(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 12 月 3 日 (03.12.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/238959 A1

(51) 国际专利分类号:
H04L 9/00 (2006.01) *G06Q 20/38* (2012.01)
H04L 9/32 (2006.01) *G06F 21/62* (2013.01)
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2020/092611

(22) 国际申请日: 2020 年 5 月 27 日 (27.05.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910471633.3 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: 刘琦 (**LIU, Qi**); 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)。 闫莺 (**YAN, Ying**); 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)。 魏长征 (**WEI, Changzheng**); 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)。

(54) **Title:** METHOD AND DEVICE FOR REALIZING DYNAMIC ENCRYPTION BASED ON BLOCK HEIGHT

(54) **发明名称:** 基于区块高度实现动态加密的方法及装置

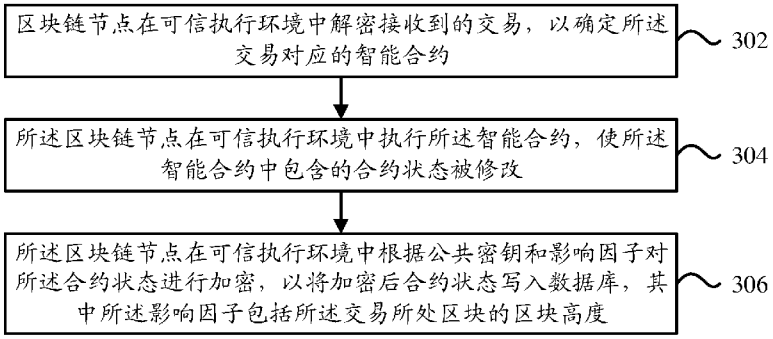

图 3

302 A block chain node decrypts a received transaction in a trusted execution environment to determine a smart contract corresponding to the transaction

304 The block chain node executes the smart contract in the trusted execution environment, so that a contract state contained in the smart contract is modified

306 The block chain node encrypts the contract state in the trusted execution environment according to a public key and an influence factor to write the encrypted contract state into a database, wherein the influence factor comprises the block height of the block where the transaction is located

(57) **Abstract:** One or more embodiments of the present description provide a method and device for realizing dynamic encryption based on a block height. The method can comprise: a block chain node decrypts a received transaction in a trusted execution environment to determine a smart contract corresponding to the transaction; the block chain node executes the smart contract in the trusted execution environment, so that a contract state contained in the smart contract is modified; the block chain node encrypts the contract state in the trusted execution environment according to a public key and an influence factor to write the encrypted contract state into a database, wherein the influence factor comprises the block height of the block where the transaction is located.

WO 2020/238959 A1

[见续页]

(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))。

(57) 摘要：本说明书一个或多个实施例提供一种基于区块高度实现动态加密的方法及装置，该方法可以包括：区块链节点在可信执行环境中解密接收到的交易，以确定所述交易对应的智能合约；所述区块链节点在可信执行环境中执行所述智能合约，使所述智能合约中包含的合约状态被修改；所述区块链节点在可信执行环境中根据公共密钥和影响因子对所述合约状态进行加密，以将加密后合约状态写入数据库，其中所述影响因子包括所述交易所处区块的区块高度。

基于区块高度实现动态加密的方法及装置

技术领域

[01]本说明书一个或多个实施例涉及区块链技术领域，尤其涉及一种基于区块高度实现动态加密的方法及装置。

背景技术

[02]区块链技术构建在传输网络（例如点对点网络）之上。传输网络中的网络节点利用链式数据结构来验证与存储数据，并采用分布式节点共识算法来生成和更新数据。这些区块链网络中的节点有时需要增加。

[03]目前企业级的区块链平台技术上最大的两个挑战就是隐私和性能，往往这两个挑战很难同时解决。大多解决方案都是通过损失性能换取隐私，或者不大考虑隐私去追求性能。常见的解决隐私问题的加密技术，如同态加密(Homomorphic encryption)和零知识证明(Zero-knowledge proof)等复杂度高，通用性差，而且还可能带来严重的性能损失。

[04]在解决隐私方面，可信执行环境（Trusted Execution Environment, TEE）是另一种解决方式。TEE 可以起到硬件中的黑箱作用，在 TEE 中执行的代码和数据都无法被操作系统层偷窥，只有通过代码中预先定义的接口才能对其进行操作。在效率方面，由于 TEE 的黑箱性质，在 TEE 中进行运算的是明文数据，而不是同态加密中的复杂密码学运算，计算过程没有效率损失，因此与 TEE 相结合可以在性能损失较小的前提下很大程度上提升区块链的安全性和隐私性。目前工业界十分关注 TEE 的方案，几乎所有主流的芯片和软件联盟都有自己的 TEE 解决方案，包括软件方面的 TPM（Trusted Platform Module，可信赖平台模块）以及硬件方面的 Intel SGX（Software Guard Extensions, 软件保护扩展）、ARM Trustzone（信任区）和 AMD PSP（Platform Security Processor，平台安全处理器）。

发明内容

[05]有鉴于此，本说明书一个或多个实施例提供一种基于区块高度实现动态加密的方法及装置。

[06]为实现上述目的，本说明书一个或多个实施例提供技术方案如下：

[07]根据本说明书一个或多个实施例的第一方面，提出了一种基于区块高度实现动态加密的方法，包括:

[08]区块链节点在可信执行环境中解密接收到的交易，以确定所述交易对应的智能合约;

[09]所述区块链节点在可信执行环境中执行所述智能合约，使所述智能合约中包含的合约状态被修改;

[10]所述区块链节点在可信执行环境中根据公共密钥和影响因子对所述合约状态进行加密，以将加密后合约状态写入数据库，其中所述影响因子包括所述交易所处区块的区块高度。

[11]根据本说明书一个或多个实施例的第二方面，提出了一种基于区块高度实现动态加密的装置，包括:

[12]解密单元，在可信执行环境中解密接收到的交易，以确定所述交易对应的智能合约;

[13]执行单元，在可信执行环境中执行所述智能合约，使所述智能合约中包含的合约状态被修改;

[14]加密单元，在可信执行环境中根据公共密钥和影响因子对所述合约状态进行加密，其中所述影响因子包括所述交易所处区块的区块高度;

[15]存储单元，用于将加密后合约状态写入数据库。

[16]根据本说明书一个或多个实施例的第三方面，提出了一种电子设备，包括:

[17]处理器;

[18]用于存储处理器可执行指令的存储器;

[19]其中，所述处理器通过运行所述可执行指令以实现如第一方面所述的方法。

[20]根据本说明书一个或多个实施例的第四方面，提出了一种计算机可读存储介质，其上存储有计算机指令，该指令被处理器执行时实现如第一方面所述方法的步骤。

附图说明

[21]图 1 是一示例性实施例提供的一种创建智能合约的示意图。

[22]图 2 是一示例性实施例提供的一种调用智能合约的示意图。

[23]图 3 是一示例性实施例提供的一种基于区块高度实现动态加密的方法的流程图。

[24]图 4 是一示例性实施例提供的一种影响因子仅包含区块高度时的加密示意图。

[25]图 5 是一示例性实施例提供的一种影响因子同时包含区块高度与交易偏移量时的加密示意图。

[26]图 6 是一示例性实施例提供的一种影响因子同时包含区块高度与合约状态的被修改次序时的加密示意图。

[27]图 7 是一示例性实施例提供的一种影响因子同时包含区块高度、交易偏移量与合约状态的被修改次序时的加密示意图。

[28]图 8 是一示例性实施例提供的一种合约状态的键值对的结构示意图。

[29]图 9 是一示例性实施例提供的另一种合约状态的键值对的结构示意图。

[30]图 10 是一示例性实施例提供的一种设备的结构示意图。

[31]图 11 是一示例性实施例提供的一种基于区块高度实现动态加密的装置的框图。

具体实施方式

[32]这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本说明书一个或多个实施例相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本说明书一个或多个实施例的一些方面相一致的装置和方法的例子。

[33]需要说明的是：在其他实施例中并不一定按照本说明书示出和描述的顺序来执行相应方法的步骤。在一些其他实施例中，其方法所包括的步骤可以比本说明书所描述的更多或更少。此外，本说明书中所描述的单个步骤，在其他实施例中可能被分解为多个步骤进行描述；而本说明书中所描述的多个步骤，在其他实施例中也可能被合并为单个步骤进行描述。

[34]区块链一般被划分为三种类型：公有链（Public Blockchain），私有链（Private Blockchain）和联盟链（Consortium Blockchain）。此外，还有多种类型的结合，比如私有链+联盟链、联盟链+公有链等不同组合形式。区块链的参与者即区块链节点（或简称节点），区块链节点可以读取链上的数据记录、参与交易以及竞争新区块的记账权等，

各个区块链节点组成了相应的区块链网络。在上述类型的区块链中，去中心化程度最高的是公有链。公有链以比特币、以太坊为代表，加入公有链的参与者可以读取链上的数据记录、参与交易以及竞争新区块的记账权等，且各参与者可自由加入以及退出网络。私有链则相反，相关网络的写入权限由某个组织或者机构控制，数据读取权限受组织或机构的规定。简单来说，私有链可以为一个弱中心化系统，参与者具有严格限制且少。这种类型的区块链更适合于特定机构内部使用。联盟链则是介于公有链以及私有链之间的区块链，可实现“部分去中心化”。联盟链中各个节点通常有与之相对应的实体机构或者组织；参与者通过授权加入网络并组成利益相关联盟，共同维护区块链运行。

[35]不论是公有链、私有链还是联盟链，都可能提供智能合约的功能。区块链上的智能合约是在区块链系统上可以被交易触发执行的合约。智能合约可以通过代码的形式定义。

[36]以以太坊为例，支持用户在以太坊网络中创建并调用一些复杂的逻辑，这是以太坊区别于比特币区块链技术的最大挑战。以太坊作为一个可编程区块链的核心是以太坊虚拟机（EVM），每个以太坊节点都可以运行EVM。EVM是一个图灵完备的虚拟机，这意味着可以通过它实现各种复杂的逻辑。用户在以太坊中发布和调用智能合约就是在EVM上运行的。实际上，虚拟机直接运行的是虚拟机代码（虚拟机字节码，下简称“字节码”）。部署在区块链上的智能合约可以是字节码的形式。

[37]例如图1所示，Bob将一个包含创建智能合约信息的交易发送到以太坊网络后，节点1的EVM可以执行这个交易并生成对应的合约实例。图中1中的“0x6f8ae93...”代表了这个合约的地址，交易的data字段保存的可以是字节码，交易的to字段为空。节点间通过共识机制达成一致后，这个合约成功创建，并且可以在后续过程中被调用。合约创建后，区块链上出现一个与该智能合约对应的合约账户，并拥有一个特定的地址，合约代码将保存在该合约账户中。智能合约的行为由合约代码控制。换句话说，智能合约使得区块链上产生包含合约代码和账户存储（Storage）的虚拟账户。

