Electronic Polling Agent Using Blockchain: A New Approach

Aishwarya Babu and Vaibhav D. Dhore

Abstract The blockchain supports all kinds of potential for improving digital systems. Frequently, we hear about all the potential of blockchain in reference to economic services and finance systems. But the digital system that could possibly be most enhanced by blockchain is e-voting. Over the progression of the former election cycle, fraud, fake votes, and "system rigging" were widespread. This makes it clear that both conventional paper-based ballot system and the centralized electronic-based voting system have definite apertures creating vulnerabilities and vote manipulation. The blockchain is an immutable ledger, and integrating blockchain technology with a voting system can give the solution to numerous problems faced by modern systems. The motive for e-voting system using blockchain is to facilitate transparency, fairness, and audibility. While the number of voters increases, the time taken to cast vote, i.e., time taken to generate block also increases due to which the throughput of the system decreases. A new system is proposed in this paper, which aims to provide a fast, secure, and transparent voting approach using blockchain.

Keywords Blockchain · Polling agent · E-voting

1 Introduction

With the sudden popularity of bitcoin, the technology behind it which is blockchain had its come back. Before it existed in cryptocurrency, it had modest origins as an idea in computer science, especially in the domains of cryptography and data structures. It consolidates the openness of the Internet with the security of cryptography to provide everyone with a quicker, secured way to verify important information and build trust. Due to its potential feature, blockchain acts as a perfect technology to combine with polling agent.

A. Babu (✉) · V. D. Dhore
VJTI, Mumbai University, Mumbai, India
e-mail: aishwaryababu95@gmail.com

V. D. Dhore
e-mail: vddhore@ce.vjti.ac.in

D. Patel et al. (eds.), *IC-BCT 2019*, Blockchain Technologies,
https://doi.org/10.1007/978-981-15-4542-9_7

1.1 Blockchain

Blockchain can be denied as a prototype of the distributed ledger for controlling a durable and tamper-proof account of transactional information. Originally, blockchain is an increasing list of records, described blocks, which are associated using cryptography. Per block comprises a cryptographic hash concerning the preceding block, a timestamp of the transaction, and the actual transaction data. By intention, a blockchain is a repellent to alteration of the data. It is "an unrestricted, distributed ledger which logs events among two parties effectively as well as efficiently in a variable and intermittent way" (Fig. 1).

To make application as a distributed ledger, a blockchain is achieved by a peer-to-peer interface jointly adhering to a contract for inter-node transmission and validating new blocks. Once recorded, the data in each assigned block cannot be remodeled retroactively without revision of all subsequent blocks, which demands an agreement of the network majority. Although blockchain recordings are not inevitable, blockchains may be thought to be guarded by design and illustrate to be a dispersed computing system with great fault immunity. Decentralized consensus has therefore been claimed with a blockchain.

