An Electronic Voting System adopting Blockchain: Interpretation, Characteristics and Investigation

Ahmed YACOUBI^{1*}, Brahim ERRAHA², and Hiba Asri²

¹Phd Student, LIMA Laboratory, National School of Applied Sciences, Ibn Zohr University, Agadir, Morocco

²Professor, LIMA Laboratory, National School of Applied Sciences, Ibn Zohr University, Agadir, Morocco

Abstract This article offers an E-voting (Electronic Voting) approach that ensures security, privacy, and transparency. We have decided to use the blockchain system. Blockchain technology lowers the cost of centralized Clouds, Datacenters, and Networking Equipment, decreases the need for middlemen, and provides data privacy and transparency; all of which are critical for a fair election. An Architecture and Algorithm are suggested for the blockchain-based voting system. An internet of things (IoT) based system is designed to exchange data from the electronic voting machine and the nodes. Furthermore, we introduced its features, and we concluded with some future investigations.

1. Introduction

Voting's objective is to elect genuine people to represent a country or organization in order to ensure democracy in administrative systems. It is necessary to ensure that the electoral process is secure, transparent, and truthful. In Morocco, the standard voting procedure is centralized and clogged with intermediaries. The voters hand up their identification documents to a third party, such as the administration's supervisors or volunteers. The voters are authorized to cast their votes after being authenticated by the a third party. A pen and a document are used by voters to elect their representatives. This document will be posted in a sealed envelope and stocked in a closed case until the operation is over to count the votes.

This previous method left several opportunities for election rigging. Representatives, for example, can authorize illegitimate voters; there is a risk of damage to the ballot box. These flaws can make the entire election process less trustworthy and dangerous. As a result, the traditional voting system requires security, transparency, and data preservation, as well as the risk of data loss.

However, blockchain technology provides a viable solution to the aforementioned issues. A blockchain is a data structure in which data is organized into a chain and exchanged across a network. The network's node-servers are all in sync. It saves the same information across the network. New records (called blocks) can be added to the existing blocks as long as they all approve the new block in the network. In addition, once blocks are recorded, it is not feasible to modify or erase them. Hence, blockchain provides a secure, reliable, and third party free system.

Blockchain has been used for a variety of reasons in recent years. The first version introduced by Nakamoto was a Cryptocurrency transaction. [1] Users use bitcoin to buy and sell legal and especially illegal products. The second version with the introduction of the smart contract, where users can operate a reliable operation. [2]. The third version of Blockchain is more oriented into applications of the blockchain architecture to solve life

problems, and Blockchain can be introduced to smart cities infrastructure.[3]

There have been several works on blockchain based smart city [4] [5], in different fields, like public health [6], smart logistics and supply chain [7], smart administration and services [8], and others implementations fields.

Pairing the technology with IoT networks is beneficial to reduce implementation costs and ensure data privacy and transparency.[3]

We propose the blockchain method for developing an IoT-based e-voting system because of its security, transparency, and flexibility.

In the first section, we will introduce blockchain, its definition, and the Proof of work consensus Method. In the second section, we will propose an IoT architecture implementation using blockchain. The Characteristics and Investigation are introduced in the last section.

2. Blockchain overview

“Blockchain is a peer-to-peer (P2P) distributed ledger technology for building trust and consensus in decentralized networks. « A blockchain is a distributed and tamper-resistant database that no single entity controls but can be shared and accessed by all. New records (called blocks) can be added to the existing blocks as long as the new block is approved by all in the network. Also, once blocks are recorded, it is not feasible to modify or erase them. By using sophisticated and computationally intensive secure hash algorithms, it achieves data integrity by preventing the deletion or manipulation of data and the storage of invalid information. These computationally intensive algorithms are part of a proof-of-work, which is a consensus method by which different nodes in a network can agree on new data or detect an anomaly. » [9]

The critical features of blockchain are as follows:

- Reduce Cost of centralized Clouds, Data centers & Networking Equipments
- Solves the single point of failure problem
- Data Integrity

* Corresponding author: ahmed.yacoubi@edu.uiz.ac.ma

2.1 A Block

A predefined-size block stores a specific amount of data in a distributed ledger. As illustrated in Figure below, each block is tagged with a unique hash to address the block and contains hashes of the preceding and next blocks. The first block of the chain is called the genesis block. N number of blocks linked according to their corresponding hash forms a chain of blocks. [9]

Figure 1. Illustrative Example of four blocks in a blockchain

2.2 Proof of work (Pow)

Proof-of-work is a computationally expensive consensus approach. In this method, different nodes in a blockchain attempt to solve a cryptographic hash function, SHA-256 in particular. SHA-256 generates a unique 256-bit hash of fixed size. Finding the next block by solving this hash problem is called mining, and the users performing this task are called miners.[10] We approach a hash-base method, where the hash function takes an input and returns a unique cryptographic code corresponding to that input.

hash(input) → SHA-256 cryptographic hash

As seen in the diagram below, the hashes of all blocks are organized in a Merkel tree. The Merkel tree's root hash ensures block integrity. As a result, hash-based proof of work (PoW) keeps a consensus mechanism in place and detects any unauthorized block changes. [11]

Figure 2. Merkel's hash tree

3.1 IoT Network

As indicated in the image below, we approach an IoT data transfer architecture by using an on-board controller, a user interface, and sensors that are connected to the database and the IoT Network via WIFI protocols.

