(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 109559122 A
(43)申请公布日 2019.04.02

(21)申请号 201811496380.7

(22)申请日 2018.12.07

(71)申请人 北京瑞卓喜投科技发展有限公司
地址 101201 北京市平谷区金海湖镇韩庄南大街111号

(72)发明人 扬子一 李斌 张勇

(74)专利代理机构 北京力量专利代理事务所（特殊普通合伙）11504
代理人 王鸿远

(51)Int.Cl.
G06Q 20/38(2012.01)
H04L 9/06(2006.01)
H04L 9/08(2006.01)
H04L 9/32(2006.01)
H04L 29/06(2006.01)

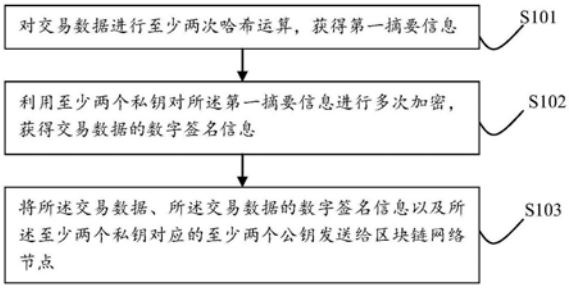
权利要求书2页 说明书11页 附图2页

(54)发明名称

区块链数据传输方法及区块链数据传输系统

(57)摘要

本发明涉及一种区块链数据传输方法及区块链数据传输系统，该方法包括：对交易数据进行至少两次哈希运算，获得第一摘要信息；利用至少两个私钥对第一摘要信息进行多次加密，获得交易数据的数字签名信息；将交易数据、交易数据的数字签名信息以及至少两个私钥对应的至少两个公钥发送给区块链网络节点。本发明的方案通过至少两次哈希算法，提高了哈希内部操作复杂度和哈希输出长度，使得任意输入改变都可以产生不同的输出，提高了抵御攻击的能力，且在不牺牲抵御冲突前提下具有高效性，同时利用至少两个私钥进行多次加密，即多重数字签名技术增加了信息可信度，能充分验证信息不是伪造的，且在传播过程中未被篡改，提高了数字钱包安全性。



CN 109559122 A

1.一种区块链数据传输方法,其特征在于,包括以下步骤:

对交易数据进行至少两次哈希运算,获得第一摘要信息;

利用至少两个私钥对所述第一摘要信息进行多次加密,获得交易数据的数字签名信息;

将所述交易数据、所述交易数据的数字签名信息以及所述至少两个私钥对应的至少两个公钥发送给区块链网络节点。

2.根据权利要求1所述的区块链数据传输方法,其特征在于,所述对交易数据进行至少两次哈希运算的步骤包括:

对交易数据采用第三代安全散列算法进行至少两次哈希运算。

3.根据权利要求1所述的区块链数据传输方法,其特征在于,利用至少两个私钥对所述第一摘要信息进行多次加密,获得交易数据的数字签名信息之前,还包括:

对交易账户生成一级权限账户和二级权限账户,一级权限账户和二级权限账户分别包含至少两个秘钥对,每个秘钥对分别包含私钥和公钥;

利用至少两个私钥对所述第一摘要信息进行多次加密的步骤包括:

利用二级权限账户的至少两个秘钥对的私钥对所述第一摘要信息进行多次加密。

4.根据权利要求3所述的区块链数据传输方法,其特征在于,一级权限账户和二级权限账户还包含每个秘钥对分别对应的权重以及权重阈值;

将所述交易数据、所述交易数据的数字签名信息以及所述至少两个私钥对应的至少两个公钥发送给区块链网络节点的同时还包括:

将二级权限账户每个秘钥对分别对应的权重以及权重阈值发送给区块链网络节点。

5.根据权利要求3所述的区块链数据传输方法,其特征在于,还包括:

接收对二级权限账户的修改请求;

利用一级权限账户的至少两个秘钥对修改请求进行验证;

在所修改请求验证通过时,执行所述修改请求。

6.一种区块链数据传输系统,其特征在于,包括:

第一摘要信息生成模块,用于对交易数据进行至少两次哈希运算,获得第一摘要信息;

数字签名模块,用于利用至少两个私钥对所述第一摘要信息进行多次加密,获得交易数据的数字签名信息;

数据发送模块,用于将所述交易数据、所述交易数据的数字签名信息以及所述至少两个私钥对应的至少两个公钥发送给区块链网络节点。

7.一种区块链数据传输方法,其特征在于,包括:

接收交易数据、交易数据的数字签名信息以及至少两个公钥,其中,所述交易数据的数字签名信息是发送节点对交易数据进行至少两次哈希运算,获得第一摘要信息之后,利用至少两个私钥对所述第一摘要信息进行多次加密获得的数字签名信息;所述至少两个公钥是至少两个私钥对应的公钥;

利用所述至少两个公钥对所述交易数据的数字签名信息进行多次解密,获得解密后的第二摘要信息;

对所述交易数据进行至少两次哈希运算,获得第三摘要信息;

当所述第二摘要信息与所述第三摘要信息一致时,向区块链网络广播所述交易数据的

数字签名认证通过的消息。

8.根据权利要求7所述的区块链数据传输方法，其特征在于，对所述交易数据进行至少两次哈希运算的步骤包括：

对所述交易数据采用第三代安全散列算法进行至少两次哈希运算。

9.根据权利要求7所述的区块链数据传输方法，其特征在于，向区块链网络广播所述交易数据的数字签名认证通过的消息之前，还包括：

接收二级权限账户每个秘钥对分别对应的权重以及权重阈值；

获取二级权限账户每个秘钥对按照对应的权重进行加权运算后的加权值；

向区块链网络广播所述交易数据的数字签名认证通过的消息的步骤包括：

当所述加权值大于或等于所述权重阈值，且所述第二摘要信息与所述第三摘要信息一致时，向区块链网络广播所述交易数据的数字签名认证通过的消息。

10.一种区块链数据传输系统，其特征在于，包括：

数据接收模块，用于接收交易数据、交易数据的数字签名信息以及至少两个公钥，其中，所述交易数据的数字签名信息是发送节点对交易数据进行至少两次哈希运算，获得第一摘要信息之后，利用至少两个私钥对所述第一摘要信息进行多次加密获得的数字签名信息；所述至少两个公钥是至少两个私钥对应的公钥；

