# 基于区块链的投票系统

目录

引言

第1章 基于区块链的投票系统

1.1 背景与现状

1.1.0 区块链简介

1.1.1 电子投票的发展历史

1.1.2 电子投票发展现状

1.1.3 区块链投票的国内外发展现状

1.1.4 区块链投票仍保守争议

1.2 区块链投票的简介及优势

1.2.1 区块链投票是什么？

1.2.2 为什么选择区块链投票？

1.2.3 区块链投票的优势

1.3 基于区块链的投票方案设计

1.3.1 业务设计

1.3.2 架构设计

1.4 总结

引言

自从“区块链”大热以来，社会上各类区块链应用层出不穷。一时

间，这门新技术似乎成为各行各业的必需品，网络上甚至出现了“区块链马桶”的恶搞段子。一直以来，解决信任危机是区块链的最大“卖点”之一。而在最需要信任的投票场景中，刷票、后台篡改数据、黑客攻击等频频发生。那么利用区块链去解决这些问题，可行吗？通过各类报道，我们可以直观地看到，区块链投票系统在世界各地的使用率在逐渐增加。不论是在美国、日本还是瑞士，倡导区块链技术的人认为，这项技术可以让选举更透明、更公平、更高效。区块链技术得到了来自社区和政治团体的支持，这在一定程度上促进了区块链技术的成功实施。

面向对象

本书的读者对象包括但不限于：

·区块链应用设计者；

·区块链应用开发者；

·区块链爱好者；

·能源互联网关注者；

·集团和社会治理者；

·使用区块链参与业务应用的公司与集体；

·开设相关课程的大专院校师生。

第1章 基于区块链的投票系统

随着社会的发展进步，许多应用场景都需要进行投票表决。针对当前电子投票系统中出现的问题，如投票数据不够公开透明且容易被篡改伪造，用户的私密信息存在被泄露的风险，选民无法验证投票结果等，提出了一种基于区块链智能合约技术的安全多候选人投票系统。系统通过智能合约自动执行机制取代传统的可信第三方计票机构来实现自我计票，并在系统中加入两轮零知识证明协议，有效确保投票者的身份合法性，同时保护选票内容的隐私性，而基于区块链的匿名特性也确保了投票系统的匿名性。最后，在以太坊的私链网络上测试运行的实验数据说明，本系统具有可行性。通过安全性分析表明，提出的投票方案满足安全性要求，可以应用于企业董事会选举等规模小且匿名隐私性高的场景。

1.1背景与现状

1.1.0 区块链简介

该平台是基于区块链开发的，但鉴于区块链的普及程度在目前来讲不是很高，还有许多人只是听说过区块链这个名词，对区块链没有实际的概念，所以在正文开始之前，先对区块链做一个简单的介绍。（部分图文来自百度）

**起源**

区块链起源于[比特币](https://baike.baidu.com/item/%E6%AF%94%E7%89%B9%E5%B8%81/4143690" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)，2008年11月1日，一位自称[中本聪](https://baike.baidu.com/item/%E4%B8%AD%E6%9C%AC%E8%81%AA/5740822" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)(Satoshi Nakamoto)的人发表了《比特币:一种点对点的电子现金系统》一文，阐述了基于[P2P](https://baike.baidu.com/item/P2P/139810" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)网络技术、加密技术、[时间戳](https://baike.baidu.com/item/%E6%97%B6%E9%97%B4%E6%88%B3/6439235" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)技术、区块链技术等的电子现金系统的构架理念，这标志着比特币的诞生。两个月后理论步入实践，2009年1月3日第一个序号为0的[创世区块](https://baike.baidu.com/item/%E5%88%9B%E4%B8%96%E5%8C%BA%E5%9D%97/22448241" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)诞生。几天后2009年1月9日出现序号为1的区块，并与序号为0的创世区块相连接形成了链，标志着区块链的诞生。

近年来，世界对比特币的态度起起落落，但作为比特币底层技术之一的区块链技术日益受到重视。在比特币形成过程中，区块是一个一个的存储单元，记录了一定时间内各个区块节点全部的交流信息。各个区块之间通过随机[散列](https://baike.baidu.com/item/%E6%95%A3%E5%88%97/9939480" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)(也称哈希算法)实现链接，后一个区块包含前一个区块的哈希值，随着信息交流的扩大，一个区块与一个区块相继接续，形成的结果就叫区块链。

**概念定义**

什么是区块链？从科技层面来看，区块链涉及数学、密码学、互联网和计算机编程等很多科学技术问题。从应用视角来看，简单来说，区块链是一个分布式的共享账本和数据库，具有去中心化、不可篡改、全程留痕、可以追溯、集体维护、公开透明等特点。这些特点保证了区块链的“诚实”与“透明”，为区块链创造信任奠定基础。而区块链丰富的应用场景，基本上都基于区块链能够解决信息不对称问题，实现多个主体之间的协作信任与一致行动。

区块链是[分布式](https://baike.baidu.com/item/%E5%88%86%E5%B8%83%E5%BC%8F/19276232" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)数据存储、[点对点传输](https://baike.baidu.com/item/%E7%82%B9%E5%AF%B9%E7%82%B9%E4%BC%A0%E8%BE%93/8491956" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)、共识机制、[加密算法](https://baike.baidu.com/item/%E5%8A%A0%E5%AF%86%E7%AE%97%E6%B3%95/2816213" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)等计算机技术的新型应用模式。区块链（Blockchain），是[比特币](https://baike.baidu.com/item/%E6%AF%94%E7%89%B9%E5%B8%81/4143690" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)的一个重要概念，它本质上是一个[去中心化](https://baike.baidu.com/item/%E5%8E%BB%E4%B8%AD%E5%BF%83%E5%8C%96/8719532" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)的数据库，同时作为[比特币](https://baike.baidu.com/item/%E6%AF%94%E7%89%B9%E5%B8%81/4143690" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)的底层技术，是一串使用[密码学](https://baike.baidu.com/item/%E5%AF%86%E7%A0%81%E5%AD%A6/480001" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)方法相关联产生的[数据块](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E5%9D%97/107672" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)，每一个数据块中包含了一批次比特币网络交易的信息，用于验证其信息的有效性（[防伪](https://baike.baidu.com/item/%E9%98%B2%E4%BC%AA/9638550" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)）和生成下一个区块。

[比特币](https://baike.baidu.com/item/%E6%AF%94%E7%89%B9%E5%B8%81/4143690" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)白皮书英文原版其实并未出现 blockchain 一词，而是使用的 chain of blocks。最早的比特币白皮书中文翻译版中，将 chain of blocks 翻译成了区块链。这是“区块链”这一中文词最早的出现时间。

国家互联网信息办公室2019年1月10日发布《[区块链信息服务管理规定](https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE%E4%BF%A1%E6%81%AF%E6%9C%8D%E5%8A%A1%E7%AE%A1%E7%90%86%E8%A7%84%E5%AE%9A/23245975" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)》，自2019年2月15日起施行。

作为核心技术自主创新的重要突破口，区块链的安全风险问题被视为当前制约行业健康发展的一大短板，频频发生的安全事件为业界敲响警钟。拥抱区块链，需要加快探索建立适应区块链技术机制的安全保障体系。

**发展历程**

2008年由[中本聪](https://baike.baidu.com/item/%E4%B8%AD%E6%9C%AC%E8%81%AA/5740822" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)第一次提出了区块链的概念，在随后的几年中，区块链成为了[电子货币](https://baike.baidu.com/item/%E7%94%B5%E5%AD%90%E8%B4%A7%E5%B8%81/82066" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)比特币的核心组成部分：作为所有交易的公共账簿。通过利用点对点网络和[分布式](https://baike.baidu.com/item/%E5%88%86%E5%B8%83%E5%BC%8F/7316617" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)时间戳服务器，区块链数据库能够进行自主管理。为比特币而发明的区块链使它成为第一个解决重复消费问题的数字货币。比特币的设计已经成为其他应用程序的灵感来源。

