

(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
2022 年 4 月 7 日 (07.04.2022)



(10) 国际公布号
WO 2022/068359 A1

- (51) 国际专利分类号:
G06F 21/60 (2013.01) **G06F 16/27** (2019.01)
G06F 21/64 (2013.01) **G06Q 40/04** (2012.01)
G06F 16/174 (2019.01)
- (21) 国际申请号: PCT/CN2021/109259
- (22) 国际申请日: 2021 年 7 月 29 日 (29.07.2021)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
202011053192.4 2020 年 9 月 29 日 (29.09.2020) CN
- (71) 申请人: 深圳壹账通智能科技有限公司(ONE CONNECT SMART TECHNOLOGY CO., LTD. (SHENZHEN)) [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 (入驻深圳市前海商务秘书有限公司), Guangdong 518000 (CN)。

(72) 发明人: 贾牧(JIA, Mu); 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 (入驻深圳市前海商务秘书有限公司), Guangdong 518000 (CN)。 谢丹力(XIE, Danli); 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 (入驻深圳市前海商务秘书有限公司), Guangdong 518000 (CN)。 陆陈一帆(LU, Frank YiFan Chen); 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 (入驻深圳市前海商务秘书有限公司), Guangdong 518000 (CN)。

(74) 代理人: 广州三环专利商标代理有限公司(SCIHEAD IP LAW FIRM); 中国广东省广州市

(54) Title: ENCRYPTION METHOD AND APPARATUS FOR COMPRESSING CIPHERTEXT OF INFORMATION, AND DEVICE AND MEDIUM

(54) 发明名称: 对信息的密文进行压缩的加密方法、装置、设备及介质

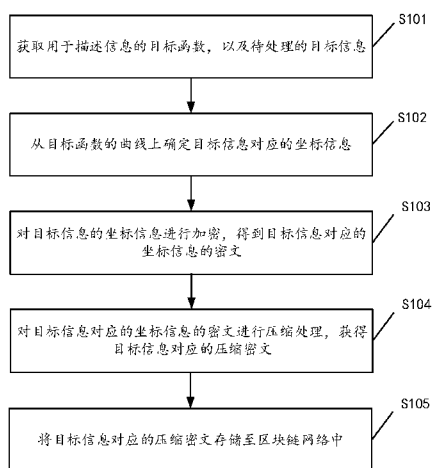


图 2

- S101 Acquire a target function for describing information, and target information to be processed
- S102 Determine, from a curve of the target function, coordinate information corresponding to the target information
- S103 Encrypt the coordinate information of the target information, so as to obtain ciphertext of the coordinate information corresponding to the target information
- S104 Compress the ciphertext of the coordinate information corresponding to the target information, so as to obtain compressed ciphertext corresponding to the target information
- S105 Store, in a blockchain network, the compressed ciphertext corresponding to the target information

(57) Abstract: An encryption method and apparatus for compressing ciphertext of information, and a device and a medium. The method comprises: acquiring a target function for describing information, and target information to be processed (S101); determining, from a curve of the target function, coordinate information corresponding to the target information (S102); encrypting the coordinate information of the target information, so as to obtain ciphertext of the coordinate information corresponding to the target information (S103); compressing the ciphertext of the coordinate information corresponding to the target information, so as to obtain compressed ciphertext corresponding to the target information (S104); and storing, in a blockchain network, the compressed ciphertext corresponding to the target information (S105).

(57) 摘要: 一种对信息的密文进行压缩的加密方法、装置、设备及介质。方法包括: 获取用于描述信息的目标函数, 以及待处理的目标信息 (S101); 从目标函数的曲线上确定目标信息对应的坐标信息 (S102); 对目标信息的坐标信息进行加密, 得到目标信息对应的坐标信息的密文 (S103); 对目标信息对应的坐标信息的密文进行压缩处理, 获得目标信息对应的压缩密文 (S104); 将目标信息对应的压缩密文存储至区块链网络中 (S105)。

越秀区先烈中路80号汇华商贸大厦1508室, Guangdong 510070 (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, IT, 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))。

对信息的密文进行压缩的加密方法、装置、设备及介质

本申请要求于 2020 年 9 月 29 日提交中国专利局、申请号为 202011053192.4, 发明名称为“对信息的密文进行压缩的加密方法、装置、设备及介质”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。

5 技术领域

本申请涉及区块链技术领域, 尤其涉及一种对信息的密文进行压缩的加密方法、装置、设备及介质。

背景技术

10 目前, 互联网正朝着移动化进一步发展, 社交网络等新兴内容也在不断兴起, 人们可以很方便的获取到想要的信息。然而, 随着需求和业务的不断发展, 所产生的数据也在呈几何式增长。大规模数据具有不可估量的价值, 数据间的关系将在公司企业的运营、决策中发挥重要作用。发明人意识到, 在大数据在集中处理和存储海量数据时, 如, 对医疗平台中大量患者的医疗数据进行存储和管理时, 用户数据对应的密文被存储在终端本地的数据库中, 容易被非法用户篡改, 导致不能根据目标信息的密文解密得到目标消息。同时, 15 将用户数据对应的密文直接存储, 容易造成存储空间不足的问题。

发明内容

本申请实施例提供一种对信息的密文进行压缩的加密方法、装置、设备及介质, 可以提高目标信息的安全性并节省存储空间。

20 第一方面, 本申请实施例提供了一种对信息的密文进行压缩的加密方法, 该方法包括: 获取用于描述信息的目标函数, 以及待处理的目标信息;

从所述目标函数的曲线上确定所述目标信息对应的坐标信息;

对所述目标信息的坐标信息进行加密, 得到所述目标信息对应的坐标信息的密文;

对所述目标信息对应的坐标信息的密文进行压缩处理, 获得所述目标信息对应的压缩密文;

25 将所述目标信息对应的压缩密文存储至区块链网络中。

第二方面, 本申请实施例提供了一种对信息的密文进行压缩的加密装置, 该装置包括:

第一获取模块, 用于获取用于描述信息的目标函数, 以及待处理的目标信息;

确定模块, 用于从所述目标函数的曲线上确定所述目标信息对应的坐标信息;

30 加密模块, 用于对所述目标信息的坐标信息进行加密, 得到所述目标信息对应的坐标信息的密文;

压缩模块, 用于对所述目标信息对应的坐标信息的密文进行压缩处理, 获得所述目标信息对应的压缩密文;

存储模块, 用于将所述目标信息对应的压缩密文存储至区块链网络中。

35 第三方面, 本申请实施例提供了一种电子设备, 该设备包括: 处理器, 适于实现一条或一条以上指令; 以及,

计算机存储介质, 所述计算机存储介质存储有一条或一条以上指令, 所述一条或一条以上指令适于由所述处理器加载并执行如下步骤:

获取用于描述信息的目标函数, 以及待处理的目标信息;

从所述目标函数的曲线上确定所述目标信息对应的坐标信息;

40 对所述目标信息的坐标信息进行加密, 得到所述目标信息对应的坐标信息的密文;

对所述目标信息对应的坐标信息的密文进行压缩处理, 获得所述目标信息对应的压缩密文;

将所述目标信息对应的压缩密文存储至区块链网络中。

第四方面, 本申请实施例提供了一种计算机可读存储介质, 所述计算机可读存储介质

存储有一条或一条以上指令,所述一条或一条以上指令适于由处理器加载并执行如下步骤:

获取用于描述信息的目标函数,以及待处理的目标信息;

从所述目标函数的曲线上确定所述目标信息对应的坐标信息;

对所述目标信息的坐标信息进行加密,得到所述目标信息对应的坐标信息的密文;

5 对所述目标信息对应的坐标信息的密文进行压缩处理,获得所述目标信息对应的压缩密文;

将所述目标信息对应的压缩密文存储至区块链网络中。

本申请实施例中,对目标信息对应的压缩密文进行存储时,可以降低目标信息对的密文的存储空间;将目标信息对应的压缩密文存储至区块链网络中,可有效避免将目标信息的密文存储至终端本地,导致目标信息的密文被篡改,导致不能根据目标信息的密文解密得到目标消息,提高目标信息的安全性。

附图说明

15 为了更清楚地说明本申请实施例技术方案,下面将对实施例描述中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图是本申请的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图获得其他的附图。

图 1a 是本申请实施例提供的一种对信息的密文进行压缩的加密系统的架构示意图;

图 1b 是本申请实施例提供的一种数据共享系统的示意图;

图 1c 是本申请实施例提供的一种区块链的结构示意图;

图 2 是本申请实施例提供的一种对信息的密文进行压缩的加密方法的流程示意图;

20 图 3 是本申请实施例提供的一种对目标信息对应的坐标信息的密文进行压缩处理方法的示意图;

图 4 是本申请实施例提供的另一种对信息的密文进行压缩的加密方法的流程示意图;

图 5 是本申请实施例提供的一种对信息的密文进行压缩的加密装置的结构示意图;

图 6 是本申请另一实施例提供的一种电子设备的结构示意图。

25 具体实施方式

下面将结合本申请实施例中的图,对本申请实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例是本申请一部分实施例,而不是全部的实施例。基于本申请中的实施例,本领域普通技术人员在没有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。

30 本申请可涉及人工智能技术领域,并可应用于基于区块链的数据加密场景。例如,可具体应用于数字医疗中的医疗数据加密场景,如区块链中可以存储医疗数据,该医疗数据可以包括个人健康档案、处方、检查报告等数据,进而可实现对该区块链中的医疗数据的加密处理。

