doi:10.3969/j.issn.1002-0802.2018.08.039

基于区块链的安全投票系统设计与实现 *

颜春辉，游 林

（杭州电子科技大学 通信工程学院，浙江 杭州 310018）

摘 要：随着社会的发展进步，许多应用场景都需要进行投票表决。针对当前电子投票系统中出现的问题，如投票数据不够公开透明且容易被篡改伪造，用户的私密信息存在被泄露的风险，选民无法验证投票结果等，提出了一种基于区块链智能合约技术的安全多候选人投票系统。系统通过智能合约自动执行机制取代传统的可信第三方计票机构来实现自我计票，并在系统中加入两轮零知识证明协议，有效确保投票者的身份合法性，同时保护选票内容的隐私性，而基于区块链的匿名特性也确保了投票系统的匿名性。最后，在以太坊的私链网络上测试运行的实验数据说明，本系统具有可行性。通过安全性分析表明，提出的投票方案满足安全性要求，可以应用于企业董事会选举等规模小且匿名隐私性高的场景。

关键词：区块链；智能合约；电子投票；零知识证明

中图分类号：TP311.13 **文献标志码**：A **文章编号**：1002-0802(2018)-08-1979-011

Design and Implementation of Secure Voting System based on Blockchain

YAN Chun-hui, YOU Lin

(School of Communication Engineering, Hangzhou Dianzi University, Hangzhou Zhejiang 310018, China)

Abstract: With the development of society, many application scenarios need to be voted on. In view of the problems in the current electronic voting system, such as the voting data is not transparent and easy to be falsified and forged, the user's private information may be exposed to the risk of being leaked, the voters can not verify the voting results, etc., a secure multi-candidate voting system based on blockchain intelligent contract technology is proposed. The system replaces the traditional trusted third-party counting mechanism with a smart contract auto-execution mechanism and realizes self-counting. The two-round zero-knowledge certification protocol is added to the system to effectively ensure the legality of the voter's identity and protect the privacy of the ballot content, while the anonymity based on the blockchain could also ensure the anonymity of the voting system. Finally, the experimental data of the test run on the private network of Ethereum indicates that this system is feasible. The security analysis shows that the proposed voting scheme could meet the security requirements and be applied to small-scale and anonymous privacy scenarios such as corporate board elections.

Key words: blockchain; smart contract; e-voting; zero-knowledge proofs

0 引 言

随着互联网、通信技术以及现代密码学技术的发展，电子投票成为一种新的投票方式，逐渐得到了社会的关注。自从 Chaum[1] 在 1981 年提出第一个电子投票协议以来，许多密码学研究者提出了不同密码体制的电子投票方案，目的是在互联网环境

* 收稿日期：2018-04-11；修回日期：2018-07-13 Received date:2018-04-11;Revised date:2018-07-13
基金项目：国家自然科学基金项目（No.61772166）；浙江省自然科学基金重点项目（No.LZ17F020002）
Foundation Items: The National Natural Science Foundation of China(No.61772166);The Zhejiang Provincial Science Foundation of China(No.LZ17F020002)

下实现安全、方便、高效的公平投票机制。这些成熟的解决方案也被应用到了政府选举、企业董事会投票以及重要决策投票中。

目前，电子投票方案主要有三类：基于盲签名、环签名的电子投票方案[2-3]、基于全同态加密的电子投票方案[4-5]和基于混合网络的电子投票方案[6-7]。这三类投票方案都存在各自的不足。基于盲签名、环签名的电子投票方案一般需要假设匿名信道和可信的签名机构；基于混合网络的电子投票方案从理论上可以实现解密计票的公开可验证性，但算法过于复杂，效率较低；基于同态加密的电子投票方案虽然可以实现密文计算保护选票的隐私性，但当前全同态加密的计算复杂度太高，并不能有效实用。

近年来，随着比特币等数字货币的逐渐流行，其底层账本技术——区块链技术也受到许多研究学者的关注。区块链的本质是一个公开透明的数据库账本，记录所有的交易记录。它的特点是没有第三方中介机构的情况下，可以提供去中心化、不可篡改、公开透明的安全特性。目前，已提出不少结合区块链技术的电子投票方案，如 2015 年 Zhao 和 Chan 等人[8]提出了一种结合比特币的电子投票协议，该协议对选民的投票行为引入了奖罚制度。尽管该协议有一些限制，但这是第一个尝试将电子投票与区块链相结合的方法。2016 年，Lee、James、Ejeta 和 Kim 等人[9]提出了另一种电子投票协议。该协议提出在区块链电子投票协议中利用 TTP（可信第三方）来保护投票者的选票。2017 年，Cruz 等人[10]提出了一种利用盲签名技术结合区块链的电子投票方案。该方案是将盲化的选票内容写入比特币交易中附加了 80 Byte 信息中。另外，该方案还引入第三方计票机构来统计选票结果。

上述的方案都存在 TTP 来执行投票过程中计票与监督的职责，要求投票参与者都信任这个 TTP。但是，无法排除第三方计票机构与管理者发生共谋攻击，导致投票过程中投票者的选票和投票结果发生篡改，还有计票机构提前泄露投票结果控制整个投票结果发生改变。另外，在比特币交易中附加信息空间的限制，也使该方案具有一定的缺陷性。

