International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 03 | March - 2023 Impact Factor: 7.185 ISSN: 2582-3930

Aadhaar Based Voting System Using Blockchain

D VISWASAHITHYA[1], K. MANISH[2], K.FIZUNNISHA[3], C.THULASI REDDY[4], K.VINAY KUMAR[5]
[1]Assitant professor, [2,3,4,5] Students, Dept of CSIT
[1,2,3,4,5] Siddharth Institute of Engineering & Technology, Puttur-517583

Abstract

Online voting is a growing trend that is gaining momentum in modern society. This has great potential to decrease organizational costs and increase voter turnout. This eliminates the need to print ballots or open polling stations-voters can vote anywhere there is an internet connection. Now that elections take place on electronic voting machines, these systems present a high risk of rigging and prone to failure and attacks from intruders (a person who intrudes, especially into a building with criminal intent) The above problems can be addressed through the implementation of new technology namely Blockchain for a transparent and reliable voting process. Blockchain is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system. A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain. To improve the quality of election we came up with the Aadhar based voting system. Aadhar based voting system helps in reducing the paperwork and decreases multiple voting, decreases the fraudulent elections, and improve election quality.

Introduction

Voting plays an important role for every citizen of India and first election voting was started in the year of General elections were held in India between 25 October 1951 to 21 February 1952.The majority rule framework in India depends on the standard of widespread grown-up testimonial; in other words, any resident beyond 18 a years old vote in a political decision to Lok Sabha or Vidhana Sabha (before 1989 as far as possible was 21). The option to cast a ballot is regardless of position, ideology, religion, or orientation.

1. PRELIMINARIES OF E-VOTING AND BLOCKCHAIN

In this section, we first expand on the design considerations when building an electronic voting system. We then provide an overview of blockchain and smart contract technology and its respective feasibility as a service for implementing an electronic voting system.

A. Design Considerations

After evaluating both existing electronic voting systems and the requirements for such systems to be used effectively in national elections, we have complied the following list of requirements for a viable electronic voting system:

(i) An election system should not enable coerced voting.
(ii) An election system must allow a method of secure authentication via an identity verification service.
(iii) An election system should not allow traceability from votes to respective voters.
(iv) An election system should provide transparency, in the form of a verifiable assurance to each voter that
their vote was counted, has been correctly, and without
compromising voter privacy.
(v) The election system must prevent any third party from tampering with a ballot.
(vi) The election system should not allow a single entity to control the counting of votes and determination of election results.
(vii) An election system must allow only eligible people to vote in an election.

B. BLOCKCHAIN AS A SERVICE

The blockchain is an append-only data structure, where data is stored in a distributed ledger that cannot be tampered with or deleted. This makes the registry immutable. The blocks are chained in such a way that each block has a hash value that is a function of the previous block, and thus by induction the complete prior chain, thereby providing guarantee of immutability. There are two different types of blockchains, with different levels of restrictions based on who can read and write blocks. Public blockchains are readable and writable for anyone in the world. This type is popular among cryptocurrencies. Private blockchains limit who can read or interact with the blockchain. Private blockchains are also referred to as permissions, where access can be granted to specific nodes that can interact with the blockchain. In addition to cryptocurrencies, blockchain provides a platform to create distributed and immutable applications or smart contracts. Smart contracts are programmable contracts that automatically execute when predetermined conditions are met. Similar to traditional written contracts, smart contracts are used as a legally binding agreements between parties. Smart contracts automate transactions and allow parties to enter into an agreement directly and automatically, without the need for a middleman. The main advantages of smart contracts compared to traditional written contracts are cost saving, enhanced efficiency, and risk reduction. Smart contracts redefine trust because contracts are visible to all the blockchain users and can, therefore be easily verified. In this work, we define our electronic voting system based on a smart contract.

2. BLOCKCHAIN A SERVICE FOR ELECTRONIC VOTING

This section offers a new electronic voting system based on established voting requirements and blockchain as a service. We explain the setup of the blockchain, define the smart contract for electronic voting that will be deployed on the blockchain and show how the proposed system meets the expected voting requirements.

BLOCKCHAIN SETUP: Configuring the blockchain to meet privacy and security requires voting and ensure that the election does not system

should not enable coerced voting, voters will have to vote in a supervised environment. In our work, we setup a Go- Ethereum permissioned proof-of-authority (POA) blockchain authorized by Go-Ethereum to achieve these goals. POA uses an algorithm that provides relatively fast transactions through a consensus mechanism based on identity as a stake. The reason for using Go-Ethereum as the blockchain infrastructure is explained in subsection.