2014年，"区块链2.0”成为一个关于去中心化区块链数据库的术语。对这个第二代可编程区块链，经济学家们认为它是一种编程语言，可以允许用户写出更精密和智能的协议。因此，当利润达到一定程度的时候，就能够从完成的货运订单或者共享证书的分红中获得收益。区块链2.0技术跳过了交易和“价值交换中担任金钱和信息仲裁的中介机构”。它们被用来使人们远离[全球化](https://baike.baidu.com/item/%E5%85%A8%E7%90%83%E5%8C%96/489841" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)经济，使隐私得到保护，使人们“将掌握的信息兑换成货币”，并且有能力保证知识产权的所有者得到收益。第二代区块链技术使存储个人的“永久数字ID和形象”成为可能，并且对“潜在的社会财富分配”不平等提供解决方案。

2016年1月20日，中国人民银行[数字货币](https://baike.baidu.com/item/%E6%95%B0%E5%AD%97%E8%B4%A7%E5%B8%81" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)研讨会宣布对数字货币[研究](https://baike.baidu.com/item/%E7%A0%94%E7%A9%B6" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)取得阶段性成果。会议肯定了数字货币在降低传统货币发行等方面的价值，并表示央行在[探索](https://baike.baidu.com/item/%E6%8E%A2%E7%B4%A2" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)发行数字货币。中国人民银行数字货币研讨会的表达大大增强了数字货币行业信心。这是继2013年12月5日央行五部委发布关于防范比特币风险的通知之后，第一次对数字货币表示明确的态度。

2016年12月20日，数字货币联盟——中国FinTech数字货币联盟及FinTech研究院正式筹建。

如今，[比特币](https://baike.baidu.com/item/%E6%AF%94%E7%89%B9%E5%B8%81/4143690" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)仍是数字货币的绝对主流，数字货币呈现了百花齐放的状态，常见的有bitcoin、litecoin、dogecoin、dashcoin，除了货币的应用之外，还有各种衍生应用，如[以太坊](https://baike.baidu.com/item/%E4%BB%A5%E5%A4%AA%E5%9D%8A/20865117" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)Ethereum、[Asch](https://baike.baidu.com/item/Asch/20112653" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)等底层应用开发平台以及NXT，SIA，比特股，MaidSafe，Ripple等行业应用。

**类型**

公有区块链

公有区块链（Public Block Chains)是指：世界上任何个体或者团体都可以发送交易，且交易能够获得该区块链的有效确认，任何人都可以参与其共识过程。公有区块链是最早的区块链，也是应用最广泛的区块链，各大bitcoins系列的虚拟数字货币均基于公有区块链，世界上有且仅有一条该币种对应的区块链。

联合（行业）区块链

行业区块链（Consortium Block Chains)：由某个群体内部指定多个预选的节点为记账人，每个块的生成由所有的预选节点共同决定（预选节点参与共识过程），其他接入节点可以参与交易，但不过问记账过程(本质上还是托管记账，只是变成分布式记账，预选节点的多少，如何决定每个块的记账者成为该区块链的主要风险点），其他任何人可以通过该区块链开放的[API](https://baike.baidu.com/item/API/10154" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)进行限定查询。

私有区块链

私有区块链（Private Block Chains)：仅仅使用区块链的总账技术进行记账，可以是一个公司，也可以是个人，独享该区块链的写入权限，本链与其他的分布式存储方案没有太大区别。传统金融都是想实验尝试私有区块链，而公链的应用例如bitcoin已经工业化，私链的应用产品还在摸索当中。

其中，我们项目中使用的就是私有区块链。

**特征**

[去中心化](https://baike.baidu.com/item/%E5%8E%BB%E4%B8%AD%E5%BF%83%E5%8C%96/8719532" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)。区块链技术不依赖额外的第三方管理机构或硬件设施，没有中心管制，除了自成一体的区块链本身，通过[分布式](https://baike.baidu.com/item/%E5%88%86%E5%B8%83%E5%BC%8F/19276232" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)核算和存储，各个节点实现了信息自我验证、传递和管理。去中心化是区块链最突出最本质的特征。

开放性。区块链技术基础是开源的，除了交易各方的私有信息被加密外，区块链的数据对所有人开放，任何人都可以通过公开的接口查询区块链数据和开发相关应用，因此整个系统信息高度透明。

独立性。基于协商一致的规范和协议(类似[比特币](https://baike.baidu.com/item/%E6%AF%94%E7%89%B9%E5%B8%81/4143690" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)采用的哈希算法等各种数学算法)，整个区块链系统不依赖其他第三方，所有节点能够在系统内自动安全地验证、交换数据，不需要任何人为的干预。

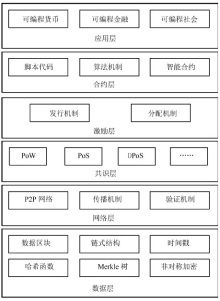
安全性。只要不能掌控全部数据节点的51%，就无法肆意操控修改网络数据，这使区块链本身变得相对安全，避免了主观人为的数据变更。

匿名性。除非有法律规范要求，单从技术上来讲，各区块节点的身份信息不需要公开或验证，信息传递可以匿名进行。

其中我们的项目中就有运用到去中心化，安全性，匿名性等特性。

**架构模型**

区块链基础架构模型



一般说来，区块链系统由[数据层](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E5%B1%82/20352986" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)、[网络层](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E5%B1%82/4329439" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)、[共识层](https://baike.baidu.com/item/%E5%85%B1%E8%AF%86%E5%B1%82/22448420" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)、[激励层](https://baike.baidu.com/item/%E6%BF%80%E5%8A%B1%E5%B1%82/22447972" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)、[合约层](https://baike.baidu.com/item/%E5%90%88%E7%BA%A6%E5%B1%82/22469234" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)和[应用层](https://baike.baidu.com/item/%E5%BA%94%E7%94%A8%E5%B1%82/16412033" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)组成。

其中，数据层封装了底层数据区块以及相关的数据加密和时间戳等基础数据和基本算法；网络层则包括分布式组网机制、数据传播机制和数据验证机制等；共识层主要封装网络节点的各类共识算法；激励层将经济因素集成到区块链技术体系中来，主要包括经济激励的发行机制和分配机制等；合约层主要封装各类[脚本](https://baike.baidu.com/item/%E8%84%9A%E6%9C%AC/1697005" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)、算法和智能合约，是区块链可编程特性的基础；应用层则封装了区块链的各种应用场景和案例。该模型中，基于时间戳的链式区块结构、分布式节点的共识机制、基于共识算力的经济激励和灵活可编程的智能合约是区块链技术最具代表性的创新点

**核心技术**

分布式账本

[分布式](https://baike.baidu.com/item/%E5%88%86%E5%B8%83%E5%BC%8F/19276232" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)账本指的是交易记账由分布在不同地方的多个节点共同完成，而且每一个节点记录的是完整的账目，因此它们都可以参与监督交易合法性，同时也可以共同为其作证。

跟传统的分布式存储有所不同，区块链的分布式存储的独特性主要体现在两个方面：一是区块链每个节点都按照块链式结构存储完整的数据，传统分布式存储一般是将数据按照一定的规则分成多份进行存储。二是区块链每个节点存储都是独立的、地位等同的，依靠[共识机制](https://baike.baidu.com/item/%E5%85%B1%E8%AF%86%E6%9C%BA%E5%88%B6/20234683" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)保证存储的一致性，而传统分布式存储一般是通过中心节点往其他备份节点同步数据。没有任何一个节点可以单独记录账本数据，从而避免了单一记账人被控制或者被贿赂而记假账的可能性。也由记账节点足够多，理论上讲除非所有的节点被破坏，否则账目就不会丢失，从而保证了账目数据的安全性。

非对称加密

存储在区块链上的交易信息是公开的，但是账户身份信息是高度加密的，只有在数据拥有者授权的情况下才能访问到，从而保证了数据的安全和个人的隐私。

共识机制

共识机制就是所有记账节点之间怎么达成共识，去认定一个记录的有效性，这既是认定的手段，也是防止篡改的手段。区块链提出了四种不同的共识机制，适用于不同的应用场景，在效率和安全性之间取得平衡。

