Iraqi E-Voting System Based on Smart Contract Using Private Blockchain Technology

Maral Hassan Jumaa* and Ahmed Chalak Shakir
E-mail: stcha018@uokirkuk.edu.iq and ahmedchalak@uokirkuk.edu.iq
College of Computer Science and Information Technology, University of Kirkuk, Kirkuk, Iraq

Keywords: e-voting, private blockchain, ECC, QRcode, smart contract

Received: June 16, 2022

In democratic societies including Iraq, electronic voting (e-voting) is an available option as a viable voting system. This system is more economically advisable than face-to-face voting by eliminating the need to pay poll staff. It may also make voting more accessible to the population with impairments and those living overseas. This study will propose an e-voting system based on smart contracts by using a decentralized private Blockchain. The proposed e-voting system will provide transparency, accuracy, fairness, eligibility, anonymity, verifiability, and immutability. This research proposed the most secure way of voting with the help of Blockchain using a mobile application that can be used to implement a large-scale solution and is cost-effective. The Blockchain-based system has been designed in conjunction with the existing ECC cryptosystem to assure the dependability, anonymity, and security of votes and voters. The system that has been developed can be used to properly conduct elections, using a quick response code (QR Code), face recognition, and fingerprint for identification before casting a ballot to ensure eligibility. This results in using mobile smartphones in the voting process where voters can observe the transparency of their votes. Furthermore, eliminates the possibility of fraud and manipulation of the votes made due to the used blockchain for secure storage.

Povzetek: Prestavljen je sistem iraškega elektronskega glasovanja s pomočjo bločnih tehnologij.

1 Introduction

Voting is a way for a group to decide, say what they think, or show their will on a question. Voting usually comes after people talk, debate, and run for office. When people vote, the person who casts a ballot is called the candidate, and the person who votes for their favorite candidate is called the voter [1]. Online voting is also called e-voting. It is a way to count votes and cast them that uses computers. E-voting could save time and effort while also being very efficient and giving people much freedom [2].

The world enters its fourth era, and all disciplines, activities, and aspects should be verified by transformational digitalization [3]. However, traditional voting methods in Iraq are still in use, such as voting on paper. In this traditional voting system, election fraud is no longer refuted since it is mainly done directly at voting locations (polling stations). Furthermore, this method has become economically unviable and lacks security and privacy. Many traditional offline services are moving online and embracing Blockchain in many industries, especially e-voting, to gain economic and security [4].

Recent researches have presented several e-voting systems utilizing Blockchain technology, [5] suggested (d-BAME) e-voting model for large-scale elections by offering the participation of two conflicting parties to ensure election integrity and accountability. [6] have proposed an e-voting system that assures dependability by incorporating Hyperledger private Blockchain technology into e-voting used on a small scale. [7] suggested that a website application is applied to a Blockchain-based e-voting system.

1.1 Motivation

E-voting can achieve higher democratic levels because it allows for remote and virtual voting and more significant participation. Electronic voting has been accused of corruption and unfair practices, such as voter impersonation, fraud, or duplication. A lack of transparency and trust in the electoral process has led to a decline in public participation in the democratic process. Developing a safer and more practical e-voting system is a trending topic in business and information security [8].

This study describes strategies for utilizing Blockchain technology to develop new e-voting systems to increase the security and anonymity of e-voting. Getting rid of the disadvantages of the paper-based technique of voting in Iraq.

* Corresponding author

1.2 Contributions

A web system was designed to register the voters and candidates and then converts the voter information into the QRcode for giving it to voters as ID cards before the voting. A mobile application was designed for voters who can vote from anywhere, which is more suitable for the elderly and handicapped. The mobile application uses factor authentication to login into the system which is QRcode, password, and biometric authentication (Fingerprint face recognition) for entering the system to ensure eligibility. The voting data model was encrypted with elliptic curve cryptography (ECC) to elevate the security and privacy of the data. A blockchain used the SHA-256 hash algorithm started with three zeros (000) to enhance the security of the blockchain

2 Related works

In this section, the research and projects based on smart contracts using blockchain technology are explained.

