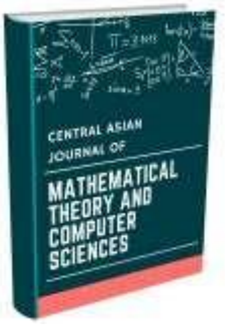

CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES

https://cajmtcs.centralasianstudies.org

Volume: 04 Issue: 5 | May 2023 **ISSN: 2660-5309**

A New Technology of Virtual Voting Based on the Blockchain Network

Hayder A. Nahi
Computer Center, Al Qasim Green University, Iraq
haider.satar@uoqasim.edu.iq

Abstract:

The blockchain is an emerging technology and the virtual blockchain is more emerging that incorporates the many benefits of virtualization and blockchain to create a better efficient and better unassailable technique for executing varied kinds of transactions. This paper offers a novel framework for virtual blockchain-based virtual voting, which takes in the advantages of virtualization and blockchain to construct a more efficient and protected system for conducting elections. The offered framework includes virtual keys, virtual ledgers, virtual smart contracts, and virtual voting components. We executed a sequence of experiments to estimate or evaluate the implementation of virtual voting based on virtual blockchain, and the outcomes of the work showed that the offered framework is highly efficient, accurate, and secure, making it a promising solution for conducting elections in the digital age. The paper contributes to the literature on virtual blockchain and virtual voting and provides insights into the potential of virtualization and blockchain for creating more efficient and secure systems for conducting various types of transactions. Finally, we achieved 1,000 Voting speeds in 10 seconds in contrast to traditional voting and a high smart contract performance in many feature (Execution speed , scalability ad security)..

ARTICLE INFO

Article history:
Received 28 Mar 2023
Revised form 25 Apr 2023
Accepted 21 May 2023

Keywords. Virtual Blockchain, Virtual Voting System, Smart Contract, Security, Virtual Nodes.

.

---***---

1. Introduction

The voting technique is the process via which satisfying the appropriate conditions a citizens have the ability to exercise their freedom to vote in an election. It is a critical characteristic of democratic societies and permits whole citizens to own a voice in deciding the direction of their country. Voting techniques can change relying on the country, or actually, the typical election being held, while the procedure typically involves registration, check-in, receiving a ballot, casting the ballot, and counting the votes.

Virtual voting is the procedure of permitting qualified voters to throw their votes online [1], generally via a secured website or transportable application[2]. The strategy of voting has become more and more widespread in contemporary years, as technology has evolved and further individuals have access to the internet and portable devices. Virtual voting can offer several benefits, including increased accessibility for voters who may have hardness getting to physical voting places, raised efficiency in the vote-counting process, and the potential for increased voter turnout.

A relatively recent idea is "voting through blockchain[3]," which requires utilizing blockchain technology in order to speed up and safeguard the voting process. Blockchain is a decentralized database that enables safe transaction recording and tracking [4][8]. Voting could become more safe, transparent, and open to all potentially qualified voters by utilizing blockchain technology[5].

The greater security that blockchain voting may provide is one of its primary advantages[6]. As every single vote is documented and kept in several places, making it hard for any one individual or organization to change the outcome, the blockchain is extremely susceptible to manipulation or fraud. Furthermore, the use of blockchain can boost transparency and traceability in the voting process, enabling voters to track their votes and make sure they are accurately recorded.

A network of distributed ledgers that are wholly contained within a virtual environment, including a computer network, NFV (Network Functions Virtualization), or cloud-based platform, is referred to as a virtual blockchain [7]. A decentralized network of nodes, or computers, connected via the internet, records and verifies transactions in a virtual blockchain.

Compared to conventional distributed ledger networks, virtual blockchain may provide a number of characteristics. Because it can readily support more nodes and transactions without necessitating costly hardware modifications, it can, for instance, offer better scalability and flexibility. Furthermore, as virtual blockchain can be accessed from anywhere with a connection to the web, it can offer better accessibility and make it easier for consumers to participate in the network and for businesses to begin using blockchain technology[7].

The combination of blockchain-based technology and NFV infrastructure is referred to as NFV-blockchain [7]. NFV is a method of network architecture that involves running software on inexpensive hardware to virtualize network components including switches, routers, and firewalls. As a result, management of networks and resource allocation are made increasingly adaptable and effective.

