Analysis and Improvement of an E-voting System Based on Blockchain

Mohammad Doost
Department of Electrical Engineering
Sharif University of Technology
Tehran, Iran
doost.mohammad@ee.sharif.edu

Alireza Kavousi
Department of Electrical Engineering
Sharif University of Technology
Tehran, Iran
kavousi.alireza@ee.sharif.edu

Javad Mohajeri
Electronics Research Institute
Sharif University of Technology
Tehran, Iran
mohajer@sharif.edu

Mahmoud Salmasizadeh
Electronics Research Institute
Sharif University of Technology
Tehran, Iran
salmasi@sharif.edu

***Abstract*— Voting is one of the important aspects of a democratic society in which people can express their opinions in a formal and legitimate way. In recent years, there has been an increasing interest in electronic voting (e-voting) systems. E-voting is a modern method of vote casting which is based on cryptographic tools. In many proposed scheme, it is a need to have a trusted entity to manage to take the votes and properly counting them. Recently and in the light of pivotal features of blockchain technology including immutability, transparency, and decentralization, blockchain based schemes have received considerable attention. In 2017, J.P.Cruz and Y.Kaji presented a blockchain based e-voting scheme with the help of some cryptographic concepts like bit-commitment and blind signatures. The vital property of their scheme was that it did not use any kind of anonymous channel which is a common and of course hard to implement tool in many e-voting protocols. In this paper, we address some security issues in the mentioned scheme and propose an improved version that has the edge on the prior one in terms of preserving privacy of voters and efficiency when it comes to large scale elections. We show how to use private blockchain instead of a public blockchain to provide more efficiency and privacy. Also, by utilizing proper entities, some security breaches like double voting are prevented.**

***Keywords*— electronic voting, blockchain, consensus**

I. Introduction

Voting is a pillar of a democratic community which is used for endorsing people's opinion about a particular matter. As a whole, voting is done in two ways: paper based voting and electronic voting [1].

In the e-voting model, facilitating in casting a vote and existing some imperative features like having more transparency lead to a good turnout in the polling process [2]; however, providing security requirements has been a major problem with this kind of voting in these years [3]. It is worth noting that e-voting is a particular type of multi-party computation (MPC) [4]. Over the past couple of years, many studies have been conducted on the e-voting system using some cryptographic tools such as blind signatures [5], zero-knowledge proofs [6], homomorphic encryption [7], and mixing networks [8]. One of the controversial subjects within the field of MPC including e-voting is the necessity to have a trusted party during the execution of the protocol. This party often has full control over the execution of the process and because of this, it can threat the validity and authenticity of the results.

Thanks to some really important features of the blockchain technology such as decentralization, transparency, immutability, and undeniability, it is considered as a decisive tool to be used for a wide range of applications. Blockchain can have an influential role in the matter of decentralization in MPC based problems like e-voting. Of course, there are several issues to be addressed before utilizing this state-of-the-art technology [9]. In recent years, many attempts have been made to use blockchain in e-voting schemes in which while providing features like anonymity and verifiability, the voting process could be done without any need to have a trusted third party [10]. The first study on the blockchain based e-voting was carried out in 2015 by Zhao and Chan [11]. In the last few years, there have been numerous proposed schemes with the help of combining diverse cryptographic techniques with blockchain technology. One of these schemes is presented by J.P.Cruz and Y.Kaji [12]. The important aspect of [12] is that there is no need to use an anonymous channel in the scheme and in this respect, it is very much remarkable. This study aims to analyze and present an improvement in [12] in which the scheme maintains some other beneficial features compared to the prior scheme.

This paper is divided into five sections. In section II, the security requirements of e-voting systems are described. Section III is devoted to reviewing the blockchain based e-voting schemes. In Section IV, J.P.Cruz and Y.Kaji protocol is explained and section V introduces our improved scheme. Security analysis of the proposed scheme is presented in section VI. In the end, conclusions are drawn in section VII.

II. E-voting

In general, an e-voting system is comprised of some parties including voters, counting entities, and other trusted third entities. Each e-voting scheme often consists of four phases including the preparation phase, registration phase, voting phase, and counting phase.

Some crucial security prerequisites of e-voting schemes are listed as below:

Privacy: There should be no meaningful link between the vote and the voter who cast it.