Currently, there are three varieties of blockchain networks

1. Public blockchain.
2. Private blockchain.
3. Consortium blockchain (Fig. 2).

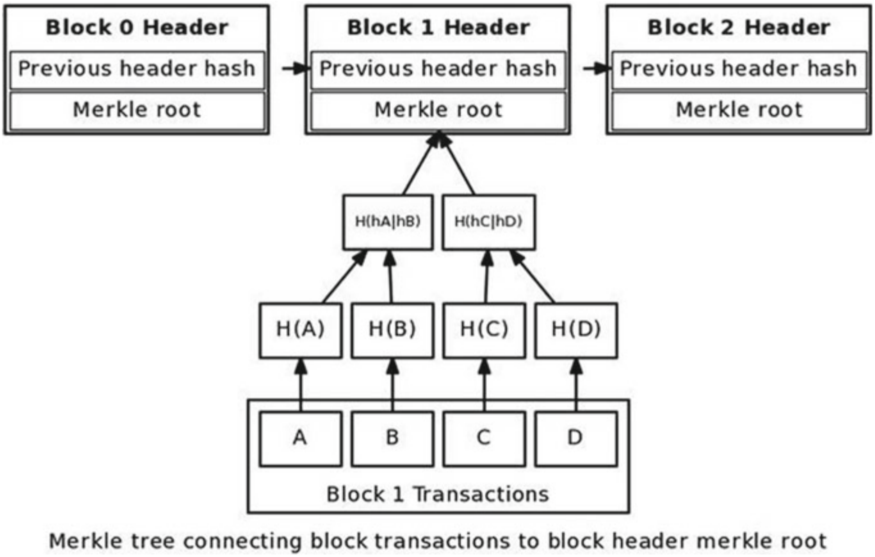


Fig. 1 Blockchain

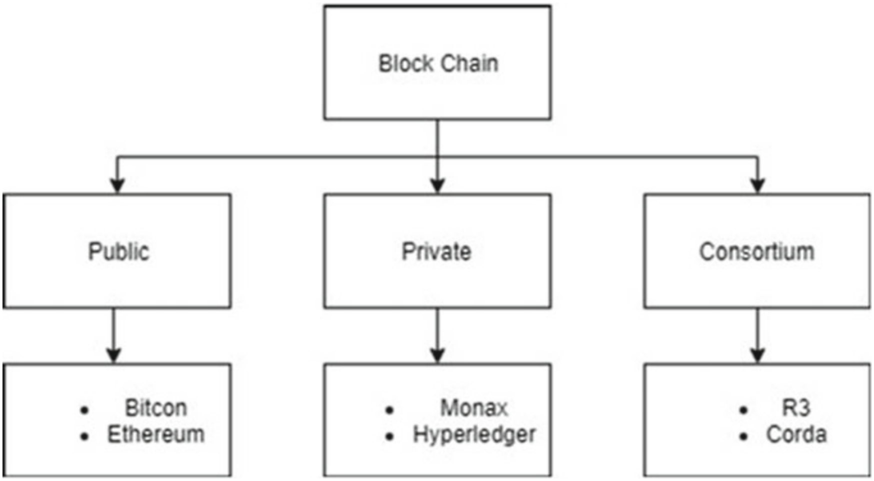


Fig. 2 Types of blockchain

1.2 Electronic Voting

Electronic voting (e-voting), which utilizes electronic systems to support casting and counting votes in an election, has remained a research topic of importance for the past several decades. In association with the conventional paper-based voting, remote e-voting is environmentally friendly, real-time counting and processing, and less error prone. Until the time and efforts to vote to reduce the overall voter attendance may progress. But such centralized e-voting system can be vulnerable to hacking, suspicious to fraud, and various manipulations. Such centralized systems are depended on the third-party to conduct the voting process and to tally the votes. Monitoring the actions performed by such systems is difficult. There is no reliability that votes counted by such systems are audited without any manipulation. Moreover, the intruder can get into the central server and alter the votes without any trace of action.

The current centralized-based e-voting system has number of disadvantages:

1. One central organization has full control over the system.
2. If intruder manipulates the data, its traces can be easily eliminated.
3. Lack of transparency.
4. It is difficult to follow the vote to check if it has been counted properly, without revealing the privacy.
5. Security is also important in fair elections as each vote needs to be secured and valued which is often not the case.

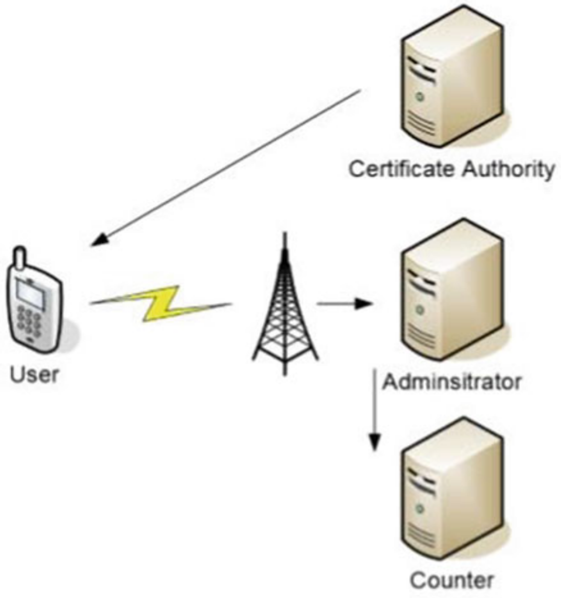
2 Literature Survey

An online voting system has been a hot subject in literature for long. Several voting models have been introduced over the years to protect the privacy of voting information. Various cryptographic tools have been used in e-voting protocol. In some cases, an assigned third-party is involved to make e-voting systems more easily to be implemented and controlled. However, a powerful third-party may also become the vulnerable spot of the whole system. Electronic voting protocol is merged with the blockchain model to design voting protocols making third-party redundant, which provides anonymity and verifiability as well.