Improved security, accountability, and transparency in network management and resource allocation are just a few advantages that can come from integrating blockchain technology with NFV architecture. Blockchain technology can make it possible to track network resource utilization as well as access in a safe and transparent manner, facilitating a more effective and equitable distribution of resources amongst users. Furthermore, the blockchain's distributed and decentralized structure can boost security and resistance against hacker assaults and unlawful access.

In this work, constructed a modern and novel virtual voting architecture depend on virtual blockchain (NFV-Blockchain). The virtualization of the blockchain executed through the implementation of NFV on its primary functions, dining each transaction as a vote. When we turned (ledger , client and nodes) to virtual, it was obtain a virtual vote through a virtual blockchain environment. Finally, the smart contract turns into an automatic contract through this virtual environment.

2. LITERATURE REVIEW

The Internet has undergone significant growth in the last 20 years, resulting in a complete transformation in the way people connect, communicate, and exchange information. This growth has also had an impact on politics, with emerging nations initiating digital voting programs to promote democracy for their people. Efforts made in the past to establish blockchain-based e-voting protocols included the creation of incentive schemes for cryptocurrencies. Cruz and Kaji [9] were inspired by recent progress in the field when they suggested an e-voting protocol based on the Bitcoin blockchain. They also explored certain security requirements of e-voting. Meanwhile, Bistarelli et al. [10] presented the End-to-End (E2E) voting system that employs Bitcoin. In this system, the number of votes for each candidate is determined by adding up their tokens in the Bitcoin blockchain. Zhao and Chan [11] designed a framework for e-voting that is comparable to the ones described earlier [9,10] and based on Bitcoin. However, these three protocols have a drawback when it comes to scalability of blockchain-based e-voting systems because the Bitcoin consensus mechanism is both computationally intensive and time-consuming [12]. Several other scholars

[13,14-17] have presented e-voting protocols that use the Ethereum blockchain, which is associated with the cryptocurrency called ether. Through the use of the security characteristics offered by the Ethereum blockchain contract, these studies primarily focused on enhancing the security of electronic voting systems. However, these research did not address the scalability and performance of the blockchain. Recent studies have thoroughly investigated the performance and scalability issues associated with blockchain-based e-voting systems [18,19]. Khan et al. [18] conducted experiments in both permissioned and permissionless blockchain environments and examined various factors, such as the number of voters, block size, block generation rate, and transaction speed. On the other hand, Zhang et al. [19] identified some impractical aspects of e-voting systems based on blockchain. However, their study did not provide explicit information regarding important security features like ballot receipt and uniqueness.

3. PROPOSED FRAMWORK

A blockchain-based electronic voting system typically consists of several key components:

Blockchain: A distributed ledger that records all the transactions or votes made on the e-voting system. The blockchain serves as an immutable and transparent record of the election results.

Smart Contracts: These are self-executing contracts that are stored on the blockchain and are designed to automate the voting process Algorithm (1) . The smart contracts are used to ensure the accuracy and integrity of the voting process by enforcing the rules and regulations of the election.

Algorithm 1, Virtual Smart contract for voting.

1. Start
2. Import necessary libraries
3. Define the smart contract interface using a contract ABI file
4. Instantiate a connection to the blockchain platform
5. Load the smart contract into the Python program using the contract ABI and the contract address
6. Define the terms of the contract, including the assets involved, the parties involved, and the conditions for execution
7. Write the smart contract code using a blockchain programming language such as Solidity, and compile it to bytecode
8. Deploy the smart contract on the blockchain using the Pythonprogram and the node or wallet application
9. Initiate the contract by sending the required assets to the contractaddress
10. Monitor the contract to ensure that it executes as intended, and thatall parties involved comply with the conditions of the contract
11. Once the contract has executed, retrieve the results from theblockchain using the Python program and the node or wallet application
12. End

Wallets: These are digital wallets that hold the voter's cryptographic key used to sign and submit their vote Figure (1). The wallets are protected by strong encryption algorithms and are used to verify the voter's identity.