McCorry et al. [9], Using the Ethereum blockchain created a distributed and self-tallying electronic voting method. ETH Smart Contract created the voting protocol, and two rounds of zero-knowledge proof were utilized to protect the confidentiality of voters' voting information during the voting process. A simulation involving 40 voters was undertaken. However, the voting system only allowed voters to choose between two options (yes/no), which did not account for the possibility of several candidates in a single operation. The smart contract stores the data of all eligible voters throughout the deployment phase, which is the second disadvantage of this solution. Large data storage on smart contracts is theoretically prohibitively costly, for example, holding the addresses of 1000 voters would surpass the current block gas limit (20 million gas). Abayomi-Zannu T. P. et al. [10], supported a secure mobile voting platform that employs Blockchain technology to manage votes cast. Voters were authenticated using multifactor authentication (VIN/PIN) and one-time password (OTP) during voting. However, the methods of encrypting and resisting coercion in voting should be improved to ensure privacy. Tso Raylin et al. [11], The decentralized e-voting system based on a blockchain and smart contract was introduced. Changing the third party with an Ethereum blockchain-based smart contract is a viable technique for fulfilling the aim of cheaper costs and greater data verifiability. Employs cryptographic approaches like oblivious transfer and homomorphic encryption to strengthen privacy protection and eligibility. However, coercion is not resisted in this system and is used on a small scale for voting. Praful M. Kukwase et al. [12], evaluated the popular Frameworks for supplying blockchain as a service (BaaS) and provided a special e-voting method that considered all the cons of the current frameworks. The system employed smart contracts in all voting operations, including election organization, and voter registration, and considered each vote as a smart contract that was then stored in the blockchain. Vehbi Neziri et al. [13], discussed current Blockchain systems and provides a novel technique for achieving privacy and anonymity by combining two separate Blockchains. The first is for managing keys and the second is for storing voting data. Using Blockchain technology to implement this strategy would dramatically improve the present voting process by ensuring anonymity and privacy. The proposed system will encrypt the nonce and the voter's hash to investigate the anonymity and privacy features of the system. Previous studies lack security research. The system may be vulnerable to quantum attack, 51% attack, and many other risks. The proposed system addresses all vulnerabilities seen in previous systems. It used the strongest encryption algorithms, scalability, multi-authentications (fingerprint and face recognition), and no need to leave the house because the mobile is used to vote. In addition, to the above, the proposed system uses its own private blockchain platform self-tally for voting.

3 Background

In this section, some of the preliminaries that are indicated in the proposed system are presented.

3.1 Problems with the voting system in Iraq

In Iraq, the paper-based technique has significant disadvantages, including the potential of lost or manipulated ballot boxes and the high cost of printing ballots and training employees. As indicated in Table 1.

The following problems were detected while utilizing an electronic device (scanning device) to read the poll, sort, and count votes: vulnerability to hacking, the possibility of changing vote results, and the slowing down of the election process [14]. E-voting is a popular option in many developing and developed countries since it

Table 1: Analysis of The Current Electoral in Iraq.

Problems	Advantages	Disadvantages
The vote results might be manipulated.	Using biometric information to register the voter for a vote.	The people utilized paper ballots to vote.
The elections have a small number of participants.	Using a verification mechanism to confirm voters' identities.	Voters must go to the polling stations to cast their ballots.
Paper ballots were utilized in the voting process.	The results are counted and transferred from polling locations to counting centers at IHEC headquarters on election day	It takes a long time to count the votes.
Most expensive	Used indelible ink as a safeguard against possible duplicate voting.	The release of election results is always delayed.

eliminates the need for subjective recounts and has excellent potential for eliminating fraud or manipulation of results [15].

3.2 Blockchain technology

Satoshi Nakamoto proposed Blockchain in 2008 and deployed it as the Bitcoin infrastructure in 2009 [16]. The data in this system may be stored worldwide within all peer-to-peer (P2P) nodes in the network while preserving data integrity [17].

The Blockchain can be considered as a chronological chain of blocks, where each block may be like a page in a ledger. Transactions for all participating parties are stored in blocks, which are then broadcasted on the network via encrypted communication [18]. Miners seek to collect as many transactions as possible, validate them using consensus procedures, and construct a new block [19]. Private Blockchains allow just a restricted number of nodes to participate, but public Blockchains allow every node connected to the P2P network to participate in the consensus protocol [20]. Because of the immutability settings, it is not easy to edit once data is deposited in a Blockchain. To provide security, blockchain employs asymmetric encryption. Each user has a private key and a public key that is generated from the private key. Because every user in the network uses this public key as identification, the user's identity is hidden. Every node must agree on the block's authenticity to add a block to the chain [21]. Blockchain technology eliminates the requirement for a centralized trusted third party (TTP) to manage transactions. On the other hand, traditional ledger systems necessitate a TTP, as seen in Figure 1.

3.3 Smart contract

The term “smart contract” was coined by Nick Szabo in the mid-1990s. "A smart contract is a computer protocol intended to facilitate, verify, or enforce the negotiation or performance of a contract" [22].

