(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 12 月 10 日 (10.12.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/244231 A1

(51) 国际专利分类号:
G06Q 50/18 (2012.01)

(21) 国际申请号: PCT/CN2020/071230

(22) 国际申请日: 2020 年 1 月 9 日 (09.01.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910478105.0 2019年6月3日 (03.06.2019) CN

(71) 申请人: 创新先进技术有限公司 (**ADVANCED NEW TECHNOLOGIES CO., LTD.**) [—/CN]; 开曼群岛大开曼岛乔治镇医院路27号开曼企业中心, Grand Cayman KY1-9008 (KY)。

(72) 发明人: **王振宇(WANG, Zhenyu)**; 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 **岳松波(YUE, Songbo)**; 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 **李楠(LI, Nan)**; 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 **晏宇(YAN, Yu)**; 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: 北京博思佳知识产权代理有限公司 (**BEIJING BESTIPR INTELLECTUAL PROPERTY LAW CORPORATION**); 中国北京市海淀区上地三街9号嘉华大厦B座409, Beijing 100085 (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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(54) **Title:** SERVICE PROCESSING SYSTEM AND METHOD BASED ON BLOCKCHAIN

(54) **发明名称:** 基于区块链的业务处理系统以及方法

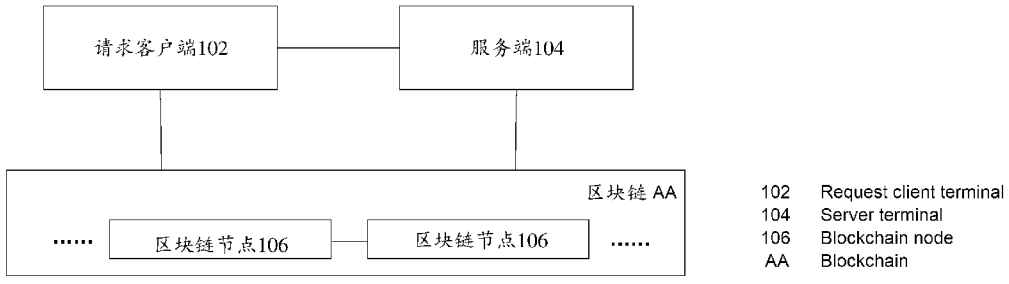

图 1

(57) **Abstract:** Provided are a service processing system and method based on blockchain. The service processing system based on blockchain comprises a request client terminal (102), a server terminal (104), and at least two blockchain nodes (106) on the blockchain. The request client terminal (102) is configured for sending a target file query request to the server terminal (104); the server terminal (104) is configured for receiving the target file query request (202), acquiring the target file, receiving a target file query by the user (204), and sending to the user prompt information about whether to upload the target file to the blockchain nodes (206), and if a target file uploading request by the user is received, the target file is uploaded to the blockchain nodes (208); and each blockchain node is configured for receiving the target file, storing the target file and returning a corresponding evidence storage hash value to the request client terminal (102).

WO 2020/244231 A1

[见续页]

(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：一种基于区块链的业务处理系统以及方法，其中所述基于区块链的业务处理系统包括：请求客户端（102）、服务端（104）以及区块链上的至少两个区块链节点（106）；请求客户端（102）被配置为向所述服务端（104）发送目标文件查询请求；服务端（104）被配置为接收所述目标文件查询请求（202），获取所述目标文件并接收所述用户进行目标文件查询（204），向所述用户发送是否将所述目标文件上传至区块链节点的提示信息（206），若接收到所述用户的目标文件上传请求，则将所述目标文件上传至所述区块链节点（208）；区块链节点被配置为接收所述目标文件，将所述目标文件进行存储并向所述请求客户端（102）返回对应的存证哈希值。

基于区块链的业务处理系统以及方法

技术领域

[01]本说明书涉及区块链技术领域，特别涉及一种基于区块链的业务处理系统。本说明书同时涉及一种基于区块链的业务处理方法以及装置，一种电子设备，以及一种计算机可读存储介质。

背景技术

[02]随着经济的发展，越来越多的理财产品随之出现，对于现有的理财项目而言，由于供应方和需求方之间存在多样的供应关系，使得整体结构错综复杂。

[03]传统的方法是在存在商业关系的双方通过签订纸质的商业合同来保障他们之间的商业关系。随着网络的发展，新的合约技术-电子合同逐渐被推广和使用。电子合同能够提高生产效率和安全性、缩短合同交易时间 、减少合同错误率、降低合同风险等等。

[04]然而，现有技术中仍然存在一些弊端，例如，目前用户缺乏有效的手段去核验电子合同是否被篡改。反之亦然，如果理财机构想证明自己未曾修改过某个电子合同的信息，需要事先对电子合同的信息进行公证。目前的举证方式主要是手工流程，如公证处公证，缺乏自动化手段，效率低，成本高，周期长，且电子合同涉及的信息难以得到全面的隐私保护。

发明内容

[05]有鉴于此，本说明书实施例提供了一种基于区块链的业务处理系统。本说明书同时涉及一种基于区块链的业务处理方法以及装置，一种电子设备，以及一种计算机可读存储介质，以解决现有技术中存在的技术缺陷。

[06]根据本说明书实施例的第一方面，提供了一种基于区块链的业务处理系统，包括:

[07]请求客户端、服务端以及区块链上的至少两个区块链节点;

[08]所述请求客户端，被配置为向所述服务端发送目标文件查询请求，所述目标文件查询请求中携带有用户的身份标识信息及所述目标文件标识信息;

[09]所述服务端，被配置为接收所述目标文件查询请求，获取所述目标文件并接收所述用户进行目标文件查询，向所述用户发送是否将所述目标文件上传至区块链节点的提示

信息,若接收到所述用户的目标文件上传请求,则将所述目标文件上传至所述区块链节点;

[10]所述区块链节点,被配置为接收所述目标文件,将所述目标文件进行存储并向所述请求客户端返回对应的存证哈希值。

[11]可选地,所述服务端,还被配置为:

[12]根据预设算法对所述目标文件进行哈希运算生成对应的数字摘要;采用非对称加密算法,对所述数字摘要进行私钥签名生成对应的数字签名,并将公钥、目标文件以及所述数字签名上传至所述区块链节点;

[13]所述区块链节点,还被配置为:接收所述公钥、目标文件以及所述数字签名,根据所述公钥以及数字签名对所述目标文件进行有效性验证;当所述目标文件的有效性验证成功后,将根据预设算法对所述目标文件进行哈希运算生成的数字摘要进行存储并向所述服务端返回对应的存证哈希值。

[14]可选地,所述服务端,还被配置为:

[15]为所述用户提供目标文件查询页面,在所述目标文件查询页面设置是否将所述目标文件上传至区块链节点的提示框,所述提示框中设置有可供所述用户进行点击操作的选项按钮,检测所述用户的选择结果,若所述用户的选择结果为确认上传,则将所述目标文件上传至所述区块链节点。

[16]可选地,所述请求客户端,还被配置为:向所述区块链节点发送目标文件摘要信息查询请求,所述目标文件摘要信息查询请求中携带有存证哈希值;

[17]所述区块链节点,还被配置为接收所述目标文件摘要信息查询请求,根据所述存证哈希值获取所述目标文件的文件摘要信息及目标文件的下载地址,并将所述目标文件摘要信息及所述目标文件的下载地址发送至所述请求客户端;

[18]所述请求客户端,还被配置为接收所述目标文件摘要信息及所述目标文件的下载地址,根据所述目标文件的下载地址下载所述目标文件。

[19]可选地,所述区块链节点,还被配置为:

[20]采用所述公钥对所述数字签名进行解密生成第一数字摘要,根据预设算法对所述目标文件进行哈希运算生成对应的第二数字摘要;比较所述第一数字摘要与所述第二数字摘要是否一致;若是,则所述目标文件的有效性验证成功;若否,则向所述服务端发送验证失败的提示信息。

[21]可选地，所述请求客户端，还被配置为：向所述服务端发送目标文件摘要信息查询请求，所述目标文件摘要信息查询请求中携带有目标文件标识信息；

[22]所述服务端，还被配置为接收所述目标文件摘要信息查询请求，根据所述目标文件标识信息确定是否存在对应的存证哈希值，若存在，则向所述请求客户端发送所述存证哈希值；

[23]所述请求客户端，还被配置为接收所述存证哈希值。

[24]可选地，所述服务端，还被配置为：

[25]若所述根据所述目标文件标识信息确定是否存在对应的存证哈希值的确定结果为不存在，则向所述请求客户端发送信息正在上传至区块链节点的提示信息。

[26]可选地，所述区块链节点，还被配置为：

[27]当所述目标文件的有效性验证成功后，向所述服务端及请求客户端分别返回已成功接收所述目标文件的数字摘要的调用结果；在所述目标文件的数字摘要存储完成后，向所述服务端返回对应的存证哈希值。

[28]可选地，所述请求客户端，还被配置为：

[29]接收所述服务端发起的协议签订交易；其中，所述协议签订交易用于触发对目标文件传输协议进行电子签名操作；响应于所述协议签订交易，执行电子签名操作，将签名后的目标文件传输协议发送至所述服务端；

[30]所述服务端，还被配置为接收所述请求客户端发送的签名后的目标文件传输协议，将所述目标文件传输协议、目标文件以及对所述目标文件进行哈希算法生成的数字签名发送至所述区块链节点。

[31]可选地，所述基于区块链的业务处理系统，还包括：第一业务端以及第二业务端；

[32]所述第一业务端，被配置为将文件模板上传至所述服务端；

[33]所述服务端，还被配置为接收所述文件模板，向所述第二业务端发送是否将所述文件模板上传至区块链节点的提示信息，所述提示信息中携带有文件模板标识信息；

[34]所述第二业务端，被配置为接收所述提示信息，基于所述提示信息确定选择结果并将携带有所述选择结果的信息发送至所述服务端；

[35]所述服务端，还被配置为接收所述第二业务端发送的携带有所述选择结果的信息，

若所述信息中携带的选择结果为确认上传，则将所述文件模板发送至所述区块链节点；

[36]所述区块链节点，还被配置为接收所述文件模板，将所述文件模板存储并返回写链成功的哈希值，将所述哈希值发送至所述服务端；

[37]所述服务端，被配置为接收所述哈希值并将所述哈希值保存于数据库。

[38]可选地，所述请求客户端，还被配置为向所述服务端发送项目加入请求，所述项目加入请求中携带有用户的身份标识信息以及项目标识信息；

[39]所述服务端，还被配置为接收所述项目加入请求，根据所述项目标识信息确定与所述项目相关联的文件模板以及项目详细信息；根据所述项目详细信息、用户的身份标识信息以及所述文件模板生成与所述项目相关的第一目标文件，向所述请求客户端发起文件签订交易；其中，所述文件签订交易用于触发对所述第一目标文件进行电子签名；

