

(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



(10) 国际公布号

WO 2020/238248 A1

(43) 国际公布日

2020 年 12 月 3 日 (03.12.2020)

(51) 国际专利分类号:

G06F 21/62 (2013.01)

(21) 国际申请号:

PCT/CN2020/071678

(22) 国际申请日:

2020 年 1 月 13 日 (13.01.2020)

(25) 申请语言:

中文

(26) 公布语言:

中文

(30) 优先权:

201910473001.0 2019年5月31日 (31.05.2019) CN

(71) 申请人: 创新先进技术有限公司 (ADVANCED

NEW TECHNOLOGIES CO., LTD.) [—/CN]; 开曼

群岛大开曼岛乔治镇医院路27号开曼企业

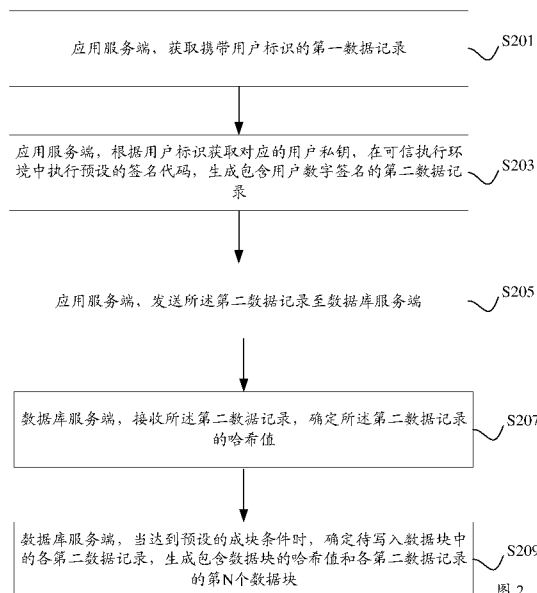
中心, Grand Cayman KY1-9008 (KY)。

(72) 发明人: 李亿泽(LI, Yize); 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)。 杨新颖(YANG, Xinying); 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)。 张渊(ZHANG, Yuan); 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)。 俞本权(YU, Benquan); 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)。 闫文远(YAN, Wen Yuan); 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

(54) Title: DATA STORAGE METHOD, APPARATUS AND DEVICE

(54) 发明名称: 一种数据存储方法、装置及设备



S201 An application serving end acquires a first data record carrying a user identifier
S203 The application serving end acquires a user private key according to the user identifier, and executes a preset signature code in a trusted execution environment to generate a second data record including a digital signature of a user
S205 The application serving end sends the second data record to a database serving end
S207 The database serving end receives the second data record and determines a hash value of the second data record
S209 When a preset block forming condition is achieved, the database serving end determines second data records in data blocks to be written to generate the Nth data block including the hash value of the data block and the second data records

(57) Abstract: Disclosed are a data storage method and apparatus and device. An application serving end performs digital signature on user data in a trusted execution environment to generate a second data record including the digital signature of a user, and the second data record is stored in a centralized blockchain account book, so that the data including the digital signature of the user cannot be tampered with.

(57) 摘要: 公开了一种数据存储方法、装置及设备。应用服务端将用户数据在可信执行环境中进行数字签名, 生成包含用户数字签名的第二数据记录, 将第二数据记录存储在中心化的区块链式账本中, 实现了对于包含用户数字签名的数据的不可篡改。

[见续页]

海淀区上地三街9号嘉华大厦B座409,
Beijing 100085 (CN)。

(81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(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))。

一种数据存储方法、装置及设备

技术领域

[01] 本说明书实施例涉及信息技术领域，尤其涉及一种数据存储方法、装置及设备。

背景技术

5 [02] 在以中心化的块链式账本存储数据时，通常而言，数据库服务端并不直接面向用户。用户的数据是基于应用服务端所产生，进而是应用服务端将用户数据转发至数据库服务端进行存储。在这种情形下，用户并不知晓自己的数据是否在存储过程中发生了错误或者改动。

[03] 基于此，需要一种可以保障用户存储数据安全性的方法，提高用户体验。

10 发明内容

[04] 本申请实施例的目的是提供一种可以保障用户存储数据安全性的方法。

[05] 为解决上述技术问题，本申请实施例是这样实现的：

[06] 一种数据存储方法，应用于包括应用服务端和数据库服务端的系统中，所述方法包括：

15 [07] 应用服务端，获取携带用户标识的第一数据记录；

[08] 应用服务端，根据用户标识获取对应的用户私钥，在可信执行环境中执行预设的签名代码，生成包含用户数字签名的第二数据记录，其中，所述签名代码用于根据用户私钥对所述第一数据记录进行数字签名；

[09] 应用服务端，发送所述第二数据记录至数据库服务端；

20 [10] 数据库服务端，接收所述第二数据记录，确定所述第二数据记录的哈希值；

[11] 数据库服务端，当达到预设的成块条件时，确定待写入数据块中的各第二数据记录，生成包含数据块的哈希值和各第二数据记录的第 N 个数据块，具体包括：

[12] 当 $N=1$ 时，初始数据块的哈希值和块高基于预设方式给定；

[13] 当 $N>1$ 时，根据待写入数据块中的第二数据记录和第 $N-1$ 个数据块的哈希值确

定第 N 个数据块的哈希值，生成包含第 N 个数据块的哈希值和各第二数据记录的第 N 个数据块，其中，数据块的块高基于成块时间的先后顺序单调递增。

[14] 对应的，本说明书实施例还提供一种数据存储系统，包括应用服务端和数据库服务端，在所述系统中，

5 [15] 应用服务端，获取携带用户标识的第一数据记录；根据用户标识获取对应的用户私钥，在可信执行环境中执行预设的签名代码，生成包含用户数字签名的第二数据记录，其中，所述签名代码用于根据用户私钥对所述第一数据记录进行数字签名；发送所述第二数据记录至数据库服务端；

