Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2021.014827
Article

Tech Science Press

Computational Intelligence Approach for Municipal Council Elections Using Blockchain

Fatmah Baothman*, Kawther Saeedi, Khulood Aljuhani, Safaa Alkatheri, Mashael Almeatani and Nourah Alothman

IS Department, King Abdulaziz University, Jeddah, 21551, Saudi Arabia
*Corresponding Author: Fatmah Baothman. Email: fbaothman@kau.edu.sa
Received: 20 October 2020; Accepted: 21 December 2020

Abstract: Blockchain is an innovative technology that disrupts different industries and offers decentralized, secure, and immutable platforms. Its first appearance is connected with monetary cryptocurrency transactions, followed by adaptation in several domains. We believe that blockchain can provide a reliable environment by utilizing its unique characteristics to offer a more secure, costless, and robust mechanism suitable for a voting application. Although the technology has captured the interest of governments worldwide, blockchain as a service is still limited due to lack of application development experience, technology complexity, and absence of standardized design, architecture, and best practices. Therefore, this study aims to build an imperial example for a blockchain electronic voting (e-voting) application using digital identity management for fulfilling immutable, transparent, and secure distributed blockchain features. The paper reviews the current types of e-voting systems and discusses the standard processes. We propose a conceptual design for a blockchain providing a digital identity management service to secure the e-voting application results. The blockchain development process implemented in this study follows the Proof of Concept to verify the e-voting application's function for illustrating the architecture and description of the application's business process model. The development is based on the Ethereum platform, which allows the implementation of the Proof of Work consensus algorithm. The developed e-voting application saves time, requires fewer processes, and results in higher accuracy, more transparency, considerable voters' privacy, and accountable system management. We expect that the e-voting blockchain application will impact governmental processes during the election, reduce spending, support digital transformation, and ensure fairness of results.

Keywords: Blockchain; election; e-voting; Ethereum; smart contracts; solidity; truffle

1 Introduction

For centuries, the expense of voting or electronic voting (e-voting) increases as the population grows; it involves a high level of integrity and security requirements. Traditional voting systems are conducted either manually based on paper verified by the individual presence in a particular location or sent by traditional mail in

a secured envelope. Such a system requires substantial manual work, time, and costs and is vulnerable to fraud [1]. Therefore, using a reliable technology that can solve such issues is urgently needed. Blockchain technology is becoming one of the world's key emergent technology in the wake of Bitcoin's growing acceptability and success [2]. Many studies have supported the use of blockchain technology in several domains, including education [3], healthcare [4], IoT [5], shipping [6], and government [7]. Furthermore, using blockchain technology enables digital authentication and secure storage for data and information, such as marriage or death certificates, assets or bank account books, and medical records [8]. The blockchain distributed, unalterable, indisputable, public ledger enhances all eligible citizens' voting processes for thriving social democracy issues [7]. Using blockchain technology to develop the e-voting application increases security and eliminates many vulnerabilities, such as a single point of failure and denial of service attack in the regular electronic system. Unlike traditional voting, the blockchain provides better data transparency and traceability because the blockchain network's operation is based on the peer-to-peer principle. The distributed control ledger also prevents any mode of failure or integrity tampering given that each new block references the previous one, and a network consensus protocol controls the entry of any new block. Smart contracts' availability allows the execution of reliable, immutable, and trackable transactions as well without third parties [9–12]. Finally, it ensures that the blockchain network remains permanent and uneditable and that transactions remain protected against corruption and deletion [13].

Therefore, continuing efforts are made to improve the election process and develop e-voting applications by leveraging blockchain's unique features, such as immutability, transparency, and anonymity, to provide a better voting environment. However, implementing and deploying a blockchain-based e-voting application is challenging because of the complexity of this technology, lack of development experience, and requirement of professional users' skills. Thus, this study investigates the features needed to build blockchain-based e-voting applications for addressing the research question "Do we need all the blockchain features to build all different types of applications?" In other words, "What are the main features that make the voting process less complicated for development and adoption?" We build an e-voting application for municipal councils' election based on Proof of Concept (PoC) to answer these questions. In some places, most municipal council elections are still held via a traditional mechanism to deal with some vulnerabilities related to fraud, security, and transparency. Therefore, this study's primary motivation was to fully utilize the blockchain features for improving municipal elections by creating an e-voting application. Overall, the key contributions of this study can be summarized as follows:

1. Highlighting the blockchain features needed to empower e-voting applications and maintain the fairness and fitness of the voting process.
2. Designing a conceptual model of e-voting application on the blockchain with application architecture and business process model that worked successfully for developing an e-voting application based on PoC for municipal council elections using the Ethereum platform.
3. Developing an e-voting application based on PoC for municipal council elections using the Ethereum platform.
4. Evaluating the proposed application to ensure that it has utilized the required blockchain features of the e-voting process.
5. Producing a state-of-the-art working application with an Arabic interface.

The rest of the paper is organized as follows. Section 2 provides an overview of blockchain technology and its features and platforms. Section 3 summarizes the work related to the blockchain features used to build an e-voting application. In Section 4, the current voting process used for municipal council elections is presented. Sections 5 and 6 introduce the proposed application and present its architecture, design, and implementation stages. Section 7 evaluates the proposed application and compares it against others. Section 8 contains the implementation, limitations, and future work. Section 9 presents the conclusion.

