IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 09 Issue 10, October 2022
ISSN (Online) 2348 – 7968 | Impact Factor – 6.72
www.ijiset.com

Development of a Secure Preserve E-Voting System Using Private Blockchain Solutions

Basil Alothman[1], Chibli Jumaa[2], Sara Alshammeri[3] and Murad Khan[4]

[1,2,3,4] Department of Computer Science and Engineering, Kuwait College of Science and Technology (KCST), Doha, Kuwait-City, Kuwait

Abstract

E-voting system based on blockchain technologies are need of the day and their demand will increase in future by manifold. However, there are few studies that focus on critical analysis of blockchain e-voting from the standpoint of stakeholders. Therefore, government decision-makers and election stakeholders lack sufficient information to assess the dangers, problems, and opportunities connected with blockchain e-voting. This article shows how using a blockchain-based architecture for a any e-voting system might help stakeholders towards transparent sufficient voting processes like use it with the national elections to study the risks, opportunities, and challenges that a blockchain e-voting system for national elections could provide. Blockchain e-voting, according to the study, can prevent several security breaches, internal vote manipulation, and enhance transparency. However, voter validation and the blockchain architecture's security are two possible flaws that will require major attention.

Keywords: *E-voting, Blockchain, Security, Election.*

1. Introduction

The traditional political registration election voting used whiteboard counting score. In this paper, we use the private Blockchain in e-voting to give the new system was insufficient to enable government decision-makers and important election stakeholders to enhance the security electronic voting system to keep it more trusted and solidness towards fairness and integrity e-voting system within a local, national assembly elections. We were using a private blockchain solution to Write Once and Read Many (WORM) saved in the candidate's blocks to current results with voter anonymity. To close this gap, we illustrated how an architecture evaluation and documentation process Informatics might help election stakeholders understand the possible dangers, problems, and prospects of blockchain e-voting. To accomplish this, national assembly election paperwork and voter feedback establish the block key requirements for a national e-voting system. Credible elections lay the groundwork for long-term democracy and effective governance to avoid any unexpected forgery. Many developing countries' elections have a history of challenges, blunders, and institutional manipulations, lowering their legitimacy. Traditional voting systems are built on governing system architectures. It started with registering the voter as soon as they could register through the local mayor or governor's district. While it requires the voter to have completed twenty-one years old o more to allow him to register, this can be solved easily with our proposed system to authenticate the registrar's voting rights. In this paper [2], the proposed design allows the voter to change their vote before a preset deadline which might affect the integrity of the voting system. Conversely, we will enable the voter once to vote after they authenticate their right to vote. In this research [3], they reviewed a blockchain e-voting system based on a smart contract that enables voter privacy while setting Go-Ethereum to the permission for Proof-of-Authority (POA). E-voting has recently been acknowledged as one of the valid applications of blockchain technology. The decentralised Most of the issues with traditional voting systems and conventional e-voting can potentially be addressed by blockchain-based e-voting architecture. These include issues such as voter authentication, vote verification, voter privacy protection, vote security, and election outcomes integrity. General elections are a type of practice that democratic countries engage in regularly. The traditional general election method is hazardous, has resulted in controversy, and costs significant money. Many countries are attempting to use e-voting technology in general elections towards an improvement scheme for e-voting preparation, to proceed with the elections process should be completed successfully. The Kuwaiti Current Traditional Voting System: The National Assembly is composed of fifty members distributed in five electoral districts, who are elected through the direct, secret, general election following the election law. Ministers who are not elected in the National Assembly are considered members of the council under their functions. Kuwait is currently divided into five provinces/districts. And ten deputies are elected from each district. The right to vote is limited to one vote for every local citizen. A voter citizen, when a voter