区块链的[共识机制](https://baike.baidu.com/item/%E5%85%B1%E8%AF%86%E6%9C%BA%E5%88%B6/20234683" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)具备“少数服从多数”以及“人人平等”的特点，其中“少数服从多数”并不完全指节点个数，也可以是计算能力、股权数或者其他的计算机可以比较的特征量。“人人平等”是当节点满足条件时，所有节点都有权优先提出共识结果、直接被其他节点认同后并最后有可能成为最终共识结果。以[比特币](https://baike.baidu.com/item/%E6%AF%94%E7%89%B9%E5%B8%81/4143690" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)为例，采用的是工作量证明，只有在控制了全网超过51%的记账节点的情况下，才有可能伪造出一条不存在的记录。当加入区块链的节点足够多的时候，这基本上不可能，从而杜绝了造假的可能。

智能合约

智能合约是基于这些可信的不可篡改的数据，可以自动化的执行一些预先定义好的规则和条款。以保险为例，如果说每个人的信息（包括医疗信息和风险发生的信息）都是真实可信的，那就很容易的在一些标准化的保险产品中，去进行自动化的理赔。在保险公司的日常业务中，虽然交易不像[银行](https://baike.baidu.com/item/%E9%93%B6%E8%A1%8C/392719" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)和[证券](https://baike.baidu.com/item/%E8%AF%81%E5%88%B8/267" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)行业那样频繁，但是对可信数据的依赖是有增无减。因此，笔者认为利用区块链技术，从数据管理的角度切入，能够有效地帮助保险公司提高[风险管理](https://baike.baidu.com/item/%E9%A3%8E%E9%99%A9%E7%AE%A1%E7%90%86/3419129" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)能力。具体来讲主要分投保人风险管理和保险公司的风险监督。

1.1.1 电子投票的发展历史

2012的美国总统大选，美国时间11月6日，美国人民就将投票选举出下一任美国总统。1960年，电视媒体的兴起开创了总统候选人之间电视辩论的先河，而现在网络时代已经来临，网络的普及能不能给总统选举带去什么新内容呢？

就当时环境而言，美国的总统选举体系并不完美，票选环节便是关键之处。票选舞弊、恐吓选民、党派操纵、故意将票站设远的案例时有发生，投票率低下（美国投票率通常小于50%）也是挥之不去的问题之一。按理来说，在这个电脑、智能手机等计算设备和网络都已经普及的时代，使用网络在线投票应该能够很好地解决这些难题。可是，网络真能发挥我们想象中的功效吗？答案是：不行。

## 技术障碍：确保投票平台安全和可靠是个大问题

由于总统大选的特殊性，该选举容不得一丝一毫的虚假。如果人们要借助网络投票系统来进行票选，那么系统的性能必须经得起多方考验。第一，这套系统要保障每一个选民的选票内容不会泄露给第三方；第二，选票系统要记录每一张选票背后的选民信息；第三，该系统要保证每张选票背后的选民信息不会被第三方探知；第四，该系统要保证每位选民只能投票一次；最后，系统的统计数据要完全反映选票的真实情况，不能出现任何误差。这必须是一套可靠、灵活、方便的系统，而且还得是一套省钱的系统。人们能否开发出满足以上所有要求的网络投票系统呢？大部分业内专家都对此持怀疑态度。

事实上，有关网络投票系统的开发从2000年就开始了，至今也有不少测试系统问世，但与之相伴的却是不绝于耳的警告声。无论是网络安全行业内的专家，还是美国国家科学技术委员会（NSTC）这样的政府组织，都从测试系统中发现了系统安全、选民身份认证和选票审计等相关方面的漏洞。行业专家认为，至少在可见的未来内，一套能够满足选举要求的网络投票系统都无法诞生。网络在我们的印象中向来是无所不能的存在，它为何突然变得如此无力了呢？



斯坦福大学教授大卫·迪尔（David Dill）是研究网络投票系统的专家，他认为这套系统的诞生不仅远在天涯，而且可能永远都不会到来。作为计算机安全领域的专家，迪尔掌管着“选举核实”（Verified Voting）组织，该组织的工作目的就是开发一套满足选举投票要求的网络投票系统。“在我看来，网络投票对于总统选举的价值是存在的，但我们始终找不到下手的地方。如果只有一两个问题需要解决那还好办一些，但事实是：存在的问题太多了。”

迪尔认为，最棘手的问题是如何确保投票平台的可信度。当人们使用网络投票系统进行投票时，他们需要依赖个人电脑、平板和手机等终端设备，然而这些终端设备无法保证选民投出的选票信息不被篡改。“网络投票就是为了便捷，所以必然要牵扯到这些非常私人化的终端设备。电脑上会不会有病毒，会不会有恶意软件，这些都不好说。” 迪尔认为，许多人的电脑事实上早已遭受网络黑客的进攻沦为肉鸡，在这种情况下，即使他们使用密码学手段加密选票信息，黑客依然有办法篡改上传的数据。况且，黑客并不是唯一的威胁来源。总统选举牵扯到太多人的利益，想方设法操纵选票的单位和个人数不胜数。这些人可能是黑客，也有可能是应用的编写人员，而应用编程人员拥有进入操作系统的合法身份。 设想一下，当用户在《疯狂的小鸟》中愉快地发射小鸟时，他可能就把自己的选票投出去了。 总之，通过移动设备投票的想法十分不靠谱。“长远地说，谁也不能保障这些设备的安全性。”迪尔表示，即使人们在移动设备上安装了安全控件，他们依然无法阻止自己的设备被操纵，安全控件挡不住拥有进入操作系统合法身份的编程人员。

虽然困难重重，但人们开发网络投票系统的信念却从未动摇。支持者认为，在目前的投票体系内，选民为了投出自己宝贵一票需要在路上耗费很长时间，在许多票站还都存在选民排起长龙的拥堵情况。如果每个人都能够轻而易举地通过身边的设备上网投票，投票率会爬升到历史无法企及的高度，这简直可以称得上是民主的福音。

在“民主福音”的召唤下，美国人民在过去的十几年内的确做了大量的尝试。1999年，比尔·克林顿要求美国国家科学基金会（National Science Foundation）开发一套值得信赖的网络投票系统，希望借此挽回日益低落的投票率。2000年，民主党在亚利桑那州的初选中使用了网络投票系统，而共和党也在阿拉斯加州的选举前民意调查中使用了网络投票系统，然而这些系统无一例外地夭折了。对于这些不完美的测试系统，计算机信息领域专家大卫·杰弗森博士（Dr. David Jefferson）和艾未尔·鲁宾博士（Dr. Aviel Rubin）认为，问题出现在计算机和网络的基础架构之上，如果没有根本性的变革出现，网络投票只能是天方夜谭。

## 用户需求：美国总统四年才选一次，公众对网络投票并没有那么大的需求

尽管网络专家预断了网络投票的不可实现性，但现实中依旧坚持走在这条路上的人还大有人在。Safevote、Everyone Counts和Diebold While等组织都在不断开发属于自己的专利技术，他们还与各级政府部分达成了小规模的合作。纸质选票的缺点也越来越多地被各州政府接受，不少州政府都为选票实现了电子化，当然他们仍旧无力采用远程网络投票。

人们在网上阅读，在网上购物，网络正在慢慢占领我们生活的每一个部分。网络投票系统的支持者认为，只要人们有在线投票的需求，困难终究会被克服。“网络投票终将实现”，这种论调看似公理般无需证明，却实为一种空泛的念想。事实上，对于普通人而言，四年一度的总统大选并不如每天都能在线购物那般重要，而政府钻研网络投票系统的动机也只有提升投票率一点。对于军方而言，开发网络投票系统是为了给身处异乡的大兵们投票权，但他们的动机也仅限于此。“一切只是时间问题。人们通过网络做任何事情，只要他们有在线投票的需求，困难终究会被克服。”联邦选举委员会（Federal Election Commission）前任理事戴夫·马森（Dave Mason）对网络投票系统的未来持有乐观态度，然而与他站在同一战线上的公众真是少之又少。

