

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2020 年 7 月 2 日 (02.07.2020)



(10) 国际公布号
WO 2020/134712 A1

(51) 国际专利分类号:
G06Q 20/38 (2012.01)

(21) 国际申请号: PCT/CN2019/119312

(22) 国际申请日: 2019 年 11 月 19 日 (19.11.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201811605307.9 2018 年 12 月 26 日 (26.12.2018) CN

(71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 开曼群岛
大开曼资本大厦一座四层 847 号邮箱,
Grand Cayman (KY)。

(72) 发明人: 栗志果 (LI, Zhiguo); 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,

(54) Title: BLOCKCHAIN DATA PROCESSING METHOD, DEVICE AND SYSTEM

(54) 发明名称: 区块链数据处理方法、装置及系统

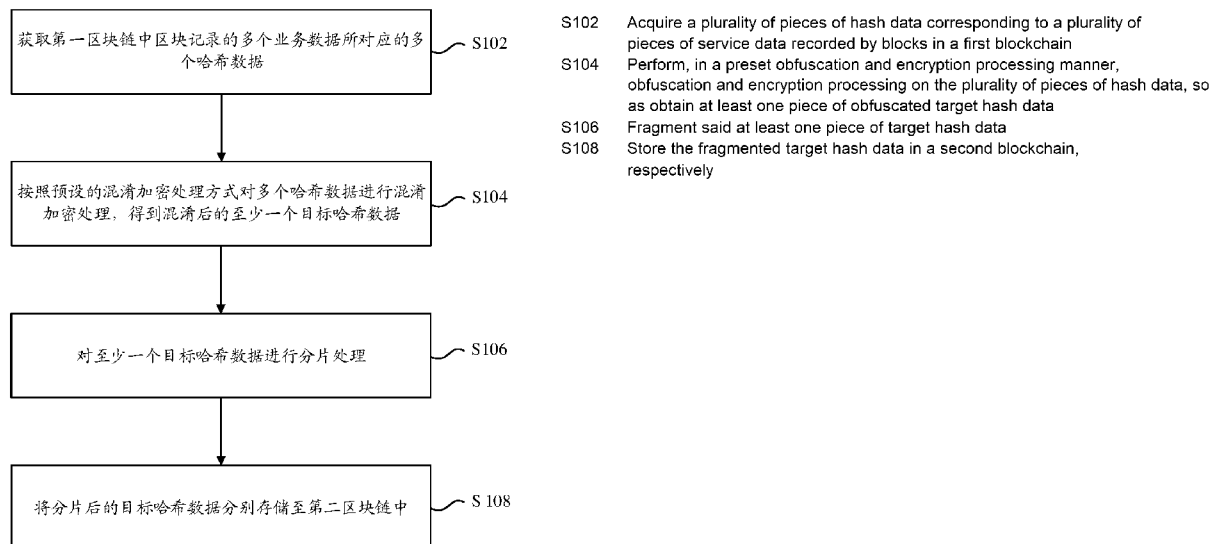


图 1

(57) Abstract: A blockchain data processing method, device and system, which are used to achieve the purpose of ensuring data security while using the blockchain technology. Said method comprises: acquiring a plurality of pieces of hash data corresponding to a plurality of pieces of service data recorded by blocks in a first blockchain (S102); performing, in a preset obfuscation and encryption processing manner, obfuscation and encryption processing on the plurality of pieces of hash data, so as to obtain at least one piece of obfuscated target hash data (S104); fragmenting said at least one piece of target hash data (S106); and storing the fragmented target hash data in a second blockchain, respectively (S108).

PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,
SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG,
US, UZ, VC, VN, ZA, ZM, ZW。

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

本国际公布:

- 包括国际检索报告(条约第21条(3))。

(57) 摘要: 一种区块链数据处理方法、装置及系统, 用以实现在使用区块链技术的同时确保数据的安全性的目的。所述方法包括: 获取第一区块链中区块记录的多个业务数据所对应的多个哈希数据(S102); 按照预设的混淆加密处理方式对所述多个哈希数据进行混淆加密处理, 得到混淆后的至少一个目标哈希数据(S104); 对所述至少一个目标哈希数据进行分片处理(S106); 将分片后的目标哈希数据分别存储至第二区块链中(S108)。

区块链数据处理方法、装置及系统

技术领域

[01] 本说明书涉及数据处理技术领域，尤其涉及一种区块链数据处理方法、装置及系统。

5 背景技术

[02] 采用区块链存储的数据具备真实透明、不可删除的特性，即使对明文进行加密、或使用哈希上链的方式，公众仍然可以通过解析区块链来获得区块链上的真实数据，如通过哈希的量级推测出区块链的真实调用量级，从而获得真实数据。可见，现有的区块链存储数据的方式对用户而言安全性不高，尤其是在利用区块链存储交易数据的场景中，
10 交易数据的透明化会给用户带来一定程度的风险。

