As per UGC guidelines an electronic bar code is provided to seure your paper

International Journal for Modern Trends in Science and Technology, 8(05):399-404, 2022

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0805059
Available online at: http://www.ijmtst.com/vol8issue05.html

Polling System using Blockchain

Himandri Sharma[1] | Sonal Bhatia[1] | Hritik Dua[1] | Harsh Agarwal[1] | Dr. S.B. Kumar[2]

[1]Department of Electronic and Communication Engineering, Bharati Vidyapeeth's College of Engineering, India.
[2]Assistant Professor, Department of Electronic and Communication Engineering, Bharati Vidyapeeth's College of Engineering, India.
Corresponding Author Email ID: himandrisharma27@gmail.com

To Cite this Article
Himandri Sharma, Sonal Bhatia, Hritik Dua, Harsh Agarwal and Dr. S.B. Kumar. Polling System using Blockchain. International Journal for Modern Trends in Science and Technology 2022, 8(05), pp. 399-404.
https://doi.org/10.46501/IJMTST0805059

Article Info
Received: 16 April 2022; Accepted: 15 May 2022; Published: 19 May 2022.

ABSTRACT

A comparative study for improved security in Polling System using Blockchain with an efficient and smoothly implemented workflow for users. Current voting systems like ballot box voting or electronic voting suffer from various security threats such as DDoS attacks, voting booths, vote-rigging and fraud, malware attacks, etc. And it requires a lot of paperwork, human resources, and time. This creates a sense of distrust between existing systems and voters. Results show the parameters that have been improved from the existing solutions in the real world.

KEYWORDS: Blockchain, ethereum, smart contracts, E-voting, solidity

1. INTRODUCTION

Trust, Transparency and mediators are the three biggest challenges we face in the present, as we are forced to trust banks to get us our money to buy. Rely on these third parties to ensure our privacy and security as per our data. So anywhere in the modern world. The need to trust these organizations that act as mediators. These three major problems can be solved with an invention called blockchain.

Blockchain is a system for recording information in a way that makes it impossible to change, hack, or cheat the system. Blockchain is a dynamic digital ledger that is distributed across a network of computers on the blockchain. Each block on this blockchain contains a number of transactions, and each time a new transaction occurs in a blockchain, its record is added to each participant's ledger. The block consists of 3 main components: Data / Information section - containing transaction information, Hash- Unique block ID, Previous Hash - Previous block Hash.

As in Blockchain, each block has a hash of its previous block, so if anyone tries to tamper data in one block then the block hash will be changed. So there is need to change the 'previous hash' of the next block. By doing so, the current hash of the next block will also change. Eventually the intruder will have to change the hashes of all the blocks in Blockchain which is very time consuming and almost impossible to do. Therefore, data in Blockchain is tamper-proof and retains its authenticity.

Some features of Blockchain are that the data stored in the blockchain is immutable and cannot be easily changed. And the data is added to the block after being approved by everyone on the network and thus allows

for secure transactions. Those who verify transactions and add to the block are called miners.

For the project, there is development of an E-Polling System using Ethereum Blockchain, smart contracts and ganache. Administrators would be able to create a new poll and allow candidates to compete in voting.

These polls can be related to any topic. Registered voters would be able to participate in voting. Results will be announced from the administrator's end. Admin is not given authority to interfere or alter the voting process. This ensures transparency and reliability in the entire process.

OBJECTIVES

In a democracy like India (the world's largest democracy), voting plays a key role in electing government officials and in expressing our vision of how a ruling party will be formed.

Developing a solution using blockchain to make the voting process more secure, transparent, immutable and reliable. This project aims to address some of the problems in current systems by greatly minimizing the human intervention in the process and thus reducing costs and errors.

2. RELATED WORK

There are numerous works that have been done related to electronic voting. A few articles have been published in recent times highlighting the security and privacy issues of blockchain-based electronic voting systems. Shows comparisons of selected blockchain-based electronic voting systems.

Zheng and Zibin proposed a comprehensive overview of Blockchain Technologies. The authors discussed the structures, key features and algorithms of compatibility used in the blockchain [1]. They also listed some of the challenges of blockchain development and the ways in which they are available to solve these problems.

Kashif & Arsha presented an attempt to exploit the benefits of the blockchain in this way in order to achieve an effective e-voting system [2].The proposed method was implemented through Multichain. The cryptographic hash has been used to protect integrity.The purpose of their research was to investigate important issues such as voter anonymity and voter confidentiality.

Various challenges and problems faced by the existing voting systems have been discussed [3]. They conclude that the Blockchain based E-voting system performs the best of all existing systems.

Ethereum smart contracts have been analyzed by various parameters to deliver basic functions [4]. Several metrics were used on over 200k contracts, libraries and links from 40k source code files. Structure of smart contracts in terms of their sizes, complexity, coupling and inheritance properties were finalized.

