(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 11 月 26 日 (26.11.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/233235 A1

(51) 国际专利分类号:
G06F 21/60 (2013.01)

(21) 国际申请号: PCT/CN2020/082203

(22) 国际申请日: 2020 年 3 月 30 日 (30.03.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910413920.9 2019年5月17日 (17.05.2019) CN

(71) 申请人: 深圳前海微众银行股份有限公司 (WEBANK CO., LTD.) [CN/CN]; 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。

(72) 发明人: 胡朝新 (HU, Chaoxin); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。 张俊麒 (ZHANG, Junqi); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。 沈超 (SHEN, Chao); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。 陈浩 (CHEN, Hao); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。 苏小康 (SU, Xiaokang); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。 张开翔 (ZHANG, Kaixiang); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。 范瑞彬 (FAN, Ruibin); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。

(74) 代理人: 北京同达信恒知识产权代理有限公司 (TDIP & PARTNERS); 中国北京市西城区裕民路18号北环中心A座2002, Beijing 100029 (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,

(54) **Title:** BLOCKCHAIN DATA VERIFICATION METHOD AND APPARATUS

(54) **发明名称:** 一种区块链的数据验证方法和装置

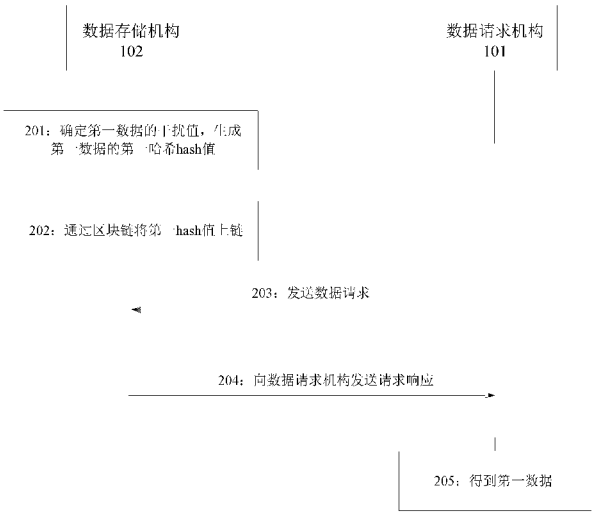

图 2

101 Data request mechanism
102 Data storage mechanism
201 Determine an interference value of first data and generate a first hash value of the first data
202 Upload the first hash value by means of a blockchain
203 Send a data request
204 Send a request response to the data request mechanism
205 Obtain the first data

(57) **Abstract:** A blockchain data verification method and apparatus, relating to the fintech field: a data request mechanism sends a data request to a data storage mechanism; the data request mechanism acquires a request response returned by the data storage mechanism, such that the data request mechanism acquires second encrypted data; the data request mechanism decrypts the second encrypted data to obtain second data; the data request mechanism acquires a first hash value of first data from the blockchain, the first hash value being generated by the data storage mechanism on the basis of the first data and an interference value of the first data and uploaded to the blockchain; and, when confirming that the first hash value is the same as a second hash value, the data request mechanism obtains the first data from the second data.

WO 2020/233235 A1

[见续页]

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。

(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：一种区块链的数据验证方法和装置，涉及科技金融(Fintech)领域，数据请求机构向数据存储机构发送数据请求；所述数据请求机构获取所述数据存储机构返回的请求响应，以使所述数据请求机构获取第二加密数据；所述数据请求机构解密所述第二加密数据，得到第二数据；所述数据请求机构从区块链上获取所述第一数据的第一哈希hash值；所述第一hash值是所述数据存储机构根据所述第一数据及所述第一数据的干扰值生成并上传至所述区块链的；所述数据请求机构在确认所述第一hash值和第二hash值一致时，从所述第二数据中得到所述第一数据。

一种区块链的数据验证方法和装置

相关申请的交叉引用

本申请要求在2019年05月17日提交中国专利局、申请号为201910413920.9、申请名称为“一种区块链的数据验证方法和装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本发明实施例涉及科技金融(Fintech)领域，尤其是涉及一种区块链(Block Chain ）的数据验证方法和装置。

背景技术

随着计算机技术的发展，越来越多的技术应用在金融领域，传统金融业正在逐步向金融科技（Finteh）转变，区块链（Block chain）技术也不例外，但由于金融行业的安全性、实时性要求，也对技术提出的更高的要求。

区块链（Block chain）是一种全民参与记账的方式，具有去中心化和去信任的特点。区块链最重要的是解决了中介信用问题。在过去，两个互不认识和信任的人要达成协作是难的，必须要依靠第三方。比如支付行为，在过去任何一种转账，必须要有银行或者支付宝这样的机构存在。但是通过区块链技术，比特币是人类第一次实现在没有任何中介机构参与的情况下，完成双方可以互信的转账行为，这是区块链的重大突破，也因此区块链越来越受到人们的关注。

在区块链使用的过程中，可以实现分布式身份认证，但是目前的验证过程仍存在传输的数据与上链的数据不一致无法验证的问题。

发明内容

本发明提供一种区块链的数据验证方法和装置，用以解决现有技术中数

据请求不可信安全性低的问题。

本发明实施例提供一种区块链的数据验证方法，包括:

数据请求机构向数据存储机构发送数据请求；所述数据请求用于获取第一数据;

所述数据请求机构获取所述数据存储机构返回的请求响应，以使所述数据请求机构获取第二加密数据;

所述数据请求机构解密所述第二加密数据，得到第二数据;

所述数据请求机构从区块链上获取所述第一数据的第一哈希 hash 值；所述第一 hash 值是所述数据存储机构根据所述第一数据及所述第一数据的干扰值生成并上传至所述区块链的;

所述数据请求机构在确认所述第一 hash 值和第二 hash 值一致时，从所述第二数据中得到所述第一数据；所述第二 hash 值是所述数据请求机构通过所述第二数据生成的。

一种可能的实现方式，所述请求响应包括所述第二加密数据;

所述数据请求机构解密所述第二加密数据，得到第二数据，包括:

所述数据请求机构根据所述数据请求机构的私钥解密所述第二加密数据，获得所述第二数据；所述第二加密数据为所述数据存储机构根据所述数据请求机构的公钥加密后获得的。

一种可能的实现方式，所述请求响应还包括所述第二加密数据的签名；所述第二加密数据的签名为所述数据存储机构通过所述数据存储机构的私钥对所述第二加密数据进行签名得到的;

所述数据请求机构解密所述第二加密数据，得到第二数据之前，还包括:

所述数据请求机构根据所述数据存储机构的公钥验证所述第二加密数据的签名。

一种可能的实现方式，所述请求响应包括所述第二加密数据及所述第二加密数据的签名;

所述数据请求机构解密所述第二加密数据，得到第二数据之前，还包括:

所述数据请求机构从所述区块链上获取所述第一数据的第三 hash 值；所述第三 hash 值是所述数据存储机构根据第一加密数据及所述第一加密数据的签名生成的；所述第一加密数据是所述数据存储机构根据所述数据请求机构的公钥对所述第一数据及所述第一数据的干扰值加密后得到的；

所述数据请求机构根据所述第二加密数据及所述第二加密数据的签名，确定第四 hash 值；

所述数据请求机构确认所述第三 hash 值和所述第四 hash 值一致。

一种可能的实现方式，所述请求响应包括第一加密数据在所述区块链上的地址；所述第一加密数据是所述数据存储机构根据所述数据请求机构的公钥对所述第一数据及所述第一数据的干扰值加密后得到的；所述地址是所述数据存储机构将所述第一加密数据上传至所述区块链后得到的；

