Valid Blockchain-Based E-Voting Using Elliptic Curve and Homomorphic Encryption

https://doi.org/10.3991/ijim.v16i20.33173

Saba Abdul-Baqi Salman[1,2(✉)], Sufyan Al-Janabi[2], Ali Makki Sagheer[2,3]
[1] Aliraqia University, Baghdad, Iraq
[2] University of Anbar, Ramadi, Iraq
[3] Al-Qalam University College, Kirkuk, Iraq
sab19c1004@uoanbar.edu.iq

Abstract—Improving the voting system has become a widely discussed issue. Paper-based elections are not safe because of the possibility of changing and adding ballots. Consequently, many countries use e-voting systems to ensure security, authenticity and time efficiency. Blockchain e-voting systems can be adopted to reduce fraud and increase voting access from home, especially in pandemics. This paper suggests a blockchain e-voting system that tackles two security and authentication issues. The security has been ensured using hybrid public-key cryptography; the voter information is encrypted using the regional election office elliptic public key, while the homomorphic public supreme election authority encrypts the vote. Using homomorphic encryption for voice enables the calculations of results as the authority encrypts it without revealing the vote itself. Authentication has been improved for home voting by a robust login system. This login system consists of two steps. In the first step, the voter enters the site using his unique QR code number scanned by webcam; in the second step, the system checks the voter's face using a face recognition system by web camera to be routed to the voting page. Voting public keys are also authenticated using a digital certificate schema. The system has been tested to show its efficiency and suitability in block establishment time and the encryption and key generator randomness using NIST tests.

Keywords—security, blockchain, e-voting system, blockchain e-voting

1 Introduction

Voting is a process inherent to all democratic societies. Many experts consider paper balloting the only acceptable way to secure and guarantee each person's right to cast a vote. However, this approach is vulnerable to mistakes and exploitation because the traditional voting process is centralized and crowded with intermediaries. The voters submit their identification documents to a third party, i.e., the supervisors or representatives deployed by the administration. After authentication by the representatives, the voters are allowed to perform their votes. This process left many holes to rig the election, e.g., the representatives may authorize illegal voters, there's a chance of ballot stuffing, ballot boxes may get damaged, etc. The involvement of more intermediaries

dramatically increases the risk in the whole voting process [1]. Recently many countries like Estonia and USA have gone towards e-voting systems. The traditional e-voting machine has an encrypted access card to extract the voting information, which may get damaged or lost. Thus, the conventional e-voting system lacks security, transparency, and data retention and has a significant risk of data tampering [2].

The most substantial weaknesses of electronic voting systems include: (i) lack of transparency and understanding of e-voting solutions that result in a lack of trust, which is crucial for any voting system; (ii) lack of widely accepted standards, which results in a decrease of trusts due to lack of certifications and meaningful system assessment; (iii) risk of fraud and manipulation by privileged insiders or hackers; (iv) increased costs of voting infrastructure concerning power supply, communication technology, etc. [3].

Blockchain is a distributed, immutable, indisputable public ledger. So, blockchain technology is a reliable method to overcome the problems mentioned above. This new technology has three main features:

1. Immutability: Any proposed "new block" to the ledger must reference the previous version of the ledger. This feature creates an immutable chain, which the blockchain gets its name, and prevents tampering with the integrity of the last entries.
2. Verifiability: The ledger is decentralized, replicated and distributed over multiple locations. This feature ensures high availability (by eliminating a single point of failure) and provides third-party verifiability as all nodes maintain the consensus version of the ledger.
3. Distributed Consensus: A distributed consensus protocol to determine who can append the next new transaction to the ledger. Most network nodes must reach a consensus before any new proposed block of entries becomes a permanent part of the ledger.

Accordingly, many researchers suggest blockchain public leaders save the ballots in the e-voting system [4].

The e-voting system faces many issues, primarily related to its security. This paper tackles a number of these issues, including the anonymity of voters, the privacy of block information, and the time consumption for creating each block representing a single vote. The contributions of this research are: At first, proposing a hybrid public key algorithm that encrypts the personal data of voters using an elliptic curve. In contrast, the vote and voter ID number are encrypted by a homomorphic key that enables the election authority to collect the encrypted ballots later. Secondly, authenticity has been improved by using the entrance system of the QR code step and the face recognition step. The last contribution is the public key distribution and verification schema for checking the voting point's elliptic public key and the election authority's homomorphic public key.

The remaining of this paper is organized as follows: Section 2 represents a literature survey of the state-of-the-art related works. The third section explains the blockchain technology; the fourth part discusses the public key algorithms that have been used in this proposed system. At the same time, the fifth section talks about authentication used to authenticate both keys and the voter himself. The last two sections are the proposed system design and result in sections.

2 Related work

In the study of related works, a set of papers dated from 2017 to 2021 with more than five citations as related work has been chosen. All associated articles used blockchain in e-voting with a public key or homomorphic encryption algorithms.

Liu Y. et al. (2017) proposed a decentralized protocol for e-voting systems. A blind signature is used to save the voter's choice during the election process. The work implements security analysis. Liu did not measure time consumption or key randomness but only put a proposed design [5].

Hsiao J. et al. (2018) built a decentralized e-voting system with a secret sharing scheme and homomorphic encryption. This work tried to ensure privacy and anonymity. This work used RSA key for signature verification and homomorphic Paillier encryption to encrypt/decrypt RSA key pairs. This paper tests the security requirements by simulation only. Many aspects have been analyzed in this paper, like anonymity, ballot eligibility, and ballot verifiability [6].

Zhang S. et al. (2019) proposed an e-voting system with a hybrid data structure mixing the counting bloom filter and blockchain for authentication. Smart contracts are used for voter verifiability, while the blind signature is for ballot signing. Different attacks have been examined, like replay attacks, denial of service, man-in-the-middle, and Sybil attacks. Time consumption was evaluated for Paillier and Okamoto-Schnorr signature system. The time consumed by Paillier encryption was 0.001299 milliseconds, and for decryption, 0.000384 milliseconds for each ballot [7].

