(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 108711105 A
(43)申请公布日 2018.10.26

(21)申请号 201810470777.2

(22)申请日 2018.05.16

(71)申请人 四川吉鼎科技有限公司
地址 610000 四川省成都市天府新区华阳街道顺河街135号1层

(72)发明人 秦瑶

(51)Int.Cl.
G06Q 40/04(2012.01)
G06Q 20/38(2012.01)
G06Q 20/40(2012.01)

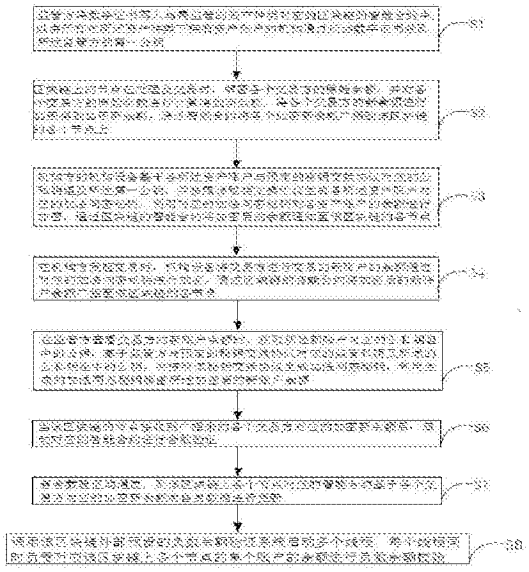
权利要求书3页 说明书12页 附图1页

(54)发明名称

一种基于区块链的安全交易验证方法及系统

(57)摘要

本发明公开了一种基于区块链的安全交易验证方法及系统，该方法包括：区块链上节点在处理带有交易类型和交易金额的交易时，通过交易方发送的第一解密参数解密各个交易方的原始余额，对各个原始余额进行计算得到新余额，将新余额通过交易方发来的加密参数加密得到加密新余额，将各加密新余额广播到该区块链各节点上；当该区块链的节点收到广播的各交易方的加密新余额后，启动智能合约进行合数验证；若合数验证均通过，则基于各对应的加密新余额更新；调用外部负数余额验证系统对单个账户余额进行负数余额检验，若负数余额检验均通过，则判定该交易验证通过。本发明既能验证交易是否正常，又能在不占用系统开销的情况下保证区块链上的交易处理速度。



CN 108711105 A

1.基于区块链的安全交易验证方法及系统,其特征在于:

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,区块链上的一个节点在处理一个带有交易类型和交易金额的交易时,该节点通过该交易的交易方发送来的第一解密参数解密各个所述交易方的原始余额,并基于所述交易类型和交易金额对各个所述交易方的原始余额进行计算得到对应的新余额,将各个所述交易方对应的新余额通过所述交易方发送来的加密参数进行加密得到加密新余额,通过智能合约将各个所述交易方对应的加密新余额广播到该区块链的各个节点上;

S4,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;

S5,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。

S6,当该区块链的节点接收到广播来的各个所述交易方对应的加密新余额后,启动对应的智能合约进行合数验证;

S7,若该区块链上各个节点对应的智能合约对各个所述交易方对应的加密新余额的合数验证通过,则该区块链上各个节点对应的智能合约基于各个所述交易方对应的加密新余额对自身数据进行更新;

S8,调用该区块链外部预设的负数余额验证系统启动多个线程,每个线程同时负责对该区块链上各个节点的单个账户的余额进行负数余额检验,若该区块链上各个节点的单个账户余额的负数余额检验通过,则判定该交易验证通过。

2.根据权利要求1所述的基于区块链的安全交易验证方法及系统,其特征在于,该方法还包括:

将第二解密参数通过该区块链的节点与该区块链上的监管方节点对应的秘钥进行加密,并将加密后的第二解密参数通过智能合约广播到该区块链上的监管方节点上,所述第二解密参数用于对各个所述交易方对应的加密新余额进行解密;

该区块链上的监管方节点读取更新过的各个所述交易方对应的加密新余额,并通过所述秘钥对加密后的第二解密参数进行解密,通过解密后的第二解密参数对各个所述交易方对应的加密新余额进行解密,并对解密后的各个新余额进行负数余额验证。

3.根据权利要求2所述的基于区块链的安全交易验证方法及系统,其特征在于,该方法还包括:

若有账户未通过负数余额检验,则所述监管方节点确定该账户对应的异常区块链节点,并将该账户的异常状况向除所述异常区块链节点外的其他节点进行通知。

4.根据权利要求2所述的基于区块链的安全交易验证方法及系统，其特征在于，该方法还包括：

若有账户未通过负数余额检验，则所述监管方节点确定该账户对应的异常区块链节点，并通过预设的区块链权限管理系统取消所述异常区块链节点在该区块链上的交易权限。

5.根据权利要求2所述的基于区块链的安全交易验证方法及系统，其特征在于，该方法还包括：

若该区块链节点对应的智能合约对各个所述交易方对应的加密新余额的合数验证不通过，则向交易事件所有参与节点发送该交易事件合数验证失败的通知，或者，向该区块链上的所有节点发送该交易事件合数验证失败的通知。