2 Blockchain Technology

The blockchain is a public distributed ledger that is shared and secure, wherein a growing list of transaction records (blocks) can be stored without being erased or changed. This technology was introduced in 2008 as a platform for a digital cryptocurrency called Bitcoin by Nakamoto. All computers or nodes that run blockchain's protocol store a copy of recorded transactions for enabling P2P transactions without an intermediary through machine consensus [9,10].

2.1 Blockchain Features

By nature, blockchain provides a secure platform that is composed of architectural elements and processes/logic. Architectural elements contain two elements: decentralization and cryptographic hashes. Decentralization means that no third party or authority is needed to authenticate the transactions. Thus, data are controlled by a decentralized network. The blockchain network operates based on the peer-to-peer principle of providing better data transparency and traceability. Meanwhile, a cryptographic hash is an algorithm that uses input and produces an output called a hash [14,15]. It is used for hashing the transactions and in some types of consensus algorithms, such as Proof of Work (PoW).

Blockchain processes and logic contain four processes: consensus algorithm, smart contract, data authentication, and digital signature. A consensus algorithm is a decision-making process where a group of active nodes reach agreement quickly and speedily. However, the rules of consensus can be modified to fit several circumstances. In other words, the consensus is similar to a voting system, where the majority wins, and the minority has to support it. A smart contract is a digital contract designed to facilitate, validate, or execute performance or negotiate the contract. It allows the performance of reliable, immutable, and trackable transactions without third parties [11]. Moreover, it is executed by nodes within the network; all nodes must derive the same execution results, and these results are recorded on the blockchain [12]. Data authentication is a process of sending the real identity with a pseudonym to the authentication center to secure the pseudonym's signature. This process is useful for conferring everyone with a pseudonym [16]. Finally, a digital signature is a process used to verify the data's authentication [14]. The users own a pair of private and public keys to access and sign the transaction. For example, when the sender signs the transaction, the hash is generated and encrypted using the private key (sign phase). Then, the receiver obtains the encrypted hash associated with the original data and validates the transaction by using the sender public key with decrypted hash and the hash obtained from the received data. These architectural elements and processes of blockchain provide the following features:

a) **Immutability:** This feature means something that cannot be changed or modified. It helps ensure that the blockchain network will remain permanent and unalterable in addition to protecting all transactions against corruption and deletion [13]. A piece of information can only be altered in all nodes in a blockchain network. This case is impossible.
b) **Transparency and Data Integrity:** This feature is automatic whereby network nodes can check and trace the transaction. Thus, the transaction cannot be changed unless all network nodes reach a consensus related to such precise change.
c) **Persistency:** If blocks need to confirm and sign every transaction, this case makes any changes or misuse of the transaction impossible [14].
d) **Anonymity:** This feature is used to reduce the possibility of tracking the sender and the transaction recipient.
e) **Data Validation:** This feature is the process of ensuring that the transactions are eligible.

In the following parts of the paper, we will emphasize the importance of these features in developing a blockchain-based e-voting application. We will also state the way some of these features have been employed in the developed application.

2.2 Blockchain Platforms

Many platforms with different features are available for blockchain. Tab. 1 provides a comparison of these features.

Table 1: Comparison of Blockchain Features [17]

Blockchain Platform	Bitcoin's limitations overcome	Network Permission	Consensus Protocol	Special Hardware Requirement	Smart Contract Support	Support Ledger Wallet
Ethereum	Digital Asset Management	Permissionless/ Permissioned	Proof-of-Work/ Proof-of-stake	No	Yes	Yes
Bitcoin	NA	Permissionless	Proof-of-Work	No	No	Yes
Zcash	Anonymity/ Privacy	Permissionless	Proof-of-Work	No	No, under development	Yes
Litecoin	ASIC Resistance	Permissionless	Proof-of-Work	No	No	Yes
Dash	Anonymity/ Privacy	Permissionless	Proof-of-Work/ Proof-of-service	No	No	Yes
Peercoin	Efficiency Long-term Energy	Permissionless	Proof-of-Work/ Proof-of-stake	No	No, under development	Yes

Three blockchain frameworks as a service for e-voting based on Ethereum, namely, Geth, Exonum, and Quorum, are available. Exonum and Quorum consensus do not support PoW, PoS, and PoA. Blockchain can be public, private, or consortium; each type is limited to read and write permissions or permissionless and consensus participations. Exonum is limited because it uses only Rust programming language and can handle only up to 5000 transactions p/s. Meanwhile, the Quorum and Geth use Go, C, and JavaScript and can handle hundreds of transactions p/s. Thus, blockchain scalability is a serious issue and cannot instantly meet the processing of millions of transactions. Ethereum technology has overcome blockchain limitations in cryptocurrency by turning blockchain into a broader solution for many world systems. One of the main advantages of Ethereum is that it supports automatic digital asset management by using smart contracts. Thus, asset managing programs become much more manageable than using scripting languages to achieve the same results. It also adapts the PoW consensus protocol [17] and offers enhancement for the state of the transaction and blockchain structure [18]. The block time of Ethereum is around 15 s, with numerous peaks up to 30 s [18,19]. The scalability of Ethereum has some concerns, but Ethereum can successfully control over one million transactions within 24 h, with an average of 11 transactions per second [18–20]. Therefore, Ethereum was selected for proposing the election voting application in this study due to its mechanism for supporting consisting accounts and smart contracts.

As mentioned previously in the blockchain technology section, architectural elements and processes of blockchain provide many features. However, this study aims to highlight the adequate features to build an e-voting application for making the public voting process easier, faster, and more transparent.

