(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 108021821 A
(43)申请公布日 2018.05.11

(21)申请号 201711218249.X

(22)申请日 2017.11.28

(71)申请人 北京航空航天大学
地址 100191 北京市海淀区学院路37号

(72)发明人 伍前红 王沁

(74)专利代理机构 北京清亦华知识产权代理事务所(普通合伙) 11201
代理人 张润

(51)Int.Cl.
G06F 21/62(2013.01)
G06F 21/60(2013.01)
H04L 9/00(2006.01)

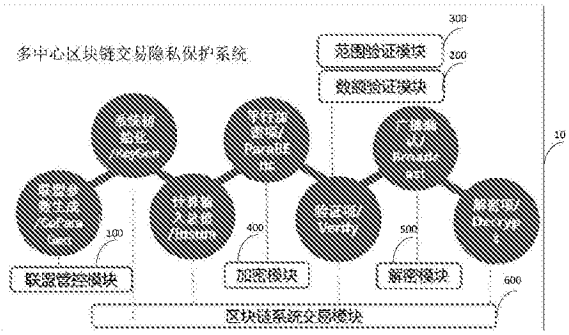
权利要求书3页 说明书18页 附图3页

(54)发明名称

多中心区块链交易隐私保护系统及方法

(57)摘要

本发明公开了一种多中心区块链交易隐私保护系统及方法，其中，系统包括：联盟管控模块用于多参与方联合生成联盟参数；数额验证模块用于验证加密后的密文数额在交易的输入和输出相等；范围验证模块用于验证交易中加密后的密文数额在特定区间，使得恒为正；加密模块和解密模块用于发送与接收过程对于数额进行同态加密和解密；区块链系统交易模块用于完整的类比特币数字货币交易系统，具备发送、接收、广播和区块确认的完整交易过程。该系统可以通过多中心监管模式下的区块链交易隐私增强通用构造，从而可以实现多方联合管控下对于陷门参数和交易过程中对于交易元数据的隐私保护，有效增强多中心类区块链系统交易过程中的明文数额安全。



CN 108021821 A

1.一种多中心区块链交易隐私保护系统，其特征在于，包括：

联盟管控模块，用于多参与方联合生成联盟参数；

数额验证模块，用于验证加密后的密文数额在交易的输入和输出相等；

范围验证模块，用于验证交易中加密后的密文数额在特定区间，使得恒为正；

加密模块和解密模块，用于发送与接收过程对于数额进行同态加密和解密；以及

区块链系统交易模块，用于完整的类比特币数字货币交易系统，具备发送、接收、广播和区块确认的完整交易过程。

2.根据权利要求1所述的多中心区块链交易隐私保护系统，其特征在于，

令Π_1=(rdmPara,coN,BipriTest,KeyGen)代表RSA门限密钥方案，其中rdmPara、coN、BipriTest和KeyGen分别为所述RSA门限密钥方案中的门限参数分配、联合生成模整数、双素性测试和联盟参数生成；

令Π_2=(PKeyGen,PEnc,PDec)代表同态加解密方案，其中PKeyGen、PEnc和PDec分别为所述同态加解密方案中的密钥生成、加密和解密算法；

令Π_3=(TKeyGen,TCom,TVer,TIndic)代表示性承诺证明方案，其中TKeyGen、TCom、TVer和TIndic分别为所述示性承诺证明方案中的密钥生成、承诺、验证和示性算法；

令Π_4=(RKeyGen,RCom,RVer,RInact)代表范围承诺证明方案，其中RKeyGen、RCom、RVer和RInact分别为方案中的密钥生成、承诺、验证和交互算法；

令Π_5=(TIn,TOut,TBroad,BCfm)代表类区块链交易系统方案，其中TIn、TOut、TBroad和BCfm分别为所述类区块链交易系统方案中的交易发送、交易接收、交易广播和区块确认。

3.根据权利要求2所述的多中心区块链交易隐私保护系统，其特征在于，所述区块链交易系统包括交易层和验证层，其中，所述交易层用于对执行所述区块链交易系统的交易步骤，包括交易单生成，输入输出，广播确认，并且经过加密的元数据取代原始明文，显示在交易单之中；所述验证层用于验证加密后的数据是否符合数值一致性以及存在于特定范围。

4.根据权利要求3所述的多中心区块链交易隐私保护系统，其特征在于，

所述联盟管控模块用于联盟成员依据分配得到的分块参数，达成共识联合生成系统交易的参数N，其中任意成员在未达到门限条件的情况下无法得知其陷门分解；

所述区块链系统交易模块用于所述交易系统输入安全参数和所述联盟参数，输出用于加解密运算的生成的公钥和私钥对(pk_i,sk_i)，同时输出用于验证的公钥pk_d，所述公钥无配对私钥；

所述区块链系统交易模块用于计算交易总输入值，其中，若交易单是作为新确认的区块，则所述交易单将获得额外的比特币费用作为奖励，所述总输入值为该部分明文与原密文相操作的总和；若所述交易单不是新确认区块首单，则无额外收入，所述总输入值为上单交易传来的值；

所述加密模块用于平行加密表示交易元数据经在所述交易层和所述验证层同时进行加密，其中，系统在所述交易层使用接受者公钥分别加密传输数额，同时在所述验证层使用系统公钥加密相同数额的各个数额；在所述交易层所加密的数额将在所述验证层通过后发送至各个接收者账户，注意到在所述验证层发送的加密数额将进入验证层账户，注意到该账户无私钥，金额在验证后丢弃；

所述加密模块和解密模块用于在所述验证层验证隐藏后的数额是否为正值，以及输入

输出总额是否相等，其中，所述验证层分为两步，第一步通过承诺值在特定区间的证明方法证明隐藏的金额始终为正值；当为真时，在所述验证层验证隐藏后的数额是否为正值后，系统验证层进入第二步，用过两个承诺值相等的证明方法证明隐藏的金额输入输出前后总数相等；当步骤都为真时，进入所述交易层的发送环节；

所述解密模块用于接收者核查无误后进行全网广播交易单等待确认，其中，经过处理后的交易单上原始的明文信息将隐藏为无法识读的密文，以保证交易过程唯一可能被分析处理的隐私；

所述区块链系统交易模块用于所述验证层验证通过后，所述交易层将加密后的数额发送给接收者，所述接收者依据自己的私钥进行解密；在所述接受者核对自己的接收金额正确后，继续下一单的交易，所述接受者的接收值为下一单的输入值。

5.根据权利要求4所述的多中心区块链交易隐私保护系统，其特征在于，

联盟成员秘密选取整数p_i和q_i，运行Π_1的rdmPara算法；

计算模整数N，其中，运行Π_1的CoN算法；

双素性测试，其中，所述联盟成员通过算法保证大整数N为两个素数的乘积，其中，运行Π_1的BipriTest算法；

联盟参数及门限密钥生成，运行Π_1的KeyGen算法，得出联盟密钥。

6.根据权利要求4所述的多中心区块链交易隐私保护系统，其特征在于，

对所述交易元数据进行加密，其中，运行Π_2的PEnc算法；

对所述交易元数据进行解密，其中，运行Π_2的PDec算法；

对密文进行同态操作，其中，运行Π_3的POper算法；

给定(m,m')，对明文秘密进行承诺计算，其中，运行Π_3的TCom算法；

验证承诺值的有效性，其中，运行Π_3的TVer算法；

对交易产生的不同密文值进行示性承诺验证是否含有相同元数据，其中，运行Π_3的TIndic算法。

7.根据权利要求4所述的多中心区块链交易隐私保护系统，其特征在于，

计算交易输入端总值，其中，运行Π_5的TIn算法；

依据路径指向交易输出端，其中，运行Π_5的TOut算法；

将交易单进行全网广播，其中，运行Π_5的TBroad算法；

旷工依据共识机制确认交易单生成区块，其中，运行Π_5的BCfm算法。

8.一种多中心区块链交易隐私保护方法，其特征在于，包括以下步骤：

联盟成员依据分配得到的分块参数，达成共识联合生成系统交易的参数N，其中任意成员在未达到门限条件的情况下无法得知其陷门分解；

交易系统输入安全参数和所述联盟参数，输出用于加解密运算的生成的公钥和私钥对(pk_i,sk_i)，同时输出用于验证的公钥pk_d，所述公钥无配对私钥；

计算交易总输入值，其中，若交易单是作为新确认的区块，则所述交易单将获得额外的比特币费用作为奖励，所述总输入值为该部分明文与原密文相操作的总和；若所述交易单不是新确认区块首单，则无额外收入，所述总输入值为上单交易传来的值；

平行加密表示交易元数据经在所述交易层和所述验证层同时进行加密，其中，系统在所述交易层使用接受者公钥分别加密传输数额，同时在所述验证层使用系统公钥加密相同

数额的各个数额;在所述交易层所加密的数额将在所述验证层通过后发送至各个接收者账户,注意到在所述验证层发送的加密数额将进入验证层账户,注意到该账户无私钥,金额在验证后丢弃;

在所述验证层验证隐藏后的数额是否为正值,以及输入输出总额是否相等,其中,所述验证层分为两步,第一步通过承诺值在特定区间的证明方法证明隐藏的金额始终为正值;当为真时,在所述验证层验证隐藏后的数额是否为正值后,系统验证层进入第二步,用过两个承诺值相等的证明方法证明隐藏的金额输入输出前后总数相等;当步骤都为真时,进入所述交易层的发送环节;

接收者核查无误后进行全网广播交易单等待确认,其中,经过处理后的交易单上原始的明文信息将隐藏为无法识读的密文,以保证交易过程唯一可能被分析处理的隐私;以及

所述验证层验证通过后,所述交易层将加密后的数额发送给接收者,所述接收者依据自己的私钥进行解密;在所述接受者核对自己的接收金额正确后,继续下一单的交易,所述接受者的接收值为下一单的输入值。

9.根据权利要求8所述的多中心区块链交易隐私保护方法,其特征在于,

令Π_1=(rdmPara,coN,BipriTest,KeyGen)代表RSA门限密钥方案,其中rdmPara、coN、BipriTest和KeyGen分别为所述RSA门限密钥方案中的门限参数分配、联合生成模整数、双素性测试和联盟参数生成;

令Π_2=(PKeyGen,PEnc,PDec)代表同态加解密方案,其中PKeyGen、PEnc和PDec分别为所述同态加解密方案中的密钥生成、加密和解密算法;

令Π_3=(TKeyGen,TCom,TVer,TIndic)代表示性承诺证明方案,其中TKeyGen、TCom、TVer和TIndic分别为所述示性承诺证明方案中的密钥生成、承诺、验证和示性算法;

令Π_4=(RKeyGen,RCom,RVer,RInact)代表范围承诺证明方案,其中RKeyGen、RCom、RVer和RInact分别为方案中的密钥生成、承诺、验证和交互算法;

令Π_5=(TIn,TOut,TBroad,BCfm)代表类区块链交易系统方案,其中TIn、TOut、TBroad和BCfm分别为所述类区块链交易系统方案中的交易发送、交易接收、交易广播和区块确认。

10.根据权利要求8或9所述的多中心区块链交易隐私保护方法,其特征在于,所述区块链交易系统包括所述交易层和所述验证层,其中,所述交易层用于对执行所述区块链交易系统的交易步骤,包括交易单生成,输入输出,广播确认,并且经过加密的元数据取代原始明文,显示在交易单之中;所述验证层用于验证加密后的数据是否符合数值一致性以及存在于特定范围。