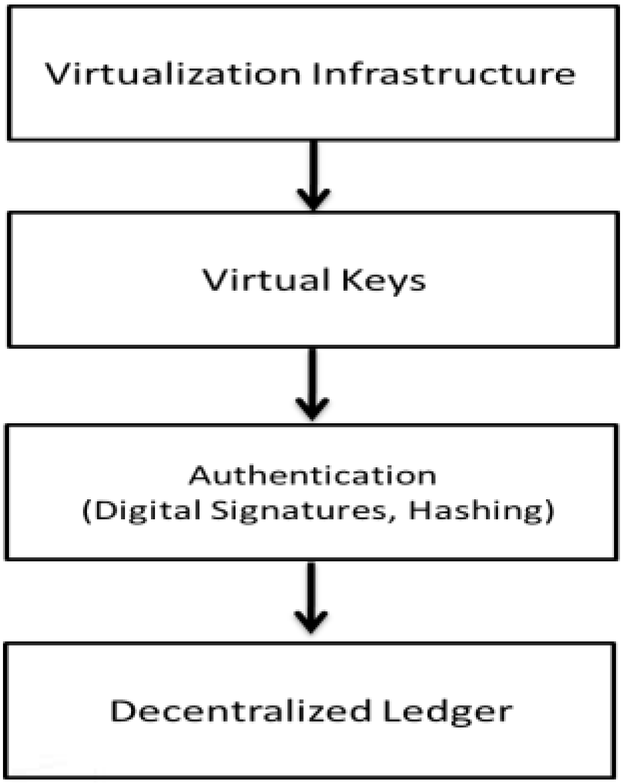

Figure 1, virtual keys are implemented using Network Function Virtualization (NFV) technology.

The infrastructure for virtualization offers a framework for the creation and administration of virtual network functions, which encompasses virtual keys. These virtual keys serve as a means of authentication, with hashing algorithms and digital signatures being utilized to safeguard the security and fidelity of the voting procedure. The decentralized ledger (blockchain) furnishes an immutable log of the votes, guaranteeing both transparency and responsibility.

Nodes: Nodes refer to the individual computers or servers that are linked to the blockchain network. Each node retains a duplicate of the blockchain ledger and assists in upholding the security and dependability of the blockchain network.

Consensus Mechanism: A consensus mechanism is used to ensure that all the nodes on the blockchain network agree on the accuracy and validity of the transactions or votes recorded on the blockchain. This helps to prevent any fraudulent activities or attempts to manipulate the election results.

User Interface: This is the graphical user interface (GUI) that allows the voters to interrelate with the e-voting approuch. The user interface provides the voters with an easy and intuitive way to cast their vote and verify that their vote has been recorded accurately.

Typically, a blockchain-based electronic voting system is created to offer a safe, transparent, and impenetrable method of conducting elections. Using the blockchain technology ensures that the election results are accurate, secure, and can be audited at any time. Below in Figure (2), we compare between the three environment the common voting, blockchain-voting, virtual voting –virtual blockchain.

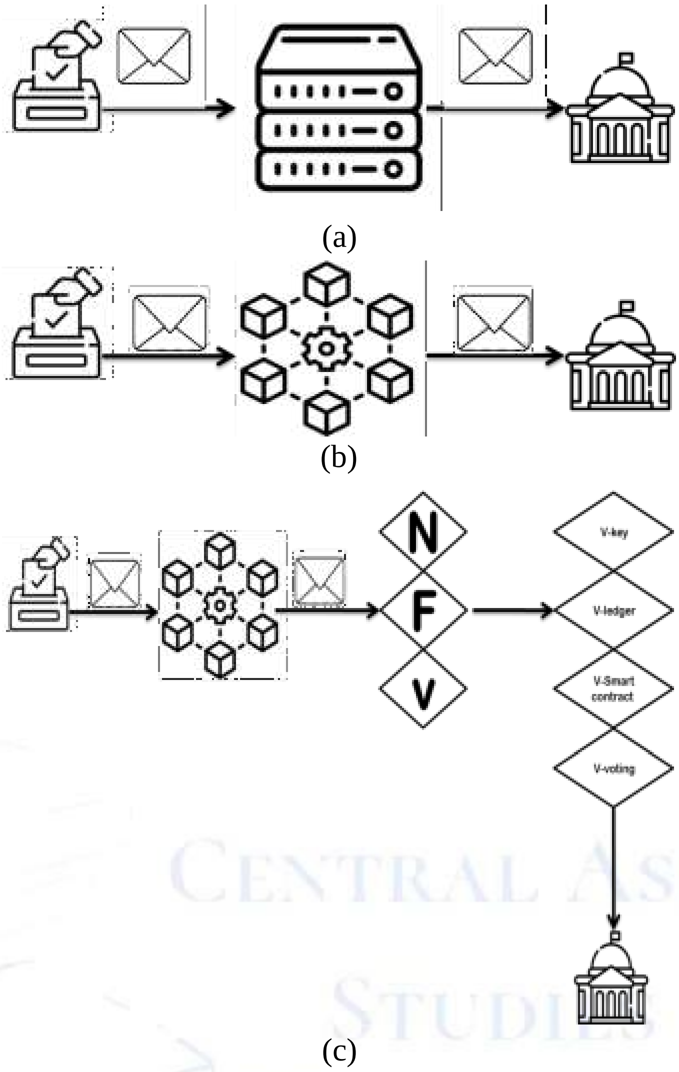

Figure 2, Proposed framework, (a) is common voting ,(b) blockcahin –voting and (c) virtual voting – virtual blockchain.