[38]如图2所示，仍以以太坊为例，Bob将一个用于调用智能合约的交易发送到以太坊网络后，某一节点的EVM可以执行这个交易并生成对应的合约实例。图中2中交易的from字段是交易发起方（即Bob）的账户的地址，to字段中的“0x6f8ae93...”代表了被调用的智能合约的地址，value字段在以太坊中是以太币的值，交易的data字段保存的调用智能合约的方法和参数。智能合约以规定的方式在区块链网络中每个节点独立的执行，所有执行记录和数据都保存在区块链上，所以当交易完成后，区块链上就保存了

无法篡改、不会丢失的交易凭证。

[39]如前所述，部署在区块链上的智能合约可以是字节码的形式。字节码由一连串的字节组成，每一字节可以标识一个操作。基于开发效率、可读性等多方面考虑，开发者可以不直接书写字节码，而是选择一门高级语言编写智能合约代码。高级语言编写的智能合约代码，经过编译器编译，生成字节码，进而该字节码可以部署到区块链上。以太坊支持的高级语言很多，如 Solidity、Serpent、LLL 语言等。

[40]以 Solidity 语言为例，用其编写的合约与面向对象编程语言中的类（Class）很相似，在一个合约中可以声明多种成员，包括合约状态、函数、函数修改器、事件等。合约状态是永久存储在智能合约的账户存储中的值，用于保存合约的状态。

[41]如下是以 Solidity 语言编写的一个简单的智能合约的代码示例:

```
Contract Example{
  int balance;
  function C( ){
      balance + = 1;
  }
 function getbalance( ) returns(int){
  return balance ;
 }
  }
```

[42]一般的，这个合约部署在区块链后，“balance”这个合约状态对应的存储状态是明文，任何人都可以看到其状态，无隐私保护的设置和能力。如果用户想将状态隐私保护起来，目前采用零知识证明、同态加密的解决方案，需要重新改写这个合约，使得“balance”这个合约状态加密保护起来，且需要支持 balance 在加密域上的所有运算。一般这种加密方式运算复杂，而且很难设计适合的算法在加密域上予以支持。而在有些区块链与 TEE 相结合的解决方案中，为了实现隐私保护，智能合约的部分或全部合约状态被当作需要隐私保护的数据存储在区块链节点维护的数据库中。所述数据库，其物理载体可以是存储介质，例如持久性存储介质。

[43]TEE 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。而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。

[44]同时，仅仅是安全的资源隔离也可能无法满足安全需求，使得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。

[45]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。以某一区块链节点采用支持 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 中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 便能确保隐私数据不会泄漏。因此，在 CPU 的加密保护下，可以在围圈内执行智能合约、生成合约状态，并对围圈内需要隐私保护的合约状态进行加密，然后将得到的密文合约状态传出后存储，从而既可以利用 CPU 强大的计算力，又不用担心数据泄漏。

[46]图 3 是一示例性实施例提供的一种区块链中实现动态加密的方法的流程图。如图 3 所示，该方法应用于区块链节点，可以包括以下步骤：

[47]步骤 302，区块链节点在可信执行环境中解密接收到的交易，以确定所述交易对应的智能合约。

[48]在一实施例中，客户端可以创建交易，该交易用于创建或调用智能合约。客户端可以通过密钥对该交易进行加密，并将加密后的交易发送至区块链节点，使得区块链节点可以在可信执行环境中对该加密后的交易进行解密，从而确定该交易对应的智能合约。

[49]如前所述，当上述交易用于创建智能合约时，该交易的 data 字段保存有智能合约的代码，使得区块链节点解密该交易后，可以从该交易的 data 字段中读取对应的智能合约。当上述交易用于调用智能合约时，该交易的 to 字段包含被调用的智能合约的地址，使得区块链节点解密该交易后，可以从该交易的 to 字段中读取智能合约的地址，并基于该地址获取相应智能合约的代码。

[50]当交易用于调用智能合约时，可以是多重嵌套结构的调用。例如，交易直接调用智能合约 1，而该智能合约 1 的代码调用了智能合约 2，且智能合约 2 中的代码指向了智能合约 3 的合约地址，使得交易实际上间接调用了智能合约 3 的代码。这样，不论是智能合约 1、智能合约 2 还是智能合约 3 中定义的合约状态被修改时，本说明书均可以对修改后的合约状态进行加密存储。

[51]在一实施例中，客户端对交易的加密方式可以为对称加密、非对称加密，或者对称加密结合非对称加密。当采用对称加密时，客户端通过加密密钥对交易进行加密，而区块链节点通过相同的加密密钥对交易进行解密；相应的，所采用的对称加密算法可以是 DES 算法，3DES 算法，TDEA 算法，Blowfish 算法，RC5 算法，IDEA 算法等。当采用非对称加密时，客户端通过公钥对交易进行加密、区块链节点通过私钥对交易进行解密；相应的，所采用的非对称加密算法，例如是 RSA、Elgamal、背包算法、Rabin、D-H、ECC（椭圆曲线加密算法）等。当采用对称加密结合非对称加密时，客户端可以采用对称加密算法加密交易，即采用对称加密算法的密钥加密交易，并用非对称加密算法加密对称加密算法中采用的密钥，譬如采用非对称加密算法的公钥加密对称加密算法中采用的密钥；这样，区块链节点接收到加密的交易后，可以先采用非对称加密算法的私钥进行解密，得到对称加密算法的密钥，进而用对称加密算法的密钥解密上述交易。

[52]步骤 304，所述区块链节点在可信执行环境中执行所述智能合约，使所述智能合约中包含的合约状态被修改。

[53]如前所述，区块链节点可以通过在 TEE 中执行智能合约，以确保合约状态及其取值

不会发生泄漏。例如，经过前述的解密过程后，区块链节点可以获得交易对应的智能合约的明文代码，并在 TEE 中执行所获得的明文代码。具体的，区块链节点可以利用 CPU 中新增的处理器指令，在内存中可以分配一部分区域 EPC，通过 CPU 内的加密引擎 MEE 对上述明文代码进行加密存入所述 EPC 中。EPC 中加密的内容进入 CPU 后被解密成明文，即上述的明文代码，使得 CPU 可以对该明文代码进行运算，完成执行过程。

[54]在 SGX 技术中，可以将 EVM 加载进上述的围圈中，使得 EVM 可以在围圈内执行上述的明文代码，从而充分利用 CPU 的强大算力。在远程证明过程中，密钥管理服务器可以计算本地 EVM 代码的 hash 值，并与区块链节点中加载的 EVM 代码的 hash 值比对，比对结果正确作为通过远程证明的一个必要条件，从而完成对区块链节点 SGX 围圈加载的代码的度量。经过度量，正确的 EVM 可以在 SGX 中执行交易对应的智能合约的明文代码，并且确保所有正确 EVM 在执行同一段代码后的结果相同。

[55]一般的，CPU 执行智能合约的明文代码后，该明文代码中定义的部分或全部合约状态会发生变化，即部分或全部合约状态被修改，本说明书可以针对这些被修改的合约状态进行可靠加密后，存储至区块链节点维护的数据库中，以实现高级别的数据安全与隐私保护。

[56]步骤 306，所述区块链节点在可信执行环境中根据公共密钥和影响因子对所述合约状态进行加密，以将加密后合约状态写入数据库，其中所述影响因子包括所述交易所处区块的区块高度。

[57]在一实施例中，将合约状态存入区块链，从区块链节点的角度，是将该合约状态写入数据库，例如本地的数据库。所述数据库，一般存储于存储介质之中，更多见的是持久性存储介质。所述持久性存储介质，可以是磁盘、软盘，也可以是通电后可恢复数据从而可以持久存储的内存之类。

[58]在一实施例中，区块链节点可以根据公共密钥和影响因子对合约状态进行加密，使得到的加密后合约状态的取值同时受到公共密钥和影响因子的作用，在公共密钥相同的情况下，可以通过差异化的影响因子来增加加密后合约状态的随机性。换言之，当公共密钥相同的情况下，通过采用不同的影响因子，即便针对相同取值的合约状态进行加密，所得到的加密后合约状态也将具有不同取值。因此，相比于对所有合约状态均采用公共密钥进行加密，可以避免不法分子掌握加密后合约状态的取值变化规律，防止不法分子通过尝试和比对而推测出合约状态的取值，具有更高的安全性。

[59]在一实施例中，影响因子可以仅包含上述交易所处区块的区块高度。因此，对于不同区块的交易被执行后被修改的合约状态，区块链节点将采用不同取值的影响因子。那么，当区块链节点根据公共密钥和影响因子对合约状态进行加密时，即便加密前的合约状态具有相同取值，由于作为影响因子的区块高度不同，也会使得加密后合约状态完全不同，从而增加了加密后合约状态的取值随机性。可见，当影响因子为交易所处区块的区块高度时，可以在区块维度上增加各个加密后合约状态的取值随机性，确保不同区块的交易分别对应的加密后合约状态之间不会产生规律可循的取值变化。

[60]假定在某一区块链网络中包含区块 B1 和区块 B2，区块 B1 的区块高度为 H1、区块 B2 的区块高度为 H2。为了便于理解，假定区块 B1 中包含交易 Tx1、Tx2，区块 B2 中包含交易 Tx3、Tx4，交易 Tx1、Tx3 在区块 B1、B2 中分别对应的位置偏移量均为 Offset1，而交易 Tx2、Tx4 在区块 B1、B2 中分别对应的位置偏移量均为 Offset2；同时，交易 Tx1、Tx3 中均定义了合约状态 Balance1、Balance2，交易 Tx2、Tx4 中均定义了合约状态 Balance3、Balance4。

[61]当影响因子仅包含区块高度时，如图 4 所示：对于区块 B1 中涉及的 Balance1、Balance2、Balance3 和 Balance4 等合约状态，不论各个合约状态是否来自于同一交易或不同交易，均采用公共密钥 Key128（即版本号为 128 的安全密钥，可参见下文关于密钥版本的描述；或者，可以采用其他形式的公共密钥，此处仅用于举例）和区块高度 H1 实施加密操作，从而分别得到相应的加密后合约状态，比如 Balance1 对应的 S-Balance1-1、Balance2 对应的 S-Balance2-1、Balance3 对应的 S-Balance3-1、Balance4 对应的 S-Balance4-1 等。

[62]类似地，对于区块 B2 而言，不论各个合约状态是否来自于同一交易或不同交易，均采用公共密钥 key128 和区块高度 H2 实施加密操作，从而分别得到相应的加密后合约状态，比如 Balance1 对应的 R-Balance1-1、Balance2 对应的 R-Balance2-1、Balance3 对应的 R-Balance3-1、Balance4 对应的 R-Balance4-1 等。

