基于联盟区块链的董事会电子投票系统

董友康[1]，张大伟[1]，韩臻[1]，常亮[2]
（1. 北京交通大学计算机与信息技术学院，北京 100044；
2. 桂林电子科技大学广西可信软件重点实验室，广西 桂林 541004）

摘 要：董事会投票是特定范围的小集体为某一问题进行匿名表决的场景，对参与者的身份要求严格。设计了一种基于联盟链的董事会电子投票协议，用智能合约取代了传统的可信第三方，降低了系统信任成本；采用基于数字证书的身份准入机制，保证了参与投票者的身份合法性；基于椭圆曲线盲签名技术设计了电子投票协议，实现了投票的匿名性。安全分析表明，所提协议能够满足电子投票协议的安全性要求，使用方便灵活，提高了系统易用性。

关键词：区块链；联盟链；电子投票；盲签名
中图分类号：TP391.1
文献标识码：A
doi: 10.11959/j.issn.2096-109x.2017.00221

Board voting system based on the consortium blockchains

DONG You-kang[1], ZHANG Da-wei[1], HAN Zhen[1], CHANG Liang[2]
(1. School of Computer and Information Technology, Beijing Jiaotong University, Beijing 100044, China;
2. Guangxi Key Laboratory of Trusted Software, Guilin University of Electronic Technology, Guilin 541004,China)

Abstract: The board voting is a scenario of anonymous voting on a particular group of individuals, which is strict with the identities of the participants. A board e-voting protocol based on the consortium blockchains was presented, which replaced the traditional trusted third party with the smart contract so as to reduce the system trust cost. It adopt a digital certificate-based identity mechanism to ensure that the voter's identity is legal. It adopt the blind signature based on elliptic curve technology to achieve the anonymity of voting. The security analysis shows that the proposed protocol can meet the requirements of unforgeability, anonymity and security etc, which is convenient and flexible to use.

Key words: blockchain, consortium blockchain, e-voting, blind signature

1 引言

电子投票协议是由Chaum[1]在1981年首先提出的，用于解决互联网环境下的选举和投票场景下的安全性问题，即满足投票的合法性、匿名性、计票完整性、不可伪造性、不可重复性、不可篡改性等要求[2]。为了解决上述问题，密码学家们经过30多年的研究，对电子投票技术已经有了较为成熟的解决方案，并应用于政府选举、董事会决策等领域。

使用匿名信道的电子投票协议的底层密码学技术主要分为盲签名、环签名、代理签名这3种。基于盲签名技术的电子投票协议主要分为有可信第三方（TTP, trusted third party）的投票协议和无

收稿日期：2017-11-15；**修回日期**：2017-12-03。**通信作者**：张大伟，dwzhang@bjtu.edu.cn
基金项目：国家自然科学基金资助项目（No.61672091）；广西可信软件重点实验室研究课题基金资助项目（No.KX201531）
Foundation Items: The National Natural Foundation of China (No.61672091), Key Laboratory of Trusted Software Program of Guangxi Province (No.KX201531)

可信第三方的投票协议 2 种。无 TTP 的投票协议最早是由 Merrit[2]设计的，该协议所需执行的投票轮数与投票者数成正比，且计算量大。苏云学等[3]提出了一种方案，可以通过固定轮数进行匿名投票。有 TTP 的投票协议中，日本学者 Fujioka 等[4]提出的电子投票协议（简记为 FOO 协议）是最早大规模使用的基于盲签名的投票协议，是电子投票发展史上一个革命性的进步，它使电子投票得到了前所未有的发展。但其被证明无法实现不可伪造性，且存在共谋攻击的风险。后续有大量的基于 FOO 协议进行改进的工作，包括丛清日等[5]提出的电子投票方案中，解决了上述缺陷，但是在最后进行选票公布的时候，将投票者的 ID 签名和公钥同时公布，破坏了投票的匿名性。由于这些协议都存在 TTP，要求投票者必须信任中央机构，且投票前必须设立这些中央机构。在这种情况下，用户无法察觉和防御计票机构和管理机构的共谋攻击。这些问题的存在增加了用户的使用代价，制约了电子投票技术的推广。