McCorry 等人[11]使用区块链实现了一种分布式且具有自我计票功能的互联网电子投票方案，并最大化地保护选民的隐私。通过以太坊智能合约编写投票协议，有效取代了第三方计票机构，在投票过程中通过两轮零知识证明（ZKP）的方式保护投票者的选票隐私信息。但是，该投票方案只允许投票者选择两个候选者（yes/no），无法满足一次投票过程中出现多候选者的情况。

除了这些基于区块链电子投票协议外，目前也有不少在区块链上的电子投票应用被推广使用，如区块链投票机（Blockchain Voting Machine）[12]和 Follow My Vote[13]。这些应用基本都是使用区块链作为一个投票箱，因此需要依赖第三方组织来保护投票者的隐私。

本文针对目前投票系统中的一些缺陷，提出了一种结合区块链的多候选者投票方案，通过智能合约实现本方案使其具有自我计票功能。其次，通过 Node.js 的 Electron 前端框架设计了本方案的投票系统 web 界面，使用 web3.js 提供 JavaScript API 来调用部署在智能合约中投票方案的方法实现与合约交互。最后，从本方案的安全性分析和实验结果分析中说明本方案结合区块链智能合约具有可行性，具有多候选者投票、保护投票者的隐私、具备自我计票的功能等特点。

1 预备知识

1.1 区块链

区块链是随着比特币等[14]数字加密货币而兴起的一种全新技术，本质是一个点对点网络（peer-to-peer）的分布式账本数据库，通过建立一个共同维护且不可篡改的数据库来记录过去的所有交易几轮和历史数据。所有的数据都是分布式存储且公开透明的。这种技术下，任何互不相识的网络用户都可以通过合约、点对点记账、数字加密等方式达成信用共识，而不需要任何中央信任机构。

区块链分为公共链（Public Blockchain）、联盟链（Consortium Blockchain）和私有链（Private Blockchain）。而随着区块链技术的演进，依据不同架构，区块链可分为三个阶段：

（1）区块链 1.0 架构：比特币区块链；

（2）区块链 2.0 架构：以太坊区块链；

（3）区块链 3.0 架构：超越货币、金融范围的区块链应用。

区块链 1.0 的典型应用是比特币应用，也是现在最受欢迎的数字货币，设计目的是允许两个区块链地址账户进行点对点的交易，而不通过第三方可信机构。2013 年，比特币的协议中引进了一项功能，即创建一种名为 OP_RETURN 的交易[15]，允许用户在一笔交易中嵌入 40 Byte 的数据（目前是 80 Byte），因此可以向比特币的区块链中写入任意

信息。不少研究人员利用此特点相继提出了不少结合区块链的应用[16–17]。这些方案有很多弊端，一方面在一笔交易中写入的信息量有限，另一方面随着比特币的交易数量增大，区块链的数据也会变得越来越庞大，交易确认时间也会变得越来越慢。

1.2　以太坊与智能合约

比特币的区块链架构主要围绕支持虚拟货币的实现，虽然具有一定的灵活性，但用来支持虚拟货币意外的应用存在局限性。区块链 2.0 架构的以太坊则提供了一套新的协议，核心是采用图灵完备的计算环境——以太坊虚拟机（EVM），可以实行任意复杂算法的编程，把区块链作为一个可编程的去中心化应用平台支撑智能合约应用。另外，以太坊区块链上写入的数据没有限制且交易确认相对较快。

以太坊有两种类型的账户：

（1）外部所有账户（EOA），一般意义上的用户账户，由用户的私钥控制；

（2）合约（Contract）账户，一种特殊的可编程账户。合约是代码（功能）和数据（状态）的集合，受代码控制，并由外部账户激活。

智能合约（Smart Contract）是一个由计算机处理的、可执行合约条款的交易协议[18]。以太坊的智能合约是一段可被以太坊虚拟机执行的代码。以以太坊特有二进制形式存储在区块链上，并由以太坊虚拟机解释，被称为以太坊虚拟机码（Bytecode）。智能合约像一个可以被信任的人，可以临时保管资产，总是按照事先的规则执行操作。它对接收的信息进行回应，可以接收和存储价值，也可以向外发送信息价值。目前，主要使用一种类似 JavaScript 语言的 Solidity 语言进行智能合约开发。智能合约部署和调用流程如图 1 所示。

