A Cost-Efficient Proof-of-Stake-Voting Based Auditable Blockchain e-Voting System

Trishie Sharma¹, C Rama Krishna² and Arshdeep Bahga³

¹PG Scholar, Computer Science Engineering Department, National Institute of Technical Teachers Training and Research, Chandigarh, India
²Professor, Computer Science Engineering Department, National Institute of Technical Teachers Training and Research, Chandigarh, India
³Director, Cloudemy Technology Labs, Chandigarh, India

E-mail: trishatrix@gmail.com

Abstract. In recent years, blockchain-based systems have emerged powerfully and led to the development of several new and improved applications in terms of increased security, trust, accountability and reliability. One important trust-based application is electronic voting system which still lacks in providing good throughput while also reducing the costs in voting given the deployment of state-of-the-art technologies. So, there is a need to imply an efficient consensus protocol to impart cost-efficiency as well as better performance of a blockchain-based electronic voting system. This paper focuses on boosting up the cost-efficiency in the voting process, while also being auditable, thus, strengthening the trust of voters on the government and lessening the overall costs incurred in voting. In this paper, Proof-of-Stake-Voting is used as consensus protocol which is observed to give a throughput of 4-5K transactions per second. Then its performance is compared with the other existing consensus protocols such as Proof-of-Work and Proof-of-Authority in terms of gas consumption, gas cost, and throughput. It has been shown through the results that there is a significant difference in the total gas cost, with Proof-of-Stake-Voting protocol consuming $3.1 \times 10^{-7}$ Ethers (ETH), as compared to the Proof-of-Work, taking $5.42536 \times 10^{-4}$ ETH and Proof-of-Authority protocols taking $2.49759 \times 10^{-4}$ ETH.

1. Introduction

Safeguarding an election in every democratic country is a critical problem for nation-wide stability. An electronic voting system is the method of accumulating, recording and managing voter data in order to process it digitally in an Electronic Voting System (EVM) [1]. By removing the opportunity to manipulate the ballot, EVM encourages voters to have fair confidence that their vote will count and prevent forgery. While the election commission ensures that the EVM works flawlessly, given the deployment of state-of-the-art technology, open and stable voting cannot be assured.

By enhancing protection and fairness in the framework using blockchain features, situations of mistrust of government officials conducting elections can be avoided. Therefore, there is an enormous opportunity for blockchain-based electronic voting systems (BEV) to give society a trustworthy voting system that can increase transparency in the voting process and, as a result, improve the confidence of the electorate.

In the research literature, there exists various blockchain-based electronic voting systems but they still lack in providing scalability which is the most common limitation of blockchain and is still a matter of concern in various existing blockchain e-voting systems. The scalability of system is limited because
of the network growth due to a large number of Ethereum transactions [2]. Hence, electronic voting using Blockchain technology needs to be practiced at a larger scale [3][4]. Another major limitation of most of the existing voting systems is the high transaction costs due to the use of such consensus protocols that are inefficient with respect to cost and memory.

By considering Proof-of-Stake-Voting protocol as an approach of deploying a voting smart contract on a private Blockchain network, we can provide the system with the ability to reduce the transaction cost [5]. A good throughput of around 4-5K transactions per second (TPS) can also be provided. This research work presents a Blockchain-based electronic voting system which uses the Proof-of-Stake-Voting (PoSV) protocol and shows a huge difference in the total cost of transaction as compared with the existing blockchain-based e-voting systems that use the Proof-of-Work (PoW) and Proof-of-Authority (PoA) protocols.

The major contributions of this paper are as follows: (1) A cost-efficient blockchain-based electronic voting (BEV) system is proposed that uses the PoSV consensus given by TomoChain, which is an Ethereum based blockchain [5], (2) an comparative analysis of the BEV system is provided demonstrating significant performance improvements in terms of gas consumption, gas cost, and throughput as compared to other existing consensus protocols, (3) an implementation case study of a Voting Dapp (Decentralized Application) is provided that comprises functions such as giving right to vote, casting a vote and declaring the winner.

The rest of the paper is organized as follows. The related work is discussed in section 2. The description of the implementation work is given in section 3. The comparative analysis and results are discussed in Section 4. The concluding remarks are presented in section 5.

2. Related Work

This section illustrates the existing work done in the field of improving the performance of electronic voting systems by using blockchain features. It illustrates the working mechanism, strengths and drawbacks of the current literature.