C. The structure of the blockchain is shown in Figure 1, which is mainly composed of two types of

(i) District nodes: Representing each voting district. Each zone node has a software agent that autonomously interacts with the "bootnode" and manages the life cycle of the smart contract on that node. When the election Administrator (see on smart contract) creates an election, a voting smart contract is distributed and deployed to its corresponding district node. When the ballot smart contracts are created, each of the corresponding district nodes is given permission to interact with their corresponding contract. When an individual voter votes from their corresponding smart contract, the voting data will be verified by a majority of the corresponding district nodes and every vote they agree on is added to the blockchain.

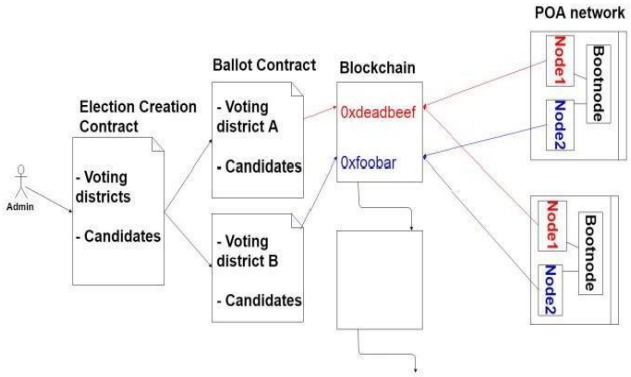


Fig. 1: Election as a smart contract

(ii) Bootnode: Each institution that has access to the network, hosts a bootnode. A bootnode is a discovery and coordination service that helps the district nodes to discover and communicate each other. The bootnode does not keep any state of the blockchain and is run on a static IP address so that district nodes can find their peers faster. After setting up a secure and private blockchain, the next step is to define and deploy a smart contract that represents the e-voting process on the blockchain infrastructure.

The Election as a smart contract: The Defining a smart contract consists of three parts: identifying the roles that are involved in the agreement (the election agreement in our case),

The agreement process (i.e., election process), and the transactions (i.e., voting transaction) used in the smart contract. Election roles: The roles in a smart contract include the parties that need to participate in the agreement. The election process has the following roles:

Election Administrator: Manages the lifecycle of an election. Various trusted institutions and companies can be registered for this role. Election administrators create elections, register voters, determine the election lifecycle, and assign authorized nodes. Voter: An individual who is eligible to vote. Voters can authenticate themselves, load election ballots, cast their vote and verify their vote after an election is over.

Election process: In our work, each election process is represented by a set of smart contracts, which are deployed on the blockchain by the election administrator, as shown in Figure 1. A smart contract

is defined for each of the voting districts. The main activities in the election process are:

TABLE I: Example of a transaction in our system

TxHash	Block	To	Value
0xdeadbeef..	1337	N1SC	D
0xG1345edf..	1330	N2SC	P

Counting Result: Election count is performed in the smart contracts. Each ballot smart contract establishes its own score for its corresponding position location in its own storage.

Validate votes: In a voting transaction, each voter receives a transaction ID for their vote. In our e-voting system, voters can use this transaction ID and go to an official election site (or authority) using a blockchain browser and (after authenticating themselves using their electronic identity)enter a transaction with the corresponding transaction ID on the blockchain. Voters can, therefore, see their votes on the blockchain, and verify that the votes were listed and counted correctly. This type of verification satisfies the transparency requirements while preventing traceability of votes.

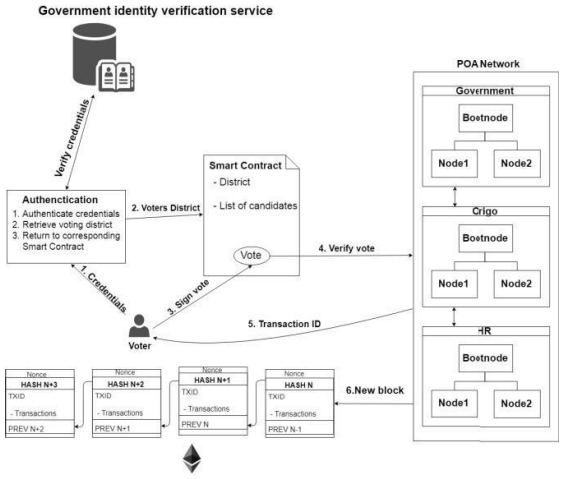


Fig. 2: Voting process.