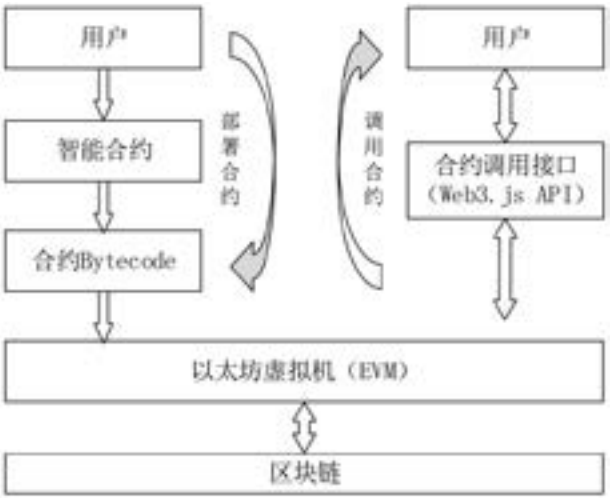

图 1　以太坊智能合约的部署和调用流程

2　一种具有自我计票的多候选人投票方案

文献[11]提出，只允许投票者选择两个候选者，即“yes/no”。本文针对多候选者投票场景，提出一种应用于小规模的董事会投票场景的“1–out–of–m”（即投票人可以从 m 位候选项中选择 1 个）类型的投票方案。第一轮中，所有选民向管理者注册后拥有投票资格，投票前还需要进行身份验证；第二轮中，合格的投票者选择投票意向后向系统广播自己的选票内容。使用区块链作为一个投票者认证的安全信道，通过运行在区块链上的智能合约实现整个投票流程和自我计票功能，通过多方共识后将投票数据写入区块链，可以让任何人都能验证投票的数据及结果。对于投票者隐私保护，在方案中采用了两轮零知识证明向系统证明自己的秘密信息和投票意向但不泄露任何信息。

2.1　两轮零知识证明协议

本投票方案的参与者主要包括 n 位合格投票者 $(V_1,V_2,\cdots,V_n)$ 和一个投票管理机构，对多位候选者 $(C_1,C_2,\cdots,C_k)$ 进行多选一形式表决投票，其中两轮零知识证明协议详细步骤如下。

2.1.1　第一轮零知识证明协议

（1）所有投票者一致同意选取满足安全要求的大素数 p，Z_p^* 为 p 阶有限乘法循环群，g 为 Z_p^* 的生成元。每位投票者 V_i 选择一个随机数 $x_i \in Z_p$ 作为他们的私钥，然后在本地计算得到 g^{x_i} 作为公钥并公开。

（2）每位投票者 V_i 广播他们的 g^{x_i}，然后向系统的智能合约进行离散对数知识证明协议 DKPP(x_i) 用于验证投票者的私钥有效性，即 g^{x_i} 的指数 x_i 是否正确。投票者 V_i 发送 $(g^v,r=v-x_i c)$，其中 $v \in {}_R Z_p$，$c=H(g\|g^v\|g^{x_i}\|A_i)$。智能合约验证 g^v 与 $g^r g^{c\cdot x_i}$ 是否相等，如果相等则证明投票者知道 g 的指数 x_i 正确合法性，从而相信投票者的身份。然后，投票者 V_i 从系统中得到重构的投票公钥：

$$g^{y_i}=\prod_{j=1}^{i-1} g^{x_j} / \prod_{j=i+1}^{n} g^{x_j} \qquad (1)$$

2.1.2　第二轮零知识证明协议

（1）假定 n 位投票者，系统选取一个最小的正整数 m，满足 $2^m > n$。然后，对 k 位候选项分别进行编码表示。投票者选择其中一个选项 $v_i \in \{2^0,2^m 2^{(k-1)m}\}$ 进行投票表决，具体如下：

$$\begin{cases} v_i = 2^0, & \text{当投票者选择候选者1} \\ v_i = 2^m, & \text{当投票者选择候选者2} \\ v_i = 2^{2m}, & \text{当投票者选择候选者3} \\ \cdots & \cdots \\ v_i = 2^{(k-1)m}, & \text{当投票者选择候选者}k \end{cases} \quad (2)$$

（2）投票者在本地表决完后发送自己的选票内容 v_i，并向智能合约进行一轮选票的合法性知识证明协议 VKPP(v_i) 来证明自己选票的合法性。

关于加密选票的合法性知识证明协议具体执行过程如表 1 所示。实际执行过程中，先将选票内容 v_i 转换成 EIGamal 密码体制的形式，即 $(x,y)=(g^{x_i},(g^{y_i})^{x_i}\cdot g^{v_i})=(g^{x_i},h^{x_i}\cdot e_i)$，其中 $e_i \in \{g^{2^0},g^{2^m},\cdots,g^{2^{(k-1)m}}\}$。例如：当选票内容为 $v_i=2^0$ 时，代表投票者选择第一个候选者，投票者的选票的 EIGamal 加密形式表示为 $(x,y)=(g^{x_i},(g^{y_i})^{x_i}\cdot g^{2^0})$。投票者在根据 VKPP 协议计算得到如下参数：$(a_i,b_i)$、$c=H(A_i,g,x,y,a_i,b_i)$、$d_i$ 和 r_i。其中，H 为安全的哈希函数，A_i 为投票者的账号索引值。之后，将 (x,y,a_i,b_i,d_i,r_i) 作为验证条件发送到智能合约上进行验证，而智能合约验证 $H(A_i,g,x,y,a_i,b_i)=d_1+d_2+,\cdots,d_n$ 是否成立来判断投票者选票内容的合法性，从而决定是否接受投票者的选票内容。此协议是为了表明投票者发送的加密选票 $g^{x_iy_i}g^{y_i}$ 是对候选人列表 $\{2^0,2^m,\cdots,2^{(k-1)m}\}$ 其中之一的选择进行加密而不泄露具体的信息，也是实现“1-out-of-m”类型投票的关键所在。另一个目的，是防止破坏者进行重复投票的行为。此外，利用 EIGamal 加密体制的同态属性，配合智能合约的自动执行操作可以依据设计好的规则实现自我计票，有效取代第三方计票机构，使投票系统更具安全性。