数字签名信息解密模块，用于利用所述至少两个公钥对所述交易数据的数字签名信息进行多次解密，获得解密后的第二摘要信息；

第三摘要信息生成模块，用于对所述交易数据进行至少两次哈希运算，获得第三摘要信息；

数字签名认证模块，用于当所述第二摘要信息与所述第三摘要信息一致时，向区块链网络广播所述交易数据的数字签名认证通过的消息。

区块链数据传输方法及区块链数据传输系统

技术领域

[0001] 本发明涉及区块链数据安全传输技术领域，尤其涉及一种区块链数据传输方法及区块链数据传输系统。

背景技术

[0002] 随着互联网网络交易普及，在交易过程中引入数字签名技术，在区块链发展中，为了防止发送节点信息和数据被恶意伪造和篡改，也引入数字签名技术。

[0003] 数字签名，也被称为秘钥数字签名，是一种通过秘钥加密鉴别数字信息的方法。基于该技术，信息发送者可以通过发送别人不能伪造的一串数字字符，也可以证明发送信息真实性。

[0004] 目前区块链中常用的数字签名算法是ECDSA(Elliptic Curve Digital Signature Algorithm，椭圆曲线数字签名算法)。在ECDSA算法中，交易双方需约定一个共同的哈希函数，将要处理的对象是发送消息的哈希值，而不是消息本身，只有发送信息方有私钥的权限，验证哈希值只需要拿到相应的公钥即可验证。

[0005] 以太坊/比特币都采用了ECDSA算法。比特币的哈希算法使用的是SHA256算法(第二代安全散列算法56，是安全散列算法SHA系列算法之一)。相对于第一代安全散列算法，第二代安全散列算法只是扩展了哈希的字节数。目前第一代安全散列算法已经被攻破，第二代安全散列算法被攻破只是时间问题。

[0006] 以太坊的数字签名技术，对交易签名步骤如下：先对交易本身进行RLP(Recursive Length Prefix，中文翻译过来叫递归长度前缀)编码，再对RLP编码进行哈希，对第一步的结果进行ecdsa曲线的签名，然后把数字签名和交易内容广播到全网。

[0007] 综上所述，区块链中，数字签名技术包含两种运算算法：数字签名和验证。

[0008] 目前，哈希算法和数字签名与验证两方面存在以下问题。

[0009] (一)哈希算法面临下面两个问题：

[0010] 1)哈希函数内部复杂度不够高

[0011] 2)哈希函数生成的数值长度不够长

[0012] (二)数字签名与验证

[0013] 区块链公钥加密系统采用非对称加密算法。采用较多的是公钥加密算法，如基于RSA Date Security公司的PKCS(Public Key Cryptography Standards，公钥密码学规范)、DSA(Digital Signature Algorithm，数字签名算法)、PGP(Pretty Good Privacy，是PGP公司的加密和/或签名工具套件，使用了有商业版权的IDEA算法并集成了有商业版权的PGPdisk工具)、ECC(Ellipse Curve Cryptography，椭圆曲线密码，基于使用椭圆曲线上的点来定义的公钥/私钥对)。1994年美国保准于技术协会公布了数字签名标准促进了公钥加密技术广泛应用。

[0014] ECC的创建基于使用椭圆曲线上的点来定义的公钥/私钥对，黑客很难用通常使用的暴力破解的方法来破解，是以较少的计算能力提供比RSA加密算法(由RSA公司发明，是一

个支持变长秘钥的公共秘钥算法,需要加密的文件块的长度也是可变的)更快的加密算法。ECC的主要缺点之一是它比RSA加密显著地增加了加密消息的大小。此外,ECC算法比RSA更复杂,更难实现,这增加了实现错误的可能性,从而降低了算法的安全性。

[0015] 但是目前区块链系统不具备挂失,冻结以及回滚功能,接二连三区块链数字货币盗窃事件,公私钥安全问题引起重视,提高钱包安全性问题迫在眉睫。

[0016] 因此,提供一种区块链数据传输方法及区块链数据传输系统。

发明内容

[0017] 鉴于上述问题,提出了本发明以便提供一种克服上述问题或者至少部分地解决上述问题的区块链数据传输方法及区块链数据传输系统,解决现有区块链上数据传输的安全性差问题。

[0018] 根据本发明的一个方面,提供一种区块链数据传输方法,包括以下步骤:

[0019] 对交易数据进行至少两次哈希运算,获得第一摘要信息;

[0020] 利用至少两个私钥对所述第一摘要信息进行多次加密,获得交易数据的数字签名信息;

[0021] 将所述交易数据、所述交易数据的数字签名信息以及所述至少两个私钥对应的至少两个公钥发送给区块链网络节点。

[0022] 进一步地,所述对交易数据进行至少两次哈希运算的步骤包括:

[0023] 对交易数据采用第三代安全散列算法进行至少两次哈希运算。

[0024] 进一步地,上述区块链数据传输方法,利用至少两个私钥对所述第一摘要信息进行多次加密,获得交易数据的数字签名信息之前,还包括:

[0025] 对交易账户生成一级权限账户和二级权限账户,一级权限账户和二级权限账户分别包含至少两个秘钥对,每个秘钥对分别包含私钥和公钥;

[0026] 利用至少两个私钥对所述第一摘要信息进行多次加密的步骤包括:

[0027] 利用二级权限账户的至少两个秘钥对的私钥对所述第一摘要信息进行多次加密。

[0028] 进一步地,一级权限账户和二级权限账户还包含每个秘钥对分别对应的权重以及权重阈值;

[0029] 将所述交易数据、所述交易数据的数字签名信息以及所述至少两个私钥对应的至少两个公钥发送给区块链网络节点的同时还包括:

[0030] 将二级权限账户每个秘钥对分别对应的权重以及权重阈值发送给区块链网络节点。

[0031] 进一步地,上述区块链数据传输方法,还包括:

[0032] 接收对二级权限账户的修改请求;

[0033] 利用一级权限账户的至少两个秘钥对修改请求进行验证;

[0034] 在所修改请求验证通过时,执行所述修改请求。

[0035] 根据本发明的另一方面,提供一种区块链数据传输系统,包括:

[0036] 第一摘要信息生成模块,用于对交易数据进行至少两次哈希运算,获得第一摘要信息;

[0037] 数字签名模块,用于利用至少两个私钥对所述第一摘要信息进行多次加密,获得

交易数据的数字签名信息；

[0038] 数据发送模块，用于将所述交易数据、所述交易数据的数字签名信息以及所述至少两个私钥对应的至少两个公钥发送给区块链网络节点。

[0039] 根据本发明的又一方面，提供一种区块链数据传输方法，包括：

[0040] 接收交易数据、交易数据的数字签名信息以及至少两个公钥，其中，所述交易数据的数字签名信息是发送节点对交易数据进行至少两次哈希运算，获得第一摘要信息之后，利用至少两个私钥对所述第一摘要信息进行多次加密获得的数字签名信息；所述至少两个公钥是至少两个私钥对应的公钥；

[0041] 利用所述至少两个公钥对所述交易数据的数字签名信息进行多次解密，获得解密后的第二摘要信息；

[0042] 对所述交易数据进行至少两次哈希运算，获得第三摘要信息；

[0043] 当所述第二摘要信息与所述第三摘要信息一致时，向区块链网络广播所述交易数据的数字签名认证通过的消息。

[0044] 进一步地，对所述交易数据进行至少两次哈希运算的步骤包括：

[0045] 对所述交易数据采用第三代安全散列算法进行至少两次哈希运算。

[0046] 进一步地，上述区块链数据传输方法，向区块链网络广播所述交易数据的数字签名认证通过的消息之前，还包括：

[0047] 接收二级权限账户每个秘钥对分别对应的权重以及权重阈值；

[0048] 获取二级权限账户每个秘钥对按照对应的权重进行加权运算后的加权值；

[0049] 向区块链网络广播所述交易数据的数字签名认证通过的消息的步骤包括：

[0050] 当所述加权值大于或等于所述权重阈值，且所述第二摘要信息与所述第三摘要信息一致时，向区块链网络广播所述交易数据的数字签名认证通过的消息。

[0051] 根据本发明的还一方面，提供一种区块链数据传输系统，包括：

[0052] 数据接收模块，用于接收交易数据、交易数据的数字签名信息以及至少两个公钥，其中，所述交易数据的数字签名信息是发送节点对交易数据进行至少两次哈希运算，获得第一摘要信息之后，利用至少两个私钥对所述第一摘要信息进行多次加密获得的数字签名信息；所述至少两个公钥是至少两个私钥对应的公钥；

[0053] 数字签名信息解密模块，用于利用所述至少两个公钥对所述交易数据的数字签名信息进行多次解密，获得解密后的第二摘要信息；

[0054] 第三摘要信息生成模块，用于对所述交易数据进行至少两次哈希运算，获得第三摘要信息；

[0055] 数字签名认证模块，用于当所述第二摘要信息与所述第三摘要信息一致时，向区块链网络广播所述交易数据的数字签名认证通过的消息。

[0056] 本发明与现有技术相比具有以下的优点：

[0057] 1.本发明的区块链数据传输方法及区块链数据传输系统通过至少两次哈希Hash算法，既可以提高Hash内部操作复杂度，又可以提高Hash输出长度，使得任意输入改变都可以产生不同的输出，提高了抵御攻击的能力，且在不牺牲抵御冲突前提下具有高效性。

[0058] 2.本发明的区块链数据传输方法及区块链数据传输系统利用至少两个私钥进行多次加密，即多重数字签名技术，既可以满足数字签名可用性和不可逆性两个基本特征，又

可以增加信息可信度，能充分验证信息不是伪造的，且在传播过程中未被篡改，提高了数字钱包安全性。

附图说明

[0059] 以下结合附图和实施例对本发明作进一步说明。

[0060] 图1是本发明第一实施例的区块链数据传输方法流程图；

[0061] 图2是本发明第一实施例的区块链数据传输系统结构图；

[0062] 图3是本发明第二实施例的区块链数据传输方法流程图；

[0063] 图4是本发明第二实施例的区块链数据传输系统结构图。

具体实施方式

[0064] 下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

[0065] 本技术领域技术人员可以理解，除非特意声明，这里使用的单数形式“一”、“一个”、“所述”和“该”也可包括复数形式。应该进一步理解的是，本发明的说明书中使用的措辞“包括”是指存在所述特征、整数、步骤、操作、元件和/或组件，但是并不排除存在或添加一个或多个其他特征、整数、步骤、操作、元件、组件和/或它们的组。

[0066] 本技术领域技术人员可以理解，除非另外定义，这里使用的所有术语(包括技术术语和科学术语)，具有与本发明所属领域中的普通技术人员的一般理解相同的意义。还应该理解的是，诸如通用字典中定义的那些术语，应该被理解为具有与现有技术的上下文中的意义一致的意义，并且除非被特定定义，否则不会用理想化或过于正式的含义来解释。

[0067] 区块链中，数字签名技术包含两种运算算法：签名和验证。签名就是利用私钥处理信息或信息的哈希数值而产生的签名。验证则是使用公钥验证签名的真实性。数字签名技术作用是保证发送信息不会被篡改。

[0068] 图1是本发明第一实施例的区块链数据传输方法流程图，如图1所示，本发明实施例提供的区块链数据传输方法，包括以下步骤：

[0069] S101，对交易数据进行至少两次哈希运算，获得第一摘要信息。

[0070] 在这里，第一摘要信息是指对交易数据进行哈希运算之后得到的哈希值，无论交易数据有多大，都可以生成一个固定长度的摘要信息。通过对交易数据进行至少两次哈希运算，既可以提高哈希内部操作复杂度，又可以提高哈希输出长度，从而提高抵御攻击的能力，同时具有高效性。

