基于区块链的电子投票选举系统研究分析

张昕伟[1],张 华[2],郭肖旺[1],张 雯[3]
(1.中国电子信息产业集团有限公司第六研究所,北京 100083;
2.北京航天飞行控制中心,北京 102206;3.IThinking Inc,北京 100083)

摘 要:区块链通过分布式公式算法实现去中心化信任,其核心是一个开放的、可编程的分布式数据库,该数据库是全球性的。区块链技术不仅是用在金融交易上,还可以用于记录所有有价值的东西,如财务账目、医疗过程、出生证明、保险理赔、投票等任何可用代码来表示的东西。分析了区块链技术应用于电子投票系统的可能性,分析采用区块链技术来构建新型电子投票选举系统的优缺点,在此基础上,给出了基于区块链技术的投票选举系统的框架需求分析,并提出了系统架构和设计方案,解决了电子投票选举系统中有关欺诈、欺骗选票的问题,最后给出了区块链在电子投票选举系统中的研究可行性结论,为基于区块链的系统设计与应用提供了新思路。

关键词:电子投票;区块链;去中心化
中图分类号:TP309.2 **文献标识码**:A **DOI**:10.16157/j.issn.0258-7998.173731

中文引用格式:张昕伟,张华,郭肖旺,等.基于区块链的电子投票选举系统研究分析[J].电子技术应用,2017,43(11):132-135.
英文引用格式:Zhang Xinwei,Zhang Hua,Guo Xiaowang,et al. Research and analysis of electronic voting system based on blockchain[J].Application of Electronic Technique,2017,43(11):132-135.

Research and analysis of electronic voting system based on blockchain

Zhang Xinwei[1],Zhang Hua[2],Guo Xiaowang[1],Zhang Wen[3]
(1.The 6th Research Institute of China Electronics Corporation,Beijing 100083,China;
2.Beijing Aerospace Control Center,Beijing 102206,China;3.IThinking Inc,Beijing 100083,China)

Abstract:The blockchain is distributed through a distributed algorithm, to realize decentralized trust. The core is an open, programmable, distributed database which is global. Blockchain technology is not only used in financial transactions, it can also be used to record all valuable things which can be represented in code, such as financial accounts, medical procedures, birth certificate, insurance claims, vote and so on. This paper analyzes the possibility of the application of blockchain technology to electronic voting, and the advantages and disadvantages of using blockchain technology to construct new electronic voting system. The system architecture and design scheme are presented. This paper solves the problem of fraudulent ballot in electronic voting system. Finally, the feasibility of blockchain in electronic voting system is given. This paper provides a new idea for system design and application based on blockchain.

Key words:electronic voting;blockchain;decentralization

0 引言

在电子投票选举系统的安全实用性研究方面,基于密码技术的投票方案是最常见的。CHAUM D 提出了第一个密码学意义上的电子投票选举方案[1],提出了在公钥密码体制结合 Mix 机制来实现匿名通信的方案,但是该方案要求所有投票者必须合作,其协议效率和可行性较低。在此方案的基础上,一系列采用 Mix-net 机制的电子投票系统[2-3]研究出现了,在协议的安全性以及可靠性方面有所提高[4]。这类方案要求所有 Mix 服务器在处理选票过程中无法篡改选票,其无法篡改的证明依赖于大量的证明计算,协议运行效率较低。

区块链技术最先在比特币白皮书中,以“工作量证明链(Proof-of-work Chain)”的形式提出。区块链本质上是一个去中心化的数据库,作为比特币的底层技术,区块链通过分布式公式算法实现去中心化,其核心是一个开放的、可编程的分布式数据库,该数据库是全球性的。区块链技术不仅是用在金融交易上,还可以用于记录所有有价值的东西,应用领域十分广泛,如财务账目、医疗过程、出生证明、保险理赔、投票等任何可用代码来表示的东西。针对现有方案存在的投票效率低下、重复投票、欺诈选票以及安全性等问题,本文在区块链技术的基础上提出了基于区块链的投票选举系统,通过在投票过程

