Journal of Theoretical and Applied Information Technology
31st March 2024. Vol.102. No 6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

VALIDATION OF SECURE E-VOTING SYSTEM BASED BLOCKCHAIN IMMUTABILITY: THE JORDANIAN PARLIAMENTARY ELECTIONS

KHALID ALTARAWNEH[1], AMER OSHOUSH[2], IBRAHIM ALTARAWNI[3], MOHAMMED AMIN ALMAIAH[4,5], TAYSEER ALKDOUR[6], ABDALWALI LUTFI[7,8], MAHMOUD AL-RAWAD [7] AND RAMI SHEHAB[6]

[1]Faculty of Information Technology, Mutah University, Det. of Data Science and Artificial Intelligence.
[2]School of Business, MIS department, Mutah University.
[3]College of Information Technology, Department of Artificial Intelligence, Tafila Technical University, Tafila, Jordan
[4]King Abdullah the II IT School, The University of Jordan, Amman 11942, Jordan
[5] Applied Science Research Center, Applied Science Private University, Amman 11931, Jordan
[6] Department of Computer Networks and Communications, College of Computer Sciences and Information Technology, King Faisal University, Al-Ahsa 31982, Saudi Arabia
[7] College of Business, King Faisal University, Al-Ahsa, 31982, Saudi Arabia
[8] MEU Research Unit, Middle East University, Amman, Jordan.

E-mail: Corresponding authors: talkhdour@kfu.edu.sa and m.almaiah@ju.edu.jo

ABSTRACT

This paper aims at providing a valid E-voting framework schema based on BC technology that serves the election process in the Jordan context. It investigates the validity and feasibility of the proposed model using a focus group study to restructure the implementation process as an initial step before the researchers develop the final software product that aligns with Jordanian parliament election law. The study initially proposes a framework for an e-voting framework based on blockchain technology and then evaluated it through a focus group. The proposed framework schema fulfills the standards of adopting E-voting by stressing a set of principles related to consistency, integrity, and identity verification. The final conceptual framework schema was developed considering the validation results recommended by the experts' evaluation to become a valid model that can move forward in following up on its implementation.
Keywords: *Security, E-Voting System, Blockchain, Jordan Parliamentarians, Elections.*

1. INTRODUCTION

The transition from a conventional to an electronic voting system is a step that many countries and electoral boards are reluctant to take. In fact, technological innovations such as Direct Recording Electronic (DRE) to facilitate voting or counting have already proven to be vulnerable and have bugs that are difficult to detect [1],[2]. Therefore, the lack of confidence in this type of system is remarkable. In systems that work online, the concern is even greater since transactions are exposed to cyberattacks, there may be vulnerabilities in personal voting devices, there is a high risk of coercion, etc. [3]. On the other hand, electronic voting improves problems of traditional systems, such as difficulties in exercising the right to vote for residents abroad, the difficulty of participating for sick people or people with mobility problems, the disincentive for participation that supposes long queues in front of a polling station [4],[5]. All this has lead technology companies and public organizations to continue working on electronic voting systems and investigate the incorporation of new technologies to improve the security and transparency of their systems. In this sense, Blockchain (BC) is a technology that has recently gained popularity in various sectors and could contribute to improving the field of electronic voting due to its immutability, integrity, and auditability [6-9].

Another outstanding feature of the blockchain, and that of most cryptocurrencies, is that it is a public system, in which not only the records can be freely consulted, but also, any node

that follows the rules of the protocol can participate in the consensus protocol and include new data without the need for special permissions [10-12]. For this reason, these blockchains are called permissionless. On the other hand, following other security and accessibility requirements, permissioned blockchains were later proposed, which could have private content and require special permissions to be able to participate in the consensus [13-15]. Ripple is one of the most prominent projects using this type of blockchain [16-20].

This paper reviews some of the main electronic voting projects and opt to investigate the contributions of blockchain as an immutable record to improve or replace part of an electronic voting system implemented with other technologies. It studies representative systems of both uses and investigates which blockchain brings advantages to Jordanian e-voting system project in terms of security.

2. Literature Review

In 2008, the white paper titled Bitcoin: A peer to peer electronic cash system , not only acts as a starting point for Bitcoin, but also introduces blockchain technology as a decentralized system that, through a consensus protocol, allows system participants to record data immutably without using a trusted third party [21-24]. Subsequently, using the same philosophy of the blockchain proposed in Bitcoin, other systems have been created that adapt to other purposes or requirements. For example, some interesting proposals that try to improve Nakamoto's original design propose the implementation of techniques aimed at preserving user privacy, such as the use of ring signatures in CryptoNote [25] or knowledge tests in ZeroCash [26].

BC technology has evolved quite a bit since its original design. Even so, the basic security properties that distinguish it as a decentralized and immutable registry system are present across all the new proposals. In this article, we focus on the use made by the different electronic voting projects of the security and privacy features linked to the blockchains used. BC as immutable record is one of the most advanced electronic voting projects that uses blockchain as an immutable registry as the centerpiece of its technology is Agora(Gailly et al., 2018) . The architecture of this project is divided into 4 layers: a bulletin board, Cotena, the Bitcoin blockchain and Votapp.