6.基于区块链的安全交易验证系统，其特征在于，所述交易验证系统包括：

广播模块，用于当区块链上的一个节点在处理一个带有交易类型和交易金额的交易时，由该节点通过该交易的交易方发送来的第一解密参数解密各个所述交易方的原始余额，并基于所述交易类型和交易金额对各个所述交易方的原始余额进行计算得到对应的新余额，将各个所述交易方对应的新余额通过所述交易方发送来的加密参数进行加密得到加密新余额，通过智能合约将各个所述交易方对应的加密新余额广播到该区块链的各个节点上；

合数验证模块，用于当该区块链的节点接收到广播来的各个所述交易方对应的加密新余额后，启动对应的智能合约进行合数验证；

更新模块，用于若该区块链上各个节点对应的智能合约对各个所述交易方对应的加密新余额的合数验证通过，则由该区块链上各个节点对应的智能合约基于各个所述交易方对应的加密新余额对自身数据进行更新；

余额检验模块，用于调用该区块链外部预设的负数余额验证系统启动多个线程，每个线程同时负责对该区块链上各个节点的单个账户的余额进行负数余额检验，若该区块链上各个节点的单个账户余额的负数余额检验通过，则判定该交易验证通过。

7.根据权利要求6所述基于区块链的安全交易验证系统，其特征在于，所述广播模块还用于：

所述余额检验模块还用于：

由该区块链上的监管方节点读取更新过的各个所述交易方对应的加密新余额，并通过所述秘钥对加密后的第二解密参数进行解密，通过解密后的第二解密参数对各个所述交易方对应的加密新余额进行解密，并对解密后的各个新余额进行负数余额验证。

8.根据权利要求7所述基于区块链的安全交易验证系统，其特征在于，所述余额检验模块还用于：

若有账户未通过负数余额检验，则由所述监管方节点确定该账户对应的异常区块链节点，并将该账户的异常状况向除所述异常区块链节点外的其他节点进行通知。

9.根据权利要求7所述基于区块链的安全交易验证系统，其特征在于，所述余额检验模块还用于：

若有账户未通过负数余额检验，则由所述监管方节点确定该账户对应的异常区块链节点，并通过预设的区块链权限管理系统取消所述异常区块链节点在该区块链上的交易权

限。

10.根据权利要求6或7所述的基于区块链的安全交易验证系统，其特征在于，所述合数验证模块还用于：

若该区块链节点对应的智能合约对各个所述交易方对应的加密新余额的合数验证不通过，则向交易事件所有参与节点发送该交易事件合数验证失败的通知，或者，向该区块链上的所有节点发送该交易事件合数验证失败的通知。

一种基于区块链的安全交易验证方法及系统

技术领域

[0001] 本发明属于计算机技术领域，具体而言是一种基于区块链的安全交易验证方法及系统。

背景技术

[0002] 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。

[0003] 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。

[0004] 虽然，目前业界采用了一些解决信息泄露的区块链交易解决方案，然而现有的解决方案要么是信息泄露解决的不够彻底，要么是计算效率低下，且系统运行开销巨大，限制区块链技术在交易场景中的运用。

[0005] 综上所述，如何在既能有效保证交易信息的安全，又能有效保证交易处理的速度且降低系统开销的情况下，将区块链技术有效运用在交易场景下，已经成为一种亟待解决的技术问题。

发明内容

[0006] 本发明的主要目的在于提供一种基于区块链的安全交易验证方法及系统，旨在有效保证交易信息的安全，且能保证交易处理的速度。

[0007] 本发明通过以下技术方案来实现：基于区块链的安全交易验证方法及系统，包括一下几个步骤：

[0008] 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；

[0009] 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；

[0010] S3，区块链上的一个节点在处理一个带有交易类型和交易金额的交易时，该节点

通过该交易的交易方发送来的第一解密参数解密各个所述交易方的原始余额，并基于所述交易类型和交易金额对各个所述交易方的原始余额进行计算得到对应的新余额，将各个所述交易方对应的新余额通过所述交易方发送来的加密参数进行加密得到加密新余额，通过智能合约将各个所述交易方对应的加密新余额广播到该区块链的各个节点上；

[0011] S4，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；

[0012] S5，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。

[0013] S6，当该区块链的节点接收到广播来的各个所述交易方对应的加密新余额后，启动对应的智能合约进行合数验证；

[0014] S7，若该区块链上各个节点对应的智能合约对各个所述交易方对应的加密新余额的合数验证通过，则该区块链上各个节点对应的智能合约基于各个所述交易方对应的加密新余额对自身数据进行更新；

[0015] S8，调用该区块链外部预设的负数余额验证系统启动多个线程，每个线程同时负责对该区块链上各个节点的单个账户的余额进行负数余额检验，若该区块链上各个节点的单个账户余额的负数余额检验通过，则判定该交易验证通过。

[0016] 作为一种优选的技术方案，该方法还包括：将第二解密参数通过该区块链的节点与该区块链上的监管方节点对应的秘钥进行加密，并将加密后的第二解密参数通过智能合约广播到该区块链上的监管方节点上，所述第二解密参数用于对各个所述交易方对应的加密新余额进行解密；

[0017] 该区块链上的监管方节点读取更新过的各个所述交易方对应的加密新余额，并通过所述秘钥对加密后的第二解密参数进行解密，通过解密后的第二解密参数对各个所述交易方对应的加密新余额进行解密，并对解密后的各个新余额进行负数余额验证。

[0018] 作为一种优选的技术方案，该方法还包括：若有账户未通过负数余额检验，则所述监管方节点确定该账户对应的异常区块链节点，并将该账户的异常状况向除所述异常区块链节点外的其他节点进行通知。