多中心区块链交易隐私保护系统及方法

技术领域

[0001] 本发明涉及信息安全中的密码学以及密码学货币技术领域，特别涉及一种多中心区块链交易隐私保护系统及方法。

背景技术

[0002] 类区块链交易系统发轫于比特币数字货币系统。2008年，日本程序员中本聪(Satoshi Nakamoto)设计并发布了一种点对点的去中心化数字货币——比特币。比特币系统提出了基于点对点的新型分布式模式，去除了传统电子货币的可信中心机构。比特币的隐蔽性与去中心化，带动了一系列基于密码学的互联网货币兴起。按照工作原理的不同，包括基于PoW(Proof of Work，工作量证明)的比特币、莱特币、狗狗币，基于PoS(Proof of Stake，股权证明)的比特股、智能坊黑币，以及基于PoW+PoS的以太坊、点点币等。

[0003] 区块链技术作为比特币系统的底层实现，展现出的去中心化、信息不可篡改、信息广泛传播、信息匿名特性逐渐被学术界与工业界关注并展开深入研究与广泛应用。区块链1.0时代，是以比特币等数字货币为核心形成的底层产业结构，形成了矿机、矿池、数字货币、支付钱包、交易所、数字货币网关的产业群和产业链。在区块链2.0时代，技术和应用的焦点从单纯电子货币转移到底层技术区块链技术的应用上来，形成了区块链+X产业的生态圈，类别和行业跨越大、独立程度高，涉及到资产验证、金融服务、慈善、媒体及社区、研究及投资、智能合约、公正防伪、电子商务、社交通讯、物联网、文件存储等领域。

[0004] 然而，随着类区块链交易系统的大面积传播，系统内在的设计与运行带来了两个公开的隐私泄露问题：1)多方监管中对于成员的信任问题，如联盟链间的配合；2)交易过程中元数据的隐私泄露问题，如交易中明文数额的暴露。

发明内容

[0005] 本发明旨在至少在一定程度上解决相关技术中的技术问题之一。

[0006] 为此，本发明的一个目的在于提出一种多中心区块链交易隐私保护系统，该系统可以实现多方联合管控下对于陷门参数和交易过程中对于交易元数据的隐私保护，有效增强多中心类区块链系统交易过程中的明文数额安全。

[0007] 本发明的另一个目的在于提出一种多中心区块链交易隐私保护方法。

[0008] 为达到上述目的，本发明一方面实施例提出了一种多中心区块链交易隐私保护系统，包括：联盟管控模块，用于多参与方联合生成联盟参数；数额验证模块，用于验证加密后的密文数额在交易的输入和输出相等；范围验证模块，用于验证交易中加密后的密文数额在特定区间，使得恒为正；加密模块和解密模块，用于发送与接收过程对于数额进行同态加密和解密；区块链系统交易模块，用于完整的类比特币数字货币交易系统，具备发送、接收、广播和区块确认的完整交易过程。

[0009] 本发明实施例的多中心区块链交易隐私保护系统，可以利用门限加解密体制实现对于多参与方联合管控中对于生成陷门参数的隐私保护，利用同态加密体制实现对数额的

加解密运算增强传输过程中的数额隐私，利用范围承诺证明与示性承诺证明保证交易过程中确保了隐藏的交易值始终为正值且交易数额前后总数一致，从而可以实现多方联合管控下对于陷门参数和交易过程中对于交易元数据的隐私保护，有效增强多中心类区块链系统交易过程中的明文数额安全。

[0010] 另外，根据本发明上述实施例的多中心区块链交易隐私保护系统还可以具有以下附加的技术特征：

[0011] 进一步地，在本发明的一个实施例中，令Π_1=(rdmPara,coN,BipriTest,KeyGen)代表RSA门限密钥方案，其中rdmPara、coN、BipriTest和KeyGen分别为所述RSA门限密钥方案中的门限参数分配、联合生成模整数、双素性测试和联盟参数生成；令Π_2=(PKeyGen,PEnc,PDec)代表同态加解密方案，其中PKeyGen、PEnc和PDec分别为所述同态加解密方案中的密钥生成、加密和解密算法；令Π_3=(TKeyGen,TCom,TVer,TIndic)代表示性承诺证明方案，其中TKeyGen、TCom、TVer和TIndic分别为所述示性承诺证明方案中的密钥生成、承诺、验证和示性算法；令Π_4=(RKeyGen,RCom,RVer,RInact)代表范围承诺证明方案，其中RKeyGen、RCom、RVer和RInact分别为方案中的密钥生成、承诺、验证和交互算法；令Π_5=(TIn,TOut,TBroad,BCfm)代表类区块链交易系统方案，其中TIn、TOut、TBroad和BCfm分别为所述类区块链交易系统方案中的交易发送、交易接收、交易广播和区块确认。

[0012] 进一步地，在本发明的一个实施例中，所述区块链交易系统包括交易层和验证层，其中，所述交易层用于对执行所述区块链交易系统的交易步骤，包括交易单生成，输入输出，广播确认，并且经过加密的元数据取代原始明文，显示在交易单之中；所述验证层用于验证加密后的数据是否符合数值一致性以及存在于特定范围。

[0013] 进一步地，在本发明的一个实施例中，所述联盟管控模块用于联盟成员依据分配得到的分块参数，达成共识联合生成系统交易的参数N，其中任意成员在未达到门限条件的情况下无法得知其陷门分解；所述区块链系统交易模块用于所述交易系统输入安全参数和所述联盟参数，输出用于加解密运算的生成的公钥和私钥对(pk_i,sk_i)，同时输出用于验证的公钥pk_d，所述公钥无配对私钥；所述区块链系统交易模块用于计算交易总输入值，其中，若交易单是作为新确认的区块，则所述交易单将获得额外的比特币费用作为奖励，所述总输入值为该部分明文与原密文相操作的总和；若所述交易单不是新确认区块首单，则无额外收入，所述总输入值为上单交易传来的值；所述加密模块用于平行加密表示交易元数据经在所述交易层和所述验证层同时进行加密，其中，系统在所述交易层使用接受者公钥分别加密传输数额，同时在所述验证层使用系统公钥加密相同数额的各个数额；在所述交易层所加密的数额将在所述验证层通过后发送至各个接收者账户，注意到在所述验证层发送的加密数额将进入验证层账户，注意到该账户无私钥，金额在验证后丢弃；所述加密模块和解密模块用于在所述验证层验证隐藏后的数额是否为正值，以及输入输出总额是否相等，其中，所述验证层分为两步，第一步通过承诺值在特定区间的证明方法证明隐藏的金额始终为正值；当为真时，在所述验证层验证隐藏后的数额是否为正值后，系统验证层进入第二步，用过两个承诺值相等的证明方法证明隐藏的金额输入输出前后总数相等；当步骤都为真时，进入所述交易层的发送环节；所述解密模块用于接收者核查无误后进行全网广播交易单等待确认，其中，经过处理后的交易单上原始的明文信息将隐藏为无法识读的密文，以保证交易过程唯一可能被分析处理的隐私；所述区块链系统交易模块用于所述验证层验证

通过后，所述交易层将加密后的数额发送给接收者，所述接收者依据自己的私钥进行解密；在所述接受者核对自己的接收金额正确后，继续下一单的交易，所述接受者的接收值为下一单的输入值。

[0014] 进一步地，在本发明的一个实施例中，联盟成员秘密选取整数p_i和q_i，运行Π_1的rdmPara算法；计算模整数N，其中，运行Π_1的CoN算法；双素性测试，其中，所述联盟成员通过算法保证大整数N为两个素数的乘积，其中，运行Π_1的BipriTest算法；联盟参数及门限密钥生成，运行Π_1的KeyGen算法，得出联盟密钥。

[0015] 进一步地，在本发明的一个实施例中，对所述交易元数据进行加密，其中，运行Π_2的PEnc算法；对所述交易元数据进行解密，其中，运行Π_2的PDec算法；对密文进行同态操作，其中，运行Π_3的POper算法。

[0016] 进一步地，在本发明的一个实施例中，给定(m,m')，对明文秘密进行承诺计算，其中，运行Π_3的TCom算法；验证承诺值的有效性，其中，运行Π_3的TVer算法；对交易产生的不同密文值进行示性承诺验证是否含有相同元数据，其中，运行Π_3的TIndic算法。

[0017] 进一步地，在本发明的一个实施例中，计算交易输入端总值，其中，运行Π_5的TIn算法；依据路径指向交易输出端，其中，运行Π_5的TOut算法；将交易单进行全网广播，其中，运行Π_5的TBroad算法；旷工依据共识机制确认交易单生成区块，其中，运行Π_5的BCfm算法。

[0018] 为达到上述目的，本发明另一方面实施例提出了一种多中心区块链交易隐私保护方法，包括以下步骤：联盟成员依据分配得到的分块参数，达成共识联合生成系统交易的参数N，其中任意成员在未达到门限条件的情况下无法得知其陷门分解；交易系统输入安全参数和所述联盟参数，输出用于加解密运算的生成的公钥和私钥对(pk_i,sk_i)，同时输出用于验证的公钥pk_d，所述公钥无配对私钥；计算交易总输入值，其中，若交易单是作为新确认的区块，则所述交易单将获得额外的比特币费用作为奖励，所述总输入值为该部分明文与原密文相操作的总和；若所述交易单不是新确认区块首单，则无额外收入，所述总输入值为上单交易传来的值；平行加密表示交易元数据经在所述交易层和所述验证层同时进行加密，其中，系统在所述交易层使用接受者公钥分别加密传输数额，同时在所述验证层使用系统公钥加密相同数额的各个数额；在所述交易层所加密的数额将在所述验证层通过后发送至各个接收者账户，注意到在所述验证层发送的加密数额将进入验证层账户，注意到该账户无私钥，金额在验证后丢弃；在所述验证层验证隐藏后的数额是否为正值，以及输入输出总额是否相等，其中，所述验证层分为两步，第一步通过承诺值在特定区间的证明方法证明隐藏的金额始终为正值；当为真时，在所述验证层验证隐藏后的数额是否为正值后，系统验证层进入第二步，用过两个承诺值相等的证明方法证明隐藏的金额输入输出前后总数相等；当步骤都为真时，进入所述交易层的发送环节；接收者核查无误后进行全网广播交易单等待确认，其中，经过处理后的交易单上原始的明文信息将隐藏为无法识读的密文，以保证交易过程唯一可能被分析处理的隐私；所述验证层验证通过后，所述交易层将加密后的数额发送给接收者，所述接收者依据自己的私钥进行解密；在所述接受者核对自己的接收金额正确后，继续下一单的交易，所述接受者的接收值为下一单的输入值。

[0019] 本发明实施例的多中心区块链交易隐私保护方法，可以利用门限加解密体制实现对于多参与方联合管控中对于生成陷门参数的隐私保护，利用同态加密体制实现对数额的加解密运算增强传输过程中的数额隐私，利用范围承诺证明与示性承诺证明保证交易过程

中确保了隐藏的交易值始终为正值且交易数额前后总数一致，从而可以实现多方联合管控下对于陷门参数和交易过程中对于交易元数据的隐私保护，有效增强多中心类区块链系统交易过程中的明文数额安全。