[16] 数据库服务端，接收所述第二数据记录，确定所述第二数据记录的哈希值；

10 [17] 当达到预设的成块条件时，确定待写入数据块中的各第二数据记录，生成包含数据块的哈希值和各第二数据记录的第 N 个数据块，具体包括：

[18] 当 $N=1$ 时，初始数据块的哈希值和块高基于预设方式给定；

[19] 当 $N>1$ 时，根据待写入数据块中的第二数据记录和第 $N-1$ 个数据块的哈希值确定第 N 个数据块的哈希值，生成包含第 N 个数据块的哈希值和各第二数据记录的第 N
15 个数据块，其中，数据块的块高基于成块时间的先后顺序单调递增。

[20] 另一方面，本说明书实施例还提供一种数据存储方法，应用于应用服务端中，所述方法包括：

[21] 获取携带用户标识的第一数据记录；

[22] 根据用户标识获取对应的用户私钥，在可信执行环境中执行预设的签名代码，生
20 成包含用户数字签名的第二数据记录，其中，所述签名代码用于根据用户私钥对所述第一数据记录进行数字签名；

[23] 发送所述第二数据记录至数据库服务端。

[24] 对应的，本说明书实施例还提供一种数据存储装置，应用于应用服务端中，所述装置包括：

25 [25] 接收模块，获取携带用户标识的第一数据记录；

[26] 生成模块，根据用户标识获取对应的用户私钥，在可信执行环境中执行预设的签名代码，生成包含用户数字签名的第二数据记录，其中，所述签名代码用于根据用户私

钥对所述第一数据记录进行数字签名；

[27] 发送模块，发送所述第二数据记录至数据库服务端。

[28] 通过本说明书实施例所提供的方案，应用服务端将用户数据在可信执行环境中进行数字签名，生成包含用户数字签名的第二数据记录，将第二数据记录存储在中心化的块链式账本中，实现了对于包含用户数字签名的数据的不可篡改，保障了用户存储数据安全性，提高用户体验。

[29] 应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本说明书实施例。

[30] 此外，本说明书实施例中的任一实施例并不需要达到上述的全部效果。

10 附图说明

[31] 为了更清楚地说明本说明书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，还可以根据这些附图获得其他的附图。

[32] 图 1 本说明书实施例中所涉及的系统架构的示意图；

15 [33] 图 2 是本说明书实施例提供的一种系统方面的数据存储方法的流程示意图；

[34] 图 3 为本说明书实施例所提供的应用服务端方面的数据存储方法的流程示意图；

[35] 图 4 是本说明书实施例提供的一种数据存储装置的结构示意图；

[36] 图 5 是用于配置本说明书实施例方法的一种设备的结构示意图。

具体实施方式

20 [37] 为了使本领域技术人员更好地理解本说明书实施例中的技术方案，下面将结合本说明书实施例中的附图，对本说明书实施例中的技术方案进行详细地描述，显然，所描述的实施例仅仅是本说明书的一部分实施例，而不是全部的实施例。基于本说明书中的实施例，本领域普通技术人员所获得的所有其他实施例，都应当属于保护的范围。

25 [38] 在当前的服务器架构中，数据库服务端可以是直接对接的客户端个人用户，也可以是由一些应用服务端对接客户端个人用户，而数据库服务端则对接所述应用服务端。如图 1 所示，图 1 本说明书实施例中所涉及的系统架构的示意图。

[39] 以下结合附图，详细说明本说明书各实施例提供的技术方案。如图 2 所示，图 2 是本说明书实施例提供的一种系统方面的数据存储方法的流程示意图，应用于包括应用服务端和数据库服务端的系统中，该流程具体包括如下步骤：

[40] S201，应用服务端，获取携带用户标识的第一数据记录。

5 [41] 第一数据记录可以是客户端发送的原始数据，例如，客户端所发送的操作命令、交易订单等等；也可以是应用服务端基于客户端的操作所产生的数据，例如，操作日志等等。

10 [42] 在应用服务端，可以获取此时的客户端所对应的用户标识，并将用户标识与第一数据记录进行绑定，例如，写入第一数据记录的指定位置中；或者，拼接第一数据记录的头部等等，从而得到携带用户标识的第一数据记录。

[43] S203，应用服务端，根据用户标识获取对应的用户私钥，在可信执行环境中执行预设的签名代码，生成包含用户数字签名的第二数据记录。

15 [44] 需要说明的是，在本说明书实施例中，应用服务端一般是中心化的提供服务，各用户可以将自身的私钥存储于应用服务端之中，并且与用户标识建立相应的对应关系，以及，可以随时使用自身的公钥对应用服务端的加密结果进行验证，从而能够保证应用服务端在加密过程中使用的是自身的私钥。

[45] 同时，应用服务端在加密过程中，执行一段可以公开所见的代码，从而公众以及用户均可以了解该代码的用途，进而保证在本说明书实施例中所得到的加密数据的公正性。

20 [46] 在本说明书实施例中，该代码为一段签名代码，用于根据用户私钥对所述第一数据记录进行数字签名。使用私钥进行数字签名的方法已经很常见，此处不再赘述。需要说明的是，在这个过程中，调用的用户私钥并不公开所见的。

25 [47] 为此，在应用服务端中，可以在可信执行环境(Trusted Execution Environment, TEE)进行私钥签名来保障公正性。TEE 可以起到硬件中的黑箱作用，在 TEE 中执行的代码和数据操作系统层都无法偷窥，只有代码中预先定义的接口才能对其进行操作。

[48] 可信执行环境是基于 CPU 硬件的安全扩展，且与外部完全隔离的可信执行环境。TEE 最早是由 Global Platform 提出的概念，用于解决移动设备上资源的安全隔离，平行于操作系统为应用程序提供可信安全的执行环境。ARM 的 Trust Zone 技术最早实现了