The goal of L. V. C. Thuy et al. [2] has been to allow free, secure elections while maintaining electoral privacy by requiring voters to be tested and cast their votes at their nearest resident voting station, which could probably improve voter turnout. The Ethereum network has been used, with one database handling the system and the other handling all blockchain-related requests. On the Rinkeby test network, implementation has been set up and the final result is independently and publicly auditable. The remaining fund may even be taken back to the Election Authority's blockchain account at the end of the election in order to avoid the depletion of the fund. A. B. Ayed [6] worked on developing a new e-voting system based on blockchain, which can be used in local or national polls where any registered voter may cast a vote using any Internet-connected computer and the blockchain is shown to be legitimate and publicly distributed in such a way that it is unchangeable. As an alternative to current voting approaches, including on-site and distant methods, T. Moura et al. [7] introduced Blockchain-based systems, underlining its essential features, such as being a decentralized trustless node network that relies on state-of-the-art authentication to ensure that transactions are performed properly.

M. Kovic [8] stated that a BEV system would mitigate the risk associated with e-voting due to the decentralized nature of the blockchain, allowing for a tamper-proof e-voting system. In practice, the key feature of a BEV scheme is a truly decentralized e-voting architecture: BEV will only function if no single agency, not even the government, is entirely governed by the e-voting network. N. Kshetri et al. [9] proposed that BEV could have greater mathematically accurate election results and that the costs associated with voting will decrease as it does not entail central authority management. BEV will reduce the cost of paper-based elections, increase voter turnout, and facilitate greater voter transparency and clarity. In addition, online voting in 23 nations was introduced in 2017. R. Hanifatunnisa et al. [10] used digital signatures and hash values to record the voting results at each interconnected electoral station and was able to handle the entire system recording process for each node in block formation in an average of 0.24 seconds and the average data storage capacity of 216.04 bytes for each block.
M. Pawlak et al. [11] defined the use of the Auditable Blockchain Voting System (ABVS) smart agents and multi-agent platform concept, integrating the e-voting mechanism with blockchain technology into a regulated, end-to-end verifiable, non-remote Internet voting system to improve the security of voting by minimizing the intermediary’s request between the voter and the polling station officers, who will undertake all the duties relating to the collection and distribution of votes. As it would not be possible to change them outside the nodes, it would easily detect any attempt to break the e-voting scheme.

It is seen from the extensive literature survey that there are many current voting systems with their significant features, but there is still no improvement in the cost and throughput factors. Existing methods, particularly those based on digital platforms, provide voters with lower transparency, thus impairing electoral confidence [7]. Also, smart contracts are an efficient means of sending information or data in the form of transactions on the blockchain network [11]. Although blockchain has evolved as one of the most prominent technologies which helps in securing systems through the use of decentralized architectures and consensus mechanisms, obtaining a minimized cost of entire system along with a better throughput still remains a topic under continuous research. Hence, the proposed BEV system uses a consensus protocol that is based upon voting of the participating staking nodes.

In the next section, the architecture of the proposed BEV system is described along with the performance metrics that are used in order to compare different consensus protocols.

3. Proposed BEV System using Proof-of-Stake-Voting Protocol

This section explains how the proposed system is deployed and run on a private Blockchain network.

3.1. System Architecture

In the proposed system, the voter is authenticated at the polling station and vote is casted by using the Voting Dapp. The votes are sent in the form of tokens to the TomoChain Blockchain network to process the transactions. The results are then shown on the dashboard where the votes and results can be verified and audited. Figure 1 depicts the architecture of the proposed BEV system.

![Architecture of Proposed BEV System](image)
The work flow of the proposed voting system is displayed in figure 2 and a brief explanation of the steps involved in this work flow is provided in the following:

![Work flow of Proposed BEV System](image)

**Figure 2. Work flow of Proposed BEV System**

3.1.1. Create Voter Accounts
Voter accounts have been created using ‘Tomochain’ in Geth [12] console for proof-of-stake-voting consensus. Voter accounts for PoW as well as PoA protocols have been created using both the Geth console as well as the Metamask interface [13]. A total number of 50 accounts of users have been created and tested for the performance metrics.

3.1.2. Design the Voting Dapp
The voting decentralized application is created using HTML/CSS for designing the interface and JavaScript for scripting of the web page. Two portals have been created:

- **Admin portal**: For creating ballot for a particular polling station, giving voting rights to voters. Figure 3 shows the user interface of the admin portal of Voting Dapp. A total number of 10 candidates have been created for this Voting Dapp.

