基于零知识证明的电子投票协议研究

王宝成,伍博文
(北方工业大学 信息学院,北京 100144)

摘 要:区块链的不可篡改、公开透明和去中心化等特性具有广阔的应用前景,它为电子投票技术带来了新的发展方向。而根据是否依赖第三方,电子投票协议的设计思路会出现巨大差异。其中,区块链的去中心和不可篡改等特性帮助自计数,不依赖第三方的电子投票类型方案更加成熟,走向实际应用。在保障投票系统安全性的同时,还能保护投票者的隐私,允许人们自行验证选举的安全性和投票结果。不足之处在与该类方案目前普遍存在最后一名投票者提前知道选举结果的缺陷。而这些方案中已有的措施无法较好地处理该缺陷引发的问题。故针对该现状提出了一种新的投票方案,结合算法特点,引入了候选者做投票者,通过候选者们之间利益不会完全一致的矛盾,配合算法,堵住了人们利用最后一名投票者提前知道选举结果,影响甚至破坏选举的漏洞。通过安全和性能分析,该方案符合电子投票系统的基本安全标准。

关键词:零知识证明;区块链;电子投票;自计数投票;博尔达计数
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2022)0044-05

Research on Electronic Voting Protocol Based on Zero-knowledge Proof

WANG Bao-cheng, WU Bo-wen
(School of Information Science and Technology, North China University of Technology, Beijing 100144, China)

Abstract: The characteristics of blockchain, such as imtamability, openness and transparency, and decentralization, have broad application prospects, which brings a new development direction for electronic voting technology. The design ideas of electronic voting protocols vary greatly depending on whether they rely on third parties or not. Among them, the decentralized and imtamable features of blockchain help self-counting and electronic voting schemes that do not rely on third parties become more mature and move towards practical applications. While ensuring the security of the voting system, it also protects the privacy of voters and allows people to verify the security of the election and the results themselves. The disadvantage of such schemes is that the last voter knows the election result in advance. And the existing measures in these programs cannot better deal with the problem caused by the defect. In view of this situation, a new voting scheme is proposed. Combining with the characteristics of the algorithm, the candidate is introduced to be a voter, and through the contradiction that the interests of the candidates are not completely consistent, the algorithm is used to plug the loophole that people use the last voter to know the election result in advance, and even to affect or destroy the election. Through security and performance analysis, the scheme meets the basic security standards of electronic voting systems.

Key words: zero knowledge proof; block chain; electronic voting; self-counting voting; borda counting

0 引 言

区块链的不可篡改、公开透明、去中心化和去信任等特性具有广阔的应用前景[1],与电子投票的设计需求有良好的契合。伴随着区块链技术的火热,电子投票也有了新的发展方向。在 2015 年,第一次有人尝试将电子投票与区块链相结合。这是由 Zhao 和 Chan 等人设计的一种结合比特币的电子投票协议[2]。那之后,结合区块链的电子投票协议被陆续提出。其中,不依赖第三方的电子投票方案开始被更多人关注,并随着发展逐渐走向成熟,在实现自计数,保护投票者隐私的同时,也能允许选择多个选择者。在选举规模较小的情况下,其效率是可以接受并投入使用的。

然而,上文的自计数电子投票方案虽有着许多优点,但该类方案目前还存在着一些普遍的不足。这类投票方案的一个典型代表是 OV-Net (open-vote network)[3]。它允许有限数量的选民在不需要任何点票机构帮助的情况下进行投票。OV-Net 包括两轮。在第一轮投票中,每个投票人都会在公布栏上公布他的

收稿日期:2021-08-18
基金项目:北京市属高校基本科研业务费(110052971921/021)
作者简介:王宝成(1979-),男,博士,副教授,研究方向为信息安全、密码学、区块链;伍博文(1995-),男,硕士研究生,研究方向为密码学、区块链。

公开密钥。在第二轮中,每个投票人发表他的随机选票,这是使用其他投票人的公开密钥、该投票人的秘密密钥和他的秘密投票生成的。一旦所有加密的选票都在公告板上,任何人都可以很容易地计算出结果。

