计算机科学
COMPUTER SCIENCE

基于区块链的分布式加密投票系统

张伯钧, 李洁, 胡凯, 曾俊豪

引用本文

张伯钧, 李洁, 胡凯, 曾俊豪.基于区块链的分布式加密投票系统[J]. 计算机科学, 2022, 49(11A): 211000212-6.

ZHANG Bo-jun, LI Jie, HU Kai, ZENG Jun-hao. Distributed Encrypted Voting System Based on Blockchain [J]. Computer Science, 2022, 49(11A): 211000212-6.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.211000212

基于区块链的分布式加密投票系统

张伯钧[1,2]　李　洁[1,2]　胡　凯[1,2]　曾俊豪[1]
1 北京航空航天大学计算机学院　北京 100191
2 云南省区块链应用技术重点实验室　昆明 650233
(zhangbojun@buaa.edu.cn)

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。当前电子投票系统具有中心化的特点,投票过程难以公开透明,选民无法验证选票结果,需可信第三方计票机构参与唱票。针对以上问题,为了更好地适应愈加丰富的应用场景,文中研究并提出了一种基于区块链的分布式加密投票系统。使用分布式环境下的ElGamal加密算法保证了整个投票过程的安全保密性,任何人或机构无法破解获得选票的中间结果。使用区块链智能合约自动执行的机制取代了传统的第三方可信计票机构,实现了自动唱票。由于所有选票信息均存储在区块链上,进一步保证了投票过程透明公开且结果可验证、可追溯。实验结果表明,投票系统的瓶颈为了唱票环节中的累乘算法。为了提高计算效率,进一步采用链上链下协同计算的方式,在保证票据安全性的前提下,链下通过并行计算加快计算速度。最后,通过安全性和性能分析表明,该机制具有良好的可扩展性,是一种实用和安全的电子投票系统设计方案。

关键词:电子投票;区块链;智能合约;ElGamal算法;协同计算
中图法分类号　TP311

Distributed Encrypted Voting System Based on Blockchain

ZHANG Bo-jun[1,2],LI Jie[1,2],HU Kai[1,2] and ZENG Jun-hao[1]
1 School of Computer Science and Engineering,Beihang University,Beijing 100191,China
2 Key Laboratory of Blockchain Application Technology of Yunnan Province,Yunnan Innovation Research Institute of Beihang University,Kunming 650233,China

Abstract　With the development and progress of society,many application scenarios require voting. The current electronic voting system has the characteristics of centralization,the voting process is difficult to be open and transparent,voters cannot verify the results of the ballot,and a trusted third-party vote-counting agency is required to participate in the voting. In response to the above problems,in order to better adapt to the increasingly abundant application scenarios,this paper studies and proposes a distributed encrypted voting system based on blockchain. The ElGamal encryption algorithm in a distributed environment ensures the security and confidentiality of the entire voting process,and no one or organization can crack the intermediate results of obtaining votes. The automatic execution mechanism of blockchain smart contract replaces the traditional third-party trusted ticket counting agency to realize automatic ticket counting. Since all voting information is stored on blockchain,it further ensures that the voting process is transparent and open,and the results can be verified and traceable. Experimental verification shows that the bottleneck of the voting system is the accumulative multiplication algorithm in the voting process. In order to improve computing efficiency,the method of on-chain and off-chain collaborative computing is further adopted. Under the premise of ensuring the security of bills,the off-chain speed of calculation is accelerated through parallel computing. Finally,the security and performance analysis shows that the mechanism has good scalability and is a practical and safe electronic voting system design scheme.

Keywords　Electronic voting,Blockchain,Smart contract,ElGamal algorithm,Collaborative computing

1　引言

投票是选民表达自己民意的方式,它被广泛应用于各类选举、决策等群治活动中。在互联网兴起之前,投票的主要形式是线下投票。随着互联网领域的蓬勃发展,大部分线下投票场景被低成本的线上电子投票所取代。线上电子投票是

基金项目:国家重点研发项目(2018YFB1402702);云南省重大科技专项:基于服务智能合约的云南稀贵金属材料基因数据可信交易技术研发(202002AB080001-8);云南省重大科技专项:生物资源数字化开发应用(202002AA100007)
This work was supported by the National Key R&D Project(2018YFB1402702),Yunnan Province Major Science and Technology Project:Research and Development of Yunnan Rare and Precious Metal Materials Gene Data Trusted Transaction Technology Based on Service Smart Contract(202002AB080001-8) and Yunnan Province Major Science and Technology Project:Digital Development and Application of Biological Resources(202002AA100007).
通信作者:胡凯(hukai@buaa.edu.cn)