![Voter Portal of Voting Dapp](image)

**Figure 3. Voter Portal of Voting Dapp**
Voter portal: For viewing own registration details (voter address, voting rights, vote counted or not, etc.), candidate details (ID, name) and result declaration. In figure 3, the admin portal displays the following:

- **Voting Contract Address**: The address where the smart contract resides on the Ethereum blockchain.
- **Chairperson Address**: The address of the chairperson, who is an authorized electoral official who is administering the voting.
- **Your Address**: The account address of the voter who is logged in to the Voting Dapp.

Once a voter logs in, his/her corresponding account details (account balance, voting rights, whether vote is casted or not, number of candidates and number of voters) are fetched as per the contract deployment and then displayed in the portal.

- **Your Balance**: This is the balance that every voter account needs in order to perform a transaction, i.e., to cast a vote. By default, 10 ETH have been assigned by the electoral officials to all the voter accounts.
- **Can You Vote**: This tells about whether the voter logged in has been provided the voting rights or not. A ‘0’ value means the voter does not have a voting right and ‘1’ means that voter has the right to vote.
- **Your Voting Weight**: The weight tells whether the logged in voter has already casted a vote or not. A value ‘0’ means that the vote has not been casted yet whereas ‘1’ signifies that his/her vote has been casted.

Apart from the above details, the total number of candidates and voters are also shown in the portal.

### 3.1.3 Set up the Consensus Protocol Type

As the proposed system is compared with the existing consensus protocols, which are, Proof-of-Work and Proof-of-Authority, different mechanisms have been used for each of them.

- **Proof-of-Work**: Genesis file has been created using ‘puppeth’ and definition of the accounts used are provided in this file. The accounts have been connected with Metamask by giving the RPC URL of localhost:8545.
- **Proof-of-Authority**: Genesis file has been created using ‘puppeth’ and definition of the accounts used are provided in this file. The accounts have been connected with Metamask by giving the RPC URL of localhost:8545.
- **Proof-of-Stake-Voting**: Genesis file has been created using TomoChain Testnet in which the Proof-of-Stake-Voting is applied. Connection to the ‘testnet’ has been given under ‘networks’ in the truffle configuration file with ‘network ID: 89’, mnemonic and RPC URL of the ‘Tomo Testnet’.

### 3.1.4 Set up the Mining/Validator Nodes

The number of full nodes for each organization is different, but, based on the existing private blockchain implementations, a key assumption of 10 nodes represents a reasonable average and portrays the realistic costs for almost all of the implementations [14]. Taking this under consideration, 10 mining nodes have been set up for PoW consensus and 10 sealing and validating nodes have been set up for PoA consensus. For both PoW and PoA, nodes were created by using Geth console. 5 master nodes and 5 other nodes, in slave mode, have been set up in the case of Proof-of-Stake-Voting protocol and for creating the nodes, Tomo console has been used.

### 3.1.5 Deploy the Voting Dapp

Smart contract has been created for electronic voting and then it has been deployed on each type of consensus protocol. Performance of each protocol is measured based on the pre-defined metrics (transaction cost, gas cost and TPS) which are described in the next section.
3.1.6. Voters Cast their Votes
Each voter will be authorized at the respective polling station. Voter casts his/her vote using the voter portal which is the Voting Dapp. After voting, the voter receives the VVPAT which contains the voter’s address and a unique and verifiable transaction hash for his/her vote.

3.1.7. Verification of Votes and Voting Results
Using the transaction hash, a voter can verify whether his/her vote is casted correctly or not. A set of instructions on how to verify the vote with transaction hash provided at the main voting portal or on the registered mobile number after voting is done.

3.2. Performance Metrics
The performance of three consensus protocols are compared on the basis of following three parameters as described below:

3.2.1. Transaction Cost and Gas Cost
Smart contracts are compiled into bytecode, and then deployed and executed as per the transaction processing mechanism. Every instruction executed is charged a fee to compensate for resources that are spent and to prevent potential Denial of Service (DoS) attacks. This fee is pre-paid by transaction sender based upon the transaction. There are two factors of the fee in notion of gas, i.e., gasLimit and gasPrice. The ‘gasLimit’ is the maximum amount of gas that is available to the transaction, and the ‘gasPrice’ converts gas units into ETH value (gasLimit * gasPrice), which is the exact fee paid by the transaction sender. Ideally, every transaction sender has to define gasLimit and gasPrice, and has to pay the amount of Ether before execution [15].