区块链在不引入第三方中介机构的前提下，可以提供去中心化、不可篡改、安全可靠等特性保证，可以看作一种无中心的 TTP。比特币[6,7]是区块链技术的典型代表，链上数据一旦生成便无法篡改，并且全网公开可见，所以比特币可以看作一个全球范围的无中心的、分布式的 TTP。联盟链是区块链技术发展的成果之一，联盟链[8,9]是具有准入机制的区块链，用户必须具备合法的身份才能加入联盟链中。联盟链可以看作一个特定范围的分布式 TTP，具有较高的安全性和可信性，是解决董事会决策等特定范围投票需求的一种新解决思路[10]。

本文提出了一种基于联盟链的、使用椭圆曲线盲签名技术的董事会电子投票协议。该协议能够满足电子投票协议的 6 个安全要求，并且通过联盟链的智能合约实现了传统 TTP 的功能，增加了该协议的可信程度和适用范围。

2 电子投票系统

电子投票系统是以密码学原理为基础，使用计算机、互联网、通信等技术代替传统的人工方式来实现投票功能。通常，一个电子选举方案包含如下步骤[11]。

1) 申请。这个步骤是由合法的投票人从选举中心取得一个以后可以验证的标志信息。投票人的一些个人信息及投票人的投票信息都有可能隐藏在这个标志信息中。

2) 投票。投票人构造出合法的选票通过某种方式送给选举中心。

3) 统计。选举中心统计选票。

4) 验证。对于一个电子选举方案，其可验证性有个人可验证性和全体可验证性 2 种。个人可验证性指投票者本人能确认自己的选票被正确地统计在选举结果之中，而整体可验证性指任何人都可以根据公布出来的选举信息确认选举的统计工作的正确性。

电子投票协议为保证公平选举、防止欺骗，有 6 个安全要求，其具体含义如下[12]。

1) 合法性。只有经授权的投票者才能投票。

2) 匿名性。所有选票必须保密，每个人都不能知道他人的投票情况。

3) 计票完整性。所有选举者都能检验他们的选票在最后的表中是否被统计上。

4) 不可重复性。每一个投票人只能够投票一次。

5) 不可伪造性。任何人不能复制别人的选票。

6) 不可篡改性。任何人都不能修改他人的投票而不被发现。

3 基于椭圆曲线的盲签名算法

盲签名算法[13]是一个包含用户和签名者两方参与的密码协议。用户将盲化后的信息发送给签名者，签名者对该信息进行签名但是无法得到所签信息的具体内容。用户收到签名后的信息后对其进行脱盲，就能得到签名者对原始信息的签名，即使以后签名者见到这个消息时，也无法确定这是否是他签署的。盲签名算法可以有效地保护所签署消息或文件的具体内容，所以在电子投票这种需要匿名性的应用场合中起到了关键作用。

椭圆曲线密码体制（ECC, elliptic curve cryptography）是一种高效的密码体制，ECC 的数学基础是椭圆曲线离散对数问题的难解性。张方国等[13]提出了一种基于椭圆曲线的盲签名算法，该方案可以看作是 Schnnor 盲签名在椭圆曲线上的模拟，能够实现弱盲签名。王化群等[14]在此基