On the one hand, the bulletin board is a permissioned blockchain with a skip chain architecture, where certain nodes operated by Agora, or third parties are granted either write or read-only permissions [27-30]. This blockchain is used as an immutable record of data generated during the electoral process (e.g., votes, null knowledge proofs evidencing the correctness of a voting system thread) [31]. Thus, there is a set of nodes with sufficient write permissions known as Cothority (Collective authority), which collectively confirm the insertion security and e-Administration transactions in the bulletin board [32-34]. The way Cothority works is based on the rotating election of a special node called an oracle, which oversees carrying out most of the management, leaving the other nodes basically collaborative tasks on and monitoring of the oracle [35].

In this way, all the nodes receive the transactions with the votes cast by the voters, among other voting data, but the oracle oversees proposing new blocks to be included in the blockchain with the transactions received [36-39]. In addition, the bulletin board acts as a central communication and memory channel, with the oracle overseeing writing blocks in the Cotena log and sending integrity tests to the blockchain of Bitcoin. Thus, nodes have the responsibility to: a) maintain a copy of the bulletin board; b) receive encrypted votes from voters, authenticate their data, and ensure that votes are cast by an authorized voter; c) confirm the blocks proposed by the oracle; d) unscramble the votes once the election is over and create plaintext votes so they can be counted; and e) keep a copy of the Cotena log and monitor that it is correct [39].

The second layer of Agora's architecture is known as Cotena. This component is basically a tamper-resistant logging mechanism built on top of the Bitcoin blockchain, where bulletin board integrity tests are written [40]. In this way, Agora uses the computational power and transparency offered by the Bitcoin network to protect the integrity of its permissioned blockchain. Agora's blockchain allows for a public record of each step of the vote and for the stages to be easily auditable [41]. The system is verifiable end-to-end since an auditor could verify that the configuration parameters are correct , the encrypted votes

correspond to authenticated voters specified in the configuration list and reflect their choices , the mixing network works correctly , the null knowledge tests that are generated correspond to correct steps to make a random verification and correctly anonymize the votes, the votes partially deciphered by each node are correct and the plain text has been successfully rebuilt; and that the final count is well computed [42-45]. Finally, official auditors can sign a certificate and register it on the bulletin board.

In this way, Agora uses a hybrid architecture of blockchain with permissions and without permissions, where the bulletin board is used to write all the data of the voting process (e.g., votes received in each node) [46-48]. This requires a system with little latency, and then screenshots of the bulletin board are made in the Bitcoin blockchain, which ensuring integrity and immutability in a more secure blockchain. However, it requires higher latency to record transactions [49]. With this design, the creators of Agora ensure that the system has a scalable architecture, high availability, usable, low cost, low latency, without single points of failure, which allows offline verifiability and that allows it to be adapted to the regulations of different types of election [50].

Although all the steps are published in the blockchain and therefore are accessible by all parties, it should be noted that this proposal also respects other previously mentioned privacy properties required in an electronic voting system. On the one hand, it does not allow knowing the partial result of the election, since the votes are published encrypted with a multi-authority system. Moreover, it also protects the privacy of the voter, since the mixing network provides anonymity, the vote is secret, and, unlike other systems, the voter is not provided with a voting receipt that can later teach a third party, avoiding possible maneuvers of coercion.

The use of blockchain as an immutable registry has also been proposed in other projects. For example, [51] propose to record integrity tests of their log system in the Bitcoin blockchain, with a proposal similar to that commented on in Agora. On the other hand, TIVI uses blockchain in a digital time stamping service [52]. Thus, with this system they can ensure that a datum has existed at a certain moment in time. For example, a fingerprint of each vote is sent to the external timestamp service. The time stamp is saved with the vote and passed to the voter, who can verify that the vote was recorded correctly, and was not altered or removed from the system.

3. PROBLEM STATEMENT AND QUESTIONS

In Jordan context, the election is a constitutional right that enables Jordanian to elect only the members of the legislative authority, the Parliament. However, this requires tedious procedures and great effort in carrying out the election. This issue can consume the entire infrastructure and resources without fully ensuring its credibility due to the related challenges, difficulties, errors, and manipulations. The current Jordan's TE system relies on administrative and human action, which sometimes can be dominated by the bias of involved people or organizations. These challenges might lead to distrust of the results and threaten the electorate's privacy and the transparency of the whole election process.

Meanwhile, The Independent Electoral Commission (IEC) is the center of the election process in Jordan, which is the TE system. The presence of such ICE as a single body that drives the election process needs to ensure the integrity and transparency of an election process, which is not an easy task and opens opportunities for tampering with the election. Furthermore, TE poses a long time in processing ballots and counting votes, which increases doubts about the integrity and transparency of the elections. Moreover, sometimes the responsible entity of the election process fails to determine the proper voting sites flexibly and dynamically, which can prevent some of the electorates from casting their votes [53].

Unfortunately, despite the proliferation of today's technology and its ability to improve the integrity and transparency of the election process; most election systems are still restricted to the TE approach. Therefore, the need to enhance citizen trust and add credibility, specifically to the voting models, has emerged and pushed many countries to introduce EV technology in their election systems. The EV has been proposed as a solution for many issues related to TE and paper-based voting, which in turn ensure error and bias-free in the election process. Moreover, the partial use of technology in TE voting systems mainly rely on

central system architectures, which make them vulnerable to cyber-attacks targeting main infrastructures [54].

Therefore, providing one-box and secure solutions for holding an election requires a decentralized system architecture, such as the BC. The characteristics and transparency of BC agents make it a promising approach to solve for the issues associated with TE voting systems. BC-based EV engineering can address most of the challenges of TE systems and traditional EVs. These include issues of voter authentication, verification of votes, protection of voter privacy, the security of voting, and integrity of election results.

