International Journal of Aquatic Science
ISSN: 2008-8019
Vol 12, Issue 02, 2021

Establishing Blockchainforvoting System Application In Local Network And Ropsten Test Network

Vairam T[1], Sarathambekai S[2], Balaji R[3]

[1,2,3]*Department of Information Technology,PSG College of Technology,Coimbatore, India*

ABSTRACT: Organizing an electronic voting system which accomplishes the genuinenecessities of legislatures has been a challenge for a long time. Conducting the free, systematic and impartial election is the vital goal of every democracy nation. Every country follows a different voting system from old paper ballot system to Electronic voting system. There facing a many problem in these voting systems. The main problem is location and the accessibility, people are suffering to go to their native place polling booth for casting their vote. This needs to be considered as every people`s vote plays significant role in deciding the right leaders. Blockchain technology offers the transparency and security requisites for the impartial election. It is a complete decentralized, immutable ledger system. The online voting system allows the voters to cast their vote from any place at any time which leads to increasing the voter participation count. The objective of the paper is to create a voting system which provides transparency and security using Blockchain technology, and deploy the smart contract in Ganache tool for local network and Ropsten to test the application.

Keywords: Blockchain, Smart Contract, Voting system, Truffle, Ropsten

1. INTRODUCTION

Generally, a single organization maintains the database. This makes the single organization, a central authority with complete control over it. The central authority has the facility to fiddle with the database and influence the data. The organization maintains the database for two purposes one is for storage purpose which doesn't require any modification of the data. The other one involves monetary matters or sensitive data such as voting, account transaction details which requires many people to involve in the data entry and modification.

Though the organization enable only the authenticated people to access the central database still the hackers will find a way to access the database easily. To evade such circumstances, blockchain consider the database as public ledger which provide every user to store their data in the database. Nevertheless, the user data must always be updated to keep consistency. The consensus algorithm is being used in blockchain technology in order to maintain a consistent decentralized database. The Blockchain is one of the evolving technologies and plays a major role in many fields such as healthcare, supply chain management, market monitoring etc. [1& 2].

Different types of voting mechanism are followed across the world [3]. Voice vote, rising vote, show of hands, ballot vote (recorded) are the traditional voting system. E-Voting (Electronic Voting) denotes that an electronic equipment is used to troupe votes in an election. The significance of e-voting is to proliferate the participation, to reduce the expenses of organizing elections and to improve the accurateness of the results.

The security civic observing the Electronic Voting Machines (EVM) as defective because the corporal security is required for such systems. The voting machine may damage due to physical access by a person hence affects the existing vote cast on the machine. In general, the EVM has less security and integrity than online voting system. The online voting system also enable the voters to cast the vote using their personal device like mobile, laptop etc. hence the secrecy is maintained and there increases a number of participants to cast the vote. Blockchain is Distributed Ledger Technology (DLT) which has digital asset unchangeable and translucent through the usage of decentralization and cryptographichashing."Blockchain-Based E-Voting System"[4] addressed the features of blockchain technology as follows:

a) Distributed ledger enables no single point of failure.
b) New transaction can be inserted into the ledger by anyone who is having the distributed control.
c) The block is created or inserted based on its previous block details.
d) Consensus algorithm plays a major role in constructing the new block and performs transaction in it.

The objective of the paper is to create a voting system which provides transparency and security using Blockchain technology. To explore the various available options in the blockchain technology and to choose the right platform to develop the voting system. With blockchain based voting, the voters turn up might also increase as people can cast their vote from any place at any time, making this as a perfect alternate to the current voting system. And also this improves the security and trust of the voting system.

This paper is organized as the literature review is explained in section 2, the proposed architecture is discussed in section 3 and the implementation details and the conclusion is discussed in section 4 and section 5 respectively.

