Yi *EURASIP Journal on Wireless Communications and Networking* (2019) 2019:137
https://doi.org/10.1186/s13638-019-1473-6

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Securing e-voting based on blockchain in P2P network

Haibo Yi

Abstract

Electronic voting (e-voting) is an electronic means for casting and counting votes. It is an efficient and cost-effective way for conducting a voting procedure, which has characteristic of being magnanimous data and real time and requesting high safety. However, concerns on security of networking and privacy of communication for e-voting have been grown. Securing e-voting is very urgent and has becoming a popular topic in the area of communications and networking. We present techniques to exploit blockchain in P2P network to improve the security of e-voting. First, we design a synchronized model of voting records based on distributed ledger technology (DLT) to avoid forgery of votes. Second, we design a user credential model based on elliptic curve cryptography (ECC) to provide authentication and non-repudiation. Third, we design a withdrawal model that allows voters to change their vote before a preset deadline. By integrating the above designs, a blockchain-based e-voting scheme in P2P network is proposed for essential requirements of e-voting process. To prove and verify the scheme, a blockchain-based e-voting system for multiple candidates has been designed on Linux platforms in P2P network. The system involves electronic voting theory, cryptography, and software engineering theory. The implementation result shows that it is a practical and secure e-voting system, which solves the problem on forgery of votes during e-voting. The blockchain-based e-voting system can be applied to a variety of networking applications directly.

Keywords: Electronic voting (e-voting), Blockchain, Secure voting, P2P network

1 Introduction

Voting is a method to make a collective decision or express an opinion among a group or a meeting or electorates [1]. Voting is usually following debates, discussions, and election campaigns. During voting, the person to be elected is the candidate of an election, and the person who casts a ballot for their chosen candidate is voter [2]. Usually, the voter can vote in accordance with the list of candidate or vote for any other persons he/her prefers. Voting ballots must be unsigned and marked by the voters in private booths so that no one else can find out for whom a citizen is voting [3]. Since the 17th century, voting has been the usual mechanism by which modern representative democracy has operated [4]. Voting is also used in many other private organizations and groups, such as clubs, corporations, and voluntary associations [5].

With the rapid development of the Internet and information technologies, many conventional offline services such as voting, mail, payment, are migrating to online ones [6]. The online voting is known as electronic voting (e-voting). It is an electronic means for casting and counting votes [7]. Users of e-voting are voters and election authorities. The voter can submit his/her or her votes electronically to the election authorities from any location via e-voting [8]. The election authorities are responsible for collecting votes from voters. E-voting can save time and effort with high efficiency and flexibility, which is getting more and more attentions instead of traditional voting [9]. With the development of Internet, e-voting became the important means of many organizations [10]. Kiayias et al. [11] proposed an efficient E2E verifiable e-voting system without setup assumptions. Ahene et al. [12] proposed a certificateless deniably authenticated encryption and its application to e-voting system. Kshetri and Voas [13] proposed a blockchain-enabled e-voting system.

1.1 Motivations

E-voting is an efficient and cost-effective way for conducting a voting procedure, which has characteristic of

Correspondence: haiboyi@szpt.edu.cn
School of Computer Engineering, Shenzhen Polytechnic, 518055, Shenzhen, China

being magnanimous data and real time and requesting high safety [14].

However, concerns on security of Internet and privacy of communication have been grown [13]. Anonymity needed by e-voting cannot meet by encryption alone [11]. For example, a vote should not be traceable back to the voter in e-voting. E-voting uses computers, mobile devices, and internet to accomplish the whole vote procedure, which is a research field of cryptography with the basic of encryption and signature algorithms [12, 15, 16].

How to design a more secure and practical e-voting system has becoming a popular topic in the area of industry and information security [17]. In order to improve the security and anonymity of the e-voting, we present techniques to exploit blockchain to build new e-voting systems.

1.2 Our contributions

Blockchain is based on distributed ledger technology (DLT) and invented by Satoshi Nakamoto in 2008 [18–22]. It synchronizes the ledgers replicated among multiple nodes by using community validation, which is adopted to serve as the public transaction ledger of the crypto-currency Bitcoin [23–37]. We present techniques to exploit blockchain to improve the security of e-voting. First, we design a synchronized model of voting records based on DLT to avoid forgery of votes. Second, we design a user credential model based on elliptic curve cryptography (ECC) to provide authentication and non-repudiation. Third, we design a withdrawal model that allows voters to change their vote before a preset deadline. By integrating the above designs, we propose a blockchain-based e-voting scheme, which meets the essential requirements of e-voting process.

To prove and verify the scheme, a blockchain-based e-voting system for multiple candidates has been designed on Linux platforms. The system involves electronic voting theory, cryptography, and software engineering theory. The implementation result shows that it is a practical and secure e-voting system, which solves the problem on forgery of votes. The blockchain-based system can be applied to a variety of voting applications directly.

