Computer Science and Information Technologies
Vol. 4, No. 3, November 2023, pp. 191~198
ISSN: 2722-3221, DOI: 10.11591/csit.v4i3.p191-198

Designing a framework for blockchain-based e-voting system for Libya

Salem S. M. Khalifa[1], Ali Mohamed E. Ejmaa[2], Abdulmawla Mohammad Ali Najih[3], Mohamed Abd Arahman Masoud Zneen[1]
[1]Department of Computer, College of Science and Technology, Alriyayna, Libya
[2]Department of Computer, The Libyan Center for Biotechnology Research, Tripoli, Libya
[3]Department of Computer, The High Institute of Science and Technology, Gharian, Libya

Article Info

Article history:

Received Feb 24, 2023
Revised May 28, 2023
Accepted Jun 24, 2023

Keywords:

Blockchain
Cryptography
E-voting
Smart contracts
Voters

ABSTRACT

A transition to democratic rule is considered the first step down a long road towards Libya's recovery and prosperity. Thus, it strives to improve the country's elections by introducing new technologies. A blockchain is a distributed ledger that is characterised by independence and security. Therefore, it has been widely applied in various fields ranging from credit encryption and digital currency. With the development of internet technology, electronic voting (E-voting) systems have been greatly popularised. However, they suffer from various security threats, which create a sense of distrust among existing systems. Integrating blockchain with online elections is a promising trend, which could lead to make an election transparent, immutable, reliable, and more secure. In this paper, we present a literature review and a case analysis of blockchain technology. Moreover, a framework for an E-voting system based on blockchain is proposed. The methodology is adopted on the basis of three activities, they are identification of the relevant literature about E-voting, system modelling, and the determination of suitable technological tools. The framework is secure and reliable. Thus, it could help increase the number of voters and ensure a high level of participation, as well as facilitate free and fair electoral processes.

This is an open access article under the CC BY-SA license.

Corresponding Author:

Salem S. M. Khalifa
Department of Computer, College of Science and Technology
Al Ain Locality, Central Post 4545, Alriyayna, Libya
Email: salemassaid@gmail.com

1. INTRODUCTION

Various forms of elections were invented around the world such as traditional way (punch-card voting systems), optical scan (voting) systems, direct-recording electronic (DRE) voting machines, voter-verified paper audit trail, and internet voting. The traditional way of voting usually uses cards and records, where a voter makes a mark on a voting card or record of voting locations. This system works if there is strong and impartial supervision, while enabling candidate delegates to follow the manual counting in the presence of independent observers. This method has negative aspects, where costing of a process is exorbitant in terms of effort and time, as well as, in case of non-neutrality for supervising of electoral process, it can be rigged, adding fake cards, and preventing voters reaching to ballot boxes [1], [2]. Since the invention of the internet, various countries are experimenting with electronic voting (E-voting) in elections.

E-voting has many advantages that enhances its position in electoral methods, where it leads to more reliable results since human error is excluded, also it encourages more voters to cast their vote remotely and

increases the likelihood of higher voter turnout for a mobile electorate. However, it suffers from various security threats, such as malware attacks, distributed denial-of-service attacks and vote alteration and manipulation; this makes it very difficult for the government to gain voters' trust [1]–[3]. These problems can be solved by blockchain technology that can plays a key role in protecting the sensitive data of voting applications, where it is characterized by its ability to prevent cyber attacks [4]. As such, we will attempt to shed light on this topic in the following sections. The remainder sections are organised. Section 2 presents the technical underpinnings and characteristics of the blockchain technology. Next, section 3 discusses the importance of using blockchain in the E-voting system. Then, section 4 presents previous works related to E-voting systems based on blockchain. Section 5 provides the methodology that was adopted in this research. In section 6 and 7, we deploy our framework of E-voting system and define the structure and the interactions between different entities. Finally, the conclusion is presented in section 8.