Smart contracts can be automatically enforced without requiring a central authority. They remove the need for third-party intermediaries by embedding the terms of code agreements [23]. This code is run on a blockchain network and cannot be altered without consent. The result is an end-to-end transparent and secure system with reduced costs and increased efficiency. Smart contracts provide security that traditional contractual negotiations cannot because they are automated, self-enforcing, and immutable [24].

3.4 ECC encryption

Elliptic curve cryptography (ECC) is a public key cryptography technique based on elliptic curves in a finite field that can provide a superior encryption mechanism with fewer keys compared to other cryptography techniques [25]. The elliptic curve cryptography offers various advantages in identification and verification algorithms with excellent performance [26], such as high security, quick speed, and minimal bandwidth requirements [27]. Applying Elliptic Curve to the following equation:

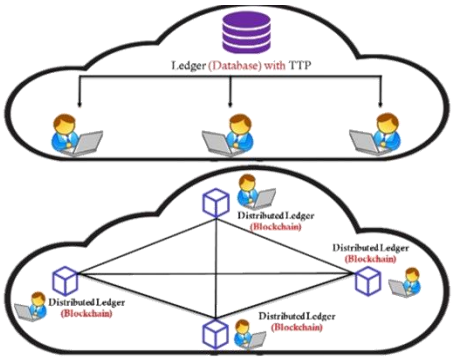


Figure 1: Centralized Conventional Ledger Vs Decentralized Ledger (Blockchain).

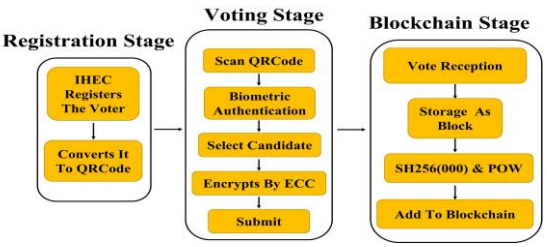


Figure 2: System Flowchart.

$$y^2 = x^3 + ax + b \ \ (a, b) \in R \qquad (1)$$

The digital signature can guarantee any content's integrity, authenticity, and nonrepudiation. ECC is used to implement digital signatures. Compared to other kinds of asymmetric cryptography algorithms, such as RSA, the main benefit of ECC is that it needs shorter key lengths while offering the same level of security (see Table 2). ECC-256 keys are 64,000 times more difficult to crack than 2048 RSA keys [28].

Table 2: NIST Recommended Key Size.

Security (strength)	Key-Size	
	ECC	RSA – DSA - DH
80 bit	160 bit	1024 bit
112 bit	224 bit	2048 bit
128 bit	256 bit	3072 bit
192 bit	384 bit	7680 bit
256 bit	521 bit	15360 bit

4 Method

The proposed system was designed based on Blockchain for a secure vote: first, a web application was used for biometrical (face recognition & fingerprint) registration and recorded as QRcode. Later, the recorded user information is used to authenticate the voter when he/she logs in to the mobile application system to vote. Second, a mobile application is used by voters to cast a vote that login by QRcode and authentication by (face recognition or fingerprint). Third, a synchronized model storing the votes based on Blockchain is designed to prevent vote falsification. Fourth, the system is an encrypted vote by ECC architecture intended to offer secure authentication. Lastly, the hash value was computed based on SHA-

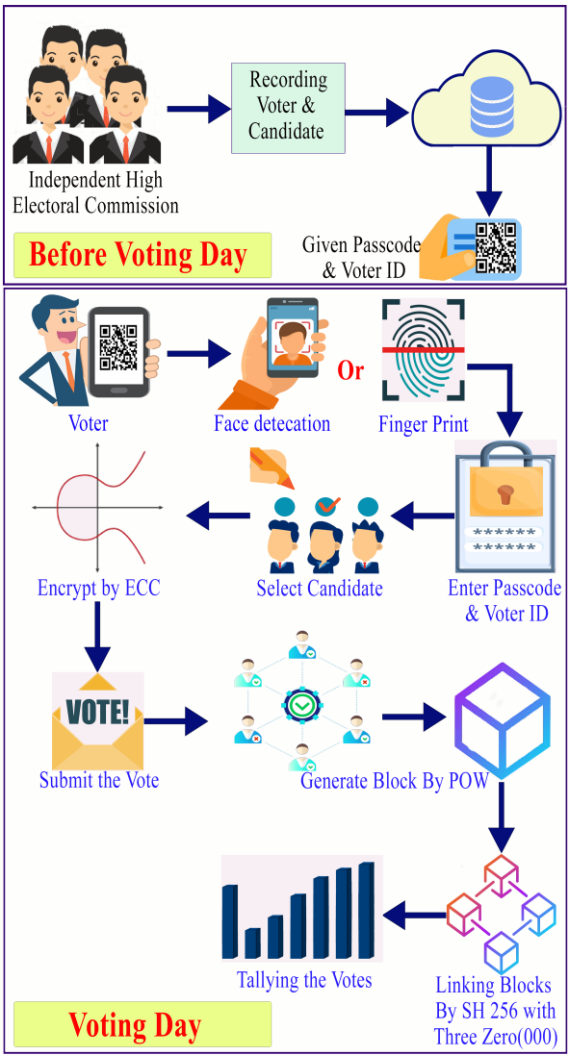


Figure 3: System Architecture.