35 本申请所涉及的区块链是一种分布式数据存储、点对点传输(P2P 传输)、共识机制、加密算法等计算机技术的新型应用模式,其本质上是一个去中心化的数据库,是一串使用密码学方法相关联产生的数据块,每一个数据块中包含了一批次网络交易的信息,用于验证其信息的有效性(防伪)和生成下一个区块。区块链可以包括区块链底层平台、平台产品服务层以及应用服务层;区块链可由多个借由密码学串接并保护内容的串连交易记录(又称区块)构成,用区块链所串接的分布式账本能让多方有效纪录交易,且可永久查验此交易(不可篡改)。其中,共识机制是指区块链网络中实现不同节点之间建立信任、获取权益的数学算法;也就是说,共识机制是区块链各网络节点共同认可的一种数学算法。

40 首先介绍本申请应用的对信息的密文进行压缩的加密系统的架构,如图 1a 所示。该系统架构示意图包括区块链网络及多个终端,图 1a 中以包括三个终端为例,分别为第一终端、第二终端和第三终端。其中,第一终端、第二终端和第三终端可用于从区块链网络获取目

标信息的密文，或者将目标信息的密文储存至区块链网络中。

其中，上述区块链网络可以是如图 1b 所示的区块链网络 100，区块链网络 100 是指用于进行节点设备与节点设备之间数据共享的系统，该区块链网络中可以包括多个节点设备 101，多个节点设备 101 可以是指区块链网络中各个客户端。每个节点设备 101 在进行正常工作可以接收到数据，并基于接收到的交易数据维护该区块链网络内的共享数据。为了保证区块链网络内的信息互通，区块链网络中的每个节点设备之间可以存在信息连接，节点设备之间可以通过上述信息连接进行信息传输。区块链网络中的每个节点设备均存储一条相同的区块链。区块链由多个区块组成，参见图 1c，区块链由多个区块组成，创始块中包括区块头和区块主体，区块头中存储有数据特征值、版本号、时间戳和难度值，区块主体中存储有数据；创始块的下一区块以创始块为父区块，下一区块中同样包括区块头和区块主体，区块头中存储有当前区块的数据特征值、父区块的区块头特征值、版本号、时间戳和难度值，并以此类推，使得区块链中每个区块中存储的区块数据均与父区块中存储的区块数据存在关联，保证了区块中数据的安全性。

其中，区块链网络中的节点设备、第一终端、第二终端和第三终端可以为计算机设备，包括手机、平板电脑、笔记本电脑、掌上电脑、智能音响、移动互联网设备（MID，mobile internet device）、POS（Point Of Sales，销售点）机、可穿戴设备（例如智能手表、智能手环等）等；还可以是一台独立的服务器、或由若干台服务器组成的服务器集群、或云计算中心；还可以是提供云服务、云数据库、云计算、云函数、云存储、网络服务、云通信、中间件服务、域名服务、安全服务、内容分发网络(Content Delivery Network, CDN)、以及大数据和人工智能平台等基础云计算服务的云服务器。

请参见图 2，为本申请实施例提供的一种对信息的密文进行压缩的加密方法的流程图，本申请实施例由电子设备来执行，该一种对信息的密文进行压缩的加密方法包括步骤 S101~S105。

S101，获取用于描述信息的目标函数，以及待处理的目标信息。

在本实施例中，目标函数用于描述目标信息，即将目标信息转化成目标函数对应的曲线上的坐标信息。目标函数可以是一种非对称椭圆曲线算法，椭圆曲线算法是基于椭圆曲线数学理论实现的加密算法。椭圆曲线算法的函数表达式为 $Y^2 = X^3 + aX + b$ ，对于椭圆曲线上的任一点坐标 (X, Y) 均满足 $Y^2 = X^3 + aX + b$ ，即可以根据已知的 X 计算出对应的 Y。因此，可以将目标信息转化为目标函数上的坐标信息，以此将目标信息存储至区块链网络中，提高目标信息的安全性。目标信息可以是指某机构的交易数据、营业数据等等。

S102，从目标函数的曲线上确定目标信息对应的坐标信息。

获取目标函数对应的曲线，将目标信息作为目标函数对应的曲线上的目标点的第一坐标，如目标点的 X 坐标。根据该目标点的第一坐标以及目标函数对应的曲线的表达式，获得目标函数对应曲线上的目标点的第二坐标，如 Y 坐标。根据目标函数对应的曲线的目标点的第一坐标以及第二坐标，获得目标信息对应的坐标信息。其中，目标函数可以是椭圆曲线对应的函数算法，也可以是其他曲线对应的函数。获取目标函数对应的曲线，目标函数对应的曲线可以是 prime256v1 曲线、secp256r1 曲线、nistp256 曲线、secp256k1 曲线等等。将目标信息作为目标函数对应的曲线上的目标点的第一坐标，即当目标信息的数据类型为数值类型，可以将目标信息作为目标函数对应的曲线上的目标点的第一坐标；或者，当目标信息的数据类型为非数值类型，可以根据数值型转化编码对该目标信息进行编码，得到数值类型的目标信息，将该数值类型的目标信息作为目标函数对应的曲线上的目标点的第一坐标。具体的，数值型转化编码包括：one-hot 编码（一种非数值型转化为数值型编码）、Label 编码（一种非数值型转化为数值型编码）、factorizing 编码（一种非数值型转化为数值型编码）等等。

例如，目标函数的曲线可以为椭圆曲线中的 secp256k1 曲线，椭圆曲线函数表达形式可以为 $Y^2=X^3+aX+b$ ，对于椭圆曲线上的任一点坐标 (X, Y) 均满足 $Y^2=X^3+aX+b$ ，即可以根据已知的 X 计算出对应的 Y。因此，若目标信息的数据类型为数值类型，可以将目标信息作为目标函数对应的 secp256k1 曲线上的目标点的 X 坐标，并根据 X 坐标获得对应的 Y 坐标；进一步，根据 secp256k1 曲线的函数表达式以及 X 坐标，计算获得目标函数对应的 secp256k1 曲线上的目标点的 Y 坐标；将目标点的 X 坐标和 Y 坐标，确定为目标信息对应的坐标信息。若目标信息的数据类型为非数值类型，为字符串类型，则根据 one-hot 编码对目标信息进行编码，得到数值类型的目标信息；将该数据类型的目标信息作为目标函数对应的 secp256r1 曲线上的目标点的 X 坐标；进一步，根据 secp256r1 曲线的函数表达式以及 X 坐标，计算获得目标函数对应的 secp256r1 曲线上的目标点的 Y 坐标；将目标点的 X 坐标和 Y 坐标，确定为目标信息对应的坐标信息，以此提高目标信息的安全性。

S103，对目标信息的坐标信息进行加密，得到目标信息对应的坐标信息的密文。

在本申请实施例，电子设备可以采用加密算法对目标信息进行加密，得到目标信息对应的坐标信息的密文，该加密算法可以包括但不限于 RSA 算法、Elgamal 算法、背包算法、Rabin 算法、D-H 算法、ECC（椭圆曲线加密算法）。RSA 算法、Elgamal 算法、背包算法、Rabin 算法、D-H 算法均为一种非对称算法。

可选的，获取目标信息对应的目标用户的用户信息；根据用户信息生成目标信息对应的密钥；采用目标信息对应的密钥，对目标信息对应的坐标信息进行加密，得到目标信息对应的坐标信息的密文。

目标信息对应的目标用户的用户信息包括但不限于用户账号、用户密码、用户电话号码等等。根据目标用户的用户信息生成目标信息对应的密钥，并采用目标信息对应的密钥对目标信息对应的坐标信息进行加密，得到目标信息对应的坐标信息的密文。具体的，可以获取目标信息对应的用户信息，根据目标信息对应的用户信息生成目标信息对应的随机数，根据目标信息对应随机数生成目标信息对应的密钥。例如，获取目标信息对应的用户账号，调用 C 语言中的 rand 函数，根据目标信息对应的用户账号生成目标信息对应的随机数，然后目标信息对应的随机数进行哈希运算，获得目标信息对应的密钥。采用该密钥对目标信息进行加密，得到目标信息对应的坐标信息的密文，这样可以增加对目标信息的密文进行解密的难度，避免目标信息的密文被非法用户破解，提高目标信息的安全性。

可选的，电子设备可以获取目标信息所属的终端的终端标识，根据目标信息所属的终端的终端标识生成该终端对应的私钥。然后根据该私钥以及目标信息对应的密钥，对目标信息对应的坐标信息进行加密，得到目标信息对应的坐标信息的密文。其中，得到目标信息对应的坐标信息的密文的具体实现方式包括：获取目标函数的曲线的基点坐标；获取该基点坐标与该终端的私钥的乘积，得到候选坐标；根据目标信息对应的密钥对该候选坐标进行加密，得到该候选坐标的密文；对目标信息对应的坐标信息与对应的候选坐标的密文进行融合，得到目标信息对应的坐标信息的密文。

例如，根据用于存储目标信息对应的压缩密文的目标区块的区块信息获得私钥 Q。获取目标函数对应的曲线为 secp256r1 曲线，获取该 secp256r1 曲线的基点坐标 G (Xg, Yg)，将上述私钥 Q 与该基点坐标做乘积，获得候选坐标 H，该候选坐标 $H=G*Q$ 。根据目标信息对应的密钥 K 对候选坐标 H 进行加密，得到该候选坐标的密文 P1，P 可以等于目标信息对应的密钥 K 与候选坐标的乘积，即 $P1=K*H$ 。得到目标信息对应的坐标信息为 P2 (X1, Y1) 后，对该目标信息对应的坐标信息 P2 (X1, Y1) 与对应的候选坐标的密文 P1 进行融合，得到该目标信息对应的坐标信息的密文 C。例如，可以将目标信息对应的坐标信息 P2 (X1, Y1) 与对应的候选坐标的密文 P1 相加，获得目标信息对应的坐标信息的密文 C，即 $C=P2+P1$ 。以此对目标信息对应的坐标信息进行加密，获得目标信息对应的坐标信息的