reaches the age of 21, is entitled to vote. A secured electronic voting system that incorporates the integrity and security of current voting systems while providing the simplicity and adaptability of electronic systems. The blockchain provides the ability to overcome the restrictions and transmission barriers of electronic voting systems, guaranteeing security and integrity of the voters. This paper introduces immutability and remote voting with their proposed system which is one of our aims in this research [1]. Elections appear to be a highly important event in current democracy. Voting is almost every time used to organize elections, which are forms of procedure with established rules. In this paper, we suggest a brand-new blockchain-based electronic voting system for multidistrict elections and work to apply an effective and trusted blockchain-based electronic voting system to electoral college election scenarios [2]. Verifiability is one of the criteria in electronic voting that can boost trust in the technology by assuring that voters do not alter their ballots. Accuracy, Invulnerability, Privacy, and Verifiability are only a few of the factors that should be included in e-voting rules. Researchers have been able to calculate the degree of verifiability in the proposed e-voting protocol using the simple verifiability metric [3]. The conventional voting process is flawed in many ways. Using the E-Voting system, many problems are resolved. The blockchain is a database that is shared among all network users and will assist in verifying all votes cast without relying solely on a third-party system [4]. To accomplish so, we used a method based on interactions with electoral officials, national assembly election paperwork, and voter feedback to establish the block's key requirements for a national e-voting system. Elections that are credible lay the groundwork for long-term democracy and effective governance. Many developing countries' elections have a history of challenges, blunders, and institutional manipulations, lowering their legitimacy. E-voting has been proposed as a solution for many of the challenges of paper-based voting to ensure error-free and bias-free elections [5]. Traditional electronic voting systems are based on centralized system architectures, making them vulnerable to cyberattacks that target central infrastructures, such as distributed denial of service assaults (DDOS). E-voting has recently been acknowledged as one of the valid applications of blockchain technology. The decentralized nature of blockchain, and its attributes of anonymity, and transparency make it a suitable approach to handle many of the difficulties associated with conventional e-voting systems [6]. Most of the issues with traditional voting systems and conventional e-voting can potentially be addressed by blockchain-based e-voting architecture. These include issues such as voter authentication, vote verification, voter privacy protection, vote security, and election outcomes integrity.

The rest of the paper is divided in the following sections. The proposed architecture of how the blockchain technology can help in reducing the risks of misconduct in elections is presented in Section 2. Also, the subsections in Section 2 thoroughly explain the working of the proposed scheme. Finally, the conclusion is given in Section 3.

2. Proposed System

The system is integrated with a local Civil ID authentication system to authenticate and verify the voter ID. The introduction of blockchain technology has revolutionised the concept of decentralised and distributed transaction authentication, in which different entities can provide transactions without the need for a central entity to participate. That will avoid the previous traditional registration issues like adding new voters each year. For example, only people who go to the local mayor to register if they missed the deadline are not supposed to give a vote. Also they give a vote. Also, they offer specific days every year to add the names of those who were unjustly neglected in the previous voter's registration table and delete the names of the deceased and delete the names who transferred their domicile or house from one domicile to another, all of these issues are solved by adding the right to register with the current local domicile that is synchronized with the local Hawiti application the transactional encrypted confidential voter logs stored as private blocks as the votes and voter data cannot be tampered with as it is added in private blocks to the Blockchain. A blockchain can be created to add information while conducting transactions. When a voter registers, other devices create and validate a mass of information. When data is collected regarding the number of votes and whether the voters can vote according to the conditions, this information is also authenticated and added to the Blockchain, etc. This information is irreversible and is only disclosed to the polling station. When voters vote for a specific candidate, a dedicated polling station in that area can access this data, while using the Blockchain. To this end, most of today's solutions are centralised or not dependent on secure decentralised collaborative solutions. In this project, we aim to design an electronic voting framework supported by blockchain technology that can be integrated into today's sustainability of democratic systems to serve citizens and governments in providing renewable and on-demand electronic voting.

2.1. Private Blockchain

Blockchain technology is categorised into two categories: (1) public and (2) private. This research focused on the private blockchain because the private blockchain allows the sensitive data only seen by selected permitted users and no need for mining as a public blockchain [17]. We use private blockchain to preserve every transaction that should store once and read many in each block. The decentralised nature of blockchain technology improves data storage such that it cannot

be exploited by other parties or even the system owner. Blockchain technology can also react to an assault, penetration and intrusion on information recorded within it due to the decentralised structure, this technology stores the data in a safe place where their sensitive information is secured, protected, and encrypted by unwanted or unauthorised parties.