2. STRUCTURE OF BLOCKCHAIN

The blockchain can be described as a single long chain that consists of growing lists of records (blocks) that are securely linked together via cryptographic hashes. The blockchain concept was proposed in 2008 by Nakamoto [5], which then had widespread acceptance after the entrance of the cryptocurrency bitcoin. Taking a deeper look at the structure of blockchain, it is essentially a fully distributed digital ledger of transactions in a peer-to-peer (P2P) network based on advanced cryptography protocol, which provides an opportunity for community members to record and share information. Each member can keep his/her own copy of the information and checks it collectively for any update. The ledger is secure and computationally impossible to change; it can only be extended by adding new blocks to the chain [6]. Blockchain has some exciting features, but the most notable and outstanding benefit is its ability to carry out transactions at high speeds without a centralised authority in a distributed environment and without the need for a centralised trusted third party [7], [8]. In other words, no person or entity is responsible for the entire chain. Rather, it is open, and everyone in the chain can see the details of each record or block and track information over a secure network.

Blockchain can be designed as, firstly, it must have a distributed ledger in the network to hold immutable information, thus ensuring the non-tamper ability of the data. Then participants are represented as nodes in the blockchain network, where each node contains private keys and a pair of public. The private key is used to authenticate the user, while the public key is used as the public address of the user. The blocks are linked together using cryptography into a chain, where each block contains a transaction data, a timestamp and a cryptographic hash of the previous block [9], as shown in Figure 1. Once adding a new transaction to the ledger, it must contain the public key of the user, the transaction message, as well as the public key of the receiver of the transaction. The system bundles blocks together using an elliptic curve digital signature algorithm (ECDSA), then sending it to the blockchain network for linking it with other nodes.

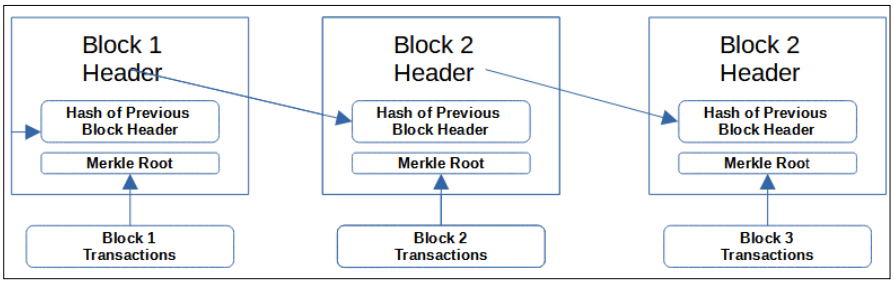

Figure 1. Simplified bitcoin block chain [1]

3. ELECTRONIC VOTING

E-voting is a new concept proposed for election that uses electronic means, such as computer or computerised voting equipment or the internet, to either aid or manage the casting and counting of ballots. It can be defined as using electronic means for voting and counting votes in an election [10]. Nowadays, the manual process uses ballot boxes and paper ballots. However, it requires huge amounts of paperwork, human resources and time. Furthermore, verification is too complicated in elections, as ballot forgery, coercion, and multiple voting may occur. Using an E-voting system instead of the traditional ways of voting can prevent any security breaches, such as data leaks and vote tampering. Moreover, it makes the process more secure, reliable, transparent, and immutable [11].

3.1. Challenges of electronic voting

The process of applying E-voting technology requires good planning and defining the challenges for the E-voting process and offering practical solutions for countering them. Significant challenges for E-voting systems are related to a variety of factors, such as election verifiability, proper management, security required for online voting, transparency, and legal requirements. These challenges can be summarized in the following sub section.

3.1.1. Security

Security is an important and necessary element of any electoral process to protect voter privacy and the integrity of final results, where this requirement is a unique challenge to online voting [12]. Thus, the voting system must be able to verify identity to ensure that a voter is eligible to vote in a given election. Furthermore, it must guarantee anonymity by separating identity from online activity. To overcome such challenges, encryption, and digital signatures with blockchain technology can be used [13].