[0019] 作为一种优选的技术方案，该方法还包括：若有账户未通过负数余额检验，则所述监管方节点确定该账户对应的异常区块链节点，并通过预设的区块链权限管理系统取消所述异常区块链节点在该区块链上的交易权限。

[0020] 作为一种优选的技术方案，该方法还包括：若该区块链节点对应的智能合约对各个所述交易方对应的加密新余额的合数验证不通过，则向交易事件所有参与节点发送该交易事件合数验证失败的通知，或者，向该区块链上的所有节点发送该交易事件合数验证失败的通知。

[0021] 作为一种优选的技术方案，所述交易验证系统包括：广播模块，用于当区块链上的一个节点在处理一个带有交易类型和交易金额的交易时，由该节点通过该交易的交易方发送来的第一解密参数解密各个所述交易方的原始余额，并基于所述交易类型和交易金额对

各个所述交易方的原始余额进行计算得到对应的新余额，将各个所述交易方对应的新余额通过所述交易方发送来的加密参数进行加密得到加密新余额，通过智能合约将各个所述交易方对应的加密新余额广播到该区块链的各个节点上；

[0022] 合数验证模块，用于当该区块链的节点接收到广播来的各个所述交易方对应的加密新余额后，启动对应的智能合约进行合数验证；

[0023] 更新模块，用于若该区块链上各个节点对应的智能合约对各个所述交易方对应的加密新余额的合数验证通过，则由该区块链上各个节点对应的智能合约基于各个所述交易方对应的加密新余额对自身数据进行更新；

[0024] 余额检验模块，用于调用该区块链外部预设的负数余额验证系统启动多个线程，每个线程同时负责对该区块链上各个节点的单个账户的余额进行负数余额检验，若该区块链上各个节点的单个账户余额的负数余额检验通过，则判定该交易验证通过。

[0025] 作为一种优选的技术方案，所述广播模块还用于：所述余额检验模块还用于：由该区块链上的监管方节点读取更新过的各个所述交易方对应的加密新余额，并通过所述秘钥对加密后的第二解密参数进行解密，通过解密后的第二解密参数对各个所述交易对应的加密新余额进行解密，并对解密后的各个新余额进行负数余额验证。

[0026] 作为一种优选的技术方案，所述余额检验模块还用于：若有账户未通过负数余额检验，则由所述监管方节点确定该账户对应的异常区块链节点，并将该账户的异常状况向除所述异常区块链节点外的其他节点进行通知。

[0027] 作为一种优选的技术方案，所述余额检验模块还用于：若有账户未通过负数余额检验，则由所述监管方节点确定该账户对应的异常区块链节点，并通过预设的区块链权限管理系统取消所述异常区块链节点在该区块链上的交易权限。

[0028] 作为一种优选的技术方案，所述合数验证模块还用于：若该区块链节点对应的智能合约对各个所述交易方对应的加密新余额的合数验证不通过，则向交易事件所有参与节点发送该交易事件合数验证失败的通知，或者，向该区块链上的所有节点发送该交易事件合数验证失败的通知。

[0029] 与现有技术相比较，本发明的有益效果在于：

[0030] (1)本发明提出的基于区块链的交易验证方法及系统，区块链上的节点在处理带有交易类型和交易金额的交易时，基于所述交易类型和交易金额对各个所述交易方的原始余额进行计算得到对应的新余额，并将各个所述交易方对应的新余额通过所述交易方发送来的加密参数进行加密得到加密新余额，广播到该区块链的各个节点上；当该区块链的节点接收到广播来的各个所述交易方对应的加密新余额后，启动对应的智能合约进行合数验证；在合数验证通过，才由所述区块链节点对应的智能合约基于所述交易参数对自身数据进行更新。由于广播的各个所述交易方对应的新余额均进行了加密处理，该区块链的其他节点无法获知该新余额，且只有在合数验证通过后，才进行数据更新，能防止多方交易中各账户的余额泄露，有效地保证了交易信息的安全。此外，还将各个节点的单个账户的余额发给所述区块链外部预设的负数余额验证系统来进行负数余额检验。由于利用外部的负数余额验证系统来进行负数余额检验，既能进一步验证多方交易是否正常，又能在不占用系统开销的情况下保证区块链上的交易处理速度。

[0031] (2)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

[0032] 图1为本发明基于区块链的交易验证方法一实施例的流程示意图；

[0033] 图2为本发明交易验证系统一实施例的功能模块示意图。

具体实施方式

[0034] 为了使本发明所要解决的技术问题、技术方案及有益效果更加清楚、明白，以下结合附图和实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0035] 本发明提供一种基于区块链的交易验证方法。

[0036] 参照图1，图1为本发明基于区块链的交易验证方法一实施例的流程示意图。

[0037] 在一实施例中，该基于区块链的交易验证方法包括：

[0038] 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。

[0039] 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。

[0040] 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。

[0041] 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。

[0042] 步骤S2，区块链上的一个节点在处理一个带有交易类型和交易金额的交易时，该节点通过该交易的交易方发送来的第一解密参数解密各个所述交易方的原始余额，并基于所述交易类型和交易金额对各个所述交易方的原始余额进行计算得到对应的新余额，将各个所述交易方对应的新余额通过所述交易方发送来的加密参数进行加密得到加密新余额，通过智能合约将各个所述交易方对应的加密新余额广播到该区块链的各个节点上。

