(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
2018 年 8 月 2 日 (02.08.2018)

WIPO | PCT

(10) 国际公布号
WO 2018/137316 A1

(51) 国际专利分类号:
G06Q 20/10 (2012.01) *G06Q 20/38* (2012.01)
H04L 9/00 (2006.01) *H04L 9/32* (2006.01)

(21) 国际申请号: PCT/CN2017/091246

(22) 国际申请日: 2017 年 6 月 30 日 (30.06.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201710060336.0 2017年1月24日 (24.01.2017) CN

(71) 申请人: 上海亿账通区块链科技有限公司 (ONECONNECT BLOCKCHAIN TECHNOLOGY CO., LTD. (SHANGHAI)) [CN/CN]; 中国上海市徐汇区龙腾大道2879号3楼3484室吴东勤, Shanghai 200030 (CN)。

(72) 发明人: 陆陈一帆(LU, Frank Yifan Chen); 中国上海市徐汇区龙腾大道2879号3楼3484室吴东勤, Shanghai 200030 (CN)。 宦鹏飞(HUAN, Pengfei); 中国上海市徐汇区龙腾大道2879号3楼3484室吴东勤, Shanghai 200030 (CN)。 张宇 (ZHANG, Yu); 中国上海市徐汇区龙腾大道2879号3楼3484室吴东勤, Shanghai 200030 (CN)。 黄宇翔(HUANG, Yuxiang); 中国上海市徐汇区龙腾大道2879号3楼3484室吴东勤, Shanghai 200030 (CN)。

(74) 代理人: 深圳市沃德知识产权代理事务所 (普通合伙) (SHENZHEN WORLD INTELLECTUAL PROPERTY AGENCY (GENERAL PARTNERSHIP)); 中国广东省深圳市福田区

WO 2018/137316 A1

(54) **Title:** SECURE TRANSACTION METHOD BASED ON BLOCK CHAIN, ELECTRONIC DEVICE, SYSTEM, AND STORAGE MEDIUM

(54) 发明名称: 基于区块链的安全交易方法、电子装置、系统及存储介质

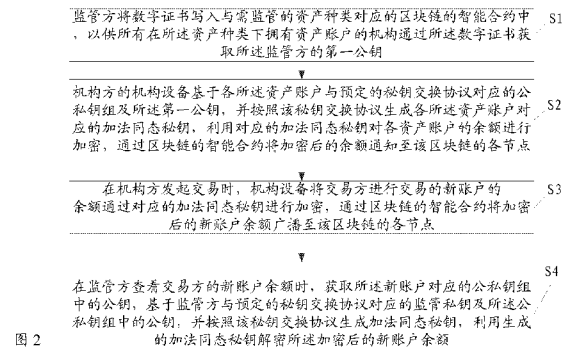

图 2

S1 A SUPERVISOR WRITES A DIGITAL CERTIFICATE INTO A SMART CONTRACT OF A BLOCK CHAIN CORRESPONDING TO AN ASSET TYPE NEEDING TO BE SUPERVISED FOR ALL THE INSTITUTIONS HAVING ASSET ACCOUNTS UNDER THE ASSET TYPE TO OBTAIN, BY MEANS OF THE DIGITAL CERTIFICATE, A FIRST PUBLIC KEY OF THE SUPERVISOR

S2 AN INSTITUTION APPARATUS OF AN INSTITUTION PARTY GENERATES, BASED ON A PUBLIC AND PRIVATE KEY GROUP CORRESPONDING TO EACH OF THE ASSET ACCOUNTS AND A PRE-DETERMINED SECRET KEY EXCHANGE PROTOCOL, AND THE FIRST PUBLIC KEY, AN ADDITIVE HOMOMORPHIC SECRET KEY CORRESPONDING TO EACH OF THE ASSET ACCOUNTS ACCORDING TO THE SECRET KEY EXCHANGE PROTOCOL, USES THE CORRESPONDING ADDITIVE HOMOMORPHIC SECRET KEY TO ENCRYPT THE BALANCE OF EACH OF THE ASSET ACCOUNTS, AND NOTIFIES EACH NODE OF THE BLOCK CHAIN OF THE ENCRYPTED BALANCE BY MEANS OF THE SMART CONTRACT OF THE BLOCK CHAIN

S3 WHEN THE INSTITUTION PARTY LAUNCHES A TRANSACTION, THE INSTITUTION APPARATUS ENCRYPTS THE BALANCE OF THE NEW ACCOUNT TRANSACTED BY A TRANSACTION PARTY BY MEANS OF THE CORRESPONDING ADDITIVE HOMOMORPHIC SECRET KEY, AND BROADCASTS THE ENCRYPTED BALANCE OF THE NEW ACCOUNT TO EACH NODE OF THE BLOCK CHAIN BY MEANS OF THE SMART CONTRACT OF THE BLOCK CHAIN

S4 WHEN THE SUPERVISOR CHECKS THE BALANCE OF THE NEW ACCOUNT OF THE TRANSACTION PARTY, OBTAIN A PUBLIC KEY IN THE PUBLIC AND PRIVATE KEY GROUP CORRESPONDING TO THE NEW ACCOUNT, BASED ON A SUPERVISION PRIVATE KEY CORRESPONDING TO THE SUPERVISOR AND THE PRE-DETERMINED SECRET KEY EXCHANGE PROTOCOL, AND A PUBLIC KEY IN THE PUBLIC AND PRIVATE KEY GROUP, GENERATE THE ADDITIVE HOMOMORPHIC SECRET KEY ACCORDING TO THE SECRET KEY EXCHANGE PROTOCOL, AND USE THE GENERATED ADDITIVE HOMOMORPHIC SECRET KEY TO DECRYPT THE ENCRYPTED BALANCE OF THE NEW ACCOUNT

(57) **Abstract:** Disclosed are a secure transaction method based on a block chain, an electronic device, a system, and a storage medium. The method comprises: a supervisor writing a digital certificate into a smart contract of a block chain corresponding to an asset type needing to be supervised for all the institutions having asset accounts under the asset type to obtain, by means of the digital certificate, a first public key of the supervisor (S1) so as to generate an additive homomorphic secret key for homomorphic encryption of the balances of the asset accounts; and when the supervisor checks the balance of a new account of a transaction party, obtaining a public key in

[见续页]

园岭街道八卦四路10号中浩大厦1528-1530室于志光, Guangdong 518000 (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)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

a public and private key group corresponding to the new account, based on a supervision private key corresponding to the supervisor and a pre-determined secret key exchange protocol, and the public key in the public and private key group, generating the additive homomorphic secret key according to the secret key exchange protocol, and using the generated additive homomorphic secret key to decrypt the encrypted balance of the new account (S4).

(57) 摘要：一种基于区块链的安全交易方法、电子装置、系统及存储介质，该方法包括：监管方将数字证书写入与需监管的资产种类对应的区块链的智能合约中，以供所有在所述资产种类下拥有资产账户的机构通过所述数字证书获取所述监管方的第一公钥（S1），以生成对资产账户的余额进行同态加密的加法同态秘钥；在监管方查看交易方的新账户余额时，获取所述新账户对应的公私钥组中的公钥，基于监管方与预定的秘钥交换协议对应的监管私钥及所述公私钥组中的公钥，并按照该秘钥交换协议生成加法同态秘钥，利用生成的加法同态秘钥解密所述加密后的新账户余额（S4）。

基于区块链的安全交易方法、电子装置、系统及存储介质

优先权申明

本申请基于巴黎公约申明享有 2017 年 01 月 24 日递交的申请号为 CN201710060336.0、名称为“基于区块链的安全交易方法及系统”中国专利申请的优先权，该中国专利申请的整体内容以参考的方式结合在本申请中。

技术领域

本发明涉及区块链技术领域，尤其涉及一种基于区块链的安全交易方法、电子装置、系统及计算机可读存储介质。

背景技术

区块链技术具备去中心化、信息不可篡改性等特点，运用区块链技术可实现多方参与的交易事件（例如，转账交易、支付交易等），例如，银行 A 与银行 B 在区块链上进行交易，那么该区块链上所有其他节点都会知晓这笔交易，其他参与方可以一起参与确认交易准确性，防止信息的篡改。然而，这种交易方式由于没有绝对权威机构节点，对每笔交易进行集体验证是必要的，其缺点在于：交易参与方的交易就会毫无私密可言，一个机构的账户有可能被其他节点上的机构跟踪，从而带来信息泄露的风险。

为了解决上述问题，业内采用一种利用加法同态加密保护的方案，来解决区块链交易中信息泄露的问题。然而仍然存在不足之处：例如，当一个账户的账户余额受到加法同态加密保护后只有同态加密秘钥拥有方可以知晓该账户的实际余额，导致监管部门难以对金融资产流动性进行监管。如果要求资产拥有方通过某种形式把同态加密用秘钥传递给监管方，则会因为系统处理步骤复杂，导致容易出现错误及/或安全隐患，且效率低。

综上所述，将区块链技术运用在交易场景下，并有效地保证交易信息的安全、交易处理的高效率及有效保证监管方对账户的监管，已成为亟待解决的技术问题。

发明内容

本发明的目的在于提供一种基于区块链的安全交易方法、电子装置、系统及计算机可读存储介质，旨在有效地保证基于区块链的交易的交易信息的安全、交易处理的高效率及有效保证监管方对账户的监管。

为实现上述目的，本发明提供一种基于区块链的安全交易方法，所述基于区块链的安全交易方法包括：

S1，监管方将数字证书写入与需监管的资产种类对应的区块链的智能合约中，以供所有在所述资产种类下拥有资产账户的机构通过所述数字证书获取所述监管方的第一公钥；

S2，机构方的机构设备基于该机构管理的各所述资产账户对应的公私钥

组与预定的秘钥交换协议及所述第一公钥，并按照该秘钥交换协议生成各所述资产账户对应的加法同态秘钥，利用对应的加法同态秘钥对各资产账户的余额进行加密，通过区块链的智能合约将加密后的余额广播至该区块链的各节点；