[0071] 优选的，对交易数据可采用第三代安全散列算法(SHA3)进行至少两次哈希运算。和第一代安全散列算法，第二代安全散列算法不一样，第三代安全散列算法并不是单纯扩展字节数，而是采用了新的Keccak算法(Keccak是一种被选定为第三代安全散列标准的单向散列函数算法)。SHA3是从根本上替代SHA2的新标准，内部算法机制完全不同，SHA3具备海绵结构机制，可以使用随机排列组合来吸收和输出数据，同时还给位未来输入数值提供随机源。在海绵体制中，数据被吸收到海绵中，然后结果被挤出，有一个吸收和挤压阶段。因

此,同样字节宽度的第三代安全散列算法比第二代安全散列算法更安全。

[0072] 长度扩展攻击要求恶意攻击者知道哈希输入长度,在这个长度基础上加上一个秘密的字符串,就可以发送哈希函数内部的一部分,扰乱哈希函数。为了缓解长度扩展攻击,本发明实施例可按照以下公式对交易数据运行两次SHA3函数运算,即可增加算法复杂度又可增加信息生成的数字字符串的长度。

[0073] H＝SHA3(SHA3(X))

[0074] 其中,H为第一摘要信息,X为交易数据,SHA3(X)为一次哈希运算结果。

[0075] 在本文中,优选KECCAK256算法对交易数据进行哈希运算,这是因为KECCAK256算法的海绵(Sponge)结构作用于输入值维持一个内部状态,使得输出信息比字符串长度长(同时能够做到对于信息的压缩),这使它克服了先前算法的局限性。KECCAK算法的立体加密思想和海绵结构,使SHA-3优于SHA-2,甚至AES(Advanced Encryption Standard,高级加密标准)。Sponge函数可建立从任意长度输入到任意长度输出的映射。

[0076] 本发明实施例的上述Hash算法满足以下两个特征:第一,任何地输入的改变都会产生不同的输出;第二,在不牺牲抵御冲突前提下,具有高效性。

[0077] 本发明实施例通过两次连续SHA3运算不仅能够增加算法内部复杂度,使得任意输入改变都可以产生不同的输出,而且生成的数字序列长度增加,提高了抵御攻击的能力,同时也可在解决抵御冲突前提下,提高效率。

[0078] S102,利用至少两个私钥对所述第一摘要信息进行多次加密,获得交易数据的数字签名信息。

[0079] 本步骤中,利用至少两个私钥对第一摘要信息进行多次加密,即采用多重数字签名技术增加了信息可信度,能充分验证信息不是伪造的,且在传播过程中未被篡改,以提高数字钱包安全性。

[0080] 在这里,数字签名可采用ECDSA椭圆曲线数字签名多重算法。特别地,私钥的个数与加密次数相同。利用至少两个私钥对所述第一摘要信息进行多次加密,使得第一摘要信息的获取更难被攻击,确保第一摘要信息的安全性。

[0081] 本发明实施例的数字签名满足以下两个要求:

[0082] 1)可用性。信息被私钥加密之后可以被公钥解密,并且可以得到正确的结果。

[0083] 2)不逆向性。即使拿到无数的密文,也无法获取私钥的内容,更加无法伪造私钥对其它信息进行加密。

[0084] S103,将所述交易数据、所述交易数据的数字签名信息以及所述至少两个私钥对应的至少两个公钥发送给区块链网络节点。

[0085] 这里,通过将交易数据、交易数据的数字签名信息以及至少两个私钥对应的至少两个公钥发送给区块链网络节点,使得区块链网络节点能够利用至少两个公钥对交易数据的数字签名信息进行多次解密,获得解密后的第二摘要信息;然后对交易数据进行至少两次哈希运算,获得第三摘要信息;当第二摘要信息与第三摘要信息一致时,向区块链网络广播交易数据的数字签名认证通过的消息。由于采用了多重数字签名技术,因此提高了信息可信度,能充分验证信息不是伪造的,且在传播过程中未被篡改,从而提高了数字钱包安全性。

[0086] 具体地,当步骤S102中利用两个私钥对所述第一摘要信息进行两次加密时,发送

给区块链网络节点的公钥个数也是两个，也就是说，公钥和私钥是成对生成且一一对应的。

[0087] 本发明实施例的区块链数据传输方法，通过至少两次哈希算法，提高了哈希内部操作复杂度和哈希输出长度，使得任意输入改变都可以产生不同的输出，提高了抵御攻击的能力，且在不牺牲抵御冲突前提下具有高效性，同时利用至少两个私钥进行多次加密，即多重数字签名技术增加了信息可信度，能充分验证信息不是伪造的，且在传播过程中未被篡改，提高了数字钱包安全性。

[0088] 优选的，上述区块链数据传输方法，利用至少两个私钥对所述第一摘要信息进行多次加密，获得交易数据的数字签名信息之前，还包括：

[0089] 对交易账户生成一级权限账户和二级权限账户，一级权限账户和二级权限账户分别包含至少两个秘钥对，每个秘钥对分别包含私钥和公钥。

[0090] 这里，通过对交易账户生成两级账户，更有利于账户管理以及确保账户安全。其中一级权限账户可用来管理其它权限变更，比如修改二级权限账户对应秘钥，新建或者删除对应权限等等。二级权限账户可用于实现转账交易或者实现智能合约过程中的数字签名加密。

[0091] 具体地，当创建一个交易账户时，默认包含owner和active两个权限账户，一级权限账户为owner权限账户，二级权限账户为active权限账户，一个权限账户生成两对秘钥对。