Shazad B. et al. (2019) have designed a secure framework for e-voting depending on a biometric authentication bank to ensure the eligibility of the voters. Hash-256 algorithm is used to sign each block with information saved in the next block. In this paper, the time or efficiency was not measured or tested online or offline [8].

In Zhang Y. et al. (2019) Ethereum smart contract e-voting system was proposed. This system uses a blind signature with homomorphic encryption. This process is done by signing the voter's key by the administrator to be added later in the smart contract of the voter. Time has been analyzed for 40 voters and took about 42 milliseconds using the pailler algorithm. This system was not tested for large scale elections [9].

Pyasetyadi G et al. (2020) used the Django python framework to build an e-voting system that uses SHA-256 for blockchain integrity and elliptic curve for authentication by signing using (ECDSA). Offline testing has been executed and simulated using 10.000 voters that consumed about 2.585ms (43 minutes and 5 seconds). Unfortunately, the system has not been tested in online operation [10].

Li H. et al. (2020) used a smart contract technique that the voter gains in the registration process and homomorphic time lock cryptography. The estimated time cost in offline and online tests was successful because the proposed system serves ten voters in five ms [11].

Zaghloul E et al. (2021) used an IoT system to implement an e-voting system with smart contract to ensure privacy. Security is guaranteed by using RSA by generating a key for a voter in the registration process. The ballot cannot be established to prevent double voting unless the voter provides his public key. The system was tested offline only using a desktop pc; the time complexity for each vote was O(3m) [12].

In Tas R. et al. (2021) double-layer encryption system in a blockchain, an e-voting system has been developed to prevent manipulation. The only drawback of that system was the fingerprint must be scanned during the registration in the election commission office. The system relies on a homomorphic encryption algorithm to encrypt the ballots. The system is scaled by measuring the time needed to share ballot after encryption among the nodes. The average ballot sharing among 600 nodes was 53 ms [13].

Unfortunately, not all the researchers tested their proposed designs in actual environments. Five of the related papers [7, 9, 11, 12, 13] were tested in time consumption, and three [5, 6, 10] were tested offline, not deployed online. These papers do not contain any contribution to the encryption itself; all of the documents focus on implementing e-voting criteria.

3 Blockchain technology

Blockchain is a decentralized database that holds and manages data records constantly growing and operated by numerous parties. Blockchain (distributed ledger) is a trusted service system for nodes [14]. Blockchain functions as a responsible third party to keep things together, mediate exchanges, and supply safe computing devices. Blockchains come in a variety of shapes and sizes. The blocks are linked together so that each block has a hash that is a function of the previous block, and therefore the entire prior chain can be inferred, ensuring immutability [15]. The reader can see Figure 1 to understand the blockchain architecture. There are two types of blockchains, each with its own set of limitations on who can read and write blocks. First, everyone in the world can read and write on a public blockchain; and this is a common cryptocurrency. Second, reading or interacting with a private blockchain is limited. Permissioned blockchains are private blockchains with access provided to selected nodes that may interact with the blockchain [4]

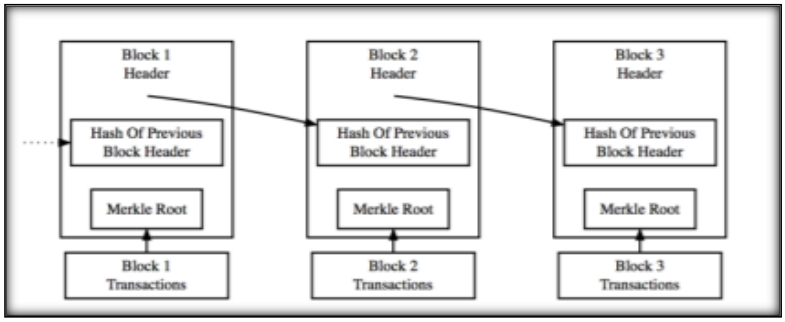

Fig. 1. Blockchain general schema [14]

4 Public cryptography

A cryptography revolution occurred with the invention of public-key encryption. Even in the 1970s and 1980s, it was clear that generic cryptography and encryption were primarily used for military purposes. Confined to the realms of military and intelligence, It was only a matter of time. Cryptography uses public-key systems and procedures. Spread to other locations. So, Users can use public-key encryption to establish trust—in communication without relying on private channels, as is the case. Without ever worrying about it, a public key can be made public [16].

In this proposed e-voting system, two public-key cryptographic algorithms have been used. They are reviewed in the following subsections.

4.1 Elliptic curve cryptography

The RSA and ElGamal cryptosystems are secure symmetric-key cryptosystems, but their enormous keys compromise their security. Scientists have looked for methods that provide the same level of security but use smaller keys. Elliptic Curve Cryptography is one promising solution (ECC). Victor Miller (IBM) and Neil Koblitz (University of Washington) devised the Elliptic Curve idea in 1985 [16]. The elliptic curve is the set of solutions from the equation (1):

$$Y^2 = axy + a3y = x^3 + a2x^2 + 4ax + 6a \tag{1}$$

This equation will only be considered over a field. The coefficient of ***ai*** are elements of a field, and there must be values of x and y to solve the equation with x and y in the field. The points of the elliptic curve for the equation (1) should satisfy the following properties in the following condition that

Closure: for all x, y in G, that x ¦ y must be in G; so the properties are:

- Associativity: for all x, y and z in G, we must have (x ¦ y) ¦ z = x ¦ (y ¦ z).
- Identity: there exists an e in G such that x ¦ e = e ¦ x = x for all x.
- Inverse: for all x, there exists a y such that x ¦ y = y ¦ x = e.

If on top of that, we have the abelian property:

- Abelian: for all x, y in G, we have x ¦ y = y ¦ x, then we say that the group is abelian.

It is possible to make a group out of a set of points on an elliptic curve, but defining a curve point operation with the properties given in the above properties can be accomplished in the following manner [17].