中引入区块链技术，每个投票数据节点都可以验证投票账本的内容和构造历史的真实性和完整性，确保投票记录是可靠的、没有被篡改的，相当于提高了系统的可追责性，降低了系统的信任风险。防止有不合法投票人欺诈选票或者其他机构破坏投票过程，干扰投票结果。此外，每个投票人都可以看到投票结果，通过匿名算法，保证投票人的隐私，同时又不损害投票的公开公正性。

1 电子投票选举系统安全性要求

电子投票选举系统在安全性方面的要求包括：

(1)合法用户参与性，不合法用户是不能进行投票的；

(2)投票中心不能拒绝合法选票；

(3)合法投票者只能进行一次投票；

(4)投票过程的不可破坏性：投票过程不能被恶意攻击者的不合法或不诚实行为破坏；

(5)选票内容的保密性，对选票内容进行加密，防止被恶意窃取后泄露选票内容，影响投票过程；

(6)投票者可以验证自己的选票是否正确有效，且被正确统计，保证选举结果的正确性和合法性；

(7)投票者身份隐藏，其他用户不可见；

(8)投票过程需简单高效，无需用户进行复杂学习；

(9)系统可支持多个候选人。

2 区块链技术适用性分析

区块链是比特币的基础技术，每个数据节点无需相互信任，在时间戳、数据加密等技术基础上实现去中心化、不可篡改和自治性等特性。系统的每个参与者都能够知晓系统的运行规则，又实现了开源透明的特性。区块链的这些技术性特点解决了现在中心化系统所存在的成本高、效率低、安全性低等问题。

在基于区块链的网络结构中，每个节点都共享系统的所有信息，不存在中心节点，每个数据节点都可以验证账本的真实内容以及历史记录，保证了数据的完整性，确保数据是没有经过篡改的、可靠的。区块链的自治性决定了节点在区块链网络中，会自主监听其他节点发生的数据信息，并随时进行共享，整个流程都是区块链网络自主实现的，不需要人工进行干预。区块链网络中的每个节点都是整个网络的维护者，网络中没有节点拥有绝对优先的权力。这种去中心化的、分布式的网络结构适用于投票选举系统，投票中心不需要专门维护和管理整理投票系统和网络，投票系统的每个用户共同维护和管理整个系统的信息，并可共享数据信息，保证了网络的透明性，也防止了恶意投票或篡改欺诈、欺骗选票的作弊行为。

由于区块链的记录是可追溯的，且不可抵赖，所有的投票记录都会被全网记录，任何投票用户的投票记录都会被记录到区块中，每一次新的投票记录都会被共享到全网所有节点，系统中所有的节点都可以收到投票记录，并把收到的记录加入区块中，在区块链算法中，始终将长度最长的区块链认为是正确的链，链会随着投票记录的增加不断变长。区块链使用了时间戳，可以提供时间上的证明，如果有欺诈选票或篡改选票的行为，将可以在区块链中回溯记录查询发生篡改或欺诈选票的时间和数据。

3 基于区块链的电子投票选举系统设计

基于区块链的电子投票选举系统拟采用 C/S 架构，本文根据区块链中去中心化、节点数据共享、节点自治性等特点，分析电子投票选举系统，要求每个投票者平等地参与投票，投票完毕后生成投票凭证报文，报文验证完毕后，系统向所有节点广播投票记录消息，所有收到消息的节点更新自己的区块链，存储投票记录，共同维护系统投票历史记录信息。