[0092] 基于两级账户，利用至少两个私钥对所述第一摘要信息进行多次加密的步骤包括：

[0093] 利用二级权限账户的至少两个秘钥对的私钥对所述第一摘要信息进行多次加密。

[0094] 这里，利用二级权限账户的至少两个秘钥对的私钥对第一摘要信息进行多次加密，即采用多重数字签名技术增加了信息可信度，能充分验证信息不是伪造的，且在传播过程中未被篡改，以提高数字钱包安全性。

[0095] 其中，二级权限账户的私钥个数可与对第一摘要信息加密的次数相同。

[0096] 本发明实施例，当创建一账户时候，天然产生两个秘钥对，这样可以保护钱包安全。

[0097] 本发明实施例，在区块链中，发送信息的节点，先对信息进行Hash运算，即连续两次SHA3运算，然后利用active权限账户的两个私钥进行私钥加密，并且信息附带摘要密文广播给剩下的所有节点。

[0098] 优选的，一级权限账户和二级权限账户还包含每个秘钥对分别对应的权重以及权重阈值；

[0099] 在这里，owner权限账户和active权限账户包含每个秘钥对分别对应的权重以及权重阈值。

[0100] 将所述交易数据、所述交易数据的数字签名信息以及所述至少两个私钥对应的至少两个公钥发送给区块链网络节点的同时还包括：

[0101] 将二级权限账户每个秘钥对分别对应的权重以及权重阈值发送给区块链网络节点。

[0102] 这里，通过将二级权限账户每个秘钥对分别对应的权重以及权重阈值发送给区块链网络节点，使得区块链网络节点能够获取二级权限账户每个秘钥对按照对应的权重进行

加权运算后的加权值，并当加权值大于或等于权重阈值，且第二摘要信息与第三摘要信息一致时，向区块链网络广播交易数据的数字签名认证通过的消息，即通过权重阈值验证和多重数字加密验证，进一步增加了信息可信度，确保了信息安全性。

[0103] 优选的，上述区块链数据传输方法，还包括：

[0104] 接收对二级权限账户的修改请求；

[0105] 利用一级权限账户的至少两个秘钥对修改请求进行验证；

[0106] 在所修改请求验证通过时，执行所述修改请求。

[0107] 这里，在对二级权限账户的修改时，需要利用一级权限账户的至少两个秘钥对修改请求进行验证，提高了账户安全性，避免了非法节点的恶意篡改。

[0108] 具体地，owner权限账户作为一级权限账户用于管理其它权限变更，比如修改active权限账户对应秘钥对，新建或者删除对应权限等等。更详细地，如果需要修改了active权限账户的密钥，需要使用owner权限账户的密钥同时对这个操作进行签名，因此，使用四对密钥来管理账户，安全性非常之高，解决了钱包不安全的问题。

[0109] 其中，利用一级权限账户的至少两个秘钥对修改请求进行验证的过程可以是利用一级权限账户的至少两个秘钥对的私钥对修改请求进行多次加密，获得修改请求的数字签名，然后将修改请求、修改请求的数字签名以及一级权限账户的至少两个秘钥对的公钥发送给验证节点，使得验证节点利用至少两个公钥对数字签名进行验证。

[0110] 本发明实施例的区块链数据传输方法，通过至少两次哈希算法，提高了哈希内部操作复杂度和哈希输出长度，使得任意输入改变都可以产生不同的输出，提高了抵御攻击的能力，且在不牺牲抵御冲突前提下具有高效性，同时利用至少两个私钥进行多次加密，即多重数字签名技术增加了信息可信度，能充分验证信息不是伪造的，且在传播过程中未被篡改，提高了数字钱包安全性。

[0111] 图2是本发明第一实施例的区块链数据传输系统结构图，如图2所示，本发明实施例提供的区块链数据传输系统，包括：

[0112] 第一摘要信息生成模块201，用于对交易数据进行至少两次哈希运算，获得第一摘要信息；

[0113] 数字签名模块202，用于利用至少两个私钥对所述第一摘要信息进行多次加密，获得交易数据的数字签名信息；

[0114] 数据发送模块203，用于将所述交易数据、所述交易数据的数字签名信息以及所述至少两个私钥对应的至少两个公钥发送给区块链网络节点。

[0115] 在第一摘要信息生成模块中，所述对交易数据进行至少两次哈希运算的步骤包括：

[0116] 对交易数据采用第三代安全散列算法进行至少两次哈希运算。

[0117] 本发明的区块链数据传输系统，还包括：

[0118] 权限账户生成模块，用于利用至少两个私钥对所述第一摘要信息进行多次加密，获得交易数据的数字签名信息之前，对交易账户生成一级权限账户和二级权限账户，一级权限账户和二级权限账户分别包含至少两个秘钥对，每个秘钥对分别包含私钥和公钥；

[0119] 其中，

[0120] 数字签名模块还用于利用二级权限账户的至少两个秘钥对的私钥对所述第一摘

要信息进行多次加密。

[0121] 在权限账户生成模块中，一级权限账户和二级权限账户还包含每个秘钥对分别对应的权重以及权重阈值；

[0122] 其中，数据发送模块将所述交易数据、所述交易数据的数字签名信息以及所述至少两个私钥对应的至少两个公钥发送给区块链网络节点的同时还用于将二级权限账户每个秘钥对分别对应的权重以及权重阈值发送给区块链网络节点。

[0123] 一级权限账户还用于接收对二级权限账户的修改请求；利用一级权限账户的至少两个秘钥对修改请求进行验证；在所修改请求验证通过时，执行所述修改请求。

[0124] 对于系统实施例而言，由于其与方法实施例基本相似，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[0125] 本发明一实施例还提供了一种智能合约执行系统，包括处理器，存储器，存储在存储器上并可在所述处理器上运行的计算机程序，该计算机程序被处理器执行时实现如下步骤：