Eligibility: Only legitimate voters who have predetermined features should be able to vote.

Verifiability: Each voter must be able to verify the casting of his/her and other voters' votes in the final counting stage. This feature divides into individual and public verifiability.

978-1-7281-7296-5/20/$31.00 ©2020 IEEE

Undeniability: It should be impossible to deny casting a vote in any stage of the voting process.

Accuracy: E-voting schemes need to be free of errors. The votes should be registered and counted accurately and authorized voter can cast only one vote.

Fairness: For the sake of having a fair election, nobody should be able to obtain the partial result during the election process.

Long-term security: In some periodic election cases, preserving privacy of voters may cause the need for long-term security.

III. Blockchain Based E-Voting

In the e-voting system, blockchain technology is used as a secure and unchangeable ballot box [13]. Thanks to the immutability feature of this innovative technology, it is almost impossible to manipulate or modify the votes. Blockchain operates in a peer-to-peer network and authorized voters can cast their votes as a transaction in this network via their devoted addresses. Then, these transactions would be verified by miners and valid transactions are gathered into a block in which each block is attached to the previous one and as a whole constitute a ledger (a ballot box). Each miner keeps a copy of this ledger by himself/herself and once a new block is generated, the ledger gets updated. On the whole, blockchain can be separated into public and private. In a public blockchain, all users are allowed to involve in the network and participate in different processes, on the other hand, in a private blockchain an organization or a group of specific parties takes the control of network and involvement is restricted [14].

Blockchain based e-voting schemes can be divided into two general categories:

- E-voting schemes based on cryptocurrencies
- E-voting schemes based on smart contracts

Many of the existing schemes are based on either bitcoin blockchain or Ethereum blockchain. Using this technology and some cryptographic tools such as ring signature [15], zero-knowledge-proofs [16], and blind signatures [12] offer a good structure for an efficient and secure e-voting system. The scheme proposed by J.P.Cruz and Y.Kaji is based on the bitcoin blockchain. In this scheme, the bitcoin blockchain is considered as a replacement for anonymous channel and while it does not use any kind of anonymous channels, it could construct a fairly efficient anonymous hidden vote-hidden voter.

IV. An Overview on J.P.Cruz and Y.Kaji Scheme

This scheme consists of three entities: a voter V_i, third party administration *A,* and a counter *C*. In the preparation phase, each voter V_i turns its vote v_i to a commitment x_i via a random key k and asymmetric algorithm. Then, he/she blinds x_i through a random value r and the public key of third party e , and to get the third party signature on this blind value $x_i^{'}$, gives it directly to *A*. Equations are as below:

$$x_i = enc(v_i, k) \quad (1)$$

$$x_i^{'} = blind_e(x_i, r) \quad (2)$$

In the registration phase, the administration *A* looks at the list of authorized users. If the user is an eligible one and cast a vote only for once, afterward this entity signs the blinded value $x_i^{'}$ and returns d_i value. In the end, *A* reveals the list of (ID_i, x_i') for all legal voters.

$$d_i = sign_A(x_i') \quad (3)$$

Then by unblinding the values received from administration d_{i} , voter obtains a valid token y_i signed by the third party.

$$y_i = unblind(d_{\mathrm{i}}, r) \quad (4)$$

$$y_i = sign_A(x_i) \quad (5)$$

Also, in this step each voter takes a packet from administration called bitcoin card, which is comprised of a bitcoin address, a public key, and a private key. The private key is disguised in the bitcoin card. Each voter generates a new bitcoin private key $\mathrm{V_i}$.BPK and by using that creates a new bitcoin address $\mathrm{V_i}$.BA for himself/herself. On this occasion, the voter can disclose the hidden private key of the bitcoin card and compose a transaction on the bitcoin network to exchange the value from the bitcoin card to his/her own new address. In the next step, voters enroll their new bitcoin address on the administration system. Furthermore, the third party's bitcoin address is publicly revealed.

