(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 106549749 A
(43)申请公布日 2017.03.29

(21)申请号 201611107715.2

(22)申请日 2016.12.06

(71)申请人 杭州趣链科技有限公司
地址 310012 浙江省杭州市西湖区文三路199号13幢南楼501室

(72)发明人 梁秀波 李启雷 尹可挺 李伟 邱炜伟

(74)专利代理机构 杭州求是专利事务所有限公司 33200
代理人 刘静 邱启旺

(51)Int.Cl.
H04L 9/00(2006.01)

权利要求书2页 说明书4页 附图2页

(54)发明名称

一种基于加法同态加密的区块链隐私保护方法

(57)摘要

本发明公开了一种基于加法同态加密的区块链隐私保护方法。在一个区块链网络上，交易发送者发起交易，经全网节点验证，最后交易接收者收到交易金额并完成交易，交易加密方法的步骤具体为：同态密钥生成；将发送者的账户可见余额拆分为交易金额和剩余余额；用全网同态公钥加密交易金额和剩余余额，记为密文X1和X2；用接收者的公钥加密交易金额，得到密文Y1；发送者发起交易，交易内容包含X1、X2和Y1三个字段；全网节点验证交易信息，维护公共账本；更新接收者的可见余额。本发明实现了利用加法同态加密技术隐藏区块链上的交易金额和用户余额的功能，解决了传统的区块链交易中暴露了真实的转账金额的问题，实现了区块链上的隐私保护功能。

CN 106549749 A

1.一种基于加法同态加密的区块链隐私保护方法，其特征在于，包括如下步骤：

1)同态密钥生成，由一个可信任的第三方机构生成一对同态密钥作为全网的同态密钥，公开其同态公钥，私钥保存在第三方机构中。用户的账户余额有两种存在形式：一种是用全网同态公钥加密后存储在区块链公共账本上的真实余额，一种是以明文形式存储在用户本地只供用户自己可见的可见余额。

2)拆分交易发送方的账户可见余额，发送方须将自己的可见余额值拆分为需要转账的交易金额和剩余余额，需要转账的交易金额不得大于可见余额，且任何金额不得小于零；

3)用全网同态公钥加密交易金额和剩余余额，同态加密后的密文分别记为X1和X2，此操作采用加法同态加密算法；

4)用接收方的公钥加密步骤2)中的交易金额，加密后的密文记为Y1；

5)发送者发起交易，交易内容包含步骤3)中的密文X1、密文X2以及步骤4)中的密文Y1三个字段，发送者将交易信息发送至全网节点进行验证；

6)交易确认，区块链全网的验证节点进行交易信息的验证，并维护公共账本。由于公共账本上以同态加密密文形式存储全网账户的真实余额，验证节点进行交易验证时应当确认，①密文X1和密文X2对应的真实金额不小于零；②密文X1和密文X2的同态加法和与发送者的公共账本余额一致；交易信息验证成功后，验证节点对公共账本上的用户真实余额进行修改。

7)更新接收者的可见余额：接收者上线接收交易信息，利用自己的私钥解密交易信息中的密文Y1得到交易金额明文，直接更新自己的可见余额。或者，接收者向可信的第三方机构申请查询真实余额，然后更新自己的可见余额。

2.如权利要求1所述的一种基于加法同态加密的区块链隐私保护方法，其特征在于，所述的步骤1)中，区块链网络创建之初，由一个可信的第三方利用加法同态加密算法生成的一对同态密钥，这对同态密钥将作为全网的同态密钥，区块链上所有用户的余额均由同态公钥加密后保存在公共账本上，公共账本上存储所有账户的真实余额的密文，全网节点只能维护公共账本的密文而无法解密；私钥保存于一个可信的第三方机构中，只有提供了用户本身的签名后，才可以申请查询用户自己的账本余额。

3.如权利要求1所述的一种基于加法同态加密的区块链隐私保护方法，其特征在于，所述的步骤2)中，用户保存自己的可见余额，可见余额存储在用户本地，其他人不可见；用户的可见余额应当与其真实余额数值相等，否则将无法发起有效的交易；当用户的可见余额数值上不等于其真实余额时，用户可以请求区块链的可信的第三方机构申请余额更新。