础上提出了强盲签名，本文设计的电子投票协议使用了文献[14]中的方案。其中算法参数设置如下。

$E(F_q)$：定义在有限域上的非奇异的椭圆曲线。

$G \in E(F_q)$：曲线上的 n 阶基点。

q：有限域的元素个数，这里 $q=p$，或者 $q=2^m$。

$d \in_R Z_n^*$：是签名私钥，$Q=dG$ 是签名验证公钥。

SHA-1：$\{0,1\}^* \to \{0,1\}^{160}$ 是美国 NIST 和 NSA 设计的一种安全 Hash 算法。

上述参数中，d 保密，其他参数公开。

接下来，介绍算法的流程，其中记号$(\cdot\|\cdot)$表示 2 个比特串连接，$R_x(A)$表示取 A 点的坐标。

签名

1) 签名者生成私钥 $k \in_R Z_n^*$，然后计算公钥 $Y=kG$，并公布给用户。

2) 用户生成盲化因子 $\alpha,\gamma,\delta \in_R Z_n^*$，计算

$$A = \alpha Y + \gamma G + \delta Q = (x, y)$$

$$t = x \bmod n$$

$$c = SHA-1(m \| t)$$

$$c' = \alpha^{-1}(c - \delta)$$

其中，m 为原始消息，c 是盲化后的消息。用户将 c'发送给签名者。

3) 签名者计算

$$s' = k - c'd \bmod n$$

s'为签名者对 c'签名后的信息。然后，签名者将 s'发送给用户。

4) 用户计算

$$s = \alpha s' + \gamma \bmod n$$

得到原始信息 m 的签名，(c,s)即为 m 的盲签名。

验证

只需验证下式是否相等。

$$c = SHA-1(m \| R_x(cQ + sG) \bmod n)$$

4　联盟链

区块链具有不可篡改、分布式存储、公开透明的特点，因此可以作为公布投票结果并防止篡改的公告板。联盟链[8]是一种具有身份准入机制的区块链，一个节点必须经过身份认证才能加入一条链中，通常由 CA 机构为节点颁发证书。区块链的节点之间通过共识机制达成信任，并提供节点间的匿名认证机制保护节点隐私。

智能合约[15,16]是运行在区块链上的、实现特定交易功能的一段程序，智能合约的代码和状态是公开的，链上用户可以对代码功能进行审核。联盟链中的智能合约语言是图灵完备的，并可与链外数据进行交互。智能合约一旦被部署到链上，就会一直运行且不可篡改。

因此，运行在联盟链上，具有特定的审核身份、审核选票、统计选票等业务逻辑的智能合约，能够取代传统的 TTP，完成投票管理和统计功能，并满足其安全特性；而且，具有身份准入机制的联盟链能够满足董事会投票等特定范围投票场景的需求和身份审核要求；此外，联盟链中节点间的通信可采用安全信道，为投票系统中的传输安全提供更好的保障。因此，基于联盟链设计董事会电子投票协议较传统的基于 TTP 的方案在安全性和便利性方面更具优势。

5　联盟链董事会电子投票协议设计

本文采用盲签名算法，设计了基于联盟链的董事会电子投票协议，通过运行在联盟链上的具有管理和统计功能的智能合约取代了传统的 TTP，实现了投票流程中的管理和计票功能，通过多方共识后写入账本的投票结果，能够满足用户的信任需求，减少用户的信任成本。通过使用盲签名方案，实现了票面信息的隐藏，防止攻击者利用系统漏洞破坏投票的匿名性。

5.1　参数说明

本协议使用的参数如下。

List1：投票记录表，由管理合约记录投票者申请签名的过程，防止投票者多次投票。

List2：计票信息表，由计票合约记录投票者投票信息，防止攻击者复制别人选票。

投票过程中的一系列计时器包括：

$t_{\text{finishRegistration}}$：注册截止时间，投票者在此时刻前完成注册；

$t_{\text{beginvote}}$：开始投票时间，投票者在此时刻后开始投票；

$t_{\text{finishvote}}$：结束投票时间，投票者在此时刻后完成投票；

t_π：最小时间间隔，在每个阶段之间会有一段间隔时间，保证智能合约可以运行并将写入链上。

5.2　系统设计

该系统中的角色有管理者、CA、投票者、管

理合约、计票合约，角色的作用分别如下。

管理者：设定并公布投票者的名单、被投票的问题及选项、椭圆曲线参数、开始注册时间、开始投票时间及结束投票时间。

CA：为有投票权的用户颁发证书、为管理合约和计票合约颁发公私钥对。

管理合约：自动审核投票者身份、为盲化后的选票信息签名、将签名后的选票发送给投票者。

计票合约：自动计算选票、公布选票、公布投票结果。

本文方案的联盟链采用 hyperledger fabric，系统架构如图 1 所示。

其中，CA 通过 fabric 网络与投票者和智能合约进行通信，投票者向智能合约发送申请、投票等参数信息，合约接收到参数后自动执行相应的业务逻辑，并将执行结果写入区块链的账本中。