3.1.2. Election verifiability

Verification is complicated in elections. Therefore, to obtain election integrity and provide transparency and verifiability, the voting system must be able to protect voter privacy. For instance, it must ensure that no manipulation occurs during the voting or tallying processes by using zero-knowledge proofs (ZKPs). These mathematical calculations allow voters to check that their votes were not manipulated during the counting process.

3.1.3. Legal frameworks

The term "legal framework" for elections usually refers to a set of legislation and rules relating to elections in a particular country. Usually, elections are carried in most countries of the world according to a set of laws and statutes [14]. It should be noted that the structure of the legal framework for elections varies markedly from country to country. Therefore, E-voting may meet legal barriers. These barriers can take many forms such as directly ban the use of E-voting out right or the laws or may not mentioned of the possible use of internet voting technology.

3.2. Electronic voting requirements

A secure E-voting system can be utilized not only to improve voter participation and confidence in politics, but also to prevent election fraud. Modern technologies currently available can be employed to develop an E-voting system in Libya that meets the necessary requirements for E-voting, especially security, accuracy, and flexibility. In order to achieve the same or higher security than that of traditional paper-based voting, online voting has to meet a number of requirements that make it a possible, safe, and acceptable solution. These requirements can be organized as defined by Rura *et al.* [15]:

3.2.1. Voter privacy

Ensuring the preservation of voter privacy and the safety of his data from unauthorized access is one of the basics of a sound electoral process. Exposing voter's information such as name, address, phone number for hacking can lead to material and moral harm. On the physical level, personal information may be used to access a bank account or credit card account, while, the moral aspect can be used for threats of physical, mental or emotional harm. Based on that, it must use a blockchain technology to protect voters' information and ensures that no undue pressure exists once the voter is voting.

3.2.2. Eligibility

The right to vote is one of the foundations of a democratic system of government. In order for a person to be eligible to register to vote they must meet the eligibility criteria such as: the nationality of the country, he/she be fully competent not to be deprived from exercising his political rights and he/she has completed the age of political majority. To ensure fair elections, voting rights are granted only to those who are registered using unique identifiers, such as passport or fingerprinting technology.

3.2.3. Un-reusability

If the same vote has already been submitted, the system must not be permitted to vote more than once. E-voting is also expected to be more open to public scrutiny. Meanwhile, system should allow voters to verify their vote by using a trace mechanism that identifies voters who vote more than once.

3.3. Advantages of electronic voting

E-voting has the potential to change the democratic process by making it more accessible, efficient, and reliable over the traditional method of voting. The advantages of online voting systems include increased

efficiency, improved accuracy, and greater voter engagement compared to paper ballots. Here a list of strengths usually associated with E-voting.

- Reduces costs of electoral process.
- Saves time and speeds up the release of election results.
- Allows decentralisation and independence in analysis of results.
- Overcomes the problem of geographic and temporal dimension.
- Provides transparency.
- Prevents multiple voting.

4. RELATED WORKS

This section focuses on related research works identified during the detailed literature survey for improving the performance of election. A new framework based on the adjustable blockchain was proposed by Shahzad and Crowcroft [16] using effective hashing techniques. Three activities were followed to develop the framework: modelling of entire E-voting process, determination of the suitable technology platform and technology integration with the perceived E-voting model. The framework debated the effectiveness of the polling process, block creation, and result declaration by using the blockchain method. Yi [17] used blockchain technology to propose an E-voting system for improving E-voting security in the P2P network. The system is composed of three models: a synchronised model, a user credential model and a withdrawal model. The author used a public-key encryption and multipart computers to improve the security of E-voting and address the problem. However, computing expenses are more significant and may be prohibitive when the number of participants is too high.