真正商用的 TEE 技术。

[49] 伴随着互联网的高速发展，安全的需求越来越高，不仅限于移动设备，云端设备，数据中心都对 TEE 提出了更多的需求。TEE 的概念也得到了高速的发展和扩充。现在所说的 TEE 相比与最初提出的概念已经是更加广义的 TEE。例如，服务器芯片厂商 Intel，AMD 等都先后推出了硬件辅助的 TEE 并丰富了 TEE 的概念和特性，在工业界得到了广泛的认可。现在提起的 TEE 通常更多指这类硬件辅助的 TEE 技术。不同于移动端，云端访问需要远程访问，终端用户对硬件平台不可见，因此使用 TEE 的第一步就是要确认 TEE 的真实可信。因此现在的 TEE 技术都引入了远程证明机制，由硬件厂商(主要是 CPU 厂商)背书并通过数字签名技术确保用户对 TEE 状态可验证。换言之，在 TEE 中执行的结果可以得到硬件厂商的数字签名。

[50] 同时仅仅是安全的资源隔离也无法满足的安全需求，进一步的数据隐私保护也被提出。包括 Intel SGX，AMD SEV 在内的商用 TEE 也都提供了内存加密技术，将可信硬件限定在 CPU 内部，总线和内存的数据均是密文防止恶意用户进行窥探。例如，英特尔的软件保护扩展 (SGX) 等 TEE 技术隔离了代码执行、远程证明、安全配置、数据的安全存储以及用于执行代码的可信路径。在 TEE 中运行的应用程序受到安全保护，几乎不可能被第三方访问。

[51] 以 Intel SGX 技术为例，SGX 提供了围圈 (enclave，也称为飞地)，即内存中一个加密的可信执行区域，由 CPU 保护数据不被窃取。以服务端采用支持 SGX 的 CPU 为例，利用新增的处理器指令，在内存中可以分配一部分区域 EPC (Enclave Page Cache，围圈页面缓存或飞地页面缓存)，通过 CPU 内的加密引擎 MEE (Memory Encryption Engine) 对其中的数据进行加密。EPC 加密的内容只有进入 CPU 后才会被解密成明文。因此，在 SGX 中，用户可以不信任操作系统、VMM (Virtual Machine Monitor，虚拟机监控器)、甚至 BIOS (Basic Input Output System，基本输入输出系统)，只需要信任 CPU 便能确保代码的执行。

[52] 在本说明书实施例中，通过在可信执行环境中执行公开的代码以进行用户私钥加密，从而可以获取得到的包含用户数字签名的第二数据记录，该第二数据记录的真实性和可信执行环境的硬件提供方所保障。

[53] S205，应用服务端，发送所述第二数据记录至数据库服务端。

[54] S207，数据库服务端，接收所述第二数据记录，确定所述第二数据记录的哈希值。

[55] S209, 数据库服务端, 当达到预设的成块条件时, 确定待写入数据块中的各第二数据记录, 生成包含数据块的哈希值和各第二数据记录的第 N 个数据块, 。

[56] 所述预设的成块条件包括: 待存储的第二数据记录数量达到数量阈值, 例如, 每接收到一千条第二数据记录时, 生成一个新数据块, 将一千条第二数据记录写入块中;

5 或者, 距离上一次成块时刻的时间间隔达到时间阈值, 例如, 每隔 5 分钟, 生成一个新数据块, 将在这 5 分钟内接收到的第二数据记录写入块中。

[57] 此处的 N 指的是数据块的序号, 换言之, 在本说明书实施例中, 数据块是以块链的形式, 基于成块时间的顺序先后排列, 具有很强的时序特征。其中, 数据块的块高基于成块时间的先后顺序单调递增。块高可以是序号, 此时第 N 个数据块的块高即为 N;

10 块高也可以其它方式生成。

[58] 当 $N=1$ 时, 即此时的数据块为初始数据块。初始数据块的哈希值和块高基于预设方式给定。例如, 初始数据块中不包含第二数据记录, 哈希值则为任一给定的哈希值, 块高 $blknum=0$; 又例如, 初始数据块的生成触发条件与其它数据块的触发条件一致, 但是初始数据块的哈希值由对初始数据块中的所有内容取哈希确定。

15 [59] 当 $N>1$ 时, 由于前一数据块的内容和哈希值已经确定, 则此时, 可以基于前一数据块 (即第 $N-1$ 个数据块) 的哈希值生成当前数据块 (第 N 个数据块) 的哈希值, 例如, 一种可行的方式为, 确定每一条将要写入第 N 个块中的第二数据记录的哈希值, 按照在块中的排列顺序, 生成一个默克尔树, 将默克尔树的根哈希值和前一数据块的哈希值拼接在一起, 再次采用哈希算法, 生成当前块的哈希值, 以及还可以根据默克尔树的根哈希值和其它一些元数据 (例如版本号、数据块的生成时间戳等等) 生成当前快的哈希值。又例如, 还可以按照块中第二数据记录的顺序进行拼接并取哈希得到整体第二数据记录的哈希值, 拼接前一数据块的哈希值和整体第二数据记录的哈希值, 并对拼接得到的字串进行哈希运算, 生成数据块的哈希值。

25 [60] 通过前述的数据块的生成方式, 每一个数据块通过哈希值确定, 数据块的哈希值由数据块中的第二数据记录的内容、顺序以及前一数据块的哈希值决定。用户可以随时基于数据块的哈希值或者第二数据记录的哈希值发起验证, 对于数据块中任何内容 (包括对于数据块中第二数据记录内容或者顺序的修改) 的修改都会造成在验证时计算得到的数据块的哈希值和数据块生成时的哈希值不一致, 而导致验证失败, 从而实现了中心化下的不可篡改。

[61] 在本说明书实施例中，数据块的格式是可以自定义的。在一种实施例中，数据块的格式可以是类似于区块链中的区块格式。在每一个数据块中，其包含用于存储元数据的块头，和，用于存储第二数据记录的块体。数据块中的块头可以用于存储诸如父哈希、自身的块哈希值、版本号、数据记录的默克尔树的根哈希、时间戳等等。

5 [62] 通过本说明书实施例所提供的方案，应用服务端将用户数据在可信执行环境中进行数字签名，生成包含用户数字签名的第二数据记录，将第二数据记录存储在中心化的块链式账本中，数字签名保障了数据确实由该用户所产生，而中心化的块链式账本存储实现了对于包含用户数字签名的数据的不可篡改，通过前述方案保障了用户存储数据安全性，提高用户体验。