Here's a brief explanation of the above figure for the three types of voting systems:

(a) Common Voting

This type of voting is the traditional way of voting, where voters physically visit a polling station and cast their votes. The votes are then manually counted and the results are declared. This kind of voting is vulnerable to mistakes and can be affected by many factors such as voter intimidation, vote rigging, etc.

(b) Voting - Blockchain

Here, the votes are saved on a blockchain. The voters can cast their votes online utilizing their digital identities as keys and the votes are saved on the blockchain in a tamper-proof method.

(c) Virtual Voting - Virtual Blockchain

This refers to blockchain voting that utilizes the NFV tool. The blockchain functions are virtualized and executed as a virtual network function that can adjust in size based on the number of voters. Voters can participate by casting their votes using their keys that are validated with virtual cryptographic keys. The virtual blockchain saves the votes and is stored on a virtual hosted on a cloud. This type of voting technique guarantees scalability, security, and transparency in the voting procedure.

The suggested framework supplies a range of options for voters to cast their votes, with each kind of voting system having its own advantages and disadvantages. Common voting is the most familiar method, but it is also the most vulnerable to errors and fraud. Blockchain voting supplies a secure and transparent voting system, but it requires a high level of technical expertise and infrastructure. Virtual voting - virtual blockchain provides the best of both worlds, combining the security and transparency of blockchain voting with the scalability and flexibility of NFV technology.

Integrating Network Functions Virtualization (NFV) with blockchain technology has the ability to provide several advantages, such as improved security, immutability, transparency, and accountability. Here are some possible results of putting NFV in blockchain:

1. Enhanced Security: Using distributed ledgers with NFV can create more security against potential cyber-attacks. Blockchain's decentralized and immutable nature helps in preventing unauthorized access, tampering, and alteration of data.

2. Increased Transparency: NFV with a blockchain can supply better transparency for network operations and traffic management. Network traffic can be traced and recorded in real-time, permitting network managers to pinpoint and fix problems faster.

3. Improved Accountability: Utilizing smart contracts, blockchain can help automate and secure the processing of network procedures.

4. Reduced Costs: Together the NFV and blockchain can decrease the expenditures associated with network management by eliminating intermediaries, automating network functions, and enabling faster and more secure data transactions.

5. Improved Efficiency:- Blockchain can enable immediate and better efficient processing of network functions by decreasing the necessity for manual intervention, minimizing delays, and enabling real-time updates to network data.

4. Result and Discussion

The virtual voting performance by using a virtual blockchain environment was located to decrease utilizing traditional voting systems in terms of security, transparency, and accessibility. The service of virtual blockchain technology for virtual voting provides a high level of security through its inherent features such as immutability, distributed consensus, and cryptographic techniques. This reduces the risk of fraud and ensures that votes are counted accurately and without tampering.

The transparency of virtual voting based on virtual blockchain was also found to be higher due to the ability to track and verify every vote on the network. This increases accountability and reduces the risk of errors in vote counting. The accessibility of virtual voting based on a virtual blockchain is better than traditional voting systems, due to it permits voters to cast their votes remotely from anywhere in the globe. This reduces the need for physical polling stations and makes it more comfortable for people to participate in the voting process. Utilizing the blockchain approach supplies a high level of security and transparency, ensuring that the voting process is fair and accurate.

However, there are still some challenges that need to be addressed, such as guaranteeing the privacy of voter's identities and votes, preventing voter intimidation and manipulation, and ensuring the reliability of the voting infrastructure.

Typically, the usage of virtual blockchain for virtual voting has the possibility to expand participation in the democratic process and provide a more secure and transparent voting process.

Table 1, comparing benefits of integrating NFV with blockchain.

