(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
2019 年 10 月 31 日 (31.10.2019)

WIPO | PCT

(10) 国际公布号
WO 2019/209168 A2

(51) 国际专利分类号:
H04L 9/30 (2006.01) *G06Q 20/38* (2012.01)
H04L 9/32 (2006.01) *H04L 9/00* (2006.01)

(21) 国际申请号: PCT/SG2018/050200

(22) 国际申请日: 2018 年 4 月 26 日 (26.04.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人: 华为国际有限公司 (HUAWEI INTERNATIONAL PTE. LTD.) [SG/SG]; 新加坡新加坡新加坡签名大厦樟宜商务园中央2 #07-08 51号, Singapore 486066 (SG)。

(72) 发明人: 阮子瀚 (YUEN, Tsz Hon); 新加坡新加坡新加坡科学园路,20号,电信科技园,#03-31/32, Singapore 117674 (SG)。 吴双 (WU, Shuang); 新加坡新加坡新加坡科学园路,20号,电信科技园,#03-31/32, Singapore 117674 (SG)。 贺伟 (HE, Wei); 新加坡新加坡新加坡科学园路,20号,电信科技园,#03-31/32, Singapore 117674 (SG)。

(74) 代理人: 艾伦格禧有限责任合伙律师事务所 (ALLEN & GLEDHILL LLP); 新加坡新加坡一号滨海林荫道#28-00, Singapore 018989 (SG)。

(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,

(54) **Title:** DATA PROCESSING METHOD, RELATED APPARATUS, AND BLOCKCHAIN SYSTEM

(54) **发明名称:** 数据处理方法、相关装置及区块链系统

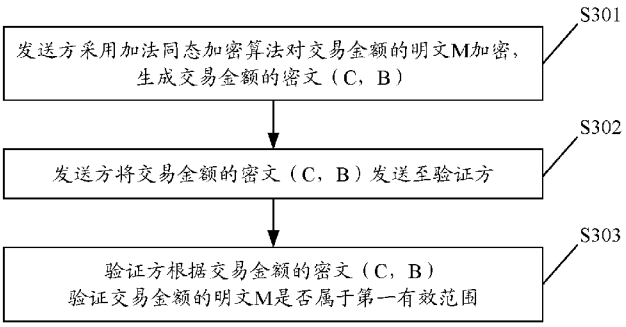

图 3

S301 ... A sender using an addition homomorphic encryption algorithm to encrypt a plaintext M of a transaction amount so as to generate a ciphertext (C, B) of the transaction amount

S302 ... The sender sending the ciphertext (C, B) of the transaction amount to a verification party

S303 ... According to the ciphertext (C, B) of the transaction amount, the verification party verifying whether the plaintext M of the transaction amount is within a first effective range

(57) **Abstract:** Provided in an embodiment of the present application are a data processing method, a related apparatus, and a blockchain system, wherein the method comprises: a sender using an addition homomorphic encryption algorithm to encrypt a plaintext M of a transaction amount so as to generate a ciphertext of the transaction amount, the bit length of the plaintext M of the transaction amount being U; the sender sending the ciphertext of the transaction amount to a verification party; according to the ciphertext of the transaction amount, the verification party verifying whether the plaintext M of the transaction amount is within a first effective range, the

WO 2019/209168 A2

[见续页]

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：

- 不包括国际检索报告，在收到该报告后将重新公布(细则48.2(g))。
- 黑白；提交的国际申请包含彩色或灰度，并且可通过PATENTSCOPE下载

first effective range being [0, 2^U-1]. The embodiment of the present application may protect the privacy of a transaction amount in a blockchain system, and protect the legitimacy of a transaction by verifying whether a transaction amount is within an effective range when a verification party is unable to learn the plaintext of the transaction amount.

(57) 摘要：本申请实施例提供了一种数据处理方法、相关装置及区块链系统，其中，该方法包括：发送方采用加法同态加密算法对交易金额的明文M加密，生成交易金额的密文；其中，上述交易金额的明文M的比特位长度为U；上述发送方将所述交易金额的密文发送至验证方；上述验证方根据上述交易金额的密文验证上述交易金额的明文M是否属于第一有效范围；上述第一有效范围为[0，2^U-1]。实施本申请实施例可以在区块链系统中保护交易金额的隐私，在验证方无法获知交易金额的明文的情况下，验证交易金额是否在有效范围内，保证交易的合法性。

数据处理方法、相关装置及区块链系统

技术领域

本申请涉及区块链技术领域，尤其涉及一种数据处理方法、相关装置及区块链系统。

背景技术

区块链是一个分布式数据库，它保持不断增长的名为区块（block）的有序记录列表。每个块包含一个时间戳和指向前一个区块的链接。区块链天然具有防篡改数据的功能，一旦记录，块中的数据不能被单方面修改。通过使用对等网络（Peer to Peer，P2P）和分布式时间戳服务器，区块链上的数据可以实现自动管理。区块链是一个开放的分布式分类帐，可以有效地记录双方之间的交易以及其它各种信息，并以可验证的方式永久记录。传统区块链上，用户的账户余额没有经过加密直接存储在区块上，导致用户的账户完全暴露在所有节点上。这种方式在实现了区块链去中心化、信息不可篡改的基本功能外，用户的账户隐私完全暴露在区块链的所有节点上。

现有技术中，采用加法同态加密可以保护区块链系统中交易金额的隐私的问题，但无法使验证方验证交易是否有效。因为验证方只能确定输出金额的明文与输入金额的明文相等，而无法确认输入金额的明文和输出金额的明文是否在有效范围内。因此，如何在区块链系统中保护交易金额隐私，在验证节点无法获知交易金额的明文的情况下，验证交易金额的明文是否在有效范围内是亟待解决的问题。

发明内容

本申请实施例提供了一种数据处理方法、相关装置及区块链系统，可以保护交易金额的隐私，在验证方无法获知交易金额的明文的情况下，验证交易金额是否在有效范围内，保证交易的合法性。

第一方面，本申请实施例提供了一种数据处理方法，应用于区块链系统，所述系统包括发送方及验证方，所述方法包括：所述发送方采用加法同态加密算法对交易金额的明文 M 加密，生成交易金额的密文（C，B）；所述发送方将所述交易金额的密文（C，B）发送至所述验证方；所述验证方根据所述交易金额的密文（C，B）验证所述交易金额的明文 M 是否属于第一有效范围；所述第一有效范围为[0，2^U-1]，U 为所述交易金额的明文 M 的比特位长度。

实施本申请实施例可以在区块链系统中保护交易金额的隐私，在验证方无法获知交易金额的明文的情况下，验证交易金额是否在有效范围内，保证交易的合法性。

在一种可能的实现方式中，所述$C = g_3^M g_4^r$，$B = g_3^r$；其中，r 为随机生成的整数，g_3 为 G_1 的生成元，G_1 是阶为素数的乘法群，g_4 为所述加法同态加密算法的公钥，$g_4=g_3^{ask}$，ask 为所述加法同态加密算法的私钥。

在一种可能的实现方式中，所述系统还包括监管方；所述发送方采用加法同态加密算法对交易金额的明文 M 加密，生成交易金额的密文（C，B）包括：所述发送方将所述交易金额的明文 M 分割成 L 份交易金额的明文 M_k，分别采用加法同态加密算法对所述 L 份

交易金额的明文 M_k 进行加密，生成 L 份交易金额的密文（C_k，B_k）；所述加法同态加密算法的公钥由所述监管方提供，k 为正整数，k=1，...，L，L 为大于或等于 2 的正整数；所述验证方根据所述交易金额的密文（C，B）验证所述交易金额的明文 M 是否属于第一有效范围包括：所述验证方验证根据所述交易金额的密文（C_k，B_k）验证所述交易金额的明文 M_k 是否属于第二有效范围；其中，所述第二有效范围为[0，2^u-1]，u 为所述交易金额的明文 M_k 的比特位长度；所述方法还包括：所述监管方采用与所述公钥对应的私钥解密所述 L 份交易金额的密文（C_k，B_k），获得所述 L 份交易金额的明文 M_k，并根据所述 L 份交易金额的明文 M_k 获得所述交易金额的明文 M。

本申请实施例可以在交易金额明文长度较大时，先将交易金额的明文 M 分割成若干份小块的明文，然后再分别对每个小块的明文进行加密、以及其属于有效范围的证明等，保证监管方可以有效地解密每个小块交易金额的密文。

在一种可能的实现方式中，上述 L 份交易金额的明文 M_k 长度相等。

在一种可能的实现方式中，所述方法还包括：所述发送方生成所述交易金额的明文 M 属于第一有效范围的零知识证明；所述验证方根据所述交易金额的密文（C，B）验证所述交易金额的明文 M 是否属于第一有效范围包括：所述验证方验证所述交易金额的明文 M 属于第一有效范围的零知识证明。

本申请实施例可以在交易金额已加密的情况下，使验证方验证交易金额是否属于有效范围内，进而验证交易的合法性。

在一种可能的实现方式中，所述交易金额包括输出金额；所述方法还包括：所述发送方计算输入金额与输出金额的差值的密文 C'，并生成 C'是加密了明文为零的密文的加法同态零知识证明；其中，所述 C'为根据所述输出金额的密文与所述输入金额的密文计算得到的密文，所述输入金额的密文为所述发送方在上一次交易中接收的金额的密文，或者所述输入金额的密文为所述发送方采用所述加法同态加密算法对当前交易中生成的金额进行加密生成的密文；所述验证方验证所述 C'是加密了明文为零的密文的加法同态零知识证明。

本申请实施例可以在交易金额已加密的情况下，使验证方验证输入金额等于输出金额，进而验证交易的合法性。

在一种可能的实现方式中，所述系统还包括监管方，所述加法同态加密算法的公钥由所述监管方提供；所述方法还包括：所述发送方生成所述监管方可解密所述交易金额的密文（C，B）的零知识证明；所述验证方验证所述监管方可解密所述交易金额的密文（C，B）的零知识证明；所述监管方采用与所述公钥对应的私钥解密所述交易金额的密文（C，B）。

本申请实施例可以在交易金额已加密的情况下，使验证方验证监管方可解密交易金额的密文，从而验证密文的合法性。

在一种可能的实现方式中，所述系统还包括第三方，用于提供随机秘密 γ，所述随机秘密 γ 用于为所述第一有效范围内的每个整数生成一个数字签名；所述发送方生成所述交易金额的明文 M 属于第一有效范围的零知识证明包括：所述发送方根据所述第三方提供的随机秘密 γ 为所述第一有效范围内的每个整数生成数字签名生成所述交易金额的明文 M 属于第一有效范围的零知识证明。

本申请实施例提供了一种具体的证明交易金额密文中的明文属于有效范围的方法，为

有效范围内的每个数字生成一个数字签名，证明交易金额密文中的明文属于上述数字签名中的一个即可证明该交易金额密文中的明文属于有效范围。在不向验证方提供交易金额明文的情况下，验证交易金额的合法性，保证交易隐私。

在一种可能的实现方式中，所述发送方生成所述交易金额的明文 M 属于第一有效范围的零知识证明包括：所述发送方生成 N 个第一参数；N 为正整数；所述验证方验证所述交易金额的明文 M 属于第一有效范围的零知识证明包括：所述验证方生成 N 个第二参数；其中，所述 N 个第一参数与所述 N 个第二参数一一对应；所述验证方验证所述 N 个第二参数是否与对应的所述第一参数相等，若相等，则所述交易金额的明文 M 属于第一有效范围。

本申请实施例根据对比发送方生成的第一参数与验证方生成的第二参数，来验证交易金额密文中的明文是否属于有效范围，在不向验证方提供交易金额明文的情况下，验证交易金额的合法性，保证交易隐私。

在一种可能的实现方式中，所述发送方生成所述交易金额的明文 M 属于第一有效范围的零知识证明还包括：所述发送方生成第一验证参数；所述第一验证参数由所述 N 个第一参数决定；所述验证方验证所述交易金额的明文 M 属于第一有效范围的零知识证明还包括：所述验证方生成第二验证参数；所述第二验证参数由所述 N 个第二参数决定；所述验证方验证所述 N 个第二参数是否与对应的所述第一参数相等包括：所述验证方验证所述第一参数是否等于所述第二验证参数，若相等，则所述 N 个第二参数与相应的所述第一参数相等。

本申请实施例根据发送方生成的第一验证参数与验证方生成的第二验证参数来验证发送方生成的第一参数是否与验证方生成的第二参数相等，进而证明交易金额密文中的明文是否属于有效范围，在不向验证方提供交易金额明文的情况下，验证交易金额的合法性，保证交易隐私。

第二方面，本申请实施例提供了一种数据处理方法，应用于区块链系统，所述系统包括发送方及验证方，所述方法包括：所述发送方采用加法同态加密算法对交易金额的明文 M 加密，生成交易金额的密文（C，B）；所述发送方将所述交易金额的密文（C，B）发送至所述验证方，以使所述验证方根据所述交易金额的密文（C，B）验证所述交易金额的明文 M 是否属于第一有效范围；所述第一有效范围为[0，2^U-1]，U 为所述交易金额的明文 M 的比特位长度。

在一种可能的实现方式中，所述 $C = g_3^M g_4^r$，$B = g_3^r$；其中，r 为随机生成的整数，g_3 为 G_1 的生成元，G_1 是阶为素数的乘法群，g_4 为所述加法同态加密算法的公钥，$g_4=g_3^{ask}$，ask 为所述加法同态加密算法的私钥。

在一种可能的实现方式中，所述系统还包括监管方；所述发送方采用加法同态加密算法对交易金额的明文 M 加密，生成交易金额的密文（C，B）包括：所述发送方将所述交易金额的明文 M 分割成 L 份交易金额的明文 M_k，分别采用加法同态加密算法对所述 L 份交易金额的明文 M_k 进行加密，生成 L 份交易金额的密文（C_k，B_k），以使所述监管方采用与所述公钥对应的私钥解密所述 L 份交易金额的密文（C_k，B_k），获得所述 L 份交易金额的明文 M_k，并根据所述 L 份交易金额的明文 M_k 获得所述交易金额的明文 M；所述加法同态加密算法的公钥由所述监管方提供，k 为正整数，k=1，...，L；L 为大于或等于 2 的正整数；所述发送方将所述交易金额的密文（C，B）发送至所述验证方，以使所述验证方根