所述数据请求机构获取所述数据存储机构返回的请求响应，以使所述数据请求机构获取第二加密数据，包括：

所述数据请求机构根据所述地址，获取所述第二加密数据。

一种可能的实现方式，所述请求响应包括二维码；所述二维码为所述数据存储机构根据第一加密数据生成的；所述第一加密数据是所述数据存储机构根据所述数据请求机构的公钥对所述第一数据及所述第一数据的干扰值加密后得到的；

所述数据请求机构获取所述数据存储机构返回的请求响应，以使所述数据请求机构获取第二加密数据，包括：

所述数据请求机构通过所述数据存储机构发送的二维码，获取所述第二加密数据。

本发明实施例提供一种区块链的数据验证方法，包括：

数据存储机构确定第一数据的干扰值；

所述数据存储机构根据所述第一数据和所述第一数据的干扰值，生成所述第一数据的第一哈希 hash 值；

所述数据存储机构通过区块链将所述第一 hash 值上链；所述第一 hash 值

用于数据请求机构确定通过所述数据存储机构获得的加密数据是否与上链信息一致。

一种可能的实现方式，所述方法还包括:

所述数据存储机构接收数据请求机构发送的数据请求；所述数据请求用于获取所述第一数据;

所述数据存储机构向所述数据请求机构发送请求响应，所述数据响应用于所述数据请求机构获取所述数据存储机构提供的第二加密数据以使所述数据请求机构通过所述第二加密数据获得所述第一数据。

一种可能的实现方式，所述数据响应用于所述数据请求机构获取所述数据存储机构提供的第二加密数据，包括:

所述数据响应包括所述第二加密数据；所述第二加密数据是所述数据存储机构根据所述数据请求机构的公钥对所述第一数据及所述第一数据的干扰值加密后得到的；或

所述数据响应包括第一加密数据在所述区块链上的地址；所述第一加密数据是所述数据存储机构根据所述数据请求机构的公钥对所述第一数据及所述第一数据的干扰值加密后得到的；所述地址是所述数据存储机构将所述第一加密数据上传至所述区块链后得到的；或

所述数据响应包括二维码，所述二维码为所述数据存储机构根据第一加密数据生成的；所述第一加密数据是所述数据存储机构根据所述数据请求机构的公钥对所述第一数据及所述第一数据的干扰值加密后得到的;

一种可能的实现方式，所述方法还包括:

所述数据存储机构使用所述数据请求机构的公钥对所述第一数据及所述第一数据的干扰值进行加密，得到第一加密数据;

所述数据存储机构通过所述数据存储机构的私钥生成所述第一加密数据的签名;

所述数据存储机构将所述第一加密数据及所述第一加密数据的签名生成第三 hash 值，并将所述第三 hash 值存储至所述区块链，以使所述数据请求机

构验证所述请求响应。

本发明实施例提供一种区块链的数据验证装置，包括:

收发单元，用于向数据存储机构发送数据请求；所述数据请求用于获取第一数据；获取所述数据存储机构返回的请求响应，以使所述数据请求机构获取第二加密数据;

处理单元，用于解密所述第二加密数据，得到第二数据；从区块链上获取所述第一数据的第一哈希 hash 值；所述第一 hash 值是所述数据存储机构根据所述第一数据及所述第一数据的干扰值生成并上传至所述区块链的；在确认所述第一 hash 值和第二 hash 值一致时，从所述第二数据中得到所述第一数据；所述第二 hash 值是所述数据请求机构通过所述第二数据生成的。

一种可能的实现方式，所述请求响应包括所述第二加密数据；所述处理单元，具体用于：根据所述数据请求机构的私钥解密所述第二加密数据，获得所述第二数据；所述第二加密数据为所述数据存储机构根据所述数据请求机构的公钥加密后获得的。

一种可能的实现方式，所述请求响应还包括所述第二加密数据的签名；所述第二加密数据的签名为所述数据存储机构通过所述数据存储机构的私钥对所述第二加密数据进行签名得到的；所述处理单元，具体用于：根据所述数据存储机构的公钥验证所述第二加密数据的签名。

一种可能的实现方式，所述请求响应包括所述第二加密数据及所述第二加密数据的签名;

所述收发单元，具体用于从所述区块链上获取所述第一数据的第三 hash 值；所述第三 hash 值是所述数据存储机构根据第一加密数据及所述第一加密数据的签名生成的；所述第一加密数据是所述数据存储机构根据所述数据请求机构的公钥对所述第一数据及所述第一数据的干扰值加密后得到的;

所述处理单元，还用于根据所述第二加密数据及所述第二加密数据的签名，确定第四 hash 值；确认所述第三 hash 值和所述第四 hash 值一致。

一种可能的实现方式，所述请求响应包括第一加密数据在所述区块链上

的地址；所述第一加密数据是所述数据存储机构根据所述数据请求机构的公钥对所述第一数据及所述第一数据的干扰值加密后得到的；所述地址是所述数据存储机构将所述第一加密数据上传至所述区块链后得到的；

所述处理单元，还用于根据所述地址，获取所述第二加密数据。

一种可能的实现方式，所述请求响应包括二维码；所述二维码为所述数据存储机构根据第一加密数据生成的；所述第一加密数据是所述数据存储机构根据所述数据请求机构的公钥对所述第一数据及所述第一数据的干扰值加密后得到的；

所述收发单元，还用于通过所述数据存储机构发送的二维码，获取所述第二加密数据。

本发明实施例提供一种区块链的数据验证装置，包括：

收发单元，用于数据存储机构确定第一数据的干扰值；

处理单元，用于根据所述第一数据和所述第一数据的干扰值，生成所述第一数据的第一哈希 hash 值；通过区块链将所述第一 hash 值上链；所述第一 hash 值用于数据请求机构确定通过所述数据存储机构获得的加密数据是否与上链信息一致。

一种可能的实现方式，所述收发单元，还用于接收数据请求机构发送的数据请求；所述数据请求用于获取所述第一数据；向所述数据请求机构发送请求响应，所述数据响应用于所述数据请求机构获取所述数据存储机构提供的第二加密数据以使所述数据请求机构通过所述第二加密数据获得所述第一数据。

一种可能的实现方式，所述数据响应包括所述第二加密数据；所述第二加密数据是所述数据存储机构根据所述数据请求机构的公钥对所述第一数据及所述第一数据的干扰值加密后得到的；或

所述数据响应包括第一加密数据在所述区块链上的地址；所述第一加密数据是所述数据存储机构根据所述数据请求机构的公钥对所述第一数据及所述第一数据的干扰值加密后得到的；所述地址是所述数据存储机构将所述第

一加密数据上传至所述区块链后得到的；或

所述数据响应包括二维码，所述二维码为所述数据存储机构根据第一加密数据生成的；所述第一加密数据是所述数据存储机构根据所述数据请求机构的公钥对所述第一数据及所述第一数据的干扰值加密后得到的；

一种可能的实现方式，所述处理单元，还用于使用所述数据请求机构的公钥对所述第一数据及所述第一数据的干扰值进行加密，得到第一加密数据；通过所述数据存储机构的私钥生成所述第一加密数据的签名；将所述第一加密数据及所述第一加密数据的签名生成第三 hash 值，并将所述第三 hash 值存储至所述区块链，以使所述数据请求机构验证所述请求响应。

本发明实施例提供一种计算机存储介质，所述计算机可读存储介质包括计算机程序，当计算机程序在计算机上运行时，使得所述计算机执行上述实施例中任一项所述的方法。

本发明实施例提供一种包含指令的计算机程序产品，当所述指令在计算机上运行时，使得所述计算机执行如上述实施例任一项所述的方法。

本发明实施例提供一种计算机设备，包括：

至少一个存储器，用于存储程序指令；

至少一个处理器，用于调用所述存储器中存储的程序指令，按照获得的程序执行如上述实施例任一项所述的方法。

本发明实施例通过向区块链网络中，原始数据存在各机构的私有数据库里，明文不会被上传到链上，只会上传数据的 Hash；每个 Hash 值经过干扰值混淆，干扰值可自主更新，杜绝了被反向攻破的可能。数据的披露经过非对称加密的公钥加密和私钥加签；公钥放在链上，参与的多方不可篡改或抵赖；每个披露的数据密文仅支持被披露方解密，不用担心数据泄露。数据的披露密文支持上链存证进一步增信。有效保证了交易数据的安全性和可靠性。