Voting transaction: Each voter interacts with a ballot smart contract their corresponding voting district. This smart contract interacts with the blockchain via the corresponding district node, which appends the vote to the blockchain. Each individual voter receives the transaction ID for their vote for verification purposes. Every vote that is agreed upon, by the majority of the corresponding district nodes, is recorded as a transaction and then appended on the blockchain. Figure 2 is a visual representation of this process. A transaction in our proposed system (see Table I) has information on i) the transaction, ii) the block in which the transaction is located, iii) the smart contract to which transaction was sent – indicating in which voting district the vote was cast, and iv) the value of the transaction, i.e., the vote, indicates for which entity (party) the voter voted. A voting transaction in our system, Therefore, reveals no information about the individual voter who cast any vote.

C. Evaluating Blockchain Implementations.

As noted at the beginning of this section, in order to comply with the privacy, security and transparency requirements of e-voting and to ensure that the election system should not enable coerced voting, in

our work, we are using a private (permissioned) blockchain for setting up our blockchain infrastructure, where the smart contracts are deployed. In this subsection, we consider three blockchain frameworks (See Table II) to implement and deploy our election smart contracts. These are Exonum, Quorum and Geth.

1) **Exonum**: The Exonum blockchain is robust from end-to end with its fully implemented in the Rust Programming Language. Exonum is specially designed for private blockchains. It has a custom Byzantine algorithm that is used to achieve consensus in the network. Exonum can support up to 5000 transactions per second. Unfortunately, a limitation of the framework is that Rust is the only programming language in the current version, which limits the developers to the constructs available in that language. Exonum is projecting to introduce Java-bindings and platform-independent interface description in the near future to make Exonum more developer-friendly.

2) Quorum: An Ethereum-based distributed ledger protocol with transaction/contract privacy and new consensus mechanisms. It is a Geth fork and is updated in line with Geth releases. Quorum has changed the consensus mechanism and is aimed more towards consortium chain-based consensus algorithms. Using this consensus allows it to support hundreds of transactions per second.

3) Geth: Go-Ethereum or Geth is one of three original implementations of the Ethereum protocol. It runs smart contract applications exactly as programmed without the possibility of downtime, censorship, fraud or third-party interference. This framework supports development beyond the Geth protocol and is the most developer-friendly framework of those we evaluated. The transaction rate is dependent on whether the blockchain is implemented as a public or private network. Because of these capabilities, Geth was the framework we chose to base our work on, any similar blockchain framework with the same capabilities as Geth could be considered for such system.

3. PROPOSED SYSTEM

We will develop a secure web application for election voting using block chain technology, and we use username and password credentials for validation. We have two panels in the application one is for the admins and one for voters. The admin panel can only be accessed by admins who are election conductors and admin have access to start the election and he can also end the election at any time and admin information is stored in the database. Voters need to be registered with the help of Aadhaar authentication and then admin will give permission to caste vote after that process the voter can caste the vote and after casting the vote that will be added to block chain using Ganache and the voting results will display after election ends. Voter's data and admin data is stored in database. In the remote areas, Election Commission of India will appoint volunteers who will have a separate interface in our application for the elderly and physically handicapped.

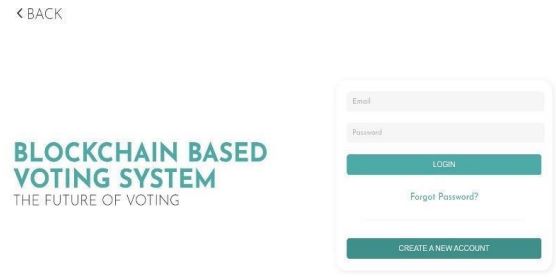
4.Experimental Results of E-Voting System

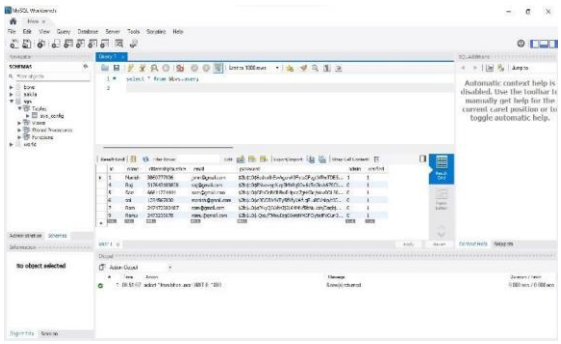
This experiment is carried out on the platform of solidity and the experimental results has done in data is collected by sending google form to family and friends.