S3，在机构方发起交易时，机构设备将交易方进行交易的新账户的余额通过对应的加法同态秘钥进行加密，通过区块链的智能合约将加密后的新账户余额广播至该区块链的各节点；

S4，在监管方查看交易方的新账户余额时，获取所述新账户对应的公私钥组中的公钥，基于监管方与预定的秘钥交换协议对应的监管私钥及所述公私钥组中的公钥，并按照该秘钥交换协议生成加法同态秘钥，利用生成的加法同态秘钥解密所述加密后的新账户余额。

为实现上述目的，本发明还提供一种电子装置，所述电子装置包括存储器及与所述存储器连接的处理器，所述存储器中存储有可在所述处理器上运行的基于区块链的安全交易系统，所述基于区块链的安全交易系统被所述处理器执行时实现如下步骤：

S1，监管方将数字证书写入与需监管的资产种类对应的区块链的智能合约中，以供所有在所述资产种类下拥有资产账户的机构通过所述数字证书获取所述监管方的第一公钥；

S2，机构方的机构设备基于该机构管理的各所述资产账户对应的公私钥组与预定的秘钥交换协议及所述第一公钥，并按照该秘钥交换协议生成各所述资产账户对应的加法同态秘钥，利用对应的加法同态秘钥对各资产账户的余额进行加密，通过区块链的智能合约将加密后的余额广播至该区块链的各节点的智能合约上；

S3，在机构方发起交易时，机构设备将交易方进行交易的新账户的余额通过对应的加法同态秘钥进行加密，通过区块链的智能合约将加密后的新账户余额广播至该区块链的各节点的智能合约上；

S4，在监管方查看交易方的新账户的余额时，获取所述新账户对应的公私钥组中的公钥，基于监管方与预定的秘钥交换协议对应的监管私钥及所述公私钥组中的公钥，并按照该秘钥交换协议生成加法同态秘钥，利用生成的加法同态秘钥解密所述加密后的新账户余额。

为实现上述目的，本发明还提供一种基于区块链的安全交易系统，所述基于区块链的安全交易系统包括：

写入模块，用于将数字证书写入与需监管的资产种类对应的区块链的智能合约中，以供所有在所述资产种类下拥有资产账户的机构通过所述数字证书获取所述监管方的第一公钥，以生成对资产账户的余额及交易后的资产账户的新账户余额进行加密的加法同态秘钥；

第一加密模块，用于基于当前机构管理的各所述资产账户对应的公私钥组中的私钥与预定的秘钥交换协议及所述第一公钥，并按照该秘钥交换协议生成各所述资产账户对应的加法同态秘钥，利用对应的加法同态秘钥对各资

产账户的余额进行加密，通过区块链的智能合约将加密后的余额广播至该区块链的各节点的智能合约上；

第二加密模块，用于在机构方发起交易时，将交易方进行交易的各资产账户的新账户余额通过对应的加法同态秘钥进行加密，通过区块链的智能合约将加密后的新账户余额广播至该区块链的各节点的智能合约上；以及，

解密模块，用于在监管方查看交易方的新账户的余额时，获取所述新账户对应的公私钥组中的公钥，基于监管方与预定的秘钥交换协议对应的监管私钥及所述公私钥组中的公钥，并按照该秘钥交换协议生成加法同态秘钥，利用生成的加法同态秘钥解密所述加密后的新账户余额。

为实现上述目的，本发明还提供一种计算机可读存储介质，所述计算机可读存储介质上存储有基于区块链的安全交易系统，所述基于区块链的安全交易系统被处理器执行时实现以下步骤：

S1，监管方将数字证书写入与需监管的资产种类对应的区块链的智能合约中，以供所有在所述资产种类下拥有资产账户的机构通过所述数字证书获取所述监管方的第一公钥；

S2，机构方的机构设备基于该机构管理的各所述资产账户对应的公私钥组与预定的秘钥交换协议及所述第一公钥，并按照该秘钥交换协议生成各所述资产账户对应的加法同态秘钥，利用对应的加法同态秘钥对各资产账户的余额进行加密，通过区块链的智能合约将加密后的余额广播至该区块链的各节点的智能合约上；

S3，在机构方发起交易时，机构设备将交易方进行交易的新账户的余额通过对应的加法同态秘钥进行加密，通过区块链的智能合约将加密后的新账户余额广播至该区块链的各节点的智能合约上；

S4，在监管方查看交易方的新账户的余额时，获取所述新账户对应的公私钥组中的公钥，基于监管方与预定的秘钥交换协议对应的监管私钥及所述公私钥组中的公钥，并按照该秘钥交换协议生成加法同态秘钥，利用生成的加法同态秘钥解密所述加密后的新账户余额。

本发明的有益效果是：本发明通过秘钥交换协议生成资产拥有方与监管方共同拥有的对称秘钥（即加法同态秘钥），用该对称秘钥作为加法同态加密的加解密秘钥，这样监管方可以解密加密后的账户余额，其他无关方无法知晓该账户的实际余额，有效保障了账户安全性及对账户进行监管，并可提高交易处理的效率。

附图说明

图 1 为本发明各个实施例一可选的应用环境示意图；

图 2 为本发明基于区块链的安全交易方法第一实施例的流程示意图；

图 3 为本发明基于区块链的安全交易方法第二实施例的流程示意图；

图 4 为本发明基于区块链的安全交易方法第三实施例的流程示意图；

图 5 为本发明基于区块链的安全交易方法第四实施例的流程示意图；

图 6 为本发明基于区块链的安全交易系统第一实施例的结构示意图;
图 7 为本发明基于区块链的安全交易系统第二实施例的结构示意图;
图 8 为本发明基于区块链的安全交易系统第三实施例的结构示意图。

具体实施方式

以下结合附图对本发明的原理和特征进行描述，所举实例只用于解释本发明，并非用于限定本发明的范围。

如图 1 所示，图 1 为本发明各个实施例一可选的应用环境示意图。该应用环境示意图包括电子装置 1 及终端设备 2。电子装置 1 可以通过网络、近场通信技术等适合的技术与终端设备 2 进行数据交互。

所述终端设备 2 包括，但不限于，任何一种可与用户通过键盘、鼠标、遥控器、触摸板或者声控设备等方式进行人机交互的电子产品，例如，个人计算机、平板电脑、智能手机、个人数字助理（Personal Digital Assistant, PDA)、游戏机、交互式网络电视（Internet Protocol Television, IPTV）、智能式穿戴式设备、导航装置等等的可移动设备，或者诸如数字 TV、台式计算机、笔记本、服务器等等的固定终端。

所述电子装置 1 是一种能够按照事先设定或者存储的指令，自动进行数值计算和/或信息处理的设备。所述电子装置 1 可以是计算机、也可以是单个网络服务器、多个网络服务器组成的服务器组或者基于云计算的由大量主机或者网络服务器构成的云，其中云计算是分布式计算的一种，由一群松散耦合的计算机集组成的一个超级虚拟计算机。

本实施例中，电子装置 1 可包括，但不仅限于，可通过系统总线相互通信连接的存储器 11、处理器 12 及网络接口 13，存储器 11 存储有可在处理器 12 上运行的基于区块链的安全交易系统。需要指出的是，图 1 仅示出了具有组件 11-13 的电子装置 1，但是应理解的是，并不要求实施所有示出的组件，可以替代的实施更多或者更少的组件。

其中，存储设备 11 包括内存及至少一种类型的可读存储介质。内存为电子装置 1 的运行提供缓存；可读存储介质可为如闪存、硬盘、多媒体卡、卡型存储器（例如，SD 或 DX 存储器等）、随机访问存储器（RAM）、静态随机访问存储器（SRAM）、只读存储器（ROM）、电可擦除可编程只读存储器（EEPROM）、可编程只读存储器（PROM）、磁性存储器、磁盘、光盘等的非易失性存储介质。在一些实施例中，可读存储介质可以是电子装置 1 的内部存储单元，例如该电子装置 1 的硬盘；在另一些实施例中，该非易失性存储介质也可以是电子装置 1 的外部存储设备，例如电子装置 1 上配备的插接式硬盘，智能存储卡（Smart Media Card, SMC），安全数字（Secure Digital, SD）卡，闪存卡（Flash Card）等。本实施例中，存储设备 11 的可读存储介质通常用于存储安装于电子装置 1 的操作系统和各类应用软件，例如本发明一实施例中的基于区块链的安全交易系统的程序代码等。此外，存储设备 11 还可以用于暂时地存储已经输出或者将要输出的各类数据。

所述处理器 12 在一些实施例中可以是中央处理器（Central Processing Unit，CPU）、控制器、微控制器、微处理器、或其他数据处理芯片。该处理器 12 通常用于控制所述电子装置 1 的总体操作，例如执行与所述终端设备 2 进行数据交互或者通信相关的控制和处理等。本实施例中，所述处理器 12 用于运行所述存储器 11 中存储的程序代码或者处理数据，例如运行基于区块链的安全交易系统等。

所述网络接口 13 可包括无线网络接口或有线网络接口，该网络接口 13 通常用于在所述电子装置 1 与其他电子设备之间建立通信连接。本实施例中，网络接口 13 主要用于将电子装置 1 与终端设备 2 相连，在电子装置 1 与终端设备 2 之间建立数据传输通道和通信连接。

所述基于区块链的安全交易系统存储在存储器 11 中，包括至少一个存储在存储器 11 中的计算机可读指令，该至少一个计算机可读指令可被处理器 12 执行，以实现本发明各实施例的基于区块链的安全交易方法；如后续所述，该至少一个计算机可读指令依据其各部分所实现的功能不同，可被划为不同的逻辑模块。