Based on the context related to TE and EVs, this study attempts to develop an election system model based on BC technology to improve the current Jordan's TE system. However, this model can be easily customized based on different election systems. It provides a semi-formal descriptive model to increase reliability, confidentiality, integrity, transparency, and security of the election process. Furthermore, it highlights the importance of voter identity through the biometrics of unique human-physiological characteristics to verify and authenticate a personal identity. In BC, the voter ID relies on a cypher-based identification system, which provides real confidence in voter eligibility and his\ her privacy [55-57]. So, an EV model based on the use of BC and Biometric Technology (BT) has been proposed to verify and authenticate voters. However, this model needs to be validated against its alignment with the current Jordanian Parliament Election Law (JPEL) and ICE procedures.

Therefore, this paper comes to fill the addressed theoretical and practical gaps by providing a valid E-voting framework schema based on BC technology that serves the election process in Jordan context. It seeks to explore the validity and feasibility of the proposed model using a focus group study (FGS) to restructure the implementation process as an initial step before the researchers developing the final software product that aligns with JPEL.

4. Methodology

The adopted methodology is structured into several phases. It starts by reviewing the literature and the JPEL and ends up with developing a final, model proposed with feasibility results (i.e., validation). Figure 1 shows the research design and workflow procedures.

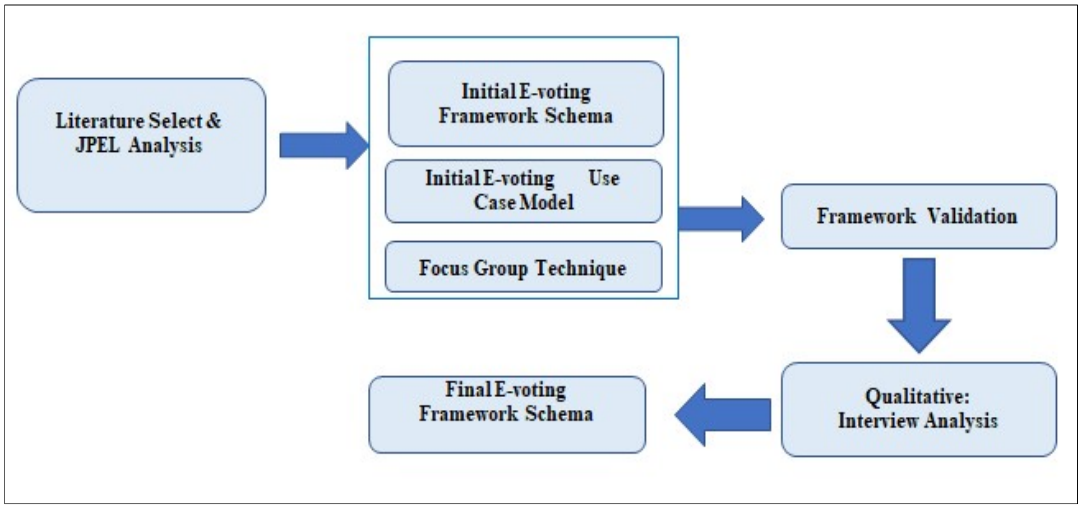

Figure 1. Research Design

PHASE 1: Literature Select and JPEL Analysis

To become familiar with the e-voting systems and the technology that is sought to be implemented in such a system, we proceeded to investigate literature related to the fundamental themes of this work. According to the development of this phase, it was possible to organize concepts and acquire new knowledge necessary to design and develop the final model, in which the blockchain technology will be implemented. Furthermore, several e-voting models were analyzed in an effort for the

development of our blockchain network, the characteristics that these models have and how we can utilize them to the needs of our project considering JPEL.

PHASE 2: Development of Initial E-voting Framework Schema

In this phase, we managed to identify the requirements that should be part of our initial E-voting Framework Schema, which we consider necessary to carry out the operation of developing e-voting model based on BC and aligns with JPEL. Figure 2 shows the initial E-voting system case Model resulted in this phase.