发明内容

[03] 本说明书一个或多个实施例的目的是提供一种区块链数据处理方法、装置及系统，用以实现在使用区块链技术的同时确保数据的安全性的目的。

[04] 为解决上述技术问题，本说明书一个或多个实施例是这样实现的：

15 [05] 一方面，本说明书一个或多个实施例提供一种区块链数据处理方法，包括：

[06] 获取第一区块链中区块记录的多个业务数据所对应的多个哈希数据；

[07] 按照预设的混淆加密处理方式对所述多个哈希数据进行混淆加密处理，得到混淆后的至少一个目标哈希数据；

[08] 对所述至少一个目标哈希数据进行分片处理；

20 [09] 将分片后的目标哈希数据分别存储至第二区块链中。

[10] 在一个实施例中，所述按照预设的混淆加密处理方式对所述多个哈希数据进行混淆加密处理，得到混淆后的至少一个目标哈希数据，包括：

[11] 分别对各所述哈希数据进行至少一次的哈希计算，得到所述至少一个目标哈希数据。

25 [12] 在一个实施例中，所述分片处理对应的每个分片中所包含的目标哈希数据不多于

预定个数。

[13] 在一个实施例中，所述将分片后的目标哈希数据分别存储至第二区块链中，包括：

[14] 将各所述分片中所包含的目标哈希数据分别作为一条业务记录存储到所述第二区块链中。

5 [15] 在一个实施例中，在获取第一区块链中区块记录的多个业务数据所对应的多个哈希数据之前，还包括：

[16] 确定所述第一区块链的数据查看权限为仅对第一指定用户组可见；及，确定所述第二区块链的数据查看权限为对所有用户可见。

[17] 在一个实施例中，所述方法还包括：

10 [18] 将所述混淆加密处理方式存储至第三区块链中；及，确定所述第三区块链的数据查看权限为仅对第二指定用户组可见。

[19] 另一方面，本说明书一个或多个实施例提供一种区块链数据处理装置，包括：

[20] 获取模块，用于获取第一区块链中区块记录的多个业务数据所对应的多个哈希数据；

15 [21] 混淆模块，用于按照预设的混淆加密处理方式对所述多个哈希数据进行混淆加密处理，得到混淆后的至少一个目标哈希数据；

[22] 分片模块，用于对所述至少一个目标哈希数据进行分片处理；

[23] 第一存储模块，用于将分片后的目标哈希数据分别存储至第二区块链中。

20 [24] 再一方面，本说明书一个或多个实施例提供一种区块链数据处理系统，包括第一区块链、数据处理节点及第二区块链；其中：

[25] 所述第一区块链，用于记录多个业务数据所对应的多个哈希数据；

[26] 所述数据处理节点，用于获取所述第一区块链中区块记录的所述多个哈希数据；

25 [27] 所述数据处理节点，还用于按照预设的混淆加密处理方式对所述多个哈希数据进行混淆加密处理，得到混淆后的至少一个目标哈希数据；对所述至少一个目标哈希数据进行分片处理；将分片后的目标哈希数据分别存储至所述第二区块链中；

[28] 所述第二区块链，用于存储所述分片后的目标哈希数据。

[29] 再一方面，本说明书一个或多个实施例提供一种区块链数据处理设备，包括：

[30] 处理器；以及

[31] 被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器：

[32] 获取第一区块链中区块记录的多个业务数据所对应的多个哈希数据；

5 [33] 按照预设的混淆加密处理方式对所述多个哈希数据进行混淆加密处理，得到混淆后的至少一个目标哈希数据；

[34] 对所述至少一个目标哈希数据进行分片处理；

[35] 将分片后的目标哈希数据分别存储至第二区块链中。

10 [36] 再一方面，本申请实施例提供一种存储介质，用于存储计算机可执行指令，所述可执行指令在被执行时实现以下流程：

[37] 获取第一区块链中区块记录的多个业务数据所对应的多个哈希数据；

[38] 按照预设的混淆加密处理方式对所述多个哈希数据进行混淆加密处理，得到混淆后的至少一个目标哈希数据；

[39] 对所述至少一个目标哈希数据进行分片处理；

15 [40] 将分片后的目标哈希数据分别存储至第二区块链中。

[41] 采用本说明书一个或多个实施例的技术方案，通过获取第一区块链中区块记录的多个业务数据所对应的多个哈希数据，并按照预设的混淆加密处理方式对多个哈希数据进行混淆加密处理，得到混淆后的至少一个目标哈希数据，以及对该至少一个目标哈希数据进行分片处理，进而将分片后的目标哈希数据分别存储至第二区块链中。可见，该技术方案通过混淆多个业务数据所对应的多个哈希数据，使得最终存储的目标哈希数据能被外部用户访问，但外部用户很难对其进行分析以获知交易规模、交易量级等信息。因此在保障区块链中数据真实透明的同时，还能够保障数据的安全性，从而有利于用户在使用区块链时能够更好地保护自身业务。

附图说明

25 [42] 为了更清楚地说明本说明书一个或多个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单地介绍，显而易见地，下面描述中的附图仅仅是本说明书一个或多个实施例中记载的一些实施例，对于本领域普通技术人员来讲，在不付出创造

性劳动性的前提下，还可以根据这些附图获得其他的附图。

[43] 图 1 是根据本说明书一实施例的一种区块链数据处理方法的示意性流程图；

[44] 图 2 是根据本说明书一实施例的一种区块链数据处理装置的示意性框图；

[45] 图 3 是根据本说明书一实施例的一种区块链数据处理系统的示意性框图；

5 [46] 图 4 是根据本说明书一实施例的一种区块链数据处理设备的示意性框图。

具体实施方式

[47] 本说明书一个或多个实施例提供一种区块链数据处理方法、装置及系统，用以实现在使用区块链技术的同时确保数据的安全性的目的。

10 [48] 为了使本技术领域的人员更好地理解本说明书一个或多个实施例中的技术方案，下面将结合本说明书一个或多个实施例中的附图，对本说明书一个或多个实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本说明书一部分实施例，而不是全部的实施例。基于本说明书一个或多个实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都应当属于本说明书一个或多个实施例保护的范围。

15 [49] 图 1 是根据本说明书一实施例的一种区块链数据处理方法的示意性流程图，如图 1 所示，该方法包括：

[50] S102，获取第一区块链中区块记录的多个业务数据所对应的多个哈希数据。

[51] S104，按照预设的混淆加密处理方式对多个哈希数据进行混淆加密处理，得到混淆后的至少一个目标哈希数据。

20 [52] S106，对至少一个目标哈希数据进行分片处理。

[53] S108，将分片后的目标哈希数据分别存储至第二区块链中。

[54] 在一个实施例中，第一区块链中区块记录的多个业务数据所对应的多个哈希数据为该第一区块链中记录的交易的账本，该账本可以是仅对第一区块链中的节点可访问。该账本经过混淆加密处理后存储至第二区块链，第二区块链中存储的混淆加密后的账本
25 可以是对外部用户可访问。由此，一方面使得外部用户如公众可访问到该账本，以保障数据真实透明，另一方面，由于外部用户获取的是混淆加密处理后的账本，其难以对混淆加密后的账本进行解析以获得真实交易量的相关信息，也保障了交易信息的安全。