据所述交易金额的密文（C，B）验证所述交易金额的明文 M 是否属于第一有效范围包括：所述发送方将所述 L 份交易金额的密文（C_k，B_k）发送至所述验证方，以使所述验证方根据所述交易金额的密文（C_k，B_k）验证所述交易金额的明文 M_k 是否属于第二有效范围；其中，所述第二有效范围为[0，2^u-1]，u 为所述交易金额的明文 M_k 的比特位长度。

在一种可能的实现方式中，上述 L 份交易金额的明文 M_k 长度相等。

在一种可能的实现方式中，所述方法还包括：所述发送方生成所述交易金额的明文 M 属于第一有效范围的零知识证明；所述发送方将所述交易金额的密文（C，B）发送至所述验证方，以使所述验证方根据所述交易金额的密文（C，B）验证所述交易金额的明文 M 是否属于第一有效范围包括：所述发送方将所述交易金额的密文（C，B）发送至所述验证方，以使所述验证方根据所述交易金额的密文（C，B）验证所述交易金额的明文 M 属于第一有效范围的零知识证明。

在一种可能的实现方式中，所述交易金额包括输出金额；所述方法还包括：所述发送方计算输入金额与输出金额的差值的密文 C'，并生成 C'是加密了明文为零的密文的加法同态零知识证明，以使所述验证方验证所述 C'是加密了明文为零的密文的加法同态零知识证明；其中，所述 C'为根据所述输出金额的密文与所述输入金额的密文计算得到的密文，所述输入金额的密文为所述发送方在上一次交易中接收的金额的密文，或者所述输入金额的密文为所述发送方采用所述加法同态加密算法对当前交易中生成的金额进行加密生成的密文。

在一种可能的实现方式中，所述系统还包括监管方，所述加法同态加密算法的公钥由所述监管方提供；所述方法还包括：所述发送方生成所述监管方可解密所述交易金额的密文 C 的零知识证明，以使所述验证方验证所述监管方可解密所述交易金额的密文 C 的零知识证明。

在一种可能的实现方式中，所述系统还包括第三方，用于提供随机秘密 γ，所述随机秘密 γ 用于为所述第一有效范围内的每个整数生成一个数字签名；所述发送方生成所述交易金额的明文 M 属于第一有效范围的零知识证明包括：所述发送方根据所述第三方提供的随机秘密 γ 为所述第一有效范围内的每个整数生成的数字签名生成所述交易金额的明文 M 属于第一有效范围的零知识证明。

第三方面，本申请实施例提供了一种数据处理方法，应用于区块链系统，所述系统包括发送方及验证方，所述方法包括：所述验证方接收所述发送方发送的交易金额的密文（C，B）；其中，所述交易金额的密文（C，B）为所述发送方采用加法同态加密算法对交易金额的明文 M 加密生成的密文；所述交易金额的明文 M 的比特位长度为 U；所述验证方根据所述交易金额的密文（C，B）验证所述交易金额的明文 M 是否属于第一有效范围；所述第一有效范围为[0，2^U-1]。

在一种可能的实现方式中，所述验证方根据所述交易金额的密文（C，B）验证所述交易金额的明文 M 是否属于第一有效范围包括：所述验证方验证所述交易金额的明文 M 属于第一有效范围的零知识证明；其中，所述交易金额的明文 M 属于第一有效范围的零知识证明由所述发送方生成。

在一种可能的实现方式中，所述交易金额包括输出金额；所述方法还包括：所述验证

方验证输入金额与所述输出金额的差值的密文 C'是加密了明文为零的密文的加法同态零知识证明；其中，所述 C'为根据所述输出金额的密文与所述输入金额的密文计算得到的密文，所述输入金额的密文为所述发送方在上一次交易中接收的金额的密文，或者所述输入金额的密文为所述发送方采用所述加法同态加密算法对当前交易中生成的金额加密生成的密文；所述输入金额与所述输出金额的差值的密文 C'是加密了明文为零的密文的加法同态零知识证明由所述发送方生成。

在一种可能的实现方式中，所述系统还包括监管方，所述加法同态加密算法的公钥由所述监管方提供；所述方法还包括：所述验证方还用于验证所述监管方可解密所述交易金额的密文（C，B）的零知识证明；其中，所述监管方可解密所述交易金额的密文（C，B）的零知识证明由所述发送方生成。

第四方面，本申请实施例提供了一种区块链系统，所述系统包括发送方及验证方：所述发送方用于采用加法同态加密算法对交易金额的明文 M 加密，生成交易金额的密文（C，B），并将所述交易金额的密文（C，B）发送至所述验证方；所述验证方用于根据所述交易金额的密文（C，B）验证所述交易金额的明文 M 是否属于第一有效范围；所述第一有效范围为[0，2^U-1]，U 为所述交易金额的明文 M 的比特位长度。

在一种可能的实现方式中，所述 $C = g_3^M g_4^r$，$B = g_3^r$；其中，r 为随机生成的整数，g_3 为 G_1 的生成元，G_1 是阶为素数的乘法群，g_4 为所述加法同态加密算法的公钥，$g_4=g_3^{ask}$，ask 为所述加法同态加密算法的私钥。

在一种可能的实现方式中，所述系统还包括监管方；所述发送方用于将所述交易金额的明文 M 分割成 L 份交易金额的明文 M_k，分别采用加法同态加密算法对所述 L 份交易金额的明文 M_k 进行加密，生成 L 份交易金额的密文（C_k，B_k）；所述加法同态加密算法的公钥由所述监管方提供，k 为正整数，k=1，...，L；L 为大于或等于 2 的正整数；所述验证方用于根据所述交易金额的密文（C_k，B_k）验证所述交易金额的的明文 M_k 是否属于第二有效范围；所述第二有效范围为[0，2^u-1]，u 为所述交易金额的明文 M_k 的比特位长度；所述监管方用于采用与所述公钥对应的私钥解密所述 L 份交易金额的密文（C_k，B_k），获得所述 L 份交易金额的明文 M_k，并根据所述 L 份交易金额的明文 M_k 获得所述交易金额的明文 M。

在一种可能的实现方式中，所述发送方还用于生成所述交易金额的明文 M 属于第一有效范围的零知识证明；所述验证方用于根据所述交易金额的密文（C，B）验证所述交易金额的明文 M 属于第一有效范围的零知识证明。

在一种可能的实现方式中，所述交易金额包括输出金额；所述发送方还用于计算输入金额与输出金额的差值的密文 C'，并生成 C'是加密了明文为零的密文的加法同态零知识证明；其中，所述 C'为根据所述输出金额的密文与所述输入金额的密文计算得到的密文，所述输入金额的密文为所述发送方在上一次交易中接收的金额的密文，或者所述输入金额的密文为所述发送方采用所述加法同态加密算法对当前交易中生成的金额加密生成的密文；所述验证方还用于验证所述 C'是加密了明文为零的密文的加法同态零知识证明。

在一种可能的实现方式中，所述系统还包括监管方，所述加法同态加密算法的公钥由所述监管方提供；所述发送方还用于生成所述监管方可解密所述交易金额的密文（C，B）

的零知识证明；所述验证方还用于验证所述监管方可解密所述交易金额的密文（C，B）的零知识证明；所述监管方用于采用与所述公钥对应的私钥解密所述交易金额的密文（C，B）。

在一种可能的实现方式中，所述系统还包括第三方，用于提供随机秘密γ，所述随机秘密γ用于为所述第一有效范围内的每个整数生成一个数字签名；所述发送方用于根据所述第三方提供的随机秘密γ为所述有效范围内的每个整数生成的数字签名生成所述交易金额的明文属于第一有效范围的零知识证明。

在一种可能的实现方式中，所述发送方用于生成N个第一参数；所述验证方用于生成N个第二参数；其中，所述N个第一参数与所述N个第二参数一一对应；验证所述N个第二参数是否与对应的所述第一参数相等，若相等，则所述交易金额的明文M属于第一有效范围。

在一种可能的实现方式中，所述发送方还用于生成第一验证参数；所述第一验证参数由所述N个第一参数决定；所述验证方还用于生成第二验证参数；所述第二验证参数由所述N个第二参数决定；所述验证方还用于验证所述第一参数是否等于所述第二验证参数，若相等，则所述N个第二参数与相应的所述第一参数相等。

第五方面，本申请实施例提供了一种发送方，应用于区块链系统，所述系统包括发送方及验证方，所述发送方包括：加密单元，用于采用加法同态加密算法对交易金额的明文M加密，生成交易金额的密文（C，B）；其中，所述交易金额的明文M的比特位长度为U；发送单元，用于将所述交易金额的密文（C，B）发送至所述验证方，以使所述验证方根据所述交易金额的密文（C，B）验证所述交易金额的明文M是否属于第一有效范围；所述第一有效范围为[0，2^U-1]，U为所述交易金额的明文M的比特位长度。

在一种可能的实现方式中，所述$C = g_3^M g_4^r$，$B = g_3^r$；其中，r为随机生成的整数，g_3为G_1的生成元，G_1是阶为素数的乘法群，g_4为所述加法同态加密算法的公钥，$g_4=g_3^{ask}$，ask为所述加法同态加密算法的私钥。

在一种可能的实现方式中，所述系统还包括监管方；所述加密单元包括：分割子单元，用于将所述交易金额的明文M分割成L份交易金额的明文M_k；其中，k为正整数，k=1，...，L；L为大于或等于2的正整数；加密子单元，用于分别采用加法同态加密算法对所述L份交易金额的明文M_k加密，生成L份交易金额的密文（C_k，B_k），以使所述监管方采用与所述公钥对应的私钥解密所述L份交易金额的密文（C_k，B_k），获得所述L份交易金额的明文M_k，并根据所述L份交易金额的明文M_k获得所述交易金额的明文M；所述加法同态加密算法的公钥由所述监管方提供；所述发送单元，用于将所述L份交易金额的密文（C_k，B_k）发送至所述验证方，以使所述验证方根据所述交易金额的密文（C_k，B_k）验证所述交易金额的明文M_k是否属于第二有效范围；其中，所述第二有效范围为[0，2^u-1]，u为所述交易金额的明文M_k的比特位长度。

在一种可能的实现方式中，所述发送方还包括：第一生成单元，用于生成所述交易金额的明文M属于第一有效范围的零知识证明；所述发送单元用于将所述交易金额的密文（C，B）发送至所述验证方，以使所述验证方根据所述交易金额的密文（C，B）验证所述交易金额的明文M属于第一有效范围的零知识证明。

在一种可能的实现方式中，所述交易金额包括输出金额；所述发送方还包括：第二生

成单元，用于计算输入金额与输出金额的差值的密文C'，并生成C'是加密了明文为零的密文的加法同态零知识证明，以使所述验证方验证所述C'是加密了明文为零的密文的加法同态零知识证明；其中，所述C'为根据所述输出金额的密文与所述输入金额的密文计算得到的密文，所述输入金额的密文为所述发送方在上一次交易中接收的金额的密文，或者所述输入金额的密文为所述发送方采用所述加法同态加密算法对当前交易中生成的金额加密生成的密文。

在一种可能的实现方式中，所述系统还包括监管方，所述加法同态加密算法的公钥由所述监管方提供；所述发送方还包括：第三生成单元，用于生成所述监管方可解密所述交易金额的密文（C，B）的零知识证明，以使所述验证方验证所述监管方可解密所述交易金额的密文（C，B）的零知识证明。

在一种可能的实现方式中，所述系统还包括第三方，用于提供随机秘密γ，所述随机秘密γ用于为所述第一有效范围内的每个整数生成一个数字签名；所述第一生成单元用于根据所述第三方提供的随机秘密γ为所述第一有效范围内的每个整数生成的数字签名生成所述交易金额的密文C的明文M属于第一有效范围的零知识证明。

第六方面，本申请实施例提供了一种验证方，应用于区块链系统，所述系统包括发送方及验证方，所述验证方包括：接收单元，用于接收所述发送方发送的交易金额的密文（C，B）；其中，所述交易金额的密文（C，B）为所述发送方采用加法同态加密算法对交易金额的明文M加密生成的密文；所述交易金额的明文M的比特位长度为U；验证单元，用于根据所述交易金额的密文（C，B）验证所述交易金额的明文M是否属于第一有效范围；所述第一有效范围为[0，2^U-1]。

在一种可能的实现方式中，所述$C = g_3^M g_4^r$，$B = g_3^r$；其中，r为随机生成的整数，g_3为G_1的生成元，G_1是阶为素数的乘法群，g_4为所述加法同态加密算法的公钥，$g_4=g_3^{ask}$，ask为所述加法同态加密算法的私钥。

在一种可能的实现方式中，所述验证单元用于验证所述交易金额的明文M属于第一有效范围的零知识证明；其中，所述交易金额的明文M属于第一有效范围的零知识证明由所述发送方生成。

在一种可能的实现方式中，所述交易金额包括输出金额；所述验证单元还用于验证输入金额与所述输出金额的差值的密文C'是加密了明文为零的密文的加法同态零知识证明；其中，所述C'为根据所述输出金额的密文与所述输入金额的密文计算得到的密文，所述输入金额的密文为所述发送方在上一次交易中接收的金额的密文，或者所述输入金额的密文为所述发送方采用所述加法同态加密算法对当前交易中生成的金额进行加密生成的密文，所述输入金额与所述输出金额的差值的密文C'是加密了明文为零的密文的加法同态零知识证明由所述发送方生成。

在一种可能的实现方式中，所述系统还包括监管方，所述加法同态加密算法的公钥由所述监管方提供；所述验证单元还用于验证所述监管方可解密所述交易金额的密文（C，B）的零知识证明；其中，所述监管方可解密所述交易金额的密文（C，B）的零知识证明由所述发送方生成。

第七方面，本申请实施例提供了一种发送方，应用于区块链系统，所述系统包括发送

方及验证方，所述发送方包括：处理器、存储器和收发器，其中：所述处理器、所述存储器和所述收发器相互连接，所述存储器用于存储计算机程序，所述计算机程序包括程序指令，所述处理器被配置用于调用所述程序指令，执行本申请实施例第二方面或第二方面的任一种可能的实现方式提供的数据处理方法。