依靠互联网技术进行在线投票、唱票的投票方式。与传统的线下投票方式相比,电子投票流程更加简单,计票更加容易,节省了大量的成本和时间,并且几乎不受投票规模的限制。在大多数大型投票场景中,由于线下投票难以组织且成本较高,因此线上投票替代了传统的线下投票成为了主流的投票方式。

然而,目前的线上电子投票也存在着一些缺陷,投票结果的安全性和透明性常常会受到质疑。大多数电子投票方案在投票过程中的安全性和隐私性由投票服务提供方或第三方可信机构 CA(Certificate Authority)来进行信誉担保。在第三方可信机构或投票服务提供方出现安全和隐私泄露问题,或者是遭遇恶意网络攻击时,整个投票结果将变得不安全。在一些对隐私性和投票结果安全性要求较高的场景中,目前的线上电子投票系统还不能较好地被广泛使用。

近年来,区块链技术受到了许多国内外研究学者的关注。区块链的本质是一个公开透明的数据库账本,记录所有的交易信息。其特点是在没有第三方中介的情况下,可以提供去中心化、不可篡改、可溯源、公开透明的安全特性。因此,区块链技术可以有效地解决现有投票系统中存在的中心化、隐私泄露等问题。区块链智能合约又由于具有一致性、可验证性与强制性,因此可以很好地替代投票系统中中间人的身份,进而自动化地执行,进行投票状态的流转。因此,区块链与投票系统的结合,是未来研究的重点,也是一种新颖的投票模式。

2 相关工作

在当下的互联网时代,线上电子投票被广泛应用在各种各样的投票场景中。线上电子投票系统可以根据投票过程分为两类:1)依赖第三方机构或者是服务提供方的中心化投票系统;2)基于分布式系统去第三方的去中心化投票系统。1981 年 Chaum 等[1]提出了首个线上电子投票方案,该方案设计了一个基于数字别称和数字加密的匿名网络,因此通过该网络进行投票来隐藏真实身份。匿名网络能够保护用户隐私,但是由于匿名网络是理论上的假想网络,因此该方案在实际应用中仍存在问题。之后,在 1992 年 Fujioka 等[2]提出了首个适用于大规模投票场景的电子投票方案,该方案基于盲签名对选票进行了加密,因此能够一定程度上保证投票者的隐私性。但是,在计票过程中仍然引入了第三方计票机构,而且对于投票者的身份验证也存在着漏洞。在 2000 年,Peng 等[3]提出了使用盲签名的投票方案。相比 Fujioka 提出的方案,Peng 的方案在安全性上有所提高,并且投票者可以验证自己的选票是否被正确计入。但是这个方案中仍然引入了第三方 CA,因此仍然存在第三方 CA 作弊等安全问题。

2015 年,Chan 等[4]首次提出了基于区块链的电子投票方案,该方案基于比特币实现了投票行为的奖惩机制,实现了投票的公开透明。但是该方案是基于比特币所实现的,在实际应用中不能得到较好的普及,并且受比特币共识机制所影响,该方案计票效率低下且复杂度较高,另外该方案在投票结果安全性方面也存在一些漏洞。2016 年,Lee 等[5]提出在 Chan 的基础上引入可信第三方来保障选票安全。2017 年,McCorry 等[6]提出了基于以太坊的自动化投票方案,该方案基于智能合约实现了在区块链上进行自动计票,并通过环签名保护了选民隐私。但是该方案设置的投票场景只能是二选一,即从两个候选者中选择一个投票的场景。同年,Qin 等[7]提出了基于认证技术的量子投票方案。该方案结合了量子认证技术,并结合量子纠缠状态,研究了两种量子投票方法。Qin 等的方案由于使用了量子认证技术,在加密算法安全性方面有所提高,但是量子技术目前尚处于前沿开拓阶段,因此 Qin 的方案实用性较弱。还有一些学者提出了其他的电子投票方案,比如 2019 年 Azougaghe 等[8]基于全同态加密的电子投票方案,2020 年 Zhuang 等[9]提出的基于格的电子投票方案,这些投票方案从其他角度对投票过程中的投票结果安全性进行了加强。但上述方案也都存在着不足,二者提出的方案均是中心化的投票系统,难以阻止第三方作弊等现象。2021 年,Abuidris 等[10]提出了一种结合分片机制的混合共识模型的区块链电子投票系统,提升了投票系统的运行效率和可扩展性。但由于引入了中心的可信节点,其安全性仍有待考察。同年,Ueda 等[11]提出了一种基于以太坊的区块链投票系统,但他们使用 Infura 以太坊服务器与区块链进行通信,而 Infura 的安全性也仍有待考察。除此之外,文献[12]使用了 Zcash 系统来进行电子投票,在不改变原有协议的情况下,利用 Zcash 自带的匿名功能保护投票者的隐私。还有许多基于区块链及智能合约的投票方案[13-15],比较典型的应用有 Fllow my Vote[16],Bitcoin Voting Machine[17]等,这些投票虽然使用了区块链作为底层技术,但仍然依赖第三方来保存用户的隐私数据。因此,如何保障选票在传输过程中的安全性、隐私性,以及去除高度中心化,是亟待解决的问题。