科技发展的力量不容置疑，所以可以肯定的是，如果有足够大的用户需求，完美的网络投票解决方案终将出现。但是，仅仅是总统选举这一件事无法激起足够的用户需求。

美国总统选举的历史可以追溯到1845年，那时的社会形态与如今完全不同，所以总统选举这个事情的概念也大不一样。当时人们没有电视，没有网络，总统选举倒成为了最好的休闲之一。“投票是一项社会活动。十九世纪时人们在投票之余会聚集在一起，押宝哪位候选人将获得成功。而现在，我们会带着自己的孩子去票站，让他体验生活，明白作为一名社会公民都有哪些权利和义务。从某些角度来说，选举投票会驱使人群有目的性地流动。”马里兰圣玛丽学院（St. Mary's College of Maryland）政治学科教授麦克·J.G·该隐（Michael J. G. Cain）认为传统的投票活动没必要改变。“当然我也不是说改变就不会发生，但至少不是现在。”

在刺激投票率方面，网络投票系统究竟能发挥多大的作用还有待考证。影响投票率的因素十分复杂，比如说，对于许多放弃选票的选民而言，给予更加便利的投票方式对他们毫无价值。在俄勒冈州（Oregon），选民在亲赴票站之余也可以通过邮件投票，但这个政策并没有收获多少的投票率。在网络投票之余，美国政府还能提供一些更为简单的促进方案，比如将选举日定为公休假，或是将放宽投票期限，这些手段都不用网络工程师出马。

值得认可的观点认为，推出网络投票系统的难度太大，人们应当把精力放到其他更亟待解决的难题上。所以，本领高强的互联网这次是碰到了一座拿不下的五指山。11月6日，美国人民仍然需要去票站排队投出自己神圣的一票。

1.1.2 电子投票的发展现状

相比于纸质投票，电子投票为人民提供了便利。网络投票”的初衷是好的。利用网络投票不仅节约成本，而且能更便捷、更迅速地传播活动信息、扩大影响规模，让更多的人知道并参与评选，最重要的是让评选更能代表“民意”。然而“网络投票”在方便了我们的同时却也产生了一系列不利的弊端。  
　　  
一些居心叵测的人利用“网络投票”的隐蔽性、非实名性、线外操作性钻空子。近些年来，各种刷票软件层出不穷，专门用于网络刷票的“网络投票代理公司”也叠见层出。而那些企图通过“刷票”获胜的人对此则欢呼雀跃。事物都具有两面性，但当弊端大于益处后，我们就不得不对其进行反思和重新界定了。“网络投票”初衷有违，我们不得不质疑其意义何在？

但时下的一些网络投票，形式大于内容，甚至就是一种新的形式主义。像上面新闻中记者所揭示的这一现象，在不少地方具有一定的普遍性，集中反映了网络投票之乱象——功利、作秀、虚假、扰民。将创新工作的成效评价寄托在相当不靠谱的网络投票上，纯粹看走了眼、用错了情，既浪费了社会资源，污染了社会风气，也是一种形式主义，让基层干部不堪其重。  
　　  
打开电脑或手机，各种QQ群、朋友圈、贴吧、论坛等时不时地弹出各种投票链接。很多时候出于交情我们不得不勉为其难地为亲戚、朋友以及其他一些略有交集的人投上“宝贵”的一票，即使他们的作品或者他们自己本身与其他选手相差甚远。更有一些人为了让自己或者自己“中意的人”或者受委托帮忙拉票的人得到更多的选票，又会去发动亲戚、朋友、同事、熟人甚至网友来投票。在学校，有的学院为了优胜于其他学院则把为本学院投票当作是一种任务，要求每个同学都必须参与。在政府、企业，某些单位为了让本单位参加比赛的人胜出而把投票当成一种“政治任务”，要求单位的所以成员都要参加。如此一来，网络投票就演变成了谁能充分利用网络资源和人际关系谁就能胜出，这和其本来的初衷已经天差地别，那么我们不得不追问其意义何在？  
　　  
此外，一些网络投票的背后往往存在商业利益。某些商家以金钱为诱要求参与者在投票前必须关注相关公众号或者下载相应的App。参与者又将其推广，积累了一定数量的“赞”或者拉了一定数量的"票"后则能获得相应的报酬。在金钱的驱使下，参与者往往会乐此不疲地为其传播、扩散。而这些商家真正的目的则是把网络投票当成扩大活动影响力、聚集粉丝的营销手段，并不在乎评选结果是否真实。网络投票中存在的“拉票”、“买票”行为，往往导致了最终结果与真实“民意”的极大偏差。  
　　  
QQ群变成了“拉票群”；朋友圈变成了“拉票圈”。各大购物平台的刷票服务，各网站不正当的刷票软件，各种“人情绑架”、“金钱绑架”使我们的评选与网络投票的初衷渐行渐远。  
　　  
而对于那些真正优秀、真正有实力，但人际关系比较弱或者不屑于拉票的人来说，“网络投票”难免有失公平。大多数人在为别人投票或者拉票时根本不知道他们所要投票的人参加了什么活动、情况怎么样、与其他选手相比表现怎样。他们只知道投谁、投几号、怎么投。人们就这样在QQ群、朋友圈、贴吧、论坛相互投票、拉票，久而久之形成了一种机械性的操作行为，只要见到投票链接就点击、关注、投票，然后又扩散到其他的QQ群、朋友圈、贴吧、论坛。这样的话“网络投票”就变成了一种比拼人气、人脉、关系的工具，失去了其原来的民主民意、公平公正的意义了。  
　　  
大大小小的“网络投票”已成为了社会的一个弊病，对其滥用已经导致了民主与公平的丢失。若不加以规范、监督，一但其进一步演变为商业人士、政府官员谋取私利的一种手段时，后果将不堪设想。

所以网络投票的当务之急，就是找到一个公开、公正、透明且安全稳定的搭载平台，从而从根本上杜绝这些不规范投票行为的发生。

1.1.3 区块链投票的国内外发展现状

二战后的日本一直没有明确统一的身份制度，但是经过几届政府的推动，2016年起，所有日本公民均有12位数字的身份证号码。重要的是，2018年8月底，这“12位身份证号码”在筑波区块链投票系统试验中被用来参与投票。

筑波是一个从1960年左右就因科技发展而迅速文明的城市。此次投票中，筑波官网公告称，选民能够为政府实施的不同决策投票，比如选民比较青睐的财政决策。

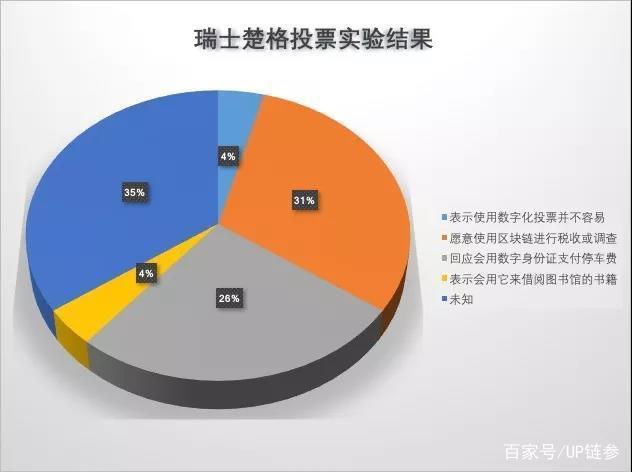
在这个试验系统中，身份验证机器与去中心化网络进行集成。选民在机器上放置身份证进行验证，然后选择喜欢的决策进行投票。系统通过防篡改的分布式网络进一步加密和存储选票数据。

筑波市市长Tatsuo lgarashi通过该系统投票后表示：“我以为这个系统会涉及到更复杂的程序，但发现这十分简单和容易”。

无独有偶，瑞士小镇楚格，拥有美丽的山景、瑞士风格建筑，它跟筑波一样是一个区块链“圣地”，市政府也允许居民使用区块链资产支付。此外，楚格的中央区块链基地吸引了大量区块链支持者涌入，这个小镇因此被冠以"加密谷"的称号。