4.如权利要求1所述的一种基于加法同态加密的区块链隐私保护方法，其特征在于，所述步骤3)中，用户发起交易时将自己的可见余额拆分为交易金额和剩下余额，并用全网同态公钥对交易金额和剩下余额进行同态加密，密文将作为交易的字段发送至全网，使得区块链上始终出现的都是用同态公钥加密后的金额数值，其它节点无法得知其真实数值。

5.如权利要求1所述的一种基于加法同态加密的区块链隐私保护方法，其特征在于，所述的步骤4)中，发起方用接收方的公钥对交易金额进行加密后作为交易字段随交易一起发出，接收方可以解密该字段得知交易金额，其目的在于使步骤7)中接收者上线更新自己的可见余额时更加方便，不必每次都申请查账操作。若接收者在交易完成后发现自己的可见余额与真实余额数值上不相等，即被发送者告知不正确的交易金额，将导致接收者的下次

交易无法完成，接收者可以选择向可信的第三方机构申请查询真实余额，然后更新自己的可见余额。

一种基于加法同态加密的区块链隐私保护方法

技术领域

[0001] 本发明涉及去中心化的区块链账本技术和加法同态加密方法，尤其涉及一种将非对称的加密同态加密技术合理集成到区块链交易中的方法。

背景技术

[0002] 区块链技术，区块链是一种新型去中心化协议，能安全地存储数字货币交易或其他数据，信息不可伪造和篡改，区块链上的交易确认由区块链上的所有节点共同完成，由共识算法保证其一致性，区块链上维护一个公共的账本，用于存储区块链网络上所有用户的余额，公共账本位于存储区块上任何节点可见，从而保证其不可伪造和篡改。

[0003] 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，同时，用户在发起交易时，交易信息中的交易金额也是完全公开的，区块链上的验证节点会对用户的账户余额和交易金额进行数学判断，从而验证交易的合法性。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，用户的账户隐私完暴露在区块链的所有节点上。

[0004] 很明显，没有人希望自己的账户信息完全暴露在所有人面前，因此，我们引入加法同态加密技术来有效的保证区块链上用户的隐私。

[0005] 加法同态加密是针对数值的一种非对称加密，对于数值A、B、C加密后密文分别为E(A)、E(B)、E(C)，有特性：

[0006] 若有，A+B＝C则有，E(A)+E(B)＝E(C)。

[0007] 对区块链上金额数值进行加法同态加密，验证节点在不需要知道交易金额的具体数值或者其他任何隐藏信息的情况下，可以对密文进行正确的加法操作，这样区块链上所有的用户余额和交易金额都以同态密文的形式存在，除了拥有私钥的可信第三方机构外，所有节点都只能验证交易而无法得知具体数值，这将有效的保护用户的账户隐私。

发明内容

[0008] 本发明的目的是针对现有技术的不足，提供一种基于加法同态加密的区块链隐私保护方法。

[0009] 本发明的目的是通过以下技术方案来实现的：在一个区块链网络上，交易发起方发送者发起交易，经全网节点验证，最后交易接收方接收者收到交易金额并完成交易，包括如下步骤：

[0010] 1)同态密钥生成，由一个可信任的第三方机构生成一对同态密钥作为全网的同态密钥，公开其同态公钥，私钥保存在第三方机构中。用户的账户余额有两种存在形式：一种是用全网同态公钥加密后存储在区块链公共账本上的真实余额，一种是以明文形式存储在用户本地只供用户自己可见的可见余额。

[0011] 2)拆分交易发送方的账户可见余额，发送方须将自己的可见余额值拆分为需要转账的交易金额和剩余余额，需要转账的交易金额不得大于可见余额，且任何金额不得小于

零；

[0012] 3)用全网同态公钥加密交易金额和剩余余额，同态加密后的密文分别记为X1和X2，此操作采用加法同态加密算法；

[0013] 4)用接收方的公钥加密步骤2)中的交易金额，加密后的密文记为Y1；

[0014] 5)发送者发起交易，交易内容包含步骤3)中的密文X1、密文X2以及步骤4)中的密文Y1三个字段，发送者将交易信息发送至全网节点进行验证；

[0015] 6)交易确认，区块链全网的验证节点进行交易信息的验证，并维护公共账本。由于公共账本上以同态加密密文形式存储全网账户的真实余额，验证节点进行交易验证时应当确认，①密文X1和密文X2对应的真实金额不小于零；②密文X1和密文X2的同态加法和与发送者的公共账本余额一致；交易信息验证成功后，验证节点对公共账本上的用户真实余额进行修改。

