(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112508564 B
(45)授权公告日 2024.04.16

(21)申请号 202011391144.6
(22)申请日 2020.12.01
(65)同一申请的已公布的文献号
申请公布号 CN 112508564 A
(43)申请公布日 2021.03.16
(73)专利权人 浙商银行股份有限公司
地址 311200 浙江省杭州市萧山区鸿宁路1788号
(72)发明人 臧铖 陈嘉俊 张少鹏
(74)专利代理机构 杭州求是专利事务所有限公司 33200
专利代理师 刘静
(51)Int.Cl.
G06Q 20/38(2012.01)
G06F 21/32(2013.01)

(56)对比文件
CN 111355592 A,2020.06.30
CN 111460420 A,2020.07.28
CN 111898991 A,2020.11.06
JP 2003162633 A,2003.06.06
WO 2019160167 A1,2019.08.22

审查员 郭艳芳

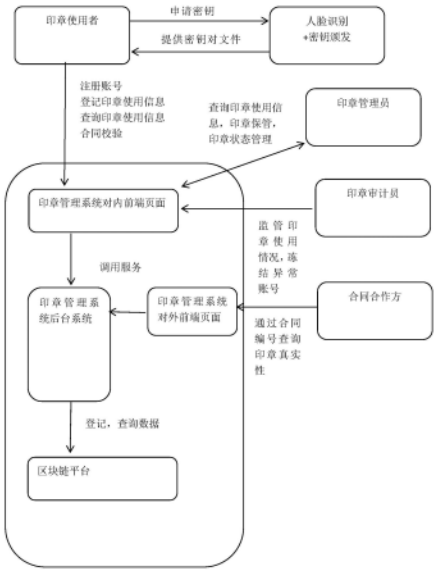
权利要求书2页 说明书4页 附图1页

(54)发明名称

基于区块链的印章使用管理方法、电子设备及存储介质

(57)摘要

本发明公开了一种基于区块链的印章使用管理方法、电子设备及存储介质。印章使用者通过人脸识别获取密钥对,通过密钥对在印章管理系统注册账号。系统将使用者的信息登记到区块链上,并在使用者每次登入系统时将登入信息登记到区块链上。印章使用者将使用时间,印章用途,合同编号等信息录入系统,系统验证通过后将该印章在该时间段内状态设置为使用中。当印章超出使用时间进行预警,并通知管理员。印章审计员可以查看印章使用情况,排查是否有异常情况。合同合作方也可以查询印章的真实性,避免萝卜章以及阴阳合同的情况出现。本发明方法使印章的使用更加透明,可追溯。方便印章的管理,规范印章的使用,确保印章真实性,保障合同签署双方的权益。



CN 112508564 B

1.一种基于区块链的印章使用管理方法,其特征在于,包括以下步骤:

(1)印章使用者向印章管理系统申请密钥对;印章管理系统对使用者进行人脸识别,通过采集使用者的人脸信息同员工信息表中的照片进行对比,完成人脸验证后系统自动生成密钥对文件;印章使用者将密钥对文件下载并保存在某物理介质中;

(2)印章使用者使用密钥对在印章管理系统注册账号,印章使用者将详细身份信息录入印章管理系统,系统将印章使用者录入身份信息同系统中的员工信息进行比对,根据印章使用者的员工等级匹配对应的印章使用权限;注册完成后,系统将印章使用者的详细身份信息通过公钥加密后登记到区块链平台;

(3)印章使用者使用注册账号登入印章管理系统,系统根据账号查询区块链中的登入者身份加密数据,并通过登入者的私钥对加密数据进行解密,解密成功则代表身份验证通过;系统将使用者的登入、登出信息登记到区块链平台;

(4)印章使用者申请印章使用,首先通过合同编号验证合同的真实性,然后验证合同的有效性,验证通过后,印章使用者将印章使用开始时间,归还时间,印章用途,合同中的重点要素信息登记到区块链平台,登记成功后区块链平台在该印章使用者下生成一条区块链登记结果的交易哈希值;

(5)印章管理员通过登记结果的交易哈希值查询印章使用的详细信息;审核通过后,印章使用者获取及使用印章,并将使用者申请使用时段的印章状态修改为使用中;当印章使用者完成印章的使用,并归还给印章管理员,印章管理员将印章在该时段时间状态修改为已按时归还;若超出使用时间未归还印章,系统将自动提醒管理员有印章使用已超出借用时间,并将对应的合同编号标记为有异常;后续管理员根据实际情况撤销异常,恢复合同的有效性;