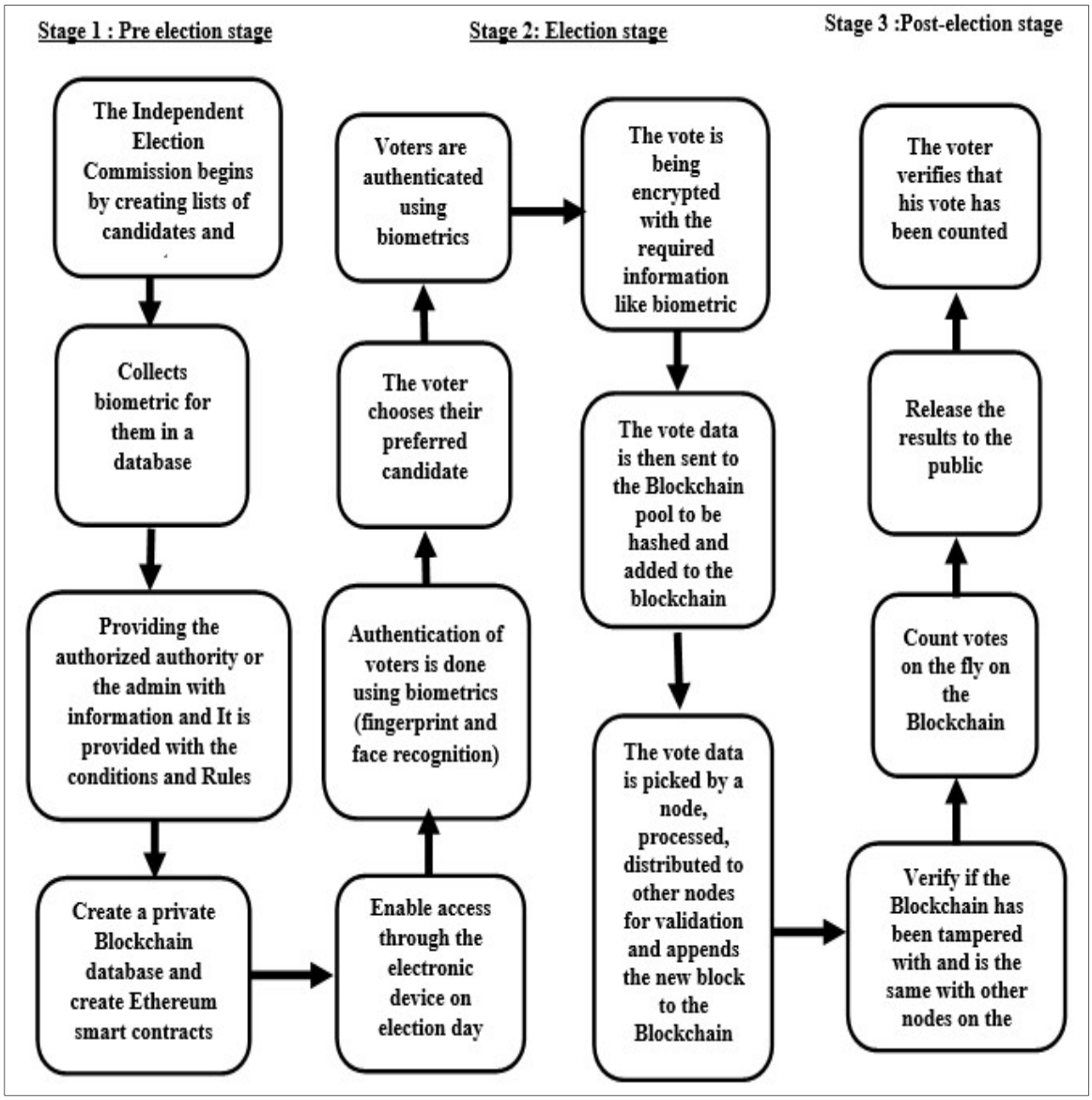

Figure 2. Initial E-Voting Framework Schema Proposed

Next, the use case model is developed based on the prior findings and JPEL analysis as shown in figure 3.

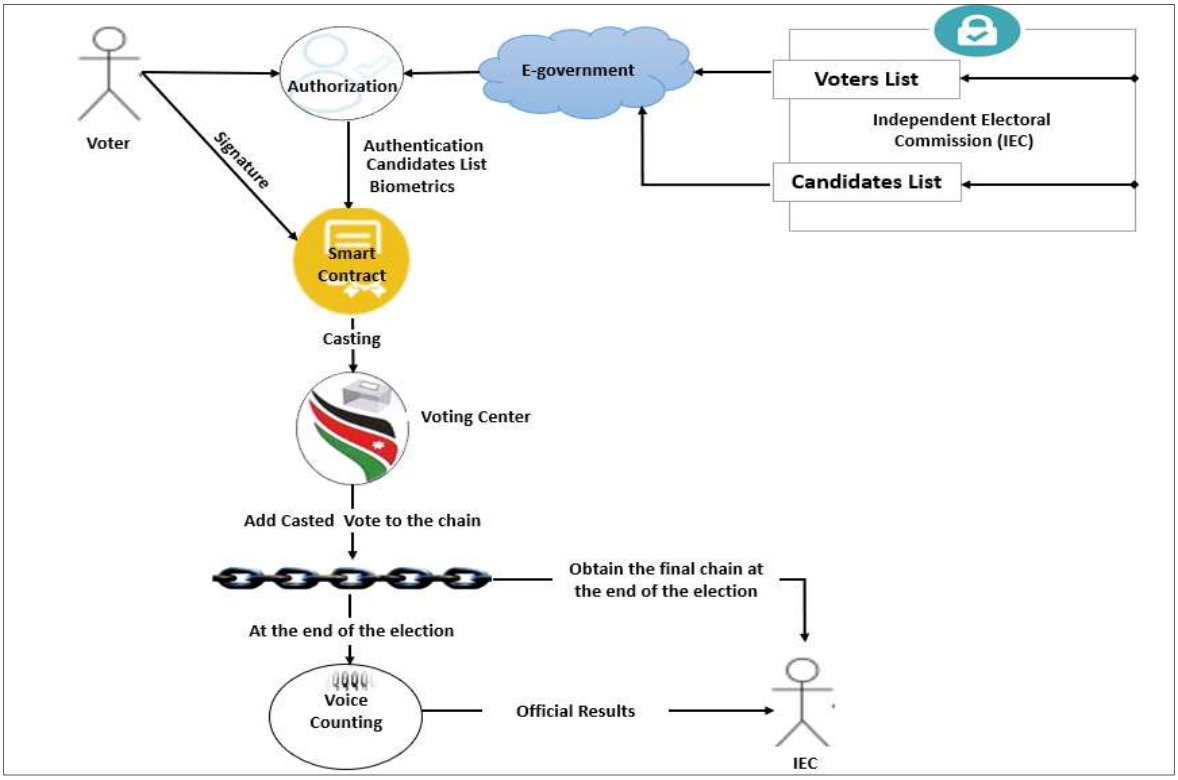

Figure 3. System Use Case Diagram

Finally, the validation criteria, objectives of the focus group, and participant's identification and recruitment are defined. Participants were recruited by research areas that possess real experience with it. Within the boundaries of this study, experts were identified as electronic election experts, legal and legislative experts in elections, BC technology experts, and IT experts with research experience in critical processes. As the research topic is narrow, the field of potential participants has been restricted to those with experience developing this specific model. Since the qualifications of the participants are more important than the number of participants, only six experts have been chosen who possess fundamental knowledge in their field and what serves the research.