- transactionCost is the number of gas units used in a transaction
- Gas Cost = transactionCost * gasPrice

If, after transaction execution, there is unused gas left, the remaining part will be refunded back to transaction sender in ETH in the same rate as gasPrice. In the case of PoSV protocol, TomoChain is used which uses its own cryptocurrency i.e., TOMO [5].

\[1 \text{TOMO (on 7th September, 2020)} = 0.0018081006 \text{ETH}\]

The total amount of gas and gas cost involved in completing all the functions are measured for result comparison. The functions that are considered are:

- **Right To Vote**: The administrator would run this function to allow a voter to be able to cast a vote.
- **Vote**: The voters would click on the ‘Vote’ button on the portal to cast their poll.
- **Winner**: This function would calculate the polling results and display them on the portal or dashboard.

3.2.2. Transactions Per Second (TPS)
The term ‘Transactions Per Second’ is commonly used when evaluating a blockchain network in terms of throughput and sometimes, scalability of the network. It is measured by observing the number of transactions the network is able to process in one second. For this, the total time taken for processing one transaction is taken and based on that, the number of transactions that can be processed in one second, is obtained.

The following section presents the results along with the comparative analysis for PoA, PoW and PoSV protocols as per the defined performance metrics.

4. Results and Discussion
The proposed system introduces a concept of a cost-efficient Blockchain-based E-voting platform with a better throughput. The performance of this proposed system is measured on a system with 16 GB RAM and i5 processor in terms of the amount of gas incurred, gas cost, and throughput. The throughput is calculated in terms of Transactions Per Second (TPS). The results obtained are shown in Table 1 and 2.
Table 1. Comparison of Transaction Time and Throughput (TPS) for Proposed PoSV-Based BEV with PoW and PoA.

| Consensus type | Time taken per transaction (μs) | Transactions Per Second (TPS) |
|----------------|---------------------------------|-----------------------------|
| PoW            | 2535                            | 395                         |
| PoA            | 306.11                          | 2390                        |
| PoSV           | 214.168                         | 4669                        |

Table 2. Comparison of (a) Transaction Costs and (b) Gas Costs of Proposed PoSV-based BEV System with PoW, PoA.

| Consensus Type | Right to Vote | Vote | Winner | Total    |
|----------------|---------------|------|--------|----------|
| (a)            |               |      |        |          |
| PoW            | 184956        | 246607 | 110973 | 542536   |
| PoA            | 83646         | 114561 | 51552  | 249759   |
| PoSV           | 52668         | 81928  | 36867  | 171463   |
| (b)            |               |      |        |          |
| PoW            | 0.000184956   | 0.000246607 | 0.000110973 | 0.000542536 |
| PoA            | 0.000083646   | 0.000114561 | 0.000051552 | 0.000249759 |
| PoSV           | 0.000000096   | 0.000000148 | 0.000000066 | 0.000000310 |

4.1. Throughput (TPS)
From the Table 1, it can be seen that the proposed E-voting system on Blockchain network was able to handle the highest number of transactions with PoSV protocol as compared with the PoW and PoA protocols. With PoSV protocol, the system gave a throughput of 4669 TPS, PoA achieved 2390 TPS whereas PoW could handle only 395 TPS. This has been obtained by taking the observations when running the Blockchain network to note the time taken for handling a single transaction. Then, this time is converted in terms of the number of transactions that can be handled in one second. The reason behind the high throughput achieved by PoSV protocol is its block confirmation time of 2 seconds [5], as compared with PoA (Clique) with block time of 15 seconds [16] and PoW with around 10 minutes [17].

4.2. Transaction and Gas Cost
Table 2 shows the different amounts of gas units for different functions and a comparative graph has been shown in figure 4 on the basis of the total gas unit for processing all the functions (Right to Vote, Vote and Winner).