密文。

S104, 对目标信息对应的坐标信息的密文进行压缩处理, 获得目标信息对应的压缩密文。

S105, 将目标信息对应的压缩密文存储至区块链网络中。

在本申请实施例中, 目标信息对应的坐标信息包括第一坐标和第二坐标, 将目标信息对应的第一坐标以及第二坐标存储至区块链网络中时, 可以对目标信息对应的第一坐标以及第二坐标进行压缩处理。获得目标信息对应的第一坐标以及第二坐标的压缩密文后, 将目标信息对应的第一坐标以及第二坐标的压缩密文存储至区块链网络中, 可以降低区块链中节点设备的存储压力, 节省存储空间。同时, 区块链网络上存储的信息不可更改, 以此将目标信息的密文存储至区块链网络中, 可以避免目标信息的密文被非法用户篡改, 提高目标信息的安全性。

如图3所示, 本申请实施例提供的一种对目标信息对应的坐标信息的密文进行压缩处理方法的示意图, 如图3所述, 该一种对目标信息对应的坐标信息的密文进行压缩处理方法的步骤包括S21~S23。

S21, 获取数据截取长度, 该数据截取长度大于第一坐标的字节长度, 或者大于第二坐标的字节长度, 且小于第一坐标的字节长度与第二坐标的字节长度之和。

获取数据截取长度, 根据该数据截取长度对目标信息的密文进行截取, 该数据截取长度大于第一坐标的字节长度, 或者大于第二坐标的字节长度, 且小于第一坐标的字节长度与第二坐标的字节长度之和。其中, 由于第二坐标可以根据目标函数以及第一坐标得到, 因此可以储存第二坐标的密文的预设长度, 以便根据该第二坐标的密文的预设长度, 获得第二坐标的密文。如根据目标函数以及第一坐标得到多个候选第二坐标的密文时, 可以根据第二坐标的密文的预设长度, 在多个候选第二坐标的密文中获得与第二坐标的密文的预设长度中的内容匹配的候选第二坐标的密文, 作为第二坐标的密文。该第二坐标的密文的预设长度可以是第二坐标的密文的长度的一半, 也可以是第二坐标的密文的长度的三分之一等等。

S22, 从目标信息对应的坐标信息的密文中连续截取长度为数据截取长度的密文。

S23, 将截取得到的密文确定为目标信息对应的压缩密文。

根据数据截取长度, 从目标信息对应的坐标信息的密文中连续截取长度为数据截取长度的密文, 将截取得到的密文确定为目标信息对应的压缩密文。当然由于目标信息作为目标函数对应的曲线上的目标点的第一坐标, 因此截取得到的密文中需包括第一坐标的密文, 也可以包括第二坐标的预设长度的密文。连续截取是为了保证截取到的密文是连续的, 以便后续准确的还原出目标信息的密文。

可选的, 从目标信息对应的坐标信息的密文中截取第一坐标的密文, 以及第二坐标的密文的最低位; 将第一坐标的密文以及第二坐标的密文的最低位确定为截取得到的密文。

其中, 可以从目标信息对应的坐标信息的密文中截取第一坐标的密文, 以及第二坐标的密文的最低位。由于本实施例中是将目标信息作为目标函数对应的曲线上的目标点的第一坐标, 因此根据数据截取长度, 从目标信息对应的坐标信息的密文中截取第一坐标的密文。由于可以根据目标函数对应的曲线的表达式, 以及第一坐标, 可以获得第二坐标, 因此可以仅截取第二坐标的密文的最低位, 以便根据第二坐标的密文的最低位, 获取到目标信息的第二坐标。将第一坐标的密文以及第二坐标的密文的最低位确定为截取得到的密文。例如, 获取目标信息对应的第一坐标的密文以及第二坐标的密文后, 第一坐标的密文以及第二坐标的密文均为32Byte。根据数据截取长度, 连续截取第一坐标的密文, 以及截取第二坐标的密文中1Byte长度的密文, 将第一坐标的密文以及第二坐标的密文中1Byte长度的密文作为截取到的密文。若不对目标信息的第一坐标的密文以及第二坐标的密文进行截

取的话,需要占用 64Byte 的存储空间来存储目标信息的密文,容易导致存储空间不足的问题。根据数据截取长度对目标信息的第一坐标的密文以及第二坐标的密文进行截取后,获得目标信息的压缩密文,这样存储目标信息的压缩密文只需要占用 33Byte 的存储空间,将目标信息的压缩密文存储至区块链网络时可以降低区块链网络中节点设备的存储压力,节省存储空间。

可选的,在将目标信息的压缩密文存储至区块链网络中后,可以将终端本地的目标信息对应的压缩密文删除。由于目标信息的压缩密文存储至区块链网络中的目标区块后,需要获取目标信息时,可以在区块链网络中的目标区块中获取到目标信息的压缩密文,对目标信息的压缩密文进行解压缩以及解密以后就可以获得目标信息。同时由于区块链网络上存储的信息不可篡改,因此是可以根据区块链网络中的目标区块中目标信息的压缩密文得到目标信息。将终端本地的目标信息对应的压缩密文删除,可以降低终端本地的存储压力,节省存储空间。

本实施例可以适用于数字医疗领域的医疗信息化、电子信息档案管理等场景,上述目标信息可以是指患者的医疗数据,如医疗影像(链接+访问码)、影像标注、药方、诊断、治疗记录、费用单据等。通过根据目标函数获取患者的医疗数据对应的坐标信息,对患者的医疗数据对应的坐标信息进行加密,再采用数据截取长度对患者的医疗数据对应的密文进行截取,获得患者的医疗数据对应的压缩密文。并将患者的医疗数据对应的压缩密文存储至区块链网络中,这样可以降低存储空间,且提高患者的医疗数据的安全性,实现对患者的医疗数据的有效管理。

本申请实施例中,通过获取用于描述信息的目标函数,以及待处理的目标信息,从目标函数的曲线上确定目标信息对应的坐标信息;对目标信息的坐标信息进行加密,得到目标信息对应的坐标信息的密文;采用数据截取长度对目标信息对应的密文进行截取,获得目标信息对应的压缩密文,对目标信息对应的压缩密文进行存储时,可以降低目标信息对应的密文的存储空间,节省存储空间;将目标信息对应的压缩密文存储至区块链网络中,可有效避免将目标信息的密文存储至终端本地,导致目标信息的密文被篡改,导致不能根据目标信息的密文解密得到目标消息,提高目标信息的安全性。

如图 4 所示,为本实施例提供的另一种对信息的密文进行压缩的加密方法的流程示意图,如图 4 所示,该另一种对信息的密文进行压缩的加密方法的流程示意图包括步骤 S201-S209。

S201,获取用于描述信息的目标函数,以及待处理的目标信息。

S202,从目标函数的曲线上确定目标信息对应的坐标信息。

S203,对目标信息的坐标信息进行加密,得到目标信息对应的坐标信息的密文。

S204,对目标信息对应的坐标信息的密文进行压缩处理,获得目标信息对应的压缩密文。

S205,将目标信息对应的压缩密文存储至区块链网络中。

在本申请实施例中,步骤 S201-S205 的具体内容可以参看图 2 中所阐述的内容,在此不再累述。

S206,接收针对目标信息的获取请求。

S207,根据获取请求从区块链网络中获取目标信息对应的压缩密文。

当接收到针对目标信息的获取请求时,即接收到获取目标信息的明文内容的请求时,根据该获取请求从用于存储目标信息的区块链网络中,获取目标信息对应的压缩密文。

可选的,上述获取请求中包括目标信息的信息标识,从本地存储中获取信息标识与区块之间的对应关系;根据对应关系确定用于存储目标信息对应的压缩密文的目标区块;从区块链网络中的目标区块中获取目标信息对应的压缩密文。

根据目标信息的信息标识,从本地存储中获取信息标识与区块之间的对应关系。其中,每一信息标识均有对应的存储区块。根据信息标识与区块之间的对应关系,确定用于存储目标信息的压缩密文的目标区块。从区块链网络中的目标区块中的至少一个候选信息的信息标识中,获取与目标信息的信息标识匹配的信息的压缩密文,作为目标信息的压缩密文。

5 可选的,在将目标信息的压缩密文存储至区块链网络中时,可以获取用于储存目标信息对应的压缩密文的目标区块;构建目标区块与目标信息的信息标识之间的对应关系;将目标区块与目标信息的信息标识之间的对应关系储存至本地存储中。

10 将目标信息的压缩密文存储至区块链网络时,可以获取用于存储目标信息的压缩密文的目标区块的区块标识,构建目标信息的信息标识与目标区块的区块标识之间的对应关系,并将目标信息的信息标识与目标区块的区块标识之间的对应关系储存至本地存储中。这样在需要获取目标信息的压缩密文时,可以快速的获取到目标信息的压缩密文。

S208,对目标信息对应的压缩密文进行解压缩处理,得到目标信息对应的坐标信息的密文。

15 S209,对目标信息对应的坐标信息的密文进行解密,得到目标信息对应的坐标信息,根据目标信息对应的坐标信息确定目标信息。

获取目标信息的压缩密文后,对目标信息的压缩密文进行解压缩处理,得到目标信息对应的坐标信息的密文。在根据目标信息的密钥,对目标信息的密文进行解密,得到目标信息对应的坐标信息,根据目标信息对应的坐标信息确定目标信息。

20 可选的,目标信息对应的压缩密文包括第一坐标的密文以及第二坐标的密文的最低位,第一坐标和第二坐标为目标信息对应的坐标信息。可以从目标函数的曲线上获取第一坐标的密文对应候选第二坐标;将候选第二坐标中最低位与所述第二坐标的密文的最低位相同的候选第二坐标,作为所述第二坐标的密文;将第一坐标的密文以及第二坐标的密文确定为目标信息对应的坐标信息的密文。