[0043] 当区块链上的一个节点在完成一个交易事件后，会将该交易事件对应的交易参数广播给该区块链上的其他节点。其中，所述交易参数可包括交易类型和/ 或交易金额，例如，若区块链上的A节点向B节点转账支付了金额X，则A节点将该交易事件对应的交易参数广播给该区块链上的其他节点，对外广播的交易参数中包括“交易类型:A节点转出”，A节点

对外广播的交易参数中还包括“交易金额:X”;同时,B节点也将该交易事件对应的交易参数广播给该区块链上的其他节点,对外广播的交易参数中包括“交易类型:B节点转入”,B节点对外广播的交易参数中还包括“交易金额:X”。

[0044] 本实施例中,当区块链上的一个节点在处理一个带有交易类型(例如,A转账给B)和交易金额的交易时,该节点通过该交易的交易方发送来的第一解密参数解密各个所述交易方的原始余额,并基于所述交易类型和交易金额对各个所述交易方的原始余额进行计算以算出对应的新余额,将各个所述交易方对应的新余额通过所述交易方发送来的加密参数(所述加密参数与所述解密参数可以相同,也可以不同)进行加密,通过智能合约将各个所述交易方对应的加密后的新余额广播到该区块链的各个节点上。

[0045] 步骤S3,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;

[0046] 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。

[0047] 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)。

[0048] 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。

[0049] 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。

[0050] 步骤S4,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。

[0051] 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。

[0052] 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)。

[0053] 步骤S5，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。

[0054] 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。

[0055] 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。

[0056] 步骤S6，当该区块链的节点接收到广播来的各个所述交易方对应的加密新余额后，启动对应的智能合约进行合数验证。

[0057] 区块链上的数据通常会被存放在参与节点上的两个地方：智能合约(每个智能合约存有自己的当前状况)中和节点上的事务记录(transaction log，用来滚出每个智能合约上数据当前的状况)中，每个区块链节点对应一个事务记录和一个或多个智能合约。当一个交易参数传到区块链的节点上时，这个交易参数会被记录到该节点对应的事务记录上并同时传给与该交易参数对应的智能合约去运行，并由该交易参数对应的智能合约上的代码对智能合约的自身数据进行更新。

[0058] 本实施例中，若有区块链节点接收到该区块链上的其他节点广播来的各个所述交易方对应的加密新余额，则该区块链节点将所述加密新余额发给该区块链节点对应的智能合约进行合数验证，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，以验证该交易是否正常。本实施例中，该区块链节点对应的智能合约可基于预设的同态加密验证算法来进行合数验证。

[0059] 其中，同态加密是基于数学难题的计算复杂性理论的密码学技术。对经过同态加密的数据进行处理得到一个输出，将这一输出进行解密，其结果与用同一方法处理未加密的原始数据得到的输出结果是一样的。本实施例中，基于预设的同态加密验证算法可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，从而验证该交易

是否正常。例如，在一种实施方式中，该区块链节点对应的智能合约可以采用加法同态加密验证算法进行合数验证，假设R 和S是域，称加密函数E:R→S为加法同态，如果存在有效算法⊕，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，这个算法不仅能验证账户合数，同时，还能确保不泄漏账户的余额x 和y。

[0060] 当运用区块链技术进行多方参与的交易事件例如转账交易、支付交易等事件时，在去中心化的区块链系统当中，由于没有绝对权威机构节点，因此对每笔交易都必须进行集体验证。本实施例中采用同态加密验证算法来进行合数验证，既能有效地验证运用区块链技术进行多方参与的交易是否正常，又能防止多方账户的余额泄露，有效地保证了交易信息的安全。

[0061] 步骤S7，若该区块链上各个节点对应的智能合约对各个所述交易方对应的加密新余额的合数验证通过，则该区块链上各个节点对应的智能合约基于各个所述交易方对应的加密新余额对自身数据进行更新；

[0062] 若该区块链节点对应的智能合约对所述交易参数的合数验证通过，则说明该交易正常，则该区块链上各个节点对应的智能合约基于各个所述交易方对应的加密新余额进行更新。例如，若所述交易参数包括的交易类型是“A节点转出”，所述交易参数包括的交易金额是X，则该区块链节点对应的智能合约将自身数据中的A节点余额减少X。

[0063] S8、调用该区块链外部预设的负数余额验证系统启动多个线程，每个线程同时负责对该区块链上各个节点的单个账户的余额进行负数余额检验，若该区块链上各个节点的单个账户余额的负数余额检验通过，则判定该交易验证通过。

[0064] 因为每个节点的余额都是独立数组，所以可以对多个节点余额进行多线程检验，同时，因为同一个节点参与每次交易的账户、交易类型和金额是被记载在案的，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所述合数验证的校验，例如，银行A可把账号001上的100张票据通过以下分账户分摊余额的形式变成400张：先创建一个002账号并放上400余额，然后再在一个新的003账号上存-300。

[0065] 本实施例中通过在所述区块链外部的负数余额验证系统，即利用不在所述区块链上运行的负数余额验证系统来启动多个线程对参与该交易事件的各个节点的各个账户的余额进行负数余额检验，能避免用户通过制造存有负数的账号的方式来骗过合数验证的情况发生，能进一步地更加准确的验证交易是否正常，而且，负数余额验证系统并不在所述区块链上运行，而是在外部单独运行，不会对区块链上的交易处理速度造成影响，有效地保证了区块链上较快的交易处理速度。