256(000) and mining and generation of voting blocks by proof of work algorithm. designed at three stages illustrated in Figure 2.

5 Results

The system was designed to run on the Windows 10 platform, and it featured a processor with an Intel(R) Core (TM) i7-5600U CPU operating at 2.60GHz and 16.0 gigabytes of random-access memory (RAM). Use the dart programming language for flutter open source from google for mobile application (user interface). Django was used for databases and electronic registration before the polls. The outcome of the implementation reveals that it was a practical and safe system for electronic voting, which overcomes the problem of vote forgery during electronic voting. The current techniques of electronic voting cannot compare to the safety and anonymity provided by the Blockchain-based solution for electronic voting. Figure 3 provides a visual representation of the system that was designed.

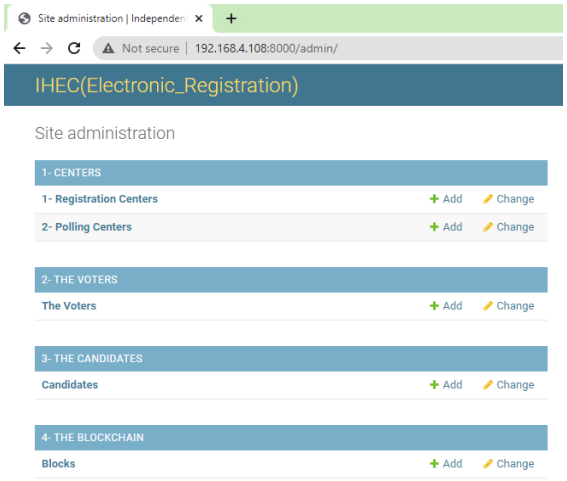


Figure 5: Input Information.

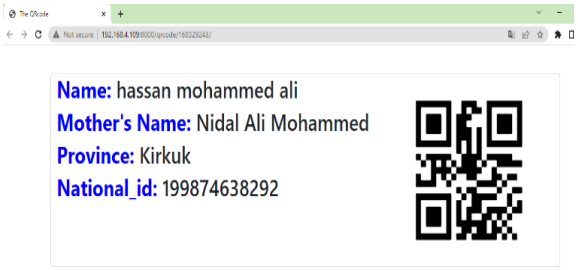


Figure 4: Voter's QRcode.

5.1 Registration

The registration of the electronic voting system is as follows by using a website application:

- IHEC registers voters and candidates at polling stations.
- Information is taken from the voter, including voter number, date of birth, mother's name, etc. A live picture and fingerprint are taken from the voter shown in Figure 4.
- Every voter is provided a secure credential, which comprises a unique identification ID and passcode as QRcode by the website application illustrated in Figure 5.

5.2 Voting

The voter employs a mobile application which is illustrated in Figure 6. The voting procedure is summarized by implementing the following:

- The system is entered by scanning the QRcode received upon electronic registration before the elections to verify the voter's eligibility.
- The voter is authenticated while entering the system by employing fingerprint or face recognition technology.
- The list of candidates is shown for him to choose his preferred candidate.
- The ECC algorithm will encrypt the vote to ensure voters' privacy and security. The system gives a code for voters to verify their vote after the voting day. The vote is transmitted to the Blockchain and saved as a

block that cannot be modified or tampered with. Figure 7 shows block contents.