所述基于区块链的安全交易系统通过秘钥交换协议生成资产拥有方与监管方共同拥有的对称秘钥（即加法同态秘钥），用该对称秘钥作为加法同态加密的加解密秘钥，这样监管方可以解密加密后的账户余额，其他无关方无法知晓该账户的实际余额，有效保障了账户安全性及对账户进行监管，并可提高交易处理的效率；另外，通过在区块链智能合约上部署监管方公钥及公开的秘钥交换协议参数，这样拥有或即将拥有该资产的用户可以根据监管方公钥及公开的秘钥交换协议参数生成只有该用户与监管方共有的同态加密秘钥，这样，在保证账户隐私性的同时，可以为不同智能合约上的不同类型资产设定不同的监管方，区块链的业务兼容性和业务扩展便捷性得到了很大的提升。

如图 2 所示，图 2 为本发明基于区块链的安全交易方法一实施例的流程示意图，该基于区块链的安全交易方法包括以下步骤:

步骤 S1，监管方将数字证书写入与需监管的资产种类对应的区块链的智能合约中，以供所有在所述资产种类下拥有资产账户的机构通过所述数字证书获取所述监管方的第一公钥。

本实施例中，监管方将 CA（Certification Authority，证书认证机构）颁发给自身的数字证书写入与需监管的资产种类对应的区块链的智能合约中，资产种类包括多种，例如，按耗用期限的长短，可分为流动资产和长期资产，根据具体形态，长期资产还可以作进一步的分类；按是否有实体形态，可分为有形资产和无形资产。或者综合几种分类标准，可将资产分为流动资产、长期投资、固定资产、无形资产、递延资产等类别。从这些资产类别中选择需要监管的资产种类。

监管方将数字证书写入与需监管的资产种类对应的区块链的智能合约

后，所有在需监管的资产种类下拥有资产账户的用户或机构（例如，金融机构、基金机构等）可以通过智能合约中写入的数字证书来获取监管方的第一公钥，该第一公钥供同态加密使用。

另外，在监管方将数字证书写入与需监管的资产种类对应的区块链的智能合约之前，证书认证机构基于监管方与预先确定的秘钥交换协议对应的第一公钥进行签名，以生成数字证书，并颁发给监管方。

步骤 S2，机构方的机构设备基于该机构管理的各所述资产账户与预定的秘钥交换协议及所述第一公钥，并按照该秘钥交换协议生成各所述资产账户对应的加法同态秘钥，利用对应的加法同态秘钥对各资产账户的余额进行加密，通过区块链的智能合约将加密后的余额广播至该区块链的各节点；

本实施例中，每一资产账户与预定的秘钥交换协议相对应，每一资产账户与预定的秘钥交换协议两者具有一对应的公私钥组，机构方的机构设备基于各资产账户与预定的秘钥交换协议（例如，Diffie-Hellman 协议，国密 SM2 协议）对应的公私钥组及监管方的第一公钥，并按照该秘钥交换协议生成各资产账户对应的加法同态秘钥，具体地，首先获取公私钥组，然后获取公私钥组中的私钥，基于该私钥及监管方的第一公钥并按照该秘钥交换协议生成各资产账户对应的加法同态秘钥。

其中，加法同态秘钥用作同态加密的加解密秘钥，该加法同态秘钥为对称秘钥（即发送和接收数据的双方必使用相同的秘钥对明文进行加密和解密运算）。

机构方利用对应的加法同态秘钥对各资产账户的余额进行加密，例如，若一个用户或者机构在一个需监管的资产种类下有两个账户 b1 和 b2，则 b1 账户的余额利用 b1 账户对应的加法同态秘钥进行加密；b2 账户的余额利用 b2 账户对应的加法同态秘钥进行加密。最后，机构方将自己在需监管的资产种类下的各个账户进行同态加密后的余额通过区块链的智能合约通知至该区块链的各节点，具体地，将进行同态加密后的余额通过区块链的智能合约写到该区块链的各个节点上的共享资产账本上。

其中，各资产账户的余额进行同态加密后，只有拥有加法同态秘钥的监管方及资产拥有方可以知晓对应的资产账户的余额。该资产账户可作为老用户，与下述的新用户对应。

步骤 S3，在机构方发起交易时，机构设备将交易方进行交易的新账户的余额通过对应的加法同态秘钥进行加密，通过区块链的智能合约将加密后的新账户余额广播至该区块链的各节点。

本实施例中，用户或者机构可以创建新的资产账户进行交易，所创建的新的资产账户称为本实施例中的新账户，例如：在交易时，银行 X 把账号 001 上的 100 张票据变成 400 张，其可以在一个 002 账号并放上 400 余额，然后再创建一个新的 003 账号上存 -300。002 账号为账户余额经过同态加密后的资产账户，为上述的老账户，则 003 账号为新账户，其账户余额也经过同态加密。

本实施例中，该区块链中的一个用户或者机构发起在上述的资产种类下的交易时，例如，A 转账给 B，该用户或机构把各个交易方进行交易的新账户的余额通过对应的各个交易方的资产账户加法同态秘钥进行同态加密，通过智能合约将各个交易方进行交易的同态加密后的新账户余额广播到该区块链的各个节点上，以便该区块链的各个节点上的其他用户或者机构能够知晓该交易（但无法知晓进行交易的新账户的余额）。

步骤 S4，在监管方查看交易方的新账户的余额时，获取所述新账户对应的公私钥组中的公钥，基于监管方与预定的秘钥交换协议对应的监管私钥及所述公私钥组中的公钥，并按照该秘钥交换协议生成加法同态秘钥，利用生成的加法同态秘钥解密所述加密后的新账户余额。

监管方需要查看一个交易方的新账户的余额时，则监管方获取该交易方的新账户对应的公私钥组中的公钥，例如，通过智能合约获取广播来的该交易方的账户对应的公私钥组中的公钥，或者，该公钥本身就是对应的账户号的预先确定的部分（例如，该公钥可以是对应的账户号的第 N1—N2 号码段，N1 和 N2 均为大于 0 的自然数），利用监管方与预定的秘钥交换协议两者对应的监管私钥及账户对应的公私钥组中的公钥，并按照该秘钥交换协议生成加法同态秘钥，该生成的加法同态秘钥能够解密账户加密后的新账户余额。

与现有技术相比，本实施例通过秘钥交换协议生成资产拥有方与监管方共同拥有的对称秘钥（即加法同态秘钥），用该对称秘钥作为加法同态加密的加解密秘钥，这样监管方可以解密加密后的账户余额，其他无关方无法知晓该账户的实际余额，有效保障了账户安全性及对账户进行监管，并可提高交易处理的效率；另外，通过在区块链智能合约上部署监管方公钥及公开的秘钥交换协议参数，这样拥有或即将拥有该资产的用户可以根据监管方公钥及公开的秘钥交换协议参数生成只有该用户与监管方共有的同态加密秘钥，这样，在保证账户隐私性的同时，可以为不同智能合约上的不同类型资产设定不同的监管方，区块链的业务兼容性和业务扩展便捷性得到了很大的提升。

在一优选地实施例中，如图 3 所示，步骤 S3 和 S4 可以分别替换为如下步骤 S10 和 S11:

S10，在机构方发起交易时，机构设备将交易方进行交易的资产账户的新余额通过对应的加法同态秘钥进行加密，通过区块链的智能合约将加密后的新余额广播至该区块链的各节点的智能合约上;

S11，在监管方查看交易方对应的资产账户的新余额时，获取所述资产账户对应的公私钥组中的公钥，基于监管方与预定的秘钥交换协议对应的监管私钥及所述公私钥组中的公钥，并按照该秘钥交换协议生成加法同态秘钥，利用生成的加法同态秘钥解密所述加密后的新余额。

该实施例与图 1 所示的实施例的区别在于，在该实施例中，交易方并未创建新的资产账户进行交易，而是使用已有的老账户进行交易，此时，进行交易后的账户余额相对于原余额而言即为新余额。该实施例中，对新余额的

加密过程及解密过程等与图 1 所示的实施例一致，在此不再赘述。

在一优选的实施例中，如图 4 所示，在上述图 2 的实施例的基础上，所述步骤 S3 之后还包括:

步骤 S5，当区块链的节点接收到广播的各所述交易方对应的加密后的新账户余额后，启动各节点对应的智能合约进行合数验证;

步骤 S6，若各节点对应的智能合约分别对各所述交易方对应的加密后的新账户余额的合数验证通过，则各节点对应的智能合约基于各所述交易方对应的加密后的新账户余额进行数据更新;

步骤 S7，若有节点对应的智能合约对所述交易方对应的加密后的新账户余额的合数验证不通过，则向各参与合数验证的节点发送合数验证失败的通知，或者，向区块链上的所有节点发送合数验证失败的通知。

本实施例中，合数验证即验证交易前的所有节点的余额之和是否等于交易之后的所有节点的余额之和，例如: 存在有效算法 ，使得 E(x+y)=E(x)⊕E(y)或者 x+y=D(E(x)⊕E(y))成立，该有效算法 即为加法同态加密验证算法，这个算法在验证账户合数的同时，并不泄漏账户的余额 x 和 y。

若各节点对应的智能合约分别对各交易方对应的加密后的新账户余额的合数验证通过，则各节点对应的智能合约基于各交易方对应的加密后的新账户余额进行数据更新; 若有节点对应的智能合约对交易方对应的加密后的新账户余额的合数验证不通过，则向各参与合数验证的节点发送合数验证失败的通知，或者，向区块链上的所有节点发送合数验证失败的通知。

在一优选的实施例中，如图 5 所示，在上述图 4 的实施例的基础上，所述步骤 S5 之后还包括:

步骤 S8，在监管方解密所述加密后的新账户余额后，启用负数余额验证系统对各所述交易方对应的解密后的新账户余额进行负数余额验证;

步骤 S9，若有资产账户未通过负数余额检验，则监管方将未通过负数余额检验的账户向除对应的异常节点外的其他节点进行通知，和/或，若有资产账户未通过负数余额检验，则监管方通过区块链权限管理系统取消未通过负数余额检验的账户在区块链上的交易权限。