3 系统设计

借鉴前述系统,通过深入分析和总结目前电子投票方案的优缺点,本文认为当前线上电子投票系统的主要问题在于选票传输过程中的安全性和隐私性无法保证,以及投票过程高度依赖第三方可信机构。为了解决这些问题,本文设计了一种基于区块链的分布式加密投票系统。通过使用分布式环境下的 ElGamal 加密算法[18]对选票进行加密,从而保证了选票在数据传输过程中的安全性和投票内容的不可破解性。使用区块链智能合约技术自动执行唱票,从而取代可信第三方计票机构,另一方面也节省了投票成本。由于所有的投票数据均存储在区块链上,保证了投票过程透明公开且结果可验证。

3.1 ElGamal 算法

ElGamal 加密体制是一种常见的非对称加密算法,它是由 Gamal 于 1985 年提出的。ElGamal 算法在有限域上求解离散对数问题,很难在可接受时间内完成,故拥有较高的安全性。ElGamal 算法是同态算法的一种,它满足乘法同态且被广泛应用在数字加密和数字签名领域中,是具有代表性的非对称加密算法。

ElGamal 算法的公私钥生成步骤如下:

步骤 1 随机选择一个位数较长(1 024 bit 以上)的大素数 p,生成有限域的一个生成元 $g\in \mathbb{Z}_p^*$。

步骤 2 选择一个素数 x 满足 $1<x<p-1$,则有公钥 $y=(g,x,p)$,私钥为 x,如式(1)所示:

$$y=g^x \% p \tag{1}$$

步骤 3 令待加密明文为 m,m 满足 $1<m<p-1$。随机选择整数 k:$0<k<p-1$,则有密文为 $C=(c_1,c_2)$。c_1 和 c_2 如式(2)和式(3)所示:

$$c_1=g^x \% p \tag{2}$$

$$c_2 = my^k \% p \tag{3}$$

对密文 C 进行解密，根据费马小定理可得明文 m，即将式(4)代入式(3)可得式(5)：

$$c_1^x * (c_1^x)^{-1} \% p = 1 \tag{4}$$

$$m = c_2 * (c_1^x)^{-1} \% p \tag{5}$$

3.2 分布式加密算法

加密算法主要负责对投票过程产生的选票进行加密，以保证选票和最终结果的安全。当前主流的加密技术分为两种，一种是对称加密算法，以 DES，RC2 为代表，另一种是非对称加密算法，以 RSA，ECC 为代表。但上述算法均为单体非分布式的加密算法，不能很好地应用在本文所提出的投票系统中。如果使用非分布式的加密算法加密选票，那么攻击者可以通过访问区块链得到已投票用户的加密密文和解密信息，再通过逆向工程生成智能合约源代码来模拟智能合约运行，最后破解得到已投票用户的明文选票，最终达到获取实时票数的目的，进而在投票过程中做出对自己有利的行为，影响最终投票结果。而基于分布式加密算法则能够解决这个问题，这是因为在加密选票时是通过所有人的密钥去共同加密的，只有当所有人都提交关于该选票的解密信息时，才能够对该选票进行解密。分布式环境下的 ElGamal 加密算法属于 ElGamal 加密算法的一种变形形式，其核心思想是每个参与者不需要重构出主私钥即可进行解密密文。为了适应本文所设计的区块链投票系统，本文采用分布式环境下的 ElGamal 算法来作为投票协议中的加密算法，巧妙地与投票场景进行结合，从而保障选票在传输过程中的安全性和不可破解性。投票场景下的分布式 ElGamal 算法由 3 部分组成：密钥生成、加密选票、共同解密。

3.2.1 密钥生成

设 p 为 1024 bit 长的大素数，g 为群 $\mathbb{Z}_p^*$ 的生成元。假设一场投票 V 有 n 个用户参与，分别为 $\{Q_1, Q_2, \cdots, Q_n\}$。每个参与者自己拟定各自的私钥 s_i，s_i 为用户自己拟定随机的 16 进制整数，然后基于式(1)生成相应的公钥 $h_i = (g, s_i, p)$，如式(6)所示：

$$h_i = g^{s_i} \% p \tag{6}$$

然后通过每个用户的公钥 h_i，生成用于加密明文选票的公共公钥 H，具体如式(7)所示：

$$H = \sum_{i=1}^{n} h_i \% p \tag{7}$$

3.2.2 加密选票

设 m 为待加密的明文选票，然后随机选取一个正整数 k，其中 $1 \leqslant k \leqslant p-1$，且 k 与 $p-1$ 的最大公约数为 1，则加密函数 $E_{(m)}$ 如式(8)所示。

