Blockchain-based Electronic Voting System for Modern Democracy: A review

DylanWeiss, Jacob Wolmer, and Avimanyou Vatsa
22dweiss@tenafly.k12.nj.us, 22jwolmer@tenafly.k12.nj.us, avatsa@fdu.edu

Abstract - **Electoral integrity is not only imperative for countries that are ruled by democracy, but it is also influential in enhancing public voters' confidence and accountability. Also, security, integrity and, trust are three essential pillars of fair and modern democracy. The use of blockchain technology leverages the expected level of protection. Also, it provides cheaper, faster, and immutable service to the liquid democracy where voters can review their casted votes at any instant. Thus, there is a need to use blockchain-based electronic voting systems. E-voting systems can be defended easily and efficiently using the blockchain principles of universal ownership, transaction format, and storage in a chain. Another wall between freedom and the fall of democracy is that to change results; one would need approval from everyone who voted and to go back through each block in the chain to get to a specific transaction. Using Smart Contracts erase the middleman of current systems and are digital documentation of the transaction and proof for certification of votes. Also, this system fulfills the essential requirements of e-voting systems which includes: no coerce to voters, no traceability of voters' identity, the assurance and proof of vote, no one could change the casted votes, the counting of votes and election result must be decentralized, security and integrity of ballot to cast individual votes. There are many proposed frameworks are available in the literature. Therefore, this paper reviewed those existing frameworks and found the essential requirements and possible solutions to implement in the e-voting system.**

Index Terms - e-Voting System, Blockchain, Ethereum, Democracy, Federal Election Commission (FEC).

INTRODUCTION

Electronic voting (e-voting) has become increasingly popular in our technology-driven world. Not only do countries vary in the form of electronic voting, but they also vary in the amount of usage, with countries like Brazil relying solely on electronic voting and countries like Italy only beginning to experiment with electronic voting methods in 2006 [3, 21]. The different forms of e-voting range from the use of punch cards, optical scan systems, and direct recording electronic (DRE) voting systems to voting via Internet ballots and telephone votes.

Initially, e-voting was proposed to solve the challenges of paper-based voting to ensure accurate and bias-free elections. While adopting an e-voting system, one must ask: Why is the electronic voting system considered a better option than a traditional ballot voting paper? It not only improves democracy but is expected to be a solution for some problematic situations such as improving accessibility to the election, the elderly, and the disabled ability to vote, increasing election turnout, and being easy to operate getting a quick result. However, it is well-known that operating e voting systems under strict security procedures is crucial, primarily when relying on advanced encryption techniques [6]. Security issues concerning e-voting systems have been extensively studied in the literature. The studies show that the utilization of e-voting may entail the following challenges: data integrity, reliability, transparency, the secrecy of the ballot, consequences of breakdown, uneducated voters, specialized IT skills, storage of equipment, security, results of fraud, and cost.

E-VOTING SYSTEMS BENEFITS AND CHALLENGES

The e-voting system has many benefits. It is very convenient in vote casting because it eliminates transportation and postage on paper ballots. A quality e-voting system would allow people to forego the usual hurdles for casting a vote and increase election participation [3, 21]**.** However, these remarkable benefits come with many challenges. People are afraid when it comes to voting online due to election tampering. There is the possibility of malicious activities, including malware attacks, with internet access.

Additionally, hackers could tamper with votes, election process, and results. Further, many people who aren't familiar with Blockchain Technology (BT) could eliminate the above drawbacks. The features of emerging and evolving BT may solve issues like election tampering, decreased voting accuracy, and disenfranchisement [3, 6, 9, 13].

The confidentiality, authentication, and integrity of e voting is also a remarkable and challenging issue. Thus, the DRE voting machines or kiosk voting (forms of e-voting in a polling station or another area that election officials supervise) solve the voters' identification issues, but it looks like a similar process as we have been using in the traditional voting system. Furthermore, voters authenticate themselves with an electronic ID card with remote Internet

voting. If such a system does not exist, they can authenticate themselves by using a combination of username, password, due authentication, and associated personal information [3, 13, 20].