A mobile-based voting system is proposed in [1]; here, the user''s votes are safeguarded by using elliptic curve cryptography (ECC) algorithm. ECC has a homomorphic encryption property which helps to keep the user anonymous. This property has made the ECC be more suitable to use in constraint devices. ECC is immediately used for encrypting data in the mobile device without using symmetric cryptography. As a result, it will conserve disk storage as there is no symmetric key encryption cost and encryption processing time will also be reduced while the security strength is still sustained (Fig. 3).

In [2], e-voting system is proposed through which people can vote using their smartphones or website. It is a central server-based system. In this, security is achieved using OTP approach which is usually used everywhere nowadays. Firstly, the user is required to register and authenticate himself using Voter-ID and if valid then by Aadhaar ID also. If the Aadhaar ID is also valid, then he will become a valid

Fig. 3 Mobile voting scheme [1]



voter to cast vote and will have login ID and password (cannot be changed). Voter registration and voting activity are strictly governed by system administrator. After election, voter is allowed to check whether his vote is counted or not on the result page. The benefit of this system is, no other person can cast vote for other person and no multiple voting is allowed. Also, unique identification of user through Aadhar and Voter-ID provides security and flexibility. Being a central server third-party-based system, it is prone to various vulnerabilities.

In [3], author has proposed a blockchain-based system in which the voter can change the vote in case it changes its mind, during the election-time window. Here, a centralized system is responsible for assuring that only qualified people can vote and get into the system, and every eligible user gets a token which takes the form of digital signature. It used Blockchain to store the votes, which was been encrypted using the token.

A Privacy-Preserving Voting Protocol on Blockchain is suggested by Zhang and Huang [4]; it consists of two components: client and smart contracts. The message flow among peers smart contract and ledger client holds the voting procedures that will be implemented by each particular voter. Client holds the voting operations that will be performed by each individual voter. Smart contract maintains the voting logic that requires collaboration and consensus between all voting participants. Here, the voters initially encrypt the vote, after which it is validated. These votes are been decrypted and verified, and if they are found invalid, then devoting is conducted. This process continues until all the votes are valid. At the end, votes are aggregated to tally results (Fig. 4).

In [5], the author has used blockchain to develop an e-voting model. Blind signature is used as encryption algorithm; it is used to hide the voter's choice. Due to the transparency property from blockchain, ballots are visible when they are cast to the blockchain network. This exposes the progress of the election during the voting phase, and may greatly influence the outcome of the election.

In [6], the author has proposed a Ethereum-based e-voting system; it is implemented for a small-scale system like department-level or university-level election.

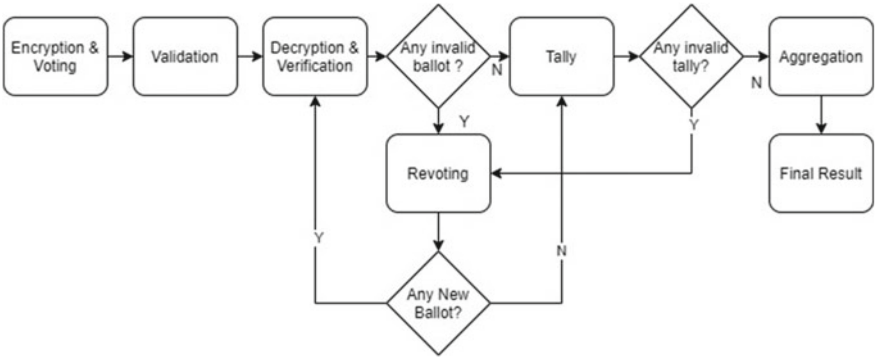


Fig. 4 Process flow [4]

Different code blocks are given which constitutes of smart contracts used for validation. Another smart contract is built to count votes at the end of the election process. The main drawback of the system is that as the number of voters increases, the time taken to cast the vote also increases.

