Chapter 11
Electronic Voting Application Powered by Blockchain Technology

Geetanjali Rathee
Jaypee University of Information Technology, India

Hemraj Saini
https://orcid.org/0000-0003-2957-1491
Jaypee University of Information Technology, India

ABSTRACT

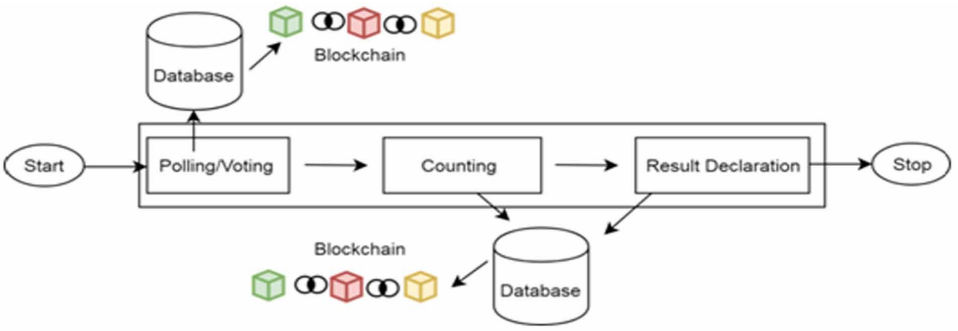
India is the largest democracy in the world, and in spite of that, it faces various challenges on a daily basis that hinder its growth like corruption and human rights violations. One of the ugliest phases of corruption and political mayhem is visible during the election process where no stone is kept unturned in order to gain power. However, it is the common citizen who suffers most in terms of clarity as well as security when it comes to his/her vote. Blockchain can play a very important role in ensuring that the voters registering their votes are legit and the counting of votes is not manipulated in any way. It is also needed in today's times where the world is available to people in their smart phones to also give them the opportunity to register their votes hassle free via their smart phones without having to worry about the system getting hacked. Therefore, in this chapter, the proposed layout will be based on a smart contract, using Ethereum software to create an e-voting app. In this chapter, the authors have proposed a secure e-voting framework through blockchain mechanism.

DOI: 10.4018/978-1-7998-3444-1.ch011

INTRODUCTION

Lately, Blockchains have pulled in overall consideration. A Blockchain is characterized as an immutable, successive chain of records called blocks. The record can contain transactions, documents or some other information, and are fastened together utilizing hashes (Iansiti & Lakhani, 2017; Crosby et al., 2016). It is executed and overseen by a peer-to-peer network of computers (also called peer nodes) spread everywhere throughout the globe. Blockchain likewise called distributed ledger which utilizes independent PCs (nodes) to record, share and synchronies transactions in their particular electronic ledgers, rather than keeping information incorporated on a server as in a customary record.

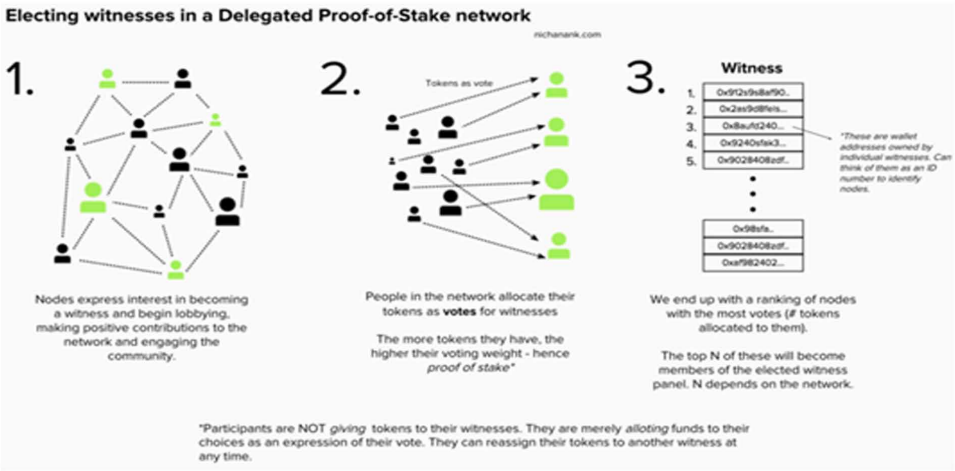
Figure 1. Schematic outline of e-voting using Blockchain