该方案依靠非交互的零知识证明(non-interactive zero-knowledge proof,NIZK)来证明每个密文的良好格式。该方案提供了最大限度的隐私保障,因为每个投票人除了最终解票数和自己的选票外什么都不知道。一个公众观察者从公告版上了解到的无非是统计数字。将选票内容加密,然后公布到区块链上,通过将所有加密选票合在一起运算,在这过程中,这些加密选票里面的随机数会被抵消掉,从而能够计算出所有选票的值,但存在最后一名投票者会提前知道选票结果的不足,以及任何一名投票者都可以通过在第二轮放弃投票来破坏此轮选举的隐患。

目前已有的方案提出的弥补措施[4]有哈希预签名,让可靠第三方做最后一名投票者等,然而这些措施要么无法很好地阻碍投票者作弊,要么依赖第三方的可靠性,因此,该文提出了一个新的方案,在不依赖第三方,保障选民隐私,选举安全性的同时,解决了最后一名投票者提前知道选举中间结果的问题。

文中贡献包括以下几点:

(1)提出了一个新的自计票去中心化计数投票协议。提议的协议提供了最大限度的选民隐私:个人投票只能通过涉及所有其他选民的完全合谋攻击来显示。所有投票数据都是公开的,任何公众观察员都可以验证协议的正确执行。提议的协议不需要任何可信的权威来计算计数;统计数字可以由每个投票人计算,也可以由任何选举观察员计算。并且,除非所有候选者达成完全共谋,无人能利用提前知道选举的中间结果这点,使得选举的公平性得到较好的保护。

(2)提供了安全措施来保护选举的顺利执行。证明了所提出的方案最大限度地防止选民串通,违规。

1　预备知识

1.1　零知识证明

零知识证明是一种密码协议,在 1985 年由 Goldwasser 等人[5]提出。该协议一般由两部分组成,一部分是证明者(Prover),此处用 P 代指,另一部分是验证者(Verifier),一般用 V 表示。零知识证明协议是指 P 试图使某人相信某个论断是正确的,却不向 V 提供任何有用的信息。总结可得,零知识证明的理念是证明某个论断是正确的,却不泄露任何信息和知识。

1.2　博尔达计数

博尔达计数亦称“博尔达程序”,群体决策方法之一,由法国数学家博尔达于 1770 年提出。其基本做法是:按照投票者的偏好程度的排序给 M 个提案中的每一个打分,分值从 1 到 M,即被投票者列为第一的提案得 M 分,列第二的提案得 $M-1$ 分,被投票者排在最后一位的提案得 1 分,把所有的投票者的每个提案的分数分别加起来,最高分的提案为获胜者。

1.3　电子投票协议基本安全要求

(1)正确性:所有无效的票都不能被计入。

(2)不可重用性:投票者不能重复投票两次以上。

(3)完整性:所有有效的票被正确统计。

(4)秘密性:投票者所投的票必须被保密。

(5)适格性:只有具有投票权的投票者才能进行投票活动。

(6)公平性:没有人知道投票的中间结果。

(7)可验证性:没有人能够伪造投票结果[6]。

2　一个安全巧妙的零知识证明投票方案

本节介绍基于零知识证明的投票协议,通过该协议,投票者们可以在不依赖第三方的前提下实现自计数投票。

2.1　选举环境

假设选举为董事会规模的小型选举,有 n 位投票者,k 位候选者,候选者也是投票者。选举管理方规定采用博尔达计数,每位投票者可以投出一张选票 $(a_1,a_2,\cdots,a_k)$,表示给从第一位候选者到第 k 位候选者的投票分值。$(a_1,a_2,\cdots,a_k)$ 是管理方规定的投票分值 $(1,2,\cdots,k)$ 的一个重新排列。

在该协议中,假设每个参与者都有一个经过身份验证的公共通道可用。这种假设在已有的电子投票协议中是常有的;这个经过身份验证的公共通道可以通过使用物理方法或公共公告板来实现,在公告板上记录的选票以仅附加的方式[7]安全地存储在公告板上[8-9]。

2.2　选举方案设计

本协议选举流程如图 1 所示,选举总共分三轮进行,总体思路是先让投票者们公布自己的公钥,之后再让投票者们根据已经公布的公钥,构造选票并公布,选票本身不会暴露投票者的投票指向,而当所有选票都公布后,对它们进行计算,就能得到各候选者最终的得票数。其中,NIZK 起到维护选举规范的作用。各流程具体含义和操作将在下文中说明。