[0016] 7)更新接收者的可见余额：接收者上线接收交易信息，利用自己的私钥解密交易信息中的密文Y1得到交易金额明文，直接更新自己的可见余额。或者，接收者向可信的第三方机构申请查询真实余额，然后更新自己的可见余额。

[0017] 进一步地，所述的步骤1)中，区块链网络创建之初，由一个可信的第三方利用加法同态加密算法生成的一对同态密钥，这对同态密钥将作为全网的同态密钥，区块链上所有用户的余额均由同态公钥加密后保存在公共账本上，公共账本上存储所有账户的真实余额的密文，全网节点只能维护公共账本的密文而无法解密；私钥保存于一个可信的第三方机构中，只有提供了用户本身的签名后，才可以申请查询用户自己的账本余额。

[0018] 进一步地，所述的步骤2)中，用户保存自己的可见余额，可见余额存储在用户本地，其他人不可见；用户的可见余额应当与其真实余额数值相等，否则将无法发起有效的交易；当用户的可见余额数值上不等于其真实余额时，用户可以请求区块链的可信的第三方机构申请余额更新。

[0019] 进一步地，所述步骤3)中，用户发起交易时将自己的可见余额拆分为交易金额和剩下余额，并用全网同态公钥对交易金额和剩下余额进行同态加密，密文将作为交易的字段发送至全网，使得区块链上始终出现的都是用同态公钥加密后的金额数值，其它节点无法得知其真实数值。

[0020] 进一步地，所述的步骤4)中，发起方用接收方的公钥对交易金额进行加密后作为交易字段随交易一起发出，接收方可以解密该字段得知交易金额，其目的在于使步骤7)中接收者上线更新自己的可见余额时更加方便，不必每次都申请查账操作。若接收者在交易完成后发现自己的可见余额与真实余额数值上不相等，即被发送者告知不正确的交易金额，将导致接收者的下次交易无法完成，接收者可以选择向可信的第三方机构申请查询真实余额，然后更新自己的可见余额。

[0021] 本发明的有益效果是：本发明在区块链上对用户账户和交易金额的数值的进行同态加密，同时又满足区块链本身的技术特性。对于传统区块链上的交易，用户的所有账户都是公开的，交易由区块链上所有节点共同完成，这保证了区块链上信息的不可伪造和篡改，但同时暴露了用户的账户信息。为保护用户的账户隐私，本发明利用加法同态加密技术对区块链上所有的账户余额和交易金额采用统一的同态公钥进行加密，基于加法同态加密本身的性质，在区块链上仍然可以使用同态密文对交易进行验证，这样验证节点在不知道交

易金额具体数值的情况下，仍可验证交易的正确性。本发明有效地解决了传统区块链上的交易隐私问题。

附图说明

[0022] 图1是区块链用户自身的账户组成及发起交易过程图；

[0023] 图2是区块链上节点处理交易信息的过程图；

[0024] 图3是接收者接收交易信息后更新可见余额过程。

具体实施方式

[0025] 下面根据附图和具体实施例详细描述本发明，本发明的目的和效果将变得更加明显。

[0026] 如图1和图2所示，本发明基于加法同态加密的区块链隐私保护方法，包括如下步骤：

[0027] 1)同态密钥生成，由一个可信任的第三方机构生成一对同态密钥作为全网的同态密钥，公开其同态公钥，私钥保存在第三方机构中，可用于在用户丢失了自己可见余额值情况下，通过申请操作重新更新用户本地保存的可见余额，仅限用户本人申请。用户的账户余额有两种存在形式：一种是用全网同态公钥加密后存储在区块链公共账本上的真实余额，一种是以明文形式存储在用户本地只供用户自己可见的可见余额。

[0028] 2)拆分交易发送方的账户可见余额，如图1所示，发送方须将自己的可见余额值拆分为需要转账的交易金额和剩余余额，需要转账的交易金额不得大于可见余额，且任何金额不得小于零；

