iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.53168

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

Election Tally-Using Blockchain and User-Identification

Gaurav Abhangrao[1], Vishal Kumar[2], Balmukund Jha[3], Pratham Singh Tomar[4], Asst. Prof. Prafull Chaudhari[5]
[1, 2, 3, 4, 5]*Computer Science & Engineering, Sandip University, Nashik, India*

Abstract: ***A lot of democratic choices are made among many different sets of people, and voting is the preferred way of doing so. The technique offers an equitable and effective way to make a choice based on the consensus, regardless of whether it is applied in formal or informal settings. Keeping track of voter choices is not difficult when fewer people are voting, but it becomes crucial and more difficult when there are thousands or even millions of voters. Modern voting processes face a record-keeping challenge, but advances in blockchain technology may offer a solution. This is because blockchain technology, by its very nature, shines in apps where numerous users are working with immutable data. This study examines the planning and Election Tally Application a voting system being developed that has its blockchain, operates on a centralized network of servers, and incorporates a biometric scanner to ensure vote accuracy and tell enrolled voters from inactive ones. This system enables data immutability while giving voter protection and ballot management. The system can scale to manage a large number of votes from numerous servers while keeping data integrity, speed, and security, according to experimental findings. To improve user security, user identification was integrated into developing and implementing the centralized and autonomous blockchain network for use as a voting platform.***

Keywords: Distributed system, publisher-subscriber, centralized syncing, polling, blockchain, and SHA-256

I. INTRODUCTION

Recent years have seen a rise in the use of blockchain technology, which has had an impact on many industries while demonstrating its versatility and rising level of security. The basic idea behind the technology is to keep data on a distributed database made up of different pieces of data that are connected. When data from one block is encoded, information from subsequent blocks can be linked together. This is a feature of the blockchain where the hash value of the subsequent block influences the hash value of the current block. This increases information security and integrity because earlier blocks in the chain of blocks cannot be changed without having an inconsistent cascade impact. The data that were captured is kept on a ledger that is disseminated to all client computers in the network and changed at a central system server.

Data distribution to the client side adds a layer of system authentication. The system can verify data with all other functions in the system if a node is hacked, since most data are constant, validation is maintained. The 51% law states that this holds as long as 5% of the ledgers are accurate. This guideline applies when a single server has most of the 6% hashing power in a blockchain network. Although, due to the dispersed nature of the blockchain and the computational power required to accomplish more than 50% of the hashing power, as the hashing calculation turns more computationally demanding with each additional block, this scenario is challenging to achieve.

Despite the fact that security and flexibility of Blockchain technology, applications outside of the finance industry have not been widely adopted, voting systems operated by a blockchain can be implemented in secure and optimized methods to maintain the integrity of the votes and decisions along with solving logistical issues with contemporary elections. With factors of security, validation, and scalability, it come up with an attractive technology to be adapted to many other industries as well as a means of resolving elections' administrative issues today.

Voting necessitates that people emerge in the same area, the voting station. In circumstances of larger-scale elections, such as parliamentary and state elections, many parties are needed to uphold order, secrecy, integrity, and synchronization of the polling system to ensure the accuracy of the result, The shortcomings of the existing voting system are addressed by a blockchain-based election system, However, there are some disadvantages to switching from a physical vote to an internet method for voting. Being able to believe the organization coordinating the ballot is a major factor to take into account. confidence in the ballot would be necessary, but it would also be necessaryto have confidence in the user statistics to be used as part of the verification process, The SHA-256 hashing algorithm encodes data in a blockchain network in one manner to reduce data privacy worries. As a result of this hashing technique and the blockchain's immutability, assaults are less successful.

©IJRASET: All Rights are Reserved

As the original data cannot be recovered, it also provides a layer of anonymity in addition to offering immutability, thereby preventing any efforts at data vulnerability.

As one may have observed at online competitions or surveys where the results or rewards are contingent on the voting result of a sizable population, using the internet to cast a ballot is not a novel idea. These techniques are effective and helpful in such use cases, even though situations like these are smaller and less significant than a political poll. This will show the efficiency of online polling systems and the fixes it offers to common issues in online voting systems through our application of a blockchain-based voting system. This version only employs the fundamentals of blockchain systems, including SHA-256 algorithm encryption, immutability, and decentralization. It is not built on any actual blockchain network anonymity, designed to achieve this, the paper's accomplishments include:

1) Propose and construct a blockchain system that makes use of user identification,
2) Creation of a blockchain from inception that may be freely used for study and teaching,
3) Evaluation outcomes and productionmeasurements based on different server loads executed on generic hardware

The remainder of this essay is structured as follows:The linked studies and present restrictions are covered in Section II. Section III discusses the suggested approach and its architecture. Section IV covers the implementation of the prototype, obstacles, and answers. Section V presents the evaluation findings, Section VI discusses validity threats, and Section VII presents conclusions and suggestions for further research.