附图说明

为了更清楚地说明本发明实施例中的技术方案，下面将对实施例描述中

所需要使用的附图作简要介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域的普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

图 1a 为本发明实施例提供的一种系统架构示意图；

图 1b 为本发明实施例提供的另一种系统架构示意图；

图 2 为本发明实施例提供的一种数据验证方法的流程示意图；

图 3 为本发明实施例提供的一种数据验证装置的结构示意图；

图 4 为本发明实施例提供的一种数据验证装置的结构示意图；

图 5 为本发明实施例提供的一种计算机设备的结构示意图。

具体实施方式

为了使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明作进一步地详细描述，显然，所描述的实施例仅仅是本发明一部份实施例，而不是全部的实施例。基于本发明中的实施例，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它实施例，都属于本发明保护的范围。

数据存储机构：这一角色用来描述存储了数据并准备将其披露的机构。其他机构可能会向数据存储机构申请数据披露。

数据请求机构：这一角色有着向数据请求机构申请披露数据的需求。

区块链：所有参与方都具有区块链的读写访问能力。

区块（block）：用于记录按照一定条件划分出的数据集合和状态结果，是在各个节点达成共识之后形成的，在本发明实施例中，需要记录的数据主要是数据，或者用户的数据变化后的履历更新信息。具体的，区块可以是以时间进行划分，例如每间隔 10 秒（s）产生一个区块，那么这个区块即是记录这 10s 内的所有数据，或者每间隔一天产生一个区块，那么这个区块即是记录这一天内的所有数据；或者，区块还可以是根据接收到的数据或者履历更新信息的数量进行划分，例如，在接收到指定数量的数据或者履历更新信息之后，

生成一个区块，那么这个区块即是用于记录已接收到的指定数量的数据更新信息，当然，本发明实施例对区块具体的划分方式并不进行限制。一个区块包括区块头和区块体。其中，区块头中包括前一区块地址（Prev-block），前一区块地址在区块头中可以通过前一区块哈希码（pre-hash）的形式进行存储，通过前一区块地址的指向将所有的区块串联起来，进而形成一条区块链。区块体中则用于存储具体的数据，例如本发明实施例中的数据。

区块链（block chain）：或称分布式数据记录账本，是一种按照一定顺序将存储数据的区块以顺序相连的方式组合成的一种链式数据结构。如图 1a 中所示，将区块按照顺序串联起来在而形成了一条区块链。

节点：指区块链网络中参与数据的记录或者验证等处理过程的计算设备，例如计算机、手机、矿机、台式机或者服务器等拥有计算能力的设备均可作为区块链网络中的节点。

另外，本文中术语“和/或”，仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 这三种情况。另外，本文中字符“/”，在不做特别说明的情况下，一般表示前后关联对象是一种“或”的关系。

为了利于对本发明实施例的技术方案的理解，下面介绍区块链的原理。

在区块链技术中，网络中的任意一个设备都可以作为区块链的一个节点，并且可以参与到区块链的记录和存储中，节点间基于共识机制，通过竞争计算共同维护整个区块链。由于任一节点都可以拥有一份完整的区块链的数据拷贝，因而任一节点失效，其余节点仍能够正常进行工作，从而基于区块链存储的方式可靠性高。

此外，由于在区块链技术中心通过众多的节点来共同维护整个区块链，每个节点所拥有的权限可以是相同的，因而并不存在中心化的设备或者管理机构。区块链中所有的数据信息都是公开透明的，单个节点甚至多个节点对自身数据的修改无法影响到其他节点的数据，除非能够控制整个区块链网络中超过一半的节点都进行修改，但是这种方式难度太大，并且区块链中的每

一个区块都与前后的两个区块进行关联，要想篡改一个区块的数据，就需要篡改与之相关的多个区块的数据，难度较大，从而基于区块链存储的数据具有不可篡改性。

Hash 值：对某种字符串生成哈希映射值的算法，例如 sha3。

在大数据时代，不同机构间存在着披露数据的需求。然而，由于各个机构之间通常难以组建有效的信任合作机制，各机构间难以将各自保管的数据安全可信地披露给其他机构。分布式身份认证的核心要素就是公钥上链。每个参与方机构使用约定的非对称加密算法，如 ECDSA 生成自己的公私钥对；将私钥存储到自己的私有数据库里，再将公钥上链。如图 1a 所示，机构 A 将自己的公钥 A 发布至区块链上，机构 B 将自己的公钥 B 发布至区块链上。然而，这类做法至少存在以下问题：数据存储机构存在道德风险，不一定保证数据存储机构上链公示的数据和自己用来传输的数据一致；对此，数据存储机构可以将数据生成 Hash 存证放在区块链上公示。例如，基于将各参与方把自己的公钥存到区块链上，然后使用对方的公钥加密、乃至再用自己的私钥做签名，并传输数据。图 1b 示例性示出了本发明实施例适用的另一种系统架构示意图，如图 1b 所示，本发明实施例适用的系统架构包括数据请求机构 101；数据存储机构 102；区块链网络 103。数据请求机构 101 向数据存储机构发送数据请求；数据存储机构与区块链网络相连，给区块链网络发送需上链的数据；数据请求机构与区块链网络相连，验证数据存储机构返回的响应数据。区块链网络中的节点可以为记账节点或者普通节点。但是数据本身变化频率不大的情况下，Hash 存在被暴力反向攻破的可能。

基于上述问题，本发明实施例提供一种区块链的数据验证方法，如图 2 所示，包括：

步骤 201：数据存储机构确定第一数据的干扰值；数据存储机构根据所述第一数据和所述第一数据的干扰值，生成所述第一数据的第一哈希 hash 值。

在一种具体的实施例中，干扰值可以为一长度不定的字符串。例如，干扰值可以为盐值，也可以为伪随机序列。以下以盐值为例进行说明。

数据存储机构确认有需要披露的数据，例如，第一数据，则随机为第一数据生成一个字符串，作为盐值。其中，盐值指一个不指定长度的字符串。举例来说，第一数据 1 和第一数据 2 的数据结构如下所示:

```
{
    [
        "key": "用户 A 的姓名",
        "value": "张三",
        "salt": "75086e6a0b56f9d8efaf62518aac25af",
    ],
    [
        "key": "用户 A 的性别",
        "value": "男",
        "salt": "5c5db136609a2ac061c8dc73bbd11310",
    ]
}
```

第一数据和干扰值用于作为 Hash 算法的输入参数，以生成哈希映射值。由于反向攻破的终端并不知晓干扰值的存在，因此，无法反向攻破出第一数据和干扰值，只能解出于第一数据相同字段的无意义字符，因此，提供了 Hash 值抗反向攻破的能力。

步骤 202: 数据存储机构通过区块链将所述第一 hash 值上链; 所述第一 hash 值用于数据请求机构确定通过所述数据存储机构获得的加密数据是否与上链信息一致。

数据存储机构将数据表公开到区块链上。数据存储机构公开一个数据表，包括每项披露的数据标识、计算出的 Hash，及其他备注属性。数据标识里面不应该包含任何真实数据，它仅仅用于给其他数据请求机构确认“这项数据里面存储的是什么内容”。数据存储机构可以将其他备注信息存入备注栏内以便于其他机构了解。本发明实施例给出一个公开数据表的范例:

表 1 公开数据表（范例）

数据项标识	数据 Hash
用户 A 的姓名	55a59340a392ecb9d8003d0bfee965d56963c57f81bc8e9184ec1674b7a0bf06
用户 A 的身份证号	eb1421481d5028a930d5a1be5fa5d4e532e4f161be1032c81c98b6929fa67f35
用户 A 的性别	2a67c9ef51aba7a69a958d072a68c38359206429a8fe2ae83d9281314b838111
用户 A 的家庭住址	aa6c976ed381c3aada783db6a24c649d68ce59f06f021de868598a3f99d3c5df
用户 B 的姓名	8e00acc4cdea7eb98c1d81864abd7ebc793decc47b54ff2a843513ee7a62666e

为进一步提高安全性，一种可能的实现方式，盐值还可以包括更新流程，由数据存储机构调用。数据存储机构可以自己定义周期，在任何时刻，更换数据的盐值。数据存储机构可以根据数据及更新后的盐值，确定出更新的 Hash 值，更新于公布在链上的公开数据表中，以进一步提高数据的安全性。

一种可能的实现方式，在数据请求机构发出数据请求之前，数据请求机构可以预先存储数据的 Hash 值，因此，数据请求机构申请披露的时候会同时附带上此 Hash 值；如果 Hash 值在这个间隙中发生了更新，那么数据存储机构就会返回“未查询到”的结果。数据请求机构可以检查 Hash 是否被更新了，并且根据实际需要，重新进行数据的 hash 值的获取。

步骤 203：数据请求机构向数据存储机构发送数据请求；所述数据请求用于获取第一数据；数据存储机构接收数据请求机构发送的数据请求。

步骤 204：数据存储机构向所述数据请求机构发送请求响应，所述数据响应用于所述数据请求机构获取所述数据存储机构提供的第二加密数据以使所

述数据请求机构通过所述第二加密数据获得所述第一数据。

数据请求机构获取所述数据存储机构返回的请求响应，以使所述数据请求机构获取第二加密数据。

步骤 205：数据请求机构解密所述第二加密数据，得到第二数据；

数据请求机构从区块链上获取所述第一数据的第一哈希 hash 值；所述第一 hash 值是所述数据存储机构根据所述第一数据及所述第一数据的干扰值生成并上传至所述区块链的；

数据请求机构在确认所述第一 hash 值和第二 hash 值一致时，从所述第二数据中得到所述第一数据；所述第二 hash 值是所述数据请求机构通过所述第二数据生成的。

本发明实施例中，通过将第一 hash 值是所述数据存储机构根据所述第一数据及所述第一数据的干扰值生成并上传至所述区块链的，使得原始数据存在各数据存储机构的私有数据库里，明文不会被上传到链上，只会上传数据的 Hash；每个 Hash 值经过干扰值混淆，干扰值可自主更新，杜绝了被反向攻破的可能。数据的披露经过非对称加密的公钥加密和私钥加签；公钥放在链上，参与的多方不可篡改或抵赖；每个披露的数据密文仅支持被披露方解密，不用担心数据泄露，有效保证了交易数据的安全性和可靠性。

在步骤 205 中，为提高数据的可信度，一种可能的实现方式，还包括：

数据存储机构使用所述数据请求机构的公钥对所述第一数据及所述第一数据的干扰值进行加密，得到第一加密数据。

在步骤 206 中，一种可能的实现方式，所述请求响应包括所述第二加密数据；所述数据请求机构解密所述第二加密数据，得到第二数据，包括：

数据请求机构根据所述数据请求机构的私钥解密所述第二加密数据，获得所述第二数据；所述第二加密数据为所述数据存储机构根据所述数据请求机构的公钥加密后获得的。

通过验证第一加密数据和第二加密数据是否为同一数据，进而确定数据请求机构获得的第二数据为第一数据。

为进一步提高数据的可信度，一种可能的实现方式，所述方法还包括：数据存储机构通过所述数据存储机构的私钥生成所述第一加密数据的签名。

对应的，所述请求响应还包括所述第二加密数据的签名；所述第二加密数据的签名为所述数据存储机构通过所述数据存储机构的私钥对所述第二加密数据进行签名得到的；

对应的，在步骤 206 中，所述数据请求机构根据所述数据存储机构的公钥验证所述第二加密数据的签名。

为进一步提高数据的可信度，一种可能的实现方式，数据存储机构将所述第一加密数据及所述第一加密数据的签名生成第三 hash 值，并将所述第三 hash 值存储至所述区块链，以使所述数据请求机构验证所述请求响应。

对应的，一种可能的实现方式，所述请求响应包括所述第二加密数据及所述第二加密数据的签名；所述方法还包括：

步骤一、数据请求机构从所述区块链上获取所述第一数据的第三 hash 值；所述第三 hash 值是所述数据存储机构根据第一加密数据及所述第一加密数据的签名生成的；所述第一加密数据是所述数据存储机构根据所述数据请求机构的公钥对所述第一数据及所述第一数据的干扰值加密后得到的；

步骤二、数据请求机构根据所述第二加密数据及所述第二加密数据的签名，确定第四 hash 值；

步骤三、数据请求机构确认所述第三 hash 值和所述第四 hash 值一致。

结合上述实施例，所述数据响应用于所述数据请求机构获取所述数据存储机构提供的第二加密数据，包括：

一种可能的实现方式，所述数据响应包括第一加密数据在所述区块链上的地址；所述地址是所述数据存储机构将所述第一加密数据上传至所述区块链后得到的；在步骤 207 中，一种可能的实现方式，所述数据请求机构根据所述地址，获取所述第二加密数据。

为满足传输数据需求的多样性，一种可能的实现方式，所述请求响应包括二维码；所述二维码为所述数据存储机构根据第一加密数据生成的；所述

第一加密数据是所述数据存储机构根据所述数据请求机构的公钥对所述第一数据及所述第一数据的干扰值加密后得到的;

在步骤 207 中，一种可能的实现方式，所述数据请求机构通过所述数据存储机构发送的二维码，获取所述第二加密数据。

本发明实施例提供一种区块链的数据验证方法，包括数据请求机构申请数据、及数据存储机构发送数据的过程，具体的，包括:

步骤一、数据请求机构访问数据存储机构的公开数据表，从中选择若干项需要申请的数据，并存储这些数据项的 Hash 值。

步骤二、数据请求机构向数据存储机构发送数据申请请求，并指名要访问的数据项及 Hash 值。

步骤三、数据存储机构访问区块链，获取数据请求机构的公钥。

步骤四、数据存储机构将被请求的所有数据内容及盐值，进行序列化。

步骤五、数据存储机构，用获取到的数据请求机构的公钥，对序列化的内容进行加密，生成对应密文。

步骤六、数据存储机构使用自己的私钥，对得到的密文进行签名。

一种可能的实现方式，为提高增信，数据存储机构可以进一步将结果上传到链上，形成链上存证。

步骤七、数据存储机构将密文+签名（如果有增信的需求，还包括链上存证地址）发送给数据请求机构。例如，通过线下纸质（二维码）、互联网、或区块链载体传输。

一种可能的实现方式，为提高增信，则需要生成链上存证。链上存证的内容最少应当包含签名值、密文。链上也可以上传签名值+密文的 Hash 值。链上存证这一步也可以被完全拿掉，对数据真实无篡改的结果没有影响。

一种可能的实现方式，如果使用链上存证的方式，那么数据存储机构可以选择直接发送链上存证的地址给数据请求机构，而不是密文+签名——因为密文+签名已经在链上存储了。具体的密文+签名发送方式不限，也不必担心是否被泄露，因为密文和签名都无法被反向推出。