（3）智能合约自动判断投票者加密选票的合法性知识证明协议过程，验证判断每一位投票者的选票内容是否正确、合法。如果正确，则接受投票者提交的选票内容；否则，放弃。当最后一位投票者提交选票后，计算所有选票的统计结果：

$$\prod_i g^{x_iy_i}g^{v_i}=g^{\sum_i x_iy_i}g^{\sum_i v_i}=g^{\sum_i v_i} \quad (3)$$

这里 $g^{\sum_i y_i}$ 为离散对数。式（4）的值可以通过小步大步算法（Baby-step Giant-step）和指数积分法（Index Calculus）得到，表示为投票统计的结果，其中系数 $(c_1,c_2,\cdots,c_k)$ 分别是 k 位候选者相对应票数。

$$\sum_i v_i = 2^0\cdot c_1 + 2^m\cdot c_2 + \cdots + 2^{(k-1)m}\cdot c_k \quad (4)$$

而式（3）的结果是因为通过重构密钥可以得到 $\sum_i x_iy_i=0$，因此可得 $g^{\sum_i x_iy_i}=1$。

对于 $\sum_i x_iy_i=0$ 具体证明过程如下。

由上述重构密钥：

$$g^{y_i}=\frac{\prod_{j=1}^{i-1}g^{x_j}}{\prod_{j=i+1}^{n}g^{x_j}} \quad (5)$$

可得：

$$y_i=\sum_{j<i}x_j-\sum_{j>i}x_j \quad (6)$$

最终，可得：

$$\sum_i x_iy_i=\sum_i\sum_{j<i}x_ix_j-\sum_i\sum_{j>i}x_ix_j=\sum\sum_{j<i}x_ix_j-\sum\sum_{i<j}x_ix_j=\sum\sum_{j<i}x_ix_j-\sum\sum_{i<j}x_ix_j=0 \quad (7)$$

2.2 投票方案的设计及流程说明

本文设计的投票方案采用 EIGamal 加密体制和两轮零知识证明协议，并运行在以太坊区块链上，通过以太坊智能合约取代传统可信第三方计票机构（TTP）实现自我计票功能。通过区块链的共识机制将投票过程的数据写入区块链账本中，能够满足用户的信任需求。通过 EIGamal 密码体制保护投票数据的隐私，经过两轮零知识证明协议一方面可以有效防止恶意攻击者的仿造冒充有效投票者进行假投票，另一方面投票者向系统验证自己的有效加密选票的正确性而不泄露具体内容，保护了投票者的隐私。本投票方案总共分为 5 个过程，由投票发起者、智能合约和投票者三部分组成。图 2 展示了整个投票方案的流程。

图 2 投票方案的流程时序

表 1　选票内容的合法性知识证明协议流程

选票内容	VKPP 执行过程	投票者发送	验证者检验
$v_i=2^0$	$w,r_i,d_i\in Z_p$, 其他 $i\in[1,k]\setminus\{1\}$ $x=g^{x_i}, y=h^{x_i}\cdot e_1$ $a_1=g^w, b_1=h^w$ $a_2=g^{r_2}x^{d_2}, b_2=h^{r_2}(\frac{y}{e_2})^{d_2}$ … $a_k=g^{r_k}x^{d_k}, b_k=h^{r_k}(\frac{y}{e_k})^{d_k}$ $c=H(A_i,x,y,a_i,b_i), d_1=c-\sum_{i\neq1}d_i, r_1=w-x_i\cdot d_1$	x,y,a_i,r_i,d_i	$c\stackrel{?}{=}\sum_i d_i$, $a_i\stackrel{?}{=}g^{r_i}x^{d_i}$, $b_i\stackrel{?}{=}h^{r_i}(\frac{y}{e_i})^{d_i}$
$v_i=2^m$	$w,r_i,d_i\in Z_p$, 其他 $i\in[1,k]\setminus\{1\}$ $x=g^{x_i}, y=h^{x_i}\cdot e_1$ $a_1=g^{r_1}x^{d_1}, b_2=h^{r_1}(\frac{y}{e_1})^{d_1}$ $a_2=g^w, b_2=h^w$ … $a_k=g^{r_k}x^{d_k}, b_k=h^{r_k}(\frac{y}{e_k})^{d_k}$ $c=H(A_i,x,y,a_i,b_i), d_2=c-\sum_{i\neq2}d_i, r_2=w-x_i\cdot d_2$		
…	…		
$v_i=2^{(k-1)m}$	$w,r_i,d_i\in Z_p$, 其他 $i\in[1,k]\setminus\{k\}$ $x=g^{x_i}, y=h^{x_i}\cdot e_1$ $a_1=g^{r_1}x^{d_1}, b_2=h^{r_1}(\frac{y}{e_1})^{d_1}$ $a_2=g^{r_2}x^{d_2}, b_2=h^{r_2}(\frac{y}{e_2})^{d_2}$ … $a_k=g^w, b_k=h^w$ $c=H(A_i,x,y,a_i,b_i), d_k=c-\sum_{i\neq k}d_i, r_k=w-x_i\cdot d_k$		