[0020] 另外，根据本发明上述实施例的多中心区块链交易隐私保护方法还可以具有以下附加的技术特征：

[0021] 进一步地，在本发明的一个实施例中，令Π_1=(rdmPara,coN,BipriTest,KeyGen)代表RSA门限密钥方案，其中rdmPara、coN、BipriTest和KeyGen分别为所述RSA门限密钥方案中的门限参数分配、联合生成模整数、双素性测试和联盟参数生成；令Π_2=(PKeyGen,PEnc,PDec)代表同态加解密方案，其中PKeyGen、PEnc和PDec分别为所述同态加解密方案中的密钥生成、加密和解密算法；令Π_3=(TKeyGen,TCom,TVer,TIndic)代表示性承诺证明方案，其中TKeyGen、TCom、TVer和TIndic分别为所述示性承诺证明方案中的密钥生成、承诺、验证和示性算法；令Π_4=(RKeyGen,RCom,RVer,RInact)代表范围承诺证明方案，其中RKeyGen、RCom、RVer和RInact分别为方案中的密钥生成、承诺、验证和交互算法；令Π_5=(TIn,TOut,TBroad,BCfm)代表类区块链交易系统方案，其中TIn、TOut、TBroad和BCfm分别为所述类区块链交易系统方案中的交易发送、交易接收、交易广播和区块确认。

[0022] 进一步地，在本发明的一个实施例中，所述区块链交易系统包括所述交易层和所述验证层，其中，所述交易层用于对执行所述区块链交易系统的交易步骤，包括交易单生成，输入输出，广播确认，并且经过加密的元数据取代原始明文，显示在交易单之中；所述验证层用于验证加密后的数据是否符合数值一致性以及存在于特定范围。

[0023] 本发明附加的方面和优点将在下面的描述中部分给出，部分将从下面的描述中变得明显，或通过本发明的实践了解到。

附图说明

[0024] 本发明上述的和/或附加的方面和优点从下面结合附图对实施例的描述中将变得明显和容易理解，其中：

[0025] 图1为根据本发明一个实施例的多中心区块链交易隐私保护系统的结构示意图；

[0026] 图2为根据本发明一个实施例的通用方案流程图；

[0027] 图3为根据本发明一个实施例的具体方案流程图；

[0028] 图4为根据本发明一个实施例的系统交易流程图；

[0029] 图5为根据本发明一个实施例的多中心区块链交易隐私保护方法的流程图。

具体实施方式

[0030] 下面详细描述本发明的实施例，所述实施例的示例在附图中示出，其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的，旨在用于解释本发明，而不能理解为对本发明的限制。

[0031] 在介绍多中心区块链交易隐私保护系统及方法之前，先简单介绍一下类区块链系统的设计原理。

[0032] 本发明实施例深入分析该类区块链系统的设计原理，通过密码学门限生成机制、同态加解密体制、承诺与零知识证明方法，提出了对上述问题的通用构造解决方法，并结合

现有的密码学工具给出了实例化方案构造。

[0033] 门限生成机制用于对多参与方联合管控下对于生成陷门参数的隐私保护，方案采用Dan Boheh提出的协议来联合生成系统的RSA(RSA algorithm,RSA加密算法)模整数。该协议使多参与方联合生成系统的参数，即RSA大整数N，然而任意一方都不知道整数的分解因子p和q。若想使系统正常运行，必须得到多个参与方的共识，才能生成其参数保证运行，但是任意一方无法得知生成后的陷门质因子。该机制保护了公平的保障了多个参与方的利益，使系统的运行在发送方便得到分布性，同时也对陷门参数进行了隐私保护，保证了系统的整体安全性。

[0034] 同态加密体制用于对交易中明文数额的隐蔽保护，方案采用Paillier加密体制对明文交易数额进行加密传输。该体制是1999年由Pascal Paillier提出，加密体制的困难性基于合数阶剩余类困难问题，具有在标准模型下的抗选择明文攻击安全。该体制具有加同态特性，使得通过对加密后的密文进行乘操作来实现相应的明文加减操作，该性质运用于在不泄露隐私情况下的验证过程。除了同态特性，该体制还具备高效性，使得方案可以通过进行预计算以及运用中国剩余定理进行快速计算，满足在比特币交易时间内的加密解密步骤。

[0035] 在运用加密体制进行加密后，生成的密文将存在于每个交易单中，为保证相应密文隐藏的明文的满足正值以及和相等的要求，方案运用了承诺证明和零知识证明来进行验证。在特定区间的范围承诺值证明(Range Proof)采用2004年伍前红等人提出的方法，该方法在步骤相对简单的过程下保证了小的扩张域，使秘密数额保持为正值可证。两个承诺值相等的示性承诺证明(Balance)运用哈希映射值相等的思想，在不泄露被承诺数的情况下验证两个承诺值包含同一个秘密值。两个证明方案都具备零知识特性，保证了加密后的数额在验证过程中不被泄露，提高了交易中对元数据的隐私保护。

[0036] 本发明实施例面向国家层面的安全需求，遵循上述原则，通过设计一种通用的多方管控的区块链交易隐私保护方案，实现该类交易系统中对于联合管控与隐私增强的实际需求。

[0037] 正是基于上述原因，本发明实施例提出了一种多中心区块链交易隐私保护系统及方法。

[0038] 下面参照附图描述根据本发明实施例提出的多中心区块链交易隐私保护系统及方法，首先将参照附图描述根据本发明实施例提出的多中心区块链交易隐私保护系统。

[0039] 图1是本发明一个实施例的多中心区块链交易隐私保护系统的结构示意图。

[0040] 如图1所示，该多中心区块链交易隐私保护系统10包括：联盟管控模块100、数额验证模块200、范围验证模块300、加密模块400、解密模块500和区块链系统交易模块600。

[0041] 其中，联盟管控模块100用于多参与方联合生成联盟参数。数额验证模块200用于验证加密后的密文数额在交易的输入和输出相等。范围验证模块300用于验证交易中加密后的密文数额在特定区间，使得恒为正。加密模块400和解密模块500用于发送与接收过程对于数额进行同态加密和解密。区块链系统交易模块600用于完整的类比特币数字货币交易系统，具备发送、接收、广播和区块确认的完整交易过程。本发明实施例的系统10可以通过多中心监管模式下的区块链交易隐私增强通用构造，从而可以实现多方联合管控下对于陷门参数和交易过程中对于交易元数据的隐私保护，有效增强多中心类区块链系统交易过

程中的明文数额安全。

[0042] 可以理解的是，本发明实施例可以用于增强多中心类区块链系统交易过程中的明文数额安全，特别适用于联盟链方式下的交易隐私保护，并设计出一种具备在在多方联合管控模式下交易隐私保护功能的通用构造。该构造有模块化结构搭建，并依据模块特性一次实现联盟管控、同态加密、零知识验证、可信交易的功能。其中模块包括：1.联合管控模块100：多参与方联合生成联盟陷门参数；2.数额验证模块200：验证加密后的密文数额在交易的输入和输出相等；3范围验证模块300：验证交易中加密后的密文数额在特定区间，即恒为正；4.同态加解密模块包括加密模块400和解密模块500：发送与接收过程对于数额进行同态加解密；5.区块链交易模块600：完整的类比特币数字货币交易系统，具备发送、接收、广播和区块确认的完整交易过程。本发明实施例可以通过门限加解密体制实现了多方联合管控下对于陷门参数的隐私保护，通过同态加密体制实现了交易过程中对于交易元数据即明文数额的隐私保护，同时通过零知识证明与承诺证明保证了交易中隐藏数额始终为正且输入输出总额相等的要求。

[0043] 进一步地，在本发明的一个实施例中，令Π_1=(rdmPara,coN,BipriTest,KeyGen)代表RSA门限密钥方案，其中rdmPara、coN、BipriTest和KeyGen分别为RSA门限密钥方案中的门限参数分配、联合生成模整数、双素性测试和联盟参数生成；令Π_2=(PKeyGen,PEnc,PDec)代表同态加解密方案，其中PKeyGen、PEnc和PDec分别为同态加解密方案中的密钥生成、加密和解密算法；令Π_3=(TKeyGen,TCom,TVer,TIndic)代表示性承诺证明方案，其中TKeyGen、TCom、TVer和TIndic分别为示性承诺证明方案中的密钥生成、承诺、验证和示性算法；令Π_4=(RKeyGen,RCom,RVer,RInact)代表范围承诺证明方案，其中RKeyGen、RCom、RVer和RInact分别为方案中的密钥生成、承诺、验证和交互算法；令Π_5=(TIn,TOut,TBroad,BCfm)代表类区块链交易系统方案，其中TIn、TOut、TBroad和BCfm分别为类区块链交易系统方案中的交易发送、交易接收、交易广播和区块确认。

[0044] 可以理解的是，如图2所示，本发明实施例可以列出通用构造用到的密码学工具，并主要给出构造通用结构时需要用到的密码学基础工具，包括门限生成体制、同态加解密体制、承诺证明体制、零知识证明体制以及区块链交易系统。首先给出这些基础工具的简单定义，然后分别对各个密码体制进行详细介绍，其中，将在下面对各个密码体制进行详细介绍。基础工具的简单定义：

[0045] 令Π_1=(rdmPara,coN,BipriTest,KeyGen)代表RSA门限密钥方案，其中rdmPara，coN,BipriTest和KeyGen分别为方案中的门限参数分配、联合生成模整数、双素性测试和联盟参数生成。

[0046] 令Π_2=(PKeyGen,PEnc,PDec)代表同态加解密方案，其中PKeyGen,PEnc和PDec分别为方案中的密钥生成、加密和解密算法。

[0047] 令Π_3=(TKeyGen,TCom,TVer,TIndic)代表示性承诺证明，其中TKeyGen,TCom，TVer和TIndic分别为方案中的密钥生成、承诺、验证和示性算法。

[0048] 令Π_4=(RKeyGen,RCom,RVer,RInact)代表范围承诺证明方案，其中RKeyGen，RCom、RVer和RInact分别为方案中的密钥生成、承诺、验证和交互算法。

[0049] 令Π_5=(TIn,TOut,TBroad,BCfm)代表类区块链交易系统方案，其中TIn,TOut，TBroad和BCfm分别为方案中的交易发送(交易单的输入端)，交易接收(交易单的输出端)，

交易广播和区块确认。

[0050] 进一步地，在本发明的一个实施例中，区块链交易系统包括交易层和验证层，其中，交易层用于对执行区块链交易系统的交易步骤，包括交易单生成，输入输出，广播确认，并且经过加密的元数据取代原始明文，显示在交易单之中；验证层用于验证加密后的数据是否符合数值一致性以及存在于特定范围。

[0051] 可以理解的是，区块链交易系统分为两个层级：1.交易层/Transaction layer：交易层用于对执行区块链交易系统的交易步骤，包括交易单生成，输入输出，广播确认等。经过加密的元数据取代原始明文，显示在交易单之中。该层级主要调用模块MEnc和Tx。2.验证层/Verification layer：与交易层为平行结构，用于验证加密后的数据是否符合数值一致性以及存在于特定范围。该层级主要调用模块MEnc，BalanceVer和RangeVer。需要说明的是，联系交易层和验证层共同调用了模块MEnc，同时加密交易元数据，只是两者使用不同的公钥，生成不同的密文/承诺值。交易层的密文用于真实交易，验证层的密文用于一致性与范围验证。