For example, if we have two points $P\ and\ Q$ in the elliptic curve in equation (2):

$$y2 = x3 - x + 1 \tag{2}$$

If P and Q are two points on this curve, then this is the form of an elliptic curve that we have chosen. Thus, using Diophantus techniques, the addition can be defined operation for P and Q by drawing a straight line through them and intersecting in the elliptic

curve in the third point. As a result, the reflection of the third point is taken on the x-axis as the sum, and R is defined as the sum of P and Q. This is closely related to Diophantus techniques. The group law is depicted in Figure 2. It is worth noting that the group is abelian; the group law of an abelian group is frequently written in additive notation [18].

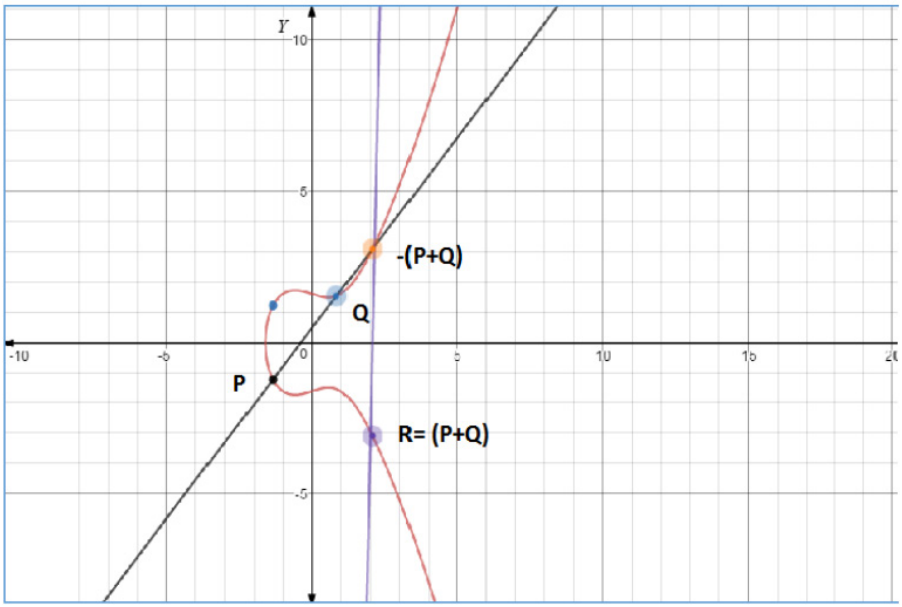

Fig. 2. Group law explanation over an elliptic curve [16]

4.2 Homomorphic encryption

Homomorphic encryption is a powerful cryptography technique that enables certain computations to be performed directly on ciphertext while ensuring that operations performed on the encrypted data produce identical results to those performed on the plaintext. It contributes to data integrity protection by allowing others to manipulate the encrypted version of the data while no one can comprehend or access the decrypted values [17]. The homomorphic encryption technique protects your privacy and enables immediate access to encrypted data. So it allows private queries to a search engine, performs encrypted data searches, and increases the efficiency of secure multiparty computation. There are two main properties of homomorphic encryption [19]:

4. Additive Homomorphic Encryption: Homomorphic encryption is additive if:

$$Enc\,(P1 \oplus P2) = Enc\,(P1) \oplus Enc\,(P2)$$

Where *Enc* is the Encryption function and P1, and P2 are the plaintexts.

5. Multiplicative Homomorphic Encryption: Homomorphic encryption is multiplicative if:

$$Enc\,(P1 \otimes P2) = Enc\,(P1) \otimes Enc\,(P2).$$

There are three main primitives or functions of Homomorphic Encryption: KeyGen, Encryption, and Decryption as follows:

1. KeyGen Function: It is an algorithm that gets a security parameter (SP) to generate each of the secret key (*sk*) and public key (*pk), (pk, sk*)⇓ KeyGen (SP).
2. Encryption *(Enc)* Function: it is a random algorithm that produces a ciphertext (c) which comes from using plaintext and *sk, c = Enc (sk, m).*
3. Decryption (Dec) Function: it is a random algorithm that produces a plaintext (m) which comes from cipher text and *sk(m)= Dec (c, sk)*[20].

5 Digital certificates and authentication

Trusted certification authority offers electronic documents known as digital certificates that identify an individual or organization with a public key (person, software, device, thing, etc.). Electronic signatures with validity work like handwritten signatures can be generated using digital certificates issued and used inside a particular legal framework, allowing secure document exchange between two unknown entities [21]. The third party is a certificate authority trusted by the user community, such as a government agency or a financial institution. A user can securely present his public key to authority and acquire a certificate. After that, the user can publish the certificate. Anyone who requires access to this user's public key may receive the certificate and verify its validity using the associated trusted signature [22]. This paper adopts a digital certificate scheme to distribute the public keys (elliptic curve key of the regional voting office and homomorphic public key of the supreme election authority) to the voter machine.

Regarding the authentication strategy, there are currently initiatives underway to improve authentication systems and growing demands for new directions. The ones that use something the user knows (i.e. password, pin) or something the user has (i.e. QR tag, face, or fingerprint) are among the most well-known and different authentication types. Biometry is a well-known paradigm utilized in both identifying and authentication systems. Face recognition is used in the majority of biometric solutions [20]. The next subsection will detail the biometric authentication system used in the proposed e-voting system.

5.1 Face recognition

Face recognition is a popular image analysis application. Face recognition is vital in today's world for security, personal data access, improved human-machine interaction, and targeted advertising. Thus, a low-cost recognition system performs faster matching, manages extensive databases, and recognizes varied contexts. Creating an automated

system that can detect faces on par with humans is difficult. It is a biometric technology that uses automated methods to verify or identify a living person's identity. Researchers and website owners are concerned about website security since hacking techniques have progressed. Most researchers assumed the first step in protecting websites and services was to ensure that people could log in. New face recognition algorithms safeguard critical areas in the clarifying process [23]. Face recognition. The face recognition system consists of the following steps:

Find faces: find all fronts by locating the faces in a scene. Face detection is done using a method known as the Histogram of gradient HOG. This algorithm begins with converting an image into a black and white picture. This method aims to find out the darkness of the current pixel compared to the pixels around it. Then draw an arrow to specify the direction in which the image is getting darker. Repeat the process with every pixel; this will yield an image with replaced pixels with arrows as in Figure 3. To find a face in the HOG image, the system matches the HOG gradient to a similar HOG pattern extracted from a set of training faces [21].

