(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)

WIPO | PCT

(10) 国际公布号
WO 2020/134898 A1

(51) 国际专利分类号:
G06F 21/62 (2013.01)

(21) 国际申请号: PCT/CN2019/122552

(22) 国际申请日: 2019 年 12 月 3 日 (03.12.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201811605349.2 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, 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)。

(54) **Title:** HASH INFORMATION PROCESSING METHOD AND SYSTEM FOR STORAGE RECORDS IN BLOCK OF BLOCKCHAIN

(54) **发明名称**: 区块链的区块中存储记录的哈希信息处理方法和系统

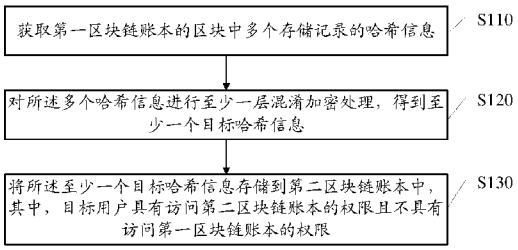

图 1

S110 Obtain hash information of a plurality of storage records in a block of a first blockchain account book

S120 Perform at least one confusion encryption processing on the plurality of pieces of hash information to obtain at least one piece of target hash information

S130 Store the at least one piece of target hash information in a second blockchain account book, wherein the target user has an authority to access the second blockchain account book but does not have an authority to access the first blockchain account book

(57) **Abstract:** A hash information processing method and system for storage records in a block of a blockchain, and an electronic device. The method comprises: obtaining hash information of a plurality of storage records in a block of a first blockchain account book (S110); performing at least one confusion encryption processing on the plurality of pieces of hash information to obtain at least one piece of target hash information (S120); and storing the at least one piece of target hash information in a second blockchain account book, wherein the target user has an authority to access the second blockchain account book but does not have an authority to access the first blockchain account book (S130).

(57) **摘要**: 一种区块链的区块中存储记录的哈希信息处理方法、系统和电子设备，该方法包括：获取第一区块链账本的区块中多个存储记录的哈希信息（S110）；对所述多个哈希信息进行至少一层混淆加密处理，得到至少一个目标哈希信息（S120）；将所述至少一个目标哈希信息存储到第二区块链账本中，其中，目标用户具有访问第二区块链账本的权限且不具有访问第一区块链账本的权限（S130）。

WO 2020/134898 A1

[见续页]

本国际公布:

— 包括国际检索报告(条约第21条(3))。

区块链的区块中存储记录的哈希信息处理方法和系统

技术领域

[01] 本申请涉及计算机软件技术领域，尤其涉及一种区块链的区块中存储记录的哈希信息处理方法和系统。

背景技术

[02] 区块链账本具备真实透明，不可删除的特性，应用范围越来越广泛，基本涉及到各个行业。

[03] 但是，由于区块链账本的架构原因，即使对明文进行加密，使用哈希（hash）上链的方式，公众仍然可以通过解析区块链账本获得区块链上的真实交易量。

[04] 在保障数据真实透明的同时，如何对业务的交易规模交易量级进行保护，是亟待解决的技术问题。

发明内容

[05] 本申请实施例的目的是提供一种区块链的区块中存储记录的哈希信息处理方法和系统，以对区块链中业务的交易规模交易量级进行保护，使得更多的业务能够使用区块链技术的同时更好地保护业务数据。

[06] 为解决上述技术问题，本申请实施例是这样实现的:

[07] 第一方面，提出了一种区块链的区块中存储记录的哈希信息处理方法，该方法包括:

[08] 获取第一区块链账本的区块中多个存储记录的哈希信息;

[09] 对所述多个哈希信息进行至少一层混淆加密处理，得到至少一个目标哈希信息;

[10] 将所述至少一个目标哈希信息存储到第二区块链账本中，其中，目标用户具有访问第二区块链账本的权限且不具有访问第一区块链账本的权限。

[11] 第二方面，提出了一种区块链系统，该区块链系统包括:

[12] 获取模块，获取第一区块链账本的区块中多个存储记录的哈希信息;

[13] 混淆加密处理模块，对所述多个哈希信息进行至少一层混淆加密处理，得到至少

一个目标哈希信息;

[14] 存储模块，将所述至少一个目标哈希信息存储到第二区块链账本中，其中，目标用户具有访问第二区块链账本的权限且不具有访问第一区块链账本的权限。

[15] 第三方面，提出了一种电子设备，该电子设备包括:

[16] 处理器；以及

[17] 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执行以下操作:

[18] 获取第一区块链账本的区块中多个存储记录的哈希信息；对所述多个哈希信息进行至少一层混淆加密处理，得到至少一个目标哈希信息；将所述至少一个目标哈希信息存储到第二区块链账本中，其中，目标用户具有访问第二区块链账本的权限且不具有访问第一区块链账本的权限。

[19] 第四方面，提出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一个或多个程序，所述一个或多个程序当被包括多个应用程序的电子设备执行时，使得所述电子设备执行以下操作:

[20] 获取第一区块链账本的区块中多个存储记录的哈希信息；对所述多个哈希信息进行至少一层混淆加密处理，得到至少一个目标哈希信息；将所述至少一个目标哈希信息存储到第二区块链账本中，其中，目标用户具有访问第二区块链账本的权限且不具有访问第一区块链账本的权限。

附图说明

[21] 为了更清楚地说明本申请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申请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的前提下，还可以根据这些附图获得其他的附图。

[22] 图 1 是本申请的一个实施例区块链的区块中存储记录的哈希信息处理方法流程图。

[23] 图 2 是本申请的一个实施例电子设备的结构示意图。

[24] 图 3 是本申请的一个实施例区块链系统的结构示意图。

具体实施方式

[25] 本申请实施例提供一种区块链的区块中存储记录的哈希信息处理方法、系统和电子设备。

[26] 为了使本技术领域的人员更好地理解本申请中的技术方案，下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅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，都应当属于本申请保护的范围。

[27] 图 1 是本申请的一个实施例区块链的区块中存储记录的哈希信息处理方法流程图。图 1 的方法可包括:

[28] S110，获取第一区块链账本的区块中多个存储记录的哈希信息。

[29] 应理解，在不同的区块链应用场景中，区块链中的存储记录可存储不同的内容。例如，在涉及区块链交易的系统中，一个存储记录即区块链的一个交易记录。

[30] 应理解，在本申请实施例中，在获取第一区块链账本的区块中多个存储记录的哈希信息时，可通过该区块的交易树获取多个存储记录的哈希信息。

[31] 应理解，在比特币等区块链 1.0 的区块链系统中，只有一个默克尔（Merkle）树，某种程度上来说，这棵树也可以称为交易树；而在以太坊等区块链 2.0 的区块链系统中，则存在交易（Transactions）树、收据（Receipts）树和状态（State）树三棵 Merkle 树。

[32] 可选地，作为一个实施例，步骤 S110 可实现为：逐个区块获取第一区块链账本的区块中多个存储记录的哈希信息，以进行混淆加密处理，直至读取完区块链的最新区块。

[33] 对于本实施例来说，可以将区块链的历史区块的信息都按照本申请实施例的方案进行混淆加密处理。

[34] 或者，可选的，作为另一个实施例，步骤 S110 可实现为：响应于第一区块链账本的最新区块的存储事件，获取所述最新区块中多个存储记录的哈希信息。

[35] 对于本实施例来说，需要在第一区块链账本所属的区块链启动时就执行本申请实施例的方案，才能保证第一区块链账本的所有区块的存储记录混淆后的哈希信息在第二区块链账本可查询。当然，如果不需要查询第一区块链账本的所有区块的存储记录混淆后的哈希信息，也可不对本申请实施例的方法的执行时机进行限制。

[36] S120，对所述多个哈希信息进行至少一层混淆加密处理，得到至少一个目标哈希信息。

[37] 在本申请实施例中，通过对区块的存储记录的哈希信息进行混淆加密处理，可以避免泄露区块链中区块的交易量信息。

[38] 特别地，所述至少一个目标哈希信息的个数不等于所述多个哈希信息的个数。

[39] S130，将所述至少一个目标哈希信息存储到第二区块链账本中，其中，目标用户具有访问第二区块链账本的权限且不具有访问第一区块链账本的权限。

[40] 本申请实施例中，通过将第一区块链账本中区块的存储记录的哈希信息进行混淆加密处理存储到目标用户能够访问的第二区块链账本中，从而能够避免目标用户直接访问第一区块链账本带来的交易规模及交易量级等信息的泄密，保障了第一区块链账本所属的区块链系统的信息安全。

[41] 应理解，目标用户具有访问第二区块链账本的权限且不具有访问第一区块链账本的权限，有多种实现方式:

[42] 例如所述第一区块链账本所在的区块链为私有链；所述第二区块链账本所在的区块链。此时，所述第一区块链账本所在的区块链的账户节点以外的其它节点将不具备第一区块链账本的访问权限，但可以访问第二区块链账本。

[43] 又例如，所述第一区块链账本所在的区块链和所述第二区块链账本所在的区块链都为私有链，目标账户配置了第二区块链账本的访问权限，但没有配置第一区块链账本的访问权限。

[44] 应理解，在本申请实施例中，对哈希信息的混淆加密处理可包括多种方式。

[45] 可选地，在一种实现方式中，可将多个哈希信息组成的内容进行哈希计算得到一个哈希信息。

[46] 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信息分别为 HashA、HashB、HashC 和 HashD，则混淆加密处理后的哈希信息 HashABCD=Hash（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。

[47] 可选地，在另一种实现方式中，可将任一个哈希信息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信息。

[48] 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信息为 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信息。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。

[49] 可选地，在另一种实现方式中，可将多个哈希信息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信息。

[50] 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信息分别为 HashA、HashB、HashC 和 HashD，其组成的内容 HashABCD=（HashA+HashB+HashC+HashD）；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信息。

[51] 当然，前面仅仅列举了几种，具体还可能存在其它处理的方式，不作限制。

[52] 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信息，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。

[53] 例如，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信息分别为 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信息为 Hash(HashABCD1)和 Hash(HashABCD2)，其中 HashABCD= HashABCD1+HashABCD2。

[54] 可选地，作为一个实施例，所述至少一个目标哈希信息为所述区块的交易树的 M 根。即参照 Merkle 树的生成方式将区块中的存储记录哈希得到哈希信息，再将哈希信息两两哈希得到新的哈希信息，直至得到一个哈希值。

[55] 可选地，作为一个实施例，步骤 S130 具体可实现为：

[56] 将所述区块的唯一标识及所述至少一个目标哈希信息存储到所述第二区块链账本中。

[57] 本申请实施例中，将区块的唯一标识和生成的至少一个目标哈希信息一起存储到所述第二区块链账本，以便目标用户能够基于区块的唯一标识确定所述至少一个目标哈希信息归属于哪个区块。

[58] 进一步的，在本申请实施例的一个具体实现方式中，可将所述区块的唯一标识及所述至少一个目标哈希信息作为一条存储记录存储到所述第二区块链账本中。

[59] 在本申请实施例中，一个区块的所有混淆后的哈希信息作为一个存储记录进行存储。

[60] 或者，进一步的，在本申请实施例的另一个具体实现方式中，可将所述区块的唯一标识及一个目标哈希信息中作为存储记录存储到所述第二区块链账本中。

[61] 在本申请实施例中，一个区块的混淆后的一个哈希信息作为一个存储记录进行存储。

[62] 或者，进一步的，在本申请实施例的另一个具体实现方式中，可将所述区块的唯一标识及不多于预定个数的目标哈希信息作为存储记录存储到所述第二区块链账本中。

[63] 当然，应理解，在本申请实施例的上述实现方式中，所述存储记录中还可携带所述区块的区块头中的至少一种信息，例如父区块的哈希信息、所述区块的时间戳信息，等等。

[64] 可选地，作为一个实施例，所述方法还包括:

[65] 将混淆算法的代码存储在第三区块链账本中，所述混淆算法用于对所述多个哈希信息进行至少一层混淆加密处理以得到所述至少一个目标哈希信息。

[66] 可选地，作为一个实施例，所述方法通过调用第一区块链账本所在的区块链的智能合约实现。

[67] 当然，应理解，所述方法可以由第一区块链账本所在的区块链以外的第三方装置实现，本申请实施例对此不做限制。

[68] 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。

[69] 图 2 是本申请的一个实施例电子设备的结构示意图。请参考图 2，在硬件层面，该电子设备包括处理器，可选地还包括内部总线、网络接口、存储器。其中，存储器可能包含内存，例如高速随机存取存储器（Random-Access Memory，RAM），也可能还包括非易失性存储器（non-volatile memory），例如至少 1 个磁盘存储器等。当然，该电子设备还可能包括其他业务所需要的硬件。