2.2.1　选民和候选者登记

在进行选举前,首先要对选民和候选者的身份进行认证,因为是董事会规模,且整个投票设计无需隐藏选民身份,所以直接由董事会委托的第三方或董事会成员自行给自己投票用的账户并在区块链上公布选民和候选者名单即可。根据公布的信息,如无人对此有

异议,说明选民和候选者都正常获取了自己的投票账户,且无多余的投票者混进来[10]。

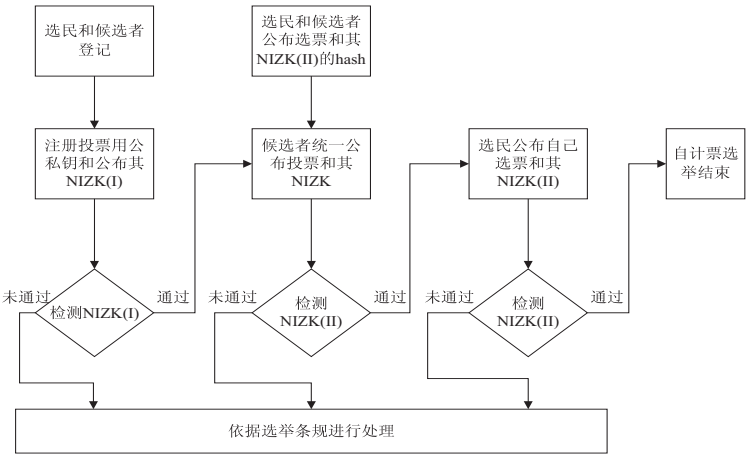

图 1 选举流程

2.2.2 第一轮

在第一轮里,为了之后的投票,每位投票者(包括候选者)在投票前,首先要生成一个公私钥对,做法如下所示:投票者选取满足安全要求的大素数 q,$\mathbb{Z}_q$ 为阶为 q 的有限乘法循环群,g 为 $\mathbb{Z}_q$ 的生成元。每位投票者选择 k 个随机数作为他们的私钥,然后在本地计算出 $(g^{x_{i1}},g^{x_{i2}},\cdots,g^{x_{ik}})$ 并公开。设定 $\sum_{i=1}^{n} v_{ij}$ 表示第 i 个投票者,$P_k\{x_j\}$ 表示投票者第 j 个私钥对应的零知识证明。之后,每位投票者 V_i 需要广播他们的公钥 $(g^{x_{i1}},g^{x_{i2}},\cdots,g^{x_{ik}})$,并向区块链上的智能合约发送公钥的零知识证明 $(P_k\{x_{i1}\},P_k\{x_{i2}\},\cdots,P_k\{x_{ik}\})$ 用于验证投票者的私钥有效性。该零知识证明的生成算法来自于 Schnorr 的方案[11]。

在协议的第一轮中使用了 Fiat-Shamir 启发式来构造零知识证明[12],验证投票者们是否忠实于选举规则。若未能通过零知识证明检测,说明投票者 V_i 出了问题,可能的原因有账户失窃,故意构造错误的零知识证明或广播的公钥与构造零知识证明时用的私钥不符合等。先将该投票者从本次投票中排除,并发公告通知。让其他投票者在之后构造选票时,不使用该投票者公布的公钥[13]。

2.2.3 第二轮

通过第一轮,选民和候选者们知道了其他人的公钥。然后,根据这些公布的信息,投票者们从系统中得到重构的投票公钥 $g^{y_i}=\prod_{j=1}^{i-1} g^{x_j}/\prod_{j=i+1}^{n} g^{x_j}$。

根据上文,已知目前有 n 位投票者,k 位候选者,且这 k 位候选者也包含在投票者中。用 Z_{ij} 来表示第 i 位投票者投给第 j 位候选者的选票。选票计算如下:

$Z_{ij}=\{g^{y_{ij}}\}^{x_{ij}}g^{v_{ij}}$; $\forall i\in\{1,2,\cdots,n\}$, $\forall j\in\{1,2,\cdots,k\}$