[0029] 3)用全网同态公钥加密交易金额和剩余余额，同态加密后的密文分别记为X1和X2，此操作采用加法同态加密算法；

[0030] 4)用接收方的公钥加密步骤2)中的交易金额，加密后的密文记为Y1，此操作采用椭圆曲线加密算法；

[0031] 5)发送者发起交易，交易内容包含步骤3)中的密文X1、密文X2以及步骤4)中的密文Y1三个字段，发送者将交易信息发送至全网节点进行验证；

[0032] 6)交易确认，区块链全网的验证节点进行交易信息的验证，并维护公共账本，如图2所示。由于公共账本上以同态加密密文形式存储全网账户的真实余额，验证节点进行交易验证时应当确认，①密文X1和密文X2对应的真实金额不小于零；②密文X1和密文X2的同态加法和与发送者的公共账本余额一致；交易信息验证成功后，验证节点对公共账本上的用户真实余额进行修改。

[0033] 7)更新接收者的可见余额，如图3所示：接收者上线接收交易信息，利用自己的私钥解密交易信息中的密文Y1得到交易金额明文，直接更新自己的可见余额。或者，接收者向可信的第三方机构申请查询真实余额，然后更新自己的可见余额。

[0034] 进一步地，所述的步骤1)中，区块链网络创建之初，由一个可信的第三方利用加法同态加密算法生成的一对同态密钥，这对同态密钥将作为全网的同态密钥，区块链上所有用户的余额均由同态公钥加密后保存在公共账本上，公共账本上存储所有账户的真实余额的密文，全网节点只能维护公共账本的密文而无法解密；私钥保存于一个可信的第三方机

构中，只有提供了用户本身的签名后，才可以申请查询用户自己的账本余额。

[0035] 进一步地，所述的步骤2)中，用户保存自己的可见余额，可见余额存储在用户本地，其他人不可见；用户的可见余额应当与其真实余额数值相等，否则将无法发起有效的交易；当用户的可见余额数值上不等于其真实余额时，用户可以请求区块链的可信的第三方机构申请余额更新。

[0036] 进一步地，所述步骤3)中，用户发起交易时将自己的可见余额拆分为交易金额和剩下余额，并用全网同态公钥对交易金额和剩下余额进行同态加密，密文将作为交易的字段发送至全网，使得区块链上始终出现的都是用同态公钥加密后的金额数值，其它节点无法得知其真实数值。

[0037] 进一步地，所述的步骤4)中，发起方用接收方的公钥对交易金额进行加密后作为交易字段随交易一起发出，接收方可以解密该字段得知交易金额，其目的在于使步骤7)中接收者上线更新自己的可见余额时更加方便，不必每次都申请查账操作。若接收者在交易完成后发现自己的可见余额与真实余额数值上不相等，即被发送者告知不正确的交易金额，将导致接收者的下次交易无法完成，接收者可以选择向可信的第三方机构申请查询真实余额，然后更新自己的可见余额。

[0038] 下面用一个区块链交易实例来说明具体实施方式：

[0039] 模拟用户A向用户B转账X金额的交易，交易发起人A，交易接受者B，交易由全网节点验证。

[0040] 首先，A在本地将自己的可见余额拆分，如图1所示，分别为交易金额和剩余余额，然后A用全网同态公钥加密交易金额和剩余余额，密文分别为X1、X2，并另将交易金额用B的公钥加密得密文Y1，A发起交易，交易信息包含字段X1、X2和Y1，当交易发布到区块链网络，验证节点将对交易合法性进行验证，并将正确结果记录在下一个区块上并维护全网公共账本(如图2所示)，B收到区块链上的交易信息，可以有两种方式更新自己的可见余额。方法一，B用自己的私钥解密Y1(如图3所示)，得知收到转账金额X，然后更新自己的可见余额，这种方法效率高；方法二，B申请第三方机构查询公共账本上自己的真实余额的具体数值，得到当前实际余额，将其更新为可见余额，这张方法更新的可见余额真实可信。以上是一个完整的交易过程。