10 [63] 在一种实施例中，数据库服务端还可以在存储第二数据记录前对第二数据记录进行验证。即根据用户标识确定对应的公钥。在数字签名过程中，对应的公钥是公开可见的，任一用户或者机构都可以知晓一名用户所对应的公钥，因而，根据用户标识即可得到对应的公钥，并对第二数据记录进行验证。

15 [64] 验证如果通过，再将数据记录写入数据块；否则，不写入，并且还可以返回相应的通知消息至应用服务端。对于数字签名的具体验证方式在当前也很常规，此处不再赘述。

[65] 在一种实施例中，数据库服务端还可以返回对于第二数据记录的哈希值至应用服务端，应用服务端转发第二数据记录的哈希值至所述用户标识所对应的第一客户端。从而第一客户端可以随时根据该哈希值查询得到相应的第二数据记录，并且可以验证该第二数据记录中的私钥的正确性。或者，可以随时根据该哈希值对第二数据记录所处的账本进行完整性验证，具体的完整性验证方式在前文已经详述。

20

[66] 在一种实施例中，若多个不同的客户端之间有可能需要共享数据。例如，在一种共享学习的平台中，不同的客户端可以分别将自己的数据作为训练样本输入到同一的学习平台（即应用服务端）中，学习平台可以对客户端的数据进行的模型训练。

25 [67] 同时，任一客户端均可以对平台得到的训练模型进行相应的操作（例如，更新，再次训练等等），以及，一个客户端可能还需要使用到其它客户端的数据进行自身相关的模型训练。在这种情形下，一名客户端有动机去查询验证其它客户端所提供的数据以及其它客户端在使用过程中所产生的数据等等。

[68] 此时，第一客户端或者应用服务端可以将第一客户端操作所产生的第二数据记录

的哈希值进行公开，其它客户端可以发送该哈希值至应用服务端进行相应的查询。

[69] 进而，应用服务端，可以接收第二客户端所发送的包含第二数据记录的哈希值的查询请求，并转发所述查询请求至数据库服务端；数据库服务端，根据所述第二数据记录的哈希值查询得到对应的第二数据记录，并返回所述数据记录至应用服务端；应用服务端转发所述查询得到的第二数据记录至所述第二客户端，第二客户端则可以采用第一客户端的公钥对所述第二数据记录进行解密验证。

[70] 通过这种方式，在这类多客户端共享数据的情形下，任一客户端均可以对其它客户端所产生的数据进行合法性验证，确认其它任一用户所提供或者所产生的数据是可靠合法的，达到共同公开监督，进一步保障用户存储数据安全性，提高用户体验。

[71] 对应的，本说明书实施例还提供一种数据存储系统，包括应用服务端和数据库服务端，在所述系统中，

[72] 应用服务端，获取携带用户标识的第一数据记录；根据用户标识获取对应的用户私钥，在可信执行环境中执行预设的签名代码，生成包含用户数字签名的第二数据记录，其中，所述签名代码用于根据用户私钥对所述第一数据记录进行数字签名；发送所述第二数据记录至数据库服务端；

[73] 数据库服务端，接收所述第二数据记录，确定所述第二数据记录的哈希值；

[74] 当达到预设的成块条件时，确定待写入数据块中的各第二数据记录，生成包含数据块的哈希值和各第二数据记录的第 N 个数据块，具体包括：

[75] 当 $N=1$ 时，初始数据块的哈希值和块高基于预设方式给定；

[76] 当 $N>1$ 时，根据待写入数据块中的第二数据记录和第 $N-1$ 个数据块的哈希值确定第 N 个数据块的哈希值，生成包含第 N 个数据块的哈希值和各第二数据记录的第 N 个数据块，其中，数据块的块高基于成块时间的先后顺序单调递增。

[77] 进一步地，在所述系统中，数据库服务端还用于，根据用户标识确定对应的用户公钥，采用所述用户公钥对第二数据记录进行验证。

[78] 进一步地，在所述系统中，在数据库服务端中，所述预设的成块条件包括：待存储的数据记录数量达到数量阈值；或者，距离上一次成块时刻的时间间隔达到时间阈值。

[79] 进一步地，在所述系统中，数据库服务端返回所述第二数据记录的哈希值至应用服务端；应用服务端转发第二数据记录的哈希值至所述第一客户端。

[80] 进一步地，在所述系统中，应用服务端还用于，接收第二客户端所发送的包含第二数据记录的哈希值的查询请求，并转发所述查询请求至数据库服务端；

[81] 相应的，数据库服务端还用于，根据所述第二数据记录的哈希值查询得到对应的第二数据记录，并返回所述数据记录至应用服务端；应用服务端转发所述查询得到的第二数据记录至所述第二客户端，以便所述第二客户端采用第一客户端的公钥对所述第二数据记录进行解密验证。

[82] 进一步地，在所述系统中，所述可信执行环境包括 Intel SGX 或 AMD SEV 或 ARM Trustzone。

[83] 在另一方面，本说明书实施例还提供一种数据存储方法，应用于应用服务端中，如图 3 所示，图 3 为本说明书实施例所提供的应用服务端方面的数据存储方法的流程图，所述方法包括：

[84] S301，获取携带用户标识的第一数据记录；

[85] S303，根据用户标识获取对应的用户私钥，在可信执行环境中执行预设的签名代码，生成包含用户数字签名的第二数据记录，其中，所述签名代码用于根据用户私钥对所述第一数据记录进行数字签名；

[86] S305，发送所述第二数据记录至数据库服务端。

[87] 对应的，本说明书实施例还提供一种数据存储装置，应用于应用服务端中，如图 4 所示，图 4 是本说明书实施例提供的一种数据存储装置的结构示意图，包括：

[88] 接收模块 401，获取携带用户标识的第一数据记录；

[89] 生成模块 403，根据用户标识获取对应的用户私钥，在可信执行环境中执行预设的签名代码，生成包含用户数字签名的第二数据记录，其中，所述签名代码用于根据用户私钥对所述第一数据记录进行数字签名；