一种可能的实现方式，通过二维码传输。可以用于需要数据出境监管的场合里。具体地，将被传输的内容转换成二维码，然后打印在纸质单上以信件形式发出。一种可能的实现方式，通过 Internet 传输，如标准 RPC 接口、Restful API。一种可能的实现方式，通过区块链网络传输，如 AMOP 协议。

本发明实施例提供一种区块链的数据验证方法，包括数据请求机构验证所接收的数据真实性的过程，具体可以包括以下步骤：

步骤一、数据请求机构访问区块链，获取数据存储机构的公钥。

步骤二、数据请求机构用获取到的数据存储机构的公钥，及接收的密文，验证签名。

步骤三、数据请求机构用自己的私钥，对密文进行解密，得到序列化的数据内容及盐值；

步骤四、数据请求机构为每条数据加上盐值，计算 Hash，并和自己在数据申请流程开始阶段所存下的 Hash 值进行对比，检查是否一致。

步骤五、如果数据请求机构还接收到了链上存证地址，则还需要去链上确认链上的签名值和收到的签名值一致。

步骤六、以上的验证步骤全部通过时，说明数据真实无篡改。数据请求机构向数据存储机构发送验证成功的信息。

基于相同的发明构思，本发明实施例提供一种区块链的数据验证装置，如图 3 所示，包括：

收发单元 301，用于向数据存储机构发送数据请求；所述数据请求用于获取第一数据；获取所述数据存储机构返回的请求响应，以使所述数据请求机构获取第二加密数据；

处理单元 302，用于解密所述第二加密数据，得到第二数据；从区块链上获取所述第一数据的第一哈希 hash 值；所述第一 hash 值是所述数据存储机构根据所述第一数据及所述第一数据的干扰值生成并上传至所述区块链的；在确认所述第一 hash 值和第二 hash 值一致时，从所述第二数据中得到所述第一数据；所述第二 hash 值是所述数据请求机构通过所述第二数据生成的。

一种可能的实现方式，所述请求响应包括所述第二加密数据；处理单元302，具体用于：根据所述数据请求机构的私钥解密所述第二加密数据，获得所述第二数据；所述第二加密数据为所述数据存储机构根据所述数据请求机构的公钥加密后获得的。

一种可能的实现方式，所述请求响应还包括所述第二加密数据的签名；所述第二加密数据的签名为所述数据存储机构通过所述数据存储机构的私钥对所述第二加密数据进行签名得到的；处理单元302，具体用于：根据所述数据存储机构的公钥验证所述第二加密数据的签名。

一种可能的实现方式，所述请求响应包括所述第二加密数据及所述第二加密数据的签名；

收发单元 301，具体用于从所述区块链上获取所述第一数据的第三 hash 值；所述第三 hash 值是所述数据存储机构根据第一加密数据及所述第一加密数据的签名生成的；所述第一加密数据是所述数据存储机构根据所述数据请求机构的公钥对所述第一数据及所述第一数据的干扰值加密后得到的；

处理单元302，还用于根据所述第二加密数据及所述第二加密数据的签名，确定第四 hash 值；确认所述第三 hash 值和所述第四 hash 值一致。

一种可能的实现方式，所述请求响应包括第一加密数据在所述区块链上的地址；所述第一加密数据是所述数据存储机构根据所述数据请求机构的公钥对所述第一数据及所述第一数据的干扰值加密后得到的；所述地址是所述数据存储机构将所述第一加密数据上传至所述区块链后得到的；

处理单元302，还用于根据所述地址，获取所述第二加密数据。

一种可能的实现方式，所述请求响应包括二维码；所述二维码为所述数据存储机构根据第一加密数据生成的；所述第一加密数据是所述数据存储机构根据所述数据请求机构的公钥对所述第一数据及所述第一数据的干扰值加密后得到的；

所述收发单元，还用于通过所述数据存储机构发送的二维码，获取所述第二加密数据。

基于相同的发明构思，如图 4 所示，本发明实施例提供一种区块链的数据验证装置，包括:

收发单元 401，用于数据存储机构确定第一数据的干扰值;

处理单元 402，用于根据所述第一数据和所述第一数据的干扰值，生成所述第一数据的第一哈希 hash 值；通过区块链将所述第一 hash 值上链；所述第一 hash 值用于数据请求机构确定通过所述数据存储机构获得的加密数据是否与上链信息一致。

一种可能的实现方式，收发单元 401，还用于接收数据请求机构发送的数据请求；所述数据请求用于获取所述第一数据；向所述数据请求机构发送请求响应，所述数据响应用于所述数据请求机构获取所述数据存储机构提供的第二加密数据以使所述数据请求机构通过所述第二加密数据获得所述第一数据。

一种可能的实现方式，所述数据响应包括所述第二加密数据；所述第二加密数据是所述数据存储机构根据所述数据请求机构的公钥对所述第一数据及所述第一数据的干扰值加密后得到的；或

所述数据响应包括第一加密数据在所述区块链上的地址；所述第一加密数据是所述数据存储机构根据所述数据请求机构的公钥对所述第一数据及所述第一数据的干扰值加密后得到的；所述地址是所述数据存储机构将所述第一加密数据上传至所述区块链后得到的；或

所述数据响应包括二维码，所述二维码为所述数据存储机构根据第一加密数据生成的；所述第一加密数据是所述数据存储机构根据所述数据请求机构的公钥对所述第一数据及所述第一数据的干扰值加密后得到的;

一种可能的实现方式，处理单元 402，还用于使用所述数据请求机构的公钥对所述第一数据及所述第一数据的干扰值进行加密，得到第一加密数据；通过所述数据存储机构的私钥生成所述第一加密数据的签名；将所述第一加密数据及所述第一加密数据的签名生成第三 hash 值，并将所述第三 hash 值存储至所述区块链，以使所述数据请求机构验证所述请求响应。

请参见图 5，基于同一技术构思，本发明实施例还提供了一种计算机设备，用于执行数据请求机构或数据存储机构在本发明任一实施例中的方法，可以包括存储器 1001 和处理器 1002。

所述存储器 1001，用于存储处理器 1002 执行的计算机程序。存储器 1001 可主要包括存储程序区和存储数据区，其中，存储程序区可存储操作系统、至少一个功能所需的应用程序等；存储数据区可存储根据计算机设备的使用所创建的数据等。处理器 1002，可以是一个中央处理单元（central processing unit， CPU），或者为数字处理单元等等。本发明实施例中不限定上述存储器 1001 和处理器 1002 之间的具体连接介质。本发明实施例在图 5 中以存储器 1001 和处理器 1002 之间通过总线 1003 连接，总线 1003 在图 5 中以粗线表示，其它部件之间的连接方式，仅是进行示意性说明，并不引以为限。所述总线 1003 可以分为地址总线、数据总线、控制总线等。为便于表示，图 5 中仅用一条粗线表示，但并不表示仅有一根总线或一种类型的总线。

存储器 1001 可以是易失性存储器（volatile memory），例如随机存取存储器（random-access memory，RAM）；存储器 1001 也可以是非易失性存储器（non-volatile memory），例如只读存储器，快闪存储器（flash memory），硬盘（hard disk drive， HDD）或固态硬盘（solid-state drive， SSD）、或者存储器 1001 是能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质，但不限于此。存储器 1001 可以是上述存储器的组合。

处理器 1002，用于调用所述存储器 1001 中存储的计算机程序时执行本发明实施例提供的区块链的数据验证方法。

本发明实施例还提供了一种计算机存储介质，存储为执行上述处理器所需执行的计算机可执行指令，其包含用于执行上述处理器所需执行的程序。

在一些可能的实施方式中，本发提供的基于区块链的数据验证方法的各个方面还可以实现为一种程序产品的形式，其包括程序代码，当所述程序产品在计算机设备上运行时，所述程序代码用于使所述计算机设备执行本说明