$$E_{(m)} = (g^k \% p, mH^k \% p) \tag{8}$$

设投票参与者 Q_i 欲投递明文选票 m_i，则 Q_i 投递的加密选票 E_{m_i} 如式(9)所示：

$$E_{m_i} = (g^k \% p, m_i H^k \% p) \tag{9}$$

3.2.3 共同解密

设所有加密选票集合为 S_{em}，则有：

$$S_{em} = \{E_{m_1}, E_{m_2}, \cdots, E_{m_i}, \cdots, E_{m_n} \mid E_{m_i} = (a_i, b_i)\} \tag{10}$$

在得到集合 S_{em}，投票者 i 通过式(11)得到解密信息 D_{m_i}，其中 $t_{m_{ij}}$ 代表投票者 i 对 j 的加密票的解密中间结果。

$$t_{m_{ij}} = (b_j)^{\frac{1}{n}} (a_j^{s_i})^{-1} \% p, E_{m_j} = (a_j, b_j) \tag{11}$$

$$D_{m_i} = \{t_{m_{i1}}, t_{m_{i2}}, \cdots, t_{m_{in}}\} \tag{12}$$

结合所有投票者的解密信息 D_{m_i}，通过式(13)最终可以获得每个投票者的明文选票。

$$\begin{aligned} m_j &= \prod_{i=1}^{n} t_{m_{ij}} \% p \\ m_j &= b_j \left(a_j^{\sum_{i=1}^{n} s_i}\right)^{-1} \% p \end{aligned} \tag{13}$$

其中与大公钥 H 所对应的主私钥 S 如式(14)所示：

$$S = \sum_{i=1}^{n} s_i \% p \tag{14}$$

由式(11)可以看出，每个投票参与者只需要利用自己的私钥 s，即可计算出加密票的解密中间结果 t_m，再利用式(13)，将所有投票参与者的中间结果进行累乘，即可还原出主私钥 S。但这个过程仅当所有人投票完毕后，才可还原出选票明文，从而保证了选票内容的不可破解性。

3.3 分布式投票协议设计

分布式投票协议是整个投票系统的核心，它占据着十分关键的地位，它的好坏以及如何与区块链有效结合直接决定了投票过程的公平性与系统的健壮性。因此，设计的协议应当能够正确地反映投票结果，并且实现投票、唱票的自动化过程。本文提出了一个基于区块链的投票协议，包括创建投票、选民参与、投加密选票、共同解密和唱票共 5 个阶段。首先由一名用户发起一场投票 V，选民选择参与该场投票，此过程会将相应的个人公钥 h 发送至区块链，等所有人均参与完毕后，由区块链智能合约计算出本场的大公钥 H，每位用户通过使用此大公钥进行加密选票。等到所有人完成加密选票后，启动共同解密阶段，每个人再用自己的私钥 s 对所有人的加密选票进行解密。最后由区块链智能合约将所有人的解密信息进行汇总唱票得出最终结果。其投票协议流程图如图 1 所示。

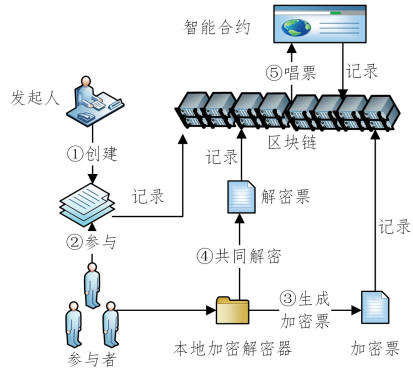

图 1 投票协议流程图

Fig. 1 Voting protocol flowchart

3.3.1 创建投票

任何用户都能够创建任意数量的符合格式的投票 V。一场投票的元数据信息应包含以下几点：投票名称、投票摘要、投票发起人、投票起始时间、投票结束时间，这些信息应该全部记录在区块链账本中，为后续投票、唱票以及查询验证选票提供基础保障。

3.3.2 选民参与

在创建一场投票 V 后，在规定的结束时间范围内，用户可参与该场投票。每一位参与投票者会将自己的公钥 h 上传至区块链账本中，为后续生成大公钥 H 提供保障。大公钥 H 在每一个选民投加密票或是投共同解密票时均有所涉及。

其中个人公钥 h 由 3.1 节的式(1)生成，大公钥 H 通过分布式 ElGamal 加密算法式(7)生成。为了满足加密模块中所制定的分布式加密算法，规定每位投票者采用共同的 g 和 p，g 和 p 的含义已在 3.1 节中定义。