[0066] 本实施例中若有区块链节点接收到区块链上的其他节点广播来的交易参数，区块链上的节点在处理带有交易类型和交易金额的交易时，基于所述交易类型和交易金额对各个所述交易方的原始余额进行计算得到对应的新余额，并将各个所述交易方对应的新余额通过所述交易方发送来的加密参数进行加密得到加密新余额，广播到该区块链的各个节点上；当该区块链的节点接收到广播来的各个所述交易方对应的加密新余额后，启动对应的智能合约进行合数验证；在合数验证通过，才由所述区块链节点对应的智能合约基于所述交易参数对自身数据进行更新。由于广播的各个所述交易方对应的新余额均进行了加密处理，该区块链的其他节点无法获知该新余额，且只有在合数验证通过后，才进行数据更新，

能防止多方交易中各账户的余额泄露，有效地保证了交易信息的安全。此外，还将各个节点的单个账户的余额发给所述区块链外部预设的负数余额验证系统来进行负数余额检验。由于利用外部的负数余额验证系统来进行负数余额检验，既能进一步验证多方交易是否正常，又能在不占用系统开销的情况下保证区块链上的交易处理速度。

[0067] 进一步地，在其他实施例中，该方法还可以包括：

[0068] 将第二解密参数通过该区块链的节点与该区块链上的监管方节点对应的秘钥进行加密，并将加密后的第二解密参数通过智能合约广播到该区块链上的监管方节点上，所述第二解密参数用于对各个所述交易方对应的加密新余额进行解密；

[0069] 该区块链上的监管方节点读取更新过的各个所述交易方对应的加密新余额，并通过所述秘钥对加密后的第二解密参数进行解密，通过解密后的第二解密参数对各个所述交易方对应的加密新余额进行解密，并对解密后的各个新余额进行负数余额验证。

[0070] 本实施例中，在该节点通过智能合约将各个所述交易方对应的加密新余额广播到该区块链的各个节点上的同时，还将用于对各个所述交易方对应的加密后的新余额进行解密的第二解密参数通过该节点与监管方节点对应的秘钥进行加密，并将加密后的解密参数通过智能合约广播到该区块链上的监管方节点上。在该区块链上各个节点对应的智能合约对各个所述交易方对应的加密新余额的合数验证通过，且该区块链上各个节点对应的智能合约基于各个所述交易方对应的加密新余额进行更新后，由该区块链上的监管方节点在读取更新过的各个所述交易方对应的加密新余额后，通过所述秘钥对所述加密后的解密参数进行解密，通过解密后的解密参数对各个所述交易方对应的加密后的新余额进行解密，并对解密后的各个新余额进行负数余额验证，进一步地从区块链本身对该区块链上的各个账户的余额进行负数余额检验，以进一步验证该交易是否正常。

[0071] 进一步地，在其他实施例中，该方法还可以包括：

[0072] 若有账户未通过负数余额检验，则所述监管方节点确定该账户对应的异常区块链节点，并将该账户的异常状况向除所述异常区块链节点外的其他节点进行通知。

[0073] 若有账户未通过负数余额检验，则有可能是出现了用户通过制造存有负数的账号的方式来骗过合数验证的情况，则由区块链上的监管方节点确定该账户对应的异常区块链节点，并将该账户的异常状况向所述区块链中除所述异常区块链节点之外的其他节点进行通知，以提醒其他节点该账户处于异常状况，该账户对应的异常区块链节点参与的交易事件可能存在风险。

[0074] 进一步地，在其他实施例中，该方法还可以包括：

[0075] 若有账户未通过负数余额检验，则由所述监管方节点通过预设的区块链权限管理系统取消所述异常区块链节点在所述区块链上的交易权限。

[0076] 若由所述负数余额验证系统对单个账户的余额进行负数余额检验时，有账户未通过负数余额检验，则有可能是出现了用户通过制造存有负数的账号的方式来骗过合数验证的情况，说明该账户对应的异常区块链节点参与的交易事件可能存在风险，则通过预设的区块链权限管理系统取消所述异常区块链节点在所述区块链上的交易权限，以阻止所述异常区块链节点在所述区块链上继续参与交易，保证所述区块链中除所述异常区块链节点之外的其他节点的交易安全。

[0077] 进一步地，在其他实施例中，该方法还可以包括：

[0078] 若所述区块链节点对应的智能合约对所述交易参数的合数验证不通过，则向该交易事件的所有参与节点发送该交易事件合数验证失败的通知，或者，向所述区块链上的所有节点发送该交易事件合数验证失败的通知。以提醒该交易事件的所有参与节点或所述区块链上的所有节点该交易事件出现异常，所述区块链节点参与的交易事件可能存在风险。

[0079] 本发明进一步提供一种基于区块链的交易验证系统。

[0080] 参照图2，图2为本发明交易验证系统一实施例的功能模块示意图。

[0081] 在一实施例中，该交易验证系统包括：

[0082] 广播模块01，用于当区块链上的一个节点在处理一个带有交易类型和交易金额的交易时，由该节点通过该交易的交易方发送来的第一解密参数解密各个所述交易方的原始余额，并基于所述交易类型和交易金额对各个所述交易方的原始余额进行计算得到对应的新余额，将各个所述交易方对应的新余额通过所述交易方发送来的加密参数进行加密得到加密新余额，通过智能合约将各个所述交易方对应的加密新余额广播到该区块链的各个节点上。

