



(12)发明专利申请

(10)申请公布号 CN 110995444 A

(43)申请公布日 2020.04.10

(21)申请号 201911220807.5

(22)申请日 2019.12.03

(71)申请人 山东爱城市网信息技术有限公司
地址 250100 山东省济南市高新区浪潮路
1036号浪潮大厦S01楼3110室

(72)发明人 姜明润 庞松涛 商广勇 王伟兵
马岩堂 赵树林 姜鑫 陶鑫
刘伟巍

(74)专利代理机构 济南信达专利事务有限公司
37100
代理人 孙晶伟

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/08(2006.01)
G06Q 40/04(2012.01)

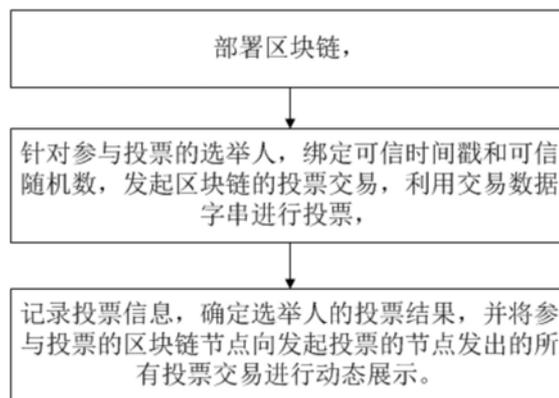
权利要求书1页 说明书3页 附图1页

(54)发明名称

一种基于区块链的选举的方法

(57)摘要

本发明公开一种基于区块链的选举的方法，涉及区块链应用技术领域；部署区块链，针对参与投票的选举人，绑定可信时间戳和可信随机数，发起区块链的投票交易，利用交易数据字串进行投票，所述交易数据字串包括被投票人、可信时间戳及可信随机数，记录投票信息，确定选举人的投票结果，并将参与投票的区块链节点向发起投票的节点发出的所有投票交易进行动态展示；本发明利用区块链对公共或者对联盟内部全部公开透明的机制，使得选举过程结果对公众全部透明，并且数据不可被任意篡改，确保了选举的公平公正。



1. 一种基于区块链的选举的方法,其特征是部署区块链,
针对参与投票的选举人,绑定可信时间戳和可信随机数,发起区块链的投票交易,利用交易数据字串进行投票,所述交易数据字串包括被投票人、可信时间戳及可信随机数,
记录投票信息,确定选举人的投票结果,并将参与投票的区块链节点向发起投票的节点发出的所有投票交易进行动态展示。
2. 根据权利要求1所述的方法,其特征是在集团内部署联盟链,或者在地域内部署联盟链或者公共链,并将针对选举人信息按照相应区块链节点分别纳入区块链。
3. 根据权利要求1或2所述的方法,其特征是通过在发起区块链的投票交易时生成时间戳,并将时间戳记录到区块链获得可信时间戳。
4. 根据权利要求3所述的方法,其特征是通过在发起区块链的投票交易时生成随机数,并将随机数记录到区块链获得可信随机数。
5. 一种基于区块链的选举工具,其特征是包括部署模块、选举发起模块、记录模块及展示模块,
部署模块部署区块链,
选举发起模块针对参与投票的选举人,绑定可信时间戳和可信随机数,发起区块链的投票交易,利用交易数据字串进行投票,所述交易数据字串包括被投票人、可信时间戳及可信随机数,
记录模块记录投票信息,确定选举人的投票结果,展示模块将参与投票的区块链节点向发起投票的节点发出的所有投票交易进行动态展示。
6. 根据权利要求5所述的选举工具,其特征是部署模块在集团内部署联盟链,或者在地域内部署联盟链或者公共链,并将针对选举人信息按照相应区块链节点分别纳入区块链。
7. 根据权利要求5或6所述的选举工具,其特征是选举发起模块通过在发起区块链的投票交易时生成时间戳,并将时间戳记录到区块链获得可信时间戳。
8. 根据权利要求7所述的选举工具,其特征是选举发起模块通过在发起区块链的投票交易时生成随机数,并将随机数记录到区块链获得可信随机数。

一种基于区块链的选举的方法

技术领域

[0001] 本发明公开一种选举的方法,涉及区块链应用技术领域,具体来说是一种基于区块链的选举的方法。

背景技术

[0002] 区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。区块链(Blockchain),是比特币的一个重要概念,本质上是一个去中心化的数据库,同时作为比特币的底层技术,是一串使用密码学方法相关联产生的数据块,每一个数据块中包含了一批比特币网络交易的信息,用于验证其信息的有效性(防伪)和生成下一个区块。目前区块链网络类型按照数据开放程度划分,分为公有链、联盟链和私有链,公有链对所有人或组织开放,任何人或组织均可加入到公有链中;联盟链属于半开放模式,具有准入机制,有指定的共识节点,由特定的多个社会群体(银行、企业、政府机构等)参与的一种区块链网络;私有链,则是指网络中所有节点均由一个社会群体掌握的区块链网络。不同的区块链可进行虚拟货币、审计治理等多方面的应用。