3 Existing E-Voting Solutions

Two categories of voting systems have been addressed in prior studies: the direct recording electronic system (e-system) and the Internet voting system (I-voting). An e-voting system, rather than the traditional paper ballot system, is utilized in polling stations [21]. Most e-voting systems that have been developed aim to reduce the cost of the election process and guarantee the election's integrity by fulfilling the requirements of security and privacy [21–23]. However, e-voting election can be impacted by manipulation in some cases [22–24]. Although I-voting is better than the e-voting system in terms of specific security aspects, the I-voting system still has drawbacks, such as transparency, security, and credibility [21–25]. The I-voting system's centralization makes it vulnerable to attacks that imperil election results or voter information [21]. Thus, the e-voting and I-voting systems cannot address stringent privacy and security requirements.

All the previously proposed systems suffer from challenges or trading off between some blockchain features and others, such as low processing speed, linearly proportional time for voting to the ring size [26,27], and centralized security servers. Thus, we attempt to build an effective and more efficient e-voting application by adding the features that more completely satisfy the e-voting process requirements and provide solutions to avoid those challenges in the implementation and deployment phases. For example, one study [26] proposed using zero-knowledge proof in the e-voting application. The system progresses through four stages and consists of two entities: the voter and the administrator. The first stage is the preparation, which consists of three phases. In the first phase, the voter creates an account and registers a bitcoin address to obtain the right to vote. In the second phase, the voter receives the voting cost from the administrator in his or her bitcoin address, exchanges the received cost to a secure digital commitment of Zerocoin, and registers this commitment to the administrative system. Thereafter, the administrator announces the list of Zerocoin commitments. In the third phase, the voter can exchange the Zerocoin for Bitcoin and deposits the declared commitment in the zero-knowledge proof. In the voting stage, the voter performs the voting and initiates a commitment to prevent voting data leakage. Thus, the voter establishes a transaction using the open return part of the protocol. In the counting stage, the administrator checks all the transactions to set valid Zerocoin commitments while exchanging Zerocoin to Bitcoin. In the publishing stage, the administrator counts the votes and publishes the results. Eliminating the tracing link between the votes and the voters is important. However utilizing this system is difficult for an election with many voters because its processing speed is slow. Furthermore, the study of [27] proposed an e-voting system based on the Ethereum blockchain by using a one-time ring signature mechanism to ensure that the voter with one key-pair could not sign a vote more than once. It entails a particular group verifying the vote and enabling anyone who has the right to access this network to access it and obtain the result of voting without the third party. This way reduces the election's cost. The ring signature has been applied in the system to ensure that the relationships between voters and their ballots are not revealed. However, the voters' spending time signing their ballot with a one-time ring signatures scheme is linearly proportional to the ring size, which is considered acceptable for maintaining voter anonymity.

Another study [28] proposed a solution to solve the personal authentication problem by developing extensions for the standard security protocols to include user privacy and anonymity. It relied on using crypto credentials as anonymous identities. These extended security protocols can enhance user privacy and anonymity and security (authentication and validation of transactions) in the blockchain applications. These protocols have been implemented based on federated security architecture, which contains secure

proxy servers and security protocols. This solution's strengths reside in providing the highest level of assurance (level 4) and all sensitive data under strong protection and ensuring user control over it. However, the protocols continue to use centralized security servers to date. All the proposed systems suffer from challenges or trading off between some blockchain features and others. Thus, we attempt to build an effective and more efficient e-voting application by adding the features that more completely satisfy the requirements of the e-voting process and provide solutions to avoid challenges in the implementation and deployment phases.

4 Current Voting Process in Municipal Councils

The applicants for the country's administrative positions are assigned through local elections, wherein all citizens participate in the decision making. Municipal council elections are conducted every 4 years, wherein the process of election consists of five stages [29]. The first stage is about submitting all the required information on the participating citizens. Then, electoral rolls are published for any corrections and contestations. The failure to register in the defined registration phase results in losing the right to candidacy or voting on the voting days. The second stage is concurrent with the first stage, which is about finalizing the voter or candidate profiles. Thereafter, the third stage starts with the publication of the final candidate names. A candidate cannot declare his or her candidacy and start his or her electoral campaign before publishing the candidate names' final list. The last stage is the ballot day or voting day, which represents the most crucial part of the whole election process. All the previous stages are considered preparatory to this stage. Voters select their suitable candidates, and the list of successful candidates and the final results are published upon completion of the vote-counting process. Fig. 1 shows the BPMN of the current voting process.

5 Design of Proposed E-Voting Application Based on Blockchain

We build a blockchain-based e-voting application and add it as a new e-voting service to the election application, which is a subsystem deployed on Ethereum smart contract. This study identifies only some features that can help build an e-voting application, as shown in Tab. 2. The proposed application consists of two different scenarios, namely, the ordinary user and admin (Fig. 2). Initially, the user creates his or her voting document with some required inputs, such as name, national ID, phone, and other mandatory personal details. Then, an admin validates these applications based on the desired policy. Only valid users can complete the voting process while the system synchronously creates the blockchain blocks. Figs. 1 and 2 show the difference between the voting process in the current and the proposed applications.

The existing application lacks an e-voting service where the voters must go to the electoral centers to participate in the election and cast their votes. By contrast, the proposed application employed the Ethereum private blockchain to automate the voting process and provide a better voting environment by leveraging blockchain technology features.

