



基于实用拜占庭容错算法的区块链电子计票方案

李靖, 景旭*, 杨会君

(西北农林科技大学 信息工程学院, 陕西 杨凌 712100)

(* 通信作者电子邮箱 jingxu@nwsuaf.edu.cn)

摘要:针对区块链电子投票中第三方计票机构不满足区块链去中心化、去信任特性以及缺乏可信度的问题,提出一种基于实用拜占庭容错(PBFT)算法的区块链电子计票方案。首先,在分布式环境中构建无中心计票模式,以节点的信任度确定计票节点;其次,基于PBFT实现待验选票的共识;再次,将PBFT中诚实节点的最低数量作为门限签名的阈值,只有达到阈值的计票结果才能形成门限签名;最后,将满足可信状态的结果记录在区块链账本上。通过测试分析表明,只有当诚实选票节点超过2/3时,才满足PBFT,得到可信的计票结果。

关键词:电子计票;区块链;实用拜占庭容错算法;门限签名

中图分类号:TP309.2 **文献标志码:**A

Blockchain electronic counting scheme based on practical Byzantine fault tolerance algorithm

LI Jing, JING Xu*, YANG Huijun

(College of Information Engineering, Northwest A&F University, Yangling Shaanxi 712100, China)

Abstract: For the problems that third party counting institution does not meet the decentralization and de-trusting characteristics of blockchain and is lack of credibility, a blockchain electronic counting scheme based on the Practical Byzantine Fault Tolerance (PBFT) algorithm was proposed. Firstly, the centerless counting model was built in the distributed environment, and the counting node was determined by the credibility level of the node. Secondly, the consensus of pending ballots was formed based on PBFT. Thirdly, the minimum number of honest nodes in PBFT was set as the threshold for threshold signature, and the threshold signature was only formed by results satisfying the threshold. Finally, the results satisfying the trusted state were recorded in the blockchain account book. Test and analysis results show that only when the honest nodes exceed two-thirds, the PBFT is satisfied, and the obtained counting result is credible.

Key words: electronic counting; blockchain; Practical Byzantine Fault Tolerance (PBFT); threshold signature

0 引言

投票与我们日常生活息息相关,大到国家选举、大政方针的制定,小到企业经营、日常社会问题的调查等,均离不开投票。电子投票是伴随着通信和网络技术的发展而诞生的全新投票模式,相较于传统投票方式,电子投票具有高效率、低成本、易操作等特点,在现代社会中发挥着越来越重要的作用。

但是,在现有一般网络化电子投票中,投票信息通常被网络传送到一个假设安全的中心机构,由其负责收集选票和统计结果,所以很有可能在计票过程中存在投票信息被恶意更改、堵塞或遗漏的情况。区块链是一种去中心化、防篡改、可追溯、多方共同维护的分布式数据库,改变了传统数据库管理系统的单一维护模式,解决了分布式环境中多方参与者对交易和状态的信任问题^[1]。目前区块链技术已经逐渐被应用到电子投票领域中:Zhao等^[2]是第一个提出将区块链技术应用到投票领域中并得以实现的研究人员,在其方案中通过引入奖励/惩罚机制约束区块链中的投票者行为;但是该方案仅考虑了一般可行性,忽视了投票应用应有的安全性和隐私性。Lee等^[3-4]为解决在分布式环境中准确计票的问题,提出在区块链中引入一个可信计票机构保护投票者的投票权力并确保

选票得以正确统计;但是区块链作为去中心化、去信任的应用,引入可信计票机构会打破其固有特性,而且由于在实际应用中并没有完全可信的第三方,因此基于任何第三方充当计票机构均存在一定的安全隐患。Somnath等^[5]提出将区块链作为公告板公开存储投票信息,以此满足DRE(Direct-Recording Electronic)系统能够在被不安全访问的情况下实现端到端可验证的电子投票方案;但是该方案同样基于公告板的假设安全性,无法应对公告板作弊或失效时对投票结果的保障。颜春辉^[6]利用分布式ELGamal加密体制和零知识证明协议提出一种基于全同态加密且无需第三方计票的多候选人投票方式;但是该方案存在同态加密算法复杂不利于合约的编写以及投票过程中单一选票验证性不强的问题。由此可见,在目前基于区块链技术实现的电子投票方案中,大多依靠假设存在的第三方可信计票机构或安全的公告板负责选票收集和计票。然而在区块链环境中,并没有所有节点都同时信任的第三方,因此,如何在区块链中完成选票结果的可信统计对基于区块链环境设计电子投票方案至关重要。

区块链作为对等(Peer-to-Peer, P2P)网络应用,在其投票过程中可以保证选票信息的真实性、不可篡改性。而在恶意模型中,恶意节点可能有意给出错误的计票结果。为了保证

收稿日期:2019-09-11;修回日期:2019-10-28;录用日期:2019-10-29。

基金项目:陕西省重点研发计划项目(2019ZDLNY07-02-01, 2018NY-127)。

作者简介:李靖(1994—),男,山西大同人,硕士研究生,主要研究方向:区块链安全; 景旭(1971—),男,陕西礼泉人,副教授,博士,主要研究方向:区块链安全、隐私保护; 杨会君(1974—),女,山西万荣人,副教授,博士,主要研究方向:电子商务物流、农产品质量溯源。



区块链中计票的准确,共识机制是一个比较好的解决方案。共识机制是解决分布式环境中数据一致性的算法,也是区块链中维持账本一致的重要组成部分技术。目前,区块链中的共识机制^[7]主要分为两类:1)应用在公有链中以工作量证明(Proof of Work, PoW)机制和权益证明(Proof of Stake, PoS)机制为代表的最终一致性共识;2)应用在联盟链中以实用拜占庭容错(Practical Byzantine Fault Tolerance, PBFT)算法为代表的强一致性共识。PoW和PoS通过节点算力或相应权益竞争区块的记账权,虽然采用激励政策鼓励矿工准确记录交易,但是会在竞争记账权时造成资源的大量浪费,降低共识效率。PBFT则是通过对节点的划分综合考虑拜占庭故障、提高共识达成效率的共识算法,因此PBFT在面向实际应用中更有实效性。