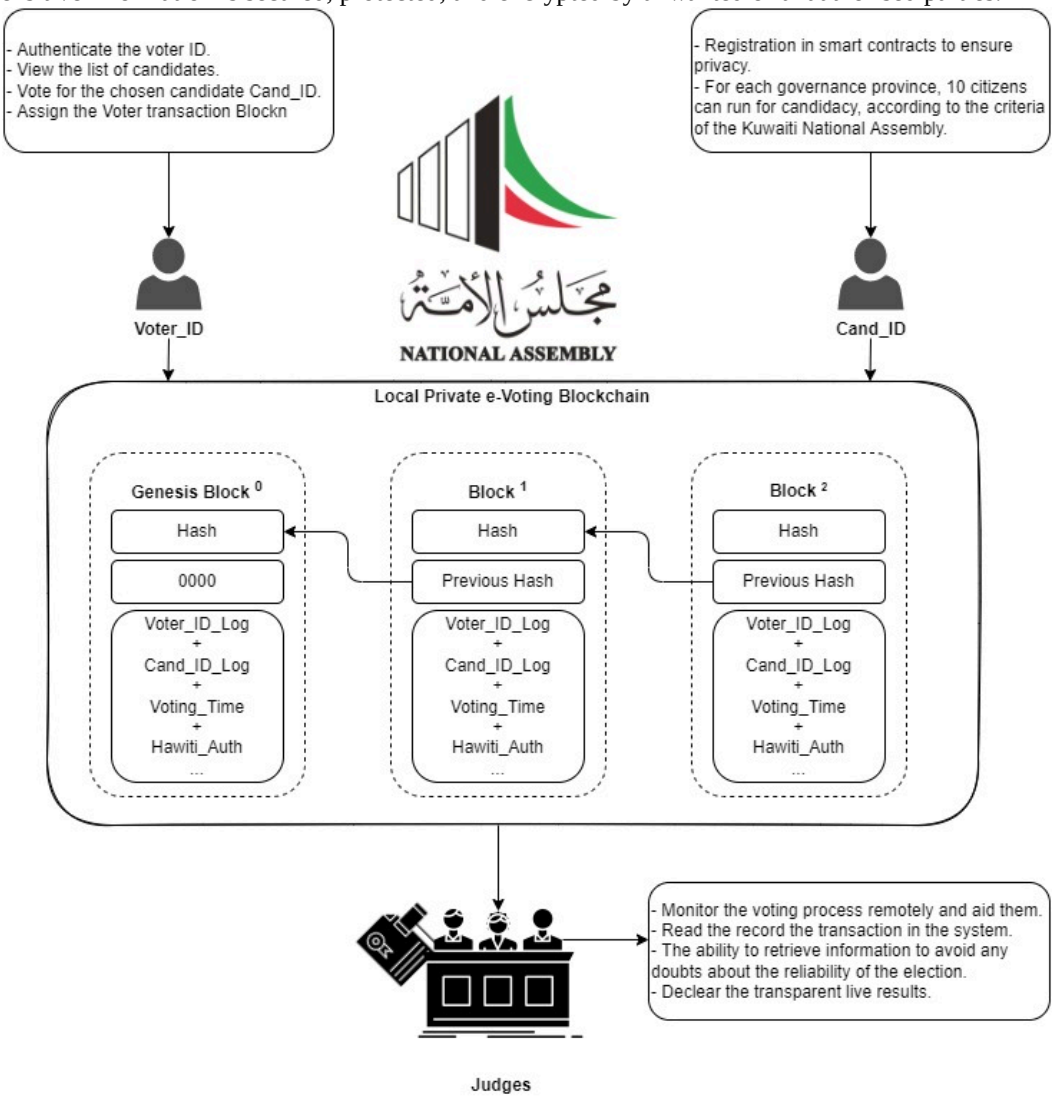

Fig. 1 E-Voting Preserve Private Blockchain System Processes.

2.2 Smart contract + PACI

Smart contracts can be made for all citizens quickly and accurately by linking the blockchain with the (My Identity) application of the Public Authority for Civil Information. So that every citizen has a unique private key. Smart contracts will contain three parties: candidates, voters, and judges, each of whom will have certain powers that he cannot override. The voter can choose only one candidate from the list of candidates, and the candidate can see the election results only and cannot change anything, while the judge is able to observe the election process and set the results. Smart contracts preserve the privacy of election results, spread confidence in the country, and eliminate fraud and corruption.

2.3. Cloud Storage

Cloud storage definition: huge storage place with huge storage space. User data is uploaded via the PACI (Hawiti app) to be stored. All files uploaded to the cloud can only be seen by others if you give your personal account information to someone else. That is why we suggested using it to store information that is done through the system.

2.4. National Assembly of Kuwait

The National Assembly of Kuwait elections are based on a voting process to select 50 elected members of the National Assembly. The election and voting process is governed by the Constitution of Kuwait and the election law. Elections are held every four years, and early elections may be held when the Emir of Kuwait dissolves parliament. Kuwait is divided into five electoral districts, and the voter in each district selects one candidate, and the top ten are chosen from each district to represent the Kuwaiti people in the National Assembly. The parties that can access the system are the polling stations associated with the National Assembly, which are distributed in each region, and usually in each area there is one or two centers in the school building. When implementing a Blockchain electronic voting system, the problems of questioning the credibility of some candidates and accusing them of fraud will be avoided.

2.5. Intended Users

The voter inserts his personal fingerprint into the voting node and provides a password. Votes are approved and declared via the Independent Electoral Commission's database. If successful, the digital ballot consists of a candidate's public key set and a unique polling identifier. The voter submits a vote for the preferred candidate.

Voter A voter citizen, when a voter reaches the age of 21, should register with the local council to entitled to vote the best candidate.

Candidates the candidate who apply to election affair to be elected by the voter

e-Judge have the authority to access the system from the voting center to track the ledger transactions of voters and their votes.