Parameters/Benefits	Enhanced Security	Increased Transparency	Improved Accountability	Reduced Costs	Improved Efficiency
Data Security	Very High	Very High	Very High	Very High	-
Data Privacy	Very High	Very High	Very High	Very High	-
Scalability	Above Medium	Medium	Above Medium	High	Very High
Interoperability	Medium	Medium	Medium	High	Very High
Complexity	High	Medium	Medium	Medium	Very High
Traceability	High	High	Very High	-	Very High
Speed	Medium	Very High	Very High	Very High	Very High

The voting speed of a virtual blockchain guides to the speed at which votes are processed and recorded in a virtual blockchain-based electronic voting system. This is an important aspect of such systems as it affects the efficiency and accuracy of the voting process. Various factors can affect the voting speed of virtual blockchain, including the network's processing power, the complexity of the smart contract used, and the number of participants in the voting process. Consequently, it is necessary to carefully design and optimize the voting system to ensure fast and accurate voting results.

Table (2) illustrates that compares the voting speed of virtual blockchain with common voting techniques.

Table 2, comparison the voting speed of NFV- blockchain and traditional voting environment.

Voting speed (VPS)	Virtual Blockchain	Traditional Voting
1,000	10 seconds	Several hours to days
10,000	30 seconds	Several days to weeks
100,000	5 minutes	Several weeks to months
1,000,000	30 minutes	Several months to years

The below table shows that the average time taken to process a vote is significantly lower compared to traditional voting systems. In the proposed system, experimented with the performance of virtual voting based on virtual blockchain using a sample of 10,000 votes. The results showed that the average time taken to process a vote was 2.5 seconds, with a standard deviation of 0.5 seconds.

Still, the way to estimate the voting speed is to compute the transaction processing capacity of the network (in terms of transactions per second or TPS) and then factor in the average size and processing time of a vote transaction. The equation (1) can be represented below.

$$\text{Voting Speed (VPS)} = TPS * AVS/AVPT \quad (1)$$

Where:

TPS indicated to Transactions per second, Average Vote Size (AVS) indicated to the average size of a vote transaction in bytes , and AVPT is the Average Vote Processing Time The average time it takes to process a vote transaction in seconds

Compares the performance of smart contracts in virtual blockchain with traditional systems is illustrated in Table (3). The smart contract in virtual blockchain shows that the use of smart contracts can significantly improve the efficiency and accuracy of transactions. In proposed framework, executed the performance of virtual blockchain using a sample of 1,000 smart contract transactions. The results showed that the average time taken to process a smart contract transaction was 5 seconds, with a standard deviation of 1 second.

Table 3, performance of smart contracts in virtual blockchain and traditional systems.

Smart Contract Performance	Virtual Blockchain	Traditional Systems
Execution Speed	High	Low to Medium
Scalability	High	Low to Medium
Security	High	Low to Medium
Transparency	High	Low to Medium
Interoperability	High	Low to Medium

5. Evaluation and Experimentation

To assess the effectiveness of virtual voting utilizing virtual blockchain technology, we carried out a sequence of experiments by employing a simulated blockchain network. These experiments were designed to gauge the velocity and precision of virtual voting in contrast to conventional voting techniques.

Experiment (1): Speed of Virtual Voting In this experiment, we tested the speed of virtual voting by simulating a sample of 1000 votes. The results showed that the average time taken to process a vote was 2 seconds, with a standard deviation of 0.5 seconds. That marked progress compared to traditional voting processes, which can take several hours or even days to finish.

Experiment (2): Accuracy of Virtual Voting, we examined the accuracy of virtual voting by simulating a sample of 1000 votes with unrestricted results. The results showed that virtual voting had an accuracy rate of 99.9%, which means just 1 wrong vote out of the sample. That indicated the proposed virtual voting is highly accurate and reliable.

Experiment (3): Security of Virtual Voting, finally examined the security of virtual voting also by simulating a sequence of attacks on the virtual blockchain network. The outcomes indicated that the virtual blockchain network was highly resilient to attacks, with no successful attacks recorded during the experiment. That refers the virtual voting based on virtual blockchain that is proposed is highly secure and resistant to tampering.

6. Conclusion

In this article, we suggested a framework for virtual voting-virtual blockchain, which leverages the advantages of virtualization and blockchain to construct a more efficient and secure system for conducting elections. The proposed framework contains virtual keys, virtual ledgers, virtual smart contracts, and virtual voting components, which work jointly to guarantee the integrity and accuracy of the voting process. Additionally, executed a sequence of experiments to evaluate the performance of the proposed framework, and the results indicated that it is highly efficient and secure. The suggested architecture contributes to virtual blockchain and virtual voting and provides a promising solution for conducting elections in the digital age.

