2018 2nd Int. Conf. on Innovations in Science, Engineering and Technology (ICISET)
27-28 October 2018, Chittagong, Bangladesh

Towards Blockchain-Based E-voting System

Asraful Alam[1], S. M. Zia Ur Rashid[2]
Department of Electrical and Electronic Engineering
International Islamic University Chittagong
Chittagong, Bangladesh
[1]asrafulalam.iiuc@gmail.com, [2]smziaurrashid@gmail.com

Md. Abdus Salam[3], Ariful Islam[4]
Department of Electrical and Electronic Engineering
International Islamic University Chittagong
Chittagong, Bangladesh
[3]salam.et_cuet@yahoo.com, [4]smarifulislam.me@gmail.com

***Abstract*—This paper proposed an Electric voting (E-voting) model that ensures security, privacy and transparency. Our approach uses blockchain method, a distributed ledger technology where data are shared and distributed into a network. Blockchain system offers transparency, decentralization, irreversibility and reduces the involvement of intermediaries which is crucial for an election process. An optimized algorithm is proposed for blockchain based e-voting system. An internet of things (IOT) based system is designed to exchange data from e-voting devices to the nodes. Moreover, we proposed several possible techniques and improvements for voting scenarios.**

Keywords—blockchain, electronic voting, internet of things

I. INTRODUCTION

The purpose of election is to elect legitimate leaders for a country or organization to ensure democracy in administrative systems. It is essential to make the voting process secure, fair and transparent to ensure a healthy democratic system.

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 representative deployed by the administration. After authentication by the representatives, the voters are allowed to perform their vote. This process left many holes to rig an 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. Traditional e-voting machine has an encrypted access card to extract the voting information, which may get damaged or lost. Thus the traditional voting system lacks security, transparency, data retention and has a significant risk of data tampering.

However, the blockchain technology is a reliable method to overcome the aforementioned problems.

Block-chain is data structures where data are arranged into a chain of blocks and distributed into a network. Every node-server in the network are synchronized i.e., stores the same data throughout the network. So, the data cannot be altered by one administrator without acknowledgement and permission of all other administrators of the network. Moreover, all the changes in the data are auditable. Thus block-chain provides a secure, auditable and third-party free data managing system that is crucial for an election process.

In recent years, blockchain has been used for several purposes. For example, blockchain has been used in Bitcoin transaction by S. Nakamoto [1]. Yong Yuan and Fei-Yue Wang proposed a block-chain based smart transportation system [2]. Several researchers approached blockchain to develop e-health system [3-5]. Blockchain-based energy distribution, transaction and trading methods are proposed by K. Mannaro group, E. R. Sanseverino group and G. Kim group [6-8]. Blockchain has been used to manage agricultural products [9]. A smart electric vehicle charging system has been developed based on blockchain [10]. A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak proposed a distributed solution to automotive security and privacy [11]. There have been several works on blockchain based smart city [12], [13].

Due to its security, transparency and flexibility, we approach the blockchain method to develop a model of IOT based e-voting system.

The rest of the paper is organized as follows: Section II briefly describes the blockchain. In Section III, we described the implementation of blockchain with IOT. Features and analysis of the proposed model described in Section IV. We conclude the paper in Section V.

II. BLOCKCHAIN: AN OVERVIEW

Blockchain is a decentralize data managing system, where the data are sequentially stored in an encrypted chain of blocks and distributed into a peer-to-peer (P2P) network. The idea of blockchain is generated from electronic Bitcoin system proposed by Satoshi Nakamoto [1].

The key properties of blockchain are as follows:

1. Maintain consensus mechanism i.e., require proof of work (PoW) throughout the chain.
2. Store data as a ledger into the blocks.
3. Synchronize the whole ledger throughout the network.
4. Offers decentralization of data.

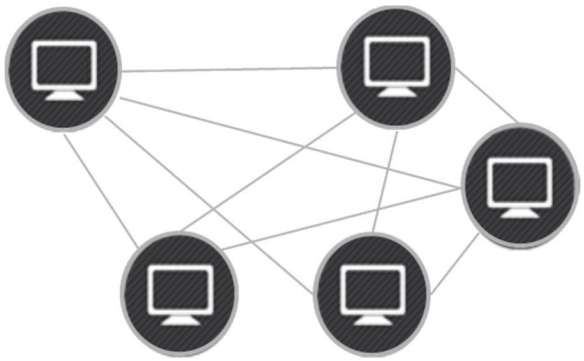


Fig. 1. Blockchain peer-to-peer (P2P) network

978-1-5386-8524-2/18/$31.00 ©2018 IEEE

A. *Block*

A block with a predefined size stores certain amount of data into a distributed ledger. Each block tagged with a unique hash to address the block and contains hashes of previous and next block as shown in Fig. 2. The first block of the chain is called genesis block [14]. N number of blocks linked according to their corresponding hash forms a chain of blocks.