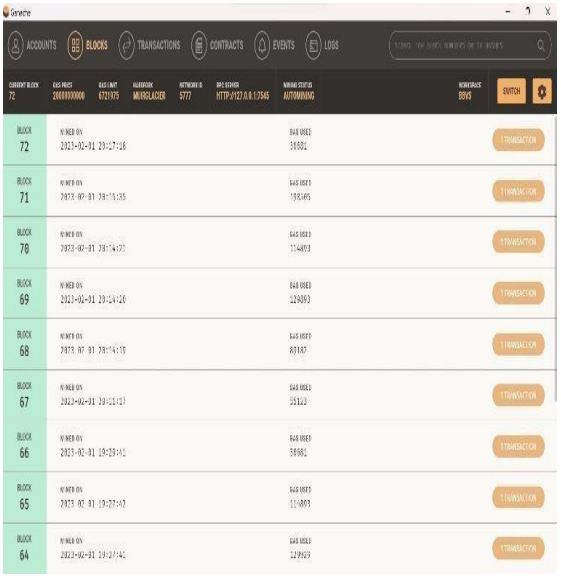
4.1 Experimental Results Analysis of Aadhaar voting system.

This is home page looks like:

This is login page looks like







5. SUMMARY

In our project, 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. 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.

6. References:

[1] Roopak T M, Dr. R Sumathi, "Electronic Voting based on Virtual ID of Aadhar using Blockchain Technology", Department of Computer Science and Engineering Siddaganga Institute of Technology 2019.

[2] Rifa Hanifatunnisa, et al, " Blockchain Based EVoting Recording System Design", School of Electrical Engineering and Informatics 2017.

[3] Vanessa Teague, Steve Schneider, Peter Y.A. Ryan, "End to End Verifiability in voting system from theory to practice" June2015.

[4] N. Satoshi, "Bitcoin: a peer-to-peer electronic cash system", 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Accessed 2018].

[5] J. L. Zhao, S. Fan and J. Yan, "Overview of business innovations and research opportunities in blockchain and introduction to the special issue", Financial Innovation, Springer Berlin Heidelberg, 2016, p. 2–28.

[6] D. Drescher, "Blockchain Basics: A Non-Technical Introduction in 25 Steps", 1 ed., Frankfurt am Main: Apress, 2017.

[7] Rifa Hanifatunnisa, et al, "Blockchain Based EVoting Recording System Design", School of Electrical Engineering and Informatics 2017.

[8] UIDAI Aadhaar API, Available From https://uidai.gov.in/images/FrontPageUpdates/aadhaar_authentication_api_2_0.pdf. 11 Bloomberg, "Why India's election is among the world's most expensive", The Economic Times, Accessed on Apr 7, 2019.

[9] Sos.ca.gov. (2007). Top-to-Bottom Review | California Secretary of State. Available at: http://www.sos.ca.gov/elections/voting systems/oversight/ top- bottom-review/.

[10] Nicholas Weaver. (2016). Secure the Vote Today Available at:https:// www.lawfareblog.com/secure-vote-today.

[11] TechCrunch, (2018). Liquid democracy uses blockchain to fix politics, and now you can vote for it. Available at: https://techcrunch.com/2018/ 02/24/liquid-democracy-uses- blockchain/ [4] Ajit Kulkarni, (2018), "How To Choose Between Public And Permissioned Blockchain For Your Project", Chronicled, 2018.

[12] "What Are Smart Contracts? A Beginner's Guide to Smart Contracts", Blockgeeks, 2016. Available at: https://blockgeeks.com/guides/ smart-contracts/

[13] Salanfe, Setup your own private Proof-of-Authority Ethereum network with Geth, Hacker Noon, 2018. Available at: https://tinyurl.com/ y7g362kd. [7] Geth.ethereum.org. (2018). Go Ethereum. Available at: https://geth. ethereum.org