1.3 Organization

Section 2 introduces the e-voting scheme based on blockchain briefly. Section 3 proposes an e-voting scheme based on blockchain. Section 4 presents efficient implementations and results are evaluated and discussed. Section 5 summarizes our design.

2 Method

The study of this paper originates from a need to design a more secure and practical e-voting system, since it has becoming a popular topic in the area of industry and information security. Blockchain is based on DLT and invented by Satoshi Nakamoto in 2008. Blockchain is a growing list of blocks. Each block except the first block stores its previous block's hash value. It synchronizes the ledgers replicated among multiple nodes by using community validation, which is adopted to serve as the public transaction ledger of the crypto-currency Bitcoin.

We present techniques to exploit blockchain to improve the security of e-voting. Compared with the original blockchain, the improvements are as follows:

(1) We design a synchronized model of voting records based on DLT to avoid forgery of votes.

(2) We design a user credential model based on ECC to provide authentication and non-repudiation.

(3) We design a withdrawal model that allows voters to change their vote before a preset deadline.

By integrating the above designs, we propose a blockchain-based e-voting scheme, which meets the essential requirements of e-voting process.

We illustrate the blockchain-based e-voting scheme as follows:

(1) The blockchain-based e-voting scheme is public, distributed, and decentralized. It can record votes from voters across many mobile devices and computers.

(2) The blockchain-based e-voting scheme allows the voters to audit and verify the votes inexpensively.

(3) The database of votes is managed autonomously and is using a distributed server of timestamp on a peer-to-peer network.

(4) Voting on blockchain is a workflow where voters' regarding data security is marginal, which removes the characteristic of infinite reproducibility from e-voting.

Based on the illustration above, the scheme is depicted in Fig. 1 and is designed as follows:

(1) Voting blockchain: it is a growing list of voting blocks.

(2) Voters: the person who casts a ballot for his/her chosen candidate is voter. The voter can vote or withdraw a vote.

(3) Voting office: it is the organization of voting. It can query the public key of the voter, verify the votes, and query the votes.

(4) Public key infrastructure (PKI): it is a set of procedures that manage public-key encryption.

(5) Vote database: it is a database according to the statistics of votes that updated by voting office.

(6) Miners: the responsibility of miners is to deal with accepted votes and adding them to the public voting blockchain.

3 A blockchain-based e-voting scheme

3.1 Overview of the blockchain-based e-voting scheme

We design a blockchain-based scheme for secure e-voting. First, a synchronized model of voting records based on DLT is designed to avoid forgery of votes. Second, a user

