by a voter is a smartphone or a computer with a webcam and an internet connection. If these are not met alternate arrangements such as pop-up cyber cafes and computers at public buildings must provide access to disadvantaged voters.

E-VOTING BACKGROUND AND REQUIREMENTS

Electronic voting has been an area of research focus for many years by using computing machines and equipment for casting votes and producing high quality and precise results in accordance with the sentiments of the participating voters. Various attempts have been adopted in practice to support election process. Initially computer counting system allowed the voter to cast vote on papers. Later on, those cards went through the process of scanning and tallying at every polling cell on a central server (Kadam et al, 2015; Rockwell, 2017; Hao et al, 2010). Direct Recording Electronic (DRE) voting systems were put in place later on which were admired and acknowledged greatly by the voters in-spite of the resistance from computer scientists. If the voting system is well understood by the voters, the system's usability can be increased remarkably. DRE systems in particular have gathered a lot of successes in bringing

the voters to use this technology. These systems work more or less in the same way as any conventional election system does. In the case of DRE, a voter begins his journey by going to their polling place and get their token to vote where he utilizes his token at the voting terminal to vote for his candidate. When the candidate selection procedure is completed, DRE systems present the final selection to the voter before actually casting it (in case if the voter wants to change his opinion) and after the final selection, the voting casting is completed (Multichain, 2017; Dalia et al, 2012).

More recently, distributed ledger technologies such as blockchain have been used to achieve e-voting systems primarily due to their advantages in terms of end-to-end verifiability. With properties such as anonymity, privacy protection and non-repudiation, blockchain is a very attractive alternative to contemporary e-voting systems. The research presented in this paper also attempts to leverage these properties of blockchain to achieve an efficient e-voting system. A detailed analysis of such systems is presented in the next section along with the identification of comparison with these approaches.

e-Voting Requirements and Compliance by the Proposed System

The generic requirements for a typical e-voting system have been defined in (Rura et al, 2016). We present a brief description of each requirement along with an explanation of how the proposed system fulfils it.

Privacy - Keeping an individual's vote secret

The system leverages cryptographic properties of blockchain to achieve privacy of a voter. More specifically, as voter is registered into the system, a voter hash is generated by blockchain which is the unique identifier of a voter into the blockchain, and is protected from misuse due to collision resistance property of the cryptographic hash. Due to this, the traceability of a vote is also non-trivial thereby protecting the voter when under duress.

Eligibility - Allowing only registered voters to vote, with each such voter voting only once

All eligible users are required to register using unique identifiers such as government-issued documents to assert their eligibility. In addition to this, our system implements strong authentication mechanism using finger printing technology to assert that only authorized voters can access the system. Furthermore, the use of biometrics also enables the system to protect against double voting.

Receipt Freeness - Voters should be unable to prove to a third party that they voted in a particular way

The proposed system enables a voter to vote as per their choice and creates a cryptographic hash for each such event (transaction). This is important to achieve verifiability i.e. to verify if a certain vote was included in the count. However, possession of this hash does not allow to extract information about the way voter has voted.

Convenience - Voters must be able to vote easily, and everyone who is eligible must be able to vote

The system has been implemented using a user friendly web based interface with the voting process requiring minimal input from the user. For instance, fingerprinting is implemented for authentication mechanism to avoid the requirement to remember username/passwords. Furthermore, the overall process is integrated which enables the user to interact with it in a seamless manner.

Verifiability - The ability to trust the vote tallying process

Upon casting their vote successfully, a user is provided with their unique transaction ID in the form of a cryptographic hash. A user can use this transaction ID to track if their vote was included in the tallying process. However, this process does not enable a user to view how they voted which has been adopted to mitigate threats when under duress.

The analysis presented above highlights the performance of the proposed system with respect to the specific requirements of e-voting. It also highlights the significance of defining characteristics of blockchain and their profound role in achieving the cornerstones of an efficient e-voting system. Therefore, we believe the work presented here makes significant contribution to the existing knowledge with respect to the application of blockchain technology to achieve a secure digital voting system

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. If the match is found, the voter is then presented with a list of available candidates with the option to cast 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 voter 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. To 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 validation process, a notification is immediately sent to the voter through message or an email providing the above defined transaction id by which user can track his/her vote into the ledger. Although this functions as a notification to the voter however 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 voter by which 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.