具体的实施过程如下。

（1）登录账户

步骤 1：投票发起者和每位投票者登录投票系统的账号都是自己的以太坊账号和密码；

步骤 2：要保证每一个投票者账户里至少有少部分代币用于投票时所需的花费，如果投票者账户余额不足，可以向系统索要。

（2）系统设置

步骤 1：投票发起者设置投票项目的名称、问题的数量及内容；

步骤 2：投票发起者设置计时器，设置投票各个环节的起止时间，确保投票能顺利进行，具体时间参数如下：

$T_{finishRegistration}$：表示所有投票者一定要在这个时间点前完成注册；

$T_{beginVote}$：表示投票发起者通知系统在这个时间开始进行投票；

$T_{finishVote}$：表示所有投票者一定要在这个时间前投出他们的选票内容；

T_{π}：最小的时间间隔，投票期间让投票者有足够时间进行投票，保证合约正常运行并写入区块链。

步骤 3：投票发起者设置完上述参数后，通知系统开始进入注册阶段，并更新智能合约。

（3）注册

步骤 1：投票发起者为每一位登记的投票者生成唯一的注册 ID 并发送给投票者；

步骤 2：投票者向投票发起者发送注册 ID 来发起注册请求，投票发起者通过智能合约验证投票者的注册 ID 是否匹配，通过认证的合格投票者名单被写入投票合约中；

步骤 3：如果匹配通过，投票者需要生成随机数 x_i 作为私钥，然后计算他们的投票公钥 g^{x_i}，通过智能合约进行 $DKPP(x_i)$（离散对数知识证明协议）来验证投票者私钥 x_i 的有效性；

步骤 4：投票者从系统中得到计算后的重构密钥 g^{y_i}。

投票发起者认证每一个投票者的账号，只有通过认证的合格投票者名单写入投票合约中。注册阶段，应该在规定的注册时间 $T_{finishRegistration}$ 内完成，否则系统不接受任何人的注册。同时，投票发起者确认后通知智能合约进入投票阶段。

（4）投票

投票阶段，投票者在投票界面中选择自己选项，然后生成自己的正式选票，通过系统的智能合约的投票方法发送他们的加密后选票内容，具体步骤如下：

步骤 1：投票者将投票内容转化为加密后的形式 $g^{x_i y_i} g^{v_i}$；

步骤 2：投票者需执行 $VKPP(v_i)$（选票内容合法性知识证明协议）向系统的智能合约证明自己的投票内容合法，即 $v_i \in \{2^0, 2^m, \cdots, 2^{(k-1)m}\}$，且选票内容的加密形式是正确的；

步骤 3：如果有人选择投弃权票，系统也会将此票作为弃权选票并统计到最终投票结果中。

投票工作必须在系统规定的投票时间 $T_{finishVote}$ 内完成，当最后一个投票者提交选票后，投票发起者通知智能合约进入计票阶段。

（5）计票

系统调用智能合约中写好的统计投票结果的方法，无需任何第三方计票机构对选票进行统计。智能合约会验证每一张选票的有效性，然后统计所有选票包括弃权票生成最终的投票结果，写入区块链账本并在投票系统上公布。

步骤 1：系统调用智能合约中计票的方法，统计所有有效的选票内容，即执行：

$$\prod_i g^{x_i y_i} g^{v_i} = g^{\sum_i x_i y_i} g^{\sum_i v_i} = g^{\sum_i v_i} \quad (8)$$

步骤 2：要得到投票的最终结果就是计算得到统计结果的离散对数的值：

$$\sum_i v_i = 2^0 \cdot c_1 + 2^m \cdot c_2 + 2^{2m} \cdot c_3 + \cdots + 2^{(k-1)m} \cdot c_k \quad (9)$$

这里 $(c_1, c_2, \cdots c_k)$ 分别代表相对应候选者的投票数量。另外，对弃权票进行单独统计并计入投票结果中。

步骤 3：系统公布每一个候选者对应的统计结果和弃权票的结果，任何人都可以验证投票结果的正确性。

投票流程结束。

3 投票系统设计及实现

本文提出的投票方案实现方法基于以太坊智能合约，通过 Web3.js 库的 JavaScript API 接口调用部署在区块链上智能合约的相应方法，实现了整个投票过程。对于智能合约开发，使用目前应用最广泛的编程语言——Solidity 语言。Solidity 是一种语法与 JavaScript 相似的高级语言，为以太坊虚拟机编译代码而设计。另外，设计了基于 Nodejs 的 Electron 前端框架开发了投票系统的 DApp，用于展示整个投票系统的交互过程。图 3 为投票系统架构图。