REQ 1: Hawiti app - If the voter does not create an account in the Hawiti app(Local Civil ID Authenticate all local citizenship with Civil information App), a voter must download the application and authenticate civil user data such as (name, age, nationality, etc.) to authorise the voter to create a private blockchain WORM User ID authentication ledger record.

REQ 2: private key - When linking a smart contract with Hawiti app, each user is given a private key that they are recommended to save it.

REQ 3: Send an email to the citizen voter confirming the creation of a civil registry in the Blockchain.

REQ 4: Choosing the constituency to which voter belongs from among the five departments in Kuwait.

2.6. Smart Contract Functional Requirements

REQ 5: Citizen voter registration.

REQ 6: Draw up a list of candidates, usually ten candidates from every circle.

REQ 7: This makes voting and candidate selection very easy.

REQ 8: Giving the right to show some voter data or the civil medical record only to the concerned party, for example (judges).

Blockchain Functional Requirements:

REQ 9: Coordinate and organise information thanks to a secure hashing algorithm.

REQ 10: Achieving data transparency because it is not stored in one place but is distributed throughout the network.

REQ 11: Ensuring the preservation of the user's identity, as this technology does not allow users to be identified and guarantees anonymity.

Table 1: Proposed System Intended Users

Name	*Responsibilities Description*	*Stakeholder*
Voter	- Authenticate the voter ID. - View the list of candidates. - Vote for the chosen candidate Cand_ID. - Assign the Voter transaction Block^{n}	Local Citizen User
Candidates	- Registration in smart contracts to ensure privacy. - For each government district/province, 10 citizens can run for candidacy, according to the criteria of the Kuwaiti National Assembly.	National Assembly
Judges	- Monitor the voting process remotely and aid them. -Record the results in the system. - The ability to retrieve information to avoid any doubts about the reliability of the election.	Ministry of Justice

2.7. E-Voting Database Schema Diagram

In the proposed system, the voter is provided with a private key, random people are not allowed to connect to the network, they can only connect once an account is created, and identity verification documents are submitted to the smart contract. Once the account authenticates and verifies the submitted documents, users are allowed to access the system, and the information recorded by smart contracts is stored in the cloud. In addition, civil information that is collected from the user, like the fingerprint features, is sent to the Blockchain. Figure2. Once completed, it is verified and sent back to the cloud for storage, and the information will be retrieved from the cloud to the election administration if needed.

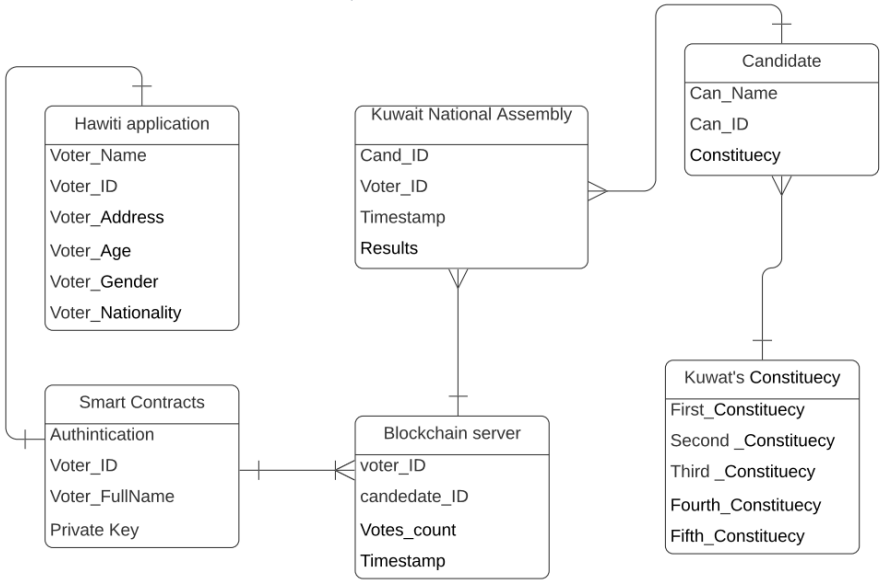

Fig. 2 E-Voting Database Schema Diagram

2.8. Blockchain for e-Voting

The Blockchain is an extensive and fragmented base, as it breaks down similar information with each other, which helps with this secure hash algorithm in fragmenting and encrypting data so that the system can quickly develop and be installed in the electoral process. The use of private Blockchain with a smart contract should help in sending the number of votes quickly and easily to the judges on an ongoing basis, which contributes to the confirmation and remote monitoring of voters and confirming their civil data, which prevents any errors or fraud and gives the voter confidence and freedom of choice. The system is integrated with local cloud storage as a reference in case of any error or failure in the Blockchain, which helps in not losing any of the user data and the ability to retrieve the data. Private Blockchain is characterised by security and privacy because it uses the secure encryption SHA-256 algorithm and is stored with the MD5 hash transaction function to add more unique ID ledger anti-forgery transactions. In this paper [5], they present an implementation study on Multichain evaluation for an e-voting scheme that contained four layers with a voter and admin that are different from our model. Because we focused on the WORM ledger and have three main user voters, candidates and judges, in the event of an election dispute, the system should be able to support any process that requires rechecking and recounting votes. The system

should be available for both voters and candidates within the borders of the country during the voting process, and it will be a useful system for the council to prevent external forgery, fraud or e-votes tampering. Judges can access voter-recorded ledger data and monitor voting remotely easily and recorded. After storing the information in the block^{n}, smart contracts will give the right to show the voter information to the judge's authority.