[90] 发送模块 405，发送所述第二数据记录至数据库服务端。

[91] 本说明书实施例还提供一种计算机设备，其至少包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其中，处理器执行所述程序时实现图 3 所示的数据存储方法。

[92] 图 5 示出了本说明书实施例所提供的一种更为具体的计算设备硬件结构示意图，该设备可以包括：处理器 1010、存储器 1020、输入/输出接口 1030、通信接口 1040 和

总线 1050。其中处理器 1010、存储器 1020、输入/输出接口 1030 和通信接口 1040 通过总线 1050 实现彼此之间在设备内部的通信连接。

[93] 处理器 1010 可以采用通用的 CPU（Central Processing Unit，中央处理器）、微处理器、应用专用集成电路（Application Specific Integrated Circuit，ASIC）、或者一个或多个集成电路等方式实现，用于执行相关程序，以实现本说明书实施例所提供的技术方案。

[94] 存储器 1020 可以采用 ROM（Read Only Memory，只读存储器）、RAM（Random Access Memory，随机存取存储器）、静态存储设备，动态存储设备等形式实现。存储器 1020 可以存储操作系统和其他应用程序，在通过软件或者固件来实现本说明书实施例所提供的技术方案时，相关的程序代码保存在存储器 1020 中，并由处理器 1010 来调用执行。

[95] 输入/输出接口 1030 用于连接输入/输出模块，以实现信息输入及输出。输入输出/模块可以作为组件配置在设备中（图中未示出），也可以外接于设备以提供相应功能。其中输入设备可以包括键盘、鼠标、触摸屏、麦克风、各类传感器等，输出设备可以包括显示器、扬声器、振动器、指示灯等。

[96] 通信接口 1040 用于连接通信模块（图中未示出），以实现本设备与其他设备的通信交互。其中通信模块可以通过有线方式（例如 USB、网线等）实现通信，也可以通过无线方式（例如移动网络、WIFI、蓝牙等）实现通信。

[97] 总线 1050 包括一通路，在设备的各个组件（例如处理器 1010、存储器 1020、输入/输出接口 1030 和通信接口 1040）之间传输信息。

[98] 需要说明的是，尽管上述设备仅示出了处理器 1010、存储器 1020、输入/输出接口 1030、通信接口 1040 以及总线 1050，但是在具体实施过程中，该设备还可以包括实现正常运行所必需的其他组件。此外，本领域的技术人员可以理解的是，上述设备中也可以仅包含实现本说明书实施例方案所必需的组件，而不必包含图中所示的全部组件。

[99] 本说明书实施例还提供一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现图 3 所示的数据存储方法。

[100] 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。

[101] 通过以上的实施方式的描述可知, 本领域的技术人员可以清楚地了解到本说明书实施例可借助软件加必需的通用硬件平台的方式来实现。基于这样的理解, 本说明书实施例的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来, 该计算机软件产品可以存储在存储介质中, 如 ROM/RAM、磁碟、光盘等, 包括若干指令用以使得一台计算机设备 (可以是个人计算机, 服务器, 或者网络设备等) 执行本说明书实施例各个实施例或者实施例的某些部分所述的方法。

[102] 上述实施例阐明的系统、方法、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, 计算机的具体形式可以是个人计算机、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、电子邮件收发设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任意几种设备的组合。

[103] 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, 对于方法实施例而言, 由于其基本相似于方法实施例, 所以描述得比较简单, 相关之处参见方法实施例的部分说明即可。以上所描述的方法实施例仅仅是示意性的, 其中所述作为分离部件说明的模块可以是或者也可以不是物理上分开的, 在实施本说明书实施例方案时可以把各模块的功能在同一个或多个软件和/或硬件中实现。也可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。本领域普通技术人员在不付出创造性劳动的情况下, 即可以理解并实施。

[104] 以上所述仅是本说明书实施例的具体实施方式, 应当指出, 对于本技术领域的普通技术人员来说, 在不脱离本说明书实施例原理的前提下, 还可以做出若干改进和润饰, 这些改进和润饰也应视为本说明书实施例的保护范围。

权利要求书

1、一种数据存储方法，应用于包括应用服务端和数据库服务端的系统中，所述方法包括：

应用服务端，获取携带用户标识的第一数据记录；

5 应用服务端，根据用户标识获取对应的用户私钥，在可信执行环境中执行预设的签名代码，生成包含用户数字签名的第二数据记录，其中，所述签名代码用于根据用户私钥对所述第一数据记录进行数字签名；

应用服务端，发送所述第二数据记录至数据库服务端；

数据库服务端，接收所述第二数据记录，确定所述第二数据记录的哈希值；

10 数据库服务端，当达到预设的成块条件时，确定待写入数据块中的各第二数据记录，生成包含数据块的哈希值和各第二数据记录的第 N 个数据块，具体包括：

当 $N=1$ 时，初始数据块的哈希值和块高基于预设方式给定；

当 $N>1$ 时，根据待写入数据块中的第二数据记录和第 $N-1$ 个数据块的哈希值确定第 N 个数据块的哈希值，生成包含第 N 个数据块的哈希值和各第二数据记录的第 N 个
15 数据块，其中，数据块的块高基于成块时间的先后顺序单调递增。

