

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2020 年 7 月 23 日 (23.07.2020)



(10) 国际公布号
WO 2020/147292 A1

(51) 国际专利分类号:
G07C 9/00 (2006.01) **G07C 1/10** (2006.01)

(21) 国际申请号: PCT/CN2019/097634

(22) 国际申请日: 2019 年 7 月 25 日 (25.07.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910044493.1 2019 年 1 月 17 日 (17.01.2019) CN

(71) 申请人: 平安科技(深圳)有限公司(PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) [CN/CN];
中国广东省深圳市福田区福田街道福安社区益田路 5033 号平安金融中心 23 楼, Guangdong 518000 (CN)。

(72) 发明人: 吴超勇(WU, Chaoyong); 中国广东省深圳市福田区福田街道福安社区益田路 5033 号平安金融中心 23 楼, Guangdong 518000 (CN)。

(74) 代理人: 北京中强智尚知识产权代理有限公司 (BEIJING STRONG WISDOM INTELLECTUAL PROPERTY AGENCY LTD.); 中国北京市朝阳区北苑东路 19 号院 3 号楼 2501 室, Beijing 100012 (CN)。

(81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK,

LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国(除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

根据细则 4.17 的声明:

- 关于申请人有权申请并被授予专利(细则 4.17(ii))
- 发明人资格(细则 4.17(iv))

本国际公布:

- 包括国际检索报告(条约第 21 条(3))。
- s1

(54) **Title:** BLOCKCHAIN-BASED ACCESS CONTROL METHOD AND SYSTEM, MANAGEMENT TERMINAL AND ACCESS CONTROL TERMINAL

(54) 发明名称: 基于区块链的门禁访问方法、系统、管理终端和门禁终端

(57) **Abstract:** A blockchain-based access control method and system, a management terminal and an access control terminal. The method applied to the management terminal comprises: receiving an identity correspondence between externally inputted identity information of at least one legitimate user and an access control identification of at least one external access control terminal (101); generating an access control smart contract carrying the identity correspondence (102); determining a corresponding blockchain node in a blockchain system and storing the access control smart contract in the blockchain node (103); separately synchronizing the access control smart contract into blockchain nodes respectively corresponding to other management terminals in the blockchain system (104); and sending the access control smart contract to the at least one external access control terminal (105). Thus, the management difficulty of the access control terminal may be reduced.

(57) 摘要: 一种基于区块链的门禁访问方法、系统、管理终端和门禁终端, 应用于管理终端的方法包括: 接收外部输入的至少一个合法用户的身份信息, 与至少一个外部的门禁终端的门禁标识的身份对应关系(101); 生成携带身份对应关系的门禁智能合约(102); 确定区块链系统中对应的区块链节点, 并将门禁智能合约存储到该区块链节点中(103); 将门禁智能合约分别同步到区块链系统中其他管理终端分别对应的区块链节点中(104); 将门禁智能合约发送给至少一个外部的门禁终端(105)。由此, 能够降低门禁终端的管理难度。

WO 2020/147292 A1

基于区块链的门禁访问方法、系统、管理终端和门禁终端

本申请要求与 2019 年 1 月 17 日提交中国专利局、申请号为 201910044493.1、申请名称为“基于区块链的门禁访问方法、系统、管理终端和门禁终端”的中国专利申请的优先权，其全部内容通过引用结合在申请中。

5

技术领域

本申请涉及门禁管理领域，特别是涉及基于区块链的门禁访问方法、系统、管理终端和门禁终端。

背景技术

门禁系统是一种管理人员进出的数字化管理系统。它可以树立公司、大厦或机关办公场所规范化管理形象，提高管理档次，同时规范化内部的管理体制。

10

目前，对于多职场的门禁访问系统，涉及的人员较多，不同人员对于不同职场的门禁终端的权限不同。但是，发明人发现当有人员变更时（例如，新增职员、职员升职），管理人员需要逐一更改变更人员涉及的门禁终端的权限，从而增加了管理人员的管理门禁终端的难度，降低门禁终端的管理效率。

发明内容

本申请实施例提供了基于区块链的门禁访问方法、系统、管理终端和门禁终端，能够降低门禁终端的管理难度。

15

第一方面，本申请实施例提供了基于区块链的门禁访问方法，应用于管理终端，包括：接收外部输入的至少一个合法用户的身份信息，与至少一个外部的门禁终端的门禁标识的身份对应关系；生成携带所述身份对应关系的门禁智能合约；确定区块链系统中对应的区块链节点，并将所述门禁智能合约存储到该区块链节点中；将所述门禁智能合约分别同步到所述区块链系统中其他管理终端分别对应的区块链节点中；将所述门禁智能合约发送给至少一个外部的门禁终端。

20

优选地，在所述接收外部输入的至少一个合法用户的身份信息，与至少一个外部的门禁终端的门禁标识的身份对应关系之后，在所述生成携带所述身份对应关系的门禁智能合约之前，进一步包括：接收外部输入的至少一个所述门禁标识与至少一个访问时段的时段对应关系；所述生成携带所述身份对应关系的门禁智能合约，包括：生成携带所述身份对应关系和所述时段对应关系的门禁智能合约。优选地，在所述将所述门禁智能合约分别同步到所述区块链系统中其他管理终端分别对应的区块链节点中之后，在所述将所述门禁智能合约发送给至少一个外部的门禁终端之前，进一步包括：利用预设的密钥对所述门禁智能合约加密，获得加密后的所述门禁智能合约；则，所述将所述门禁智能合约发送给至少一个外部的门禁终端，

25

包括：将加密后的所述门禁智能合约发送给至少一个外部的门禁终端。优选地，在所述接收外部输入的至少一个合法用户的身份信息，与至少一个外部的门禁终端的门禁标识的身份对应关系之前，进一步包括：接收外部输入的当前验证信息；确定预先存储的至少一个预存验证信息中，是否存在与所述当前验证信息相同的同一验证信息；如果是，执行所述接收外部输入的至少一个合法用户的身份信息，与至少一个外部的门禁终端的门禁标识的身份对应关系；否则，输出无管理权限。优选地，在所述将所述门禁智能合约发送给至少一个外部的门禁终端之后，进一步包括：按照预设的反馈周期，向所述至少一个外部的门禁终端中的目标门禁终端发送反馈请求；接收所述目标门禁终端根据所述反馈请求返回的至少一个所述合法用户的出入记录；根据所述出入记录，生成每一个所述合法用户对应的考勤表，并输出所述考勤表。

第二方面，本申请实施例提供了基于区块链的门禁访问方法，应用于门禁终端，预先接收外部的管理终端发送的门禁智能合约，将当前门禁标识记录到所述门禁智能合约中，并存储记录后的所述门禁智能合约，包括：利用存储的所述门禁智能合约，执行：获取当前用户的身份信息；确定所述当前门禁标识对应的至少一个合法用户的身份信息中，是否存在与所述当前用户的身份信息相同的同一身份信息；如果是，开启控制的安全门；否则，输出无出入权限。优选地，在确定存在同一身份信息时，在所述开启控制的安全门之前，进一步包括：确定获取所述当前用户的身份信息的时间点；确定所述时间点是否在所述当前门禁标识对应的访问时段内；如果是，执行所述开启控制的安全门；否则，输出出入受限。优选地，在所述预先接收外部的管理终端发送的门禁智能合约之后，在所述将当前门禁标识记录到所述门禁智能合约之前，进一步包括：利用预设的密钥对所述门禁智能合约解密，获得解密后的所述门禁智能合约；则，所述将当前门禁标识记录到所述门禁智能合约中，包括：将当前门禁标识记录到解密后的所述门禁智能合约中。优选地，在所述开启控制的安全门之后，进一步包括：将所述当前用户作为合法用户，并存储所述合法用户的出入记录；在接收到所述管理终端发送的反馈请求时，将所述出入记录返回给发来所述反馈请求的所述门禁终端。

第三方面，本申请实施例提供了一种管理终端，包括：

终端接收单元，用于接收外部输入的至少一个合法用户的身份信息，与至少一个外部的门禁终端的门禁标识的身份对应关系；终端处理单元，用于生成携带所述终端接收单元接收的所述身份对应关系的门禁智能合约；确定区块链系统中对应的区块链节点，并将所述门禁智能合约存储到该区块链节点中；将所述门禁智能合约分别同步到所述区块链系统中其他管理终端分别对应的区块链节点中；终端发送单元，用于将所述终端处理单元生成的所述门禁智能合约发送给至少一个外部的门禁终端。