A necessary precondition is an electronic voters' registration. In the case of voter identification, additional arrangements need to be in place to ensure that the voters' identity may not be linked to the content of their vote. Specific cryptographic or BT security measures are needed in order to guarantee that these two sets of information cannot be connected at any time and under any circumstances (secrecy of the vote). Also, it is essential that these measures are reliable and they can be communicated and demonstrated to interested stakeholders [3, 5, 6].

A secure electoral process ensures that votes are counted in accordance with the will of the voters. In civiciti's e-voting processes, in addition to logical and physical protection layers, mechanisms are established to ensure that only users accredited by an official document participate so that all security guarantees are provided that equate the electronic voting process with a classic electoral process [17].

Another issue is the psychological and social aspects; making people believe in this new reality is necessary. There is much skepticism aimed at anything online replacing the authentication and integrity of paper ballots. Especially BT, which is relatively new and not known widely in the general public. Many believe it is a scam due to the fact that it is tough, almost nearly impossible, to differentiate legitimacy and fraud. Due to the truth is relies on an individual verifying their vote, there can be significant pressures. A local man can force someone else to vote how he wants to as the only way to approve the vote is by the individual, and someone can physically force you to vote a particular way. Many also believe that it does not solve many of the issues that voting has, in fact, it only creates more. It is impossible to detect using BT to know if a vote has been hacked and altered prior to its receiving in the blockchain system (meet in-middle attacks). There are a few issues to BT voting systems that are crucial to solving in order to replace the current election system [16,18,19].

USEFULNESS OF BLOCKCHAIN TECHNOLOGY AND SMART CONTRACT

BT is a decentralized system that enables connected and shared securely and immutable information. The simplest form is blocks of information that are connected one a chain which is a public digital database [3, 22]. The idea that blockchain is public is very important because it creates a system of checking. There is no one ruler or commander of blockchain technology; therefore, it is more secure and immutable than other systems. The blocks in the system are essential and remarkable for three main reasons. First, they share a plethora of information about transactions on aspects such as date, time, and dollar amount. It also stores information on the person who made the purchase and from what. But it has a safety aspect, so the name displayed is not the actual name of a person but rather a code (public key), so others do not know your personal information on your purchases. The technology also uses hash code (cryptographic hash), creating a secret code for your transaction that is so unique that it is impossible to tell what it is. Even if someone purchases something very similar to what you did, the hash code would be extremely different. Blocks can also store a few MegaByte (MB) of data, which means that each block can hold any different transactions from many different people [2, 9]. Each new transaction is added to the chain. To have the block added to the chain, four things happen. First, a transaction has to happen. Then, it has to be verified, and this is a crucial step because many nodes check to see this, which secures the integrity and safety of blockchain. Next, the block is stored. And finally, the block has a unique hash assigned to it [2, 9]. There are four main benefits to the security aspect of BT. The first is immutability, or no other person can change data. Next is tamper prom, which essentially makes censorship impossible. Then security hacking is protected against, and there is no centralization, so hacking is much more complex. And lastly, zero downtime, which means applications are always running and can never be turned off.

BT leverages the opportunity to have secure e voting that protects the privacy and integrity of the individual (voters, candidates, and FEC personnel, etc.) and correctly counts the number of votes without any interference. Due to the advanced security measures, it is nearly impossible to hack the associated data or activities. Since it is a chain, going back and changing something would essentially mean one must go back and change everything on the chain after that point. Also, the uniqueness of the hash code makes it even harder to hack. No one can figure out what each hash means therefor, it would be impossible to hack if one did not know the hash code. And, the voters' authentication, privacy, and integrity would be held as no one knows who each individual is because of the code number that acts as a username for each individual person. Lastly, the verification system that involves many computers would be nearly impossible to attack. Overall, the BT has fascinating security aspects that make it very close to impossible to attack and change the votes. The smart contracts of BT and cryptographic methods are a great way to collect and count votes. Additionally, it fulfills the requirements of remote voting and protects the democracy in a fair and trustworthy way [1, 3, 5, 7, 8, 14, 22].