PBFT本质上是一种基于状态机副本复制的算法,通过每个状态副本保持相同的服务状态,实现客户的合法请求。在系统存在不多于 $(N-1)/3$ 数量的拜占庭故障节点的情况下(N 是节点总数),仍然可以维持系统整体的稳定性,正确达成分布式共识。为了实现区块链电子投票中节点对计票结果的正确响应,门限签名是一个比较有效的技术。门限签名是一种特殊的数字签名,指合法的签名必须由系统多个签名者共同签署,即只有签名的参与人员大于或等于规定的门限值时才可以生成合法签名,一方面实现对消息的多重保护,另一方面满足不同层级或数量构成的集合访问,提高数据的可读性。

因此,针对现有区块链电子投票研究中存在的问题,本文主要做了以下工作:

- 1)提出一种基于实用拜占庭容错协议的区块链电子计票方案,实现无可信计票中心的计票过程,消除计票组织对统计结果的绝对控制;
- 2)引入门限签名保障本文方案计票过程的正确性,综合考虑分布式因素和确保结果的高可信度,以PBFT中对诚实节点的最低要求作为合法门限签名的阈值;
- 3)区别于传统PBFT中主、从节点的确定方式,引入信任度的衡量机制,规范计票节点行为,提高共识效率。

1 相关技术

1.1 区块链电子投票

一个完整的电子投票方案包括制票、投票、验票、计票等基本过程。制票是对不同投票环境中选票内容及格式的指定,可以根据不同的要求设计选票形式。投票是在规定时间内完成选票提交。验票是对选票合法性的检验,主要是验证投票者身份。在验票过程为解决可能泄露投票者隐私的问题,可以采用盲签名^[4,8-9]等技术保护投票者隐私。计票是对所有选票结果的统计,多数投票方案^[3-5]均由计票机构负责选票统计。由此可见,一个好的计票方案首先应该保证收集到的选票都是可以通过验证的合法选票,只有确保选票来源,才可能得到正确的计票结果。在基于盲签名的电子投票方案中,典型合法选票构造过程^[10]如下:

1)投票者挑选随机数 k_i 作为比特承诺密钥,用位承诺方案 f 加密选票 m_i ,计算加密信息 $fm_i=f(m_i, k_i)$,然后随机选择盲因子 r_i 盲化 fm_i 得到消息 M_i ,如式(1)所示。其中 (e, n) 是组织者公钥信息,之后将该消息连同投票者身份标识发送给投票组织,等待签名。

$$M_i = r_i H(fm_i)^e \bmod n \quad (1)$$

2)投票组织验证签名确认是投票者发送的消息,并对消息 M_i 进行盲签名,如式(2)所示,其中 d 是组织者私钥信息;然后将 D_i 作为投票授权证书颁发给投票者。

$$D_i = M_i^d \bmod n \quad (2)$$

3)若签名有效,投票者对盲签名脱盲,得到基于消息 m_i 的签名 σ_i ,如式(3)所示;然后将消息/签名信息发送给计票机构

用于无记名投票。

$$\sigma_i = (r_i^{-1} D_i) \bmod n \quad (3)$$

1.2 实用拜占庭容错算法

1999年, Castro等^[11]基于拜占庭容错(Byzantine Fault Tolerance, BFT)算法^[12]提出了PBFT算法,首次将算法复杂度从指数级降为多项式级,使得方案在实际系统中变得可行。在区块链技术和比特币出现后,为解决PoW等需要消耗巨大算力竞争记账权的问题, PBFT开始被应用在区块链中作为新的共识机制。在基于PBFT算法的区块链中,为保证数据在分布式环境中快速达成共识,包含三部分:

1)一致性协议,是共识算法的基础协议。网络对参与的节点进行主、从节点划分,各节点按序轮流充当主节点。主节点负责率先对交易请求的响应和广播,从节点负责对主节点广播的交易进行确认和再次广播。主、从节点的划分方式节省了竞争记账权时所浪费的资源,能有效避免分叉的产生,显著缩短达成共识的时间。

2)视图更换协议,是共识算法处理主节点故障的协议。当主节点长时间未响应客户端请求或响应结果出现错误,此时需要启动视图更换协议变更主节点。该协议可以保障网络运行畅通,确保不会因为单一主节点的故障影响整个网络。

3)检查点协议,是共识算法中关于删除历史共识日志的协议,起到清理系统内存、降低数据冗余的作用。

1.3 门限签名

本文选择文献^[13]中设计的无中心化门限签名方案作为验票节点对结果的签名方式,该方案利用联合秘密共享技术改进了前人方案,避免了泄露签名者私钥,防止恶意签名者联合伪造其他签名者签名的问题,提高了每个部分签名的安全性。其构造方法^[14]如下:

1)密钥生成中心(Key Generation Center, KGC)选取两个安全的大素数 p 和 q ,满足 $q|p-1$,同时在 $GF(q)$ 上选取一个 q 阶生成元素 g ,公开 p, q, g 。

2)KGC从 $[1, q-1]$ 选取整数 X ,并分为 a 个不同的子份额,即 $X = x_1 + x_2 + \dots + x_a$,将 x_i 发给每个签名者 S_i ,对于每一个支持的不同级别访问的结构 $\Gamma_i (i=1, 2, \dots, a)$, KGC分别计算 G_{Γ_i} ,如式(4)所示,同时公开所有的 G_{Γ_i} 。

$$G_{\Gamma_i} = X - \sum_{x_i \in \Gamma_i} x_i \quad (4)$$

3) S_i 在 $[1, q-1]$ 中挑选私钥 sk_i ,并计算各自公钥 $pk_i = g^{sk_i} \bmod p$,然后由KGC计算总公钥 PK ,如式(5)所示:

$$PK = \prod_{i=1}^n pk_i \bmod p \quad (5)$$

4) S_i 从 $[1, q-1]$ 挑取整数 t_i ,分别计算参数 T_i 和 z_i ,如式(6)~(7)所示:

$$T_i = g^{t_i} \bmod p \quad (6)$$

$$z_i = g^{t_i sk_i^{-1}} \bmod p \quad (7)$$

5) S_i 验证所有 z_i ,并计算公共信息 Z 和部分签名 s_i ,如式(8)~(9)所示:

$$Z = \prod_{i=1}^n z_i \bmod p \quad (8)$$

$$s_i = [x_i h(Z, m) - Z t_i sk_i^{-1}] \bmod q \quad (9)$$

6)根据各部分签名 s_i ,计算整体门限签名 s_{thr} ,如式(10)所示:

$$s_{thr} = \sum_{i \in \Gamma_i} s_i + G_{\Gamma_i} h(Z, m) \quad (10)$$

2 本文方案整体思路

针对区块链电子投票中,基于第三方可信计票机构计票不能满足区块链去中心化、去信任特性及无法保障可信计票



机构“可信”的问题,本文提出一种基于PBFT的区块链电子计票方案,实现区块链中的可信计票。在该方案中,首先需要满足区块链去中心化、去信任模式,因此,本文的计票过程不再由可信计票机构负责,而是选择由投票者节点负责。但是如果让区块链中所有节点同时计票,又会增加网络的计算开销,造成资源的浪费并且导致结果难以统一,因此需要固定节点负责选票收集。PBFT中将所有节点划分为主、从节点,然而对主节点的选取方式较为随意,而且某一节点在被选作主节点后没有对其进行真伪性验证,因此使得可能挑选出来的节点是拜占庭故障节点。对此,本文根据PBFT的基本流程,结合区块链电子计票过程,引入对节点信任度的衡量。在计票阶段中,将投票者节点分为计票节点和验票节点,规定由信任值最高的节点充当计票节点,其他节点均为验票节点;其中,计票节点负责收集所有投票节点发送的合法选票,汇总选票信息得到待验计票结果,并对所有选票和待验计票结果签名,形成待验选举结果,然后发布到投票区块链;验票节点在计票节点公布待验选票结果后,验证统计情况,并根据验证结果对待验选票结果进行部分签名或表示拒绝。如此确定计票节点的选取方式,可以更快、更真实得到正确的待验选票结果,有效减少更换视图协议产生的次数。

另一方面,为防止计票节点成为“伪中心”,本文采用验票签名的形式确保待验选票结果的正确性,使得选票结果只有在经过多数节点认可时才可以最终公布,单一计票节点的信任度并不能代表结果的可信。理想情况下,投票区块链中所有参与节点都可以对待验选票结果进行验证签名,则最终公布的选票结果可以彻底杜绝选票由计票节点计票时可能产生的选票填塞或遗漏问题。但是,区块链作为分布式环境,且无法要求所有验票节点在有效时间内参与对待验选票结果的验证,因此,在确定合法部分签名的量化指标中,本文将PBFT中对诚实节点要求的最少数量作为门限签名的阈值基础,即只有至少得到 $(2n+1)/3$ 的部分签名时,系统才可以生成有效的门限签名,确保最终选票结果的可信。这样不仅可以提升方案的可行性,提高门限签名生成的概率,而且能够监督计票节点的统计行为和保证待验选票结果可以受到多数验票节点的验证;同时,方案允许超过门限的验票签名,最终选票结果可以根据具体的签名人数得到最低的可信任度,保障对最终选票结果的高信任共识。

本文旨在解决投票方案中计票环节的可信任处理,因此在计票阶段前假定系统收到的选票均是满足1.1节中合法选票的构造方案,充分确保选票来源的合法性,即投票者构成的集合 $\{V_1, V_2, \dots, V_n\}$ 经过投票组织机构(Org)完成对身份合法性的检查,分别得到基于投票消息 $\{m_1, m_2, \dots, m_n\}$ 的盲签名 $\{\sigma_1, \sigma_2, \dots, \sigma_n\}$,形成可以用于投票的消息/签名元组 (m_i, σ_i) 。当系统发布投票阶段开始后,各投票节点开始将各自的元组信息 (m_i, σ_i) 发送到投票区块链中,开始投票。本文方案计票整体流程如图1所示。

3 本文方案设计

3.1 计票节点选取

根据投票区块链中节点的信任度高低确定计票节点,信任度越高的节点表明该节点的历史行为越诚实,越适合负责统计选票任务。本文对所有参与投票的投票者节点记为 $Node_i$,并统一赋予相同的初始化信任度 T_0 ,此后根据该节点在投票以及验票阶段的表现动态更新其最新信任值。节点更新信任度方式如式(11)所示:

$$T_{ij} = T_{i(j-1)} + \varepsilon \quad (11)$$

其中: T_{ij} 表示第 i 个节点的第 j 次信任值; $T_{i(j-1)}$ 表示第 i 个节点的第 $j-1$ 次信任值,即该节点的前次信任值; ε 代表在前次选

举中对于该节点行为表现的奖励或惩罚。若节点行为良好,具体表现为每次参与投票、积极验证选票并针对待验选票结果作出正确的响应,此时 ε 为正值,不断提高其基础信任度;若节点行为较差,具体表现为缺席投票、不验证选票或响应结果与真实结果相悖、存在恶意捣乱,此时 ε 为负值,显著降低该节点的信任度。对于改变量 ε 可以根据具体业务的需求和选举本身的要求动态决定。在投票开始前,根据投票区块链中所有节点的信任度划分为最可信节点、普通节点和不可信节点,如图2所示。其中,最可信节点即为链上信任度最高的节点,也就是负责收集选票、统计结果的计票节点,网络中只有一个节点是最可信节点,在普通节点中产生;不可信节点包括信任度低于某个固定限值的节点和作弊被发现的计票节点,投票区块链中可以有多个不可信节点;其余节点则属于普通节点,普通节点和不可信节点均为验票节点。

从节点的信任值变化不难看出,对于每次投票都能积极作出正确响应的节点会不断提升该节点的信任度,也就是说,某一节点的信任度越高说明该节点在历史投票、计票、验票过程中都能够诚实地响应各阶段结果,偏向于相对可靠的节点,因此由这样的节点负责计票会较大程度上更好地完成计票任务。