A. Related Works

Although the idea to combine the Internet of Things with the democratic method of voting is not novel, it has not yet been widely adopted on a big politicalscale. Large-scale internet voting methods have occasionally been successful, with a recent election having a 53% acceptance rate for the online voting medium [1], Estonia, a nation in Northern Europe surrounding the Gulf of Ireland and the Baltic Sea regions, has done online voting for roughly the last 17 years. The advantages of an online voting method include lowering election expenses and making it simple for voters to submit their ballots [2], preserving a single record of polling information, and permitting only one party If this material were accessed, it might become corrupted. Voting malpractice can be a serious problem if there is no proof in place [3], However, due to the popularity of blockchain, massive voting systems have been deployed using blockchain technologies in recent years [4, 5]. Blockchain technology offers solutions that make it possible to adopt an online polling system without many of the drawbacks thatmight typically occur.

Early attempts to incorporate coins into the electionsystem used blockchain technology, A Bitcointransmission was used as a voting ballot in the writings of Zhao and Chan [6], Although the systemwas designed to handle votes with only two candidate choices, the use of Bitcoin offered the anonymity and verifiability that are essential components of a blockchain voting system. Tian et al. streamlined the method and used Zhao and Chan's protocol as a subroutine to handle the restriction on the number of applicants [7], As demonstrated by Ballotchain, an online voting platform powered by RegNet Bitcoin, the use of cryptocurrencies in voting systems has advanced to business settings. The polling platform supports Bitcoin transfers without really buying them [3], Every vote will bear the advantages of a blockchain transaction as a result of Ballotchain's emphasis on. solution that employs a Bitcoin transaction. A tinyquantity of cryptocurrency is used by Ballotcoin, thevote used by Ballotchain, and is then moved to thewallet of the candidate they wish to win [3], The features of blockchain-based voting have been shaped by the use of coins in voting. This includes attributes like confidentiality, revocability, verifiability, and sincere voting rewards. The original transfer charge and operating costs of cryptocurrencies can be a deterrent to involvementand system scalability, which can reduce voting turnout.

Standards for blockchain-integrated voting systemswere created as blockchain technology gained more focus over time. For starters, Dimitriou suggested a blockchain-based voting system based on theresolution of a few fundamental characteristics describing the security of the system, including secrecy, completeness, soundness, eligibility, reusability, and justice [8], The smart card was usedin Dimitriou's answer to enable voting on public devices, but because it is a tangible object that canbe lost or taken, the risk of fraud still exists. Shah et al. [9] suggested an online polling method using the user-identification reader on Android to address the authentication problem. The method entailed using biometric information to verify the voter and encrypting the information with SHA-256. Ethereum's blockchain system had limitations that caused scalability and transmission problems.

The decentralized nature, which means there is no single authority that users must rely on to verify theinformation on the blockchain, is a common characteristic of many blockchain platforms. Instead, data is shared across the network and verified by peers when at least 51% of users agree on the information [10], This 51% rule offers a high degree of security as networks grow in size becausethe only way to change the data is to gain malevolent control of more than half of the active nodes. A centralized database can also be usedwhen the 51% criterion is insufficient for security [11],

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

However, in a centralized system, trustbetween the user and the controlling authority must be created, Instead data is shared across the network and verified by peers when at least 51% ofusers agree on the information [10], This 51% rule offers a high degree of security as networks grow insize because the only way to change the data is to gain malevolent control of more than half of the active nodes. A centralized database can also be a solution that employs a Bitcoin transaction. A tinyquantity of cryptocurrency is used by Ballotcoin, thevote used by Ballotchain, and is then moved to thewallet of the candidate they wish to win [3], The features of blockchain-based voting have been shaped by the use of coins in voting. This includes attributes like confidentiality, revocability, verifiability, and sincere voting rewards. The original transfer charge and operating costs of cryptocurrencies can be a deterrent to involvementand system scalability, which can reduce voting turnout.

Standards for blockchain-integrated voting systemswere created as blockchain technology gained morefocus over time. For starters, Dimitriou suggested ablockchain-based voting system based on theresolution of a few fundamental characteristics describing the security of the system, including secrecy, completeness, soundness, eligibility, reusability, and justice [8], The smart card was usedin Dimitriou's answer to enable voting on public devices, but because it is a tangible object that canbe lost or taken, the risk of fraud still exists. Shah et al. [9] suggested an online polling method using the user-identification reader on Android to address the authentication problem. The method entailed usingbiometric information to verify the voter and encrypting the information with SHA-256.Ethereum's blockchain system had limitations that caused scalability and transmission problems.

