(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 16 日 (16.07.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/143312 A1

(51) 国际专利分类号:
G06F 21/60 (2013.01)

(21) 国际申请号: PCT/CN2019/118073

(22) 国际申请日: 2019 年 11 月 13 日 (13.11.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910027204.7 2019年1月11日 (11.01.2019) 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: 汤琦 (TANG, Qi); 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: 北京英特普罗知识产权代理有限公司 (INTELLECPRO CHINA LIMITED); 中国北京市西城区车公庄大街9号五栋大楼C座11层, Beijing 100044 (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,

(54) **Title:** DATA SAVING AND QUERYING METHOD, APPARATUS, COMPUTER SYSTEM AND READABLE STORAGE MEDIUM

(54) **发明名称**: 数据保存查询方法、装置、计算机系统及可读存储介质

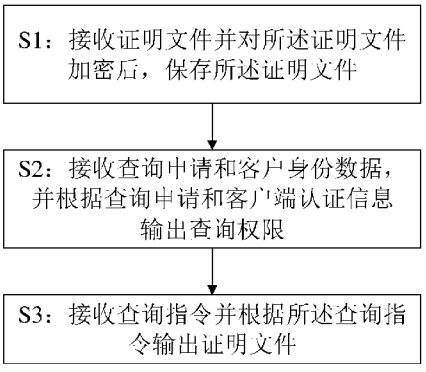

图 1

S1 Receive a certification document, encrypt the certification document, and then save the certification document
S2 Receive a query application and client authentication information, and output query rights according to the query application and client authentication information
S3 Receive a query instruction, and output the certification document according to the query instruction

(57) **Abstract:** A data saving and querying method, an apparatus, a computer system and a readable storage medium, wherein a blockchain database is used and the blockchain database is provided with multiple certification nodes, the method comprising the following steps: receiving a certification document, encrypting the certification document, and then saving the certification document (S1); receiving a query application and client authentication information, and outputting query rights according to the query application and client authentication information (S2); and receiving a query instruction, and outputting the certification document according to the query instruction (S3). The described method prevents the situation in which nodes outside of a blockchain database tamper with, counterfeit and forge a certification document so as to influence a comprehensive assessment result for a company, and prevents the situation in which a certain certification node in a blockchain database tampers with a certification document for which another certification node is responsible, thus improving the credibility of a comprehensive assessment result for a company; and the described method is adapted to the requirements of relevant parties for certification documents of customers so as to protect private data and eliminate the risk of leaking business secrets.

WO 2020/143312 A1

[见续页]

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)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

(57) 摘要：一种数据保存查询方法、装置、计算机系统及可读存储介质，利用区块链数据库，所述区块链数据库中具有若干个证明节点，包括以下步骤：接收证明文件并对所述证明文件加密后，保存所述证明文件（S1）；接收查询申请和客户端认证信息，并根据查询申请和客户端认证信息输出查询权限（S2）；接收查询指令并根据所述查询指令输出证明文件（S3）。该方法避免了区块链数据库以外的节点对证明文件进行篡改、仿冒、造假，以影响对公司的综合评估结果的情况出现，同时还避免了区块链数据库中的某一证明节点篡改其他证明节点所负责的证明文件的情况发生，提高了公司综合评估结果信用度；适应了相关方对客户的证明文件的需求，保护了私密数据，消除了商业秘密泄露的风险。

数据保存查询方法、装置、计算机系统及可读存储介质

本申请申明享有 2019 年 1 月 11 日递交的申请号为 CN2019100272047、名称为“数据保存查询方法、装置、计算机系统及可读存储介质”的中国专利申请的优先权，该中国专利申请的整体内容以参考的方式结合在本申请中。

技术领域

本申请涉及区块链技术领域，尤其涉及数据保存查询方法、装置、计算机系统及可读存储介质。

背景技术

目前业界对企业信用证明主要基于各个评估公司对于公司各种公开数据的综合评估。然而评估公司在获取公开数据以及开展综合评估时，很容易因人为因素或市场因素肆意对公开数据进行篡改、仿冒、造假，以影响对公司的综合评估结果，进而造成当前的公司综合评估结果信用度较低的情况出现；

当前业界有通过建立联盟链，区块链作为“信任的机器”，具有可溯源、共识和去中心化的特性，且区块链上的数据都带有时间戳，即使某个节点的数据被修改，也无法只手遮天，因而区块链能够提供绝对可信的环境，通过所述区块链的去中心化架构发挥全局互信机制，形成强的 P2P 信任关系；共信机制的建立可以有效地减少资金端的风控成本，解决银行对于被信息篡改的疑虑；但是这种方法无法解决区块链内部的证明节点对证明文件进行篡改的情况发生，因此，仍然无法消除证明文件被篡改的风险。

申请内容

本申请的目的是提供一种数据保存查询方法、装置、计算机系统及可读存储介质，用于解决现有技术存在的问题。

为实现上述目的，本申请提供一种数据保存查询方法，利用区块链数据库，所述区块链数据库中具有若干个证明节点，包括以下步骤：

S1：接收证明文件并对所述证明文件加密后，保存所述证明文件；

S2：接收查询申请和客户端认证信息，并根据查询申请和客户端认证信息输出查询权限；

S3：接收查询指令并根据所述查询指令输出证明文件。

为实现上述目的，本申请还提供一种数据保存查询装置，包括：

加密保存模块，用于接收证明文件并对所述证明文件加密后，保存所述证明文件；

权限管理模块，用于接收查询申请和客户端认证信息，并根据查询申请和客户端认证信息输出查询权限；

查询管理模块，用于根据查询申请输出证明文件。

为实现上述目的，本申请还提供一种计算机系统，其包括多个计算机设备，各计算机设备包括存储器．处理器以及存储在存储器上并可在处理器上运行的计算机程序，所述多个计算机设备的处理器执行所述计算机程序时共同实现上述数据保存查询方法的以下步骤：