[0083] 当区块链上的一个节点在完成一个交易事件后，会将该交易事件对应的交易参数广播给该区块链上的其他节点。其中，所述交易参数可包括交易类型和/或交易金额，例如，若区块链上的A节点向B节点转账支付了金额X，则A节点将该交易事件对应的交易参数广播给该区块链上的其他节点，对外广播的交易参数中包括“交易类型:A节点转出”，A节点对外广播的交易参数中还包括“交易金额:X”；同时，B节点也将该交易事件对应的交易参数广播给该区块链上的其他节点，对外广播的交易参数中包括“交易类型:B节点转入”，B节点对外广播的交易参数中还包括“交易金额:X”。

[0084] 本实施例中，当区块链上的一个节点在处理一个带有交易类型(例如，A转账给B)和交易金额的交易时，该节点通过该交易的交易方发送来的第一解密参数解密各个所述交易方的原始余额，并基于所述交易类型和交易金额对各个所述交易方的原始余额进行计算以算出对应的新余额，将各个所述交易方对应的新余额通过所述交易方发送来的加密参数(所述加密参数与所述解密参数可以相同，也可以不同)进行加密，通过智能合约将各个所述交易方对应的加密后的新余额广播到该区块链的各个节点上。

[0085] 合数验证模块02，用于当该区块链的节点接收到广播来的各个所述交易方对应的加密新余额后，启动对应的智能合约进行合数验证。

[0086] 区块链上的数据通常会被存放在参与节点上的两个地方：智能合约(每个智能合约存有自己的当前状况)中和节点上的事务记录(transaction log，用来滚出每个智能合约上数据当前的状况)中，每个区块链节点对应一个事务记录和一个或多个智能合约。当一个交易参数传到区块链的节点上时，这个交易参数会被记录到该节点对应的事务记录上并同时传给与该交易参数对应的智能合约去运行，并由该交易参数对应的智能合约上的代码对智能合约的自身数据进行更新。

[0087] 本实施例中，若有区块链节点接收到该区块链上的其他节点广播来的各个所述交易方对应的加密新余额，则该区块链节点将所述加密新余额发给该区块链节点对应的智能合约进行合数验证，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，以验证该交易是否正常。本实施例中，该区块链节点对应的智能合约可基于预设的同态加密验证算法来进行合数验证。

[0088] 其中，同态加密是基于数学难题的计算复杂性理论的密码学技术。对经过同态加密的数据进行处理得到一个输出，将这一输出进行解密，其结果与用同一方法处理未加密的原始数据得到的输出结果是一样的。本实施例中，基于预设的同态加密验证算法可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，从而验证该交易是否正常。例如，在一种实施方式中，该区块链节点对应的智能合约可以采用加法同态加密验证算法进行合数验证，假设R 和S是域，称加密函数E:R→S为加法同态，如果存在有效算法⊕，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，这个算法不仅能验证账户合数，同时，还能确保不泄漏账户的余额x 和y。

[0089] 当运用区块链技术进行多方参与的交易事件例如转账交易、支付交易等事件时，在去中心化的区块链系统当中，由于没有绝对权威机构节点，因此对每笔交易都必须进行集体验证。本实施例中采用同态加密验证算法来进行合数验证，既能有效地验证运用区块链技术进行多方参与的交易是否正常，又能防止多方账户的余额泄露，有效地保证了交易信息的安全。

[0090] 更新模块03，用于若该区块链上各个节点对应的智能合约对各个所述交易方对应的加密新余额的合数验证通过，则由该区块链上各个节点对应的智能合约基于各个所述交易方对应的加密新余额对自身数据进行更新。

[0091] 若该区块链节点对应的智能合约对所述交易参数的合数验证通过，则说明该交易正常，则该区块链上各个节点对应的智能合约基于各个所述交易方对应的加密新余额进行更新。例如，若所述交易参数包括的交易类型是“A节点转出”，所述交易参数包括的交易金额是X，则该区块链节点对应的智能合约将自身数据中的A节点余额减少X。

[0092] 余额检验模块04，用于调用该区块链外部预设的负数余额验证系统启动多个线程，每个线程同时负责对该区块链上各个节点的单个账户的余额进行负数余额检验，若该区块链上各个节点的单个账户余额的负数余额检验通过，则判定该交易验证通过。

[0093] 因为每个节点的余额都是独立数组，所以可以对多个节点余额进行多线程检验，同时，因为同一个节点参与每次交易的账户、交易类型和金额是被记载在案的，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所述合数验证的校验，例如，银行A可把账号001上的100张票据通过以下分账户分摊余额的形式变成400张：先创建一个002账号并放上400余额，然后再在一个新的003账号上存-300。

[0094] 本实施例中通过在所述区块链外部的负数余额验证系统，即利用不在所述区块链上运行的负数余额验证系统来启动多个线程对参与该交易事件的各个节点的各个账户的余额进行负数余额检验，能避免用户通过制造存有负数的账号的方式来骗过合数验证的情况发生，能进一步地更加准确的验证交易是否正常，而且，负数余额验证系统并不在所述区块链上运行，而是在外部单独运行，不会对区块链上的交易处理速度造成影响，有效地保证了区块链上较快的交易处理速度。

[0095] 本实施例中若有区块链节点接收到区块链上的其他节点广播来的交易参数，区块链上的节点在处理带有交易类型和交易金额的交易时，基于所述交易类型和交易金额对各个所述交易方的原始余额进行计算得到对应的新余额，并将各个所述交易方对应的新余额通过所述交易方发送来的加密参数进行加密得到加密新余额，广播到该区块链的各个节点