Blockchains have the potential to disrupt any industry that employs the use of a trusted middleman and give direct control back to the end user. In any case, similarly as with any technological revolution and the paradigm shift that joins it, there is a procedure of trial and error. What works and what does not and we are as of now in that stage with Blockchain advancements (Zyskind, & Nathan, 2015; Eyal et al. 2016; Pilkington, 2016). 99% of the business sectors are filled by unadulterated hypothesis. There are no completely useful Blockchain items that can oblige the requests of the majority. Blockchains must be less expensive, snappier, simpler to utilize and similarly as versatile, if not more thus, than the present frameworks set up. The coming of the web drove the technological revolution of the 90's and the industrial upheaval was in the late eighteenth century. These quantum jumps in human capacity and accomplishment change our whole reality and disturb pretty much every settled industry. They change the manner in which we travel, cooperate, communicate, business with one another, even think. All that we once knew is flipped on its head and life gets improved, making things a lot less demanding and

progressively productive. The same is the appearance of Blockchain technology where the component of trust is the whole sudden put under the control of target numbers and PCs. Blockchain is the initial step at placing trust into PCs. Sounds kind of terrifying and we would state that it is. Rest guaranteed however, the seasons of skynet and eliminators are far away and except if we create methods for keeping self-aware robots from turning into a reality, at that point we ought to be safe. In a vibrant and large democracy like India which holds the title of conducting the biggest electoral practice in the world, issues of political mayhem and electoral malpractice are becoming grim year after year with this once considered a holy festival of our republic touching its low ebb (Cachin, 2016; Rathee et al. 2019). It is needed to ensure fair and free election across the globe in democratic countries, by allowing voters safety to cast their free decisions. In democratic countries, voting is a process where people choose their government by making their decisions through registration and cast their votes (Tsang & Wei, V.K, 2005; Christian & Carter, 2005). However, it is much necessary to avoid manipulations and provide integrity during voting process. Further, security and privacy of voters during their voting casts where paper based scheme was used before introduction of EVM. The EVMs or Electronic Voting Machines came into being, that had marvelous advantages over paper ballots however, voters have to cast their votes at polling stations only (Zissis & Lekkas, 2011; Moynihan, 2004; Keller, 2006). Elections anywhere in the world are a very daunting affair where individuals use every kind of manipulation to gain seats in the office. In India especially, some of the risks involved is voter manipulation, spreading of fake news, hacking and extreme files of violence basing damage to property and life. EVM counters many such issues for example Bogus voting, cost saving and providing faster result but there is still room for expansion and more security. Blockchain can play a very important role in ensuring that the voters registering their votes are legit and the vote counts are not manipulated in any way. Further, it is desired in current times where the world is accessible to people in their smart phones to also offer them the chance to register and cast their votes irritate free via their smart phones without worrying about the system receiving hacked. Blockchain is a distributed ledger that stores information in the form of blocks where each block associated to the next via cryptography (Yavuz, 2018; Goguen & Meseguer, 1984). It is distributed, decentralized and immutable that makes it nearly unfeasible to tamper with. When blockchain is applied in the procedure of voting will have a proper user account for every valid Voter ID holder and will therefore nullify the risk of a single person voting multiple times. Also, once every individual has an application in their smart phones, it is not requisite to stand in long line in the polling stations and panicking any kind of poll aggression. It will provide a kind of transparency that will not let the results be questioned and provide a new poise to the voters as depicted in Figure 1.

Figure 2. Proof-of-work using Blockchain in voting application



Blockchain technology is still without a doubt so in its earliest stages. Blockchains are moderate, user unfriendly, unscalable, and costly. For instance, DApps created on Ethereum require the end user to initially buy Ethereum and afterward pay a transaction fee each time they accomplish something in the DApp. Then again, EOS expects developers to buy over the top expensive RAM to build up a DApp while the users get transaction fee, simply after the user gets some EOS, downloads an EOS wallet from github, makes a key pair and sends EOS to that key pair. Not to speaking to the average consumer who could think less about decentralization. The fact of the matter being that Blockchain technology needs to develop before mainstream adoption happens (Hjálmarsson, 2018; Aitzhan, & Svetinovic, 2016). UI will be absolutely critical thus will administrations. A Blockchain that takes care of an enormous real-world problems, finds a harmony among decentralization and administration while giving speed, scalability, cost viability, and an overall smooth user experience will be the Blockchain that ascents above them all. 2018 was an incredibly dynamic year for Blockchain and crypto currencies. Numerous jumps in advancement were made and Blockchain is entering the worldwide awareness increasingly every day (Wüst & Gervais, 2018; Taylor et al. 2019). The subject of mass selection is when, not in the event that it occurs. We unquestionably observe this occurrence very soon, however as things remain at the present minute, the Blockchain space still makes them develop agonies to traverse. All the weaknesses of the Blockchain can be removed using three different consensus protocols named proof-of-work, proof-of-stake and proof-of-useful-work. A brief summary of these three protocols are given in Figure 2.