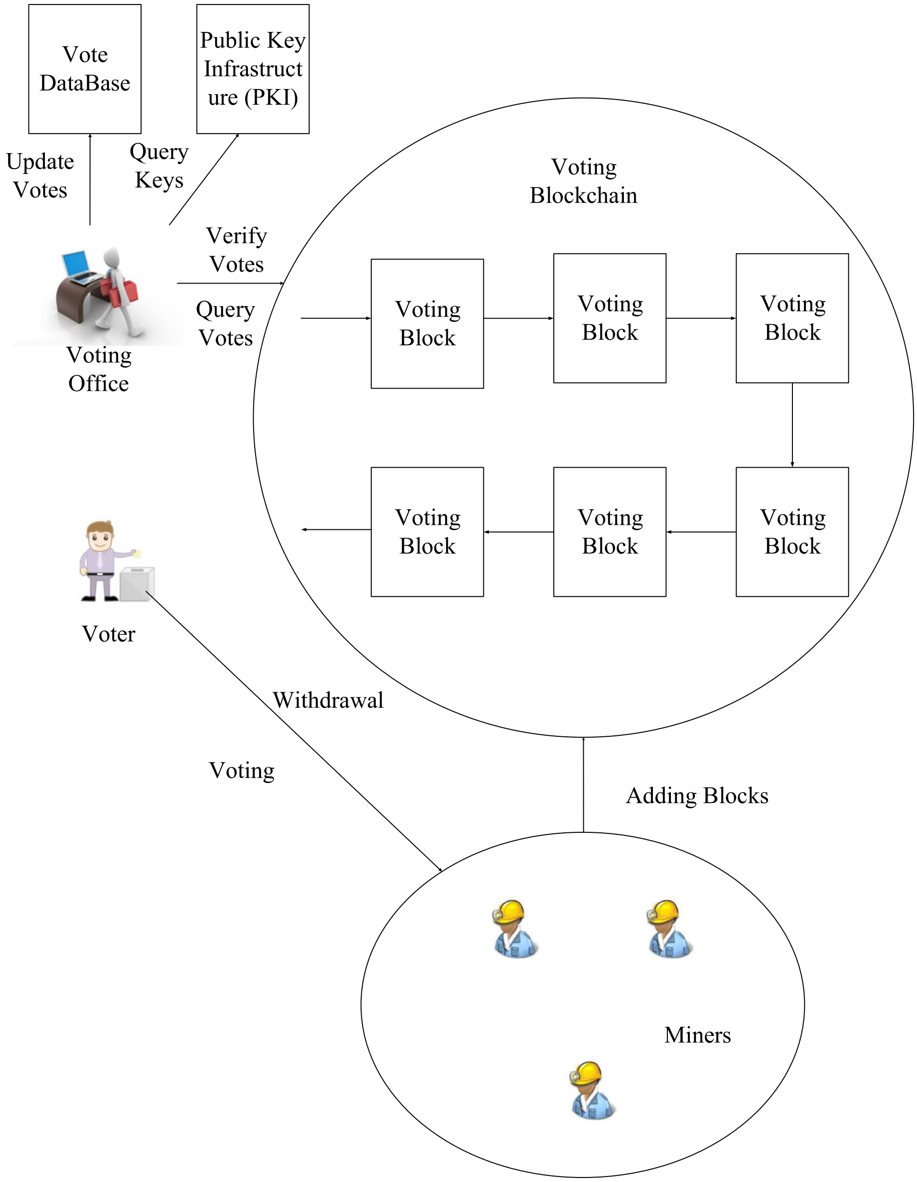

Fig. 1 Blockchain-based e-voting scheme

credential model based on ECC is designed to provide authentication and non-repudiation. Third, a withdrawal model is designed that allows voters to change their vote before a preset deadline.

We introduce the block definition, user credential based on ECC, computing the hash value based on SHA-256 and mining and generation of voting blocks in the following.

3.2 Block definition

The blockchain for e-voting is designed based on DLT. It is a list of blocks, which is depicted in Fig. 2. It can be observed from Fig. 2 that the blockchain for e-voting is represented as a series of voting blocks chained to each other in a sequential manner. The first block is called genesis block.

Each block contains voter's ID, vote, voter's signature, timestamp, and digest(hash) of the previous block, which is depicted in Fig. 3 and illustrated as follows:

(1) Voter's ID: the person who casts a ballot for his/her chosen candidate is voter. Voter's ID is randomly assigned to a person who has the right to vote.

(2) Vote: voting ballot is to state a ballot to voter's chosen candidate.

(3) Voter's signature: voting ballot is marked by the voters as a signature so that no one else can find out for whom a citizen is voting. Voter uses his/her private key

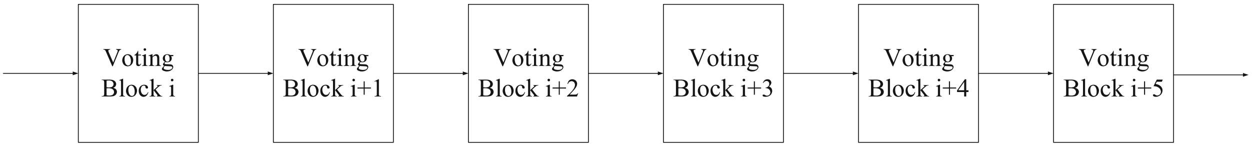

Fig. 2 The blockchain for e-voting

to sign the hash of the vote, which is used to judge the authenticity of vote.

(4) Timestamp: timestamp is used to record submission time of the block. The block with a higher value of signature is selected over others when they have the same timestamp.

(5) Hash of the previous block: we use SHA-256 algorithm to compute the hash value of the previous block.

Thus, the blockchain-based e-voting scheme is non-repudiation and is resistant to modification of the data.

3.3 User credential based on ECC

We design a user credential model based on ECC to provide authentication and non-repudiation. The main improvement is as follows:

(1) Voting ballot is marked by the voters as a signature so that no one else can find out for whom a citizen is voting.

(2) Voter uses his/her private key to sign the hash of the vote by using ECDSA signature, which is used to judge the authenticity of the vote.

We use O to denote the identity element and use G to denote the elliptic curve base point. n is the integer order in $n \times G = O$. L_n is used to denote the bit length of n.

For a voter to sign his/her vote v, he/she must create private and public keys. The private key is a integer, which is denoted by d_A. The public key is a curve point $Q_A = d_A \times G$, where × is elliptic cure point multiplication.

The signing process is depicted in Fig. 4 and illustrated as follows:

(1) Compute $v' = HASH(v)$.

(2) Suppose that z be the L_n leftmost bits of v'.

(3) Select a random integer k from $[1, n-1]$.

(4) Compute $(x_1, y_1) = k \times G$.

(5) Compute $r = x_1 \ mod \ n$. If $r == 0$, return to (3).

(6) Compute $s = k^{-1}(v' + rd_A) \ mod \ n$. If $s == 0$, return to (3).

(7) The signature of the vote is (r, s).

3.4 Compute the hash value based on SHA-256

We compute the hash value based on SHA-256. By comparing the hash value to a expected hash value, the data's integrity can be determined.

SHA-256 is frequently used in the e-voting scheme for compute the hash value, which is depicted in Fig. 5 and illustrated as follows:

(1) The message is denoted by m with binary expression.

(2) Pad m with 100...000 sequence and the length of m with 64-bit expression, i.e., $m' = \text{pad}(m)$.