[55] 由此，上述技术方案通过混淆多个业务数据所对应的多个哈希数据，使得最终存储的目标哈希数据能被外部用户访问，但外部用户很难对其进行分析以获知交易规模、交易量级等信息。因此在保障区块链中数据真实透明的同时，还能够保障数据的安全性，从而有利于用户在使用区块链时能够更好地保护自身业务。

5 [56] 应理解，在本申请实施例中，对哈希数据的混淆加密处理可包括多种方式。

[57] 可选地，在一种实现方式中，可将多个哈希数据组成的内容进行哈希计算得到一个哈希数据。

[58] 例如，假设区块链的某个区块中的 4 个存储记录对应的哈希数据分别为 HashA、HashB、HashC 和 HashD，则混淆加密处理后的哈希数据 HashABCD=Hash
10 (HashA+HashB+HashC+HashD)，其中，函数 Hash() 表示哈希计算函数，例如 MD5、SHA-1、SHA-256、SHA-384 及 SHA-512，等等。在比特币系统中，采用的哈希算法为 SHA-256。

[59] 可选地，在另一种实现方式中，可将任一个哈希数据分成多个部分的内容再分别进行哈希计算，得到所述多个部分的内容对应的多个哈希数据。

15 [60] 例如，假设区块链的某个区块中的一个存储记录对应的哈希数据为 HashA，可将 HashA 拆分成 HashA1 和 HashA2，然后分别进行哈希处理，即得到 HashA1'=Hash(HashA1)，HashA2'=Hash(HashA2)，此时的 HashA1' 和 HashA2' 即对 HashA 进行混淆加密处理后得到的哈希数据。当然，还可将 HashA 拆分成 3 个部分、4 个部分乃至更多部分，具体拆分成多少个部分，怎么拆分，是可配置的。

20 [61] 可选地，在另一种实现方式中，可将多个哈希数据组成的内容再分成多个部分的内容，并对每个部分的内容分别进行哈希计算，得到所述多个部分的内容对应的多个哈希数据。

[62] 例如，假设区块链的某个区块中的 4 个存储记录对应的哈希数据分别为 HashA、HashB、HashC 和 HashD，其组成的内容 HashABCD=(HashA+HashB+HashC+HashD)；

25 可将 HashABCD 分成 HashABCD1 和 HashABCD2，再对 HashABCD1 和 HashABCD2 分别进行哈希计算得到 Hash(HashABCD1) 和 Hash(HashABCD2)，Hash(HashABCD1) 和 Hash(HashABCD2) 即为该多个部分的内容对应的多个哈希数据。

[63] 此外，应理解，本申请实施例的混淆方案，还可进行多层混淆加密处理，即将一层混淆加密处理之后的哈希数据，再进行一层或多层的混淆加密处理。不同层混淆加密

处理的算法，可以相同，也可以不同。

[64] 例如，假设区块链的某个区块中的 4 个存储记录对应的哈希数据分别为 HashA、HashB、HashC 和 HashD，则第一层混淆加密处理后的哈希信息 HashABCD=Hash(HashA+HashB+HashC+HashD)；第二层混淆加密处理后的哈希数据为 Hash(HashABCD1)和 Hash(HashABCD2)，其中 HashABCD= HashABCD1+HashABCD2。

[65] 可选的，在另一种实现方式中，可对哈希数据进行一次或多次的分片处理和/或哈希计算。具体的，可仅对哈希数据进行分片处理以得到目标哈希数据，也可将分片处理和哈希计算的方式结合起来对哈希数据进行混淆加密以得到目标哈希数据。

[66] 以下列举一种详细的混淆加密处理方式。

10 [67] 首先，按照指定分片规则对哈希数据进行分片处理，得到多个第一数据片段。

[68] 其中，指定分片规则包括：按照指定数据长度进行分片的规则；例如，指定数据长度为 64KB，则按照每个数据片段大小为 64KB 的规则对哈希数据进行分片；或者，按照指定时长进行分片的规则；例如，指定时长为 1 秒，则按照每秒内存储的哈希数据进行分片，如当前 1 秒内存储的哈希数据为一个数据片段，下 1 秒内存储的哈希数据则为下一个数据片段。

[69] 其次，分别对各第一数据片段进行哈希计算，得到多个第二数据片段。

[70] 最后，根据多个第二数据片段确定混淆加密后的目标哈希数据。具体的，可直接确定第二数据片段为目标哈希数据，还可再次对第二数据片段进行一次或多次的分片处理和/或哈希计算，最终得到目标哈希数据。

20 [71] 本实施例中，列举了首先对哈希数据进行分片处理、然后对分片后得到的数据片段进行哈希计算的混淆加密处理方式。显然，由于混淆加密处理方式的多样性，经过混淆加密处理后的目标哈希数据很难被外部用户获知，因此可确保目标哈希数据的安全性。

[72] 当然，除上述列举的混淆加密处理方式之外，还可采用其他多种混淆加密处理方式对哈希数据进行混淆加密处理，包括多次分片处理和多次哈希计算相结合的方式，且多次分片处理和多次哈希计算的顺序不受限定。分片处理和/或哈希计算的次数越多，即混淆加密处理方式越复杂，得到的目标哈希数据的安全性也就越高。