In the voting stage, every single voter provides a transaction that in its input his new address and in its output the third party's address are written. This transaction also includes (x_i, y_i). Besides, each voter transfers a little amount of bitcoin to the third party's address as a transaction fee. This fee should be as much as the transaction be validated. Once a transaction is accepted by the network, information such as sender and receiver's addresses, amount of transaction fee, pair of (x_i, y_i), transaction ID, and a timestamp signifies the time of registering are all visible. Preceding to record a transaction into the new block, the administration *A* verifies that whether this transaction is valid or not. Later on, administration releases ($\mathrm{V_i}$.BA, x_i, y_i). At the end of this stage, the number of ($\mathrm{V_i}$.BA,x_i,y_i) and (ID_i, x_i') should be equal.

In the stage of counting the votes, all voters make another transaction to the counting entity destination. As a whole, this transaction consists of voter's bitcoin address $\mathrm{V_i}$.BA, counter bitcoin address C.BA, and a specific value *k* which is used to open the commitment voters made in the past. This will enable the counting entity to open the commitments and extract the vote v_i . Eventually, the counting entity will announce the outcome publicly.

A. Analysis of J.P.Cruz and Y.Kaji Scheme

[12] offers an anonymity hidden vote-hidden voter scheme which does not use of anonymous or inaudible channels which are very difficult to implement. Some of the weaknesses of this scheme are as follows:

1**) The possibility of third party infringement and issuing several unauthorized tokens for fake IDs.** Assumption of having a trusted third party is a heavy one to take into account in the real world. Hence, in this scheme, the third party can generate some fake identities and produces bitcoin cards equal to their numbers and cast a vote for each card.

2) **The possibility of casting a vote by a third party instead of an absent voter.** The third party can easily look at its list, identify the absent persons on it, and cast a vote as a replacement for them.

3) **The unsuitability of the scheme for large scale elections.** If the election takes place on a large scale, then voting and counting processes take a huge amount of time. In fact, the reason for this is because of the constraint in the number of allowable transactions in the network that is only seven per second. In the last few years, many more studies on improving this weakness have become available [17]. Many of the schemes based on this feature need to have many more transactions, which are registered in the network. For instance, if seven million voters participate in the election process, concerning the best case in recording their votes which means there are necessarily seven voting transactions per second, then the voting process will take more than ten days.

4) **Needing to recharge the bitcoin cards by election process authorities.** Bitcoin cards need to be recharged; otherwise, only a few people tend to participate in the election process and spend money.

5) **The possibility of revealing the identity of a voter from the ballot in the long run.** If a voter uses the same address that is used for voting in the execution of other transactions, it is feasible to disclose his identity using some learning techniques [18].

V. Improvement of J.P.Cruz and Y.Kaji scheme

The proposed improved scheme consists of concepts such as RSA blind signature, commitment scheme, and private blockchain. Our scheme includes four entities: voters V_i, the issuing authority for card A_1, the issuing authority for token A_2, the election execution authority A_3 . The steps are as follows:

The preparation phase. A_1 and A_2 arrange a list of persons who are legal to vote. Each time a voter visits these two entities, two subjects would be investigated: first, the voter is an eligible one, and second, he/she requests registration only for once.

The registration phase. The voters' addresses are produced by the trusted third party A_1, and each voter receives his/her address manually or through a secure channel. In this regard, the voters' addresses and their corresponding private keys are produced and put into the sealed envelopes by A_1 and each voter randomly selects an envelope. So, tracking the address is not possible even for A_1. Voters are implicitly registered to participate in the blockchain network. Afterward, each voter turns its vote v_i to a commit using a random value r_i as follows:

$$x_i = commit(v_i, r_i) \tag{5}$$

Then, he/she blinds this commitment by a random value r_j and the public key of A_2 as below:

$$x_i' = x_i . r_j^e \tag{6}$$

A_2 signs on this blinded value and returns it to the voter

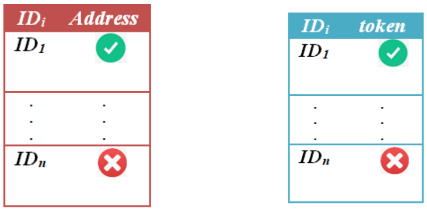
$$y_i' = (\, x_i . r_j^e)^d \tag{7}$$

$$= x_i^d . r_j$$

So, the voter can unblind the blinded signature and acquire the A_2's signature on his commitment. The procedure is as below:

$$\frac{y_i'}{r_j} = x_i^d \tag{8}$$

$$y_i \;=\; x_i^d \tag{9}$$



ID_i	*Address*
ID_1	✓
⋮	⋮
ID_n	✗

ID_i	*token*
ID_1	✓
⋮	⋮
ID_n	✗

Fig. 1. An address list and a token list belong to A_1 and A_2 respectively

$$y_i \;= unblind(y_i') \tag{10}$$

$$y_i \;= token_i \tag{11}$$

The voting phase. In the current phase, each voter generates a transaction like a bitcoin transaction. Transaction's input includes the voter's address which is written on bitcoin card and A_3's address that is written on the output of the transaction. Besides, a pair of $(x_i, token_i)$ is also available. Before adding the transaction to a new block in the blockchain network, a consortium which is a coalition of election candidates verifies whether this $token_i$ is signature of x_i or not. If this verification is valid and the corresponding address is eligible to vote, the transaction would be validated and added to the blockchain network. The authorized tokens are issued by the trusted third party A_2, so A_1 will not be able to cast a vote instead of an absent voter. It should be noted that the consortium can determine the uniqueness of the voter's address to prevent double-voting.

The counting phase. This stage begins with generating a transaction by each voter to the A_3's destination within the network. This transaction includes r_i which is the value that opens the commitment. Consortium verifies whether this value opens the commitment or not. If validation is successful, the transaction is added to the blockchain and voters tally increased by one.

VI. Analysis of the proposed scheme

In the proposed scheme, we deprive third parties of the possibility to abuse and cast vote instead of absent voters and present a decentralized scheme. Besides, our scheme provides all of the primary security requirements, which is described as follows:

Privacy: Each voter casts vote to his desired candidate by means of an anonymous address and there is no significant dependency between his identity and network address.

Eligibility: In our scheme, the voter implicitly gets registered to be a part of the network by A_1, and also for taking the eligible token, should be registered by A_2 for one more time.

Verifiability: Any Voter can check whether his/her vote is registered in the system simply by observing his transaction specification in the blockchain, which is a transparent and immutable structure.

Accuracy: Given that in a blockchain once a transaction is registered it will unchangeable, everyone can access the network and count the votes.

Undeniability: Since votes are registered in a transparent ledger, no voter who cast a vote can deny his action.

Fairness: Voters publish values which open commitments only during the counting stage and no partial counting can occur in the middle of voting process.

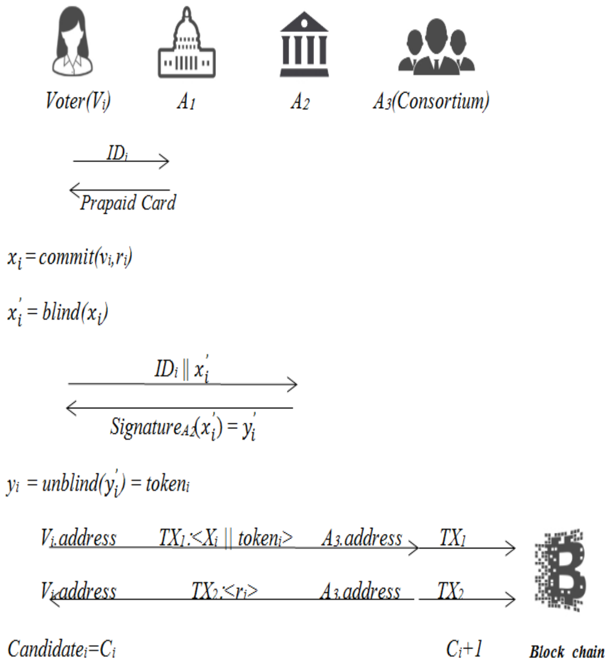


Fig.2. An overview on our scheme

Long-term privacy: Unlike [12], in our scheme the transaction is only used to vote and to the best of our knowledge, there is no known way to relate the identity of the voters to their corresponding addresses in the network.

As we mentioned, the limitation in the number of registered transactions is one of the weaknesses of [12]. In the improved scheme, deploying private blockchain seems to be a useful way to fix this weakness. In table 1, we present a comparison among our scheme, [12], and [16].

