

**项目计划书修订版（B）**

2020.11.17

王芳琴

**基于区块链的投票方案**

**区块链学院**

**江西软件职业技术大学**

目录

[基于区块链投票系统 1](#_Toc5993)

[1.1 背景和现状 1](#_Toc22555)

[1.2 匹配度分析 4](#_Toc4961)

[投票流程分为四个阶段： 4](#_Toc13547)

# 基于区块链投票系统

**一** 需求分析

### 背景和现状

#### 1.1.1 背景

投票活动是社会生活中制定决策的重要依据，投票形式从传统的举手表决、匿名投票到电子投票演化，投票成本不断降低，投票过程愈发便捷。但是不管在投票的哪种形式下都有各种问题。

记录中最早得雅典投票之一是多数决的陶片放逐，由每个人放陶片选择放逐的人，这种方法简单直接，但是只能在小范围使用。随着时代的发展这种方法逐渐被取代。在早期投票方式多为人工投票，由政府或机构组织，给人投票权，并由这些组织和机构计票这避免不了暗箱操作。

#### 1.1.2 国内外现状

数字签名是数据鉴权和身份认证的主要手段，是一项重要的信息安全技术，它的基本作用是保证传送信息的安全性和可用性，并确认签名者的身份7，盲签名技术是一种特殊的数字签名，它可以保证在签名者不知道所签消息真实内容的前提下得到签名者的有效签名。D.Chaum于1983年首先提出盲签名），并设计了基于RSA签名体制的盲签名方案。1993年，Okamoto首先提出了基于离散对数难题的盲签名方案1，之后，对盲签名的研究不断深入，盲签名中也增加了群盲签名、部分盲签名等特殊算法，盲签名是数字签名技术的重要组成部分，有着重要的地位。现今，已经提出的盲签名应用主要涉及电子支付、电子现金、电子合同签署及公平电子投票协议等安全场景。

电子投票协议是现代民主活动的象征，用于满足互联网环境下的选举和投票活动的各种需求，电子投票的应用已经深入到民主生活和政治选举中，比较著名的应用案例：2000年，美国的佛罗里达州选举试验、2002年，巴西总统选举、2004年，美国总统大选、2007年，法国总统大选初选、2009年，中国杭州市基层选举、2014年，法国国家教育部投票。

许多研究者都致力于设计一种安全高效的电子投票协议，目前主要有两个发

展方向：一是基于同态加密技术，掩盖选票的票面信息，并通过公开信道传输1；二是基于匿名信道技术，掩盖投票者的身份信息，其中，基于同态加密技术的投票协议1l采用高次剩余加密方式，需要进行大规模的计算和传输，效率低下，实用性弱，基于匿名信道的投票协议所采用的底层密码学技术可以分为盲签名、环签名和代理签名三种。其中盲签名算法可以有效地保护所签署消息的具体内容，在电子投票这种需要匿名的应用场景中能够发挥重要作用。基于百签名算法的电子投票协议可分为有可信第三方（Trusted Third Party，TP）的投票协议和无TTP的投票协议两种.

无TTP的投票协议最初是由Michael Merrit等1）提出，该协议每次投票需要运行的投票次数与投票者数成正比，每轮的计算量大。苏云学3等提出了一种匿名投票的方案，一次完整的投票过程需要执行固定的六轮计算.Patrick Mcorryl1）

等提出了一种利用区块链平台--以太场--实现的投票协议，但是由于以太坊不支持加密计算，导致程序冗余复杂：总体来说，无TTP的电子投票协议鱼有一定发展，但是协议通常较为复杂，因为效率问题而无法进入实用阶段（347在有TTP的电子投票协议中，D.Chauml1"1提出的方案首先引进盲签名思想来保护选民的身份隐私。1992年，Okamoto和Ohta提出FO0协议18，它是最早实现大量商用的投票协议，该协议结合了盲签名和比特承诺技术，是投票协议发展过程中一个重要的进步，FO0协议简单高效，它使电子投票技术正式进入实用阶段。

基于FO0协议出现了大量的商用投票软件，例如EVOX和SENSUS，但后来FOO协议被证明存在选票碰撞缺陷，无法满足不可伪造性要求，而且存在共谋攻击的威协，此后有许多在FO0协议基础上的改进研究。1996年，Juang和Leil0提出了FO0的改进方案，方案要求所有投票者全部参加投票.丛清日等21提出新的方案，解决了F00协议的弊端，但是在结果公布阶段，公开了投票者的身份信息签名和公钥，渔成隐私数据泄露，破坏了匿名性，上述协议均存在TTP，投票者被动信任TTP，且必须设立TTP.在这种情况下用户无法发现和防止TTP的共谋攻击，上述存在的问题增加了电子投票协议的使用门槛和信任成本，限制了电子投票协议的普及.