[73] 在一个实施例中，在获取第一区块链中记录的业务数据所对应的哈希数据之前，可先确定第一区块链的数据查看权限为仅对第一指定用户组可见，如仅对第一区块链中

的各节点可见；及，确定第二区块链的数据查看权限为对所有用户可见，如外部用户如公众均可访问该数据。

[74] 其中，第一指定用户组可以是一个用户或多个用户。

5 [75] 本实施例中，由于第一区块链仅对第一指定用户组可见，其他外部用户不可见，因此第一区块链中区块存储的多个业务数据所对应的多个哈希数据很难被外部用户获知，从而确保多个业务数据所对应的多个哈希数据的安全性；此外，由于第二区块链对所有用户可见，即所有用户都能够获知第二区块链中存储的混淆加密后的目标哈希数据，因此保障了区块链中数据的透明真实性，且即使外部用户获知了第二区块链中存储的混淆加密后的目标哈希数据，由于不知道目标哈希数据对应的混淆加密处理方式，因此也
10 无法获知业务数据的真实数据，从而确保业务数据的安全性，有利于用户在使用区块链时能够更好地保护自身业务。

[76] 在一个实施例中，将混淆加密后的至少一个目标哈希数据存储至第二区块链中时，可先对混淆加密后的至少一个目标哈希数据进行分片处理，进而将分片后的目标哈希数据分别存储至第二区块链中。

15 [77] 本实施例中，分片处理对应的每个分片中所包含的目标哈希数据不多于预定个数，其中，预定个数个目标哈希数据的总长度应不大于第二区块链中区块记录数据的最大长度。因此，在对混淆加密后的至少一个目标哈希数据进行分片处理时，可按照每个分片中包含固定数量个目标哈希数据的方式进行分片，其中，固定数量应不大于预定个数。

20 [78] 本实施例中，对混淆加密后的至少一个目标哈希数据进行分片处理后，得到多个分片。因此，将分片后的目标哈希数据分别存储至第二区块链中时，可将各分片中所包含的目标哈希数据分别作为一条业务记录存储到第二区块链中。

[79] 在一个实施例中，可将混淆加密处理方式存储至第三区块链中，并确定第三区块链的数据查看权限为仅对第二指定用户组可见。

25 [80] 其中，第二指定用户组可以是一个用户或多个用户。第二指定用户组可与第一指定用户组（即针对第一区块链可见的用户组）相同或不同。第二指定用户组可以是与第一区块链/第二区块链中所存储的数据相关的工作人员，如区块链的维护人员，该（些）用户可对第一区块链/第二区块链中所存储的哈希数据进行管理，如存储、更新等操作；或者，该（些）用户还可对第三区块链中存储的混淆加密处理方式进行管理，如存储、修改等操作。

[81] 本实施例中，通过将混淆加密处理方式单独存储至第三区块链中，使得第二指定用户组方便获知混淆加密处理方式，从而通过获取混淆加密处理方式来获取业务数据的真实数据。并且，由于第三区块链仅对第二指定用户组可见，其他外部用户不可见，因此外部用户很难获知第三区块链中存储的混淆加密处理方式，从而很难获知业务数据的真实数据，确保了业务数据的安全性。

[82] 在一个实施例中，也可将混淆加密处理方式存储至第一区块链中，由于第一区块链仅对第一指定用户组可见，其他外部用户不可见，因此第一区块链中存储的混淆加密处理方式很难被外部用户获知，从而使外部用户很难获知业务数据的真实数据，确保了业务数据的安全性。

[83] 本实施例中，将混淆加密处理方式与业务数据对应的哈希数据一起存储在第一区域链中，不仅能确保业务数据的安全性，还能节省混淆加密处理方式对区块链的占用。

[84] 综上，已经对本主题的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可以按照不同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，以实现期望的结果。在某些实施方式中，多任务处理和并行处理可以是有利的。

[85] 以上为本说明书一个或多个实施例提供的区块链数据处理方法，基于同样的思路，本说明书一个或多个实施例还提供一种区块链数据处理装置。

[86] 图 2 是根据本说明书一实施例的一种区块链数据处理装置的示意性框图，如图 2 所示，区块链数据处理装置 200 包括：

[87] 获取模块 210，用于获取第一区块链中区块记录的多个业务数据所对应的多个哈希数据；

[88] 混淆模块 220，用于按照预设的混淆加密处理方式对多个哈希数据进行混淆加密处理，得到混淆后的至少一个目标哈希数据；

[89] 分片模块 230，用于对所述至少一个目标哈希数据进行分片处理；

[90] 第一存储模块 240，用于将分片后的目标哈希数据分别存储至第二区块链中。

[91] 在一个实施例中，混淆模块 220 包括：

[92] 计算单元，用于分别对各哈希数据进行至少一次的哈希计算，得到至少一个目标哈希数据。

[93] 在一个实施例中，分片处理对应的每个分片中所包含的目标哈希数据不多于预定个数。

[94] 在一个实施例中，第一存储模块 240 包括：

[95] 存储单元，用于将各分片中所包含的目标哈希数据分别作为一条业务记录存储到第二区块链中。

[96] 在一个实施例中，装置 200 还包括：

[97] 第一确定模块，用于在获取第一区块链中区块记录的多个业务数据所对应的多个哈希数据之前，确定第一区块链的数据查看权限为仅对第一指定用户组可见；及，确定第二区块链的数据查看权限为对所有用户可见。