第四方面，本申请实施例提供了一种门禁终端，包括：门禁交互单元，用于预先接收外部的管理终端

发送的门禁智能合约；门禁管理单元，用于将当前门禁标识记录到所述门禁交互单元接收的所述门禁智能合约中，并存储记录后的所述门禁智能合约；门禁控制单元，用于利用所述门禁管理单元存储的所述门禁智能合约，执行：获取当前用户的身份信息；确定所述当前门禁标识对应的至少一个合法用户的身份信息中，是否存在与所述当前用户的身份信息相同的同一身份信息；如果是，开启控制的安全门；否则，输出无出入权限。

第五方面，本申请实施例提供了基于区块链的门禁访问系统，包括：至少两个第三方面所述的管理终端和至少一个第四方面所述的门禁终端。

第六方面，本申请实施例提供了一种计算机设备，包括非易失性可读存储介质和处理器，所述存储器中存储有计算机可读指令，所述计算机可读指令被所述处理器执行时，使得所述处理器执行如第一方面和第二方面中，所述基于区块链的门禁访问方法的步骤。

第七方面，本申请实施例提供了一种存储有计算机可读指令的非易失性可读存储介质，所述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如第一方面和第二方面中，所述基于区块链的门禁访问方法的步骤。

在本申请实施例提供了基于区块链的门禁访问方法，在应用于管理终端的方法中，外部（例如，管理人员）可以将变更后的至少一个合法用户的身份信息与至少一个外部门禁终端的身份对应关系，输入到管理终端中，这样管理终端根据外部输入的身份对应关系，即可生成管理终端对应的门禁智能合约。由于区块链具有不可篡改和可溯源的特性，因此将该门禁智能合约存储到自身对应的区块链节点中，并同步到其他管理终端分别对应的区块链节点中，以使各个区块链节点记录的数据相同，即共同维护同一数据库，这样外部通过任一管理终端仍可获知合法用户的身份信息与门禁终端的身份对应关系，便于外部管理门禁终端，还可以约束外部不能随意更改合法用户的身份信息与至少一个外部的门禁终端的身份对应关系，即避免外部随意更改合法用户出入各个门禁终端的权限，从而保证了区块链中数据的可信性；再将门禁智能合约发送给至少一个外部的门禁终端，可以使得接收到门禁智能合约的门禁终端共享同一个身份信息账本，这样当有人发生变更时，外部无需逐一更改变更人员所涉及的每一个门禁终端的权限，因此可以降低管理人员管理门禁终端的难度，提高门禁终端的管理效率，同时，还可以避免在特殊情况下门禁终端需要人工临时授权而造成人力资源的浪费，并且还可以消除因人工临时授权带来的安全隐患。

附图说明

图1为一个实施例中提供的基于区块链的门禁访问方法的流程图；

图2为另一个实施例中基于区块链的门禁访问方法的流程图；

图 3 为一个实施例中一种管理终端的结构示意图；

图 4 为一个实施例中一种门禁终端的结构示意图；

图 5 为一个实施例中基于区块链的门禁访问系统的结构示意图；

图 6 为另一个实施例中基于区块链的门禁访问系统的结构示意图。

5 具体实施方式

为了使本申请的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本申请进行进一步详细说明。应当理解，此处所描述的具体实施例仅用以解释本申请，并不用于限定本申请。如图 1 所示，本申请实施例提供了基于区块链的门禁访问方法，应用于管理终端，包括：步骤 101：接收外部输入的至少一个合法用户的身份信息，与至少一个外部的门禁终端的门禁标识的身份对应关系；步骤 102：生成携带所述身份对应关系的门禁智能合约；步骤 103：确定区块链系统中对应的区块链节点，并将所述门禁智能合约存储到该区块链节点中；步骤 104：将所述门禁智能合约分别同步到所述区块链系统中其他管理终端分别对应的区块链节点中；步骤 105：将所述门禁智能合约发送给至少一个外部的门禁终端。

在本申请实施例提供了基于区块链的门禁访问方法，在应用于管理终端的方法中，外部（例如，管理人员）可以将变更后的至少一个合法用户的身份信息与至少一个外部门禁终端的身份对应关系，输入到管理终端中，这样管理终端根据外部输入的身份对应关系，即可生成管理终端对应的门禁智能合约。由于区块链具有不可篡改和可溯源的特性，因此将该门禁智能合约存储到自身对应的区块链节点中，并同步到其他管理终端分别对应的区块链节点中，以使各个区块链节点记录的数据相同，即共同维护同一数据库，这样外部通过任一管理终端仍可获知合法用户的身份信息与门禁终端的身份对应关系，便于外部管理门禁终端，还可以约束外部不能随意更改合法用户的身份信息与至少一个外部的门禁终端的身份对应关系，即避免外部随意更改合法用户出入各个门禁终端的权限，从而保证了区块链中数据的可信性；再将门禁智能合约发送给至少一个外部的门禁终端，可以使得接收到门禁智能合约的门禁终端共享同一个身份信息账本，这样当有人员发生变更时，外部无需逐一更改变更人员所涉及的每一个门禁终端的权限，因此可以降低管理人员管理门禁终端的难度，提高门禁终端的管理效率，同时，还可以避免在特殊情况下门禁终端需要人工临时授权而造成人力资源的浪费，并且还可以消除因人工临时授权带来的安全隐患。需要说明的是，管理终端可以是智能手机、平板电脑、笔记本电脑、台式计算机等，但并不局限于此。在本申请一实施例中，在所述接收外部输入的至少一个合法用户的身份信息，与至少一个外部的门禁终端的门禁标识的身份对应关系之后，在所述生成携带所述身份对应关系的门禁智能合约之前，进一步包括：接收外部输入的至少一个所述门禁标识与至少一个访问时段的时段对应关系；所述生成携带所述身份对应关系的门禁智能合约，

包括：生成携带所述身份对应关系和所述时段对应关系的门禁智能合约。

在本申请实施例中，外部可以控制每一个外部的门禁终端对应的访问时段，以避免合法用随意出入某些重要的办公区域，这样管理终端在接收到外部输入的合法用户的身份信息与外部的门禁终端的时段对应关系后，即可生成携带身份对应关系和时段对应关系生成的门禁终端合约，以使外部的门禁终端按照该门
5 禁智能合约确定出入安全门的用户是否由出入权限。在本申请一实施例中，在所述将所述门禁智能合约分别同步到所述区块链系统中其他管理终端分别对应的区块链节点中之后，在所述将所述门禁智能合约发送给至少一个外部的门禁终端之前，进一步包括：利用预设的密钥对所述门禁智能合约加密，获得加密后的所述门禁智能合约；则，所述将所述门禁智能合约发送给至少一个外部的门禁终端，包括：将加密后的所述门禁智能合约发送给至少一个外部的门禁终端。在本申请实施例中，利用预设的密钥加密生成的门禁
10 智能合约获得加密后的门禁智能合约，即获得密文，再将密文发送给外部的门禁终端，可以避免非法用户窃取明文形式的门禁智能合约，导致合法用户的出入权限信息泄露，从而可以提高门禁智能合约传输过程中的安全性。

在本申请一实施例中，在所述接收外部输入的至少一个合法用户的身份信息，与至少一个外部的门禁终端的门禁标识的身份对应关系之前，进一步包括：接收外部输入的当前验证信息；确定预先存储的至少
15 一个预存验证信息中，是否存在与所述当前验证信息相同的同一验证信息；如果是，执行所述接收外部输入的至少一个合法用户的身份信息，与至少一个外部的门禁终端的门禁标识的身份对应关系；否则，输出无管理权限。在本申请实施例中，在接收到外部输入的当前验证信息时，需要利用预存验证信息对当前验证信息进行验证，以确订外部的身份是否合法，避免非法用户随意更改门禁终端的出入权限，提高门禁终端管理的安全性。当且仅当在确定外部的身份合法后，才允许外部设置外部的门禁终端的出入权限，即设
20 置至少一个合法用户的身份信息与至少一个外部的门禁终端的门禁标识的身份对应关系。

需要说明的是，当前验证信息可以包括：外部的用户名、身份证号、办公人员 ID 和密码中的任意一个或多个；在当前验信息包括用户名，预存验证信息包括用户名；在当前验信息包括身份证号，预存验证信息包括身份证号；在当前验信息包括办公人员 ID，预存验证信息包括办公人员 ID；在当前验信息包括密码中，预存验证信息包括密码。在本申请一实施例中，在所述将所述门禁智能合约发送给至少一个外部
25 的门禁终端之后，进一步包括：按照预设的反馈周期，向所述至少一个外部的门禁终端中的目标门禁终端发送反馈请求；接收所述目标门禁终端根据所述反馈请求返回的至少一个所述合法用户的出入记录；根据所述出入记录，生成每一个所述合法用户对应的考勤表，并输出所述考勤表。在本申请实施例中，为了方便外部统计合法用户的考勤情况，外部可以根据实际需求，在目标管理终端中设置反馈周期，管理终端即