In the architecture and workflow of the proposed application, the voter logs in to the application by submitting the ID information. If the voter is authorized, then Ethereum coins are released, and the voter can vote. After voting, the application communicates with the smart contract to show the candidates' list and the total number of votes for each candidate (Fig. 3). Every voter (using a browser) connects with the application directly. The benefit of decentralization is that individuals do not need to rely on a single central server, which might disappear at any point. Any transaction performed in the Ethereum network is recorded into blocks, and every block is linked to the following block.

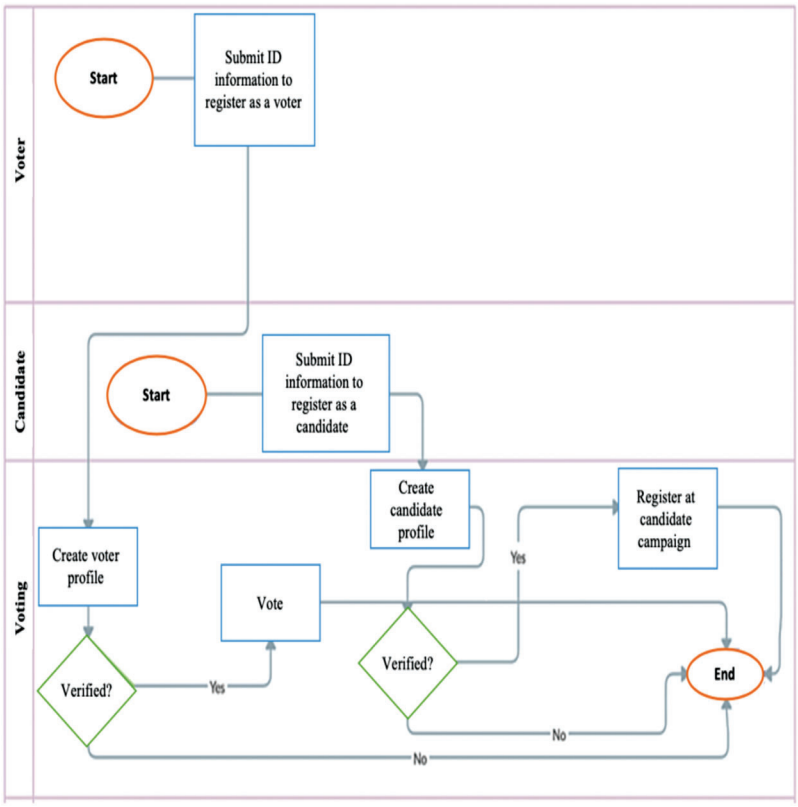

Figure 1: Current voting process

Table 2: Blockchain Features Used in the Proposed Application

BC Feature	Effect on The Voting Process
Smart Contract	It is responsible for reading and writing data to the blockchain. In the proposed e-voting system, the smart contract represents an agreement that states that each vote will count, and every vote is only counted once. The candidate who has the most votes will win the election.
Wallet	Each voter must have an Ethereum wallet with Ethers to cast a vote and complete the voting process. The votes will be stored in the Ethereum blockchain using the smart contract, which will validate and verify the votes and voters.
Transparency	In the proposed application, the e-voting process must not allow voters to cast a vote twice, and the process must achieve full transparency. The transparency is achieved by providing the voter with election results after each voting process, which allows the voters to ensure that their votes were counted.
Anonymity	Given that each voter must have an Ethereum wallet to cast a vote, the wallet address will be used to maintain voters' anonymity by reducing the possibility of tracking the voters and their votes.

(Continued)

Table 2 (continued).

BC Feature	Effect on The Voting Process
Decentralization	It must be used to automate the voting process without the need for a central authority.
Immutability	In the Ethereum blockchain, the complete code is immutable, and the smart contract cannot be modified.
Data Validation	Ensures that the voters are eligible and that votes are legitimate before placing the votes into blocks.
Data Authentication	Involves using the voter's wallet address and smart contract functions.

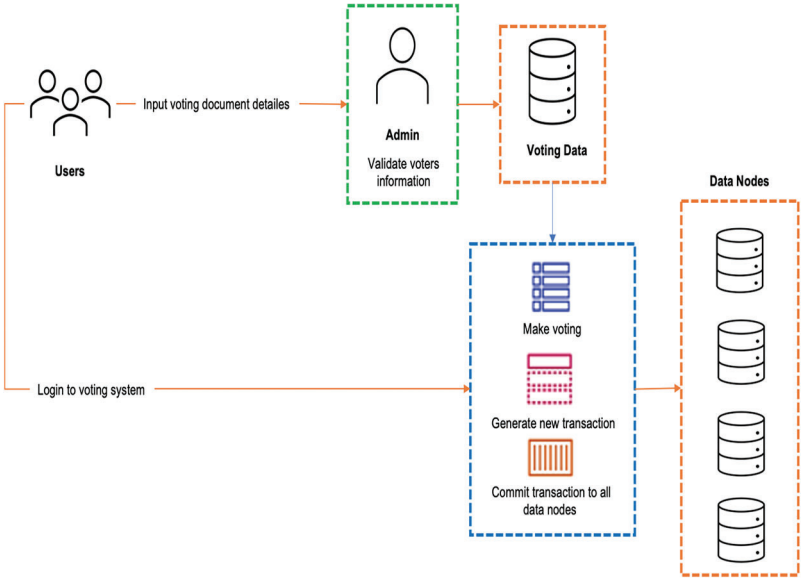

Figure 2: Architecture of e-voting in blockchain

6 Implementation of the Proposed Application

We used HTML, CSS, and JavaScript to design graphical user interfaces, and we used Solidity language to write the smart contract. We also used some dependencies as follows:

1. **Node Package Manager (NPM):** It allows downloading and using many free packages.
2. **Truffle Framework:** It provides a development environment, asset pipeline, and testing environment using the Ethereum virtual machine [30]. It allows building distributed applications, offers different kits to write smart contracts with the Solidity programming language, and has a built-in smart contract compilation.
3. **Ganache:** It is a local in-memory blockchain that gives ten external accounts with associated addresses on the local Ethereum blockchain.
4. **MetaMask:** It provides an extension for Google Chrome to link to the local Ethereum with a personal account and cooperate with the smart contract we built.