To manage the results of the research study and obtain sufficient information to reach valid conclusions. The focus group participants were contacted face to face or through the Zoom program and the Team program.

PHASE 3:* Framework *validation

With the aim of revealing the validity of the proposed model in the real environment, the focus group discussion was conducted in this study, which was participated by domain experts. The interview results and discussion were analyzed and reflected on producing the final E-voting framework schema proposed.

5. Analysis and Results

The results of this study are qualitative and derived from an analysis of participants' responses and discussion to topics, patterns, and relationships. The results indicated that there is a need to use secure e-voting system, with the necessity to work on the initial proposed model due to the factors related to transparency, trust, security, and voter privacy, which all participants agreed upon. This qualitative data represents the perspectives of those with expertise in developing a valid e-voting framework schema-based BC technology. Given everyone's unique contexts and perspectives, a consensus was reached on each practice identified by the participants. Table 1 compares between the initial and final framework schema proposed for e-voting system based on BC technology. These comparisons reflect the contribution added by the participants to ensure the validity of the proposed framework.

Table 1. Compare And Contrast The Proposed Models

Comparison Category	Initial proposed Framework	Final Proposed Framework	Benefit
model Design	It was built based on previous studies and related works	It was built based on the expert judgment of the initial proposed model	Coming up with effective practices and critical issues that helped improve the proposed model and the possibility of its effective application
Legislative and legal aspects	Not applied	Applied	Implementing Article 67 of the Election Law, which guarantees the integrity and secrecy of the electoral process and the right of the candidate to monitor the electoral process, as appropriate blockchain components have been used to achieve them.
Consensus algorithm	Not set	Delegated Proof of Stake	Enabling observers and candidates to monitor the integrity of the electoral process, as it is possible to delegate some powers and elect a simple sample for observation.
Blockchain type	Private Ethereum blockchain	Permissioned private blockchain	As the use of Permissioned is suitable for institutional work, unlike the private Ethereum blockchain that is suitable for digital currencies, while the Permissioned enables to give an authorization to an authorized party to grant terms and procedures for programming smart contracts to prevent third-party interference from controlling the process and preventing human interference.

Based on the consensus of the experts and the set of recommendations and amendments they recommended, this was the final form of the proposed e-voting framework schema as shown in Figure 4.

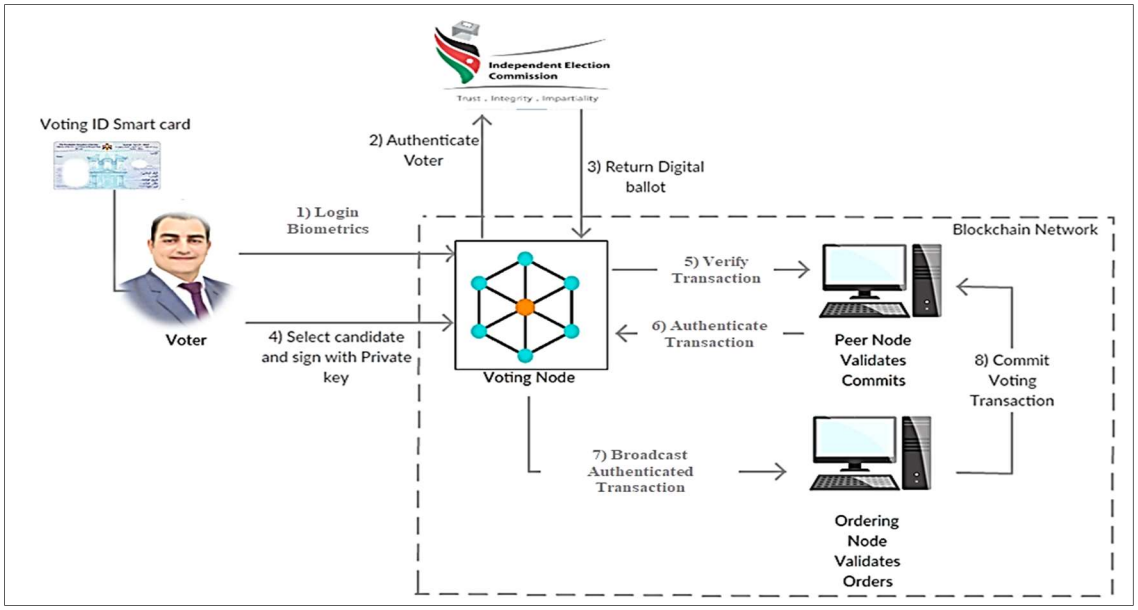

Figure 4. E-Voting Final Framework Schema Proposed

The proposed framework schema keeps track to fulfill the standards of adopting EE by stressing a set of principles related to consistency [54], integrity [55], [65], identity verification [57], eligibility[57], secrecy of the elector [55-57], resistance to tampering [55-57], uniqueness, and verifiability by individuals [55-57]. Thus, the rules that regulate the proposed system are explained as follows:

1. After providing the director of elections with conditions, procedures, lists, and essential measures, the IEC begins by preparing voters' and candidate lists and then collecting vital measurements relevant to them. IEC begins the process of elections and control their life cycle by: Specifying the type of the election; creating the election; Deciding the lifespan of the election and the length of the election.