(3) m' is broken into 512-bit chunks, i.e., $M^{(1)}, M^{(2)}$, ..., $M^{(N)}$.

(4) 64 constants are used, which are denoted by W_0, W_1, ..., W_{63}, respectively.

(5) Eight working variables labeled $A = 0x6A09E667$, $B = 0xBB67AE85$, $C = 0x3C6EF372$, $D = 0xA54FF53A$, $E = 0x510E527F$, $F = 0x9B05688C$, $G = 0x1F83D9AB$, and $H = 0x5BE0CD19$ are used as the initial hash value.

(6) Compute the 64-cycle cryptographic iterative computation for the first chunk, i.e., $M^{(1)}$. Repeat the iterative

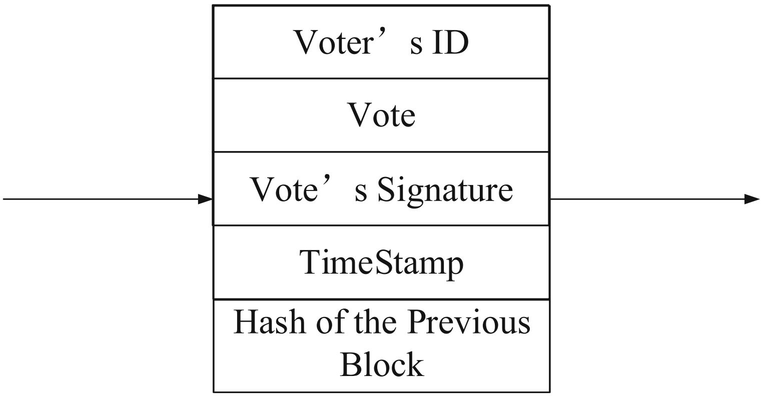

Fig. 3 Voting block

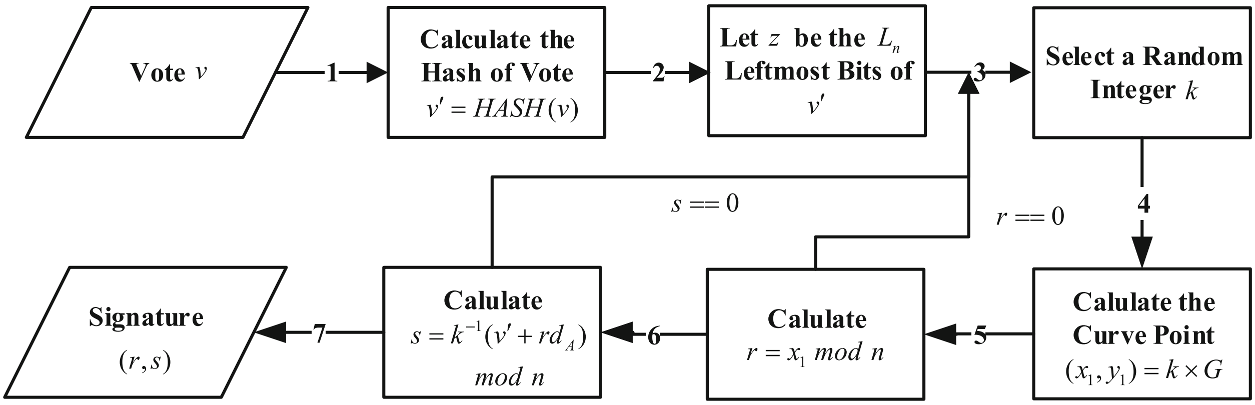
Vote v
1
Calculate the Hash of Vote $v' = HASH(v)$
2
Let z be the L_n Leftmost Bits of v'
3
Select a Random Integer k
4
$s == 0$
$r == 0$
Calulate the Curve Point $(x_1, y_1) = k \times G$
5
Calulate $r = x_1 \ mod \ n$
6
Calulate $s = k^{-1}(v' + rd_A) \ mod \ n$
7
Signature (r, s)

Fig. 4 Sign the hash of the vote

computation for the next chunk based on the result for the last chunk.

(7) The result of the last iterative computation is the hash.

3.5 Mining and generation of voting blocks

All votes in the blockchain are cryptographically linked block by block. Many secure hash algorithms can be applied to solve the problem of condensing the message in the current block to produce a message digest, such as SHA-256.

New block is generated by users from the P2P network. The new block generation is based on PoW algorithm. When a new vote is submitted and verified, miner generates a new block with the information of vote and broadcasts the new blocks to the network. If new blocks have the same timestamp, the block with a higher value of signature is selected over others.

4 Results

In this section, we illustrate the scheme and implement th e system on Linux platform. We use Python programming language for source codes. The Linux platform for implementation is Ubuntu. Each block contains voter's ID, vote, voter's signature, timestamp, and hash of the previous block. Blockchain-based e-voting system for multiple candidates has been designed on Linux platforms. The implementation result shows that it is a practical and secure e-voting system, which solves the problem on forgery of votes during e-voting.

Compared with other e-voting systems, blockchain-based e-voting system is more secure and anonymous.