2. LITERATURE SURVEY

There are many researchers shown their interest to implement a novel research work in the area of block chain technology as this becoming the mandatory of many applications.[4] proposed the permissioned block chain for E-voting system which uses the smart contracts to ensure the security and cost-efficient election. Also worked in BEV, the authorized voters can cast a ballot using digital currency. Tamper-proof audit trails is created by enabling by block chain for voting which makes a perfect way for casting vote. In [5], tabulated the deployment of blockchain based solutions for various level such as corporate, community, city and national voting. Also addressed Block chain enabled voting (BEV) opportunities and challenges.

[6] analyzed the I-voting system for various countries. "E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy" [7], a prospective e-voting protocol is proposed that utilizes the blockchain as a transparent ballot box. Comparison of commercial block chain e- voting protocols was carried in their work. They considered Bitcongress[8], Follow My Vote[9] and TIVI[10] commercial protocol for comparison.

[11] Proposed the Open Vote Network which is best suited for boardroom elections, this open vote network does not depend on any trustworthy authority to calculate the number of votes. The reason behind this is, the Open Vote Network is a self-tallying protocol, and every voter is in under the control of their privacy. The consensus mechanism is used to secure the Ethereumblockchain. [12] addresses the drawbacks of two-round decentralized voting protocols by enabling the election result using recovery round also considered the computational security proof of ballot secrecy. The blockchain technology could also be used in open science.

[14] reviewed how an open science can be benefited from the Blockchain. The blockchain review based on systematically was done by [15] considered the theme for reviewing the blockchain and the few research themes are economic benefits and fintech revolution. The detailed review on blockchain technology with respect to various applications was done by [16]. The most demanding applications such as Internet of Things and Healthcare require the role of blockchain technology. From all these research works, the integration and usage of blockchain technology into many applications to improve the security and trust of the system can be seen.

3. PROPOSED SYSTEM

The voting system architecture is shown in Figure 1. The whole system can be divided into four main activities.

Registration: Before participating in voting, each valid voter is given a public address and a private key, which will be used later for authentication. Each voter account is filled with enough ethers to carry out one single transaction. Both public address and private key should not be revealed to anyone. This helps the voters to cast their votes anonymously.

Authentication: The voting process starts with Authentication. Each valid voter is given an address and key for verifying their identity. Each voter is asked to enter his public address and private key (authentication credentials). Once the credential is valid, the voter is allowed to cast their vote.

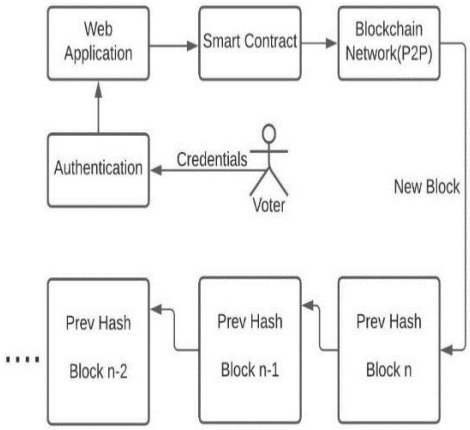

Figure 1: Voting system architecture

Voting: Once authenticated, they can choose a candidate from the list of available candidates by using the Frond end application. Only one chance is being given to every voter. To cast a vote, a function call is made to the deployed smart contract with the candidate id.

Results: The transaction of the block is successful only when the transaction id conformed by the miner (any one) and acknowledged by all the miners.

3.1 Design Considerations

The system is designed with these following points in consideration.

1. Only one chance is given to the voter to prevent double voting.
2. Only eligible voters are enabled to cast the vote by checking their identity.
3. While vote counting, the system should not depend on a single authority.
4. The privacy of the voters should be maintained.
5. The stored votes should be verifiable and tamper proof.

3.2 EthereumBlockchain Network

For implementing this proposed work an Ethereum block chain network is used. It is a decentralized open source blockchain network featuring smart contract functionality. In Ethereum platform, the crypto currency used here is Ether (ETH). It uses Proof of Work as the consensus algorithm where the one who can quickly solve a problem using the computation power can add a new block to the network. The blockchain arrangement takes care of vote tampering problems.