The proposed layout is based on a smart contract, using Ethereum to generate an e-voting app. The users have to create an account with proper confirmation done via id and other biometric schemes. Every transmission done via this account which in this case will be registering vote will be verified by a miner. The miner further has taken into account the voter's permanent address depends on voter id and thereby conveying that vote to a vote pool of that constituency. Every vote registered will be done via biometric schemes and the miner will verify the authenticity of the vote. This will counter the issue of bogus votes. Biometric data will remain in the peer to peer network and will be very difficult to obtain otherwise. Once the election date of the electorate has passed and there is any other vote registered, the miner may cancel the request. Similarly, if the biometric authentication has failed for the user, the request will be cancelled by the miner.

The remaining organization of the paper is defined as follows. Section II illustrates the literature work. The e-voting application using blockchain technology is described in section III. Further, the performance metrics of e-voting application is presented in section IV. Finally, section V concludes the paper.

RELATED WORK

This section illustrates the number of security methods in voting procedures proposed by several scientists/researchers. For instance, Salahuddin et al., 2018 have projected an agile and softwarized system for providing a secure, flexible and cost efficient, privacy IoT deployment system in smart healthcare services and applications. Further, kang et al., 2019 have proposed a blockchain enables security system by addressing the security and privacy issues among Internet-of-Vehicles (IoV). They have proposed a two-stage solution that is data verification and miners selection by designing a reputation based voting approach and past summary interactions. The selection of miners is done by analyzing behavior of each device and consulting their previous interaction before including them in communication process. The proposed reputation and blockchain based approach was simulated over different data sharing results in IoV. Though, wireless networks ensured a vital role in the support of IoT solutions, however, the comparison is not adopting them properly. The reason of not adopting the IoT with wireless networks is various privacy and security challenges. Though researchers have proposed various security solutions to avoid these limitations.

She et al., 2019 have projected trusted approach using blockchain technique to identify the malicious behavior of communicating nodes in wireless environment. They have proposed a trust based scheme with the integration of blockchain to provide transparency and immediate identification of malicious devices. Further, the authors

have realized the detection of malicious devices through smart contracts and node's quadrilaterals. The simulated graphs depicted the efficiency that is able to trace and identify every single malicious behavior in real time environment. Moreover, the management and efficiency enhancements, several oil and gas companies have shifted towards digitalization by simply adopting blockchain. In addition, Lu et al., 2019 have reviewed the importance and usage of blockchain in oil and gas industries in several aspects such as trading, management, supervision and cyber security. Finally the authors have also highlighted the usage of blockchain at just in their initial levels because of their new systems, transformations and techniques.

Lamas et al., 2019 focused on reviewing various blockchain integrated applications by emphasizing on their security and privacy challenges. They have discussed various business models creating and car economy disruption and their solutions with blockchain integration. In addition, they have highlighted the threats, strengths and weaknesses by recommending various companies and guidelines in futuristic developments. Further, Jarodi et al., 2019 have focused on only one application of blockchain i.e. industries by highlighting or discussing various challenges, benefits and opportunities in other use cases also. They have highlighted various implementation requirements for integrating the blockchain technique in industries. The authors have integrated the blockchain usage in financial areas where digital payments for verifying the financial transactions deployed on various proxy nodes are integrated through blockchain mechanism. They have projected several probability based metrics for realizing the rigorous operations and demonstrated the feasibility with near field communication on raspberry pi mobile wallets and mining nodes applications. For reducing the redundancies and inconsistencies in voting phenomenon, e-voting has altered traditional voting schemes. However, the e-voting further leads to several security and privacy issues with the growth of time. Shahzad & Crowcroft, 2019 have applied blockchain in voting procedures by block sealing to provide transparency. The proposed approach described the hash utility, information accumulation, polling generation, creation, sealing in blocks till the declaration of results. The proposed scheme has claimed the security and management of issues by ensuring an enhanced digital voting approach. Kdhetri & Voas, 2018 have projected a blockchain based e-voting process by increasing the access rights to voters and reducing the access rights to other entities. The registered voters are allowed to casts their votes through online such as computer based or smart phones through blockchain. The authors have presented a proof id of each voter's to ensure transparency during votes. The proposed scheme is further highlighting various potential challenges. Further, Anjum et al., 2017 have discussed and illustrated several blockchain use cases to highlight their importance in today's era. They have tracing of products, smart healthcare, industries and other verification processes. Though the continuous increment of shifts in health services, information is secured by limiting their access rights and