S1：接收证明文件并对所述证明文件加密后，保存所述证明文件；

S2：接收查询申请和客户端认证信息，并根据查询申请和客户端认证信息输出查询权限；

S3：接收查询指令并根据所述查询指令输出证明文件。

为实现上述目的，本申请还提供一种计算机可读存储介质，其包括多个存储介质，各存储介质上存储有计算机程序，所述多个存储介质存储的所述计算机程序被处理器执行时共同实现上述数据保存查询方法的以下步骤：

S1：接收证明文件并对所述证明文件加密后，保存所述证明文件；

S2：接收查询申请和客户端认证信息，并根据查询申请和客户端认证信息输出查询权限；

S3：接收查询指令并根据所述查询指令输出证明文件。

本申请提供的数据保存查询方法、装置、计算机系统及可读存储介质，通过加密保存模块对区块链数据库中证明节点接收的证明文件进行加密，最后由验证节点验证证明文件的加密是否成功，以证明该证明文件确实由区块链数据库中的某一证明节点所对应的证明用户端所上传，因此避免了区块链数据库以外的节点对证明文件进行篡改、仿冒、造假，以影响对公司的综合评估结果的情况出现，同时还避免了区块链数据库中的某一证明节点篡改其他证明节点所负责的证明文件的情况发生，所进而提高了公司综合评估结果信用度；

通过权限管理模块根据查询申请和客户端数据输出查询权限，并通过查询管理模块根据查询权限使客户端获得与所述目标身份数据匹配的客户身份信息、私密数据和公开数据，或客户身份信息和公开数据；

使得具有授权身份数据的客户端能够获得证明文件的私密数据和公开数据，因此不仅适应了市场的相关方对客户的证明文件的需求；而不具有授权身份数据的客户端或仅采用他查申请对其他企业的公开数据进行查看，保证了企业的证明文件的公开数据公开，实现了企业运营透明化，不仅降低了社会对企业的信任风险，同时还有效保护了客户的私密数

据，消除了客户的商业秘密泄露的风险；

最后，客户还可利用客户端对企业自身的私密数据和公开数据进行查看，为企业的运营管理提供了便利。

附图说明

图 1 为本申请数据保存查询方法实施例一的流程图；

图 2 为本申请数据保存查询方法实施例一中数据保存查询装置与服务系统之间的工作流程图；

图 3 为本申请数据保存查询装置实施例二的程序模块示意图；

图 4 为本申请计算机系统实施例三中计算机设备的硬件结构示意图。

附图标记：

1、数据保存查询装置　　2、区块链数据库　　3、证明用户端

4、客户端　　5、计算机设备　　11、加密保存模块

12、权限管理模块　13、查询管理模块　51、存储器　52、处理器

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。基于本申请中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

本申请提供的数据保存查询方法、装置、计算机系统及可读存储介质，适用于区块链领域，为提供一种基于加密保存模块、权限管理模块和查询管理模块的数据保存查询方法。本申请通过加密保存模块对区块链数据库中证明节点接收的证明文件进行加密，最后由验证节点验证证明文件的加密是否成功，以证明该证明文件确实由区块链数据库中的某一证明节点所对应的证明用户端所上传，因此避免了区块链数据库以外的节点对证明文件进行篡改、仿冒、造假，以影响对公司的综合评估结果的情况出现，同时还避免了区块链数据库中的某一证明节点篡改其他证明节点所负责的证明文件的情况发生，进而提高了公司综合评估结果信用度；

通过权限管理模块根据查询申请和客户端数据输出查询权限，并通过查询管理模块根据查询权限使客户端获得与所述目标身份数据匹配的客户身份信息、私密数据和公开数据，或客户身份信息和公开数据；

使得具有授权身份数据的客户端能够获得证明文件的私密数据和公开数据，因此不仅

适应了市场的相关方对客户的证明文件的需求；而不具有授权身份数据的客户端或仅采用他查申请对其他企业的公开数据进行查看，保证了企业的证明文件的公开数据公开，实现了企业运营透明化，不仅降低了社会对企业的信任风险，同时还有效保护了客户的私密数据，消除了客户的商业秘密泄露的风险；

最后，客户还可利用客户端对企业自身的私密数据和公开数据进行查看，为企业的运营管理提供了便利。

实施例一：

请参阅图 1 和图 2，本实施例的一种数据保存查询方法，利用区块链数据库 2 和数据保存查询装置 1，区块链数据库 2 中具有若干个证明节点，包括以下步骤：

S1：接收证明文件并对所述证明文件加密后，保存所述证明文件；

S2：接收查询申请和客户端认证信息，并根据查询申请和客户端认证信息输出查询权限；其中，客户端认证信息为用于证明客户端身份的信息，所述客户端认证信息可为客户端的 IP 地址，也可为客户端的唯一码，还可为客户端的 IP 地址和唯一码的组合。

S3：接收查询指令并根据所述查询指令输出证明文件。

具体的，所述 S1 中包括以下步骤：

S1-01：接收由证明用户端 3 上传的证明文件，并将所述证明文件输出至与所述证明用户端 3 对应的证明节点中；将接收证明文件的证明节点设定为工作节点；其中，证明用户端服务于证明文件的管理单位，如税务管理机关、工商管理机关、消防单位、质量监督机关等证明文件管理企业；每个证明用户端 3 均在区块链数据库中有且只有一个对应的证明节点。