上;当该区块链的节点接收到广播来的各个所述交易方对应的加密新余额后,启动对应的智能合约进行合数验证;在合数验证通过,才由所述区块链节点对应的智能合约基于所述交易参数对自身数据进行更新。由于广播的各个所述交易方对应的新余额均进行了加密处理,该区块链的其他节点无法获知该新余额,且只有在合数验证通过后,才进行数据更新,能防止多方交易中各账户的余额泄露,有效地保证了交易信息的安全。此外,还将各个节点的单个账户的余额发给所述区块链外部预设的负数余额验证系统来进行负数余额检验。由于利用外部的负数余额验证系统来进行负数余额检验,既能进一步验证多方交易是否正常,又能在不占用系统开销的情况下保证区块链上的交易处理速度。

[0096] 进一步地,在其他实施例中,上述广播模块01还可以用于:

[0097] 将第二解密参数通过该区块链的节点与该区块链上的监管方节点对应的秘钥进行加密,并将加密后的第二解密参数通过智能合约广播到该区块链上的监管方节点上,所述第二解密参数用于对各个所述交易方对应的加密新余额进行解密;

[0098] 上述余额检验模块04还可以用于:

[0099] 由该区块链上的监管方节点读取更新过的各个所述交易方对应的加密新余额,并通过所述秘钥对加密后的第二解密参数进行解密,通过解密后的第二解密参数对各个所述交易方对应的加密新余额进行解密,并对解密后的各个新余额进行负数余额验证。

[0100] 本实施例中,在该节点通过智能合约将各个所述交易方对应的加密新余额广播到该区块链的各个节点上的同时,还将用于对各个所述交易方对应的加密后的新余额进行解密的第二解密参数通过该节点与监管方节点对应的秘钥进行加密,并将加密后的解密参数通过智能合约广播到该区块链上的监管方节点上。在该区块链上各个节点对应的智能合约对各个所述交易方对应的加密新余额的合数验证通过,且该区块链上各个节点对应的智能合约基于各个所述交易方对应的加密新余额进行更新后,由该区块链上的监管方节点在读取更新过的各个所述交易方对应的加密新余额后,通过所述秘钥对所述加密后的解密参数进行解密,通过解密后的解密参数对各个所述交易方对应的加密后的新余额进行解密,并对解密后的各个新余额进行负数余额验证,进一步地从区块链本身对该区块链上的各个账户的余额进行负数余额检验,以进一步验证该交易是否正常。

[0101] 进一步地,在其他实施例中,上述余额检验模块04还可以用于:

[0102] 若有账户未通过负数余额检验,则由所述监管方节点确定该账户对应的异常区块链节点,并将该账户的异常状况向除所述异常区块链节点外的其他节点进行通知。

[0103] 若有账户未通过负数余额检验,则有可能是出现了用户通过制造存有负数的账号的方式来骗过合数验证的情况,则由区块链上的监管方节点确定该账户对应的异常区块链节点,并将该账户的异常状况向所述区块链中除所述异常区块链节点之外的其他节点进行通知,以提醒其他节点该账户处于异常状况,该账户对应的异常区块链节点参与的交易事件可能存在风险。

[0104] 进一步地,在其他实施例中,上述余额检验模块04还可以用于:

[0105] 若有账户未通过负数余额检验,则由所述监管方节点通过预设的区块链权限管理系统取消所述异常区块链节点在所述区块链上的交易权限。

[0106] 若由所述负数余额验证系统对单个账户的余额进行负数余额检验时,有账户未通过负数余额检验,则有可能是出现了用户通过制造存有负数的账号的方式来骗过合数验证

的情况，说明该账户对应的异常区块链节点参与的交易事件可能存在风险，则通过预设的区块链权限管理系统取消所述异常区块链节点在所述区块链上的交易权限，以阻止所述异常区块链节点在所述区块链上继续参与交易，保证所述区块链中除所述异常区块链节点之外的其他节点的交易安全。

[0107] 进一步地，在其他实施例中，上述合数验证模块02还可以用于：

[0108] 若所述区块链节点对应的智能合约对所述交易参数的合数验证不通过，则向该交易事件的所有参与节点发送该交易事件合数验证失败的通知，或者，向所述区块链上的所有节点发送该交易事件合数验证失败的通知。以提醒该交易事件的所有参与节点或所述区块链上的所有节点该交易事件出现异常，所述区块链节点参与的交易事件可能存在风险。

[0109] 需要说明的是，在本文中，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、物品或者装置不仅包括那些要素，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、物品或者装置所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该要素的过程、方法、物品或者装置中还存在另外的相同要素。

[0110] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到上述实施例方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件来实现，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明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，该计算机软件产品存储在一个存储介质(如ROM/RAM、磁碟、光盘)中，包括若干指令用以使得一台终端设备(可以是手机，计算机，服务器，空调器，或者网络设备等)执行本发明各个实施例所述的方法。

[0111] 以上参照附图说明了本发明的优选实施例，并非因此局限本发明的权利范围。上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。另外，虽然在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤。

[0112] 本领域技术人员不脱离本发明的范围和实质，可以有多种变型方案实现本发明，比如作为一个实施例的特征可用于另一实施例而得到又一实施例。凡在运用本发明的技术构思之内所作的任何修改、等同替换和改进，均应在本发明的权利范围之内。