第八方面，本申请实施例提供了一种验证方，应用于区块链系统，所述系统包括发送方及验证方，所述验证方包括：处理器、存储器和收发器，其中：所述处理器、所述存储器和所述收发器相互连接，所述存储器用于存储计算机程序，所述计算机程序包括程序指令，所述处理器被配置用于调用所述程序指令，执行本申请实施例第三方面或第三方面的任一种可能的实现方式提供的数据处理方法。

第九方面，本申请实施例提供了一种计算机可读存储介质，所述计算机可读存储介质存储有计算机程序，所述计算机程序包括程序指令，所述程序指令当被处理器执行时，使所述处理器执行本申请实施例第二方面或第二方面的任一种可能的实现方式提供的数据处理方法。

第十方面，本申请实施例提供了一种计算机可读存储介质，所述计算机可读存储介质存储有计算机程序，所述计算机程序包括程序指令，所述程序指令当被处理器执行时，使所述处理器执行本申请实施例第三方面或第三方面的任一种可能的实现方式提供的数据处理方法。

实施本申请实施例可以在区块链系统中保护交易金额的隐私，在验证方无法获知交易金额的明文的情况下，验证交易金额是否在有效范围内，保证交易的合法性。同时，在交易金额明文的比特位长度较大时，可以将交易金额的明文分割成若干份小块的交易金额的明文，然后再分别对每个小块的交易金额的明文进行加密、以及其属于有效范围的证明等，保证监管方可以有效地解密每个小块交易金额的密文。

附图说明

为了更清楚地说明本申请实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍。

图 1 为本申请实施例提供的区块链系统架构示意图；

图 2 为输入金额及输出金额示意图；

图 3 为本申请实施例提供的一种数据处理方法流程示意图；

图 4 为本申请实施例提供的另一种数据处理方法流程示意图；

图 5 为本申请实施例中发送方处理交易金额明文 M 的过程示意图；

图 6 为本申请实施例提供的另一种数据处理方法流程示意图；

图 7 为本申请实施例提供的一种发送方的结构示意图；

图 8 为本申请实施例提供的一种验证方的结构示意图；

图 9 为本申请实施例提供的另一种发送方的结构示意图；

图 10 为本申请实施例提供的另一种验证方的结构示意图。

具体实施方式

下面将结合附图对本申请实施例中的技术方案进行清楚、详尽地描述。

首先结合图 1 介绍本申请实施例提供的区块链系统。如图 1 所示，区块链系统至少可以包括发送方及验证方。其中，发送方用于向接收方发起交易，将交易金额加密；验证方用于验证发送方向接收方发起的交易是否合法。该区块链系统还可以包括监管方，用于提供一对公私钥，将公钥提供给发送方使其对交易金额进行加密处理，监管方可采用其私钥对交易金额进行解密，以便监测区块链网络的交易行为，及时发现异常交易行为并作出相应处理。在具体地实现中，发送方可以是发款人的手机或电脑等终端，验证方可以是银行的服务器等，监管方可以是监管机构的电脑或服务器等。

该区块链系统可应用于联盟链场景中，即可应用于多个无法找到统一可信第三方的组织之间组成的联盟，例如在金融业务的联盟链中，发送方向接收方发起一个交易，发送方向接收方支付一定的交易金额，验证方可以验证该交易是否合法。交易是否合法主要体现在两个方面：第一，输出金额是否等于输入金额；第二，输出金额及输入金额是否属于有效范围。若输出金额等于输入金额，且输出金额及输入金额均属于有效范围，则说明该交易为合法的交易。对于输出金额及输入金额的解释，具体可参见图 2。假设发送方 A 打算支付的交易金额为 X，现在发送方 A 要将 X 分别支付给接收方 A_1 及接收方 A_2，接收方 A_1 接收到的交易金额为 Y，接收方 A_2 接收到的交易金额为 Z。那么，X 即为输入金额，Y 和 Z 即为输出金额。只有当 X=Y+Z，且 X，Y，Z 均大于或等于 0，且小于或等于最大值时，表明该交易合法。其中，上述最大值由交易金额的比特位长度决定，若该交易金额的比特位长度为 U，则最大值为 2^U-1。

接下来结合图 1 介绍的区块链系统，介绍本申请实施例提供的数据处理方法。如图 3 所示，数据处理方法至少可以包括以下几个步骤：

S301：发送方采用加法同态加密算法对交易金额的明文 M 加密，生成交易金额的密文（C，B）。

具体地，上述加法同态加密算法可以是 ElGamal 算法。交易金额的密文（C，B）中的 C 为交易金额明文 M 的密文主体，B 为交易金额明文 M 的辅助密文，用于在后续监管方解密过程中辅助解密密文主体 C。

具体地，$C = g_3^M g_4^r$，$B = g_3^r$；其中，r 为随机生成的整数，g_3 为 G_1 的生成元，G_1 是阶为素数的乘法群，g_4 为上述加法同态加密算法的公钥，$g_4=g_3^{ask}$，ask 为上述加法同态加密算法的私钥。

其中，交易金额的明文 M 的比特位长度为 U，U 为正整数。

在一种可能的实现方式中，上述交易金额包括输出金额。当交易金额只包括输出金额时，输入金额可以是发送方在上一次交易中接收的金额的密文，无需再进行加密以及后续对于交易金额属于有效范围的零知识证明的步骤。

在另外一种可能的实现方式中，交易金额除了包括输出金额外，还可以包括输入金额。即发送方需同时对输出金额及输入金额进行加密，以及后续对于交易金额属于有效范围的零知识证明等。

可以知道的是，发送方是否直接使用上一次交易中接收的金额的密文，或者发送方是否需要对输入金额进行加密以及后续对于交易金额属于有效范围的零知识证明等，取决于

该区块链系统的初始化设置，即该区块链系统中的交易模型是发送方直接向接收方转发其在上一次交易中接收的交易金额，还是该发送方在每一次交易中都会重新产生输入金额。

需要说明的是，输入金额的个数可以是至少一个，输出金额的个数也可以是至少一个。

在一种可能的实现方式中，监管方拥有一对非对称密码，包括公钥及私钥。发送方可采用监管方提供的公钥对交易金额的明文 M 加密，生成交易金额的密文，可以保证监管方能够采用与该公钥对应的私钥解密该交易金额的密文，以便监管方对交易进行监管。

S302：发送方将交易金额的密文（C，B）发送至验证方。

具体地，发送方采用上述加法同态加密算法对交易金额加密后，验证方无法获知该交易金额的明文 M，避免了该发送方被其他节点上的用户跟踪，从而导致信息泄露。因此，发送方在对交易金额的明文 M 加密后，生成交易金额的密文（C，B），并将该交易金额的密文（C，B）发送至验证方，以使验证方对交易金额的合法性进行验证。

S303：验证方根据交易金额的密文（C，B）验证交易金额的明文 M 是否属于第一有效范围。

具体地，若交易金额的明文 M 的比特位长度为 U，那么第一有效范围为[0，2^U-1]。

具体地，验证方可以验证交易金额的明文 M 属于第一有效范围的零知识证明。该交易金额的明文 M 属于第一有效范围的零知识证明由发送方生成。可以知道的是，本申请实施例可以采用加法同态的 ElGamal 加密算法，因为在该区块链系统中，加法同态的 ElGamal 加密算法可以与交易金额的明文 M 属于第一有效范围的零知识证明算法兼容。具体来说，加法同态的 ElGamal 加密算法得出的数据是二维的数据，且有效范围的零知识证明算法得出的数据也是二维的，上述两种算法属于同一组数学体系，因此这两种算法在该数学体系里可以兼容。可以知道的是，零知识证明指的是证明者能够在不向验证者提供任何有用信息的情况下，使验证者相信某个论断是正确的。对于交易金额的明文 M 属于第一有效范围的零知识证明，发送方不能向验证方提供该交易金额的明文 M，但是要使验证方相信交易金额的明文 M 属于第一有效范围。在本申请实施例中可以为第一有效范围内的所有整数生成一个数字签名，发送方只需证明该交易金额的明文对应的是该第一范围内所有整数的数字签名中的其中一个，即可证明该交易金额的明文 M 属于第一有效范围。加法同态加密是一种加密形式，它允许人们对密文进行特定的代数运算得到仍是加密的结果，将其解密所得到的结果与对明文进行同样的运算结果一样。换言之，加法同态加密可以使人们在加密的数据中进行操作得出正确的结果，而整个过程无需对数据进行解密。

此外，当发送方对交易金额的明文 M 使用加法同态的 ElGamal 加密算法的公钥由监管方提供时，发送方还可以生成监管方可解密交易金额的密文（C，B）的零知识证明。验证方还可以验证上述监管方可解密交易金额的密文（C，B）的零知识证明。

可以知道的是，发送方生成上述交易金额的明文 M 属于第一有效范围的零知识证明与生成上述监管方可解密交易金额的密文（C，B）的零知识证明的先后顺序不做限定。验证方验证上述交易金额的明文 M 属于第一有效范围的零知识证明与验证上述监管方可解密交易金额的密文（C，B）的零知识证明的先后顺序也不做限定。

此外，发送方还可以计算输入金额与输出金额的差值的密文 C'，并生成 C'是加密了明文为零的密文的加法同态零知识证明。验证方还可以验证上述 C'是加密了明文为零的密文

的加法同态零知识证明。

可以知道的是，当输出金额等于输入金额，且输出金额及输入金额均属于有效范围时，可证明该交易是合法的。

具体地，发送方在生成交易金额的明文 M 属于第一有效范围的零知识证明时，可生成至少一个第一参数。而验证方在验证交易金额的明文 M 属于第一有效范围的零知识证明时，也可生成至少一个第二参数。其中，上述第一参数与上述第二参数一一对应。当验证方生成的至少一个第二参数分别与发送方生成的至少一个第一参数相等时，即可验证交易金额的明文 M 属于第一有效范围。同样的计算方式适用于监管方可解密交易金额的密文（C，B）的零知识证明，也适用于 C'是加密了明文为零的密文的加法同态零知识证明，即验证了输入金额等于输出金额，在此不再赘述。

具体地，发送方在生成上述零知识证明时，还可生成一个第一验证参数，该第一验证参数由上述多个第一参数决定。而验证方在验证上述零知识证明时，也还可生成一个第二验证参数，该第二验证参数由上述多个第二参数决定。当验证方生成的第二验证参数等于上述发送方生成的第一验证参数时，意味着上述多个第一参数分别等于上述多个第二参数中与之对应的第二参数。从而验证了上述零知识证明。

实施本申请实施例可以在区块链系统中保护交易金额的隐私，在验证方无法获知交易金额的明文的情况下，验证交易金额是否在有效范围内，保证交易的合法性。且在有需要时能够配合监管方的监管。

在另一种可能的实施例中，本申请实施例提供了另外一种数据处理方法，当交易金额明文 M 的比特位长度较大时，监管方可能无法有效地解密比特位长度较大的交易金额明文的密文。因此，在本申请实施例中可以先将交易金额的明文 M 分割成若干份小块的交易金额的明文，然后再分别对每个小块的交易金额的明文进行加密、解密以及其属于有效范围的证明等，保证监管方可以有效地解密每个小块交易金额的密文。具体请参见图 4。如图 4 所示，数据处理方法至少可以包括以下几个步骤：

S401：发送方将交易金额的明文 M 分割为 L 份交易金额的明文 M_k。

可选地，若交易金额的明文 M 的比特位长度为 U，将其分割成 L 份比特位长度为 u 的交易金额的明文 M_k，其中，L*u=U，k 为正整数，k=1、…、L。

例如，当交易金额的明文 M 的比特位长度为 64 时，可以设置 L=4，u=16，即将该交易金额的明文 M 分割成 4 份比特位长度为 16 的交易金额的明文 M_k，其中，k=1、2、3、4。此时，每个交易金额的明文 M_k 的最大值即为 2^{16}-1。

又例如，当交易金额的明文 M 的比特位长度为 64 时，可以设置 L=8，u=8，即将该交易金额的明文 M 分割成 8 份比特位长度为 8 的交易金额的明文 M_k，其中，k=1、2、3……、8。此时，每个交易金额的明文 M_k 的最大值即为 2^8-1。

可以知道的是，上述 L 份交易金额的明文 M_k 的比特位长度也可以不相等。

具体地，交易金额可以是输出金额，或者交易金额可以是输出金额及输入金额，具体取决于该区块链系统的初始化设置。详细说明可参考 S301 中的描述，在此不再赘述。

可以知道的是，输出金额与输入金额的比特位长度不一定会相同，因此发送方在分别对输出金额及输入金额进行分割加密时，分割的份数可以不同，分割的交易金额的比特位

长度也可以不同。此外，输入金额的个数可以是至少一个，输出金额的个数也可以是至少一个，即在一次交易中，可以有多个输入金额，也可以有多个输出金额。

S402：发送方分别采用加法同态加密算法对 L 份交易金额的明文 M_k 加密，生成 L 份交易金额的密文（C_k，B_k）。

具体地，k=1、…、L。上述加法同态加密算法的公钥可以由监管方提供。采用监管方提供的公钥对交易金额进行加密，可以保证监管方能够采用与该公钥对应的私钥解密该交易金额的密文（C_k，B_k），以便监管方对交易进行监管。

具体地，上述加法同态加密算法可以是 ElGamal 算法。交易金额的密文（C_k，B_k）中的 C_k 为交易金额明文 M_k 的密文主体，B_k 为交易金额明文 M_k 的辅助密文，用于在后续监管方解密过程中辅助解密密文主体 C_k。

具体地，$C_k = g_3^{M_k} g_4^{r_k}$，$B_k = g_3^{r_k}$；其中，$r_k$ 为随机生成的整数，g_3 为 G_1 的生成元，G_1 是阶为素数的乘法群，g_4 为上述加法同态加密算法的公钥，$g_4=g_3^{ask}$，ask 为上述加法同态加密算法的私钥。

S403：发送方将 L 份交易金额的密文（C_k，B_k）发送至验证方。

具体地，发送方对交易金额进行加法同态的 ElGamal 加密后，验证方无法获知该交易金额的明文，避免了该发送方被其他节点上的用户跟踪，从而导致信息泄露。因此，发送方在对交易金额的明文进行加法同态的 ElGamal 加密后，直接将该交易金额的密文发送至验证方，以使验证方对交易金额的合法性进行验证。

S404：验证方根据交易金额的密文（C_k，B_k）验证交易金额的明文 M_k 是否属于第二有效范围。

具体地，验证方分别验证每一个交易金额的明文 M_k 是否属于第二有效范围，其中，交易金额的明文 M_k 的比特位长度为 u，上述第二有效范围为[0，2^u-1]。