[98] 在一个实施例中，装置 200 还包括：

[99] 存储及确定模块，用于将混淆加密处理方式存储至第三区块链中；及，确定第三区块链的数据查看权限为仅对第二指定用户组可见。

[100] 采用本说明书一个或多个实施例的装置，通过获取第一区块链中区块记录的多个业务数据所对应的多个哈希数据，并按照预设的混淆加密处理方式对多个哈希数据进行混淆加密处理，得到混淆后的至少一个目标哈希数据，以及对该至少一个目标哈希数据进行分片处理，进而将分片后的目标哈希数据分别存储至第二区块链中。可见，该技术方案通过混淆多个业务数据所对应的多个哈希数据，使得最终存储的目标哈希数据能被外部用户访问，但外部用户很难对其进行分析以获知交易规模、交易量级等信息。因此在保障区块链中数据真实透明的同时，还能够保障数据的安全性，从而有利于用户在使用区块链时能够更好地保护自身业务。

[101] 本领域的技术人员应可理解，上述区块链数据处理装置能够用来实现前文所述的区块链数据处理方法，其中的细节描述应与前文方法部分描述类似，为避免繁琐，此处不另赘述。

[102] 基于同样的思路，本说明书一个或多个实施例还提供一种区块链数据处理系统。

[103] 图 3 是根据本说明书一实施例的一种区块链数据处理系统的示意性框图，如图 3 所示，区块链数据处理系统 300 包括第一区块链 310、数据处理节点 320 及第二区块链 330；其中：

[104] 第一区块链 310，用于记录多个业务数据所对应的多个哈希数据；

[105] 数据处理节点 320, 用于获取第一区块链 310 中区块记录的多个哈希数据;

[106] 数据处理节点 320, 还用于按照预设的混淆加密处理方式对多个哈希数据进行混淆加密处理, 得到混淆后的至少一个目标哈希数据; 对至少一个目标哈希数据进行分片处理; 将分片后的目标哈希数据分别存储至第二区块链 330 中;

5 [107] 第二区块链 330, 用于存储分片后的目标哈希数据。

[108] 在一个实施例中, 数据处理节点 320 还用于:

[109] 分别对各哈希数据进行至少一次的哈希计算, 得到至少一个目标哈希数据。

[110] 在一个实施例中, 分片处理对应的每个分片中所包含的目标哈希数据不多于预定个数。

10 [111] 在一个实施例中, 数据处理节点 320 还用于:

[112] 将各所述分片中所包含的目标哈希数据分别作为一条业务记录存储到所述第二区块链中。

[113] 在一个实施例中, 数据处理节点 320 还用于:

[114] 确定第一区块链的数据查看权限为仅对第一指定用户组可见; 及, 确定第二区块

15 链的数据查看权限为对所有用户可见。

[115] 在一个实施例中, 系统 300 还包括:

[116] 第三区块链, 用于存储混淆加密处理方式;

[117] 相应的, 数据处理节点 320, 还用于确定第三区块链数据查看权限为仅对第二指定用户组可见。

20 [118] 采用本说明书一个或多个实施例的系统, 通过获取第一区块链中区块记录的多个业务数据所对应的多个哈希数据, 并按照预设的混淆加密处理方式对多个哈希数据进行混淆加密处理, 得到混淆后的至少一个目标哈希数据, 以及对该至少一个目标哈希数据进行分片处理, 进而将分片后的目标哈希数据分别存储至第二区块链中。可见, 该技术方案通过混淆多个业务数据所对应的多个哈希数据, 使得最终存储的目标哈希数据能被
25 外部用户访问, 但外部用户很难对其进行分析以获知交易规模、交易量级等信息。因此在保障区块链中数据真实透明的同时, 还能够保障数据的安全性, 从而有利于用户在使用区块链时能够更好地保护自身业务。

[119] 本领域的技术人员应可理解，上述区块链数据处理系统能够用来实现前文所述的区块链数据处理方法，其中的细节描述应与前文方法部分描述类似，为避免繁琐，此处不另赘述。

[120] 基于同样的思路，本说明书一个或多个实施例还提供一种区块链数据处理设备，
5 如图 4 所示。区块链数据处理设备可因配置或性能不同而产生比较大的差异，可以包括一个或一个以上的处理器 401 和存储器 402，存储器 402 中可以存储有一个或一个以上存储应用程序或数据。其中，存储器 402 可以是短暂存储或持久存储。存储在存储器 402 的应用程序可以包括一个或一个以上模块（图示未示出），每个模块可以包括对区块链数据处理设备中的一系列计算机可执行指令。更进一步地，处理器 401 可以设置为与存
10 储器 402 通信，在区块链数据处理设备上执行存储器 402 中的一系列计算机可执行指令。区块链数据处理设备还可以包括一个或一个以上电源 403，一个或一个以上有线或无线网络接口 404，一个或一个以上输入输出接口 405，一个或一个以上键盘 406。

[121] 具体在本实施例中，区块链数据处理设备包括有存储器，以及一个或一个以上的程序，其中一个或者一个以上程序存储于存储器中，且一个或者一个以上程序可以包括
15 一个或一个以上模块，且每个模块可以包括对区块链数据处理设备中的一系列计算机可执行指令，且经配置以由一个或者一个以上处理器执行该一个或者一个以上程序包含用于进行以下计算机可执行指令：

[122] 获取第一区块链中区块记录的多个业务数据所对应的多个哈希数据；

[123] 按照预设的混淆加密处理方式对所述多个哈希数据进行混淆加密处理，得到混淆
20 后的至少一个目标哈希数据；

[124] 对所述至少一个目标哈希数据进行分片处理；

[125] 将所述分片后的目标哈希数据分别存储至第二区块链中。

[126] 可选地，计算机可执行指令在被执行时，还可以使所述处理器：

[127] 分别对各所述哈希数据进行至少一次的哈希计算，得到所述至少一个目标哈希数
25 据。

[128] 可选地，所述分片处理对应的每个分片中所包含的目标哈希数据不多于预定个数。
可选地，计算机可执行指令在被执行时，还可以使所述处理器：

[129] 将各所述分片中所包含的目标哈希数据分别作为一条业务记录存储到所述第二区

块链中。

[130] 可选地，计算机可执行指令在被执行时，还可以使所述处理器：

[131] 在获取第一区块链中区块记录的多个业务数据所对应的多个哈希数据之前，确定所述第一区块链的数据查看权限为仅对第一指定用户组可见；及，确定所述第二区块链的数据查看权限为对所有用户可见。