S1-02：生成私钥，并利用私钥获得加密文件、公钥和哈希值；

S1-03：将所述区块链数据库中除工作节点以外的其他证明节点设定为验证节点；将公钥、加密文件和哈希值发送至所述区块链数据库中的所有验证节点；

S1-04：通过验证节点并利用公钥对所述加密文件进行解密，以获得解密摘要；

S1-05：若所有验证节点获得的解密摘要均与所述哈希值一致，则认定工作证明节点对所述证明文件加密成功并生成加密成功信号；

若至少有一个验证节点获得的解密摘要与所述哈希值不一致，则认定工作证明节点对所述证明文件加密失败并生成加密失败信号；

S1-06：接收并根据加密成功信号将所述证明文件保存在所述工作节点中；或

接收并根据加密失败信号删除工作节点中接收的证明文件。

进一步的，所述步骤 S1-02 包括：

S1-02-1：接收由工作节点输出的接收成功信号，根据接收成功信号控制证明用户端 3 并利用随机数生成模块生成私钥；

S1-02-2：接收所述私钥并利用所述私钥对所述证明文件加密，获得加密文件；

S1-02-3：利用椭圆曲线算法对所述私钥进行运算获得公钥；

S1-02-4：利用单向散列算法对所述证明文件进行哈希运算获得哈希值。

具体的，所述 S1 中的证明文件包括客户身份信息、私密数据和公开数据。

优选的，所述步骤 S1 还包括：

S1-07：接收由所述工作节点输出的保存成功信号；或

接收由所述工作节点输出的删除成功信号。

优选的，所述步骤 S2 还包括：

S2-00：创设客户端数据库并根据所述保存成功信号向客户端 4 输出查询许可信号；所述客户端数据库用于储存各客户端 4 的客户端数据，并将各客户端 4 的客户端数据分别与各客户端的客户端认证信息一一对应并匹配；其中，将客户端 4 所服务的企业的客户身份信息作为客户端数据储存至客户端数据库。

优选的，所述 S2 中的查询申请的类型包括自查申请、他查申请和授权申请，所述查询申请具有目标身份数据，并且所述查询申请中的授权申请具有授权身份数据；所述查询权限包括一级权限和二级权限。

进一步的，一级权限用于查看客户身份信息、私密数据和公开数据，二级权限用于查看客户身份信息和公开数据。

具体的，所述步骤 S2 包括：

S2-01：接收由客户端 4 根据所述查询许可信号输出的查询申请和客户端认证信息，并从客户端数据库中获取与所述客户端认证信息匹配的客户端数据；；其中，客户端服务于证明文件的查询单位，如企业，第三方服务机构等需要查询企业的证明文件的查询单位；其中，客户端数据为客户端 4 所服务的企业的客户身份信息，因此，每个客户端 4 有且仅有一个客户身份信息，并且有且仅有一个客户端认证信息；其中，客户身份信息可为企业名称、统一社会信用代码或组织机构代码；

S2-02：确认查询申请的类型，根据所述查询申请的类型比对所述查询申请中的目标身份数据和客户端数据并生成比对结果，或比对查询申请中的授权身份数据和目标身份数据并生成授权结果；其中，所述目标身份数据和授权身份数据均为客户端 4 要查询的证明文件的所有者的客户身份信息，客户身份信息可为企业名称、统一社会信用代码或组织机构代码。

可选的，授权身份数据为电子签名。

S2-03：根据查询申请的类型，以及对比结果或授权结果输出查询权限。

进一步的，所述步骤 S2-03 包括：

当确认所述查询申请为自查申请时，若所述目标身份数据与客户端数据一致，则生成身份有效的对比结果并对客户端 4 发出一级权限；若所述目标身份数据与客户端数据不一致，则生成身份无效的对比结果并对客户端 4 发出二级权限；或

当确认所述查询申请为他查申请时，则对客户端 4 发出二级权限；或

当确认所述查询申请为授权申请时，若所述授权申请中的授权身份数据和目标身份数据一致，则生成授权有效的授权结果并对客户端 4 发出一级权限；若所述授权申请中的授权身份数据和目标身份数据不一致，或所述授权申请中不具有授权身份数据，则生成授权无效的授权结果并对客户端 4 发出二级权限。

具体的，所述步骤 S3 中的查询指令包括一级指令和二级指令；

所述步骤 S3 包括：

接收客户端 4 根据一级权限所输出的一级指令；根据所述一级指令向所述客户端 4 输出与所述目标身份数据匹配的客户身份信息、私密数据和公开数据；或

接收客户端 4 根据二级权限所输出的二级指令；根据所述二级指令向所述客户端 4 输出与所述目标身份数据匹配的客户身份信息和公开数据。

具体的，客户身份信息可为企业名称、统一社会信用代码或组织机构代码；

公开数据可包括但不限于以下信息：企业名称、公司注册地址、统一社会信用代码、注册资金及法定代表人等信息；企业通信地址、邮政编码、联系电话、电子邮箱等信息；企业开业、歇业、清算等存续状态信息；企业投资设立企业、购买股权信息；企业为有限责任公司或者股份有限公司的，其股东或者发起人认缴和实缴的出资额、出资时间、出资方式等信息；有限责任公司股东股权转让等股权变更信息；企业网站以及从事网络经营的网店的名称、网址等信息； 有限责任公司股东或者股份有限公司发起人认缴和实缴的出资额、出资时间、出资方式等信息；有限责任公司股东股权转让等股权变更信息；行政许可取得、变更、延续信息；知识产权出质登记信息；受到行政处罚的信息；