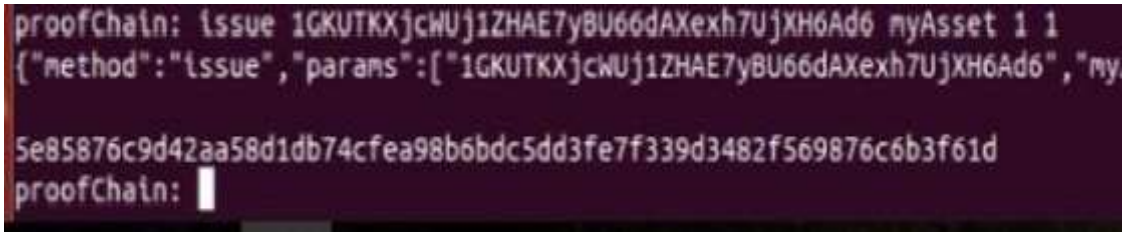


Figure 1. Asset creation using Multichain

Architecture

Shown below is the network architecture of the proposed system.

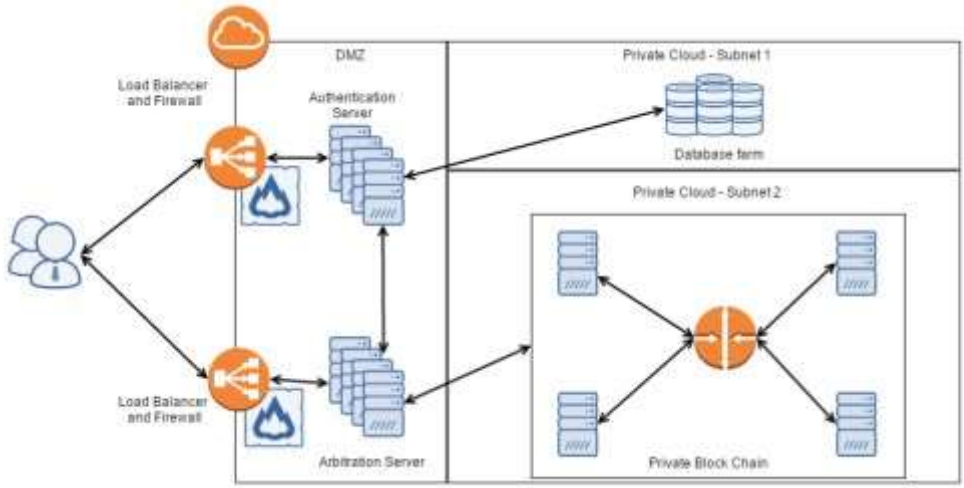
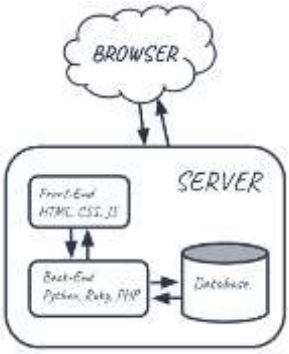


Figure 2. Network architecture of proposed system



The above diagram shows how the user interacts with the different parts of the system. The system will be explained in two parts – explaining the functionality of each part and the processes associated with the system.

Parts of the system

There are four main parts to the system. Each of them will be explained in detail below.

User

The user must have a smartphone, laptop or any device with a browser and a front facing camera. The user should likewise have a web association with register and vote also. On the off chance that the client doesn't have a PC or a web association, he/she could go to a public structure, for example, a library or a school which has PCs to enrol to cast a voting. These could be kept open the entire day during casting a voting enrolment and casting a voting day to guarantee individuals with low kinds of revenue don't get forgotten about.

Authentication Server (AS)

The Authentication Server is a conventional unified web server. It has a backend data set associated with it which has the data of the multitude of residents in the country. This framework is utilized by individuals to enlist to decide in favour of their races. Individuals make login accounts when they register. It additionally makes accounts on the blockchain framework for the clients when they vote. The blockchain account is utilized by the Arbitration Server to decide in favour of an up-and-comer of the clients' decision. The AS additionally verifies the token given to the Authorization Server by the user while voting.