[63]除了“交易所处区块的区块高度”之外，影响因子还可以进一步包含其他条件，比如其他条件可以包括“交易在所处区块中的位置偏移量”、“合约状态在智能合约被执行时的被修改次序”等其中的一个或多个，以得到由多个条件组合而成的影响因子，可以在其他维度上对合约状态实施加密操作。

[64]在一实施例中，影响因子可以为交易所处区块的区块高度、交易在所处区块中的位

置偏移量。结合上文分别对条件“交易所处区块的区块高度”、条件“交易在所处区块中的位置偏移量”的描述，可知：条件“交易所处区块的区块高度”可以实现区块维度的加密控制、确保不同区块之间必然不会使得加密后合约状态产生规律可循的取值变化，条件“交易在所处区块中的位置偏移量”可以实现交易维度的加密控制、确保同一区块内的不同交易之间必然不会使得加密后合约状态产生规律可循的取值变化，那么当影响因子同时包含上述两个条件时，可以实现区块维度和交易维度的加密控制，使得不同交易之间必然不会使得加密后合约状态产生规律可循的取值变化，而不论这些交易是否处于同一区块或不同区块。其中，对于同一区块的不同交易，可以通过条件“交易在所处区块中的位置偏移量”实现加密控制，这是由于同一区块中的不同交易必然具有不同的位置偏移量；而对于不同区块的不同交易，即便这些交易在所处区块分别对应的位置偏移量相同，也可以进一步通过条件“交易所处区块的区块高度”实现加密控制，这是由于不同区块的交易必然具有不同的区块高度。

[65]仍以上述的区块 B1、B2 为例。如图 5 所示，当区块链节点同时考量区块高度与交易对应的位置偏移量时，对于区块 B1 涉及的 Balance1、Balance2、Balance3 和 Balance4 等合约状态，由于 Balance1 与 Balance2 来自于交易 Tx1、该交易 Tx1 对应的位置偏移量为 Offset1，因而通过公共密钥 Key128、区块高度 H1 与位置偏移量 Offset1 对 Balance1 与 Balance2 进行分别加密，比如对 Balance1 进行加密后得到 S-Balance1-2、对 Balance2 进行加密后得到 S-Balance2-2。同时，由于 Balance3 与 Balance4 来自于交易 Tx2、该交易 Tx2 对应的位置偏移量为 Offset2，因而通过公共密钥 Key128、区块高度 H1 与位置偏移量 Offset2 对 Balance3 与 Balance4 进行分别加密，比如对 Balance3 进行加密后得到 S-Balance3-2、对 Balance4 进行加密后得到 S-Balance4-2。

[66]类似地，对于区块 B2 而言，由于 Balance1 与 Balance2 来自于交易 Tx3、该交易 Tx3 对应的位置偏移量为 Offset1，因而通过公共密钥 Key128、区块高度 H2 与位置偏移量 Offset1 对 Balance1 与 Balance2 进行分别加密，比如对 Balance1 进行加密后得到 R-Balance1-2、对 Balance2 进行加密后得到 R-Balance2-2。同时，由于 Balance3 与 Balance4 来自于交易 Tx4、该交易 Tx4 对应的位置偏移量为 Offset2，因而通过公共密钥 Key128、区块高度 H2 与位置偏移量 Offset2 对 Balance3 与 Balance4 进行分别加密，比如对 Balance3 进行加密后得到 R-Balance3-2、对 Balance4 进行加密后得到 R-Balance4-2。

[67]在一实施例中，影响因子可以为交易所处区块的区块高度、合约状态在智能合约被执行时的被修改次序。结合上文分别对条件“交易所处区块的区块高度”、条件“合约

状态在智能合约被执行时的被修改次序”的描述，可知：条件“交易所处区块的区块高度”可以实现区块维度的加密控制、确保不同区块之间必然不会使得加密后合约状态产生规律可循的取值变化，条件“合约状态在智能合约被执行时的被修改次序”可以实现状态维度的加密控制、确保同一交易产生的不同合约状态之间必然不会使得加密后合约状态产生规律可循的取值变化，那么当影响因子同时包含上述两个条件时，可以实现区块维度和状态维度的加密控制，使得不同区块上的多个交易分别产生的合约状态之间即便具有相同的被修改次序，也必然不会使得加密后合约状态产生规律可循的取值变化。其中，对于同一交易产生的多个合约状态，可以通过条件“合约状态在智能合约被执行时的被修改次序”实现加密控制，这是由于同一交易产生的不同合约状态必然具有不同的被修改次序；而对于不同区块的多个交易分别产生的合约状态，即便这些合约状态在各自的交易中具有相同的被修改次数，也可以进一步通过条件“交易所处区块的区块高度”实现加密控制，这是由于不同区块的交易必然具有不同的区块高度。

[68]仍以上述的区块 B1、B2 为例。如图 6 所示，当区块链节点同时考量区块高度与合约状态的被修改次序时，对于区块 B1 涉及的 Balance1、Balance2、Balance3 和 Balance4 等合约状态，由于 Balance1 与 Balance2 来自于同一交易 Tx1，使得 Balance1 与 Balance2 必然分别对应于不同的被修改次序，譬如 Balance1 对应于被修改次序 U1、Balance2 对应于被修改次序 U2，因而通过公共密钥 Key128、区块高度 H1 与被修改次序 U1 对 Balance1 进行加密，得到加密后的 S-Balance1-3，而通过公共密钥 Key128、区块高度 H1 与被修改次序 U2 对 Balance2 进行加密，得到加密后的 S-Balance2-3。同时，由于 Balance3 与 Balance4 来自于同一交易 Tx2，使得 Balance3 与 Balance4 必然分别对应于不同的被修改次序，譬如 Balance3 对应于被修改次序 U1、Balance4 对应于被修改次序 U2，因而通过公共密钥 Key128、区块高度 H1 与被修改次序 U1 对 Balance3 进行加密，得到加密后的 S-Balance3-3，而通过公共密钥 Key128、区块高度 H1 与被修改次序 U2 对 Balance4 进行加密，得到加密后的 S-Balance4-3。

[69]类似地，对于区块 B2 涉及的 Balance1、Balance2、Balance3 和 Balance4 等合约状态，由于 Balance1 与 Balance2 来自于同一交易 Tx3，使得 Balance1 与 Balance2 必然分别对应于不同的被修改次序，譬如 Balance1 对应于被修改次序 U1、Balance2 对应于被修改次序 U2，因而通过公共密钥 Key128、区块高度 H2 与被修改次序 U1 对 Balance1 进行加密，得到加密后的 R-Balance1-3，而通过公共密钥 Key128、区块高度 H2 与被修改次序 U2 对 Balance2 进行加密，得到加密后的 R-Balance2-3。同时，由于 Balance3 与

Balance4 来自于同一交易 Tx4，使得 Balance3 与 Balance4 必然分别对应于不同的被修改次序，譬如 Balance3 对应于被修改次序 U1、Balance4 对应于被修改次序 U2，因而通过公共密钥 Key128、区块高度 H2 与被修改次序 U1 对 Balance3 进行加密，得到加密后的 R-Balance3-3，而通过公共密钥 Key128、区块高度 H2 与被修改次序 U2 对 Balance4 进行加密，得到加密后的 R-Balance4-3。

[70]在一实施例中，影响因子可以为“交易所处区块的区块高度”、“交易在所处区块中的位置偏移量”和“合约状态在智能合约被执行时的被修改次序”，可以实现区块维度、交易维度和状态维度的加密控制，使得任意两个合约状态所产生的加密后合约状态都必然不会产生规律可循的取值变化，而不论该任意两个合约状态是否来自同一交易或不同交易、不同交易是否来自同一区块或不同区块。其中，对于同一交易产生的多个合约状态，可以通过条件“合约状态在智能合约被执行时的被修改次序”实现加密控制，这是由于同一交易产生的不同合约状态必然具有不同的被修改次序；而对于同一区块的不同交易分别产生的合约状态，即便这些合约状态在各自的交易中具有相同的被修改次数，也可以进一步通过条件“交易在所处区块中的位置偏移量”实现加密控制，这是由于同一区块的不同交易必然具有不同的位置偏移量；而对于不同区块的多个交易分别产生的合约状态，即便这些合约状态在各自的交易中具有相同的被修改次数，也可以进一步通过条件“交易所处区块的区块高度”实现加密控制，这是由于不同区块的交易必然具有不同的区块高度。

[71]仍以上述的区块 B1、B2 为例。如图 7 所示，当区块链节点同时考量区块高度、交易对应的位置偏移量与合约状态的被修改次序时，对于区块 B1 涉及的 Balance1、Balance2、Balance3 和 Balance4 等合约状态，由于 Balance1 与 Balance2 来自于交易 Tx1，使得 Balance1 与 Balance2 必然分别对应于不同的被修改次序，譬如 Balance1 对应于被修改次序 U1、Balance2 对应于被修改次序 U2，同时假定交易 Tx1 对应的位置偏移量为 Offset1，那么可以通过公共密钥 Key128、区块高度 H1、位置偏移量 Offset1 和被修改次序 U1 对 Balance1 进行加密，得到加密后的 S-Balance1-4，而通过公共密钥 Key128、区块高度 H1、位置偏移量 Offset1 和被修改次序 U2 对 Balance2 进行加密，得到加密后的 S-Balance2-4。同时，由于 Balance3 与 Balance4 来自于交易 Tx2，使得 Balance3 与 Balance4 必然分别对应于不同的被修改次序，譬如 Balance3 对应于被修改次序 U1、Balance4 对应于被修改次序 U2，同时假定交易 Tx2 对应的位置偏移量为 Offset2，那么可以通过公共密钥 Key128、区块高度 H1、位置偏移量 Offset2 和被修改次序 U1 对

Balance3 进行加密，得到加密后的 S-Balance3-4，而通过公共密钥 Key128、区块高度 H1、位置偏移量 Offset2 和被修改次序 U2 对 Balance4 进行加密，得到加密后的 S-Balance4-4。