私密数据可包括但不限于以下信息：企业从业人数、资产总额、负债总额、对外提供保证担保、所有者权益合计、营业总收入、主营业务收入、利润总额、净利润、纳税总额信息；

因此，所述一级指令中可为用于获取客户身份信息、公开数据及私密数据中任一信息的申请指令；

例如：一级指令中可为“资产总额查看申请指令”、“负债总额查看申请指令”等。

所述二级指令中可为用于获取客户身份信息和公开数据中任一信息的申请指令；例如，二级指令中可为“企业名称查看申请指令”、“企业通信地址查看申请指令”等。

实施例二：

请参阅图 3，本实施例的一种数据保存查询装置 1，包括：

加密保存模块 11，用于接收证明文件并对所述证明文件加密后，保存所述证明文件；

权限管理模块 12，用于接收查询申请和客户端认证信息，并根据查询申请和客户端认证信息输出查询权限；

查询管理模块 13，用于根据查询申请输出证明文件。

本技术方案基于区块链，利用区块链数据库作为区块存储系统，通过加密保存模块 11 对区块链数据库的证明节点接收证明文件进行加密，最后由验证节点验证证明文件的加密是否成功，以证明该证明文件确实由区块链数据库中的某一证明节点所对应的证明用户端所上传；通过权限管理模块 12 根据查询申请和客户端数据输出查询权限，并通过查询管理模块 13 根据查询权限使客户端获得与所述目标身份数据匹配的客户身份信息、私密数据和公开数据，或客户身份信息和公开数据。

实施例三：

为实现上述目的，本申请还提供一种计算机系统，该计算机系统包括多个计算机设备 5，实施例二的数据保存查询装置 1 的组成部分可分散于不同的计算机设备中，计算机设备可以是执行程序的智能手机、平板电脑、笔记本电脑、台式计算机、机架式服务器、刀片式服务器、塔式服务器或机柜式服务器（包括独立的服务器，或者多个服务器所组成的服务器集群）等。本实施例的计算机设备至少包括但不限于：可通过系统总线相互通信连接的存储器 51、处理器 52，如图 4 所示。需要指出的是，图 4 仅示出了具有组件-的计算机设备，但是应理解的是，并不要求实施所有示出的组件，可以替代的实施更多或者更少的组件。

本实施例中，存储器 51（即可读存储介质）包括闪存、硬盘、多媒体卡、卡型存储器（例如，SD 或 DX 存储器等）、随机访问存储器（RAM）、静态随机访问存储器（SRAM）、只读存储器（ROM）、电可擦除可编程只读存储器（EEPROM）、可编程只读存储器（PROM）、磁性存储器、磁盘、光盘等。在一些实施例中，存储器 51 可以是计算机设备的内部存储单元，例如该计算机设备的硬盘或内存。在另一些实施例中，存储器 51 也可以是计算机设备的外

部存储设备，例如该计算机设备上配备的插接式硬盘，智能存储卡（Smart Media Card, SMC），安全数字（Secure Digital, SD）卡，闪存卡（Flash Card）等。当然，存储器 51 还可以既包括计算机设备的内部存储单元也包括其外部存储设备。本实施例中，存储器 51 通常用于存储安装于计算机设备的操作系统和各类应用软件，例如实施例一的数据保存查询装置的程序代码等。此外，存储器 51 还可以用于暂时地存储已经输出或者将要输出的各类数据。

处理器 52 在一些实施例中可以是中央处理器（Central Processing Unit，CPU）、控制器、微控制器、微处理器、或其他数据处理芯片。该处理器 52 通常用于控制计算机设备的总体操作。本实施例中，处理器 52 用于运行存储器 51 中存储的程序代码或者处理数据，例如运行数据保存查询装置，以实现实施例一的数据保存查询方法。

实施例四：

为实现上述目的，本申请还提供一种计算机可读存储系统，其包括多个存储介质，如闪存、硬盘、多媒体卡、卡型存储器（例如，SD 或 DX 存储器等）、随机访问存储器（RAM）、静态随机访问存储器（SRAM）、只读存储器（ROM）、电可擦除可编程只读存储器（EEPROM）、可编程只读存储器（PROM）、磁性存储器、磁盘、光盘、服务器、App 应用商城等等，其上存储有计算机程序，程序被处理器 52 执行时实现相应功能。本实施例的计算机可读存储介质用于存储数据保存查询装置，被处理器 52 执行时实现实施例一的数据保存查询方法。

权利要求书

1、一种数据保存查询方法，利用区块链数据库，所述区块链数据库中具有若干个证明节点，其特征在于，包括以下步骤：

S1：接收证明文件并对所述证明文件加密后，保存所述证明文件；

S2：接收查询申请和客户端认证信息，并根据查询申请和客户端认证信息输出查询权限；

S3：接收查询指令并根据所述查询指令输出证明文件。

2、根据权利要求 1 所述的数据保存查询方法，其特征在于，所述 S1 中包括以下步骤：

S1-01：接收由证明用户端上传的证明文件，并将所述证明文件输出至与所述证明用户端对应的证明节点中；将接收证明文件的证明节点设定为工作节点；

S1-02：生成私钥，并利用私钥获得加密文件、公钥和哈希值；

S1-03：将所述区块链数据库中除工作节点以外的其他证明节点设定为验证节点；将公钥、加密文件和哈希值发送至所述区块链数据库中的所有验证节点；

S1-04：通过验证节点并利用公钥对所述加密文件进行解密，以获得解密摘要；

S1-05：若所有验证节点获得的解密摘要均与所述哈希值一致，则认定工作证明节点对所述证明文件加密成功并生成加密成功信号；

若至少有一个验证节点获得的解密摘要与所述哈希值不一致，则认定工作证明节点对所述证明文件加密失败并生成加密失败信号；

S1-06：接收并根据加密成功信号将所述证明文件保存在所述工作节点中；或

接收并根据加密失败信号删除工作节点中接收的证明文件。

3、根据权利要求 2 所述的数据保存查询方法，其特征在于，所述步骤 S1-02 包括：

S1-02-1：控制证明用户端并利用随机数生成模块生成私钥；

S1-02-2：接收所述私钥并利用所述私钥对所述证明文件加密，获得加密文件；

S1-02-3：利用椭圆曲线算法对所述私钥进行运算获得公钥；

S1-02-4：利用单向散列算法对所述证明文件进行哈希运算获得哈希值。

4、根据权利要求 1 所述的数据保存查询方法，其特征在于，所述 S1 中的证明文件包括客户身份信息、私密数据和公开数据；

所述 S2 中的查询申请的类型包括自查申请、他查申请和授权申请，所述查询申请具有目标身份数据，所述授权申请中具有授权身份数据；所述查询权限包括一级权限和二级权限。