可按照反馈中后期向外部的目标门禁终端发送反馈请求,以使目标门禁终端返回其记录的合法用户的出入记录,根据出入记录即可生成考勤表,并输出该考勤表,以便于外部根据输出的考勤表快速确定各个合法用户的考勤情况,节省外部统计合法用户考勤的时间。

如图2所示,本申请实施例提供了基于区块链的门禁访问方法,应用于门禁终端,包括:步骤201:

- 5 预先接收外部的管理终端发送的门禁智能合约,将当前门禁标识记录到所述门禁智能合约中,并存储记录后的所述门禁智能合约;步骤202:利用存储的所述门禁智能合约,执行:获取当前用户的身份信息;步骤203:确定所述当前门禁标识对应的至少一个合法用户的身份信息中,是否存在与所述当前用户的身份信息相同的同一身份信息;步骤204:如果是,开启控制的安全门;步骤205:否则,输出无出入权限。

在本申请实施例提供了基于区块链的门禁访问方法,在应用于门禁终端的方法中,在接收到外部的管
10 理终端发送的门禁智能合约时,需要将自身的当前门禁标识记录到该门禁智能合约中,以使在当前用户需要出入控制的安全门时,利用门禁智能合约根据记录的当前门禁标识和获取到的当前用户的身份信息,确定当前用户是否具有出入所控制的安全门的出入权限,避免非法用户随意出入办公职场,提高办公职场的安全性,当且仅当在确定当前用户具有出入权限时,开启控制的安全门,以便当前用户出入。需要说明的是,身份信息可以包括:用户的面部图像、虹膜、指纹、掌纹、声音以及门禁卡中的任意一个或多个,以
15 提供不同的身份认证方式供用户选择,提高用户的使用体验。在本申请一实施例中,在确定存在同一身份信息时,在所述开启控制的安全门之前,进一步包括:确定获取所述当前用户的身份信息的时间点;确定所述时间点是否在所述当前门禁标识对应的访问时段内;如果是,执行所述开启控制的安全门;否则,输出出入受限。在本申请实施例中,在利用门禁智能合约根据当前用户的身份信息,确定当前用户与控制的
20 安全门存在身份对应关系时,还需要确定用户出入该安全门的时间是否在对应的访问时段内,如果在访问时段内,则可以确定当前用户可以出入该安全门,如果不在访问时段内,则需要输出出入受限的提示信息,以使用户了解该时间点无法访问门禁终端管控的区域。在本申请一实施例中,在所述预先接收外部的管理终端发送的门禁智能合约之后,在所述将当前门禁标识记录到所述门禁智能合约中之前,进一步包括:利用预设的密钥对所述门禁智能合约解密,获得解密后的所述门禁智能合约;则,所述将当前门禁标识记录到所述门禁智能合约中,包括:将当前门禁标识记录到解密后的所述门禁智能合约中。在本申请实施例中,
25 在接收到外部的管理终端发送的加密后的门禁智能合约后,需要利用预设的密钥解密密文形式的门禁智能合约,以获得明文形式的门禁智能合约,再将自身对应的当前门禁标识记录到解密后的门禁智能合约,以使利用该门禁智能合约确定出入所管控的区域的用户的出入权限。

在本申请一实施例中,在所述开启控制的安全门之后,进一步包括:将所述当前用户作为合法用户,

并存储所述合法用户的出入记录；在接收到所述管理终端发送的反馈请求时，将所述出入记录返回给发来所述反馈请求的所述门禁终端。在本申请实施例中，在确定当前用户具有出入权限后，即可确定当前用户为合法用户，因此可以存储其出入记录，以使在接收到管理终端发来的反馈请求时，将反馈请求对应的合法用户的出入记录返回给管理终端，以使管理终端根据出入记录生成考勤表，供外部参考。

5 如图3所示，本申请实施例提供了一种管理终端，包括：终端接收单元301，用于接收外部输入的至少一个合法用户的身份信息，与至少一个外部的门禁终端的门禁标识的身份对应关系；终端处理单元302，用于生成携带所述终端接收单元301接收的所述身份对应关系的门禁智能合约；确定区块链系统中对应的区块链节点，并将所述门禁智能合约存储到该区块链节点中；将所述门禁智能合约分别同步到所述区块链系统中其他管理终端分别对应的区块链节点中；终端发送单元303，用于将所述终端处理单元302生成的
10 所述门禁智能合约发送给至少一个外部的门禁终端。

在本申请实施例提供了一种管理终端，管理终端的终端接收单元可以接收外部（例如，管理人员）输入的变更后的至少一个合法用户的身份信息，与至少一个外部门禁终端的身份对应关系，这样终端处理单元根据终端接收单元接收的身份对应关系，即可生成对应的门禁智能合约。由于区块链具有不可篡改和可溯源的特性，因此将该门禁智能合约存储到自身对应的区块链节点中，并同步到其他管理终端分别对应的
15 区块链节点中，以使各个区块链节点记录的数据相同，即共同维护同一数据库，这样外部通过任一管理终端仍可获知合法用户的身份信息与门禁终端的身份对应关系，便于外部管理门禁终端，还可以约束外部不能随意更改合法用户的身份信息与至少一个外部的门禁终端的身份对应关系，即避免外部随意更改合法用户出入各个门禁终端的权限，从而保证了区块链中数据的可信性；再通过终端发送单元将门禁智能合约发送给至少一个外部的门禁终端，可以使得接收到门禁智能合约的门禁终端共享同一个身份信息账本，这样
20 当有人发生变更时，外部无需逐一更改变更人员所涉及的每一个门禁终端的权限，因此可以降低管理人员管理门禁终端的难度，提高门禁终端的管理效率，同时，还可以避免在特殊情况下门禁终端需要人工临时授权而造成人力资源的浪费，并且还可以消除因人工临时授权带来的安全隐患。

在本申请一实施例中，所述终端接收单元，进一步用于接收外部输入的至少一个所述门禁标识与至少一个访问时段的时段对应关系；所述终端处理单元，用于生成携带所述身份对应关系和所述时段对应关系的门禁智能合约。在本申请一实施例中，所述终端处理单元，进一步用于利用预设的密钥对所述门禁智能合约加密，获得加密后的所述门禁智能合约；所述终端发送单元，用于将加密后的所述门禁智能合约发送给至少一个外部的门禁终端。在本申请一实施例中，所述终端接收单元，进一步用于接收外部输入的当前
25 验证信息；在接收到所述终端处理单元的触发时，执行所述接收外部输入的至少一个合法用户的身份信息，

与至少一个外部的门禁终端的门禁标识的身份对应关系；所述终端处理单元，进一步用于确定预先存储的至少一个预存验证信息中，是否存在与所述当前验证信息相同的同一验证信息，如果是，触发所述终端接收单元，否则，输出无管理权限。在本申请一实施例中，所述终端发送单元，进一步用于按照预设的反馈周期，向所述至少一个外部的门禁终端中的目标门禁终端发送反馈请求；所述终端接收单元，进一步用于接收所述目标门禁终端根据所述反馈请求返回的至少一个所述合法用户的出入记录；所述终端处理单元，进一步用于根据所述出入记录，生成每一个所述合法用户对应的考勤表，并输出所述考勤表。

如图4所示，本申请实施例提供了一种门禁终端，包括：门禁交互单元401，用于预先接收外部的管理终端发送的门禁智能合约；门禁管理单元402，用于将当前门禁标识记录到所述门禁交互单元401接收的所述门禁智能合约中，并存储记录后的所述门禁智能合约；门禁控制单元403，用于利用所述门禁管理单元402存储的所述门禁智能合约，执行：获取当前用户的身份信息；确定所述当前门禁标识对应的至少一个合法用户的身份信息中，是否存在与所述当前用户的身份信息相同的同一身份信息；如果是，开启控制的安全门；否则，输出无出入权限。在本申请实施例提供了一种门禁终端，门禁终端的门禁交互单元在接收到外部的管理终端发送的门禁智能合约时，门禁管理单元需要将自身的当前门禁标识记录到门禁交互单元接收的门禁智能合约中，以使在当前用户需要出入控制的安全门时，门禁控制单元利用门禁智能合约根据记录的当前门禁标识和获取到的当前用户的身份信息，确定当前用户是否具有出入所控制的安全门的出入权限，避免非法用户随意出入办公职场，提高办公职场的安全性，当且仅当在确定当前用户具有出入权限时，开启控制的安全门，以便当前用户出入。