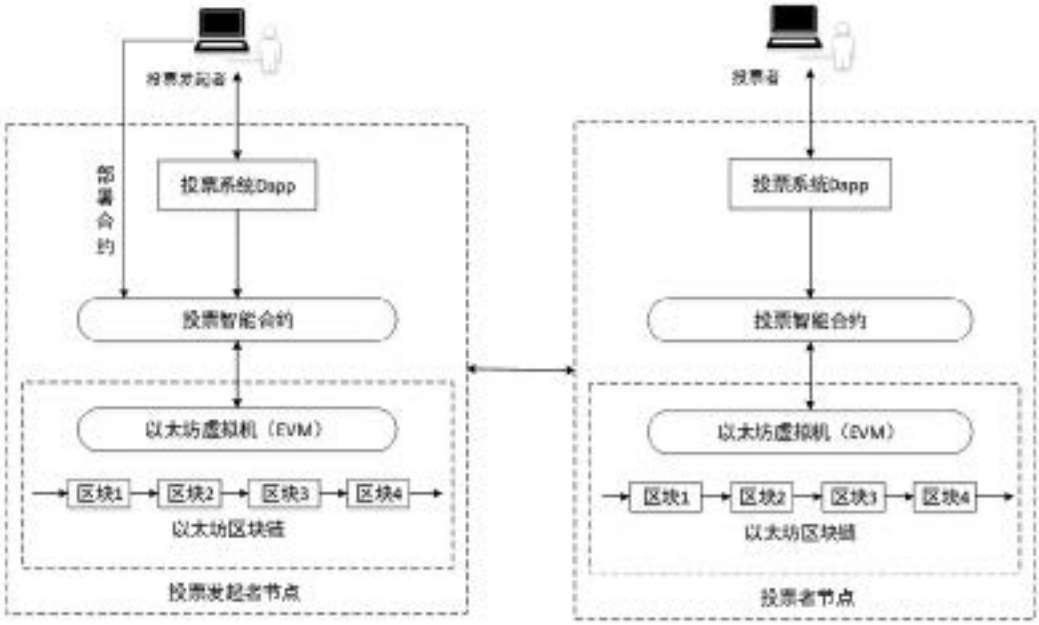

图 3 投票系统架构

3.1　投票方案智能合约设计

将整个投票方案设计成三个智能合约，分别为 LocalCrypt.sol、Vote.sol 和 VoteContractRegistery.sol。这三个合约的功能介绍如表 2 所示。

表 2　智能合约功能介绍

智能合约	功能
VoteContractRegistery.sol	主合约，通过合约的 ABI 和 Address 实现调用 Vote.sol 和 LocalCrypt.sol 两个合约的方法
Vote.sol	投票协议智能合约，实现投票者认证注册、投票、提交选票、自我计票等方法
LocalCrypt.sol	加密方法的智能合约，用于零知识证明协议及加密的方法

3.2　投票系统设计及实现

基于区块链的多候选人投票系统 DApp 整体实现是通过 web 前端页面使用 Web3.js 库提供的 JavaScript API 接口调用部署在区块链上智能合约的相应方法，实现了投票交互的整个过程。该设计开发实现了管理员和投票者两个客户端，图 4 展示了投票系统 DApp 的界面功能和投票过程。

投票发起者客户端（admin.html）：管理员管理、控制、监督整个投票过程，包括部署投票项目智能合约、认证投票者、建立合格投票者列表、发起投票问题、设置注册环节的起止时间、设置投票环节的起止时间、启动计票环节和强制关闭投票项目等功能。

投票者客户端（voter.html）：选民登录注册成为合格投票者进行投票，包括登录注册、参与投票、提交选票和查询投票结果等功能。

（a）投票发起者登录界面

（b）投票者登录界面

（c）投票问题设置

（d）投票时间设置

（e）投票者发送注册码

（f）投票发起者接受注册

（g）投票选择界面

（h）选票查询界面

（i）计票界面

（j）结果公布

图 4　投票系统界面

4　性能分析与安全性分析

4.1　系统性能分析

本文实验平台使用 Intel Core i5-3470 3.2GHz 的 CPU，8 GB 内存，运行 64 位 Windows10 操作系统；采用以太坊作为区块链的框架，通过创世区块文件在本地搭建以太坊私链环境，以太坊 geth 客户端为 1.7.2 版本，以太坊钱包为 win64-0.8.10 版本。将以太坊钱包连接到本地私有链网络后，通过钱包将投票方案的智能合约部署在本地私链上，获取 LocalCrypto.sol 和 Vote.sol 的合约地址 address 和二进制文件 ABI，把它们发送到主合约 VoteContractRegistry.sol 上，实现调用这两份合约的方法。另外，通过 Web3.js 库提供的 JavaScript API 接口与合约互动，设计了前端页面，实现整个投票的交互过程。

表 3 为一次投票过程中统计每项操作所需消耗的 Gas 和消耗的 Gas 总量。此次投票过程中包含 40 位投票者进行模拟投票，投票过程中产生的费用是由 *GasUsed*（消耗量）和 *GasPrice*（价格）两个因素决定，即 *Cost=GasPrice*GasUsed*。其中 *GasUsed* 由交易（或执行合约代码）的计算量来决定，而 *GasPrice* 由交易的发起者来设置。

将投票方案的智能合约分成三份，一方面是为了区分彼此之间功能关系，如 LocalCrypto. Sol 主要涉及基本的加密解密方法和零知识证明协议的运行，这样模块化设计可以提高代码的重复使用。另一方面，考虑到以太坊上部署智能合约受 GasLimit 限制，无法将整个投票方案的合约代码通过一份合约上执行。采取的方案是通过主合约

VoteContractRegistery.sol 调用另外两个合约中的方法。通过表 3 中统计的 Gas 消耗显示，部署这三个智能合约都是在以太坊公链中单笔交易 Gas 最大限制值（8 000 000 Gas）之内，证明投票方案可以在本地私链中运行，同样可以让其在公链中正常运行。

表 3　投票中每项操作所需 Gas 消耗统计表

参与人员	操作	Gas 消耗	Gas 消耗总量
投票发起者	部署 VoteContractRegistery.sol	883 487	13 216 196
	部署 Vote.sol	3 779 963	
	部署 LocalCrypto. sol	4 171 615	
	设置投票项目	254 974	
	验证投票者	2 052 471	
	启动投票	2 975 334	
	计票	2 500 312	
投票者	注册	663 116	3 153 531
	投票	2 490 415	