Smart contracts are a new and advanced way to essentially "erase the middleman" in an exchange of anything from money to the property to shares of a value. Smart contracts are significant because they clearly show the rules and penalties that are similar to a contract. Still, they also automatically enforce those rules in the agreement. Vittalik Buterin nicely states, "in a smart contract approach,

an asset or currency is transferred into a program and the program runs this code and at some point, it automatically validates a condition and it automatically determines whether the asset should go to one person or back to the other person, or whether it should be immediately refunded to the person who sent it or some combination thereof."

Smart contracts are also a good tool as they create an automatic receipt that replicates the document and stores it for security purposes and integrity to create fewer issues further down the road. The smart contract is written in code that is highly useful due it being simple yet complex. It identifies and portrays the rules and regulations of an agreement and erases the need for a middleman. The contract helps with the security aspect as it creates digital documentation and receipt of any transaction. It is also helpful because it is a validation tool to ensure something happens or does not happen. Smart contracts are revolutionary and help in many different ways [4, 20].

Smart contracts are very unique and useful. It is an extremely useful tool that can propel blockchain and even society's services further. The ability for the smart contract to initiate the agreement is one of the many essential steps that it takes to achieve the overall goal. Also, the fact that it checks for verification is critical and crucial in the sense that it can help with other projects (including the e-voting system) by securing the data and helping reduce the risk of violating the integrity and hacking. Smart contracts make it clear what is being agreed upon and verify the transaction. Also, they "erase" the middleman because the contract themselves establishes the principles in the agreement going forward. This helps even more with the security aspect as it makes it so no one will have to rely on a third-party source that can potentially be biased or interfere with important matters such as online voting. Lastly, they create an online receipt that makes ensuring and validation even easier so no lies can be told essentially and there is forever data and evidence of something. Smart contracts are very important and are helpful in numerous ways [3, 12, 15, 20].

BLOCKCHAIN TECHNOLOGY FRAMEWORK: ETHEREUM

Ethereum is a platform that is available for everyone across the globe that is decentralized so not run by anyone who is primarily focused on money and other general applications (e.g., e-voting). It is a platform that enables people to write their code for applications for others to use globally. It is based on blockchain technology but is simpler and easier to use source to build and deploy applications (e-voting). It focuses on the coding aspect and uses people's code to run projects. The token (cryptocurrency) is called an Ether in the platform, but gas is also needed to execute a task. The beauty of it is that there is no possibility for any disruptions such as fraud or interference. Ethereum is unique because it does not have a limited amount of operation, giving the developer more freedom. Ethereum is unique and platforms independently because it has a specific Ethereum Virtual Machine (EVM), enabling anyone using any language to use the platform. This helps make different applications all in one same site. It saves a lot of time and is extremely efficient. Ethereum allows any centralized system to be decentralized and not have/run by a single person or network. Ethereum also uses DAO's (Decentralized Autonomous Organizations), which are autonomous and decentralized and use code under the smart contracts which are created on the platform [3, 8, 10]. The basic principles of DAO's are "owned by everyone who purchases tokens, but instead of each token equating to equity shares & ownership, tokens act as contributions that give people voting rights." Ethereum is so universal that is enables other applications and more cryptocurrencies (Ether) to be based and off from Ethereum. The downside is that humans create smart contracts, so they can be prone to human error, creating issues further down the road. Ethereum has many upsides and is a new and efficient way to build, design, implement, and learn.

HOW AND WHY IS ETHEREUM FRAMEWORK A GOOD FIT FOR AN E-VOTING SYSTEM?