[13] used the Ethereum block chain network for online voting application. In blockchain, each and every block is chained with its next block and its previous block. Hence if the hackers tries to access the Block N then it will be notified to Block N+1, and the changes in Block N+1 also relects in Block N+2 and so on. The hash value of Block N+1 is computed using (1)

$$Hash(Block(N+1) = f(timestamp + Hash\big(Block(N)\big) + Payload + (Hash(Merkle\ Root) + Target + Nonce) \quad (1)$$

4. EXPERIMENTAL RESULTS

Ganache is used to create aEthereumblockchain network in the local machine and the smart contract is deployed in the network using the Truffle framework. Ganache provides 10 account with 100 fake ethers which can be used to test the working of the developed application. Figure 2 shows the deployed smart contract in Ganache.

The Ropstentestnet allows blockchain developers to test their work in a live setting, but without the need for real ether. Instead of real Ether, here Ropsten-ether is used. This is the only proof of work test network available. The working of Ropstentestnet is more or less similar to that of main Ethereum network. Figure 2 shows the deployed smart contract in Ropsten.

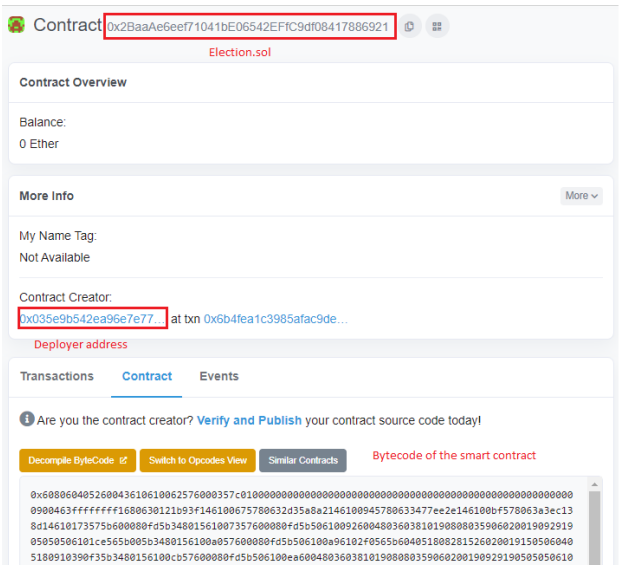

Figure 2: Deployed smart contract

When the smart contract is triggered Migrations are used to update the blockchain. A numbered JavaScript is used, a migration which is created for every smart contract. The migration or the numbered JavaScript file is being called automatically by Truffle

framework. For each migration, certain amount of ether is spent from the account which is used to deploy the smart contract in the blockchain network as shown in Figure 3. The frond end application is deployed in Heroku, which is a cloud platform as a service (PaaS) supporting several programming languages.

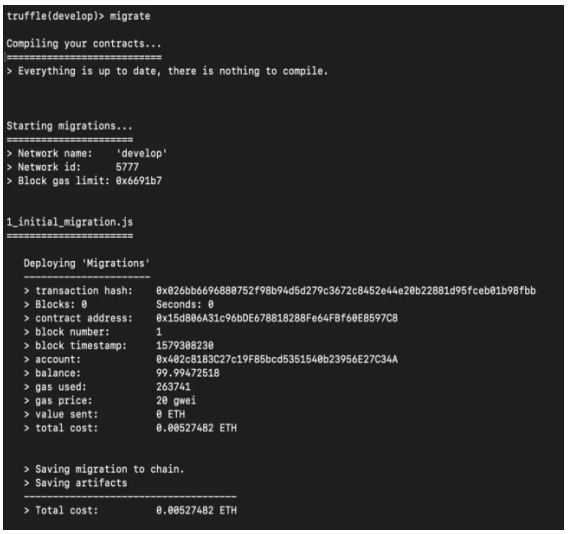

Figure 3: Migration using Truffle

Figure 4 and Figure 5 represents the user interface for proposed system before voting and after voting respectively. When the user clicks the vote button, metamask will ask the user for confirmation. On confirming, the transaction is added to the Pending transaction pool of Ropstentestnet. Ropstentestnet uses Proof of work as the consensus algorithm. The miner should make tons of computation to find the right hash, to add the block in the network. The miner will be rewarded once the blocks gets added to the network. When the transaction gets verified, the page gets reloaded to show the updated results. After performing the transaction, the confirmation has been notified through metamask. Figure 6 shows the meta mask transaction conformation for the transaction.