(6)印章审计员负责审计印章使用规范,印章审计员通过印章管理系统,查看印章使用情况,排查异常情况,审核是否有违规使用的情况;若发现有违规使用印章情况,印章监管员有权冻结该账号的使用,并将对应未完成的合同编号标记为有异常,对已完成的合同进行审计有效性和真实性;

(7)合同合作方通过合同编号在印章管理系统对外开放界面查询印章使用情况,查询印章真实性和合同的有效性,防止萝卜章以及阴阳合同的出现。

2.根据权利要求1所述的基于区块链的印章使用管理方法,其特征在于,所述的步骤(1)中,密钥对是满足非对称加密技术的公私钥,私钥由使用者持有用于解密公钥加密数据,公钥则公布给他人用于数据加密。

3.根据权利要求1所述的基于区块链的印章使用管理方法,其特征在于,所述的步骤(1)中,密钥对文件需要使用者自己保管,且密钥丢失后无法找回。

4.根据权利要求1所述的基于区块链的印章使用管理方法,其特征在于,所述的步骤(2)中,印章使用者将身份详细信息登记到系统中,并用公钥对身份详细信息进行加密发送给区块链平台,区块链平台登记完成身份信息后,返回身份信息登记结果。

5.根据权利要求1所述的基于区块链的印章使用管理方法,其特征在于,所述的步骤(3)中,由于区块链数据采用非对称加密算法,只有持有正确的私钥才能获取使用者的详细信息;登入者除了需要通过账号的密码验证,还需要通过私钥获取其登记在区块链上的身份信息,才能通过登入验证。

6.根据权利要求1所述的基于区块链的印章使用管理方法,其特征在于,所述的步骤(4)中,企业的每一份合同都会在系统的合同管理页面进行备案,无备案的合同都属于虚假合同;当印章使用者申请印章使用的时候,需要先查询该合同是否已经备案;若无备案的合同,则申请无效。

7.根据权利要求1所述的基于区块链的印章使用管理方法,其特征在于,所述的步骤(6)中,印章审计员主要负责印章使用情况的审计,在系统中具有较大的权限,能够查询某个印章使用者所有印章使用记录,或查询某个时间段内印章使用情况;当发现某个使用者有异常时,冻结该账号的使用,冻结后的账号,无法再登入印章管理系统,并且标记可能出现异常的合同,进行进一步的审核。

8.一种电子设备,包括:处理器和用于存储处理器可执行指令的存储器;其中,所述处理器通过运行所述可执行指令以实现如权利要求1-7中任一项所述的基于区块链的印章使用管理方法。

9.一种计算机可读存储介质,其上存储有计算机指令,该指令被处理器执行时实现如权利要求1-7中任一项所述基于区块链的印章使用管理方法的步骤。

基于区块链的印章使用管理方法、电子设备及存储介质

技术领域

[0001] 本发明涉及区块链技术领域,具体涉及一种基于区块链的印章使用管理方法、电子设备及存储介质。

背景技术

[0002] 区块链技术是一个去中心化的账本,没有任何一机构或者个人可以实现对全局数据的控制。区块链技术中的共识算法也保证了登记到区块链上的数据具有不可篡改性。区块链上的数据都是公开透明的,可以追溯到任何一笔历史交易。目前很多企业存在印章的管理缺乏规范,使用混乱,并且难以追溯印章的使用情况,给公司带来风险和不良影响。萝卜章的出现更是会造成公司巨大的经济损失。

发明内容

[0003] 针对印章管理的难题,加强印章使用的监管,本发明提出了一种基于区块链的印章使用管理方法、电子设备及存储介质,以解决目前多数企业存在的印张管理和使用的乱象,使印张管理和使用具有规范化,并实现印章使用事后审查,追责。

[0004] 本发明的目的是通过以下技术方案实现的:

[0005] 根据本发明的第一方面,提供一种基于区块链的印章使用管理方法,该方法包括以下步骤:

[0006] (1)印章使用者首先需要向印章管理系统申请密钥对。印章管理系统对使用者进行人脸识别,通过采集使用者的人脸信息同员工信息表中的照片进行对比,完成人脸验证后系统自动生成密钥对文件。印章使用者将密钥对文件下载并保存在某物理介质中。

[0007] (2)印章使用者使用密钥对在印章管理系统注册账号,印章使用者将详细身份信息录入印章管理系统,系统将印章使用者录入身份信息同系统中的员工信息进行比对,根据印章使用者的员工等级匹配对应的印章使用权限。注册完成后,系统将印章使用者的详细身份信息通过公钥加密后登记到区块链平台。