2. Voters: Voters are the registered participants in particular elections. The role of the voter includes authentication at the start of the voting process using biometrics credentials; casting a vote; verify that his\her vote has been counted after the casting.

3. Peer and ordering are managerial nodes, they serve as networked servers of a stand location station machines that receives all verified votes with vote's projections on candidates. These server nodes project the votes and allows the results published for public after the completion time of the election process.

6. CONCLUSION

This paper comes to fill the addressed theoretical and practical gaps by providing a valid E-voting framework schema based on BC technology that serves the election process in Jordan context. It seeks to explore the validity and feasibility of the proposed model using a focus group study (FGS) to restructure the implementation process as an initial step before the researchers developing the final software product that aligns with JPEL. The results of the multi-phases methodology allow to develop and recommend a conceptual framework for implementing e-voting system with all acting schemas that represents the different stages of the election process. Moreover, the proposed conceptual framework developed with a thematic regulation that align with expert's comments and JPEL standards.

7. FUTURE WORK

The proposed conceptual framework focuses on involving the BC technology to improve authenticity regulation and increase voter trust in the election system. This conceptual framework can be expanded to include extra BC nodes that allows the candidates to follow up their progress in the election contest. Moreover, Machine learning applications can be used to design e-voting models through the use of its various applications in terms of security and networking.

Conflict of interest

The authors declare no potential conflict of interest regarding the publication of this work. In addition, the ethical issues including plagiarism, informed consent, misconduct, data fabrication and, or falsification, double publication and, or submission, and redundancy have been completely witnessed by the author.

ACKNOWLEDGMENT

This work was supported through the Annual Funding track by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Project No. Grant No. 5923).

REFERENCES

[1] Akbari, E., Wu, Q., Zhao, W., Arabnia, H. R., & Yang, M. Q. (2017). From blockchain to internet-based voting. *2017 International Conference on Computational Science and Computational Intelligence (CSCI)*, 218–221.

[2]Akcora, C. G., Gel, Y. R., & Kantarcioglu, M. (2022). Blockchain networks: Data structures of Bitcoin, Monero, Zcash, Ethereum, Ripple, and Iota. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *12*(1), e1436.

[3] Ali, A., Almaiah, M. A., Hajjej, F., Pasha, M. F., Fang, O. H., Khan, R., ... & Zakarya, M. (2022). An industrial IoT-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network. Sensors, 22(2), 572.

[4] Almaiah, M. A., & Al-Khasawneh, A. (2020). Investigating the main determinants of

mobile cloud computing adoption in university campus. Education and Information Technologies, 25(4), 3087-3107.

[5] Al Nafea, R., & Almaiah, M. A. (2021, July). Cyber security threats in cloud: Literature review. In 2021 international conference on information technology (ICIT) (pp. 779-786). IEEE.

[6] Almaiah, M. A., Hajjej, F., Ali, A., Pasha, M. F., & Almomani, O. (2022). A novel hybrid trustworthy decentralized authentication and data preservation model for digital healthcare IoT based CPS. Sensors, 22(4), 1448.

[7] Adil, M., Khan, R., Ali, J., Roh, B. H., Ta, Q. T. H., & Almaiah, M. A. (2020). An energy proficient load balancing routing scheme for wireless sensor networks to maximize their lifespan in an operational environment. IEEE Access, 8, 163209-163224.

[8] Adil, M., Almaiah, M. A., Omar Alsayed, A., & Almomani, O. (2020). An anonymous channel categorization scheme of edge nodes to detect jamming attacks in wireless sensor networks. Sensors, 20(8), 2311.

[9] Akour, I., Alnazzawi, N., Alshurideh, M., Almaiah, M. A., Al Kurdi, B., Alfaisal, R. M., & Salloum, S. (2022). A Conceptual Model for Investigating the Effect of Privacy Concerns on E-Commerce Adoption: A Study on United Arab Emirates Consumers. Electronics, 11(22), 3648.

[10] Siam, A. I., Almaiah, M. A., Al-Zahrani, A., Abou Elazm, A., El Banby, G. M., El-Shafai, W., ... & El-Bahnasawy, N. A. (2021). Secure health monitoring communication systems based on IoT and cloud computing for medical emergency applications. Computational Intelligence and Neuroscience, 2021.

[11] Almaiah, M. A., Ali, A., Hajjej, F., Pasha, M. F., & Alohali, M. A. (2022). A lightweight hybrid deep learning privacy preserving model for FC-based industrial internet of medical things. Sensors, 22(6), 2112.

[12] Khan, M. N., Rahman, H. U., Almaiah, M. A., Khan, M. Z., Khan, A., Raza, M., ... & Khan, R. (2020). Improving energy efficiency with content-based adaptive and dynamic scheduling in wireless sensor networks. IEEE Access, 8, 176495-176520.

[13] Alabadleh, A., Aljaafreh, S., Aljaafreh, A., & Alawasa, K. (2018). A RSS-based localization method using HMM-based error correction. *Journal of Location Based Services*, *12*(3–4), 273–285.