applies crypto schemes to further identify privacy and security concerns. Further, the authors Esposito et al., 2018 have projected the blockchain usage that may clearly provide the security in health services over the clouds. In addition, Espocito et al., 2018 have described the potential issues with their future perspectives.

PROPOSED SOLUTION

Our application determines the vote count of the voter for certain people who are to be selected. Firstly, in this application, we determine the illegibility of the voters using blind signatures. For high availability and result immutability of privacy using double private block chain and using bit coin logic to redesign transactions and new protocols to cast a vote. The proposed system will contain 1) Anonymity, 2) Check flag for voter's illegibility, 3) Voting integrity with the system and 4) Vote Verification.

Different Phases in the System

Publishing phase

It's a dummy approach to publicize the system and generating candidate ballots. The Authority has eligible bling signature which are communicated securely to prevent any attacks like DOS, Men-in-the-middle Attack

Login phase

After the publishing phase, the voters will login and then verification will be done for eligibility. This phase also deals with the impersonation and EIDs establishment.

EID generation phase

This phase will be used to generate public private key for electronic identity. For every identity made, an EID password will be established in order to prevent tampering and impersonation. Generation of OTP can also be done.

Voting phase

For the generation of Block chain transactions, our Voting phase will ensure data consistency and isolation.

Figure 3. Implementing blind signatures

Blind signatures

These digital signatures are heavily used in our application for transactions working. Eligible voter sign and extract public and private keys and encrypt them in Ballot. This Ballot is sent to Electoral Authority (admin) and verifies the source of the ballot, removes outer envelope and Encrypt the keys and sends back to the eligible voter as depicted in Figure 3.

System Protocol

This phase depicts the working of voting application using different phase.

Threat Model

Various models have been taken in care for the full functionality of the Block chain without any foreboding of threat initiation. As Block chain helps with Decentralization, and impenetrable security level, various threats are seldom to be seen. Some of the most common threats are DDoS Attack, Sybil Attack, Freak Attack, Malwares, Cross Site Scripting (Xss) etc. the compete proposed solution of e-voting through blockchain is depicted in Figure 4.

Evaluation

After the completion of the project, we will study all the sufficient properties of the proposed system design and these are availability of the project, Integrity with the OS and web page, Uniqueness, Accuracy, and Election secrecy.

Figure 4. Proposed complete Solution

Some Other Security Analysis and Legal Issues

Security Analysis

i. DDoS: For the application to fail under DDOS Attack, the attacker must perform it on every node in the network. But tampering with the boot nodes will eventually inform the institution and the location could be found out. For locating failed blocks, we can use fault tolerance algorithm
ii. Authentication Vulnerability: As the value of the hash will be unique to each and every individual or eligible voter, there is seldom chance of multiple voting process by the voters. This will not only helps with the ease to finalize the output result with incrementing by +1, but also eradicates out the total chances of the system malfunctioning.
iii. Sybil Attacks: The consensus algorithms implemented in the project are prone to these attacks. Furthermore, with the incoming of the strong cryptography features and limited access to the ledger, Block chain solves today's most often security problems

Legal Issues

i. Transparency: No method of transparency can be offered to the voters in today's electoral scheme. Without some other tech involvement, the transparency In the system is a very tedious task with formulation of new law by government officials.

ii. Voter Privacy: Voter privacy in pen and paper scheme is meandering which may involve leakage of voter credentials and vote to the party or the candidate. To satisfy the privacy, initiation of non-traceable vote will be prominent to implement.

iii. Remote Voting: To prevent coercion resistance in the election, remote voting could be of good use. If the results can be used in websites, or mobile applications, there is no chance of misconfigured results, but on the negative side, people with good hacking skills can take down host website and different threats can be introduced. This requires security. We can use Block chain features to subdue these affects.