5.3　投票协议设计

投票协议分为 5 个步骤，协议的时序如图 2 所示。

5.3.1　初始化

管理者是由投票者共同选举出的，管理者设置选举过程用到的参数并公布。

1) 管理者设置被投票的问题以及选项 $\{v \mid v \in N\}$。

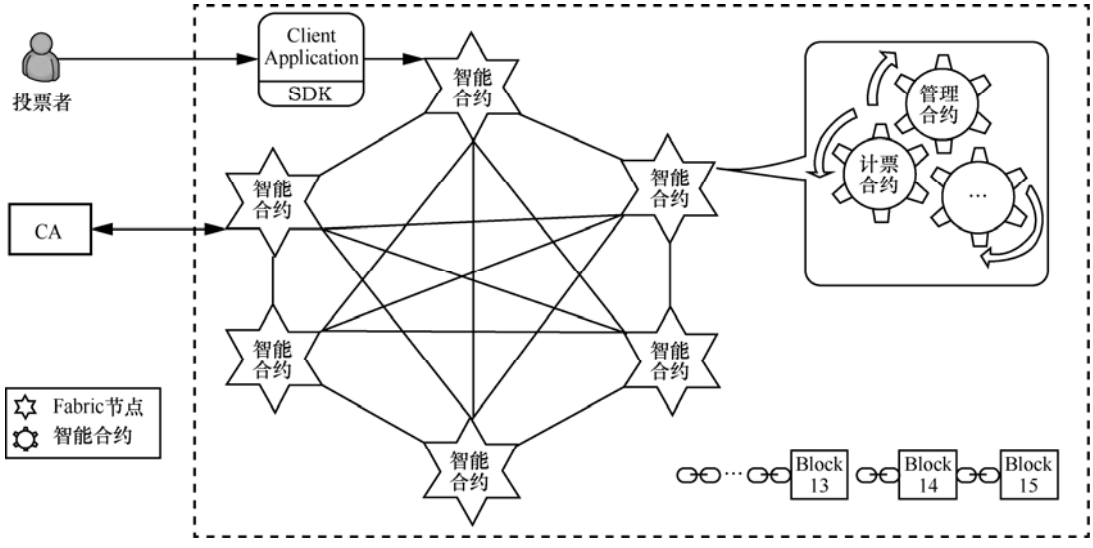

图 1　投票协议架构

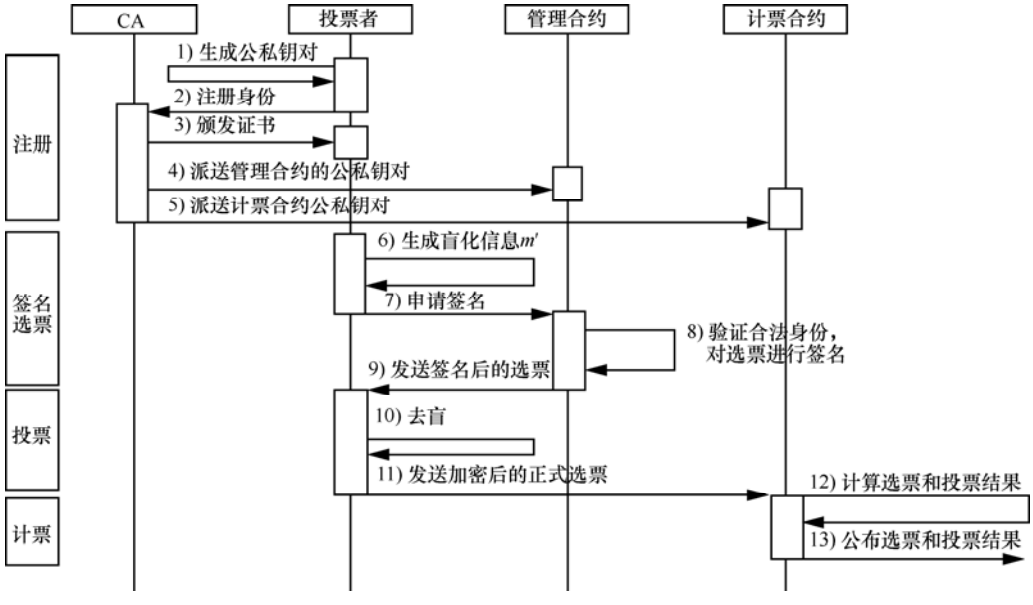

图 2　投票协议时序

2) 管理者设置计时器信息，用于通知投票者注册和投票的时间点。

3) 管理者确定 $E(F_q)$ 和 $G \in E(E_q)$ 。

4) 设置完成后，管理者公布上述参数，通知投票者开始注册，通知管理合约进入注册阶段。

5.3.2　注册

投票者向 CA 注册身份，CA 为投票者颁发证书。同时，CA 为管理合约和计票合约派发公私钥对。下述步骤对应图 2 中步骤 1)~步骤 5)。

1) 投票者 V_i 生成随机数 x_i 作为私钥，计算公钥 $y_i=x_iG$。

2) V_i 将 $\{y_i, ID_i\}$ 发送给 CA 进行注册。

3) CA 审查 V_i 身份，审查 V_i 是否有投票资格，审查通过后 CA 向 V_i 颁发实名证书 $Ecert_i$。

4) CA 生成管理合约的两对签名密钥对 (X_A,Y_A)和(d, Q)，将 X_A 和 d 通过安全信道发送给管理合约。本文的安全信道是通过 TLS 实现的，能够保护信息的机密性和完整性，具有实名认证和不可窃听的性质。

5) 管理合约生成投票记录表 List1，列表由投票者证书和投票标志位组成，投票标志位用于标志用户是否申请签名，“0”表示尚未申请，“1”表示已经申请。List1 的内容如表 1 所示。

表 1　　投票记录

序号	投票者证书	投票标志位
1	$Ecert_1$	0
2	$Ecert_2$	1
M	M	M

6) CA 生成计票合约的密钥对(X_J, Y_J)，将 X_J 通过安全信道发送给计票合约。

注册阶段工作应在 $t_{\text{finishRegistration}}$ 内完成。

5.3.3　生成选票的签名

投票者将投票信息进行盲化后发送给管理合约请求签名，管理合约对其进行签名后返回给投票者。下述步骤对应图 2 中的步骤 6)~步骤 9)。

1) 投票者 V_i 生成盲化因子 $\alpha_i, \gamma_i, \delta_i \in_R Z_n^*$，计算

$$A = \alpha_i Y_A + \gamma_i G + \delta_i Q = (x_i, y_i)$$

$$t_i = x_i \bmod n$$

$$c_i = SHA-1(v_i \parallel t_i)$$

$$c_i' = \alpha_i^{-1}(c_i, \delta_i)$$