[72]类似地，对于区块 B2 涉及的 Balance1、Balance2、Balance3 和 Balance4 等合约状态，由于 Balance1 与 Balance2 来自于交易 Tx3，使得 Balance1 与 Balance2 必然分别对应于不同的被修改次序，譬如 Balance1 对应于被修改次序 U1、Balance2 对应于被修改次序 U2，同时假定交易 Tx3 对应的位置偏移量为 Offset1，那么可以通过公共密钥 Key128、区块高度 H2、位置偏移量 Offset1 和被修改次序 U1 对 Balance1 进行加密，得到加密后的 R-Balance1-4，而通过公共密钥 Key128、区块高度 H2、位置偏移量 Offset1 和被修改次序 U2 对 Balance2 进行加密，得到加密后的 R-Balance2-4。同时，由于 Balance3 与 Balance4 来自于交易 Tx4，使得 Balance3 与 Balance4 必然分别对应于不同的被修改次序，譬如 Balance3 对应于被修改次序 U1、Balance4 对应于被修改次序 U2，同时假定交易 Tx4 对应的位置偏移量为 Offset2，那么可以通过公共密钥 Key128、区块高度 H2、位置偏移量 Offset2 和被修改次序 U1 对 Balance3 进行加密，得到加密后的 R-Balance3-4，而通过公共密钥 Key128、区块高度 H2、位置偏移量 Offset2 和被修改次序 U2 对 Balance4 进行加密，得到加密后的 R-Balance4-4。

[73]在一实施例中，区块链节点将收到的加密后的交易读入可信执行环境中进行解密并执行对应的智能合约，并在可信执行环境中对产生修改的合约状态进行加密，然后写入数据库中进行存储，确保可信执行环境之外均为密文、以保证数据安全性，而可信执行环境之内可以解密为明文进行处理、以充分利用 CPU 的算力。

[74]区块链节点在可信执行环境中根据公共密钥和影响因子对合约状态进行加密时，存在多种可选用的加密手段，可以借鉴相关技术中的加密解决方案。下面对两种可能采用的加密解决方案予以介绍。

[75]在一实施例中，区块链节点可以通过 GCM（Galois/Counter Mode）算法对上述的合约状态进行加密；GCM 中的字母 G 代表 GMAC (Galois message authentication code mode, 伽罗瓦消息验证码)、字母 C 代表 CTR (CounTeR 计数器模式)。GCM 算法的输入包括 3 部分：待加密数据、对称密钥和初始化向量（IV，Initialization Vector），本说明书中可以将上述的合约状态作为待加密数据、将上述的公共密钥作为 GCM 算法所需的对称密钥、将上述的影响因子作为 GCM 算法所需的初始化向量，从而对合约状态进行加密，

生成相应的加密后合约状态和相应的校验码，该校验码可以用于校验加密后合约状态的完整性。

[76]因此，区块链节点在存储加密后合约状态时，可以将校验码与加密后合约状态相关联地写入数据库。那么，在后续针对加密后合约状态进行解密时，如果解密失败可以通过校验码对加密后合约状态进行校验：当校验成功时，表明加密后合约状态的数据完整，应当是由其他因素导致的解密失败，比如输入的密钥或影响因子错误；当校验失败时，表明加密后合约状态的数据不完整。

[77]在另一实施例中，区块链节点可以根据公共密钥和影响因子生成衍生密钥，比如将公共密钥与影响因子拼接后进行哈希运算或其他运算，以得到衍生密钥；然后，区块链节点可以根据衍生密钥对合约状态进行加密，生成加密后合约状态。

[78]在一实施例中，公共密钥存储于区块链节点上的围圈中。由于仅CPU能够访问围圈内存储的公共密钥，使得该公共密钥足够安全，理论上无法被不法分子获得，从而确保了加密后合约状态的安全性。

[79]公共密钥可以由区块链节点通过远程证明后，由密钥管理服务器（KMS）分配至该区块链节点；或者，公共密钥可由区块链网络中的各个节点之间协商得到；或者，可以通过其他方式得到公共密钥，本说明书并不对此进行限制。

[80]基于上述途径获得的密钥可以并非公共密钥。例如，上述渠道获得的密钥可以为安全密钥，而该安全密钥可以实现版本演化，从而演化得到上述的公共密钥。换言之，上述的公共密钥可以为指定版本的安全密钥；其中，在相邻版本的安全密钥中，低版本的安全密钥由高版本的安全密钥不可逆地计算得到，譬如最高版本的安全密钥为根密钥（root key），而其他版本的安全密钥直接或间接由根密钥不可逆地计算得到。比如低版本的安全密钥由高版本的安全密钥与预设信息进行哈希运算得到，那么由于哈希运算的特性，使得低版本的安全密钥无法逆推出高版本的安全密钥，这样有助于通过安全密钥的版本演进实现对公共密钥的更换，而避免长时间使用相同的公共密钥。并且，在更换公共密钥时，可以确保更换后密钥的版本总是高于更换前密钥的版本，以确保：一方面，即便先前使用的密钥发生泄漏，也可以更换为高版本的密钥而及时止损；另一方面，只要拥有高版本的密钥，即可演化得到低版本的密钥，对先前所使用的密钥进行兼容，从而对先前加密的合约状态进行解密。

[81]安全密钥之间的版本演化规则可以为：相邻的高版本密钥与相邻的低版本密钥对应

的版本号进行哈希运算，得到相邻的低版本密钥。例如，如果需要衍生出版本号分别为0~255 的 256 个版本的密钥，可以将根密钥与版本号 0xFF（对应的十进制取值为 255）进行哈希计算，得到版本号为 255 的密钥 key-255；通过将密钥 key-255 与版本因子 0xFE（对应的十进制取值为 254）进行哈希计算，得到版本号为 254 的密钥 key-254；……通过将密钥 key-1 与版本因子 0x00（对应的十进制取值为 0）进行哈希计算，得到版本号为 0 的密钥 key-0。由于哈希算法的特性，使得高版本密钥与低版本密钥之间的计算不可逆，比如可以由密钥 key-1 与版本因子 0x00 计算得到密钥 key-0，但是不能够通过密钥 key-0 与版本因子 0x00 反推出密钥 key-1。因此，可以选定某一版本的安全密钥，并将其设置为区块链节点所使用的公共密钥，以用于对合约状态进行加密处理。

[82]如前所述，区块链节点根据公共密钥和影响因子对合约状态进行加密，以得到加密后合约状态。如果公共密钥和影响因子为固定取值，那么只需要将公共密钥、影响因子分别单独存储于围圈中即可；但是，如果公共密钥或影响因子具有动态取值，即对于不同的合约状态进行加密时，可能采用不同的公共密钥或影响因子，那么应当在存储加密后合约状态时，对相应采用的公共密钥、影响因子或者用于表明其取值的信息进行关联存储，以便于后续实施解密操作。

[83]假定影响因子的取值存在动态变化，可以将影响因子与加密后合约状态相关联地写入数据库。例如图 8 所示，区块链节点以键值对（key-value）的形式对加密后合约状态进行存储。Key 的取值可以参考相关技术中的方式确定，比如 key=hash(RLP(value))，即 key 的取值为 RLP（Recursive Length Prefix，递归长度前缀）编码后的 value 的哈希值。而 value 的组成部分可以包括：加密后合约状态、校验值和影响因子。加密后合约状态可由上述实施例中的方式，根据公共密钥和影响因子进行加密得到。而当采用诸如 GCM 算法或其他加密算法实施加密时，还可以得到校验值；当然，如果不存在校验值，那么 value 中可以不包含校验值。而影响因子的取值存在上文所述的多种情况，图 8 中以影响因子同时包含区块高度、交易偏移量和修改次序为例，即影响因子由“交易所处区块的区块高度”、“交易在所处区块中的位置偏移量”和“合约状态在智能合约被执行时的被修改次序”构成。

[84]基于图 8 所示的实施例，区块链节点在读取这一键值对后，可以从该键值对的 value 中获得解密所需的影响因子，从而结合公共密钥对加密后合约状态进行解密。而在一些场景中，可以对影响因子进行加密，譬如在存储阶段由区块链节点在 TEE 中对影响因子进行加密，使得 value 中包含加密后的影响因子，而非明文形式的影响因子；相应地，

在读取如图 8 所示的键值对后，将无法直接得到明文形式的影响因子，可以进一步提升对加密后合约状态的解密门槛，提升安全性。

[85] 区块链节点可以采用任意密钥对影响因子进行加密。虽然也可以采用上述的公共密钥对影响因子进行加密，但是为了增加密钥的多样性、提升安全性，可以采用区别于公共密钥的其他密钥对影响因子进行加密。例如，当公共密钥为前述某一版本的密钥时，对影响因子进行加密的密钥可以为另一版本，从而区别于公共密钥；譬如，可以采用版本号为 0 的最低版本密钥对影响因子进行加密，而公共密钥的版本号可被设定为必然大于 0。

[86] 公共密钥可能存在版本信息，譬如公共密钥为上述某一版本的安全密钥。区块链节点在针对加密后合约状态的键值对进行存储时，可以在 value 中包含公共密钥的版本信息，尤其是区块链节点使用的公共密钥存在版本更新的情况下，当前采用的公共密钥的版本可能区别于先前存储的加密后合约状态在加密时采用的历史公共密钥，因而 value 中所含的版本信息可以帮助区块链节点准确选取所需采用的密钥。例如图 9 所示，在图 8 所示实施例的基础上，在键值对的 value 中可以包含信息字段，该信息字段可以进一步包含版本信息子字段，该版本信息子字段用于记录公共密钥的版本信息。

[87] 其中，区块链节点可以对版本信息进行加密后，添加至 value 中，而非采用明文形式记录版本信息。用于对版本信息加密的密钥可以为公共密钥，或者区别于公共密钥的其他密钥，比如与前述的影响因子相类似的，可以采用版本号为 0 的最低版本密钥对版本信息进行加密。

[88] 综上所述，本说明书根据公共密钥和影响因子对合约状态进行加密，相比于单纯采用公共密钥进行加密，可以通过影响因子增加加密后合约状态的随机性，以提升数据安全性。

[89] 图 10 是一示例性实施例提供的一种设备的示意结构图。请参考图 10，在硬件层面，该设备包括处理器 1002、内部总线 1004、网络接口 1006、内存 1008 以及非易失性存储器 1010，当然还可能包括其他业务所需要的硬件。处理器 1002 从非易失性存储器 1010 中读取对应的计算机程序到内存 1008 中然后运行，在逻辑层面上形成基于区块高度实现动态加密的装置。当然，除了软件实现方式之外，本说明书一个或多个实施例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。

[90]请参考图 11，在软件实施方式中，该基于区块高度实现动态加密的装置可以包括:

[91]解密单元 1101，在可信执行环境中解密接收到的交易，以确定所述交易对应的智能合约;

[92]执行单元 1102，在可信执行环境中执行所述智能合约，使所述智能合约中包含的合约状态被修改;

[93]加密单元 1103，在可信执行环境中根据公共密钥和影响因子对所述合约状态进行加密，其中所述影响因子包括所述交易所处区块的区块高度;

[94]存储单元 1104，用于将加密后合约状态写入数据库。

[95]可选的，所述影响因子还包括以下至少之一: 所述交易在所处区块中的位置偏移量、所述合约状态在所述智能合约被执行时的被修改次序。

[96]可选的，所述影响因子被与所述加密后合约状态相关联地写入数据库。

[97]可选的，所述影响因子在可信执行环境中被加密后，与所述加密后合约状态相关联地写入数据库。

[98]可选的，加密单元 1103 具体用于:

[99]将所述公共密钥作为 GCM 算法所需的对称密钥、将所述影响因子作为 GCM 算法所需的初始化向量，通过 GCM 算法对所述合约状态进行加密，生成所述加密后合约状态和相应的校验码; 其中，所述校验码被与所述加密后合约状态相关联地写入数据库。

[100] 可选的，加密单元 1103 具体用于:

[101] 根据所述公共密钥和所述影响因子生成衍生密钥;

[102] 根据所述衍生密钥对所述合约状态进行加密，生成所述加密后合约状态。

[103] 可选的，所述公共密钥包括: 指定版本的安全密钥; 其中，在相邻版本的安全密钥中，低版本的安全密钥由高版本的安全密钥不可逆地计算得到。

[104] 可选的，最高版本的安全密钥为根密钥，其他版本的安全密钥直接或间接由所述根密钥不可逆地计算得到。

[105] 可选的，所述公共密钥的版本信息被与所述加密后合约状态相关联地写入数据库。

[106] 可选的，所述公共密钥的版本信息在可信执行环境中被加密后，与所述加密后合约状态相关联地写入数据库。

[107] 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，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。

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

[109] 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。

[110] 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、磁盘存储、量子存储器、基于石墨烯的存储介质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。

[111] 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。

[112] 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。

[113] 在本说明书一个或多个实施例使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本说明书一个或多个实施例。在本说明书一个或多个实施例和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

[114] 应当理解，尽管在本说明书一个或多个实施例可能采用术语第一、第二、第三等来描述各种信息，但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如，在不脱离本说明书一个或多个实施例范围的情况下，第一信息也可以被称为第二信息，类似地，第二信息也可以被称为第一信息。取决于语境，如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”。

[115] 以上所述仅为本说明书一个或多个实施例的较佳实施例而已，并不用以限制本说明书一个或多个实施例，凡在本说明书一个或多个实施例的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本说明书一个或多个实施例保护的范围之内。

权利要求书

1. 一种基于区块高度实现动态加密的方法，包括:

区块链节点在可信执行环境中解密接收到的交易，以确定所述交易对应的智能合约;

所述区块链节点在可信执行环境中执行所述智能合约，使所述智能合约中包含的合约状态被修改;

所述区块链节点在可信执行环境中根据公共密钥和影响因子对所述合约状态进行加密，以将加密后合约状态写入数据库，其中所述影响因子包括所述交易所处区块的区块高度。

2. 根据权利要求 1 所述的方法，所述影响因子还包括以下至少之一:

所述交易在所处区块中的位置偏移量、所述合约状态在所述智能合约被执行时的被修改次序。

3. 根据权利要求 1 或 2 所述的方法，所述影响因子被与所述加密后合约状态相关联地写入数据库。

4. 根据权利要求 3 所述的方法，所述影响因子在可信执行环境中被加密后，与所述加密后合约状态相关联地写入数据库。

5. 根据权利要求 1 所述的方法，所述区块链节点在可信执行环境中根据公共密钥和影响因子对所述合约状态进行加密，包括:

所述区块链节点将所述公共密钥作为 GCM 算法所需的对称密钥、将所述影响因子作为 GCM 算法所需的初始化向量，通过 GCM 算法对所述合约状态进行加密，生成所述加密后合约状态和相应的校验码; 其中，所述校验码被与所述加密后合约状态相关联地写入数据库。

6. 根据权利要求 1 所述的方法，所述区块链节点在可信执行环境中根据公共密钥和影响因子对所述合约状态进行加密，包括:

所述区块链节点根据所述公共密钥和所述影响因子生成衍生密钥;

所述区块链节点根据所述衍生密钥对所述合约状态进行加密，生成所述加密后合约状态。

7. 根据权利要求 1 所述的方法，所述公共密钥包括: 指定版本的安全密钥; 其中，在相邻版本的安全密钥中，低版本的安全密钥由高版本的安全密钥不可逆地计算得到。

8. 根据权利要求 7 所述的方法，最高版本的安全密钥为根密钥，其他版本的安全密钥直接或间接由所述根密钥不可逆地计算得到。

9. 根据权利要求 7 所述的方法，所述公共密钥的版本信息被与所述加密后合约状态相关联地写入数据库。

10. 根据权利要求 9 所述的方法，所述公共密钥的版本信息在可信执行环境中被加密后，与所述加密后合约状态相关联地写入数据库。

11. 一种基于区块高度实现动态加密的装置，包括:

解密单元，在可信执行环境中解密接收到的交易，以确定所述交易对应的智能合约;

执行单元，在可信执行环境中执行所述智能合约，使所述智能合约中包含的合约状态被修改;

加密单元，在可信执行环境中根据公共密钥和影响因子对所述合约状态进行加密，其中所述影响因子包括所述交易所处区块的区块高度;

存储单元，用于将加密后合约状态写入数据库。

12. 一种电子设备，包括:

处理器;

用于存储处理器可执行指令的存储器;

其中，所述处理器通过运行所述可执行指令以实现如权利要求 1-10 中任一项所述的方法。

13. 一种计算机可读存储介质，其上存储有计算机指令，该指令被处理器执行时实现如权利要求 1-10 中任一项所述方法的步骤。

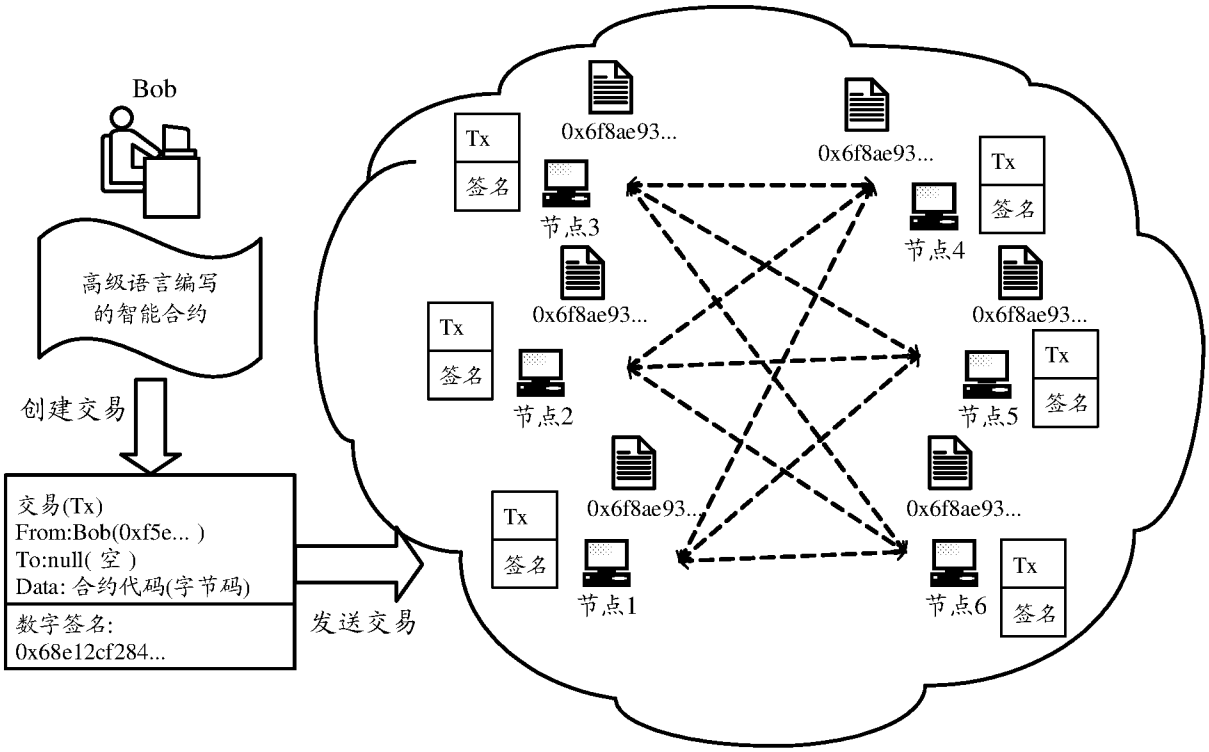
Bob
高级语言编写
的智能合约
创建交易
交易(Tx)
From:Bob(0xf5e...)
To:null(空)
Data: 合约代码(字节码)
数字签名:
0x68e12cf284...
发送交易
Tx
签名
0x6f8ae93...
节点1
节点2
节点3
节点4
节点5
节点6

图 1

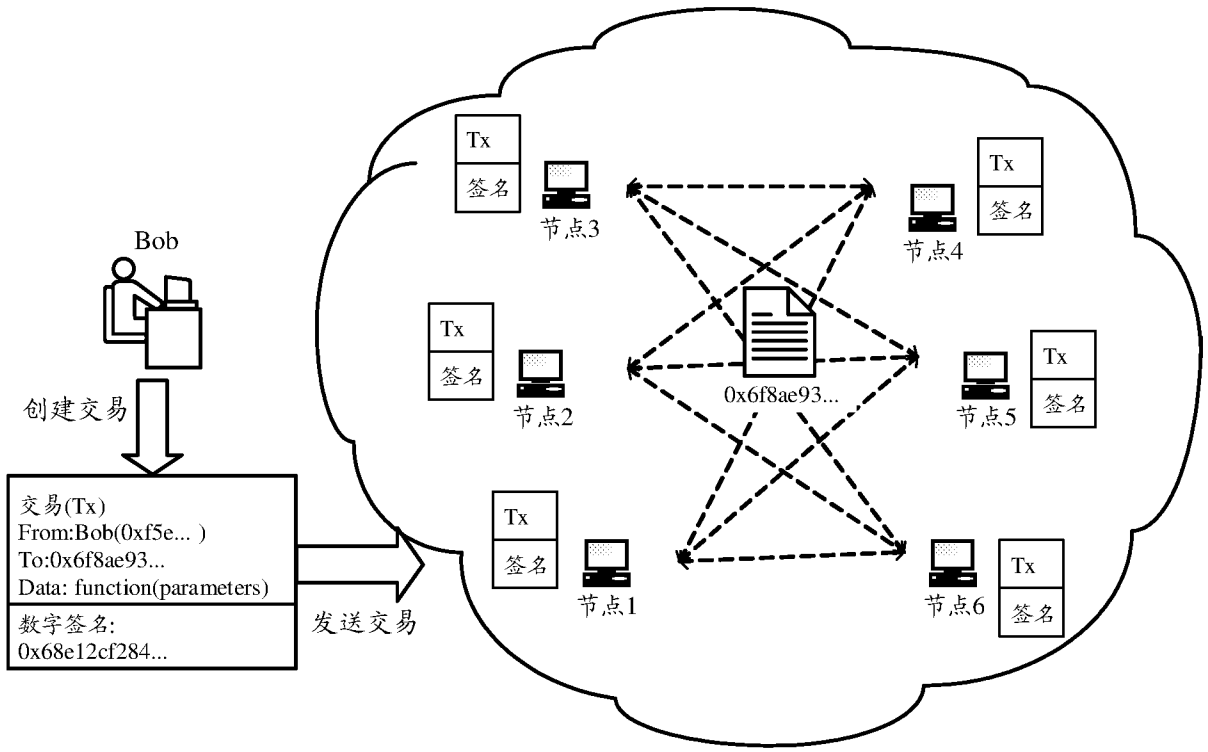
Bob
创建交易
交易(Tx)
From:Bob(0xf5e...)
To:0x6f8ae93...
Data: function(parameters)
数字签名:
0x68e12cf284...
发送交易
Tx
签名
0x6f8ae93...
节点1
节点2
节点3
节点4
节点5
节点6