Comparison

Traditional Blockchain Solution: In the traditional Blockchain solution, we can observe the common implementation of lit coin, dash, ripple and many other programming languages based bit coin implementation. There is less privacy though, if implemented in suitable domain of programming languages.

Proposed Blockchain Solution: Our platform implements all the solution in Ethereum, solidity and other bitcoin consensus protocols to be in use, usage of RSA algorithm can also be implemented with the generation of private keys. Table 1 depicts the comparison among traditional and proposed blockchain voting application.

As the scope of this paper does not end till execution as more functionality can also be appended such as login-logout scenarios, more data related storage for large count of voters.

Table 1. Traditional Blockchain Solution Vs Proposed Blockchain Solution

Traditional blockchain solution	Proposed blockchain solution
Operated with decentralized property	Operated with decentralized property
Programming tools: Native Programming Languages (Java, Python, C++, ASP.NET, C#)	Programming tools: Ethereum, Solidity, web3.js
Time of Transaction: Minutes	Time of Transaction: Seconds
Implementing client server architecture and RDBMS	Facilitates P2P architecture and smart contracts; no RDBMS required

The main idea of proposing this Blockchain solution for voting system is to make electoral system cheaper and quicker. By doing this, the barrier between voter and officials to be elected will be an endgame. Furthermore, with the ease in operation, we can assure a direct form of democracy as people will be in more ease

to use it and give a better result in return without any involvement of central agency. In the report, we implemented a simple voting application using smart contracts (solidity, Ethereum) for proper conduct of system execution while maintaining security features like privacy and authentication verification. By comparing with the current process of electoral system, we can observe that block chain technology has a new future for democratic countries where most of it are pen and paper based. Using the Ethereum private block chain, we can transmit hundreds of transaction in one second, for countries with bigger democracy; this system can provide well executed result with seldom chances of result tampering. With the use of modern hash algorithms makes the data fetching impenetrable and isolated within each and every block. Decentralization has made the platform much more secret and private than that of centralized systems. Our proposed system will ensure that all the block chain concepts will be executed properly resulting in better approach to implement the platform practically in the provinces or the region.

PERFORMANCE ANALYSIS

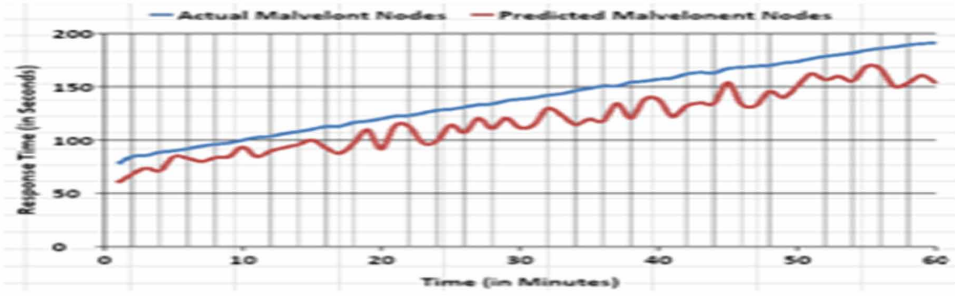
System State

For providing the verification and validation of proposed approach, the numerically simulated results are verified over NS2. The analyzed metrics are analyzed against various security measures over various metrics. Though, security analysis of e-voting is considered to be a very challenging task. In this manuscript, we have proposed a blockchain based voting method which not only ensures node's security but also provides transparency in the network. In the proposed voting frameworks, network simulator version 2.5 having predefined various nodes is executed. 500*500 network area is generated having various numbers of nodes. Further, for verifying the security procedures, nodes metrics are measured where most of them are hacked by various attackers. The malevolent devices are further added on probability basis. The response time and accuracy based on malevolent node prediction is analyzed against varying number of nodes. The execution of proposed framework is accomplished for one minute.