The primary function of this application is voting, whereby the voters select a candidate and then can pay some Ethers to cast their votes. The application ensures that all voters are legal and authorized. It also

prevents any voter from voting for more than one candidate, guarantees that all the votes are counted correctly, and ensures the confidentiality of voting whereby no one can know which candidate the voter selected. The voting process in the application involves two main functions, which are discussed as follows:

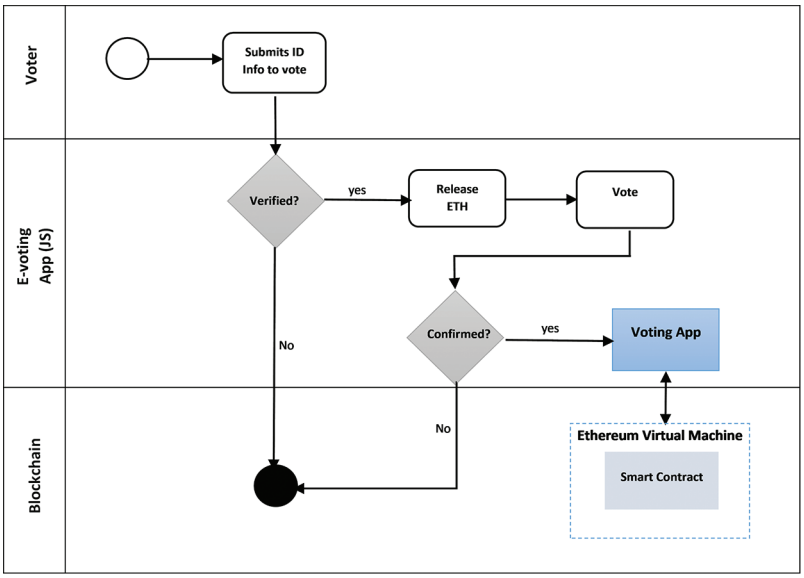

Figure 3: Voting Decentralized Application Process

Adding the Council Candidates: Herein, the smart contract and the local Ethereum blockchain (Ganache) are migrated first. Then, we declare the candidate and a function to add a candidate with the codes obtained from [31]. Fig. 4 shows the election page before the voting process.

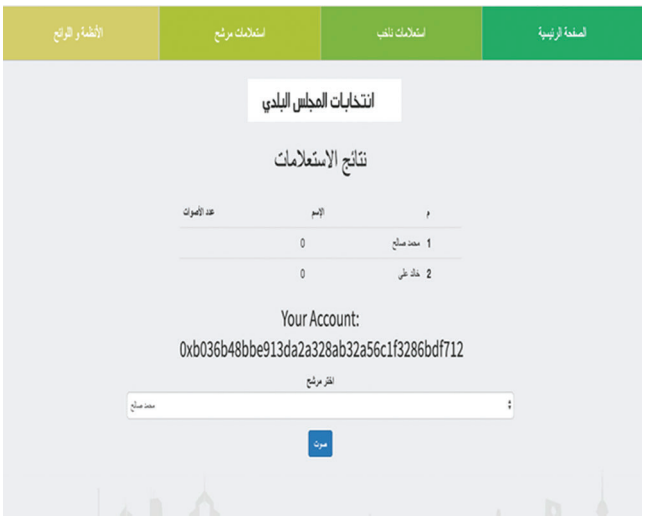

Figure 4: Election Page before the Process of Voting

Casting a Vote: This function enables the voters to vote. It also takes the candidate ID as an argument and adds the voter account to the voters mapping to track the voter's account. Moreover, it applies some conditions to ensure that the voter ID is valid and has not voted before. The voter who has sufficient

funds can select a candidate by clicking on the "Vote" button. When the voter selects the desired candidate, his or her voting will be either confirmed or rejected by MetaMask (Figs. 5 and 6), and the funds of that account are decreased. However, when the voter tries to vote again, the application will reject his or her vote. The election page is updated with each candidate's results, as shown in Fig. 7, when the voting is completed successfully.