书上述描述的根据本发明各种示例性实施提供的基于区块链的数据验证方法中的步骤，例如，所述计算机设备可以执行本发明实施例提供的基于区块链的数据验证方法。

所述程序产品可以采用一个或多个可读介质的任意组合。可读介质可以是可读信号介质或者可读存储介质。可读存储介质例如可以是——但不限于——电、磁、光、电磁、红外线、或半导体的系统、装置或器件，或者任意以上的组合。可读存储介质的更具体的例子（非穷举的列表）包括：具有一个或多个导线的电连接、便携式盘、硬盘、随机存取存储器（RAM）、只读存储器（ROM）、可擦式可编程只读存储器（EPROM 或闪存）、光纤、便携式紧凑盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。

本发明的实施方式中提供的基于区块链的数据验证方法的程序产品可以采用便携式紧凑盘只读存储器(CD-ROM)并包括程序代码，并可以在计算设备上运行。然而，本发明的程序产品不限于此，在本文件中，可读存储介质可以是任何包含或存储程序的有形介质，该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。

可读信号介质可以包括在基带中或者作为载波一部分传播的数据信号，其中承载了可读程序代码。这种传播的数据信号可以采用多种形式，包括——但不限于——电磁信号、光信号或上述的任意合适的组合。可读信号介质还可以是可读存储介质以外的任何可读介质，该可读介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。

可读介质上包含的程序代码可以用任何适当的介质传输，包括——但不限于——无线、有线、光缆、RF 等等，或者上述的任意合适的组合。

可以以一种或多种程序设计语言的任意组合来编写用于执行本发明操作的程序代码，所述程序设计语言包括面向对象的程序设计语言—诸如 Java、C++等，还包括常规的过程式程序设计语言—诸如“C”语言或类似的程序设计语言。程序代码可以完全地在用户计算设备上执行、部分地在用户设备上执

行、作为一个独立的软件包执行、部分在用户计算设备上部分在远程计算设备上执行、或者完全在远程计算设备或服务器上执行。在涉及远程计算设备的情形中，远程计算设备可以通过任意种类的网络——包括局域网（LAN）或广域网（WAN）—连接到用户计算设备，或者，可以连接到外部计算设备（例如利用因特网服务提供商来通过因特网连接）。

应当注意，尽管在上文详细描述中提及了装置的若干单元或子单元，但是这种划分仅仅是示例性的并非强制性的。实际上，根据本发明的实施方式，上文描述的两个或更多单元的特征和功能可以在一个单元中具体化。反之，上文描述的一个单元的特征和功能可以进一步划分为由多个单元来具体化。

此外，尽管在附图中以特定顺序描述了本发明方法的操作，但是，这并非要求或者暗示必须按照该特定顺序来执行这些操作，或是必须执行全部所示的操作才能实现期望的结果。附加地或备选地，可以省略某些步骤，将多个步骤合并为一个步骤执行，和/或将一个步骤分解为多个步骤执行。

本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

本发明是参照根据本发明实施例的方法、设备（系统）、和计算机程序产品的流程图和／或方框图来描述的。应理解可由计算机程序指令实现流程图和／或方框图中的每一流程和／或方框、以及流程图和／或方框图中的流程和／或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设

备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的步骤。

尽管已描述了本发明的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例做出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本发明范围的所有变更和修改。

显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

权 利 要 求

1、一种区块链的数据验证方法，其特征在于，包括：

数据请求机构向数据存储机构发送数据请求；所述数据请求用于获取第一数据；

所述数据请求机构获取所述数据存储机构返回的请求响应，以使所述数据请求机构获取第二加密数据；

所述数据请求机构解密所述第二加密数据，得到第二数据；

所述数据请求机构从区块链上获取所述第一数据的第一哈希 hash 值；所述第一 hash 值是所述数据存储机构根据所述第一数据及所述第一数据的干扰值生成并上传至所述区块链的；

所述数据请求机构在确认所述第一 hash 值和第二 hash 值一致时，从所述第二数据中得到所述第一数据；所述第二 hash 值是所述数据请求机构通过所述第二数据生成的。

2、如权利要求 1 所述的方法，其特征在于，所述请求响应包括所述第二加密数据；

所述数据请求机构解密所述第二加密数据，得到第二数据，包括：

所述数据请求机构根据所述数据请求机构的私钥解密所述第二加密数据，获得所述第二数据；所述第二加密数据为所述数据存储机构根据所述数据请求机构的公钥加密后获得的。

3、如权利要求 2 所述的方法，其特征在于，所述请求响应还包括所述第二加密数据的签名；所述第二加密数据的签名为所述数据存储机构通过所述数据存储机构的私钥对所述第二加密数据进行签名得到的；

所述数据请求机构解密所述第二加密数据，得到第二数据之前，还包括：

所述数据请求机构根据所述数据存储机构的公钥验证所述第二加密数据的签名。

4、如权利要求 1 所述的方法，其特征在于，所述请求响应包括所述第二

加密数据及所述第二加密数据的签名；

所述数据请求机构解密所述第二加密数据，得到第二数据之前，还包括：

所述数据请求机构从所述区块链上获取所述第一数据的第三 hash 值；所述第三 hash 值是所述数据存储机构根据第一加密数据及所述第一加密数据的签名生成的；所述第一加密数据是所述数据存储机构根据所述数据请求机构的公钥对所述第一数据及所述第一数据的干扰值加密后得到的；

所述数据请求机构根据所述第二加密数据及所述第二加密数据的签名，确定第四 hash 值；

所述数据请求机构确认所述第三 hash 值和所述第四 hash 值一致。

5、如权利要求 1 所述的方法，其特征在于，所述请求响应包括第一加密数据在所述区块链上的地址；所述第一加密数据是所述数据存储机构根据所述数据请求机构的公钥对所述第一数据及所述第一数据的干扰值加密后得到的；所述地址是所述数据存储机构将所述第一加密数据上传至所述区块链后得到的；

所述数据请求机构获取所述数据存储机构返回的请求响应，以使所述数据请求机构获取第二加密数据，包括：

所述数据请求机构根据所述地址，获取所述第二加密数据。

6、如权利要求 1 所述的方法，其特征在于，所述请求响应包括二维码；所述二维码为所述数据存储机构根据第一加密数据生成的；所述第一加密数据是所述数据存储机构根据所述数据请求机构的公钥对所述第一数据及所述第一数据的干扰值加密后得到的；

所述数据请求机构获取所述数据存储机构返回的请求响应，以使所述数据请求机构获取第二加密数据，包括：

所述数据请求机构通过所述数据存储机构发送的二维码，获取所述第二加密数据。

7、一种区块链的数据验证方法，其特征在于，包括：

数据存储机构确定第一数据的干扰值；

所述数据存储机构根据所述第一数据和所述第一数据的干扰值，生成所述第一数据的第一哈希 hash 值；

所述数据存储机构通过区块链将所述第一 hash 值上链；所述第一 hash 值用于数据请求机构确定通过所述数据存储机构获得的加密数据是否与上链信息一致。

8、如权利要求 7 所述的方法，其特征在于，所述方法还包括：

所述数据存储机构接收数据请求机构发送的数据请求；所述数据请求用于获取所述第一数据；

所述数据存储机构向所述数据请求机构发送请求响应，所述数据响应用于所述数据请求机构获取所述数据存储机构提供的第二加密数据以使所述数据请求机构通过所述第二加密数据获得所述第一数据。