The E-voting System use case diagram explained in figure 3 includes the services for each user. At the same time, the role of each of them is as follows, the user (voter) should be able to create, authenticate, view candidates and cast or ballot the confirmation of the vote through accessing the account or logging in to the voter account and receive a confirmation authentication message from Hawiti app, they can view their data, and the electronic voting blockchain WORM ledger record will facilitate all these Blockchain transactions. The responsible (election authority or judges) will be able monitor, view, publish or declare the results Blockchain System are responsible for doing all the E-voting database schema diagram operations like adding, controlling and saving the information in the Blockchain and can monitor the process remotely.

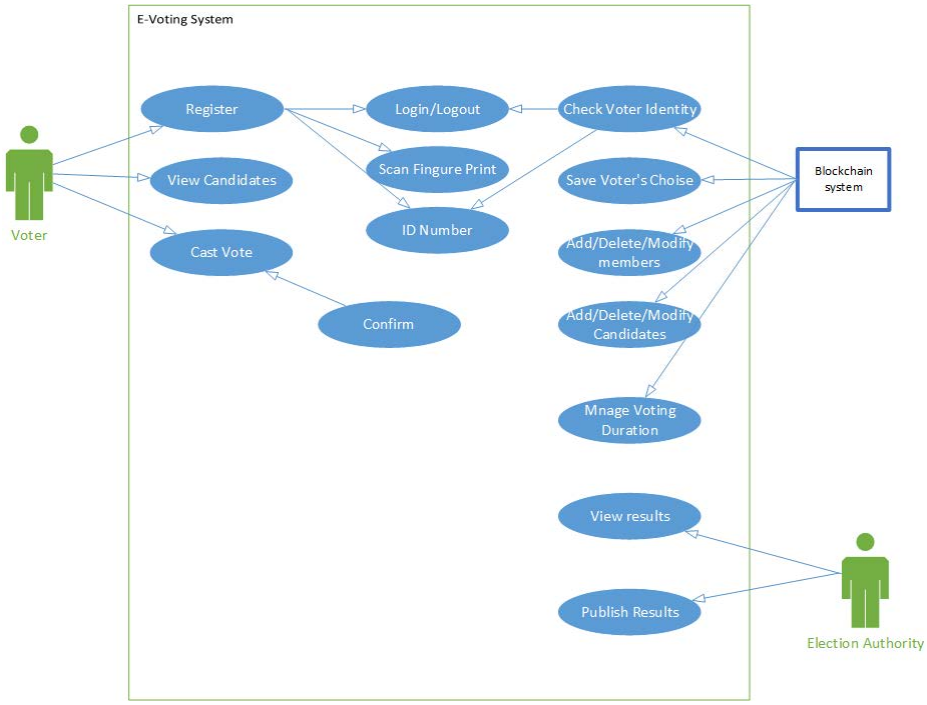

Fig. 3 E-Voting System Use Case Diagram

2.9. Securing E-Voting Process

The voter can vote once, and the vote keeps its anonymity feature process in the ledger. It can read many by the voter, judgers or candidates opposed by Hiabo Yi[6], that designed a "withdrawal model that allows voters to change their vote before a preset deadline". The process starts with authenticating and verifying the voter's voting eligibility by checking the birth date. If it is eligible, it goes to authenticate that the voter is not registered by any police or military service. If not registered, it goes to the next step, and then it issues the Voter_ID to allow the voter to choose the best national assembly candidate as the voter should choose only one candidate. The server will maintain two different repositories: Voter/ID repository: This database will have the list of eligible voters who will be accessed during the authentication process in the registration phase to check if the voter has the eligibility to vote and once a voter is approved the registrations and Voter_ID has been an issue it will be stamped and authenticated the voting attempt by block^{n}. The authors of BroncoVote [7], proposed Ethererum Blockchain-based e-voting system. They used homomorphic encryption that might slow the ballot and voting system. If it is used for a national assembly, the test of BroncoVote was based on university-scaled ensured using ballot-card and password for each voter candidate that is different from our system that should authenticate through hawiti app to allow the voter to vote. While on the other hand, [8] introduced the block sealing concept successfully, and we continued to use the block concept linked by the previous hash instead of linking to the next hash as explained in [8] also explained. Both the process after block n generated by entities for 'n' number of persons. The proposed e-voting approach[9], using a Non-Fungible Token (NFT), gives a nice try to use NFT in e-voting, but NFT is normally used for digital assets like a piece of art or digital online content used to track the royalty of the media art through tracking NFT ownership blocks in our proposed system we don't need it because we used MD5 to record the blocks ledger for each transaction. Recently, the researcher introduced many similar ideas to enhance the working of the e-voting systems using

blockchain technology [11-16]. However, these techniques are difficult to deploy in the current e-voting systems there for we developing a generic e-voting system based on private blockchain technology.