图 2

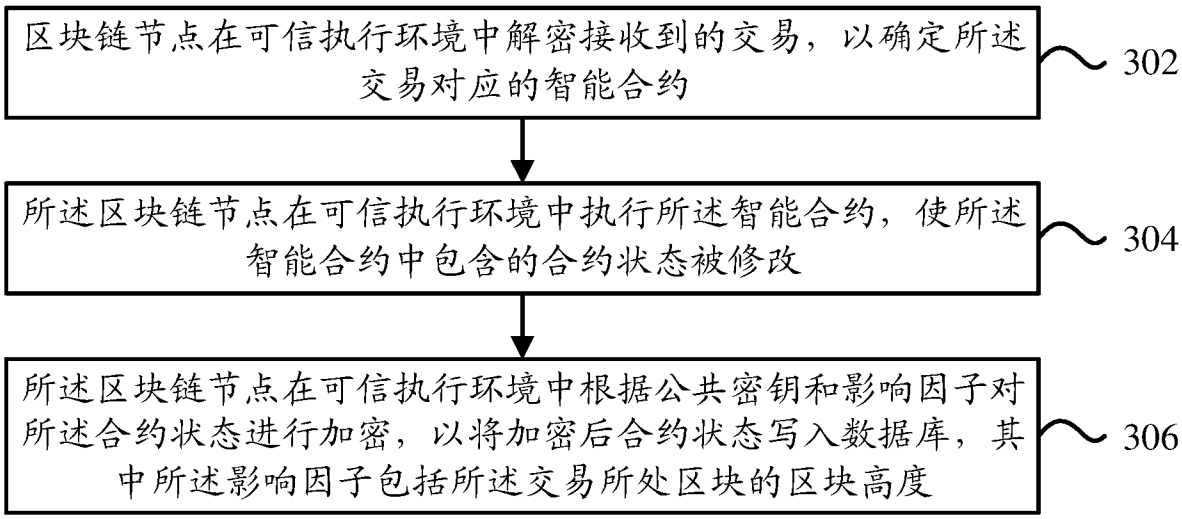
区块链节点在可信执行环境中解密接收到的交易，以确定所述交易对应的智能合约
302
所述区块链节点在可信执行环境中执行所述智能合约，使所述智能合约中包含的合约状态被修改
304
所述区块链节点在可信执行环境中根据公共密钥和影响因子对所述合约状态进行加密，以将加密后合约状态写入数据库，其中所述影响因子包括所述交易所处区块的区块高度
306

图 3

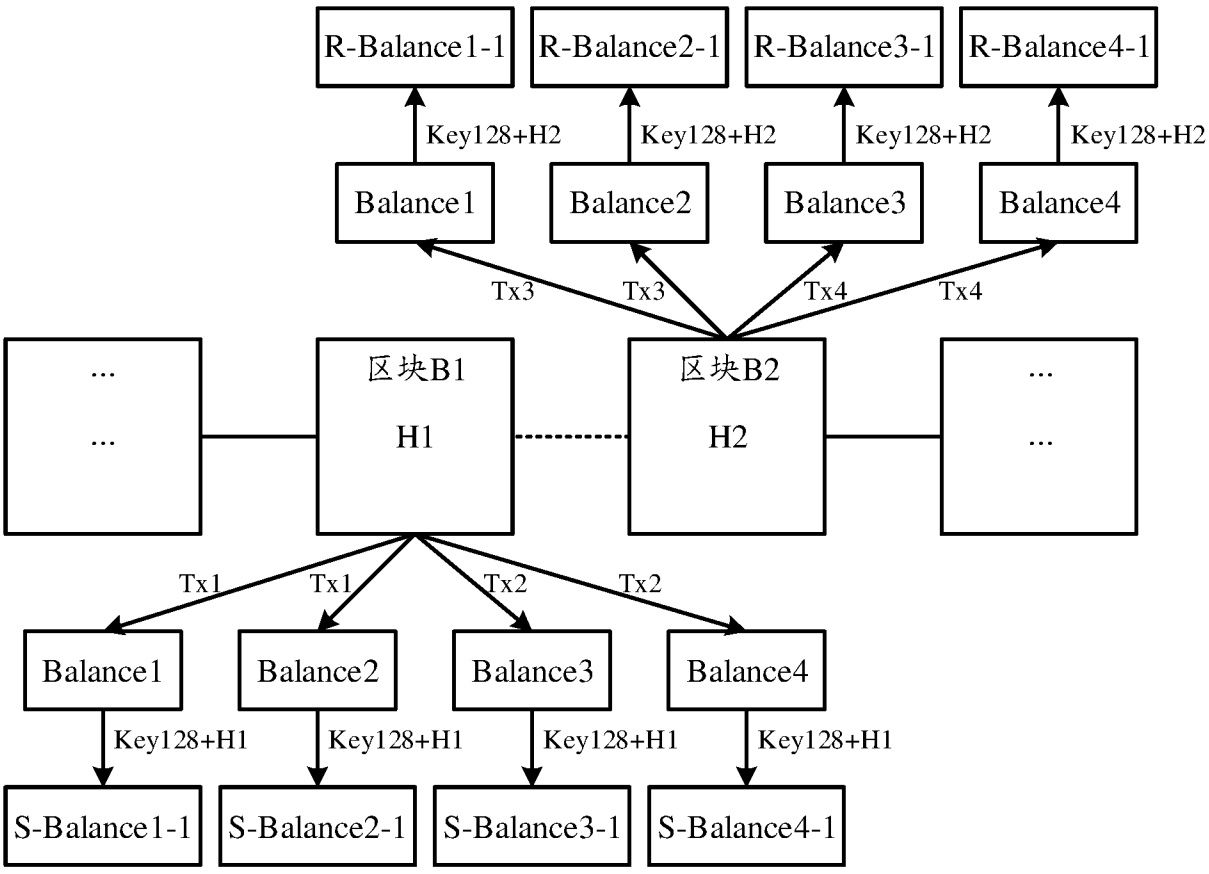
R-Balance1-1
R-Balance2-1
R-Balance3-1
R-Balance4-1
Key128+H2
Key128+H2
Key128+H2
Key128+H2
Balance1
Balance2
Balance3
Balance4
Tx3
Tx3
Tx4
Tx4
...
...
区块B1
H1
区块B2
H2
...
...
Tx1
Tx1
Tx2
Tx2
Balance1
Balance2
Balance3
Balance4
Key128+H1
Key128+H1
Key128+H1
Key128+H1
S-Balance1-1
S-Balance2-1
S-Balance3-1
S-Balance4-1

图 4

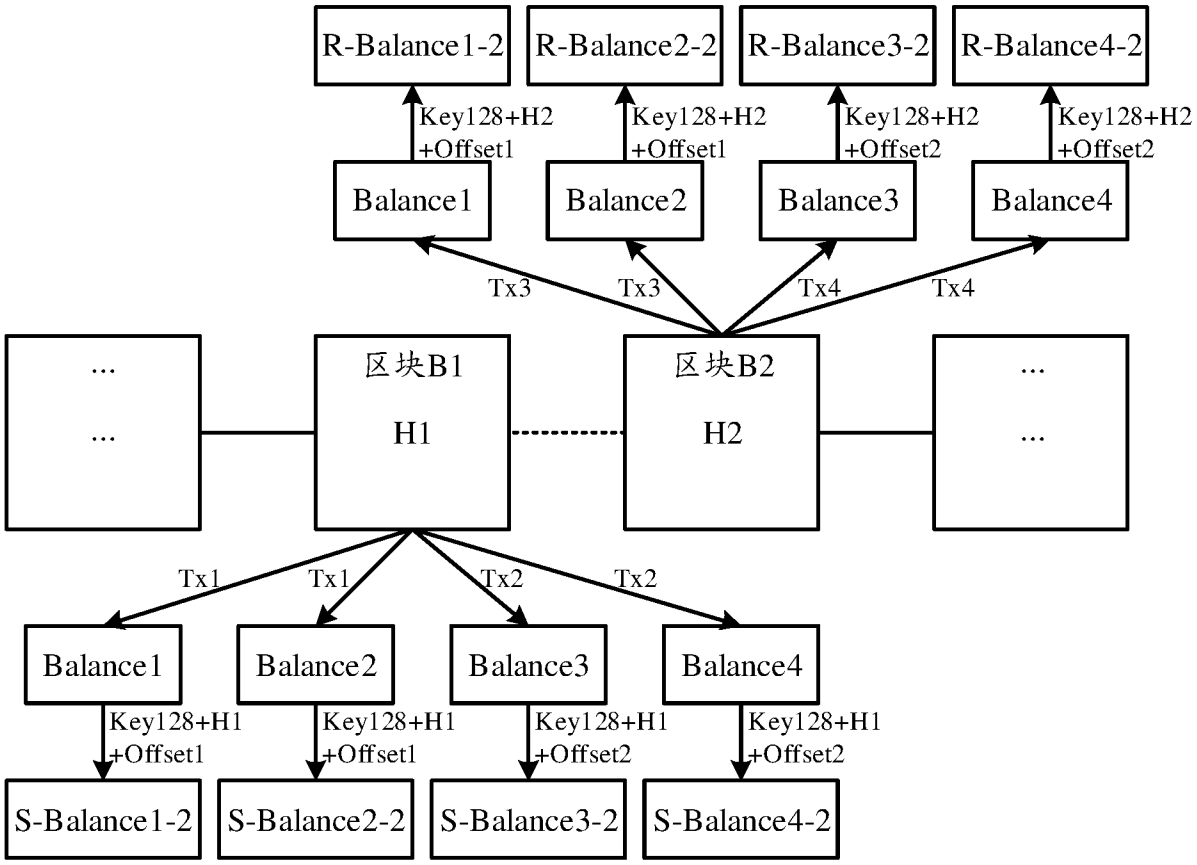
R-Balance1-2
R-Balance2-2
R-Balance3-2
R-Balance4-2
Key128+H2 +Offset1
Key128+H2 +Offset1
Key128+H2 +Offset2
Key128+H2 +Offset2
Balance1
Balance2
Balance3
Balance4
Tx3
Tx3
Tx4
Tx4
...
...
区块B1
H1
区块B2
H2
...
...
Tx1
Tx1
Tx2
Tx2
Balance1
Balance2
Balance3
Balance4
Key128+H1 +Offset1
Key128+H1 +Offset1
Key128+H1 +Offset2
Key128+H1 +Offset2
S-Balance1-2
S-Balance2-2
S-Balance3-2
S-Balance4-2