3.3.3 投加密票

已参与投票 V 的用户必须在规定时间内进行(第一阶段)投加密票，如果超过规定时间投递加密票，则视为超时。如果多次投递，则视为异常。正常的加密选票将会被记录在区块链账本中，为后续共同解密以及存证验证提供保障。参与投票的用户需要按照以下步骤进行投加密票。

首先生成规定格式的明文选票 X_i，明文选票格式的统一规定如式(15)所示：

$$X_i=(a_{i1},a_{i2},\cdots,a_{ij}),a_{ij}\in\{0,1\} \tag{15}$$

其中，X_i 表示参与者 i 的明文选票，为二进制格式，其中 a_{ij} 为 0 表示参与者 i 支持候选者 j，为 1 表示参与者 i 不支持候选者 j。X_i 是维度为 n 的向量，n 表示候选者的总数。在得到规定格式的明文选票之后，需要对选票进行加密，加密算法在 3.2.2 节中介绍。根据分布式算法可得，加密选票 E_x 如式(16)所示，T 是选票明文 X 的数学表达。

$$E_x=(g^k\%p,TH^k\%p),T=\sum 2^{a_{ij}} \tag{16}$$

其中，加密选票 E_x 即为投票内容。

3.3.4 共同解密

投票 V 在第一阶段投加密票结束之后，用户必须在规定时间内进行第二阶段投票共同解密，如果超过规定时间解密，则视为超时。如果多次提交解密，则视为异常。参与共同解密的用户需要按照规定步骤提交共同解密信息。

通过举例的形式来解释共同解密环节的具体流程。设有正处于共同解密阶段的投票 V，参与投票人数为 N，候选者人数为 M。参与者 i 所投加密选票为 E_{x_i}，其中 $1\leqslant i\leqslant N$。则对于参与者 i 而言，待解密选票集合 S_{ex} 由表达式(17)所示。获得 S_{ex} 之后，参与者 i 需要按照加密模块所定义的分布式加密算法生成 S_{cx_i}，S_{cx_i} 的计算式如式(18)所示。c_j 为中间变量，无实际意义。

$$S_{ex}=\{a_1,a_2,\cdots,a_j,\cdots,a_n\},E_{x_i}=(a_j,b_j) \tag{17}$$

$$S_{cx_i}=\{c_1,c_2,\cdots,c_j,\cdots,c_n\},c_j=(a_j^{s_i})^{-1} \tag{18}$$

共同解密实际上是已投票用户根据第一阶段记录在区块链账本中的所有人所投的加密选票，提交各自对应解密信息的过程。

算法 1 共同解密算法

输入：(S_{ex}, s_i) / * S_{ex}为加密选票集合，s_i 为个人私钥 * /

输出：(S_{cx_i}) / * 共同解密票信息集合 * /

1. S_{cx_i}←{} / * 初始化共同解密信息集合 * /

2. for a_j in range $S_{ex}=\{a_1,a_2,\cdots,a_j,\cdots,a_n\}$ / * 循环遍历加密选票集合 * /

2.1. c_j←$(a_j^{s_i})^{-1}$ / * 计算加密选票的中间结果 * /

2.2. c_j append to S_{cx_i} / * 将中间结果加入共同解密信息集合 * /

3. return S_{cx_i} / * 返回某人的最终共同解密信息 * /

3.3.5 唱票

此阶段不需要任何第三方可信的 CA 参与，而是由区块链智能合约技术自动化执行，进行票数计算。根据获得的解密信息 S_{cx_i} 对选票进行解密，解密算法如式(5)所示。其中，t_{ij} 表示参与投票的用户 i 对候选者 j 是否投票，c_{ij} 为 S_{cx_i} 中的元素 c_j。

$$t_{ij}=b_i\prod_{j=1}^{n}c_{ij}\%p,c_{ij}=(a_j^{s_i})^{-1} \tag{19}$$

最后得到投票结果 R 如式(20)所示：

$$R=(r_1,r_2,\cdots,r_j,\cdots,r_n),r_j=\sum_{i=1}^{n}t_{ij} \tag{20}$$

其中，t_{ij} 表示参与投票的用户 i 对候选者 j 是否投票，r_j 为候选者 j 的总票数。

算法 2 唱票算法

输入：(S_{cx_n}, b_n, n, p) / * S_{cx_n}为所有人的共同解密信息，b_n 为所有人的加密信息密文 $E_{(m)}=(a,b)$中的 b 集合，n 为候选者人数，p 为随机 1024 bit 长的大素数 * /