2、如权利要求 1 所述的方法，数据库服务端，在确定待写入数据块中的各第二数据记录之前，所述方法还包括：

根据用户标识确定对应的用户公钥，采用所述用户公钥对第二数据记录进行验证。

3、如权利要求 1 所述的方法，所述预设的成块条件包括：

20 待存储的第二数据记录数量达到数量阈值；或者，
距离上一次成块时刻的时间间隔达到时间阈值。

4、如权利要求 1 所述的方法，所述方法还包括：

数据库服务端返回所述第二数据记录的哈希值至应用服务端；

应用服务端转发第二数据记录的哈希值至所述用户标识所对应的第一客户端。

25 5、如权利要求 1 所述的方法，所述方法还包括：

应用服务端，接收第二客户端所发送的包含第二数据记录的哈希值的查询请求，并转发所述查询请求至数据库服务端；

数据库服务端，根据所述第二数据记录的哈希值查询得到对应的第二数据记录，并返回所述数据记录至应用服务端；

30 应用服务端转发所述查询得到的第二数据记录至所述第二客户端，以便所述第二客户端采用第一客户端的公钥对所述第二数据记录进行解密验证。

6、如权利要求 1 所述的方法，所述可信执行环境包括 Intel SGX 或 AMD SEV 或 ARM Trustzone。

7、一种数据存储系统，包括应用服务端和数据库服务端，在所述系统中，

应用服务端，获取携带用户标识的第一数据记录；根据用户标识获取对应的用户私钥，在可信执行环境中执行预设的签名代码，生成包含用户数字签名的第二数据记录，其中，所述签名代码用于根据用户私钥对所述第一数据记录进行数字签名；发送所述第二数据记录至数据库服务端；

数据库服务端，接收所述第二数据记录，确定所述第二数据记录的哈希值；

当达到预设的成块条件时，确定待写入数据块中的各第二数据记录，生成包含数据块的哈希值和各第二数据记录的第 N 个数据块，具体包括：

当 $N=1$ 时，初始数据块的哈希值和块高基于预设方式给定；

当 $N>1$ 时，根据待写入数据块中的第二数据记录和第 $N-1$ 个数据块的哈希值确定第 N 个数据块的哈希值，生成包含第 N 个数据块的哈希值和各第二数据记录的第 N 个数据块，其中，数据块的块高基于成块时间的先后顺序单调递增。

8、如权利要求 7 所述的系统，数据库服务端还用于，根据用户标识确定对应的用户公钥，采用所述用户公钥对第二数据记录进行验证。

9、如权利要求 7 所述的系统，在数据库服务端中，所述预设的成块条件包括：

待存储的数据记录数量达到数量阈值；或者，距离上一次成块时刻的时间间隔达到时间阈值。

10、如权利要求 7 所述的系统，

数据库服务端返回所述第二数据记录的哈希值至应用服务端；应用服务端转发第二数据记录的哈希值至所述第一客户端。

11、如权利要求 7 所述的系统，

应用服务端还用于，接收第二客户端所发送的包含第二数据记录的哈希值的查询请求，并转发所述查询请求至数据库服务端；

相应的，数据库服务端还用于，根据所述第二数据记录的哈希值查询得到对应的第二数据记录，并返回所述数据记录至应用服务端；

应用服务端转发所述查询得到的第二数据记录至所述第二客户端，以便所述第二客户端采用第一客户端的公钥对所述第二数据记录进行解密验证。

12、如权利要求 7 所述的系统，所述可信执行环境包括 Intel SGX 或 AMD SEV 或 ARM Trustzone。

13、一种数据存储方法，应用于应用服务端中，所述方法包括：

获取携带用户标识的第一数据记录；

根据用户标识获取对应的用户私钥，在可信执行环境中执行预设的签名代码，生成包含用户数字签名的第二数据记录，其中，所述签名代码用于根据用户私钥对所述第一

5 数据记录进行数字签名；

发送所述第二数据记录至数据库服务端。

14、一种数据存储装置，应用于应用服务端中，所述装置包括：

接收模块，获取携带用户标识的第一数据记录；

生成模块，根据用户标识获取对应的用户私钥，在可信执行环境中执行预设的签名
10 代码，生成包含用户数字签名的第二数据记录，其中，所述签名代码用于根据用户私钥
对所述第一数据记录进行数字签名；

发送模块，发送所述第二数据记录至数据库服务端。

15、一种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的
的计算机程序，其中，所述处理器执行所述程序时实现如权利要求 13 所述的方法。