25 对目标信息的压缩密文进行解压缩处理后,获得目标信息的第一坐标的密文,以及第二坐标的密文的最低位,第一坐标以及第二坐标为目标信息的坐标信息。可以获取目标信息对应的密钥,根据目标信息对应的密钥对第一坐标的密文进行解密,获得第一坐标。根据目标函数对应的曲线的表达式以及第一坐标,获得第一坐标对应的多个候选第二坐标。对第二坐标的密文的最低位进行解密,获得第二坐标的最低位的内容,根据第二坐标的最低位的内容,在多个候选第二坐标中最低位与第二坐标最低位的内容相同的候选第二坐标,作为第二坐标,根据第一坐标以及第二坐标,确定目标信息对应坐标信息。例如,目标函数对应的曲线为 secp256K1 曲线,目标信息中第一坐标为 secp256K1 曲线上目标点的 X 坐标,目标信息中第二坐标为 secp256K1 曲线上目标点的 Y 坐标。对第一坐标的密文进行解密,得到第一坐标后,根据第一坐标以及 secp256K1 曲线的表达式,获得多个候选第二坐标。由于 secp256K1 曲线为椭圆曲线,根据一个 X 坐标求解时,会获得多个候选 Y 坐标的值,因此,可以根据第二坐标的密文的最低位,在多个候选坐标中,确定与第二坐标的最低位的内容相同的候选 Y 坐标,作为第二坐标。

35 本申请实施例中,通过获取用于描述信息的目标函数,以及待处理的目标信息,从目标函数的曲线上确定目标信息对应的坐标信息;对目标信息的坐标信息进行加密,得到目标信息对应的坐标信息的密文;采用数据截取长度对目标信息对应的密文进行截取,获得目标信息对应的压缩密文,对目标信息对应的压缩密文进行存储时,可以降低目标信息对应的密文的存储空间,节省存储空间;将目标信息对应的压缩密文存储至区块链网络中,可有效避免将目标信息的密文存储至终端本地,导致目标信息的密文被篡改,导致不能根据目标信息的密文解密得到目标消息,提高目标信息的安全性。在需要获取目标信息时,可以对目标信息对应的压缩密文进行解压缩处理,得到目标信息对应的坐标信息的密文;对

目标信息对应的坐标信息的密文进行解密，得到目标信息。

请参见图 5，是本申请实施例提供的一种对信息的密文进行压缩的加密装置的结构示意图，本申请实施例的所述装置可以在上述提及的电子设备中。本实施例中，该对信息的密文进行压缩的加密装置包括：

5 第一获取模块 11，用于获取用于描述信息的目标函数，以及待处理的目标信息。

确定模块 12，用于从目标函数的曲线上确定目标信息对应的坐标信息。

加密模块 13，用于对目标信息的坐标信息进行加密，得到目标信息对应的坐标信息的密文。

其中，所述加密模块 13 包括：第四获取单元、生成单元、加密单元。

10 第四获取单元，用于获取所述目标信息对应的目标用户的用户信息；

生成单元，用于根据所述用户信息生成所述目标信息对应的密钥；

加密单元，用于采用所述目标信息对应的密钥，对所述目标信息对应的坐标信息进行加密，得到所述目标信息对应的坐标信息的密文。

15 压缩模块 14，用于对目标信息对应的坐标信息的密文进行压缩处理，获得目标信息对应的压缩密文。

上述压缩模块 14 包括：第一获取单元、截取单元、第一确定单元。

第一获取单元，用于获取数据截取长度，所述数据截取长度大于所述第一坐标的字节长度，或者大于所述第二坐标的字节长度，且小于所述第一坐标的字节长度与所述第二坐标的字节长度之和；

20 截取单元，用于从所述目标信息对应的坐标信息的密文中连续截取长度为所述数据截取长度的密文；

第一确定单元，用于将截取得到的密文确定为所述目标信息对应的压缩密文。

其中，所述截取单元具体用于：

25 从所述目标信息对应的坐标信息的密文中截取所述第一坐标的密文，以及所述第二坐标的密文的最低位；

将所述第一坐标的密文以及所述第二坐标的密文的最低位确定为所述截取得到的密文。

存储模块 15，用于将所述目标信息对应的压缩密文存储至区块链网络中。

其中，所述目标信息对应的坐标信息包括第一坐标和第二坐标；

其中，所述装置还包括：

30 接收模块，用于接收针对所述目标信息的获取请求；

第二获取模块，用于根据所述获取请求从所述区块链网络中获取所述目标信息对应的压缩密文；

解压缩模块，用于对所述目标信息对应的压缩密文进行解压缩处理，得到所述目标信息对应的坐标信息的密文；

35 解密模块，用于对所述目标信息对应的坐标信息的密文进行解密，得到所述目标信息对应的坐标信息，根据所述目标信息对应的坐标信息确定所述目标信息。

其中，所述目标信息对应的压缩密文包括所述第一坐标的密文以及所述第二坐标的密文的最低位，所述第一坐标和所述第二坐标为所述目标信息对应的坐标信息；

所述解压缩模块包括：

40 第二获取单元，用于从所述目标函数的曲线上获取所述第一坐标的密文对应候选第二坐标；

第二确定单元，用于将所述候选第二坐标中最低位与所述第二坐标的密文的最低位相同的候选第二坐标，作为所述第二坐标的密文；

第三确定单元，用于将所述第一坐标的密文以及所述第二坐标的密文确定为所述目标

信息对应的坐标信息的密文。

其中，所述获取请求中包括所述目标信息的信息标识，所述第二获取模块包括：

第四确定单元，用于从本地存储中获取信息标识与区块之间的对应关系；根据所述对应关系确定用于存储所述目标信息对应的压缩密文的目标区块；

5 第三获取单元，用于从所述区块链网络中的目标区块中获取所述目标信息对应的压缩密文。

本申请实施例中，通过获取用于描述信息的目标函数，以及待处理的目标信息，从目标函数的曲线上确定目标信息对应的坐标信息；对目标信息的坐标信息进行加密，得到目标信息对应的坐标信息的密文；采用数据截取长度对目标信息对应的密文进行截取，获得目标信息对应的压缩密文，对目标信息对应的压缩密文进行存储时，可以降低目标信息对应的密文的存储空间，节省存储空间；将目标信息对应的压缩密文存储至区块链网络中，可有效避免将目标信息的密文存储至终端本地，导致目标信息的密文被篡改，导致不能根据目标信息的密文解密得到目标消息，提高目标信息的安全性。在需要获取目标信息时，可以对目标信息对应的压缩密文进行解压缩处理，得到目标信息对应的坐标信息的密文；对目标信息对应的坐标信息的密文进行解密，得到目标信息。

10 请参见图 6，是本申请实施例提供的一种电子设备的结构示意图，该电子设备还可以叫做计算机设备，包括处理器和存储器。可选的，该电子设备还可以包括网络接口，处理器与存储器、网络接口相连。进一步可选的，该网络接口可以包括输入装置和输出装置中的至少一种，或者，该电子设备还可包括输入装置和输出装置中的至少一种。例如，如图 20 6 所示的本实施例中的电子设备可以包括：一个或多个处理器 21；一个或多个输入装置 22，一个或多个输出装置 23 和存储器 24。上述处理器 21、输入装置 22、输出装置 23 和存储器 24 通过总线 25 连接。

所处理器 21 可以是中央处理单元(Central Processing Unit, CPU)，该处理器还可以是其他通用处理器、数字信号处理器 (Digital Signal Processor, DSP)、专用集成电路 (Application Specific Integrated Circuit, ASIC)、现成可编程门阵列 (Field-Programmable Gate Array, FPGA) 或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

30 输入装置 22 可以包括触控板、指纹采传感器（用于采集用户的指纹信息和指纹的方向信息）、麦克风等，输出装置 23 可以包括显示器 (LCD 等)、扬声器等，输出装置 23 可以输出校正处理后的数据表。

该存储器 24 可以包括只读存储器和随机存取存储器，并向处理器 21 提供指令和数据。存储器 24 的一部分还可以包括非易失性随机存取存储器，存储器 24 用于存储计算机程序，所述计算机程序包括程序指令，处理器 21 用于执行存储器 24 存储的程序指令，以用于执行一种对信息的密文进行压缩的加密方法，即用于执行以下操作：