具体地，验证方可以验证交易金额的明文 M_k 属于第二有效范围的零知识证明。该交易金额的明文 M_k 属于第二有效范围的零知识证明由发送方生成。在本申请实施例中，该区块链系统还可以包括可信第三方，可以由该可信第三方分别为第二有效范围内的每个整数生成一个数字签名，发送方只需证明该交易金额的密文（C_k，B_k）中的明文 M_k 对应的是该第二有效范围内所有整数的数字签名中的其中一个，即可证明该交易金额的明文 M_k 属于第二有效范围。

具体可见图 5，图 5 示出了发送方对交易金额明文 M 分割、加密及范围证明的过程。如图 5 所示，将交易金额的明文 M 分割成 8 份比特位长度为 u 的交易金额的明文 M_k，其中，k=1，2，…，8。首先是加密交易金额的明文 M_k 的过程，发送方分别采用加法同态的加密算法对交易金额的明文 M_k 加密后得到相应的交易金额的密文（C_k，B_k）。其次是证明交易金额的明文 M_k 属于第二有效范围的过程，发送方分别为交易金额的明文 M_k 生成其属于第二有效范围的零知识证明，交易金额的明文 M_k 属于第二有效范围的零知识证明由 π_k 表示。具体来说就是根据交易金额的密文（C_k，B_k）证明交易金额的明文 M_k 对应的是 0 到 2^u-1 中 2^u 个数字签名 σ_i 中的其中一个，从而证明交易金额的明文 M_k 是属于第二有效范围[0，2^u-1]以内的。其中，数字签名 σ_i 由该数据处理系统中的可信第三方生成，σ_i 表示数字 i 的签名，其中 i∈[0，2^u-1]，i 为整数。可以知道的是，在实际计算过程中，针对每一个

交易金额的明文 M_k，生成对应的 a_k 表征交易金额的明文 M_k 属于第二有效范围，发送方生成 a_k 后，由验证方验证 a_k 的正确性，若正确，则表示交易金额的明文 M_k 属于第二有效范围。a_k 具体的计算方式可参见下一实施例里的描述。

此外，发送方还可以生成监管方可解密交易金额的密文（C_k，B_k）的零知识证明。验证方还可以验证上述监管方可解密交易金额的密文（C_k，B_k）的零知识证明。

可以知道的是，发送方生成上述交易金额的明文 M_k 属于第二有效范围的零知识证明与生成上述监管方可解密交易金额的密文（C_k，B_k）的零知识证明的先后顺序不做限定。验证方验证上述交易金额的明文 M_k 属于第二有效范围的零知识证明与验证上述监管方可解密交易金额的密文（C_k，B_k）的零知识证明的先后顺序也不做限定。

此外，发送方还可以计算输入金额与输出金额的差值的密文 C'，并生成 C'是加密了明文为零的密文的加法同态零知识证明。验证方还可以验证上述 C'是加密了明文为零的密文的加法同态零知识证明。可以知道的是，当输出金额等于输入金额，且输出金额及输入金额均属于有效范围时，可证明该交易是合法的。

可以知道的是，上述交易金额的明文 M_k 属于第二有效范围的零知识证明、上述 C'是加密了明文为零的密文的加法同态零知识证明及上述监管方可解密交易金额的密文（C_k，B_k）的零知识证明均由发送方生成，由验证方验证。具体由发送方生成相应的参数，由验证方验证相应的参数的正确性。

具体地，发送方在为每个小块的明文 M_k 生成交易金额的明文 M_k 属于第二有效范围的零知识证明时，分别针对每个小块的明文 M_k 生成至少一个第一参数。而验证方在验证交易金额的明文 M_k 属于第二有效范围的零知识证明时，也可生成至少一个第二参数。其中，上述第一参数与上述第二参数一一对应。当验证方生成的至少一个第二参数分别与发送方生成的至少一个第一参数相等时，即可验证交易金额的明文 M_k 属于第二有效范围。同样地，上述方式也用于证明监管方可解密每个小块的交易金额的密文（C_k，B_k）。对于验证 C'是加密了明文为零的密文的加法同态零知识证明，发送方需根据所有的输入金额及所有的输出金额整体计算出一个第一参数，此处无需根据每个小块的交易金额来计算。验证方也可根据所有的输出金额及所有的输入金额整体计算出一个第二参数。当验证方生成的第二参数与发送方式生成的第一参数相等时，即可验证 C'是加密了明文为零的密文，即验证了输入金额等于输出金额。

具体地，发送方在生成上述零知识证明时，还可生成一个第一验证参数，该第一验证参数由上述多个第一参数决定。而验证方在验证上述零知识证明时，也还可生成一个第二验证参数，该第二验证参数由上述多个第二参数决定。当验证方生成的第二验证参数等于上述发送方生成的第一验证参数时，意味着上述多个第一参数分别等于上述多个第二参数中与之对应的第二参数。从而验证了上述零知识证明。

S405：监管方采用与公钥对应的私钥解密 L 份交易金额的密文（C_k，B_k），获得 L 份交易金额的明文 M_k。

具体地，监管方拥有一对非对称密码，包括公钥及私钥。公钥提供给发送方使其使用加法同态加密算法对交易金额的明文 M_k 加密，获得加密后的密文（C_k，B_k），保护交易隐私，防止信息泄露。私钥由监管方保存，用于解密发送方发送的交易金额的密文（C_k，B_k），

获得解密后的明文 M_k，以便监管方重组上述 L 个 M_k 获得最初的交易金额 M，从而对交易进行监管。

S406：监管方根据上述 L 份交易金额的明文 M_k 获得交易金额的明文 M。

具体地，若上述 L 份交易金额的明文 M_k 的比特位长度均为 u，监管方需将此 L 份比特位长度为 u 的交易金额的明文 M_k 重组得到原始的比特位长度为 U 的交易金额的明文 M，以便监管方对交易进行监管。

其中，$M=\sum_{k=1}^{L}M_k\left(2^u\right)^k$，k=1、…、L。

实施本申请实施例可以在交易金额的明文 M 的比特位长度较长时，将交易金额的明文 M 分割成若干份小块的明文，然后再分别对每个小块的明文进行加密、解密以及其属于有效范围的证明等，在保护交易隐私、配合监管的同时，保证监管方可有效地解密每个小块交易金额的密文。

接下来结合图 6 介绍本申请实施例提供的另一种数据处理方法。如图 6 所示，数据处理方法至少包括以下几个步骤：

S601：系统初始化。

具体地，系统初始化可以包括以下几个方面：

1）设置将交易金额的明文 M 分割成 L 份，每份的比特位长度为 u。例如，在交易金额的明文的比特位长度为 64 的场景下，可以设置 L=4，u=16。 g_3、g_5 分别为 G_1、G_2 的生成元，G_1、G_2 均是阶为素数的乘法群。H 为一个安全的哈希函数。

2）设置监管方的私钥为 ask，公钥为 $g_4=g_3^{ask}$。

3）可信第三方生成随机秘密 γ，生成 $\hat{Y}=g_5^{\gamma}$，为[0, 2^u-1]中的整数生成 2^u 个数字签名：

$\sigma_i=g_3^{\frac{1}{\gamma+i}}$，其中，$i$ 为整数，$i\in\left[0,2^u-1\right]$，即 σ_i 为数字 i 的签名。

可以知道的是，上述 L、u、H、g_3、g_5、g_4、σ_i 在该区块链系统中均为公开的参数。

S602：发送方加密每个输出金额。

具体地，以下介绍发送方对单个输出金额进行加密的过程，若存在多个输出金额，重复以下对单个输出金额加密的过程即可。

在本实施例以对输出金额的明文 M 进行分割为例进行说明。发送方采用加法同态加密算法对输出金额的明文 M 加密具体包括以下几个步骤：

1）发送方将输出金额的明文 M 分割为 L 份比特位长度为 u 的输出金额的明文 M_k，$M_k\in[0,2^u-1]$，其中，k=1，2，…，L，$M=\sum_{k=1}^{L}M_k\left(2^u\right)^k$。

假设，输出金额的明文 M 的比特位长度为 64，设置 L=4，u=16，将该输出金额的明文 M 分割成 4 份比特位长度为 16 的输出金额的明文 M_k，其中，k=1、2、3、4。则：

$$M=\sum_{k=1}^{4}M_k\left(2^{16}\right)^k=M_1*2^{16}+M_2*2^{16*2}+M_3*2^{16*3}+M_4*2^{16*4}。$$

2）分别采用加法同态的加密算法对每个输出金额的明文 M_k 加密，生成输出金额的密

文（C_k，B_k）。

具体地，上述加法同态的加密算法可以是 ElGamal 算法。输出金额的密文（C_k，B_k）中的C_k为输出金额明文M_k的密文主体，B_k为输出金额明文M_k的辅助密文，用于在后续监管方解密过程中辅助解密密文主体C_k。

具体地，计算$B_k = g_3^{r_k}$，$C_k = g_3^{M_k} g_4^{r_k}$，其中，$r_k$为随机生成的整数。

S603：发送方生成零知识证明。

具体地，此处依然是对于单个输出金额生成零知识证明的过程，若存在多个输出金额，重复以下对单个输出金额生成零知识证明的过程即可。

具体地，发送方生成的零知识证明包括以下几个方面：

1）发送方生成监管方可解密每个输出金额的密文（C_k，B_k）的零知识证明。

具体地，生成随机数ω_k，计算第一参数$E_k = g_3^{\omega_k}$，$D_k = g_3^{s_k} g_4^{\omega_k}$。

2）发送方生成输出金额的明文M_k属于第二有效范围的零知识证明。

具体地，证明输出金额的明文M_k对应的是第二有效范围[0，2^u-1]中2^u个数字签名中的其中一个，从而证明输出金额的明文M_k属于第二有效范围[0，2^u-1]。

具体地，生成随机数v_k，s_k，t_k计算$V_k = \sigma_{M_k}^{v_k}$，并计算第一参数$a_k = e(V_k, g_5)^{-s_k} e(g_3, g_5)^{t_k}$。

可以知道的是，一个输出金额的密文主体 C 可以根据分割后得到的 L 份输出金额的密文主体C_k计算：$C = \prod_{k=1}^{L} C_k^{2^{u^k}}$。

可以知道的是，上述是对于输出金额的加密及证明（证明监管方可解密每个小块的 ElGamal 密文及证明密文中的明文属于第二有效范围）。对于输入金额，可以是重复上述过程进行加密及证明；或者直接源用上次交易中该发送方接收的交易金额的密文，作为本次交易的输入金额，无需重复上述过程。发送方是否直接源用上次交易中接收的交易金额的密文取决于该区块链系统对于交易模型的初始化设置，即该区块链系统中的交易模型是发送方直接向接收方转发其在上一次交易中接收的交易金额，还是该发送方在每一次交易中都会重新产生输入金额。

3）发送方计算 C'=（总输入金额-总输出金额）的密文，并生成 C'是加密了明文为零的密文的加法同态零知识证明。

具体地，假设有 Y 个输出金额$M^{(out,y)}$及其密文主体$C^{(out,y)}$，X 个输入金额$M^{(in,x)}$及其密文主体$C^{(in,x)}$，其中，x=1，2，...，X，y=1，2，...，Y。发送方可利用各密文主体的随机数计算 δ，使得$C' = \frac{\prod_{x=1}^{X} C^{(in,x)}}{\prod_{y=1}^{Y} C^{(out,y)}} = g_4^{\delta}$。具体来说，$\delta = \sum_{x=1}^{X}\sum_{k=1}^{L} r_k^{(in,x)} - \sum_{y=1}^{Y}\sum_{k=1}^{L} r_k^{(out,y)}$，其中$r_k^{(in,x)}$为密文主体$C^{(in,x)}$的随机数，$r_k^{(out,y)}$为密文主体$C^{(out,y)}$的随机数。生成随机数$r_\delta$，计算第一参数$R_\delta = g_4^{r_\delta}$。

需要说明的是，在证明总输入金额与总输出金额相等时，计算的是总输入金额的明文

与总输出金额的明文的差值，在加密后的数据中采用的计算方式是总输入金额的密文与总输出金额的密文的比值。而总输出金额的密文等于多个输出金额密文的累乘，总输入金额的密文等于多个输入金额密文的累乘。

4）发送方计算第一验证参数d，该第一验证参数d是利用哈希函数H计算的结果，其中H的输入包括上述B_k，C_k，D_k，E_k，V_k，a_k及R_δ。发送方根据验上述第一验证参数d计算：$Z_{M_k}=s_k+dM_k$，$Z_{r_k}=\omega_k+dr_k$，$Z_{v_k}=t_k+dv_k$及$Z_\delta=r_\delta+d\delta$。

发送方最终分别针对每个输出金额输出一个B_k，C_k，V_k，Z_{M_k}，Z_{r_k}，Z_{v_k}，其中k=1，2，...，L，发送方还针对所有的输出金额及所有的输入金额输出一个Z_δ及d。可以知道的是，若在该区块链系统中，发送方在每一次交易中都会重新产生输入金额，那么发送方最终还需针对每个输入金额输出一个B_k，C_k，V_k，Z_{M_k}，Z_{r_k}，Z_{v_k}，发送方将输出的上述参数发送至验证方。

S604：验证方验证零知识证明。

具体地，验证方验证零知识证明包括以下几个方面：

1）验证方验证每个输出金额的明文M_k属于第二有效范围的零知识证明与监管方可解密的零知识证明。

可以知道的是，发送方生成的第一参数V_k，a_k用于证明输出金额的明文M_k存在对应的可信第三方生成的数字签名，即$0\le M_k\le 2^u-1$，即证明输出金额的明文M_k属于第二有效范围；发送方生成的第一参数D_k，E_k用于证明B_k，C_k为合法的密文，即证明监管方可解密该密文。

具体地，验证方可对于每个小块计算第二参数$a_k'=e\left(V_k,\hat{Y}^d g_5^{Z_{M_k}}\right)e\left(g_3,g_5\right)^{-Z_{v_k}}$，$D_k'=g_3^{Z_{M_k}}g_4^{Z_{r_k}}C_k^{-d}$，$E_k'=g_3^{Z_{r_k}}B_k^{-d}$，其中k=1，2，...，L。