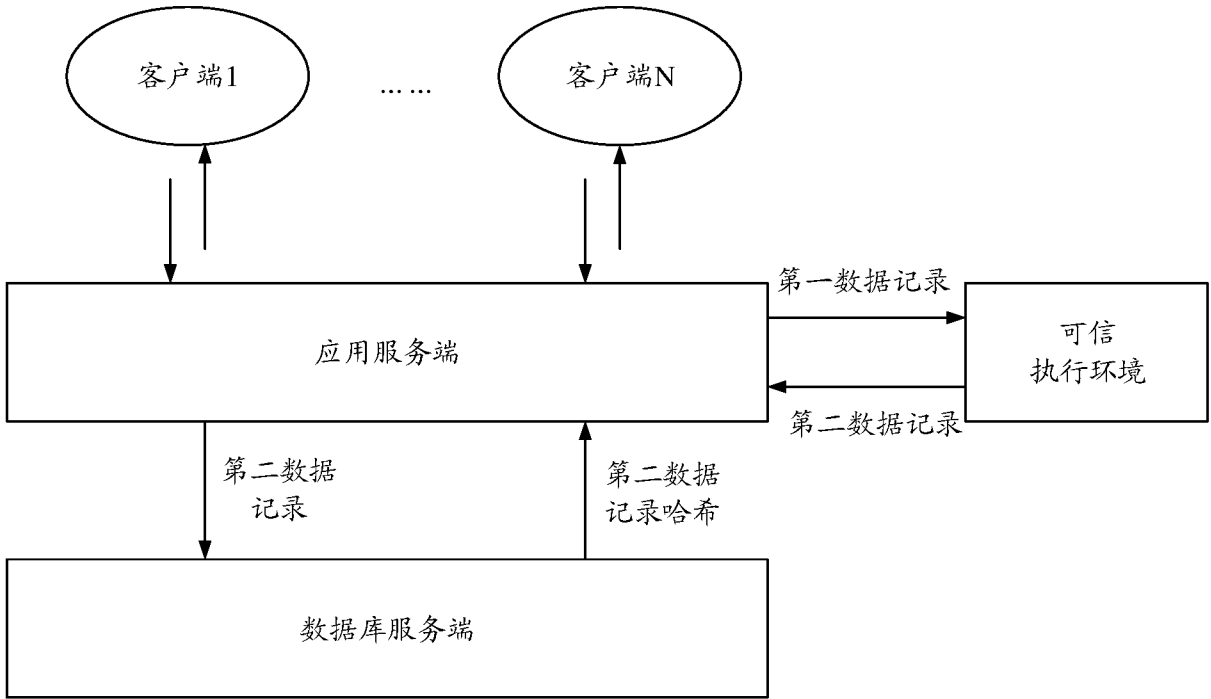


图 1

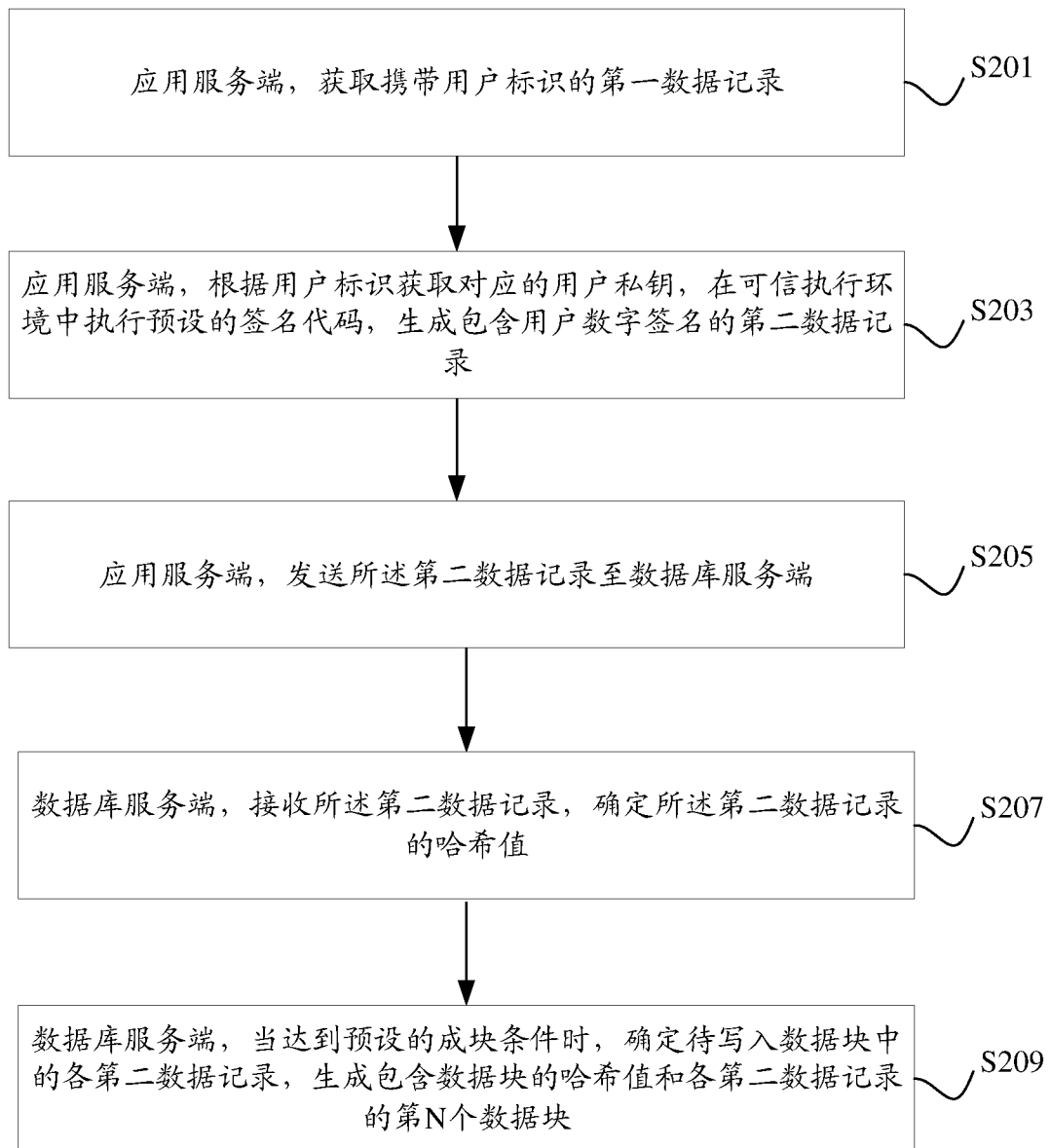


图 2

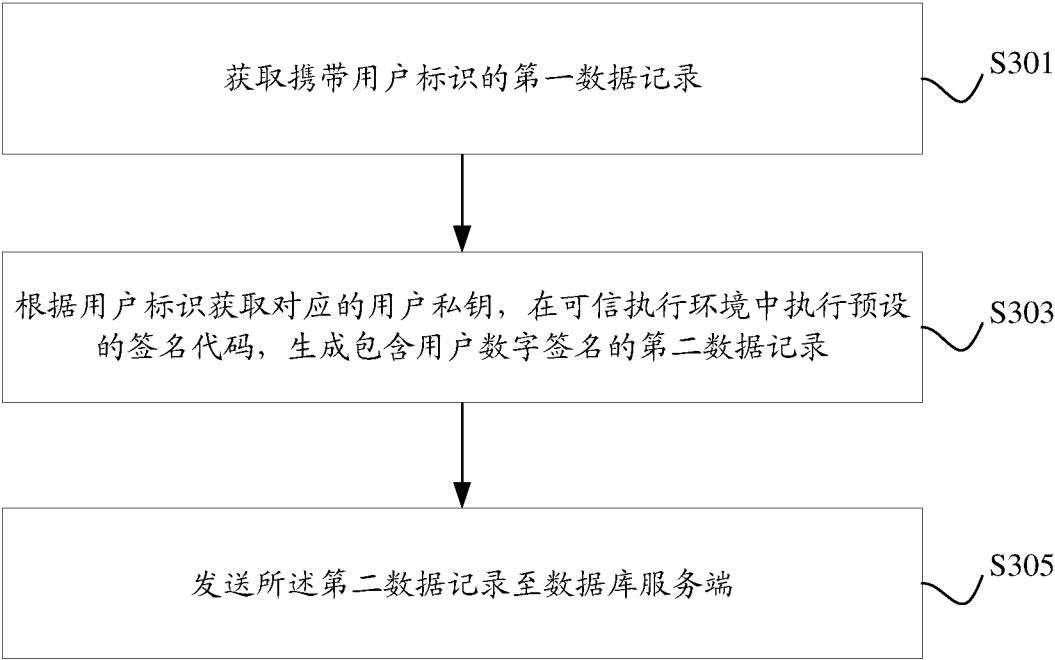


图 3

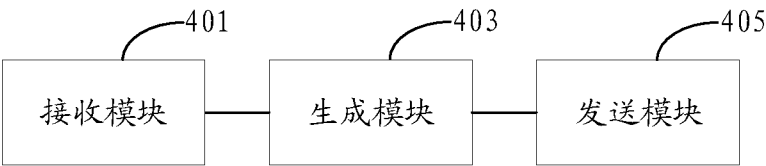


图 4

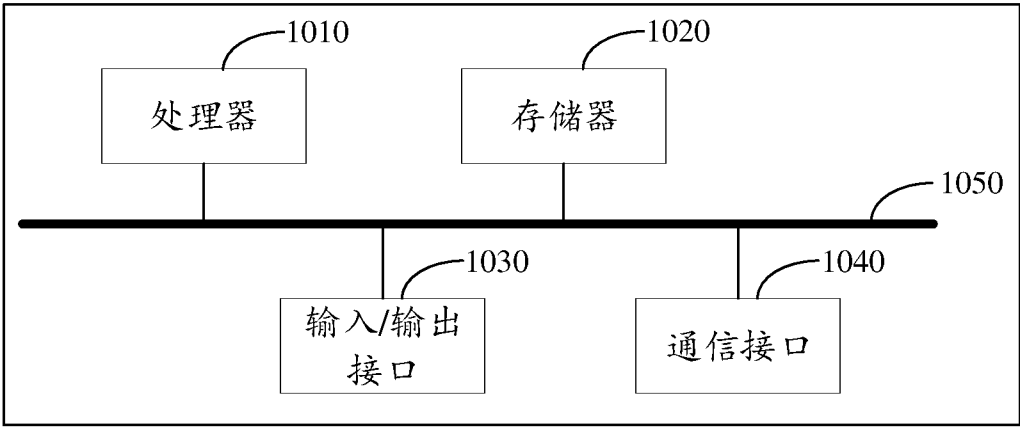


图 5

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2020/071678

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)

WPI, EPODOC, CNPAT, CNKI, IEEE: 数据, 存储, 用户, 标识, 私钥, 密钥, 加密, 签名, 哈希, 块, 查询, 请求, 解密, data, store, user, private key, secret key, encryption, signature, hash, block, query, request, decryption

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110245518 A (ALIBABA GROUP HOLDING LIMITED) 17 September 2019 (2019-09-17) claims 1-15	1-15
Y	CN 109635581 A (SHENZHEN WANGXIN TECHNOLOGY CO., LTD.) 16 April 2019 (2019-04-16) description, paragraphs [0058]-[0141]	1-15
Y	CN 106022154 A (TMAXDATA CO., LTD.) 12 October 2016 (2016-10-12) description, paragraphs [0054]-[0109]	1-15
A	CN 105975870 A (SHANGHAI DIANRONG FINANCIAL INFORMATION SERVICE CO., LTD.) 28 September 2016 (2016-09-28) entire document	1-15
A	CN 103685162 A (CHINA MOBILE COMMUNICATIONS CORPORSTION) 26 March 2014 (2014-03-26) entire document	1-15
A	US 7962765 B2 (RED HAT, INC.) 14 June 2011 (2011-06-14) 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

31 March 2020

Date of mailing of the international search report

13 April 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/CN2020/071678

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	110245518	A	17 September 2019	None			
CN	109635581	A	16 April 2019	None			