[0052] 进一步地，在本发明的一个实施例中，联盟管控模块100用于联盟成员依据分配得到的分块参数，达成共识联合生成系统交易的参数N，其中任意成员在未达到门限条件的情况下无法得知其陷门分解；区块链系统交易模块600用于交易系统输入安全参数和联盟参数，输出用于加解密运算的生成的公钥和私钥对(pk_i, sk_i)，同时输出用于验证的公钥pk_d，公钥无配对私钥；区块链系统交易模块600用于计算交易总输入值，其中，若交易单是作为新确认的区块，则交易单将获得额外的比特币费用作为奖励，总输入值为该部分明文与原密文相操作的总和；若交易单不是新确认区块首单，则无额外收入，总输入值为上单交易传来的值；加密模块400用于平行加密表示交易元数据经在交易层和验证层同时进行加密，其中，系统在交易层使用接受者公钥分别加密传输数额，同时在验证层使用系统公钥加密相同数额的各个数额；在交易层所加密的数额将在验证层通过后发送至各个接收者账户，注意到在验证层发送的加密数额将进入验证层账户，注意到该账户无私钥，金额在验证后丢弃；加密模块400和解密模块500用于在验证层验证隐藏后的数额是否为正值，以及输入输出总额是否相等，其中，验证层分为两步，第一步通过承诺值在特定区间的证明方法证明隐藏的金额始终为正值；当为真时，在验证层验证隐藏后的数额是否为正值后，系统验证层进入第二步，用过两个承诺值相等的证明方法证明隐藏的金额输入输出前后总数相等；当步骤都为真时，进入交易层的发送环节；解密模块500用于接收者核查无误后进行全网广播交易单等待确认，其中，经过处理后的交易单上原始的明文信息将隐藏为无法识读的密文，以保证交易过程唯一可能被分析处理的隐私；区块链系统交易模块600用于验证层验证通过后，交易层将加密后的数额发送给接收者，接收者依据自己的私钥进行解密；在接受者核对自己的接收金额正确后，继续下一单的交易，接受者的接收值为下一单的输入值。

[0053] 具体而言，区块链交易系统可以分为八个步骤：

[0054] 步骤1：联盟参数生成/ParaGen：联盟成员依据分配得到的分块参数，达成共识联合生成系统交易的参数N，其中任意成员在未达到门限条件的情况下无法得知其陷门分解。

[0055] 步骤2：交易系统初始化/KeyGen：交易系统输入安全参数和上一步所生成的联盟参数，输出用于加解密运算的生成的公钥和私钥对(pk_i, sk_i)，同时输出用于验证的公钥pk_d，注意此公钥无配对私钥；

[0056] 步骤3:计算输入总值/Insum:计算交易总输入值,即上单交易与挖矿总收入(非初始区块链则无此项收入);若该交易单是作为新确认的区块,则该交易单将获得额外的比特币费用作为奖励,总收入为该部分明文与原密文相操作的总和;若该交易单不是新确认区块首单,则无额外收入,总收入即为上单交易传来的值;

[0057] 步骤4:平行加密/Parallel Encrypt:平行加密表示交易元数据经在交易层和验证层同时进行加密。系统在交易层使用接受者公钥分别加密传输数额,同时在验证层使用系统公钥加密相同数额的各个数额;在交易层所加密的数额将在验证层通过后发送至各个接收者账户,注意到在验证层发送的加密数额将进入验证层账户,注意到该账户无私钥,金额在验证后即丢弃;

[0058] 步骤5:范围承诺验证/Range Proof:在验证层验证隐藏后的数额是否为正值,以及输入输出总额是否相等;验证层分为两步,第一步通过承诺值在特定区间的证明方法证明隐藏的金额始终为正值;当该步骤为真时,验证进入下一步;

[0059] 步骤6:示性承诺验证/Balance:在验证层验证隐藏后的数额是否为正值后,系统验证层进入第二步,用过两个承诺值相等的证明方法证明隐藏的金额输入输出前后总数相等;当两个步骤都为真时,进入交易层的发送环节;该步骤调用

[0060] 步骤7:广播确认/Broadcast:即接收者核查无误后进行全网广播交易单等待确认;经过该方案处理后的交易单上原始的明文信息将隐藏为无法识读的密文,保证了交易过程唯一可能被分析处理的隐私。

[0061] 步骤8:解密/Decrypt:验证层验证通过后,交易层将加密后的数额发送给接收者,接收者依据自己的私钥进行解密;在接受者核对自己的接收金额正确后,继续下一单的交易;该接受者的接收值即为下一单的输入值。

[0062] 进一步地,定义$\Pi=(CoParaGen,MEnc,RangeVer,BalanceVer,Tx)$为多中心监管区块链交易隐私保护方案通用构造,依次表示联盟参数生成、加密元数据数额项、密文范围承诺证明、密文示性承诺证明和区块链交易。下面将对各个密码体制进行详细介绍。

[0063] 可选地,在本发明的一个实施例中,联盟成员秘密选取整数p_i和q_i,运行Π_1的rdmPara算法;计算模整数N,其中,运行Π_1的CoN算法;双素性测试,其中,联盟成员通过算法保证大整数N为两个素数的乘积,其中,运行Π_1的BipriTest算法;联盟参数及门限密钥生成,运行Π_1的KeyGen算法,得出联盟密钥。

[0064] 可以理解的是,(1)联盟成员秘密选取整数p_i和q_i,运行Π_1的rdmPara算法,分配参数;(2)计算模整数N,运行Π_1的CoN算法,$N=pq=(p_i+...+p_k)(q_i+...+q_k)$。(3)双素性测试,联盟成员通过算法保证大整数N为两个素数的乘积,运行Π_1的BipriTest算法,验证需通过。(4)联盟参数及门限密钥生成,运行Π_1的KeyGen算法,得出联盟密钥,MEnc(m,pk,c,sk):定义消息$m\in\{0,1\}^*$。

[0065] 具体而言,生成RSA门限密钥(Generation of Shared RSA Key)

[0066] 联盟成员联合生成联盟陷门参数N,却不知其分解,这样防止了单独或少量恶意成员对交易系统的攻击;只有在联盟成员达成共识后,才可以对得出大整数N的因式分解,进而解密加密的交易额密文。此功能非常适合多中心下的监管。

[0067] 定义1(门限RSA):定义$\Pi_1=(rdmPara,coN,BipriTest,KeyGen)$代表RSA门限密钥方案,其中rdmPara,coN,BipriTest和KeyGen分别为方案中的门限参数分配、联合生成大整

数、双素性测试和联盟参数生成。分别定义为：

[0068] rdmPara(1^k)：联盟成员秘密选取整数p_i和q_i，并进行长除范围测试。

[0069] coN(p_i,q_i)：计算模整数N，并进行长除范围测试。其中：$N=pq=(p_i+...+p_k)(q_i+...+q_k)$。

[0070] BipriTest(N)：双素性测试。联盟成员通过算法保证大整数N为两个素数的乘积。

[0071] KeyGen(N,d)：联盟参数及门限密钥生成。

[0072] 可选地，在本发明的一个实施例中，对交易元数据进行加密，其中，运行Π_2的PEnc算法；对交易元数据进行解密，其中，运行Π_2的PDec算法；对密文进行同态操作，其中，运行Π_3的POper算法。

[0073] 可以理解的是，对于交易数据加解密算法分为以下几个部分：

[0074] (1)对交易元数据进行加密。运行Π_2的PEnc算法，c=PEnc(pk,m)。

[0075] (2)对交易元数据进行解密。运行Π_2的PDec算法，m=PDec(sk,c)。

[0076] (3)对密文进行同态操作。运行Π_3的POper算法，$PDec(PEnc(m_i)\cdot PEnc(m_j)\ modn^2)=m_i+m_j\ modn$。

[0077] 具体而言，同态加解密体制(Homomorphic Cryptosystem)

[0078] 同态加密为公钥加密体制的一种，是基于数学难题的计算复杂性理论的密码学技术。该加密体制具备同态性，可以将明文操作隐蔽为密文操作，即对经过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保持不变。同态加密体制按运算方式分为加同态算法，乘同态算法与混合同态算法。同态加密方案通常包含四个(概率)多项式时间算法。

[0079] 定义2(同态加密)：定义$\Pi_2=(PKeyGen,PEnc,PDec,POper)$代表具备同态性的加密方案，其中PKeyGen，PEnc和PDec分别为方案中的密钥生成、加密、解密以及操作算法。分别定义为：

[0080] PKeyGen(1^k)：是一个概率多项式时间算法。它输入1^k，输出接收者的公私钥对(pk,sk)。

[0081] PEnc(pk,m)：是一个概率多项式时间算法。它输入公钥pk和消息$m\in M$，输出密文c=PEnc(pk,m)。

[0082] PDec(sk,c)：是一个确定多项式时间算法。它输入私钥sk和密文c，输出消息m或者符号⊥(表示c是一个无效密文)。

[0083] POper(c_i,c_j)：是一个概率多项式算法。它输入两个经过同态加密算法加密后的密文进行多项式操作，其算式满足同态操作的步骤，按结果满足$PDec(PEnc(m_i)\cdot PEnc(m_j)\ modn^2)=m_i+m_j\ modn$。

[0084] 并且，同态加密方案必须满足正确性和同态性。正确性即对于所有的$(pk,sk)\leftarrow PKeyGen(1^k)$和消息$m\in M$，满足PDec(sk,PEnc(pk,m))=m，同态性即满足$PDec_{sk}(PEnc_{pk}(m_i)\cdot PEnc_{pk}(m_j)\ modn^2)=m_i+m_j\ modn$。

[0085] 可选地，在本发明的一个实施例中，给定(m,m')，对明文秘密进行承诺计算，其中，运行Π_3的TCom算法；验证承诺值的有效性，其中，运行Π_3的TVer算法；对交易产生的不同密文值进行示性承诺验证是否含有相同元数据，其中，运行Π_3的TIndic算法。

[0086] 可以理解的是，BalanceVer(m,m',pk)：对承诺值进行数额一致性确认。具体包括：

[0087] (1)给定(m,m')，对明文秘密进行承诺计算。运行Π_3的TCom算法，TCom(pk,r,r',m,m')→(C,C')。

[0088] (2)验证承诺值的有效性。运行Π_3的TVer算法，TVer(pk,r,m,C)→1/0，若输出为1，说明生成的承诺值有效，否则输出0终止程序。

[0089] (3)对交易产生的不同密文值进行示性承诺验证是否含有相同元数据。运行Π_3的TIndic算法，TIndic(sk,C,C')→1/0，若输出为1，说明两个承诺值内包含相同的秘密元数据，否则输出0终止程序。

[0090] 另外，RangeVer(m,[a,b],pk)：对承诺值进行范围确认。具体包括：

[0091] (1)给定明文元数据m，对明文秘密进行承诺计算。运行Π_4的RCom算法，RCom(pk,r,m)→C。

[0092] (2)验证承诺值的有效性。运行Π_4的TVer算法，RVer(pk,r,m,C)→1/0，若输出为1，说明生成的承诺值有效，否则输出0终止程序，

[0093] (3)对交易产生的不同密文值进行范围承诺验证是否在特定区间。运行Π_4的交互式RInact算法，RInact(sk,[a,b],C)→1/0，若输出为1，说明承诺值内包含的秘密元数据在区间[a,b]之间，否则输出0终止程序。