In [7], after verification process, every node produces private and public key pair. The generated public key is distributed to all nodes listed in the system; as a result, every node maintains a public key list of every node. "Get turn method" is used to generate blocks. As a result, collision that can occur in a data transmission network is minimized. But, due to this method, the voter has to wait until its turn to cast vote which may be very tedious in real time situation, as each voter has to wait for its turn.

3 Proposed Methodology

The proposed methodology integrates blockchain paradigm into electronic polling and came up with a feasible and general e-polling idea with a high degree of decentralization. A three-tier authentication protocol is been used to ensure that vote is casted by eligible and verified candidates only. After each authentication round, the voters are certified by digital signature, which is been verified during tally phase. Votes are only been counted if they have digital signature certificate from both authorities (Fig. 5).

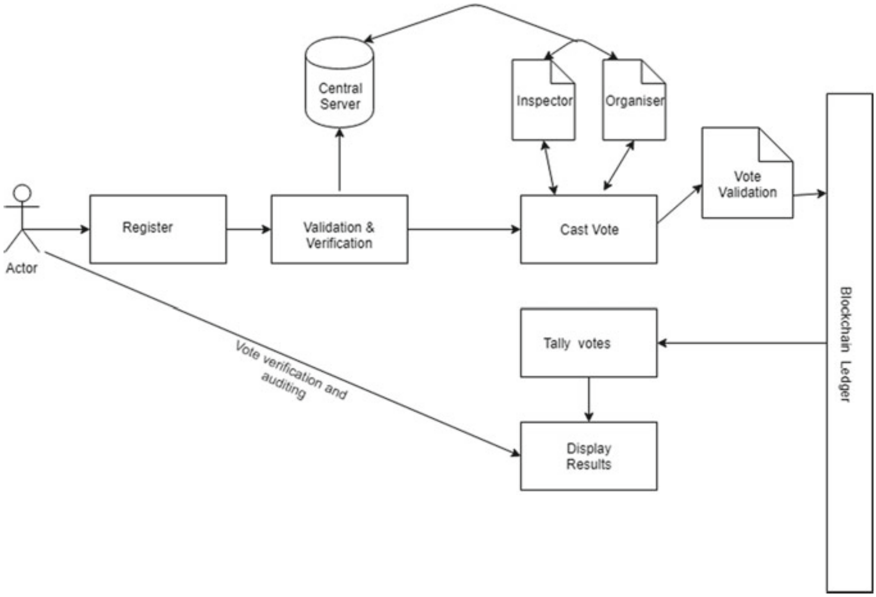


Fig. 5 Architecture diagram of proposed electronic polling agent

The system can be divided into three major modules according to its functionality:

- Identity management.
- Cryptographic privacy.
- Aggregation and auditing.

3.1 Identity Management

Identity management is the major field in blockchain, and this module determines who all can enter the system. Initially, the user needs to register into the system by providing all the required documents and credentials. This information will be stored in a separate private blockchain, which will be broadcasted to the election authority during authentication phase. The requirement of documents and information will vary according to the polling environment. After which the system will check user's identity and eligibility of voting by cross checking it with the data given by the polling organization. For experimental purpose, phone number or email id, OTP methodology will be used for verification. After users are found eligible, then they will be given access to blockchain network and required cryptographic keys will be given to them. Now, they can proceed for polling process.

3.2 Cryptographic Privacy

In any polling system, securing voters identity is the primary motive. No one should know, accept the user that to whom it cast the vote. There should be no traceable link between the vote and the voter. To ensure this kind of anonymity in the system, various cryptographic methodology and algorithm are applied. Blind signature will be the methodology used to ensure vote anonymity in this system.