35 获取用于描述信息的目标函数，以及待处理的目标信息；

从所述目标函数的曲线上确定所述目标信息对应的坐标信息；

对所述目标信息的坐标信息进行加密，得到所述目标信息对应的坐标信息的密文；

对所述目标信息对应的坐标信息的密文进行压缩处理，获得所述目标信息对应的压缩密文；

40 将所述目标信息对应的压缩密文存储至区块链网络中。

可选的，处理器 21 用于执行存储器 24 存储的程序指令，用于执行以下操作：

获取数据截取长度，所述数据截取长度大于所述第一坐标的字节长度，或者大于所述第二坐标的字节长度，且小于所述第一坐标的字节长度与所述第二坐标的字节长度之和；

从所述目标信息对应的坐标信息的密文中连续截取长度为所述数据截取长度的密文；

将截取得到的密文确定为所述目标信息对应的压缩密文。

可选的，处理器 21 用于执行存储器 24 存储的程序指令，用于执行以下操作：

从所述目标信息对应的坐标信息的密文中截取所述第一坐标的密文，以及所述第二坐标的密文的最低位；

5 将所述第一坐标的密文以及所述第二坐标的密文的最低位确定为所述截取得到的密文。

可选的，处理器 21 用于执行存储器 24 存储的程序指令，用于执行以下操作：

接收针对所述目标信息的获取请求；

根据所述获取请求从所述区块链网络中获取所述目标信息对应的压缩密文；

10 对所述目标信息对应的压缩密文进行解压缩处理，得到所述目标信息对应的坐标信息的密文；

对所述目标信息对应的坐标信息的密文进行解密，得到所述目标信息对应的坐标信息，根据所述目标信息对应的坐标信息确定所述目标信息。

可选的，处理器 21 用于执行存储器 24 存储的程序指令，用于执行以下操作：

从所述目标函数的曲线上获取所述第一坐标的密文对应候选第二坐标；

15 将所述候选第二坐标中最低位与所述第二坐标的密文的最低位相同的候选第二坐标，作为所述第二坐标的密文；

将所述第一坐标的密文以及所述第二坐标的密文确定为所述目标信息对应的坐标信息的密文。

可选的，处理器 21 用于执行存储器 24 存储的程序指令，用于执行以下操作：

20 从本地存储中获取信息标识与区块之间的对应关系；根据所述对应关系确定用于存储所述目标信息对应的压缩密文的目标区块；

从所述区块链网络中的目标区块中获取所述目标信息对应的压缩密文。

可选的，处理器 21 用于执行存储器 24 存储的程序指令，用于执行以下操作：

获取所述目标信息对应的目标用户的用户信息；

25 根据所述用户信息生成所述目标信息对应的密钥；

采用所述目标信息对应的密钥，对所述目标信息对应的坐标信息进行加密，得到所述目标信息对应的坐标信息的密文。

30 本申请实施例中所描述的处理器 21、输入装置 22、输出装置 23 可执行本申请实施例提供的对信息的密文进行压缩的加密方法的实施例中所描述的实现方式，也可执行本申请实施例所描述的电子设备的实现方式，在此不再赘述。

35 本申请实施例中，通过获取用于描述信息的目标函数，以及待处理的目标信息，从目标函数的曲线上确定目标信息对应的坐标信息；对目标信息的坐标信息进行加密，得到目标信息对应的坐标信息的密文；采用数据截取长度对目标信息对应的密文进行截取，获得目标信息对应的压缩密文，对目标信息对应的压缩密文进行存储时，可以降低目标信息对应的密文的存储空间，节省存储空间；将目标信息对应的压缩密文存储至区块链网络中，可有效避免将目标信息的密文存储至终端本地，导致目标信息的密文被篡改，导致不能根据目标信息的密文解密得到目标消息，提高目标信息的安全性。在需要获取目标信息时，可以对目标信息对应的压缩密文进行解压缩处理，得到目标信息对应的坐标信息的密文；对目标信息对应的坐标信息的密文进行解密，得到目标信息。

40 本申请实施例中还提供一种计算机可读存储介质，所述计算机可读存储介质存储有计算机程序，所述计算机程序包括程序指令，所述程序指令被处理器执行时实现如图 2 及图 4 实施例所示的对信息的密文进行压缩的加密方法。

可选的，本申请涉及的存储介质可以为可读存储介质，本申请涉及的存储介质如计算机可读存储介质可以是非易失性的，也可以是易失性的。

所述计算机可读存储介质可以是前述任一实施例所述的电子设备的内部存储单元，例如电子设备的硬盘或内存。所述计算机可读存储介质也可以是所述电子设备的外部存储设备，例如所述电子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。进一步地，所述计算机可读存储介质还可以既包括所述电子设备的内部存储单元也包括外部存储设备。所述计算机可读存储介质用于存储所述计算机程序以及所述电子设备所需的其他程序和数据。所述计算机可读存储介质还可以用于暂时地存储已经输出或者将要输出的数据。

本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、计算机软件或者二者的结合来实现，为了清楚地说明硬件和软件的可互换性，在上述说明中已经按照功能一般性地描述了各示例的组成及步骤。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。所属领域的技术人员可以清楚地了解到，为了描述的方便和简洁，上述描述的电子设备和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

在本申请所提供的几个实施例中，应该理解到，所揭露的电子设备和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例是示意性的，例如，所述单元的划分，可以为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。

以上所述，仅为本申请的具体实施方式，但本申请的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本申请揭露的技术范围内，可轻易想到各种等效的修改或替换，这些修改或替换都应涵盖在本申请的保护范围之内。因此，本申请的保护范围应以权利要求的保护范围为准。

权利要求

1、一种对信息的密文进行压缩的加密方法，包括：

获取用于描述信息的目标函数，以及待处理的目标信息；

从所述目标函数的曲线上确定所述目标信息对应的坐标信息；

5 对所述目标信息的坐标信息进行加密，得到所述目标信息对应的坐标信息的密文；

对所述目标信息对应的坐标信息的密文进行压缩处理，获得所述目标信息对应的压缩密文；

将所述目标信息对应的压缩密文存储至区块链网络中。

10 2、根据权利要求1所述的方法，其中，所述目标信息对应的坐标信息包括第一坐标和第二坐标；所述对所述目标信息对应的坐标信息的密文进行压缩处理，获得所述目标信息对应的压缩密文，包括：

获取数据截取长度，所述数据截取长度大于所述第一坐标的字节长度，或者大于所述第二坐标的字节长度，且小于所述第一坐标的字节长度与所述第二坐标的字节长度之和；

从所述目标信息对应的坐标信息的密文中连续截取长度为所述数据截取长度的密文；

15 将截取得到的密文确定为所述目标信息对应的压缩密文。

3、根据权利要求2所述的方法，其中，所述从所述目标信息对应的坐标信息的密文中连续截取长度为所述数据截取长度的密文，包括：

从所述目标信息对应的坐标信息的密文中截取所述第一坐标的密文，以及所述第二坐标的密文的最低位；

20 将所述第一坐标的密文以及所述第二坐标的密文的最低位确定为所述截取得到的密文。

4、根据权利要求3所述的方法，其中，所述方法还包括：

接收针对所述目标信息的获取请求；

根据所述获取请求从所述区块链网络中获取所述目标信息对应的压缩密文；

25 对所述目标信息对应的压缩密文进行解压缩处理，得到所述目标信息对应的坐标信息的密文；

对所述目标信息对应的坐标信息的密文进行解密，得到所述目标信息对应的坐标信息，根据所述目标信息对应的坐标信息确定所述目标信息。

30 5、根据权利要求4所述的方法，其中，所述目标信息对应的压缩密文包括所述第一坐标的密文以及所述第二坐标的密文的最低位，所述第一坐标和所述第二坐标为所述目标信息对应的坐标信息；

所述对所述目标信息对应的压缩密文进行解压缩处理，得到所述目标信息对应的坐标信息的密文，包括：

从所述目标函数的曲线上获取所述第一坐标的密文对应候选第二坐标；

35 将所述候选第二坐标中最低位与所述第二坐标的密文的最低位相同的候选第二坐标，作为所述第二坐标的密文；

将所述第一坐标的密文以及所述第二坐标的密文确定为所述目标信息对应的坐标信息的密文。

6、根据权利要求4所述的方法，其中，所述获取请求中包括所述目标信息的信息标识，所述根据所述获取请求从所述区块链网络中获取所述目标信息对应的压缩密文，包括：

40 从本地存储中获取信息标识与区块之间的对应关系；根据所述对应关系确定用于存储所述目标信息对应的压缩密文的目标区块；

从所述区块链网络中的目标区块中获取所述目标信息对应的压缩密文。

7、根据权利要求1所述的方法，其中，所述对所述目标信息的坐标信息进行加密，得到所述目标信息对应的坐标信息的密文，包括：

获取所述目标信息对应的目标用户的用户信息；

根据所述用户信息生成所述目标信息对应的密钥；

采用所述目标信息对应的密钥，对所述目标信息对应的坐标信息进行加密，得到所述目标信息对应的坐标信息的密文。

5 8、一种对信息的密文进行压缩的加密装置，包括：

第一获取模块，用于获取用于描述信息的目标函数，以及待处理的目标信息；

确定模块，用于从所述目标函数的曲线上确定所述目标信息对应的坐标信息；

加密模块，用于对所述目标信息的坐标信息进行加密，得到所述目标信息对应的坐标信息的密文；

10 压缩模块，用于对所述目标信息对应的坐标信息的密文进行压缩处理，获得所述目标信息对应的压缩密文；

存储模块，用于将所述目标信息对应的压缩密文存储至区块链网络中。

9、一种计算机设备，包括：处理器、存储器以及网络接口；

15 所述处理器与存储器、网络接口相连，其中，网络接口用于提供数据通信功能，所述存储器用于存储程序代码，所述处理器用于调用所述程序代码，以执行以下方法：

获取用于描述信息的目标函数，以及待处理的目标信息；

从所述目标函数的曲线上确定所述目标信息对应的坐标信息；

对所述目标信息的坐标信息进行加密，得到所述目标信息对应的坐标信息的密文；

20 对所述目标信息对应的坐标信息的密文进行压缩处理，获得所述目标信息对应的压缩密文；

将所述目标信息对应的压缩密文存储至区块链网络中。

10、根据权利要求 9 所述的计算机设备，其中，所述目标信息对应的坐标信息包括第一坐标和第二坐标；执行所述对所述目标信息对应的坐标信息的密文进行压缩处理，获得所述目标信息对应的压缩密文，包括：

25 获取数据截取长度，所述数据截取长度大于所述第一坐标的字节长度，或者大于所述第二坐标的字节长度，且小于所述第一坐标的字节长度与所述第二坐标的字节长度之和；

从所述目标信息对应的坐标信息的密文中连续截取长度为所述数据截取长度的密文；

将截取得到的密文确定为所述目标信息对应的压缩密文。

30 11、根据权利要求 10 所述的计算机设备，其中，执行所述从所述目标信息对应的坐标信息的密文中连续截取长度为所述数据截取长度的密文，包括：

从所述目标信息对应的坐标信息的密文中截取所述第一坐标的密文，以及所述第二坐标的密文的最低位；

将所述第一坐标的密文以及所述第二坐标的密文的最低位确定为所述截取得到的密文。

12、根据权利要求 11 所述的计算机设备，其中，所述处理器还用于执行：

35 接收针对所述目标信息的获取请求；

根据所述获取请求从所述区块链网络中获取所述目标信息对应的压缩密文；

对所述目标信息对应的压缩密文进行解压缩处理，得到所述目标信息对应的坐标信息的密文；

40 对所述目标信息对应的坐标信息的密文进行解密，得到所述目标信息对应的坐标信息，根据所述目标信息对应的坐标信息确定所述目标信息。

13、根据权利要求 12 所述的计算机设备，其中，所述目标信息对应的压缩密文包括所述第一坐标的密文以及所述第二坐标的密文的最低位，所述第一坐标和所述第二坐标为所述目标信息对应的坐标信息；