本实施例中，由于同一个节点参与每次交易的账户和发生额是被记载在案的，所以通过虚假余额检验可以有效防止用户在某个节点通过分账户分摊余额的形式改变某个分账户的余额，从而规避合数验证的校验，例如，用户可以通过制造存有负数的账号来骗过验证: 银行 X 把账号 001 上的 100 张票据变成 400 张: 他可以创建一个 002 账号并放上 400 余额，然后再在一个新的 003 账号上存 -300，因此，需要进行负数余额验证。（注: 负数在密码使用时一般是因为取摸（mod）溢出造成的， 如当摸是 300 时，400 mod 300 就变成了 100）

如果各节点对应的智能合约分别对各交易方对应的加密后的新账户余

额的合数验证通过，监管方对各个交易方对应的加密后的新账户余额进行解密，并在解密完毕后，启用负数余额验证系统对各个交易方对应的解密后的新账户余额进行负数余额验证，若有账户未通过负数余额检验，则监管方确定该账户，并将该账户的异常状况向除异常区块链节点外的其他节点进行通知，和/或，若有账户未通过负数余额检验，则监管方通过区块链权限管理系统取消异常账户在区块链上的交易权限。

如图 6 所示，图 6 为本发明基于区块链的安全交易系统一实施例的结构示意图，该系统包括写入模块 101、第一加密模块 107、第二加密模块 108 及解密模块 102。

写入模块 101，用于将数字证书写入与需监管的资产种类对应的区块链的智能合约中，以供所有在所述资产种类下拥有资产账户的机构通过所述数字证书获取所述监管方的第一公钥。

本实施例中，监管方将 CA（Certification Authority，证书认证机构）颁发给自身的数字证书写入与需监管的资产种类对应的区块链的智能合约中，资产种类包括多种，例如，按耗用期限的长短，可分为流动资产和长期资产，根据具体形态，长期资产还可以作进一步的分类；按是否有实体形态，可分为有形资产和无形资产。或者综合几种分类标准，可将资产分为流动资产、长期投资、固定资产、无形资产、递延资产等类别。从这些资产类别中选择需要监管的资产种类。

监管方将数字证书写入与需监管的资产种类对应的区块链的智能合约后，所有在需监管的资产种类下拥有资产账户的用户或机构（例如，金融机构、基金机构等）可以通过智能合约中写入的数字证书来获取监管方的第一公钥，该第一公钥供同态加密使用。

另外，在监管方将数字证书写入与需监管的资产种类对应的区块链的智能合约之前，证书认证机构基于监管方与预先确定的秘钥交换协议对应的第一公钥进行签名，以生成数字证书，并颁发给监管方。

第一加密模块 107，用于基于当前机构管理的各所述资产账户与预定的秘钥交换协议及所述第一公钥，并按照该秘钥交换协议生成各所述资产账户对应的加法同态秘钥，利用对应的加法同态秘钥对各资产账户的余额进行加密，通过区块链的智能合约将加密后的余额广播至该区块链的各节点。

本实施例中，第一加密模块 107 可以设置于机构方的机构设备上。由于每一资产账户与预定的秘钥交换协议相对应，每一资产账户与预定的秘钥交换协议两者具有一对应的公私钥组，机构方的机构设备基于各资产账户与预定的秘钥交换协议（例如，Diffie-Hellman 协议，国密 SM2 协议）对应的公私钥组及监管方的第一公钥，并按照该秘钥交换协议生成各资产账户对应的加法同态秘钥，具体地，首先获取公私钥组，然后获取公私钥组中的私钥，基于该私钥及监管方的第一公钥并按照该秘钥交换协议生成各资产账户对应的加法同态秘钥。

其中，加法同态秘钥用作同态加密的加解密秘钥，该加法同态秘钥为对

称秘钥（即发送和接收数据的双方必使用相同的秘钥对明文进行加密和解密运算）。

机构方利用对应的加法同态秘钥对各资产账户的余额进行加密，例如，若一个用户或者机构在一个需监管的资产种类下有两个账户 b1 和 b2，则 b1 账户的余额利用 b1 账户对应的加法同态秘钥进行加密；b2 账户的余额利用 b2 账户对应的加法同态秘钥进行加密。最后，机构方将自己在需监管的资产种类下的各个账户进行同态加密后的余额通过区块链的智能合约通知至该区块链的各节点，具体地，将进行同态加密后的余额通过区块链的智能合约写到该区块链的各个节点上的共享资产账本上。

其中，各资产账户的余额进行同态加密后，只有拥有加法同态秘钥的监管方及资产拥有方可以知晓对应的资产账户的余额。该资产账户可作为老用户，与下述的新用户对应。

第二加密模块 108，用于在机构方发起交易时，将交易方进行交易的新账户的余额通过对应的加法同态秘钥进行加密，通过区块链的智能合约将加密后的新账户余额广播至该区块链的各节点。

本实施例中，用户或者机构可以创建新的资产账户进行交易，所创建的新的资产账户称为本实施例中的新账户，例如：在交易时，银行 X 把账号 001 上的 100 张票据变成 400 张，其可以在一个 002 账号并放上 400 余额，然后再创建一个新的 003 账号上存 -300。002 账号为账户余额经过同态加密后的资产账户，为上述的老账户，则 003 账号为新账户，其账户余额也经过同态加密。

本实施例中，第二加密模块 108 设置于机构方的机构设备上。当该区块链中的一个用户或者机构发起在上述的资产种类下的交易时，例如，A 转账给 B，该用户或机构把各个交易方进行交易的新账户的余额通过对应的各个交易方的资产账户加法同态秘钥进行同态加密，通过智能合约将各个交易方进行交易的同态加密后的新账户余额广播到该区块链的各个节点上，以便该区块链的各个节点上的其他用户或者机构能够知晓该交易（但无法知晓进行交易的新账户的余额）。

解密模块 102，用于在监管方查看交易方的新账户余额时，获取所述新账户对应的公私钥组中的公钥，基于监管方与预定的秘钥交换协议对应的监管私钥及所述公私钥组中的公钥，并按照该秘钥交换协议生成加法同态秘钥，利用生成的加法同态秘钥解密所述加密后的新账户余额。

本实施例中，用户或者机构可以创建新的资产账户进行交易，所创建的新的资产账户称为本实施例中的新账户，例如：在交易时，银行 X 把账号 001 上的 100 张票据变成 400 张，其可以在一个 002 账号并放上 400 余额，然后再创建一个新的 003 账号上存 -300。002 账号为账户余额经过同态加密后的资产账户，为上述的老账户，则 003 账号为新账户，其账户余额也经过同态加密。

监管方需要查看一个交易方的新账户的余额时，则监管方获取该交易方

的新账户对应的公私钥组中的公钥，例如，通过智能合约获取广播来的该交易方的新账户对应的公私钥组中的公钥，或者，该公钥本身就是对应的账户号的预先确定的部分（例如，该公钥可以是对应的账户号的第 N1—N2 号码段，N1 和 N2 均为大于 0 的自然数），利用监管方与预定的秘钥交换协议两者对应的监管私钥及该公钥，并按照该秘钥交换协议生成加法同态秘钥，该生成的加法同态秘钥能够解密新账户余额。

在一优选的实施例中，在进行交易时，交易方也可使用已有账户进行交易而非创建新账户进行交易，此时，第二加密模块 108 所加密的余额可以是已有账户在交易完成后的新余额，而解密模块 102 所解密的余额相应地为已有账户在交易完成后的新余额。该实施例中，第二加密模块 108 对新余额的加密过程及解密模块 102 对新余额的解密过程等与图 5 所示的实施例一致，在此不再赘述。

在一优选的实施例中，如图 7 所示，在上述图 6 的实施例的基础上，上述系统还包括:

第一验证模块 103，用于当区块链的节点接收到广播的各所述交易方对应的加密后的新账户余额后，启动各节点对应的智能合约进行合数验证;

更新模块 104，用于若各节点对应的智能合约分别对各所述交易方对应的加密后的新账户余额的合数验证通过，则各节点对应的智能合约基于各所述交易方对应的加密后的新账户余额进行数据更新。

本实施例中，合数验证即验证交易前的所有节点的余额之和是否等于交易之后的所有节点的余额之和，例如：存在有效算法 ，使得 $E(x+y)=E(x)\oplus E(y)$或者 $x+y=D(E(x)\oplus E(y))$成立，该有效算法 即为加法同态加密验证算法，这个算法在验证账户合数的同时，并不泄漏账户的余额 x 和 y。

若各节点对应的智能合约分别对各交易方对应的加密后的新账户余额的合数验证通过，则各节点对应的智能合约基于各交易方对应的加密后的新账户余额进行数据更新。

优选地，还包括发送模块，用于若有节点对应的智能合约对所述交易方对应的加密后的新账户余额的合数验证不通过，则向各参与合数验证的节点发送合数验证失败的通知，或者，向区块链上的所有节点发送合数验证失败的通知。

在一优选的实施例中，如图 8 所示，在上述图 7 的实施例的基础上，上述系统还包括:

第二验证模块 105，用于在监管方解密所述新账户加密后的新账户余额后，启用负数余额验证系统对各所述交易方对应的解密后的新账户余额进行负数余额验证;

处理模块 106，用于若有资产账户未通过负数余额检验，则监管方将未通过负数余额检验的账户向除对应的异常节点外的其他节点进行通知，和/或，若有资产账户未通过负数余额检验，则监管方通过区块链权限管理系统

取消未通过负数余额检验的账户在区块链上的交易权限。

本实施例中，由于同一个节点参与每次交易的账户和发生额是被记载在案的，所以通过虚假余额检验可以有效防止用户在某个节点通过分账户分摊余额的形式改变某个分账户的余额，从而规避合数验证的校验，例如，用户可以通过制造存有负数的账号来骗过验证：银行 X 把账号 001 上的 100 张票据变成 400 张：他可以创建一个 002 账号并放上 400 余额，然后再在一个新的 003 账号上存 -300，因此，需要进行负数余额验证。

如果各节点对应的智能合约分别对各交易方对应的加密后的新账户余额的合数验证通过，监管方对各个交易方对应的加密后的新账户余额进行解密，并在解密完毕后，启用负数余额验证系统对各个交易方对应的解密后的新账户余额进行负数余额验证，若有账户未通过负数余额检验，则监管方确定该账户，并将该账户的异常状况向除异常区块链节点外的其他节点进行通知，和/或，若有账户未通过负数余额检验，则监管方通过区块链权限管理系统取消异常账户在区块链上的交易权限。