Three main entities in the blind signature process are

- **Voters**: a set containing all eligible voters.
- **Organizers**: the set of the election organizer, where |organizer| ≥ 1
  The organizer's duties are to hold the election, verify and record eligible voters' information, and associate with voters throughout the election.
- **Inspectors**: the set of all inspectors, where |Inspector| ≤ |Organizer|
  Inspectors are introduced in order to restrict the organizer's power and inspect the organizer's behaviors. Inspectors also interact with voters throughout the election (Fig. 6).

Organizer and Inspector:

- It owns a signing function S'() which is private.
- Its Inverse S() is public.

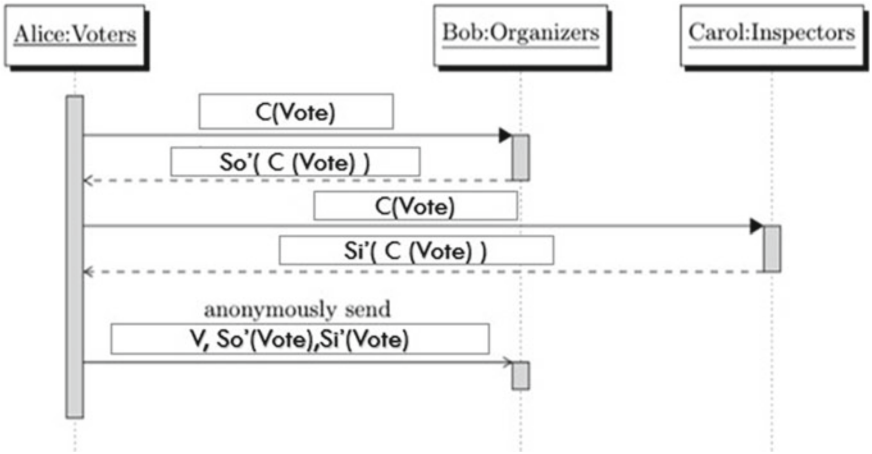


Fig. 6 Sequence diagram of blind signature

- And it has a property S(S'(X)) = X Voter.
- It owns two set of signing function C() and C'(), both are private.
- And it has a property C'(S'(C(Vote))) = S'(Vote).

3.3 Aggregation and Auditing

After the polling window timeouts, all the eligible votes are filtered and counted. With smart contract, it is ensured if the ballot has a proper digital signature of both organizer and inspector. After which the votes are tallied to display the results. After results are been displayed, inverse function of the signatures is given to the voters, with which they can decrypt the votes and audit it to verify if the results are displayed correctly.

4 Conclusion

In this paper, a privacy-preserving system using blockchain is introduced, which prunes out the need of a trusted third-party to tally votes. Blockchain enforces a trust factor into the system, as every transaction in the system is traceable and no one can wipe it out without any trace. And with the use of blind signature mythology, the voters are being verified without their votes getting relieved. The traditional E-voting system lacks this level of transparency. The voters need to trust the system blindly, on the fact that the vote which they casted is recorded and tallied intently. The proposed system has solved this issue by incorporating blockchain technology.

References

1. Ahmad T, Hu J, Han S (2009) An efficient mobile voting system security scheme based on elliptic curve cryptography. Third international conference on network and system security. © 2009 IEEE
2. Sontakke C, Payghan S, Raut S et al (2017) Online voting system via mobile. Int J Eng Sci Comput
3. Hardwick FS, Gioulis A et al. E-voting with blockchain: an evoting protocol with decentralisation and voter privacy. arXiv:1805.10258v2
4. Zhang W, Huang S (2018) A privacy-preserving voting protocol on blockchain. 11th international conference on cloud computing. © 2018 IEEE
5. Liu Y, Wang. An e-voting protocol based on blockchain. Department of Computer Science and Engineering, Southern University of Science and Technology, Shenzhen, China
6. Koc AK et al. Towards secure e-voting using Ethereum Blockchain. Comput Control Netw 978-1-5386-3449-3/18. ©2018 IEEE
7. Hanifatunnisa R, Rahardjo B, Blockchain based e-voting recording system design. 978-1-5386-3546-9/17. © 2017 IEEE