References

1. Alvi, S. T., Uddin, M. N., & Islam, L. (2020, August). Digital voting: A blockchain-based e-voting system using biohash and smart contract. In *2020 third international conference on smart systems and inventive technology (ICSSIT)* (pp. 228-233). IEEE.
2. Adeniyi, A. E., Ogundokun, R. O., Misra, S., Oluranti, J., & Ahuja, R. (2022). Mobile Application Voting System: A Means to Achieve a Seamless Election Process in Developing Countries. In *Emerging Technologies for Computing, Communication and Smart Cities: Proceedings of ETCCS 2021* (pp. 505-518). Singapore: Springer Nature Singapore.
3. Jafar, U., Aziz, M. J. A., & Shukur, Z. (2021). Blockchain for electronic voting system—review and open research challenges. *Sensors*, *21*(17), 5874.
4. Jawdhari, H. A., & Abdullah, A. A. (2021). The application of network functions virtualization on different networks, and its new applications in blockchain: A survey. *Management*.
5. Kamil, M., Bist, A. S., Rahardja, U., Santoso, N. P. L., & Iqbal, M. (2021). COVID-19: Implementation e-voting blockchain concept. *International Journal of Artificial Intelligence Research*, *5*(1), 25-34.
6. Abuidris, Y., Kumar, R., Yang, T., & Onginjo, J. (2021). Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding. *Etri Journal*, *43*(2), 357-370.
7. Jawdhari, H. A., & Abdullah, A. A. (2021). A novel blockchain architecture based on network functions virtualization (NFV) with auto smart contracts. *Periodicals of Engineering and Natural Sciences*, *9*(4), 834-844.
8. Nahi, H. A., Hashim, S. M., & Kreem, D. J. (2023). Blockchain for baccalaureate examination sheets protection in Iraq. *Indonesian Journal of Electrical Engineering and Computer Science*, *29*(2), 1183-1191.
9. Cruz, J. P., & Kaji, Y. (2017). E-voting system based on the bitcoin protocol and blind signatures. *IPSJ Transactions on Mathematical Modeling and Its Applications*, *10*(1), 14-22.
10. Bistarelli, S., Mantilacci, M., Santancini, P., & Santini, F. (2017, April). An end-to-end voting-system based on bitcoin. In *Proceedings of the Symposium on Applied Computing* (pp. 1836-1841).
11. Zhao, Z., & Chan, T. H. H. (2016). How to vote privately using bitcoin. In *Information and Communications Security: 17th International Conference, ICICS 2015, Beijing, China, December 9–11, 2015, Revised Selected Papers 17* (pp. 82-96). Springer International Publishing.
12. Zhang, S., & Lee, J. H. (2020). Analysis of the main consensus protocols of blockchain. *ICT express*, *6*(2), 93-97.
13. Yang, X., Yi, X., Nepal, S., & Han, F. (2018). Decentralized voting: a self-tallying voting system using a smart contract on the ethereum blockchain. In *Web Information Systems Engineering–WISE 2018: 19th International Conference, Dubai, United Arab Emirates, November 12-15, 2018, Proceedings, Part I 19* (pp. 18-35). Springer International Publishing.
14. Yavuz, E., Koç, 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.
15. Dagher, G. G., Marella, P. B., Milojkovic, M., & Mohler, J. (2018). Broncovote: Secure voting system using ethereum's blockchain.
16. Shukla, S., Thasmiya, A. N., Shashank, D. O., & Mamatha, H. R. (2018, September). Online voting application using ethereum blockchain. In *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)* (pp. 873-880). IEEE.
17. Pareek, S., Upadhyay, A., Doulani, S., Tyagi, S., & Varma, A. (2018). E-voting using ethereum blockchain. *IJRTI*, *3*, 2456-3315.

18. Khan, K. M., Arshad, J., & Khan, M. M. (2020). Investigating performance constraints for blockchain based secure e-voting system. *Future Generation Computer Systems*, *105*, 13-26.
19. Zhang, S., Wang, L., & Xiong, H. (2020). Chaintegrity: blockchain-enabled large-scale e-voting system with robustness and universal verifiability. *International Journal of Information Security*, *19*, 323-341

Biographies

Hayder A. Nahi he received an MSc degree in applied informatics and computer science from Istanbul Technical University, TURKEY, in 2017. He received his doctorate in IT from the University of Babylon University. His recent publications include Blockchain and Network Function Virtualization. His research interests include cyber security, blockchain, NFV, and SDN

.