3.1 系统功能说明

电子投票选举系统的主要功能是记录投票者的投票信息，记录投票过程并生成投票凭证，将投票凭证存入本地数据结构。该结构中记录了投票时间、投票数据等信息。投票记录加密后共享给系统所有节点，当网络中的大部分节点甚至所有节点认为该投票记录有效时，系统记录票数，并将投票凭证记录到区块中，然后系统公布候选者票数，整个过程中投票者的信息都是隐藏的。每个投票系统用户节点都可以收到投票凭证，保存到区块中，在区块链算法中，始终将长度最长的区块链认为是正确的链，链会随着投票记录的增加不断变长。投票凭证的传输采用了签名认证，系统会定时检测区块链文件，确保文件未被篡改。区块链文件表示记录投票凭证的账本。系统还提供了两个辅助功能来方便用户了解投票功能和查看当前投票系统公开选票记录。两个辅助功能包括：(1)获取投票信息功能，在用户完成投票后，系统自动生成投票凭证，并在本地保存；(2)查看投票历史记录，所有用户都可以在公共信息页上查看所有候选者的选票情况。

3.2 功能设计

系统按照功能可以分为 3 个模块：投票模块、区块链管理模块、投票凭证管理模块。在本系统中，节点指的是位于系统中、可以被用户进行投票使用的 PC 或者手机 APP，这些节点可以互相通信，并且在节点中可以存储区块链信息，并提供区块链系统的维护功能，节点内部的工作对于投票用户来说是不可见的。图 1 描述了系统的总体功能划分。

投票模块主要承担投票者用户选择候选者进行投票的功能，并达到投票去中心化、去信任的目标。在该模块中，用户选择候选者，选择投票，点击确定，生成投票记录，即投票凭证报文。为保证投票凭证在传输模块传输过程中不被篡改，系统根据区块链中最后一条记录的散列值，使用私钥签名，并把投票记录、签名和公钥一起封装成投票凭证报文，该报文被发送给候选者节点。候选者节点接收投票记录凭证，利用公钥验证其签名，若签名正确，则增加此候选者的票数。此过程对于候选者

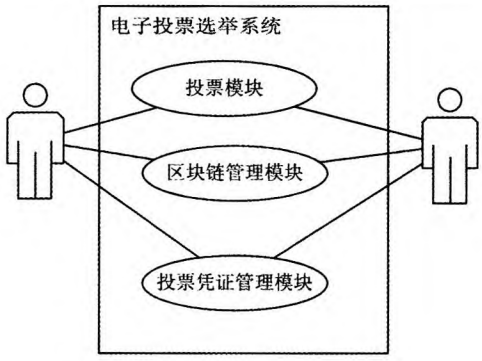

图 1 电子投票选举系统用例图

节点来说，可见的只是选票的增加，并不会显示投票者的信息，签名验证通过后，系统封装确认消息报文，并共享给所有节点，收到消息的节点更新自己本身的区块链。

区块链管理模块主要用于管理分布式区块链账本，及时更新区块链文件，提供查询详细投票记录的功能。及时更新区块链文件主要是指 Merkle 根数据的定点更新，系统每隔一定时间，会向所有节点共享区块链 Merkle 根的数据，收到消息的节点，比较本地 Merkle 根数据是否一致，以此来判断系统是否在安全状态下，是否已遭受恶意攻击或数据被篡改。