[0008] (3)印章使用者使用注册账号登入印章管理系统,系统根据账号查询区块链中的登入者身份加密数据,并通过登入者的私钥对加密数据进行解密,解密成功则代表身份验证通过。并且系统会自动将使用者的登入、登出信息例如登入时间,登出时间等信息登记到区块链平台。

[0009] (4)印章使用者申请印章使用,首先通过合同编号验证合同的真实性,然后验证合同的有效性,在完成验证后,印章使用者将印章使用开始时间,归还时间,印章用途,合同中的重点要素等信息登记到区块链平台,登记成功后区块链平台会在该使用者用户下生成一条区块链登记结果的交易哈希值。

[0010] (5)印章管理员通过登记结果的交易哈希值查询印章使用的详细信息。审核通过后,印章使用者可以获取及使用印章,并将使用者申请使用时段的印章状态修改为使用中。当印章使用者完成印章的使用,并归还给印章管理员,印章管理员将印章在该时段时间状

态修改为已按时归还。若超出使用时间未归还印章,系统将自动提醒管理员有印章使用已超出借用时间,并将对应的合同编号标记为有异常(即为无效状态)。后续通过管理员根据具体实际情况,可撤销异常,恢复合同的有效性。

[0011] (6)印章审计员负责审计印章使用规范,印章审计员通过印章管理系统,查看印章使用情况,排查异常情况,审核是否有违规使用的情况。若发现有违规使用印章情况,印章监管员有权冻结该账号的使用,并将对应未完成的合同编号标记为有异常,对已完成的合同进行审计有效性和真实性。

[0012] (7)合同合作方可以通过合同编号在印章管理系统对外开放界面查询印章使用的情况,查询印章真实性和合同的有效性,防止萝卜章以及阴阳合同的出现。

[0013] 进一步地,所述的步骤(1)中,密钥对是满足非对称加密技术的公私钥,私钥由使用者持有用于解密公钥加密数据,公钥则可以公布给他人用于数据加密。

[0014] 进一步地,所述的步骤(1)中,密钥对文件需要使用者自己保管,且密钥丢失后无法找回,所以可以将密钥对文件保存在私人的物理介质上。

[0015] 进一步地,所述的步骤(2)中,印章使用者将身份详细信息登记到系统中,并用公钥对身份详细信息进行加密发送给区块链平台,区块链平台登记完成身份信息后,返回一个身份信息登记结果。

[0016] 进一步地,所述的步骤(3)中,由于区块链数据采用非对称加密算法,只有持有正确的私钥才能获取使用者详细信息。登入者除了需要通过账号的密码验证,还需要通过私钥获取其登记在区块链上的身份信息,才能通过登入验证。

[0017] 进一步地,所述的步骤(4)中,企业的每一份合同都会在系统的合同管理页面进行备案,无备案的合同都属于虚假合同。当印章使用者申请印章使用的时候,需要先查询该合同是否已经备案。若无备案的合同,则申请无效。

[0018] 进一步地,所述的步骤(6)中,印章审计员主要负责印章使用情况的审计,在系统中具有较大的权限,可以查询某个印章使用者所有印章使用记录,也可以查询某个时间段内印章使用情况。当发现某个使用者有异常时,可以冻结该账号的使用,冻结后的账号,无法再登入印章管理系统,并且标记可能出现异常的合同,进行进一步的审核。

[0019] 根据本发明的第二方面,提供一种电子设备,包括:处理器和用于存储处理器可执行指令的存储器;其中,所述处理器通过运行所述可执行指令以实现上述的基于区块链的印章使用管理方法。

[0020] 根据本发明的第三方面,提供一种计算机可读存储介质,其上存储有计算机指令,该指令被处理器执行时实现上述基于区块链的印章使用管理方法的步骤。

[0021] 本发明的有益效果是:本发明方法使印章的使用更加透明,可追溯。方便印章的管理,规范印章的使用,确保印章真实性,保障合同签署双方的权益。

附图说明

[0022] 图1为本发明实施例提供的基于区块链的印章使用管理方法的流程图。

具体实施方式

[0023] 为了更好的理解本申请的技术方案,下面结合附图对本申请实施例进行详细描

述。

[0024] 应当明确,所描述的实施例仅仅是本申请一部分实施例,而不是全部的实施例。基于本申请中的实施例,本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其它实施例,都属于本申请保护的范围。

[0025] 在本申请实施例中使用的术语是仅仅出于描述特定实施例的目的,而非旨在限制本申请。在本申请实施例和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式,除非上下文清楚地表示其他含义。