Fig. 3. Histogram of Gradient for face [21]

1. The central concept is to identify 68 distinct places (known as landmarks) on every face. The face recognition system trains a machine-learning algorithm to locate these 68 specific points: Normalizing faces: warp the picture so that the eyes and lips in the sample are placed in the image using the face landmark estimation algorithm.

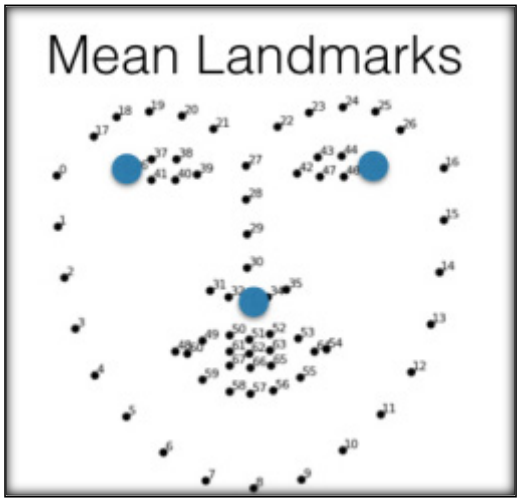

Fig. 4. 68 landmark points specified in the human face [22]

It's easy now that the system knows where the eyes and mouth are. The algorithms then rotate, scale, and shear this image to centre the eyes and mouth as best as possible (See Figure 5).

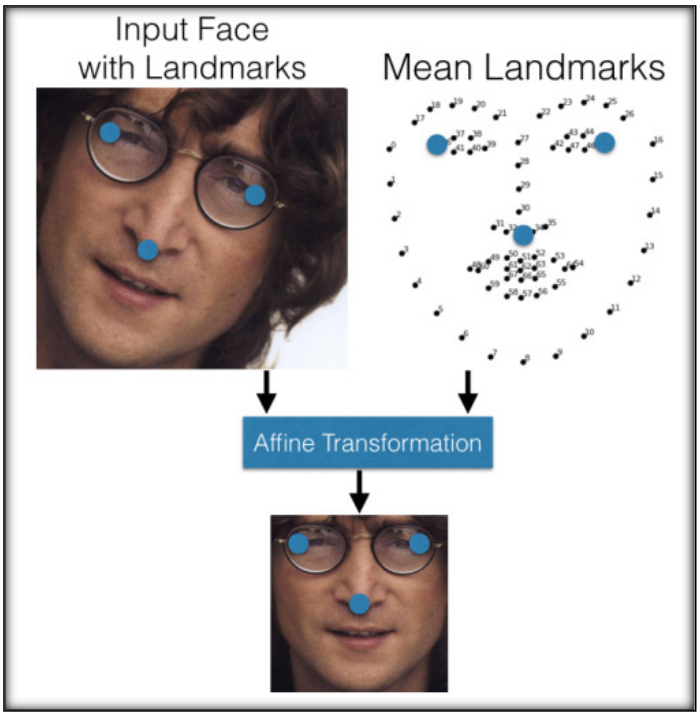

Fig. 5. Rotation and scale of landmarks [21]

2. Encoding faces: Most people start by looking at the pictures of people who have been tagged. Then, they compare the unknown face we found in Step 2 to the images of people who have already been ordered. People who have already been tagged with the same face as us must be the same person. This research used the model of Brandon Amos of openFcae project. OpenFace is trained with 500k images from two of the most extensive datasets for face recognition research, CASIA-WebFace [YLLL14] and FaceScrub [NW14]. These two datasets have the most labelled faces for research. The classification can be done using the SVM algorithm [24].

6 The proposed system

The proposed e-voting system may become a milestone in the Iraqi election system. The adopted Iraqi voting system now consists of regional election offices in each district. A central election authority manages these regional offices called the "Independent high electoral commission". So the basic elements of the proposed e-voting system are:

1. IHEC stands for Independent high electoral commission. In the proposed system, this IHEC is responsible for sending homomorphic keys to the voter frontend, calculating and declaring the results
2. REO stands for Regional election office. Regional offices in each election are where the system's backend resides. These offices are in charge of voter authentication checking, creating the wallet, and sending keys and certificates to the user frontend. And save the vote (block) in the database.
3. Cloud: It is responsible for saving the block in the blockchain of the cloud database.
4. Key certificate authority: An authority to initiate key authentication certificates for both (IHEC homomorphic key and REO elliptic curve key.

The blockchain has been built using Python 3.8 as a class representing the block's schema, as illustrated in Figure 6 below. This class is named voter block, consisting of (index of block, voter name, voter id, vote, date, previous hash, and current hash). This block class contains one constructor and two actions (functions), one for constructing a hash and the other for mining to find the hash that fulfils the condition of the beginning of 4 zeros.

```python
class voteblock:
    def __init__(self, index, name, voteid, vote, date, previousvotehash):
        self.index = index
        self.name = name
        self.voteid = voteid
        self.vote = vote
        self.date = date
        self.prevousvotehash = previousvotehash
        self.currenthash = self.mine()

    def Hash(self):
        sha = hasher.sha256()
        sha.update((str(self.index)+str(self.name)+str(self.voteid)+str(self.vote)+str(self.date)
                    +str(self.prevousvotehash)).encode('utf-8'))
        return sha.hexdigest()
    def mine(self):
        def SHA256(text):
            return sha256(text.encode('ascii')).hexdigest()

        prefix_zero = 4
        for nonce in range(MAX_NONCE):
            text = str(self.index) + str(self.name) + str(self.voteid) + str(self.vote) + str(self.date) + str(
                self.prevousvotehash) + str(nonce)

            new_hash = SHA256(text)
            prefix_str = '0' * prefix_zero
            if new_hash.startswith(prefix_str):
                return new_hash
```

Fig. 6. The class of voter block in Python language

The e-voting process in this proposed system includes two steps: registration and voting stages. The voter must have his ID card to register in the voting system in the registration stage. In Iraq, every citizen must have a voting-ID card to vote. The election committee initializes this card. The registration process is illustrated in Figure 7.