The decentralized nature, which means there is no single authority that users must rely on to verify theinformation on the blockchain, is a commoncharacteristic of many blockchain platforms.Instead, data is shared across the network and verified by peers when at least 51% of users agree on the information [10], This 51% rule offers a highdegree of security as networks grow in size becausethe only way to change the data is to gain malevolent control of more than half of the active nodes. A centralized database can also be used when the 51% criterion is insufficient for security [11], However, in a centralized system, trust between the user and the controlling authority must be created, Instead data is shared across the network and verified by peers when at least 51% ofusers agree on the information [10], This 51% rule offers a high degree of security as networks grow in size because the only way to change the data is to gain malevolent control of more than half of the active nodes. A centralized database can also be solution that employs a Bitcoin transaction. A tinyquantity of cryptocurrency is used by Ballotcoin, thevote used by Ballotchain, and is then moved to thewallet of the candidate they wish to win [3], The features of blockchain-based voting have been shaped by the use of coins in voting. This includes attributes like confidentiality, revocability, verifiability, and sincere voting rewards. The original transfer charge and operating costs of cryptocurrencies can be a deterrent to involvement and system scalability, which can reduce voting turnout.

Standards for blockchain-integrated voting systemswere created as blockchain technology gained morefocus over time. For starters, Dimitriou suggested ablockchain-based voting system based on theresolution of a few fundamental characteristics describing the security of the system, including secrecy, completeness, soundness, eligibility, reusability, and justice [8], The smart card was usedin Dimitriou's answer to enable voting on public devices, but because it is a tangible object that canbe lost or taken, the risk of fraud still exists. Shah et al. [9] suggested an online polling method using the user-identification reader on Android to address the authentication problem. The method entailed usingbiometric information to verify the voter and encrypting the information with SHA-256. Ethereum's blockchain system had limitations that caused scalability and transmission problems. used when the 51% criterion is insufficient for security [11], However, because the blockchain ledger is held by a single person in a centralized system, trust between the user and the authority incharge of it must be created. The Quantum Ledger Database (QLDB), developed by the Amazon Webservices team, is a convincing illustration of this distributed confidence but is prized as a tamper-proof, immutable record [12]. used when the 51% criterion is insufficient for security [11], However, because the blockchain ledger is held by a single person in a centralized system, trust between the user and the authority incharge of it must be created. The Quantum Ledger Database (QLDB), developed by the Amazon Webservices team, is a convincing illustration of this distributed confidence but is prized as a tamper-proof, immutable record [12].

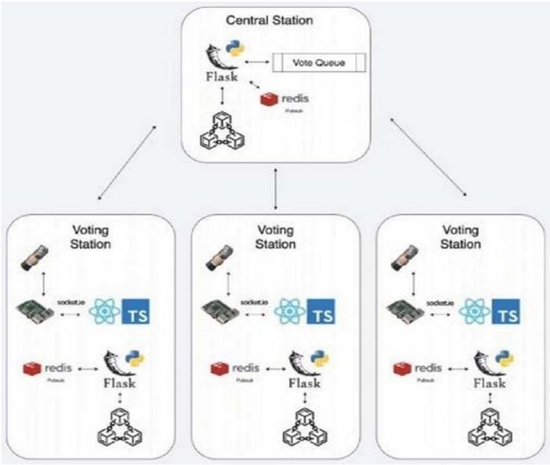
ElectionTally

ElectionTally is intended to be a use-case application that shows how useful a controlled, permission-based blockchain system can be. It assumes that a centralized system's architecture is what is wanted, and confidence is given to thegoverning group for its use of the blockchain.

All parties using the software are deemed to agree with the gathering of this biometric data because biometrics are also being gathered and used as a means of verification. Since many contemporary mobile devices use both facial recognition and user identification as a means of authentication, it did not show itself as a significant problem during the brainstorming process and choose to use the user-identification reader.

B. Architecture

The following essential elements make up the architecture of ElectionBlock, which is shown in Fig. 1: the central office, and the polling locations.



Fig, 1, Architectural diagram utilizing 3 votingstations and one central station, In the implementation, the voting stations are not limitedto 3 as the central station does not have a limit on the number of nodes it can handle.

C. Voting Station

The place of entry for the individual is the polling station, It has a user-identification reader, and the Raspberry Pi 4 serves as its computer. The React application, which will make the necessary method calls to request, confirm, and check the user's biometric data, is connected to the Raspberry Pi 4 via a socket link. To transmit polling data to the central queue, the React application also interacts with the central server. The client program only interacts with this part of the central computer. A Redis publisher-subscriber (pub-sub) aggregator is utilized to obtain serialized information from the server, The central server publishes blockchain changes that the polling machines adhere to. Recalculating the checksum verifies and validates the received changes depending on info from the blockchain, the voting location will refresh its record with the new blockchain file if the consistency of all prior blocks in the blockchain allows.