Mukherjee *et al.* [18] proposed a framework based on a blockchain technology called the hyper-ledger fabric-based framework as a service (FaaS), which can used to implement E-voting. The framework consists of three layers: hyper-ledger fabric framework, micro-services layer, and RESTful APIs layer. The researchers addressed the issue of designing a solution for E-voting with the minimal possible execution and operational cost. Wu [19] proposed an E-voting protocol based on blockchain using the ring signature algorithm. The protocol was implemented using personal home page (PHP) and JavaScript programming languages. From the point of view of this work, even though the protocol included many features and works that are efficient for ring signature, it does not fulfil the needs of fairness and receipt freeness. Moreover, the efficiency of the ring signature algorithm is limited by the number of participants.

Abuidris *et al.* [20] proposed a hybrid consensus model based on the bitcoin blockchain to address the problems of energy consumption for the classical consensus method of blockchain as implemented in bitcoin. Gupta *et al.* [21] proposed an E-voting system based on blockchain and quantum key distribution, which addresses the weaknesses of blockchain technology and makes blockchain more resistant to technological breakthroughs. The system consists of two parts: the central tabulating facility (CTF) for vote counting and the central legitimisation agency (CLA) for voter validation. Research by Schultz [22], built an E-voting application using the PHP programming language and the MySQL (My", the name of co-founder Michael Widenius's daughter My, structured query language) database were used to develop the application. He applied Rivest-Shamir-Adleman (RSA) security methods, such as public and private keys for verification. Willysandro *et al.* [23] proposed a voting prototype using fingerprints, which can help in overcoming election fraud. Although this proposed system is built in the form of a prototype, it is considered as the first attempt to combine E-voting with blockchain and fingerprints.

5. METHOD

Finding the most efficient and appropriate approach is the most important part of any research. This methodology focused on features of systems models and that have been leveraged to developed the framework. Following a wide literature search on various aspects of technology-based blockchain technology and a review of the E-voting system. A three-phase methodology was applied in this research as:

5.1. Identify relevant literature about electronic voting

Several frameworks of E-voting were discussed based on the blockchain. We have highlighted for its weaknesses, strengths. As a result, tried to avoid it in our framework and makes it more resistant to technological breakthroughs.

5.2. System modelling

Systems modelling is used to conceptualize and construct systems in business and information and technology (IT) development. We have used it for conceptualising and constructing our framework through defining the structure, behaviour of a system, observing errors and flaws before it can be implemented. The framework consists of system components and the sub-systems developed, that will work together to implement the overall system.

5.3. Determination the suitable technological tools

In order to choose a new technology, it must meet some criteria such as: user-friendliness, security, flexibility, interoperability, setup costs, license costs, and maintenance costs. Blockchain technology has unique features, for example security, credibility, data sharing, and independence. It can make information and communications more secure based on cryptographic protocols, thus protecting voter privacy and the integrity of final results [24]. Using blockchain technology can keep the information unchanged and distribute it over time. Thus, any participant can verify the authenticity of data and be certain that it has not been tampered with Reyna *et al.* [25]. Decentralised blockchain network can directly exchange data based on the trust system and reduce points of weakness in systems by eliminating the central points of failures and bottlenecks.

6. PROPOSED FRAMEWORK FOR ELECTRONIC VOTING SYSTEM

The technical features of the blockchain can be used to solve many problems that face E-voting process. The architecture of the proposed framework is characterized by features a secure blockchain, ensuring that data is safe from all threats. In this section, an overview of our framework based on blockchain is presented, including defining the structure and the interactions between different entities, as shown in Figure 2.