投票凭证管理模块用于管理投票者投票产生的投票记录数据，按照加密协议，生成投票凭证，并把投票凭证报文存储至本地存储模块中。

3.2.1 投票模块功能

投票模块主要实现投票并生成投票记录和投票凭证报文，传输投票记录。该模块包括投票凭证生成、投票凭证传输、投票凭证校验、投票凭证确认等 4 个功能，如图 2 所示。

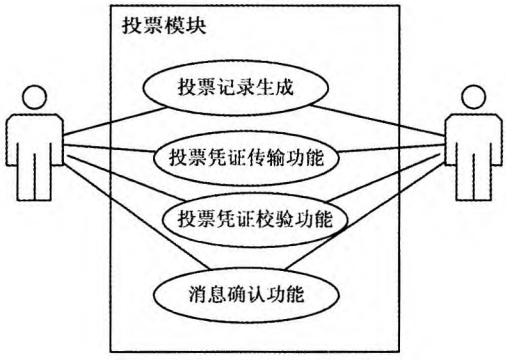

图 2 投票模块用例图

投票功能分析如下：

(1)投票记录生成：用户选择要进行投票的候选人，点击投票，确定投票信息，则系统生成投票记录，记录用户 ID、用户投票时间、候选者 ID，并加密生成投票凭证报文。

(2)投票凭证传输功能：系统将生成的投票凭证报文发送出去。系统根据区块链中最后一条记录的散列值，使用私钥签名。将投票记录、签名和公钥封装到消息中，发送给候选者节点。消息中包含候选者用户 ID、投票凭证报文、投票者用户签名、公钥等信息，便于系统校验消息正确性。

(3)投票凭证校验：候选者节点接收到消息后，需要进行如下校验过程：首先判断消息的发送方是否系统中合法节点，若不是则丢弃消息；若是，则取出本地区块文件的 Hash 散列值以及消息中的公钥检验签名，进行签名认证，返回校验结果，若认证成功，则确认消息传输过程中没有被篡改，若认证失败，则丢弃消息。

(4)消息确认功能：上一步中若消息校验成功，则确认消息，并对消息进行系统签名，共享给所有节点，通知所有节点更新区块链文件。

3.2.2 区块链管理模块功能

区块连管理模块主要实现维护区块链文件安全可靠及完整性，实现区块链文件更新，及向全网节点共享更新区块链功能。本模块还提供投票历史记录查询功能。本模块的用例图如图 3 所示。

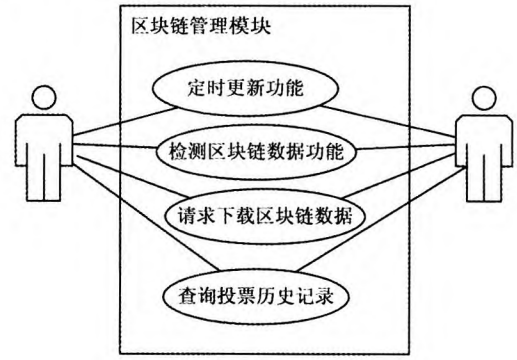

图 3 区块链管理模块用例图

区块链管理模块的功能说明：

(1)定时更新功能：定时向系统中所有节点共享区块链数据。

(2)检测区块链数据功能：检测功能用于检测区块链数据的正确性，在检测开始前，发送检测消息给所有节点，然后等待一定时间，在该事件间隔内接收其他节点回复的 Merkle 根数据，时间间隔默认是 5 s，在这个时间内接收的 Merkle 根数据个数上限设置为 100。接收完毕后，进行数据检测，于存储在本地的区块链数据进行对比，统计相同数据记录的数量，若与本地区块链 Merkle 根吻合的节点超过 50%，则认为本地区块链文件正确，否则删除本地区块中的数据。

(3)请求下载区块链数据：系统发现本地缺少区块链时，可以发送请求区块链数据消息给系统中所有节点，并等待一定时间间隔用于接收其他节点返回的数据，等待返回消息时间默认设置为 5 s，系统中其他节点接收

到请求会整理本节点的区块链文件，然后发送最新的区块链数据给请求节点。请求节点获取最先收到的消息，并更新本地区块链文件。

(4)查询投票历史记录：根据用户输入的查询时间范围，向所有节点发送查询请求消息，请求等待响应时间设置为5 s。等待5 s时间用于接收返回的消息，并根据时间顺序来排序收到的数据消息，生成历史记录。