其中，v_i 为原始选票消息，c_i 是盲化后的选票。

2) 投票者将 $\{Ecert_i \parallel c_i'\}$ 通过安全信道发送给管理合约。

3) 管理合约收到 V_i 发送的盲化选票后，检查证书的合法性。若证书非法，则拒绝签名。

4) 管理合约检查 List1 中 $Ecert_i$ 对应的标志位是否等于 0。若标志位为“1”，则拒绝签名。

5) 管理合约对盲化后的选票进行签名，即计算

$$s_i' = k - c_i' d \bmod n$$

然后将 List1 中 $Ecert_i$ 对应的位置标志为 1。

6) 管理合约将 $\{s_i'\}$ 发送给投票者。

5.3.4　投票

投票者通过去盲得到原始选票的签名，然后生成正式选票，加密后匿名发送给计票合约。下述步骤对应图 2 中的步骤 10)和步骤 11)。

1) V_i 对 s_i' 进行去盲，即计算

$$s_i = \alpha_i s_i' + \gamma_i \bmod n$$

得到原始选票的签名。

2) V_i 生成选票信息 $\{(c_i, s_i) \parallel v_i\}$，并用计票合约的公钥 V_J 进行加密，即计算

$$m_i = ENC\{(c_i, s_i) \parallel v_i\}_{Y_J}$$

生成正式选票。

3) V_i 将正式选票 m_i 匿名发送给计票合约。

申请签名和投票工作在 $t_{\text{finishvote}}$ 前完成。

5.3.5　计票并公布

计票合约解密选票后验证签名的有效性，检查投票是否已存在，然后统计选票生成最终投票结果，最后将投票结果写入账本并公布。下述步骤对应图 2 中的步骤 12)和步骤 13)。

1) 计票合约收到 m_i，用私钥 X_J 进行解密，取出盲签名(c_i, s_i)，验证签名是否来自管理合约，即计算

$$c_i = SHA-1(v_i \parallel R_x(c_i Q + s_i G) \bmod n)$$

若相等，则签名通过验证；若不相等，则抛弃选票。

2) 计票合约取出 c_i，在计票记录表 List2 中查询 c_i 是否存在。若存在，则抛弃选票；若不存在，则将 c_i 写入 List2 中。

3) 计票合约取出 v_i 并进行统计，得到投票结果。

4) 计票合约公布所有的 $\{(c_i, s_i) \parallel v_i\}$，公布投

票结果 List3，并将 $\{(c_i, s_i) \| v_i\}$ 和 List3 通过共识算法和节点验证后写入账本。

投票流程结束。

6 安全性分析

6.1 盲签名方案的安全性分析

文献[13]中提出了盲签名方案的安全性证明过程，作者将签名的有效性规约到 Schnorr 盲签名方案的安全性保证，并将该方案的盲性规约到有限域上的椭圆曲线的离散对数难解问题。