An open voting network (OVN) was introduced by [5], which is the first deployment of a transparent and accountable online voting protocol using Ethereum. At OVN, voting size is limited to 50–60 voters per frame. OVN cannot stop fraudulent miners from damaging the system. A fraudulent voter may also avoid the voting process by submitting an invalid vote. The protocol does nothing to ensure resistance to violence, and the election administrator wants to trust [6,7]. In addition, since firmness does not support elliptic curve cryptography, they use an external library to perform calculations [8]. After the addition of the library, the voting contract became too large to be stored on the blockchain. As with all the history of the Bitcoin network, OVN is at risk of being attacked for denial of service [9].

Layi et al. [10] suggested decentralized anonymous transparent electronic voting system (DATE) requires a low level of confidence among participants. They think that in the big electoral election, the current voting system for DATE is appropriate. Unfortunately, their proposed system is not strong enough to protect against DoS attacks because there was no external company authority in the accounting system responsible for voting after the election process. This program is only suitable for small scales due to platform limitations [11]. Although the use of the Signature Ring keeps the privacy of each voter, it is difficult to manage and coordinate a few signatory organizations.

They also exploit the PoW consensus, which has significant limitations such as energy consumption: "supercomputers" monitor the millions of computations per second, which is occurring around the world. Because this system requires high integration capacity, it is expensive and energy-consuming. Shahzad et al. [12]

made the BSJC's proposal for proof of completeness as a reliable method of electronic voting. They used a process model to describe the structure of the whole system. On a small scale, it also tried to address anonymity, privacy, and security issues in elections. However, many more problems have been highlighted. Another problem is the involvement of a third party as there is a high risk of data breaches, leaks, and improperly entered tables, all of which may contribute to the final verification.

3. BLOCKCHAIN

Blockchain technology has corrected the shortcomings of the electoral system, made the voting process more transparent and accessible, stopped illegal voting, strengthened data protection, and evaluated the voting effect. The implementation of an electronic voting system in the blockchain is very important. However, electronic voting has significant risks, such as when an electronic voting system is in jeopardy, all elected ballots may be improperly used. We are building a solution to all these problems using Ethereum blockchain, smart contracts and Solidity.

Ethereum -

Blockchain is a growing list of records, called blocks, that are securely connected together using cryptography. Each block contains a cryptographic hash of the previous block, timestamp, and performance data. Ethereum allows anyone to install applications that are permanently divided and unchangeable, with which users can share.

Smart contract -

Smart contracts are simply blockchain-based systems that operate when predetermined conditions are met. They are usually used to automate the execution of an agreement so that all stakeholders can immediately be sure of the outcome, without the involvement of any arbitrator or loss of time.

Solidity -

Solidity is an object-oriented, high-level language for executing smart contracts. Solidity is designed to target Ethereum Virtual Machine (EVM). Influenced by C++, Python and JavaScript.

Security Requirements for Voting System :

- Anonymity- Throughout the voting process, the number of voters must be protected from external information.
- Audit and Accuracy - Accuracy, also called fairness, requires that the declared results accurately match the election results.
- Democracy/Singularity - A "democratic" system is defined only when eligible voters can vote, and only one vote can be cast for each registered voter.
- Voting Privacy - After voting, no one should be in a position to attach voter identity by their vote.
- Stability and Integrity - This condition means that a reasonably large group of voters or representatives cannot interfere with elections.

4. METHODOLOGY

The Ethereum-based blockchain is used as an open source with smart contract functionality. Smart Contracts are programmed in Solidity for various functionalities like adding or removing candidates, voters and elections. Truffle and Ganache are used to set up a personal Ethereum blockchain which can be used to run tests and execute commands. For transactional privacy and allowing users to access the ethereum wallet, Metamask extension is used.

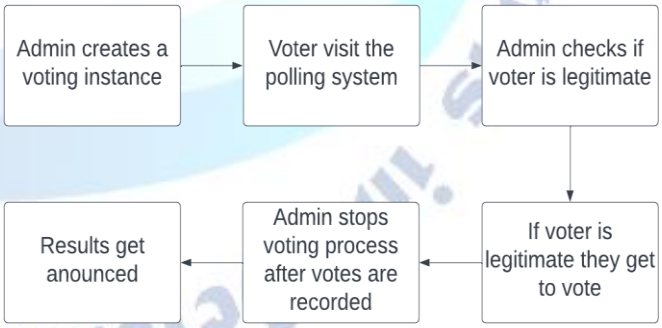

Figure 1: Block Diagram of the Voting System

Admin will create a voting instance and voters connect to the same blockchain to become a voter. Admin, then will check if the registration information (blockchain account address, name, and phone number) is valid and matches with his record. If yes, then the admin approves the registered user making them eligible to vote in the

election. Voter, following the approval from the admin, casts their vote to the candidate of interest. The results are displayed announcing the winner.