5、根据权利要求 4 所述的数据保存查询方法，其特征在于，所述步骤 S2 包括：

S2-01：接收由客户端根据所述查询许可信号输出的查询申请和客户端认证信息，并从客户端数据库中获取与所述客户端认证信息匹配的客户端数据；

S2-02：确认查询申请的类型，根据所述查询申请的类型比对所述查询申请中的目标身份数据和客户端数据并生成比对结果，或比对查询申请中的授权身份数据和目标身份数据并生成授权结果；

S2-03：根据查询申请的类型，以及对比结果或授权结果输出查询权限。

6、根据权利要求 5 所述的数据保存查询方法，其特征在于，所述步骤 S2-03 包括：

当确认所述查询申请为自查申请时，若所述目标身份数据与客户端数据一致，则生成身份有效的对比结果并对客户端发出一级权限；若所述目标身份数据与客户端数据不一致，则生成身份无效的对比结果并对客户端发出二级权限；或

当确认所述查询申请为他查申请时，则对客户端发出二级权限；或

当确认所述查询申请为授权申请时，若所述授权申请中的授权身份数据和目标身份数据一致，则生成授权有效的授权结果并对客户端发出一级权限；若所述授权申请中的授权身份数据和目标身份数据不一致，或所述授权申请中不具有授权身份数据，则生成授权无效的授权结果并对客户端发出二级权限。

7、根据权利要求 4 所述的数据保存查询方法，其特征在于，所述步骤 S3 中的查询指令包括一级指令和二级指令；

所述步骤 S3 包括：

接收客户端根据一级权限所输出的一级指令；根据所述一级指令向所述客户端输出与所述目标身份数据匹配的客户身份信息、私密数据和公开数据；或

接收客户端根据二级权限所输出的二级指令；根据所述二级指令向所述客户端输出与所述目标身份数据匹配的客户身份信息和公开数据。

8、一种数据保存查询装置，其特征在于，包括：

加密保存模块，用于接收证明文件并对所述证明文件加密后，保存所述证明文件；

权限管理模块，用于接收查询申请和客户端认证信息，并根据查询申请和客户端认证信息输出查询权限；

查询管理模块，用于根据查询申请输出证明文件。

9、一种计算机系统，其包括多个计算机设备，各计算机设备包括存储器. 处理器以及存储在存储器上并可在处理器上运行的计算机程序，其特征在于，所述多个计算机设备的处理器执行所述计算机程序时共同实现所述数据保存查询方法的以下步骤：

S1：接收证明文件并对所述证明文件加密后，保存所述证明文件；

S2：接收查询申请和客户端认证信息，并根据查询申请和客户端认证信息输出查询权限；

S3：接收查询指令并根据所述查询指令输出证明文件。

10、根据权利要求 9 所述的计算机系统，其特征在于，所述 S1 中包括以下步骤：

S1-01：接收由证明用户端上传的证明文件，并将所述证明文件输出至与所述证明用户端对应的证明节点中；将接收证明文件的证明节点设定为工作节点；

S1-02：生成私钥，并利用私钥获得加密文件、公钥和哈希值；

S1-03：将所述区块链数据库中除工作节点以外的其他证明节点设定为验证节点；将公钥、加密文件和哈希值发送至所述区块链数据库中的所有验证节点；

S1-04：通过验证节点并利用公钥对所述加密文件进行解密，以获得解密摘要；

S1-05：若所有验证节点获得的解密摘要均与所述哈希值一致，则认定工作证明节点对所述证明文件加密成功并生成加密成功信号；

若至少有一个验证节点获得的解密摘要与所述哈希值不一致，则认定工作证明节点对所述证明文件加密失败并生成加密失败信号；

S1-06：接收并根据加密成功信号将所述证明文件保存在所述工作节点中；或

接收并根据加密失败信号删除工作节点中接收的证明文件。

11、根据权利要求 10 所述的计算机系统，其特征在于，所述步骤 S1-02 包括：

S1-02-1：控制证明用户端并利用随机数生成模块生成私钥；

S1-02-2：接收所述私钥并利用所述私钥对所述证明文件加密，获得加密文件；

S1-02-3：利用椭圆曲线算法对所述私钥进行运算获得公钥；

S1-02-4：利用单向散列算法对所述证明文件进行哈希运算获得哈希值。

12、根据权利要求 9 所述的计算机系统，其特征在于，所述 S1 中的证明文件包括客户身份信息、私密数据和公开数据；

所述 S2 中的查询申请的类型包括自查申请、他查申请和授权申请，所述查询申请具有目标身份数据，所述授权申请中具有授权身份数据；所述查询权限包括一级权限和二级权限。

13、根据权利要求 12 所述的计算机系统，其特征在于，所述步骤 S2 包括：

S2-01：接收由客户端根据所述查询许可信号输出的查询申请和客户端认证信息，并从客户端数据库中获取与所述客户端认证信息匹配的客户端数据；

S2-02：确认查询申请的类型，根据所述查询申请的类型比对所述查询申请中的目标身份数据和客户端数据并生成比对结果，或比对查询申请中的授权身份数据和目标身份数据并生成授权结果；