[0026] 图1为本发明一个实施例中的基于区块链的印章使用管理方法流程图,该方法包括如下步骤:

[0027] (1)印章使用者首先需要向印章管理系统申请密钥对。印章管理系统对接人脸识别系统会对使用者进行人脸识别,通过采集使用者的人脸信息同员工信息表中的照片进行对比,完成人脸验证后系统自动生成密钥对文件。印章使用者将密钥对文件下载并保存在某物理介质中。

[0028] 在一个实施例中,密钥对是满足非对称加密技术的公私钥,私钥由使用者持有用于解密公钥加密数据,公钥则可以公布给他人用于数据加密。密钥对文件需要使用者自己保管,且密钥丢失后无法找回,所以可以将密钥对文件保存在私人的物理介质上,例如私人u盘。

[0029] (2)印章使用者使用密钥对在印章管理系统注册账号,印章使用者将详细身份信息录入印章管理系统,系统将印章使用者录入身份信息同系统中的员工信息进行比对,根据印章使用者的员工等级匹配对应的印章使用权限。注册完成后,系统将印章使用者的详细身份信息通过公钥加密后登记到区块链平台,区块链平台登记完成身份信息后,返回一个身份信息登记结果,例如返回状态码000000表示身份登记成功。

[0030] (3)印章使用者使用注册账号登入印章管理系统,系统根据账号查询区块链中的登入者身份加密数据,并通过登入者的私钥对加密数据进行解密,解密成功则代表身份验证通过。并且系统会自动将使用者的登入、登出信息例如登入时间,登出时间等信息登记到区块链平台。

[0031] 在一个实施例中,由于区块链数据采用非对称加密算法,只有持有正确的私钥才能获取使用者的详细信息。登入者除了需要通过账号的密码验证,还需要通过私钥获取其登记在区块链上的身份信息,才能通过登入验证。

[0032] (4)印章使用者申请印章使用,首先通过合同编号在合同备案系统中验证合同编号的真实性。然后验证合同的有效性,在完成合同有效性验证后,印章使用者将印章使用开始时间,归还时间,印章用途,合同中的重点要素等信息登记到区块链平台,登记成功后区块链平台会在该使用者用户下生成一条区块链登记结果的交易哈希值。

[0033] 在一个实施例中,企业的每一份合同都会在系统的合同管理页面进行备案,无备案的合同都属于虚假合同。当印章使用者申请印章使用的时候,需要先查询该合同是否已经备案。若无备案的合同,则申请无效。

[0034] (5)印章管理员通过登记结果的交易哈希值查询印章使用的详细信息。审核通过后,印章使用者可以获取及使用印章,并将使用者申请使用时段的印章状态修改为使用中。当印章使用者完成印章的使用,并归还给印章管理员,印章管理员将印章在该时段时间状

态修改为已按时归还。若超出使用时间未归还印章,系统将自动提醒管理员有印章使用已超出借用时间,并将对应的合同编号标记为有异常(即为无效状态)。后续通过管理员根据具体实际情况,可撤销异常,恢复合同的有效性。

[0035] (6)印章审计员负责审计印章使用规范,在系统中具有较大的权限,印章审计员通过印章管理系统,查看印章使用情况,排查异常情况,审核是否有违规使用的情况。若发现有违规使用印章情况,印章监管员有权冻结该账号的使用,冻结后的账号无法再登入印章管理系统,并将对应未完成的合同编号标记为有异常,对已完成的合同进行审计有效性和真实性,进行进一步的审核。

[0036] (7)合同合作方可以通过合同编号在印章管理系统对外开放界面查询印章使用的情况,查询印章真实性和合同的有效性,防止萝卜章以及阴阳合同的出现。

[0037] 在一个实施例中,提出了一种电子设备,包括存储器和处理器,存储器中存储有计算机可读指令,计算机可读指令被处理器执行时,使得处理器执行上述各实施例中基于区块链的印章使用管理方法中的步骤。

[0038] 在一个实施例中,提出了一种存储有计算机可读指令的存储介质,计算机可读指令被一个或多个处理器执行时,使得一个或多个处理器执行上述各实施例中基于区块链的印章使用管理方法中的步骤。其中,存储介质可以为非易失性存储介质。

[0039] 本领域普通技术人员可以理解上述实施例的各种方法中的全部或部分步骤是可以通过程序来指令相关的硬件来完成,该程序可以存储于一计算机可读存储介质中,存储介质可以包括:只读存储器(ROM,Read Only Memory)、随机存取存储器(RAM,Random Access Memory)、磁盘或光盘等。