Ethereum is the perfect fit for voting systems due to the many factors and benefits that come with it. First, e-voting systems need to be equipped and ready to handle attacks and be very secure to avoid such problems. In addition, there is the factor that it is run by everyone involved, not one group, so it is even harder to hack. Furthermore, it is a blockchain technology with its many cryptographic benefits, like a public key, digital signature, and hash coding that makes it impossible to go back and alter the data. Thus, Ethereum is very secure and can implement e-voting systems. There are numerous benefits, and it has the necessary detection against hacking and changing data is essentially impossible due to the complex and intricate technology that is inside of Ethereum platform [4, 16, 18, 19]. The programming language used to implement the e-voting and other applications are Solidity. Due to its specificity and easily to handle language with a large amount of data, it is the best with e-voting [3, 15, 20]. Since the elections will have millions of transactions, the language needs to be able to handle large amounts of data, which is the main reason solidity will be used [2].

PROS, CONS, AND SOLUTION OF A NEW E VOTING SYSTEMS

E-voting systems have been around for a long time, but there are many cons. Manually having to go to a specific place can put a strain on voting and make people less likely to vote than voting digitally online. An example of this includes during the coronavirus pandemic (COVID-19), voting

cannot be taking place as people should not be in contact with others. Online or e-voting fixes the issue as one can vote from wherever.

E-voting systems have many issues that can potentially be exploited to alter an election. As of now, there are still many flaws in the system that have been deciding leaders of the world. There is also an aspect of unfairness and voter suppression with the current system. States can decide where to put voting areas and put fewer options in areas that tend to vote a certain way. There are many other issues and flaws with the current system that need to be addressed for future elections to prevent the integrity of elections and the democracy that our country was founded on and makes us who we are. It is our duty to protect and establish a right and just system to elect our leaders [5, 7, 9].

Another problem is that voting means taking a lot of time in some cases out of one's day and driving/going to the nearest polling station, which in some cases is miles away. This is another issue as it can steer people away from voting as many values work more and do not want to go through the tricky hassle to cast a vote over voting. The issues that occur right now need to be fixed and they will only create more problems in the future. With the utmost urgency, society transitions to a new form of voting that can ensure fairness and stop the issues that are going on right now.

These are fixed in the blockchain-based e-voting system (e.g., BCT-Voting [3]). Although it solves many other major problems, it is tough for people to accept change and many might be hesitant to adapt to the new BT world. An important strategy to fix this issue is to educate and inform the public on what the new system is and how it operates to know what happens and the integrity and success of the new system. This can be done in various ways. Educating the public on a certain topic can come in all forms. For example, creating many websites makes it easy to learn what is happening and broadcasting on news channels what is happening so those who are skeptical or wish to learn more have the opportunity to do so. The last issue is that someone can coerce and force someone to vote a certain way. This is a problem because only you can confirm your vote virtually. But someone can physically be next to you and watch you and make you vote a certain way. This is a more significant issue of people harming others. If this is the case, it is best to report this to authorities and have them handle the issue as it is a crime to do this. The new system clears the way to a brighter future that can erase the issues of current voting systems. Although its potential brings some problems, these issues can be dealt with and fixed. Therefore, the new online blockchain voting system is the optimal option [10, 11, 13].

Another aspect of the plan is to make it, so people do not have to travel places to vote and do not have to go through the time-consuming and stressful form of voting that is currently in place. The BCT-Voting system is an excellent win for elections as it will ensure that everyone can vote no matter the circumstance as well as being able to protect and continue fair and balanced elections \cite{raikar2021}. Since BCT-Voting is a Dapp, it would mean that anyone can vote from anywhere. Due to the BT in place, it is more secure and non-vulnerable to attacks than current systems. Additionally, smart contracts in the Ethereum framework make it even safer for people to use and keep the integrity of the vote and the election safe and secure. Many small details and preventions, like codes and computer checking, make it essentially impossible to hack [3, 4, 12, 15].