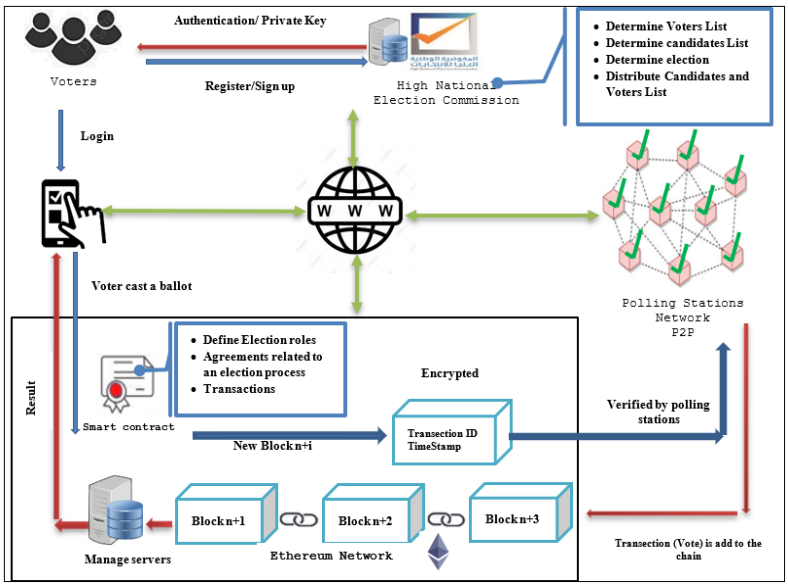

Figure 2. Proposed framework of E-voting system

6.1. Interacting entities

It is important to define each interacting entities before disscusing the details of the proposed framework. The framework consists of four entities which are: voter, ethereum network, election administrator and polling stations network P2P. In this section the interacting entities will be explained as the following:

6.1.1. Voter

A voter is someone who is eligible to vote in an election. Each voter has a digital wallet that allows him/her to store his/her own credentials. A smartphone or computer are the basic equipment used by each voter for the election process.

6.1.2. Ethereum network

Ethereum is a decentralised, open-source blockchain with smart contract functionality. It is composed of multiple blockchains that have a cryptographic hash and timestamp, which work side by side on a cryptographic protocol.

- Smart contract: a smart contract is self-executed snippet of code when pre-defined conditions are met on the network. It provides contracts between parties that will share in the agreement without the need for a middleman. Contracts are self-executed, which will become a legally binding agreement between parties.
- Manage servers (MS): these servers are used to store the node information that includes user credentials to log into the system and the node authentication.

6.1.3. Election administrator (high national election commission)

The job of election administrator is a complex and critical one. Election administrator is the primary point of contact for an election district and the chief administrative officer of the commission. The duties of the administrator include, but are not limited of creating the election, structure the voting process and then tabulate and audit the results. Furthermore, the administrator determines the list of voters and candidates and distributes it over the network.

6.1.4. Polling stations network P2P

P2P computing or networking is a distributed application architecture that partitions tasks or workloads between peers which is characterized by less vulnerable to hacking and manipulation while also being significantly more efficient. A polling place is where voters cast their ballots in elections. In our framework, each polling stations is represented as a node, where each polling station has a software agent that manages the life cycle of the smart contract on that node.

7. BLOCKCHAIN VOTING SYSTEM PROCESS

Our framework is an election platform that runs entirely on blockchain technology. Several stages are followed by different countries for different kinds of elections that is the fundamental to all democratic elections. The framework uses a five-phase voter authentication process, including the pre-election phase, voter registration phase, voter authentication phase, polling process phase, counting, and verification phase.

7.1. Pre-election phase

Election setup starts with selecting the locations of polling places which will be used as nodes in the blockchain system. The second step is to prepare voting devices, open ballot systems and paper ballots and to provide computing power and storage capabilities, as well as vote counting systems, verification, and auditing used. The following step is to create a database of candidates to allow electronic registration for each candidate to ensure that the candidacy conditions are met in accordance with the law, as well as voters who have the right to cast their votes in the elections that will be held.