执行所述对所述目标信息对应的压缩密文进行解压缩处理，得到所述目标信息对应的

坐标信息的密文，包括：

从所述目标函数的曲线上获取所述第一坐标的密文对应候选第二坐标；

将所述候选第二坐标中最低位与所述第二坐标的密文的最低位相同的候选第二坐标，
作为所述第二坐标的密文；

5 将所述第一坐标的密文以及所述第二坐标的密文确定为所述目标信息对应的坐标信息的密文。

14、根据权利要求12所述的计算机设备，其中，所述获取请求中包括所述目标信息的信息标识，执行所述根据所述获取请求从所述区块链网络中获取所述目标信息对应的压缩密文，包括：

10 从本地存储中获取信息标识与区块之间的对应关系；根据所述对应关系确定用于存储所述目标信息对应的压缩密文的目标区块；

从所述区块链网络中的目标区块中获取所述目标信息对应的压缩密文。

15、一种计算机可读存储介质，其中，所述计算机可读存储介质存储有计算机程序，所述计算机程序包括程序指令，所述程序指令当被处理器执行时，执行以下方法：

15 获取用于描述信息的目标函数，以及待处理的目标信息；

从所述目标函数的曲线上确定所述目标信息对应的坐标信息；

对所述目标信息的坐标信息进行加密，得到所述目标信息对应的坐标信息的密文；

对所述目标信息对应的坐标信息的密文进行压缩处理，获得所述目标信息对应的压缩密文；

20 将所述目标信息对应的压缩密文存储至区块链网络中。

16、根据权利要求15所述的计算机可读存储介质，其中，所述目标信息对应的坐标信息包括第一坐标和第二坐标；执行所述对所述目标信息对应的坐标信息的密文进行压缩处理，获得所述目标信息对应的压缩密文，包括：

25 获取数据截取长度，所述数据截取长度大于所述第一坐标的字节长度，或者大于所述第二坐标的字节长度，且小于所述第一坐标的字节长度与所述第二坐标的字节长度之和；

从所述目标信息对应的坐标信息的密文中连续截取长度为所述数据截取长度的密文；

将截取得到的密文确定为所述目标信息对应的压缩密文。

17、根据权利要求16所述的计算机可读存储介质，其中，执行所述从所述目标信息对应的坐标信息的密文中连续截取长度为所述数据截取长度的密文，包括：

30 从所述目标信息对应的坐标信息的密文中截取所述第一坐标的密文，以及所述第二坐标的密文的最低位；

将所述第一坐标的密文以及所述第二坐标的密文的最低位确定为所述截取得到的密文。

18、根据权利要求17所述的计算机可读存储介质，其中，所述程序指令当被处理器执行时，还用于执行：

35 接收针对所述目标信息的获取请求；

根据所述获取请求从所述区块链网络中获取所述目标信息对应的压缩密文；

对所述目标信息对应的压缩密文进行解压缩处理，得到所述目标信息对应的坐标信息的密文；

40 对所述目标信息对应的坐标信息的密文进行解密，得到所述目标信息对应的坐标信息，根据所述目标信息对应的坐标信息确定所述目标信息。

19、根据权利要求18所述的计算机可读存储介质，其中，所述目标信息对应的压缩密文包括所述第一坐标的密文以及所述第二坐标的密文的最低位，所述第一坐标和所述第二坐标为所述目标信息对应的坐标信息；

执行所述对所述目标信息对应的压缩密文进行解压缩处理，得到所述目标信息对应的

坐标信息的密文，包括：

从所述目标函数的曲线上获取所述第一坐标的密文对应候选第二坐标；

将所述候选第二坐标中最低位与所述第二坐标的密文的最低位相同的候选第二坐标，
作为所述第二坐标的密文；

5 将所述第一坐标的密文以及所述第二坐标的密文确定为所述目标信息对应的坐标信息的密文。

20、根据权利要求 18 所述的计算机可读存储介质，其中，所述获取请求中包括所述目标信息的信息标识，执行所述根据所述获取请求从所述区块链网络中获取所述目标信息对应的压缩密文，包括：