D. Central Server Station

The ElectionTally network is concentrated, so all blockchain transactions are sent from the polling station's React application to the Flask server running on the central server. The central server serves as the single source of truth for the network. A predetermined amount of votes are dequeued after the centralized vote queue receives the vote data from the Flask server. As shown in Fig. 2, each dequeued vote includes the voter's identification number, the campaign identification number, the candidate they supported, and the moment the vote was cast. This data is handled as a Merkle tree and encoded, The new block that is put into the network is then hashed using the tree's base hash; the poll info is also contained in this block. Once thisnew block has been added to the chain, the pub-subbroker is used to send it to the polling sites that have subscribed.



Fig, 2, Block structure is shown consisting of multiplevotes

II. PROTOTYPE IMPLEMENTATION

ElectionTally uses a pub-sub design and incorporated biometric verification to carry out the job of online voting with a secure immutable record,adhering to the general principles of centralized blockchain technology. Registered electors' biometric data will be stored in a directory that the user-identification scanner can access. The system will conduct two checks after receiving a user-identification reading: first, it will authenticate the user against the database to confirm that they are registered voters, and second, it will check the blockchain to ensure that they haven't already voted in the chosen campaign as a safeguard against duplicate votes.

The Merkle tree method is used to organize and hash the ballots as they are gathered by different polling devices and sent to a central queue. Our application's block size was set to 16. The block size typically affects the network's efficiency in terms of speed and capacity. If the block size is too tiny, blocks are transferred more frequently, which puts more strain on the network. If the block capacity is too large, there will be delays because fresh blocks must be mined, which takes time. Since mining is not used on ElectionTally's permissioned blockchain, the block size of 16 has proven to be an effective measurement for maintaining steady network traffic and updating the blockchain at the normal cost. The Merkle tree method, which hashes together pairs of votes until one final hash is left that contains all 16 votes, can also effectively use this block size. The secure hash technique SHA-256 is used in the Merkle tree to hash data. This is a fixed-for-any-source one-way encryption algorithm. This states that no two non-identical bits of data can produce the same hash, and the generated hash cannot be converted back into the original text through decryption.

Votes are hashed into blocks, and the blocks are connected to the current database as they are created. Redis-based pub-sub architecture is used to apply updates to polling sites so that distributed nodes always have a local copy of the most recent chain. To enable recovery from failures and shutdowns, these chains are serialized using the Python Pickle module and saved locally on each client.

The process of the user is shown in Fig. 3. After the biometric validation procedure, the system must confirm the voter's uncast ballot in order to stop election fraud. The process's design takes into consideration a variety of voter fraud situations, including repeated voting with different timings and inactive participants.

A. Scalability

The system manages three key scalability issues as a voting system with the capacity to handle national-level election events;

1) Discussing ways to expand the system's polling locations is an example of extensibility.
2) Sequential Consistency: How our system handles situations where there may be thousands of simultaneous ballot requests at many distinct polling locations.
3) Fault Tolerance: This refers to how our system protects against network failures or malicious efforts to meddle with our data.

Our system was developed with the ability for polling locations to be expanded in mind. The fact that there are numerous various voting locations so that as many voters as feasible can cast a ballot is one of the core components of the present voting system. Multiple voting locations are an important part of voters' rights, even though the polling place may frequently be the subject of disputes. Each polling station in our system is deployed as a duplicate of the other. The IP address must be added to a whitelist after the device is connected to the internet in order to communicate with the central server. Another important component of the voting system is sequential consistency. During a national voting event, thousands of ballots may be sent concurrently, producing concurrent writes in the blockchain. Sequential consistency in writing is crucial in our application because the Merkle tree and blockchain technology both rely significantly on the order of the data. We chose to use a permission-based blockchain system, where the ultimate truth is held by a reliable party, to account for this. We designed a queue that stores ballots sent from the polling locations because computations for the Merkle tree and adding the new block to the blockchain are a bottleneck of the writing operation. Once there are 16 ballots in the list the ballots are then put into a Merkle tree and dequeued. A new block is added to the network after computing the tree's base hash. The blockchain data is then released to the subscribing nodes, keeping them up to date, once the new blockchain is available. The IoT-based system is constantly at risk from network failures because it is a dispersed system that depends on the internet. Blockchain technology offers authentication through the use of hash value verification to protect against possible network mistakes and malicious efforts at data tampering. All recipients of the published blockchain undergo blockchain verification after the source of truth blockchain is released to the polling locations. If the value computed does not match the given hash value, the station server will simply not accept the new blockchain as it verifies the individual hashes of the block and the block that came before. The complete database will be regarded as invalid, for instance, if a network error changed the block's hash value.