近期，楚格也成功完成了区块链投票试验。

2018年，6月25日到7月1日，楚格进行了区块链投票实验。在参与投票的240名公民中，只有72人参加了不具约束力的审判投票。投票结果如下图所示：



在这场投票实验中，楚格人民除了要对市政事务进行投票以外，还就“区块链是否能够应用于开斋节制度”进行了投票。

走出日本小城筑波和瑞典小镇楚格，区块链投票系统也将在美国西弗吉尼亚州“大展身手”。

2018年11月，弗吉尼亚州联邦选举将首次使用智能手机进行投票。弗吉尼亚允许在武装部队服役及居住在国外的其他公民使用智能手机投票。这些居民可以通过 Voatz 软件进行投票。

弗吉尼亚州的官员通过 PDF 文件概述了投票过程:“投票所需要的只是苹果或安卓移动设备，以及经过批准、经过验证的州或联邦身份证。”

但是，目前还是有许多国家及地方政府不信任区块链投票的安全性。

据报道，3月7日，Agora 首席执行官Leonardo Gammar表示，塞拉利昂在清点总统选票时采用了区块链技术，显然，塞拉利昂是世界上第一个将区块链技术应用在选举上的国家了。然而，Gammar的说法并不准确，因为塞拉利昂并未直接使用区块链技术来统计选票，只是展示了下如何利用区块链技术进行选举。

因为Gammar的表述，使得媒体对塞拉利昂进行了大范围报道，而塞拉利昂政府则否认使用了区块链技术，并迫使Gammar纠正他的表述。

尽管塞拉利昂政府的这一做法引起了人们的愤怒，但区块链技术在选举方面的应用已经开始浮出水面，而且看起来，各国政府都有兴趣使用这种技术。

Gammar表示，塞拉利昂的国家选举委员会仍有兴趣让他们回到塞拉利昂实施递补选举计划：

几周之后，塞拉利昂的递补选举就将举行，我会回到塞拉利昂，看看我们如何进一步发挥区块链投票的潜力。尽管卷入了媒体风暴，他们仍希望可以看到有其他什么可以做的事情。

相比之下，5月8日的弗吉尼亚初选的规模就显得小一些。

这是美国历史上首次由政府操作的，应用了区块链技术的投票。但是，这也不是完全的区块链选举，因为只是开放给一些特定的选民，比如军队成员。

此外，由于在投票中使用区块链技术的尝试仍在不断增加，人们对此举的反应也逐渐热烈起来,表现出了很大关注。

Mike Queen是西弗吉尼亚州秘书长Mac Warner的通讯主任，他表示：

秘书长办公室相信区块链技术确实能提高这种类型的移动选举应用的安全级别。我们真诚地希望，能够尽早允许军事选民使用这种类型的手机应用。

然而，有一些人认为这样的做法“真是疯了”。尽管目前为止，西弗吉尼亚州的选举还没有任何进展。

南卡罗来纳大学的计算机科学教授Duncan Buell，专注于投票系统和选举的完整性。他一直对自2015年开始的数字投票表示强烈反对，他认为，数字投票就跟区块链投票一样，给现实世界带来了很多问题。

Buell表示：

我强烈反对电子投票，我认为整个互联网投票的想法太疯狂了。事实上，目前已经出现了很多问题。首先是身份验证。你该如何验证机器的另一头是什么人呢？

他所指的应该是Voatz这个公司了。Voatz负责本次选举的执行，技术层面包括在用户的智能手机上使用指纹扫描或人脸识别，但Buell认为这些技术会受到黑客攻击。

由此可见，目前为止，还是有许多人不认可区块链投票。

1.1.4 区块链投票仍饱受争议

最近，美国国家科学院、工程和医学院（NASEM）发布了长达150页，题为《安全投票: 保护美国民主》(Securing the Vote: Protecting American Democracy)该报告不但认为目前不应该使用区块链投票系统，还提倡2020年的美国选举应该使用纸质选票。原因在于，尽管使用区块链技术作为“投票箱”似乎非常有“希望”，但这项技术并没有从根本上解决选举的基础安全问题。目前的区块链应用仍然缺乏保证投票过程可核查性、保密性、选票安全性的可用技术。最近，美国国家科学院、工程和医学院（NASEM）发布了长达150页，题为《安全投票: 保护美国民主》(Securing the Vote: Protecting American Democracy)。该报告不但认为目前不应该使用区块链投票系统，还提倡2020年的美国选举应该使用纸质选票。原因在于，尽管使用区块链技术作为“投票箱”似乎非常有“希望”，但这项技术并没有从根本上解决选举的基础安全问题。目前的区块链应用仍然缺乏保证投票过程可核查性、保密性、选票安全性的可用技术。

最近，美国国家科学院、工程和医学院（NASEM）发布该报告不但认为目前不应该使用区块链投票系统，还提倡2020年的美国选举应该使用纸质选票。原因在于，尽管使用区块链技术作为“投票箱”似乎非常有“希望”，但这项技术并没有从根本上解决选举的基础安全问题。目前的区块链应用仍然缺乏保证投票过程可核查性、保密性、选票安全性的可用技术。

NASEM还进一步列举了一些反对区块链投票系统的理由：

引入区块链技术就相当于引入了其他安全漏洞。在投票未达区块链时，投票设备上的恶意软件可能会篡改选票。由此看来，选票并不会因为区块链的不可变性而免受人为或恶意修改。

此外，报告中还认为，区块链倡导者吹捧的透明性和不可篡改性，可以以更简单的方式实现。同时，解决选票的安全性等问题应该依赖额外的机制，而不是使用区块链。

同时，宾夕法尼亚大学的密码学和安全研究者马特布雷泽(Matt Blaze)也认为区块链在投票系统中引入了其他漏洞。布雷泽还表示，使用其他方法也可以确保投票更容易、更简单、更安全地完成。

美国智库布鲁金斯学会(Brookings Institute)的一份报告指出，区块链技术有可能改变投票过程，但仍然需要对区块链进行全面测试，并考虑广泛实施的成本。此外，如果要广泛使用电子投票，必须解决的问题具体包括安全问题、选民胁迫、认证以及给地方官员带来的不便等。

非政府组织Verified Voting的总裁 Marian k. Schneider认为，弗吉尼亚州将在2018年1月采用的 Voatz投票应用并不是区块链技术支持的应用程序，更像是具有区块链特点的移动应用程序。更关键问题在于，尽管应用程序对选民的数据进行了加密，但目前的系统无法保证选民的手机和使用的网络不会出现漏洞。

早在2007年，加州和俄亥俄州就对他们的电子投票机制进行了全面审计。可是审计结果并不乐观，投票的所有环节普遍存在漏洞:

"研究人员能够在无法检测的情况下更改投票记录、删除审计日志，并将恶意软件加载到系统中。这些攻击可以由个人实施，而攻击者并没有太多的访问权限，甚至他们还可以远程执行其他类型攻击。"

所以在密码学家Bruce Schneier看来，区块链投票作为电子投票的一种新方式，不但没有摆脱传统电子投票的缺陷，还带来了更多麻烦。他在自己发表的一篇反对区块链选举的博客中写到：

"或许，区块链是保护选举过程不受恶意攻击和意外伤害唯一办法，但它却不是最好的办法。最好的办法是使用纸质投票。"

1.2 区块链投票的简介及应用

1.2.1 区块链投票是什么？

区块链投票类似于我们习惯的模拟投票。他们的概念和流程也很大同小异。为了进行数字投票，公民需要在特定的司法管辖区注册并证明其公民身份。然后，我们可以在与该用户密钥关联的区块链上记录其身份和国籍。

接下来，公民需要投票来表决。在区块链中，这很可能采用一种特殊的投票通证的形式，将这种通证存到用户的帐户中。这个通证也可能有一个投票的时间限制，之后它将通过智能合约销毁或失效。

用区块链进行投票，将涉及将投票通证(选票)发送到特定的地址。选民们将知道哪个地址与哪个候选人或公民投票一致。将通证发送到该地址即代表选票。

从技术角度来说，这听起来很简单。投票会在区块链上注册，而区块链是不可篡改、可验证和透明化的。我们可以轻而易举地唱票，并宣布选举的获胜者。此外，我们可以设计友好的用户界面，把向特定地址发送通证的过程隐藏在后台，自动化进行。相反，选民将会看到一个简单的线上界面，让他们选择候选人或议案，然后单击提交。