图 5

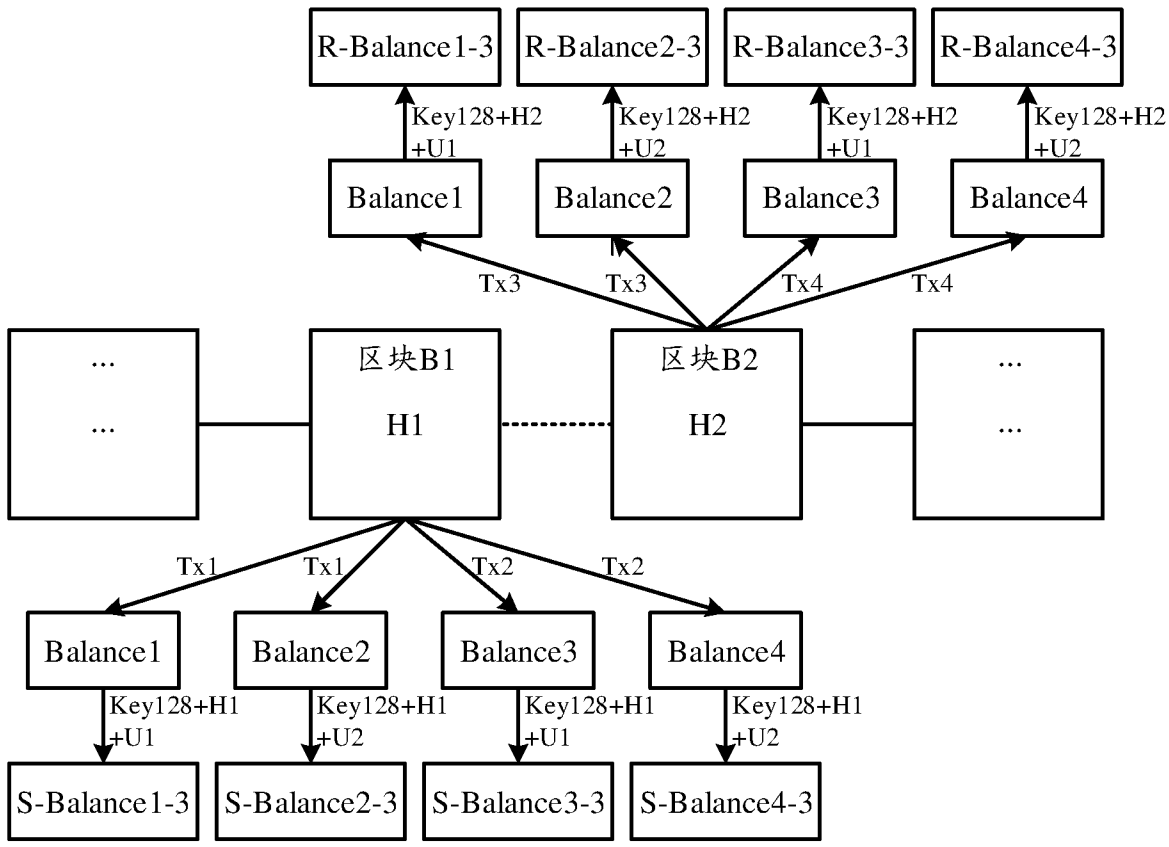
R-Balance1-3
R-Balance2-3
R-Balance3-3
R-Balance4-3
Key128+H2 +U1
Key128+H2 +U2
Key128+H2 +U1
Key128+H2 +U2
Balance1
Balance2
Balance3
Balance4
Tx3
Tx3
Tx4
Tx4
...
...
区块B1
H1
区块B2
H2
...
...
Tx1
Tx1
Tx2
Tx2
Balance1
Balance2
Balance3
Balance4
Key128+H1 +U1
Key128+H1 +U2
Key128+H1 +U1
Key128+H1 +U2
S-Balance1-3
S-Balance2-3
S-Balance3-3
S-Balance4-3

图 6

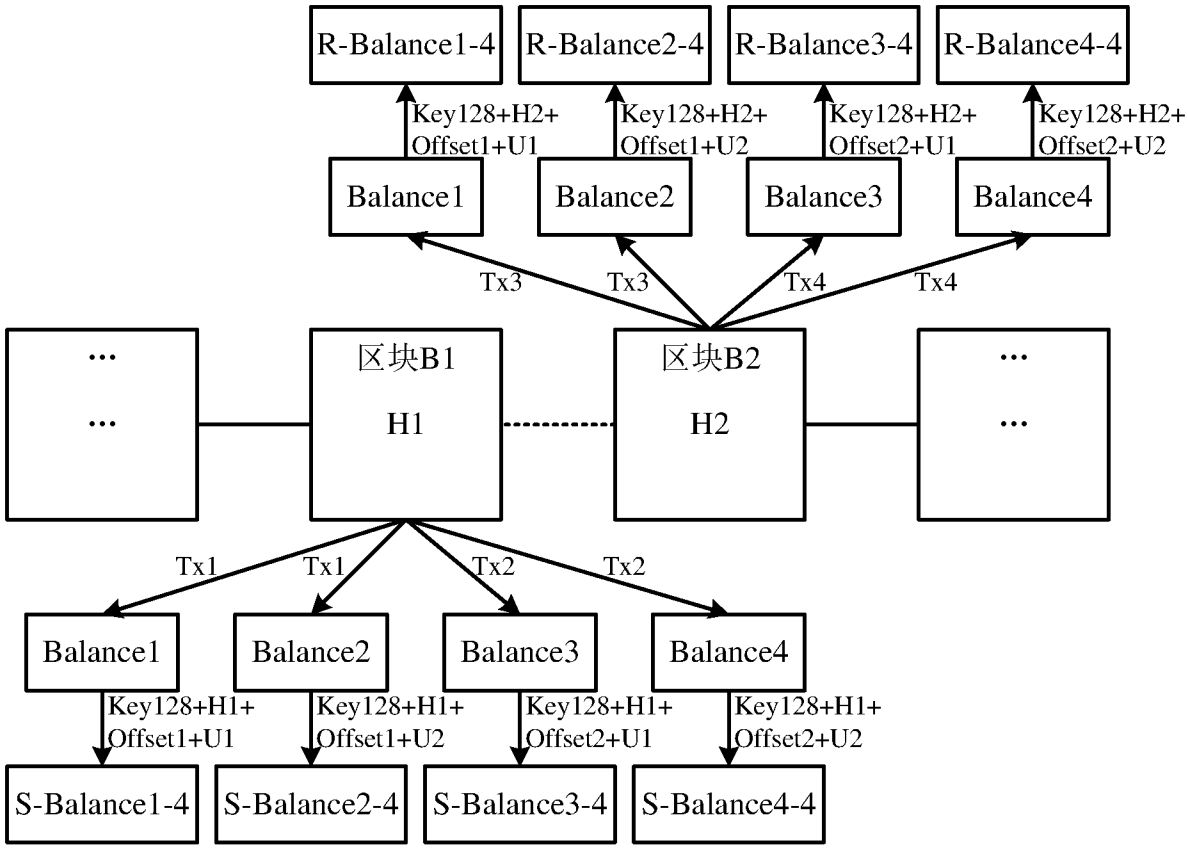
R-Balance1-4
R-Balance2-4
R-Balance3-4
R-Balance4-4
Key128+H2+ Offset1+U1
Key128+H2+ Offset1+U2
Key128+H2+ Offset2+U1
Key128+H2+ Offset2+U2
Balance1
Balance2
Balance3
Balance4
Tx3
Tx3
Tx4
Tx4
区块B1
H1
区块B2
H2
Tx1
Tx1
Tx2
Tx2
Balance1
Balance2
Balance3
Balance4
Key128+H1+ Offset1+U1
Key128+H1+ Offset1+U2
Key128+H1+ Offset2+U1
Key128+H1+ Offset2+U2
S-Balance1-4
S-Balance2-4
S-Balance3-4
S-Balance4-4

图 7

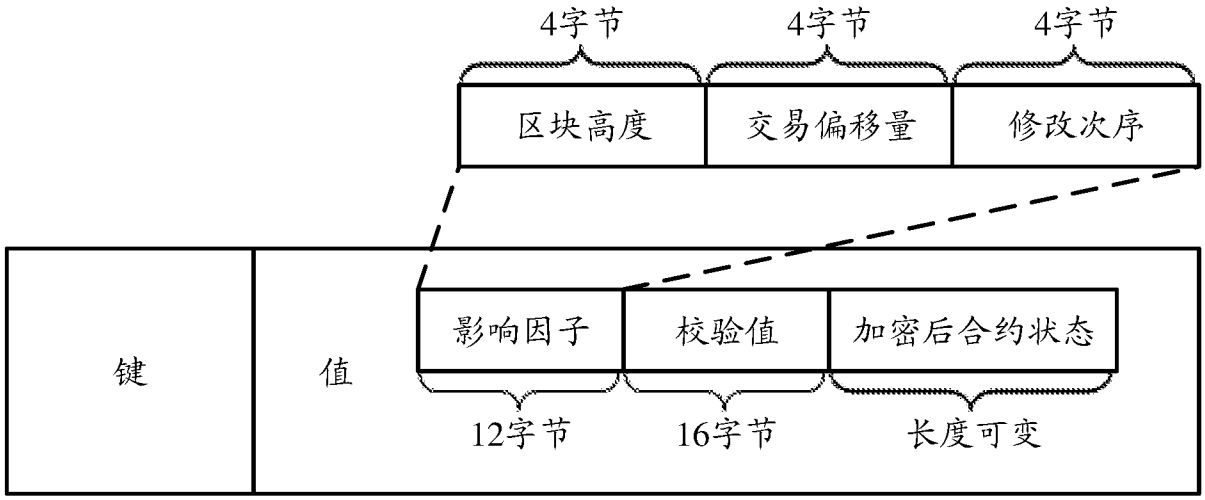
4字节
4字节
4字节
区块高度
交易偏移量
修改次序
键
值
影响因子
校验值
加密后合约状态
12字节
16字节
长度可变