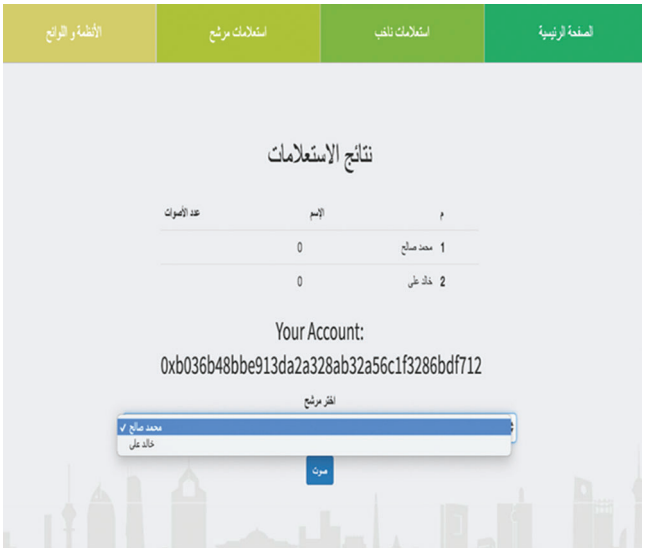

Figure 5: Voter Selects the Desired Candidate

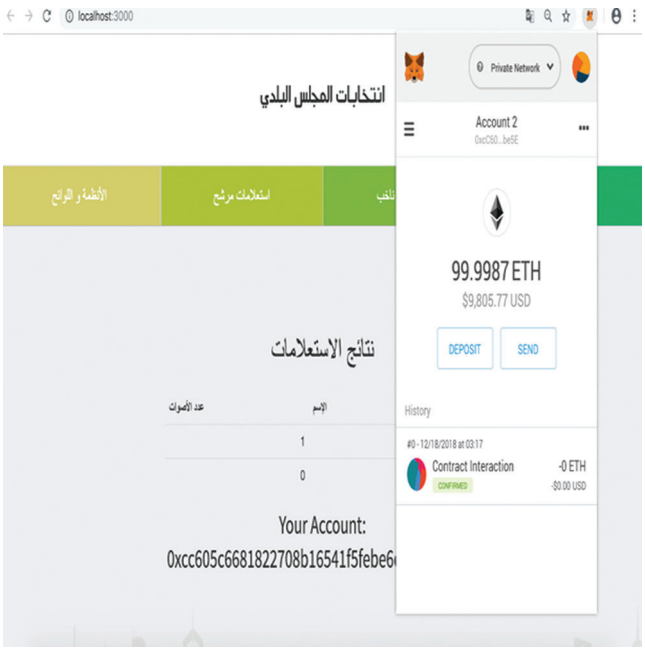

Figure 6: Voting is Successful

Figure 7: Election Results

7 Evaluation of the Proposed Approach

Regarding the features used in the proposed e-voting system in terms of anonymity (used to reduce the possibility of tracking the voters and their votes by using the wallet address), we found that this way does not provide a high degree of anonymity. Specifically, the process of voting requires a coin wallet for each voter; thereafter, the voters transfer their coins to the candidates of their choice. Similarly, the study of [25] proposed using zero-knowledge proof in the e-voting application to solve the problem of anonymity and privacy. However, as mentioned in related work, utilizing this system with many voters is difficult because the processing speed is relatively slow. In terms of privacy and transparency, the voting process of the proposed system has high transparency given that the application provides the voter with election results after each voting process. This step ensures that each voter's vote has been counted. However, data privacy tends to be less because the nature of the relationship between the two features is an inverse relationship. Using an intermediate unit between the voters and the candidates to convert transferred coins to another and using a one-time ring signature would be a reasonable solution to solve anonymity and make the process of tracking the voters more difficult [26–32]. Tab. 3 compares this application and other blockchain voting applications.

Table 3: Comparison between e-voting applications based on blockchain

Ref.	Principle/platform	Advantages	Disadvantages
[25]	Zero-knowledge proof	High anonymity	Low processing speed
[26]	One-time ring signature	High anonymity	Spending time for voting is linearly proportional to the ring size
[27]	Crypto credentials	High anonymity, user control, and security	Uses centralized security servers
Our study	Ethereum private blockchain	Middle anonymity and high transparency	We cannot accurately determine them

The current practice of physically conducting elections has some vulnerabilities related to security and transparency. Thus, the primary purpose of this study was to utilize blockchain technology to improve the mechanism for municipal elections through a suitable application [33–40]. A blockchain-based e-voting application was built to fully utilize the blockchain features and demonstrate the blockchain-based application's benefits compared with the existing application. The application was designed and implemented using an Ethereum private blockchain. As mentioned previously, the Truffle Framework, Ganache, and Solidity language were used as the development environment to build the application [41–48].

A block contains three data cells: (1) block header that contains information about the voter identity as a hash value produced by the PoW, the source IP address, the target IP address, and the voter actions; (2) the timestamp that indicates the voting time; (3) and the transactions used for the voting process. During a block validation, transactional knowledgebase (TK) uses a private key (Pn) with the source IP address and hash algorithms SHA-256 using Eq. 1.

$$TK = SHA\text{-}256(H||Vc) \tag{1}$$

In the abovementioned equations, H and Vc denote the header and voter action, respectively; the miner node computes the PoW using Eqs. 2, 3, and 4.

$$P_n = SHA\text{-}512(C||Mrk(H)||\text{previousblockhash}) \tag{2}$$

$$P_{n+1} = SHA\text{-}256(P_n||t) \tag{3}$$

$$PoW = SHA\text{-}256(P_{n+1}||N) \tag{4}$$

In Eq. 2, Mrk denotes the Merkle root, t is a timestamp, and N is nonce generated by PoW. The value of PoW is saved to the ledger distributed nodes. This procedure is repeated to generate all validated blocks producing a blockchain.