最终,投票者可以得到选票 $(Z_{i1},Z_{i2},\cdots,Z_{ik})$,用来表示给 k 位候选者的投票。除了选票,还需生成一个相应的合法性零知识证明来证明选票符合规范。这个与选票关联的合法性零知识证明证明了 $(v_{i1},v_{i2},\cdots,v_{ik})$ 是预先规定的选票分值 $(a_1,a_2,\cdots,a_k)$ 的一个重新排列。为了证明这个论断,需要先证明下面的 k 个关系:

$a_1\in\{v_{i1},v_{i2},\cdots,v_{ik}\}$ 对应于第一位的分数。

$a_2\in\{v_{i1},v_{i2},\cdots,v_{ik}\}$ 对应于第二位的分数。

…

$a_k\in\{v_{i1},v_{i2},\cdots,v_{ik}\}$ 对应于第 k 位的分数。

这 k 个关系当且仅当下列关系为真时成立:

$\vee_{j=1}^{k}(X_{ij}=g^{x_{ij}}\wedge Z_{ij}=\{g^{y_{ij}}\}^{x_{ij}}g^{a})$

$\forall a\in\{a_1,a_2,\cdots,a_k\}$。

把这个零知识证明记为 $\prod_j[x_{i1},x_{i2},\cdots,x_{ik},X_i,Z_i]$; $\forall j\in\{1,2,\cdots,k\}$,那里 $X_i=(X_{i1},X_{i2},\cdots,X_{ik})$,$Z_i=(Z_{i1},Z_{i2},\cdots,Z_{ik})$。

每位投票者 V_i 在第二轮公布信息时,需要发布 $Z_i=(Z_{i1},Z_{i2},\cdots,Z_{ik})$ 和相关的 k 个零知识证明 $\prod_j[x_{i1},x_{i2},\cdots,x_{ik},X_i,Z_i]$; $\forall j\in\{1,2,\cdots,k\}$。

任何人都可以计算 $\prod_{i=1}^{n}\{g^{y_{ij}}\}^{x_{ij}}g^{v_{ij}}=g^{\sum_{i=1}^{n}v_{ij}}$, $\forall j\in\{1,2,\cdots,k\}$。这个结论源于事实 $\sum_{i=1}^{n}x_{ij}y_{ij}=0$; $\forall j\in\{1,2,\cdots,k\}$[14]。证明如下所示:

对于上文定义的 x_{ij},y_{ij},$\sum_{i=1}^{n}x_{ij}y_{ij}=0$; $\forall j\in\{1,2,\cdots,k\}$。

证明:根据协议,$(\sum_{l<i}x_{lj}-\sum_{l>i}x_{lj})=0$; $\forall j\in\{1,2,\cdots,k\}$。

对于任何固定的 $\forall j\in\{1,2,\cdots,k\}$,$\sum_{i=1}^{n}x_{ij}y_{ij}=\sum_{i=1}^{n}x_{ij}(\sum_{l<i}x_{lj}-\sum_{l>i}x_{lj})=0$;

根据上文,不难得出,第 j 位候选者的总分是 $\sum_{i=1}^{n} v_{ij}$,在一个小型的董事会选举中,对任意的 $\forall j \in \{1,2,\cdots,k\}$ 来说,它显然是一个较小的数字。可以依靠穷举计算得到 $g^{\sum_{i=1}^{n} v_{ij}}$ 的离散对数值,从而获取所有候选者最终的总分。而在这个过程中,不会泄露投票者的投票意向。

但是,为了让选民和候选者遵守选举规范,在生成选票后,首先要让所有投票者(包括候选者)计算选票和其选票的合法性零知识证明的哈希值并公布。待全部投票者都公布哈希值后,候选者以外的投票者方可公布选票和选票的合法性零知识证明。

2.2.4　第三轮

第三轮:只有当候选者以外的投票者都投完票后,才会进行第三轮投票,候选者会被要求在某一个短暂的时间段内投票,且投票期间候选者们需要开摄像头直播,记录自己和其他候选者的操作,并将录像上传至区块链。待所有候选者的选票和其选票的合法性零知识证明都被公布后,系统自计数,得到选举结果,选举结束。