[40]所述请求客户端，还被配置为接收所述服务端发起的文件签订交易，响应于所述文件签订交易，对所述第一目标文件进行电子签名操作，将签名后的第二目标文件发送至所述服务端；

[41]所述服务端，还被配置为：接收所述第二目标文件，基于认证机构证书对所述第二目标文件进行认证签章操作。

[42]根据本说明书实施例的另一方面，提供了一种基于区块链的业务处理方法，包括：

[43]接收目标文件查询请求，所述目标文件查询请求中携带有用户的身份标识信息及目标文件标识信息；

[44]根据所述用户的身份标识信息及目标文件标识信息获取所述目标文件并接收所述用户进行目标文件查询；

[45]向所述用户发送是否将与所述目标文件上传至区块链节点的提示信息；

[46]若接收到所述用户的目标文件上传请求，则将所述目标文件上传至所述区块链节点。

[47]可选地，所述将所述目标文件上传至所述区块链节点包括：

[48]根据预设算法对所述目标文件进行哈希运算生成对应的数字摘要；采用非对称加密算法，对所述数字摘要进行私钥签名生成对应的数字签名，并将公钥、所述数字签名以及目标文件上传至所述区块链节点。

[49]可选地，所述将所述目标文件上传至所述区块链节点之后，还包括：

[50]接收由所述区块链节点返回的存证哈希值。

[51]可选地，所述向所述用户发送是否将与所述目标文件上传至区块链节点的提示信息包括:

[52]为所述用户提供目标文件查询页面，在所述目标文件查询页面设置是否将所述目标文件上传至区块链节点的提示框，所述提示框中设置有可供所述用户进行点击操作的选项按钮;

[53]检测所述用户的选择结果;

[54]所述若接收到所述用户的目标文件上传请求，则将所述目标文件上传至所述区块链节点，包括:

[55]若所述用户的选择结果为确认上传，则将所述目标文件上传至所述区块链节点。

[56]可选地，所述将所述目标文件上传至所述区块链节点之后，还包括:

[57]接收所述目标文件摘要信息查询请求，根据所述目标文件标识信息确定是否存在对应的存证哈希值;

[58]若存在，则向所述请求客户端发送所述存证哈希值;

[59]若不存在，则向所述请求客户端发送信息正在上传至区块链节点的提示信息。

[60]可选地，所述若接收到所述用户的目标文件上传请求，则将所述目标文件上传至所述区块链节点，包括:

[61]若接收到所述用户的目标文件上传请求，则向所述用户发起协议签订交易；其中，所述协议签订交易用于触发对目标文件传输协议进行电子签名操作;

[62]接收所述用户发送的签名后的目标文件传输协议，将所述目标文件传输协议、目标文件以及对所述目标文件进行哈希算法生成的数字签名发送至所述区块链节点。

[63]可选地，所述接收目标文件查询请求之前，还包括:

[64]接收文件模板，向所述第二业务端发送是否将所述文件模板上传至区块链节点的提示信息，所述提示信息中携带有文件模板标识信息;

[65]接收所述第二业务端发送的携带有所述选择结果的信息，在所述信息中携带的选择结果为确认上传时，将所述文件模板发送至所述区块链节点;

[66]接收由区块链节点返回的所述文件模板写链成功的哈希值并将所述哈希值保存于数

据库。

[67]根据本说明书实施例的另一方面，提供了一种基于区块链的业务处理装置，包括:

[68]文件查询请求接收模块，被配置为接收目标文件查询请求，所述目标文件查询请求中携带有用户的身份标识信息及目标文件标识信息;

[69]目标文件查询模块，被配置为根据所述用户的身份标识信息及目标文件标识信息获取所述目标文件并接收所述用户进行目标文件查询;

[70]提示信息发送模块，被配置为向所述用户发送是否将与所述目标文件上传至区块链节点的提示信息;

[71]目标文件传输模块，被配置为若接收到所述用户的目标文件上传请求，则将所述目标文件上传至所述区块链节点。

[72]根据本说明书实施例的另一方面，提供了一种电子设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机指令，所述处理器执行所述指令时实现所述基于区块链的业务处理方法的步骤。

[73]根据本说明书实施例的另一方面，提供了一种计算机可读存储介质，其存储有计算机指令，该指令被处理器执行时实现所述基于区块链的业务处理方法的步骤。

[74]本说明书实施例中，通过请求客户端向服务端发送目标文件查询请求，所述目标文件查询请求中携带有用户的身份标识信息及所述目标文件标识信息;服务端接收所述目标文件查询请求，获取所述目标文件并接收所述用户进行目标文件查询，向所述用户发送是否将所述目标文件上传至区块链节点的提示信息,若接收到所述用户的目标文件上传请求，则将所述目标文件上传至所述区块链节点;区块链节点接收所述目标文件，将所述目标文件进行存储并向所述请求客户端返回对应的存证哈希值。

[75]本说明书实施例中，通过将目标文件上传至区块链节点，利用区块链技术的去中心化以及公开透明等特点，区块链中的每个节点均可参与信息记录，任意节点的权利和义务都是均等的，一旦信息经过验证并添加至区块链，就会永久的存储起来，单个节点上对数据库的修改是无效的，因此利用区块链技术可有效提高目标文件中信息的稳定性和可靠性。

附图说明

[76]图 1 是本申请实施例提供的基于区块链的业务处理系统的示意图;

[77]图 2 是本申请实施例提供的基于区块链的业务处理方法的流程图;

[78]图 3 是本申请实施例提供的基于区块链的业务处理方法实现过程中的保单信息查询页面示意图;

[79]图 4 是本申请实施例提供的基于区块链的业务处理方法实现过程中的目标文件摘要信息查询页面示意图;

[80]图 5 是本申请实施例提供的基于区块链的业务处理方法的交互示意图;

[81]图 6 是本申请实施例提供的基于区块链的业务处理装置的结构示意图;

[82]图 7 是本申请实施例提供的电子设备的结构框图。

具体实施方式

[83]在下面的描述中阐述了很多具体细节以便于充分理解本申请。但是本申请能够以很多不同于在此描述的其它方式来实施，本领域技术人员可以在不违背本申请内涵的情况下做类似推广，因此本申请不受下面公开的具体实施的限制。

[84]在本说明书一个或多个实施例中使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本说明书一个或多个实施例。在本说明书一个或多个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。还应当理解，本说明书一个或多个实施例中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

[85]应当理解，尽管在本说明书一个或多个实施例中可能采用术语第一、第二等来描述各种信息，但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如，在不脱离本说明书一个或多个实施例范围的情况下，第一也可以被称为第二，类似地，第二也可以被称为第一。取决于语境，如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”。

[86]首先，对本发明一个或多个实施例涉及的名词术语进行解释。

[87]电子商务认证授权机构(Certificate Authority):简称为 CA，它是负责发放和管理数字

证书的权威机构，并作为电子商务交易中受信任的第三方，承担公钥体系中公钥的合法性检验的责任。

[88]本说明书实施例提供了一种基于区块链的业务处理系统。本说明书同时涉及一种基于区块链的业务处理方法以及装置，一种电子设备，以及一种计算机可读存储介质，在下面的实施例中逐一进行详细说明。

[89]图 1 示出了根据本说明书一实施例的基于区块链的业务处理系统的示意图，包括:

[90]请求客户端 102、服务端 104 以及区块链上的至少两个区块链节点 106。

[91]所述请求客户端 102，被配置为向所述服务端发送目标文件查询请求，所述目标文件查询请求中携带有用户的身份标识信息及所述目标文件标识信息;

[92]所述服务端 104，被配置为接收所述目标文件查询请求，获取所述目标文件并接收所述用户进行目标文件查询，向所述用户发送是否将所述目标文件上传至区块链节点的提示信息，若接收到所述用户的目标文件上传请求，则将所述目标文件上传至所述区块链节点;

[93]所述区块链节点 106，被配置为接收所述目标文件，将所述目标文件进行存储并向所述请求客户端返回对应的哈希值。

[94]本说明书提供的一个实施例中，所述服务端，还被配置为：根据预设算法对所述目标文件进行哈希运算生成对应的数字摘要；采用非对称加密算法，对所述数字摘要进行私钥签名生成对应的数字签名，并将公钥、目标文件以及所述数字签名上传至所述区块链节点;

[95]所述区块链节点，还被配置为：接收所述公钥、目标文件以及所述数字签名，根据所述公钥以及数字签名对所述目标文件进行有效性验证；当所述目标文件的有效性验证成功后，将根据预设算法对所述目标文件进行哈希运算生成的数字摘要进行存储并向所述服务端返回对应的存证哈希值。

[96]具体的，所述服务端，还被配置为:

[97]为所述用户提供目标文件查询页面，在所述目标文件查询页面设置是否将所述目标文件上传至区块链节点的提示框，所述提示框中设置有可供所述用户进行点击操作的选项按钮，检测所述用户的选择结果，若所述用户的选择结果为确认上传，则将所述目标文件上传至所述区块链节点。

[98]本说明书提供的一个实施例中，所述请求客户端，还被配置为：向所述区块链节点发送目标文件摘要信息查询请求，所述目标文件摘要信息查询请求中携带有存证哈希值；

[99]所述区块链节点，还被配置为接收所述目标文件摘要信息查询请求，根据所述存证哈希值获取所述目标文件的文件摘要信息及目标文件的下载地址，并将所述目标文件摘要信息及所述目标文件的下载地址发送至所述请求客户端；

[100] 所述请求客户端，还被配置为接收所述目标文件摘要信息及所述目标文件的下载地址，根据所述目标文件的下载地址下载所述目标文件。

[101] 具体的，所述区块链节点，还被配置为：

[102] 采用所述公钥对所述数字签名进行解密生成第一数字摘要，根据预设算法对所述目标文件进行哈希运算生成对应的第二数字摘要；比较所述第一数字摘要与所述第二数字摘要是否一致；若是，则所述目标文件的有效性验证成功；若否，则向所述服务端发送验证失败的提示信息。