[0040] 以上所述仅为本说明书一个或多个实施例的较佳实施例而已,并不用以限制本说明书一个或多个实施例,凡在本说明书一个或多个实施例的精神和原则之内,所做的任何修改、等同替换、改进等,均应包含在本说明书一个或多个实施例保护的范围之内。

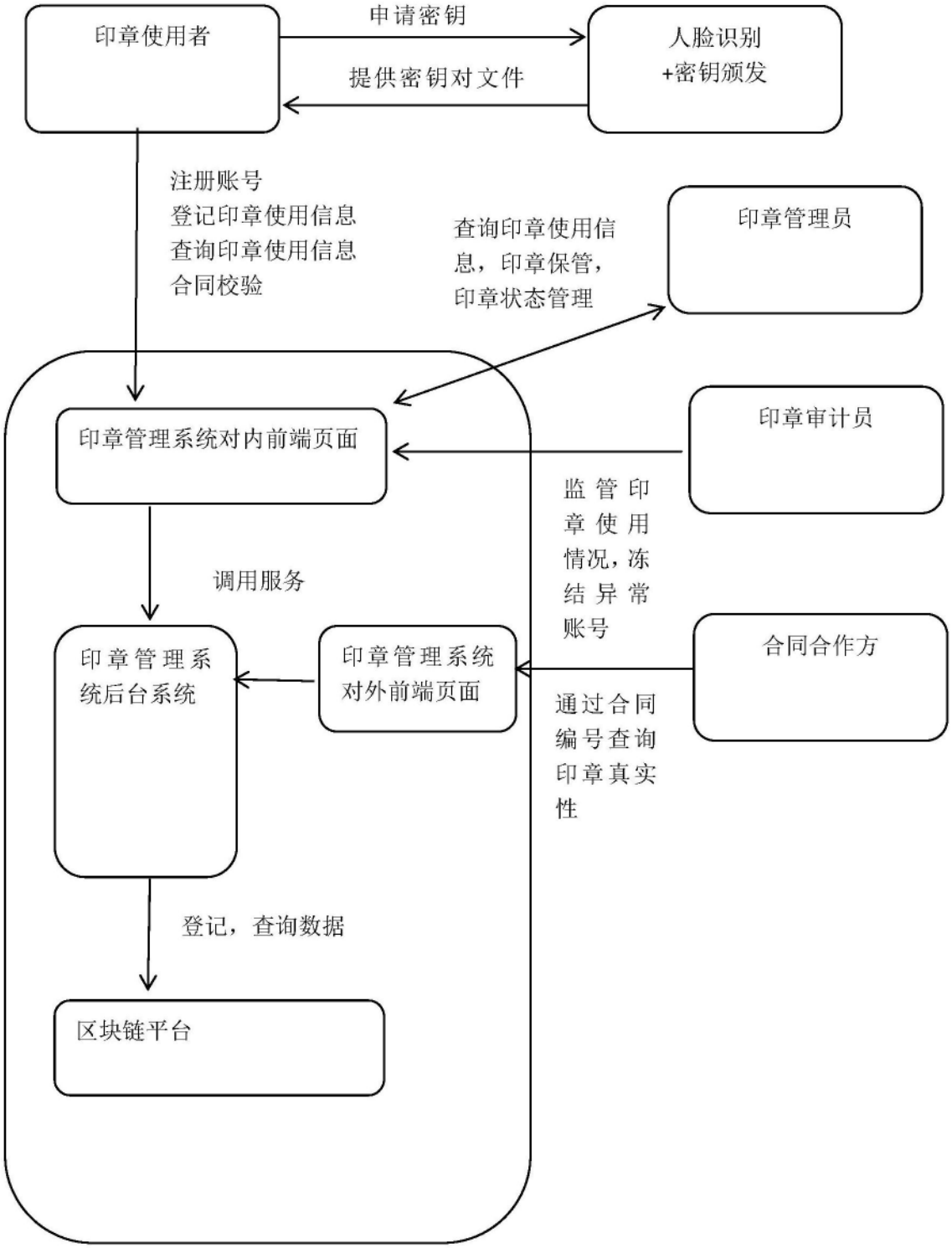

印章使用者
申请密钥
提供密钥对文件
人脸识别
+密钥颁发
注册账号
登记印章使用信息
查询印章使用信息
合同校验
查询印章使用信息，印章保管，印章状态管理
印章管理员
印章管理系统对内前端页面
印章审计员
监管印章使用情况，冻结异常账号
调用服务
印章管理系统后台系统
印章管理系统对外前端页面
合同合作方
通过合同编号查询印章真实性
登记，查询数据
区块链平台

图1