2.2.5　安全分析

在该选举方案中,协议采用了数种安全措施,归纳如下所示。

(1)两种零知识证明,前者证明了投票者知道公钥对应的私钥,确保了投票者的身份。后者证明了投票者构造的选票的合法性。两者的结合保护了投票者的隐私不被泄露。

(2)哈希的使用,要求投票者们在公布选票和选票的合法性零知识证明前,先公布它们的哈希值,使得投票者如果更改选票,就会被发现。

(3)让候选者们在第三轮投票,通过把候选者和普通选民的投票时间区分开,使得普通选民不可能成为最后一名投票者,提前知道选举的结果。这使得普通选民临时更改自己的选票或放弃投票,破坏此轮选举的行动失去了意义。再配合适当的惩罚措施,极大地降低了选民违规的概率,参考西方尽年来选举活动中出现的各种骚乱现象,这种做法是非常有现实意义的。

(4)让候选者们彼此监督,候选者之间天然的矛盾使得他们难以达成完全共谋,否则,选举本身失去意义。而候选者们特殊的身份也使得他们受到更多的约束,难以向普通的选民一样在已经公布了选票的哈希值后,再临时更改选票或放弃投票。而纵使有候选者冒着巨大的代价违规,让选举重新举行即可。且专为候选者定制的短暂的投票时间,直播录像,都进一步压缩了最后一位投票的候选者的操作空间,让他难以利用提前知道投票结果这一点。

而如果是特别重大的选举,甚至可以采取限制其人身行动,直到选举最终结束,使得即使他知道了选举的结果,也无法透露给他人。将其对选举的影响降到最低。

3　协议性能分析

在本节中,将会分析协议的计算和通信成本,并与其他已有的协议作对比。该文提出的协议总共三轮。而任何安全多方计算协议中,至少需要两轮才能安全地计算一个函数。因为在类似的协议中,指数运算是最昂贵的操作,所以根据指数运算的次数来分析协议。假设在选举中竞争的候选人的数量是 k,在第一轮中,每个选民需要做 k 次幂运算来生成公钥。另外,它们的 k 个密钥也需要 k 个零知识证明与之对应,其中的每一个零知识证明都需要一次幂运算来创建和 1.2 次幂运算来验证。这里不计算验证公钥的代价,这需要在有限域设置中进行一次幂运算,但在椭圆曲线设置中基本上是无代价的,假设同时多次指数(SME)技术[15]被用来优化计算。使用 SME 方法,$g^x h^y$ 形式的项需要大约 1.2 次幂运算。因此,投票者需要在第一轮中做 $2k$ 次幂运算来创建她的公钥以及零知识证明。为了验证这些零知识证明,需要做 $1.2k$ 次的幂运算。在第二轮,一个选民需要做 k 次幂运算来生成选票。此外,投票人需要创建 k 个选票的合法性零知识证明。每一个合法性零知识证明需要 $(2.4(k-1)+2)$ 次幂运算来生成,以及 $2.4k$ 次幂运算来验证。因此,k 个合法性零知识证明需要 $(2.4k^2-0.4k)$ 次幂运算来生成,并需要 $2.4k^2$ 次幂运算来验证。因此,在第二轮中,投票人需要做 $(k+(2.4k^2-0.4k))$ 次求幂来生成他的选票。总而言之,投票人需要做 $(2k+(k+(2.4k^2-0.4k)))$ 次求幂,即 $(2.4k^2+2.6k))$ 次求幂才能在选举中投票。验证选票所需的求幂总次数等于 $(1.2k+2.4k^2)$。表 1 强调了当 k 个候选人参与选举时,协议的计算成本。

表 1　方案的代价

第一轮			第二轮			第三轮		
公钥	零知识证明	总计	选票	零知识证明	总计	选票	零知识证明	总计
k	k	$2k$	k	$2.4k^2-0.4k$	$2.4k^2+2.6k$	k	$2.4k^2-0.4k$	$2.4k^2+2.6k$