[0126] 对交易数据进行至少两次哈希运算，获得第一摘要信息；

[0127] 利用至少两个私钥对所述第一摘要信息进行多次加密，获得交易数据的数字签名信息；

[0128] 将所述交易数据、所述交易数据的数字签名信息以及所述至少两个私钥对应的至少两个公钥发送给区块链网络节点。

[0129] 可选的，该计算机程序被处理器执行时还实现如下步骤：

[0130] 对交易数据采用第三代安全散列算法进行至少两次哈希运算。

[0131] 可选的，该计算机程序被处理器执行时还实现如下步骤：

[0132] 利用至少两个私钥对所述第一摘要信息进行多次加密，获得交易数据的数字签名信息之前，对交易账户生成一级权限账户和二级权限账户，一级权限账户和二级权限账户分别包含至少两个秘钥对，每个秘钥对分别包含私钥和公钥；

[0133] 利用二级权限账户的至少两个秘钥对的私钥对所述第一摘要信息进行多次加密。

[0134] 可选的，一级权限账户和二级权限账户还包含每个秘钥对分别对应的权重以及权重阈值；该计算机程序被处理器执行时还实现如下步骤：将二级权限账户每个秘钥对分别对应的权重以及权重阈值发送给区块链网络节点。

[0135] 可选的，该计算机程序被处理器执行时还实现如下步骤：

[0136] 接收对二级权限账户的修改请求；

[0137] 利用一级权限账户的至少两个秘钥对修改请求进行验证；

[0138] 在所修改请求验证通过时，执行所述修改请求。

[0139] 本发明一实施例提供了一种计算机可读存储介质，其上存储有计算机程序，上述计算机程序被处理器执行时实现上述智能合约执行方法实施例的各个过程，且能达到相同的技术效果，为避免重复，这里不再赘述。其中，所述的计算机可读存储介质，如只读存储器(Read-Only Memory，简称ROM)、随机存取存储器(Random Access Memory，简称RAM)、磁碟或者光盘等。

[0140] 图3是本发明第二实施例的区块链数据传输方法流程图，如图3所示，本发明实施例提供的区块链数据传输方法，包括：

[0141] S301，接收交易数据、交易数据的数字签名信息以及至少两个公钥，其中，所述交易数据的数字签名信息是发送节点对交易数据进行至少两次哈希运算，获得第一摘要信息之后，利用至少两个私钥对所述第一摘要信息进行多次加密获得的数字签名信息；所述至少两个公钥是至少两个私钥对应的公钥。

[0142] S302，利用所述至少两个公钥对所述交易数据的数字签名信息进行多次解密，获得解密后的第二摘要信息。

[0143] 在这里，对应于步骤S102中用于加密的私钥个数，加密次数和加密算法，当加密的私钥个数是两个，加密次数为两次，且根据椭圆曲线数字签名算法进行加密时，这一步骤中利用两个公钥根据椭圆曲线数字签名认证算法对交易数据的数字签名信息进行两次解密，其中，这一步骤中的公钥与步骤S102中的私钥一一对应。

[0144] S303，对所述交易数据进行至少两次哈希运算，获得第三摘要信息。

[0145] 优选的，对所述交易数据可采用第三代安全散列算法进行至少两次哈希运算。第三代安全散列算法与步骤S101中进行哈希运算的算法相同。

[0146] S304，当所述第二摘要信息与所述第三摘要信息一致时，向区块链网络广播所述交易数据的数字签名认证通过的消息。

[0147] 在这里，利用多重数字签名认证能够确保信息是发送者发送的，不是伪造的，并且信息在发送过程中没有被篡改，因此，这一步骤用于校验第一摘要信息是否被篡改，只要交易数据被修改任意一任意一个字节，第一摘要信息的校验都会失败。

[0148] 本发明实施例的区块链数据传输方法，发送节点通过至少两次哈希算法，提高了哈希内部操作复杂度和哈希输出长度，使得任意输入改变都可以产生不同的输出，提高了抵御攻击的能力，且在不牺牲抵御冲突前提下具有高效性，同时发送节点利用至少两个私钥进行多次加密，即多重数字签名技术增加了信息可信度，接收节点通过多重数字签名验证能充分验证信息不是伪造的，且在传播过程中未被篡改，提高了数字钱包安全性。

[0149] 优选的，上述区块链数据传输方法，向区块链网络广播所述交易数据的数字签名认证通过的消息之前，还包括：

[0150] 接收二级权限账户每个秘钥对分别对应的权重以及权重阈值；

[0151] 获取二级权限账户每个秘钥对按照对应的权重进行加权运算后的加权值；

[0152] 向区块链网络广播所述交易数据的数字签名认证通过的消息的步骤包括：

[0153] 当所述加权值大于或等于所述权重阈值，且所述第二摘要信息与所述第三摘要信息一致时，向区块链网络广播所述交易数据的数字签名认证通过的消息。

[0154] 此时，接收节点通过权重阈值验证和多重数字加密验证，进一步增加了信息可信度，确保了信息安全性。

[0155] 具体地，节点A转账给节点B，需要把节点A二级权限账户中进行数字签名的两个私钥权重相加，如果结果大于或等于私钥权重阈值，则交易可以被认为合法，否则认为不合法。

[0156] 本发明实施例的上述方法，接收节点在接收到发送者信息时候，先验证其身份，然后验证其是否被篡改。具体的，接收节点接收到发送节点发来的数据包，其中包括发送节点的两个公钥信息/数字签名/信息数据文件；接收节点会对信息数据做两次SHA3加密算法得到一串散列数值；接收节点利用发送节点给予的两个公钥对数字签名进行解密，得出一串

散列值;通过两次SHA3加密算法得到的散列数值跟数字签名解密得到的散列数值进行对比,若相同则签名有效。签名有效说明信息在传输过程中没有被篡改,并且通过多重验证增加了可信度,证明信息是发送者发送的,不是伪造的。且满足数字签名两个要求。

[0157] 本发明利用两次SHA3哈希算法对交易数据进行加密生成摘要,增加了哈希算法内部复杂度,增大了生成散列数值长度,同时,利用多重数字签名技术,可以让交易数据产生的摘要跟多个私钥一起加密生成数字签名,保证了数字钱包安全性,因为多重签名,数字签名验证技术能够更好的验证交易数据无篡改并且确实是发送者所发送的。