目前，区块链技术因其不可幕改、安全可信等特点，被称为是具有改变传统业务乃至机构运作方式的潜力的重大煎覆性技术1，随着区块链技术的快速发展，些研究人员提出了使用区块链技术的电子投票协议.2015年，Czepluchl22提出区块链技术可以应用于电子投票领域，同年ZHAO12）等人提出一种使用比特币和zk-SNARKs进行投票的方法，具有隐私性、有效性和不可撤销性.2016年，一种使用零币的投票协议也被提出24，但是由于零币的软件开发比较困难，所以不具备实用性，同年，CJason9等提出一个使用百签名和比特币实现的协议，但是系统管理员能够通过比特币地址和消息得知投票者的身份，即存在管理员共谋攻击的可能性。

除此之外，利用区块链技术的电子投票应用也不断涌现，2018年11月，泰国民主党利用区块链技术选举党内领导人，比较典型的应用还有Bicongress，Pollow MyVote 和TIVI，这些应用使用区块链网络提供投票底层服务，但是仍然依赖第三方机构来保护用户隐私数据，同时这些应用大多缺乏适当的文档，关于其内部工作的问题仍然存在不透明的问题。

## 匹配度分析

在网络投票应用中引入区块链技术，可以借助区块链的去中心化同步记账、身份认证、数据加密和数据不可篡改等特征，确保投票信息可信任且可追溯，使各社会主体共同建造、共同维护、共同监督，从而满足公众的知情权、监督权，增强网络投票的客观性与可信度。

（1）保证投票匿名性：用户只需注册，登录，投票，数据记录在区块链中，过程由智能合约完成，投票中途不受第三方平台控制，防止用户投票信息泄露。同时，点对点查询投票信息，实现投票信息只由投票者查询。

（2）可信的投票数据：区块链将加密技术的功能与透明性相结合，这使其成为在线投票的便捷且安全的选择。 记录在区块链上的选票将具有防篡改功能。 人们现在可以在家中方便地进行投票。 他们可以在不损害安全性或隐私的情况下使用计算机或移动设备进行投票。 此外，他们将能够核实自己的选票并确保被计票。

（3）投票的可验证性：投票者进行投票操作后，选票信息将公开 存储在区块链上，并且无法窜改,无论是投票者本人或是其他 人都可以对选票的真实性和有效性进行验证。在计票阶段，候 选者的私钥公开后,所有人都可以验证和统计有效的选票数。

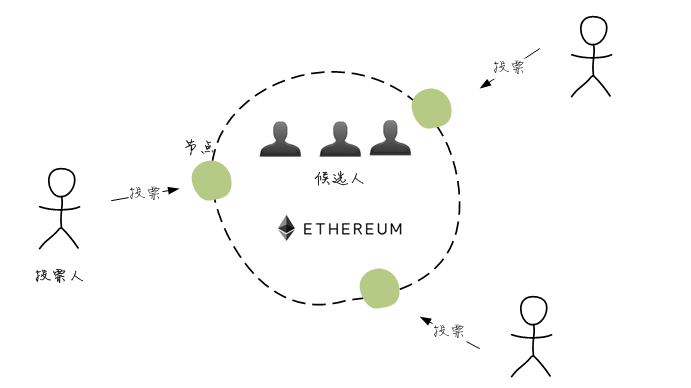
（4）投票的唯一性：唯一性，发送令牌，一个用户只有一次投票权。 所以一个投票者只能进行一次投票，重复的投票将被视为无效,该方案满足唯一性。