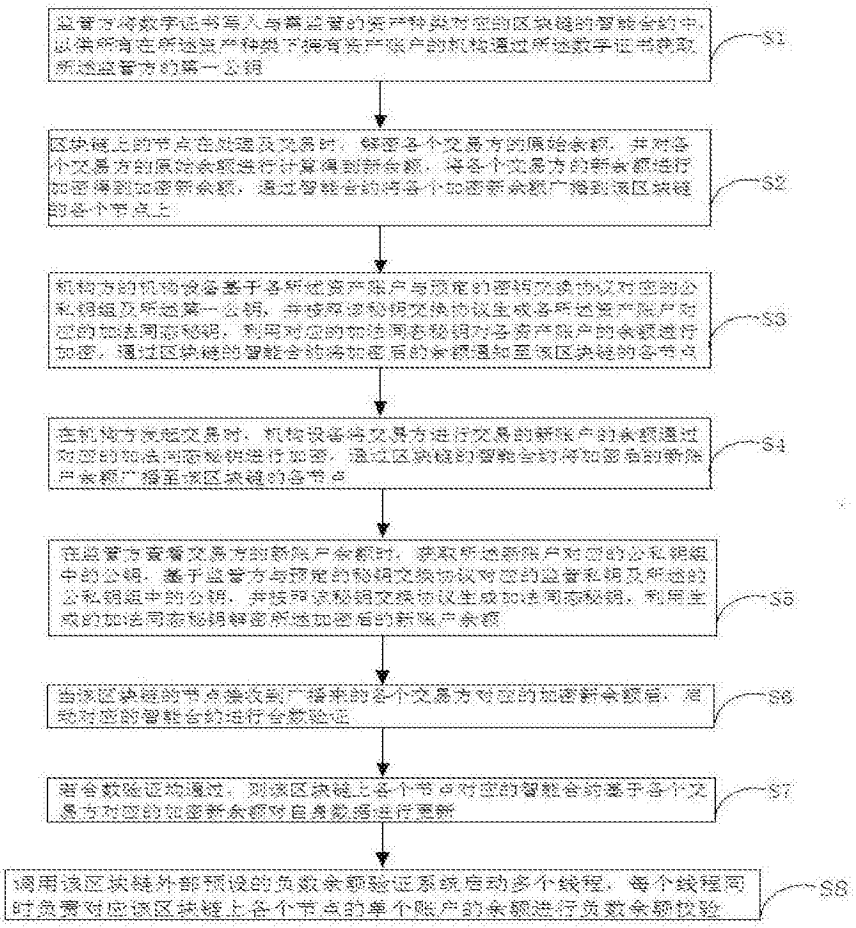

监管方将数字证书写入与其监管的资产种类对应的区块链的智能合约中，以使所有在所述资产种类下拥有资产账户的机构通过所述数字证书确定所述监管方的第一公钥
S1
区块链上的节点在处理及交易时，解密各个交易方的原始余额，并对各个交易方的原始余额进行计算得到新余额，将各个交易方的新余额进行加密得到加密新余额，通过智能合约将各个加密新余额广播到该区块链的各个节点上
S2
机构方的机构设备基于各所述资产账户与预定的密钥交换协议对应的公私钥组及所述第一公钥，并使用密钥交换协议生成各所述资产账户对应的加法同态秘钥，利用对应的加法同态秘钥对各资产账户的余额进行加密，通过区块链的智能合约将加密后的余额通知至该区块链的各节点
S3
在机构方完成交易时，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，利用生成的加法同态秘钥解密所述加密后的新账户余额
S5
当该区块链的节点接收到广播来的各个交易方对应的加密新余额后，调取对应的智能合约进行合数验证
S6
若合数验证均通过，则该区块链上各个节点对应的智能合约基于各个交易方对应的加密新余额对自身数据进行更新
S7
调用该区块链外部预设的负数余额验证系统启动多个线程，每个线程同时负责对应该区块链上各个节点的单个账户的余额进行负数余额校验
S8

图1

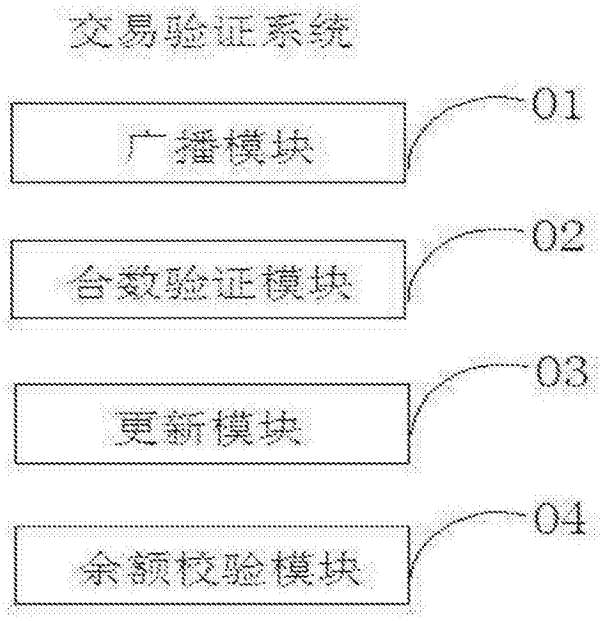

交易验证系统
广播模块
01
合数验证模块
02
更新模块
03
余额校验模块
04

图2