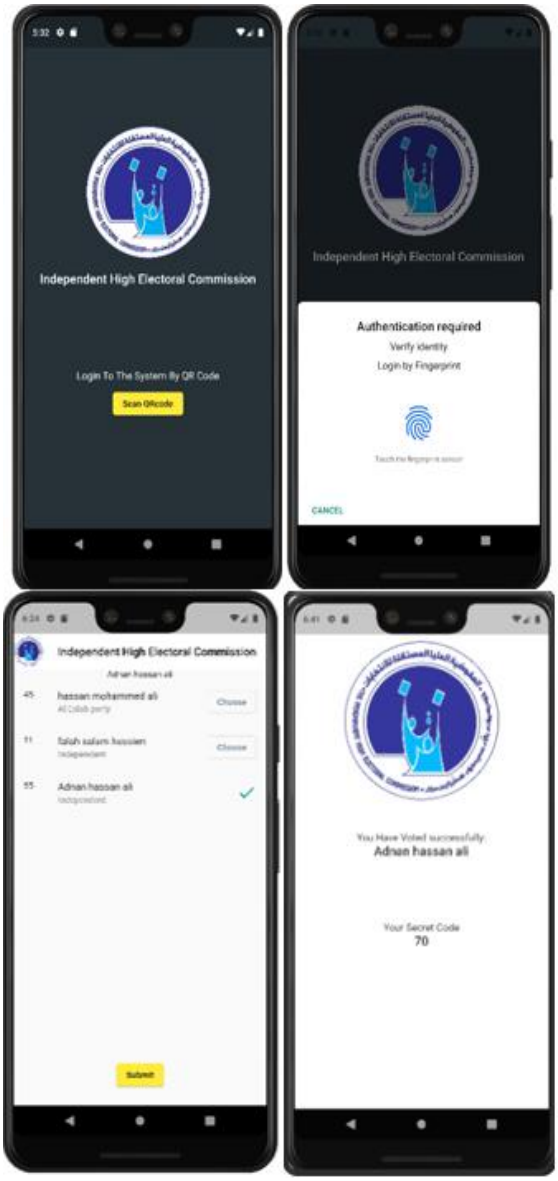


Figure 6: Voting Interface.

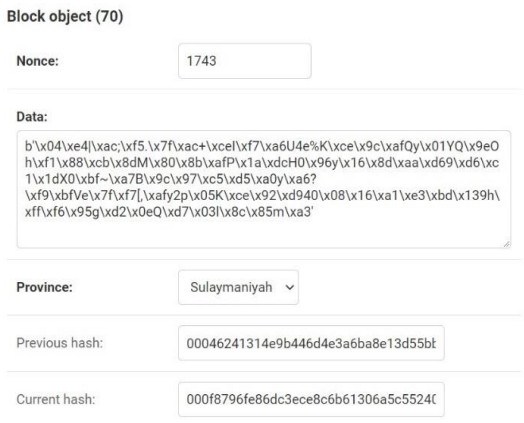


Figure 7: Block Contents.

5.3 Tallying

After voting, the system automatically self-tallies the votes and shows the number of votes for each candidate. Announcing the election results in this system does not require time, as in traditional manual elections, which can waste days announcing the results. In the case of the elections in Iraq since 2005 [15], they are delayed every year, due to the recounting and counting manually, as seen in the following Figure:

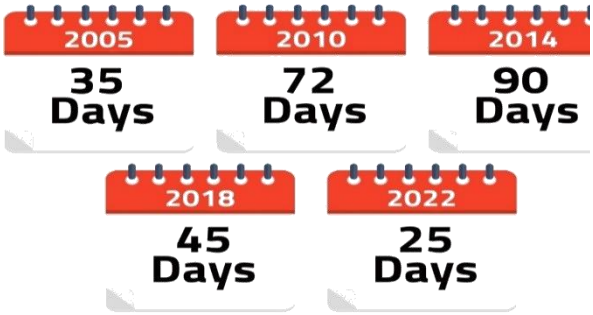


Figure 8: Delayed Announcement of Results.

In our system, the results will be computed according to $\sum_{i=1}^{n} x_i$ where i denote the vote and announced immediately after the end of the election time as illustrated in the following Figure:

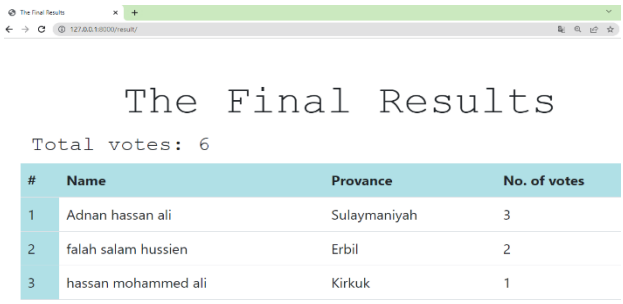


Figure 9: Candidate's Number of Votes.

6 Discussion

6.1 Security system requirement

The proposed system keeps all of the basic security measures that are required to deliver a trustworthy environment to the voter. Several required and crucial security elements were identified from a system standpoint that should be given top emphasis(see Table 3):

- **Eligibility**: Only legitimate voters should be allowed to vote. In the suggested system, the voters used fingerprint or face recognition, a recognized registration mechanism to identify themselves.
- **Anonymity and Authenticity**: Voters must first authenticate their identity to the Authentication Server (AS) before engaging with the voting system and scanning the QRcode containing the passcode and voter ID delivered by AS before voting.
- **Completeness:** Invalid ballots should be discovered and not counted while counting. In the current system,

the invalid vote will be discovered by verifying it with the proof of work consensus algorithm and SHA-256.