如图5所示，本申请实施例提供了基于区块链的门禁访问系统，包括：至少两个图3所述的管理终端501和至少一个图4所述的门禁终端502。在本申请实施例提供了基于区块链的门禁访问系统，外部（例如，管理人员）可以将变更后的至少一个合法用户的身份信息，与至少一个门禁终端的身份对应关系输入到管理终端中，这样管理终端根据外部输入的身份对应关系，即可生成对应的门禁智能合约。由于区块链具有不可篡改和可溯源的特性，因此将该门禁智能合约存储到自身对应的区块链节点中，并同步到其他管理终端分别对应的区块链节点中，以使各个区块链节点记录的数据相同，即共同维护同一数据库，这样外部通过任一管理终端仍可获知合法用户的身份信息与门禁终端的身份对应关系，便于管理门禁终端，还可以约束外部不能随意更改合法用户的身份信息与至少一个门禁终端的身份对应关系，即避免外部随意更改合法用户出入各个门禁终端的权限，从而保证了区块链中数据的可信性；再将门禁智能合约发送给至少一个门禁终端，门禁终端即可利用门禁终端智能合约确定用户是否具有出入权限，同时，还可以使得接收到门禁智能合约的门禁终端共享同一个身份信息账本，这样当有人员发生变更时，外部无需逐一更改变更人

员所涉及的每一个门禁终端的权限，因此可以降低管理人员管理门禁终端的难度，提高门禁终端的管理效率，同时，还可以避免在特殊情况下门禁终端需要人工临时授权而造成人力资源的浪费，并且还可以消除因人工临时授权带来的安全隐患。

图 5 中示出了 2 个管理终端 501 和一个门禁终端 502。如图 6 所示，为了更加清楚的本申请的技术方案及优点，下面以管理终端 a601、管理终端 b602、门禁终端 c603 和门禁终端 d604 为例，其中，门禁终端 c603 为目标门禁终端，对本申请提供的基于区块链的门禁访问系统进行详细描述，具体可以包括：管理终端 a601，用于接收外部输入的当前验证信息，确定存储的至少一个预存验证信息中，是否存在与当前验证信息相同的同一验证信息，如果是，接收外部输入的至少一个合法用户的身份信息与至少一个门禁终端的门禁标识的身份对应关系，以及至少一个合法用户的身份信息与至少一个门禁终端的门禁标识的时段对应关系，否则，输出无管理权限。具体地，外部如需设置合法用户访问门禁终端的权限，需要先通过管理终端 a 的身份验证，当且仅当在验证通过时，才可向管理终端 a 输入合法用户的身份信息与门禁终端的门禁标识的身份对应关系，以及门禁标识与访问时段的时段对应关系，这样可以避免非法用户随意篡改门禁终端的访问权限，从而可以实现提高门禁终端管理的安全性。管理终端 a601，用于生成携带身份对应关系和时段对应关系的门禁智能合约，确定区块链系统中对应的区块链节点，并将门禁智能合约存储到该区块链节点中，将门禁智能合约分别同步到区块链系统中管理终端 b602 对应的区块链节点中。利用预设的密钥对门禁智能合约加密，获得加密后的门禁智能合约。将加密后的门禁智能合约发送给门禁终端 c603 和门禁终端 d604。具体地，管理终端 a 根据身份对应关系和时段对应关系，可以生成对应的门禁终端合约，门禁终端合约存储到自身对应的区块链节点中，并同步到管理终端 b 对应的区块链节点中，可以使得不同的管理终端共享同一身份信息账本，以便不同的管理人员通过不同的管理终端认可获知合法用户的出入权限，并且当有人员变更时，无需管理人员逐一更改每一个变更人员所涉及的门禁终端的权限，因此可以降低管理人员管理门禁终端的难度，提高门禁终端的管理效率。由于区块链具有不可篡改和可溯源的特性，所以可以约束管理人员不能随意更改合法用户出入门禁终端的权限，以提高办公区域的安全性。再将门禁智能合约利用预设的密钥进行加密，将密文发送给门禁终端 c 和门禁终端 d，即可使得门禁终端 c 和门禁终端 d 利用门禁终端合约确定用户是否具有出入安全门的出入权限，以确保办公区域的安全性。

门禁终端 c603 和门禁终端 d604，用于预先接收管理终端 a601 发送的门禁智能合约，并利用预设的密钥对门禁智能合约解密，获得解密后的门禁智能合约，将自身分别对应的当前门禁标识记录到解密后的门禁智能合约中，并存储记录后的门禁智能合约。具体地，门禁终端 c 和门禁终端 d 在接收到门禁智能合约时，需要先利用密钥对门禁智能合约进行解密，再将自身对应的当前门禁标识记录到解密后门禁智能合约，

以使利用记录由当前门禁标识的门禁智能合约，确定用户是否具有出入安全门的权限。门禁终端 c603，用于利用存储的门禁智能合约，执行：获取当前用户的身份信息，执行：S0：确定当前门禁标识对应的至少一个合法用户的身份信息中，是否存在与当前用户的身份信息相同的同一身份信息，如果是，执行 S1，否则，执行 S4。S1：确定获取当前用户的身份信息的时间点，执行 S2。S2：确定时间点是否在当前门禁标识对应的访问时段内，如果是，执行 S3，否则，执行 S5。S3：开启控制的安全门，并将当前用户作为合法用户，并存储合法用户的出入记录。S4：输出无出入权限。S5：输出出入受限。

具体地，门禁终端 c 利用存储的门禁智能合约，在获取到当前用户的面部图像、虹膜、指纹、掌纹、声音以及门禁卡中的任意一个或多个身份信息时，可以根据获取的身份信息，确定用户是否具有所控制的安全门的出入权限，如果确定当前用户有出入权限，还需要确定当前用户出入所控制的安全门的时间点，是否在其对应的访问时段内，如果在访问时段内，则可以控制安全门开启，以使用户出入，否则，需要输出出入受限的提示信息，以提示用户此时间点无法出入门禁终端 c603 所控制的安全门。管理终端 a601，用于按照预设的反馈周期，向门禁终端 c603 发送反馈请求。门禁终端 c603，用于在接收到管理终端 a601 发送的反馈请求时，将存储的出入记录返回给发来反馈请求的门禁终端 a。管理终端 a601，用于接收门禁终端 c603 根据反馈请求返回的至少一个合法用户的出入记录，根据出入记录，生成每一个合法用户对应的考勤表，并输出考勤表。具体地，管理人员可以在目标管理终端内设置反馈周期，以使目标管理终端按照反馈周期向对应的目标门禁终端发送反馈请求，这样目标门禁终端根据反馈请求即可将存储的出入记录返回给对应的管理终端，管理终端根据返回的出入记录即可生成考勤表，并提供给外部人员，以便外部人员根据考勤表快速确定各个合法用户的考勤情况，节省外部人员统计考勤的时间。

需要说明的是，考勤表中可以包括每一个合法用户的考勤次数、并标记出考勤不合格的合法用户、加班的合法用户的以及加班时长。本申请实施例提供了一种计算机设备，所述计算机设备包括非易失性可读存储介质、处理器及存储在所述非易失性可读存储介质上并可在所述处理器上运行的计算机可读指令，所述处理器执行所述计算机可读指令时实现以下步骤：接收外部输入的至少一个合法用户的身份信息，与至少一个外部的门禁终端的门禁标识的身份对应关系；生成携带所述身份对应关系的门禁智能合约；确定区块链系统中对应的区块链节点，并将所述门禁智能合约存储到该区块链节点中；将所述门禁智能合约分别同步到所述区块链系统中其他管理终端分别对应的区块链节点中；将所述门禁智能合约发送给至少一个外部的门禁终端。在一个实施例中，所述处理器在执行所述接收外部输入的至少一个合法用户的身份信息，与至少一个外部的门禁终端的门禁标识的身份对应关系步骤之后，在执行所述生成携带所述身份对应关系的门禁智能合约步骤之前，进一步执行：接收外部输入的至少一个所述门禁标识与至少一个访问时段的时

段对应关系；所述处理器所执行的所述生成携带所述身份对应关系的门禁智能合约步骤包括：生成携带所述身份对应关系和所述时段对应关系的门禁智能合约。在一个实施例中，所述处理器在执行所述将所述门禁智能合约分别同步到所述区块链系统中其他管理终端分别对应的区块链节点中步骤之后，在执行所述将所述门禁智能合约发送给至少一个外部的门禁终端步骤之前，进一步执行：利用预设的密钥对所述门禁智能合约加密，获得加密后的所述门禁智能合约；则，所述处理器执行所述将所述门禁智能合约发送给至少一个外部的门禁终端的步骤包括：将加密后的所述门禁智能合约发送给至少一个外部的门禁终端。