输出：(R) / * 最终每个人的得票情况 * /

1. K←{}, R←{} / * 初始化汇总后解密信息集合 K 和最终每个人的得票集合 R * /

2 for i in range S_{cx_n} / * 循环遍历所有人的共同解密信息集合 * /

2.1. K_i←getFromKSet(S_{cx_i}) / * 将第 i 人的共同解密信息汇总后放入集合 K * /

3. for i in range K / * 循环遍历汇总后解密信息集合 K * /

3.1. C_i← getFromKSet(i) / * 得到第 i 人的汇总后解密信息 C_i * /

3.2. for j in range of C_i / * 遍历第 i 人的汇总后解密信息 C_i * /

3.2.1. t_{ij}←$b_i\prod_{j=1}^{n}c_{ij}\%p$ / * 计算中间结果 t_{ij} * /

3.2.2. $r_j=\sum_{i=1}^{n}t_{ij}$ / * 汇总第 j 人的得票结果 r_j * /

3.2.3. r_j append to R / * 将每个人的得票情况添加至结果集 R * /

4. return R / * 返回最终每个人的得票情况 * /

4 实验验证

为了验证本文方案的执行效率与可行性，在实验室搭建了测试用的云计算环境。云计算环境采用 4 台配置相同的 Inter(R) Xeon E5-2620 处理器，64 GB，DDR4 内存，512 GB，SSD 硬盘的工作站组成的服务器集群，集群上部署北航链作为底层的区块链平台。使用配置为 Inter i7-8550U，1.99 GHz 处理器，16 GB 内存的 1 台笔记本电脑作为测试入口，部署区块链投票系统。实验使用 Java 1.8 语言，通过启动线程的方式来模拟用户投票行为，下述所有实验数据均为 10 次实验的平均值。实验组网如图 2 所示。

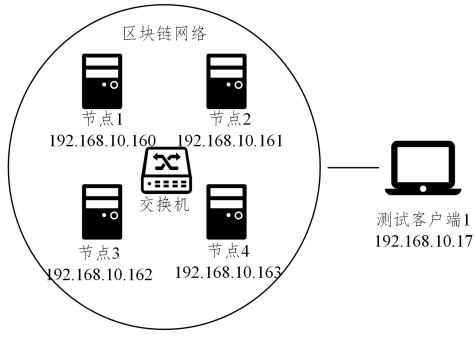

图 2 实验组网图

Fig. 2 Experimental network diagram

4.1 实验 1:可扩展性实验分析

对于一个人来讲，投票过程主要分为两个阶段，第一阶段是对明文的加密投票，第二阶段是对所有人的密文进行解密投票，这两个阶段的时间复杂度前者为 O(1)，后者为 O(n)，但由于这些过程均在本地加密解密器进行操作，因此理论上来讲是真正的并行操作。对于本文提出的加密解密算法均

需要个人的私钥来进行参与运算，因此私钥长度对于加密后的密文的安全性有很强的相关性，因此实验 1-1 测试密钥长度与加密解密的时间关系如图 3 所示。

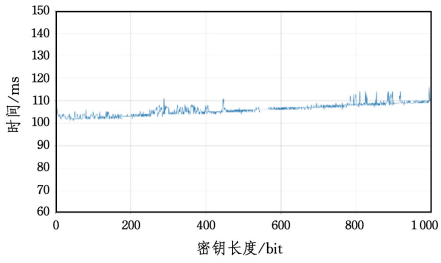

图 3　实验 1-1 密钥长度与加密解密时间关系

Fig. 3　Relationship between key length and encryption and decryption time of experiment 1-1

由图 3 可知，加密与解密的时间几乎趋近于常数 105 ms，与密钥长度无关。密钥越长，对密文的保护性就越高，因此从加解密的效率以及对密文的安全性考虑，密钥长度具有很好的扩展性。

为了保证投票公平公正，没有引入第三方中介，唱票阶段应在区块链智能合约中自动执行，算法本身的效率与所依托的区块链系统及其选用的共识算法有很强的相关性。为了控制变量，实验 1-2 与实验 2 采用相同的区块链共识算法，实验 1-2 测试参与人数与唱票时间的关系，结果如图 4 所示。

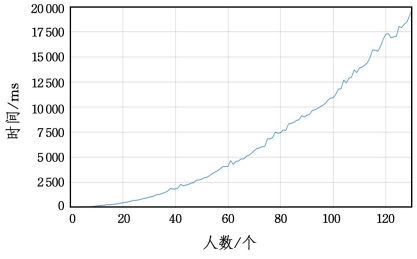

图 4　实验 1-2 参与人数与唱票时间的关系

Fig. 4　Relationship between number of participants and voting time of experiment 1-2

由图 4 可见，参与人数和最终唱票时间基本成正比，当人数增至 100 人时，唱票阶段耗时 10 s 左右，对于区块链投票系统来讲，实时性要求不高，因此该实验的结果可以接受。