- **Privacy**: No one other than the voter has access to information regarding the voter's choice. The ECC algorithm will encrypt the voter's information in the given system.
- **Fairness**: This means that no one receiving intermediate outcomes is easy. This issue is handled by sharing the key among many nodes by employing ECC public key generation to produce a private key and a public key for each province, which are then distributed throughout the province's nodes.
- **Auditability**: No one may influence the votes of other voters and the final total results include all valid votes. In this study using Blockchain with no TTP can alter the vote.
- **Verifiability**: The system can test the election once the tally is declared by code has been received when voting.

6.2 Security analysis

The proposed system used the ECC algorithm to encrypt the votes because it is more secure at keeping data safe. The ECC is distinguished from other types of traditional cryptosystems because the best method currently known for solving the ECC for a well-chosen curve is a wholly exponential method. Conventional cryptosystems make use of sub-exponential algorithms, and this discrepancy adds significantly to the considerable differences in their relative running times. ECC keys also contain many fewer bits than other cryptosystems. Other than exponential algorithms. Figure 10 depicts the difference in key lengths between RSA, DSA, and ECC [29] .

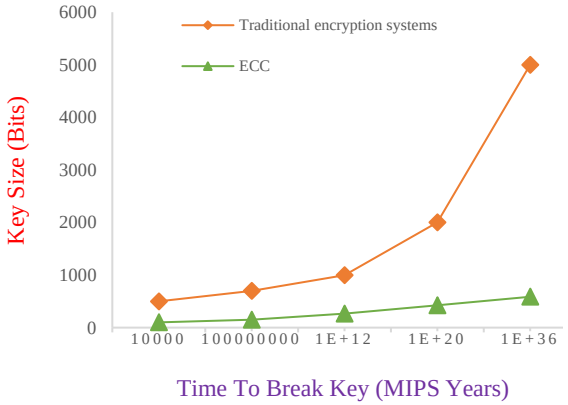


Figure 10: Difference in Key Lengths.

6.3 Time analysis

The proposed system was tested in three stages of hashing with one zero and two zeros. The voting and hash generation process was quite fast. However, when using three zeros (hash), every voting process takes place within a second to improve the system's security and penetration difficulty. It is high security with SHA-256(000). The

Table 3: The Comparison Between the Proposed System and Other Systems.

References	System name	Publication year	Blockchain Type	Framework	The Algorithm Used	Security requirement						
						Eligibility	Anonymity	Privacy	Completeness	Fairness	Auditability	Verifiability
[9]	A Smart Contract for Boardroom Voting with Maximum Voter Privacy	2017	Public	Ethereum	ZKP & Smart Contract	✓	✓	✓	✓	×	×	✓
[10]	Mobile Voting	2019	Private	Blockchain	OTP & (VIN/PIN) authentication	✓	✓	×	×	×	✓	✓
[11]	Distributed E-voting and E-bidding systems based on smart contract	2019	Public	Blockchain	secret sharing & Homomorphic	✓	✓	✓	×	✓	×	✓
[12]	Blockchain-Based E-Voting System	2022	Public	Ethereum	NIZKP	✓	✓	×	×	×	×	✓
[13]	Assuring anonymity and privacy in e-voting with distributed technologies based on Blockchain	2022	Public & Private	Ethereum & Hyperledger	Consensus algorithms and Smart Contract	✓	✓	✓	✓	×	×	✓
	The Proposed System	2022	Private	Blockchain	QR Code & ECC & SHA-256(000) & POW	✓	✓	✓	✓	✓	✓	✓

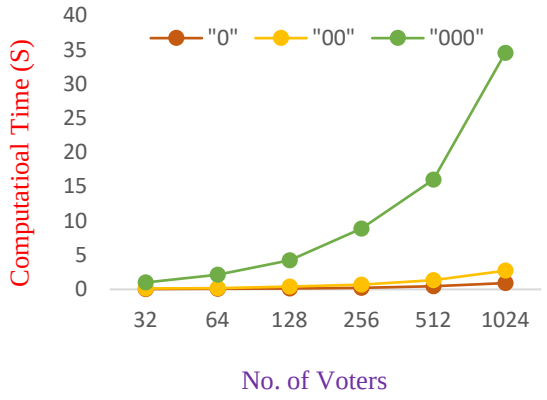
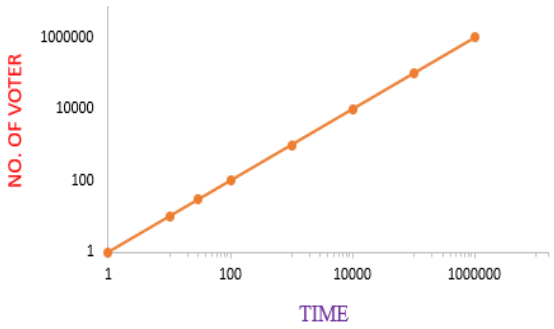


Figure 11: Time Analysis: A) No. of Zeros for Hash Value.