This results in the subscribing node dropping the most recent effort to update the blockchain and forcing it to simply wait for the next publication to resynchronize.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

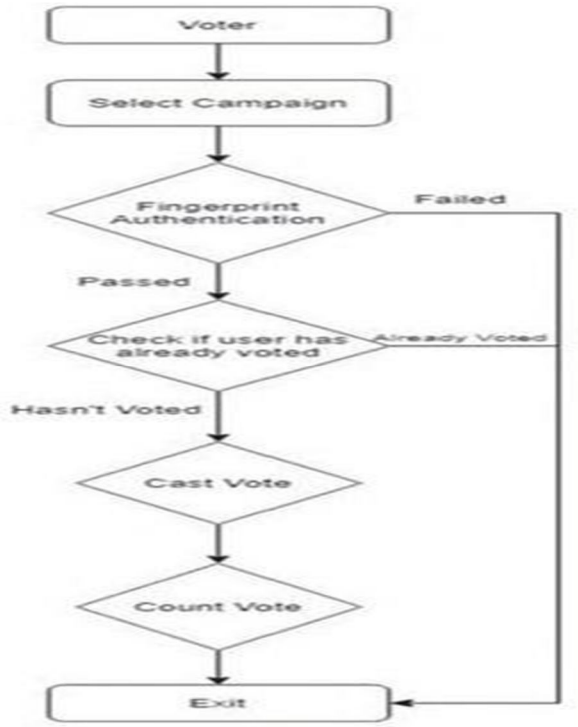


Fig. 3. Voter verification and voting processprevent potential voting fraud.

E. Challenges and Solutions

There were a few issues that surfaced during the creation of the ElectionTally programme and had to be resolved quickly. Handling numerous requestsat once was one of the more important difficulties that the group considered for several days. Millions of votes are being submitted simultaneously from various voting places during a real-world election. Large numbers of ballots may need to be handled slowly in a paper ballot voting method, but the sequence is not crucial. On the other hand, in a blockchain-based voting system, it is crucial to keep eventual consistency throughout the complete network. It is very challenging to make sure that the blockchain is updated at every node when thousands of ballots are being transmitted to it at once. In this case, the voting application's major disadvantage will be time usage. A real-world application would be poorly implemented if it required that each server have an updated copy of the blockchain as well as an ordered succession between nodes before sending ballots. Data loss without appropriate data safeguard processes in place is another potential problem. Using a voting queue at a central computer was one method usedto address the problems with numerous ballotsbeing submitted simultaneously. Any ballots cast bypeers would be received by this central computer, which would then queue them up. This would makeit feasible for a voting system to be used in the realworld and enable all voting stations to simultaneously submit ballots while keeping overallconsistency.

Determining how electors would identify themselves to be enrolled was another major problem that arose early in the development process. There are numerous methods for confirming a voter's name, so this was difficult. It was challenging to come up with a concept that would make the ElectionTally application stick outfrom the competition. In the traditional ballot-based voting method, registering to vote is necessary before receiving a ticket in the mail at your residence. You can carry your ticket and a form of identification, such as a driver's license, to the polls on election day. The use of polling stations is very comparable to this method, so it was carefullytaken into account when ElectionBlock's user authentication was implemented. The sign-in Partnerships with bank accounts that are frequently used on websites like Service Canada and the Canada Revenue Agency were among the choices we considered, though. Although the ElectionTally development team gave this a lot of thought, they ultimately chose to go with a unique and possibly even controversial choice. The procedure for authenticating voters was found to be a biometric reader. Registered voters would be given a polling station if there were a referendum. All of the user identification for those allocated to that particular spot would be stored in a database at this site. It was well known that people who opposed giving their data straight to the government might have some reservations. However, user identification is used by many contemporary mobiledevices and seems to be becoming more commonplace. The research team ultimately concluded that this is the voting method of the future and that a step forward in this sector wasrequired.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Scalability was a problem that was also encountered. Scaling the blockchain becomes more computationally demanding as it gets bigger because the capacity of the ledger increases. It would be necessary for later-added nodes to the blockchain to receive and load huge quantities of data into memory. The network was shared in order to address this scaling issue [13]. A shard, which is made up of ten (10) transactions, is created using this method to divide the blockchain into digestible pieces. Writing to a blockchain fragment becomes easier as the size of the complete record increases because each shard is smaller than the full blockchain.

The defense against voting fraud was the last obstacle to be overcome in the creation of this application. If there was malicious purpose behind the manipulation of the data in the blockchain, there would not be much of a worry in a normal decentralized blockchain system. The central server modifies the database in ElectionTally permission-based blockchain technology, though. One obvious worry was that the data could be readily altered in the event of a server assault. Each server will hold a duplicate of the database to avoid this problem. Nodes can detect attacks and quickly address the problem, preventing data manipulation on the central computer. The biometric reader stated above is one of the additional measures used in the application to check for voter fraud because it will stop people from voting more than once. To guarantee that specific devices are being used at the polling places, whitelisted IP addresses have been implemented. This will help stop malicious actors from destabilizing the system.