4.2　实验 2：链上链下协同计算实验分析

由实验 1-2 以及唱票算法表达式(19)可知，上述唱票过程阶段耗时最多的是将每个人的解密票进行累乘操作，得到最终个人的投票结果。为了提高性能，这部分可以采用链上链下协同计算。链下读取链上投票数据，做累乘计算获取每个人的投票中间结果，汇总结果后传至区块链，再通过智能合约共识进行最终结果的计算。具体步骤如下：

步骤 1　在链上获取存储在区块链中参与者的共同解密选票，并汇总每个人的解密选票结果集合 S_{cx}。

步骤 2　将集合 S_{cx} 发送至链下，由表达式(19)计算每个人的投票中间结果 $\sum_{j=1}^{n} c_j$。

步骤 3　将中间结果集合返回至链上，通过区块链智能合约再次进行计算，得出最终结果 R，并将此信息记录在区块链中，以便今后发生争议后可以进行追溯。其性能对比图如图 5 所示。

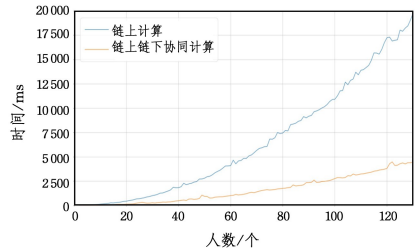

图 5　链上与链上链下协同计算对比图

Fig. 5　Comparison of on-chain and on-chain&off-chain collaborative computing

由图 5 可见，当参与投票人数为 120 时，协同计算方式占时仅为链上计算方式的 1/5，说明协同计算可以很好地提高唱票效率，并且由加密算法原理可知，链下部分如果篡改了结果将无法解密得到正确结果，因此该方法是安全且有效率的，很好地提高了算法的可扩展性。

5　方案分析与评估

5.1　安全性分析

在本文设计的投票系统中，每一位投票者所投出的选票内容都是通过个人私钥经过本地线下加密器加密产生的。该私钥仅自己可知，不需要上传至系统中，并且对于不同的选票主题来讲，每次都会有一个随机数 k 来保证所投的加密票无规律性可言。唱票智能合约的状态和内容是保存在区块链上且公开透明的，链上的用户可以对唱票代码进行审查，不会发生合约创建者规定之外的行为。在每次的投票环节，投票者没有透露一点关于投票的详细信息，即便攻击者得到了某个人的投票加密信息，由于分布式 ElGamal 加密算法保证，当且仅当只有得到所有人的解密投票信息时才可以计算出某个人的投票明文内容，最大程度地保证了方案的安全性。使用反证法证明如下：

不妨设共有 n 人参与某场投票，已有 k 人进行投递解密选票信息，其中 $1 \leqslant k < n$。假设命题成立，即得到部分人的解密投票信息即可计算出这些人的选票内容。

由式(11)、式(13)可知，第 j 人的解密信息如式(21)所示：

$$\begin{aligned} m_j &= \prod_{i=1}^{k} t_{m_{ij}} \% p \\ m_j &= (b_j)^{\frac{k}{n}} \left(\prod_{i=1}^{k} (a_j^{s_i})^{-1}\right) \\ m_j &= (b_j)^{\frac{k}{n}} \left(a_j^{\sum_{i=1}^{k} s_i}\right)^{-1} \end{aligned} \tag{21}$$

其中，可推导出主私钥 $S = \sum_{i=1}^{k} s_i$，由于 $1 \leqslant k < n$ 与式(14)相矛盾。即假设命题不成立，证明完毕。

5.2　方案正确性分析

下面对以上设计的基于区块链的分布式加密投票系统的正确性做一个客观分析与评价。

(1)民主性：通过投票主题发布的形式，选民可以在公示栏内看到所有投票主题与相关内容，自主选择想要参与决策的方案，从而保障每个选民的选择自由与灵活性，在民主性方面可以满足要求。

(2)自唱票性：本投票方案符合自唱票特性，通过智能合约程序自我执行的特点，取代了第三方中心化的计票机构，

进而也避免了第三方机构可能会作弊的风险。

(3)公平性:在统计选票阶段,只有在规定投票时间内,当最后一位选民投票成功后,系统才会自动触发唱票智能合约进行最终结果的计算。因此,只要存在未在规定的时间内投票的选民,投票结果就无法被预先计算。因此,该方案具有公平性。

(4)无争议性:本文方案以区块链为身份认证的通道,对投票者的区块链地址进行有效验证,任何无效的地址均不能在此投票系统中参与投票。这样也保证了投票结果的准确性,投票方案无争议性。

(5)保密性:本文设计的投票系统中,每一位选民投出的选票内容 E_x 均是经过 ElGamal 分布式加密算法加密过的,每次都会有一个随机数 k 来保证所投的加密票无规律性可言,进而保证了选票的保密性。