[132] 可选地，计算机可执行指令在被执行时，还可以使所述处理器：

[133] 将所述混淆加密处理方式存储至第三区块链中；及，确定所述第三区块链的数据查看权限为仅对第二指定用户组可见。

[134] 本说明书一个或多个实施例还提出了一种计算机可读存储介质，该计算机可读存储介质存储一个或多个程序，该一个或多个程序包括指令，该指令当被包括多个应用程序的电子设备执行时，能够使该电子设备执行上述区块链数据处理方法，并具体用于执行：

[135] 获取第一区块链中区块记录的多个业务数据所对应的多个哈希数据；

[136] 按照预设的混淆加密处理方式对所述多个哈希数据进行混淆加密处理，得到混淆后的至少一个目标哈希数据；

[137] 分片模块，用于对所述至少一个目标哈希数据进行分片处理；

[138] 将所述分片后的目标哈希数据分别存储至第二区块链中。

[139] 上述实施例阐明的系统、装置、模块或单元，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。一种典型的实现设备为计算机。具体的，计算机例如可以为个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任何设备的组合。

[140] 为了描述的方便，描述以上装置时以功能分为各种单元分别描述。当然，在实施本说明书一个或多个实施例时可以把各单元的功能在同一个或多个软件和/或硬件中实现。

[141] 本领域内的技术人员应明白，本说明书一个或多个实施例可提供为方法、系统、或计算机程序产品。因此，本说明书一个或多个实施例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，本说明书一个或多个实施例

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。

[142] 本说明书一个或多个实施例是参照根据本申请实施例的方法、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。

10 [143] 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。

15 [144] 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。

[145] 在一个典型的配置中，计算设备包括一个或多个处理器（CPU）、输入/输出接口、网络接口和内存。

20 [146] 内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器（RAM）和/或非易失性内存等形式，如只读存储器（ROM）或闪存（flash RAM）。内存是计算机可读介质的示例。

25 [147] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存（PRAM）、静态随机存取存储器（SRAM）、动态随机存取存储器（DRAM）、其他类型的随机存取存储器（RAM）、只读存储器（ROM）、电可擦除可编程只读存储器（EEPROM）、快闪记忆体或其他内存技术、只读光盘只读存储器（CD-ROM）、数字多功能光盘（DVD）或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于

存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体（transitory media），如调制的数据信号和载波。

[148] 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[149] 本说明书一个或多个实施例可以在由计算机执行的计算机可执行指令的一般上下文中描述，例如程序模块。一般地，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。也可以在分布式计算环境中实践本申请，在这些分布式计算环境中，由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中，程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

[150] 本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于系统实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[151] 以上所述仅为本说明书一个或多个实施例而已，并不用于限制本说明书。对于本领域技术人员来说，本说明书一个或多个实施例可以有各种更改和变化。凡在本说明书一个或多个实施例的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本说明书一个或多个实施例的权利要求范围之内。