Evaluated Performance Metrics

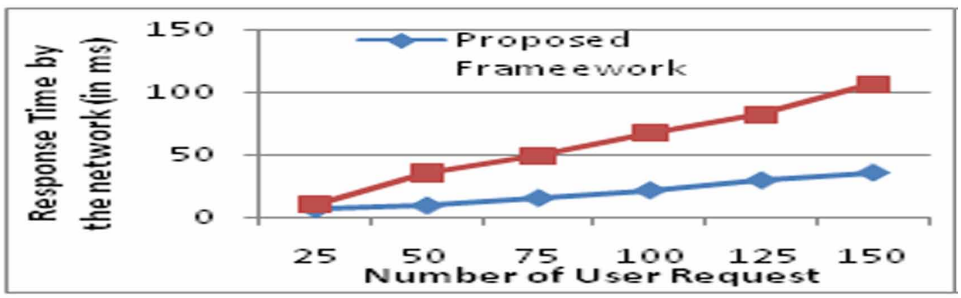
Number of measuring parameters such as response time, accuracy, number of processed request and resource utilization are evidenced on mentioned test bed. The depicted figures represent proposed and traditional mechanisms over certain metrics. The depicted graphs 5 and 6 shows the accuracy and response time of

Figure 5. Accuracy to predict malevolent nodes



detected malicious nodes over varying number of nodes. Proposed scheme close to 83% accuracy against malevolent system is predicted. In addition, it is supposed the response time of proposed approach augments better results than traditional mechanisms. Traditional approaches are not able to productively able to guarantee transparency that may further cover way to reduce response time and accuracy of individuals who cast their voters and voting counts. Whilst proposed mechanism that is based on Blockchain that successfully able to remove and detect the malicious activities of devices.

Figure 6. Response Time with presence of malicious devices

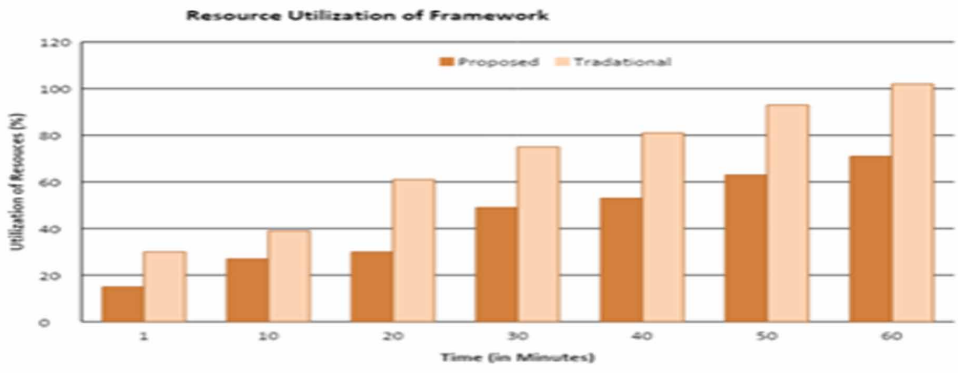


In addition, the transparent feature of proposed approach provides the trust among polling/ voting procedures. The framework analysis is further measured against resource utilization as revealed in Figure 7, 8. All the depicted figures clearly realistic that the nodes augmentation is linear and the processed requests also enhances linearly.

Proposed scheme is close to 83% accuracy for the malicious devices prediction which may be further enhanced if simulation runs for longer time. Further, it is

alleged that proposed scheme response time from sensors will augment as depicted in Figure 7 shows better values than existing system.