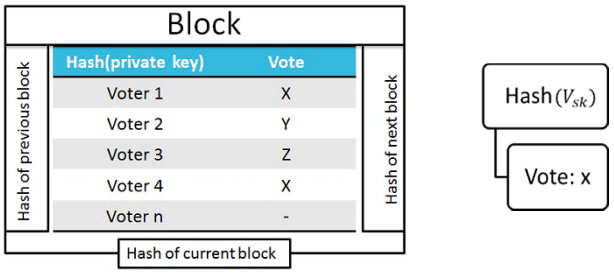


Fig. 2. (a) Architecture of a block, containing a ballot ledger and the hashes. (b) illustrates the vote stored corresponding to hash of voter's private key.

B. *PoW*

A Proof-of-work (PoW) should be hard to produce yet easy to verify [15]. We approach a hash-base method, where hash function takes an input and returns a unique cryptographic-code corresponding to that input.

h(input) →SHA-256 cryptographic hash

The hashes of all blocks are arranged in a Merkel tree as illustrated in Fig. 3. The root hash of the Merkel tree ensures blocks integrity. Thus hash-based proof of work (PoW) maintains a consensus mechanism and detects any unauthorized change in blocks by cross-checking with root hash.

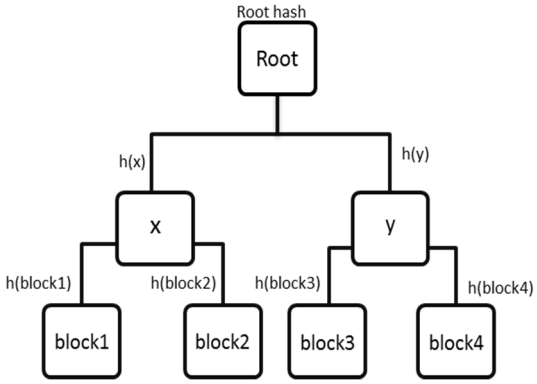


Fig. 3. A Merkel tree of four blocks generates a root hash

III. Implementation of Blockchain on IOT-based EVM

A. *Simplified Algorithm:*

1. Voter 'V' submits *V(ID+Thumbprint)* to database for verification.
2. **If** V ∈*Voter_list* & *hasNotBeenSubmitted*(V)=True **return** key & proceed to 3.
   Else, **return** False & reject.
3. Send the generated key to EVM.
4. **If** *key_Received()*= True **do**
   Unlock UI of EVM & connect with blockchain network. Proceed to 5.
   Else recheck.
   Endif
5. Cast a vote using a private key only the voter knows. The *hash(private key+nonce)* represents the voter in blockchain ledger. The casted vote will be stored under this hash.
6. Sync the current voting ledger throughout the block-chain P2P network.
7. If new block creates, check network current root hash with Merkel tree's root hash to ensure blockchain integrity.

B. *IOT model*

We approach IOT based data transfer system, which facilitates the exchange of data or information among EVMs to the servers of blockchain network.

To maintain low cost, we propose Raspberry Pi as onboard controller of EVM.

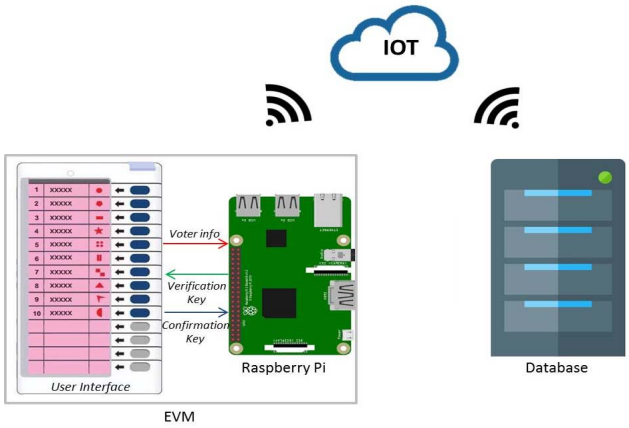


Fig. 4. IOT based data verification process

Raspberry Pi is a single board computer that runs on 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, onboard BCM43143 Wi-Fi module and Ethernet port [16].

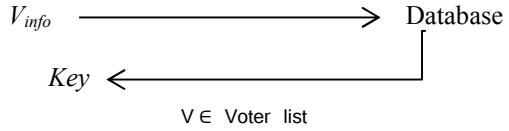
This implies Raspberry Pi is powerful enough to handle the data operation of blockchain network. The onboard sensors of EVM scan thumbprint and the digital information from the voter's ID card. Raspberry Pi processes the extracted data and sends over the data to database in order to verify the voter.