(6)准确性:本文设计的投票方案为 5 个阶段:创建投票、选民参与、投加密票、共同解密以及唱票。在选民参与阶段,若该选民选择参与本场投票,系统会将其区块链地址记录,来保证每个地址只能投两次票,即一次加密票和一次共同解密票。与此同时,选民每次做出决策之后,都需要使用各自的私钥进行签名,区块链收到此选票后,会先进行验签操作来保证票力的准确性。由于私钥是保存在自己本地,因此作弊者也无法伪造弃权者签名,并且也可检测作弊的行为。

(7)可验证性:所有的选票信息会记录在区块链中,投票者在提交了自己的选票之后,可以在区块链浏览区中查询自己的选票信息哈希值是否一致,基于区块链上的数据公开可验证性,从而保证本文方案的投票结果具有可验证性。

结束语 本文提出了一种分布式加密并结合区块链智能合约的电子投票系统。将分布式环境下的 ElGamal 加密算法应用到了电子投票系统中,有效地解决了选票在传输过程中的安全性等问题。通过唱票智能合约自动执行的特性,取代了原有中心化的第三方可信计票机构。同时由于区块链具有不可篡改、不可逆的特性,保证了选票结果的安全性与真实性。将所有与投票相关的数据记录在区块链中,使整个的选举过程公开透明,所有参与者均可从链上获得相同的信息。最后通过性能分析,本系统在满足安全要求的前提下具有一定可扩展性;另外,唱票阶段可以通过链上链下协同计算,在保证票据安全性的前提下,链下可以通过并行计算加快执行速度,因此该系统也适用于大规模的投票。在未来的研究工作中,可以针对本文提出的电子投票协议,研究更加安全可靠的链上链下传输算法,以进一步保证数据传输过程的安全性。

参 考 文 献

[1] CHAUM D L. Untraceable electronic mail, return addresses, and digital pseudonyms[J]. Communications of the ACM, 1981, 4(2):84-88.

[2] FUJIOKA A, OKAMOTO T, OHTA K. A practical secret voting scheme for large scale elections[C]// International Workshop on the Theory and Application of Cryptographic Techniques. Berlin: Springer, 1992: 244-251.

[3] PENG S S. Research on the secure electronic voting scheme and its anonymity[D]. Shanghai: Shanghai Jiaotong University, 2008.

[4] ZHAO Z, CHAN T H. How to vote privately using bitcoin [C]// International Conference on Information and Communications Security. Cham: Springer, 2015: 82-96.

[5] 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(2): 123.

[6] 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.

[7] QIN J Q, SHI R H, ZHANG R. Quantum voting protocol based on controlled quantum secure direct communication[J]. Journal of Quantum Electronics, 2018, 35(5): 558-566.

[8] AZOUGAGHE A, BENMILOUD M, BELKASMI M, et al. Electronic voting scheme based on additive homomorphic encryption[J]. Journal of Information Assurance & Security, 2019, 14(4).

[9] ZHUANG L S, CHEN J, WANG Q Y. Lattice-based Linkable Threshold Ring Signature under Electronic Voting Protocol[J]. Journal of Cryptography, 2020, 8(3): 402-416.

[10] ABUIDRIS Y, KUMAR R, YANG T, et al. Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding[J]. Etri Journal, 2021, 43(2): 357-370.

[11] UEDA E T, DA S M, DA S A, et al. A Proposed Blockchain-Based Voting System with User Authentication through Biometrics[J]. Journal of Information Security and Cryptography (Enigma), 2021, 8(1): 1-11.

[12] TARASOV P, TEWARI H. Internet voting using zcash[J]. International Association of Cryptological Research Cryptol ePrint Arch, 2017, 23(4): 585-593.

[13] AYED A B. A conceptual secure blockchain-based electronic voting system[J]. International Journal of Network Security & Its Applications, 2017, 9(3): 1-9.

[14] DAGHER G, MARELLA P B, MILOJKOVIC M, et al. Broncovote: secure voting system using ethereum's blockchain[J]. Information Systems Security and Privacy, 2018, 4(4): 96-107.

[15] LAI W J, HSIEH Y C, HSUEH C W, et al. DATE: a decentralized, anonymous, and transparent e-voting system[C]// 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN). IEEE, 2018: 24-29.

[16] Fllowmyvote: Follow my vote[EB/OL]. (2012-09-01). https://followmyvote.com, 2017.

[17] OSGOOD R. The future of democracy: blockchain voting[J]. COMP116: Information Security, 2016, 8(1): 1-21.

[18] ElGAMAL T. A public key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE Transactions on Information Theory, 1985, 31(4): 469-472.

ZHANG Bo-jun, born in 1997, postgraduate. His main research interests include blockchain and distributed system.

HU Kai, born in 1963, professor. His main research interests include distributed system, blockchain and formal verification.