7.2. Voter registration phase

A voter who would like to participate in an election has to visit the registration page. After successful registration with the system, the voter receives a voter identification document (ID). The organiser will save his/her information, including his ID and primary key (PK) into the database. The organiser generates the list of the voters, which should contain voters' names, national identification numbers, and fingerprint. This list will be distributed among the polling stations network. Then the organizer distributes the list of eligible voters and the list of nominees, which include the start date–time, and end date–time, on the polling stations network as an input on the genesis block.

7.3. Voter authentication phase

The first step in the blockchain-based voting system is a mechanism for electronic verification of voter identity by ensuring that the identity of a person is not falsified because every vote is of equal importance. To ensure the authenticity of information, the voter needs to connect to link of online voting using his/her mobile phone or other smart devices. He/she then logs into the system via fingerprint, and the information will be converted to binary data. Afterwards, the database will be checked by the smart contract whether the voter is registered and is eligible to vote.

7.4. The polling process phase

This stage starts at each of the electoral centers once the voting systems are launched by the election officials. Once a smart contract ensures that the voter's name is on the voting list and is eligible for voting,

he/she can select a candidate through the voting screen, which carries the details of contestants. Once the voter has selected one from the list of nominees, the vote becomes a transaction (new block), which consists of the hash (fingerprint) value binary, transection ID, and timestamp. Then, the block is distributed over the polling stations network P2P.

7.5. Counting and verification

In this stage, all voter choices are encrypted and sent over the network through a secured and encrypted communication channel to the election server. Then, they are verified and processed by the blockchain algorithm, where approved blocks are added (after successful mining) to the blockchain and then recorded in the database. The counter of the total votes are incremented for the current election. Once the voter has casted his/her vote, he/she can then verify that his/her vote has been casted and counted. He/she is then given the option to print the receipt as a proof of casting the vote.

8. CONCLUSION

An equitable, transparent, and fair electoral process is the foundation for supporting confidence in the process and strengthening a healthy democracy. Therefore, the use of technological development by majority of countries and institutions is considered an advantage for improving democratic institutions and processes. Counting votes and announcing results using traditional way may take several days. Moreover, these results are prone to human error. To avoid these problems, the high commission for elections can declare the election results immediately using blockchain. Blockchain is characterized by transparent, immutable, and cannot be hacked into. Thus, it can be considered an effective means to implement an E-voting system and to conduct fair election. This study proposed a framework using of blockchain-based E-voting for digitising voting. The framework satisfies all the requirements of E-voting and provides a solution for problems that electoral processes face.

REFERENCES

[1] A. Susanto, "Implementation of smart contracts ethereum blockchain in web-based electronic voting (E-voting)," *Jurnal Transformatika*, vol. 18, no. 1, Jul. 2020, doi: 10.26623/transformatika.v18i1.1779.

[2] C. D. Faveri, A. Moreira, J. Araujo, and V. Amaral, "Towards security modeling of E-voting systems," in *2016 IEEE 24th International Requirements Engineering Conference Workshops (REW)*, Beijing, China: IEEE, Sep. 2016, pp. 145–154, doi: 10.1109/REW.2016.037.

[3] F. Lehoucq, "Electoral fraud: causes, types, and consequences," *Annual Review of Political Science*, vol. 6, no. 1, pp. 233–256, Jun. 2003, doi: 10.1146/annurev.polisci.6.121901.085655.

[4] M. Pawlak, J. Guziur, and A. Poniszewska-Marańda, "Voting process with blockchain technology: auditable blockchain voting system," in *Advances in Intelligent Networking and Collaborative Systems*, F. Xhafa, L. Barolli, and M. Greguš, Eds., in Lecture Notes on Data Engineering and Communications Technologies, vol. 23. Cham: Springer International Publishing, 2019, pp. 233–244, doi: 10.1007/978-3-319-98557-2_21.

[5] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," *presented at the Bitcoin Glossary: 2018 Annual National Seminar*, United States, 2018, pp. 1–9.