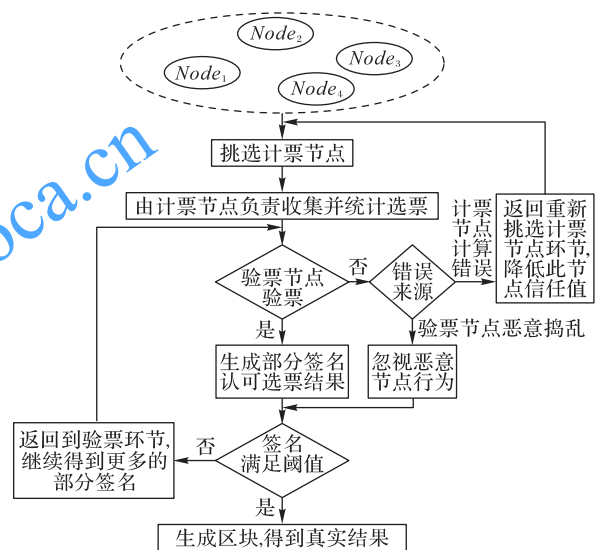


图1 计票方案整体流程

Fig. 1 Overall flowchart of counting scheme

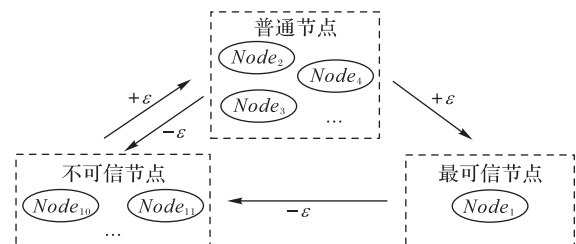


图2 各节点信任值的变化

Fig. 2 Change of credibility of each node

3.2 计票节点统计选举结果

假定 $Node_e$ 为当前选举中信任度最高的节点,于是该节点即被暂定为此次收集选举信息、统计选票结果的计票节点。当投票阶段开始后,所有合法投票者节点 $Node_i$ (包括计票节点 $Node_e$)向投票区块链中匿名发送自己的选票信息,即消息/签名对 (m_i, σ_i) ,并且每张选票中应明确此次选举的主题和节点发送选票的时间;其中写明主题是防止选票信息收集错误,保证投票内容和主题息息相关;标记节点发送时间是为选票



提供时间证明,解决选票在规定时间内没有被统计时引发的争议问题。选票具体格式和包含内容如图3所示。

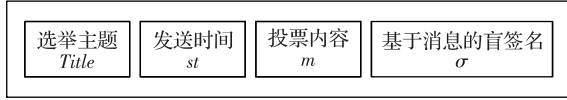


图3 合法选票结构

Fig. 3 Legal ballot structure

计票节点 $Node_c$ 收集选票信息,形成待验选票结果的过程如下:

1) 收集发送到投票区块链中符合投票主题的选票,在收集过程中也可以继续验证投票者身份是否合法、其盲签名信息是否正确,再度确保选票来源的合法性。

2) 将规定投票时间 T_1 内收集的所有合法选票汇总形成表单 $List_{pre}$, 并且根据 $List_{pre}$ 计算投票结果,得到待验计票结果 $Vote_{result}$ 。

3) 将 $List_{pre}$ 和 $Vote_{result}$ 以及其他相关信息一起加密打包形成待验选票结果 (WVR), 如式(12)所示:

$$WVR = ENC_{csk}(List_{pre} || Vote_{result} || Title) \quad (12)$$

其中: csk 为计票节点的私钥; ENC 为加密算法保证消息的隐私。

4) 对待验选票结果添加时间戳证明 TS , 防止恶意投票节点在 T_1 后发送选票信息不被接纳而产生对计票节点的争议。并对待验选票结果和时间戳证明进行哈希运算的结果签名, 如式(13)所示:

$$C = Sig_{csk}(\text{Hash}(WVR || TS)) \quad (13)$$

其中: Sig 为签名算法保证消息的完整性, 确保各节点如实、平等获取计票节点计算的结果。

5) $Node_c$ 将 WVR 和 C 发送到投票区块链中, 等待各验票节点对计票节点统计结果的验证。

3.3 验票节点检验待验选举结果

计票节点 $Node_c$ 在投票区块链公布待验选票结果后, 各验票节点首先用计票节点的公钥 cpk 验证签名信息 C 是否正确, 若验证成功, 则表示消息完整, 确实由计票节点发布并且没有受到恶意节点对待验选票结果的篡改, 然后再解密打开密文消息, 获取相关信息。解密方式如式(14)所示:

$$DEC_{cpk}(WVR) = (List_{pre} || Vote_{result} || Title) \quad (14)$$

验票节点得到计票节点公布的待验选票结果后, 开始验证其统计信息是否正确。具体验证流程如下:

1) 首先检查表单 $List_{pre}$ 中是否包含自己的投票/签名信息元组 (m_i, σ_i) , 若包含自己的选票则继续下一步验证; 否则发出拒绝信号, 请求“re-counting”。

2) 由于区块链属于分布式环境, 各节点地位相等, 任何节点可以获取其他节点发送到投票区块链中的选票, 所以验票节点在投票阶段可以自主获取其他选票。因此, 自主收集选票信息的验票节点可以验证计票节点选票收集是否完备。若选票收集完备, 则继续验证; 否则同样发出拒绝信号, 请求“re-counting”。

3) 然后根据当前表单 $List_{pre}$ 中包含的所有合法投票信息, 独立计算其待验计票结果 $Vote_{result}$ 是否正确。若计算有误, 则发出拒绝信号, 请求“re-counting”; 反之则说明计票节点计算待验选票结果正确, 验票节点可以对其进行部分签名。签名过程如下:

① KGC 选取两个安全的大素数 p 和 q , 满足 $q | p - 1$, 在 $GF(q)$ 上选取一个 q 阶生成元素 g , 公开 p, q, g ; 同时确定秘密值 X , 并分解为 $X = x_1 + x_2 + \dots + x_n$, 然后将每一个 x_i 发送给验票节点 $Node_i$ 作为秘密份额。

② 验票节点挑选随机数 b_i 作为签名时的私钥, 然后根据

离散对数难解问题计算签名用到的公钥信息, 如式(15)所示:

$$pk_{Node_i} = g^{b_i} \bmod p \quad (15)$$

③ 验票节点挑取整数 u_i , 根据式(16)~(17)分别计算签名时用到的参数 U_i 和 o_i , 并将其广播到投票区块链中, 然后在验证时间 T_2 内收集所有其他验证节点计算的参数 o_i , 得到由所有 o_i 连乘的公开参数 O 。

$$U_i = g^{u_i} \bmod p \quad (16)$$

$$o_i = g^{u_i b_i^{-1}} \bmod p \quad (17)$$

④ 验证节点根据自己的秘密份额 x_i 和各公开参数, 对 WVR 进行签名, 形成有效的部分签名, 如式(18)所示:

$$s_{Node_i} = [x_i h(O, WVR) - O u_i b_i^{-1}] \bmod q \quad (18)$$

此时验票节点完成验票任务, 将自己对待验选票结果的反馈情况(签名或拒绝)发到投票区块链中, 等待其他节点的验证情况。同时验票节点本地保存该信息, 方便用于验证最终宣布的结果信息是否和此信息相同。

3.4 选票结果的发布

在系统规定的验证时间 T_2 结束后, 计票节点 $Node_c$ 收集各验票节点对待验选票结果的验证情况, 查看是否满足门限阈值。验证结果根据各验票节点对计票节点公布的信息是否接受分为 $accept$ 和 $reject$ 。其中: $accept$ 代表该节点认可计票节点统计和计算得到的待验选票结果, 并给出自己部分签名; $reject$ 代表该节点不同意计票节点公布的信息, 不论是统计错误或是计票错误, 验证节点都发出“re-counting”请求。此时, 计票节点 $Node_c$ 将根据收到的 $accept$ 和 $reject$ 数量对待验选票结果进行如下操作:

1) 当 $Node_c$ 收到 $accept$ 数量少于投票节点总数的 $2/3$ 时, 代表验证选票的验票节点数量没有达到方案的最低门限要求, 此时由于待验选票结果仅由较少的节点参与验证, 无法保证该结果的正确性, 因此, 不能生成基于待验选票结果的合法门限签名。但有部分验票节点签名则表示计票节点的行为正确, 导致无法生成最终选票结果的原因仅因为验票签名不足, 因此网络陷入等待环节, 继续等候验票节点的签名, 直到满足签名阈值, 才能出示最终选举结果。

2) 当 $Node_c$ 收到 $reject$ 数量大于投票节点总数的 $1/3$ 时, 表示计票节点公布的表单 $List_{pre}$ 和选举结果 $Vote_{result}$ 确实存在作弊风险, 没有合理正确的统计选票结果, 此时调用 PBFT 中视图更换协议取消 $Node_c$ 计票节点身份, 并降低其信任度; 同时选用信任度次高的节点担任计票节点, 然后重新完成选票统计和计票任务。

3) 当 $Node_c$ 收到 $accept$ 数量大于投票者总数的 $2/3$ 时, 表示验证选票节点数达到门限签名最低要求, 且计票节点统计的待验选票结果得到了大多数节点的认可, 此时可以生成对最终选票结果提供证明的门限签名, 如式(19)所示:

$$s_{thr} = \sum_{i \in I_i} s_{Node_i} + G_{F_i} h(O, WVR) \quad (19)$$

同时, 根据验票节点具体生成的部分签名数量, 可以得到关于最终选票结果的最低可信度 ζ , 如式(20)所示。

$$\zeta = \frac{1}{N} \sum_{i=1}^i Node_i \quad (20)$$

在上述三种情况中, 前两种验证情况均代表计票任务以失败告终, 都不能被视为准确完成电子计票任务, 只有第3)种情况才代表选举结果真实可靠。同时, 本文通过对参与验票签名人数(记为 sn)的划分明确了选举结果的最低可信度, 并对不同信任度下的结果进行标识, 具体对应情况如表1所示。

当计票节点 $Node_c$ 成功完成计票任务, 即将所有投票内容以及相关签名信息打包生成区块。在生成单体区块时,



仍然选择由区块头和区块体两部分组成,选票区块结构如图4所示。

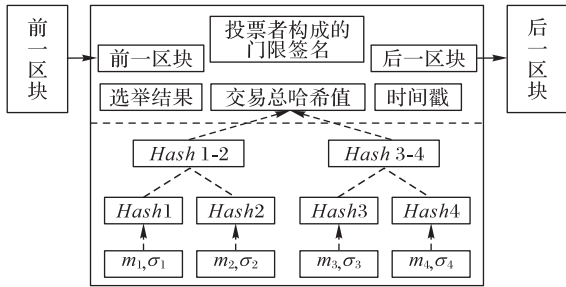


图4 选票区块结构

Fig. 4 Ballot block structure diagram

区块头包含当前区块体内所有交易形成的哈希根值、前一区块的哈希值、用于验证结果真实的门限签名以及选举结果,区块体包含所有合法的投票交易,在每条交易信息中包含消息/签名对 (m, σ) ,最后对区块添加时间戳证明,形成不可篡改、可供验证、结果真实的投票记录。

表1 选举结果状态标识

Tab. 1 Status identifications of election result

验票人数	状态标识	代表符号	理论可信区间 ζ 范围
$[0, 2N/3)$	不可信	$State_{ub}$	$[0, 2/3)$
$[2N/3, N)$	可信	$State_b$	$[2/3, 1)$
N	完全可信	$State_{mb}$	1