Similarly, on the basis of the gas units incurred, the gas cost is calculated (gasUnits * gasPrice). Here, the gas price is shown in terms of Ether where:

\[
1 \text{ ETH} = 10^9 \text{ GWei or } 1 \text{ GWei} = 10^{-9} \text{ ETH}
\]

Here, Wei is the smallest denomination of Ether [18]. As the system is deployed on TomoChain network that uses PoSV protocol, the gas costs have been observed and calculated in their cryptocurrency (TOMO) and then converted into Ether. This causes the overall cost to drop, so even if there are large amounts of gas units used, the overall gas cost would not be very high. This effect benefits in increasing the cost-efficiency of the system.
5. Conclusions
This paper focuses on deploying a blockchain-based voting system that increases the throughput, while reducing the total gas consumption and ultimately the overall gas cost. The total gas cost of this BEV Dapp with PoSV protocol is seen to be very less (3.1 x 10^{-7} ETH) as compared to the PoA (2.49759 x 10^{-4} ETH) and PoW (5.42536 x 10^{-4} ETH) protocols. The PoSV protocol also gives a good throughput of 4669 transactions per second which would help to enhance the scalability of the system in a private Blockchain network, to some extent.

6. References
[1] Santhosh M, Kavitha S, Keerthana R, Suganya L and Krishnakumar S Electronic voting machine using internet 2016 Int. J. Comm. and Comp. Tech. 4 2 pp 4025-28
[2] Thuy L V C, Minh K C, Bao C D L and Nguyen T A Votereum: an ethereum-based e-voting system 2019 IEEE-RIVF Int. Conf. on Computing and Communication Technologies (Danang Vietnam) (New York City: IEEE) pp 1-6
[3] Shahzad B and Crowcroft J Trustworthy electronic voting using adjusted blockchain technology 2019 IEEE Access 7 pp 24477-88
[4] Ramadhani A M, Hong S G, Kim N and Ryu S A study on the conceptual model of an e-voting system based on blockchain 2019 Internet E-Commerce Research 19 2 pp 99-111
[5] TomoChain R&D Team TomoChain: masternodes design technical white paper version 1.0 2018 (Singapore: TomoChain Pte. Ltd) pp 1-19
[6] Ayed A B A conceptual secure blockchain-based electronic voting system 2017 Int. J. Net. Sec. & Its Applications (IJNSA) 9 3 pp 1-9
[7] Moura T, Gomes A Blockchain voting and its effects on election transparency and voter confidence 2017 Proc. of the 18th Annual Int. Conf. on Digital Government Research (New York) (New York: ACM) pp 574-575
[8] Kovic M Blockchain for the people - blockchain technology as the basis for a secure and reliable e-voting system 2017 ZIPAR Discussion Paper Series vol 1 (Zurich: ZIPAR) pp 1-25
[9] Kshetri N and Voas J Blockchain-enabled e-voting 2018 IEEE Soft. 35 4 pp 95-99
[10] Hanifatunnisa R and Rahardjo B Blockchain based e-voting recording system design 2018 11th IEEE Int. Conf. on Telecommunication Systems Services and Applications (Indonesia) (New York: IEEE) pp 1-6
[11] Pawlak M, Poniszewska-Mara´nda A and Kryvinska N Towards the intelligent agents for blockchain e-voting system 2018 The 9th Int. Conf. on Emerging Ubiquitous Systems and Pervasive Networks Procedia Computer Science (Belgium) (Netherlands: Elsevier) pp 239–246
[12] ethereum/go-ethereum GitHub 2020 (https://github.com/ethereum/go-ethereum) [Last accessed: 29-Sep-2020]
[13] Introduction | MetaMask Docs 2020 Docs.metamask.io (https://docs.metamask.io/guide/) [Last accessed: 29-Sep-2020]
[14] Total cost of ownership for blockchain solutions 2019 Global: Ernst & Young p 7 (https://www.ey.com/Publication/vwLUAssets/ey-total-cost-of-ownership-for-blockchain-
solutions/%24File/ey-total-cost-of-ownership-for-blockchain-solutions.pdf) [Last accessed: 10-Sep-2020]

[15] Liu C, Gao J, Li Y, Wang H and Chen Z. Studying gas exceptions in blockchain-based cloud applications 2020 J. of Cloud Comp.: Advances, Systems and Applications Springer 9 35 pp 1-25

[16] Szilágyi P. EIP-225: clique proof-of-authority consensus protocol (https://eips.ethereum.org/EIPS/eip-225) [Last accessed: 23-Sep-2020]

[17] Nakamoto S. Bitcoin: a peer-to-peer electronic cash (https://bitcoin.org/bitcoin.pdf) [Last accessed: 23-Sep-2020]

[18] Wood G. Ethereum: a secure decentralised generalised transaction ledger Petersburg version 3e2c089 2020 Yellowpaper (https://ethereum.github.io/yellowpaper/paper.pdf) [Last accessed: 22-Sep-2020]