[70] 处理器、网络接口和存储器可以通过内部总线相互连接，该内部总线可以是 ISA(Industry Standard Architecture，工业标准体系结构）总线、PCI（Peripheral Component Interconnect，外设部件互连标准）总线或 EISA(Extended Industry Standard Architecture，扩展工业标准结构）总线等。所述总线可以分为地址总线、数据总线、控制总线等。为便于表示，图 2 中仅用一个双向箭头表示，但并不表示仅有一根总线或一种类型的总线。

[71] 存储器，用于存放程序。具体地，程序可以包括程序代码，所述程序代码包括计算机操作指令。存储器可以包括内存和非易失性存储器，并向处理器提供指令和数据。

[72] 处理器从非易失性存储器中读取对应的计算机程序到内存中然后运行，在逻辑层面上形成区块链系统。处理器，执行存储器所存放的程序，并具体用于执行以下操作：

[73] 获取第一区块链账本的区块中多个存储记录的哈希信息；

[74] 对所述多个哈希信息进行至少一层混淆加密处理，得到至少一个目标哈希信息；

[75] 将所述至少一个目标哈希信息存储到第二区块链账本中，其中，目标用户具有访问第二区块链账本的权限且不具有访问第一区块链账本的权限。

[76] 上述如本申请图 1 所示实施例揭示的区块链系统执行的方法可以应用于处理器中，或者由处理器实现。处理器可能是一种集成电路芯片，具有信号的处理能力。在实现过程中，上述方法的各步骤可以通过处理器中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器可以是通用处理器，包括中央处理器（Central Processing Unit，CPU）、网络处理器（Network Processor，NP）等；还可以是数字信号处理器（Digital Signal Processor，DSP）、专用集成电路（Application Specific Integrated Circuit，ASIC）、现场可编程门阵列（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。可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。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。结合本申请实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随

机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器，处理器读取存储器中的信息，结合其硬件完成上述方法的步骤。

[77] 该电子设备还可执行图 1 的方法，并实现区块链系统在图 1 所示实施例的功能，本申请实施例在此不再赘述。

[78] 当然，除了软件实现方式之外，本申请的电子设备并不排除其他实现方式，比如逻辑器件抑或软硬件结合的方式等等，也就是说以下处理流程的执行主体并不限定于各个逻辑单元，也可以是硬件或逻辑器件。

[79] 本申请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便携式电子设备执行时，能够使该便携式电子设备执行图 1 所示实施例的方法，并具体用于执行以下操作:

[80] 获取第一区块链账本的区块中多个存储记录的哈希信息;

[81] 对所述多个哈希信息进行至少一层混淆加密处理，得到至少一个目标哈希信息;

[82] 将所述至少一个目标哈希信息存储到第二区块链账本中，其中，目标用户具有访问第二区块链账本的权限且不具有访问第一区块链账本的权限。

[83] 图 3 是本申请的一个实施例区块链系统 300 的结构示意图。请参考图 3，在一种软件实施方式中，区块链系统 300 可包括:

[84] 获取模块 310，获取第一区块链账本的区块中多个存储记录的哈希信息;

[85] 混淆加密处理模块 320，对所述多个哈希信息进行至少一层混淆加密处理，得到至少一个目标哈希信息;

[86] 存储模块 330，将所述至少一个目标哈希信息存储到第二区块链账本中，其中，目标用户具有访问第二区块链账本的权限且不具有访问第一区块链账本的权限。

[87] 本申请实施例中，通过将第一区块链账本中区块的存储记录的哈希信息进行混淆加密处理存储到目标用户能够访问的第二区块链账本中，从而能够避免目标用户直接访问第一区块链账本带来的交易规模及交易量级等信息的泄密，保障了第一区块链账本所属的区块链系统的信息安全。

[88] 可选地，获取模块 310 具体可用于:

[89] 响应于第一区块链账本的最新区块的存储事件，获取所述最新区块中多个存储记录的哈希信息。

[90] 可选地，所述第一区块链账本所在的区块链为私有链，所述第二区块链账本所在的区块链为公有链。

[91] 或者，可选地，所述第一区块链账本所在的区块链为私有链，所述第二区块链账本所在的区块链为私有链。

[92] 可选地，一层所述混淆加密处理包括如下之一:

[93] 将多个哈希信息组成的内容进行哈希计算得到一个哈希信息;

[94] 将任一个哈希信息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信息;

[95] 将多个哈希信息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信息。

[96] 可选地，所述至少一个目标哈希信息为所述区块的交易树的 M 根。

[97] 可选地，作为一个实施例，存储模块 330 具体用于:

[98] 将所述至少一个目标哈希信息存储到第二区块链账本中，包括:

[99] 将所述区块的唯一标识及所述至少一个目标哈希信息存储到所述第二区块链账本中。

[100] 进一步地，在本实施例的一种实现方式中，存储模块 330 具体用于:

[101] 将所述区块的唯一标识及所述至少一个目标哈希信息作为一条存储记录存储到所述第二区块链账本中。

[102] 或者，进一步地，在本实施例的另一种实现方式中，存储模块 330 具体用于:

[103] 将所述区块的唯一标识及一个目标哈希信息中作为存储记录存储到所述第二区块链账本中。

[104] 或者，进一步地，在本实施例的再一种实现方式中，存储模块 330 具体用于:

[105] 将所述区块的唯一标识及不多于预定个数的目标哈希信息作为存储记录存储到所述第二区块链账本中。

[106] 更进一步地，在上述具体的实现方式中，所述存储记录中还可携带所述区块的区

块头中的至少一种信息。

[107] 可选地，所述存储模块 330 还可用于:

[108] 将混淆算法的代码存储在第三区块链账本中，所述混淆算法用于对所述多个哈希信息进行至少一层混淆加密处理以得到所述至少一个目标哈希信息。

[109] 可选地，所述至少一个目标哈希信息的个数不等于所述多个哈希信息的个数。

[110] 区块链系统 300 还可执行图 1 所示实施例的方法，具体实现可参考图 1 所示实施例，不再赘述。

[111] 总之，以上所述仅为本申请的较佳实施例而已，并非用于限定本申请的保护范围。凡在本申请的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本申请的保护范围之内。

[112] 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。

[113] 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。

[114] 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。

[115] 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。

5

权利要求书

1、一种区块链的区块中存储记录的哈希信息处理方法，包括:

获取第一区块链账本的区块中多个存储记录的哈希信息;

对所述多个哈希信息进行至少一层混淆加密处理，得到至少一个目标哈希信息;

将所述至少一个目标哈希信息存储到第二区块链账本中，其中，目标用户具有访问第二区块链账本的权限且不具有访问第一区块链账本的权限。

2、如权利要求 1 所述的方法，

所述第一区块链账本所在的区块链为私有链，所述第二区块链账本所在的区块链为公有链; 或者

所述第一区块链账本所在的区块链和所述第二区块链账本所在的区块链都为私有链。

3、如权利要求 1 所述的方法，一层所述混淆加密处理包括如下之一:

将多个哈希信息组成的内容进行哈希计算得到一个哈希信息;

将任一个哈希信息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信息;

将多个哈希信息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信息。

4、如权利要求 1 所述的方法，

所述至少一个目标哈希信息为所述区块的交易树的 M 根。

5、如权利要求 1 所述的方法，

将所述至少一个目标哈希信息存储到第二区块链账本中，包括:

将所述区块的唯一标识及所述至少一个目标哈希信息存储到所述第二区块链账本中。

6、如权利要求 5 所述的方法，

将所述区块的唯一标识及所述至少一个目标哈希信息存储到所述第二区块链账本中，包括:

将所述区块的唯一标识及所述至少一个目标哈希信息作为一条存储记录存储到所述第二区块链账本中。

7、如权利要求 5 所述的方法，

将所述区块的唯一标识及所述至少一个目标哈希信息存储到所述第二区块链账本中，包括:

将所述区块的唯一标识及一个目标哈希信息中作为存储记录存储到所述第二区块链账本中。

8、如权利要求 5 所述的方法，

将所述区块的唯一标识及所述至少一个目标哈希信息存储到所述第二区块链账本中，包括:

将所述区块的唯一标识及不多于预定个数的目标哈希信息作为存储记录存储到所述第二区块链账本中。

9、如权利要求 6-8 任一项所述的方法，所述存储记录中还携带所述区块的区块头中的至少一种信息。

10、如权利要求 1 所述的方法，所述方法还包括:

将混淆算法的代码存储在第三区块链账本中，所述混淆算法用于对所述多个哈希信息进行至少一层混淆加密处理以得到所述至少一个目标哈希信息。

11、如权利要求 1 所述的方法，所述方法通过调用第一区块链账本所在的区块链的智能合约实现。

12、如权利要求 1 所述的方法，

所述至少一个目标哈希信息的个数不等于所述多个哈希信息的个数。

13、如权利要求 1 所述的方法，

获取第一区块链账本的区块中多个存储记录的哈希信息，包括:

响应于第一区块链账本的最新区块的存储事件，获取所述最新区块中多个存储记录的哈希信息。

14、一种区块链系统，包括:

获取模块，获取第一区块链账本的区块中多个存储记录的哈希信息;

混淆加密处理模块，对所述多个哈希信息进行至少一层混淆加密处理，得到至少一个目标哈希信息;

存储模块，将所述至少一个目标哈希信息存储到第二区块链账本中，其中，目标用户具有访问第二区块链账本的权限且不具有访问第一区块链账本的权限。

15、一种电子设备，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器执行以下操作:

获取第一区块链账本的区块中多个存储记录的哈希信息;

对所述多个哈希信息进行至少一层混淆加密处理，得到至少一个目标哈希信息；

将所述至少一个目标哈希信息存储到第二区块链账本中，其中，目标用户具有访问第二区块链账本的权限且不具有访问第一区块链账本的权限。

16、一种计算机可读存储介质，所述计算机可读存储介质存储一个或多个程序，所述一个或多个程序当被包括多个应用程序的电子设备执行时，使得所述电子设备执行以下操作：

获取第一区块链账本的区块中多个存储记录的哈希信息；

对所述多个哈希信息进行至少一层混淆加密处理，得到至少一个目标哈希信息；

将所述至少一个目标哈希信息存储到第二区块链账本中，其中，目标用户具有访问第二区块链账本的权限且不具有访问第一区块链账本的权限。

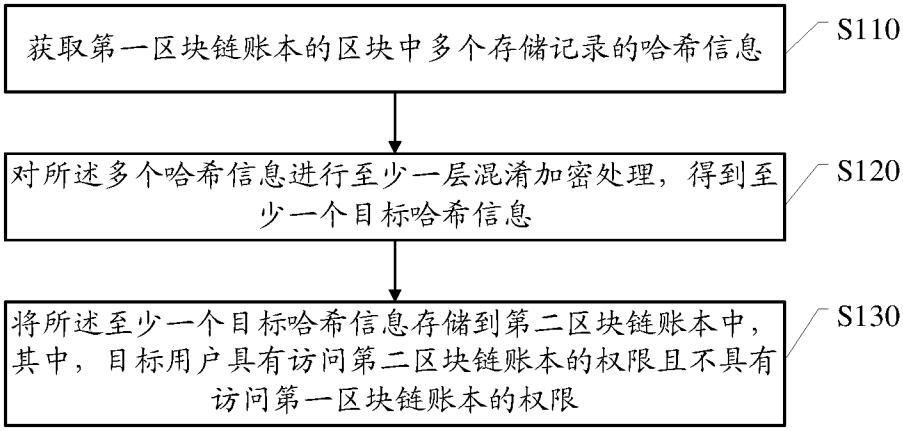
获取第一区块链账本的区块中多个存储记录的哈希信息
S110
对所述多个哈希信息进行至少一层混淆加密处理，得到至少一个目标哈希信息
S120
将所述至少一个目标哈希信息存储到第二区块链账本中，其中，目标用户具有访问第二区块链账本的权限且不具有访问第一区块链账本的权限
S130

图 1

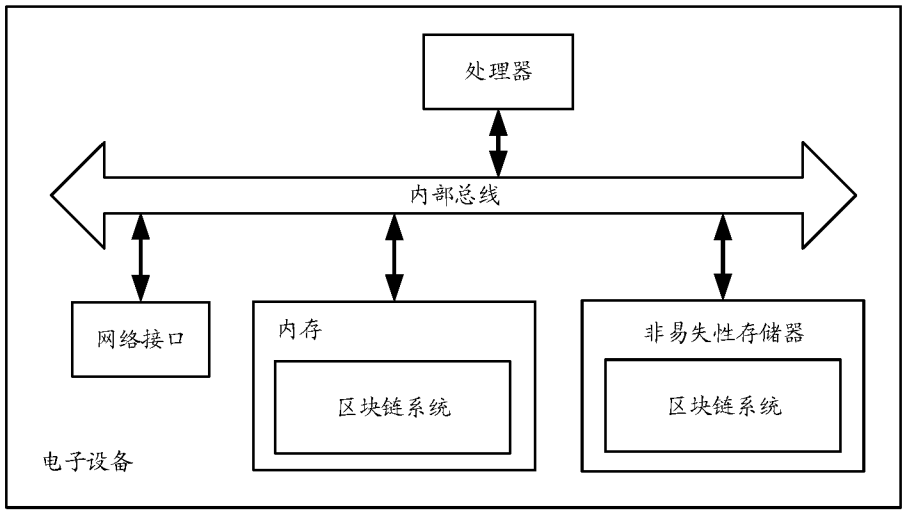
处理器
内部总线
网络接口
内存
区块链系统
非易失性存储器
区块链系统
电子设备