8 Conclusion

We proposed using an e-voting blockchain application to improve the traditional voting process and made it secure, untampered, cheaper, and faster. Studying the issues of previous voting systems ensured the need for developing an improved, reliable process for an e-voting application. The work sheds light into blockchain limitations and enhancing features of e-voting applications. We introduced a conceptual design for a blockchain e-voting application, which follows the PoC and PoW consensus algorithms. We described the architecture and verified the processes using the Ethereum platform with the Arabic language interface for allowing hundreds of transactions to be processed at once using computational techniques. We successfully developed a blockchain e-voting application for the Arabic language based on the Ethereum platform to support fewer processes, costs, and less time with enhanced security. The developed application allows voters to select a candidate. The application ensures that all the voters are legal and authorized to be part of the election. It also prevents voters from voting for more than one candidate and ensures the confidentiality of voting whereby no one can know which candidate the voter selected. The main limitation of this study is that the developed e-voting application is a PoC and not linked to the official system of the elections' council. In other words, the proposed application is built as a private local blockchain, and it has been tested locally without real-time network deployment. The Quorum blockchain can be integrated with an Ethereum platform in the future work for allowing people to easily cast their votes via their smart devices. The blockchain will evolve with fog computing, smartphones, and other smart devices. Its limitations will also be reduced with artificial intelligence, IoT, teleportation, and 6G technology in the future.

Funding Statement: This work is funded by the Deanship of Scientific research (DSR), King Abdulaziz University, Jeddah, under grant No. (DF-618-165-1441). The authors, therefore, gratefully acknowledge DSR technical and financial support.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] N. Weaver, "Secure the vote today," 2016. [Online]. Available: https:// www.lawfareblog.com/secure-vote-today.

[2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/ bitcoin.pdf.

[3] A. Grech and A. F. Camilleri, *Blockchain in Education*. Luxembourg: Publications Office of the European Union, 2017.

[4] A. Ekblaw, A. Azaria, J. D. Halamka and A. Lippman, "A case study for blockchain in healthcare: MedRec prototype for electronic health records and medical research data," in *Proc. OBD*, Vienna, Austria, pp. 13, 2016.

[5] M. A. Walker, A. Dubey, A. Laszka and D. C. Schmidt, "Platibart: A platform for transactive IoT blockchain applications with repeatable testing," in *Proc. M4IoT*, USA, pp. 17–22, 2017.

[6] N. Hackius and M. Petersen, "Blockchain in logistics and supply chain: Trick or treat?," in *Proc. HICL*, Berlin, Germany, pp. 3–18, 2017.

[7] R. Osgood, *The future of democracy: Blockchain voting*. COMP116: Information Security, 1–21, 2016.

[8] G. Wood, "Ethereum: A secure decentralized generalized transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, no. 2014, pp. 1–32, 2014.

[9] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends, in Proc. BigData Congress, USA, pp. 557–564, 2017.

[10] Q. F. Hassan, "Blockchain-based security solutions for iot systems," in *IEEE Internet of Things A to Z: Technologies and Applications*, pp. 255–274, 2018.

[11] S. Wang, Y. Yuan, X. Wang, J. Li and R. Qin, "An overview of smart contract: Architecture, applications, and future trends," in *2018 IEEE Intelligent Vehicles Symposium (IV)*, Changshu, pp. 108–113, 2018.

[12] D. Yaga, P. Mell, N. Roby and K. Scarfone, Blockchain technology overview, Gaithersburg, MA: NIST, U.S. Department of Commerce, 2019.

[13] S. Kawther, A. Wali, D. Alahmadi, A. Babour and F. Al Qahtani, "Building a blockchain application: A showcase for healthcare providers and insurance companies," in *Proc. FTC*, San Francisco, CA, pp. 785–801, 2019.

[14] Z. Zheng, S. Xie, H. N. Dai, X. Chen and H. Wang, "Blockchain challenges and opportunities: A survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[15] A. Alketbi, Q. Nasir and M. A. Talib, "Blockchain for government services—Use cases, security benefits, and challenges," in *Proc. L&T*, KSA, pp. 112–119, 2018.

[16] S. Wu and D. Galindo, "Valuation and improvement of two blockchain-based e-voting system: Agora and proof of vote (Master theses)," Birmingham University, Birmingham, UK, 2018.

[17] T.-T. Kuo, H. Z. Rojas and L. Ohno-Machado, "Comparison of blockchain platforms: A systematic review and healthcare examples," *Journal of the American Medical Informatics Association*, vol. 26, no. 5, pp. 462–478, 2019.

[18] D. Vujičić, D. Jagodić and S. Ranđić, "Blockchain technology, bitcoin, and ethereum: A brief overview," in *17th Int. Sym. Infoteh-iahorina (INFOTEH)*, East Sarajevo, pp. 1–6, 2018.

[19] Etherscan, "The Ethereum Blockchain Explorer," 2020. [Online]. Available: https://etherscan.io/.

[20] J. Filiba, "Ethereum breaks one million transactions in a single day," *Coinsquare News*, 2017. [Online]. Available: https://news.coinsquare.com/digital-currency/ethereum-one-million-transaction-day/.

[21] A. B. Ayed, "A conceptual secure blockchain-based electronic voting system," *International Journal of Network Security & Its Applications*, vol. 9, no. 3, pp. 01–09, 2017.

[22] S. M. Anggriane, S. M. Nasution and F. Azmi, "Advanced e-voting system using paillier homomorphic encryption algorithm," in *Proc. ICIC*, Indonesia, pp. 338–342, 2016.

[23] California Secretary of State, "Top-to-bottom review," 2007. [Online]. Available: http://www.sos.ca.gov/elections/voting-systems/oversight/top-bottom-review/.

[24] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. Eurocrypt*, Prague, pp. 223–238, 1999.