(1) Anonymous: each user in blockchain-based e-voting system uses an ID instead of his real identity and the system is decentralized without a third party. Thus, the privacy of the users is protected.

(2) Security: we design a synchronized model of voting records based on DLT to avoid forgery of votes. Thus, it is very difficult to forge votes.

(3) Non-repudiation: we design a user credential model based on ECC to provide authentication and non-repudiation. Thus, it is very difficult to deny a vote.

(4) Withdrawable: we design a withdrawal model that allows voters to change their vote before a preset

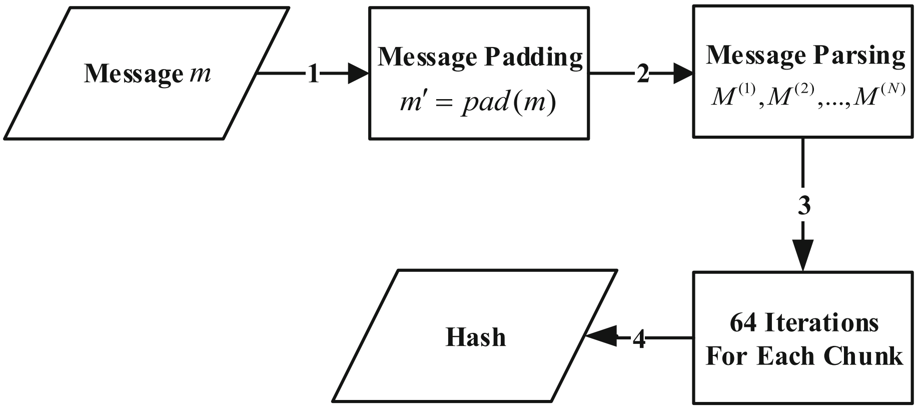
Message m
1
Message Padding $m' = pad(m)$
2
Message Parsing $M^{(1)}, M^{(2)}, ..., M^{(N)}$
3
64 Iterations For Each Chunk
4
Hash

Fig. 5 Compute the hash value based on SHA-256

deadline. It meets the essential requirements of e-voting process.

4.1 Initialization

At this stage, initialization of the e-voting system is depicted in Fig. 6 and illustrated as follows:

(1) Every voter is issued a credential by voting office in a secure way, which includes a unique identity ID and a list of candidates.

(2) Every voter generates private key randomly.

(3) Every voter computes the public key based on the private key.

(4) Voters keep their private keys.

(5) Voters send their public keys to the PKI in a secure way.

(6) Miners are elected randomly.

(7) The first block is generated.

4.2 Voting

The voter can vote in accordance with the list of candidate or vote for any other persons he/her prefers. Generally, the vote is public, thus the information of vote is not encrypted.

The voting process is depicted in Fig. 7 and illustrated as follows:

(1) Voter uses SHA-256 to generate the hash value of $H = \text{Hash(ID + Vote + Timestamp)}$.

(2) Voter uses his/her private key to generate a signature S of the hash value H.

(3) Voter sends ID, Vote, Timestamp, S to the miner.

(4) The miner obtains the public key from the PKI according to voter's ID.

(5) The miner uses SHA-256 to generate the hash value of $H = \text{Hash(ID+Vote+Timestamp)}$.

(6) The miner uses the public key to verify S and get H'.

(7) The miner compares H and H'. If H and H' are the same, S is accepted. Otherwise, it is rejected.

(8) The miner queries and verifies that voter has the right to vote or enough votes.