Board Controller:

We suggest the Raspberry Pi as the on-board controller of an Electronic Voting Machine to keep costs down. The Raspberry Pi is a single-board computer powered by the Broadcom BCM2837 64bit ARMv7 Quad Core Processor at a maximum frequency of 1.2GHz. Raspberry Pi 3 model B comes with 40 pin GPIO, 1GB RAM, on-board BCM43143 Wi-Fi module and Ethernet port. [12]. This indicates that the Raspberry Pi is capable of handling the data operations of a blockchain network. The fingerprint and digital information from the voter's ID card are scanned by the EVM's inbuilt sensors. In order to validate the voter, the Raspberry Pi analyses the gathered data and sends it to a database.

Sensors:

For the sensors, we need to have biometric information that are stored on the voter's Id, and we will need to check the fingerprint of the voter. Therefore, we are using a sensor that combines the both specifications. For this we are using this sensor: Visionis VIS-3024 Weatherproof IP68 Access Control Standalone Biometric Fingerprint RFID Reader Wiegand 200 Fingerprints and 500 EM Cards with Sensor.[13]

User Interface :

Users can vote using a web view application, that communicates with the raspberry pie using Javascript frameworks. As long as the voter is not confirmed, the EVM's user interface (UI) stays closed. Once the voter has been validated, the database sends a verification key to the EVM, which opens the user interface and links it to the blockchain network. The voters used a private key that was only known by the corresponding voters to cast their ballots. Each vote cast affects the ballot ledger, which is then synchronised across the blockchain network.

Figure 3. The Suggested IoT implementation

3 . IoT Electronic Voting Machine (EVM) Implementation

3.2 Algorithm simplified

```

1. Voter 'P' submits P(ID+Fingerprint) to database for verification.
2. If P ∈ Voter_list & hasNotBeenSubmitted(P)=True
   return key & GO to 3.
   Else, return False & ABORT.
3. Send the generated key to EVM.
4. If key_Received()= True do
   Unlock UI of EVM & connect with the blockchain network. Proceed to 5.
   Else recheck.
   Endif
5. Vote with a private key that only the voter knows. In the blockchain ledger, the hash(private key+nonce) reflects the voter. This hash will be used to store the results of the vote.
6. Synchronize the current voting ledger over the blockchain peer-to-peer network.
7. If a new block is created, compare the current root hash of the network with the root hash of the Merkel tree to maintain blockchain integrity.
    
```

3.3 Pre-voting Phase

A. Verification

Elector 'P' enters a digital ID and a fingerprint into the Electronic Voting Machine with a private key. The fingerprint verifies that the corresponding ID card belongs to the rightful person. The introduced IoT technology delivered the voter's data to the voter's database. When the database receives a verification request, a function called **hasNotBeenVoted(P)** checks to see if the requested ID has already been used. This prevents ballot stuffing. The database function verify Voter(P) checks the voter's legitimacy. The function verify Voter(voter) delivers a verification key to unlock the EVM UI and link the EVM to the blockchain network if P exists in the Voter list.

Figure 4 User Verification Process

B. Casting Votes

Voter V used a private keys to cast his vote. As shown in the diagram below, a similar header is formed in blockchain with a **hash(private key +nonce)** that stores the vote under the hash..

The voter's identity in the chain stays anonymous since the vote is saved behind a hash created by the voter's private key. Only the casted vote is visible. Each

vote syncs the blockchain ledger across the network and updates the ledger. The EVM sends a confirmation key to the central voter database after successfully casting a vote and syncing it over the blockchain ledger, marking the associated voter as '**submitted**'. Whenever a new voter seeks verification during the verification step, the function **hasNotBeenSubmitted(V)** first checks to see if the voter is already in the log.

Overall, the blockchain technology allows us to count votes in real time while maintaining the anonymity of the voter. Anyone who is interested in keeping track of the voting process can join the blockchain network.

Hence, the proposed blockchain-based e-voting model offers privacy, transparency and security in the election process.

Figure 5. The Data In the Block

3.4 Post-voting Phase

A. Counting Votes

After completing the voting phase, organizer collects all ballots in blockchain ledger or any interested party. The result is obtained by running this Algorithm.

```

Input: The ballot ledger of blockchain
Output: Vote obtained by each candidate
1: for each c ∈ Candidates do
2: function check_Ballot_Ledger (c)
3: return total obtained vote of c
4: end
5: endfor
    
```

4 Features and Investigation

In comparison to traditional voting, the suggested blockchain-based e-voting approach provides a more reliable election.