Arbitration Server (AR)

The Arbitration Server acts as an intermediary between a user and the Blockchain voting system. It verifies the user while voting using the Authentication Server. The AR is a blockchain thin client that sends the users' vote to a blockchain node [3]. It also sends the user the key to encrypt their vote. The AR sends the users' vote to the appropriate node to be added to the blockchain. The user can verify their vote using the AR as an intermediary.

Blockchain system

The blockchain system is the system on which the actual voting takes place. The users' vote is sent to the one of the nodes on the system depending on the load on each node. The node then adds the transaction to the blockchain depending on the smart contracts that exist on each node. The smart contracts are the rules that the nodes follow to not only verify but also add the vote in the system. Each node follows the smart contract to verify the vote. The blockchain is a private system and is not accessible to the public directly. The system will currently have node server in each state to ensure a distributed network traffic on the system.

Processes in the system

The process of voting has two steps in the old process, i.e., registering to vote and the process of voting itself. The proposed system will have an extra step, i.e., the ability for the user to

verify their vote. This is an important step where the user can get a confirmation of their vote. The other steps include counting the votes by the organizer and recounting in case of any discrepancies.

Registering to vote

The process of registering to vote begins with the user interacting with the Authentication Server via a website. The AS contains data about electors in a data set. The client enters his/her Personally Identifiable Information (PII) and outputs supporting documentation to transfer into the framework alongside an email address. The clients' image is additionally taken for check. If the data is checked and is right, the client is permitted to make a record. Their preferred client enters a username and a secret key to sign in. This data is put away independently and not connected to the clients' PII. This guarantees security and secrecy while casting a voting. Likewise, a passage is made close to the clients' information base section putting away whether he/she has enrolled to cast a voting. In case the clients' data can't be checked, he/she isn't permitted to make a record.

All the data between the client and the AS is sent utilizing TLS v1.2 convention to guarantee it is all protected. The code for enlistment process is set in Appendix B and Appendix C of this archive.

Voting

The process of voting is a multi-step process. It includes confirming your personality with the AS and afterward casting a voting utilizing the AR. Upon the arrival of casting a voting every applicant is given a record on the blockchain framework so they can get votes. There is likewise a "Decline account" for avoided votes to be shipped off.

During the democratic day, the client signs into the confirmation server utilizing the username and secret word made in the past advance. A picture of the client is taken to guarantee that the client is the proprietor of the record. This picture is contrasted, and the picture taken during enlistment.

A little video of the client is taken before they sign in and is shipped off the Authentication Server. Utilizing the Affective API, the AS can distinguish client feelings dependent on AI innovation [4]. On the off chance that the framework distinguishes dread, the clients' meeting is halted and told to retry following 5 minutes. While signing in for the subsequent time if the framework recognizes dread once more, the client should go to their nearby surveying community like a library to cast a voting. This framework would diminish the effect of the issue identified with casting a voting under coercion.

When the client signs in, their framework would make a public key which they would ship off the Authentication Server. The AS would add partner the key with the username. The key would be utilized to make a record for the client on the blockchain framework to cast a voting. A particular measure of ether (money the client can use to cast a voting) is added to the clients' record which empowers them to cast a voting.

The AS would then send a meeting token back to the client.

The client would be diverted to the AR. The client would give the AR the meeting token, would confirm it with AS. The confirmation and age of tokens between the AR, client and AS is finished utilizing the Modified Needham-Schroeder convention. This shields the framework from pantomime and man in the centre assaults.

The AR would send a confirmation message to the client alongside the public key of the blockchain hub to which his/her vote would be sent.

The client would encode their vote with the public key and send it to AR. This would guarantee that the AR can't peruse the clients' vote and thus the vote would stay confidential. The AR would send the scrambled vote to the proper hub. The hub would unscramble the message with their private key and send a particular measure of ether from the clients' record to the applicants' (or to the Abstain account if they might want to relinquish their vote) blockchain account. Every hub would confirm the exchange as indicated by the brilliant agreements. These agreements would confirm a specific exchange was a copy one or no and really look at its legitimacy. After this cycle, the hub would pass this exchange to different hubs in the blockchain framework.

The code for the savvy contracts utilized in the Blockchain framework is set in Appendix A.