5. CALCULATIONS

Multiple virtual users are set to calculate the TPS(Transactions per second). The Transactions recorded in 16 seconds turned out to be 7 in total. This is recorded manually by using a timer. The formula used for calculating total transactions is -

VU * time * TPS = total_transactions

where,

VU = Number of virtual users

time = test time in seconds

TPS = transactions per second

VU * time * TPS = total_transactions

10 users executing at 7 transactions per 16 seconds for one hour would execute a total of 10 * 7/16 * 3600 = 15,750 transactions.

Hence the system is able to handle more than 15000 transactions in 1 hour with 10 users.

Performance Comparison of Proposed Solution-

Comparison of generation time :

The average amount of time it takes for a new block to be added to a blockchain. The faster a block is generated, the better the user is able to interact with the chain. Generation speed of a blockchain is one of the prime parameters through which viability of a blockchain is gauged.

The average block time of the network is evaluated after n number of blocks, and if it is greater than the expected block time, then the difficulty level of the proof of work algorithm will be reduced, and if it is less than the expected block time then the difficulty level will be increased.

After comparing all the chains with respect to each other the result observed is that ethereum is one chain which has above average capacity of generation time at 10-19s and performs 96-98% better than the competitive chain including Bitcoin.

Comparison of Hash rate:

Hash rate is a measure of the total computational power being used by a proof-of-work cryptocurrency network to process transactions in a blockchain. It can also be a measure of how fast a cryptocurrency miner's machines complete these computations.

In other words, Hashrate is a measure of the computational power per second used when mining. More simply, it is the speed of mining. It is measured in units of hash/second, meaning how many calculations per second can be performed. Machines with a high hash power are highly efficient and can process a lot of data in a single second.

Comparison of Hash rate showed that high hash rate is favorable to us and ethereum stands at 168.59 Th/s (Trillion hash per second) which is better than ~70% of the competitive frameworks.

Comparison in Tx rate:

Transaction speed measures how fast an individual transaction takes to get settled. Transaction times can vary wildly. This is because it is affected by factors such as the total network activity, hashrate and transaction fees.In the context of blockchains, transactions per second (TPS) refers to the number of transactions that a network is capable of processing each second. The approximate average TPS of the Bitcoin blockchain is about 5 – though this may vary at times. Ethereum, in contrast, can handle roughly double that amount.

Cryptographic algorithm suitability:

Cryptographic algorithms are processes for encryption and decryption. Most cryptography algorithms involve the use of encryption, which allows two parties to communicate while preventing unauthorized third parties from understanding those communications.

Cryptography provides for secure communication in the presence of malicious third-parties—known as adversaries. Encryption uses an algorithm and a key to transform an input (i.e., plaintext) into an encrypted output (i.e., ciphertext).

The best technique available for encryption in the real world till now is ECDSA as it combines the best practices of every other algorithm with best possible result and less memory and time requirements.

Framework	Generation time	Hash rate (Th/s)	Transactions per second	Cryptographic Algorithm
Bitcoin	9.7 min	899.624	4.6 max 7	ECDSA
Ethereum	10 to 19 s	168.59	15	ECDSA
Hyperledger Fabric	10 ms	NA	3500	ECC
Litecoin	2.5 min	1.307	56	Scrypt
Ripple	3.5 s	NA	1500	RPCA
Dogecoin	1 min	1.4	33	Scrypt
Peercoin	10 min	693.098	8	Hybrid

Table 1 : Performance Comparison

Existing solutions comparison with ours:

Follow my vote : It uses bitcoin in framework technology which has poor generation time and a very low transaction rate which makes it difficult for users to perform smooth and fast voting.

Voatz: It uses hyperledger fabric framework which has undefined hash rate and incompetent crytographic algorithm which makes it highly insecure to use and hence makes the users' information reliability low. It is not immune from cyberattacks or security vulnerabilities.

Polynas: It is based upon local blockchain and hence addition for any new user is difficult to proceed through as it requires a whole new set-up in the local environment and any person who does not understand technology well won't be able to do so. The scalability issues increase to a high level.

Luxoft: It uses hyperledger fabric as the underlying framework which has a low transaction rate. The consensus protocol used is PBFT which is vulnerable to DOS attacks and has a high communication complexity.

Agora: It uses bitcoin in framework technology which has poor generation time and a very low transaction rate which makes it difficult for users to perform smooth and fast voting. BFTr algorithm is prime to Byzantine fault in which a component such as a server can inconsistently appear both failed and functioning to failure-detection systems, presenting different symptoms to different observers. It is difficult for the other components to declare it failed and shut it out of the network, because they need to first reach a consensus regarding which component has failed in the first place.