III. EVALUATION RESULT

The following specs were used to install and record the program on our computer to evaluate the ElectionTally system's performance: Intel Core i5 quad-core processor running at 2GHz, paired with 16 GB of 3733 MHz LPDD4 RAM

A. Algorithm Complexity

The four tenets of blockchain architecture were used to assess our approach [14];

1) Algorithm throughput
2) Degree of decentralization
3) Consensus algorithm vulnerabilities
4) Security issues.

ElectionTally employs the Merkle tree and the SHA-
256 algorithms, which are two basic hashing algorithms.

Both algorithms can handle all data given to them, which results in high throughput. The hashlib module in Python provides an optimized version of the SHA-256 algorithm. The hashlib processed all the input. As the SHA256 algorithm's time complexity is O(n), where n is the length of the text being hashed, the sha256() function is transformed into a byte string and handled with the least amount of computational delay possible. For a complete traversal of the Merkle tree using this method, we obtain a temporal complexity of 0(n-log(n)). A temporal complexity of 0(n-s-log(n)) is produced by combining these two numbers, where n is the total number of votes in the Merkle tree and s is the length of the serialized vote string. This means that a large number of queries can be processed by our program without noticeably degrading its efficiency. By distributing 1008 random queries with a 0.2-second delay between each one, this was put to the test. The entire system was able to handle all queries without experiencing any speed degradation by hashing the votes, adding the new block to the blockchain, and disseminating the new blockchain to the users.

ElectionTally does not employ a mining procedure because it is a permission system. The center node serves as the source of truth for all hashing computations. Since there is no need for miners with this approach, the revenue can be discounted. Likewise, consensus systems with a singular source of truth are impervious to flaws.

However, a centralized application does present a potential security danger because there is only one point of failure. This danger has been reduced in the ElectionTally version by comparing current blocks with prior blocks before a node receives an updated chain. When comparing the new chain to the local duplicate of the blockchain kept at a subscribing node, all blocks before the recently added block in the chain will match in a formalized process. During this comparison, any malicious modification of the data will be found and recognized.

B. Performance Measurement

Three various amounts of votes that were to be saved per block—1000, 2500, and 5000 votes held per block—were tried to determine the average time required to add a new block to the blockchain. (Fig. 4). Ten blocks were added with varying numbers of votes per block and combined to determine the average time it took for one vote to be added to a block at each occurrence. The time it took to add a new block had a linear relationship with the number of votes kept in each block, with a rise in the average time it took to add a block.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Using Locust, a Python stress testing tool, the scalability of the ElectionTally system was tested. To imitate electors submitting ballots, tenusers were created to transmit a random number ofqueries during testing. (Fig. 5). The load test findings showed an average reaction time of 350 ms and a failure rate of 0%. (Fig. 6 and Table I).

IV. THREATS TO VALIDITY AND SOLUTIONS

Every answer to contemporary issues has some drawbacks, and ElectionTally is no exception. The region of fault tolerance is where our answer couldmost benefit from growth. In order to manage casesof crashes and avoid data loss, future iterations of the program would need to employ an algorithmsimilar to Byzantine Fault Tolerance [15]. Since thereis only one central server, there is currently noconsensus method in use. A consensus algorithm could be performed across the nodes and havemore of a blockchain consensus strategy, though, with the inclusion of more nodes.

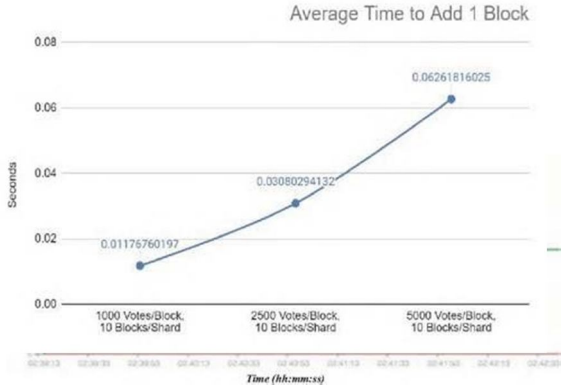


Fig. 4. Average time taken to add one (1) block whenhandling different quantities of votes stored perblock.

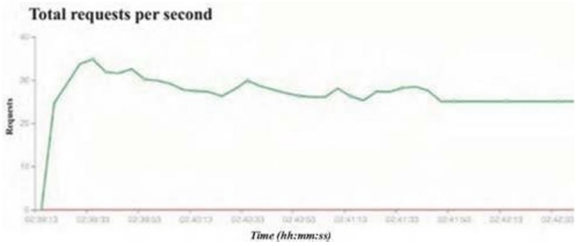


Fig. 5. Requests per second measured by locustusing 10 simulated users

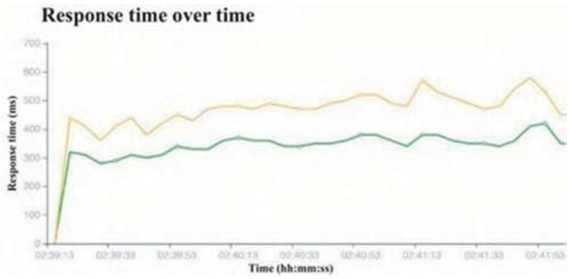


Fig. 6. Response time of requests over time measured by locust using 10 simulated users. (Green Line: Median Response Time, Yellow Line: 95% Percentile Response Time)

TABLE I. LOAD TEST DATA GATHEREDFROM LOCUST SIMULATION USING 10USERS.