权利要求书

1、一种区块链数据处理方法，包括：

获取第一区块链中区块记录的多个业务数据所对应的多个哈希数据；

按照预设的混淆加密处理方式对所述多个哈希数据进行混淆加密处理，得到混淆后

5 的至少一个目标哈希数据；

对所述至少一个目标哈希数据进行分片处理；

将分片后的目标哈希数据分别存储至第二区块链中。

2、根据权利要求 1 所述的方法，按照预设的混淆加密处理方式对所述多个哈希数据进行混淆加密处理，得到混淆后的至少一个目标哈希数据，包括：

10 分别对各所述哈希数据进行至少一次的哈希计算，得到所述至少一个目标哈希数据。

3、根据权利要求 2 所述的方法，所述分片处理对应的每个分片中所包含的目标哈希数据不多于预定个数。

4、根据权利要求 3 所述的方法，将分片后的目标哈希数据分别存储至第二区块链中，包括：

15 将各所述分片中所包含的目标哈希数据分别作为一条业务记录存储到所述第二区块链中。

5、根据权利要求 1 所述的方法，在获取第一区块链中区块记录的多个业务数据所对应的多个哈希数据之前，还包括：

20 确定所述第一区块链的数据查看权限为仅对第一指定用户组可见；及，确定所述第二区块链的数据查看权限为对所有用户可见。

6、根据权利要求 1 所述的方法，还包括：

将所述混淆加密处理方式存储至第三区块链中；及，确定所述第三区块链的数据查看权限为仅对第二指定用户组可见。

7、一种区块链数据处理装置，包括：

25 获取模块，用于获取第一区块链中区块记录的多个业务数据所对应的多个哈希数据；

混淆模块，用于按照预设的混淆加密处理方式对所述多个哈希数据进行混淆加密处理，得到混淆后的至少一个目标哈希数据；

分片模块，用于对所述至少一个目标哈希数据进行分片处理；

第一存储模块，用于将分片后的目标哈希数据分别存储至第二区块链中。

30 8、一种区块链数据处理系统，包括第一区块链、数据处理节点及第二区块链；其中：

所述第一区块链，用于记录多个业务数据所对应的多个哈希数据；

所述数据处理节点，用于获取所述第一区块链中区块记录的所述多个哈希数据；

所述数据处理节点，还用于按照预设的混淆加密处理方式对所述多个哈希数据进行混淆加密处理，得到混淆后的至少一个目标哈希数据；对所述至少一个目标哈希数据进行

5 行分片处理；将分片后的目标哈希数据分别存储至所述第二区块链中；

所述第二区块链，用于存储所述分片后的目标哈希数据。

9、一种区块链数据处理设备，包括：

处理器；以及

被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理

10 器：

获取第一区块链中区块记录的多个业务数据所对应的多个哈希数据；

按照预设的混淆加密处理方式对所述多个哈希数据进行混淆加密处理，得到混淆后的至少一个目标哈希数据；

对所述至少一个目标哈希数据进行分片处理；

15 将分片后的目标哈希数据分别存储至第二区块链中。

10、一种存储介质，用于存储计算机可执行指令，所述可执行指令在被执行时实现以下流程：

获取第一区块链中区块记录的多个业务数据所对应的多个哈希数据；

按照预设的混淆加密处理方式对所述多个哈希数据进行混淆加密处理，得到混淆后

20 的至少一个目标哈希数据；

对所述至少一个目标哈希数据进行分片处理；

将分片后的目标哈希数据分别存储至第二区块链中。

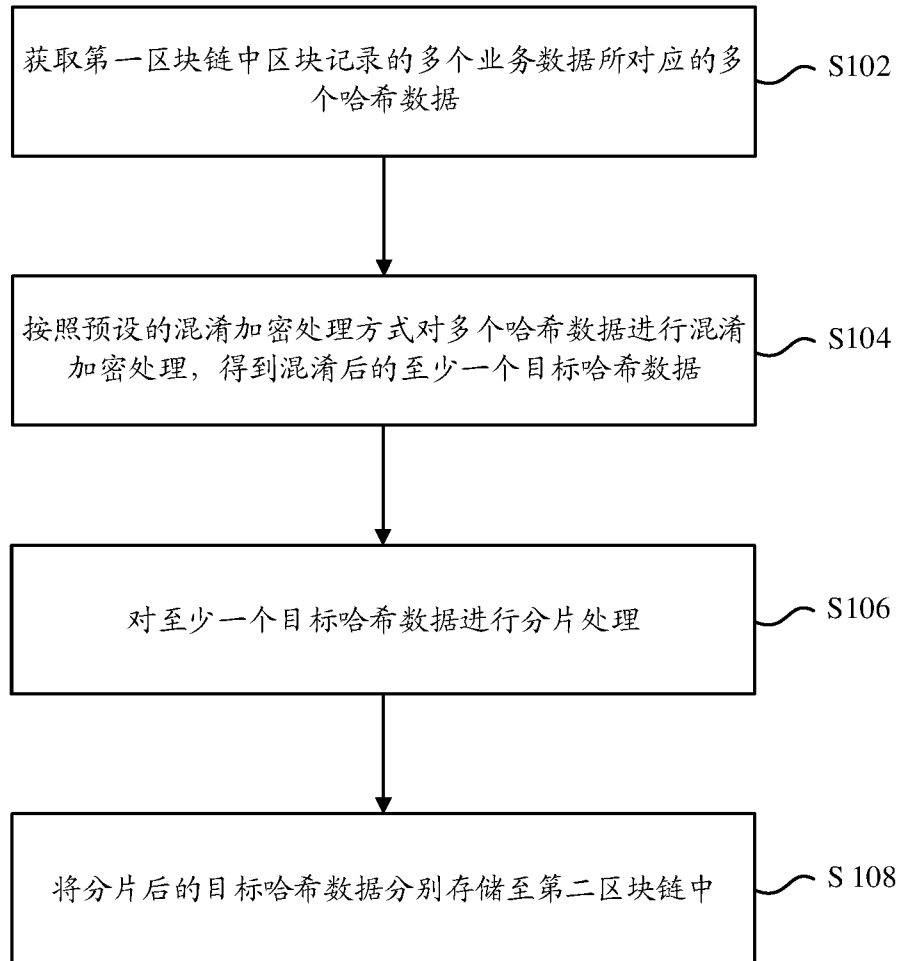


图 1

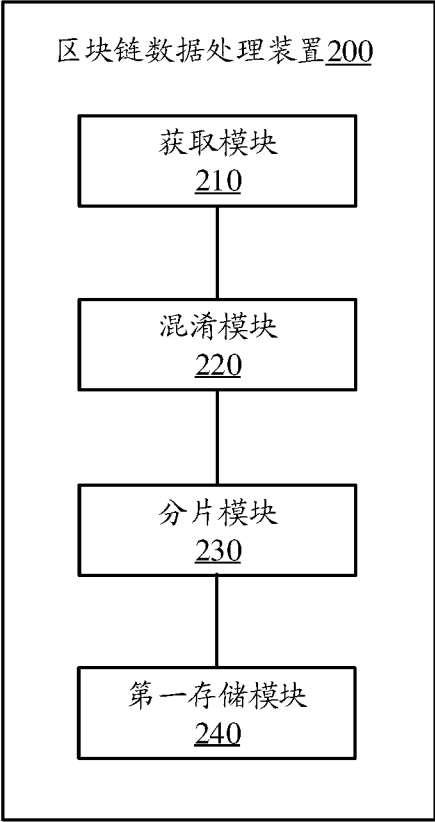


图 2

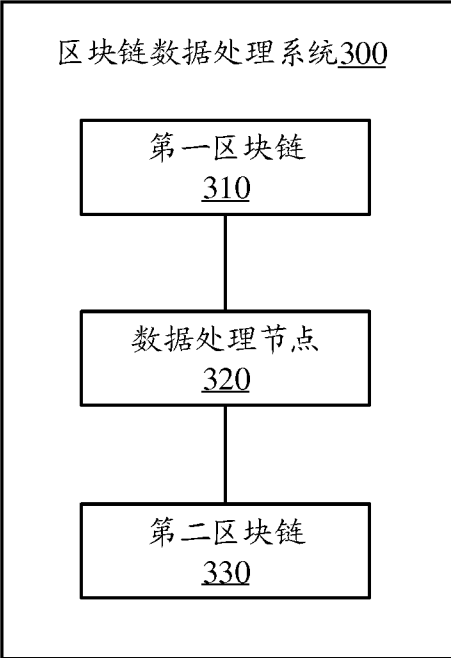


图 3

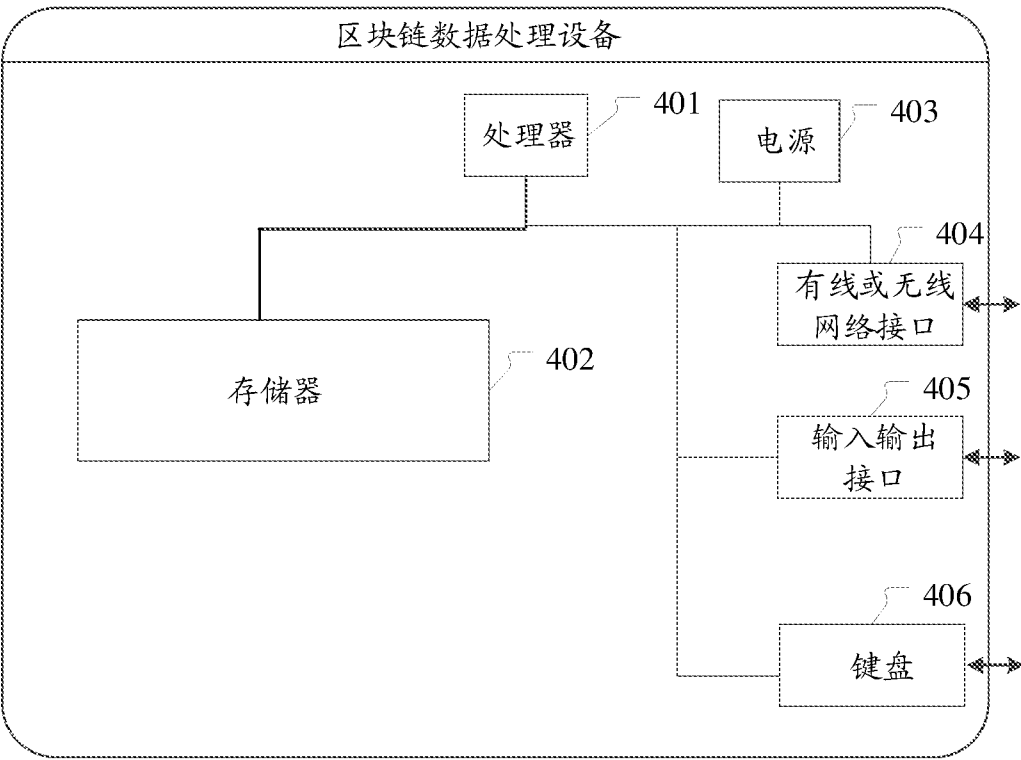


图 4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/119312

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/38(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: 区块链, 混淆, 哈希, 散列, 加密, 分片, 隐私, 私密, block chain, hash, confus+, encrypt, privacy

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110033261 A (ALIBABA GROUP HOLDING LIMITED) 19 July 2019 (2019-07-19) claims 1-10 and description, paragraphs [0005]-[0040]	1-10