CN	106022154	A	12 October 2016	US	2016283749	A1	29 September 2016
				KR	101613146	B1	18 April 2016
CN	105975870	A	28 September 2016	HK	1228537	A0	03 November 2017
CN	103685162	A	26 March 2014	None			
US	7962765	B2	14 June 2011	None			

国际检索报告

国际申请号

PCT/CN2020/071678

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))

WPI, EPDOC, CNPAT, CNKI, IEEE: 数据, 存储, 用户, 标识, 私钥, 密钥, 加密, 签名, 哈希, 块, 查询, 请求, 解密, data, store, user, private key, secret key, encryption, signature, hash, block, query, request, decryption

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 110245518 A (阿里巴巴集团控股有限公司) 2019年 9月 17日 (2019 - 09 - 17) 权利要求1-15	1-15
Y	CN 109635581 A (深圳市网心科技有限公司) 2019年 4月 16日 (2019 - 04 - 16) 说明书第0058-0141段	1-15
Y	CN 106022154 A (株式会社特迈数据) 2016年 10月 12日 (2016 - 10 - 12) 说明书第0054-0109段	1-15
A	CN 105975870 A (上海点荣金融信息服务有限公司) 2016年 9月 28日 (2016 - 09 - 28) 全文	1-15
A	CN 103685162 A (中国移动通信集团公司) 2014年 3月 26日 (2014 - 03 - 26) 全文	1-15
A	US 7962765 B2 (RED HAT, INC.) 2011年 6月 14日 (2011 - 06 - 14) 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

2020年 3月 31日

国际检索报告邮寄日期

2020年 4月 13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

杨庆丽

电话号码 86-(10)-53961433

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2020/071678

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	110245518	A	2019年 9月 17日	无			
CN	109635581	A	2019年 4月 16日	无			
CN	106022154	A	2016年 10月 12日	US	2016283749	A1	2016年 9月 29日
				KR	101613146	B1	2016年 4月 18日
CN	105975870	A	2016年 9月 28日	HK	1228537	A0	2017年 11月 3日
CN	103685162	A	2014年 3月 26日	无			
US	7962765	B2	2011年 6月 14日	无			