Request Statistics

Method	Name	# Requests	# Fails	Average (ms)	Min (ms)	Max (ms)	Average size (bytes)	RPS	Failures/s
POST	/api/vote	4430	0	350	34	694	22	26.4	0.0
	Aggregated	4430	0	350	34	694	22	26.4	0.0

A larger number of core hubs would also improve security. You can always check the validity of the vote and hash values across the other nodes if one node is hacked and data is altered.

This product would be greatly accelerated by the use of numerous central servers because it would improve the voting system's security and availability. If the primary central node is compromised, the system will provide improved uptime. To maintain the system's functioning, a new primary central node would be chosen using a voting process. Additionally, the sharding method raises performance worries as well as security and data integrity threats, despite improving the blockchain's ability to grow [12]. This is mainly because each component created by sharding the blockchain functions as a separate blockchain. States across fragments would need to be watched because in this case, the corruption of a single component could be troublesome [12]. Inter-shard contacts and other techniques, which are presently being tried, will lead to better methods in this area. The biggest overhead in our approach is caused by verifying all shards during voting to stop users from casting, and it is believedthat inter-shard communication will also enhance the efficiency of a number of ballots. The ElectionTally application would improve by putting the suggested ideas into practice, and there would be a genuine chance to sell the answer.

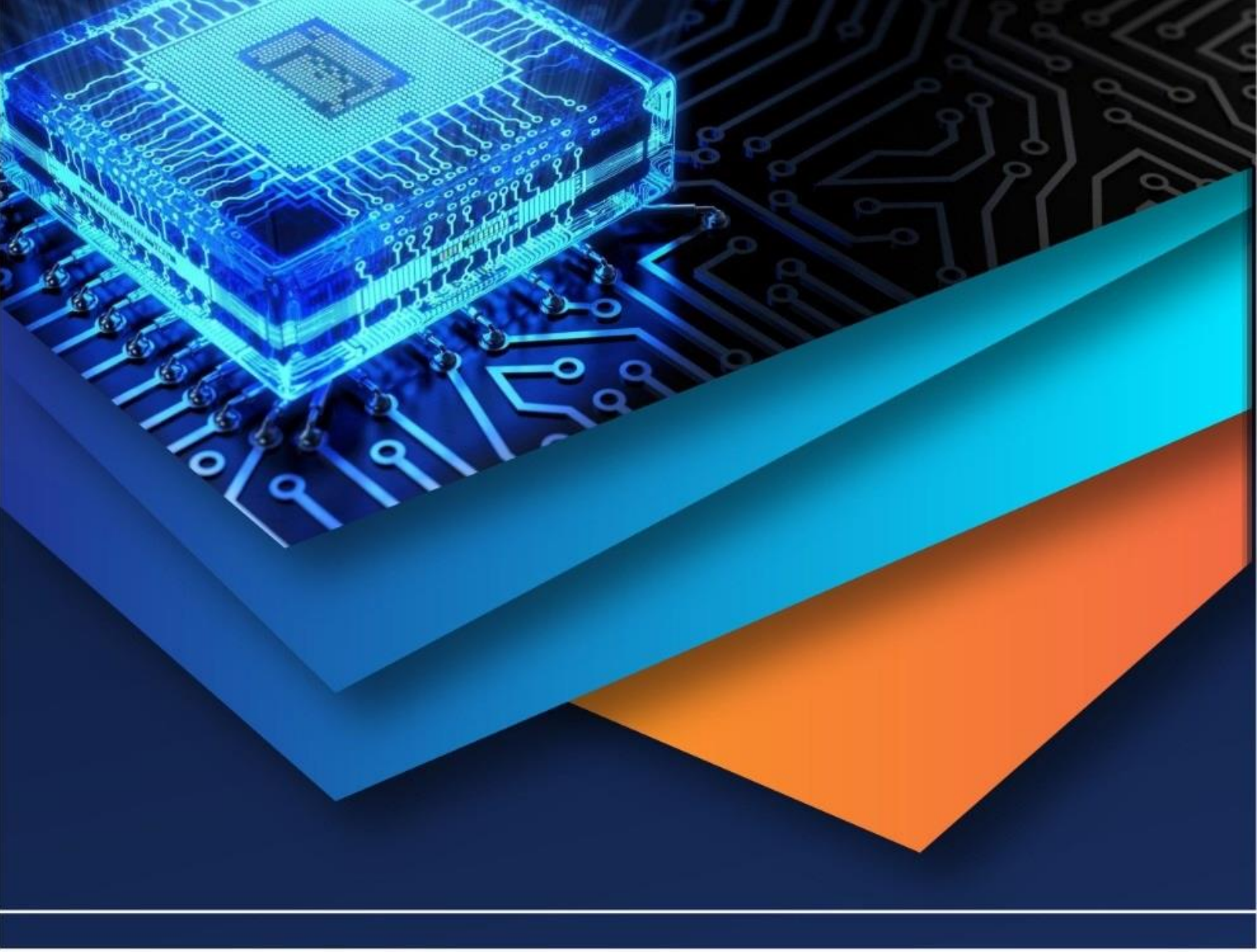
V. CONCLUSION AND FUTURE WORK

Overall, the ElectionTally application's growth yields a useful, controlled, and permission-based blockchain election system. The application's goal is to improve the existing ballot-based voting method used in most significant elections. Voter fraud can be significantly reduced by using the ElectionTally platform, which also offers the advantages of total openness and a user-friendly UI. Blockchain technology also effectively handles voting privacy and security. To promote further integration of innovative ideas into the system, we have made the source code of our pilot version accessible to the public.

REFERENCES

[1] C. O'Brien, "What Estonia could teach us aboutinternet voting in a post-pandemic world," VentureBeat, 12-Jun-2020. [Online]. Available: https://venturebeat.com/2020/06711/what- estonia-could-teach-us-aboutinternet-voting-in-a- post-pandemic-world/.