以上所述仅为本发明的较佳实施例，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

权 利 要 求 书

1. 一种基于区块链的安全交易方法，其特征在于，所述基于区块链的安全交易方法包括:

S1，监管方将数字证书写入与需监管的资产种类对应的区块链的智能合约中，以供所有在所述资产种类下拥有资产账户的机构通过所述数字证书获取所述监管方的第一公钥;

S2，机构方的机构设备基于该机构管理的各所述资产账户对应的公私钥组与预定的秘钥交换协议及所述第一公钥，并按照该秘钥交换协议生成各所述资产账户对应的加法同态秘钥，利用对应的加法同态秘钥对各资产账户的余额进行加密，通过区块链的智能合约将加密后的余额广播至该区块链的各节点的智能合约上;

S3，在机构方发起交易时，机构设备将交易方进行交易的新账户的余额通过对应的加法同态秘钥进行加密，通过区块链的智能合约将加密后的新账户余额广播至该区块链的各节点的智能合约上;

S4，在监管方查看交易方的新账户的余额时，获取所述新账户对应的公私钥组中的公钥，基于监管方与预定的秘钥交换协议对应的监管私钥及所述公私钥组中的公钥，并按照该秘钥交换协议生成加法同态秘钥，利用生成的加法同态秘钥解密所述加密后的新账户余额。

2. 根据权利要求 1 所述的基于区块链的安全交易方法，其特征在于，所述步骤 S4 和 S5 可以被替换为:

S10，在机构方发起交易时，机构设备将交易方进行交易的资产账户的新余额通过对应的加法同态秘钥进行加密，通过区块链的智能合约将加密后的新余额广播至该区块链的各节点的智能合约上;

S11，在监管方查看交易方对应的资产账户的新余额时，获取所述账户对应的公私钥组中的公钥，基于监管方与预定的秘钥交换协议对应的监管私钥及所述公私钥组中的公钥，并按照该秘钥交换协议生成加法同态秘钥，利用生成的加法同态秘钥解密所述加密后的新余额。

3. 根据权利要求 1 所述的基于区块链的安全交易方法，其特征在于，所述数字证书由证书认证机构基于所述监管方与预先确定的秘钥交换协议对应的第一公钥进行签名后生成，并颁发给监管方。

4. 根据权利要求 2 或 3 所述的基于区块链的安全交易方法，其特征在于，所述步骤 S3 之后还包括:

S5，当区块链的节点接收到广播的各所述交易方对应的加密后的新账户余额后，启动各节点对应的智能合约进行合数验证;

S6，若各节点对应的智能合约分别对各所述交易方对应的加密后的新账户后余额的合数验证通过，则各节点对应的智能合约基于各所述交易方对应的加密后的新账户余额进行数据更新。

5. 根据权利要求 4 所述的基于区块链的安全交易方法，其特征在于，

所述步骤 S5 之后还包括:

S7，若有节点对应的智能合约对所述交易方对应的加密后的新账户余额的合数验证不通过，则向各参与合数验证的节点发送合数验证失败的通知，或者，向区块链上的所有节点发送合数验证失败的通知。

6. 根据权利要求 4 所述的基于区块链的安全交易方法，其特征在于，所述步骤 S6 之后还包括:

S8，在监管方解密所述账户加密后的新账户余额后，启用负数余额验证系统对各所述交易方对应的解密后的新账户余额进行负数余额验证;

S9，若有资产账户未通过负数余额检验，则监管方将未通过负数余额检验的账户向除对应的异常节点外的其他节点进行通知，和/或，若有资产账户未通过负数余额检验，则监管方通过区块链权限管理系统取消未通过负数余额检验的账户在区块链上的交易权限。

7. 一种电子装置，其特征在于，所述电子装置包括存储器及与所述存储器连接的处理器，所述存储器中存储有可在所述处理器上运行的基于区块链的安全交易系统，所述基于区块链的安全交易系统被所述处理器执行时实现如下步骤:

S1，监管方将数字证书写入与需监管的资产种类对应的区块链的智能合约中，以供所有在所述资产种类下拥有资产账户的机构通过所述数字证书获取所述监管方的第一公钥;

S2，机构方的机构设备基于该机构管理的各所述资产账户对应的公私钥组与预定的秘钥交换协议及所述第一公钥，并按照该秘钥交换协议生成各所述资产账户对应的加法同态秘钥，利用对应的加法同态秘钥对各资产账户的余额进行加密，通过区块链的智能合约将加密后的余额广播至该区块链的各节点的智能合约上;

S3，在机构方发起交易时，机构设备将交易方进行交易的新账户的余额通过对应的加法同态秘钥进行加密，通过区块链的智能合约将加密后的新账户余额广播至该区块链的各节点的智能合约上;

S4，在监管方查看交易方的新账户的余额时，获取所述新账户对应的公私钥组中的公钥，基于监管方与预定的秘钥交换协议对应的监管私钥及所述公私钥组中的公钥，并按照该秘钥交换协议生成加法同态秘钥，利用生成的加法同态秘钥解密所述加密后的新账户余额。

8. 根据权利要求 7 所述的电子装置，其特征在于，所述步骤 S4 和 S5 可以被替换为:

S10，在机构方发起交易时，机构设备将交易方进行交易的资产账户的新余额通过对应的加法同态秘钥进行加密，通过区块链的智能合约将加密后的新余额广播至该区块链的各节点的智能合约上;

S11，在监管方查看交易方对应的资产账户的新余额时，获取所述账户对应的公私钥组中的公钥，基于监管方与预定的秘钥交换协议对应的监管私钥及所述公私钥组中的公钥，并按照该秘钥交换协议生成加法同态秘钥，利

用生成的加法同态秘钥解密所述加密后的新余额。

9. 根据权利要求 7 所述的基于区块链的电子装置，其特征在于，所述数字证书由证书认证机构基于所述监管方与预先确定的秘钥交换协议对应的第一公钥进行签名后生成，并颁发给监管方。

10. 根据权利要求 8 或 9 所述的电子装置，其特征在于，所述基于区块链的安全交易系统被所述处理器执行时，还实现如下步骤:

S5，当区块链的节点接收到广播的各所述交易方对应的加密后的新账户余额后，启动各节点对应的智能合约进行合数验证;

S6，若各节点对应的智能合约分别对各所述交易方对应的加密后的新账户后余额的合数验证通过，则各节点对应的智能合约基于各所述交易方对应的加密后的新账户余额进行数据更新。

11. 根据权利要求 10 所述的电子装置，其特征在于，所述基于区块链的安全交易系统被所述处理器执行时，还实现如下步骤:

S7，若有节点对应的智能合约对所述交易方对应的加密后的新账户余额的合数验证不通过，则向各参与合数验证的节点发送合数验证失败的通知，或者，向区块链上的所有节点发送合数验证失败的通知。

12. 根据权利要求 10 所述的电子装置，其特征在于，所述基于区块链的安全交易系统被所述处理器执行时，还实现如下步骤:

S8，在监管方解密所述账户加密后的新账户余额后，启用负数余额验证系统对各所述交易方对应的解密后的新账户余额进行负数余额验证;

S9，若有资产账户未通过负数余额检验，则监管方将未通过负数余额检验的账户向除对应的异常节点外的其他节点进行通知，和/或，若有资产账户未通过负数余额检验，则监管方通过区块链权限管理系统取消未通过负数余额检验的账户在区块链上的交易权限。

13. 一种基于区块链的安全交易系统，其特征在于，所述系统包括写入模块、第一加密模块、第二加密模块及解密模块，其中:

所述写入模块，用于将数字证书写入与需监管的资产种类对应的区块链的智能合约中，以供所有在所述资产种类下拥有资产账户的机构通过所述数字证书获取所述监管方的第一公钥;

所述第一加密模块，用于基于当前机构管理的各所述资产账户对应的公私钥组中的私钥与预定的秘钥交换协议及所述第一公钥，并按照该秘钥交换协议生成各所述资产账户对应的加法同态秘钥，利用对应的加法同态秘钥对各资产账户的余额进行加密，通过区块链的智能合约将加密后的余额广播至该区块链的各节点的智能合约上;

所述第二加密模块，用于在机构方发起交易时，将交易方进行交易的新账户的余额通过对应的加法同态秘钥进行加密，通过区块链的智能合约将加密后的新账户余额广播至该区块链的各节点的智能合约上；以及，

所述解密模块，用于在监管方查看交易方的账户的新账户余额时，获取所述新账户对应的公私钥组中的公钥，基于监管方与预定的秘钥交换协议对

应的监管私钥及所述公私钥组中的公钥，并按照该秘钥交换协议生成加法同态秘钥，利用生成的加法同态秘钥解密所述账户加密后的新账户余额。

14. 根据权利要求 13 所述的系统，其特征在于，所述系统还包括:

第一验证模块，用于当区块链的节点接收到广播的各所述交易方对应的加密后的新账户余额后，启动各节点对应的智能合约进行合数验证;

更新模块，用于若各节点对应的智能合约分别对各所述交易方对应的加密后的新账户余额的合数验证通过，则各节点对应的智能合约基于各所述交易方对应的加密后的新账户余额进行数据更新。

15. 一种计算机可读存储介质，其特征在于，所述计算机可读存储介质上存储有基于区块链的安全交易系统，所述基于区块链的安全交易系统被处理器执行时实现以下步骤:

S1，监管方将数字证书写入与需监管的资产种类对应的区块链的智能合约中，以供所有在所述资产种类下拥有资产账户的机构通过所述数字证书获取所述监管方的第一公钥;

S2，机构方的机构设备基于该机构管理的各所述资产账户对应的公私钥组与预定的秘钥交换协议及所述第一公钥，并按照该秘钥交换协议生成各所述资产账户对应的加法同态秘钥，利用对应的加法同态秘钥对各资产账户的余额进行加密，通过区块链的智能合约将加密后的余额广播至该区块链的各节点的智能合约上;