3.2.3 投票凭证管理模块功能

投票凭证管理功能主要实现获取用户输入的投票数据，整理封装成投票记录报文，保存在本地。用例图如图4所示。

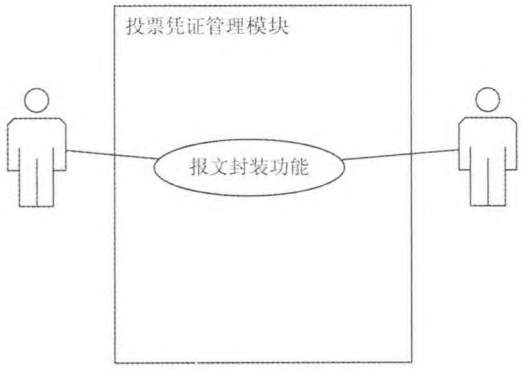

图4 投票凭证管理模块用例图

投票凭证管理模块的具体功能是报文封装功能：用户确认选票，确定投票后，系统自动对投票记录进行分析，采用私有加密协议，对投票数据封装成投票凭证报文，与生成时间戳一并保存。

4 结论

本文通过分析区块链的底层密码学原理以及应用场景，针对现有方案存在的投票效率低下、重复投票、欺诈选票以及安全性等问题，在区块链技术的基础上提出了基于区块链的投票选举系统。在投票过程中引入区块链技术，每个投票数据节点都可以验证投票账本的内容和构造历史的真实性和完整性，确保投票记录是可靠的、没有被篡改的，相当于提高了系统的可追责性，降低了系统的信任风险。本文重点提出了一种将区块链应用于投票选举系统的设计方案，提出了系统框架和模块功能划分实施方案。通过该方案，防止有不合法投票人欺诈选票或者其他机构破坏投票过程，干扰投票结果。此外，每个投票人都可以看到投票结果，通过匿名算法，保证投票人的隐私，同时又不损害投票的公开公正性。

参考文献

[1] CHAUM D，RYAN P Y A，SCHNEIDER S.A practical voter-verifiable election scheme[J].Lecture Notes in Computer Science，2005，10(3)：118-139.

[2] CICHON J，KLONWSKI M，KUTYLOWSKI M.Distributed verification of mixing-local forking proofs model[C].The 13th Australasian Conference of Information Security and Privacy 2008，LNCS 5107.Berlin：Springer-Verlag，2008：128-140.

[3] PANG L，SUN M H，LUO S S，et al.Full privacy preserving electronic voting scheme[J].The Journal of China Universities of Posts and Telecommunications，2012，19(4)：86-93.

[4] 张文芳，熊丹，王小敏.基于关联环签名的抗第三方欺诈安全电子投票方案[J].西南交通大学学报，2015，50(5)：905-911.

(收稿日期：2017-08-26)

作者简介：

张昕伟(1984-)，男，硕士，工程师，主要研究方向：网络信息安全。

张华(1972-)，女，高级工程师，主要研究方向：计算机网络、通信网络。

郭肖旺(1986-)，女，硕士，工程师，主要研究方向：工业控制与信息安全。

(上接第131页)

[12] 郭强.基于改进的A星算法和B样条函数的仿生机器鱼路径规划研究[D].天津：天津大学，2012.

[13] 张万绪，张向兰，李莹.基于改进粒子群算法的智能机器人路径规划[J].计算机应用，2014，34(2)：510-513.

[14] 吴斌.车辆路径问题的粒子群算法研究与应用[D].杭州：浙江工业大学，2008.

[15] 刘关俊.基于粒子群算法的移动机器人路径规划研究[D].长沙：中南大学，2007.

[16] 王亚春.移动机器人路径规划算法研究[D].天津：天津理工大学，2015.

[17] 禹建丽，成元洋之，Valeri.Kroumov.无人驾驶农用运输车路径规划研究[J].拖拉机与农用运输车，2002，29(4)：22-24.

[18] 卜新苹，苏虎，邹伟，等.基于复杂环境非均匀建模的蚁群路径规划[J].机器人，2016，38(3)：276-284.

(收稿日期：2016-11-30)

作者简介：

唐焱(1962-)，男，硕士生导师，教授，主要研究方向：车辆工程。