Table 1. Comparison between different schemes in terms of providing security requirements

Ours	[15]	[12]	security requirement
✓	✓	✗	privacy
✓	✓	✓	eligibilty
✓	✓	✓	verifiability
✓	✓	✓	undeniability
✓	✗	✗	accuracy
✓	✓	✓	fairness
✓	✗	✗	long-term privacy
✓	✗	✗	implemantability

VII. CONCLUSION

We have presented an improved scheme for J.P.Cruz and Y.Kaji scheme [12] which in addition to benefiting from some useful features of blockchain technology in e-voting such as immutability of votes, decentralization, and transparency, provides main security requirements. Also, infringements like creating invalid tokens or voting instead of absent voters are no longer possible.

REFERENCES

[1] Schaupp, L. Christian, and Lemuria Carter. "E-voting: from apathy to adoption." *Journal of Enterprise Information Management* (2005).

[2] Harrison, Teresa M., Theresa A. Pardo, and Meghan Cook. "Creating open government ecosystems: A research and development agenda." Future Internet 4, no. 4 (2012): 900-928

[3] Wang, King-Hang, Subrota K. Mondal, Ki Chan, and Xiaoheng Xie. "A review of contemporary e-voting: Requirements, technology, systems and usability." *Data Science and Pattern Recognition* 1, no. 1 (2017): 31-47.

[4] Yao, Andrew C. "Protocols for secure computations." In *23rd annual symposium on foundations of computer science (sfcs 1982)*, pp. 160-164. IEEE, 1982.

[5] Baiardi, Fabrizio, Alessandro Falleni, Riccardo Granchi, Fabio Martinelli, Marinella Petrocchi, and Anna Vaccarelli. "SEAS, a secure e-voting protocol: design and implementation." *Computers & Security* 24, no. 8 (2005): 642-652.

[6] Sako, Kazue, and Joe Kilian. "Receipt-free mix-type voting scheme." In *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 393-403. Springer, Berlin, Heidelberg, 1995.

[7] Sako, Kazue, and Joe Kilian. "Secure voting using partially compatible homomorphisms." In *Annual International Cryptology Conference*, pp. 411-424. Springer, Berlin, Heidelberg, 1994.

[8] Chaum, David L. "Untraceable electronic mail, return addresses, and digital pseudonyms." Communications of the ACM 24, no. 2 (1981): 84-90.

[9] Wüst, Karl, and Arthur Gervais. "Do you need a blockchain?." In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pp. 45-54. IEEE, 2018.

[10] Zou, Xukai, Huian Li, Yan Sui, Wei Peng, and Feng Li. "Assurable, transparent, and mutual restraining e-voting involving multiple conflicting parties." In *IEEE INFOCOM 2014-IEEE Conference on Computer Communications*, pp. 136-144. IEEE, 2014.

[11] Zhao, Zhichao, and T-H. Hubert Chan. "How to vote privately using bitcoin." In *International Conference on Information and Communications Security*, pp. 82-96. Springer, Cham, 2015.

[12] Cruz, Jason Paul, and Yuichi Kaji. "E-voting system based on the bitcoin protocol and blind signatures." *IPSJ Transactions on Mathematical Modeling and Its Applications* 10, no. 1 (2017): 14-22.

[13] Hardwick, Freya Sheer, Apostolos Gioulis, Raja Naeem Akram, and Konstantinos Markantonakis. "E-voting with blockchain: An e-voting protocol with decentralisation and voter privacy." In *2018 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)*, pp. 1561-1567. IEEE, 2018.

[14] Zheng, Zibin, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, and Huaimin Wang. "Blockchain challenges and opportunities: A survey." *International Journal of Web and Grid Services* 14, no. 4 (2018): 352-375.

[15] Wu, Yifan. "An e-voting system based on blockchain and ring signature." Master. University of Birmingham (2017).

[16] McCorry, Patrick, Siamak F. Shahandashti, and Feng Hao. "A smart contract for boardroom voting with maximum voter privacy." In International Conference on Financial Cryptography and Data Security, pp. 357-375. Springer, Cham, 2017.

[17] Dorri, Ali, Salil S. Kanhere, Raja Jurdak, and Praveen Gauravaram. "Lsb: A lightweight scalable blockchain for iot security and privacy." arXiv preprint arXiv:1712.02969 (2017).

[18] Alkhalifah, Ayman, Alex Ng, A. S. M. Kayes, Jabed Chowdhury, Mamoun Alazab, and Paul Watters. "A taxonomy of blockchain threats and vulnerabilities." (2019).