A	CN 108664223 A (BAIDU ONLINE NETWORK TECHNOLOGY (BEIJING) CO., LTD.) 16 October 2018 (2018-10-16) description, paragraphs [0106]-[0120]	1-10
A	US 2018101701 A1 (ACRONIS INTERNATIONAL GMBH) 12 April 2018 (2018-04-12) entire document	1-10
A	CN 109034800 A (HANGZHOU FUZAMEI TECHNOLOGY CO., LTD.) 18 December 2018 (2018-12-18) entire document	1-10
A	CN 108737068 A (CHINA UNIVERSITY OF GEOSCIENCES WUHAN) 02 November 2018 (2018-11-02) entire document	1-10



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

13 February 2020

Date of mailing of the international search report

21 February 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

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2019/119312

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)		Publication date (day/month/year)
CN	110033261	A	19 July 2019	None		
CN	108664223	A	16 October 2018	WO	2019218717	A1 21 November 2019
US	2018101701	A1	12 April 2018	None		
CN	109034800	A	18 December 2018	None		
CN	108737068	A	02 November 2018	None		

国际检索报告

国际申请号

PCT/CN2019/119312

A. 主题的分类

G06Q 20/38 (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, EPDOC, CNPAT, CNKI: 区块链, 混淆, 哈希, 散列, 加密, 分片, 隐私, 私密, block chain, hash, confus+, encrypt, privacy

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 110033261 A (阿里巴巴集团控股有限公司) 2019年 7月 19日 (2019 - 07 - 19) 权利要求1-10, 说明书第[0005]-[0040]段	1-10
A	CN 108664223 A (百度在线网络技术北京有限公司) 2018年 10月 16日 (2018 - 10 - 16) 说明书第[0106]-[0120]段	1-10
A	US 2018101701 A1 (ACRONIS INTERNATIONAL GMBH) 2018年 4月 12日 (2018 - 04 - 12) 全文	1-10
A	CN 109034800 A (杭州复杂美科技有限公司) 2018年 12月 18日 (2018 - 12 - 18) 全文	1-10
A	CN 108737068 A (中国地质大学武汉) 2018年 11月 2日 (2018 - 11 - 02) 全文	1-10

☐ 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

2020年 2月 13日

国际检索报告邮寄日期

2020年 2月 21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

丁文勃

电话号码 86-(10)-53961330

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2019/119312

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	110033261	A	2019年 7月 19日	无	
CN	108664223	A	2018年 10月 16日	W0 2019218717 A1	2019年 11月 21日
US	2018101701	A1	2018年 4月 12日	无	
CN	109034800	A	2018年 12月 18日	无	
CN	108737068	A	2018年 11月 2日	无	