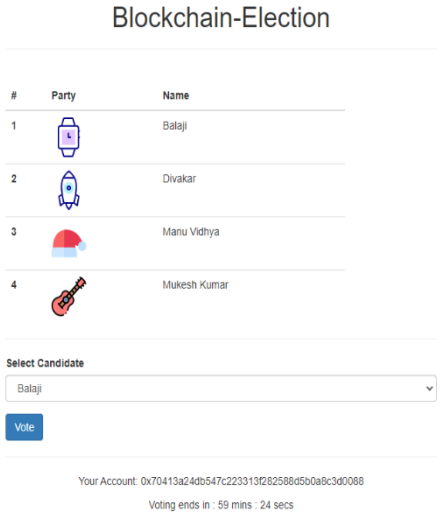

Figure 4: Before voting (UI)

International Journal of Aquatic Science
ISSN: 2008-8019
Vol 12, Issue 02, 2021

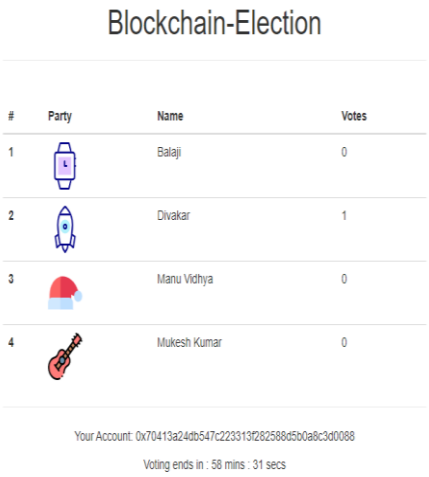

Figure 5: After voting (UI)

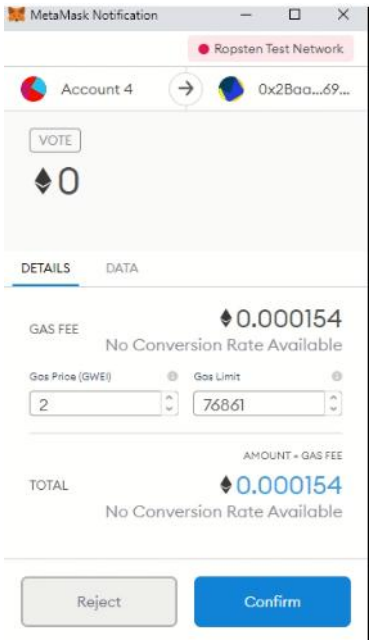

Figure 6: Metamask transaction confirmation

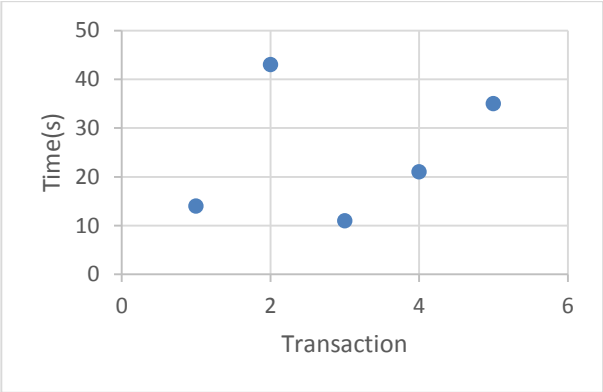

Figure7: Time taken to verify transaction for Ropsten Network

Figure 7 shows the graphical representation of time taken for every transaction. The time in seconds and transaction represented in y-axis and x-axis respectively. The time range for transaction verification is 15 to 45 seconds.From the Figure 7, it is inferred that the time taken for verifying the transaction in done between 15 seconds to 45 seconds. Hence the blockchain ensure the security as well as quick transaction. The Table 1 shows the transaction and its hash value generated during the transaction execution. The unique and strings of character is generated for each transaction. This will ensure the secured transaction in the Ropsten Network. The corresponding transaction details includes transaction number, block number, timestamp, transaction hash value and the amount are shown in Table 2