现在,将提议的投票协议与一些知名的投票协议的性能进行比较。文献中提出了几种加密投票协议,但是大多数协议通过引入一组可信任的计数权限来提供安全性和完整性保证。为了便于比较,只考虑不涉及任何计数机构的自计数投票协议。因此,主要将文中协议与 Kiayias-Yung[16]、Groth[17]、OV-Net[3] 协议和 Panja[18] 协议进行比较。表 2 强调了候选者人数为 k 时,提出的博尔达计数方案与已有的四个多数投票解决方案之间的比较。

表 2 不同方案计算量的对比

协议	选举类型	轮数	总计
Kiayias-Yung[16]	非排序投票	3	$O(n^2k)$
Groth[17]	非排序投票	$n+1$	$O(nk)$
OV-Net[3]	非排序投票	2	$O(nk)$
Somnath[18]	排序投票	2	$O(nk^2)$
文中协议	排序投票	3	$O(nk^2)$

4 结束语

提出了一个 3 轮自计数的博尔达计数电子投票方案。该方案不依赖第三方,能自计数,允许同时对多个候选人按博尔达计数的方式投票。与同类方案相比,在保留了自计数,不依赖第三方等特点的同时,还堵住了自计数方案选民利用最后一位投票者提前知道投票结果的漏洞,大幅降低了普通投票者恶意影响,破坏选举的概率。其运行效率也无明显差异。具有实用性,能为现实中的选举活动提供参考。

参考文献:

[1] 袁 勇,王飞跃. 区块链技术发展现状与展望[J]. 自动化学报,2016,42(4):481-494.

[2] ZHAO Z,CHAN T H H. How to vote privately using bitcoin [M]. Switzerland:Springer International Publishing,2016.

[3] FENG Hao,PETER Y A R,ZIELINSKI P. Anonymous voting by two-round public discussion[J]. IET Information Security,2010,4:62-67.

[4] 张 奥,白晓颖. 区块链隐私保护研究与实践综述[J]. 软件学报,2020,31(5):1406-1434.

[5] GOLDWASSER S,MICALI S,RACKOFF C. The knowledge complexity of interactive proof systems[J]. SIAM Journal on Computing,1989,18(1):186-208.

[6] 蒲泓全,崔 喆,刘 霆,等. 安全性电子投票方案研究综述[J]. 计算机科学,47(9):275-282.

[7] MCCORRY P,SHAHANDASHTI S F,FENG Hao. A smart contract for boardroom voting with maximum voter privacy [C]//Financial cryptography and data security, volume 10322 of lecture notes in computer science. Switzerland: Springer,2017:357-375.

[8] 董友康,张大伟,韩 臻,等. 基于联盟区块链的董事会电子投票系统[J]. 网络与信息安全学报,2017,3(12):17-23.

[9] 于天娇,曹春杰,王隆娟,等. 基于联盟链的匿名电子投票方案[J]. 网络空间安全,2019,10(12):22-29.

[10] 颜春辉,游 林. 基于区块链的安全投票系统设计与实现[J]. 通信技术,2018(8):1979-1989.

[11] SCHNORR C P. Efficient signature generation by smart cards [J]. Journal of Cryptography,1991,4:161-174.

[12] FIAT A,SHAMIR A. How to prove yourself:practical solutions to identification and signature problems[J]. Advances in Cryptology-Eurocrypt'86,1999,263:186-194.

[13] 周 振,严广乐. 基于区块链技术的匿名电子投票协议设计[J]. 软件导刊,2020,19(1):229-233.

[14] HAO F,ZIELINSKI P. A 2-round anonymous veto protocol [C]//Security protocols, international workshop. Cambridge,UK:Springer,2006.

[15] MENEZES A,VAN OORSCHOT P C,VANSTONE S A. Handbook of applied cryptography[M]. Boca Raton:CRC Press,1996.

[16] KIAYIAS A,YUNG M. Self-tallying elections and perfect ballot secrecy[C]//International workshop on practice & theory in public key cryptosystems:public key cryptography. Switzerland:Springer-Verlag,2002:141-158.

[17] GROTH J. Efficient maximal privacy in boardroom voting and anonymous broadcast[C]//8th international conference on financial cryptography. Berlin:Springer,2004.

[18] PANJA S,BAG S,HAO F,et al. A smart contract system for decentralized Borda count voting[J]. IEEE Trans. Eng. Manage,2020,67(4):1323-1339.