Figure 7. Resource Utilization in Fog Environment 1



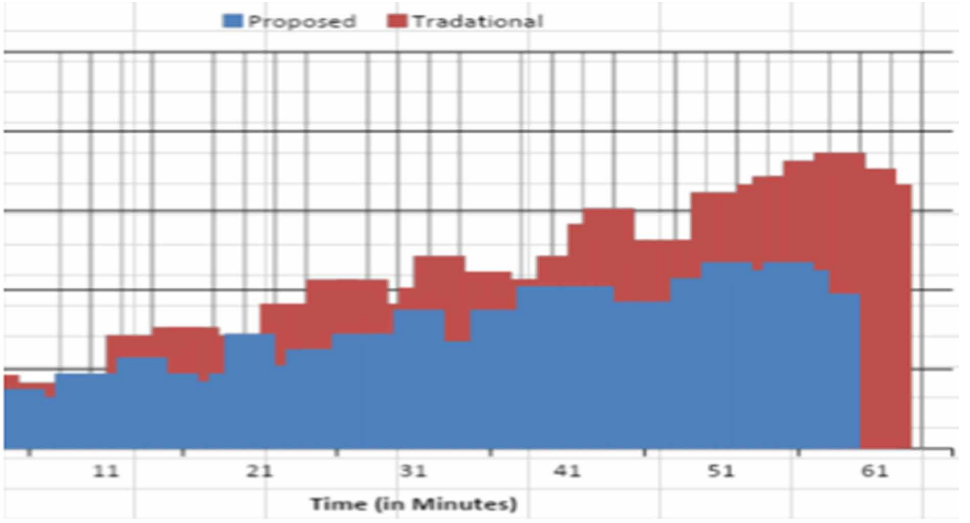
Here, traditional schemes are not efficient to identify or able to eliminate malevolent nodes from the environment that further escort to increase in response time of the traditional system. However, in proposed phenomenon that detects any malevolent node and able to instantly remove it from the network so that it does not obstruct the performance. This analysis further results in improved response time and resources utilization as revealed in Figure 6, Figure 7. Moreover, Figure 8 depicts the number of processed request by the proposed system regarding linear trend for all three networks. It can be clearly practical augmentation is linear the proposed requests also lead to linear time.

Discussion on Evaluated Results

The proposed and traditional voting schemes have been detected over various numbers of devices. The simulation evaluation is victorious where various several results over certain metrics were recorded. The evaluation of simulation conduction was victorious where numbers of concerned results against several parameters were recorded. The proposed blockchain based voting approach behaves as preferred having an optimized analyzed metrics over traditional procedures. In addition, the accuracy of Blockchain based on voting scheme enabled framework reached to 83% that can be further improved and superior over increased period of time. Moreover, remaining metrics such as response time, processed request during malicious environment provides better results. The removal and detection of malevolent nodes in proposed scheme is entirely based on Blockchain technique to provide transparency

and security among all the devices. Any alteration and change in polling process may immediately change the remaining polling stations and authorized individual's information.

Figure 8. Number of processed request by each network through a linear line



CONCLUSION

This manuscript has proposed a secure online voting mechanism based on Blockchain approach. The proposed framework provides the security by intimating and capturing each and every illegal and legal activity of the voters and counting EVM's. The proposed Blockchain voting framework has considerably enhanced the accuracy, response time, number of processed request and resource utilization against traditional mechanisms in the presence of malicious nodes. Furthermore, the simulated results of proposed scheme show 83% accuracy compared to traditional voting procedures. The real time situation where EVM can instantly detect the malevolent activity and blocked will be reported in future directions.

REFERENCES

Aitzhan, N. Z., & Svetinovic, D. (2016). Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Transactions on Dependable and Secure Computing*, *15*(5), 840–852. doi:10.1109/TDSC.2016.2616861

Al-Jaroodi, J., & Mohamed, N. (2019). Blockchain in Industries: A Survey. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 36500–36515. doi:10.1109/ACCESS.2019.2903554

Anjum, A., Sporny, M., & Sill, A. (2017). Blockchain standards for compliance and trust. *IEEE Cloud Computing*, *4*(4), 84–90. doi:10.1109/MCC.2017.3791019

Cachin, C. (2016), July. Architecture of the hyperledger blockchain fabric. *Workshop on distributed cryptocurrencies and consensus ledgers*, *310*, 1-4.

Christian Schaupp, L., & Carter, L. (2005). E-voting: From apathy to adoption. *Journal of Enterprise Information Management*, *18*(5), 586–601. doi:10.1108/17410390510624025

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation*, *2*(71), 6–10.

Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K. K. R. (2018). Blockchain: A panacea for healthcare cloud-based data security and privacy? *IEEE Cloud Computing*, *5*(1), 31–37. doi:10.1109/MCC.2018.011791712

Eyal, I., Gencer, A. E., Sirer, E. G., & Van Renesse, R. (2016). Bitcoin-ng: A scalable blockchain protocol. *13th USENIX Symposium on Networked Systems Design and Implementation*, 45-59.