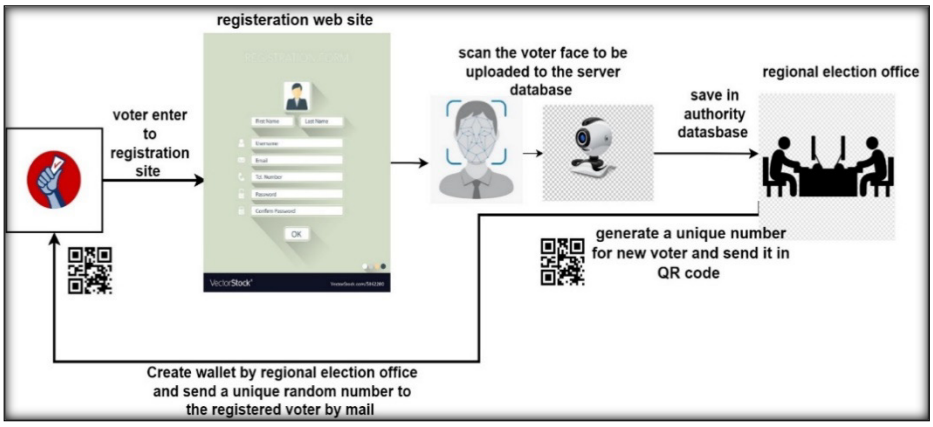

Fig. 7. Registration process for new voter

The step begins when the voter enters his information to the registration home page (first name, last name, address, gender, age, personal- ID, and voter-id card). The election authority server saves the voter's personal information (V_i) and creates a wallet or

a record. Creating the wallet process includes generating a unique random number for voter V_i. The voter unique number V_i is converted to a QR code $_{QV_i}$ and sent to the voter V_i by mail toward his e-mail. The voter V_i has to keep the $_{QR}$ V_i in his mobile to be used on election day to enter the voting room. Entrance the voter V_i through the QR code will save the anonymity and his personality from being known physically by stolen or logically revealed. Figure 8 is a flowchart of registering new voters' process.

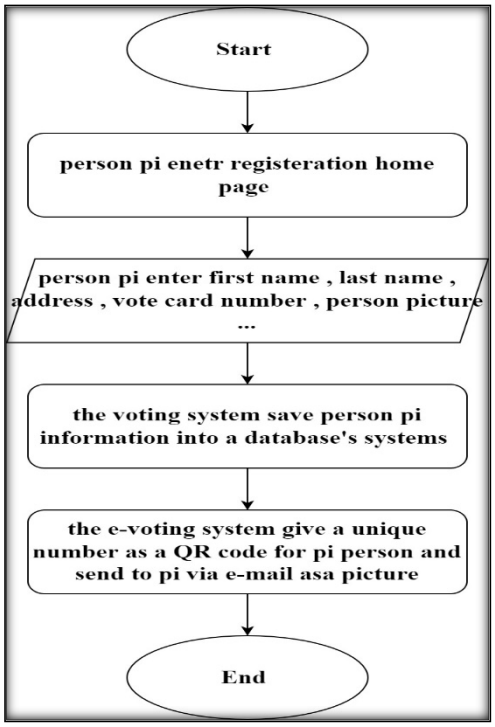

Fig. 8. New voter registration flowchart

The second step is the voting step. This process begins with entering the home page of the voting system, as shown in Figure 9.

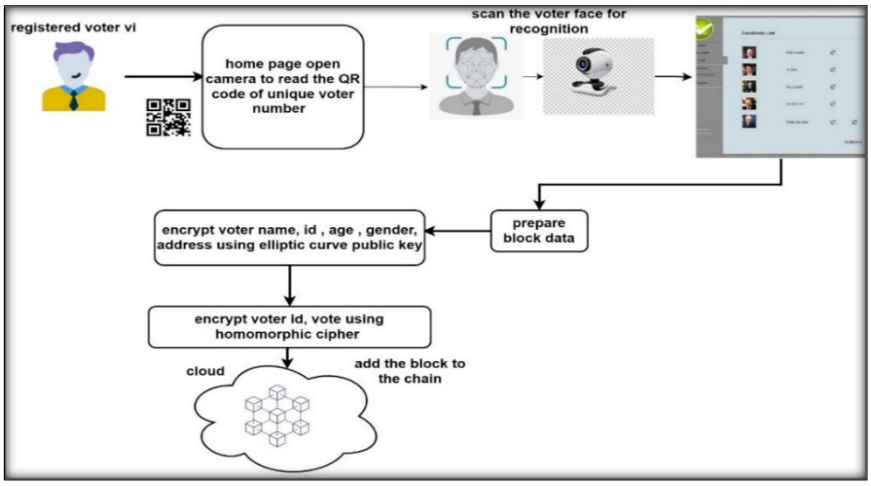

Fig. 9. Voting process for each registered voter

The user has the QR code $_{QRVi}$ photo that must be directed toward a web camera activated when the home page appears in the browser. Suppose the voting system recognizes the unique voter number of the voter $_{Vi}$ from his QR code. In that case, the system will redirect the voter $_{Vi}$ to the next step of biometric authentication. In the next authentication step, the voter vi has to show his face to the website camera to be redirected and then to the voting room (voting web page).

After authenticating the voter $_{Vi}$, and before redirecting voter $_{Vi}$ to the voting page, the step of distributing public keys begins. Revealing public keys can be done using a digital certificate signed by an authority. The certificate contains the public key of an election point and is signed with the private key given by a trusted certificate authority. Digital certificates allow any voter needing the election serve's public key to obtain the certificate and verify its validation through the attached authorized signature. Figure 10 illustrates the proposed scheme for generating public-key certificates for election points, including unique information.