4 本文方案分析

4.1 可行性分析

在电子投票领域中,Cortier等^[15-16]提到在当前研究中众多的选举方案由于或存在中心机构或选票结果不被验证,导致很大程度上最终结果存在选票填充、遗漏或篡改的问题,从而影响选举结果的真实性。本文基于区块链环境提出了无需可信第三方计票机构的可信计票方案,整体采用PBFT共识机制保障计票结果的正确性,同时区别于当前PBFT中主、从节点的划分机制,以信任度高低确定计票节点和验票节点。一方面提高分布式环境中计票效率,降低网络开销;另一方面可

以监督计票节点统计选票和计票结果的行为。当网络中超过1/3的验票节点在验证过程中计算的结果信息与计票节点公布的待验选票结果存在差异时,更换计票节点,结果完全根据共识机制,杜绝计票节点对数据的绝对控制,并且由于计票节点在公布待验选票结果时并不能确定参与验票的投票节点,因此更大程度上可以促进计票节点的诚实行为,防止其恶意遗漏、篡改某些选票。采用门限签名达成投票者范围内对待验选票结果的验证,考虑到分布式环境中无法强制要求所有节点验证选票结果和尽可能较大程度保证选举结果的真实性,方案将PBFT在分布式环境中可信节点的数量作为门限签名的阈值:若达到签名数量则结果可信,反之结果视为无效,可有效增加方案的可行性。

4.2 安全性分析

本文重在解决选票在计票过程中存在的安全性问题,在此阶段前依赖高效的盲签名技术完成验票等环节保障选票的合法性。在收集选票过程中,方案选择由可信度最高的节点负责统计选票,消除了传统“可信”计票机构对结果的作弊风险,且计票节点不同于可信机构,投票区块链中的任何节点都可以且必须在最终结果正式公布前验证待验选票结果的正确性,从而保证计票的稳定性。在表示验证成功时,运用门限签名的形式达成对待验选票结果的共识,每个验票节点的部分签名只能由其独立签名,其他任何节点均不能伪造该节点对结果的签名,并且只有当系统中得到的部分签名数超过门限阈值时才可以生成合法门限签名,证明最终结果的真实性。区块链作为去中心化、去信任、防篡改的分布式数据库,任何想要否定存储在区块链数据的攻击者都需要打破既定的共识机制,在PBFT中,只有攻击者控制1/3以上的节点才可以对合法数据进行否定,而在分布式环境中,控制总体数量的1/3几乎难以实现,且如果确实全网超过1/3的节点不能对合法数据达成共识,则说明网络存在问题,选举受到操控,因此正常情况下,若选票结果在统计正确时,至多只有不超过1/3的恶意节点或非故障节点提出异议。在选举结果达成共识后,使用哈希算法对交易打包形成区块,任何试图篡改选票的行为都会改变哈希值进而影响区块信息而被发现,因此使用区块链技术可以保障选票在区块账本中的安全性。

4.3 方案对比分析

将本文方案和其他方案进行了有关计票结果正确性的对比分析,具体如表2所示。

表2 不同方案的对比

Tab. 2 Comparison of different schemes

方案	是否需要可信计票机构	结果公示前是否支持投票者确认	检验计票结果需要的验票人数	计票中未被验证选票被遗漏风险系数	选票达成一致的方式	结果是否可能被篡改
文献[8]方案	是	否	1	1/2	受计票机构绝对控制	是
文献[4]方案	是	否	1	1/2	受计票机构绝对控制	否
文献[17]方案	是	否	t	$[0, 1/2)$	超过一半的验票员认可	是
本文方案	否	是	$[2/3N, N]$	$[0, 1/3]$	PBFT共识算法	否

在文献[18]的研究基础上,文献[8]方案有效地解决了电子投票方案中容易发生的选票碰撞问题,但是该方案的实现严重依赖于第三方的绝对可信,忽略了计票机构和中心控制机构的“不可信”行为对结果的影响。文献[4]方案在基于区块链技术设计电子投票方案时,虽然保证了结果存储时的安全性和抗篡改性,但是同样需要引入可信第三方负责计票,如此不仅破坏了区块链自身的特性,也会影响计票结果的真实性。文献[17]方案考虑到无法保证单一验票员诚实的问题,提出采用多个验票员验证选票并收集信息,从而降低对单一验票员的绝对可信;但是却没有考虑验票员可以通过联合作弊来对计票结果产生较大的影响。和上述方案相比,本文方案彻底取消了计票时常用的第三方,消除了传统投票方案过

程中对计票机构可信的假设条件,满足了区块链环境的去中心化、去信任特性,防止了“可信”计票机构的“不可信”行为。本文方案通过计票节点计票+验证节点验票模式的共识机制保障了计票过程的完整性;采用区块链技术负责数据的安全性,降低了中心数据机构的绝对控制权;通过提高验票者的数量,降低了选票信息被遗漏的风险,充分保证计票结果的稳定性。

5 仿真实验

5.1 测试环境

本文根据联盟链环境设计基于实用拜占庭容错算法的区块链电子计票方案,在实验过程中涉及的测试工具和其相应

的作用如表3所示。

表3 测试工具及其作用

Tab. 3 Testing tools and their functions

测试工具	作用
Ubuntu16.04	实验底层系统环境
Hyperledger Fabric1.0	测试环境
Docker	获取和运行fabric网络
Fabric-peer	充当投票者的节点
Fabric-ca	为节点颁发合法证书
Java	编程语言,用于业务逻辑的开发和测试,以链码的形式部署在联盟链中

5.2 测试过程

在测试过程中,通过调试不同节点总数 N 、不同拜占庭故障节点数 N_f 以及不同诚实节点签名数 N_s 测试系统能否得到选票结果以及该公布结果的正确性。具体包括:PBFT算法主节点选取和本文基于信任确定计票节点的效率对比,不同节点总数下故障节点对计票结果的影响,以及固定节点总数下故障节点对计票结果的影响。