[6] M. Turkanovic, M. Holbl, K. Kosic, M. Hericko, and A. Kamisalic, "EduCTX: a blockchain-based higher education credit platform," *IEEE Access*, vol. 6, pp. 5112–5127, 2018, doi: 10.1109/ACCESS.2018.2789929.

[7] C. Agbo, Q. Mahmoud, and J. Eklund, "Blockchain technology in healthcare: a systematic review," *Healthcare*, vol. 7, no. 2, Apr. 2019, doi: 10.3390/healthcare7020056.

[8] M. Sharples and J. Domingue, "The blockchain and kudos: a distributed system for educational record, reputation and reward," in *Adaptive and Adaptable Learning*, K. Verbert, M. Sharples, and T. Klobučar, Eds., in Lecture Notes in Computer Science, vol. 9891. Cham: Springer International Publishing, 2016, pp. 490–496, doi: 10.1007/978-3-319-45153-4_48.

[9] D. Bradbury, "In blocks we trust [Bitcoin security]," *Engineering & Technology*, vol. 10, no. 2, pp. 68–71, Mar. 2015, doi: 10.1049/et.2015.0208.

[10] T. Haryadi, A. Nurmandi, I. Muallidin, D. Kurniawan, and Salahudin, "Implementing 'SIREKAP' application based on election for improving the integrity of election administrators and increasing public trust," in *Human Interaction, Emerging Technologies and Future Systems V*, T. Ahram and R. Taiar, Eds., in Lecture Notes in Networks and Systems, vol. 319. Cham: Springer International Publishing, 2022, pp. 159–165, doi: 10.1007/978-3-030-85540-6_21.

[11] N. Weaver, "Secure the vote today," Washington, DC: The Lawfare Institute, Aug. 2016.

[12] J. Willemson, "Bits or paper: which should get to carry your vote?," *Journal of Information Security and Applications*, vol. 38, pp. 124–131, Feb. 2018, doi: 10.1016/j.jisa.2017.11.007.

[13] B.-A. Schuelke-Leech, "A model for understanding the orders of magnitude of disruptive technologies," *Technological Forecasting and Social Change*, vol. 129, pp. 261–274, Apr. 2018, doi: 10.1016/j.techfore.2017.09.033.

[14] J. P. Gibson and J.-L. Raffy, "Modelling an E-voting domain for the formal development of a software product line: when the implicit should be made explicit," in *Implicit and Explicit Semantics Integration in Proof-Based Developments of Discrete Systems*, Y. Ait-Ameur, S. Nakajima, and D. Méry, Eds., Singapore: Springer Singapore, 2021, pp. 3–18, doi: 10.1007/978-981-15-5054-6_1.

[15] L. Rura, B. Issac, and M. K. Haldar, "Implementation and evaluation of steganography based online voting system:," *International Journal of Electronic Government Research*, vol. 12, no. 3, pp. 71–93, Jul. 2016, doi: 10.4018/IJEGR.2016070105.

[16] B. Shahzad and J. Crowcroft, "Trustworthy electronic voting using adjusted blockchain technology," *IEEE Access*, vol. 7, pp. 24477–24488, 2019, doi: 10.1109/ACCESS.2019.2895670.