Table 1 Transaction hash for Ropsten Network

Txn	Txhash
1	0xa00549e6d2e81757215b44bd89a6470e0fb 6f0e2886115b5b76617b177f435cb
2	0x2c2a17fde6bc617a6fa80248b28f5f94be 49013d025ebb5dbe7195795db3ff94
3	0x4d6874707128cab51b05793cefe890ea b58e3082e1420231df2c42f8f46e630a
4	0x3742410ce789cb54659eeafc70eff9e9a 2c6400656b0586f70e92425d3a136e2

Table 2 Transaction Details for Ropsten Network

Tx	Block	Timestamp	From	TxnFee (ETH)
1	8932241	1603435406	0x035e9b542ea96e7e77299d5eb0ac1a1fae7778cc	0.000105986
2	8977670	1604088859	0x211beaba57569ece034b65426afc4083c3f4faa5	0.002219074
3	9062805	1605282651	0xe41a8b1d4c4222a67e41f38d146a9313fb4a2249	0.000051241
4	9062855	1605283220	0x960ea8ec7730925ec9484a80a1b20e87842db306	0.000102482

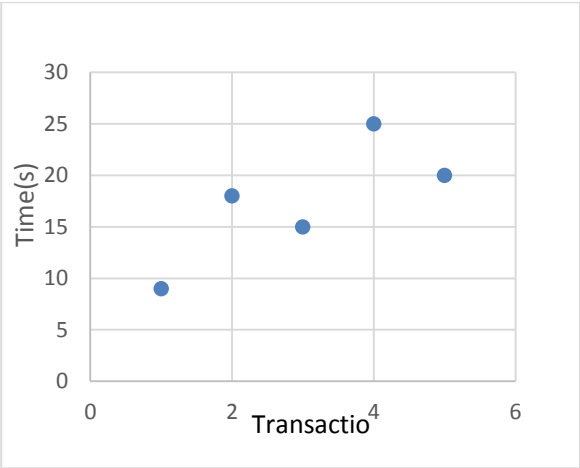

Figure 8: Time taken to verify transaction for Local Network

The Figure 8 shows the graphical representation of time taken for every transaction for Local Network. The time in seconds and transaction represented in y-axis and x-axis respectively. Figure 8, it is observed that the time taken for performing the transaction in local network is less than for the Ropsten network. The Table 3 shows the transaction and its hash value generated during the transaction execution The generated transaction Hash value ensure the security in Local block chain network. The transaction details includes transaction number, block number, timestamp, transaction hash value and the amount are shown in Table 2

Table 3 Transaction hash for Local Network

Txn	Txhash
1	0xa00549e6d2e81757215b44bd89a64 70e0fb6f0e2886115b5b76617b177f435cb
2	0x2c2a17fde6bc617a6fa80248b28f5f9 4be49013d025ebb5dbe7195795db3ff94
3	0x4d6874707128cab51b05793cefe890 eab58e3082e1420231df2c42f8f46e630a
4	0x3742410ce789cb54659eeafc70eff9e9a 2c6400656b0586f70e92425d3a136e2

Table 4 Transaction Details for Local Network

Tx	**Block**	**Timestamp**	**From**	**TxnFee(ETH)**
1	8932241	1603435406	0x035e9b542ea96e7e77299d5eb0ac1a1fae7778cc	0.000105986
2	8977670	1604088859	0x211beaba57569ece034b65426afc4083c3f4faa5	0.002219074
3	9062805	1605282651	0xe41a8b1d4c4222a67e41f38d146a9313fb4a2249	0.000051241
4	9062855	1605283220	0x960ea8ec7730925ec9484a80a1b20e87842db306	0.000102482