S2-03：根据查询申请的类型，以及对比结果或授权结果输出查询权限。

14、根据权利要求 13 所述的计算机系统，其特征在于，所述步骤 S2-03 包括：

当确认所述查询申请为自查申请时，若所述目标身份数据与客户端数据一致，则生成身份有效的对比结果并对客户端发出一级权限；若所述目标身份数据与客户端数据不一致，则生成身份无效的对比结果并对客户端发出二级权限；或

当确认所述查询申请为他查申请时，则对客户端发出二级权限；或

当确认所述查询申请为授权申请时，若所述授权申请中的授权身份数据和目标身份数据一致，则生成授权有效的授权结果并对客户端发出一级权限；若所述授权申请中的授权身份数据和目标身份数据不一致，或所述授权申请中不具有授权身份数据，则生成授权无效的授权结果并对客户端发出二级权限。

15、根据权利要求 12 所述的计算机系统，其特征在于，所述步骤 S3 中的查询指令包括一级指令和二级指令；

所述步骤 S3 包括：

接收客户端根据一级权限所输出的一级指令；根据所述一级指令向所述客户端输出与所述目标身份数据匹配的客户身份信息、私密数据和公开数据；或

接收客户端根据二级权限所输出的二级指令；根据所述二级指令向所述客户端输出与所述目标身份数据匹配的客户身份信息和公开数据。

16、一种计算机可读存储介质，其包括多个存储介质，各存储介质上存储有计算机程序，其特征在于，所述多个存储介质存储的所述计算机程序被处理器执行时共同实现所述数据保存查询方法的以下步骤：

S1：接收证明文件并对所述证明文件加密后，保存所述证明文件；

S2：接收查询申请和客户端认证信息，并根据查询申请和客户端认证信息输出查询权限；

S3：接收查询指令并根据所述查询指令输出证明文件。

17、根据权利要求 16 所述的计算机可读存储介质，其特征在于，所述 S1 中包括以下步骤：

S1-01：接收由证明用户端上传的证明文件，并将所述证明文件输出至与所述证明用户端对应的证明节点中；将接收证明文件的证明节点设定为工作节点；

S1-02：生成私钥，并利用私钥获得加密文件、公钥和哈希值；

S1-03：将所述区块链数据库中除工作节点以外的其他证明节点设定为验证节点；将公钥、加密文件和哈希值发送至所述区块链数据库中的所有验证节点；

S1-04：通过验证节点并利用公钥对所述加密文件进行解密，以获得解密摘要；

S1-05：若所有验证节点获得的解密摘要均与所述哈希值一致，则认定工作证明节点对所述证明文件加密成功并生成加密成功信号；

若至少有一个验证节点获得的解密摘要与所述哈希值不一致，则认定工作证明节点对所述证明文件加密失败并生成加密失败信号；

S1-06：接收并根据加密成功信号将所述证明文件保存在所述工作节点中；或

接收并根据加密失败信号删除工作节点中接收的证明文件。

18、根据权利要求 17 所述的计算机可读存储介质，其特征在于，所述步骤 S1-02 包括：

S1-02-1：控制证明用户端并利用随机数生成模块生成私钥；

S1-02-2：接收所述私钥并利用所述私钥对所述证明文件加密，获得加密文件；

S1-02-3：利用椭圆曲线算法对所述私钥进行运算获得公钥；

S1-02-4：利用单向散列算法对所述证明文件进行哈希运算获得哈希值。

19、根据权利要求 16 所述的计算机可读存储介质，其特征在于，所述 S1 中的证明文件包括客户身份信息、私密数据和公开数据；

所述 S2 中的查询申请的类型包括自查申请、他查申请和授权申请，所述查询申请具有目标身份数据，所述授权申请中具有授权身份数据；所述查询权限包括一级权限和二级权限；

所述步骤 S2 包括：

S2-01：接收由客户端根据所述查询许可信号输出的查询申请和客户端认证信息，并从客户端数据库中获取与所述客户端认证信息匹配的客户端数据；

S2-02：确认查询申请的类型，根据所述查询申请的类型比对所述查询申请中的目标身份数据和客户端数据并生成比对结果，或比对查询申请中的授权身份数据和目标身份数据并生成授权结果；

S2-03：根据查询申请的类型，以及对比结果或授权结果输出查询权限；

所述步骤 S2-03 包括：

当确认所述查询申请为自查申请时，若所述目标身份数据与客户端数据一致，则生成身份有效的对比结果并对客户端发出一级权限；若所述目标身份数据与客户端数据不一致，则生成身份无效的对比结果并对客户端发出二级权限；或

当确认所述查询申请为他查申请时，则对客户端发出二级权限；或

当确认所述查询申请为授权申请时，若所述授权申请中的授权身份数据和目标身份数据一致，则生成授权有效的授权结果并对客户端发出一级权限；若所述授权申请中的授权身份数据和目标身份数据不一致，或所述授权申请中不具有授权身份数据，