图 2

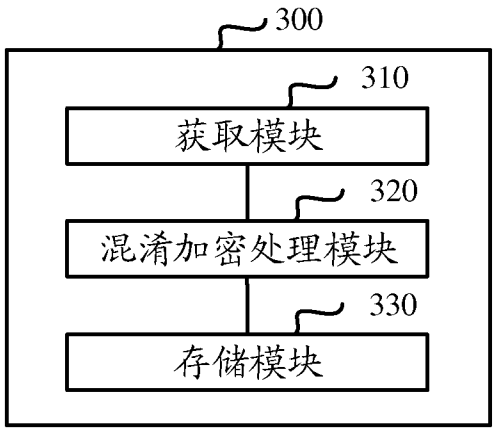

图 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/122552

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/62(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)

CNPAT, IEEE, CNKI, EPODOC, WPI, GOOGLE: 区块链, 第一, 第二, 链, 哈希, 公有, 私有, M根, 权限, 访问, 保护, 交易量, blockchain, first, second, chain, hash, private, public, root, authority, access, protect, transaction

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110020544 A (ALIBABA GROUP HOLDING LIMITED) 16 July 2019 (2019-07-16) claims 1-16	1-16
X	CN 106372533 A (CHINA UNIONPAY CO., LTD.) 01 February 2017 (2017-02-01) description, paragraphs 0027-0041	1-16
A	CN 108710658 A (ALIBABA GROUP HOLDING LIMITED) 26 October 2018 (2018-10-26) entire document	1-16
A	US 2018285869 A1 (ALIBABA GROUP HOLDING LIMITED) 04 October 2018 (2018-10-04) entire document	1-16

☐ 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
25 February 2020	**04 March 2020**

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

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/122552

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 110020544 A	16 July 2019	None	
CN 106372533 A	01 February 2017	None	
CN 108710658 A	26 October 2018	None	
US 2018285869 A1	04 October 2018	CA 3057331 A1	04 October 2018
		CN 107395557 A	24 November 2017
		AU 2018243625 A1	03 October 2019
		TW 201837772 A	16 October 2018
		WO 2018183055 A1	04 October 2018
		SG 11201908382P A	30 October 2019
		KR 20190123774 A	01 November 2019

国际检索报告

国际申请号
PCT/CN2019/122552

A. 主题的分类

G06F 21/62(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））

CNPAT,IEEE,CNKI,EPODOC,WPI,GOOGLE：区块链，第一，第二，链，哈希，公有，私有，M根，权限，访问，保护，交易量，blockchain，first，second，chain，hash，private，public，root，authority，access，protect，transaction

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 110020544 A (阿里巴巴集团控股有限公司) 2019年 7月 16日 (2019-07-16) 权利要求1-16	1-16
X	CN 106372533 A (中国银联股份有限公司) 2017年 2月 1日 (2017-02-01) 说明书第0027-0041段	1-16
A	CN 108710658 A (阿里巴巴集团控股有限公司) 2018年 10月 26日 (2018-10-26) 全文	1-16
A	US 2018285869 A1 (ALIBABA GROUP HOLDING LIMITED) 2018年 10月 4日 (2018-10-04) 全文	1-16

☐ 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 2月 25日	2020年 3月 4日

ISA/CN的名称和邮寄地址	受权官员
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	王平
传真号 (86-10)62019451	电话号码 86-(10)-53961372

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/122552

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	110020544	A	2019年 7月 16日	无			
CN	106372533	A	2017年 2月 1日	无			
CN	108710658	A	2018年 10月 26日	无			
US	2018285869	A1	2018年 10月 4日	CA	3057331	A1	2018年 10月 4日
				CN	107395557	A	2017年 11月 24日
				AU	2018243625	A1	2019年 10月 3日
				TW	201837772	A	2018年 10月 16日
				WO	2018183055	A1	2018年 10月 4日
				SG	11201908382P	A	2019年 10月 30日
				KR	20190123774	A	2019年 11月 1日