在一个实施例中，所述处理器在执行所述接收外部输入的至少一个合法用户的身份信息，与至少一个外部的门禁终端的门禁标识的身份对应关系步骤之前，进一步执行：接收外部输入的当前验证信息；确定预先存储的至少一个预存验证信息中，是否存在与所述当前验证信息相同的同一验证信息；如果是，执行所述接收外部输入的至少一个合法用户的身份信息，与至少一个外部的门禁终端的门禁标识的身份对应关系；否则，输出无管理权限。在一个实施例中，所述处理器在执行所述将所述门禁智能合约发送给至少一个外部的门禁终端步骤之后，进一步执行：按照预设的反馈周期，向所述至少一个外部的门禁终端中的目标门禁终端发送反馈请求；接收所述目标门禁终端根据所述反馈请求返回的至少一个所述合法用户的出入记录；根据所述出入记录，生成每一个所述合法用户对应的考勤表，并输出所述考勤表。在一个实施例中，所述处理器执行所述计算机可读指令时还可以实现以下步骤：预先接收外部的管理终端发送的门禁智能合约，将当前门禁标识记录到所述门禁智能合约中，并存储记录后的所述门禁智能合约；利用存储的所述门禁智能合约，执行：获取当前用户的身份信息；确定所述当前门禁标识对应的至少一个合法用户的身份信息中，是否存在与所述当前用户的身份信息相同的同一身份信息；如果是，开启控制的安全门；否则，输出无出入权限。在一个实施例中，所述处理器在执行在确定存在同一身份信息时，在所述开启控制的安全门步骤之前，进一步执行：确定获取所述当前用户的身份信息的时间点；确定所述时间点是否在所述当前门禁标识对应的访问时段内；如果是，执行所述开启控制的安全门；否则，输出出入受限。在一个实施例中，所述处理器在执行在所述预先接收外部的管理终端发送的门禁智能合约步骤之后，在执行所述将当前门禁标识记录到所述门禁智能合约中步骤之前，进一步执行：利用预设的密钥对所述门禁智能合约解密，获得解密后的所述门禁智能合约；所述处理器执行的所述将当前门禁标识记录到所述门禁智能合约中步骤，包括：将当前门禁标识记录到解密后的所述门禁智能合约中。在一个实施例中，所述处理器在执行所述开启控制的安全门步骤之后，进一步执行：将所述当前用户作为合法用户，并存储所述合法用户的出入记录；在接收到所述管理终端发送的反馈请求时，将所述出入记录返回给发来所述反馈请求的所述门禁终端。在一个实施例中，提出了一种存储由计算机可读指令的非易失性可读存储介质，该计算机可读指令被

一个或多个处理器执行时,使得一个或多个处理器执行以下步骤:接收外部输入的至少一个合法用户的身份信息,与至少一个外部的门禁终端的门禁标识的身份对应关系;生成携带所述身份对应关系的门禁智能合约;确定区块链系统中对应的区块链节点,并将所述门禁智能合约存储到该区块链节点中;将所述门禁智能合约分别同步到所述区块链系统中其他管理终端分别对应的区块链节点中;将所述门禁智能合约发送

5 给至少一个外部的门禁终端。在一个实施例中,所述处理器在执行所述接收外部输入的至少一个合法用户的身份信息,与至少一个外部的门禁终端的门禁标识的身份对应关系步骤之后,在执行所述生成携带所述身份对应关系的门禁智能合约步骤之前,进一步执行:接收外部输入的至少一个所述门禁标识与至少一个访问时段的时段对应关系;所述处理器所执行的所述生成携带所述身份对应关系的门禁智能合约步骤包括:生成携带所述身份对应关系和所述时段对应关系的门禁智能合约。

10 在一个实施例中,所述处理器在执行所述将所述门禁智能合约分别同步到所述区块链系统中其他管理终端分别对应的区块链节点中步骤之后,在执行所述将所述门禁智能合约发送给至少一个外部的门禁终端步骤之前,进一步执行:利用预设的密钥对所述门禁智能合约加密,获得加密后的所述门禁智能合约;则,所述处理器执行所述将所述门禁智能合约发送给至少一个外部的门禁终端的步骤包括:将加密后的所述门禁智能合约发送给至少一个外部的门禁终端。在一个实施例中,所述处理器在执行所述接收外部输入的至

15 少一个合法用户的身份信息,与至少一个外部的门禁终端的门禁标识的身份对应关系步骤之前,进一步执行:接收外部输入的当前验证信息;确定预先存储的至少一个预存验证信息中,是否存在与所述当前验证信息相同的同一验证信息;如果是,执行所述接收外部输入的至少一个合法用户的身份信息,与至少一个外部的门禁终端的门禁标识的身份对应关系;否则,输出无管理权限。在一个实施例中,所述处理器在执行所述将所述门禁智能合约发送给至少一个外部的门禁终端步骤之后,进一步执行:按照预设的反馈周期,

20 向所述至少一个外部的门禁终端中的目标门禁终端发送反馈请求;接收所述目标门禁终端根据所述反馈请求返回的至少一个所述合法用户的出入记录;根据所述出入记录,生成每一个所述合法用户对应的考勤表,并输出所述考勤表。在一个实施例中,所述处理器执行所述计算机可读指令时还可以实现以下步骤:预先接收外部的管理终端发送的门禁智能合约,将当前门禁标识记录到所述门禁智能合约中,并存储记录后的所述门禁智能合约;利用存储的所述门禁智能合约,执行:获取当前用户的身份信息;确定所述当前门禁

25 标识对应的至少一个合法用户的身份信息中,是否存在与所述当前用户的身份信息相同的同一身份信息;如果是,开启控制的安全门;否则,输出无出入权限。在一个实施例中,所述处理器在执行在确定存在同一身份信息时,在所述开启控制的安全门步骤之前,进一步执行:确定获取所述当前用户的身份信息的时间点;确定所述时间点是否在所述当前门禁标识对应的访问时段内;如果是,执行所述开启控制的安全门;

否则，输出出入受限。在一个实施例中，所述处理器在执行在所述预先接收外部的管理终端发送的门禁智能合约步骤之后，在执行所述将当前门禁标识记录到所述门禁智能合约中步骤之前，进一步执行：利用预设的密钥对所述门禁智能合约解密，获得解密后的所述门禁智能合约；所述处理器执行的所述将当前门禁标识记录到所述门禁智能合约中步骤，包括：将当前门禁标识记录到解密后的所述门禁智能合约中。在一个实施例中，所述处理器在执行所述开启控制的安全门步骤之后，进一步执行：将所述当前用户作为合法用户，并存储所述合法用户的出入记录；在接收到所述管理终端发送的反馈请求时，将所述出入记录返回给发来所述反馈请求的所述门禁终端。

需要说明的是，在本文中，诸如第一和第二之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同因素。本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，该计算机程序可存储于一计算机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。其中，前述的存储介质可为磁碟、光盘、只读存储记忆体（Read-Only Memory，ROM）等非易失性存储介质，或随机存储记忆体（Random Access Memory，RAM）等。以上所述实施例的各技术特征可以进行任意的组合，为使描述简洁，未对上述实施例中的各个技术特征所有可能的组合都进行描述，然而，只要这些技术特征的组合不存在矛盾，都应当认为是本说明书记载的范围。以上所述实施例仅表达了本申请的几种实施方式，其描述较为具体和详细，但并不能因此而理解为对本申请专利范围的限制。应当指出的是，对于本领域的普通技术人员来说，在不脱离本申请构思的前提下，还可以做出若干变形和改进，这些都属于本申请的保护范围。因此，本申请专利的保护范围应以所附权利要求为准。

权利要求书

1、基于区块链的门禁访问方法，应用于管理终端，包括：

接收外部输入的至少一个合法用户的身份信息，与至少一个外部的门禁终端的门禁标识的身份对应关系；

5 生成携带所述身份对应关系的门禁智能合约；

确定区块链系统中对应的区块链节点，并将所述门禁智能合约存储到该区块链节点中；

将所述门禁智能合约分别同步到所述区块链系统中其他管理终端分别对应的区块链节点中；

将所述门禁智能合约发送给至少一个外部的门禁终端。

2、如权利要求1所述的基于区块链的门禁访问方法，在所述接收外部输入的至少一个合法用户的身份信息，与至少一个外部的门禁终端的门禁标识的身份对应关系之后，在所述生成携带所述身份对应关系的门禁智能合约之前，进一步包括：接收外部输入的至少一个所述门禁标识与至少一个访问时段的时段对应关系；