[0094] 具体而言，示性承诺证明(Indicative Commitment Proof)

[0095] 示性承诺证明是一种特殊的承诺方案。传统承诺针对一个承诺值根据陷门信息进行运算，而陷门示性承诺针对两个承诺值进行操作，其示性特征仅允许拥有陷门信息的人能够判断出两个承诺里的秘密值是否相等，却不能打开承诺。即概念中的示性特征体现在方案的输出结果是判断结果1或0，而不是具体的承诺值。当且仅当拥有陷门密钥且承诺里的秘密值相等情形发生时，方案输出1，其他情形输出0。

[0096] 定义3(示性承诺证明)：定义Π_3=(TKeyGen,TCom,TVer,TIndic)代表示性承诺证明，其中TKeyGen,TCom,TVer和TIndic分别为方案中的密钥生成、承诺、验证和示性算法。

[0097] TKeyGen(1^k)：输入1^k，输出公开参数pk和陷门密钥sk。

[0098] TCom(pk,m)：输入公开参数pk和承诺值m，输出承诺C=TCom(pk,m)和验证承诺的参数(r,m)。

[0099] TVer(pk,C,r,m)：输入公开参数pk、承诺C和验证承诺的参数(r,m)，检查是否满足验证函数TVer(pk,C,r,m)。

[0100] TIndic(sk,C,C')：输入陷门密钥sk和两承诺C,C′，判断承诺C,C′中的承诺秘密值m,m′是否相同。若相同，此时输出1，否则输出0。

[0101] 范围承诺证明(Range Commitment Proof)

[0102] 范围承诺证明用于证明承诺值在一个特定的区间。承诺方案通常是指发送方向接收方发送一个秘密值，接收方不知道该秘密值，而随后发送方能够打开该秘密值，接收方进行验证。承诺方案包含两个阶段，承诺阶段和打开阶段(或称揭示阶段)。范围承诺证明方案在不打开承诺值的情况下，对密文值的大致范围进行证明，具备良好的隐秘性。

[0103] 定义4(范围承诺证明)：定义Π_4=(RKeyGen,RCom,RVer,RInact)代表范围承诺证明方案，其中RKeyGen,RCom、RVer和RInact分别为方案中的密钥生成、承诺、验证和交互算法。

[0104] RKeyGen(1^k)：输入1^k，输出公开参数pk和陷门密钥sk。

[0105] RCom(pk,m)：输入公开参数pk和承诺值m，输出承诺C＝RCom(pk,m)和验证承诺的参数(r,m)。

[0106] RVer(pk,C,r,m)：输入公开参数pk、承诺C和验证承诺的参数(r,m)，检查是否满足验证函数RVer(pk,C,r,m)。

[0107] RInact(a,b,sk,C)：输入陷门密钥sk和承诺值C，判断承诺C中的承诺秘密值m是否在区间[a,b]之中。若是，此时输出1，否则输出0。

[0108] 可选地，在本发明的一个实施例中，计算交易输入端总值，其中，运行Π_5的TIn算法；依据路径指向交易输出端，其中，运行Π_5的TOut算法；将交易单进行全网广播，其中，运行Π_5的TBroad算法；旷工依据共识机制确认交易单生成区块，其中，运行Π_5的BCfm算法。

[0109] 可以理解的是，Tx(TIn,TOut)：类区块链交易系统的通用操作层次：

[0110] (1)计算交易输入端总值。运行Π_5的TIn算法，Insum＝TIn(TOut$_{i-1}$,reward)；

[0111] (2)依据路径指向交易输出端。运行Π_5的TOut算法，$\overrightarrow{To}=TOut(TIn,address)$；

[0112] (3)将交易单进行全网广播。运行Π_5的TBroad算法，Comfirm＝TBroad(Tx)；

[0113] (4)旷工依据共识机制确认交易单生成区块。运行Π_5的BCfm算法，Block＝BCfm(Tx$_i$,Tx$_j$...)。

[0114] 具体而言，类区块链交易系统(Blockchain-based System)

[0115] 类区块链交易系统泛指使用区块链形式进行设计和发行代币的一类项目。该系统采用了中本聪架构，对数据进行可信化分布式存储和公开交易，并以代币为计量单位。该类交易系统由交易单、数据块和区块链层层架构为单向不可逆的链式结构。

[0116] 定义5(类区块链交易系统)：定义Π_5＝(TIn,TOut,TBroad,BCfm)代表类区块链交易系统方案，其中TIn,TOut,TBroad和BCfm分别为方案中的交易发送(交易单的输入端)，交易接收(交易单的输出端)，交易广播和区块确认。

[0117] TIn(TOut$_{i-1}$,reward)：系统输入端承接上一交易的输出，若为区块的首个交易则有挖矿的额外奖励reward，得到输入端的总和进行发送。

[0118] TOut(TIn,address)：系统的输入总和发送至接收端即为输出值，根据指定的公钥地址address进行交易指向。

[0119] TBroad(Tx)：系统对于已经产生的交易单进行全网广播，等待旷工进行确认。

[0120] BCfm(Tx$_i$,Tx$_j$...)：旷工对矿池的交易单进行确认，并依据共识机制将无数交易单进行打包，生成链接上一区块的新区块。

[0121] 在本发明的一个具体实施例中，如图3所示，本发明实施例给出了多中心监管区块链交易隐私保护方案的一种实例化具体构造，即在实例化每个模块的算法后，方案的步骤即可实现。该方案的具体实现介绍如下：

[0122] 1.工具模块的具体方案构造

[0123] 1.1具体的联盟参数生成算法/ParaGen，即本发明实施例给出DanBoneh提出的联合生成RSA门限密钥方案。

[0124] 1)联盟成员秘密选取整数p_i和q_i。

[0125] a)联盟成员秘密选取整数p_i

[0126] b)计算p＝p_i+...+p_k,,保证联盟整数和p不可被小于B_1的素数分解

[0127] c)联盟成员选取整数q_i并进行验证

[0128] 2)计算模整数N。

[0129] a)$N=pq=(p_i+...+p_k)(_i+...+q_k)$,生成参数N时不可额外信息

[0130] b)联盟成员可通过trial division算法来保证不被$[B_1,B_2]$间的素数分解因式

[0131] 3)双素性测试。联盟成员通过算法保证大整数N为两个素数的乘积。

[0132] 4)联盟参数生成。联盟成员联合生成用于交易系统中加密体制的参数N,但是任意成员无法得知其因式分解。

[0133] 1.2具体的同态加密算法/Homomorphic Cryptosystem,即本发明实施例给出Paillier加密方案。

[0134] Paillier加密体制提供了标准模型下的抗选择明文攻击安全,具备高效的加密解密效率以及加同态的特性,该体制加解密步骤如下:

[0135] PKeyGen:设p和q为大素数,g为系统生成元,令n=pq,计算$\lambda=\lambda(n)=1cm(p-1,q-1)$,其中公钥为(n,g),私钥为λ。

[0136] PEnc:$c=g^m\cdot r^n \bmod n^2$,其中r为任意选取。

[0137] $PDec:\ m=\dfrac{L(c^{\lambda} \bmod n^2)}{L(g^{\lambda} \bmod n^2)} \bmod n$。

[0138] $POper(c_i,c_j):Dec_{sk}(Enc_{pk}(m_1)\cdot Enc_{pk}(m_2) \bmod n^2)=m_1+m_2 \bmod n$。

[0139] 1.3具体的示性承诺方案/Indicative Commitment Proof,即本发明实施例给出非交互式示性承诺方案:

[0140] $PK\{x,r_1,r_2:E=E_1(x,r_1) \bmod n_1 \wedge F=E_2(x,r_2) \bmod n_2\}$。

[0141] 1).Alice随机选择$\omega\in\{1,...,2^{i+t}b-1\}$,$\eta_\alpha\in\{1,...,2^{l+t+s}n-1\}$,$\eta_\beta\in\{1,...,2^{l+t+s}n-1\}$;然后计算:

[0142] $W_\alpha=g_\alpha^{\omega}h_\alpha^{\eta_\alpha} \bmod n_\alpha,\ \ W_\beta=g_\beta^{\omega}h_\beta^{\eta_\beta} \bmod n_\beta$;

[0143] 2)Alice计算$u=H(W_\alpha||W_\beta)$;

[0144] 3)Alice计算:

[0145] $D=\omega+um$,$D_\alpha=\eta_\alpha+ur_\alpha$,$D_\beta=\eta_\beta+ur_\beta$

[0146] 并且发送(u,D,D_α,D_β)给验证层账户”;

[0147] 4)Bob检验是否u=u′,其中

[0148] $u'=H(g_\alpha^{D}h_\alpha^{D_\alpha}E^{-u} \bmod n_\alpha \| g_\beta^{D}h_\beta^{D_\beta}F^{-u} \bmod n_\beta)$;

[0149] 如果该部分步骤验证成功,则两个承诺值包含相同秘密值。

[0150] 1.4具体的范围承诺方案/Range Commitment Proof,即本发明实施例给出Wu在2004的范围承诺证明协议

[0151] $PK\{x,r:E=E(x,r) \bmod n \wedge x\in[a,b]\}$。

[0152] 1)Alice设置$v=\alpha^2y+\omega>2^{t+1+s+T}$,其中任意选择$\alpha\neq0$,$0<\omega\leqslant2^{s+T}$;设置$r_3-r\alpha^2+r_1\alpha+r_2\in[-2^sn+1,...,2^sn-1]$,其中任意选择$r_1,r_2,r_3\in[-2^sn+1,...,2^sn-1]$;然后计算:

[0153] $E_1=g^{m_i-a}h^{r}=g^{y}h^{r} \bmod n$,

[0154] $E_2=E_1^{\alpha}h^{r_1} \bmod n, E_3=E_2^{\alpha}h^{r_2} \bmod n$,

[0155] $F=g^{\omega}h^{r_3} \bmod n$,

[0156] $V = g^{v} / E_2 = g^{\omega} h^{-r\alpha^2 - r_1\alpha - r_2} \bmod n$，

[0157] Alice发送(V,E_2,E_3,F)给接收者；

[0158] 2)接收者计算：

[0159] $E_1 = E_0(m_i, r) / g^{a} = g^{y} h^{r} \bmod n$，

[0160] $V = g^{v} / E_3 = g^{\omega} h^{-r\alpha^2 - r_1\alpha - r_2} \bmod n$，

[0161] 3)Alice和接收者各自计算：

[0162] $PK1\{\alpha, r_1, r_2 : E_2 = E_1^{\alpha} h^{r_1} \bmod n \wedge E_3 = E_2^{\alpha} h^{r_2} \bmod n\}$，

[0163] $PK2\{\omega, r^* : F = g^{\omega} h^{r_3} \bmod n \wedge V = g^{\omega} h^{r^*} \bmod n\}$，

[0164] $PK3\{\omega, r_3 : F = g^{\omega} h^{r_3} \bmod n \wedge \omega \in [-2^{t+l+s+T}, 2^{t+l+s+T}]\}$，