表 4 列出了投票方案中一些方法计算所需的平均时间。投票协议合约 Vote.sol 主要包括注册投票、计算重构公钥、提交选票和计票这几个主要步骤。使用 Web3 框架提供的接口方法让 Web 浏览器和以太坊守护进程之间进行通信，所有智能合约中可执行的方法都可用 .Call() 来调用执行而不会产生 Gas 消耗，可以在本地的守护进程中测量代码执行时所需的计算时间。其中，加密合约 LocalCrypto.Sol 主要包括创建和认证零知识证明的两个步骤。在投票注册过程中，创建零知识协议所耗时为 81 ms，验证零知识协议所耗时为 180 ms；投票过程中，提交选票时创建选票合法性知识证明协议所耗时为 356 ms，验证选票合法性知识证明协议耗时为 548 ms。

表 4　投票方案不同方法执行消耗平均时间

操作	平均时间 /ms
Begin Sign UP	277
Register Account	76
Ask For Registration	91
Computer Reconstructed Key	212
Generate DKPP	81
Verify DKPP	180
Generate VKPP	356
Verify VKPP	548
Submit Vote	537
Compute Tally	239

整个投票方案的执行流程都是按照智能合约的执行顺序进行。实验结果表明，整个投票方案最耗时的地方是零知识证明协议和统计投票结果，涉及验证选票的合法性知识证明协议和离散对数知识证明协议两个步骤。此外，还有计算投票结果的离散对数运算，主要是因为目前以太坊智能合约缺乏公钥加密体制的原生支持。

4.2　安全性分析

本文改进的具有自我计票的多候选投票方案是通过区块链上的智能合约实现的，投票者使用以太坊账号进行认证，在投票过程将自己加密后的选票提交到区块链上，投票系统调用智能合约计票方法实现自动计票并计算出投票结果，可以做到无需第三方计票机构。本方案的投票系统基于区块链的安全性，可以实现投票过程的公开可验证、数据防篡改特点。下面对投票系统进行以下几个方面的安全性分析。

4.2.1　选票完全保密性

本文设计的投票系统中，每一位投票者投出的选票内容 $g^{x_i y_i} g^{y_i}$ 都是经过加密的，且投票者向系统发送两轮零知识证明协议验证选票内容的正确性。第一轮中，投票者发送自己的投票密钥 g^{x_i}；第二轮中，投票者发送自己的选择内容 v_i。投票者的密钥 x_i 是一个随机数，而 y_i 也是一个随机值，所以对于攻击者来说无法确定。根据 Diffie–Hellman 假设，任何人无法区分 $g^{x_i y_i}$ 在群中所对应的阶数，其中间环节投票者没有透露一点关于自己投票的详细信息，所以任何人无法区分加密选票 $g^{x_i y_i} g^{y_i}$ 所选择的投票内容 v_i，最大化保护选票的保密性。

智能合约的本质是运行在区块链上的具有特定业务逻辑的一段代码。智能合约的状态和内容是公开的，链上的用户可以对代码进行审查，从而判断合约的功能。智能合约的运行结果会写入账本并公开可验证，不会发生合约创建者规定之外的行为。区块链本身具有匿名性，即使攻击者获取投票者的数据，也无法确定投票者的身份和投票信息。

4.2.2 公平性

统计选票阶段，只有在规定投票时间内，当最后一位投票者广播了自己的投票结果 v_i 后，系统的智能合约才能被管理者执行统计投票结果的方法并得到计票结果。所以，只要存在未在正确时间内广播选票的投票者，投票结果将无法被预先计算。因此，该方案具有公平性。

4.2.3 无争议性

本文方案中以区块链作为身份认证的通道，对于投票者的以太坊账号进行有效性验证，任何无效的账号都不能在投票系统中进行投票。此外，限定一人投一票，每一张选票选择一个候选者，保证了投票结果的准确性，投票方案是无争议的。

4.2.4 可验证性

投票者在提交选票后在系统统计投票结果前，可以在自己的客户端查询确认选票是否被篡改。基于区块链上的数据具有公开性可验证。在统计结果出来后，每一位投票者也获取到所有投票者的选票 $g^{x_i y_i} g^{y_i}$ 去验证计算 $\prod_i g^{x_i y_i} g^{v_i}$ 的值与系统给出的结果是否一致。本方案具有投票结果的可验证性。

4.2.5 合格性

方案中，投票者都在管理员那里进行登记注册。管理员会在投票智能合约中建立一份有效的投票者名单，确保登录到投票系统中的投票者都是合法的。之后在投票过程中，投票者还需要验证由管理者发送的唯一验证码进行双重验证，确保每一位投票者都是合格的，每一张选票都是合格有效的。

4.2.6 抗重播攻击

所有的投票密钥 g^{x_i} 和零知识证明 $DKPP(x_i)$ 被公开发送到以太坊区块链。因此，另外的合格投票者可能会尝试使用另一组 g^{x_i} 和 $DKPP(x_i)$ 来获得再一次的投票权。而在零知识证明过程中，要求投票者在哈希函数中包含 msg.sender（即投票者的以太坊账号）。如果 msg.sender 与调用合约的账户不匹配，智能合约将不接受 $DKPP(x_i)$ 的验证。因此，在没有共谋的情况下，攻击者想重播攻击另一位投票者的投票密钥 g^{x_i} 来获得另一次投票是不可能的。同样，在对选票的零知识证明 $VKPP(v_i)$ 验证过程也是不能通过。