[2] D. Lohrmann, "Could Estonia Be the Model for Secure Online Voting?," Government Technology State; Local Articles - e.Republic, 26-Sep-2020. [Online]. Available: https://www.govtech.com/blogs/lohrmann-oncybersecurity/could-estonia-be-the-model-for-secure-online-voting.html.
[3] "Mohamed Ibrahim, Kajan Ravindran, Hyon Lee, Omair Farooqui, Qusay H. Mahmoud. "ElectionBlock: An Electronic Voting System using Blockchain and Fingerprint Authentication.
[4] "Blockchain Technology based e-voting system," Prof.AnitaLahane, JunaidPatel, Talif Pathan Prathamesh Potdar 01-Jul-2020.ITM Web of Conferences 32 [Online].ICACC-2020 Available:
[5] Sayada Tasmia Alvi, Mohammed Nasir Uddin, Linta Islam "Digital Voting: A blockchain-based e-voting system using biohash and smart contract. 2020[ICSSIT]
[6] Z. Zhao and T.-H. H. Chan, "How to Vote Privately Using Bitcoin," Information and Communications Security, vol. 9543, pp. 82-96, Mar. 2016.
[7] H. Tian, L. Fu, and J. He, "A Simpler Bitcoin Voting Protocol," Information Security and Cryptology Lecture Notes in Computer Science, pp. 81-98, Jan. 2018.
[8] T. Dimitriou, "Efficient, Coercion-free and Universally Verifiable Blockchain-based Voting," Computer Networks, vol. 174, p. 107234, Jun. 2020.
[9] A. Shah, N. Sodhia, S. Saha, S. Banerjee, and M. Chavan, "Blockchain Enabled Online-Voting System," ITM Web of Conferences, vol. 32, p. 03018, Jan. 2020.
[10] J. Frankenfield, "What Is a 51% Attack?," Investopedia, 28-Aug-2020. [Online]. Available: https://www.investopedia.com/terms/1/51- attack. asp.
[11] F. Stacey. "THE BLOCKCHAIN BRIEF." The Journal of Government Financial Management, Association of Government Accountants, vol. 67, no. 4, pp. 24-29, Dec. 2018.
[12] B. Pirns, "Amazon Tackles Centralized And Decentralized Blockchain Solutions," Forbes, 23-Jul- 2019. [Online]. Available: https://www.forbes.com/sites/benjaminpirus/201 9/07/11/amazon-tackles-centralized-and- decentralized blockchainsolutions/?sh=7f2c97471d54.
[13] M. Salimitari, M. Chatterjee, and Y. P. Fallah, "A survey on consensus methods in blockchain for resource-constrained IoT networks," Internet of Things, vol. 11, p. 100212, 2020.
[14] S. M. H. Bamakan, A. Motavali, and A. B. Bondarti, "A survey of blockchain consensus algorithms performance evaluation criteria," Expert Systems with Applications, vol. 154, p. 113385, Sep. 2020.
[15] M. Castro and B. Liskov, "Practical byzantine fault tolerance and proactive recovery," ACM Transactions on Computer Systems, vol. 20, no. 4, pp. 398-461, 2002.
[16] ElectionBlock Repository is publicly available on GitHub. [Online]. Available: https://github.com/mibrah42/electionblock

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)