[0165] 其中$r^* = -r\alpha^2 - r_1\alpha - r_2$；

[0166] 4)接收者验证PK1,PK2,PK3的正确性，以及是否满足$v > 2^{t+1+s+T}$，若满足则接收者可以确信x>a；同理可证得x<b。

[0167] 1.5具体的区块链交易方案/Blockchain-based System，即采用比特币交易系统作为通用构造的实例载体。

[0168] 2、具体方案实施步骤如下：

[0169] 如图4所示，本发明实施例可以基于各个模块的实例化算法，以及系统的双层层级结构，最终的实例化方案实施步骤如下：

[0170] 步骤1：联盟参数生成/ParaGen：联盟成员依据分配得到的分块参数，达成共识联合生成系统交易的参数N，其中任意成员在未达到门限条件的情况下无法得知其陷门分解。首先联盟成员秘密选取整数p_i，并计算$p = p_i + \ldots + p_k$，保证联盟整数和p不可被小于范围上限B_1的素数分解。同理，联盟成员选取整数q_i并进行验证。然后，成员选取整数完毕，计算模整数$N = pq = (p_i + \ldots + p_k)(q_i + \ldots + q_k)$，在此期间，生成参数N将不会泄露额外信息。为保证参数在指定区间内，联盟成员可通过trial division算法来保证不被$[B_1, B_2]$间的素数分解因式。同理，为保证参数为两个素数的乘积，联盟成员进行双素性测试，保证其乘积性质。最后，在保证参数N正确可用的条件下，联盟成员联合生成用于交易系统中加密体制的陷门参数d，并将两门参数N传入系统，用于下面步骤的加密。

[0171] 步骤2：交易系统初始化/KeyGen：输入安全参数，输出用于加解密运算以及验证的参数。在交易层，对于每个不同的接收者i，系统生成给每个接收者生成两个大素数p_i和q_i。接收者私钥为$sk_i = \lambda_i$，公钥为$pk_i = (n_i, g_i)$，其中$n_i = p_i q_i$；

[0172] 同时在验证层，系统输出用于验证的账户的公钥$pk_d = (n_d, g_d)$，注意到此公钥无配对私钥。即该系统账户不能对收到的金额进行操作；系统生成参数$V_\alpha(g_\alpha, h_\alpha)$和$V_\beta(g_\beta, h_\beta)$用于验证。注意到，由于验证层账户和承诺值证明同处于验证层，且其参数都是由系统生成，方案设定$g_\beta = g_d$以及$n_\beta = n_d^2$，来确保操作后的密文可以成为承诺数；

[0173] 步骤3：计算总输入值/Insum：计算交易总输入值，即上单交易与挖矿总收入。若该交易单是作为新确认的区块，则该交易单将获得额外的数额费用作为奖励，总收入为该部分明文与原密文相操作的数目总和，表示为$m = m_{in} + 12.5 = \mathrm{Dec}_{pk_{Alice}}(c_{in} \otimes 12.5)$；若该交易单不是新确认区块首单，则无额外收入，总收入即为上单交易传来的值，表示为

$m = m_{in} = \mathrm{Dec}_{pk_{Alice}}(c_{in})$；

[0174] 步骤4：平行加密项/ParallelEncrypt：在交易层，方案使用不同接收者的公钥$pk_1, pk_2, \ldots, pk_i$使用Paillier加密体制来加密发送的明文数额$m_1, m_2, \ldots, m_i$为$c_1, c_2, \ldots, c_i$，表示为：$c_i = \mathrm{Enc}_{pk_i}(m_i) = g_i^{m_i} r_i^{n_i} \bmod n_i^2$。同时，在验证层，方案使用系统的同一个公钥$pk_d$将交易层中每一个发送的数额$m_1, m_2, \ldots, m_i$进行加密，表示为：$c_{id} = \mathrm{Enc}_{pk_d}(m_i) = g_d^{m_i} r_d^{n_d} \bmod n_d^2$。其中方案设定随机数$r_d = h_\beta$；两层的共同点是加密了相同的交易数额$m_i$，不同之处在于交易层使用来自接收者的不同的公钥$pk_i$，验证层使用了来自系统的相同公钥$pk_d$用于实现Paillier体制的加同态特性。其内在相同的数额m_i保证了接收者在验证后得到值的正确性；

[0175] 步骤5：范围承诺验证/Range Proof：系统在验证层验证隐藏后的数额是否为正值。整个验证层分为两步，第一步通过承诺值在特定区间的证明方法证明隐藏的金额始终为正值。方案范围承诺证明来保证被加密的数额m_i为正值，发送者Alice对于不同的接收者i，分别做出承诺$E_{i0}(m_i, r) = g^{m_i} h_r \bmod n$，为了简化，使用$E_0, E_1, E_2, E_3, F, V$来代替$E_{i0}, E_{i1}, E_{i2}, E_{i3}, F_i, V_i$。

[0176] 1) Alice设置$v = \alpha^2 y + \omega > 2^{t+1+s+T}$，其中任意选择$\alpha \neq 0, 0 < \omega \leqslant 2^{s+T}$；设置$r_3 - r\alpha^2 + r_1\alpha + r_2 \in [-2^s n + 1, \ldots, 2^s n - 1]$，其中任意选择$r_1, r_2, r_3 \in [-2^s n + 1, \ldots, 2^s n - 1]$；并计算：$E_1 = g^{m_i - a} h^r = g^y h^r \bmod n$； $E_2 = E_1^\alpha h^{r_1} \bmod n, E_3 = E_2^\alpha h^{r_2} \bmod n$；

[0177] $F = g^\omega h^{r_3} \bmod n$； $V = g^v / E_2 = g^\omega h^{-r\alpha^2 - r_1\alpha - r_2} \bmod n$；

[0178] Alice发送(V,E_2,E_3,F)给接收者；

[0179] 2) 接收者计算：$E_1 = E_0(m_i, r) / g^a = g^y h^r \bmod n$，

[0180] $V = g^v / E_3 = g^\omega h^{-r\alpha^2 - r_1\alpha - r_2} \bmod n$，

[0181] 3) Alice和接收者各自计算：

[0182] $PK1\{\alpha, r_1, r_2 : E_2 = E_1^\alpha h^{r_1} \bmod n \wedge E_3 = E_2^\alpha h^{r_2} \bmod n\}$，

[0183] $PK2\{\omega, r^* : F = g^\omega h^{r_3} \bmod n \wedge V = g^\omega h^{r^*} \bmod n\}$，

[0184] $PK3\{\omega, r_3 : F = g^\omega h^{r_3} \bmod n \wedge \omega \in [-2^{t+l+s+T}, 2^{t+l+s+T}]\}$，，

[0185] 其中$r^* = -r\alpha^2 - r_1\alpha - r_2$；

[0186] 4) 接收者验证PK1,PK2,PK3的正确性，以及是否满足$v > 2^{t+1+s+T}$，若满足则接收者可以确信$x > a$；

[0187] 5) 对于每个接收者m_i，方案重复步骤1-4即可证明$m_i > 0$ ($i = \{1, 2, \ldots, i\}$)。

[0188] 该证明部分将对每个接收者的m_i重复执行i次，如果其中有任意一次失败，交易失败；如果全部成功，系统返回1，并继续下个步骤的验证。

[0189] 步骤6：示性承诺验证/Balance：系统在验证层验证隐藏后的数额输入输出总额是否相等。验证层分为两步，该步为第二步，用过两个承诺值相等的证明方法证明隐藏的金额输入输出前后总数相等。方案使用证明两个承诺值相等的证明来保证交易输出输入前后一致，即$m = m_1 + m_2 + \ldots + m_i = \sum m_i$。现在，Alice做出两个承诺如下：

[0190] $E = E_\alpha(m, r_\alpha) = g_\alpha^m h_\alpha^{r_\alpha}, F = E_\beta(\sum m_i, r_\beta) = g_\beta^m h_\beta^{r_\beta}$。

[0191] 其中$r_\alpha \in \{-2^s n+1,\ldots,2^s n-1\}$，$r_\beta = n_d \in \{-2^s n+1,\ldots,2^s n-1\}$；如果收到相同数额的“哑巴账户”想验证其收到的密文中所含的明文数额是否与Alice发送的值相等，那么它需要进行如下两个步骤：

[0192] A)隐藏在承诺值E和F中的秘密值相等$m = \Sigma m_i$；

[0193] B)操作后的密文$H = \prod c_{id}$等于其中一个承诺F。

[0194] 为了实现上述步骤1)，我们进行如下算法：

[0195] 1).Alice随机选择$\omega \in \{1,\ldots,2^{i+t}b-1\}$，$\eta_\alpha \in \{1,\ldots,2^{l+t+s}n-1\}$，$\eta_\beta \in \{1,\ldots,2^{l+t+s}n-1\}$；然后计算：$W_\alpha = g_\alpha^{\omega} h_\alpha^{\eta_\alpha} \bmod n_\alpha$，$W_\beta = g_\beta^{\omega} h_\beta^{\eta_\beta} \bmod n_\beta$；

[0196] 2).Alice计算$u = H(W_\alpha || W_\beta)$；

[0197] 3).Alice计算：$D = \omega + um$，$D_\alpha = \eta_\alpha + ur_\alpha$，$D_\beta = \eta_\beta + ur_\beta$；

[0198] 并且发送$(u, D, D_\alpha, D_\beta)$给验证层账户；

[0199] 4验证层账户检验是否$u = u'$，其中

[0200] $u' = H(g_\alpha^D h_\alpha^{D_\alpha} E^{-u} \bmod n_\alpha \| g_\beta^D h_\beta^{D_\beta} F^{-u} \bmod n_\beta)$.。

[0201] 如果该部分步骤验证成功，继续进行下部分步骤证明：

[0202] a)验证层账户对收到的密文进行计算：

[0203] $H = \prod c_{id} = c_1 c_2' \ldots c_i' = g_d^{m_1'+m_2'+\ldots+m_i'} r_d^{n_d} = g_d^{\sum m_i'} r_d^{n_d} \bmod n_d^2$。

[0204] b).从上面可以看出，我们可以在加密过程中任意选取$r_d = h_\beta$，在验证过程中任意选取$r_\beta = n_d$；并且在系统初始化过程中，我们设置$n_\beta = n_d^2$以及$g_d = g_\beta$，是故：

[0205] $H = g_d^{\sum m_i'} r_d^{n_d} \bmod n_d^2$

[0206] $F = g_\beta^{\sum m_i} h_\beta^{r_\beta} \bmod n_\beta$

[0207] $= g_d^{\sum m_i} r_d^{n_d} \bmod n_d^2$

[0208] c).检查H是否等于F，如果否，交易失败，如果是返回1，并进行下一步。

[0209] 综上验证，当两个部分的步骤都为真时，进入交易层的发送环节；

[0210] 步骤7：广播确认/Broadcast：验证层核查无误后进行全网广播交易单等待确认。经过该方案处理后的交易单上原始的明文信息将隐藏为无法识读的密文，保证了交易过程唯一可能被分析处理的隐私。我们可以将此交易单标志为T_{Alice}，该过程同样适用于任意其他单交易。

[0211] 步骤8：解密项/Dcrypt：广播确认通过后，接收者收到加密后的数额c_i，接收者依据自己的私钥sk_i进行解密：$m_i = \dfrac{L(c_i^{\lambda_i} \bmod n_i^2)}{L(g_i^{\lambda_i} \bmod n_i^2)} \bmod n_i$，