6.2 投票协议的安全性分析

基于联盟链的董事会电子投票协议具有合法性、匿名性、不可重复性、不可伪造性、计票完整性、不可篡改性的安全特性，同时具备抗共谋攻击的能力。

1) 合法性

联盟链的 CA 可以实现用户的身份审核和准入机制，保证了加入链中进行投票的人都是合法的投票者。

2) 匿名性

本文从 3 个方面进行匿名性分析。

第一，假设存在不诚实的投票者 Malice 试图通过智能合约写在账本上的数据，得到其他投票者的投票信息。那么 Malice 能获得投票结果和 $\{(c_i, s_i) \| v_i\}$。由于盲签名算法的有效性和盲性，所以 Malice 无法通过(c_i, c_i)得到投票者的身份信息。

第二，投票者在申请签名过程中，通过无法窃听的安全信道与管理合约进行通信，能够防止 Malice 窃听。

第三，如果 Malice 节点能够读取智能合约的运行结果，Malice 可以获得的信息用 2 个集合 D_A、D_J 表示，D_A 是通过管理合约获得的信息，D_J 是通过计票合约获得的信息。其中

$$D_A = \{(s_i', c_i'), Ecert_i\}$$

$$D_J = \{(s_i, c_i), v_i\}$$

Malice 试图通过计算 (s_i', c_i') 和 (s_i, c_i) 的关联性，推断出 $Ecert_i$ 和 v_i 的关联性。根据 6.1 节可知，文中使用的盲签名方案具有强盲性，因此 Malice 无法计算出盲签名对和普通签名对的对应关系。

此处分析表明，该方案满足匿名性。

3) 不可重复性

管理合约将申请过签名的 $Ecert_i$ 标记为“1”，当投票者重复投票时，管理合约会发现 $Ecert_i$ 对应的标志位为“1”，然后拒绝签名。因此每个投票者只能获得一次管理合约的签名，所以该方案满足不可重复性。

4) 计票完整性

计票合约公布 $\{(c_i, s_i) \| v_i\}$ 和 List4 后，投票者可以通过比对 (s_i, c_i) 的值验证其选票是否被统计上；投票者可以比对 List4 中结果与 v_i 的信息，验证计票结果的正确性。因此该方案满足计票完整性。

5) 不可伪造性

如果 Malice 截获了投票信息 $m_i = ENC\{(c_i, s_i) \| v_i\}_{Y_J}$，并发送给计票合约。计票合约取出 c_i 的信息，在 List3 中进行查询时发现 c_i 已经存在，所以该伪造的选票是无效选票。因此该攻击无效。

Malice 试图伪造一份选票，必须伪造管理合约的签名。此问题可以规约到签名算法的安全性，根据 6.1 节可知，Malice 无法伪造签名。因此该方案满足不可伪造性。

6) 不可篡改性

如果 Malice 截获了投票信息 $m_i = ENC\{(c_i, s_i) \| v_i\}_{Y_J}$，试图对 m_i 进行篡改。由于加密算法的安全性，Malice 无法对 m_i 进行解密，所以无法在不被发现的情况下对投票信息进行篡改，因此该方案满足安全性。

7) 抗共谋攻击

智能合约本质上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，链上的用户都可以对代码进行审查，从而判断智能合约的功能。智能合约的运行结果都会写入账本并公开，而且不会做出开发者规定之外的行为。因此，协议中的管理合约和计票合约是安全可信的。

文中对于匿名性的分析也表明，即使管理合约和计票合约被攻击者窃听，获得 2 个合约的运行结果，攻击者也无法破坏匿名性。因此，该方案具有抗共谋攻击性。

7 结束语

本文介绍了一种基于联盟链的董事会电子投票协议，用特定业务逻辑的智能合约代替了传统的 TTP。安全分析表明，该协议能够满足电子投票协议的安全要求，是安全可靠的。由于用户无

需设立和信任 TTP，只需加入联盟链中就可进行投票，因此降低了协议的实施成本，提高了协议的适用范围。

参考文献：

[1] CHAUM D. Untraceable electronic mail，return address，and digital pseudonyms[J]. Communications of the ACM, 198l, 28(2): 84-88.