1.3基于区块链的投票系统方案设计

1.3.1 业务设计

基于区块链的投票系统是一个去中心化的投票应用。利用这个投票应用，用户可以在不可信的分布环境中对特定的候选人投票，每次投票都会被记录在区块链上，所谓去中心化应用（DApp：Dcentralized Application），就是一个不存在中心服务器 的应用。在网络中成百上千的电脑上，都可以运行该应用的副本，这使得它几乎不可能 出现宕机的情况。

基于区块链的投票是完全去中心化的，因此无须任何中心化机构的存在。

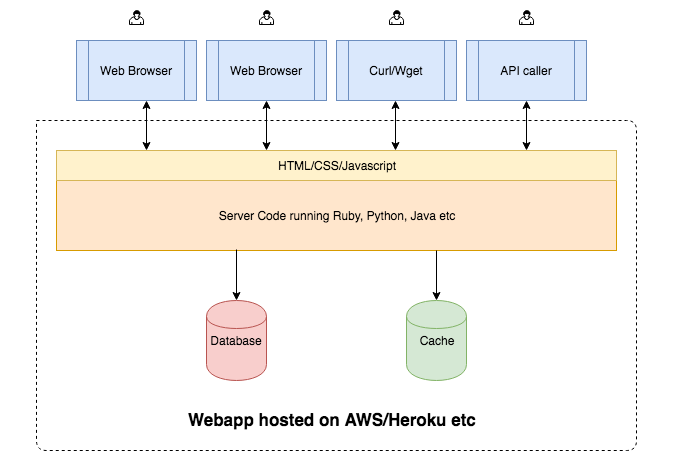


1.3.2 架构设计

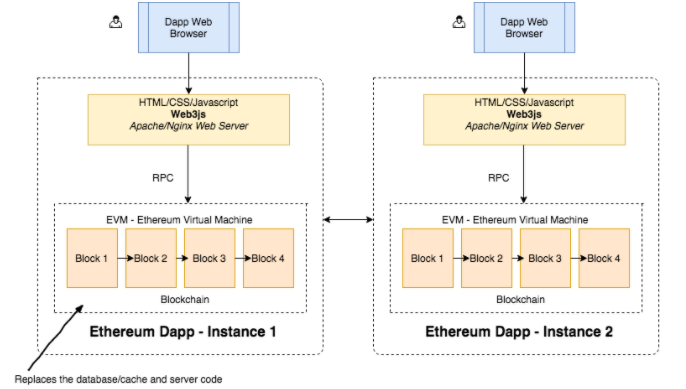
一．中心化应用构架

一个典型web应用的服务端通常由 Java，Ruby，Python 等等语言实现。前端代码由 HTML/CSS/JavaScript 实现。 然后将整个应用托管在云端，比如 AWS、Google Cloud Platform、Heroku....，或者放在你租用的一个VPS 主机上。

用户通过客户端（Client）与 web 应用（Server）进行交互。典型的客户端包括浏览器、命令行工具（curl、wget等）、 或者是API访问代码。注意在这种架构中，总是存在一个（或一组）中心化的 web 服务器，所有的客户端都需要 与这一（组）服务器进行交互。当一个客户端向服务器发出请求时，服务器处理该请求，与数据库/缓存进行交互， 读/写/更新数据库，然后向客户端返回响应。



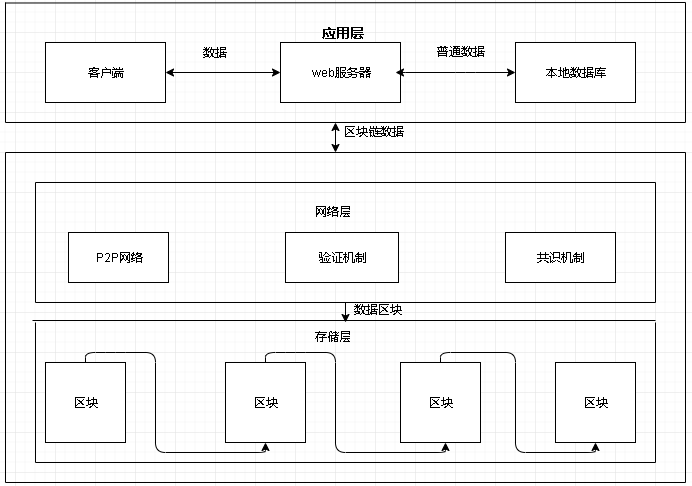
1. **基于以太坊的去中心化应用构架**



基于以太坊的去中心化应用构架，每个客户端（浏览器）都是与各自的节点应用实例进行交互，而不是向 一个中心化的服务器请求服务。

### 三．基于区块链投票系统构架

从业务流程上看，基于区块链的投票系统是一个典型的分布式应用（DApp），因此我们采用以太坊的技术底层作为支撑，其架构自上而下分为三个层面：应用层，网络层，存储层。