9、如权利要求 8 所述的方法，其特征在于，所述数据响应用于所述数据请求机构获取所述数据存储机构提供的第二加密数据，包括：

所述数据响应包括所述第二加密数据；所述第二加密数据是所述数据存储机构根据所述数据请求机构的公钥对所述第一数据及所述第一数据的干扰值加密后得到的；或

所述数据响应包括第一加密数据在所述区块链上的地址；所述第一加密数据是所述数据存储机构根据所述数据请求机构的公钥对所述第一数据及所述第一数据的干扰值加密后得到的；所述地址是所述数据存储机构将所述第一加密数据上传至所述区块链后得到的；或

所述数据响应包括二维码，所述二维码为所述数据存储机构根据第一加密数据生成的；所述第一加密数据是所述数据存储机构根据所述数据请求机构的公钥对所述第一数据及所述第一数据的干扰值加密后得到的。

10、如权利要求 7 所述的方法，其特征在于，所述方法还包括：

所述数据存储机构使用所述数据请求机构的公钥对所述第一数据及所述第一数据的干扰值进行加密，得到第一加密数据；

所述数据存储机构通过所述数据存储机构的私钥生成所述第一加密数据

的签名；

所述数据存储机构将所述第一加密数据及所述第一加密数据的签名生成第三 hash 值，并将所述第三 hash 值存储至所述区块链，以使所述数据请求机构验证所述请求响应。

11、一种区块链的数据验证装置，其特征在于， 包括：

收发单元，用于向数据存储机构发送数据请求；所述数据请求用于获取第一数据；获取所述数据存储机构返回的请求响应，以使所述数据请求机构获取第二加密数据；

处理单元，用于解密所述第二加密数据，得到第二数据；从区块链上获取所述第一数据的第一哈希 hash 值；所述第一 hash 值是所述数据存储机构根据所述第一数据及所述第一数据的干扰值生成并上传至所述区块链的；在确认所述第一 hash 值和第二 hash 值一致时，从所述第二数据中得到所述第一数据；所述第二 hash 值是所述数据请求机构通过所述第二数据生成的。

12、一种区块链的数据验证装置，其特征在于，包括：

收发单元，用于数据存储机构确定第一数据的干扰值；

处理单元，用于根据所述第一数据和所述第一数据的干扰值，生成所述第一数据的第一哈希 hash 值；通过区块链将所述第一 hash 值上链；所述第一 hash 值用于数据请求机构确定通过所述数据存储机构获得的加密数据是否与上链信息一致。

13、一种计算机存储介质，其特征在于，所述计算机可读存储介质包括计算机程序，当计算机程序在计算机上运行时，使得所述计算机执行如权利要求 1 至 6 任一所述的方法或执行使得所述计算机执行如权利要求 7 至 10 任一所述的方法。

14、一种包含指令的计算机程序产品，其特征在于，当所述指令在计算机上运行时，使得所述计算机执行如权利要求 1 至 6 任一所述的方法或执行使得所述计算机执行如权利要求 7 至 10 任一所述的方法。

15、一种计算机设备，其特征在于，包括：

至少一个存储器，用于存储程序指令；

至少一个处理器，用于调用所述存储器中存储的程序指令，按照获得的程序执行如权利要求 1 至 6 任一所述的方法或执行使得所述计算机执行如权利要求 7 至 10 任一所述的方法。

5

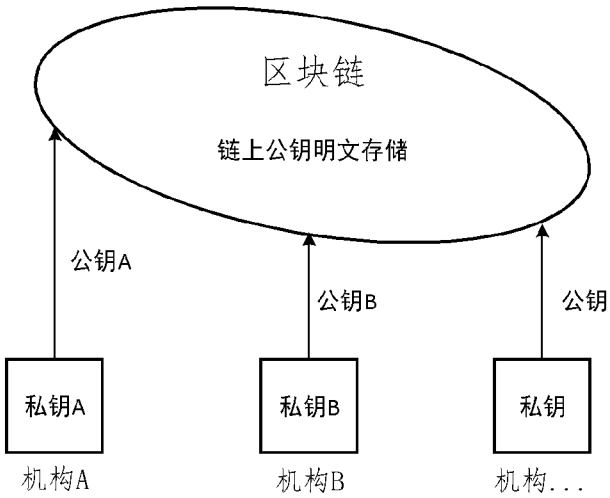
区块链
链上公钥明文存储
公钥A
公钥B
公钥
私钥A
私钥B
私钥
机构A
机构B
机构...