所述生成携带所述身份对应关系的门禁智能合约，包括：生成携带所述身份对应关系和所述时段对应关系的门禁智能合约；和/或，

15 在所述将所述门禁智能合约分别同步到所述区块链系统中其他管理终端分别对应的区块链节点中之后，在所述将所述门禁智能合约发送给至少一个外部的门禁终端之前，进一步包括：利用预设的密钥对所述门禁智能合约加密，获得加密后的所述门禁智能合约；则，

所述将所述门禁智能合约发送给至少一个外部的门禁终端，包括：将加密后的所述门禁智能合约发送给至少一个外部的门禁终端；和/或，

20 在所述接收外部输入的至少一个合法用户的身份信息，与至少一个外部的门禁终端的门禁标识的身份对应关系之前，进一步包括：接收外部输入的当前验证信息；确定预先存储的至少一个预存验证信息中，是否存在与所述当前验证信息相同的同一验证信息；如果是，执行所述接收外部输入的至少一个合法用户的身份信息，与至少一个外部的门禁终端的门禁标识的身份对应关系；否则，输出无管理权限。

3、如权利要求1所述的基于区块链的门禁访问方法，在所述将所述门禁智能合约发送给至少一个外部的门禁终端之后，进一步包括：按照预设的反馈周期，向所述至少一个外部的门禁终端中的目标门禁终端发送反馈请求；接收所述目标门禁终端根据所述反馈请求返回的至少一个所述合法用户的出入记录；根据所述出入记录，生成每一个所述合法用户对应的考勤表，并输出所述考勤表。

4、基于区块链的门禁访问方法，应用于门禁终端，预先接收外部的管理终端发送的门禁智能合约，将当前门禁标识记录到所述门禁智能合约中，并存储记录后的所述门禁智能合约，包括：

利用存储的所述门禁智能合约，执行：获取当前用户的身份信息；确定所述当前门禁标识对应的至少一个合法用户的身份信息中，是否存在与所述当前用户的身份信息相同的同一身份信息；如果是，开启控制的安全门；否则，输出无出入权限。

5、如权利要求4所述的基于区块链的门禁访问方法，在确定存在同一身份信息时，在所述开启控制的安全门之前，进一步包括：确定获取所述当前用户的身份信息的时间点；确定所述时间点是否在所述当前门禁标识对应的访问时段内；如果是，执行所述开启控制的安全门；否则，输出出入受限；和/或，在所述预先接收外部的管理终端发送的门禁智能合约之后，在所述将当前门禁标识记录到所述门禁智能合约中之前，进一步包括：利用预设的密钥对所述门禁智能合约解密，获得解密后的所述门禁智能合约；则，所述将当前门禁标识记录到所述门禁智能合约中，包括：将当前门禁标识记录到解密后的所述门禁智能合约中；和/或，

在所述开启控制的安全门之后，进一步包括：将所述当前用户作为合法用户，并存储所述合法用户的出入记录；在接收到所述管理终端发送的反馈请求时，将所述出入记录返回给发来所述反馈请求的所述门禁终端。

6、一种管理终端，包括：

终端接收单元，用于接收外部输入的至少一个合法用户的身份信息，与至少一个外部的门禁终端的门禁标识的身份对应关系；

终端处理单元，用于生成携带所述终端接收单元接收的所述身份对应关系的门禁智能合约；确定区块链系统中对应的区块链节点，并将所述门禁智能合约存储到该区块链节点中；将所述门禁智能合约分别同步到所述区块链系统中其他管理终端分别对应的区块链节点中；

终端发送单元，用于将所述终端处理单元生成的所述门禁智能合约发送给至少一个外部的门禁终端。

7、如权利要求6所述的管理终端，所述终端接收单元，进一步用于接收外部输入的至少一个所述门禁标识与至少一个访问时段的时段对应关系；所述终端处理单元，用于生成携带所述身份对应关系和所述时段对应关系的门禁智能合约；所述终端处理单元，进一步用于利用预设的密钥对所述门禁智能合约加密，获得加密后的所述门禁智能合约；所述终端发送单元，用于将加密后的所述门禁智能合约发送给至少一个外部的门禁终端；所述终端接收单元，进一步用于接收外部输入的当前验证信息；确定预先存储的至少一

个预存验证信息中, 是否存在与所述当前验证信息相同的同一验证信息; 如果是, 执行所述接收外部输入的至少一个合法用户的身份信息, 与至少一个外部的门禁终端的门禁标识的身份对应关系; 否则, 输出无管理权限。

8、如权利要求 6 所述的管理终端, 所述终端发送单元, 进一步用于按照预设的反馈周期, 向所述至少一个外部的门禁终端中的目标门禁终端发送反馈请求; 所述终端接收单元, 进一步用于接收所述目标门禁终端根据所述反馈请求返回的至少一个所述合法用户的出入记录; 所述终端处理单元, 进一步用于根据所述出入记录, 生成每一个所述合法用户对应的考勤表, 并输出所述考勤表。

9、一种门禁终端, 包括:

门禁交互单元, 用于预先接收外部的管理终端发送的门禁智能合约;

10 门禁管理单元, 用于将当前门禁标识记录到所述门禁交互单元接收的所述门禁智能合约中, 并存储记录后的所述门禁智能合约;

门禁控制单元, 用于利用所述门禁管理单元存储的所述门禁智能合约, 执行: 获取当前用户的身份信息; 确定所述当前门禁标识对应的至少一个合法用户的身份信息中, 是否存在与所述当前用户的身份信息相同的同一身份信息; 如果是, 开启控制的安全门; 否则, 输出无出入权限。

15 10、如权利要求 9 所述的门禁终端, 所述门禁控制单元, 进一步用于确定获取所述当前用户的身份信息的时间点; 确定所述时间点是否在所述当前门禁标识对应的访问时段内; 如果是, 执行所述开启控制的安全门; 否则, 输出出入受限; 和/或, 在所述预先接收外部的管理终端发送的门禁智能合约之后, 在所述将当前门禁标识记录到所述门禁智能合约中之前, 进一步包括: 利用预设的密钥对所述门禁智能合约解密, 获得解密后的所述门禁智能合约; 则, 所述将当前门禁标识记录到所述门禁智能合约中, 包括: 将当前门禁标识记录到解密后的所述门禁智能合约中; 和/或, 在所述开启控制的安全门之后, 进一步包括: 将所述当前用户作为合法用户, 并存储所述合法用户的出入记录; 在接收到所述管理终端发送的反馈请求时, 将所述出入记录返回给发来所述反馈请求的所述门禁终端。

11、基于区块链的门禁访问系统, 包括: 至少两个权利要求 6 所述的管理终端和至少一个权利要求 9 所述的门禁终端。

25 12、一种计算机设备, 包括存储器和处理器, 所述存储器中存储有计算机可读指令, 所述计算机可读指令被所述处理器执行时实现基于区块链的门禁访问方法, 包括: 接收外部输入的至少一个合法用户的身份信息, 与至少一个外部的门禁终端的门禁标识的身份对应关系; 生成携带所述身份对应关系的门禁智能

合约；确定区块链系统中对应的区块链节点，并将所述门禁智能合约存储到该区块链节点中；将所述门禁智能合约分别同步到所述区块链系统中其他管理终端分别对应的区块链节点中；将所述门禁智能合约发送给至少一个外部的门禁终端。

13、如权利要求 12 所述的计算机设备，所述计算机可读指令被所述处理器执行时实现在所述接收外部输入的至少一个合法用户的身份信息，与至少一个外部的门禁终端的门禁标识的身份对应关系之后，在所述生成携带所述身份对应关系的门禁智能合约之前，进一步包括：接收外部输入的至少一个所述门禁标识与至少一个访问时段的时段对应关系；

所述计算机可读指令被所述处理器执行时实现所述生成携带所述身份对应关系的门禁智能合约，包括：生成携带所述身份对应关系和所述时段对应关系的门禁智能合约；和/或，在所述将所述门禁智能合约分别同步到所述区块链系统中其他管理终端分别对应的区块链节点中之后，在所述将所述门禁智能合约发送给至少一个外部的门禁终端之前，进一步包括：利用预设的密钥对所述门禁智能合约加密，获得加密后的所述门禁智能合约；则，所述将所述门禁智能合约发送给至少一个外部的门禁终端，包括：将加密后的所述门禁智能合约发送给至少一个外部的门禁终端；和/或，在所述接收外部输入的至少一个合法用户的身份信息，与至少一个外部的门禁终端的门禁标识的身份对应关系之前，进一步包括：接收外部输入的当前验证信息；确定预先存储的至少一个预存验证信息中，是否存在与所述当前验证信息相同的同一验证信息；如果是，执行所述接收外部输入的至少一个合法用户的身份信息，与至少一个外部的门禁终端的门禁标识的身份对应关系；否则，输出无管理权限。