[103] 除此之外，所述请求客户端，还被配置为：向所述服务端发送目标文件摘要信息查询请求，所述目标文件摘要信息查询请求中携带有目标文件标识信息；

[104] 所述服务端，还被配置为接收所述目标文件摘要信息查询请求，根据所述目标文件标识信息确定是否存在对应的存证哈希值，若存在，则向所述请求客户端发送所述存证哈希值；

[105] 所述请求客户端，还被配置为接收所述存证哈希值。

[106] 可选地，所述服务端，还被配置为：若所述根据所述目标文件标识信息确定是否存在对应的存证哈希值的确定结果为不存在，则向所述请求客户端发送信息正在上传至区块链节点的提示信息。

[107] 本说明书提供的一个实施例中，所述区块链节点，还被配置为：当所述目标文件的有效性验证成功后，向所述服务端及请求客户端分别返回已成功接收所述目标文件的数字摘要的调用结果；在所述目标文件的数字摘要存储完成后，向所述服务端返回对应的存证哈希值。

[108] 本说明书提供的一个实施例中，所述请求客户端，还被配置为：接收所述服务端发起的协议签订交易；其中，所述协议签订交易用于触发对目标文件传输协议进行电子签名操作；响应于所述协议签订交易，执行电子签名操作，将签名后的目标文件传输

协议发送至所述服务端；

[109] 所述服务端，还被配置为接收所述请求客户端发送的签名后的目标文件传输协议，将所述目标文件传输协议、目标文件以及对所述目标文件进行哈希算法生成的数字签名发送至所述区块链节点。

[110] 可选地，所述基于区块链的业务处理系统，还包括：第一业务端以及第二业务端；

[111] 所述第一业务端，被配置为将文件模板上传至所述服务端；

[112] 所述服务端，还被配置为接收所述文件模板，向所述第二业务端发送是否将所述文件模板上传至区块链节点的提示信息，所述提示信息中携带有文件模板标识信息；

[113] 所述第二业务端，被配置为接收所述提示信息，基于所述提示信息确定选择结果并将携带有所述选择结果的信息发送至所述服务端；

[114] 所述服务端，还被配置为接收所述第二业务端发送的携带有所述选择结果的信息，若所述信息中携带的选择结果为确认上传，则将所述文件模板发送至所述区块链节点；

[115] 所述区块链节点，还被配置为接收所述文件模板，将所述文件模板存储并返回写链成功的哈希值，将所述哈希值发送至所述服务端；

[116] 所述服务端，被配置为接收所述哈希值并将所述哈希值保存于数据库。

[117] 本说明书提供的一个实施例中，所述请求客户端，还被配置为向所述服务端发送项目加入请求，所述项目加入请求中携带有用户的身份标识信息以及项目标识信息；

[118] 所述服务端，还被配置为接收所述项目加入请求，根据所述项目标识信息确定与所述项目相关联的文件模板以及项目详细信息；根据所述项目详细信息、用户的身份标识信息以及所述文件模板生成与所述项目相关的第一目标文件，向所述请求客户端发起文件签订交易；其中，所述文件签订交易用于触发对所述第一目标文件进行电子签名；

[119] 所述请求客户端，还被配置为接收所述服务端发起的文件签订交易，响应于所述文件签订交易，对所述第一目标文件进行电子签名操作，将签名后的第二目标文件发送至所述服务端；

[120] 所述服务端，还被配置为：接收所述第二目标文件，基于认证机构证书对所述第二目标文件进行认证签章操作。

[121] 具体的，所述认证机构为电子商务认证授权机构，即基于 CA 证书对所述第二目标文件进行 CA 签章操作。

[122] 本说明书提供的一个实施例中，区块链技术因其数据不可篡改等特点非常适合用于目标文件的存证。通过与司法机构、法院以及公证处等机构组成联盟区块链来实现目标文件存证信息的共享。目标文件存证信息一旦写入区块链，即会自动同步到公证处数据服务器，区块链每个节点均保存了所有的目标文件存证信息，保证任意一个节点都无法随意修改数据。当用户与服务端间对于目标文件发生纠纷时，可以在公证处查证目标文件的真实性，从技术上保证了目标文件的不可篡性，提高了目标文件的可信度。

[123] 图 2 示出了根据本说明书一实施例的基于区块链的业务处理方法的流程图，包括步骤 202 至步骤 208。

[124] 步骤 202: 接收目标文件查询请求，所述目标文件查询请求中携带有用户的身份标识信息及目标文件标识信息。

[125] 本说明书提供的一个实施例中，接收目标文件查询请求之前，由第一业务端向所述服务端发送与项目相关的初始文件模板。具体的，所述项目包括保险项目、理财项目、互助共济项目、公益项目、医疗项目以及生活服务项目。服务端接收初始文件模板后，向第二业务端发送是否将所述初始文件模板上传至区块链的提示信息，所述提示信息中携带有文件模板标识信息；若接收到所述第二业务端发送的确定上传指示，则由服务端将所述初始文件模板上传至区块链节点；接收区块链节点返回的存储所述初始文件模板所生成的哈希值并将所述哈希值保存于数据库。

[126] 可选地，服务端将初始文件模板上传至区块链后，若需对所述初始模板进行改进，则将改进后的版本重新上传至区块链节点，并保存区块链节点返回的对应的哈希值。

[127] 本说明书提供的一个实施例中，服务端通过页面为用户展示项目详情，若用户有加入项目的意向，则由用户以及项目承办方共同签订生成所述目标文件。

[128] 具体的，目标文件的生成过程可以通过以下步骤实现:

[129] 请求客户端向服务端发送项目加入请求，所述项目加入请求中携带有用户的身份标识信息以及项目标识信息;

[130] 服务端接收所述项目加入请求，根据所述项目标识信息确定与所述项目相关联的文件模板以及项目详细信息；根据所述项目详细信息以及所述文件模板生成与所述项目相关的第一目标文件，向所述请求客户端发起文件签订交易；其中，所述文件签订交

易用于触发对所述第一目标文件进行电子签名；

[131] 请求客户端接收所述服务端发起的文件签订交易，响应于所述文件签订交易，对所述第一目标文件进行电子签名操作，并将签名后的第二目标文件发送至所述服务端；服务端接收所述第二目标文件，基于CA证书对所述第二目标文件进行CA签章操作生成所述目标文件。

[132] 可选地，服务端将预设时长内生成的一个或多个目标文件发送至第二业务端进行机构签章，所述第二业务端为项目经办方，第二业务端将签章后的文件批处理发送至服务端，服务端将文件进行存储。

[133] 以保险项目为例，用户向保险公司发送参保请求，所述参保请求中携带有用户的身份标识信息以及参保种类标识信息；假设用户的身份标识信息包括用户的姓名、年龄、性别以及身份证信息，参保种类标识信息为健康险种A。保险公司接收所述参保请求，根据所述参保种类标识信息确定与所述参保种类相关联的保单模板以及参保种类详细信息；根据所述参保种类详细信息、用户的身份标识信息以及所述保单模板生成与所述参保种类相关的第一保单。其中，将用户的身份标识信息及参保种类详细信息填入保单模板即生成第一保单。

[134] 生成第一保单后，保险公司向所述用户发起保单签订交易；其中，所述保单签订交易用于触发用户对所述第一保单进行电子签名。用户接收所述保单签订交易，对所述第一保单进行电子签名操作，并将签名后的第二保单发送至所述保险公司。保险公司接收所述第二保单，基于CA证书对所述第二保单进行CA签章操作生成最终的目标保单。

[135] 本说明书提供的一个实施例中，在目标文件签订成功后，若用户未保存该文件，可向服务端发送目标文件查询请求，所述目标文件查询请求中携带有所述用户的身份标识信息以及目标文件标识信息。

[136] 步骤204：根据所述用户的身份标识信息及目标文件标识信息获取所述目标文件并接收所述用户进行目标文件查询。

[137] 本说明书提供的一个实施例中，服务端接收所述目标文件查询请求后，根据所述用户的身份标识信息在数据库中查询与所述用户相关的文件，再根据目标文件标识信息在与所述用户相关的文件中查询所述目标文件。

[138] 可选地，若服务端根据所述用户的身份标识信息未在数据库中查询到与所述用

户相关的文件，则向用户展示项目产品详情界面。

[139] 步骤 206: 向所述用户发送是否将与所述目标文件上传至区块链节点的提示信息。

[140] 具体的，若服务端根据目标文件标识信息在所述用户相关的文件中查询到所述目标文件，则为所述用户提供目标文件查询页面，在所述目标文件查询页面设置是否将所述目标文件上传至区块链节点的提示框，所述提示框中设置有可供所述用户进行点击操作的选项按钮；服务端检测所述用户在所述提示框的选择结果并根据选择结果进行后续操作。

[141] 以用户所加入的项目为保险项目为例，服务端即为保险公司，所述目标文件即为保单信息，保险公司向用户提供的保单信息查询页面示意图如图 3 所示，在检测到用户正在查看目标文件的情况下，在交互界面上弹出选项窗口，以提示用户选择对应的图标以进行下一步操作。其中，如图 3 所示，弹出的选项窗口中的内容为“是否将目标文件上传至区块链？”，并且设置两个可点击按钮，分别为“是”和“否”，若监测到用户点击的按钮为“是”，则将所述保单信息上传至所述区块链节点。

[142] 可选地，所述是否将所述目标文件上传至区块链节点的提示框还可设置在资产详情查询界面，以理财项目为例，用户购买理财产品后，若检测到用户正在查看所购买的理财产品详情，则弹出是否将所述目标文件上传至区块链节点的提示框，并检测用户在所述提示框的选择结果，根据用户的选择结果进行后续操作。

[143] 步骤 208: 若接收到所述用户的目标文件上传请求，则将所述目标文件上传至所述区块链节点。

[144] 具体的，若所述用户的选择结果为确认上传，则将所述目标文件上传至所述区块链节点。

[145] 可选地，服务端接收到所述用户的目标文件上传请求后，向所述用户发起协议签订交易；其中，所述协议签订交易用于触发对目标文件传输协议进行电子签名操作；用户接收所述服务端发起的协议签订交易，执行电子签名程序以响应所述协议签订交易，并将签名后的目标文件传输协议发送至所述服务端。