The user interface (UI) of EVM remains locked as long as the voter is not verified. Once the voter is verified, database returns a verification key to EVM that unlocks UI and connects the EVM to blockchain network. The voters cast votes using a private key only known by the corresponding voters. Each casted vote updates the ballot ledger and synced throughout the blockchain network. The whole process depicted in Fig. 5.

C. *Pre-voting phase*

1) Verification:

Every voter owns a private key, V_{sk}. Voter 'V' submits digital ID and a thumbprint through the EVM. The thumbprint confirms the ownership of corresponding ID card. The voter's data transmit to voter's database through proposed IOT system. Once database receives a verification request, a function *hasNotBeenSubmitted*(V) checks whether the requested ID has been already used or not. Thus prevents ballot staffing. A function *verify_Voter*(V) in database checks validity of the voter. If V ∈ Voter list, the function verify_Voter(voter) returns a verification key to unlock the UI of EVM and connects the EVM to blockchain network.



The verification process only verifies the voter identity, but doesn't have any clue about the vote casted by the voter, which ensures the privacy of the voter.

2) Casting vote:

The voter V cast vote using a private key V_{sk} . A corresponding header is created with *hash(private key +nonce)* in blockchain that stores the vote under the hash as depicted in Fig. 2(b).

As the vote stored under a hash, generated by the private key of the voter, the identity of voter in the chain remain anonymous and only the casted vote is visible. Each vote updates the blockchain ledger and syncs the ledger throughout the network. Upon successfully casting the vote and syncing throughout the blockchain ledger, the EVM send a confirmation key to central voter database so that, the corresponding voter will be logged as '*submitted'*. Whenever a new voter requests for verification at the verification step, the function *hasNotBeenSubmitted*(V) initially runs a check whether the requested voter is already in the log or not. Overall, blockchain method enables us to count votes in real-time while keep the voter's identity anonymous. Any interested party can join in the blockchain network to keep track on voting process.

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

D. *Post-voting phase*

1) Vote Counting:

After completing the voting phase, all ballots in blockchain ledger are collected by organizer or any interested party. The result is obtained by running Algorithm 1.