Verifying the vote

The process of verifying the vote depends on the type of election it is. Some elections allow for interim results, and some do not. In either case the voter must get a confirmation that his/her transaction has been approved by the blockchain system.
In case of the election that allows interim results, one of the nodes of the blockchain could be made publicly accessible. It would have a website similar to https://blockchain.info where a user could enter their public key to verify whether their vote was counted. This node would not have the ability to add any transactions to the system. This will be implemented through smart contracts. It will only be a reader of the transactions. This will reduce the attack surface of the system.

If the organizers of an election want to keep the interim results a secret, he/she could only get a binary verification via the AR. Since the AR is a thin client, it would act as an intermediary to verify the transaction [3]. At the end of the election in above case, the user will be able to check the result for the election.

Counting votes

The process of counting votes of a candidate can be very simple. Each voter has a fixed amount of ether or currency value that they use to vote for a candidate of their choice. The candidate with the highest amount of ether in their account wins the election.
For users who abstained from voting, their ether will be sent to an Abstain Account. This ensures their vote does not get misused.

Recounting the cotes

There are instances of disputes in the results of an election. These can be resolved in the proposed system easily.

The entire tree associated with a single account root can be made public for people to verify if their vote has been tallied or no [5]. This makes the system transparent for users. Since no one knows which user is associated with which account, it protects the users' anonymity in voting. The public keys for each transaction in the blockchain system can be mapped to accounts in the AS. The list of public keys generated gives the list of people who voted. By mapping this list with the public keys associated with each transaction, the election can be verified.

Economic advantages of the system

Cost benefit analysis of proposed system

Cost of labour per person = $80/hour
Requirement of 25 people over 12 months to build and test the system
One time Cost to customer = $4,000,000
Cost of hardware and maintenance for 1st election = $100,000,000 for a voter base of 100 million (based on EC2 calculator)
(Includes data centre costs, network equipment and bandwidth)
For subsequent election cycles cost = $50,000,000
Cost of running a voting-based election = $2 per person [6]
= $200,000,000 for 100 million voters

The cost of running the election for the 1st year using proposed system = $104,000,000