REQUIRED DATABASE AND PROCESSES ON E VOTING SYSTEM

E-voting (e.g., BCT-Voting, etc.) is a voting method that uses electronic devices to record or count votes. The e voting system needs to include registration, verification, voting, tallying phases, and donation module [3, 20]. Furthermore, these steps are involved in the e-voting system: The first process is to register voters and candidates (registration). Then, BT-based authentication is based on voters' credentials on election day (verification, validation, and authentication). Next phase, eligible voters can vote (casting collation). The vote should be encrypted and verifiable. The confidentiality, anonymity, and accuracy of the votes must be guaranteed and cannot be changed or deleted in any way. Finally, e-voting systems counting is done by adding all the votes according to the design (counting presentation of results) [3,20].

THREATS OF VALIDITY AND FUTURE DIRECTION

Several threats may arise when conducting a systematic mapping study. For example, not all relevant sources of voters' credentials may be identified. In order to eliminate this threat, we have to identify the correct source and search criteria on various databases of FEC. The external verification and validation refer to the extent of the results of the trust. It can be generalized for other situations, people and times. In addition, what are the other possible research questions and corresponding solutions that need to be addressed in the e-voting system? Also, do we need to change the platforms/consensus algorithm in e-voting deployment?

Moreover, we may create public and private keys with crypto phrases, a sequence of less than or greater than twelve words. The crypto phrases may be created using smart contract. This will give each user a unique and easy to remember public and private keys that needs to be entered to gain access to the e-voting system. An example of a crypto phrase is "the cat runs donkey fdu yale ronny displacement energy cow mice corn", an easy crypto phrase for more efficiency. Crypto phrase may retrieve on-chain data quickly from the database of BCT-Voting systems.

CONCLUSION

In our systematic review, e-voting as a result of emerging research questions and benefits are discussed in terms of current blockchain research and trends. Further, this paper mentioned issues like current benefits and challenges and the usefulness of BT and smart contrast in e-voting. It contributes to the possible chances of progressive growth and benefit of society or community. In addition, it argued on pros, cons, and potential remedies such that vulnerable threats may differ. Finally, it addressed the possible improvement in the e-voting system for humanity.

ACKNOWLEDGMENT

Fairleigh Dickinson University supports this work under the research release time grant.

REFERENCES

[1] Conway, L. (2020, November 18). Blockchain Explained. Retrieved June 18, 2020, https://www.investopedia.com/terms/b/blockchain.asp [2] Cryptopusco, Bytes and strings in Solidity. Retrieved May 03, 2020, https://medium.com/@cryptopusco/bytes-and-strings-in-solidity f2cd4e53f388

[3] Deepali Raikar and Avimanyou Vatsa (2021). BCT–Voting: A Blockchain Technology Based Voting Sys- tem. The 27th International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA'21), July 26 - 29, 2021, Las Vegas, USA (It is held jointly with the 2021 World Congress in Computer Science, Computer Engineering, and Applied Computing (CSCE'21) - American Council on Science and Education)

[4] Ethereum Developer Resources. (n.d.). Retrieved July 11, 2020, https://ethereum.org/developers/

[5] Fowler, S. Why do Nonwhite Georgia voters have to wait in line for HOURS? Too Few polling places. Retrieved March 18, 2021, https://www.npr.org/2020/10/17/924527679/why-do-nonwhite georgia-voters-have-to-wait-in-line-for-hours-too-few-polling-pl

[6] F. p´. Hjálmarsson, G. K. Hreióarsson, M. Hamdaqa, and G. Hjálmtýsson, "Blockchain-based e-voting system," in IEEE 11th International Conference on Cloud Computing (CLOUD), no. 18079263 in IEEE 11th International Conference on Cloud Computing (CLOUD), (San Francisco, CA), pp. 983–986, IEEE, 2018.

[7] Kirillov, D., Korkhov, V., Petrunin, V., Makarov, M., Khamitov, I., & Dostov, V. (2019, July 01). Implementation of an E-Voting Scheme Using Hyperledger Fabric Permissioned Blockchain. Retrieved January 03, 2021, https://link.springer.com/chapter/10.1007/978-3-030-24296-1_40

[8] Kosinski, John R. "Ethereum Oracle Contracts: Setup and Orientation." Toptal Engineering Blog, Toptal, 17 Oct. 2018, www.toptal.com/ethereum/ethereum-oracle-contracts-tutorial-pt1.