14、如权利要求 12 所述的计算机设备，所述计算机可读指令被所述处理器执行时实现在所述将所述门禁智能合约发送给至少一个外部的门禁终端之后，进一步包括：按照预设的反馈周期，向所述至少一个外部的门禁终端中的目标门禁终端发送反馈请求；接收所述目标门禁终端根据所述反馈请求返回的至少一个所述合法用户的出入记录；根据所述出入记录，生成每一个所述合法用户对应的考勤表，并输出所述考勤表。

15、如权利要求 12 所述的计算机设备，所述计算机可读指令被所述处理器执行时实现基于区块链的门禁访问方法，应用于门禁终端，预先接收外部的管理终端发送的门禁智能合约，将当前门禁标识记录到所述门禁智能合约中，并存储记录后的所述门禁智能合约，包括：利用存储的所述门禁智能合约，执行：获取当前用户的身份信息；确定所述当前门禁标识对应的至少一个合法用户的身份信息中，是否存在与所述当前用户的身份信息相同的同一身份信息；如果是，开启控制的安全门；否则，输出无出入权限。

16、如权利要求 12 所述的计算机设备，所述计算机可读指令被所述处理器执行时实现基于区块链的门禁访问方法，具体在确定存在同一身份信息时，在所述开启控制的安全门之前，进一步包括：确定获取所述当前用户的身份信息的时间点；确定所述时间点是否在所述当前门禁标识对应的访问时段内；如果是，执行所述开启控制的安全门；否则，输出出入受限；和/或，在所述预先接收外部的管理终端发送的门禁智能合约之后，在所述将当前门禁标识记录到所述门禁智能合约中之前，进一步包括：利用预设的密钥对所述门禁智能合约解密，获得解密后的所述门禁智能合约；则，所述将当前门禁标识记录到所述门禁智能合约中，包括：将当前门禁标识记录到解密后的所述门禁智能合约中；和/或，在所述开启控制的安全门之后，进一步包括：将所述当前用户作为合法用户，并存储所述合法用户的出入记录；在接收到所述管理终端发送的反馈请求时，将所述出入记录返回给发来所述反馈请求的所述门禁终端。

17、一种存储有计算机可读指令的非易失性可读存储介质，所述计算机可读指令被一个或多个处理器执行时实现基于区块链的门禁访问方法，包括：接收外部输入的至少一个合法用户的身份信息，与至少一个外部的门禁终端的门禁标识的身份对应关系；生成携带所述身份对应关系的门禁智能合约；确定区块链系统中对应的区块链节点，并将所述门禁智能合约存储到该区块链节点中；将所述门禁智能合约分别同步到所述区块链系统中其他管理终端分别对应的区块链节点中；将所述门禁智能合约发送给至少一个外部的门禁终端。

18、如权利要求 17 所述的非易失性可读存储介质，所述计算机可读指令被所述处理器执行时实现在所述接收外部输入的至少一个合法用户的身份信息，与至少一个外部的门禁终端的门禁标识的身份对应关系之后，在所述生成携带所述身份对应关系的门禁智能合约之前，进一步包括：接收外部输入的至少一个所述门禁标识与至少一个访问时段的时段对应关系；

所述计算机可读指令被所述处理器执行时实现所述生成携带所述身份对应关系的门禁智能合约，包括：生成携带所述身份对应关系和所述时段对应关系的门禁智能合约；和/或，在所述将所述门禁智能合约分别同步到所述区块链系统中其他管理终端分别对应的区块链节点中之后，在所述将所述门禁智能合约发送给至少一个外部的门禁终端之前，进一步包括：利用预设的密钥对所述门禁智能合约加密，获得加密后的所述门禁智能合约；则，所述将所述门禁智能合约发送给至少一个外部的门禁终端，包括：将加密后的所述门禁智能合约发送给至少一个外部的门禁终端；和/或，在所述接收外部输入的至少一个合法用户的身份信息，与至少一个外部的门禁终端的门禁标识的身份对应关系之前，进一步包括：接收外部输入的当前验证信息；确定预先存储的至少一个预存验证信息中，是否存在与所述当前验证信息相同的同一验

证信息；如果是，执行所述接收外部输入的至少一个合法用户的身份信息，与至少一个外部的门禁终端的门禁标识的身份对应关系；否则，输出无管理权限。

19、如权利要求 17 所述的非易失性可读存储介质，所述计算机可读指令被所述处理器执行时实现在所述将所述门禁智能合约发送给至少一个外部的门禁终端之后，进一步包括：按照预设的反馈周期，向所述至少一个外部的门禁终端中的目标门禁终端发送反馈请求；接收所述目标门禁终端根据所述反馈请求返回的至少一个所述合法用户的出入记录；根据所述出入记录，生成每一个所述合法用户对应的考勤表，并输出所述考勤表。

20、如权利要求 17 所述的非易失性可读存储介质，所述计算机可读指令被所述处理器执行时实现基于区块链的门禁访问方法，应用于门禁终端，预先接收外部的管理终端发送的门禁智能合约，将当前门禁标识记录到所述门禁智能合约中，并存储记录后的所述门禁智能合约，包括：利用存储的所述门禁智能合约，执行：获取当前用户的身份信息；确定所述当前门禁标识对应的至少一个合法用户的身份信息中，是否存在与所述当前用户的身份信息相同的同一身份信息；如果是，开启控制的安全门；否则，输出无出入权限。