B) No. of Voters.

system needs a longer time to vote with an increase in voters, as shown in the following Figure:

7 Conclusion

E-voting is an effective voting method in Iraq that allows voters to vote more precisely and dependably. Furthermore, Blockchain is an intriguing and appealing technology that gives data security and has become a top topic in different fields.

The suggested protocol reduces the restrictions of current traditional paper-based voting in Iraq and other Blockchain-based e-voting systems. The prevention of vote forging in the current system is performed by casting the votes on the unchangeable Blockchain network, which aggregates them into blocks and is linked by SHA-256 with three zeros. The approaches utilized in the protocol are relatively straightforward. The suggested system makes it easier for the disabled and the elderly to participate in the elections and the number of participants in voting increases. This system is designed to increase security and decrease time consumption and cost to speed up processes. The future work will be executed by the OTP technique which provides each voter with a one-time password for voting.

References

[1] Schmidt, & L. A. Albert. (2022). Designing pandemic-resilient voting systems. Socio-Economic Planning Sciences, 80. https://doi.org/10.1016/j.seps.2021.101174

[2] Abayomi-Zannu T. P., I. A.Odun-Ayo, & T. F. Barka. (2019). A proposed mobile voting framework utilizing blockchain technology and multi-factor authentication. Journal of Physics: Conference Series, 1378(3), p.032104. https://doi.org/10.1007/s10773-018-3789-0

[3] Aini, Q., Bob, S. R., Santoso, N. P. L., Faturahman, A., & Rahardja, U. (2020). Digitalization of Smart Student Assessment Quality in Era 4.0. International Journal of Advanced Trends in Computer Science and Engineering, 9(1.2), 257–265. https://doi.org/10.30534/ijatcse/2020/3891.22020.

[4] Aitzhan, N. Z., & Svetinovic, D. (2018). Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams. IEEE Transactions on Dependable and Secure Computing, 15(5), 840–852. https://doi.org/10.3390/s21123958

[5] Dong, M. T., & Zhou, X. (2016). Fog Computing: Comprehensive Approach for Security Data Theft Attack Using Elliptic Curve Cryptography and Decoy Technology. OALib, 03(09), 1–14. https://doi.org/10.1109/jiot.2021.3074877

[6] Fan, W., Shubham Kumar, Vrushali Jadhav, Sang-Yoon Chang, & Younghee Park. (2020). A Privacy Preserving E-Voting System Based on Blockchain. Silicon Valley Cybersecurity Conference: First Conference, SVCC 2020, San Jose, CA, USA, December 17-19, 2020, Revised Selected Papers, 1383, 148-159. http://doi.org/10.3745/JIPS.03.0135

[7] Giraldo, F. D., Barbosa Milton C., & Carlos E. Gamboa. (2020). Electronic Voting Using Blockchain And Smart Contracts: Proof Of Concept. IEEE Latin America Transactions, 18(10), 1743-1751. https://doi.org/10.1007/978-3-030-72725-3_11

[8] Guan, P. (2021). Supply Chain Optimization of Agricultural Products in The Internet Environment with Blockchain. Informatica, 45(6). https://doi.org/10.1109/tr.2017.2686396

[9] Islam, A., & Shin, S. Y. (2019). BUAV: A blockchain based secure UAV-Assisted data acquisition scheme in Internet of Things. Journal of Communications and Networks, 21(5), 491–502. https://doi.org/10.1007/978-3-319 70972-7_20

[10] J, G., & Koppu, S. (2022). An empirical study to demonstrate that EdDSA can be used as a performance improvement alternative to ECDSA in Blockchain and IoT. Informatica, 46(2). https://doi.org/10.1088/17426596/1378/3/03214

[11] Kukwase, P. M., Kolte, G. P., Sawarkar, A. D., Rajput, C. K., & Dehankar, J. (2022). Blockchain Based E-Voting System. International Journal of

Research in Engineering and Science (IJRES) ISSN, 10(5), 74–76. www.ijres.orghttps://doi.org/10.3390/electronics8040422

[12] Liu, Q., & Zhang, H. (2017). Weighted voting system with unreliable links. IEEE Transactions on Reliability, 66(2), 339–350. [Online]. Available: https://www.ijres.org/v10-i5.html.