对于输入金额，若发送方源用上次交易接收的金额密文，则无需再验证输入金额；否则验证方需重复上述运算验证输入金额属于第二有效范围的零知识证明与监管方可解密的零知识证明。

2）验证方验证C'是加密了明文为零的密文的加法同态零知识证明。

具体地，计算$C'=\dfrac{\prod_{x=1}^{X}C^{(in,x)}}{\prod_{y=1}^{Y}C^{(out,y)}}$，并计算第二参数$R_\delta'=g_4^{Z_\delta}C'^{-d}$。

验证方利用哈希函数计算第二验证参数d'，其中H的输入包括B_k，C_k，D_k'，E_k'，V_k，a_k'及R_δ'。若第二验证参数等于第一验证参数，即$d'=d$，则表明验证方验证通过。此处“验

证方验证通过”指的是以下三个方面：

1、验证方验证了每个输出金额的明文 M_k 属于第二有效范围；

2、验证方验证了以及 C'是加密了明文为零的密文，即输出金额等于输入金额；

3、验证方验证了监管方可解密每个输出金额的密文（C_k，B_k）。

以上验证的第 1 和第 2 两个方面，验证了交易的合法性；以上验证的第 3 方面，验证了密文的合法性。

可以知道的是，发送方计算第一验证参数 d 时，哈希函数 H 的输入包括 B_k，C_k，D_k，E_k，V_k，a_k 及 R_δ。验证方计算第二验证参数 d' 时，哈希函数 H 的输入包括 B_k，C_k，D_k'，E_k'，V_k，a_k' 及 R_δ'。当计算出 $d'=d$ 时，意味着该哈希函数 H 的各个输入参数也各自相等。即 $D_k'=D_k$，$E_k'=E_k$，$a_k'=a_k$，$R_\delta'=R_\delta$。由于第一参数 D_k，E_k 用于证明（C_k，B_k）为合法的密文，那么 $D_k'=D_k$，$E_k'=E_k$ 意味着（C_k，B_k）为合法的密文，即验证了监管方可解密每个小块的输出金额。由于第一参数 a_k 用于证明输出金额的明文 M_k 存在对应的可信第三方生成的数字签名，那么 $a_k'=a_k$ 意味着输出金额的明文 M_k 属于第二有效范围。由于第一参数 R_δ 用于证明 C'是加密了明文为零的密文，那么 $R_\delta'=R_\delta$ 验证了 C'是加密了明文为零的密文，即验证了总的输入金额等于总的输出金额。再结合前述验证的每个输出金额的密文属于其有效范围的结果，验证方验证了该交易的合法性。

S605：监管方解密。

具体地，监管方解密可以包括以下几个方面：

1）监管方采用其私钥 ask 解密每个输出金额的密文（C_k，B_k），得到 $g_3^{M_k}=\frac{C_k}{B_k^{ask}}$。

2）监管方计算 g_3^0、g_3^1、…、$g_3^{2^u-1}$，并分别与 $g_3^{M_k}$ 比较，找出输出金额的明文 M_k。

具体地，监管方可预先计算 g_3^i，其中，i 为整数，$i\in\left[0,2^u-1\right]$，生成预计算表（g_3^0、g_3^1、…、$g_3^{2^u-1}$），监管方可在多次解密过程中重复使用该预计算表，将每次解密得到的 $g_3^{M_k}$ 与该预计算表进行比较，找出输出金额的明文 M_k 的值。

3）根据解密得出的多个输出金额的明文 M_k 的值还原输出金额的明文 M。其中，$M=\sum_{k=1}^{L}M_k\left(2^u\right)^k$。

可以知道的是，上述监管方解密的过程同样适用于输入金额的解密，在此不再赘述。

可以知道的是，上述计算过程同样适用于无需分割交易金额明文的场景，在此不再赘述。

本申请实施例提供了该数据处理方法具体的计算方法，根据该计算方法可以对交易金额的明文进行分割。然后再分别对每个小块的明文进行加密、解密以及其属于有效范围的证明等，在保护交易隐私、配合监管的同时，保证监管方有效地解密每个小块交易金额的密文，顺利地还原交易金额的明文 M，对交易进行有效的监管。

本申请实施例还提供了一种发送方，应用于图 1 所示的区块链系统，该系统至少可以包括发送方及验证方，如图 7 所示，发送方 70 至少可以包括：加密单元 710、发送单元 720，其中：

加密单元 710，采用加法同态加密算法对交易金额的明文 M 加密，生成交易金额的密文（C，B）；其中，上述交易金额的明文 M 的比特位长度为 U，详细说明请参照 S301 的描述。

发送单元 720，用于将上述交易金额的密文（C，B）发送至上述验证方，以使上述验证方验证上述交易金额的明文 M 是否属于第一有效范围；上述第一有效范围为[0，2^U-1]，详细说明请参照 S302 的描述。

在一种可能的实现方式中，上述加法同态加密算法可以是 ElGamal 算法，上述 $C = g_3^M g_4^r$，$B = g_3^r$；其中，r 为随机生成的整数，g_3 为 G_1 的生成元，G_1 是阶为素数的乘法群，g_4 为上述加法同态加密算法的公钥，$g_4=g_3^{ask}$，ask 为上述加法同态加密算法的私钥。

在一种可能的实现方式中，上述区块链系统还包括监管方。上述加密单元 710 包括：分割子单元 7110 及加密子单元 7120。其中：

分割子单元 7110，用于将上述交易金额的明文 M 分割成 L 份交易金额的明文 M_k；其中，k 为正整数，k=1，...，L；L 为大于或等于 2 的正整数，详细说明请参照 S401 的描述，或者参照 S602 中 1）的描述。

加密子单元 7120，用于分别采用加法同态加密算法对上述 L 份交易金额的明文 M_k 加密，生成 L 份交易金额的密文（C_k，B_k），以使上述监管方采用与上述公钥对应的私钥解密上述 L 份交易金额的密文（C_k，B_k），获得上述 L 份交易金额的明文 M_k，并根据上述 L 份交易金额的明文 M_k 获得交易金额的明文 M，上述加法同态加密算法的公钥由所述监管方提供；详细说明请参照 S402、S405 及 S406 的描述，或者参照 S602 中 2）的描述。

发送单元 720，用于将上述 L 份交易金额的密文（C_k，B_k）发送至上述验证方，以使上述验证方验证上述 L 份交易金额的密文（C_k，B_k）的明文 M_k 是否属于第二有效范围；其中，第二有效范围为[0，2^u-1]，u 为交易金额的明文 M_k 的比特位长度，详细说明请参照 S403 及 S404 的描述。

在一种可能的实现方式中，发送方 70 还包括：第一生成单元 730，用于生成上述交易金额的明文 M 属于第一有效范围的零知识证明，详细说明请参照 S603 中 2）的描述。

发送单元 720 用于将上述交易金额的密文（C，B）发送至上述验证方，以使上述验证方根据所述交易金额的密文（C，B）验证上述交易金额的明文 M 属于第一有效范围的零知识证明。

在一种可能的实现方式中，所述交易金额包括输出金额。发送方 70 还包括：第二生成单元 740，用于计算输入金额与输出金额的差值的密文 C'，并生成 C'是加密了明文为零的密文的加法同态零知识证明，以使上述验证方验证上述 C'是加密了明文为零的密文的加法同态零知识证明；其中，上述 C'为根据上述输出金额的密文与上述输入金额的密文计算得到的密文，上述输入金额的密文为发送方 70 在上一次交易中接收的金额的密文，或者上述输入金额的密文为发送方 70 采用所述加法同态加密算法对当前交易中生成的金额加密生成的密文，详细说明请参照 S603 中 3）的描述。

在一种可能的实现方式中，上述系统还包括监管方，所述加法同态加密算法的公钥由所述监管方提供；详细说明请参照 S301 的描述。

发送方 70 还包括：第三生成单元 750，用于生成上述监管方可解密上述交易金额的密文（C，B）的零知识证明，以使上述验证方验证上述监管方可解密上述交易金额的密文（C，B）的零知识证明，详细说明请参照 S603 中 1）的描述。

在一种可能的实现方式中，上述系统还包括第三方，用于提供随机秘密 γ，上述随机秘密 γ 用于为上述第一有效范围内的每个整数生成一个数字签名，详细说明请参照 S601 中 3）的描述。

第一生成单元 730 用于根据上述第三方提供的随机秘密 γ 为第一有效范围内的每个整数生成的数字签名生成所述交易金额的密文 C 的明文 M 属于第一有效范围的零知识证明，详细说明请参照 S603 中 2）的描述。

本申请实施例还提供了一种验证方，应用于图 1 所示的区块链系统，该系统至少可以包括发送方及验证方，如图 7 所示，验证方 80 至少可以包括：接收单元 810、验证单元 820，其中：

接收单元 810，用于接收发送方 70 发送的交易金额的密文（C，B）；其中，交易金额的密文（C，B）为发送方 70 采用加法同态加密算法对交易金额的明文 M 加密生成的密文；交易金额的明文 M 的比特位长度为 U，详细说明请参照 S302 或 S403 的描述。

验证单元 820，用于根据上述交易金额的密文（C，B）验证交易金额的明文 M 是否属于第一有效范围；第一有效范围为[0，2^U-1]，详细说明请参照 S303 或 S404 的描述。

在一种可能的实现方式中，上述加法同态加密算法可以是 ElGamal 算法，上述 $C = g_3^M g_4^r$，$B = g_3^r$；其中，r 为随机生成的整数，g_3 为 G_1 的生成元，G_1 是阶为素数的乘法群，g_4 为所述加法同态加密算法的公钥，$g_4=g_3^{ask}$，ask 为所述加法同态加密算法的私钥。

在一种可能的实现方式中，验证单元 820 用于验证交易金额的明文 M 属于第一有效范围的零知识证明；其中，交易金额的明文 M 属于第一有效范围的零知识证明由发送方 70 生成，详细说明请参照 S604 中 1）的描述。

在一种可能的实现方式中，交易金额包括输出金额；验证单元 820 还用于验证输入金额与输出金额的差值的密文 C'是加密了明文为零的密文的加法同态零知识证明；其中，C'为根据输出金额的密文与输入金额的密文计算得到的密文，输入金额的密文为发送方 70 在上一次交易中接收的金额的密文，或者输入金额的密文为发送方 70 采用所述加法同态加密算法对当前交易中生成的金额加密生成的密文，输入金额与输出金额的差值的密文 C'是加密了明文为零的密文的加法同态零知识证明由发送方 70 生成，详细说明请参照 S604 中 2）

的描述。

在一种可能的实现方式中，上述区块链系统还包括监管方，上述加法同态加密算法的公钥由监管方提供。

验证单元820还用于验证监管方可解密交易金额的密文（C，B）的零知识证明；其中，监管方可解密上述交易金额的密文（C，B）的零知识证明由发送方 70 生成，详细说明请参照 S604 中 1）的描述。

本申请实施例还提供了另外一种发送方，如图 9 所示，发送方 90 至少可以包括：至少一个处理器 901，至少一个网络接口 904，用户接口 903，存储器 905，至少一个通信总线 902，显示屏 906。其中，通信总线 902 用于实现这些组件之间的连接通信，应当理解，发送方 90 中的各个组件还可以通过其他连接器相耦合，所述其他连接器可包括各类接口、传输线或总线等，在本申请的各个实施例中，耦合是指通过特定方式的相互联系，包括直接相连或通过其他设备间接相连。

其中，处理器 901 可以包括如下至少一种类型：通用中央处理器（Central Processing Unit，CPU）、数字信号处理器（Digital Signal Processor，DSP）、微处理器、专用集成电路（Application Specific Integrated Circuit，ASIC）、微控制器（Microcontroller Unit，MCU）、现场可编程门阵列（Field Programmable Gate Array，FPGA）、或者用于实现逻辑运算的集成电路。例如，处理器 901 可以是一个单核（single-CPU）处理器或多核（multi-CPU）处理器。处理器 901 内包括的多个处理器或单元可以是集成在一个芯片中或位于多个不同的芯片上。

用户接口 903 可以包括键盘、物理按钮（按压按钮、摇臂按钮等）、拨号盘、滑动开关、操纵杆、点击滚轮、光鼠（光鼠是不显示可视输出的触摸敏感表面，或者是由触摸屏形成的触摸敏感表面的延伸）等等。网络接口 904 可选的可以包括标准的有线接口、无线接口（如 WI-FI 接口）。

存储器 905 可以是非掉电易失性存储器，例如是 EMMC（Embedded Multi Media Card，嵌入式多媒体卡）、UFS（Universal Flash Storage，通用闪存存储）或只读存储器（Read-Only Memory，ROM），可选的，存储器 905 包括本申请实施例中的 flash，或者是可存储静态信息和指令的其他类型的静态存储设备，还可以是掉电易失性存储器（volatile memory），例如随机存取存储器（Random Access Memory，RAM）或者可存储信息和指令的其他类型的动态存储设备，也可以是电可擦可编程只读存储器（Electrically Erasable Programmable Read-Only Memory，EEPROM）、只读光盘（Compact Disc Read-Only Memory，CD-ROM）或其他光盘存储、光碟存储（包括压缩光碟、激光碟、光碟、数字通用光碟、蓝光光碟等）、磁盘存储介质或者其他磁存储设备、或者能够用于携带或存储具有指令或数据结构形式的程序代码并能够由计算机存取的任何其他计算机可读存储介质，但不限于此。可选的，存储器 905 可选的还可以是至少一个位于远离前述处理器 901 的存储系统。如图 9 所示，作为一种计算机存储介质的存储器 905 中可以包括操作系统、网络通信模块、用户接口模块以及程序指令。

存储器 905 可以是独立存在，通过连接器与处理器 901 相耦合。存储器 905 也可以和处理器 901 集成在一起。其中，存储器 905 能够存储执行本申请方案的程序指令在内的各

类计算机程序指令，并由处理器 901 来控制执行，被执行的各类计算机程序指令也可被视为是处理器 901 的驱动程序。例如，处理器 901 用于执行存储器 905 中存储的计算机程序指令，从而实现本申请中图 3-图 6 方法实施例中的方法。所述计算机程序指令数量很大，可形成能够被处理器 901 中的至少一个处理器执行的计算机可执行指令，以驱动相关处理器执行各类处理，如支持上述各类无线通信协议的通信信号处理算法、操作系统运行或应用程序运行。