Fraga-Lamas, P., & Fernández-Caramés, T. M. (2019). A Review on Blockchain Technologies for an Advanced and Cyber-Resilient Automotive Industry. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 17578–17598. doi:10.1109/ACCESS.2019.2895302

Goguen, J. A., & Meseguer, J. (1982). Security policies and security models. In *1982 IEEE Symposium on Security and Privacy* (pp. 11-11). IEEE. 10.1109/SP.1982.10014

Hjálmarsson, F. Þ., Hreiðarsson, G. K., Hamdaqa, M., & Hjálmtýsson, G. (2018). Blockchain-based e-voting system. In *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)* (pp. 983-986). IEEE.

Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. *Harvard Business Review*, *95*(1), 118–127.

Kang, J., Xiong, Z., Niyato, D., Ye, D., Kim, D. I., & Zhao, J. (2019). Towards Secure Blockchain-enabled Internet of Vehicles: Optimizing Consensus Management Using Reputation and Contract Theory. *IEEE Transactions on Vehicular Technology*, *68*(3), 2906–2920. Advance online publication. doi:10.1109/TVT.2019.2894944

Keller, A. M., Mertz, D., Hall, J. L., & Urken, A. (2006). Privacy issues in an electronic voting machine. In *Privacy and Technologies of Identity* (pp. 313–334). Springer. doi:10.1007/0-387-28222-X_18

Kshetri, N., & Voas, J. (2018). Blockchain-enabled e-voting. *IEEE Software*, *35*(4), 95–99. doi:10.1109/MS.2018.2801546

Lu, H., Huang, K., Azimi, M., & Guo, L. (2019). Blockchain technology in the oil and gas industry: A review of applications, opportunities, challenges, and risks. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 41426–41444. Advance online publication. doi:10.1109/ACCESS.2019.2907695

Moynihan, D. P. (2004). Building secure elections: E-voting, security, and systems theory. *Public Administration Review*, *64*(5), 515–528. doi:10.1111/j.1540-6210.2004.00400.x

Pilkington, M. (2016). 11 Blockchain technology: principles and applications. *Research handbook on digital transformations*, 225.

Rathee, G., Sharma, A., Iqbal, R., Aloqaily, M., Jaglan, N., & Kumar, R. (2019). A blockchain framework for securing connected and autonomous vehicles. *Sensors (Basel)*, *19*(14), 3155–3165. doi:10.339019143165 PMID:31323870

Salahuddin, M. A., Al-Fuqaha, A., Guizani, M., Shuaib, K., & Sallabi, F. (2018). *Softwarization of Internet of Things infrastructure for secure and smart healthcare*. arXiv preprint arXiv:1805.11011

Shahzad, B., & Crowcroft, J. (2019). Trustworthy Electronic Voting Using Adjusted Blockchain Technology. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 24477–24488. doi:10.1109/ACCESS.2019.2895670

She, W., Liu, Q., Tian, Z., Chen, J. S., Wang, B., & Liu, W. (2019). Blockchain Trust Model for Malicious Node Detection in Wireless Sensor Networks. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 38947–38956. doi:10.1109/ACCESS.2019.2902811

Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K. K. R. (2019). *A systematic literature review of blockchain cyber security*. Digital Communications and Networks. doi:10.1016/j.dcan.2019.01.005

Tsang, P. P., & Wei, V. K. (2005). April. Short linkable ring signatures for e-voting, e-cash and attestation. In *International Conference on Information Security Practice and Experience* (pp. 48-60). Springer. 10.1007/978-3-540-31979-5_5

Wüst, K., & Gervais, A. (2018). June. Do you need a Blockchain? In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)* (pp. 45-54). IEEE. 10.1109/CVCBT.2018.00011

Yavuz, E., Koc, A. K., Çabuk, U. C., & Dalkılıç, G. (2018). March. Towards secure e-voting using ethereum blockchain. In *2018 6th International Symposium on Digital Forensic and Security (ISDFS)* (pp. 1-7). IEEE.

Zissis, D., & Lekkas, D. (2011). Securing e-Government and e-Voting with an open cloud computing architecture. *Government Information Quarterly*, *28*(2), 239–251. doi:10.1016/j.giq.2010.05.010

Zyskind, G., & Nathan, O. (2015). May. Decentralizing privacy: Using blockchain to protect personal data. 2015 IEEE Security and Privacy Workshops, 180-184.