[17] H. Yi, "Securing E-voting based on blockchain in P2P network," *EURASIP Journal on Wireless Communications and Networking volume*, vol. 2019, no. 1, pp. 1–9, Dec. 2019, doi: 10.1186/s13638-019-1473-6.
[18] P. P. Mukherjee, A. A. Boshra, M. M. Ashraf, and M. Biswas, "A hyper-ledger fabric framework as a service for improved quality E-voting system," in *2020 IEEE Region 10 Symposium (TENSYMP)*, Dhaka, Bangladesh: IEEE, 2020, pp. 394–397, doi: 10.1109/TENSYMP50017.2020.9230820.
[19] Y. Wu, "An E-voting system based on blockchain and ring signature," Msc Computer Science, University of Birmingham, Inggris, 2017.
[20] Y. Abuidris, R. Kumar, T. Yang, and J. Onginjo, "Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding," *ETRI Journal*, vol. 43, no. 2, pp. 357–370, Apr. 2021, doi: 10.4218/etrij.2019-0362.
[21] S. Gupta, A. Gupta, I. Y. Pandya, A. Bhatt, and K. Mehta, "End to end secure E-voting using blockchain & quantum key distribution," *Materials Today: Proceedings*, vol. 80, pp. 3363–3370, 2023, doi: 10.1016/j.matpr.2021.07.254.
[22] C. Schultz, "Electronic voting implementation through bitcoin blockchain technology," *Scholarly Horizons: University of Minnesota, Morris Undergraduate Journal*, vol. 8, no. 2, Aug. 2021, doi: 10.61366/2576-2176.1095.
[23] H. Willysandro, J. Setiawan, and A. Sulaiman, "Designing a blockchain-based pemilu E-voting information system," *International Journal of New Media Technology*, vol. 8, no. 1, pp. 42–49, Jun. 2021, doi: 10.31937/ijnmt.v8i1.1865.
[24] G. Prisco, "Slock.it to introduce smart locks linked to smart ethereum contracts, decentralize the sharing economy," *Bitcoin Magazine-Bitcoin News, Articles and Expert Insights*, Nov. 05, 2015, [Online], Accessed: 1 Feb 2023, https://bitcoinmagazine.com/technical/slock-it-to-introduce-smart-locks-linked-to-smart-ethereum-contracts-decentralize-the-sharing-economy-1446746719
[25] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Generation Computer Systems*, vol. 88, pp. 173–190, Nov. 2018, doi: 10.1016/j.future.2018.05.046.

BIOGRAPHIES OF AUTHORS

Salem S. M. Khalifa is a lecturer at the Department of Computer Science, College of Science and Technology, Alriyayna. He received the higher diploma degree in programming and systems analysis from the Higher Vocational Computer Technologies Institute, Tripoli, Libya in 1995, the B.S. degree in programming and systems analysis/from Ebn. Al. Haytham Higher Technological Education and Scientific Research Center, Tripoli, Libya in 2005, the M.S. degree in information technology from University Utara Malaysia in 2010, and the Ph.D. in science and technology from University Science Islam, Malaysia in 2017. His research interests include desktop applications, web applications (PHP and ASP.NET programming languages), and artificial intelligence. He can be contacted at email: Salemassaid@gmail.com.

Ali Mohamed E. Ejmaa is a research scholar at the Libyan Center for Biotechnology Research. He received the B.S. degree in Computer Science from the Faculty of Science, Tripoli University, Tripoli, Libya, in 2003, and the M.S. degree from the Faculty of Computer Science, Universiti Putra Malaysia, Serdang, Malaysia, in 2008. He received his Ph.D. degree from the Faculty of Computer Science, Universiti Putra Malaysia, Serdang, Malaysia, in 2017. His research interests are computer networks and simulation. He can be contacted at email: aliejmaa81@gmail.com.

Abdulmawla Mohammad Ali Najih was born in 1969 in Gharian, Libya. He received his bachelor of science degree in computer engineering (hardware) from Sebha University in 1993. He completed his master's and Ph.D. degrees in computer engineering at University Putra Malaysia (UPM), Malaysia in 2003 and 2019. His research interests include digital signal processing, biometric recognition, and digital watermarking. He can be contacted at email: nabdulmawla@gmail.com.

Mohamed Abd Arahman Masoud Zneen is a lecturer at the Department of Computer Science, College of Science and Technology, Alriyayna. He received the higher diploma degree in information technology from the Higher Institute of Comprehensive Professions, Al-Ryayna, Libya in 2008. He received his master degree of computing and information systems from the University of South Wales, United Kingdom in 2017. He can be contacted at email: moh_soh8689@yahoo.com.