[14] Almaiah, M. A., Al-Zahrani, A., Almomani, O., & Alhwaitat, A. K. (2021). Classification of cyber security threats on mobile devices and applications. In Artificial Intelligence and Blockchain for Future Cybersecurity Applications (pp. 107-123). Cham: Springer International Publishing.

[15] Adil, M., Khan, R., Almaiah, M. A., Al-Zahrani, M., Zakarya, M., Amjad, M. S., & Ahmed, R. (2020). MAC-AODV based mutual authentication scheme for constraint oriented networks. IEEE Access, 8, 44459-44469.

[16] Almomani, O., Almaiah, M. A., Alsaaidah, A., Smadi, S., Mohammad, A. H., & Althunibat, A. (2021, July). Machine learning classifiers for network intrusion detection system: comparative study. In 2021 International Conference on Information Technology (ICIT) (pp. 440-445). IEEE.

[17] Adil, M., Khan, R., Almaiah, M. A., Binsawad, M., Ali, J., Al Saaidah, A., & Ta, Q. T. H. (2020). An efficient load balancing scheme of energy gauge nodes to maximize the lifespan of constraint oriented networks. IEEE Access, 8, 148510-148527.

[18] Alsyouf, A., Lutfi, A., Al-Bsheish, M., Jarrar, M. T., Al-Mugheed, K., Almaiah, M. A., ... & Ashour, A. (2022). Exposure detection applications acceptance: The case of COVID-19. International Journal of Environmental Research and Public Health, 19(12), 7307.

[19] Bubukayr, M. A. S., & Almaiah, M. A. (2021, July). Cybersecurity concerns in smart-phones and applications: A survey. In 2021 international conference on information technology (ICIT) (pp. 725-731). IEEE.

[20] Almaiah, M. A. (2021). A new scheme for detecting malicious attacks in wireless sensor networks based on blockchain technology. In Artificial intelligence and blockchain for future cybersecurity applications (pp. 217-234). Cham: Springer International Publishing.

[21] Alnabhan, M., Al-Jaafreh, S., Abadleh, A., Atoum, M., Hammouri, A., & Al-dalahmeh, M. (2021). Enhanced D2D Communication Model in 5G Networks. *International Journal of Computing and Digital Systems*, *10*(1), 217–223.

[22] Alnabhan, M., Al-qatawneh, E., Alabadleh, A., Atoum, M., & Alnawyseh, M. (2020). Efficient Handover Approach in 5G Mobile

Networks. *Int. J. Adv. Sci. Eng. Inform. Technol*, *10*, 1417–1422.

[23] Alamer, M., & Almaiah, M. A. (2021, July). Cybersecurity in Smart City: A systematic mapping study. In 2021 international conference on information technology (ICIT) (pp. 719-724). IEEE.

[24] Almaiah, M. A., Almomani, O., Alsaaidah, A., Al-Otaibi, S., Bani-Hani, N., Hwaitat, A. K. A., ... & Aldhyani, T. H. (2022). Performance investigation of principal component analysis for intrusion detection system using different support vector machine kernels. Electronics, 11(21), 3571.

[25] Almaiah, M. A., Dawahdeh, Z., Almomani, O., Alsaaidah, A., Al-Khasawneh, A., & Khawatreh, S. (2020). A new hybrid text encryption approach over mobile ad hoc network. Int. J. Electr. Comput. Eng.(IJECE), 10(6), 6461-6471.

[26] Alrawad, M., Lutfi, A., Alyatama, S., Elshaer, I. A., & Almaiah, M. A. (2022). Perception of occupational and environmental risks and hazards among mineworkers: A psychometric paradigm approach. International journal of environmental research and public health, 19(6), 3371.

[27] Almaiah, M. A., Al-Rahmi, A., Alturise, F., Hassan, L., Lutfi, A., Alrawad, M., ... & Aldhyani, T. H. (2022). Investigating the effect of perceived security, perceived trust, and information quality on mobile payment usage through near-field communication (NFC) in Saudi Arabia. Electronics, 11(23), 3926.

[28] Altulaihan, E., Almaiah, M. A., & Aljughaiman, A. (2022). Cybersecurity threats, countermeasures and mitigation techniques on the IoT: Future research directions. Electronics, 11(20), 3330.

[29] Albalawi, A. M., & Almaiah, M. A. (2022). Assessing and reviewing of cyber-security threats, attacks, mitigation techniques in IoT environment. J. Theor. Appl. Inf. Technol, 100, 2988-3011.

[30] Alves, J., & Pinto, A. (2018). On the use of the blockchain technology in electronic voting systems. *International Symposium on Ambient Intelligence*, 323–330.

[31] Bulut, R., Kantarci, A., Keskin, S., & Bahtiyar, S. (2019). Blockchain-Based Electronic Voting System for Elections in Turkey. *UBMK 2019 - Proceedings, 4th International Conference on Computer Science and Engineering*, 183–188. https://doi.org/10.1109/UBMK.2019.8907102

[32] Cash, M., & Bassiouni, M. (2018). Two-tier permission-ed and permission-less blockchain for secure data sharing. *2018 IEEE International Conference on Smart Cloud (SmartCloud)*, 138–144.

[33] Qasem, M. H., Obeid, N., Hudaib, A., Almaiah, M. A., Al-Zahrani, A., & Al-Khasawneh, A. (2021). Multi-agent system combined with distributed data mining for mutual collaboration classification. IEEE Access, 9, 70531-70547.