显示屏 906，用于显示由用户输入的信息。示例性的，显示屏 906 可以包括显示面板和触控面板。其中，显示面板可以采用液晶显示器（Liquid Crystal Display，LCD）、有机发光二极管（Organic Light-Emitting Diode，OLED）、发光二级管（Light Emitting Diode，LED）显示设备或阴极射线管（Cathode Ray Tube，CRT）等来配置显示面板。触控面板，也称为触摸屏、触敏屏等，可收集用户在其上或附近的接触或者非接触操作（比如用户使用手指、触笔等任何适合的物体或附件在触控面板上或在触控面板附近的操作，也可以包括体感操作；该操作包括单点控制操作、多点控制操作等操作类型），并根据预先设定的程式驱动相应的连接装置。

本申请实施例提供了另外一种验证方，如图 10 所示，验证方 100 至少可以包括：至少可以包括：至少一个处理器 1001，至少一个网络接口 1004，用户接口 1003，存储器 1005，至少一个通信总线 1002，显示屏 1006。其中，通信总线 1002 用于实现这些组件之间的连接通信，应当理解，验证方 100 中的各个组件还可以通过其他连接器相耦合，所述其他连接器可包括各类接口、传输线或总线等，在本申请的各个实施例中，耦合是指通过特定方式的相互联系，包括直接相连或通过其他设备间接相连。

其中，处理器 1001 与处理器 901 类似，在此不再赘述。

用户接口 1003 与用户接口 903 类似，在此不再赘述。

存储器 1005 与存储器 905 类似，处理器 1001 用于执行存储器 905 中存储的计算机程序指令，从而实现本申请中图 3-图 6 方法实施例中的方法，在此不再赘述。

显示屏 1006 与显示屏 906 类似，在此不再赘述。

本申请实施例还提供了一种计算机可读存储介质，该计算机可读存储介质中存储有指令，当其在计算机或处理器上运行时，使得计算机或处理器执行上述任一个数据处理方法中的一个或多个步骤。上述装置的各组成模块如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在所述计算机可读取存储介质中。

基于这样的理解，本申请实施例还提供一种包含指令的计算机程序产品，本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或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中，包括若干指令用以使得一台计算机设备、移动终端或其中的处理器执行本申请各个实施例所述方法的全部或部分步骤。该存储介质的种类请参考存储器 905 或 1005 的相关描述。

本申请实施例方法中的步骤可以根据实际需要进行顺序调整、合并和删减。

本申请实施例装置中的模块可以根据实际需要进行合并、划分和删减。

以上所述，以上实施例仅用以说明本申请的技术方案，而非对其限制；尽管参照前述实施例对本申请进行了详细的说明，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申请各实施例技术方案的范围。

权 利 要 求

1、一种数据处理方法，应用于区块链系统，所述系统包括发送方及验证方，其特征在于，所述方法包括:

所述发送方采用加法同态加密算法对交易金额的明文 M 加密，生成交易金额的密文（C，B）；

所述发送方将所述交易金额的密文（C，B）发送至所述验证方;

所述验证方根据所述交易金额的密文（C，B）验证所述交易金额的明文 M 是否属于第一有效范围，所述第一有效范围为[0，2^U-1]，U 为所述交易金额的明文 M 的比特位长度。

2、如权利要求 1 所述的方法，其特征在于，所述 $C = g_3^M g_4^r$，$B = g_3^r$；其中，r 为随机生成的整数，g_3 为 G_1 的生成元，G_1 是阶为素数的乘法群，g_4 为所述加法同态加密算法的公钥，$g_4=g_3^{ask}$，ask 为所述加法同态加密算法的私钥。

3、如权利要求 1 或 2 所述的方法，其特征在于，所述系统还包括监管方;

所述发送方采用加法同态加密算法对交易金额的明文 M 加密，生成交易金额的密文（C，B）包括: 所述发送方将所述交易金额的明文 M 分割成 L 份交易金额的明文 M_k，分别采用加法同态加密算法对所述 L 份交易金额的明文 M_k 进行加密，生成 L 份交易金额的密文（C_k，B_k）；所述加法同态加密算法的公钥由所述监管方提供，k 为正整数，k=1，...，L，L 为大于或等于 2 的正整数;

所述验证方根据所述交易金额的密文（C，B）验证所述交易金额的明文 M 是否属于第一有效范围包括: 所述验证方验证根据所述交易金额的密文（C_k，B_k）验证所述交易金额的明文 M_k 是否属于第二有效范围；其中，所述第二有效范围为[0，2^u-1]，u 为所述交易金额的明文 M_k 的比特位长度;

所述方法还包括: 所述监管方采用与所述公钥对应的私钥解密所述 L 份交易金额的密文（C_k，B_k），获得所述 L 份交易金额的明文 M_k，并根据所述 L 份交易金额的明文 M_k 获得所述交易金额的明文 M。

4、如权利要求 1-3 任一项所述的方法，其特征在于，所述方法还包括: 所述发送方生成所述交易金额的明文 M 属于第一有效范围的零知识证明;

所述验证方根据所述交易金额的密文（C，B）验证所述交易金额的明文 M 是否属于第一有效范围包括: 所述验证方验证所述交易金额的明文 M 属于第一有效范围的零知识证明。

5、如权利要求 1-4 任一项所述的方法，其特征在于，所述交易金额包括输出金额;

所述方法还包括: 所述发送方计算输入金额与输出金额的差值的密文 C'，并生成 C'是加密了明文为零的密文的加法同态零知识证明；其中，所述 C'为根据所述输出金额的密文与所述输入金额的密文计算得到的密文，所述输入金额的密文为所述发送方在上一次交易

中接收的金额的密文，或者所述输入金额的密文为所述发送方采用所述加法同态加密算法对当前交易中生成的金额进行加密生成的密文；

所述验证方验证所述 C'是加密了明文为零的密文的加法同态零知识证明。

6、如权利要求 1 或 2 所述的方法，其特征在于，所述系统还包括监管方，所述加法同态加密算法的公钥由所述监管方提供；

所述方法还包括：所述发送方生成所述监管方可解密所述交易金额的密文（C，B）的零知识证明；

所述验证方验证所述监管方可解密所述交易金额的密文（C，B）的零知识证明；

所述监管方采用与所述公钥对应的私钥解密所述交易金额的密文（C，B）。

7、如权利要求 4 所述的方法，其特征在于，所述发送方生成所述交易金额的明文 M 属于第一有效范围的零知识证明包括：所述发送方生成 N 个第一参数；N 为正整数；

所述验证方验证所述交易金额的明文 M 属于第一有效范围的零知识证明包括：

所述验证方生成 N 个第二参数；其中，所述 N 个第一参数与所述 N 个第二参数一一对应；

所述验证方验证所述 N 个第二参数是否与对应的所述第一参数相等，若相等，则所述交易金额的明文 M 属于第一有效范围。

8、如权利要求 7 所述的方法，其特征在于，所述发送方生成所述交易金额的明文 M 属于第一有效范围的零知识证明还包括：所述发送方生成第一验证参数；所述第一验证参数由所述 N 个第一参数决定；

所述验证方验证所述交易金额的明文 M 属于第一有效范围的零知识证明还包括：

所述验证方生成第二验证参数；所述第二验证参数由所述 N 个第二参数决定；

所述验证方验证所述 N 个第二参数是否与对应的所述第一参数相等包括：

所述验证方验证所述第一参数是否等于所述第二验证参数，若相等，则所述 N 个第二参数与相应的所述第一参数相等。

9、一种数据处理方法，应用于区块链系统，所述系统包括发送方及验证方，其特征在于，所述方法包括：

所述发送方采用加法同态加密算法对交易金额的明文 M 加密，生成交易金额的密文（C，B）；

所述发送方将所述交易金额的密文（C，B）发送至所述验证方，以使所述验证方根据所述交易金额的密文（C，B）验证所述交易金额的明文 M 是否属于第一有效范围；所述第一有效范围为[0，2^U-1]，U 为所述交易金额的明文 M 的比特位长度。

10、如权利要求 9 所述的方法，其特征在于，所述 $C = g_3^M g_4^r$，$B = g_3^r$；其中，r 为随机生成的整数，g_3 为 G_1 的生成元，G_1 是阶为素数的乘法群，g_4 为所述加法同态加密算法的

公钥，$g_4=g_3^{ask}$，ask 为所述加法同态加密算法的私钥。

11、如权利要求 9 或 10 所述的方法，其特征在于，所述系统还包括监管方；

所述发送方采用加法同态加密算法对交易金额的明文 M 加密，生成交易金额的密文（C，B）包括：所述发送方将所述交易金额的明文 M 分割成 L 份交易金额的明文 M_k，分别采用加法同态加密算法对所述 L 份交易金额的明文 M_k 进行加密，生成 L 份交易金额的密文（C_k，B_k），以使所述监管方采用与所述公钥对应的私钥解密所述 L 份交易金额的密文（C_k，B_k），获得所述 L 份交易金额的明文 M_k，并根据所述 L 份交易金额的明文 M_k 获得所述交易金额的明文 M；所述加法同态加密算法的公钥由所述监管方提供，k 为正整数，k=1，...，L；L 为大于或等于 2 的正整数；

所述发送方将所述交易金额的密文（C，B）发送至所述验证方，以使所述验证方根据所述交易金额的密文（C，B）验证所述交易金额的明文 M 是否属于第一有效范围包括：所述发送方将所述 L 份交易金额的密文（C_k，B_k）发送至所述验证方，以使所述验证方根据所述交易金额的密文（C_k，B_k）验证所述交易金额的明文 M_k 是否属于第二有效范围；其中，所述第二有效范围为[0，2^u-1]，u 为所述交易金额的明文 M_k 的比特位长度。

12、一种数据处理方法，应用于区块链系统，所述系统包括发送方及验证方，其特征在于，所述方法包括：

所述验证方接收所述发送方发送的交易金额的密文（C，B）；其中，所述交易金额的密文（C，B）为所述发送方采用加法同态加密算法对交易金额的明文 M 加密生成的密文；所述交易金额的明文 M 的比特位长度为 U；

所述验证方根据所述交易金额的密文（C，B）验证所述交易金额的明文 M 是否属于第一有效范围；所述第一有效范围为[0，2^U-1]。

13、如权利要求 12 所述的方法，其特征在于，所述 $C=g_3^M g_4^r$，$B=g_3^r$；其中，r 为随机生成的整数，g_3 为 G_1 的生成元，G_1 是阶为素数的乘法群，g_4 为所述加法同态加密算法的公钥，$g_4=g_3^{ask}$，ask 为所述加法同态加密算法的私钥。

14、一种区块链系统，所述系统包括发送方及验证方，其特征在于：

所述发送方用于采用加法同态加密算法对交易金额的明文 M 加密，生成交易金额的密文（C，B），并将所述交易金额的密文（C，B）发送至所述验证方；

所述验证方用于根据所述交易金额的密文（C，B）验证所述交易金额的明文 M 是否属于第一有效范围；所述第一有效范围为[0，2^U-1]，U 为所述交易金额的明文 M 的比特位长度。

15、如权利要求 14 所述的系统，其特征在于，所述 $C=g_3^M g_4^r$，$B=g_3^r$；其中，r 为随机生成的整数，g_3 为 G_1 的生成元，G_1 是阶为素数的乘法群，g_4 为所述加法同态加密算法的公钥，$g_4=g_3^{ask}$，ask 为所述加法同态加密算法的私钥。

16、如权利要求 14 或 15 所述的系统，其特征在于，所述系统还包括监管方；

所述发送方用于将所述交易金额的明文 M 分割成 L 份交易金额的明文 M_k，分别采用加法同态加密算法对所述L份交易金额的明文M_k进行加密，生成L份交易金额的密文（C_k，B_k）；所述加法同态加密算法的公钥由所述监管方提供，k 为正整数，k=1，...，L，L 为大于或等于 2 的正整数；

所述验证方用于根据所述交易金额的密文（C_k，B_k）验证所述交易金额的明文 M_k 是否属于第二有效范围；所述第二有效范围为[0，2^u-1]，u 为所述交易金额的明文 M_k 的比特位长度；

所述监管方用于采用与所述公钥对应的私钥解密所述 L 份交易金额的密文（C_k，B_k），获得所述 L 份交易金额的明文 M_k，并根据所述 L 份交易金额的明文 M_k 获得所述交易金额的明文 M。

17、如权利要求 14-16 任一项所述的系统，其特征在于，所述发送方还用于生成所述交易金额的明文 M 属于第一有效范围的零知识证明；

所述验证方用于根据所述交易金额的密文（C，B）验证所述交易金额的明文 M 属于第一有效范围的零知识证明。

18、如权利要求 14-17 任一项所述的系统，其特征在于，所述交易金额包括输出金额；

所述发送方还用于计算输入金额与输出金额的差值的密文 C'，并生成 C'是加密了明文为零的密文的加法同态零知识证明；其中，所述 C'为根据所述输出金额的密文与所述输入金额的密文计算得到的密文，所述输入金额的密文为所述发送方在上一次交易中接收的金额的密文，或者所述输入金额的密文为所述发送方采用所述加法同态加密算法对当前交易中生成的金额加密生成的密文；

所述验证方还用于验证所述 C'是加密了明文为零的密文的加法同态零知识证明。

19、如权利要求 14 或 15 所述的系统，其特征在于，所述系统还包括监管方，所述加法同态加密算法的公钥由所述监管方提供；

所述发送方还用于生成所述监管方可解密所述交易金额的密文（C，B）的零知识证明；

所述验证方还用于验证所述监管方可解密所述交易金额的密文（C，B）的零知识证明；

所述监管方用于采用与所述公钥对应的私钥解密所述交易金额的密文（C，B）。

20、如权利要求 17 所述的系统，其特征在于，所述发送方用于生成 N 个第一参数；

所述验证方用于生成 N 个第二参数；其中，所述 N 个第一参数与所述 N 个第二参数一一对应；

验证所述 N 个第二参数是否与对应的所述第一参数相等，若相等，则所述交易金额的明文 M 属于第一有效范围。

21、如权利要求 20 所述的系统，其特征在于，所述发送方还用于生成第一验证参数；所述第一验证参数由所述 N 个第一参数决定；

所述验证方还用于生成第二验证参数；所述第二验证参数由所述 N 个第二参数决定；

所述验证方还用于验证所述第一参数是否等于所述第二验证参数，若相等，则所述 N 个第二参数与相应的所述第一参数相等。

22、一种发送方，应用于区块链系统，所述系统包括发送方及验证方，其特征在于，所述发送方包括：

加密单元，用于采用加法同态加密算法对交易金额的明文 M 加密，生成交易金额的密文（C，B）；其中，所述交易金额的明文 M 的比特位长度为 U；

发送单元，用于将所述交易金额的密文（C，B）发送至所述验证方，以使所述验证方根据所述交易金额的密文（C，B）验证所述交易金额的明文 M 是否属于第一有效范围；所述第一有效范围为[0，2^U-1]，U 为所述交易金额的明文 M 的比特位长度。