[146] 服务端接收所述用户发送的签名后的目标文件传输协议，将所述目标文件传输协议、目标文件以及对所述目标文件进行哈希算法生成的数字签名发送至所述区块链节点，除此之外，服务端向区块链节点发送的信息还包括：所述目标文件的签订时间以及与所述项目相关联的文件模板对应的哈希值。

[147] 仍以用户加入的项目为保险项目为例，保险公司接收到用户的保单文件上传请求后，与用户共同签订用户与区块链主体协议，协议签订成功后，由保险公司将保单文件以及对所述保单文件进行哈希算法生成的数字签名发送至区块链节点，除此之外，保险公司向区块链节点发送的信息还包括：所述保单文件的签订时间、用户与保险公司共同签订的主体协议以及所述用户所签保单的保单模板对应的哈希值。

[148] 由于服务端在将初始文件模板上传至区块链后，若需对所述初始模板进行改进，则将改进后的版本重新上传至区块链节点，并保存区块链节点返回的对应的哈希值，因此，服务端将与用户所签保单的保单模板对应的哈希值与保单文件一起上传至区块链，使得用户在后期查询保单信息的同时还可追溯保单模板的版本，能够为用户带来更好的服务体验。

[149] 本说明书提供的一个实施例中，区块链技术也被称之为分布式账本技术，是一种由若干台设备共同参与“记账”，共同维护一份完整的分布式数据库的新兴技术。由于区块链技术具有去中心化、公开透明、每台设备可以参与数据库记录、并且各设备之间可以快速的进行数据同步的特性，使得区块链技术已在众多的领域中广泛的进行应用。本说明书实施例中涉及的区块链节点包括接入所述区块链的业务相关设备机构节点、互联网平台的服务设备、监管机构的设备、请求客户端的服务设备、公证处的服务设备、法院的服务设备以及司法鉴定中心的服务设备。

[150] 具体的，将所述目标文件上传至所述区块链节点可以通过以下步骤实现：

[151] 根据预设算法对所述目标文件进行哈希运算生成对应的数字摘要；

[152] 采用非对称加密算法，对所述数字摘要进行私钥签名生成对应的数字签名，并将公钥、所述数字签名以及目标文件上传至所述区块链节点。

[153] 区块链节点接收所述公钥、目标文件以及所述数字签名后，还需对目标文件进行有效性验证，具体的，目标文件的有效性验证可通过以下步骤实现：

[154] 采用所述公钥对所述数字签名进行解密生成第一数字摘要；

[155] 根据预设算法对所述目标文件进行哈希运算生成对应的第二数字摘要；

[156] 比较所述第一数字摘要与所述第二数字摘要是否一致；

[157] 若是，则所述目标文件的有效性验证成功；

[158] 若否，则向所述服务端发送验证失败的提示信息。

[159] 具体的，当所述目标文件的有效性验证成功后，区块链节点将根据预设算法对所述目标文件哈希运算生成的数字摘要进行存储并向所述服务端返回对应的存证哈希值。

[160] 本说明书提供的一个实施例中，用户签订目标文件传输协议后，可向服务端发送目标文件摘要信息查询请求，服务端接收所述目标文件摘要信息查询请求，根据所述目标文件标识信息确定是否存在对应的存证哈希值，若是，则向所述请求客户端发送所述存证哈希值；若否，则向所述请求客户端发送信息正在上传至区块链节点的提示信息。

[161] 请求客户端接收到存证哈希值后，向区块链节点发送目标文件摘要信息查询请求，所述目标文件摘要信息查询请求中携带有存证哈希值；区块链节点接收所述目标文件摘要信息查询请求，根据所述存证哈希值获取所述目标文件的文件摘要信息及目标文件的下载地址，并将所述目标文件摘要信息及所述目标文件的下载地址发送至所述请求客户端；请求客户端接收所述目标文件摘要信息及所述目标文件的下载地址，根据所述目标文件的下载地址下载所述目标文件。

[162] 实际应用中，区块链节点为用户提供目标文件摘要信息查询页面，具体的，区块链节点为用户提供的目标文件摘要信息查询页面示意图如图 4 所示，在检测到用户点击存证哈希值的情况下，在交互界面弹出信息查询页面，该页面显示目标文件摘要信息以及目标文件的下载地址，若监测到用户点击目标文件的下载地址，则将为用户下载目标文件。

[163] 本说明书实施例中，区块链中的目标文件可存储于本地存储空间，也可存储于区块链外的其他存储空间，在此不做限制。另外，本说明书实施例仅以图 4 中的目标文件摘要信息为 CXHK WDCQ RJHS KIYV 以及目标文件的下载地址为 https://abcd.ef/mnopqrstuv/为例进行示意性说明，具体的目标文件摘要信息以及目标文件的下载地址根据实际应用确定，在此不做限制。

[164] 仍以保险项目为例，区块链节点为用户提供保单摘要信息查询页面，在将根据预设算法对所述目标文件哈希运算生成的数字摘要进行存储完成后，在交互界面显示对应的存证哈希值，用户点击交互界面显示的存证哈希值即可获取保单文件的文件摘要信息及保单文件的下载地址，用户可自行选择是否下载所述保单文件。

[165] 本说明书提供的一个实施例中，由于区块链使用分布式核算和存储，不存在中心化的硬件或管理机构， 并且司法链上存储的是目标文件的数字摘要，数字摘要算法

的数学原理保证了无法由数字摘要反向生成目标文件，因此用户隐私得到了保护，在确保用户隐私的前提下，实现目标文件的透明、不可篡改，并且用户可通过区块链节点提供的目标文件下载地址下载所述目标文件，使得用户获取目标文件的方式更加便捷。

[166] 图 5 示出了本说明书一实施例的基于区块链的业务处理方法的交互示意图，该基于区块链的业务处理方法以对理财项目为例进行描述，包括步骤 502 至步骤 522。

[167] 步骤 502：请求客户端向服务端发送理财合同查询请求。

[168] 本说明书提供的一个实施例中，所述理财合同查询请求中携带有用户的身份标识信息及所述理财合同标识信息。

[169] 可选地，接收理财合同查询请求之前，由第一业务端及合同模板生成端向理财机构发送与理财产品相关的初始理财合同模板，理财机构接收初始理财合同模板后，向第二业务端即理财项目经办方发送是否将所述初始理财合同模板上传至区块链的提示信息，所述提示信息中携带有初始理财合同模板标识信息；若接收到所述理财项目经办方发送的确定上传指示，则由理财机构将所述初始理财合同模板上传至区块链节点；接收区块链节点返回的存储所述初始理财合同模板所生成的哈希值并将所述哈希值保存于数据库。

[170] 此外，服务端将初始文件模板上传至区块链后，若需对所述初始模板进行改进，则将改进后的版本重新上传至区块链节点，并保存区块链节点返回的对应的哈希值。

[171] 理财机构通过页面为用户展示理财产品详情，若用户有购买理财产品的意向，则由用户以及理财项目经办方共同签订生成所述理财合同。

[172] 可选地，理财机构将预设时长内生成的一个或多个理财合同发送至理财项目经办方进行机构签章，理财项目经办方将签章后的理财合同批处理发送至理财机构，理财机构将接收到的理财合同进行存储。

[173] 以预设时长为 1 个工作日为例，理财机构将 1 个工作日内生成的 M 个理财合同发送至理财项目经办方进行机构签章，其中，M 为大于等于 0 的整数。理财项目经办方将签章后的 M 个理财合同批处理发送至理财机构，理财机构将接收到的 M 个理财合同进行存储。

[174] 仍以理财项目为例，用户向理财机构发送理财产品购买请求，所述理财产品购买请求中携带有用户的身份标识信息以及理财产品标识信息；假设用户的身份标识信息包括用户的姓名、年龄、性别以及身份证信息，理财产品标识信息为产品 B。理财机构

接收所述理财产品购买请求，根据所述理财产品标识信息确定与所述理财产品相关联的理财合同模板以及理财产品详细信息；根据所述理财产品详细信息、用户的身份标识信息以及所述理财合同模板生成与所述理财产品种类相关的第一理财合同。其中，将用户的身份标识信息及理财产品详细信息填入理财合同模板即生成第一理财合同。

[175] 生成第一理财合同后，理财机构向所述用户发起理财合同签订交易；其中，所述理财合同签订交易用于触发用户对所述第一理财合同进行电子签名。用户接收所述理财合同签订交易，对所述第一理财合同进行电子签名操作，并将签名后的第二理财合同发送至所述理财机构。理财机构接收所述第二理财合同，基于CA证书对所述第二理财合同进行CA签章操作生成最终的理财合同。

[176] 本说明书提供的一个实施例中，在理财合同签订成功后，若用户未保存该合同，可向理财机构发送理财合同查询请求，所述理财合同查询请求中携带有所述用户的身份标识信息以及理财合同标识信息。

[177] 步骤504：服务端接收所述理财合同查询请求，获取所述理财合同。

[178] 本说明书提供的一个实施例中，理财机构接收所述理财合同查询请求后，根据所述用户的身份标识信息在数据库中查询与所述用户相关的合同，再根据理财合同标识信息在与所述用户相关的合同中查询所述理财合同。

[179] 可选地，若理财机构根据所述用户的身份标识信息未在数据库中查询到与所述用户相关的合同，则向用户展示理财产品详情界面。

[180] 步骤506：服务端接收用户进行理财合同查询。

[181] 步骤508：服务端向所述用户发送是否将所述理财合同上传至区块链节点的提示信息。

[182] 步骤510：服务端接收用户发送的理财合同上传请求。

[183] 具体的，具体的，若理财机构根据理财合同标识信息在所述用户相关的文件中查询到所述理财合同，则为所述用户提供理财合同查询页面，在所述理财合同查询页面设置是否将所述理财合同上传至区块链节点的提示框，所述提示框中设置有可供所述用户进行点击操作的选项按钮；理财机构检测所述用户在所述提示框的选择结果并根据选择结果进行后续操作。

[184] 步骤512：服务端将理财合同上传至区块链节点。

[185] 具体的，若所述用户的选择结果为确认上传，则将所述目标文件上传至所述区块链节点。

[186] 可选地，理财机构接收到所述用户的理财合同上传请求后，向所述用户发起协议签订交易；其中，所述协议签订交易用于触发对理财合同传输协议进行电子签名操作；用户接收所述理财机构发起的协议签订交易，执行电子签名程序以响应所述协议签订交易，并将签名后的理财合同传输协议发送至所述理财机构。