5. CONCLUSION & FUTURE WORKS

This paper provides an Electronics voting system which is deployed on Ethereum network. Many research works proved that the blockchain technology helps in improving the existing system hence it also provides a better way to conduct the Election. It also used to evade the drawbacks of centralized voting systems. This Electronic Voting system is implemented using Local network and Ropsten test network to check the working of the voting system.
After the Votes are casted by the voters, it is stored as immutable and tamper-proof. This addresses the security issues with the current EVM system. Though it provides transparency, as the transactions are visible to everyone, it conserves voter's confidentiality and secrecy. It helps in announcing the result fast. It takes more than 2 weeks to announce result in the current system. The voting results are publicly auditable. In future the frontend UI of the application can be improved to show the election statistics and any other authentication methods can be integrated to further add security and trust to the voting system.

6. REFERENCES

[1] Xu, M., Chen, X. & Kou, G. A systematic review of blockchain. FinancInnov5, 27 (2019). https://doi.org/10.1186/s40854-019-0147-
[2] Fran Casino, Thomas K.Dasaklis, ConstantinosPatsakis, " A systematic literature review of blockchain-based applications: Current status, classification and open issues", Telematics and Informatics, 36, pp.55-81, 2019.
[3] https://www.britannica.com/topic/electronic-voting Types of Voting
[4] Fridrik .P. Hjalmarsson, Gunnlaugur .K. Hreidarsson, "Blockchain-Based E-Voting System", in School of Computer Science Reykjavik University, Iceland
[5] NirKshetri and Jeffrey Voas, "Blockchain-Enabled E-Voting", in IEEE Software,doi: 10.1109/MS.2018.2801546
[6] Ahmed Ben Ayed, "A Conceptual Secure Blockchain- Based Electronic Voting System", in International Journal of Network Security & Its Applications (IJNSA) Vol.9, No.3
[7] Freya Sheer Hardwick, ApostolosGioulis, Raja NaeemAkram, and KonstantinosMarkantonakis, "E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy", in ISG-SCC, Royal Holloway, University of London, Egham, United Kingdom
[8] BitCongress. Control the world from your phone. [Online]. Available:http://www.bitcongress.org/BitCongress\Whitepaper.pdf
[9] Rana, A., Nigam, U. and Jain, D. "Insider Threats: Risk to Organization", IARS' International Research Journal. Vic. Australia, 2(1) 2012. doi: 10.51611/iars.irj.v2i1.2012.18.
[10] FollowMyVote.com, Tech. Rep., 2017. [Online]. Available: https: //followmyvote.com
[11] "Tivi - verificable voting: Accesssible, anytime, anwhere," TIVI, Tech. Rep., 2017. [Online]. Available: https://tivi.io
[12] P. McCorry, S. F. Shahandashti, and F. Hao, "A smart contract for boardroom voting with maximum voter privacy," in International Conference on Financial Cryptography and Data Security. Springer, 2017, pp. 357–375.
[13] Punhani, R., Kakkar, A. and Jain, D. "Implementation of ISMS and its Practical Shortcomings", IARS' International Research Journal. Vic. Australia, 2(1) 2012. doi: 10.51611/iars.irj.v2i1.2012.19.
[14] D. Khader, B. Smyth, P. Y. Ryan, and F. Hao. "A fair and robust voting system by broadcast". In 5th International Conference on Electronic Voting, volume 205, pages 285–299. Gesellschaftf¨urInformatik, 2012.
[15] Shalini Shukla, A.N. Thasmiya, D.O. Shashank, H.R. Mamatha. "Online Voting Application Using Ethereum Blockchain", 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2018.
[16] Stephan Leible, Steffen Schlager, Moritz Schubotz and Bela Gipp, " A Review on Blockchain Technology Projects Fostering Open Science", Fronties in Blockchain, Vol 2, pp.1-28, 2019.
[17] Min Xu, Xingtong and Gang Kou, " A Systematic review of blockchain", Financial Innovation, Vol. 4 pp1-14, 2019.
[18] Bhabendu Kumar Mohanta et al, " Blockchain Technology: A survy on Applications and Security Privacy Challenges", Internet of Things,pp1-20, 2019.