Algorithm 1: To calculate candidates results

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
```

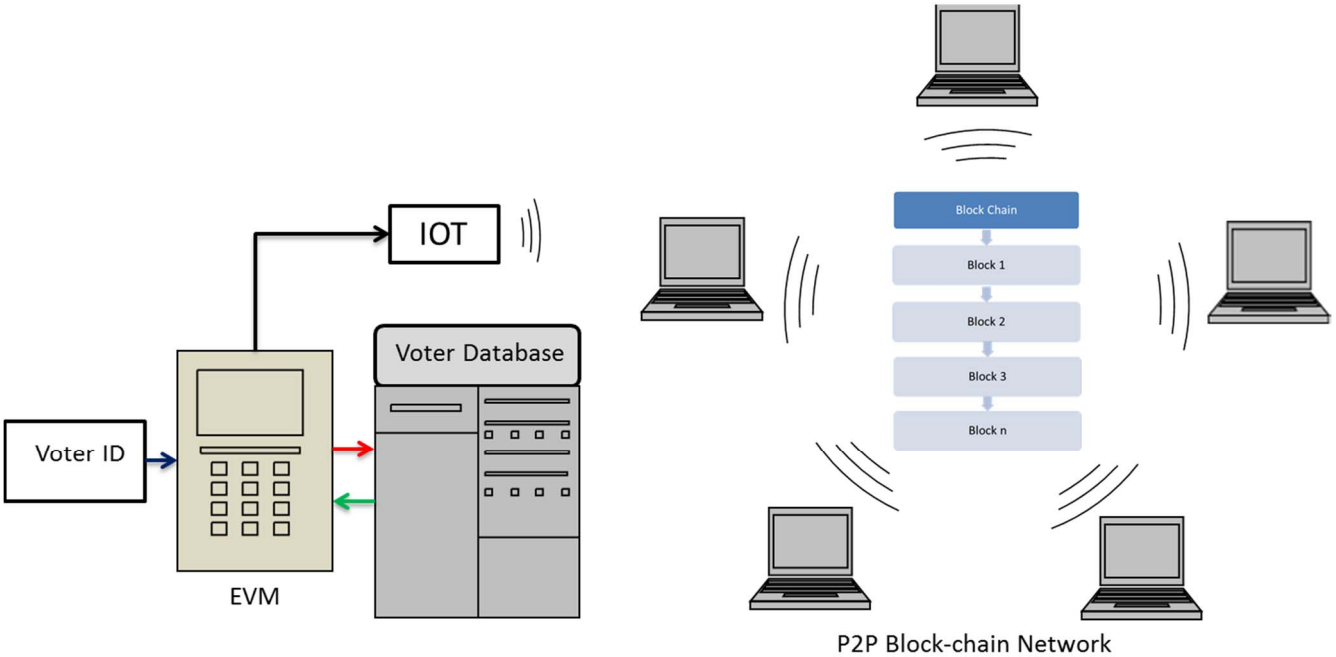


Fig. 5. Architecture of IOT based EVM with blockchain P2P network

IV. Features and Analysis

The proposed blockchain based e-voting model offers a reliable election over the traditional voting process.

A. Secure and transparent

The ballots are stored in a distributed ballot ledger throughout the blockchain. As our proposed blockchain is public i.e., anyone can join in P2P network to keep update on blockchain's data. As the chain is public and synced throughout the network, so any attempt to change in ballot ledger is detectable and not possible without the permission of all node administrators. Any concerned party can verify the result on real-time from public blockchain ledger hence, eliminates the chance of result manipulation and miscalculation. Thus blockchain approach ensures security and transparency in an election process.

B. Eliminate ballot staffing

Ballot staffing is a major issue in an election process. In our proposed system, each voter passes through a verification process by matching voter's information in the database.

The database tags all the IDs, those have already been verified and successfully casted the vote. Whenever database receives a new verification request, it first checks whether the requested ID is tagged or not. So any attempt to casting vote more than once from a particular ID will be rejected. Thus the proposed model prevents ballot staffing.

C. Redeem election cost

The proposed model requires less workforce and eliminates intermediaries, which massively reduce the election cost. Also reduce some inescapable election costs i.e., ballot printing cost, transportation cost etc.

D. Reduce political violence

The proposed model ensures decentralization. Hence, no party has influence over the election process. As the whole voting process is transparent and auditable, so there is no chance of political violence initiated from a rigged election.

V. Conclusion and Future Work

Blockchain has become a popular and emerging technology that being implemented in various fields for its decentralized and transparent property. In this paper, we proposed an IoT based e-voting model using blockchain technology for a transparent, cost-effective and smooth election. Also, we proposed an algorithm that helps to protect voters privacy and verifies the result in real-time. There's a scope for further research on developing an optimized algorithm and on network-based attacks e.g., Dos and 51% attack.

References

[1] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System. 2009.

[2] Y. Yuan and F. Y. Wang, "Towards blockchain-based intelligent transportation systems," in 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), 2016, pp. 2663-2668.

[3] H. Zhao, P. Bai, Y. Peng, and R. Xu, "Efficient key management scheme for health blockchain," CAAI Transactions on Intelligence Technology, vol. 3, no. 2, pp. 114-118, 2018.

[4] J. Tsai, "Transform Blockchain into Distributed Parallel Computing Architecture for Precision Medicine," in 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), 2018, pp. 1290-1299.

[5] A. Ekİn and D. Ünay, "Blockchain applications in healthcare," in 2018 26th Signal Processing and Communications Applications Conference (SIU), 2018, pp. 1-4.

[6] K. Mannaro, A. Pinna, and M. Marchesi, "Crypto-trading: Blockchain-oriented energy market," in 2017 AEIT International Annual Conference, 2017, pp. 1-5.

[7] E. R. Sanseverino, M. L. D. Silvestre, P. Gallo, G. Zizzo, and M. Ippolito, "The Blockchain in Microgrids for Transacting Energy and Attributing Losses," in 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2017, pp. 925-930.

[8] G. Kim, J. Park, and J. Ryou, "A Study on Utilization of Blockchain for Electricity Trading in Microgrid," in 2018 IEEE International Conference on Big Data and Smart Computing (BigComp), 2018, pp. 743-746.

[9] C. Xie, Y. Sun, and H. Luo, "Secured Data Storage Scheme Based on Block Chain for Agricultural Products Tracking," in 2017 3rd International Conference on Big Data Computing and Communications (BIGCOM), 2017, pp. 45-50.

[10] M. Pustišek, A. Kos, and U. Sedlar, "Blockchain Based Autonomous Selection of Electric Vehicle Charging Station," in 2016 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI), 2016, pp. 217-222.

[11] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "BlockChain: A Distributed Solution to Automotive Security and Privacy," IEEE Communications Magazine, vol. 55, no. 12, pp. 119-125, 2017.

[12] C. Lazaroiu and M. Roscia, "Smart district through IoT and Blockchain," in 2017 IEEE 6th International Conference on Renewable Energy Research and Applications (ICRERA), 2017, pp. 454-461.

[13] 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.

[14] 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.

[15] A. Judmayer, N. Stifter, K. Krombholz, and E. Weippl, Blocks and Chains: Introduction to Bitcoin, Cryptocurrencies, and Their Consensus Mechanisms. 2017, pp. 1-123.

[16] Raspberrypi.org. Raspberry Pi 3 model B -Datasheet [Online].