[13] Majeed, A. A., Ameen, K. A., Shakir, A. C., & Alyeksyeyenkov, Y. (2014). The Enhanced data sequence method for ECC cryptosystem. Applied Mathematical Sciences, 8(109–112), 5553–5564. https://doi.org/10.3390/app12115477

[14] McCorry, P., Shahandashti, S. F., & Hao, F. (2017). A smart contract for boardroom voting with maximum voter privacy. International Conference on Financial Cryptography and Data Security. Springer, Cham., 10322 LNCS, 357–375. https://doi.org/10.1109/hora52670.2021.9461387

[15] Mijoska, M., & Ristevski, B. (2021). Possibilities for applying blockchain technology – A survey. Informatica (Slovenia), 45(3), 319–333. https://doi.org/10.35950/cbej.v26i108.5216

[16] Mohsen Hassan, S., Hasan Khanjar, A., & Ali Abead, S. (2020). Subject Reviewer: A Proposal for An Electronic Voting System as Trust Mediation to Adopting In Iraq. Journal of the College of Basic Education, 26(108), 499–510 https://nakamotoinstitute.org/bitcoin/

[17] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Decentralized Business Review, 21260. https://doi.org/10.1007/s12083-020-00977-4

[18] Neziri, V., Shabani, I., Dervishi, R., & Rexha, B. (2022). Assuring Anonymity and Privacy in Electronic Voting with Distributed Technologies Based on Blockchain. Applied Sciences, 12(11), 5477. https://doi.org/10.31449/inf.v45i6.3729

[19] Rathore, D., & Ranga, V. (2021). Secure remote E-voting using blockchain. Proceedings - 5th International Conference on Intelligent Computing and Control Systems, ICICCS 2021, 282–287. https://doi.org/10.1007/978-981-15-4542-9_14

[20] Roh, C. H., & Lee, I.-Y. (2020). A study on electronic voting system using private blockchain. Journal of Information Processing Systems, 16(2), 421–434. https://doi.org/10.1109/jiot.2020.3004273

[21] Sadia, K., Masuduzzaman, Md., Paul, R. K., & Islam, A. (2020). Blockchain-Based Secure E-Voting with the Assistance of Smart Contract. IC-BCT 2019, 161–176. https://doi.org/10.1109/jcn.2019.000050

[22] Salman, W., Yakovlev, V., & Alani, S. (2021, June 11). Analysis of the traditional voting system and transition to the online voting system in the republic of Iraq. HORA 2021 - 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications, Proceedings. https://doi.org/10.1109/tse.2019.2942301

[23] Shankar, A., Pandiaraja, P., Sumathi, K., Stephan, T., & Sharma, P. (2020). Privacy preserving E-voting cloud system based on ID based encryption. Peer-to-Peer Networking and Applications, 1–11. https://doi.org/10.31449/inf.v45i3.3248

[24] Song, J. G., Moon, S. J., & Jang, J. W. (2021). A scalable implementation of anonymous voting over ethereum blockchain. Sensors, 21(12). https://doi.org/10.1109/tla.2020.9387645

[25] Tso, R., Liu, Z. Y., & Hsiao, J. H. (2019). Distributed E-voting and E-bidding systems based on smart contract. Electronics (Switzerland), 8(4), 422. https://doi.org/10.1109/iciccs51141.2021.9432249

[26] Zaghloul, E., Li, T., Mutka, M. W., & Ren, J. (2020). Bitcoin and Blockchain: Security and Privacy. IEEE Internet of Things Journal, 7(10), 10288–10313. https://doi.org/10.12988/ams.2014.47558

[27] Zaghloul, E., Li, T., & Ren, J. (2021). d-BAME: Distributed Blockchain-based Anonymous Mobile Electronic Voting. IEEE Internet of Things Journal, 8(22), p.16585-16597. https://doi.org/10.31449/inf.v46i2.3807.

[28] Zhang, J. L., Zhang, J. Z., & Xie, S. C. (2018). A Choreographed Distributed Electronic Voting Scheme. International Journal of Theoretical Physics, 57(9), 2676–2686. https://doi.org/10.1109/tdsc.2016.2616861

[29] Zou, W., Lo, D., Kochhar, P. S., Le, X. B. D., Xia, X., Feng, Y., Chen, Z., & Xu, B. (2021). Smart Contract Development: Challenges and Opportunities. IEEE Transactions on Software Engineering, 47(10), 2084–2106. https://doi.org/10.4236/oalib.1102802