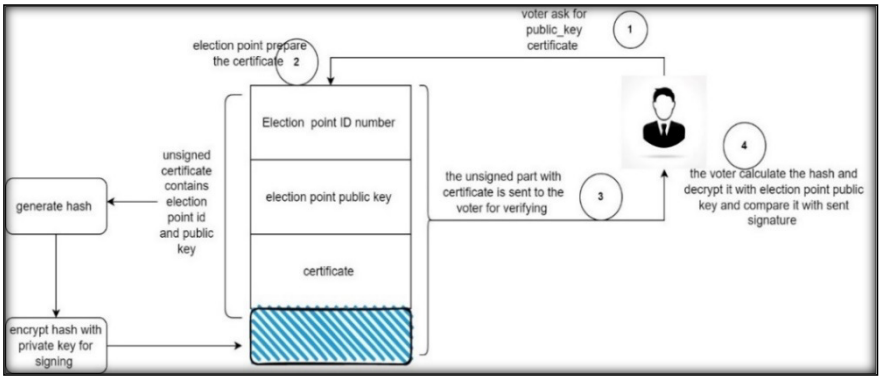

Fig. 10. Generating public keys certificate process

Election point's public key and identifying information about certificate authority, election point, then sign this information by computing the hash value of mentioned information and generating a digital signature using hash and election point private key. Verifying the public keys of election points is illustrated in Figure 11.

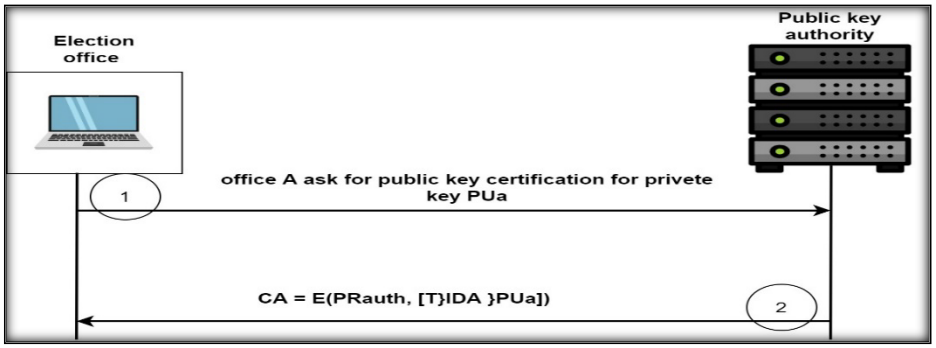

Fig. 11. Digital certificate verification process

Getting the certificate from the public key authority requires the following steps:

1. The election office asks for the certificate for its public key $_{PUa}$ from a certificate authority. Public key authority sends certificate as follows:

$$CA = E(PRauth, [T\{IDA, PUa\}])$$

$_{PRauth}$ is the authority's private key, and T is the time stamp. $_{IDA}$ is the number or information about the regional election office, $_{PUa}$ is the public key of the regional election office

2. The regional election office could forward the certificate to any voter who can verify the certificate:

$$D(PUauth, CA) = D(PUauth, E(PRauth, [T\}IDA\}PUa])) = (T\}IDA\}PUa)$$

The voter uses the authority public key, $_{PUauth}$, to decrypt the certificate because the certificate is readable only using the authority public key. Both $_{IDA}$ and $_{PUa}$ provide the recipient with the name and public key of the certificate holder.

Now the voter $_{Vi}$ enters the voting page that is in Figure 12.

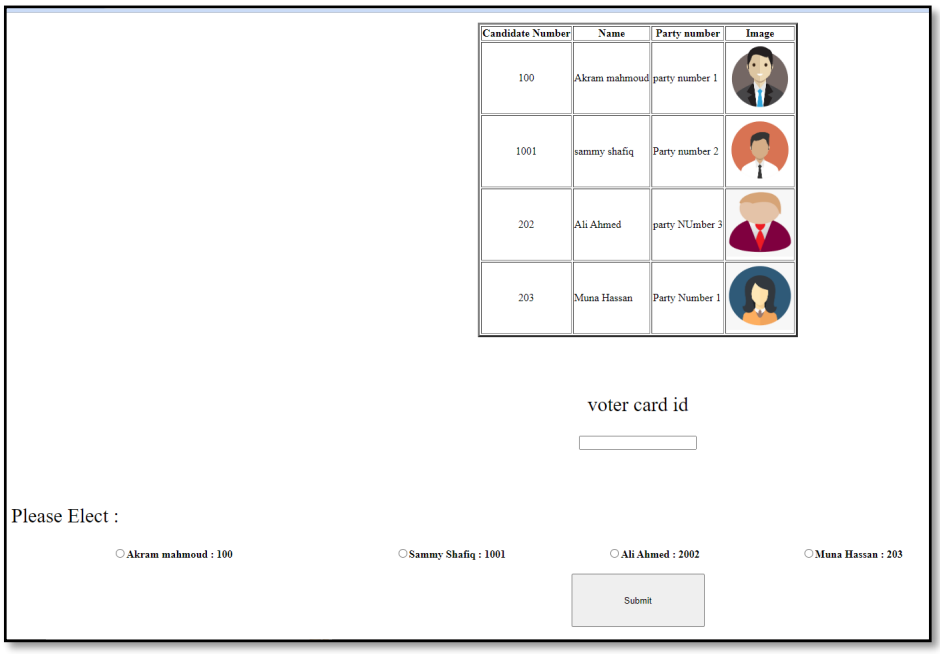

Fig. 12. Proposed system blockchain e-voting system

When voter v_i chooses the candidate, a new block will be initiated. The data in the block (virtual ballot) is encrypted in a hybrid way. Voter personal data (id, first name, last name, address, age) are encrypted using a regional e-voting office elliptic public key, as shown in Figure 12. The rest of the data ($_{voter\_id}$, $_{vote}$) is encrypted using general homomorphic election supreme authority. The use of homomorphic encryption enables the votes to be calculated while encrypted. Then, decrypt the final results using the supreme election authority private homomorphic key.