[0003] 目前实体选举存在问题:一,虽然为民主选举,但是选举结果的统计过程不受大众监督,选举结果容易被恶意篡改;二,投票人隐私无法全面保护,哪个投票选举人投了那张票,可通过电子投票器等电子投票设备溯源找到,投票选举人隐私无法保护,使投票人投票存在风险,不能公平公正合理的投票;三,电子投票器比普通的省时省力,但是因前述等原因更加不受人信任,而普通的纸质投票,过程漫长也存在过程不可见等暗箱操作问题。

发明内容

[0004] 本发明针对现有技术的问题,提供一种基于区块链的选举的方法,搭建的区块链网络为基础平台,为用户提供一种完全透明的选举方法,实现公平公正的选择,并能够保护选举人隐私,且实施方便快捷,应用前景广阔。

[0005] 本发明提出的具体方案是:

[0006] 一种基于区块链的选举的方法:部署区块链,

[0007] 针对参与投票的选举人,绑定可信时间戳和可信随机数,发起区块链的投票交易,利用交易数据字串进行投票,所述交易数据字串包括被投票人、可信时间戳及可信随机数,

[0008] 记录投票信息,确定选举人的投票结果,并将参与投票的区块链节点向发起投票的节点发出的所有投票交易进行动态展示。

[0009] 所述的方法在集团内部署联盟链,或者在地域内部部署联盟链或者公共链,并将针对选举人信息按照相应区块链节点分别纳入区块链。

[0010] 所述的方法通过在发起区块链的投票交易时生成时间戳,并将时间戳记录到区块链获得可信时间戳。

[0011] 所述的方法通过在发起区块链的投票交易时生成随机数,并将随机数记录到区块链获得可信随机数。

[0012] 一种基于区块链的选举工具,包括部署模块、选举发起模块、记录模块及展示模块,

[0013] 部署模块部署区块链,

[0014] 选举发起模块针对参与投票的选举人,绑定可信时间戳和可信随机数,发起区块链的投票交易,利用交易数据字串进行投票,所述交易数据字串包括被投票人、可信时间戳及可信随机数,

[0015] 记录模块记录投票信息,确定选举人的投票结果,展示模块将参与投票的区块链节点向发起投票的节点发出的所有投票交易进行动态展示。

[0016] 所述的选举工具中部署模块在集团内部署联盟链,或者在地域内部署联盟链或者公共链,并将针对选举人信息按照相应区块链节点分别纳入区块链。

[0017] 所述的选举工具中选举发起模块通过在发起区块链的投票交易时生成时间戳,并将时间戳记录到区块链获得可信时间戳。

[0018] 所述的选举工具中选举发起模块通过在发起区块链的投票交易时生成随机数,并将随机数记录到区块链获得可信随机数。

[0019] 本发明的有益之处是:

[0020] 本发明方法提供一种基于区块链的选举的方法,利用区块链对公共或者对联盟内部全部公开透明的机制,使得选举过程结果对公众全部透明,并且数据不可被任意篡改,确保了选举的公平公正;

[0021] 保护选举人隐私的同时,哪个选举人投了那张票,可通过电子投票器等电子投票设备溯源找到,不会丢失数据;

[0022] 并且方便快捷与普通的纸质投票,过程漫长也存在过程不可见相比,电子投票器比普通的省时省力,选举过程实时可见,节省了很多人力物力,也防止过程不可见等暗箱操作问题的出现。

附图说明

[0023] 图1是本发明方法流程示意图。

具体实施方式

[0024] 本发明提供一种基于区块链的选举的方法:部署区块链,

[0025] 针对参与投票的选举人,绑定可信时间戳和可信随机数,发起区块链的投票交易,利用交易数据字串进行投票,所述交易数据字串包括被投票人、可信时间戳及可信随机数,

[0026] 记录投票信息,确定选举人的投票结果,并将参与投票的区块链节点向发起投票的节点发出的所有投票交易进行动态展示。

[0027] 同时提供与上述方法相应的一种基于区块链的选举工具,包括部署模块、选举发起模块、记录模块及展示模块,

[0028] 部署模块部署区块链,

[0029] 选举发起模块针对参与投票的选举人,绑定可信时间戳和可信随机数,发起区块链的投票交易,利用交易数据字串进行投票,所述交易数据字串包括被投票人、可信时间戳及可信随机数,

[0030] 记录模块记录投票信息,确定选举人的投票结果,展示模块将参与投票的区块链节点向发起投票的节点发出的所有投票交易进行动态展示。

[0031] 下面结合附图和具体实施例对本发明作进一步说明,以使本领域的技术人员可以更好地理解本发明并能予以实施,但所举实施例不作为对本发明的限定。

[0032] 利用本发明方法基于区块链进行选举投票,具体过程为:

[0033] 部署区块链,在集团内部可以部署联盟链,在地域内部可部署联盟链或者公共链,可以直接调用的api接口或者下载sdk,获取区块链服务,并将针对选举人信息按照相应区块链节点分别纳入区块链,使集团内或地域内参与投票的人全部参加进区块链服务中,保证去中心化的真实可靠,选举时可遵守少数服从多数的智能合约;

[0034] 针对参与投票的选举人,绑定可信时间戳和可信随机数,发起区块链的投票交易,利用交易数据字串进行投票,其中交易数据字串包括被投票人、可信时间戳及可信随机数,可信时间戳可通过在发起区块链的投票交易时生成时间戳,并将时间戳记录到区块链获得,可信随机数通过在发起区块链的投票交易时生成随机数,并将随机数记录到区块链获得,

[0035] 记录投票信息,确定选举人的投票结果,比如记录投票是此次投票的第几张选票,确定选举人的选票,真实有效的起到了选举的作用,保证选举真实可靠,无法被暗地修改;

[0036] 并将参与投票的区块链节点向发起投票的节点发出的所有投票交易进行动态展示,即在选举过程中多个节点对外同时实时展示选举数据,展示数据在任意发起投票交易方都可以核对其对错,使选举过程透明公开。

[0037] 利用本发明工具基于区块链进行选举投票,具体过程为:

[0038] 部署模块部署区块链,在集团内部可以部署联盟链,在地域内部可部署联盟链或者公共链,可以直接调用的api接口或者下载sdk,获取区块链服务,并将针对选举人信息按照相应区块链节点分别纳入区块链,使集团内或地域内参与投票的人全部参加进区块链服务中,保证去中心化的真实可靠,选举时可遵守少数服从多数的智能合约;

[0039] 选举发起模块针对参与投票的选举人,绑定可信时间戳和可信随机数,发起区块链的投票交易,利用交易数据字串进行投票,其中交易数据字串包括被投票人、可信时间戳及可信随机数,可信时间戳可通过在发起区块链的投票交易时生成时间戳,并将时间戳记录到区块链获得,可信随机数通过在发起区块链的投票交易时生成随机数,并将随机数记录到区块链获得,

[0040] 记录模块记录投票信息,确定选举人的投票结果,比如记录投票是此次投票的第几张选票,确定选举人的选票,真实有效的起到了选举的作用,保证选举真实可靠,无法被暗地修改;

[0041] 展示模块将参与投票的区块链节点向发起投票的节点发出的所有投票交易进行动态展示,即在选举过程中多个节点对外同时实时展示选举数据,展示数据在任意发起投票交易方都可以核对其对错,使选举过程透明公开。

[0042] 以上所述实施例仅是为充分说明本发明而所举的较佳的实施例,本发明的保护范围不限于此。本技术领域的技术人员在本发明基础上所作的等同替代或变换,均在本发明的保护范围之内。本发明的保护范围以权利要求书为准。

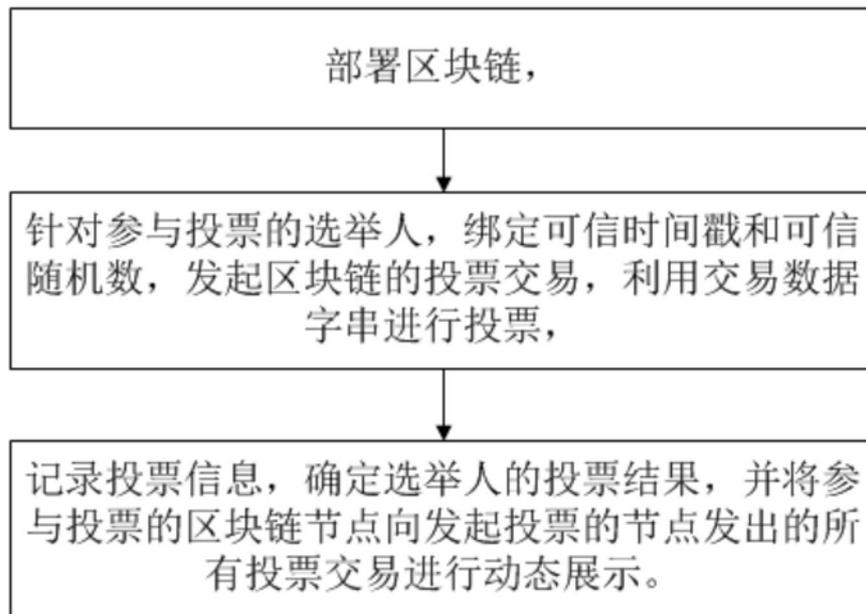


图1