Online Voting Platforms	Framework	Language	Cryptographic Algorithm	Consensus Protocol
Follow My Vote	Bitcoin	C++/Python	ECC	PoW
Voatz	Hyperledger Fabric	Go/ JavaScript	AES/GCM	PBFT
Polynas	Private/local Blockchains	NP	ECC	PET
Luxoft	Hyperledger Fabric	Go/JavaScript	ECC/ElGamal	PBFT
Agora	Bitcoin	Python	ElGamal	BFT-r

Table 2 : Existing solutions

6. FUTURE SCOPE AND CONCLUSION

The project is aimed at building a reliable voting system which can precisely conduct elections of any type. The research on project implementation tools has been under study and will further proceed the same way for the best outcomes. Setting up for Ganache local ethereum and transactions using Metamask was completed. The smart contracts for addition and removal of candidates, voters and elections have been programmed. The solution is based upon the Ethereum blockchain which has 96-98% better generation time than others and a competitive hash rate generation per second. ECDSA requires a minimum key length to provide the same security as other cryptographic algorithms. The great advantage of having this small key size is that the calculation can be done quickly. In addition, this helps to reduce storage space, power consumption, processing power, and bandwidth. This project also enforces smooth transactions with a manual recorded Transactions Per Second as 7/16.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] Zheng, Zibin & Xie, Shaoan & Dai, Hong-Ning & Chen, Xiangping & Wang, Huaimin, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", 2017, 10.1109/BigDataCongress.2017.85.

[2] Mehboob, Kashif & Arshad, Junaid & Khan, Muhammad, "Secure Digital Voting System Based on Blockchain Technology", 2021, 10.4018/978-1-7998-5351-0.ch071.

[3] Garg, Kanika & Saraswat, Pavi & Bisht, Sachin & Aggarwal, Sahil & Kothuri, Sai & Gupta, Sahil, "A Comparative Analysis on

E-Voting System Using Blockchain", 2019, 1-4. 10.1109/IoT-SIU.2019.8777471.

[4] Hegedüs, Péter, "Towards Analyzing the Complexity Landscape of Solidity Based Ethereum Smart Contracts. Technologies", 2019, 7. 6. 10.3390/technologies7010006.

[5] McCorry, P.; Shahandashti, S.F.; Hao, F. "A smart contract for boardroom voting with maximum voter privacy". In Proceedings of the International Conference on Financial Cryptography and Data Security, Sliema, Malta, 3–7 April 2017.

[6] Zhang, S.; Wang, L.; Xiong, H. "Chaintegrity: Blockchain-enabled large-scale e-voting system with robustness and universal verifiability". Int. J. Inf. Secur. 2019, 19, 323–341.

[7] Chaieb, M.; Koscina, M.; Yousfi, S.; Lafourcade, P.; Robbana, R. "DABSTERS: Distributed Authorities Using Blind Signature to Effect Robust Security in E-Voting".

[8] Woda, M.; Huzaini, Z. "A Proposal to Use Elliptical Curves to Secure the Block in E-voting System Based on Blockchain Mechanism". In Proceedings of the International Conference on Dependability and Complex Systems, Wrocław, Poland, 28 June–2 July 2021.

[9] Hjálmarsson, F.Þ.; Hreiðarsson, G.K.; Hamdaqa, M.; Hjálmtýsson, G. "Blockchain-based e-voting system". In Proceedings of the 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, USA, 2–7 July 2018.

[10] Lai, W.J.; Hsieh, Y.C.; Hsueh, C.W.; Wu, J.L. "Date: A decentralized, anonymous, and transparent e-voting system". Proceedings of the 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), Shenzhen, China, 15–17 August 2018.

[11] Gao, S.; Zheng, D.; Guo, R.; Jing, C.; Hu, C. "An Anti-Quantum E-Voting Protocol in Blockchain with Audit Function". IEEE Access 2019, 7, 115304–115316.

[12] Shahzad, B.; Crowcroft, J. Trustworthy Electronic Voting Using Adjusted Blockchain Technology. IEEE Access 2019, 7, 24477–24488.

[13] Fernández-Caramés, T.M.; Fraga-Lamas, P. Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. IEEE Access 2020, 8, 21091–21116.

[14] Yi, H. Securing e-voting based on blockchain in P2P network. EURASIP J. Wirel. Commun. Netw. 2019, 2019, 137.

[15] Torra, V. Random dictatorship for privacy-preserving social choice. Int. J. Inf. Secur. 2019, 19, 537–543.

[16] Alaya, B.; Laouamer, L.; Msilini, N. Homomorphic encryption systems statement: Trends and challenges. Comput. Sci. Rev. 2020,36, 100235 have successfully programmed the smart contracts for addition and removal of candidates, voters and elections.