[9] Lopes, J., Pereira, J. L., & Varajão, J. (n.d.). Blockchain Based E voting System: A Proposal, Retrieved May 03,2020, https://aisel.aisnet.org/amcis2019/global_dev/global_dev/14/

[10] Neisse, R., Steri, G., and Nai-Fovino, I. (2017). A blockchain-based approach for Data accountability and Provenance Tracking. Proceedings of the 12th International Conference on Availability, Reliability and Security. https://doi.org/10.1145/3098954.3098958

[11] Kenny Li. Crypto Wallet Vs. Address. Retrieved July 28, 2020, https://hackernoon.com/crypto-wallet-vs-address-54f7fb980bd3 [12] Rosic, A. and Blockgeeks. Smart Contracts: The Blockchain Technology That Will Replace Lawyers. Retrieved July 08, 2020, from https://blockgeeks.com/guides/smart-contracts/

[13] Ruhi Ta¸ and Ömer Özgür Tanrıöver "A Systematic Review of Challenges and Opportunities of Blockchain for E-Voting" https://www.mdpi.com/2073-8994/12/8/1328/htm

[14] Shankland, Stephen. "No, Blockchain Isn't the Answer to Our Voting System Woes." CNET, CNET, 5 Nov. 2018, www.cnet.com/news/blockchain-isnt-answer-to-voting-system-woes/.

[15] Solidity, "Solidity is an object-oriented and high-level programing language," tech. rep., Ethereum Revision, https://docs.soliditylang.org/en/v0.8.11/ (Solidity Documentation Release 0.8.11), Accessed on January 2022.

[16] Hacker Noon , "Technical Guide to Generating an Ethereum Addresses.", 15 Jan, 2020, https://hackernoon.com/how-to-generate ethereum-addresses-technical-address-generation-explanation-25r3zqo

[17] Wang, B., & Sun, J. (2017, August 18). Large-scale Election Based on Blockchain. Retrieved May 12, 2020, https://www.researchgate.net/publication/324513622_Large scale_Election_Based_On_Blockchain

[18] Vatsa, A., Indu Singh and Anju Shukla (2011). Novel Architecture of Delay and Routing in MANET for QoS. International Journal of Engineering Science and Technology 3, 582–591.

[19] Vatsa, A. and Gaurav Kumar (2010). A Novel Architecture for QoS Management in MANET using Mobile Agent. International Journal of Computer and Network Security 2, 113–119.

[20] Jacob Wolmer, DylanWeiss, and Avimanyou Vatsa, "Retrieval of Data from the Database of a BCT-Voting System", IEEE Integrated STEM Education Conference (ISEC), March 26, 2022. (Under review)

[21] Yousif Abuidris, Rajesh Kumar, Ting Yang, and Joseph Onginjo, Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding, ETRI Journal, Volume 43, No. 2, pp: 357-370, Wiley, 2021. DOI: 10.4218/etrij.2019-0362

[22] Baocheng Wang, Jiawei Sun, Yunhua He, Dandan Pang, and Ningxiao Lu , Large-scale Election Based On Blockchain, 2017 International Conference on Identification, Information and Knowledge in the Internet of Things, ScienceDirect, Procedia Computer Science 129 (2018) 234–237, 2018. DOI: 10.1016/j.procs.2018.03.063

AUTHOR INFORMATION

Dylan Weiss, Deep Chain Lab, Fairleigh Dickinson University and a student of Tenafly High School, Tenafly, NJ.

Jacob Wolmer, Deep Chain Lab, Fairleigh Dickinson University and a student of Tenafly High School, Tenafly, NJ.

Avimanyou Vatsa, Assistant Professor, Department of Computer Science, Fairleigh Dickinson University, Teaneck, NJ.