2.10. Flowchart

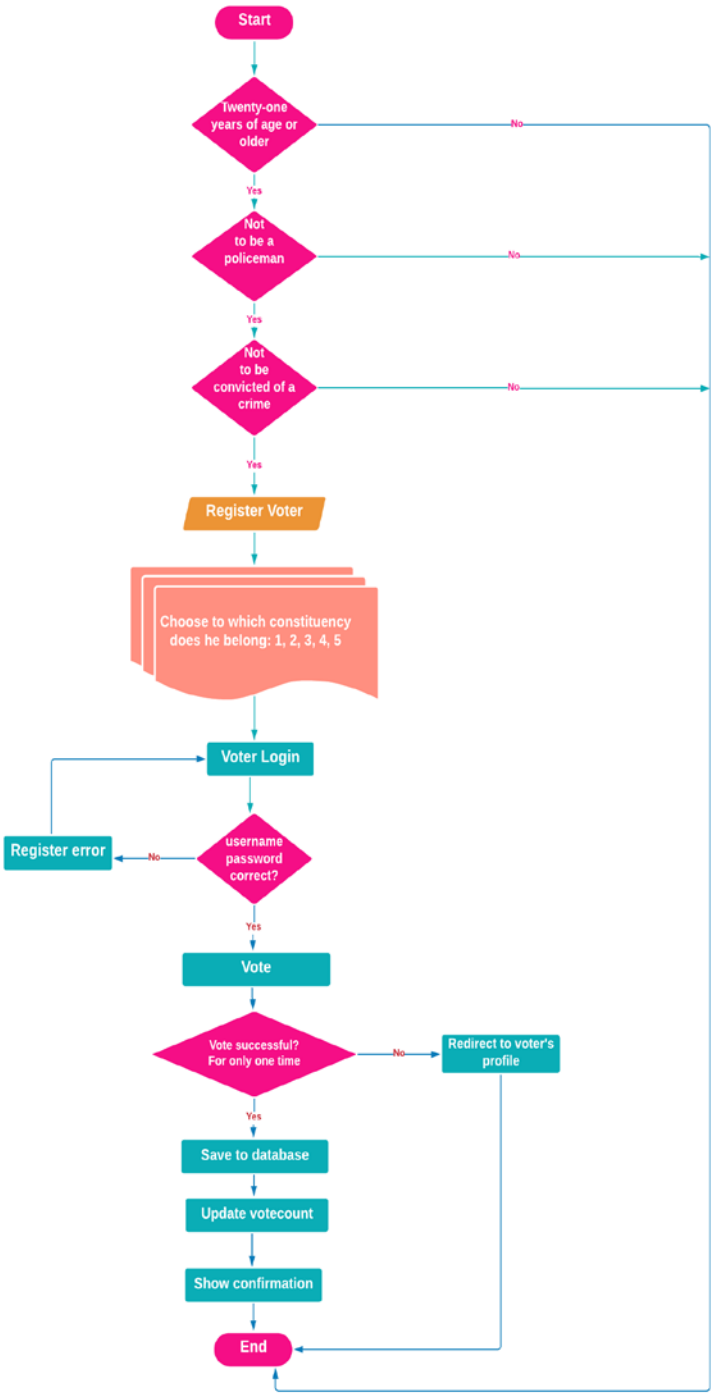

Fig. 4 E-Voting System Flowchart

In Figure 4, before completing the voting process, the voter must meet the conditions to be allowed to vote based on the Kuwaiti Election Law, and its conditions are as follows: The voter must be twenty-one years old or more, which can be

known by applying Hawiti, and not be a policeman, solider, or working in the military service. The voter must not have been convicted of a crime and can be verified by linking smart contracts to the website of the Ministry of Justice and Kuwaiti courts. Voters cannot vote more than once, and the voter must be in the same constituency they registered with. For example, the voter belongs to (the first, second, third, fourth, or fifth constituency). After the voter completes the registration process and logs into his account, the voter can read his voting transactions logs information, which the e-voting smart contract should facilitate. If there is a problem with the registry, an error alert will appear, and it should be recorded in the ledger logs. The responsible (judges' authority) should be able to monitor and read the block information in the Blockchain and can monitor the process remotely. According to his civil data, the system will also help to send an alert if there is any error. After completing the conditions, the voting process is completed successfully, and the votes are saved in the database with the continuous updating process. Then the results are displayed with the constant updating process, and then the results are displayed with ongoing updates until the end of the electoral process.