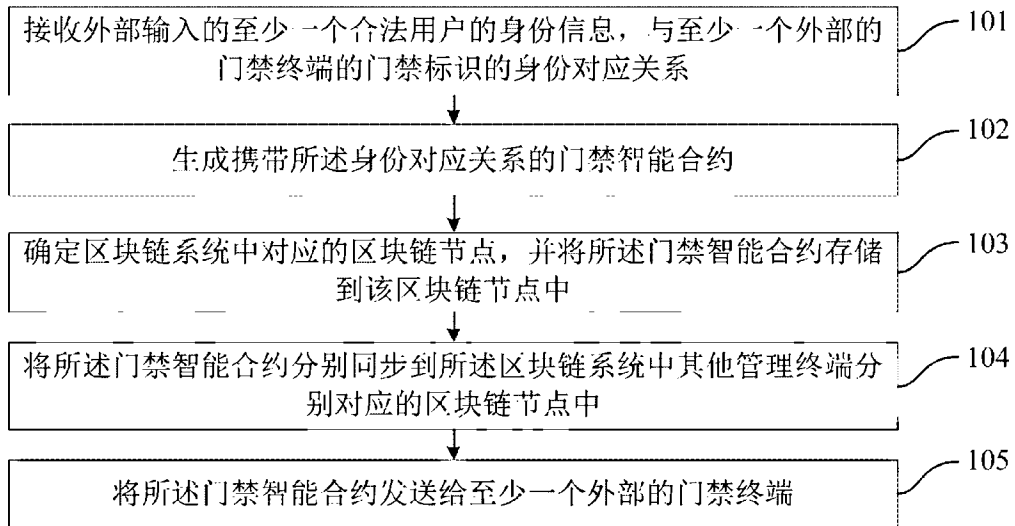


图 1

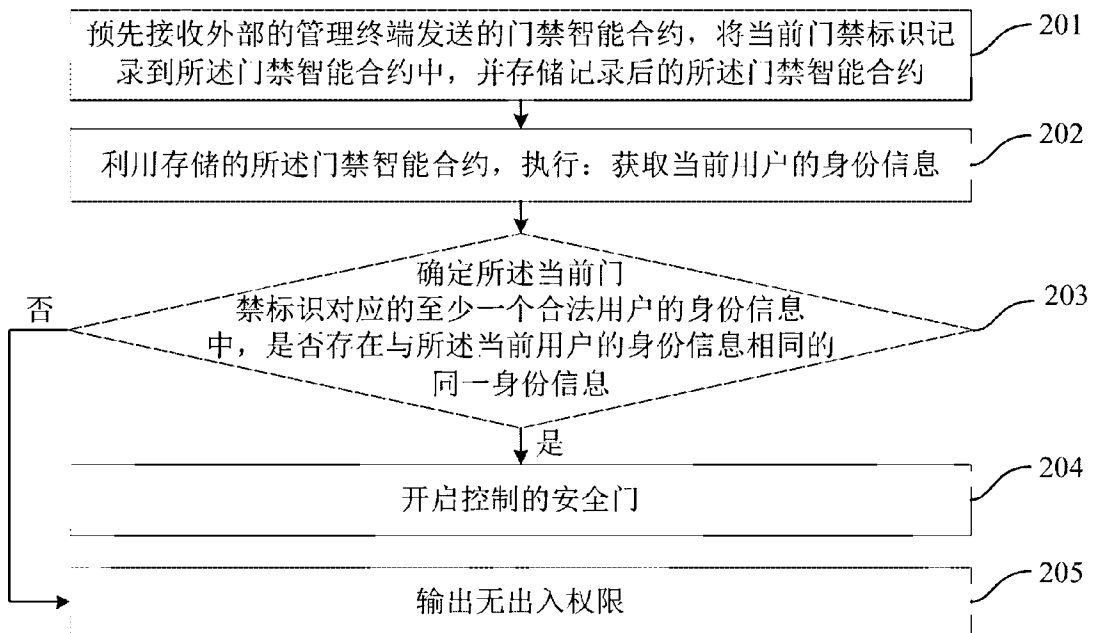


图 2

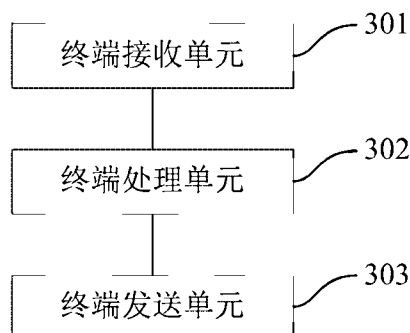


图 3

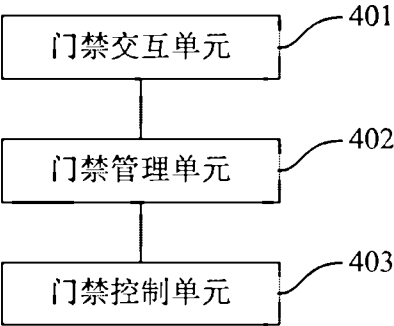


图 4

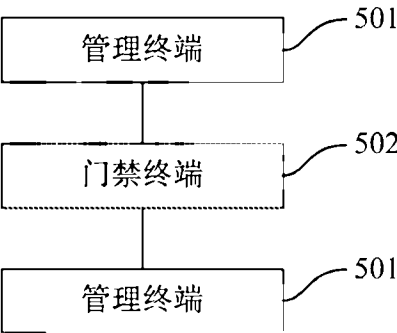


图 5

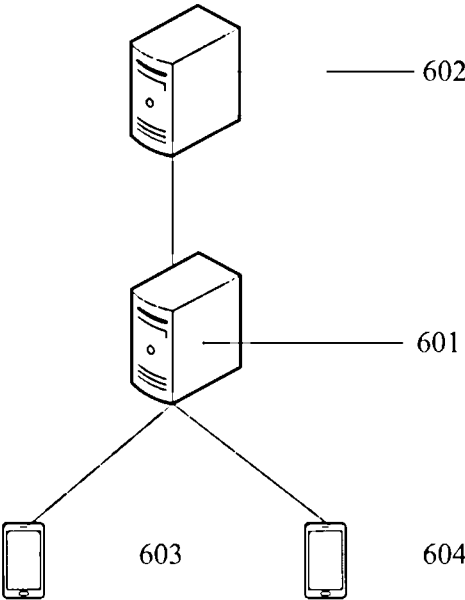


图 6

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/097634

A. CLASSIFICATION OF SUBJECT MATTER

G07C 9/00(2006.01)i; G07C 1/10(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G07C; H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, WPI, EPODOC: 门禁或锁或进门, 区块链, 授权或权限或身份, 节点, 共享或分享或同步, 合约, 时间或时段, 记录, 认证或验证或识别, 加密或解密, lock+ or entrance? or door?, block w chain?, shar???, time, record+ or log+, verif+ or identi+ or certificat+ or recogni+, encrypt+, node

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 109767534 A (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) 17 May 2019 (2019-05-17) description, paragraphs [0075]-[0196], and figures 1-6	1-20
X	CN 109118620 A (GUANGZHOU ZHILE INTERNET OF THINGS TECHNOLOGY CO., LTD.) 01 January 2019 (2019-01-01) description, paragraphs [0016]-[0019], and figures 1 and 2	1-20
X	CN 109064591 A (ANHUI LINGTUYI INTELLIGENT TECHNOLOGY CO., LTD.) 21 December 2018 (2018-12-21) description, paragraphs [0040]-[0064], and figures 1-4	1-20
X	CN 108600213 A (KONG, Dejian) 28 September 2018 (2018-09-28) description, paragraphs [0002]-[0045]	1-20
X	CN 108712389 A (TRACESOFT CO., LTD.) 26 October 2018 (2018-10-26) description, paragraphs [0023]-[0069], and figure 1	1-20
A	CN 108921555 A (JIANGSU HENGBAO INTELLIGENT SYSTEM TECHNOLOGY CO., LTD.) 30 November 2018 (2018-11-30) entire document	1-20



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance
 “E” earlier application or patent but published on or after the international filing date
 “L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
 “O” document referring to an oral disclosure, use, exhibition or other means
 “P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
 “X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
 “Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
 “&” document member of the same patent family

Date of the actual completion of the international search

19 September 2019

Date of mailing of the international search report

24 October 2019

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing
100088
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/097634**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 108777675 A (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) 09 November 2018 (2018-11-09) entire document	1-20
A	KR 101875725 B1 (SOGANG UNIVERSITY RESEARCH FOUNDATION) 06 July 2018 (2018-07-06) entire document	1-20

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2019/097634

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	109767534	A	17 May 2019	None	
CN	109118620	A	01 January 2019	None	
CN	109064591	A	21 December 2018	None	
CN	108600213	A	28 September 2018	None	
CN	108712389	A	26 October 2018	None	
CN	108921555	A	30 November 2018	None	
CN	108777675	A	09 November 2018	None	
KR	101875725	B1	06 July 2018	None	

国际检索报告

国际申请号

PCT/CN2019/097634

A. 主题的分类

G07C 9/00(2006.01)i; G07C 1/10(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G07C; H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

CNPAT, CNKI, WPI, EPDOC: 门禁 or 锁 or 进门, 区块链, 授权 or 权限 or 身份, 节点, 共享 or 分享 or 同步, 合约, 时间 or 时段, 记录, 认证 or 验证 or 识别, 加密 or 解密, lock+ or entrance? or door?, block w chain?, shar???, time, record+ or log+, verif+ or identi+ or certificat+ or recogni+, encrypt+, node

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
PX	CN 109767534 A (平安科技深圳有限公司) 2019年 5月 17日 (2019 - 05 - 17) 说明书第[0075]-[0196]段、图1-6	1-20
X	CN 109118620 A (广州智乐物联网技术有限公司) 2019年 1月 1日 (2019 - 01 - 01) 说明书第[0016]-[0019]段、图1, 2	1-20
X	CN 109064591 A (安徽灵图壹智能科技有限公司) 2018年 12月 21日 (2018 - 12 - 21) 说明书第[0040]-[0064]段、图1-4	1-20
X	CN 108600213 A (孔德键) 2018年 9月 28日 (2018 - 09 - 28) 说明书第[0002]-[0045]段	1-20
X	CN 108712389 A (杭州全视软件有限公司) 2018年 10月 26日 (2018 - 10 - 26) 说明书第[0023]-[0069]段、图1	1-20
A	CN 108921555 A (江苏恒宝智能系统技术有限公司) 2018年 11月 30日 (2018 - 11 - 30) 全文	1-20
A	CN 108777675 A (平安科技深圳有限公司) 2018年 11月 9日 (2018 - 11 - 09) 全文	1-20

☒ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

2019年 9月 19日

国际检索报告邮寄日期

2019年 10月 24日

ISA/CN的名称和邮寄地址

中国国家知识产权局(ISA/CN)

中国北京市海淀区蓟门桥西土城路6号 100088

传真号 (86-10)62019451

受权官员

李思思

电话号码 86-(10)-53962608

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
A	KR 101875725 B1 (UNIV. SOGANG RES. FOUNDATION) 2018年 7月 6日 (2018 - 07 - 06) 全文	1-20

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2019/097634

检索报告引用的专利文件			公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN	109767534	A	2019年 5月 17日	无	
CN	109118620	A	2019年 1月 1日	无	
CN	109064591	A	2018年 12月 21日	无	
CN	108600213	A	2018年 9月 28日	无	
CN	108712389	A	2018年 10月 26日	无	
CN	108921555	A	2018年 11月 30日	无	
CN	108777675	A	2018年 11月 9日	无	
KR	101875725	B1	2018年 7月 6日	无	