[187] 理财机构接收所述用户发送的签名后的理财合同传输协议，将所述理财合同传输协议、理财合同以及对所述理财合同进行哈希算法生成的数字签名发送至所述区块链节点，除此之外，理财机构向区块链节点发送的信息还包括：所述理财合同的签订时间以及与所述理财产品相关联的理财合同模板对应的哈希值。

[188] 具体的，将所述目标文件上传至所述区块链节点可以通过以下步骤实现：

[189] 根据预设算法对所述目标文件进行哈希运算生成对应的数字摘要；

[190] 采用非对称加密算法，对所述数字摘要进行私钥签名生成对应的数字签名，并将公钥、所述数字签名以及目标文件上传至所述区块链节点。

[191] 区块链节点接收所述公钥、目标文件以及所述数字签名后，还需对目标文件进行有效性验证，具体的，目标文件的有效性验证可通过以下步骤实现：

[192] 采用所述公钥对所述数字签名进行解密生成第一数字摘要；

[193] 根据预设算法对所述目标文件进行哈希运算生成对应的第二数字摘要；

[194] 比较所述第一数字摘要与所述第二数字摘要是否一致；

[195] 若是，则所述目标文件的有效性验证成功；

[196] 若否，则向所述服务端发送验证失败的提示信息。

[197] 具体的，当所述目标文件的有效性验证成功后，区块链节点将根据预设算法对所述目标文件哈希运算生成的数字摘要进行存储并向所述服务端返回对应的存证哈希值。

[198] 可选地，区块链节点接收目标文件后，对目标文件进行有效性验证，当所述目标文件的有效性验证成功后，向所述服务端及请求客户端分别返回已成功接收所述目标文件的数字摘要的调用结果；在所述目标文件的数字摘要存储完成后，向所述服务端返回对应的存证哈希值。

[199] 步骤 514：区块链节点向服务端返回存证哈希值。

[200] 步骤 516：请求客户端向服务端发送摘要查询请求。

[201] 步骤 518：服务端向请求客户端返回存证哈希值。

[202] 本说明书提供的一个实施例中，用户签订目标文件传输协议后，可向服务端发送目标文件摘要信息查询请求，服务端接收所述目标文件摘要信息查询请求，根据所述目标文件标识信息确定是否存在对应的存证哈希值，若存在，则向所述请求客户端发送所述存证哈希值；

[203] 若所述根据所述目标文件标识信息确定是否存在对应的存证哈希值的确定结果为不存在，则向所述请求客户端发送信息正在上传至区块链节点的提示信息。

[204] 步骤 520：请求客户端向区块链节点发送摘要信息查询请求。

[205] 步骤 522：区块链节点向请求客户端发送摘要信息及目标文件下载地址。

[206] 本说明书提供的一个实施例中，请求客户端接收到存证哈希值后，向区块链节点发送目标文件摘要信息查询请求，所述目标文件摘要信息查询请求中携带有存证哈希值；区块链节点接收所述目标文件摘要信息查询请求，根据所述存证哈希值获取所述目标文件的文件摘要信息及目标文件的下载地址，并将所述目标文件摘要信息及所述目标文件的下载地址发送至所述请求客户端；请求客户端接收所述目标文件摘要信息及所述目标文件的下载地址，根据所述目标文件的下载地址下载所述目标文件。

[207] 本说明书提供的一个实施例中，由于区块链使用分布式核算和存储，不存在中心化的硬件或管理机构，并且司法链上存储的是理财合同的数字摘要，数字摘要算法的数学原理保证了无法由数字摘要反向生成理财合同，因此用户隐私得到了保护，同时也保证了理财合同的不可篡改，并且用户可通过区块链节点提供的合同下载地址下载所述理财合同，使得用户获取理财合同的方式更加便捷。

[208] 与上述方法实施例相对应，本说明书还提供了基于区块链的业务处理装置实施例，图 6 示出了本说明书一个实施例的基于区块链的业务处理装置的结构示意图。如图 6 所示，该装置包括：文件查询请求接收模块 602、目标文件查询模块 604、提示信息发送模块 606 以及目标文件传输模块 608。

[209] 文件查询请求接收模块 602，被配置为接收目标文件查询请求，所述目标文件查询请求中携带有用户的身份标识信息及目标文件标识信息；

[210] 目标文件查询模块604，被配置为根据所述用户的身份标识信息及目标文件标识信息获取所述目标文件并接收所述用户进行目标文件查询；

[211] 提示信息发送模块606，被配置为向所述用户发送是否将与所述目标文件上传至区块链节点的提示信息；

[212] 目标文件传输模块608，被配置为若接收到所述用户的目标文件上传请求，则将所述目标文件上传至所述区块链节点。

[213] 具体的，所述目标文件传输模块，还被配置为：根据预设算法对所述目标文件进行哈希运算生成对应的数字摘要；采用非对称加密算法，对所述数字摘要进行私钥签名生成对应的数字签名，并将公钥、所述数字签名以及目标文件上传至所述区块链节点。

[214] 可选地，所述基于区块链的业务处理装置，还包括：

[215] 存证哈希值接收模块，被配置为接收由所述区块链节点返回的存证哈希值。

[216] 可选地，所述提示信息发送模块，还被配置为：为所述用户提供目标文件查询页面，在所述目标文件查询页面设置是否将所述目标文件上传至区块链节点的提示框，所述提示框中设置有可供所述用户进行点击操作的选项按钮；检测所述用户的选择结果；

[217] 所述目标文件传输模块，还被配置为：

[218] 若所述用户的选择结果为确认上传，则将所述目标文件上传至所述区块链节点。

[219] 可选地，所述基于区块链的业务处理装置，还包括：目标文件摘要信息查询请求接收模块，被配置为：

[220] 接收所述目标文件摘要信息查询请求，根据所述目标文件标识信息确定是否存在对应的存证哈希值；若存在，则向所述请求客户端发送所述存证哈希值；

[221] 若不存在，则向所述请求客户端发送信息正在上传至区块链节点的提示信息。

[222] 可选地，所述目标文件传输模块，还被配置为：

[223] 若接收到所述用户的目标文件上传请求，则向所述用户发起协议签订交易；其中，所述协议签订交易用于触发对目标文件传输协议进行电子签名操作；

[224] 接收所述用户发送的签名后的目标文件传输协议，将所述目标文件传输协议、目标文件以及对所述目标文件进行哈希算法生成的数字签名发送至所述区块链节点。

[225] 可选地，所述基于区块链的业务处理装置，还包括：

[226] 文件模板传输提示信息发送模块，被配置为接收文件模板，向所述第二业务端发送是否将所述文件模板上传至区块链节点的提示信息，所述提示信息中携带有文件模板标识信息；

[227] 选择结果接收模块，被配置为接收所述第二业务端发送的携带有所述选择结果的信息，在所述信息中携带的选择结果为确认上传时，将所述文件模板发送至所述区块链节点；

[228] 存储模块，被配置为接收由区块链节点返回的所述文件模板写链成功的哈希值并将所述哈希值保存于数据库。

[229] 本说明书提供的一个实施例中，区块链技术因其数据不可篡改等特点非常适合用于目标文件的存证。我们通过与司法机构、法院以及公证处等机构组成联盟区块链来实现目标文件存证信息的共享。目标文件存证信息一旦写入区块链，即会自动同步到公证处数据服务器，区块链每个节点均保存了所有的目标文件存证信息，保证任意一个节点都无法随意修改数据。当用户与服务端间对于目标文件发生纠纷时，可以在公证处查证目标文件的真实性，从技术上保证了目标文件的不可篡性，提高了目标文件的可信度。

[230] 图 7 示出了根据本说明书一实施例的电子设备 700 的结构框图。该电子设备 700 的部件包括但不限于存储器 710 和处理器 720。处理器 720 与存储器 710 通过总线 730 相连接，数据库 750 用于保存数据。

[231] 电子设备 700 还包括接入设备 740，接入设备 740 使得电子设备 700 能够经由一个或多个网络 760 通信。这些网络的示例包括公用交换电话网（PSTN）、局域网（LAN）、广域网（WAN）、个域网（PAN）或诸如因特网的通信网络的组合。接入设备 740 可以包括有线或无线的任何类型的网络接口（例如，网络接口卡（NIC））中的一个或多个，诸如 IEEE802.11 无线局域网（WLAN）无线接口、全球微波互联接入（Wi-MAX）接口、以太网接口、通用串行总线（USB）接口、蜂窝网络接口、蓝牙接口、近场通信（NFC）接口，等等。

[232] 在本说明书的一个实施例中，电子设备 700 的上述部件以及图 7 中未示出的其他部件也可以彼此相连接，例如通过总线。应当理解，图 7 所示的电子设备结构框图仅仅是出于示例的目的，而不是对本说明书范围的限制。本领域技术人员可以根据需要，增添或替换其他部件。

[233] 电子设备 700 可以是任何类型的静止或移动电子设备，包括移动计算机或移动

电子设备（例如，平板计算机、个人数字助理、膝上型计算机、笔记本计算机、上网本等）、移动电话（例如，智能手机）、可佩戴的电子设备（例如，智能手表、智能眼镜等）或其他类型的移动设备，或者诸如台式计算机或 PC 的静止电子设备。电子设备 700 还可以是移动式或静止式的服务器。

[234] 其中，处理器 720 用于执行该指令被处理器执行时实现如前所述基于区块链的业务处理方法的步骤。

[235] 上述为本实施例的一种电子设备的示意性方案。需要说明的是，该电子设备的技术方案与上述的基于区块链的业务处理方法的技术方案属于同一构思，电子设备的技术方案未详细描述的细节内容，均可以参见上述基于区块链的业务处理方法的技术方案的描述。

[236] 本说明书一实施例还提供一种计算机可读存储介质，其存储有计算机指令，该指令被处理器执行时实现如前所述基于区块链的业务处理方法的步骤。

[237] 上述为本实施例的一种计算机可读存储介质的示意性方案。需要说明的是，该存储介质的技术方案与上述的基于区块链的业务处理方法的技术方案属于同一构思，存储介质的技术方案未详细描述的细节内容，均可以参见上述基于区块链的业务处理方法的技术方案的描述。

[238] 上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的 范围内。在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者可能是有利的。