4.1 Security and transparency

The ballots are maintained in a blockchain-wide distributed ballot ledger. Because our proposed blockchain is open to the public, anyone can join a peer-to-peer network to keep up with the blockchain's data. Any effort to modify the ballot ledger without the consent of all node administrators is detectable and impossible because the chain is public and synchronised throughout the network.

Any interested party can check the outcome in real time using a public blockchain ledger, removing the possibility of result manipulation and computation

errors. As a result, the blockchain approach ensures election transparency and security.

4.2. Elimination of ballot staffing

In the electoral process, ballot staffing is a major concern. In our suggested approach, each voter goes through a verification procedure in which their information is compared to that of other voters in the database. All of the IDs that have been confirmed and successfully cast a vote are stored in the database. When the database receives a new verification request, it checks to see if the requested ID has been tagged.

When the database receives a new verification request, it checks to see if the requested ID has been tagged. As a result, any attempt to vote multiple times from the same ID will be rejected. As a result, the suggested methodology eliminates the need for ballot workers.

4.3. Decreasing election cost

The proposed strategy involves fewer workers and removes intermediaries and papers, lowering election costs dramatically. Also, reduce some unavoidable election expenditures, such as documents printing and transportation.

4.4. Protect the environment

"Less paper, less garbage and more trees" The recommended architecture will add to the protection of our ecosystem. The entire process is digital, and we will be able to preserve some trees from being cut.

4.5. Reduce political confusion

The proposed model ensures decentralization. As a result, no political party has any influence over the electoral process. Because the entire voting process is public and auditable, there is no risk of political chaos because of a rigged election.

5 Conclusion

Because of its decentralized and transparent nature, blockchain has become a popular and rising technology in a variety of areas. This article presented a blockchain-based IoT-based e-voting methodology for a fair, cost-effective, and smooth election. Furthermore, we suggested an algorithm that protects voters' anonymity while also verifying the outcome in real time. There is room for more research into optimizing an algorithm and testing it on a large-scale network.

References

1. S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System. 2009.M. Ben Rabha, M.F. Boujmil,
2. Tikhomirov, S. (2018). Ethereum: State of Knowledge and Research Perspectives. Lecture Notes in Computer Science, **206–221**. doi:10.1007/978-3-319-75650-9_14
3. Biswas, K., & Muthukkumarasamy, V. (2016). Securing Smart Cities Using Blockchain Technology. 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS). doi:10.1109/hpcc-smartcity-dss.2016.0198
4. C. LazaroIU and M. Roscia, "Smart district through IoT andBlockchain," in 2017 IEEE 6th International Conference on Renewable Energy Research and Applications (ICRERA), 2017, pp. 454-461.
5. P. K. Sharma, S. Rathore, and J. H. Park, "DistArch-SCNet: Blockchain-Based Distributed Architecture with Li-Fi Communication for a Scalable Smart City Network," IEEE Consumer Electronics Magazine, vol. 7, no. 4, pp. **55-64**, 2018.
6. Stafford, T.F.; Treiblmaier, H. Characteristics of a blockchain ecosystem for secure and sharable electronic medical records. *IEEE Trans. Eng. Manag.* **2020**, **1–23**.
7. Liao, D.-Y.; Wang, X. Applications of blockchain technology to logistics management in integrated casinosand entertainment. *Informatics* 2018, **5**, **44**.
8. França, A.S.L.; Amato Neto, J.; Gonçalves, R.F.; Almeida, C.M.V.B. Proposing the use of blockchain to improve the solid waste management in small municipalities. *J. Clean. Prod.* **2020**, **244**, 118529.
9. Blockchain Basics: Introduction to Distributed Ledgers, IBM Developer Documentation, <https://developer.ibm.com/technologies/blockchain/tutorials/cl-blockchain-basics-intro-blumix-trs/>
10. Jake Frankenfield, Proof of Work (PoW), Investopedia, <https://www.investopedia.com/terms/p/proof-work.asp>
11. Noizat, P. (2015). Blockchain Electronic Vote. Handbook of Digital Currency, 453–461. doi:10.1016/b978-0-12-802117-0.00022-9
12. Raspberrypi.org. Raspberry Pi 3 model B – Datasheet, <https://static.raspberrypi.org/files/product-briefs/Raspberry-Pi-Model-Bplus-Product-Brief.pdf>
13. VIS-3024 - Indoor + Outdoor Rated IP68 Access Control Standalone Biometric Fingerprint + Reader + Wiegand 600 Fingerprints and 10.000 EM Cards, with Capacitive Semiconductor Sensor – Visionis, Visionis, <https://www.visionistech.com/en/product/biometric-fingerprint-reader-wiegand-weatherproof-vis-3024/>