Cost for a country

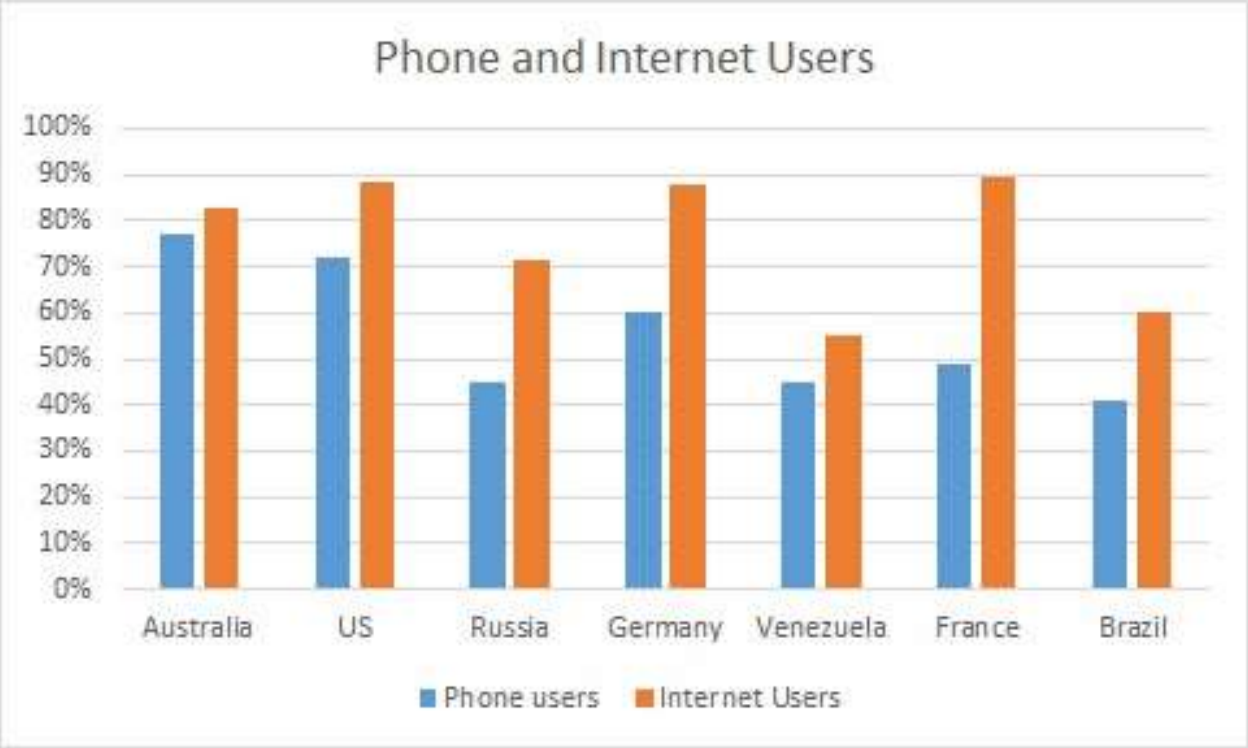


Figure 3. Graph of phone and internet penetration of a country

The graph above shows the internet and smartphone penetration in a country. These are the two minimum requirements of a user to vote. The internet entrance is given a higher significance since individuals can in any case go to government buildings like libraries to cast a voting. The framework requires the web entrance of a nation to be more noteworthy than or equivalents to 90% to make this venture doable. Anything beneath that will require the public authority to put into a lot of foundation to set up a web association for clients. These are current insights of nations on the planet. An enormous number of individuals on the planet are accessing the web each day. As this number develops the proposed framework will become attainable for a greater number of nations on the planet than it is presently.