图 8

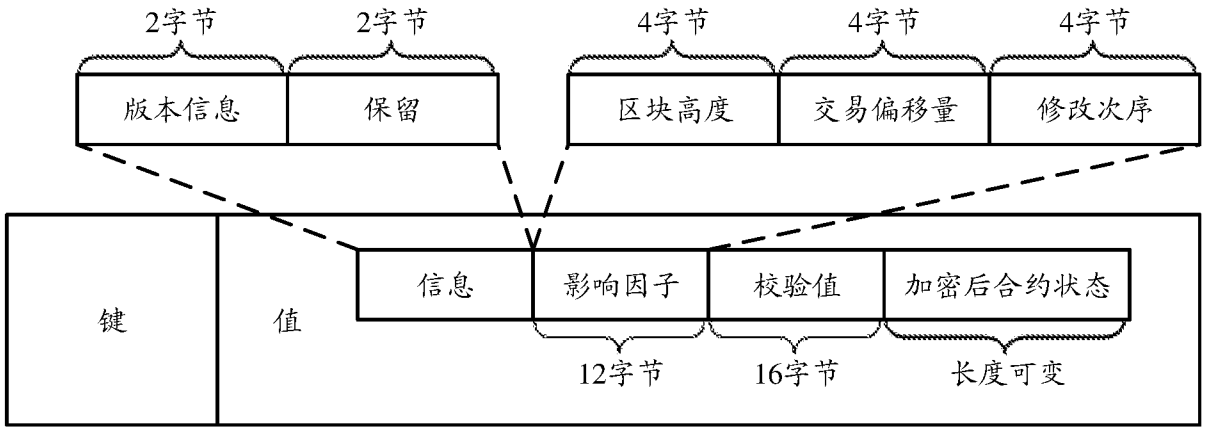
2字节
2字节
4字节
4字节
4字节
版本信息
保留
区块高度
交易偏移量
修改次序
键
值
信息
影响因子
校验值
加密后合约状态
12字节
16字节
长度可变

图 9

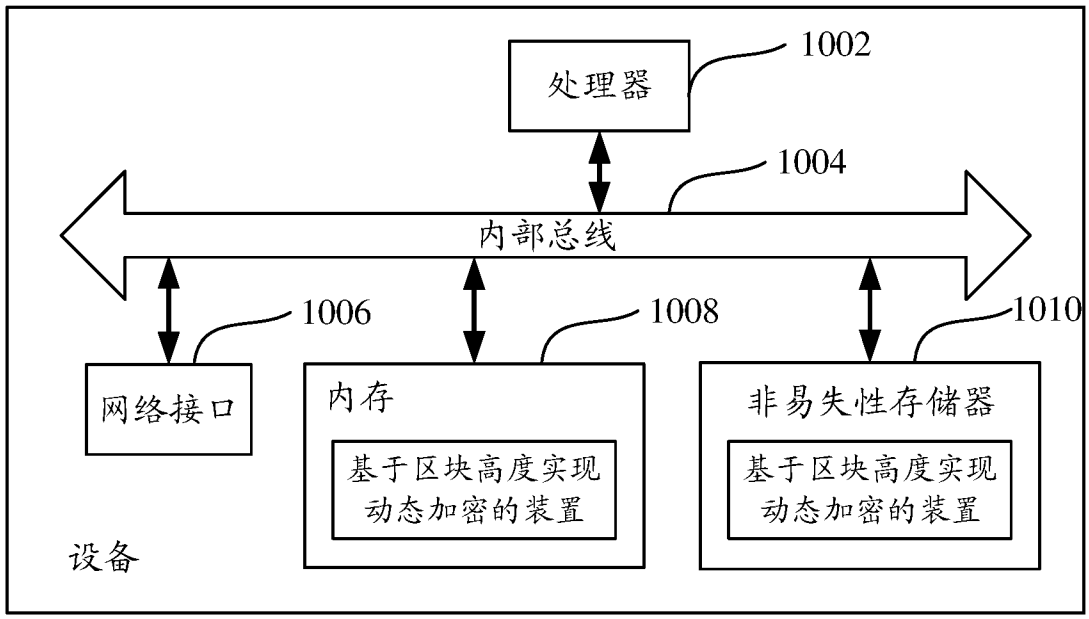
处理器
1002
1004
内部总线
1006
1008
1010
网络接口
内存
基于区块高度实现
动态加密的装置
非易失性存储器
基于区块高度实现
动态加密的装置
设备

图 10

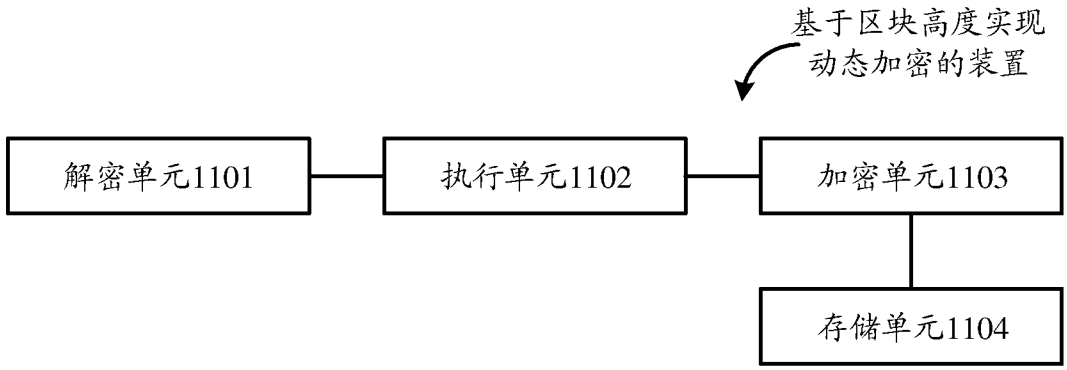
基于区块高度实现
动态加密的装置
解密单元1101
执行单元1102
加密单元1103
存储单元1104

图 11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2020/092611

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/00(2006.01)i; H04L 9/32(2006.01)i; H04L 29/06(2006.01)i; G06Q 20/38(2012.01)i; 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)

H04L; G06F; G06Q

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, CNKI, WPI, EPODOC: 区块, 链, 合约, 状态, 加密, 以太坊, 高度, 公钥, 可信, TEE, block, chain, state, cryptogra+, encrypt+, balance, height, contract, EVM, public, key

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110266467 A (ALIBABA GROUP HOLDING LIMITED) 20 September 2019 (2019-09-20) claims 1-13	1-13
PX	CN 110276610 A (ALIBABA GROUP HOLDING LIMITED) 24 September 2019 (2019-09-24) claims 1-13	1-13
PX	CN 110263547 A (ALIBABA GROUP HOLDING LIMITED) 20 September 2019 (2019-09-20) claims 1-13	1-13
Y	WO 2018200166 A1 (MICROSOFT TECHNOLOGY LICENSING, LLC) 01 November 2018 (2018-11-01) description, paragraphs 28-186	1-13
Y	CN 109345242 A (BAIDU ONLINE NETWORK TECHNOLOGY (BEIJING) CO., LTD.) 15 February 2019 (2019-02-15) description, paragraphs 44-64	1-13
A	CN 108632045 A (ALIBABA GROUP HOLDING LIMITED) 09 October 2018 (2018-10-09) entire document	1-13

☑ 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
11 August 2020	**26 August 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

International application No.
PCT/CN2020/092611

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 107425982 A (ZHONG'AN INFORMATION TECHNOLOGY SERVICES CO., LTD.) 01 December 2017 (2017-12-01) entire document	1-13

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2020/092611

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	110266467	A	20 September 2019	None			
CN	110276610	A	24 September 2019	None			
CN	110263547	A	20 September 2019	None			
WO	2018200166	A1	01 November 2018	CN	110546636	A	06 December 2019
				EP	3616105	A1	04 March 2020
				US	2018309567	A1	25 October 2018
CN	109345242	A	15 February 2019	None			
CN	108632045	A	09 October 2018	US	2019347653	A1	14 November 2019
				WO	2019217692	A1	14 November 2019
				TW	201947444	A	16 December 2019
				HK	1261591	A0	03 January 2020
CN	107425982	A	01 December 2017	WO	2019007396	A1	10 January 2019
				HK	1247743	A0	28 September 2018

国际检索报告

国际申请号
PCT/CN2020/092611

A. 主题的分类

H04L 9/00(2006.01)i; H04L 9/32(2006.01)i; H04L 29/06(2006.01)i; G06Q 20/38(2012.01)i; 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)

H04L; G06F; G06Q

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,CNKI,WPI,EPODOC:区块，链，合约，状态，加密，以太坊，高度，公钥，可信，TEE, block, chain, state, cryptogra+, encrypt+, balance, height, contract, EVM, public, key

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 110266467 A (阿里巴巴集团控股有限公司) 2019年 9月 20日 (2019-09-20) 权利要求1-13	1-13
PX	CN 110276610 A (阿里巴巴集团控股有限公司) 2019年 9月 24日 (2019-09-24) 权利要求1-13	1-13
PX	CN 110263547 A (阿里巴巴集团控股有限公司) 2019年 9月 20日 (2019-09-20) 权利要求1-13	1-13
Y	WO 2018200166 A1 (MICROSOFT TECHNOLOGY LICENSING , LLC) 2018年 11月 1日 (2018-11-01) 说明书第28-186段	1-13
Y	CN 109345242 A (百度在线网络技术北京有限公司) 2019年 2月 15日 (2019-02-15) 说明书第44-64段	1-13
A	CN 108632045 A (阿里巴巴集团控股有限公司) 2018年 10月 9日 (2018-10-09) 全文	1-13
A	CN 107425982 A (众安信息技术服务有限公司) 2017年 12月 1日 (2017-12-01) 全文	1-13

☐ 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 8月 11日	2020年 8月 26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	田琳琳
传真号 (86-10)62019451	电话号码 86-(10)-53961736

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2020/092611

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	110266467	A	2019年 9月 20日	无			
CN	110276610	A	2019年 9月 24日	无			
CN	110263547	A	2019年 9月 20日	无			
WO	2018200166	A1	2018年 11月 1日	CN	110546636	A	2019年 12月 6日
				EP	3616105	A1	2020年 3月 4日
				US	2018309567	A1	2018年 10月 25日
CN	109345242	A	2019年 2月 15日	无			
CN	108632045	A	2018年 10月 9日	US	2019347653	A1	2019年 11月 14日
				WO	2019217692	A1	2019年 11月 14日
				TW	201947444	A	2019年 12月 16日
				HK	1261591	A0	2020年 1月 3日
CN	107425982	A	2017年 12月 1日	WO	2019007396	A1	2019年 1月 10日
				HK	1247743	A0	2018年 9月 28日