10 从本地存储中获取信息标识与区块之间的对应关系；根据所述对应关系确定用于存储所述目标信息对应的压缩密文的目标区块；

从所述区块链网络中的目标区块中获取所述目标信息对应的压缩密文。

15

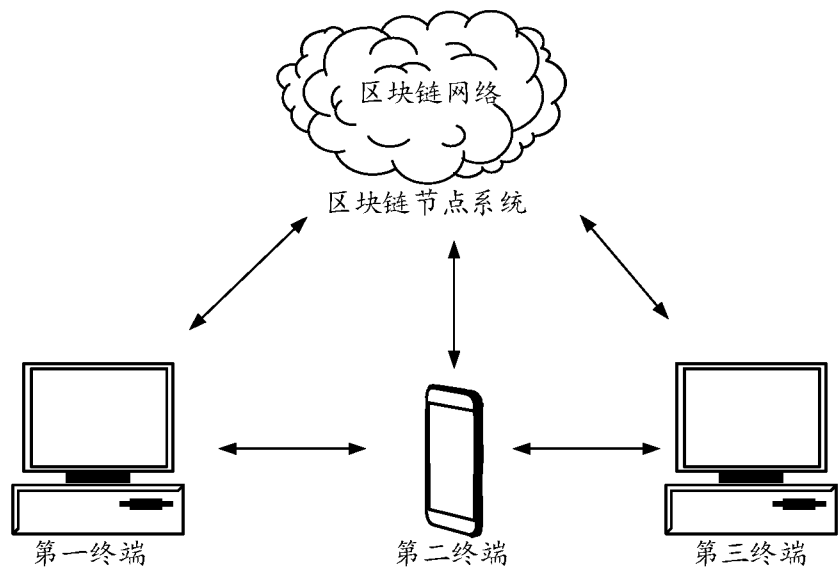


图 1a

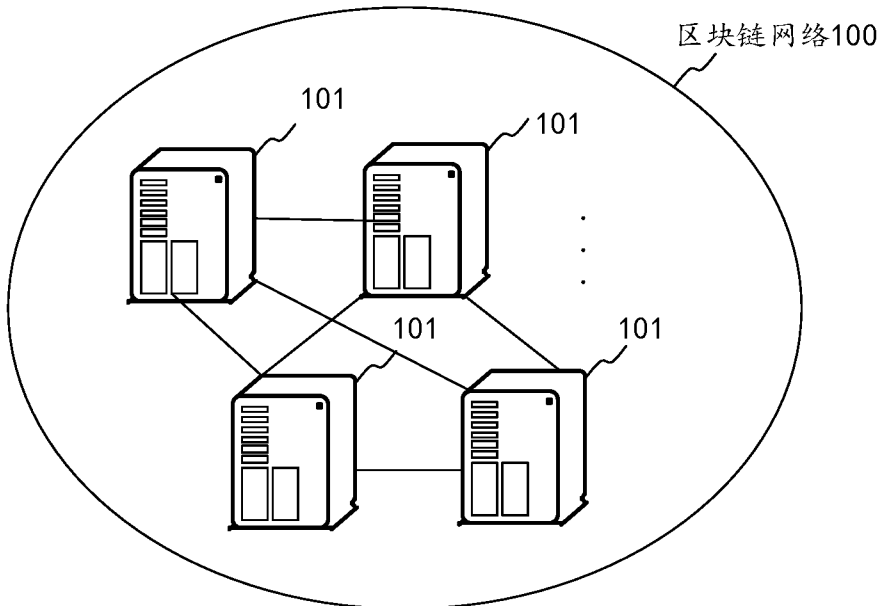


图 1b

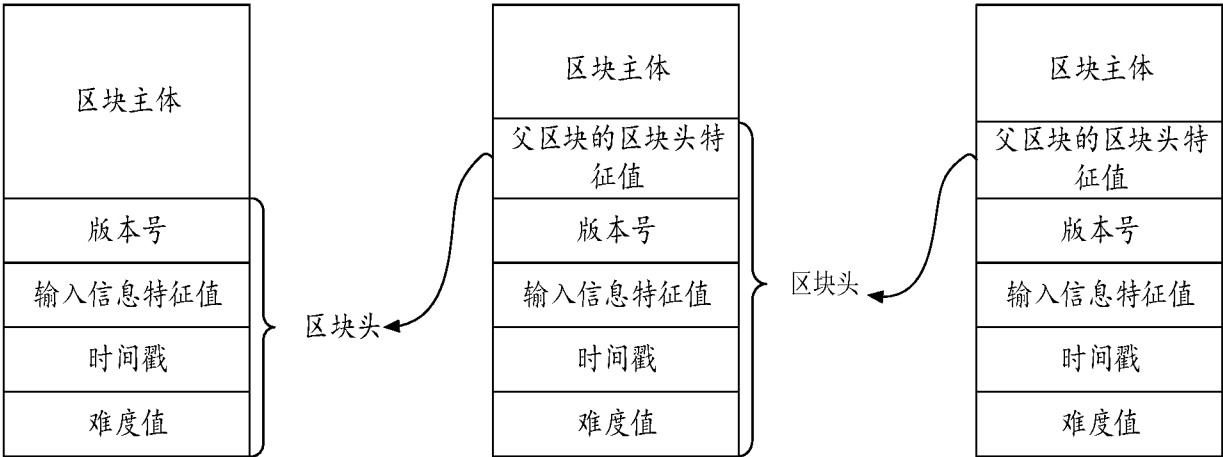


图 1c

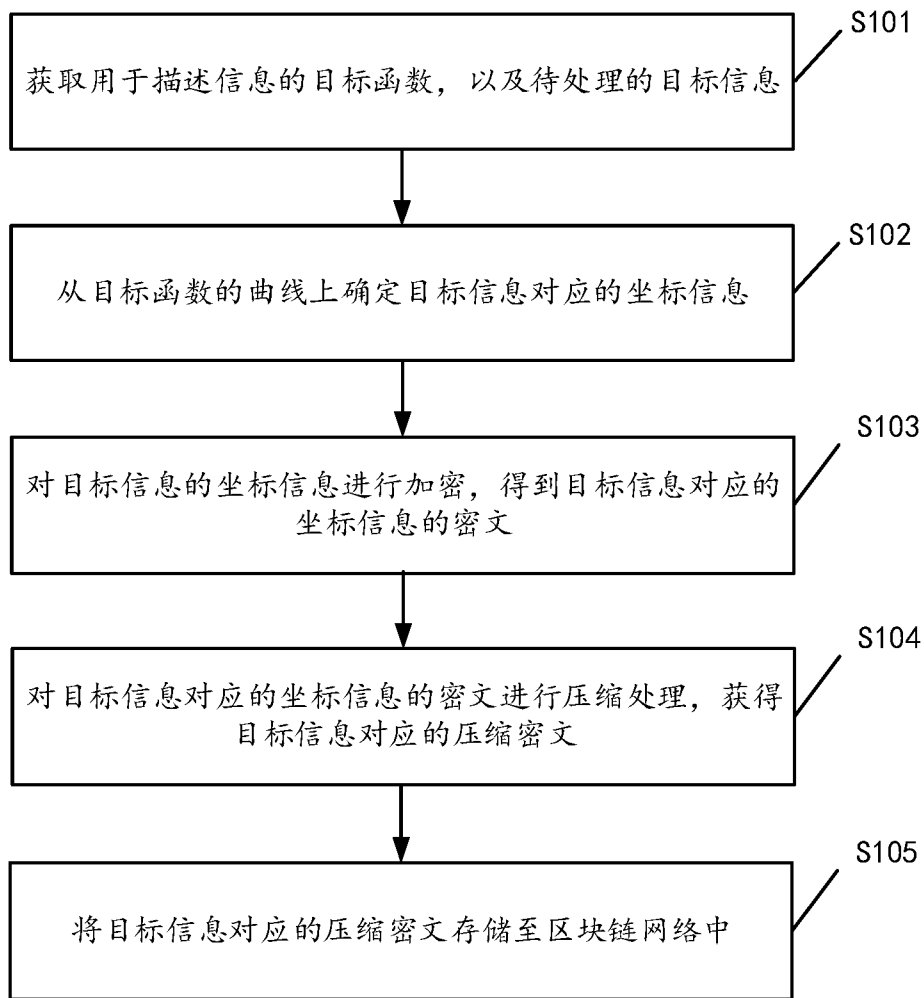


图 2

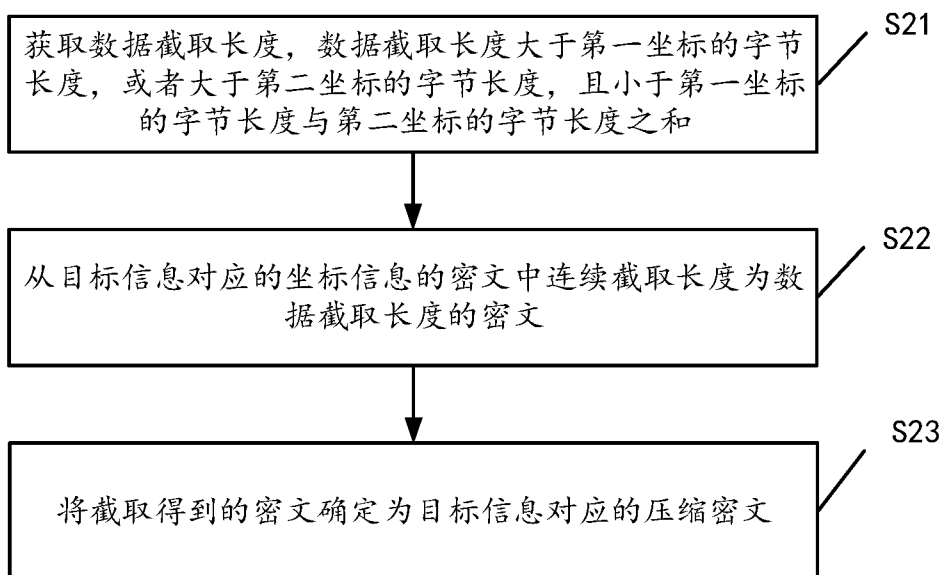


图 3

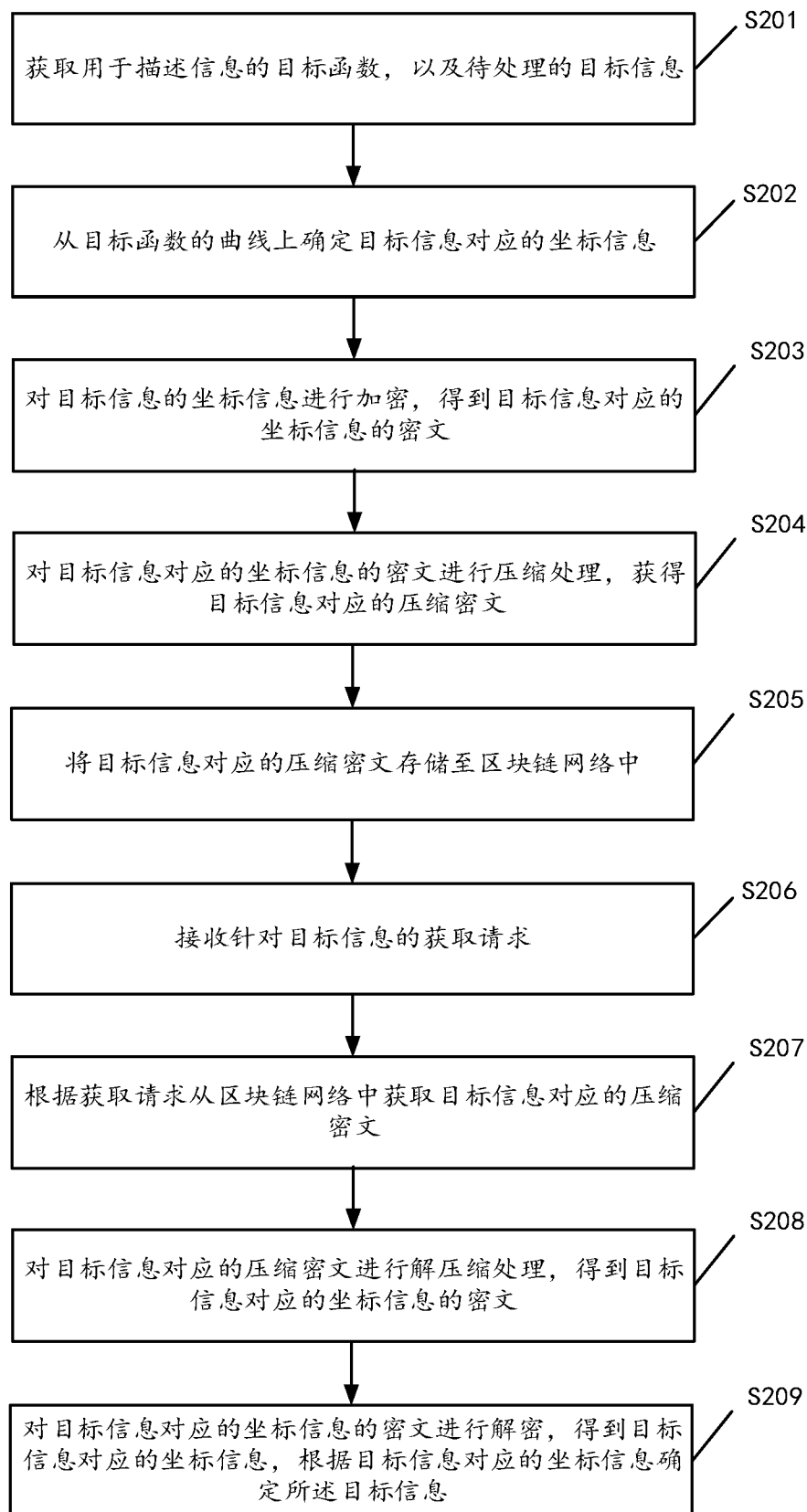


图 4

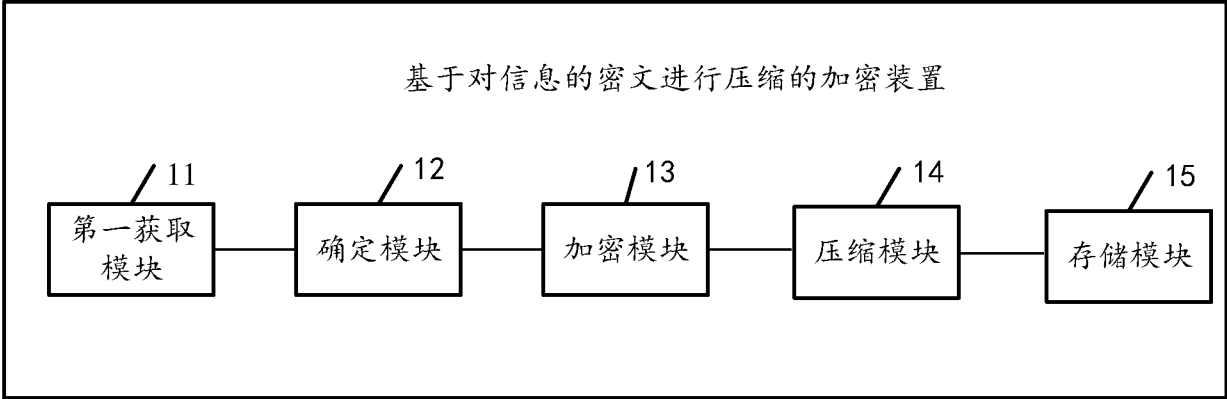


图 5

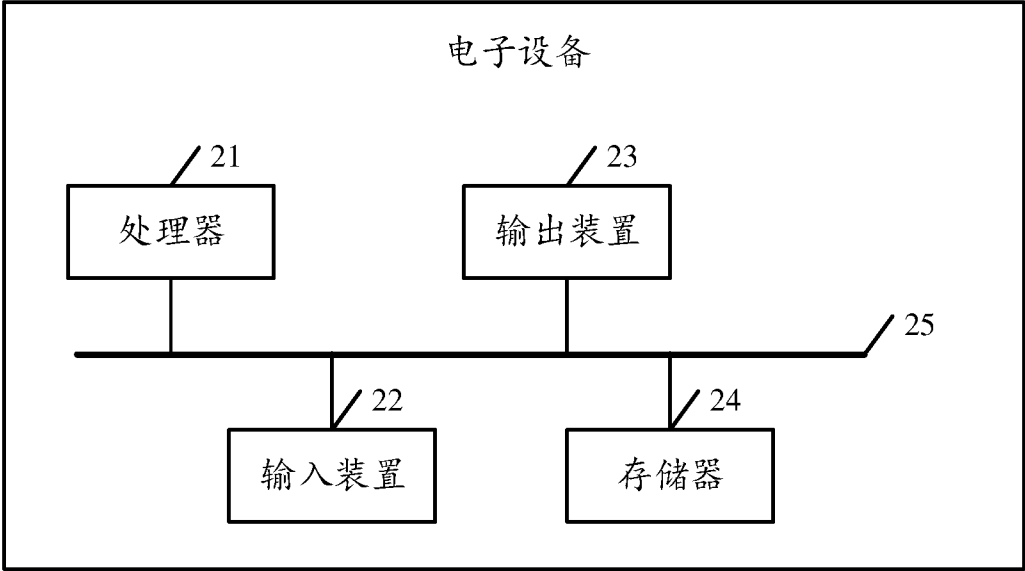


图 6

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2021/109259

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/60(2013.01)i; G06F 21/64(2013.01)i; G06F 16/174(2019.01)i; G06F 16/27(2019.01)i; G06Q 40/04(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)

G06F21/-; G06F16/-; G06Q40/-

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)

CNABS, CNTXT, CNKI: 壹账通, 区块链, 坐标, 曲线, 目标函数, 加密, 密文, 存储, 网络, 长度, 截取, 拼接, 用户信息, 标识, 对应, 小于, 密钥, 压缩, 解密; VEN, USTXT; IEEE: chain block, curve, targe, function, store, encryption, compress, coordinate, label, network, user information, decode, encode, length, corresponding;

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 112131591 A (SHENZHEN ONECONNECT TECHNOLOGY CO., LTD.) 25 December 2020 (2020-12-25) claims 1-10	claims 1-20
Y	CN 110839026 A (SHENZHEN WANGXIN TECHNOLOGY CO., LTD.) 25 February 2020 (2020-02-25) description, paragraphs 70-98	claims 1-20
Y	CN 111079162 A (SHANDONG ZHONGYANG HEALTH SCIENCE AND TECH GROUP CO LTD.) 28 April 2020 (2020-04-28) description, paragraphs 26-47	claims 1-20
Y	CN 103023892 A (JIANGSU LEMDAO NETWORK SCIENCE AND TECHNOLOGY CO., LTD.) 03 April 2013 (2013-04-03) description, paragraphs 15-18	claims 2-6, 10-14, 16-20
A	CN 111079171 A (CHONGQING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS) 28 April 2020 (2020-04-28) entire document	claims 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

10 September 2021

Date of mailing of the international search report

30 September 2021

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/CN2021/109259**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 108964916 A (YUANYI TECHNOLOGY HOLDINGS CO., LTD.) 07 December 2018 (2018-12-07) entire document	claims 1-20
A	CN 109948357 A (SHAANXI MEDICINE CHAIN BLOCK CHAIN GROUP CO., LTD.) 28 June 2019 (2019-06-28) entire document	claims 1-20
A	CN 110602083 A (SHANGHAI QIANYI DATA TECHNOLOGY CO., LTD.) 20 December 2019 (2019-12-20) entire document	claims 1-20
A	CN 108830600 A (FORESEE TECHNOLOGY CO., LTD.) 16 November 2018 (2018-11-16) entire document	claims 1-20
A	CN 110830235 A (HUAQIAO UNIVERSITY; XIAMEN CHUANYOU INTELLIGENT TECHNOLOGY CO., LTD.) 21 February 2020 (2020-02-21) entire document	claims 1-20
A	CN 109347878 A (XIDIAN UNIVERSITY) 15 February 2019 (2019-02-15) entire document	claims 1-20
A	WO 2020034151 A1 (BCM SOCIAL CORP.) 20 February 2020 (2020-02-20) entire document	claims 1-20