[239] 所述计算机指令包括计算机程序代码，所述计算机程序代码可以为源代码形式、对象代码形式、可执行文件或某些中间形式等。所述计算机可读介质可以包括：能够携带所述计算机程序代码的任何实体或装置、记录介质、U 盘、移动硬盘、磁碟、光盘、计算机存储器、只读存储器（ROM，Read-Only Memory）、随机存取存储器（RAM，Random Access Memory）、电载波信号、电信信号以及软件分发介质等。需要说明的是，所述计算机可读介质包含的内容可以根据司法管辖区内立法和专利实践的要求进行适当的增减，例如在某些司法管辖区，根据立法和专利实践，计算机可读介质不包括电载波信号和电信信号。

[240] 需要说明的是，对于前述的各方法实施例，为了简便描述，故将其都表述为一系列的动作组合，但是本领域技术人员应该知悉，本申请并不受所描述的动作顺序的限制，因为依据本申请，某些步骤可以采用其它顺序或者同时进行。其次，本领域技术人员也应该知悉，说明书中所描述的实施例均属于优选实施例，所涉及的动作和模块并不一定都是本申请所必须的。

[241] 在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述的部分，可以参见其它实施例的相关描述。

[242] 以上公开的本申请优选实施例只是用于帮助阐述本申请。可选实施例并没有详尽叙述所有的细节，也不限制该发明仅为所述的具体实施方式。显然，根据本说明书的内容，可作很多的修改和变化。本说明书选取并具体描述这些实施例，是为了更好地解释本申请的原理和实际应用，从而使所属技术领域技术人员能很好地理解和利用本申请。本申请仅受权利要求书及其全部范围和等效物的限制。

权利要求书

1、一种基于区块链的业务处理系统，其特征在于，包括:

请求客户端、服务端以及区块链上的至少两个区块链节点;

所述请求客户端，被配置为向所述服务端发送目标文件查询请求，所述目标文件查询请求中携带有用户的身份标识信息及所述目标文件标识信息;

所述服务端，被配置为接收所述目标文件查询请求，获取所述目标文件并接收所述用户进行目标文件查询，向所述用户发送是否将所述目标文件上传至区块链节点的提示信息,若接收到所述用户的目标文件上传请求,则将所述目标文件上传至所述区块链节点;

所述区块链节点，被配置为接收所述目标文件，将所述目标文件进行存储并向所述请求客户端返回对应的存证哈希值。

2、根据权利要求 1 所述的系统，其特征在于，所述服务端，还被配置为:

根据预设算法对所述目标文件进行哈希运算生成对应的数字摘要; 采用非对称加密算法，对所述数字摘要进行私钥签名生成对应的数字签名，并将公钥、目标文件以及所述数字签名上传至所述区块链节点;

所述区块链节点，还被配置为: 接收所述公钥、目标文件以及所述数字签名，根据所述公钥以及数字签名对所述目标文件进行有效性验证; 当所述目标文件的有效性验证成功后，将根据预设算法对所述目标文件进行哈希运算生成的数字摘要进行存储并向所述服务端返回对应的存证哈希值。

3、根据权利要求 1 所述的系统，其特征在于，所述服务端，还被配置为:

为所述用户提供目标文件查询页面，在所述目标文件查询页面设置是否将所述目标文件上传至区块链节点的提示框，所述提示框中设置有可供所述用户进行点击操作的选项按钮，检测所述用户的选择结果，若所述用户的选择结果为确认上传，则将所述目标文件上传至所述区块链节点。

4、根据权利要求 2 所述的系统，其特征在于，

所述请求客户端，还被配置为: 向所述区块链节点发送目标文件摘要信息查询请求，所述目标文件摘要信息查询请求中携带有存证哈希值;

所述区块链节点，还被配置为接收所述目标文件摘要信息查询请求，根据所述存证哈希值获取所述目标文件的文件摘要信息及目标文件的下载地址，并将所述目标文件摘要信息及所述目标文件的下载地址发送至所述请求客户端;

所述请求客户端，还被配置为接收所述目标文件摘要信息及所述目标文件的下载地址，根据所述目标文件的下载地址下载所述目标文件。

5、根据权利要求 2 所述的系统，其特征在于，所述区块链节点，还被配置为：

采用所述公钥对所述数字签名进行解密生成第一数字摘要，根据预设算法对所述目标文件进行哈希运算生成对应的第二数字摘要；比较所述第一数字摘要与所述第二数字摘要是否一致；若是，则所述目标文件的有效性验证成功；若否，则向所述服务端发送验证失败的提示信息。

6、根据权利要求 1 所述的系统，其特征在于，

所述请求客户端，还被配置为：向所述服务端发送目标文件摘要信息查询请求，所述目标文件摘要信息查询请求中携带有目标文件标识信息；

所述服务端，还被配置为接收所述目标文件摘要信息查询请求，根据所述目标文件标识信息确定是否存在对应的存证哈希值，若存在，则向所述请求客户端发送所述存证哈希值；

所述请求客户端，还被配置为接收所述存证哈希值。

7、根据权利要求 6 所述的系统，其特征在于，所述服务端，还被配置为：

若所述根据所述目标文件标识信息确定是否存在对应的存证哈希值的确定结果为不存在，则向所述请求客户端发送信息正在上传至区块链节点的提示信息。

8、根据权利要求 2 所述的系统，其特征在于，所述区块链节点，还被配置为：

当所述目标文件的有效性验证成功后，向所述服务端及请求客户端分别返回已成功接收所述目标文件的数字摘要的调用结果；在所述目标文件的数字摘要存储完成后，向所述服务端返回对应的存证哈希值。

9、根据权利要求 1 所述的系统，其特征在于，所述请求客户端，还被配置为：

接收所述服务端发起的协议签订交易；其中，所述协议签订交易用于触发对目标文件传输协议进行电子签名操作；响应于所述协议签订交易，执行电子签名操作，将签名后的目标文件传输协议发送至所述服务端；

所述服务端，还被配置为接收所述请求客户端发送的签名后的目标文件传输协议，将所述目标文件传输协议、目标文件以及对所述目标文件进行哈希算法生成的数字签名发送至所述区块链节点。

10、根据权利要求 1 所述的系统，其特征在于，还包括：第一业务端以及第二业务端；

所述第一业务端，被配置为将文件模板上传至所述服务端；

所述服务端，还被配置为接收所述文件模板，向所述第二业务端发送是否将所述文件模板上传至区块链节点的提示信息，所述提示信息中携带有文件模板标识信息；

所述第二业务端，被配置为接收所述提示信息，基于所述提示信息确定选择结果开将携带有所述选择结果的信息发送至所述服务端；

所述服务端，还被配置为接收所述第二业务端发送的携带有所述选择结果的信息，若所述信息中携带的选择结果为确认上传，则将所述文件模板发送至所述区块链节点；

所述区块链节点，还被配置为接收所述文件模板，将所述文件模板存储并返回写链成功的哈希值，将所述哈希值发送至所述服务端；

所述服务端，被配置为接收所述哈希值并将所述哈希值保存于数据库。

11、根据权利要求 1 所述的系统，其特征在于，

所述请求客户端，还被配置为向所述服务端发送项目加入请求，所述项目加入请求中携带有用户的身份标识信息以及项目标识信息；

所述服务端，还被配置为接收所述项目加入请求，根据所述项目标识信息确定与所述项目相关联的文件模板以及项目详细信息；根据所述项目详细信息、用户的身份标识信息以及所述文件模板生成与所述项目相关的第一目标文件，向所述请求客户端发起文件签订交易；其中，所述文件签订交易用于触发对所述第一目标文件进行电子签名；

所述请求客户端，还被配置为接收所述服务端发起的文件签订交易，响应于所述文件签订交易，对所述第一目标文件进行电子签名操作，将签名后的第二目标文件发送至所述服务端；

所述服务端，还被配置为：接收所述第二目标文件，基于认证机构证书对所述第二目标文件进行认证签章操作。

12、一种基于区块链的业务处理方法，其特征在于，应用于服务端，包括：

接收目标文件查询请求，所述目标文件查询请求中携带有用户的身份标识信息及目标文件标识信息；

根据所述用户的身份标识信息及目标文件标识信息获取所述目标文件并接收所述用户进行目标文件查询；

向所述用户发送是否将与所述目标文件上传至区块链节点的提示信息；

若接收到所述用户的目标文件上传请求，则将所述目标文件上传至所述区块链节点。

13、根据权利要求 12 所述的方法，其特征在于，所述将所述目标文件上传至所述区块链节点包括：

根据预设算法对所述目标文件进行哈希运算生成对应的数字摘要；采用非对称加密算法，对所述数字摘要进行私钥签名生成对应的数字签名，并将公钥、所述数字签名以及目标文件上传至所述区块链节点。

14、根据权利要求 12 所述的方法，其特征在于，所述将所述目标文件上传至所述区块链节点之后，还包括:

接收由所述区块链节点返回的存证哈希值。

15、根据权利要求 12 所述的方法，其特征在于，所述向所述用户发送是否将与所述目标文件上传至区块链节点的提示信息包括:

为所述用户提供目标文件查询页面，在所述目标文件查询页面设置是否将所述目标文件上传至区块链节点的提示框，所述提示框中设置有可供所述用户进行点击操作的选项按钮;

检测所述用户的选择结果;

所述若接收到所述用户的目标文件上传请求，则将所述目标文件上传至所述区块链节点，包括:

若所述用户的选择结果为确认上传，则将所述目标文件上传至所述区块链节点。

16、根据权利要求 12 所述的方法，其特征在于，所述将所述目标文件上传至所述区块链节点之后，还包括:

接收所述目标文件摘要信息查询请求，根据所述目标文件标识信息确定是否存在对应的存证哈希值;

若存在，则向所述请求客户端发送所述存证哈希值;

若不存在，则向所述请求客户端发送信息正在上传至区块链节点的提示信息。

17、根据权利要求 12 所述的方法，其特征在于，所述若接收到所述用户的目标文件上传请求，则将所述目标文件上传至所述区块链节点，包括:

若接收到所述用户的目标文件上传请求，则向所述用户发起协议签订交易；其中，所述协议签订交易用于触发对目标文件传输协议进行电子签名操作;

接收所述用户发送的签名后的目标文件传输协议，将所述目标文件传输协议、目标文件以及对所述目标文件进行哈希算法生成的数字签名发送至所述区块链节点。

18、根据权利要求 12 所述的方法，其特征在于，所述接收目标文件查询请求之前，还包括:

接收文件模板，向所述第二业务端发送是否将所述文件模板上传至区块链节点的提示信息，所述提示信息中携带有文件模板标识信息;