4. Conclusions

In conclusion, we proposed a secure solid e-voting system using local private Blockchain that solved double voting, voting forgery, late winner declaration announcement that can work to any voting system started from cooperative organization, association or clubs voting system to large number of voters like the parliament, municipality or council voting processes. The traditional voting system was insufficient to enable government decision-makers and important election stakeholders to make an educated conclusion on the merits of blockchain e-voting for national assembly elections. To close this gap, we illustrated how an architecture evaluation and documentation process Informatics might help election stakeholders understand the possible dangers, problems, and prospects of blockchain e-voting. The system should be highly recommended to use it instead of the current traditional whiteboard crossing the candidate voters to count the voters to announce the declaration winner announcement. As Yavuz et al. said, "E-voting is still a controversial topic within both political and scientific circles" [10]. That's why we will continue to implement more module to secure our private blockchain e-voting system. In future work, we will focus on enhancing the DDoS and session hijacking attacks detection during the voting time to detect any future expected vote forgery phenomenon. That's will allow us to elicit more explicit and implicit needs related to e-voting in the Kuwaiti context. This will show a more solid foundation for the proper design towards solidness securing private blockchain e-voting system and its proof-of-concept implementation.

References

[1] T. N. Suharsono, D. Anggraini, Kuspriyanto, B. Rahardjo and Gunawan, "Implementation of Simple Verifiability Metric to Measure the Degree of Verifiability of E-Voting Protocol," 2020 14th International Conference on Telecommunication Systems, Services, and Applications (TSSA, 2020, pp. 1-3, doi: 10.1109/TSSA51342.2020.9310915.

[2] H. Zhu, L. Feng, J. Luo, Y. Sun, B. Yu and S. Yao, "BCvoteMDE: A Blockchain-based EVoting Scheme for Multi-District Elections," 2022 IEEE 25th International Conference on Computer Supported Cooperative Work in Design (CSCWD), 2022, pp. 950-955, doi: 10.1109/CSCWD54268.2022.9776193.

[3] T. N. Suharsono, D. Anggraini, Kuspriyanto, B. Rahardjo and Gunawan, "Implementation of Simple Verifiability Metric to Measure the Degree of Verifiability of E-Voting Protocol," 2020 14th International Conference on Telecommunication Systems, Services, and Applications (TSSA, 2020, pp. 1-3, doi: 10.1109/TSSA51342.2020.9310915.

[4] Kamran, M. H. Nasir, M. Imran and J. -S. Yang, "Study on E-Voting Systems: A Blockchain Based Approach," 2021 IEEE International Conference on Consumer Electronics-Asia (ICCEAsia), 2021, pp. 1-4, doi: 10.1109/ICCE-Asia53811.2021.9641914.

[5] Ayo, C.; Daramola, O.; Azeta, A. Developing A Secure Integrated E-Voting System. In Handbook of Research on E-Services in the Public Sector: E-Government Strategies and Advancements; IGI Global: Hershey, PA, USA, 2011; pp. 278–287.

[6] Osgood, R. The Future of Democracy: Blockchain Voting'. COMP116: Information Security. Available online: http://www.cs.tufts.edu/comp/116/archive/fall2016/rosgood.pdf (accessed on 14 May 2020).

[7] G. Rathee, R. Iqbal, O. Waqar and A. K. Bashir, "On the Design and Implementation of a Blockchain Enabled E-Voting Application Within IoT-Oriented Smart Cities," in IEEE Access, vol. 9, pp. 34165-34176, 2021, doi: 10.1109/ACCESS.2021.3061411.

[8] Shahzad, B.; Crowcroft, J. Trustworthy Electronic Voting Using Adjusted Blockchain Technology. IEEE Access 2019, 7, 24477–24488. [CrossRef]

[9] Ayo, C.; Daramola, O.; Azeta, A. Developing A Secure Integrated E-Voting System. In Handbook of Research on E-Services in the Public Sector: E-Government Strategies and Advancements; IGI Global: Hershey, PA, USA, 2011; pp. 278–287. Osgood, R. The Future of

[10] N. Kshetri and J. Voas, "Blockchain-Enabled E-Voting," in IEEE Software, vol. 35, no. 4, pp. 95-99, July/August 2018, doi: 10.1109/MS.2018.2801546.

[11] acm. 1999. Software engineering code of ethics is approved. [ONLINE] Available at: https://dl.acm.org/doi/abs/10.1145/317665.317682. [Accessed 13 January 2021].