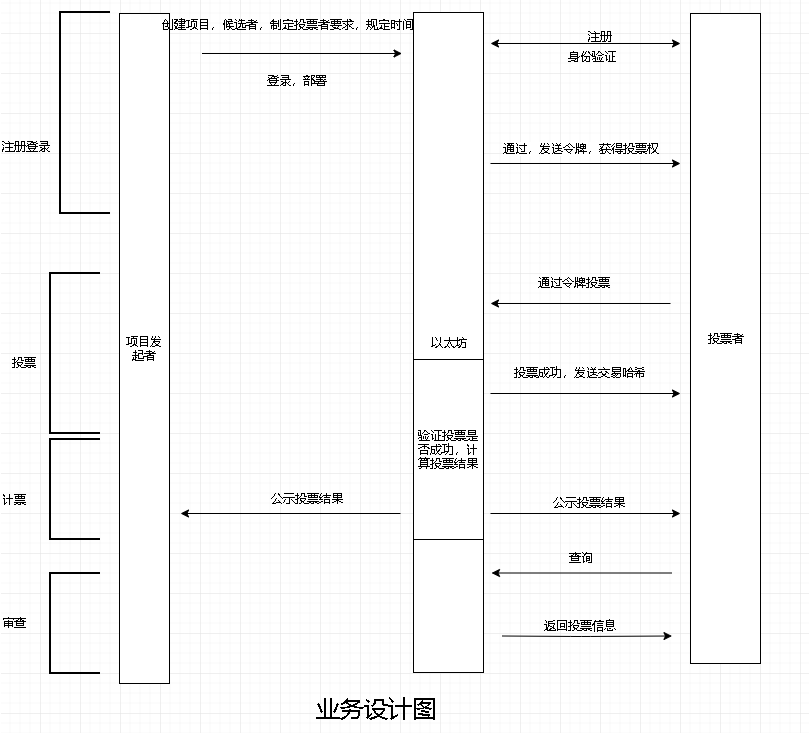


1.3.3 交互设计

（一）整体业务流程设计

投票流程分为四个阶段：注册登录、投票、计票、审查。

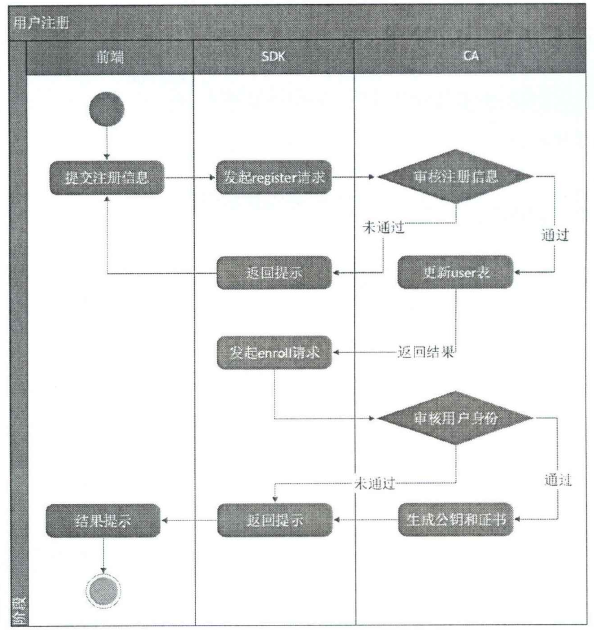
1. 注册登录：项目发起者登录以太坊，创建项目，候选者，制定投票者要求，规定投票起始和结束时间，部署合约。投票者向以太坊发送注册请求，以太坊确定其身份，向其发送令牌，投票者则获得投票权。
2. 投票：投票者通过令牌进行投票，若投票成功则会返回交易哈希。
3. 计票：每一次成功的投票都会被记录在区块上，并会显示，每一次成功的投票都能看到票数的变化，事先制定好的时间截止后，程序自动停止，计算出总数，并排出得票最高者公示。
4. 审查：投票者可以通过自己的地址查询自己的投票信息，每个人只能看到他人是否投票，不能查询他人的投票详情。