接收所述第二业务端发送的携带有所述选择结果的信息，在所述信息中携带的选择结果为确认上传时，将所述文件模板发送至所述区块链节点;

接收由区块链节点返回的所述文件模板写链成功的哈希值并将所述哈希值保存于

数据库。

19、一种基于区块链的业务处理装置，其特征在于，包括:

文件查询请求接收模块，被配置为接收目标文件查询请求，所述目标文件查询请求中携带有用户的身份标识信息及目标文件标识信息;

目标文件查询模块，被配置为根据所述用户的身份标识信息及目标文件标识信息获取所述目标文件并接收所述用户进行目标文件查询;

提示信息发送模块，被配置为向所述用户发送是否将与所述目标文件上传至区块链节点的提示信息;

目标文件传输模块，被配置为若接收到所述用户的目标文件上传请求，则将所述目标文件上传至所述区块链节点。

20、一种电子设备，其特征在于，包括:

存储器、处理器;

所述存储器用于存储计算机可执行指令，所述处理器用于执行所述计算机可执行指令:

接收目标文件查询请求，所述目标文件查询请求中携带有用户的身份标识信息及目标文件标识信息;

根据所述用户的身份标识信息及目标文件标识信息获取所述目标文件并接收所述用户进行目标文件查询;

向所述用户发送是否将与所述目标文件上传至区块链节点的提示信息;

若接收到所述用户的目标文件上传请求，则将所述目标文件上传至所述区块链节点。

21、一种计算机可读存储介质，其存储有计算机指令，其特征在于，该指令被处理器执行时实现权利要求 12 至 18 任意一项所述方法的步骤。

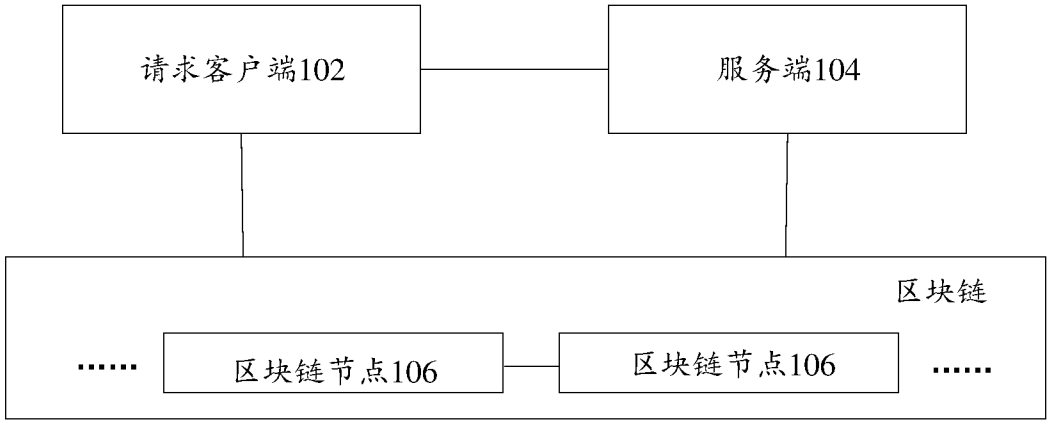
请求客户端102
服务端104
区块链
……
区块链节点106
区块链节点106
……

图 1

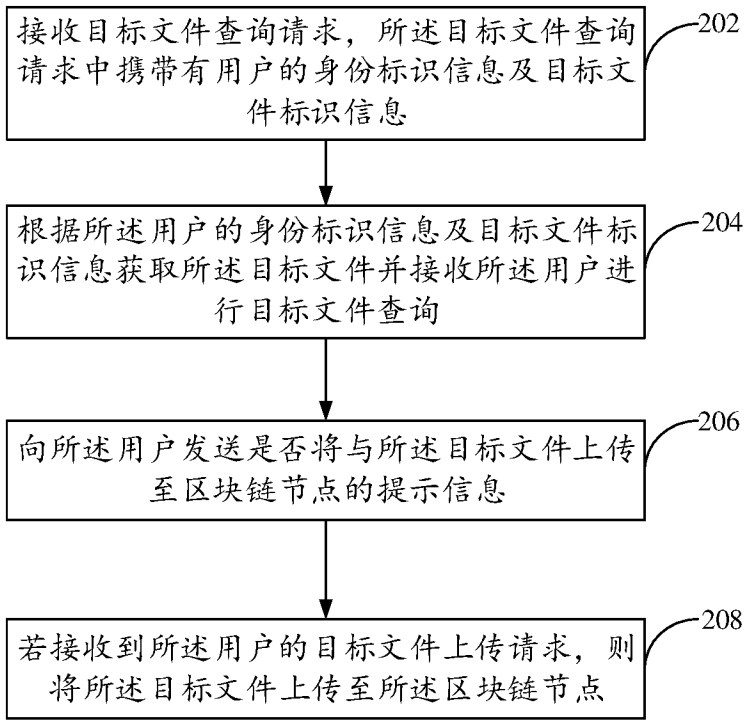
接收目标文件查询请求，所述目标文件查询请求中携带有用户的身份标识信息及目标文件标识信息
202
根据所述用户的身份标识信息及目标文件标识信息获取所述目标文件并接收所述用户进行目标文件查询
204
向所述用户发送是否将与所述目标文件上传至区块链节点的提示信息
206
若接收到所述用户的目标文件上传请求，则将所述目标文件上传至所述区块链节点
208

图 2

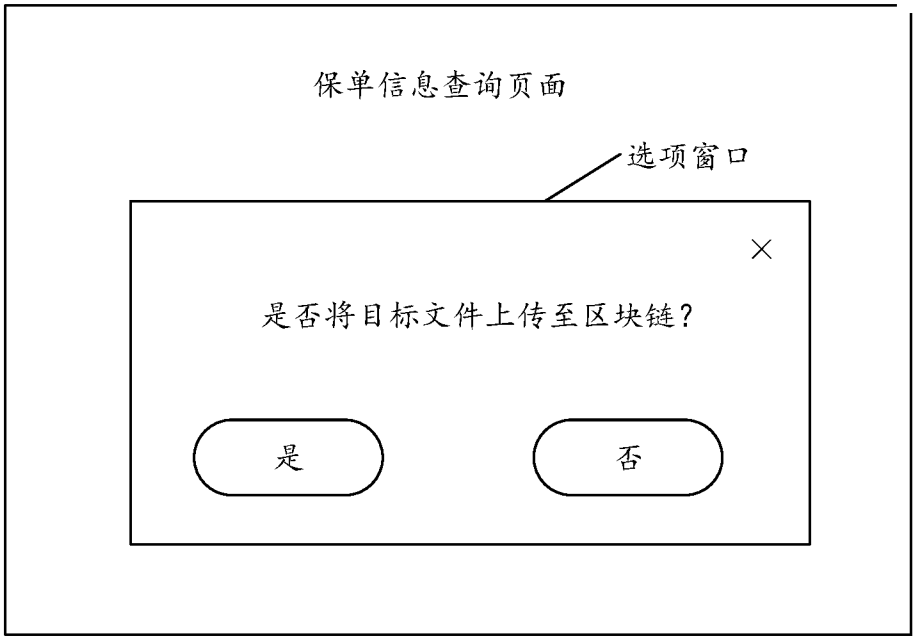
保单信息查询页面
选项窗口
×
是否将目标文件上传至区块链？
是
否

图 3


目标文件摘要信息查询窗口
目标文件摘要信息：CXHK WDCQ RJHS KIYV
目标文件下载地址：https://abcd.ef/mnopqrstuv/

图 4

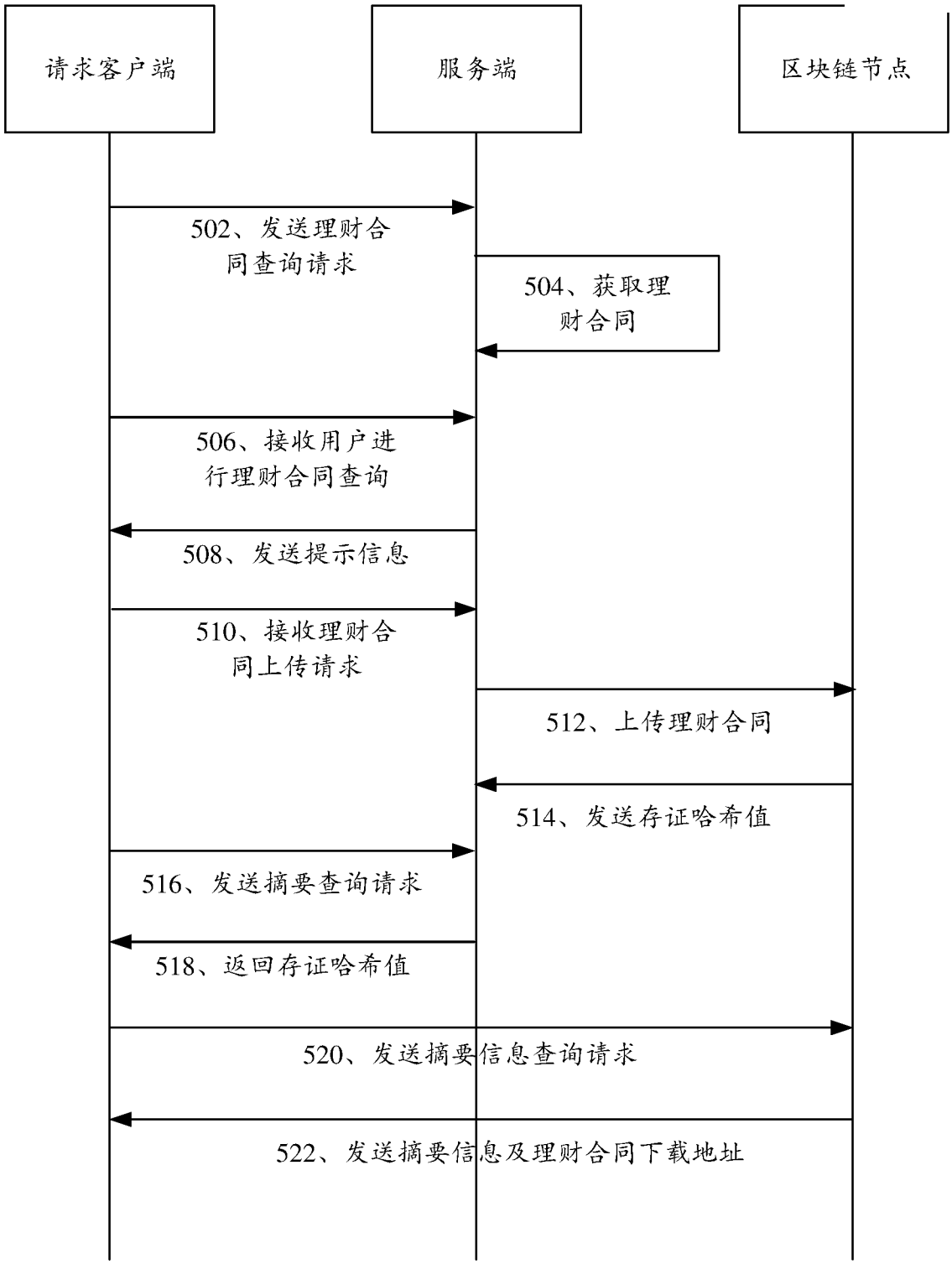
请求客户端
服务端
区块链节点
502、发送理财合同查询请求
504、获取理财合同
506、接收用户进行理财合同查询
508、发送提示信息
510、接收理财合同上传请求
512、上传理财合同
514、发送存证哈希值
516、发送摘要查询请求
518、返回存证哈希值
520、发送摘要信息查询请求
522、发送摘要信息及理财合同下载地址