ER Diagram

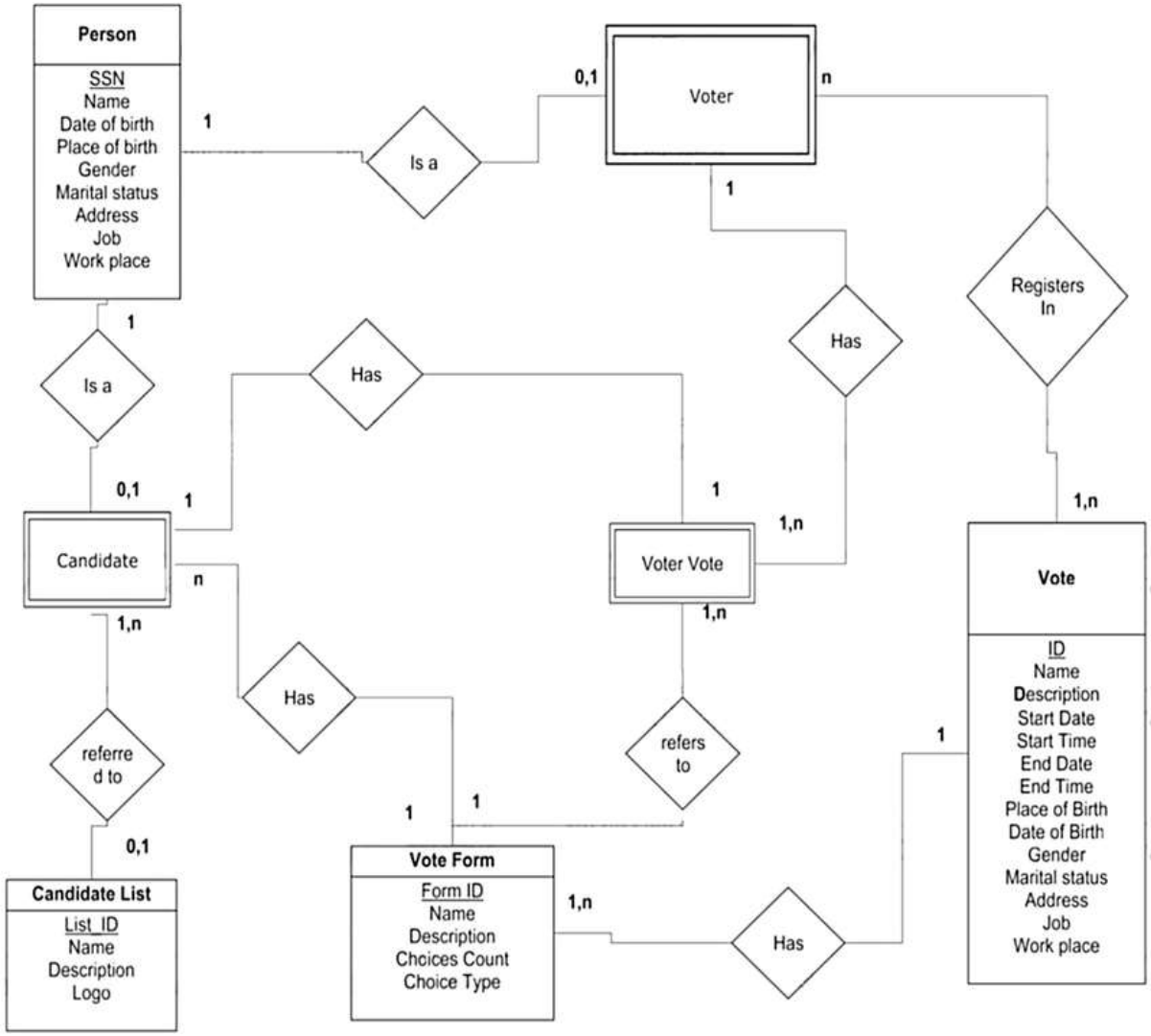


Figure 4. ER Diagram

IMPLEMENTATION AND EVALUATION

Implementation

The implementation of the proposed system has been carried out within a controlled environment with a web-based application created to serve as the front-end application enabling the users to interact in a convenient manner. The application uses a MySQL as the backend database for the application and contains the data entered manually by an admin such as the voter details, constituency details and the information about different political parties running for the election. An application screenshot demonstrating the admin function to view list of eligible voters is presented in Fig. 1. In addition to manual entries, the application also supports importing data using MS Excel spread sheets to perform bulk import in view of the size of the data in real-world voting scenarios. We have used Multichain as the blockchain platform to create a private blockchain for this application which is used for recording the voting transactions. This choice is influenced by the ease of use provided by this platform and therefore it was easily integrated into our proposed architecture.

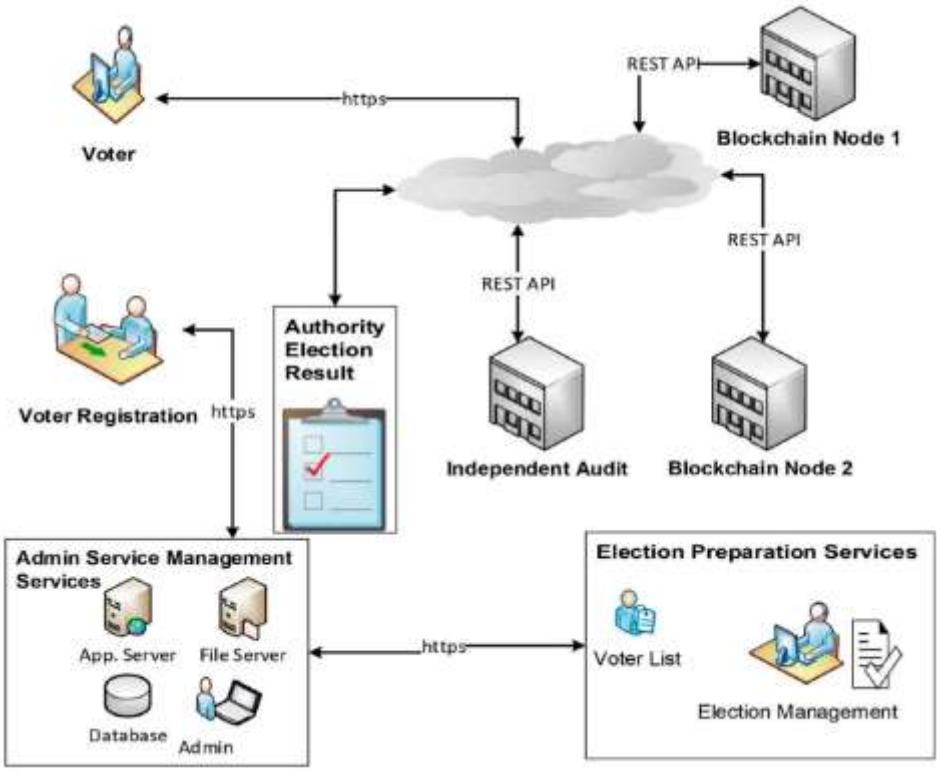


Figure 5. Class Diagram

Evaluation and Experimentation

The primary objective of evaluation was to assess the performance of the system in view of the e-voting system requirements presented in section 2 and to identify any considerations with regards to its application in a real-world scenario. The experimentation consisted of multiple steps i.e., conducting multiple transactions, verification of transactions, mining transactions into blockchain, reflection of the changes made in the public ledger to all the nodes in the network and the usability of the system.