1)测试PBFT算法主节点选取和本文基于信任确定计票节点的效率对比。

本文方案的计票过程中,计票节点的确定方式不同于原PBFT算法的主节点选取方式,在PBFT共识算法中,只要网络中总体节点数量多于3倍的故障节点,使用该算法就可以解决分布式环境中数据的一致性和正确性。换句话说,如果网络中每4个节点中只存在1个故障节点时就不会影响系统的稳定性。因此,本文以4个节点为例,设定其中1个节点为故障节点,其余3个是正常节点,在不影响系统稳定性的情况下模拟20次的投票结果共识中,两种不同计票节点选取方式中计票节点发生更换的次数对比如图5所示。

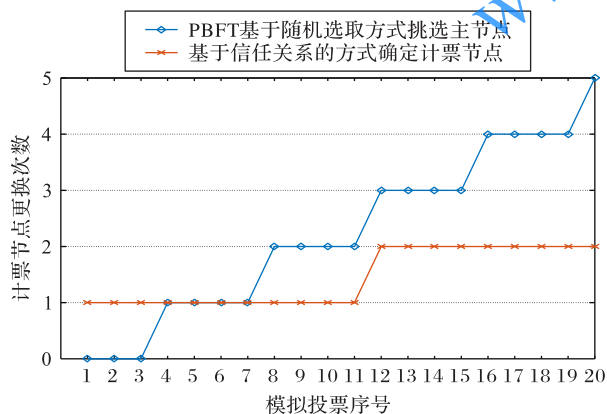


图5 两种计票节点选取随模拟投票总数递增的更换次数

Fig. 5 Number of replacements of two types of counting node selection with increasing simulated ballot number

从图5不难看出,在模拟20次投票过程中,通过PBFT随机选取计票节点的模式共发生5次计票节点的更换。而采用信任关系确定计票节点时,仅发生过两次计票节点更换;第一次是对初始消息共识时选定了故障节点充当计票节点,由于初始阶段4个节点信任度相同,所以存在较大概率选择故障节点充当计票节点;第二次是人为关闭该节点网络,阻止其参与共识,此时该节点发生故障,导致系统重新挑选计票节点。

由此可见,无论采用何种模式挑选计票节点都不影响消息的一致性和正确性确认,但是基于信任关系确定计票节点的模式可以有效降低故障节点充当计票节点的次数或概率,

从而减少视图更换协议产生次数,提高共识效率。

2)测试不同节点总数下 N_f 和 N_s 对计票结果的影响。

本文以节点的形式代表合法投票者,不同的节点总数模拟不同数量的投票场景。在测试过程中,分别测试了当节点总数 $N = 4, 10, 30$ 时,计票结果受拜占庭故障节点数和诚实签名数的影响,测试结果如表4所示。可以看出,只要网络中收到诚实节点的签名数是已知拜占庭故障节点数的3倍及以上,系统就可以公布计票节点统计的计票结果,并且该计票结果完全正确,可以实现基于区块链环境的可信电子计票,如图6所示;但是如果签名数量不满足最低阈值要求,系统则返回提示信息:“签名不足,请继续等待!”,如图7所示,即不被允许公布计票结果,由此也无需判断该结果的正确性。

表4 不同节点总数下 N_f 和 N_s 对计票结果的影响

Tab. 4 Impact of N_f and N_s on counting results under different number of nodes

节点总数	设置故障节点数	参与签名的节点数	是否允许公布计票结果	计票结果正确性/%
4	1	2	否	—
4	1	3	是	100
10	3	5	否	—
10	4	4	否	—
10	2	8	是	100
30	5	25	是	100
30	10	20	否	—
30	9	20	是	100

The number of the voters:30
The number of the signatures:25
Corresponding PBFT threshold requirements and the results are as follows!
Alice 8
Bob 13
Cindy 6
David 3

图6 可信计票结果的公示

Fig. 6 Publicity of trusted counting result

The number of the voters:10
The number of the signatures:2
The number of signatures don't meet the requirement, please continue to wait!

图7 持续等待签名结果的提示

Fig. 7 Prompt of continuous waiting for signature result

3)测试固定节点总数下 N_f 和 N_s 对计票结果的影响。

假定网络中节点总数固定不变,测试不同数量的拜占庭故障节点和获得的诚实签名数量对计票结果的影响程度。本文以节点总数是10为例,通过动态调试网络中的故障节点数和诚实签名数观察能否得到计票结果以及该结果的正确性,测试结果如表5所示。

表5 固定节点总数10下 N_f 和 N_s 对计票结果的影响

Tab. 5 Impact of N_f and N_s on counting results under 10 nodes

拜占庭故障节点数	诚实节点签名数	能否显示投票结果	结果正确性/%
0	1~10	能	100
1	0~2	否	—
	3~9	能	100
2	0~4	否	—
	5~8	能	100
3	0~6	否	—
	7	能	100
4~10	0~6	否	—

从表5可知,随着故障节点的不断增加,网络中能够获得的诚实签名逐渐减少,同时不同数量的拜占庭节点对于获取计票结果时要求的诚实节点签名数量不同:当故障节点越少



时,需要的诚实签名越少,越容易得到可信计票结果;故障节点越多时,需要的诚实签名越多。当网络中如果没有故障节点,所有节点均为可信节点时,任何节点对计票结果签名都可以代表结果的真实性。当网络中故障节点数量超过4时,即便剩余节点(6个)均对计票结果作诚实签名也无法显示投票结果。因为此时故障节点数量已经超过PBFT共识算法的假设条件,网络本身处于不可信状态,计票结果存在较大概率被恶意节点操控,因此难以在不可信网络中获得公平可信的投票结果,所以系统不公布该结果,保障投票的公平性。

由表4~5可知,当网络中拜占庭故障节点数低于总数的1/3且由诚实节点对计票结果的签名数超过总数的2/3时,系统均能够显示最终的选票结果并且该结果的正确性均为100%。由此可以说明,本文使用PBFT共识算法+门限签名的方案可以起到和计票机构相同的可信作用,因此,将本文方案应用到实际选举或投票场景的计票过程中,可以更加客观地保障选票结果的真实性和公平性。