[0158] 本发明通过多次SHA3哈希算法、多重数字签名和多次数字签名认证的结合,不仅提高Hash内部操作复杂度,提高Hash输出长度,还保证满足数字签名可用性和不可逆性的两个特征,又满足数字签名验证确认信息不是伪造的,并且在传播过程中没有被篡改这一目的,使得本发明能够确保区块链数据的安全传输。

[0159] 图4是本发明第二实施例的区块链数据传输系统结构图,如图4所示,本发明实施例提供的区块链数据传输系统,包括:

[0160] 数据接收模块401,用于接收交易数据、交易数据的数字签名信息以及至少两个公钥,其中,所述交易数据的数字签名信息是发送节点对交易数据进行至少两次哈希运算,获得第一摘要信息之后,利用至少两个私钥对所述第一摘要信息进行多次加密获得的数字签名信息;所述至少两个公钥是至少两个私钥对应的公钥;

[0161] 数字签名信息解密模块402,用于利用所述至少两个公钥对所述交易数据的数字签名信息进行多次解密,获得解密后的第二摘要信息;

[0162] 第三摘要信息生成模块403,用于对所述交易数据进行至少两次哈希运算,获得第三摘要信息;

[0163] 数字签名认证模块404,用于当所述第二摘要信息与所述第三摘要信息一致时,向区块链网络广播所述交易数据的数字签名认证通过的消息。

[0164] 此外,第三摘要信息生成模块,还用于对所述交易数据采用第三代安全散列算法进行至少两次哈希运算。

[0165] 本发明的区块链数据传输系统,还包括:

[0166] 加权值获取模块,获取二级权限账户每个秘钥对按照对应的权重进行加权运算后的加权值;

[0167] 其中,

[0168] 数据接收模块,还用于向区块链网络广播所述交易数据的数字签名认证通过的消息之前,接收二级权限账户每个秘钥对分别对应的权重以及权重阈值;

[0169] 数字签名认证模块还用于在所述加权值大于或等于所述权重阈值,且所述第二摘要信息与所述第三摘要信息一致时,向区块链网络广播所述交易数据的数字签名认证通过的消息。

[0170] 对于系统实施例而言,由于其与方法实施例基本相似,所以描述的比较简单,相关之处参见方法实施例的部分说明即可。

[0171] 本发明一实施例还提供了一种智能合约执行系统,包括处理器,存储器,存储在存储器上并可在所述处理器上运行的计算机程序,该计算机程序被处理器执行时实现如下步骤:

[0172] 接收交易数据、交易数据的数字签名信息以及至少两个公钥，其中，所述交易数据的数字签名信息是发送节点对交易数据进行至少两次哈希运算，获得第一摘要信息之后，利用至少两个私钥对所述第一摘要信息进行多次加密获得的数字签名信息；所述至少两个公钥是至少两个私钥对应的公钥；

[0173] 利用所述至少两个公钥对所述交易数据的数字签名信息进行多次解密，获得解密后的第二摘要信息；

[0174] 对所述交易数据进行至少两次哈希运算，获得第三摘要信息；

[0175] 当所述第二摘要信息与所述第三摘要信息一致时，向区块链网络广播所述交易数据的数字签名认证通过的消息。

[0176] 可选的，该计算机程序被处理器执行时还实现如下步骤：

[0177] 对所述交易数据采用第三代安全散列算法进行至少两次哈希运算。

[0178] 可选的，该计算机程序被处理器执行时还实现如下步骤：

[0179] 向区块链网络广播所述交易数据的数字签名认证通过的消息之前，接收二级权限账户每个秘钥对分别对应的权重以及权重阈值；

[0180] 获取二级权限账户每个秘钥对按照对应的权重进行加权运算后的加权值；

[0181] 当所述加权值大于或等于所述权重阈值，且所述第二摘要信息与所述第三摘要信息一致时，向区块链网络广播所述交易数据的数字签名认证通过的消息。

[0182] 本发明一实施例提供了一种计算机可读存储介质，其上存储有计算机程序，上述计算机程序被处理器执行时实现上述智能合约执行方法实施例的各个过程，且能达到相同的技术效果，为避免重复，这里不再赘述。其中，所述的计算机可读存储介质，如只读存储器(Read-Only Memory，简称ROM)、随机存取存储器(Random Access Memory，简称RAM)、磁碟或者光盘等。

[0183] 在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述的部分，可以参见其他实施例的相关描述。

[0184] 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。

[0185] 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，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(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。

[0186] 以上实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

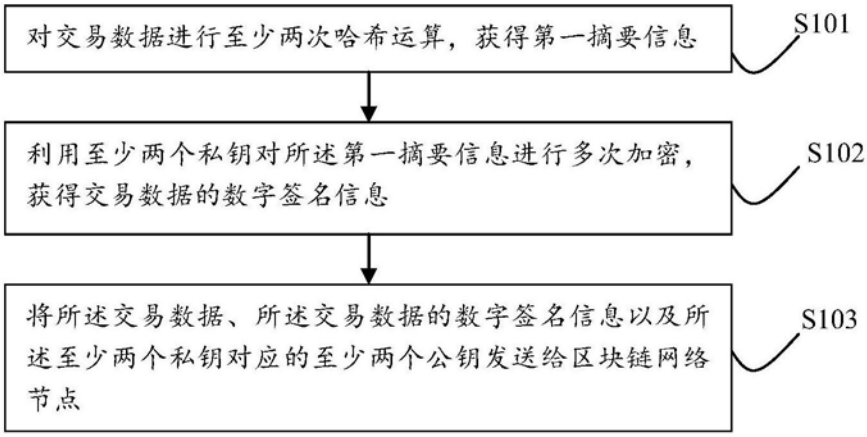

对交易数据进行至少两次哈希运算，获得第一摘要信息
S101
利用至少两个私钥对所述第一摘要信息进行多次加密，获得交易数据的数字签名信息
S102
将所述交易数据、所述交易数据的数字签名信息以及所述至少两个私钥对应的至少两个公钥发送给区块链网络节点
S103