A test run was made directly at Multichain by starting from asset creation. An outcome of this is demonstrated by Fig. 3. We can refer these assets as votes. Since Multichain by default ideally suits to cryptocurrency, therefore we wrote our APIs to design it in the context of vote. In order to perform transaction in Multichain, we identified the address and the balance in the address of the node of Multichain from where the asset (vote) will be sent.

While sending the asset to the address, the transaction hash was generated carrying the transfer of vote. The balance of the receiving node was incremented by one vote (asset). The transaction becomes a part of the public ledger which shows that it has been mined. A sample transaction within the proposed system is presented by Fig. 3. Since our customized API for asset creation is designed in such a way that an address can have at max only one vote (asset), therefore, it will not be possible for a voter to caste multiple votes unless the node receives it from some other address which is only allowed in the case of the candidate.

Social benefits

The system of remote blockchain voting will impact society in a very positive way.
The system will increase convenience for voters [7]. It will make it very easy for people with disabilities or who have trouble moving around to vote. It is very quick and private way to vote [8]. This will increase the number of voters since the process does not take up too much of their time of the day. It will help increase the trust of the people in the government since it is more transparent than the current voting system. The system is better for the environment as compared to the paper voting system. It eliminates the need for paper voting and the carbon emitted by the logistics of those voting's. Hence this system has a much smaller carbon footprint.

Conclusion

Electronic democracy has been utilized in changing structures since 1970s with key advantages over paper-based frameworks like expanded effectiveness and decreased blunders. With the remarkable development in the utilization of blockchain innovations, various drives have been made to investigate the attainability of utilizing blockchain to help a viable answer for e-casting a voting. This paper has introduced one such exertion which use advantages of blockchain, for example, cryptographic establishments and straightforwardness to accomplish a viable answer for e-casting a voting. The proposed approach has been carried out with Multichain and in-depth assessment of approach features its adequacy regarding accomplishing essential prerequisites for an e-casting a voting conspire.

In continuation of this work, we are engaged at working on the opposition of blockchain innovation to 'twofold spending' issue which will interpret as 'twofold deciding in favour of' e-casting a voting framework. Even though blockchain innovation makes critical progress in discovery of pliant change in an exchange anyway effective showing of such occasions have been accomplish which spurs us to examine it further. To this end, we accept a successful model to build up reliable provenance for e-casting a voting framework will be critical to accomplish a start to finish undeniable e-casting a voting conspire. The work to accomplish this is in progress as an extra provenance layer to help the current blockchain based foundation.

References & Bibliography

1. Gallup, "Trust in Government," Gallup, 30 September 2015. [Online]. Available: http://www.gallup.com/poll/5392/trust-government.aspx. [Accessed 28 Septmeber 2016].
2. Wikipedia, "List of controversial elections," 20 September 2016. [Online]. Available: https://en.wikipedia.org/wiki/List_of_controversial_elections. [Accessed 27 September 2016].
3. R. Skudnov, "Bitcoin Clients," Turku University of Applied Sciences, Turku, 2012.
4. Affectiva, "Affective Product Overview," 15 January 2016. [Online]. Available: http://www.affectiva.com/wp-content/uploads/2014/11/AffectivaProductOverview.pdf. [Accessed 28 September 2016].
5. P. Noizat, "Blockchain Electronic Vote," in *handbook of digital Currency*, Paris, Elsevier Inc., 2015, pp. 453-461.
6. The electoral knowledge network, "Cost of Registration and Elections," ACE Project, 15 Jan 2016. [Online]. Available: http://aceproject.org/ace-en/focus/core/crb/crb03. [Accessed 28 September 2016].
7. N. Uribe, "10 Benefits of Electronic Voting," 01 August 2016. [Online]. Available: http://www.fobsoftware.com/blog/10-benefits-of-electronic-voting-for-home-ownerassociations. [Accessed 28 September 2016].
8. G. Schryen, "Security Aspects of Internet Voting," in *IEEE*, Hawaii, 2004.
9. Wikipedia, "List of countries by smartphone penetration," 18 September 2016. [Online].