则生成授权无效的授权结果并对客户端发出二级权限。

20、根据权利要求 19 所述的计算机可读存储介质，其特征在于，所述步骤 S3 中的查询指令包括一级指令和二级指令；

所述步骤 S3 包括：

接收客户端根据一级权限所输出的一级指令；根据所述一级指令向所述客户端输出与所述目标身份数据匹配的客户身份信息、私密数据和公开数据；或

接收客户端根据二级权限所输出的二级指令；根据所述二级指令向所述客户端输出与所述目标身份数据匹配的客户身份信息和公开数据。

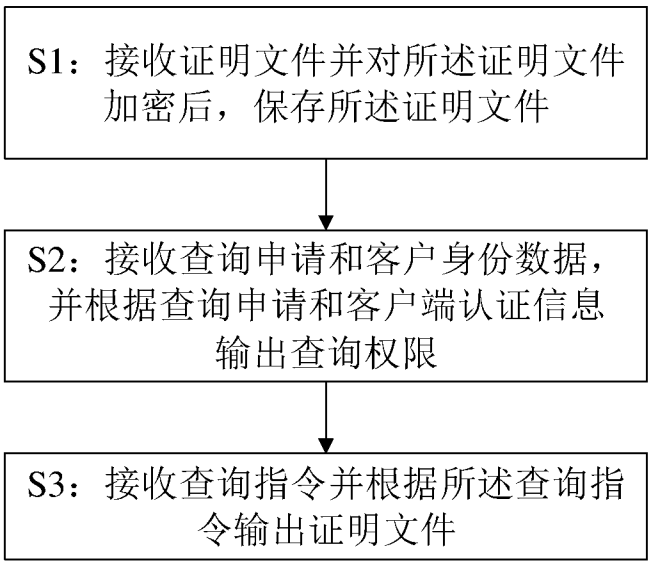
S1：接收证明文件并对所述证明文件加密后，保存所述证明文件
S2：接收查询申请和客户身份数据，并根据查询申请和客户端认证信息输出查询权限
S3：接收查询指令并根据所述查询指令输出证明文件

图 1

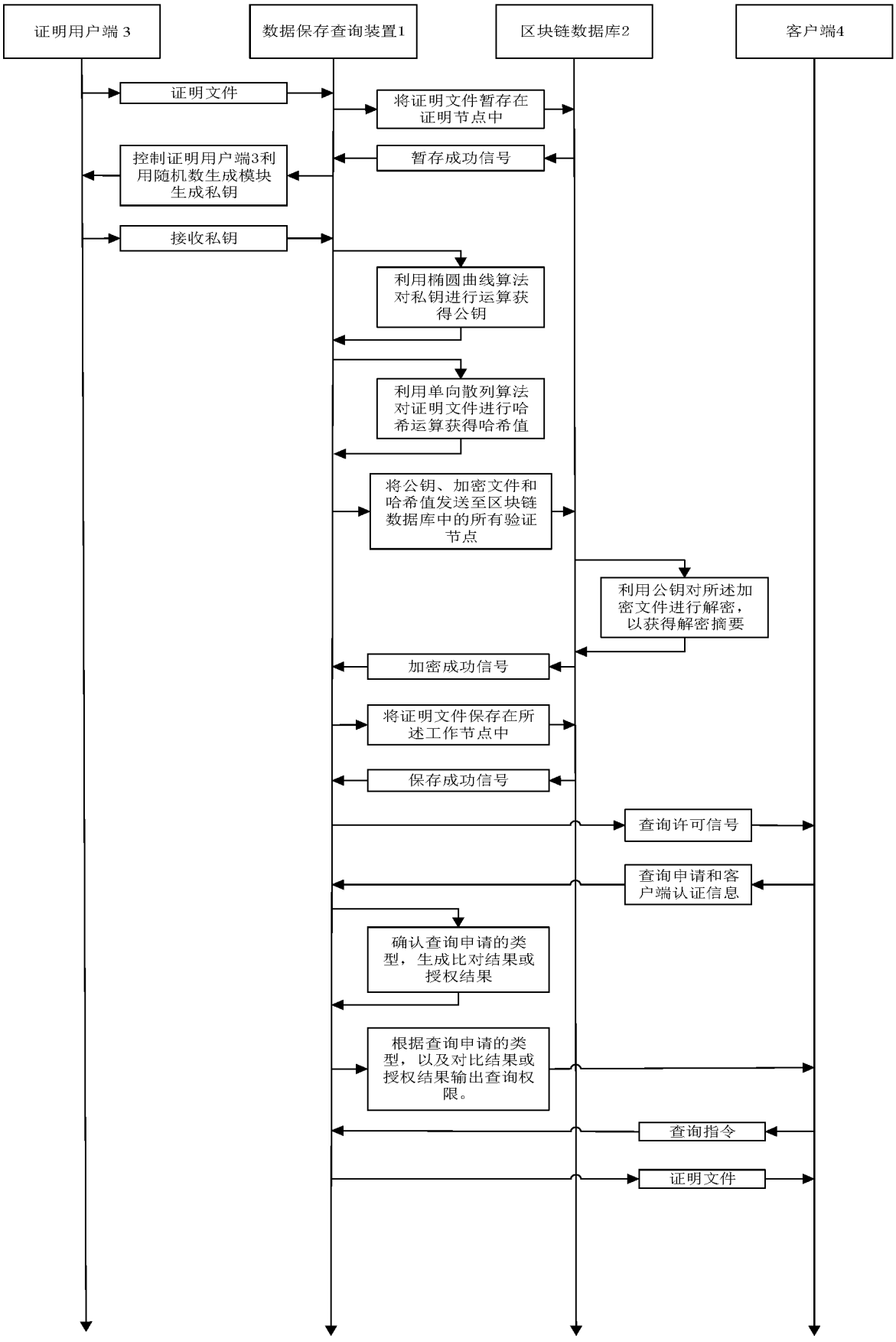
证明用户端 3
数据保存查询装置1
区块链数据库2
客户端4
证明文件
将证明文件暂存在证明节点中
暂存成功信号
控制证明用户端3利用随机数生成模块生成私钥
接收私钥
利用椭圆曲线算法对私钥进行运算获得公钥
利用单向散列算法对证明文件进行哈希运算获得哈希值
将公钥、加密文件和哈希值发送至区块链数据库中的所有验证节点
利用公钥对所述加密文件进行解密，以获得解密摘要
加密成功信号
将证明文件保存在所述工作节点中
保存成功信号
查询许可信号
查询申请和客户端认证信息
确认查询申请的类型，生成比对结果或授权结果
根据查询申请的类型，以及对比结果或授权结果输出查询权限。
查询指令
证明文件