5 结 语

本文介绍了一种基于以太坊区块链的多候选人的电子投票方案，用特定业务逻辑的智能合约实现自我计票功能而取代了传统的第三方计票机构。同时，在投票方案的智能合约引入了两轮零知识证明，有效保护了投票者的隐私问题。从对投票方案的安全性分析中证明，投票方案是安全可靠的。另外，在本地的私有链节点上部署智能合约，模拟了 40 位投票者进行投票。从实验的数据中可知，投票系统在保护投票者隐私的前提下能做到公开可验证，可适用于小规模的董事会投票场景。

参考文献：

[1] Chaum D L.Untraceable Electronic Mail,Return Addresses,and Digital Pseudonyms[J].Communications of the ACM,1981,4(02):84-88.

[2] 张江霄，李舟军，刘霞等．基于群盲签名的多授权电子投票系统 [J]. 中国科技论文，2015(08):980-983.
ZHANG Jiang-xiao,LI Zhou-jun,LIU Xia,et al.Multi-licensing Electronic Voting System Based on Group Blind Signatures[J].China Science and Technology Paper,2015(08):980-983.

[3] 范安东，孙琦，张杨松．基于环签名的匿名电子投票方案 [J]. 工程科学与技术，2008,40(01):113-117.
FAN An-dong,SUN Qi,ZHANG Yang-song.The Scheme of Anonymous Electronic Voting Based on Ring Signature[J]. Advanced Engineering Sciences,2008,40(01):113-117.

[4] Chillotti I,Gama N,Georgieva M,et al.A Homomorphic LWE Based E-voting Scheme[M].Springer International Publishing,2016.

[5] 王永恒，徐晨，陈经纬等．基于 HElib 的安全电子投票方案 [J]. 计算机应用研究，2017,34(07):2167-2171.
WANG Yong-heng,XU Chen,CHEN Jiang-wei,et al.Scheme on Secure Voting System Based on HElib[J].Application Research of Computers,2017,34(07):2167-2171.

[6] Islam N,Alam K M R,Tamura S,et al.A New e-voting Scheme Based on Revised Simplified Verifiable Re-Encryption Mixnet[C].International Conference on Networking,Systems and Security IEEE,2017:12-20.

[7] 高虎明，王继林，王育民．一个基于 Mix net 的电子投票方案 [J]. 电子学报，2004,32(06):1047-1049.
GAO Hu-ming,WANG Ji-lin,WANG Yu-min.An Electronic Voting Scheme Based on A New Mix Net[J]. Acta Electronica Sinica,2004,32(06):1047-1049.

[8] Zhao Z,Chan T H H.How to Vote Privately Using Bitcoin[J].Computers & Education,2015(69):514-516.
[9] Lee K,James J I,Ejeta T G,et al.Electronic Voting Service Using Block-chain[J].The Journal of Digital Forensics,Security and Law:JDFSL,2016,11(02):123.
[10] Jason P C,Yuichi K.E-voting System Based on the Bitcoin Protocol and Blind Signatures[J]. Transactions on Mathematical Modeling and Its Applications,2017,10(01):14-22.
[11] McCorry P,Shahandashti S F,Hao F.A Smart Contract for Boardroom Voting with Maximum Voter Privacy[C]. International Conference on Financial Cryptography and Data Security,Springer,2017:357-375.
[12] Wire B.Now You Can Vote Online with a Selfie[EB/OL].2016[2018-04-01].https://www.businesswire.com/news/home/20161017005354/en/.
[13] Aradhya P.Followmyvote[EB/OL].2016 [2018-03-31]. https://www.huffingtonpost.com/pradeep-aradhya/are-we-ready-for-a-global_b_9591580.html.
[14] Nakamoto S.Bitcoin:A Peer-to-Peer Electronic Cash System[OL].2008[2018-03-31]https://bitcoin.org/bitcoin.pdf.
[15] Bartoletti M,Pompianu L.An Analysis of Bitcoin OP_RETURN Metadata[C].International Conference on Financial Cryptography and Data Security,2017:218-230.
[16] Kuo T T,Ohno-Machado L.ModelChain:Decentralized Privacy-Preserving Healthcare Predictive Modeling Framework on Private Blockchain Networks[J].arXiv preprint arXiv:1802.01746,2018.
[17] Kuo T T,Kim H E,Ohno-Machado L.Blockchain Distributed Ledger Technologies for Biomedical and Health Care Applications[J].J Am Med Inform Assoc,2017,24(06):1211-1220.
[18] 邹均 , 张海宁 , 唐屹等 . 区块链技术指南 [M]. 北京 : 机械工业出版社 ,2016.
ZOU Jun,ZHANG Hai-ning,TANG Yi,et al.Blockchain Technical Guide[M].Bei Jing:China Machine Press,2016.

作者简介：

颜春辉（1992—），男，硕士，主要研究方向为区块链技术、生物特征密码学技术；

游　林（1966—），男，博士，教授，主要研究方向为计算代数、密码学、生物特征识别及其应用等。