图 5

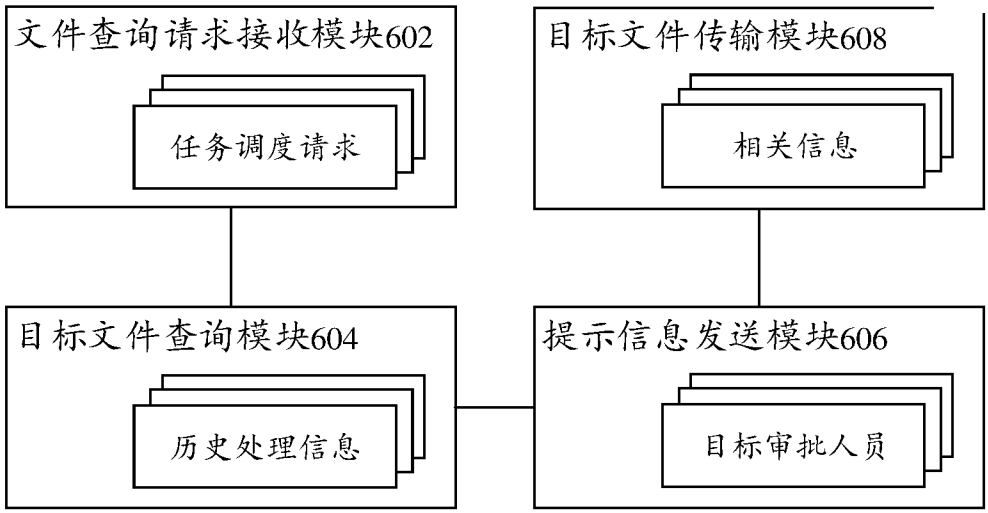
文件查询请求接收模块602
任务调度请求
目标文件传输模块608
相关信息
目标文件查询模块604
历史处理信息
提示信息发送模块606
目标审批人员

图 6

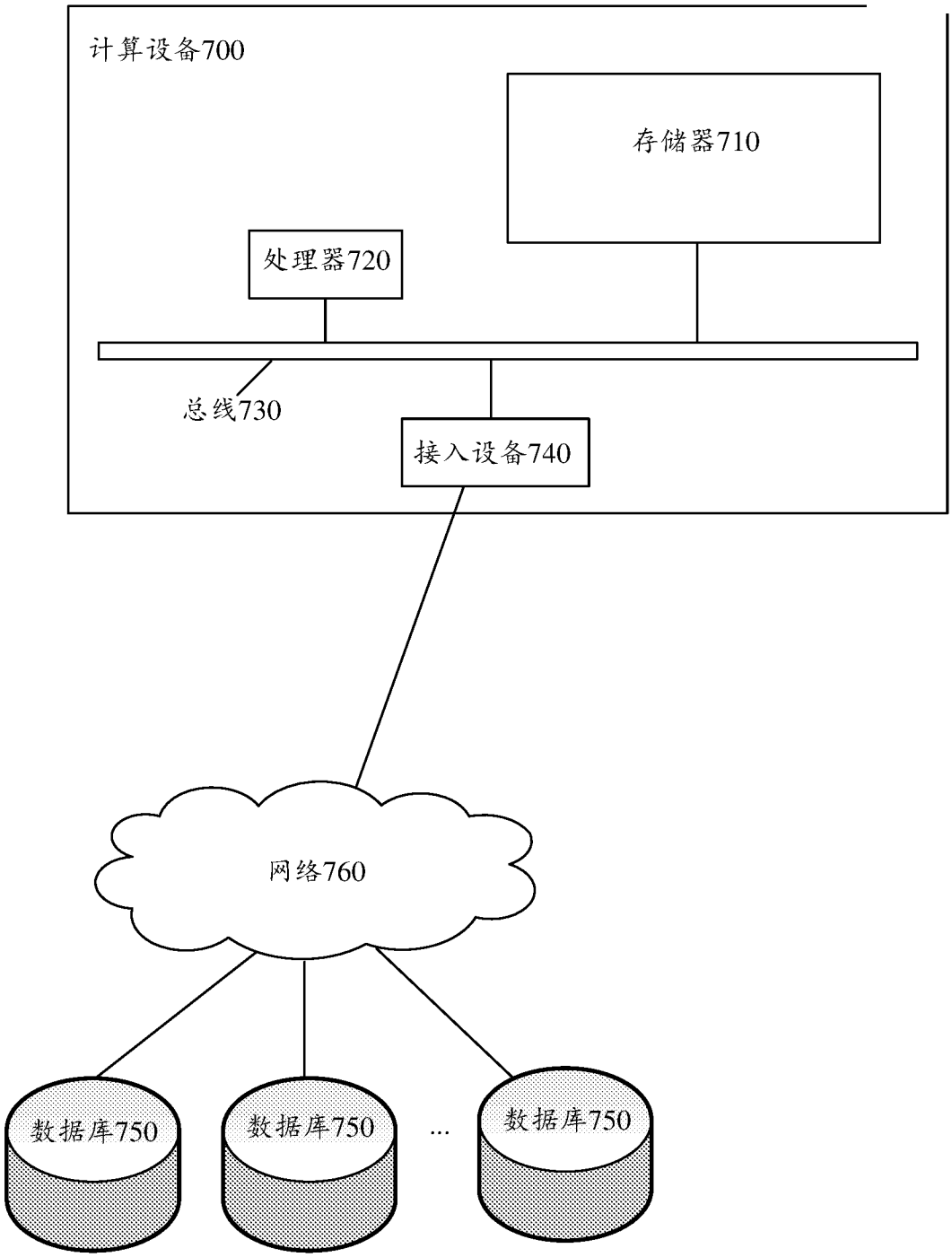
计算设备700
存储器710
处理器720
总线730
接入设备740
网络760
数据库750
数据库750
...
数据库750

图 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2020/071230

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 50/18(2012.01)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)

G06Q,; 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)

WPI, EPODOC, CNPAT, CNKI, IEEE: 合同, 签约, 合约, 区块链, 存证, 哈希, 摘要, 签名, 验证, contract, agreement, blockchain, block chain, evidence storage, hash, abstract, signature, verification

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110349056 A (ALIBABA GROUP HOLDING LIMITED) 18 October 2019 (2019-10-18) claims 1-21	1-21
X	CN 109784870 A (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) 21 May 2019 (2019-05-21) description, paragraphs [0037]-[0081]	12, 15, 17-21
Y	CN 109784870 A (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) 21 May 2019 (2019-05-21) description, paragraphs [0037]-[0081]	1-11, 13, 14, 16
Y	CN 109064120 A (MASHANGYOU TECHNOLOGY CO., LTD.) 21 December 2018 (2018-12-21) description, paragraphs [0005]-[0008] and [0015]-[0024]	1-11, 13, 14, 16
A	CN 108197891 A (FAXIN NOTARIZATION CLOUD (XIAMEN) TECHNOLOGY CO., LTD.) 22 June 2018 (2018-06-22) entire document	1-21
A	US 2019108140 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 11 April 2019 (2019-04-11) entire document	1-21

☐ 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
22 March 2020	**08 April 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/CN2020/071230

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 110349056 A	18 October 2019	None	
CN 109784870 A	21 May 2019	None	
CN 109064120 A	21 December 2018	None	
CN 108197891 A	22 June 2018	None	
US 2019108140 A1	11 April 2019	None	

国际检索报告

国际申请号
PCT/CN2020/071230

A. 主题的分类

G06Q 50/18(2012.01)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)

G06Q,; 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））

WPI, EPODOC, CNPAT, CNKI, IEEE: 合同，签约，合约，区块链，存证，哈希，摘要，签名，验证，contract, agreement, blockchain, block chain, evidence storage, hash, abstract, signature, verification

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 110349056 A (阿里巴巴集团控股有限公司) 2019年 10月 18日 (2019-10-18) 权利要求1-21	1-21
X	CN 109784870 A (平安科技深圳有限公司) 2019年 5月 21日 (2019-05-21) 说明书第[0037]-[0081]段	12, 15, 17-21
Y	CN 109784870 A (平安科技深圳有限公司) 2019年 5月 21日 (2019-05-21) 说明书第[0037]-[0081]段	1-11, 13, 14, 16
Y	CN 109064120 A (马上游科技股份有限公司) 2018年 12月 21日 (2018-12-21) 说明书第[0005]-[0008], [0015]-[0024]段	1-11, 13, 14, 16
A	CN 108197891 A (法信公证云厦门科技有限公司) 2018年 6月 22日 (2018-06-22) 全文	1-21
A	US 2019108140 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 2019年 4月 11日 (2019-04-11) 全文	1-21

☐ 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 3月 22日	2020年 4月 8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 郭明华 电话号码 86-(10)-53961414

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2020/071230

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 110349056 A	2019年 10月 18日	无	
CN 109784870 A	2019年 5月 21日	无	
CN 109064120 A	2018年 12月 21日	无	
CN 108197891 A	2018年 6月 22日	无	
US 2019108140 A1	2019年 4月 11日	无	