图 2

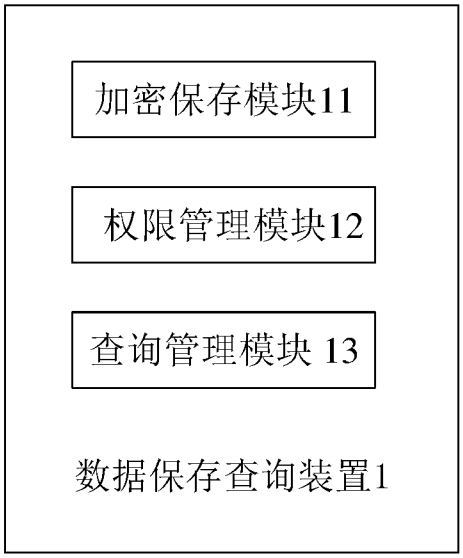

图 3

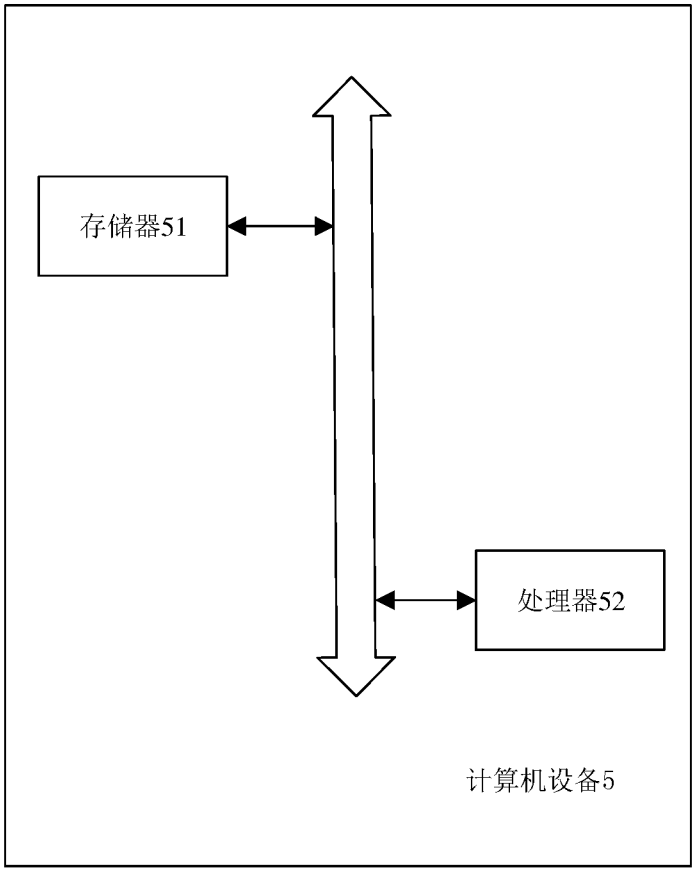

图 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/118073

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/60(2013.01)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)

G06F

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)

CNKI, WPI, EPODOC, CNPAT, IEEE: 区块链, 证书, 证明, 加密, 查询, 权限, 分级, 哈希, 公钥, 私钥, 密钥, 认证, blockchain, certificate, encrypt, query, classif+, hash, public key, private key, authentic+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 109886026 A (PING'AN TECHNOLOGY (SHENZHEN) CO., LTD.) 14 June 2019 (2019-06-14) claims 1-10	1-20
X	CN 108959457 A (BEIJING WENCHUANGYUAN INVESTMENT MANAGEMENT CO., LTD.) 07 December 2018 (2018-12-07) description, paragraphs [0024] and [0027]-[0037]	1-20
A	CN 108647523 A (SOUTH CHINA UNIVERSITY OF TECHNOLOGY) 12 October 2018 (2018-10-12) entire document	1-20
A	CN 106789875 A (SHENZHEN XINGUODU PAYMENT TECHNOLOGY CO., LTD.) 31 May 2017 (2017-05-31) 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	Date of mailing of the international search report
14 January 2020	**31 January 2020**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/118073

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 109886026 A	14 June 2019	None	
CN 108959457 A	07 December 2018	None	
CN 108647523 A	12 October 2018	None	
CN 106789875 A	31 May 2017	None	

国际检索报告

国际申请号
PCT/CN2019/118073

A. 主题的分类

G06F 21/60(2013.01)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)

G06F

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））

CNKI, WPI, EPODOC, CNPAT, IEEE:区块链，证书，证明，加密，查询，权限，分级，哈希，公钥，私钥，密钥，认证，blockchain, certificate, encrypt, query, classif+, hash, public key, private key, authentic+

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 109886026 A (平安科技深圳有限公司) 2019年 6月 14日 (2019-06-14) 权利要求1-10	1-20
X	CN 108959457 A (北京文创园投资管理有限公司) 2018年 12月 7日 (2018-12-07) 说明书第[0024], [0027]-[0037]段	1-20
A	CN 108647523 A (华南理工大学) 2018年 10月 12日 (2018-10-12) 全文	1-20
A	CN 106789875 A (深圳市新国都支付技术有限公司) 2017年 5月 31日 (2017-05-31) 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	国际检索报告邮寄日期
2020年 1月 14日	2020年 1月 31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 董刚 电话号码 86-(10)-53961348

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/118073

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 109886026 A	2019年 6月 14日	无	
CN 108959457 A	2018年 12月 7日	无	
CN 108647523 A	2018年 10月 12日	无	
CN 106789875 A	2017年 5月 31日	无	