[12] . S. alZahir and L. Kombo, "Towards a global Code of Ethics for engineers," 2014 IEEE International Symposium on Ethics in Science, Technology and Engineering, Chicago, IL, 2014, pp. 1-5, doi: 10.1109/ETHICS.2014.6893407.

[13] S. A. Adeshina and A. Ojo, "Design imperatives for e-voting as a sociotechnical system," 2014 11th International Conference on Electronics, Computer and Computation (ICECCO), Abuja, Nigeria, 2014, pp. 1-4, doi: 10.1109/ICECCO.2014.6997569.

[14] G. Rathee, R. Iqbal, O. Waqar and A. K. Bashir, "On the Design and Implementation of a Blockchain Enabled E-Voting Application Within IoT-Oriented Smart Cities," in IEEE Access, vol. 9, pp. 34165-34176, 2021, doi: 10.1109/ACCESS.2021.3061411.

[15] F. Sheer Hardwick, A. Gioulis, R. Naeem Akram and K. Markantonakis, "E-Voting With Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy," 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 2018, pp. 1561-1567, doi: 10.1109/Cybermatics_2018.2018.00262.

[16] Y. Abuidris, A. Hassan, A. Hadabi and I. Elfadul, "Risks and Opportunities of Blockchain Based on E-Voting Systems," 2019 16th International Computer Conference on Wavelet Active Media Technology and Information Processing, Chengdu, China, 2019, pp. 365-368, doi: 10.1109/ICCWAMTIP47768.2019.9067529.

[17] Alothman B, Joumaa C, Alotaibi A, Alotaibi B, Almutairi B, Aldhafairi A, Khan M. Development of an Electronic Smart Safe Box Using Private Blockchain Technology. Applied Sciences. 2022; 12(13):6445. https://doi.org/10.3390/app12136445.

[18] E. Yavuz, A. K. Koç, U. C. Çabuk and G. Dalkılıç, "Towards secure e-voting using ethereum blockchain," 2018 6th International Symposium on Digital Forensic and Security (ISDFS), 2018, pp. 1-7, doi: 10.1109/ISDFS.2018.8355340.

Basil Alothman joined Kuwait College of Science and Technology (KCST) as Assistant Professor at Computer Science and Engineering Department. Dr. Basil graduated from De Montfort University, Leicester, UK with a PhD in Computer Science. He received his MSc in Computer Science from University of Hertfordshire, UK and his BSc in Computing and Information Systems from University of Dubai, UAE. Dr. Basil is mainly interested in cybersecurity science or, more specifically, computer and network security issues, mobile security, computer privacy, OSINT, reverse engineering, cloud and VM security, big data security, IoT security, and Botnet detection techniques.

Chibli Joumaa is an Associate Professor of Computer Engineering in the Faculty of Engineering and Computer Science of the Kuwait College of Science and Technology (KCST) since April 2020. In addition to his role in the Computer Science and Engineering department, he oversees accreditation related processes in collaboration with the coordinators, dean, and president. He has previously occupied several teaching, administrative, and managerial positions in reputed education institutions.Dr. Chibli Joumaa holds a bachelor's and master's degree in electrical engineering from the University of Balamand in Lebanon, in 2004, and a master's in Network Telecommunication and System Architecture from France, in 2005. He received his PhD in Computer Engineering from the the University of Technology of Belfort-Montbeliard, France in 2010. He is the author of many publications and have attended many professional trainings and workshops for accreditation and academic advancement

Sarah Alshammeri is Kuwaiti computer engineer graduated from Kuwait College of Science and Technology (KCST). Sarah got work experienced within Ministry of Education. She developed many projects related to C++. Sarah would like to extend her academic experience within research achievement with programming information security projects.

Murad Khan has completed his Master and Ph.D. degrees both in computer science and engineering from the School of Computer Science and Engineering in Kyungpook National University, Daegu, Korea. Dr. Khan is currently working as an assistant professor at the Kuwait College of Science and Technology, Kuwait. Dr. Khan also served as Brain Pool Fellow at Kyungpook National University, Daegu, Korea from December 2019 to December 2021. Dr. Khan published over 100 International conference and Journal papers along with two book chapters and is an editor of books in Springer and CRC Press. Dr. Khan served as an editorial member of various special sections in world-renowned journals such as Computer & Electrical Engineering, Transactions on Emerging Telecommunications Technologies, etc. He also served as a TPC member in world-reputed conferences and as a reviewer in numerous journals such as IEEE Communication Magazine, Future Generation Computer Systems, IEEE Access, etc. His area of expertise includes ad-hoc and wireless networks, architecture designing for the Internet of Things, Communication Protocols designing for smart cities and homes, Big Data Analytics, etc.