1. **用户注册流程设计**

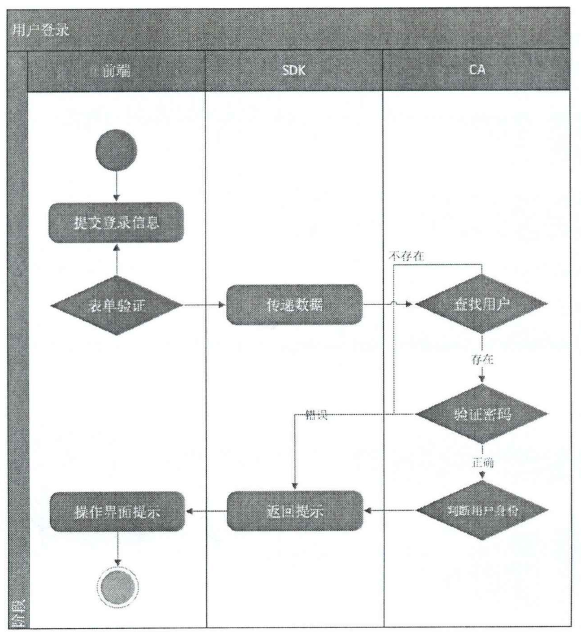
在用户注册模块的运行过程中，首先由界面展示层为用户提供注册信息填写的输入接口，具体表现为注册页面的输入窗口或框体与提交信息按钮。之后将用户填写的注册信息发送至业务逻辑层SDK客户端，客户端接收到信息后调用CA的接口发起register请求，并等待CA判断请求结果，若用户填写的信息有误或用户并非首次申请注册则拒绝其注册请求并返回提示信息并告知用户。

若注册请求通过则告知客户端，随后客户端向CA发起enroll请求，请求发起后CA将审核用户身份是否有效，若有效则为用户生成密钥和证书并将其加入节点网络中并返回结果，若无效则返回无效提示。客户端收到提示结果后将其转发到前端，由前端告知用户的注册操作是否成功。



1. **登录流程设计**

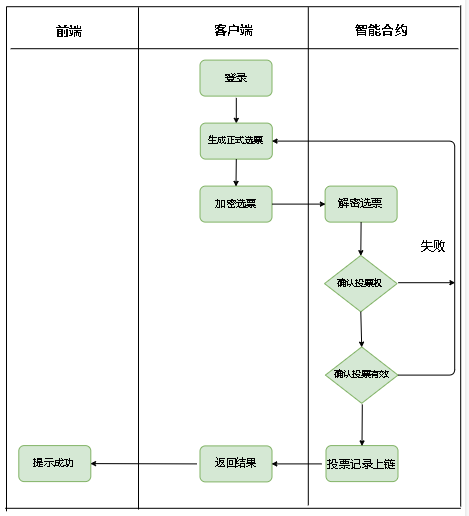
在用户登录模块的运行过程中，首先由界面展示层为用户提供登录信息填写的输入接口，具体表现为登录页面的输入窗口或框体与登录按钮。之后将用户填写的登录信息发送至客户端，客户端接收到信息后向CA发起查询请求，等待CA返回查询结果，若用户登录信息有误则拒绝其登录请求并返回提示信息并告知用户。若查询到对应记录，则将成功标识与用户身份返回到客户端，客户端收到相应数据后将其转发到前端，由前端进行判断并跳转到对应身份类别的主页中。



1. **投票流程设计**

投票中有客户端和区块链中智能合约参与，客户端先登录，第一步先生成正式选票，再加密选票，

1. 接下来由智能合约对选票进行解密，再由智能合约确认该客户端是否具有投票权，待确认后，再次确认该客户投票是否有效，若在确认投票权和确认投票是否有效失败，则返回客户端生成正式投票阶段。
2. 若上述阶段都成功认证，则投票成功，投票记录上链，交易信息记录在块。结果再返回客户端。在前端页面提示投票成功。