图1

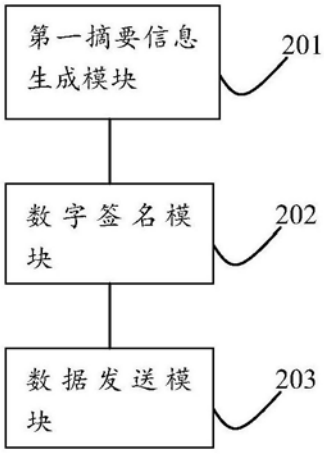

第一摘要信息生成模块
201
数字签名模块
202
数据发送模块
203

图2

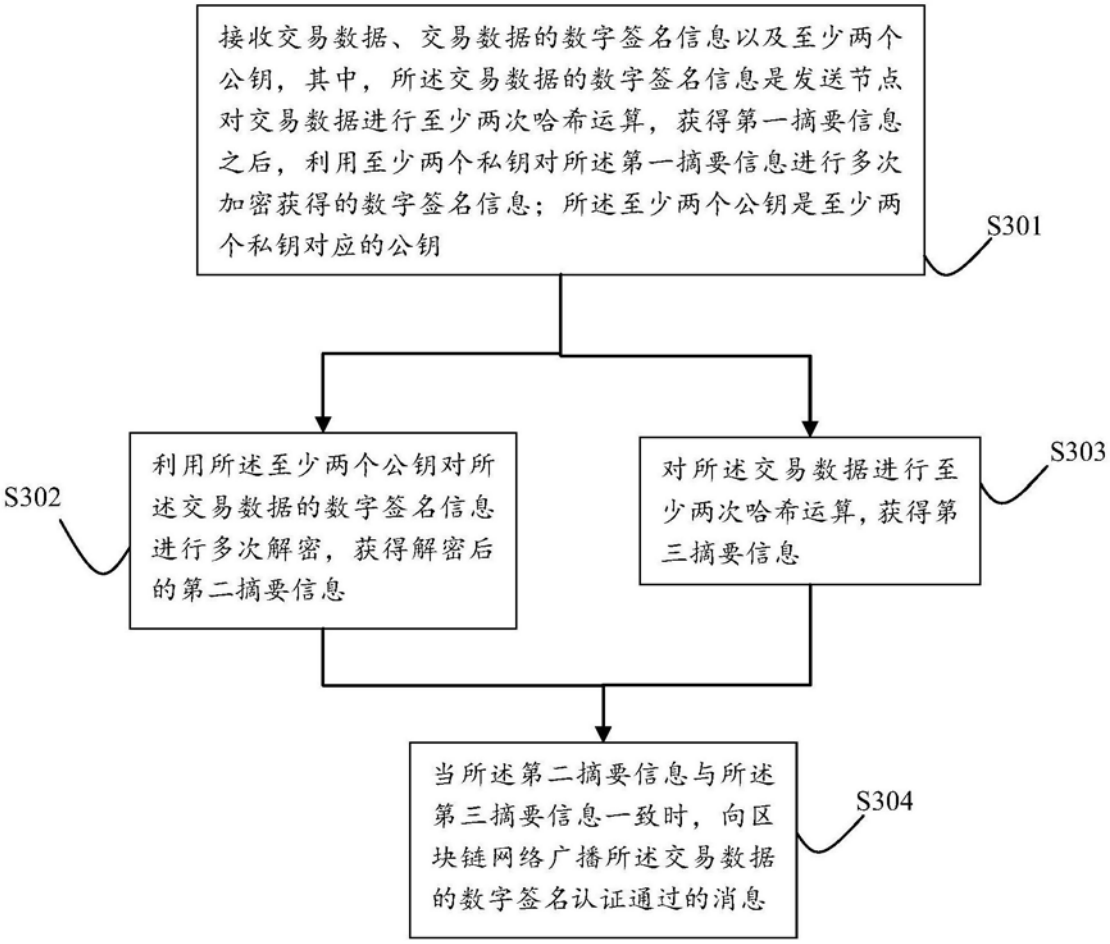

接收交易数据、交易数据的数字签名信息以及至少两个公钥，其中，所述交易数据的数字签名信息是发送节点对交易数据进行至少两次哈希运算，获得第一摘要信息之后，利用至少两个私钥对所述第一摘要信息进行多次加密获得的数字签名信息；所述至少两个公钥是至少两个私钥对应的公钥
S301
利用所述至少两个公钥对所述交易数据的数字签名信息进行多次解密，获得解密后的第二摘要信息
S302
对所述交易数据进行至少两次哈希运算，获得第三摘要信息
S303
当所述第二摘要信息与所述第三摘要信息一致时，向区块链网络广播所述交易数据的数字签名认证通过的消息
S304

图3

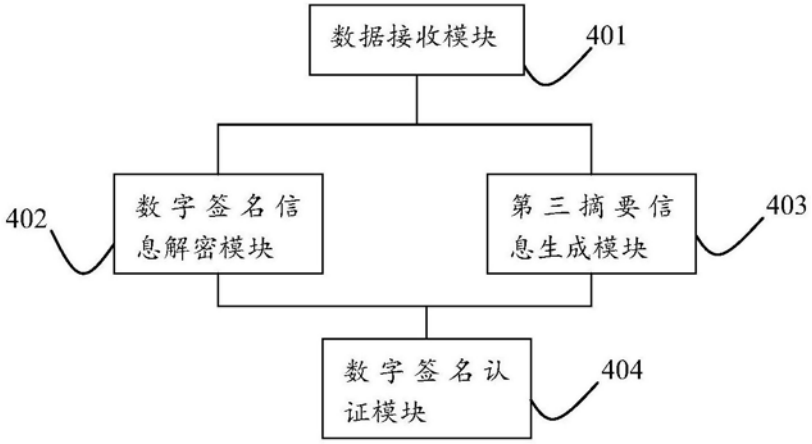

数据接收模块
401
数字签名信息解密模块
402
第三摘要信息生成模块
403
数字签名认证模块
404

图4