S3，在机构方发起交易时，机构设备将交易方进行交易的新账户的余额通过对应的加法同态秘钥进行加密，通过区块链的智能合约将加密后的新账户余额广播至该区块链的各节点的智能合约上;

S4，在监管方查看交易方的新账户的余额时，获取所述新账户对应的公私钥组中的公钥，基于监管方与预定的秘钥交换协议对应的监管私钥及所述公私钥组中的公钥，并按照该秘钥交换协议生成加法同态秘钥，利用生成的加法同态秘钥解密所述加密后的新账户余额。

16. 根据权利要求 15 所述的计算机可读存储介质，其特征在于，所述步骤 S4 和 S5 可以被替换为:

S10，在机构方发起交易时，机构设备将交易方进行交易的资产账户的新余额通过对应的加法同态秘钥进行加密，通过区块链的智能合约将加密后的新余额广播至该区块链的各节点的智能合约上;

S11，在监管方查看交易方对应的资产账户的新余额时，获取所述账户对应的公私钥组中的公钥，基于监管方与预定的秘钥交换协议对应的监管私钥及所述公私钥组中的公钥，并按照该秘钥交换协议生成加法同态秘钥，利用生成的加法同态秘钥解密所述加密后的新余额。

17. 根据权利要求 15 所述的计算机可读存储介质，其特征在于，所述数字证书由证书认证机构基于所述监管方与预先确定的秘钥交换协议对应的第一公钥进行签名后生成，并颁发给监管方。

18. 根据权利要求 16 或 17 所述的计算机可读存储介质，其特征在于，

所述基于区块链的安全交易系统被所述处理器执行时，还实现如下步骤：

S5，当区块链的节点接收到广播的各所述交易方对应的加密后的新账户余额后，启动各节点对应的智能合约进行合数验证；

S6，若各节点对应的智能合约分别对各所述交易方对应的加密后的新账户后余额的合数验证通过，则各节点对应的智能合约基于各所述交易方对应的加密后的新账户余额进行数据更新。

19. 根据权利要求 18 所述的计算机可读存储介质，其特征在于，所述基于区块链的安全交易系统被所述处理器执行时，还实现如下步骤：

S7，若有节点对应的智能合约对所述交易方对应的加密后的新账户余额的合数验证不通过，则向各参与合数验证的节点发送合数验证失败的通知，或者，向区块链上的所有节点发送合数验证失败的通知。

20. 根据权利要求 18 所述的计算机可读存储介质，其特征在于，所述基于区块链的安全交易系统被所述处理器执行时，还实现如下步骤：

S8，在监管方解密所述账户加密后的新账户余额后，启用负数余额验证系统对各所述交易方对应的解密后的新账户余额进行负数余额验证；

S9，若有资产账户未通过负数余额检验，则监管方将未通过负数余额检验的账户向除对应的异常节点外的其他节点进行通知，和/或，若有资产账户未通过负数余额检验，则监管方通过区块链权限管理系统取消未通过负数余额检验的账户在区块链上的交易权限。

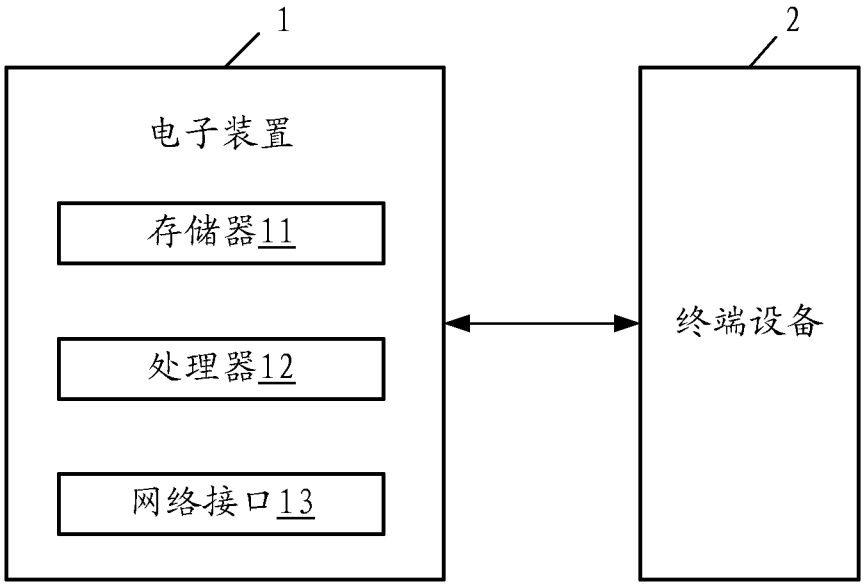
1
2
电子装置
存储器11
处理器12
网络接口13
终端设备

图 1

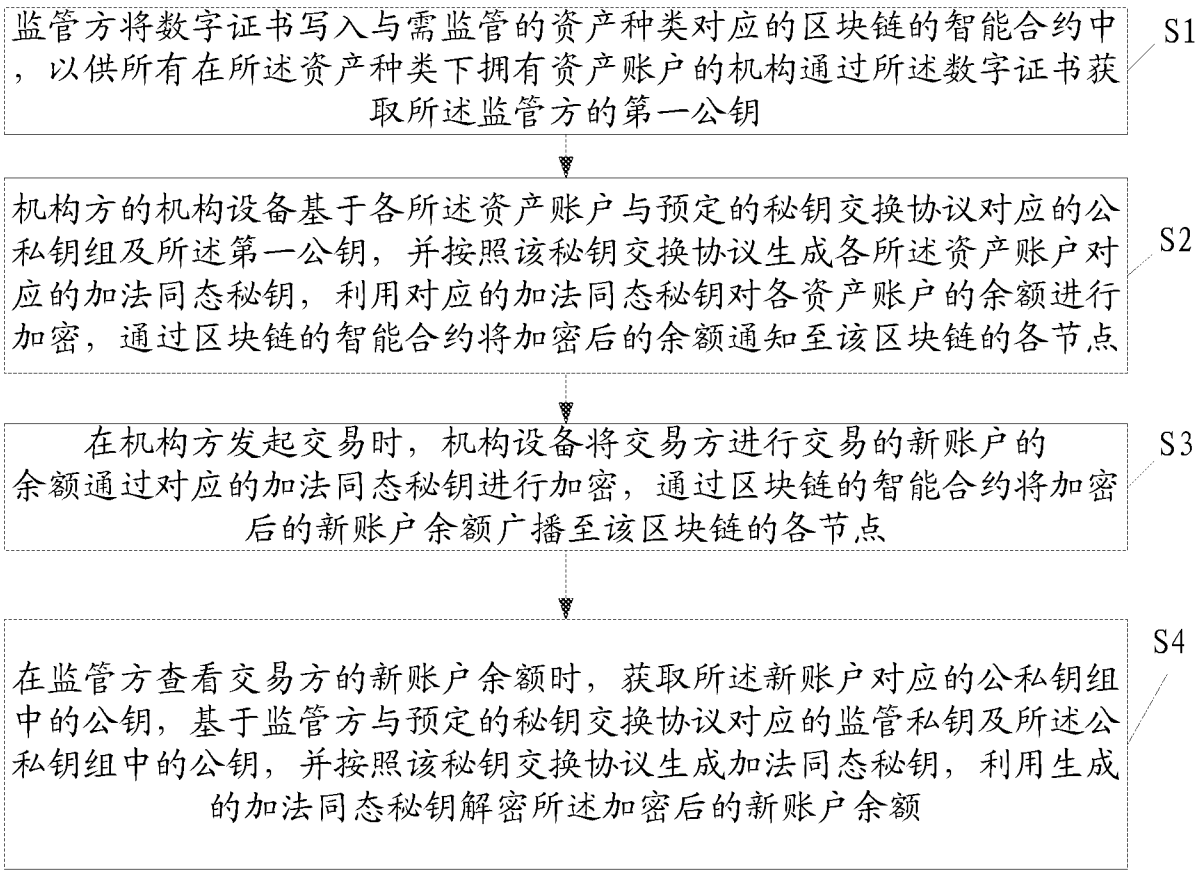
监管方将数字证书写入与需监管的资产种类对应的区块链的智能合约中，以供所有在所述资产种类下拥有资产账户的机构通过所述数字证书获取所述监管方的第一公钥
S1
机构方的机构设备基于各所述资产账户与预定的秘钥交换协议对应的公私钥组及所述第一公钥，并按照该秘钥交换协议生成各所述资产账户对应的加法同态秘钥，利用对应的加法同态秘钥对各资产账户的余额进行加密，通过区块链的智能合约将加密后的余额通知至该区块链的各节点
S2
在机构方发起交易时，机构设备将交易方进行交易的新账户的余额通过对应的加法同态秘钥进行加密，通过区块链的智能合约将加密后的新账户余额广播至该区块链的各节点
S3
在监管方查看交易方的新账户余额时，获取所述新账户对应的公私钥组中的公钥，基于监管方与预定的秘钥交换协议对应的监管私钥及所述公私钥组中的公钥，并按照该秘钥交换协议生成加法同态秘钥，利用生成的加法同态秘钥解密所述加密后的新账户余额
S4