[0212] 其中$L(x) = \dfrac{x-1}{n}$，$x \in S_n = \{u < n^2 \mid x = 1 \bmod n\}$；在接受者核对自己的接收金额正确后，可继续下一单的交易。该接受者的接收值即为下一单的输入值。值得注意的是，当交易完成后，验证层账户中的密文数额将被丢弃，其作用仅作为桥梁使验证层的值与发送的值产生联系。

[0213] 此外，本发明实施例可以结合密码学门限体制、同态加密技术以及承诺证明机制，

解决现有的类区块链交易系统中在多方管控下存在的交易隐私保护问题，本发明实施例的系统10包括多中心区块链交易隐私保护系统的系统架构及定义；多中心区块链交易隐私保护系统的通用方案构造；多中心区块链交易隐私保护系统的具体方案构造。其中，所涉及的多中心区块链交易隐私系统由五个密码学模块组成，具体交易流程分为两个层级，八个步骤。涉及的密码学工具包括门限生成体制、同态加解密体制、承诺证明体制、零知识证明体制以及区块链交易系统。具有以下功能：

[0214] (1)实现了多参与方联合管控下对陷门参数的隐私保护。联盟方在取得共识达到门限条件后生成系统启动的参数，但是任意一方无法得知参数的分解因子。

[0215] (2)实现对交易元数据的隐私保护。在交易过程中将交易元数据中的明文数额加密为密文进行交易，并可以对其进行密文运算。

[0216] (3)实现对交易密文的正确性验证。系统能够保证在交易中隐藏的交易值始终为正值，且交易的数额前后总数一致。

[0217] 综上，本发明实施例系统10具有以下特点：

[0218] (1)本发明实施例中多中心监管下区块链交易隐私保护体制的设计是一种通用化构造，任何满足本发明要求的基础密码学工具都可组合实现具备联合管控和隐私保护功能的类区块链交易系统具体方案。

[0219] (2)本发明实施例给出了一个具体的多中心监管下区块链隐私增强方案的构造步骤及构造实例，对于本领域普通技术人员来讲，可以根据自己所期望的性能及安全需求，仿照这一实例构造其他的区块链交易方案。

[0220] (3)构造方案通过门限加解密体制实现了联合管控下的对于陷门参数的隐私保护，通过同态加密体制实现了对数额的加密解密运算保证传输过程中的数额隐私，同时通过范围承诺证明与示性承诺证明保证了交易中隐藏数额始终为正且输入输出总额相等的要求。

[0221] 根据本发明实施例提出的多中心区块链交易隐私保护系统，可以利用门限加解密体制实现对于多参与方联合管控中对于生成陷门参数的隐私保护，利用同态加密体制实现对数额的加解密运算增强传输过程中的数额隐私，利用范围承诺证明与示性承诺证明保证交易过程中确保了隐藏的交易值始终为正值且交易数额前后总数一致，从而可以实现多方联合管控下对于陷门参数和交易过程中对于交易元数据的隐私保护，有效增强多中心类区块链系统交易过程中的明文数额安全。

[0222] 其次参照附图描述根据本发明实施例提出的多中心区块链交易隐私保护方法的流程图。

[0223] 如图5所示，该多中心区块链交易隐私保护方法包括以下步骤：

[0224] 在步骤S501中，联盟成员依据分配得到的分块参数，达成共识联合生成系统交易的参数N，其中任意成员在未达到门限条件的情况下无法得知其陷门分解。

[0225] 在步骤S502中，交易系统输入安全参数和联盟参数，输出用于加解密运算的生成的公钥和私钥对(pk_i,sk_i)，同时输出用于验证的公钥pk_d，公钥无配对私钥。

[0226] 在步骤S503中，计算交易总输入值，其中，若交易单是作为新确认的区块，则交易单将获得额外的比特币费用作为奖励，总输入值为该部分明文与原密文相操作的总和；若交易单不是新确认区块首单，则无额外收入，总输入值为上单交易传来的值。

[0227] 在步骤S504中，平行加密表示交易元数据经在交易层和验证层同时进行加密，其中，系统在交易层使用接受者公钥分别加密传输数额，同时在验证层使用系统公钥加密相同数额的各个数额；在交易层所加密的数额将在验证层通过后发送至各个接收者账户，注意到在验证层发送的加密数额将进入验证层账户，注意到该账户无私钥，金额在验证后丢弃。

[0228] 在步骤S505中，在验证层验证隐藏后的数额是否为正值，以及输入输出总额是否相等，其中，验证层分为两步，第一步通过承诺值在特定区间的证明方法证明隐藏的金额始终为正值；当为真时，在验证层验证隐藏后的数额是否为正值后，系统验证层进入第二步，用过两个承诺值相等的证明方法证明隐藏的金额输入输出前后总数相等；当步骤都为真时，进入交易层的发送环节。

[0229] 在步骤S506中，接收者核查无误后进行全网广播交易单等待确认，其中，经过处理后的交易单上原始的明文信息将隐藏为无法识读的密文，以保证交易过程唯一可能被分析处理的隐私。

[0230] 在步骤S507中，验证层验证通过后，交易层将加密后的数额发送给接收者，接收者依据自己的私钥进行解密；在接受者核对自己的接收金额正确后，继续下一单的交易，接受者的接收值为下一单的输入值。

[0231] 进一步地，在本发明的一个实施例中，令$\Pi_1=(rdmPara,coN,BipriTest,KeyGen)$代表RSA门限密钥方案，其中rdmPara、coN、BipriTest和KeyGen分别为RSA门限密钥方案中的门限参数分配、联合生成模整数、双素性测试和联盟参数生成；令$\Pi_2=(PKeyGen,PEnc,PDec)$代表同态加解密方案，其中PKeyGen、PEnc和PDec分别为同态加解密方案中的密钥生成、加密和解密算法；令$\Pi_3=(TKeyGen,TCom,TVer,TIndic)$代表示性承诺证明方案，其中TKeyGen、TCom、TVer和TIndic分别为示性承诺证明方案中的密钥生成、承诺、验证和示性算法；令$\Pi_4=(RKeyGen,RCom,RVer,RInact)$代表范围承诺证明方案，其中RKeyGen、RCom、RVer和RInact分别为方案中的密钥生成、承诺、验证和交互算法；令$\Pi_5=(TIn,TOut,TBroad,BCfm)$代表类区块链交易系统方案，其中TIn、TOut、TBroad和BCfm分别为类区块链交易系统方案中的交易发送、交易接收、交易广播和区块确认。

[0232] 进一步地，在本发明的一个实施例中，区块链交易系统包括交易层和验证层，其中，交易层用于对执行区块链交易系统的交易步骤，包括交易单生成，输入输出，广播确认，并且经过加密的元数据取代原始明文，显示在交易单之中；验证层用于验证加密后的数据是否符合数值一致性以及存在于特定范围。

[0233] 需要说明的是，前述对多中心区块链交易隐私保护装置实施例的解释说明也适用于该实施例的多中心区块链交易隐私保护方法，此处不再赘述。

[0234] 根据本发明实施例提出的多中心区块链交易隐私保护方法，可以利用门限加解密体制实现对于多参与方联合管控中对于生成陷门参数的隐私保护，利用同态加密体制实现对数额的加解密运算增强传输过程中的数额隐私，利用范围承诺证明与示性承诺证明保证交易过程中确保了隐藏的交易值始终为正值且交易数额前后总数一致，从而可以实现多方联合管控下对于陷门参数和交易过程中对于交易元数据的隐私保护，有效增强多中心类区块链系统交易过程中的明文数额安全。

[0235] 在本发明的描述中，需要理解的是，术语“中心”、“纵向”、“横向”、“长度”、“宽度”、

“厚度”、“上”、“下”、“前”、“后”、“左”、“右”、“竖直”、“水平”、“顶”、“底”“内”、“外”、“顺时针”、“逆时针”、“轴向”、“径向”、“周向”等指示的方位或位置关系为基于附图所示的方位或位置关系，仅是为了便于描述本发明和简化描述，而不是指示或暗示所指的装置或元件必须具有特定的方位、以特定的方位构造和操作，因此不能理解为对本发明的限制。

[0236] 此外，术语“第一”、“第二”仅用于描述目的，而不能理解为指示或暗示相对重要性或者隐含指明所指示的技术特征的数量。由此，限定有“第一”、“第二”的特征可以明示或者隐含地包括至少一个该特征。在本发明的描述中，“多个”的含义是至少两个，例如两个，三个等，除非另有明确具体的限定。

[0237] 在本发明中，除非另有明确的规定和限定，术语“安装”、“相连”、“连接”、“固定”等术语应做广义理解，例如，可以是固定连接，也可以是可拆卸连接，或成一体；可以是机械连接，也可以是电连接；可以是直接相连，也可以通过中间媒介间接相连，可以是两个元件内部的连通或两个元件的相互作用关系，除非另有明确的限定。对于本领域的普通技术人员而言，可以根据具体情况理解上述术语在本发明中的具体含义。

[0238] 在本发明中，除非另有明确的规定和限定，第一特征在第二特征“上”或“下”可以是第一和第二特征直接接触，或第一和第二特征通过中间媒介间接接触。而且，第一特征在第二特征“之上”、“上方”和“上面”可是第一特征在第二特征正上方或斜上方，或仅仅表示第一特征水平高度高于第二特征。第一特征在第二特征“之下”、“下方”和“下面”可以是第一特征在第二特征正下方或斜下方，或仅仅表示第一特征水平高度小于第二特征。

[0239] 在本说明书的描述中，参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本发明的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不必须针对的是相同的实施例或示例。而且，描述的具体特征、结构、材料或者特点可以在任一个或多个实施例或示例中以合适的方式结合。此外，在不相互矛盾的情况下，本领域的技术人员可以将本说明书中描述的不同实施例或示例以及不同实施例或示例的特征进行结合和组合。

[0240] 尽管上面已经示出和描述了本发明的实施例，可以理解的是，上述实施例是示例性的，不能理解为对本发明的限制，本领域的普通技术人员在本发明的范围内可以对上述实施例进行变化、修改、替换和变型。