[2] MERRITT M J. Cryptographic protocols[C]//The Fourteenth ACM Symposium on Theory of Computing. 1982: 383-400.

[3] 苏云学, 逯海军, 祝跃飞. 一个无需中央机构的电子投票协议[J]. 计算机工程, 2004, 30(11): 96-97.
SU Y X, LU H J, ZHU Y F. An electronic vote protocol without authority[J]. Computer Engineering, 2004, 30(11): 96-97

[4] FUJIOKA A, OKAMOTO T, OHTA K. A practical secret voting scheme for large scale elections[C]//Advances in Cryptology—Ausocrpt'92. 1993.

[5] 丛清日, 胡金初. 基于椭圆曲线盲数字签名的电子选举[J]. 计算机工程, 2010, 36(13): 156-158.
CONG Q R, HU J C. E-elections based on elliptic curve blind digital signature[J]. Computer Engineering, 2010,36(13):156-158.

[6] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[EB/OL]. http://bitcoin.org/bitcoin.pdf.

[7] 田海博, 何杰杰, 付利青. 基于公开区块链的隐私保护公平合同签署协议[J]. 密码学报, 2017, 4(2): 187-198.
TIAN H B, HE J J, FU L Q. A privacy preserving fair contract signing protocol based on block chains. [J]. Journal of Cryptologic Research, 2017, 4(2): 187-198.

[8] Hyperledger-fabricdocs documentation[EB/OL] http://hyperledger-fabric.readthedocs.io/en/latest/.

[9] KIAYIAS A, ZHOU H S, ZIKAS V. Fair and robust multi-party computation using a global transaction ledger[C]//The Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2016: 705-734.

[10] MCCORRY P, SHAHANDASHTI S F, HAO F. A smart contract for boardroom voting with maximum voter privacy[C]// Financial Cryptography and Data Security. 2017.

[11] 龚俭, 陆晟, 王倩. 计算机网络安全导论[M]. 南京: 东南大学出版社, 2005: 144-147.
GONG J, LU C, WANG Q. Introduction to network security[M]. Nanjing: Southeast University Press, 2005:144-147.

[12] SCHNEIER B. Applied cryptography, second edition: protocols, algorithms, and source code in C[J]. Government Information Quarterly, 1997, 13(3):336.

[13] 张方国, 王常杰, 王育民. 基于椭圆曲线的数字签名与盲签名[J]. 通信学报, 2001(8): 22-28.
ZHANG F G, WANG C J, WANG Y M. Digital signature and blind signature based in elliptic curve[J]. Journal of China Institute of Communications, 2001(8): 22-28.

[14] 王化群, 张力军, 赵君喜. 基于椭圆曲线的 Schnorr 盲签名[J]. 计算机工程与设计, 2005, 26(7):1819-1822.
WANG H Q, ZHANG L J, ZHAO J X. Schnorr blind signature based on elliptic curve[J]. Computer Engineering and Design, 2005, 26(7): 1819-1822.

[15] SZABO N. Formalizing and securing relation-ships on public networks[DB/OL]. https://www.researchgate.net/publication/220167894_Formalizing_and_Securing_Relationships_on_Public_Networks.

[16] KOSBA A, MILLER A, SHI E, et al. Hawk: the blockchain model of cryptography and privacy-preserving smart contracts[C]// Security and Privacy. 2016:839-858.

作者简介:

董友康（1993-），男，山西介休人，北京交通大学硕士生，主要研究方向为区块链、密码协议。

张大伟（1974-），男，辽宁朝阳人，博士，北京交通大学副教授，主要研究方向为智能卡安全、支付安全和区块链技术。

韩臻（1962-），男，浙江宁波人，博士，北京交通大学教授、博士生导师，主要研究方向为信息安全体系结构、可信计算。

常亮（1980-），男，贵州赫章人，博士，桂林电子科技大学教授，主要研究方向为知识表示与推理、可信计算。