The block is stored in a table of blocks that created using sqlite3 as in Figure 13. Each record in the table represent a block (vote) that come in consequence manner with previous block and has the previous hash of the preceding block

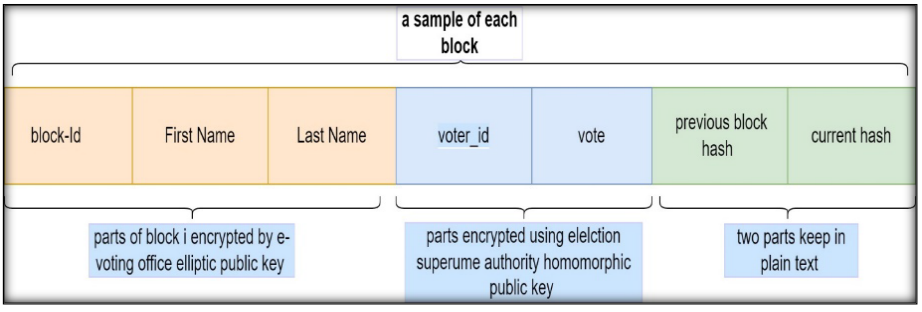

Fig. 13. Sample of encrypting each block (vote)

7 Results and discussion

In this section, the experiments on securing the e-voting system are illustrated. The tests have been executed offline in a system of PC Lenovo idea pad Intel COREi7 with RAM 8GB. In an e-voting blockchain-based system, there is a need to test the encryption/ decryption of the public key encryption algorithms (RSA, elliptic curve, and homomorphic) in addition to the proposed hybrid encryption schema (encrypt voter information with the elliptic curve and vote, vote-id encrypted by homomorphic public key to be accumulated later while it is encrypted). These tests take two factors: first, the encryption time and the second key generator randomness. Time of encryption has been tested on creating 1000 blocks in an e-voting process. Each block represents 126 bytes that make 126 kilobytes. The time is registered in the Table (1).

Table 1. Time comparison table between various public key algorithms

Encryption Type	Average Time
Homomorphic	4.47 minutes
RSA	14.5 minutes
Elliptic curve	7.5 minutes
Proposed hybrid algorithm	4.55 minutes

The second test is the key generator randomness for the proposed system key generator compared with RSA, elliptic curve and homomorphic key generators by using NIST tests. five randomness tests were implemented: frequency test (mono bit) represents the proportion of zeroes, and ones for the entire sequence are the test's subject. The test determines whether the fraction of ones in a sequence is close to 12; the number of ones and zeroes in a sequence should be roughly equal. The second frequency test within a block means determining whether the frequency of ones in an M-bit block is approximately M/2, as would be expected under an assumption of randomness.

Third, the run test, the total number of runs in the sequence, is the subject of this test, where a run is an uninterrupted sequence of identical bits. The fifth test is cumulative sums (forward test), and the sixth is the backward test; both are the maximum excursion (from zero) of the random walk defined by the cumulative total of adjusted (-1, +1) digits in the sequence is the focus of this test. The goal of the test is to see if the cumulative sum of the partial sequences in the tested sequence is too big or too small compared to the expected behavior of the cumulative sum for random sequences. The randomness tests results are listed in Table (2).

Table 2. Randomness tests results

Test	Elliptic	RSA	Homomorphic
Monobit	Random	Random	Random
Frequency test within a block	Random	Random	Random
Run test	Random	Random	Random
Cumulative sums (forward)	Random	Random	Random
Cumulative sums (backwards)	Random	Random	Random

In this research, validity has been achieved for public key distribution processes and voter personality detection. The public key distribution between the regional voting office and any voter is validated by a digital certificate CA signed by the private key. The voter validity is ensured so no unregistered or unauthorized person can enter the voting page using a robust login system of two steps. The first step was using a face recognition login page that was tested using the face dataset of RiweiChen (https://github.com/RiweiChen/DeepFace), and the average accuracy was 0.99.

8 Conclusion

E-voting system nowadays is one of the beneficial applications. E-voting systems make people to participate in the election from their homes, especially in the pandemic of COVID-19 circumstances, for example. The proposed system used a blockchain ledger to secure the voting process. But, the e-voting blockchain-based system still has bugs like authentication and security. The proposed system tackled the issue of authenticity through two steps login schema. Authentication is ensured by letting the voter login into the voting page using his unique QR code number and face recognition system. Face biometric recognition logging has been preferred over fingerprint because the fingerprint must need a fingerprint scanner that may not be available in some of the user's gadget. In contrast, face recognition needs just a webcam available on all the gadgets. The second issue is improving the security of the blockchain. The blockchain is a public ledger, and the data inside each block is public. So, the block data must be secured and unread publicly in the application of e-voting. Blockchain security is handled by proposing a hybrid encryption model that encrypts the voter's data using an election point public key (elliptic curve). The vote itself and the voter id are encrypted using homomorphic encryption public key of the election authority. Encrypting the vote using homomorphic encryption enables the election authority to calculate votes while encrypted, ensuring the voter's anonymity. This encryption schema lets the voter information and votes be saved in one blockchain, so there is no need for another separated blockchain for personal voter details for anonymity. The public keys are also ensured using a key certification and distribution method used for the first time in this paper. The speed of the proposed encryption has been tested and found to be suitable compared to other public-key algorithms. The key generator also has achieved all the five NIST key randomness tests.

9 References

[1] 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, 2021. https://doi.org/10.4218/etrij.2019-0362

[2] A. Alam, S. M. Zia Ur Rashid, Md. Abdus Salam, and A. Islam, "Towards Blockchain-Based E-voting System," in *2018 International Conference on Innovations in Science, Engineering and Technology (ICISET)*, Chittagong, Bangladesh, Oct. 2018, pp. 351–354. https://doi.org/10.1109/ICISET.2018.8745613

[3] M. Pawlak and A. Poniszewska-Marańda, "Blockchain e-voting system with the use of intelligent agent approach," in *Proceedings of the 17th International Conference on Advances in Mobile Computing & Multimedia*, Munich Germany, Dec. 2019, pp. 145–154. https://doi.org/10.1145/3365921.3365927

[4] F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa, and G. Hjálmtýsson, "Blockchain-based e-voting system," in *2018 IEEE 11th international conference on cloud computing (CLOUD)*, 2018, pp. 983–986. https://doi.org/10.1109/CLOUD.2018.00151

[5] Y. Liu and Q. Wang, "An E-voting Protocol Based on Blockchain," *IACR Cryptol.* ePrint *Arch.*, 2017.