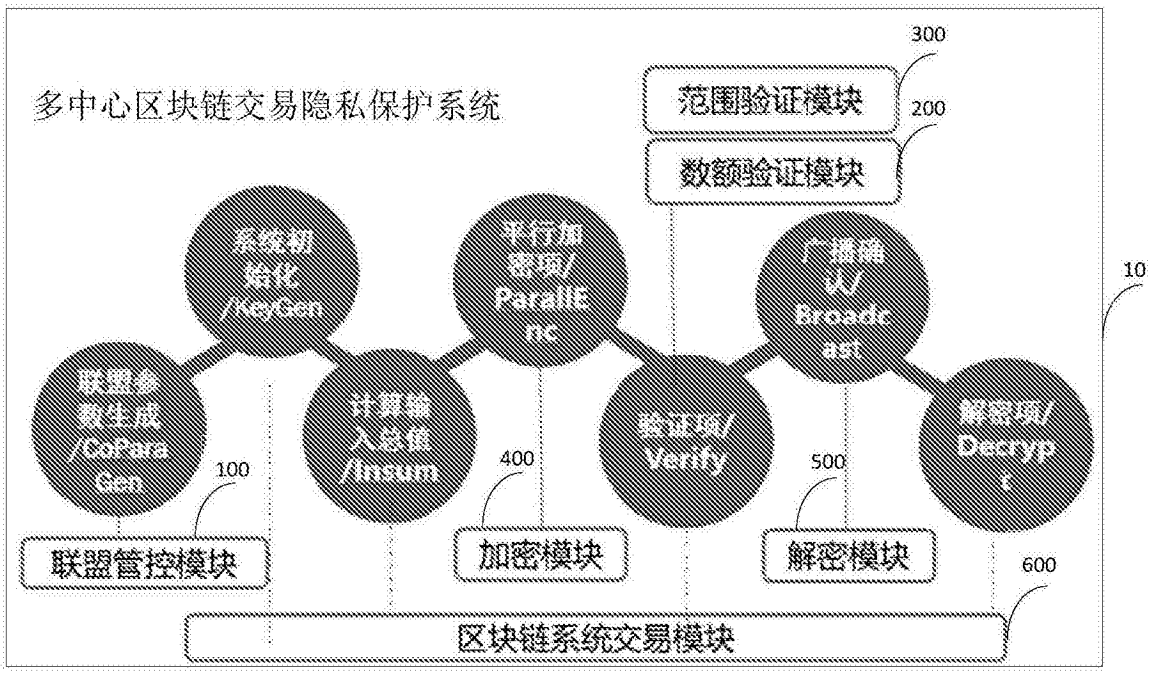

多中心区块链交易隐私保护系统
范围验证模块
300
数额验证模块
200
系统初始化/KeyGen
平行加密项/ParallEnc
广播确认/Broadcast
联盟参数生成/CoParaGen
计算输入总值/Insum
验证项/Verify
解密项/Decrypt
10
100
400
500
联盟管控模块
加密模块
解密模块
600
区块链系统交易模块

图1


多中心监管区块链交易隐私增强系统通用构造
方案模块
密码学工具
联盟管控模块
门限密码体制
加解密模块
同态密码体制
范围验证模块
范围承诺证明
数额验证模块
示性承诺证明
区块链交易模块
类比特币系统

图2

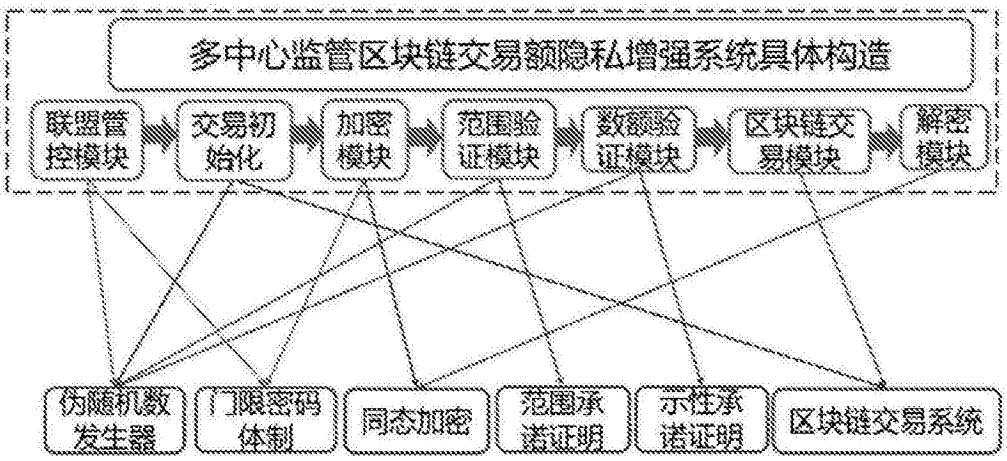

多中心监管区块链交易额隐私增强系统具体构造
联盟管控模块
交易初始化
加密模块
范围验证模块
数额验证模块
区块链交易模块
解密模块
伪随机数发生器
门限密码体制
同态加密
范围承诺证明
示性承诺证明
区块链交易系统

图3

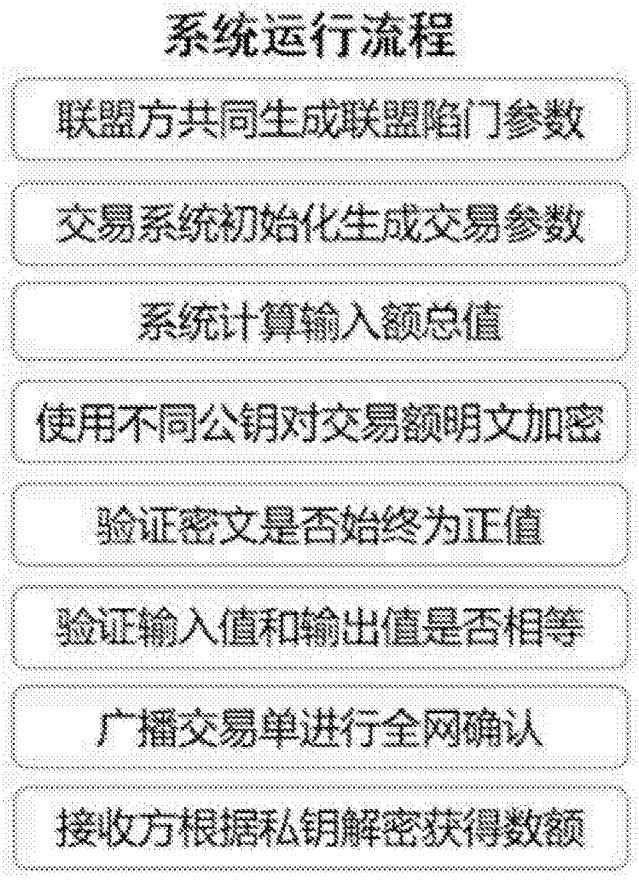

系统运行流程
联盟方共同生成联盟陷门参数
交易系统初始化生成交易参数
系统计算输入额总值
使用不同公钥对交易额明文加密
验证密文是否始终为正值
验证输入值和输出值是否相等
广播交易单进行全网确认
接收方根据私钥解密获得数额

图4

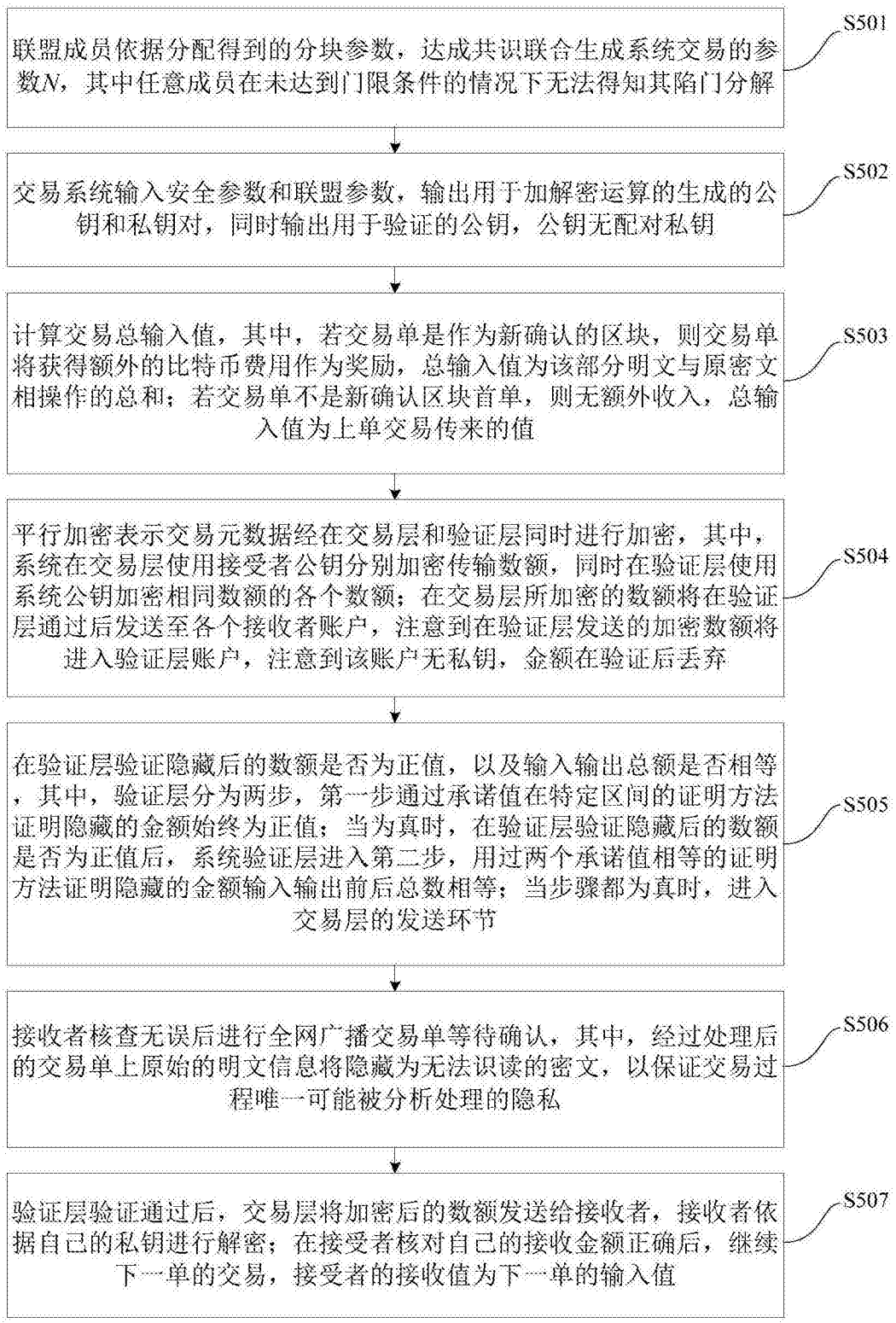

联盟成员依据分配得到的分块参数，达成共识联合生成系统交易的参数N，其中任意成员在未达到门限条件的情况下无法得知其陷门分解
S501
交易系统输入安全参数和联盟参数，输出用于加解密运算的生成的公钥和私钥对，同时输出用于验证的公钥，公钥无配对私钥
S502
计算交易总输入值，其中，若交易单是作为新确认的区块，则交易单将获得额外的比特币费用作为奖励，总输入值为该部分明文与原密文相操作的总和；若交易单不是新确认区块首单，则无额外收入，总输入值为上单交易传来的值
S503
平行加密表示交易元数据经在交易层和验证层同时进行加密，其中，系统在交易层使用接受者公钥分别加密传输数额，同时在验证层使用系统公钥加密相同数额的各个数额；在交易层所加密的数额将在验证层通过后发送至各个接收者账户，注意到在验证层发送的加密数额将进入验证层账户，注意到该账户无私钥，金额在验证后丢弃
S504
在验证层验证隐藏后的数额是否为正值，以及输入输出总额是否相等，其中，验证层分为两步，第一步通过承诺值在特定区间的证明方法证明隐藏的金额始终为正值；当为真时，在验证层验证隐藏后的数额是否为正值后，系统验证层进入第二步，用过两个承诺值相等的证明方法证明隐藏的金额输入输出前后总数相等；当步骤都为真时，进入交易层的发送环节
S505
接收者核查无误后进行全网广播交易单等待确认，其中，经过处理后的交易单上原始的明文信息将隐藏为无法识读的密文，以保证交易过程唯一可能被分析处理的隐私
S506
验证层验证通过后，交易层将加密后的数额发送给接收者，接收者依据自己的私钥进行解密；在接受者核对自己的接收金额正确后，继续下一单的交易，接受者的接收值为下一单的输入值
S507

图5