图 2

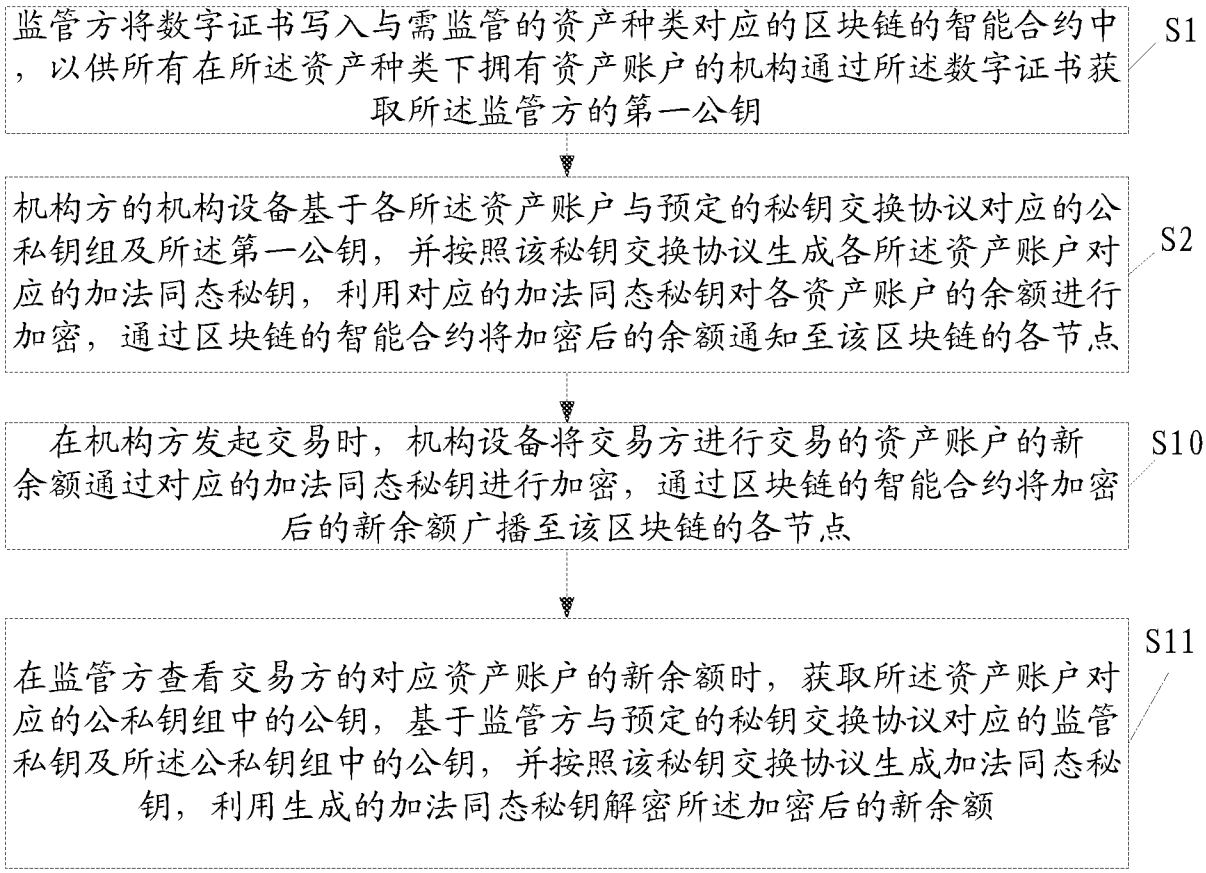
监管方将数字证书写入与需监管的资产种类对应的区块链的智能合约中，以供所有在所述资产种类下拥有资产账户的机构通过所述数字证书获取所述监管方的第一公钥
S1
机构方的机构设备基于各所述资产账户与预定的秘钥交换协议对应的公私钥组及所述第一公钥，并按照该秘钥交换协议生成各所述资产账户对应的加法同态秘钥，利用对应的加法同态秘钥对各资产账户的余额进行加密，通过区块链的智能合约将加密后的余额通知至该区块链的各节点
S2
在机构方发起交易时，机构设备将交易方进行交易的资产账户的新余额通过对应的加法同态秘钥进行加密，通过区块链的智能合约将加密后的新余额广播至该区块链的各节点
S10
在监管方查看交易方的对应资产账户的新余额时，获取所述资产账户对应的公私钥组中的公钥，基于监管方与预定的秘钥交换协议对应的监管私钥及所述公私钥组中的公钥，并按照该秘钥交换协议生成加法同态秘钥，利用生成的加法同态秘钥解密所述加密后的新余额
S11

图 3

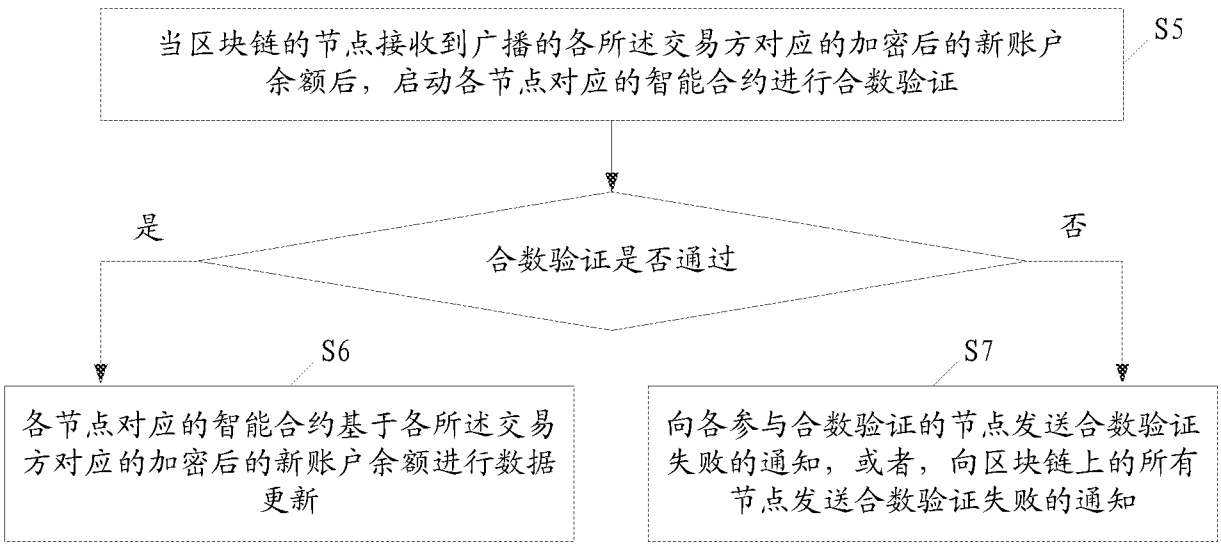
当区块链的节点接收到广播的各所述交易方对应的加密后的新账户余额后，启动各节点对应的智能合约进行合数验证
S5
合数验证是否通过
是
否
S6
各节点对应的智能合约基于各所述交易方对应的加密后的新账户余额进行数据更新
S7
向各参与合数验证的节点发送合数验证失败的通知，或者，向区块链上的所有节点发送合数验证失败的通知

图 4

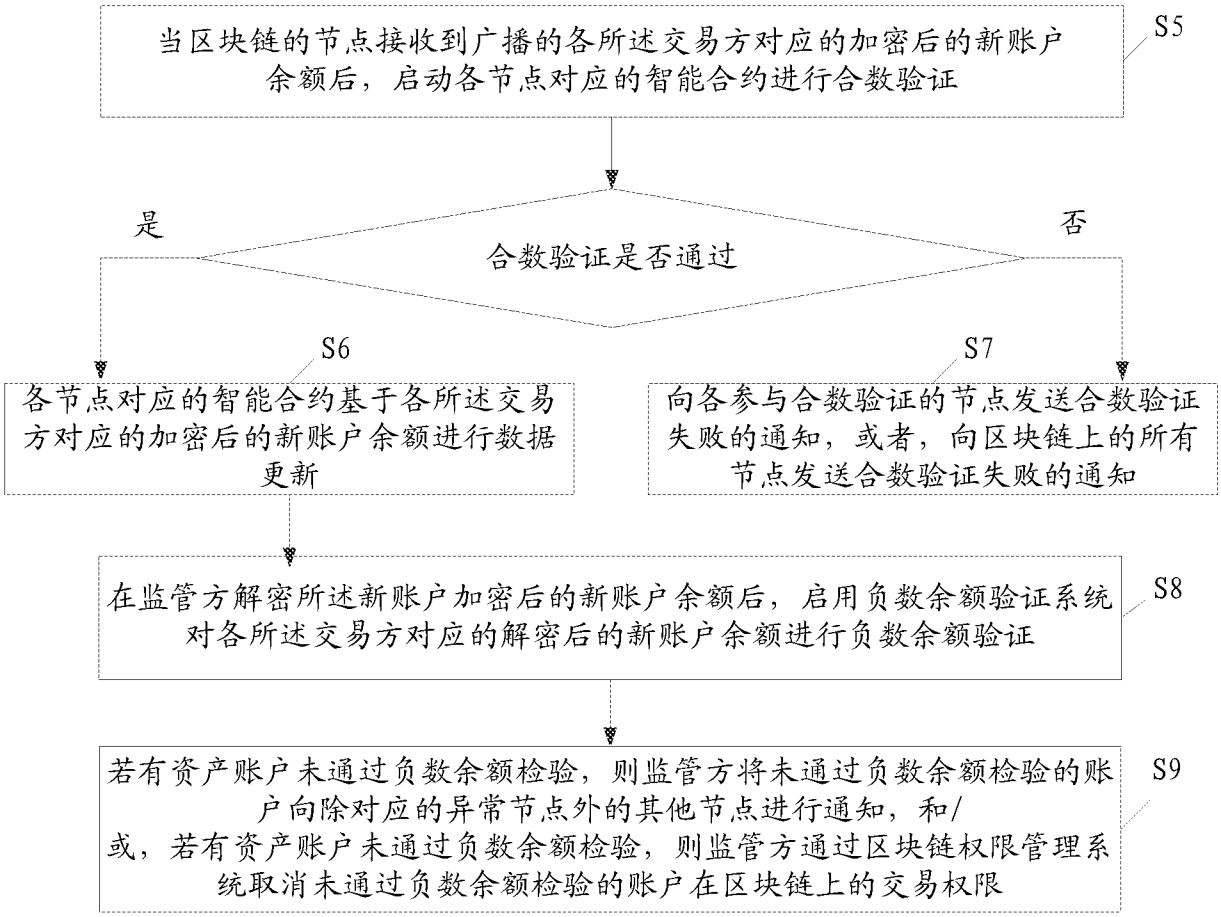
当区块链的节点接收到广播的各所述交易方对应的加密后的新账户余额后，启动各节点对应的智能合约进行合数验证
S5
合数验证是否通过
是
否
S6
各节点对应的智能合约基于各所述交易方对应的加密后的新账户余额进行数据更新
S7
向各参与合数验证的节点发送合数验证失败的通知，或者，向区块链上的所有节点发送合数验证失败的通知
在监管方解密所述新账户加密后的新账户余额后，启用负数余额验证系统对各所述交易方对应的解密后的新账户余额进行负数余额验证
S8
若有资产账户未通过负数余额检验，则监管方将未通过负数余额检验的账户向除对应的异常节点外的其他节点进行通知，和/
或，若有资产账户未通过负数余额检验，则监管方通过区块链权限管理系统取消未通过负数余额检验的账户在区块链上的交易权限
S9