1.2.2 为什么选择区块链投票？

由于种种原因，在提名、推选村委会候选人的过程中，出现了一些不可思议的怪现象，令人可笑、不解和担忧，这些现象并有逐步蔓延扩大之势。长此以往，可严重影响今后农村选举工作的正常进行，可是如果用区块链投票，我们就能知道每一票都来自一个真实的个体，区块链的匿名性也能保证大家的权利和安全。

竞选出现的问题多种多样：大搞阴谋诡计、贿赂选民、大送空头支票、不正当竞争的危害、影响安定团结严重影响。而这些问题，在区块链面前，都不存在。能完美的解决人类一直无法完成的问题。

1.2.3 区块链投票的优势

区块链投票使民主更加透明

匿名投票是保护投票完整性最简单的方法，同时也可以保护选民的隐私。数字投票一直是一个巨大的挑战，因为很难在保持匿名性的同时确保每张选票有效。而区块链投票可以通过加密来改变这一现状。

将民主中最重要的方面数字化，这可能会对全世界的政治管理产生深远而持久的影响。公民可以更快地做出决定，全民公投成为一个可行的选择。代议制民主可能会因为公民的直接民主而被边缘化——但这仅仅略见一斑。区块链选举还会让操纵选举可能变得更加困难，甚至几乎不可能。本文探讨了区块链投票的工作原理及其对世界的影响。

如果区块链投票在普及程度和可用性方面不断提高，它将产生巨大的影响。它可能从根本上改变民主的运作方式。区块链投票是什么意思？

#### 1、提高投票过程的透明度

区块链投票的最大优点是让透明度增加。现在，一旦你投完票，接下来会发生什么就都与你无关了。即使你相信投票工作人员会准确地计算票数，你也没有办法确保你的选票算数。

而在区块链上，你可以跟踪你的投票并看到它最终出现在正确的位置。 即使它不会将你的信息与之相关联，你的投票也会存在于区块链中，所有历史情况都不会变。

#### 2、减少欺诈和选举舞弊

提高透明度的一个连带作用是减少欺诈。通过区块链身份验证，欺骗系统或在错误的司法管辖区投票变得更加困难。此外，在独裁者操纵选举的国家，区块链可以带来真正的民主。当然，启动区块链投票系统需要现任政府的支持。然而，随着时间的推移，区块链可能成为一个国际投票标准，国际社会将提倡在所有国家实行区块链治理。

#### 3、每天实时投票

如果区块链使投票透明，那么我们就可以实时跟踪和统计选票。这意味着选举可以在更短的时间内完成。此外，如果它们是数字化的，那么投票基础设施的投入就会减少。因此，投票选举可以在很短的准备时间内进行，以便迅速投票进行全民投票。

这将完全改变我们的日常生活。想象一下，如果你可以在手机上投票决定你所在城市的交通路线，或者是否要增加税收来为你所在社区的建造一个新的公园。投票可能成为高度定向的，甚至会出现面向社区的投票。投票更频繁，而几乎不需要增加开销，这可能使投票成为日常事件。

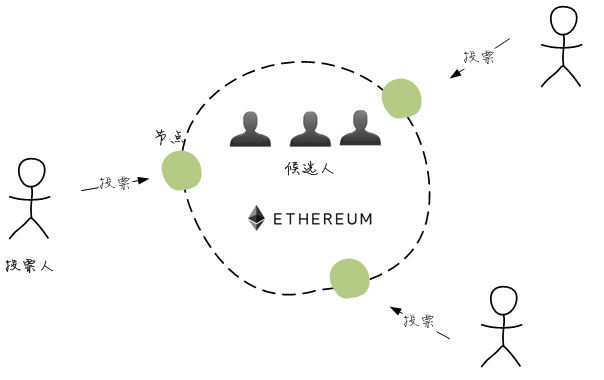
**4、企业治理和自治组织**

政府并不是唯一能从区块链投票中受益的机构。公司的员工或股东也可以为公司计划投票表决。我们甚至可以想象，可能会出现一种无主企业，企业的每一个决定都是由股东公开投票决定的。

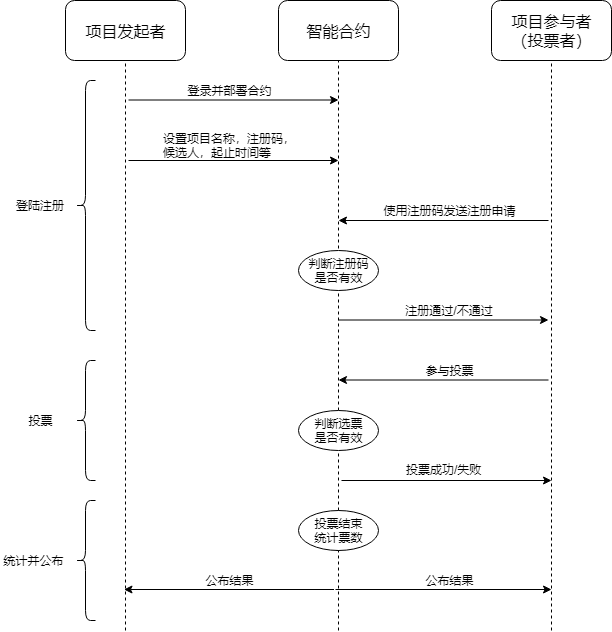
#### 5、增加选民参与度

区块链投票的一大优势可能是提高参与度。 如果区块链让你可以通过智能手机或计算机进行数字投票，选举就会像在几分钟内登录和投出选票一样简单。 这将会大大增加选民的投票率，从而使民主更加彻底。

1.3 基于区块链的投票方案设计



1.3.1 业务设计



区块链投票系统主要分为两部分：项目发起者界面和项目参与者界面，分别在各自的节点上运行，实现不同的功能和操作。

(1) 项目发起者界面：投票发起者初始化整个投票过程。包括以下功能：部署投票项目智能合约、认证投票者、设置注册码、发起投票项目、设置注册和投票的起止时间、查看投票结果等。

(2) 项目参与者界面：选民登录注册成为合格投票者进行投票。包括以下功能：登录注册、参与投票、提交选票、查看投票结果等。

(3) 具体操作流程：首先项目发起者登录到私人账户，部署智能合约，新建投票项目，设置参与者注册所需的注册码，设置投票选项，投票起止时间以及注册起止时间，至此，投票项目新建成功。然后，发起人将注册码发放至各个参与者手中，参与者登录到本人账号，通过发起人发放的注册码进行注册，随即注册成功，否则将无法通过注册。注册成功后可参与投票，选择要投票的候选项为其投票，每个账户只可以选择一个候选项进行投票，并且只能投一票，不可重复投票。待所有参与者都参与投票或到达投票截止时间后，智能合约会自行统计票数，并将最终的投票结果公布出来。投票结果所有人可见并且不会被私下修改，保证了投票的公平、公正、公开。

1.3.2 智能合约的实现

（1）合约概述

|  |  |
| --- | --- |
| 合约名称 | 合约功能 |
| Voting.sol | 投票智能合约，通过项目发起者部署，实现项目参与者注册，投票并附有自我计票等方法。 |

（2）功能概述

|  |  |
| --- | --- |
| 合约方法 | 具体功能 |
| projectSetup(string memory title, string memory select1, string memory select2, string memory select3) | 投票项目初始化，设置项目的名称及项目候选项 |
| registerIdSetup(bytes32 register1, bytes32 register2, bytes32 register3) | 设置项目参与者注册所需注册码 |
| TimeSetSetup(string memory register\_start\_time,string memory register\_end\_time, string memory vote\_start\_time, string memory vote\_end\_time) | 设置投票项目起止时间及注册起止时间 |
| voteForCandidate(bytes32 candidate) | 给候选项投票 |
| totalVotesFor(bytes32 candidate) | 候选项票数统计 |
| someoneRegister(bytes32 registerId) | 参与者注册 |
| VaildID() | 判断参与者是否有资格参与投票（是否注册） |
| isVoted() | 判断参与者是否已经参与投票（防止重复刷票） |