[25] Ministry of Local Government and Modernisation, "Internet voting pilot to be discontinued," *Government. no. 2014*. [Online]. Available: https://www.regjeringen.no/en/aktuelt/Internet-voting-pilot-tobediscontinued/id764300/.

[26] Y. Takabatake, D. Kotani and Y. Okabe, "An anonymous distributed electronic voting system using zerocoin," *IEICE Techinical Report*, vol. 54, no. 11, pp. 127–131, 2016.

[27] W. J. Lai, Y. C. Hsieh, C. W. Hsueh and J. L. Wu, "Date: A decentralized, anonymous, and transparent e-voting system," in *Proc. HotICN*, China, pp. 24–29, 2018.

[28] N. bin Abdullah and S. Muftic, "Security protocols with privacy and anonymity of users," *Universal Journal of Communications and Networks*, vol. 3, no. 4, pp. 89–98, 2015.

[29] S. E-Government, "Saudi—National Portal—Elections in the Kingdom of Saudi Arabia." 2029. [Online]. Available: https://www. saudi.gov.sa/wps/portal/snp/pages/electionsInTheKingdomOfSaudiArabia.

[30] S. Pareek, A. Upadhyay, S. Doulani, S. Tyagi and A. Varma, "E-voting using ethereum blockchain," *International Journal for Research Trends and Innovation*, vol. 3, no. 11, pp. 30–34, 2018.

[31] G. McCubbin, "The ultimate ethereum dapp tutorial, how to build a full stack decentralized application step-by-step," 2018. [Online]. Available: http://www.dappuniversity.com/articles/the-ultimate-ethereum-dapp-tutorial.

[32] W. Lai and J. Wu, "An efficient and effective Decentralized Anonymous Voting System," *ArXiv*, vol. abs/1804.06674, 2018.

[33] Y. Liu and Q. Wang, "An e-voting protocol based on blockchain," *IACR Cryptology ePrint Archive*, vol. 2017, pp. 1043, 2017.

[34] R. Hanifatunnisa and B. Rahardjo, "Blockchain-based e-voting recording system design," in *Proc. TSSA*, Indonesia, pp. 1–6, 2017.

[35] F. S. Hardwick, A. Gioulis, R. N. Akram and K. Markantonakis, "E-voting with blockchain: An e-voting protocol with decentralization and voter privacy," in *Proc. iThings and GreenCom and CPSCom and SmartData*, Canada, pp. 1561–1567, 2018.

[36] F. R. Batubara, J. Ubacht and M. Janssen, "Challenges of blockchain technology adoption for e-government: A systematic literature review," in *Proc. DG.O*, Netherlands, pp. 76, 2018.

[37] H. V. Patil, K. G. Rathi and M. V. Tribhuwan, "A study on decentralized e-voting system using blockchain technology," *International Research Journal of Engineering and Technology (IRJET)*, vol. 5, no. 11, pp. 48–53, 2018.

[38] C. Sullivan and E. Burger, "E-residency and blockchain," *Computer Law & Security Review*, vol. 33, no. 4, pp. 470–481, 2017.

[39] S. Ølnes and A. Jansen, "Blockchain technology as s support infrastructure in e-government," in *Proc. ICEG*, Russia, pp. 215–227, 2017.

[40] M. Sharples and J. Domingue, "The blockchain and kudos: A distributed system for the educational record, reputation and reward," in *Proc. EC-TEL*, France, pp. 490–496, 2016.

[41] S. Ølnes, "Beyond bitcoin enabling smart government using blockchain technology," in *Proc. ICEG*, Portugal, pp. 253–264, 2016.

[42] N. Kshetri and J. Voas, "Blockchain-enabled e-voting," *IEEE Software*, vol. 35, no. 4, pp. 95–99, 2018.

[43] A. A. Mutlag, M. Khanapi Abd Ghani, M. A. Mohammed, M. S. Maashi, O. Mohd *et al.,* "MAFC: Multi-agent fog computing model for healthcare critical tasks management," *Sensors*, vol. 20, no. 7, pp. 1853, 2020.

[44] R. Krishnamurthy, G. Rathee, N. Jaglan, "An enhanced security mechanism through blockchain for E-polling/counting process using IoT devices," *Wireless Networks*, vol. 26, no. 4, pp. 2391–2402, 2020.

[45] S. A. Mostafa, S. S. Gunasekaran, A. Mustapha, M. A. Mohammed and W. M. Abduallah, "Modelling an adjustable autonomous multi-agent internet of things system for elderly smart home," in *Proc. AHFE*, Washington, pp. 301–311, 2019.

[46] O. A. Mahdi, Y. R. B. Al-Mayouf, A. B. Ghazi, A. W. A. Wahab and M. Y. I. B. Idris, "An energy-aware and load-balancing routing scheme for wireless sensor networks," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 12, no. 3, pp. 1312–1319, 2018.

[47] K. H. Abdulkareem, M. A. Mohammed, S. S. Gunasekaran, M. N. Al-Mhiqani, A. A. Mutlag *et al.,* "A review of fog computing and machine learning: Concepts, applications, challenges, and open issues," *IEEE Access*, vol. 7, pp. 153123–153140, 2019.

[48] A. A. Mutlag, M. K. Abd Ghani, N. Arunkumar, M. A. Mohammed and O. Mohd, "Enabling technologies for fog computing in healthcare IoT systems," *Future Generation Computer Systems*, vol. 90, pp. 62–78, 2019.