6 结语

针对区块链电子投票中基于第三方计票机构既不满足区块链去中心化、去信任特性,又无法保障其在计票中完全“可信”的行为,本文提出一种基于实用拜占庭容错算法的区块链电子计票方案。本文方案首先满足区块链环境特性,通过共识机制替代可信第三方计票机构;其次,运用门限签名的方法在结果被所有节点共识之前增加投票者自身的验证,保障计票过程的真实性;同时综合考虑实际因素和保证结果高度可信,将PBFT共识机制对诚实节点要求的最低数量作为签名的门限阈值,不仅能够解决可能存在的拜占庭故障问题,而且可以起到监督计票节点的作用,进一步实现去信任化。最后通过区块链技术将选票记录以及结果存入区块中,由各节点共同维护账本信息,降低传统中心机构对数据的绝对控制和防止中心机构故障导致数据的丢失。未来将进一步研究计票结果根据验票人数的变化趋势,量化可信程度,准确衡量结果的真实性。

参考文献 (References)

- [1] 邵奇峰,金澈清,张召,等. 区块链技术:架构及进展[J]. 计算机学报, 2018, 41(5): 969-988. (SHAO Q F, JIN C Q, ZHANG Z, et al. Blockchain: architecture and research progress[J]. Chinese Journal of Computers, 2018, 41(5): 969-988.)
- [2] ZHAO Z, CHAN T H H. How to vote privately using bitcoin [C]// Proceedings of the 2015 International Conference on Information and Communications Security, LNCS 9543. Cham: Springer, 2015: 82-96.
- [3] LEE K, JAMES J I, EJETA T G, et al. Electronic voting service using blockchain [J]. Journal of Digital Forensics, Security and Law, 2016, 11(2): No. 8.
- [4] CRUZ J P, KAJI Y. E-voting system based on the bitcoin protocol and blind signature [J]. IPSJ Transactions on Mathematical Modeling and Its Applications, 2017, 10(1): 14-22.
- [5] SOMNATH P, ROY B K. A secure end-to-end verifiable e-voting system using zero knowledge based blockchain[EB/OL]. [2018-12-21]. <https://eprint.iacr.org/2018/466.pdf>.
- [6] 颜春辉. 基于区块链的安全投票系统研究与设计[D]. 杭州: 杭州电子科技大学, 2018. (YAN C H. Blockchain-based secure e-voting system [D]. Hangzhou: Hangzhou Dianzi University, 2018.)
- [7] 刘敖迪,杜学绘,王娜,等. 区块链技术及其在信息安全领域的研究进展[J]. 软件学报, 2018, 29(7): 2092-2115. (LIU A D, DU X H, WANG N, et al. Research progress of blockchain technology and its application in information security[J]. Journal of Software, 2018, 29(7): 2092-2115.)
- [8] 罗芬芬,林昌露,张胜元,等. 基于FOO投票协议的无收据电子投票方案[J]. 计算机科学, 2015, 42(8): 180-184. (LUO F F, LIN C L, ZHANG S Y, et al. Receipt-freeness electronic voting scheme based on FOO voting protocol [J]. Computer Science, 2015, 42(8): 180-184.)
- [9] 郭玲玲,谷利泽,李忠献. 基于群盲签名的无收据电子投票方案[C]// 2009年中国高校通信类院系学术研讨会论文集. 南宁: 中国通信学会青年工作委员会, 2009: 225-230. (GUO L L, GU L Z, LI Z X. The scheme of non-receipt electronic voting based on group and blind signature [C]// Proceedings the 2009 of Academic Conference on Communications in China Colleges and Universities. Nanning: China Communications Society Youth Work Committee, 2009: 225-230.)
- [10] JOAQUIM R, FERREIRA P, RIBEIRO C. EVIV: an end-to-end verifiable internet voting system [J]. Computer and Security, 2013, 32(2): 170-191.
- [11] CASTRO M, LISKOV B. Practical Byzantine fault tolerance [C]// Proceedings of the 3rd Symposium on Operating Systems Design and Implementation. Berkeley: USENIX Association, 1999: 173-186.
- [12] LAMPORT L, SHOSTAK R, PEASE M. The Byzantine generals problem [J]. ACM Transactions on Programming Languages and Systems, 1982, 4(3): 382-401.
- [13] 王斌,李建华. 无可信中心的 (t, n) 门限签名方案[J]. 计算机学报, 2003, 26(11): 1581-1584. (WANG B, LI J H. (t, n) threshold signature scheme without a trusted party [J]. Chinese Journal of Computers, 2003, 26(11): 1581-1584.)
- [14] AGNEW G B, MULLIN R C, VANSTONE S A. Improved digital signature scheme based on discrete exponentiation [J]. Electronic Letters, 1990, 26(14): 1024-1025.
- [15] CORTIER V, GALINDO D, KÜSTERS R, et al. SoK: verifiability notions for e-voting protocols [C]// Proceedings of the 2016 IEEE Symposium on Security and Privacy. Piscataway: IEEE, 2016: 779-798.
- [16] BERNHARD M, BENALOH J, HALDERMAN J A, et al. Public evidence from secret ballots [C]// Proceedings of the 2017 International Joint Conference on Electronic Voting, LNCS 10615. Cham: Springer, 2017: 84-109.
- [17] 邹秀斌,崔永泉,付才. 一种基于门限的电子投票方案[J]. 计算机科学, 2012, 39(7): 39-43. (ZOU X B, CUI Y Q, FU C. Threshold-based electronic voting scheme [J]. Computer Science, 2012, 39(7): 39-43.)
- [18] FUJIOKA A, OKAMOTO T, OHTA K. A practical secret voting scheme for large scale elections [C]// Proceedings of the 1992 International Workshop on the Theory and Application of Cryptographic Techniques, LNCS 718. Cham: Springer, 1992: 244-251.

This work is partially supported by the Key Research and Development Program of Shaanxi (2019ZDLNY07-02-01, 2018NY-127).

LI Jing, born in 1994, M. S. candidate. His research interests include blockchain security.

JING Xu, born in 1971, Ph. D., associate professor. His research interests include blockchain security, privacy protection.

YANG Huijun, born in 1974, Ph. D., associate professor. Her research interests include e-commerce logistics, agricultural product quality traceability.