23、如权利要求 22 所述的发送方，其特征在于，所述 $C = g_3^M g_4^r$，$B = g_3^r$；其中，r 为随机生成的整数，g_3 为 G_1 的生成元，G_1 是阶为素数的乘法群，g_4 为所述加法同态加密算法的公钥，$g_4=g_3^{ask}$，ask 为所述加法同态加密算法的私钥。

24、如权利要求 22 或 23 所述的发送方，其特征在于，所述系统还包括监管方；

所述加密单元包括：

分割子单元，用于将所述交易金额的明文 M 分割成 L 份交易金额的明文 M_k；其中，k 为正整数，k=1，…，L；L 为大于或等于 2 的正整数；

加密子单元，用于分别采用加法同态加密算法对所述 L 份交易金额的明文 M_k 加密，生成 L 份交易金额的密文（C_k，B_k），以使所述监管方采用与所述公钥对应的私钥解密所述 L 份交易金额的密文（C_k，B_k），获得所述 L 份交易金额的明文 M_k，并根据所述 L 份交易金额的明文 M_k 获得所述交易金额的明文 M；所述加法同态加密算法的公钥由所述监管方提供；

所述发送单元，用于将所述 L 份交易金额的密文（C_k，B_k）发送至所述验证方，以使所述验证方根据所述交易金额的密文（C_k，B_k）验证所述交易金额的明文 M_k 是否属于第二有效范围；其中，所述第二有效范围为[0，2^u-1]，u 为所述交易金额的明文 M_k 的比特位长度。

25、一种验证方，应用于区块链系统，所述系统包括发送方及验证方，其特征在于，所述验证方包括：

接收单元，用于接收所述发送方发送的交易金额的密文（C，B）；其中，所述交易金额的密文（C，B）为所述发送方采用加法同态加密算法对交易金额的明文 M 加密生成的密文；所述交易金额的明文 M 的比特位长度为 U；

验证单元，用于根据所述交易金额的密文（C，B）验证所述交易金额的明文 M 是否

属于第一有效范围；所述第一有效范围为[0，2^U-1]。

26、如权利要求 25 所述的验证方，其特征在于，所述$C = g_3^M g_4^r$，$B = g_3^r$；其中，r 为随机生成的整数，g_3 为 G_1 的生成元，G_1 是阶为素数的乘法群，g_4 为所述加法同态加密算法的公钥，$g_4=g_3^{ask}$，ask 为所述加法同态加密算法的私钥。

27、一种发送方，应用于区块链系统，所述系统包括发送方及验证方，其特征在于，所述发送方包括：处理器、存储器和收发器，其中：

所述处理器、所述存储器和所述收发器相互连接，所述存储器用于存储计算机程序，所述计算机程序包括程序指令，所述处理器被配置用于调用所述程序指令，执行如权利要求 9-11 任意一项所述的数据处理方法。

28、一种验证方，应用于区块链系统，所述系统包括发送方及验证方，其特征在于，所述验证方包括：处理器、存储器和收发器，其中：

所述处理器、所述存储器和所述收发器相互连接，所述存储器用于存储计算机程序，所述计算机程序包括程序指令，所述处理器被配置用于调用所述程序指令，执行如权利要求 12 或 13 所述的数据处理方法。

29、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存储有计算机程序，所述计算机程序包括程序指令，所述程序指令当被处理器执行时，使所述处理器执行如权利要求 9-11 任意一项所述的数据处理方法。

30、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存储有计算机程序，所述计算机程序包括程序指令，所述程序指令当被处理器执行时，使所述处理器执行如权利要求 12 或 13 任意一项所述的数据处理方法。

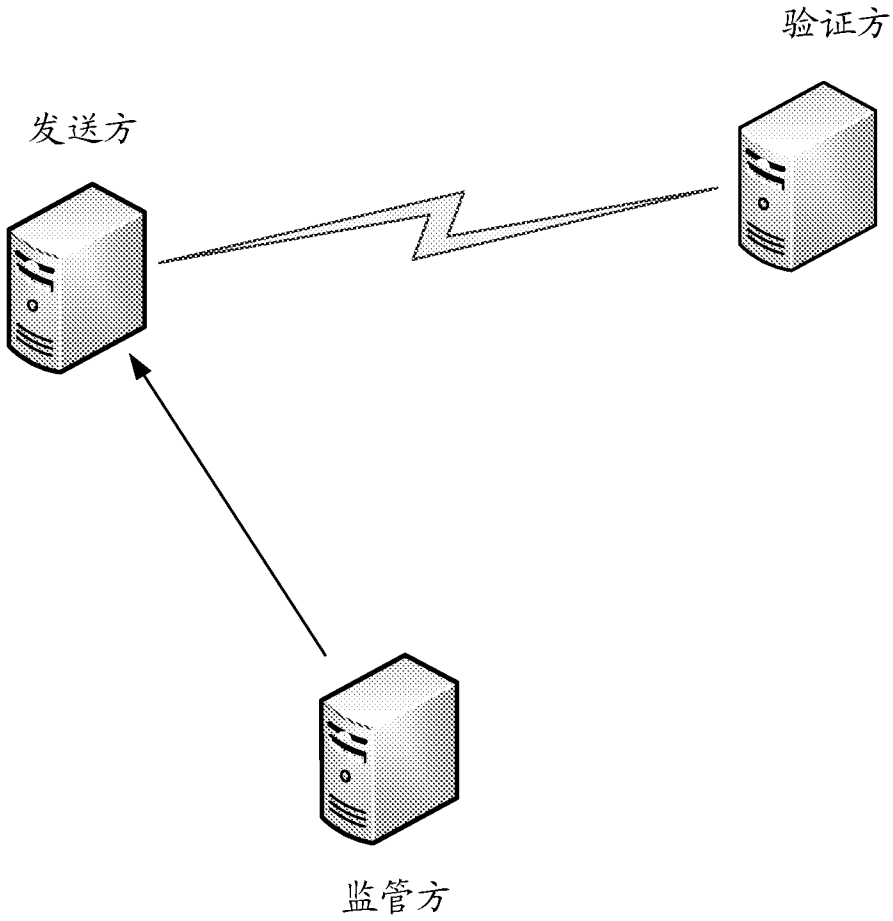

图 1

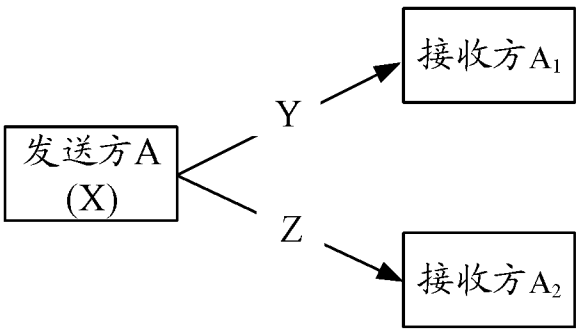

图 2

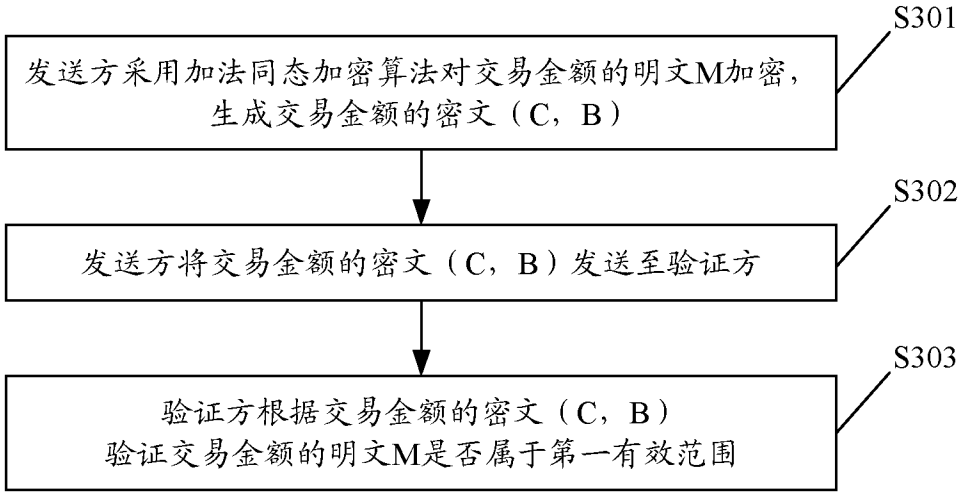
S301
发送方采用加法同态加密算法对交易金额的明文M加密，
生成交易金额的密文（C，B）
S302
发送方将交易金额的密文（C，B）发送至验证方
S303
验证方根据交易金额的密文（C，B）
验证交易金额的明文M是否属于第一有效范围

图 3

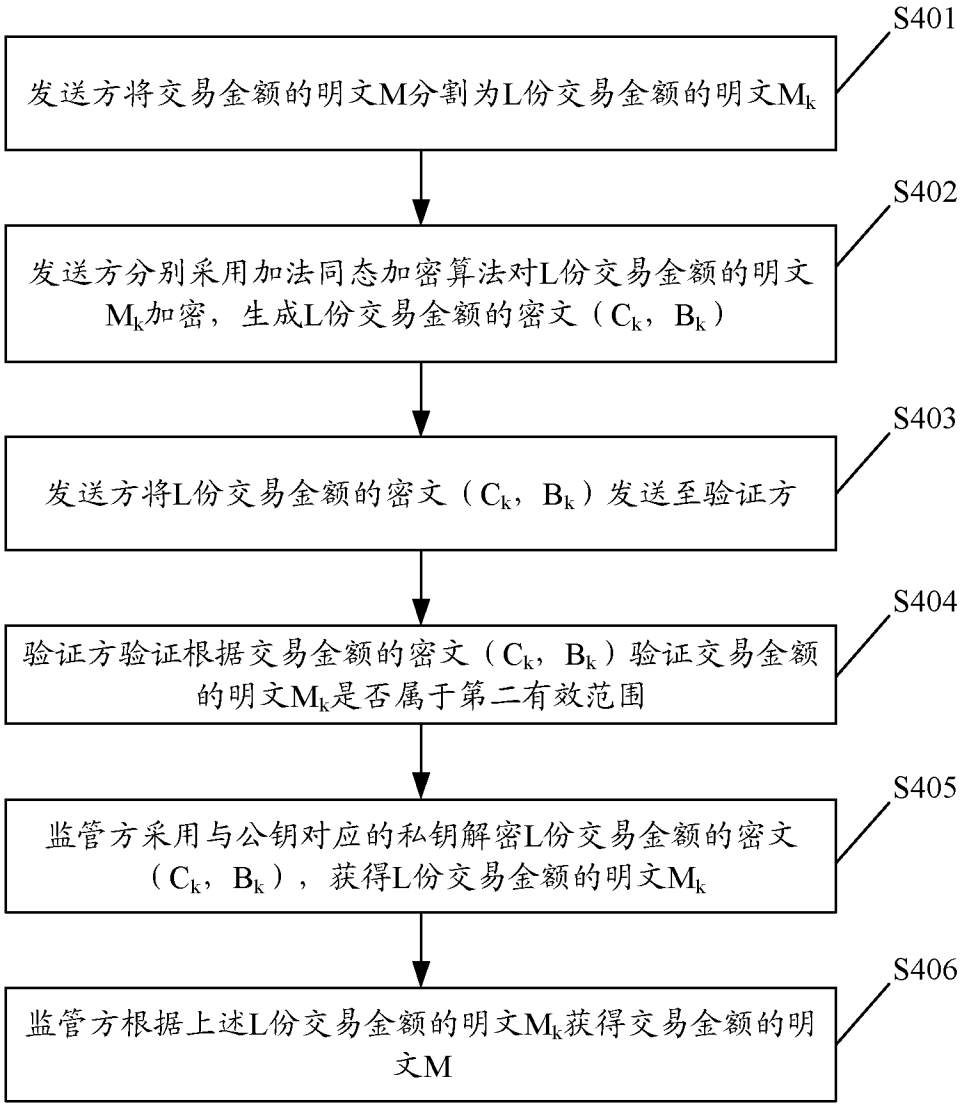
S401
发送方将交易金额的明文M分割为L份交易金额的明文M_k
S402
发送方分别采用加法同态加密算法对L份交易金额的明文M_k加密，生成L份交易金额的密文（C_k，B_k）
S403
发送方将L份交易金额的密文（C_k，B_k）发送至验证方
S404
验证方验证根据交易金额的密文（C_k，B_k）验证交易金额的明文M_k是否属于第二有效范围
S405
监管方采用与公钥对应的私钥解密L份交易金额的密文（C_k，B_k），获得L份交易金额的明文M_k
S406
监管方根据上述L份交易金额的明文M_k获得交易金额的明文M