* 1. 关键技术及方法

在区块链的模型架构中，共识机制和安全机制是区块链的核心技术组件，现根据电子投票系统的应用，分别对非对称数字密码、分布式结构、共识机制等几个关键技术问题简要描述。

1.3.1非对称数字加密

区块链的模型设计中，一般采用非对称加密技术对数据进行加密验证。该算法使用的是一对密钥：公钥和私钥。这对密钥在非对称加密应用方式有两种。一种是公钥加密私钥解密，主要接收数据信息。另一种是私钥加密（签名）公钥解密（验证签名），主要判断是否是该节点发送的消息。因此，利用非对称数字加密技术在安全性能方面大大提高。

RSA是常用的非对称加密算法之一，该算法既能用于数据加密又能用于数字签名，因此本系统采用了RSA算法。该算法RSA算法是将两个约数较多且容易相乘的大素数进行乘积运算，若想要将乘积因式分解则困难7，因此可公开乘积并可将其作为加密密钥。RSA算法具有抗攻击性，因此在数据加密方面采用RSA算法安全可靠。

1.3.2分布式结构

区块链是一个具有共享状态的密码性安全交易的单机，分布式网络结构保证了数据记录存储在非中央计算机上，计算任务运行在多台计算机上，全网中的所有节点都将记录并存储计算任务中的数据交易信息。为此，区块链技术采用了开源的、去中心化的协议18，构建了一个分布式的结构体系，保证数据的完整记录和存储。

1. 分布式传播。区块链中产生新的交易数据均由单个节点向全网节点发送，若信息拦截者对部分节点传播路径进行恶意摧毁，不会影响整体信息的传输，全网中的所有节点均收到该数据信息。（2）分布式记账。区块链通过构建分布式机构体系和共识协议，允许所有节点在参与数据记录和验证其他节点结果的正确性。只有当所有参与记录的节点（或者大部分节点）比对结果一致通过，记录数据才允许被写入区块并最终将交易结果写入区块链。

（3）分布式存储。区块链构建一个分布式结构的网络系统，数据库中所有数据实时更新并存放于所有参与记录的节点。即使部分节点损坏或被攻击，也不会影响整个数据库的数据记录。

1.3.3共识机制

分布式系统中，最重要问题是全网所有节点如何达成共识。共识机制就是为了保证底层区块链数据的一致性，并有效的抵抗恶意节点的攻击和破坏。在节点网络中，所有节点在是否攻击外部节点问题上达成一致，但存在部分恶意节点，故意传递错误消息给其余正确节点，干扰判断，这就是拜占庭容错问题。传统的Paxos，Raft没有考虑这个问题；而POW算力过高，POS，DPOS过于集中化，三者广泛应用于公有链的虚资产。PBFT算法是联盟链中最常用的共识算法，通过投票来达成共识的机制，并解决数据分叉以及投票数据丢失和篡改等问题。

PBFT容错算法是一种基于消息传递一致性的算法，节点集合P中，每个节点都有对应唯一的编号，该系统中能容忍恶意或坏死节点的数最多为f，当节点数P13f+1的情况下可以达成共识。PFBT共识过程如下：（1）客户向服务器中的主节点发送调用服务操作的请求命令。（2）主节点向全网的节点广播请求。（3）所有的节点处理该请求，并将结果返回客户。（4）客户将返回的处理结果进行整理，当返回结果中至少有f+1个结果相同，则可停止该操作。

PFBT验证过程三阶段：预准备、准备、确认阶段。

预准备阶段，主节点分配一个系列号n，将PRE-PREPARE消息发送给其余节点。之后主节点将PRE-PREPARE消息广播到其他各节点。

准备阶段，各节点在收到PRE-PREPARE消息后，需验证消息的内容没有被篡改，验证结束后，该主节点会向各节点发送PREPARE消息。

确认阶段，当节点验证PREPARE消息为真后，会在全网中广播PREPARE消息。

验证完COMMIT消息后，节点可以将结果返回给客户端。

该算法性能比较高，消耗资源少。因此比较适合现代的电子投票系统。执行流程如图1所示。