图 1a

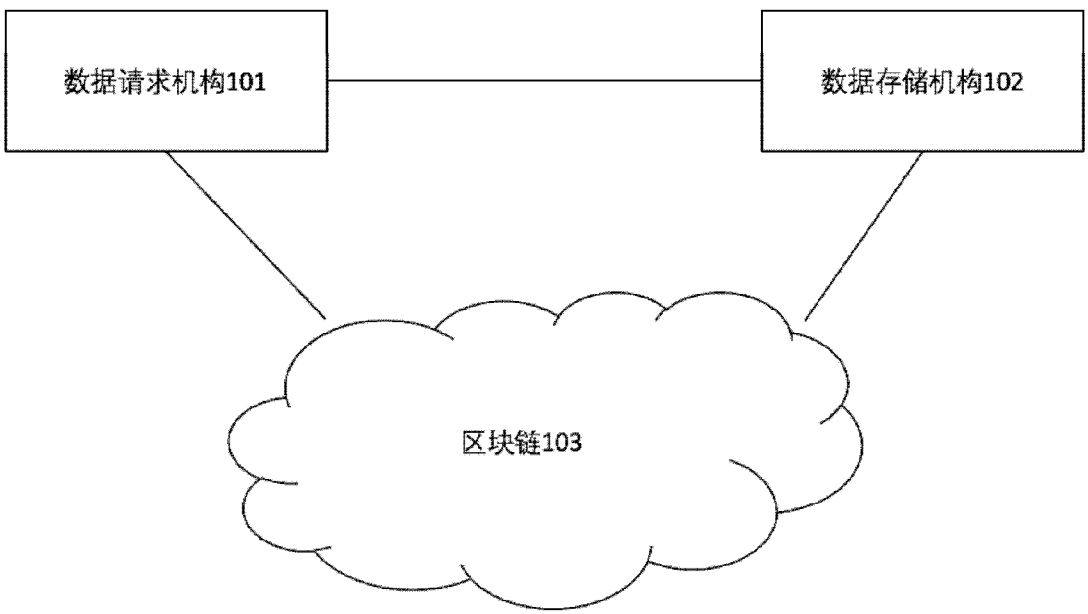
数据请求机构101
数据存储机构102
区块链103

图 1b

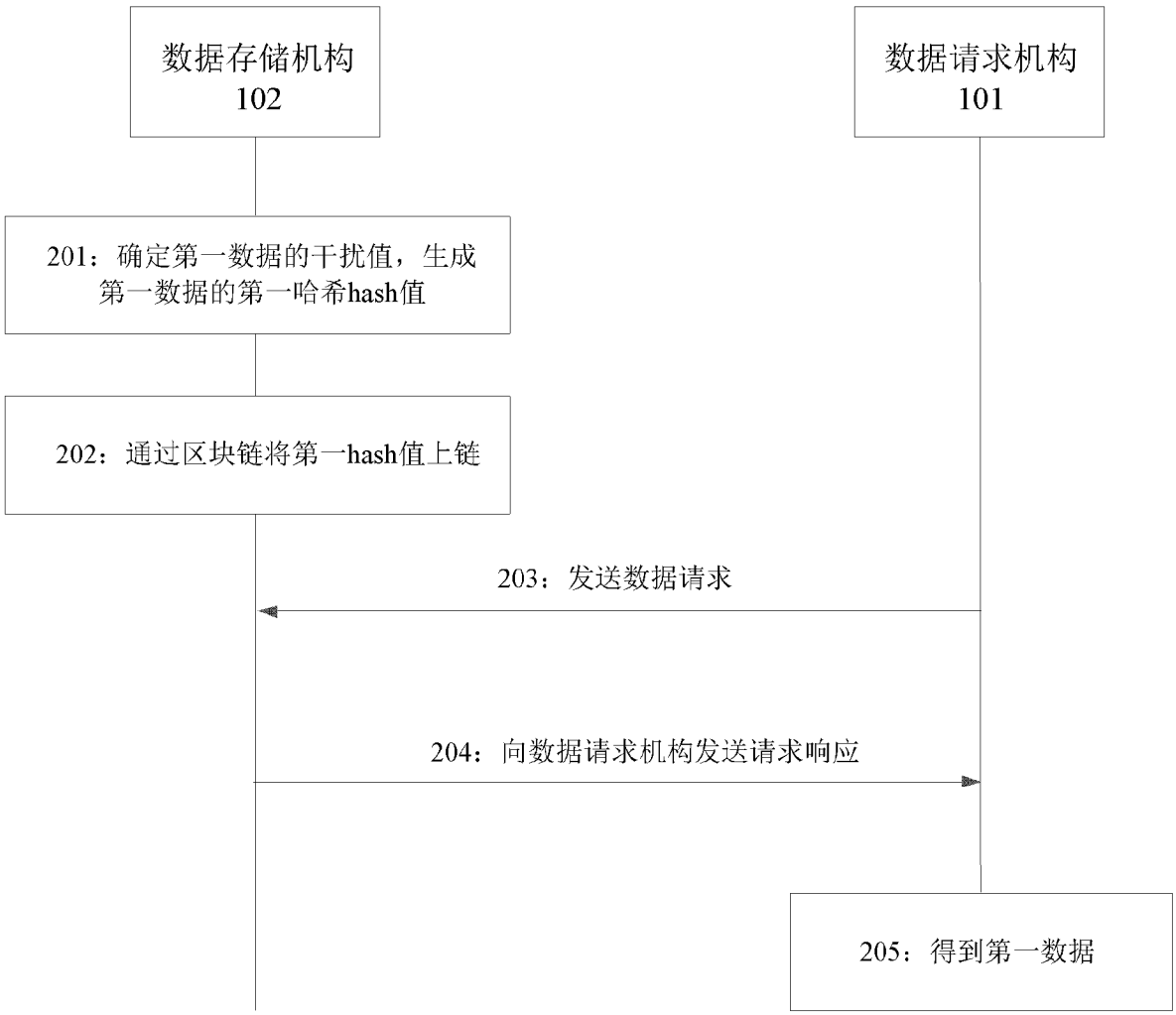
数据存储机构
102
数据请求机构
101
201：确定第一数据的干扰值，生成第一数据的第一哈希hash值
202：通过区块链将第一hash值上链
203：发送数据请求
204：向数据请求机构发送请求响应
205：得到第一数据

图 2

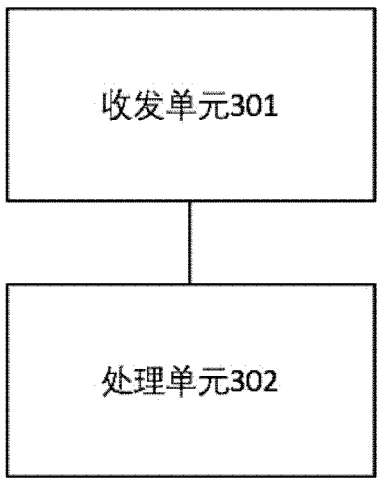
收发单元301
处理单元302

图 3

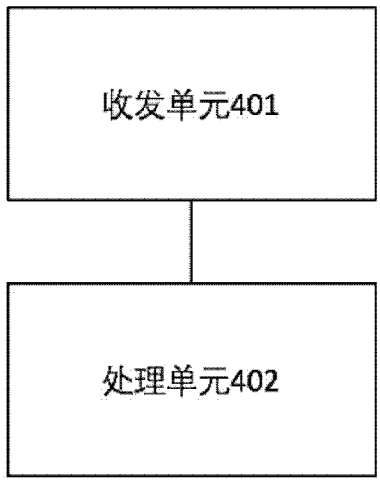

图 4

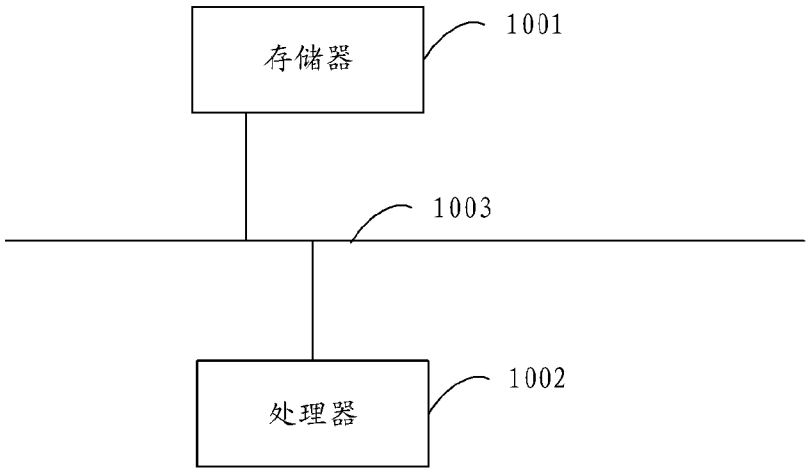

图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2020/082203

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, CNPAT, WPI, EPODOC, GOOGLE, IEEE: 区块链, 验证, 校验, 核验, 加密, 公钥, 哈希, 干扰, 随机, 盐值, block chain, verif+, hash, encrypt+, key, random, compar+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110188550 A (SHENZHEN QIANHAI WEBANK CO., LTD.) 30 August 2019 (2019-08-30) description, paragraphs [0005]-[0066]	1-15
X	CN 105610578 A (HANGZHOU FUZAMEI TECHNOLOGY CO., LTD.) 25 May 2016 (2016-05-25) description, paragraphs [0004]-[0017], and figures 1-2	1-15
A	CN 108833111 A (INSPUR GROUP CO., LTD.) 16 November 2018 (2018-11-16) entire document	1-15
A	JP 2007060336 A (TOHOKU INFORMATION SYSTEMS CO.) 08 March 2007 (2007-03-08) entire document	1-15

☐ 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
15 June 2020	**03 July 2020**
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**	Authorized officer
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2020/082203

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	110188550	A	30 August 2019	None	
CN	105610578	A	25 May 2016	None	
CN	108833111	A	16 November 2018	None	
JP	2007060336	A	08 March 2007	None	

国际检索报告

国际申请号 PCT/CN2020/082203

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, CNPAT, WPI, EPODOC, GOOGLE, IEEE: 区块链，验证，校验，核验，加密，公钥，哈希，干扰，随机，盐值，block chain, verif+, hash, encrypt+, key, random, compar+

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 110188550 A (深圳前海微众银行股份有限公司) 2019年 8月 30日 (2019-08-30) 说明书[0005]-[0066]段	1-15
X	CN 105610578 A (杭州复杂美科技有限公司) 2016年 5月 25日 (2016-05-25) 说明书[0004]-[0017]段，附图1-2	1-15
A	CN 108833111 A (浪潮软件集团有限公司) 2018年 11月 16日 (2018-11-16) 全文	1-15
A	JP 2007060336 A (TOHOKU INFORMATION SYSTEMS CO.) 2007年 3月 8日 (2007-03-08) 全文	1-15

☐ 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 6月 15日	2020年 7月 3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 吴瑶 电话号码 86-10-53961339

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2020/082203

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 110188550 A	2019年 8月 30日	无	
CN 105610578 A	2016年 5月 25日	无	
CN 108833111 A	2018年 11月 16日	无	
JP 2007060336 A	2007年 3月 8日	无	