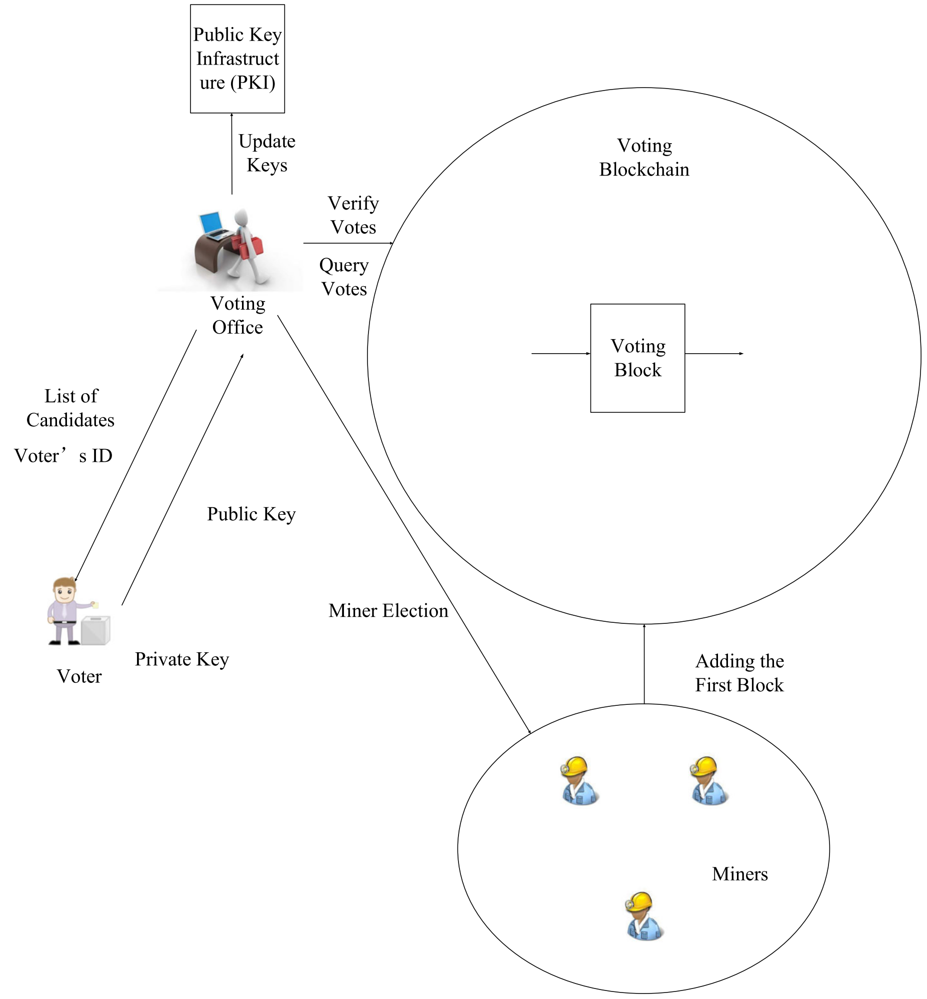

Fig. 6 Initialization of the e-voting system

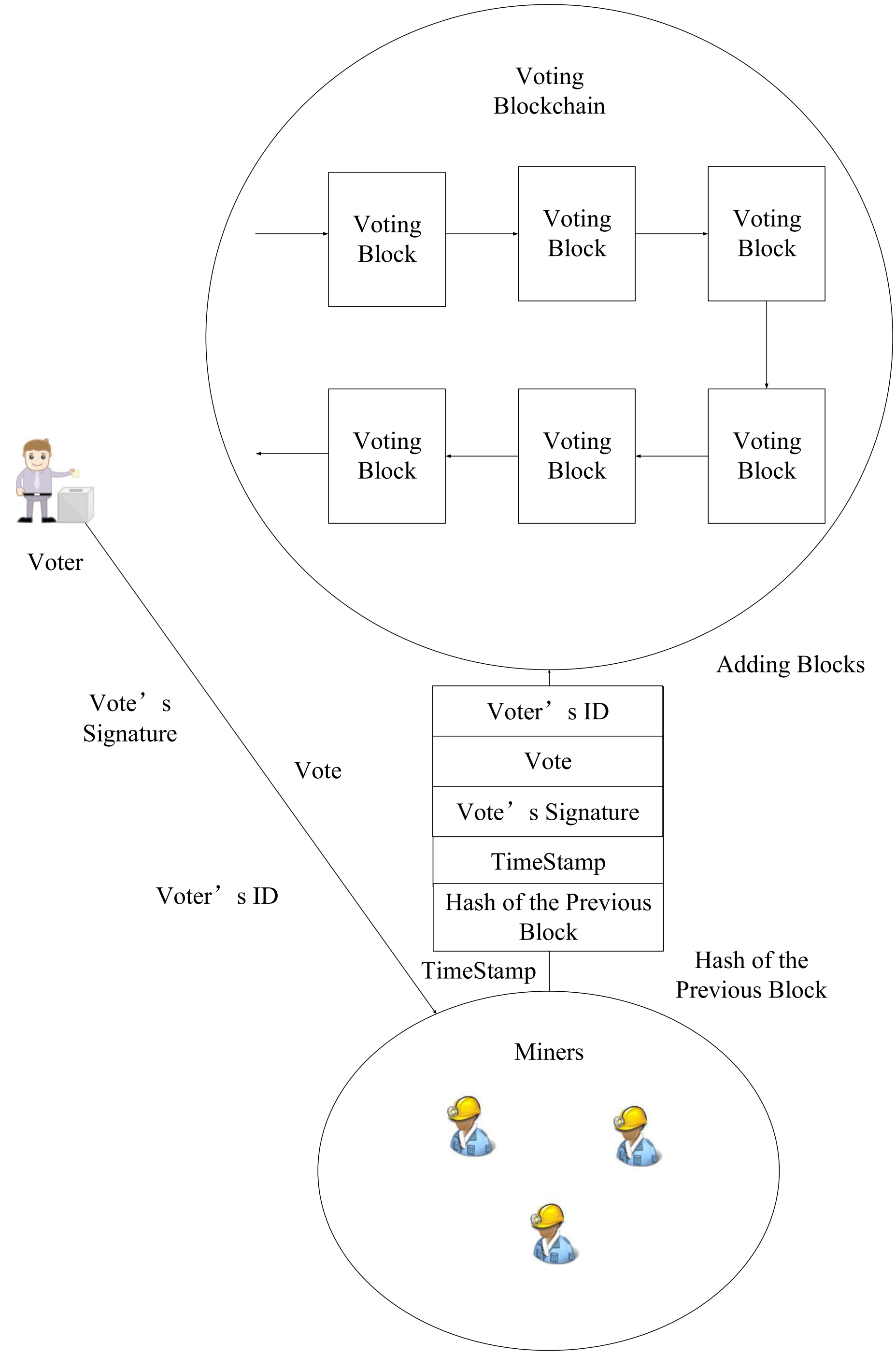

Fig. 7 Voting

(9) The miner generates a new block with the previous block’s hash value and the information of vote and adds it to the blockchain.