[34] Almudaires, F., & Almaiah, M. (2021, July). Data an overview of cybersecurity threats on credit card companies and credit card risk mitigation. In 2021 International Conference on Information Technology (ICIT) (pp. 732-738). IEEE.

[35] AlMedires, M., & AlMaiah, M. (2021, July). Cybersecurity in industrial control system (ICS). In 2021 International Conference on Information Technology (ICIT) (pp. 640-647). IEEE.

[36] Almaiah, M. A., Al-Otaibi, S., Shishakly, R., Hassan, L., Lutfi, A., Alrawad, M., ... & Alghanam, O. A. (2023). Investigating the role of perceived risk, perceived security and perceived trust on smart m-banking application using sem. Sustainability, 15(13), 9908.

[37] Al Hwaitat, A. K., Almaiah, M. A., Ali, A., Al-Otaibi, S., Shishakly, R., Lutfi, A., & Alrawad, M. (2023). A new blockchain-based authentication framework for secure IoT networks. Electronics, 12(17), 3618.

[38] Cucurull, J., Rodríguez-Pérez, A., Finogina, T., & Puiggali, J. (2018). Blockchain-based internet voting: systems' compliance with international standards. *International Conference on Business Information Systems*, 300–312.

[39] Fusco, F., Lunesu, M. I., Pani, F. E., & Pinna, A. (2018). Crypto-voting, a Blockchain based e-Voting System. *KMIS*, 221–225.

[40] Gailly, N., Jovanovic, P., Ford, B., Lukasiewicz, J., & Gammar, L. (2018). *Agora: bringing our voting systems into the 21st century*.

[41] Gibson, J. P., Krimmer, R., Teague, V., & Pomares, J. (2016). A review of e-voting: the past, present and future. *Annals of Telecommunications*, *71*(7), 279–286.

[42] Hjálmarsson, F. Þ., Hreiðarsson, G. K.,

Hamdaqa, M., & Hjálmtýsson, G. (2018). Blockchain-based e-voting system. *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, 983–986.

[43] Jafar, U., Aziz, M. J. A., & Shukur, Z. (2021). Blockchain for electronic voting system—review and open research challenges. *Sensors*, *21*(17), 5874.

[44] Kajal, B., Vala, B., & Patel, W. (2021). A Review of Online Voting System Security Based on Cryptography. *Proceedings of the International Conference on Smart Data Intelligence (ICSMDI 2021)*.

[45] Košt'ál, K., Bencel, R., Ries, M., & Kotuliak, I. (2019). Blockchain e-voting done right: Privacy and transparency with public blockchain. *2019 IEEE 10th International Conference on Software Engineering and Service Science (ICSESS)*, 592–595.

[46] Majeed, N. A. (2021). Review on Blockchain based e-Voting Systems. *Konferenzband Zum Scientific Track Der Blockchain Autumn School 2021*, *004*, 1–8.

[47] Mars, A., Abadleh, A., & Adi, W. (2019). Operator and Manufacturer Independent D2D Private Link for Future 5G Networks. *IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 1–6.

[48] Mols, J., & Vasilomanolakis, E. (2020, June). EthVote: Towards secure voting with distributed ledgers. *International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2020*. https://doi.org/10.1109/CyberSecurity49315.2020.9138866

[49] Nakamoto, S., & Bitcoin, A. (2008). A peer-to-peer electronic cash system. *Bitcoin.–URL: Https://Bitcoin. Org/Bitcoin. Pdf*, *4*, 2.

[50] Pawlak, M., & Poniszewska-Marańda, A. (2019). Blockchain e-voting system with the use of intelligent agent approach. *Proceedings of the 17th International Conference on Advances in Mobile Computing & Multimedia*, 145–154.

[51] Peng, L., Feng, W., Yan, Z., Li, Y., Zhou, X., & Shimizu, S. (2021). Privacy preservation in permissionless blockchain: A survey. *Digital Communications and Networks*, *7*(3), 295–307.

[52] Politou, E., Casino, F., Alepis, E., & Patsakis, C. (2019). Blockchain mutability: Challenges and proposed solutions. *IEEE Transactions on Emerging Topics in Computing*.

[53] Sasson, E. Ben, Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014). Zerocash: Decentralized anonymous payments from bitcoin. *2014 IEEE Symposium on Security and Privacy*, 459–474.

[54] Soud, M., Helgason, S., Hjalmtysson, G., & Hamdaqa, M. (2020). TrustVote: On Elections We Trust with Distributed Ledgers and Smart Contracts. *2020 2nd Conference on Blockchain Research and Applications for Innovative Networks and Services, BRAINS 2020*, 176–183. https://doi.org/10.1109/BRAINS49436.2020.9223306

[55] Syta, E., Tamas, I., Visher, D., Wolinsky, D. I., Jovanovic, P., Gasser, L., Gailly, N., Khoffi, I., & Ford, B. (2016). Keeping authorities" honest or bust" with decentralized witness cosigning. *2016 IEEE Symposium on Security and Privacy (SP)*, 526–545.

[56] Wu, S., & Galindo, D. (2018). Evaluation and Improvement of Two Blockchain Based E-voting System: Agora and Proof of Vote. *Edited by David Galindo. University of Birmingham. Http://Www. Dgalindo. Es/Mscprojects/Shuang. Pdf*.

[57] Zenin, S., Kuteynikov, D., Izhaev, O., & Yapryntsev, I. (2019). Applying technologies of distributed registries and blockchains in popular voting and lawmaking: Key methods and main problems. *Amazonia Investiga*, *8*(20), 330–339.