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2021/109259

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	112131591	A	25 December 2020	None	
CN	110839026	A	25 February 2020	None	
CN	111079162	A	28 April 2020	None	
CN	103023892	A	03 April 2013	None	
CN	111079171	A	28 April 2020	None	
CN	108964916	A	07 December 2018	None	
CN	109948357	A	28 June 2019	None	
CN	110602083	A	20 December 2019	None	
CN	108830600	A	16 November 2018	None	
CN	110830235	A	21 February 2020	None	
CN	109347878	A	15 February 2019	CN 109347878	B 05 June 2020
WO	2020034151	A1	20 February 2020	CN 109691013	A 26 April 2019

国际检索报告

国际申请号

PCT/CN2021/109259

A. 主题的分类 G06F 21/60(2013.01)i; G06F 21/64(2013.01)i; G06F 16/174(2019.01)i; G06F 16/27(2019.01)i; G06Q 40/04(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) G06F21/-; G06F16/-; G06Q40/- 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)) CNABS, CNTXT, CNKI:壹账通, 区块链, 坐标, 曲线, 目标函数, 加密, 密文, 存储, 网络, 长度, 截取, 拼接, 用户信息, 标识, 对应, 小于, 密钥, 压缩, 解密; VEN, USTXT; IEEE:chain block, curve, targe, function, store, encryption, compress, coordinate, label, network, user information, decode, encode, length, corresponding;		
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 112131591 A (深圳壹账通智能科技有限公司) 2020年 12月 25日 (2020 - 12 - 25) 权利要求1-10	权利要求1-20
Y	CN 110839026 A (深圳市网心科技有限公司) 2020年 2月 25日 (2020 - 02 - 25) 说明书70-98段	权利要求1-20
Y	CN 111079162 A (SHANDONG ZHONGYANG HEALTH SCIENCE AND TECH GROUP CO LTD.) 2020年 4月 28日 (2020 - 04 - 28) 说明书26-47段	权利要求1-20
Y	CN 103023892 A (江苏乐买到网络科技有限公司) 2013年 4月 3日 (2013 - 04 - 03) 说明书15-18段	权利要求2-6, 10-14, 16-20
A	CN 111079171 A (重庆邮电大学) 2020年 4月 28日 (2020 - 04 - 28) 全文	权利要求1-20
A	CN 108964916 A (元一科技控股有限公司) 2018年 12月 7日 (2018 - 12 - 07) 全文	权利要求1-20
A	CN 109948357 A (陕西医链区块链集团有限公司) 2019年 6月 28日 (2019 - 06 - 28) 全文	权利要求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 2021年 9月 10日		国际检索报告邮寄日期 2021年 9月 30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		授权官员 张雪锋 电话号码 (86-28)62967633

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	CN 110602083 A (上海黔易数据科技有限公司) 2019年 12月 20日 (2019 - 12 - 20) 全文	权利要求1-20
A	CN 108830600 A (方欣科技有限公司) 2018年 11月 16日 (2018 - 11 - 16) 全文	权利要求1-20
A	CN 110830235 A (华侨大学 厦门传邮智能科技有限公司) 2020年 2月 21日 (2020 - 02 - 21) 全文	权利要求1-20
A	CN 109347878 A (西安电子科技大学) 2019年 2月 15日 (2019 - 02 - 15) 全文	权利要求1-20
A	W0 2020034151 A1 (BCM SOCIAL CORP.) 2020年 2月 20日 (2020 - 02 - 20) 全文	权利要求1-20

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2021/109259

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	112131591	A	2020年 12月 25日	无	
CN	110839026	A	2020年 2月 25日	无	
CN	111079162	A	2020年 4月 28日	无	
CN	103023892	A	2013年 4月 3日	无	
CN	111079171	A	2020年 4月 28日	无	
CN	108964916	A	2018年 12月 7日	无	
CN	109948357	A	2019年 6月 28日	无	
CN	110602083	A	2019年 12月 20日	无	
CN	108830600	A	2018年 11月 16日	无	
CN	110830235	A	2020年 2月 21日	无	
CN	109347878	A	2019年 2月 15日	CN	109347878 B 2020年 6月 5日
WO	2020034151	A1	2020年 2月 20日	CN	109691013 A 2019年 4月 26日