Besides, the voter can withdraw his/her vote before a preset deadline. The withdrawal process is similar to the voting process.

5 Discussion

We propose a blockchain-based e-voting scheme, which meets the essential requirements of e-voting process. All votes in the blockchain is cryptographically linked block by block. The block with a higher value of signature is selected over others when they have the same timestamp.

The voter can vote in accordance with the list of candidate or vote for any other persons he/her prefers. Generally, the vote is public, thus the information of vote is not encrypted. The blockchain-based e-voting system can be applied to a variety of voting situations and other applications. Although blockchain is a secure technology, it uses ECC public key cryptography, which is not secure to quantum computer attacks. Thus, blockchain with countermeasures to quantum computer attacks is a future research topic in this area.

Abbreviations

DLT: Distributed ledger technology; E-voting: Electronic voting; ECC: Elliptic curve cryptography; ECDSA: Elliptic curve digital signature algorithm; PKI: Public key infrastructure; SHA: Secure hash algorithm

Acknowledgements

The author would like to express his cordial thanks to the section editor in charge and the respected reviewers for their time, accurate review of our manuscript, and their invaluable comments on this paper.

Funding

The authors acknowledge Natural Science Foundation of Guangdong Province, China (no. 2018A030310030), Foundation for Distinguished Young Talents in Higher Education of Guangdong, China (no. 2017GkQNCX059), Special funds for Shenzhen Strategic Emerging Industries and Future Industrial Development (no. 20170502142224600), Shenzhen Science and Technology Program under Grant (no. JCYJ20170306144219159), and Science and Technology Program of Shenzhen Polytechnic (no. 601722K20018).

Availability of data and materials

Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Authors' contributions

HY proposed the main idea, designed and implemented the architecture, and drafted the manuscript. He read and approved the final manuscript.

Authors' information

Haibo Yi received the bachelor degree in computer science from Beijing Jiaotong University, China, in 2009, and the PhD. from South China University of Technology, China, in 2015. Since 2015, he has been with School of Computer Engineering of Shenzhen Polytechnic as a lecturer. He has published over 20 technical papers. His main research areas are information security, cloud computing, and big data. He is a member of Chinese Association for Cryptologic Research.

Competing interests

The author declares that he has no financial and personal relationships with other people or organizations that can inappropriately influence his work, and there is no professional or other personal interest of any nature or kind in any product, service, and/or company that could be construed as influencing the position presented in, or the review of, the manuscript entitled.