1. 合约演示
2. 代码段：

mapping (bytes32 => uint8) public votesReceived;

mapping (address=>bool) public voters;

mapping (address=>bool) public register;

mapping (address=>string) public voteData;

作用：创建多个映射关系，建立键－值的对应关系，用来改变返回值类型，后续便于通过键来查找或调用值。

1. 代码段：

string[] public candidateList;

bytes32[] public registerIdList;

string ProjectName;

string RegisterStartTime;

string RegisterEndTime;

string VoteStartTime;

string VoteEndTime;

uint8 registerCount = 0;

uint8 voteCount = 0;

代码分析：定义后续需要传参或使用的变量和数组

1. 代码段：

function projectSetup(string memory title, string memory select1, string memory select2, string memory select3) public{

ProjectName = title;

candidateList=[select1, select2, select3];

}

代码分析：定义一个名为projectSetup的方法，传递4个参数，将title传给ProjectName，并将3个select加入candidateList数组中，便于之后的调取

4、代码段：

function registerIdSetup(bytes32 register1, bytes32 register2, bytes32 register3) public{

registerIdList.push(register1);

registerIdList.push(register2);

registerIdList.push(register3);

}

代码分析：定义一个名为registerIdSetup的方法，传递3个数据类型为bytes32的注册码参数，并将其push到registerIdList数组中，便于之后的检测

5、代码段：

function TimeSetSetup(string memory register\_start\_time,string memory register\_end\_time, string memory vote\_start\_time, string memory vote\_end\_time) public{

RegisterStartTime = register\_start\_time;

RegisterEndTime = register\_end\_time;

VoteStartTime = vote\_start\_time;

VoteEndTime = vote\_end\_time;

}

代码分析：定义一个名为TimeSetSetup的方法，传递4个时间参数

1. 代码段：

function getProjectName() public view returns (string memory){

return ProjectName;

}

function getRegisterStartTime() public view returns (string memory){

return RegisterStartTime;

}

function getRegisterEndTime() public view returns (string memory){

return RegisterEndTime;

}

function getVoteStartTime() public view returns (string memory){

return VoteStartTime;

}

function getVoteEndTime() public view returns (string memory){

return VoteEndTime;

}

function getCandidateList1() public view returns (string memory){

return candidateList[0];

}

function getCandidateList2() public view returns (string memory){

return candidateList[1];

}

function getCandidateList3() public view returns (string memory){

return candidateList[2];

}

function getVoteCount() public view returns (uint8){

return voteCount;

}

function getVoteData() public view returns (string memory){

return voteData[msg.sender];

}

代码分析：参数调取函数，用于读出各数组或变量中的值，例如（ProjectName，RegisterStartTim等参数）

1. 代码段：

function totalVotesFor(bytes32 candidate) view public returns (uint8) {

return votesReceived[candidate];

}

代码分析：统计计票关键代码段，通过bytes32类型序数分别统计各个候选项的合计票数

1. 代码段：

function voteForCandidate(bytes32 candidate) public {

votesReceived[candidate] += 1;

}

代码分析：投票关键代码段，通过筛选数组中的元素序数，为指定的候选项添加票数

1. 代码段：

function someoneRegister(bytes32 registerId) public{

for(uint i = 0; i < registerIdList.length; i++){

if(registerIdList[i] == registerId){

register[msg.sender] = true;

registerIdList[i] = "0x0";

registerCount += 1;

}

}

}

代码分析：注册关键代码段，将注册码与msg.sender设置的注册码进行比对，若匹配，则完成注册

1. 代码段：

function VaildID() public view returns (bool) {

if(register[msg.sender]) {

return true;

}

return false;

}

代码分析：用于检测用户账号是否注册的函数，返回值为bool型

1. 代码段：

function isVoted() public view returns (bool) {

if(voters[msg.sender]) {

return true;

}

return false;

}

}

代码分析：同上，也为用于检测类型的函数，用于检测用户是否已经投票，防止用户有刷票行为，返回值为bool型

1. 功能演示

开发语言：solidity，web3js

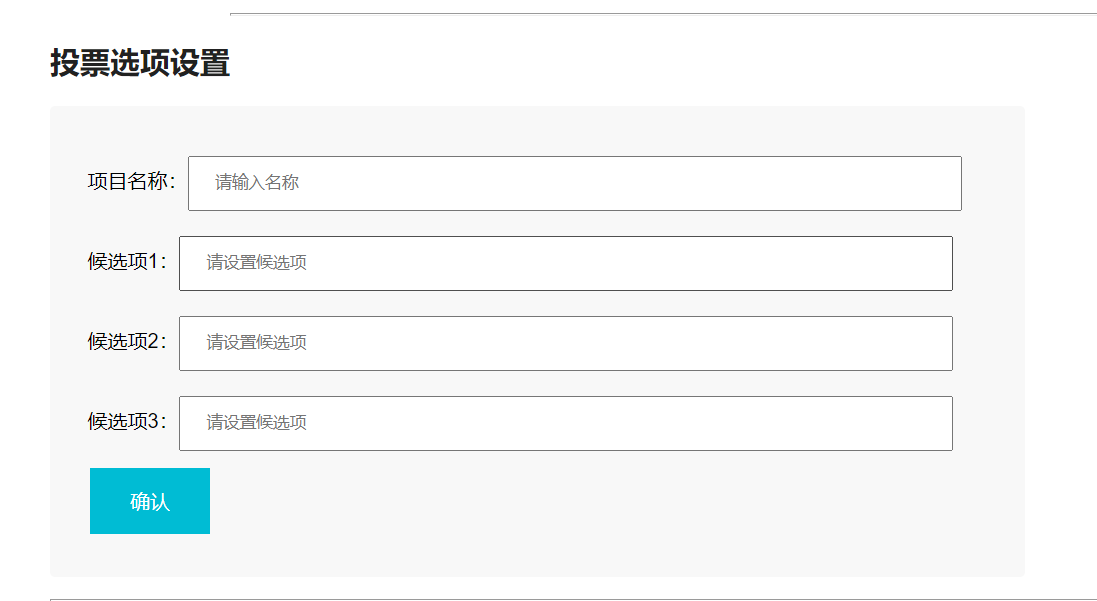
在线编译器：Remix

在线钱包：Metamask

1. 主页：主页设置的五个按钮（发起投票，账号注册，账号检测，参与投票，结果查询）可供用户跳转到不同的需求界面。



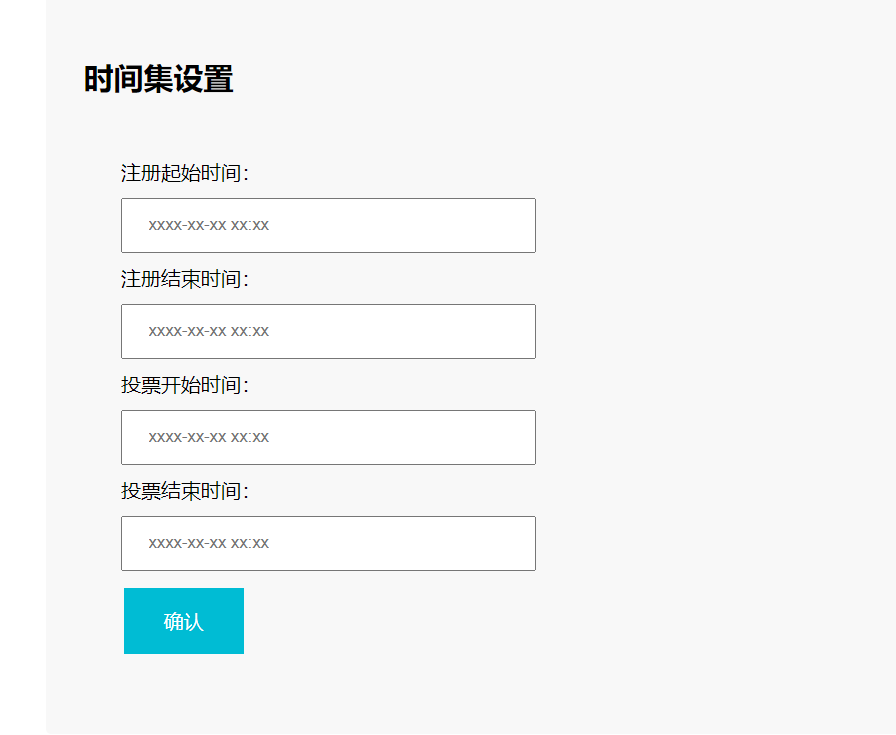
1. 发起投票：新建一个投票项目，在用户获取账号之后，设置投票的名称以及多个候选项名称：