图 4

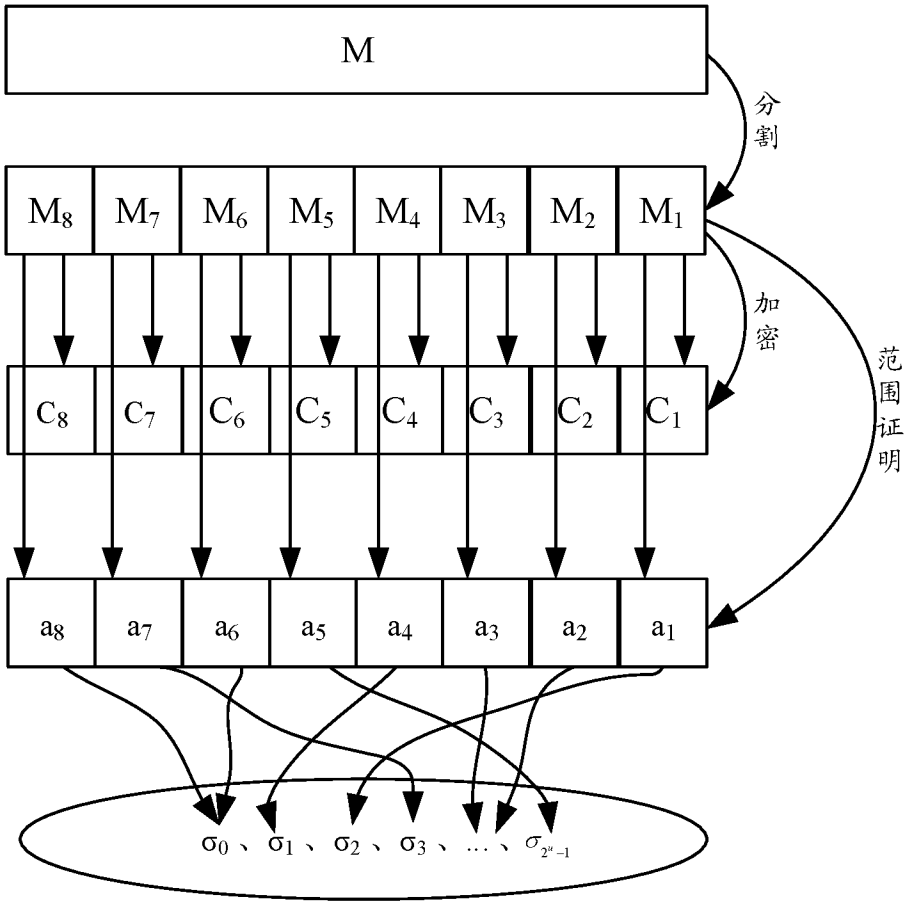
M
分割
M8 M7 M6 M5 M4 M3 M2 M1
加密
范围证明
C8 C7 C6 C5 C4 C3 C2 C1
a8 a7 a6 a5 a4 a3 a2 a1
σ0、σ1、σ2、σ3、…、σ2^u−1

图 5

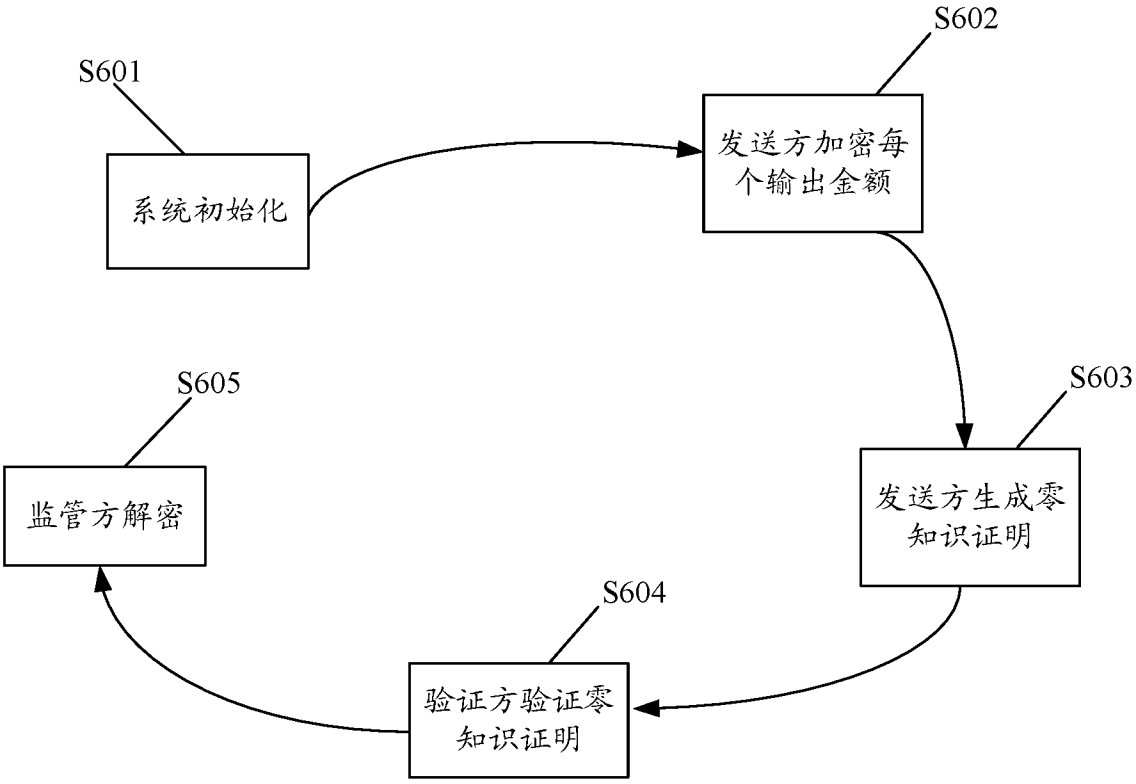
S601
系统初始化
S602
发送方加密每个输出金额
S603
发送方生成零知识证明
S604
验证方验证零知识证明
S605
监管方解密

图 6

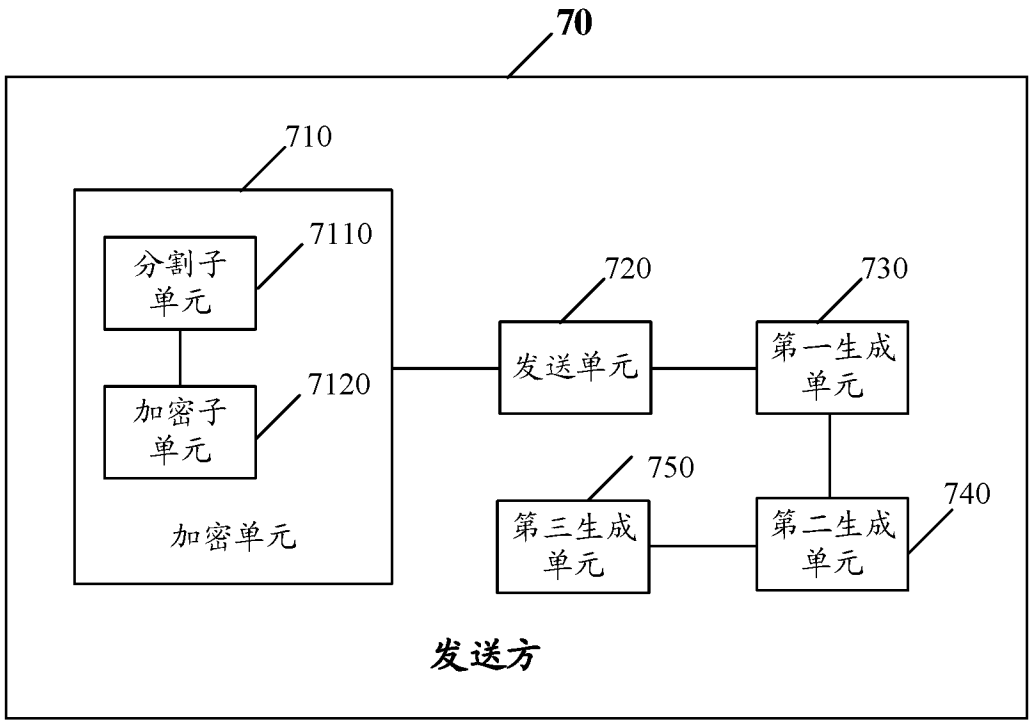
70
710
分割子单元
7110
加密子单元
7120
加密单元
720
发送单元
730
第一生成单元
750
第三生成单元
740
第二生成单元
发送方

图 7

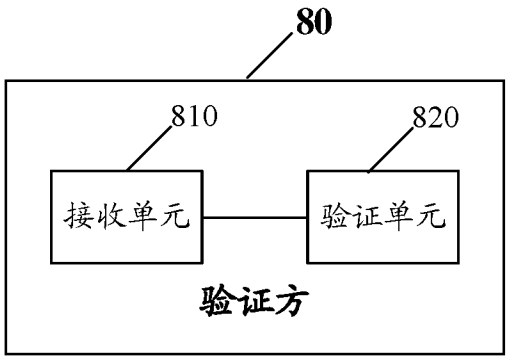
80
810
820
接收单元
验证单元
验证方

图 8

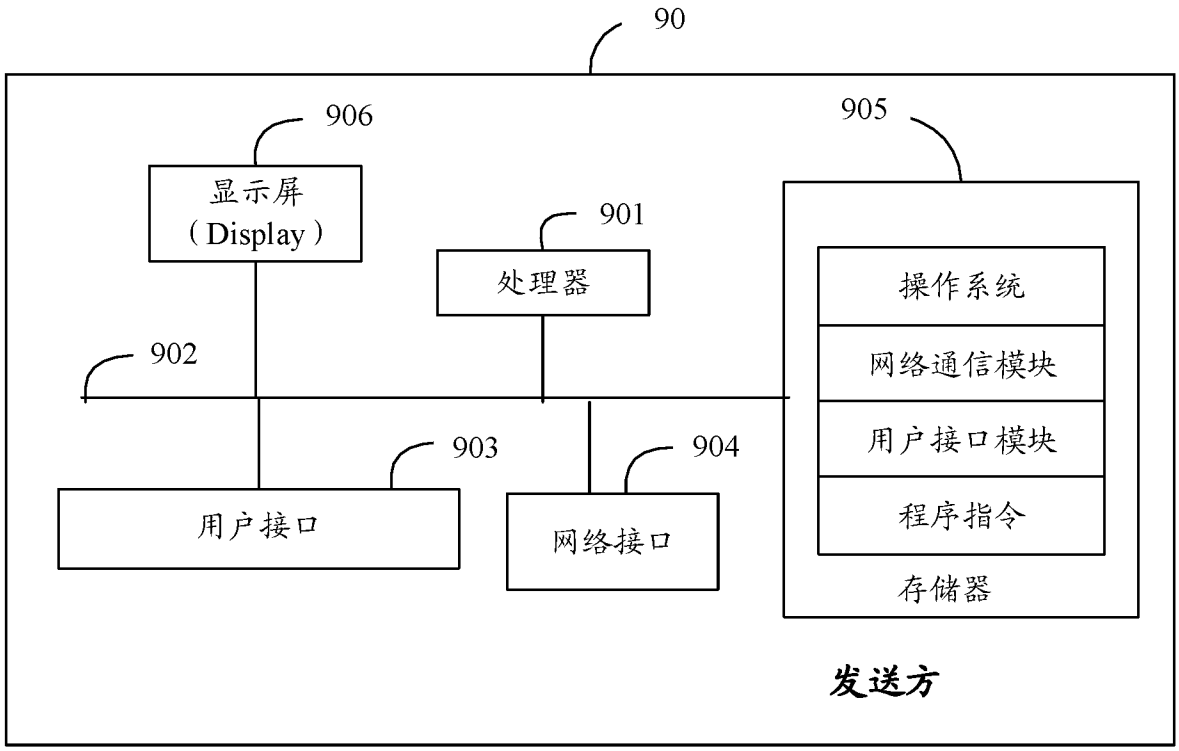
90
906
显示屏
（Display）
901
处理器
905
操作系统
网络通信模块
用户接口模块
程序指令
存储器
902
903
904
用户接口
网络接口
发送方

图 9

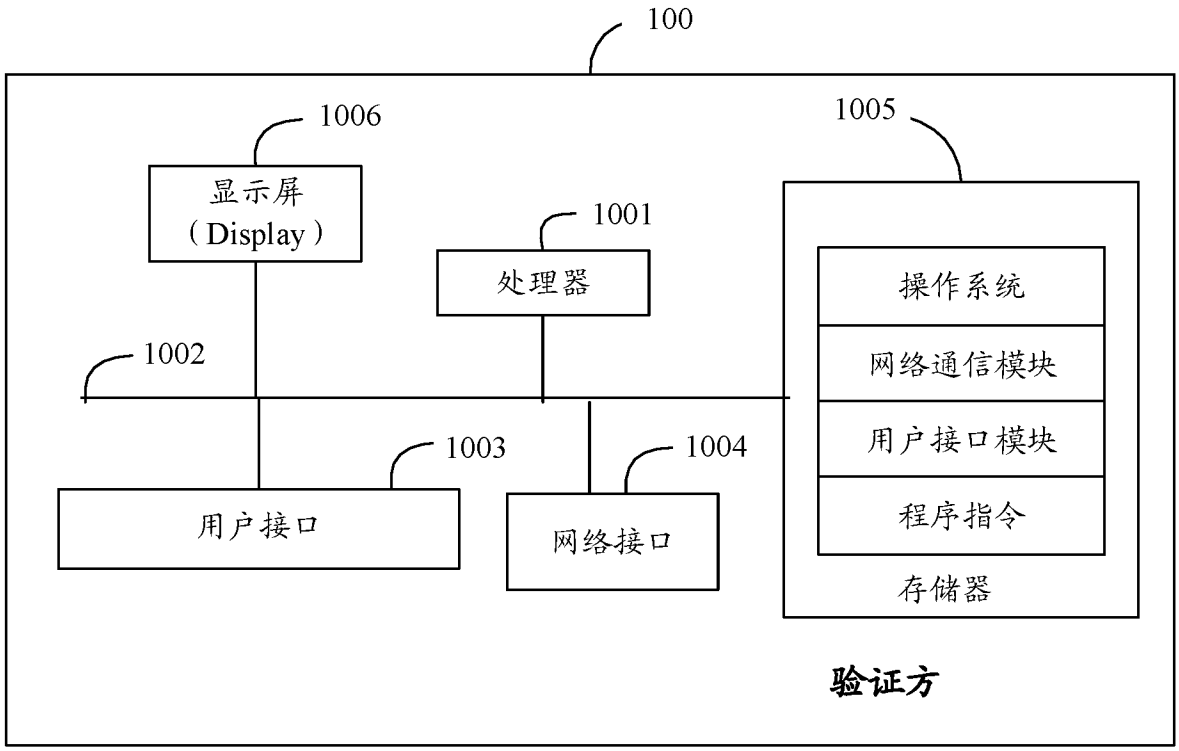
100
1006
显示屏
（Display）
1001
处理器
1005
操作系统
网络通信模块
用户接口模块
程序指令
存储器
1002
1003
用户接口
1004
网络接口
验证方

图 10