Publisher's Note

Received: 19 February 2019 Accepted: 15 May 2019
Published online: 28 May 2019

References

1. Y. Xie, Who Overreports Voting?J J. Am. Polit. Sci. Rev. **80**, 613–624 (2017)
2. T. Green, O. Sarrasin, R. Baur, et al., From stigmatized immigrants to radical right voting: a multilevel study on the role of threat and contact[J]. Polit. Psychol. **37**(4), 1–22 (2016)
3. B. Los, P. Mccann, J. Springford, et al., The mismatch between local voting and the local economic consequences of Brexit[J]. Reg. Stud. **51**(5), 1–14 (2017)
4. S. Eijffinger, R. Mahieu, L. Raes, Inferring hawks and doves from voting records[J]. Eur. J. Polit. Econ. Elsevier. **51**(C), 107–120 (2017)
5. T. Rogers, P. Green, J. Ternovski, et al., Social pressure and voting: a field experiment conducted in a high-salience election[J]. Elect. Stud. **46**, 87–100 (2017)
6. E. Aljarrah, H. Elrehail, B. Aababneh, E-voting in Jordan: assessing readiness and developing a system[J]. Comput. Hum. Behav. **63**, 860-867 (2016)
7. C. Burton, C. Culnane, S. Schneider, vVote: verifiable electronic voting in practice[J]. IEEE Secur. & Priv. **14**(4), 64-73 (2016)
8. J. Cao, Y. Ding, L. Jiang, et al., A new proxy electronic voting scheme achieved by six-particle entangled states[J]. Int. J. Theor. Phys. **57**(3), 674-681 (2018)
9. L. Zhang, Z. Zhang, C. Xie, A Choreographed distributed electronic voting scheme[J]. Int. J. Theor. Phys. **57**(9), 1-11 (2018)
10. J. Cao, Y. Ding, F. Yu, et al., A Electronic voting scheme achieved by using quantum proxy signature[J]. Int. J. Theor. Phys. **55**(9), 1-8 (2016)
11. A. Kiayias, T. Zacharias, B. Zhang, An efficient E2E verifiable E-voting system without setup assumptions. IEEE Secur. & Priv. **15**(3), 14–23 (2017)
12. E. Ahene, C. Jin, F. Li, Certificateless deniably authenticated encryption and its application to e-voting system[J]. Telecommun. Syst. **70**, 1-18 (2018)
13. N. Kshetri, J. Voas, Blockchain-Enabled E-Voting. IEEE Softw. **35**, 95–99 (2018). https://doi.org/10.1109/MS.2018.2801546
14. M. Shakiba, A. Doostari, M. Mohammadpourfard, ESIV: an end-to-end secure internet voting system[J]. Electron. Commer. Res., 1-32 (2017)
15. G. Madhavan, C. Phelps, R. Rappuoli, Compare voting systems to improve them[J]. Nature. **541**(7636), 151 (2017)
16. S. Polyakovskiy, R. Berghammer, F. Neumann, Solving hard control problems in voting systems via integer programming[J]. Eur. J. Oper. Res. **250**(1), 204-213 (2016)
17. Q. Liu, H. Zhang, Weighted voting system with unreliable links[J]. IEEE Trans. Reliab. **66**(2), 339-350 (2017)
18. M. Nofer, P. Gomber, O. Hinz, et al., Blockchain[J]. Bus. & Inf. Syst. Eng. **59**(3), 183–187 (2017)
19. N. Kshetri, Can blockchain strengthen the Internet of things?J IT Prof. **19**(4), 68–72 (2017)
20. A. Dorri, M. Steger, S. Kanhere, et al., Blockchain: a distributed solution to automotive security and privacy[J]. IEEE Commun. Mag. **55**(12), 119-125 (2017)
21. D. Kraft, Difficulty control for blockchain-based consensus systems[J]. Peer-to-Peer Netw. Appl. **9**(2), 397-413 (2016)
22. J. Sikorski, J. Haughton, M. Kraft, Blockchain technology in the chemical industry: Machine-to-machine electricity market[J]. Appl. Energy. **195**, 234–246 (2017)
23. B. Lee, H. Lee, Blockchain-based secure firmware update for embedded devices in an Internet of Things environment[J]. J. Supercomput. **73**(3), 1-16 (2016)
24. Y. Zhang, J. Wen, The IoT electric business model: Using blockchain technology for the internet of things[J]. Peer-to-Peer Netw. Appl. **10**(4), 1-12 (2017)
25. X. Yue, H. Wang, D. Jin, et al., Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control[J]. J. Med. Syst. **40**(10), 218 (2016)
26. D. Pierro, What Is the Blockchain?J Comput. Sci. & Eng. **19**(5), 92–95 (2017)
27. H. Subramanian, Decentralized blockchain-based electronic marketplaces[J]. Commun. ACM. **61**(1), 78–84 (2017)
28. T. Aste, P. Tasca, D. Matteo, Blockchain technologies: the foreseeable impact on society and industry[J]. Computer. **50**(9), 18-28 (2017)
29. C. Pop, T. Cioara, M. Antal, et al., Blockchain based decentralized management of demand response programs in smart energy grids:[J]. Sensors. **18**(1), 162 (2018)
30. I. Eyal, Blockchain technology: transforming libertarian cryptocurrency dreams to finance and banking realities[J]. Computer. **50**(9), 38-49 (2017)
31. E. Peck, Blockchain world - Do you need a blockchain?This chart will tell you if the technology can solve your problem[J]. IEEE Spectr. **54**(10), 38–60 (2017)
32. P. Fairley, Blockchain world - Feeding the blockchain beast if bitcoin ever does go mainstream, the electricity needed to sustain it will be enormous[J]. IEEE Spectr. **54**(10), 36–59 (2017)

33. M. Singh, S. Kim, Intelligent vehicle-trust point: reward based intelligent vehicle communication using blockchain[J]. Opt. Eng. **33**(1), 701-709 (2017)
34. E. Peck, K. Moore, The blossoming of the blockchain[J]. IEEE Spectr. **54**(10), 24–25 (2017)
35. R. Beck, M. Avital, M. Rossi, et al., Blockchain technology in business and information systems research[J]. Bus. & Inf. Syst. Eng. **59**(6), 1-4 (2017)
36. Y. Chen, S. Ding, Z. Xu, et al., Blockchain-based medical records secure storage and medical service framework[J]. J. Med. Syst. **43**(1), 5 (2018)
37. M. Li, J. Weng, A. Yang, W. Lu, Y. Zhang, L. Hou, L. Jia-Nan, Y. Xiang, R. H. Deng, CrowdBC: A Blockchain-Based Decentralized Framework for Crowdsourcing. IEEE Trans. Parallel Distrib. Syst., 1 (2018). https://doi.org/10.1109/TPDS.2018.2881735