[6] J.-H. Hsiao, R. Tso, C.-M. Chen, and M.-E. Wu, "Decentralized E-voting systems based on the blockchain technology," in *Advances in Computer Science and Ubiquitous Computing*, Springer, 2017, pp. 305–309. https://doi.org/10.1007/978-981-10-7605-3_50

[7] S. Zhang, L. Wang, and H. Xiong, "Chaintegrity: blockchain-enabled large-scale e-voting system with robustness and universal verifiability," *International Journal of Information Security*, 2019. https://doi.org/10.1007/s10207-019-00465-8

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

[9] Y. Zhang, Y. Li, L. Fang, P. Chen, and X. Dong, "Privacy-protected Electronic Voting System Based on Blockchin and Trusted Execution Environment," in *2019 IEEE 5th International Conference on Computer and Communications (ICCC)*, Dec. 2019, pp. 1252–1257. https://doi.org/10.1109/ICCC47050.2019.9064387

[10] G. C. Prasetyadi, A. B. Mutiara, and R. Refianti, "Blockchain-based Electronic Voting System with Special Ballot and Block Structures that Complies with Indonesian Principle of Voting," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 11, no. 1, Art. no. 1, Jan. 2020. https://doi.org/10.14569/IJACSA.2020.0110121

[11] H. Li, Y. Li, Y. Yu, B. Wang, and K. Chen, "A Blockchain-Based Traceable Self-Tallying E-Voting Protocol in AI Era," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 2, pp. 1019–1032, Jun. 2021. https://doi.org/10.1109/TNSE.2020.3011928

[12] E. Zaghloul, T. Li, and J. Ren, "d-BAME: Distributed Blockchain-Based Anonymous Mobile Electronic Voting," *IEEE Internet of Things Journal*, vol. 8, no. 22, pp. 16585–16597, Nov. 2021. https://doi.org/10.1109/JIOT.2021.3074877

[13] R. Taş and Ö. Ö. Tanrıöver, "A Manipulation Prevention Model for Blockchain-Based E-Voting Systems," *Security and Communication Networks*, vol. 2021, p. 6673691, Apr. 2021. https://doi.org/10.1155/2021/6673691

[14] A. Ghazi *et al.*, "A Systematic Literature Review of Blockchain Technology," *Int. J. Interact. Mob. Technol.*, vol. 16, no. 10, pp. 97–108, May 2022. https://doi.org/10.3991/ijim.v16i10.30083

[15] R. Hanifatunnisa and B. Rahardjo, "Blockchain based e-voting recording system design," in *2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)*, 2017, pp. 1–6. https://doi.org/10.1109/TSSA.2017.8272896

[16] A. M. Qadir and N. Varol, "A review paper on cryptography," in *2019 7th international symposium on digital forensics and security (ISDFS)*, 2019, pp. 1–6. https://doi.org/10.1109/ISDFS.2019.8757514

[17] M. A. Dar, A. Askar, D. Alyahya, and S. A. Bhat, "Lightweight and Secure Elliptical Curve Cryptography (ECC) Key Exchange for Mobile Phones," *Int. J. Interact. Mob. Technol.*, vol. 15, no. 23, pp. 89–103, Dec. 2021. https://doi.org/10.3991/ijim.v15i23.26337

[18] M. Albahri, "Efficient Elliptic Curve Cryptography Software Implementation on Embedded Platforms," University of Sheffield, 2019.

[19] P. Martins, L. Sousa, and A. Mariano, "A survey on fully homomorphic encryption: An engineering perspective," *ACM Computing Surveys (CSUR)*, vol. 50, no. 6, pp. 1–33, 2017. https://doi.org/10.1145/3124441

[20] H. Shihab and S. Makki, "Design of fully homomorphic encryption by prime modular operation," *Telfor J*, vol. 10, no. 2, pp. 118–122, 2018. https://doi.org/10.5937/telfor1802118S

[21] E. P. Quiroz, A. Cuno, W. R. Lovón, and E. Cruzado, "ECC usage on X. 509 digital certificates," in *2020 IEEE Engineering International Research Conference (EIRCON)*, 2020, pp. 1–4. https://doi.org/10.1109/EIRCON51178.2020.9254050

[22] W. Stallings, *Cryptography and network security: principles and practice*, Seventh edition. Boston: Pearson, 2017.

[23] Y. Azizi, M. Azizi, and M. Elboukhari, "Log Data Integrity Solution based on Blockchain Technology and IPFS," *Int. J. Interact. Mob. Technol.*, vol. 16, no. 15, pp. 4–15, Aug. 2022. https://doi.org/10.3991/ijim.v16i15.31713

[24] B. Amos, B. Ludwiczuk, and M. Satyanarayanan, "Openface: A general-purpose face recognition library with mobile applications," *CMU School of Computer Science*, vol. 6, no. 2, p. 20, 2016.

10 Authors

Saba Abdul-Baqi Salman, M.Sc University of Information and Commuication Technology She is currently Assistant Professor Computer Science Dept., Aliraqia University, Baghdad, Iraq. She is working for a PhD in College of Computer Science and IT, University of Anbar, Ramadi, Iraq (E-mail: sab19c1004@uoanbar.edu.iq).

Sufyan Al-Janabi obtained his B.Sc. (1992), M.Sc. (1995), and Ph.D. (1999) in Electronic and Communications Engineering from the College of Engineering, Al-Nahrain University in Baghdad. His research interest includes internet protocols, information security, and quantum cryptography. He is currently a Professor at the College of Computer Science and IT, University of Anbar, Ramadi, Iraq (E-mail: sufyan.aljanabi@uoanbar.edu.iq).

Ali Makki Sagheer, PhD, M.Sc and B.sc from Technology University. He is currently Professor in Al-Qalam University College, ,Kirkuk, Iraq and he affiliation of University of Anbar, Ramadi, Iraq (E-mail: prof.ali@alqalam.edu.iq, ali_makki@ uoanbar.edu.iq).

Article submitted 2022-06-10. Resubmitted 2022-07-14. Final acceptance 2022-07-16. Final version published as submitted by the authors.