然后，设置给投票参与者使用的注册码，注册码需要bytes32类型：

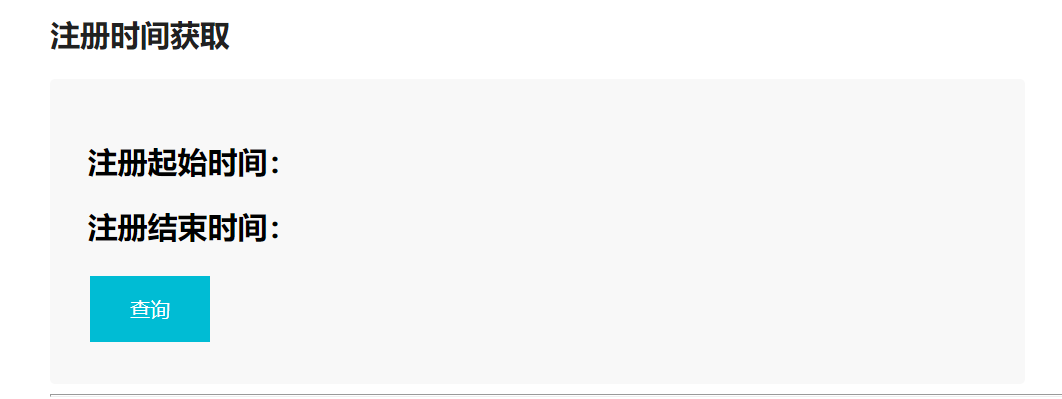


最后，进行时间集设置，设置你所需的投票起止时间以及注册起止时间：

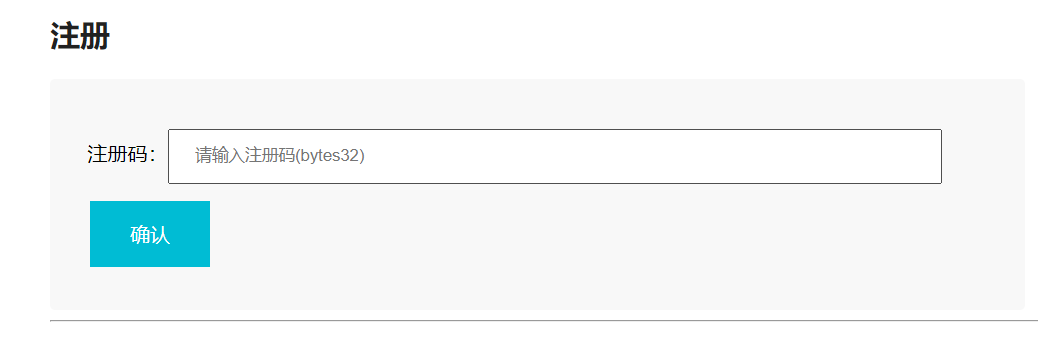


设置成功后完成新建项目，将注册码分发给参与者后，参与者即可在注册后，于投票规定时间内参与投票。

1. 账号注册：参与者在获得注册码后可在该界面进行注册，同样，在获取完账号后可通过该功能查看注册的起止时间：

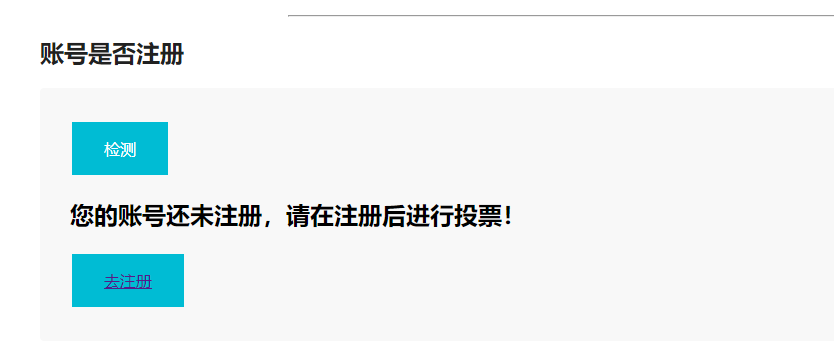


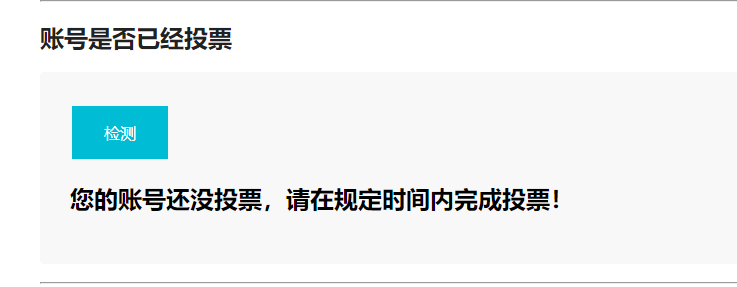
随后可在规定时间内使用正确的注册码进行注册，其中注册码必须是投票发起者设置的bytes32位注册码，其他的不符合规格或与设置者规定的注册码不相同的都无法通过注册：



1. 账号检测：成功完成注册的参与者可在该界面进行账户检测：

首先检测账号是否注册，如果还未注册，则会提示先注册后投票：

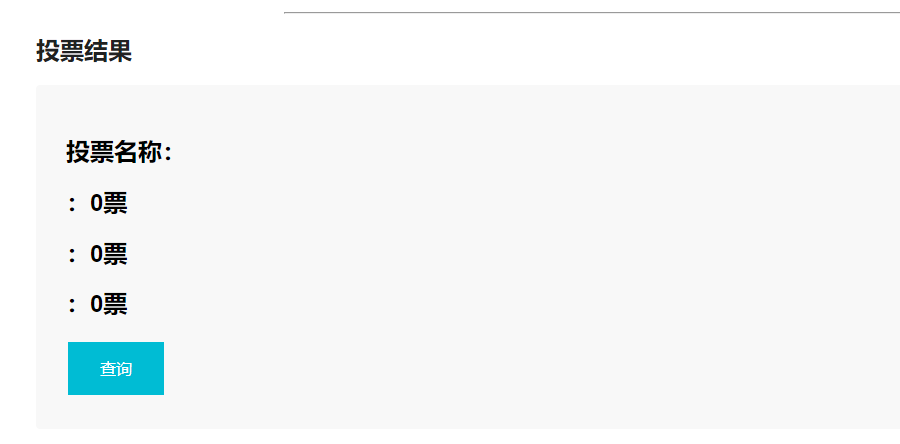


其次检测账号是否已经投过票，防止恶意刷票等行为的产生：

1. 参与投票：参与者的投票界面，先点击获取列表后，下方会出现三个投票按钮，分别对应三个候选项，点击并提交交易后完成投票：



1. 结果查询：无论是发起者或是参与者都可在该界面查看投票的最终结果，通过点击按钮，后台会自行调用合约统计票数，并读取候选项的名称，并把它们按固定格式打印出来：



1.4 总结

本文介绍了一种基于以太坊区块链的多候选人的电子投票方案，用特定业务逻辑的智能合约实现自我计票功能而取代了传统的第三方计票机构。同时，在投票方案的智能合约引入了两轮零知识证明，有效保护了投票者的隐私问题。从对投票方案的安全性分析中证明，投票方案是安全可靠的。另外，在本地的私有链节点上部署智能合约，模拟了多位投票者进行投票。从实验的数据中可知，投票系统在保护投票者隐私的前提下能做到公开可验证，可适用于小规模的董事会投票场景。