图 5

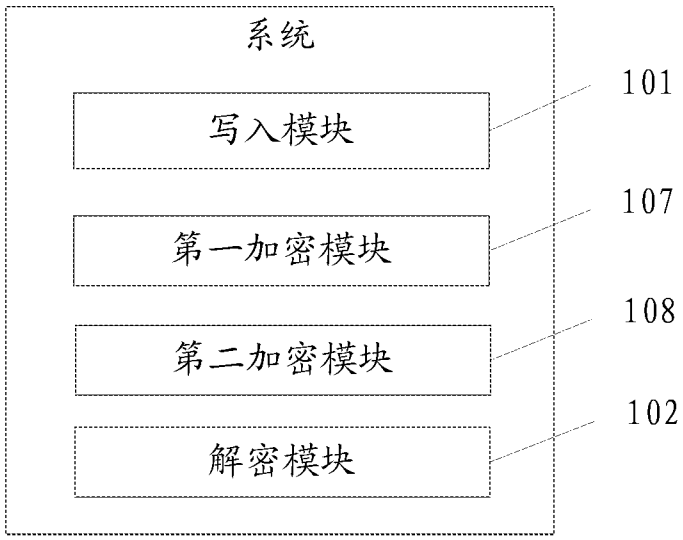
系统
写入模块
101
第一加密模块
107
第二加密模块
108
解密模块
102

图 6

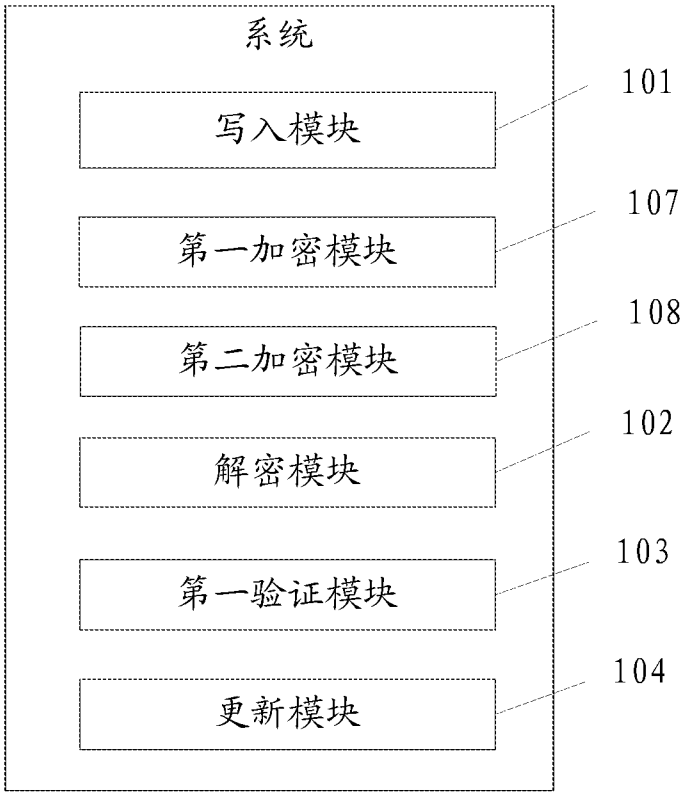
系统
写入模块
101
第一加密模块
107
第二加密模块
108
解密模块
102
第一验证模块
103
更新模块
104

图 7

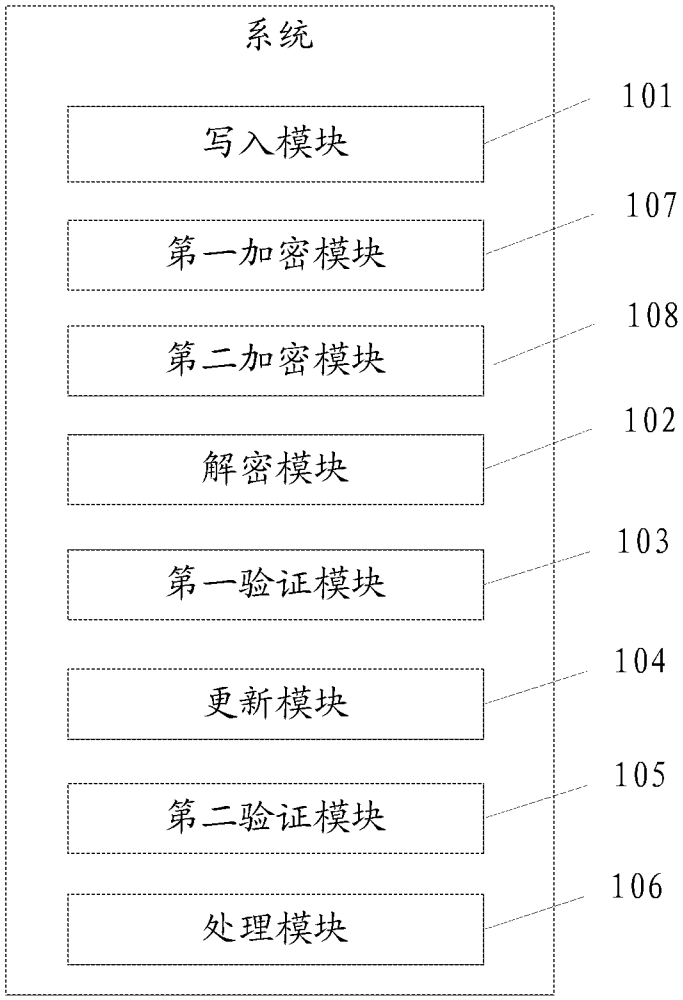
系统
写入模块
101
第一加密模块
107
第二加密模块
108
解密模块
102
第一验证模块
103
更新模块
104
第二验证模块
105
处理模块
106

图 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/091246

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/10 (2012.01) i; H04L 9/00 (2006.01) i; G06Q 20/38 (2012.01) n; H04L 9/32 (2006.01) n

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; H04L

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, GOOGLE: 区块链, 交易, 账户, 公钥, 余额, 广播, 监管, block, chain, transaction, account, public, key, balance, broadcast, supervision

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 106845960 A (SHANGHAI ACCOUNT BLOCK CHAIN TECHNOLOGY CO., LTD.), 13 June 2017 (13.06.2017), description, paragraphs [0005]-[0038]	1-20
A	CN 106097073 A (SHENZHEN TAOTAOGU INFORMATION TECHNOLOGY CO., LTD.), 09 November 2016 (09.11.2016), description, paragraphs [0006]-[0015]	1-20
A	CN 104751364 A (SHANGHAI F-ROAD COMMERCE SERVICE CO., LTD.), 01 July 2015 (01.07.2015), entire document	1-20
A	CN 102956000 A (CHINA MERCHANTS BANK CO., LTD.), 06 March 2013 (06.03.2013), entire document	1-20
A	CN 104717067 A (CHINA MOBILE GROUP LIAONING CO., LTD.), 17 June 2015 (17.06.2015), entire document	1-20
A	US 2002046335 A1 (BAUM-WAIDNER, B.), 18 April 2002 (18.04.2002), entire document	1-20

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 September 2017	19 October 2017
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer MA, Xin Telephone No. (86-10) 62414428

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/091246

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 106845960 A	13 June 2017	None	
CN 106097073 A	09 November 2016	None	
CN 104751364 A	01 July 2015	None	
CN 102956000 A	06 March 2013	None	
CN 104717067 A	17 June 2015	None	
US 2002046335 A1	18 April 2002	None	

国际检索报告

国际申请号
PCT/CN2017/091246

A. 主题的分类

G06Q 20/10(2012.01)i；H04L 9/00(2006.01)i；G06Q 20/38(2012.01)n；H04L 9/32(2006.01)n

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；H04L

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，EPODOC，CNPAT，CNKI，IEEE，GOOGLE： 区块链，交易，账户，公钥，余额，广播，监管，block， chain, transaction, account, public, key, balance, broadcast, supervision

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 106845960 A (上海亿账通区块链科技有限公司) 2017年 6月 13日 (2017-06-13) 说明书第[0005]-[0038]段	1-20
A	CN 106097073 A (深圳市淘淘谷信息技术有限公司) 2016年 11月 9日 (2016-11-09) 说明书第[0006]-[0015]段	1-20
A	CN 104751364 A (上海方付通商务服务有限公司) 2015年 7月 1日 (2015-07-01) 全文	1-20
A	CN 102956000 A (招商银行股份有限公司) 2013年 3月 6日 (2013-03-06) 全文	1-20
A	CN 104717067 A (中国移动通信集团辽宁有限公司) 2015年 6月 17日 (2015-06-17) 全文	1-20
A	US 2002046335 A1 (BAUM-WAIDNER, BIRGIT) 2002年 4月 18日 (2002-04-18) 全文	1-20

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2017年 9月 15日	2017年 10月 19日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	马鑫
传真号 (86-10)62019451	电话号码 (86-10)62414428

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2017/091246

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 106845960 A	2017年 6月 13日	无	
CN 106097073 A	2016年 11月 9日	无	
CN 104751364 A	2015年 7月 1日	无	
CN 102956000 A	2013年 3月 6日	无	
CN 104717067 A	2015年 6月 17日	无	
US 2002046335 A1	2002年 4月 18日	无	