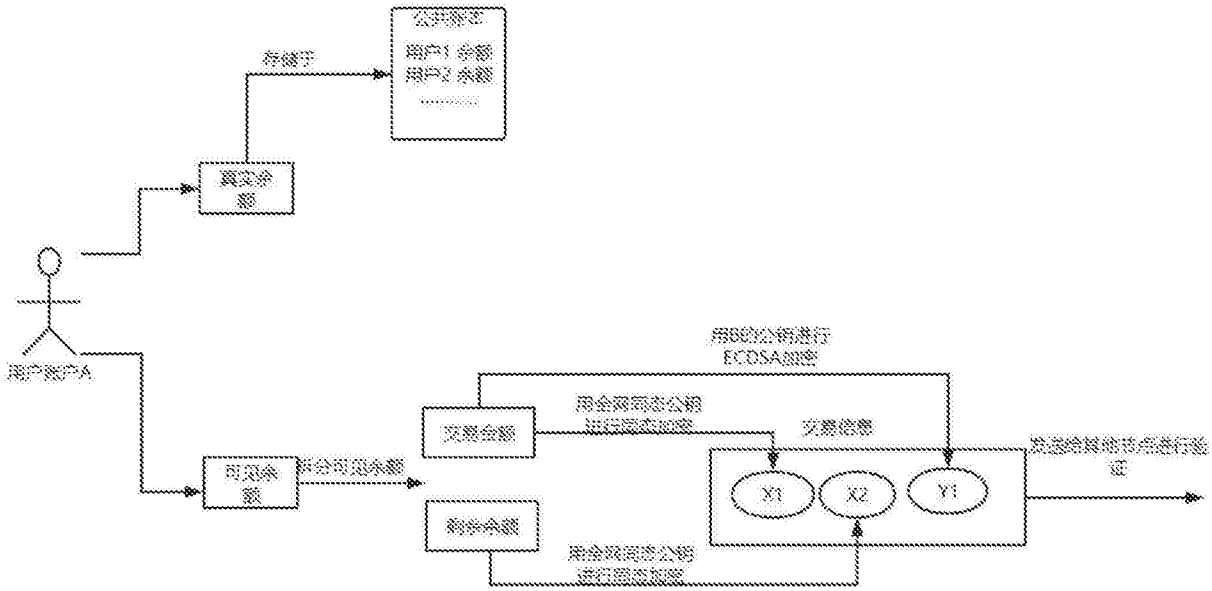
公开账本
用户1 余额
用户2 余额
.....
存储于
真实余额
用户账户A
可见余额
部分可见余额
交易金额
用全网同态公钥进行同态加密
用SM2公钥进行ECDSA加密
交易信息
X1
X2
Y1
剩余余额
用全网同态公钥进行同态加密
发送给其他节点进行验证

图1

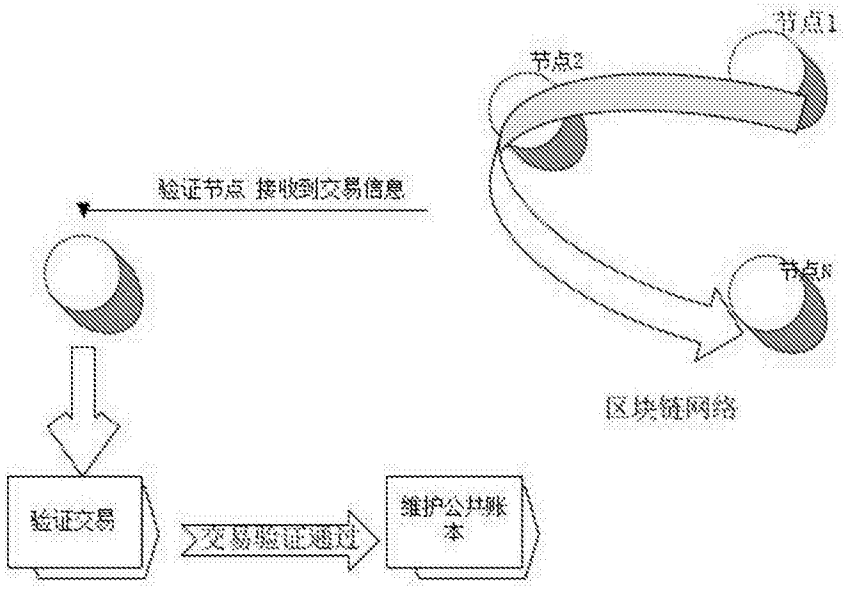
节点1
节点2
节点K
验证节点 接收到交易信息
区块链网络
验证交易
交易验证通过
维护公共账本

图2

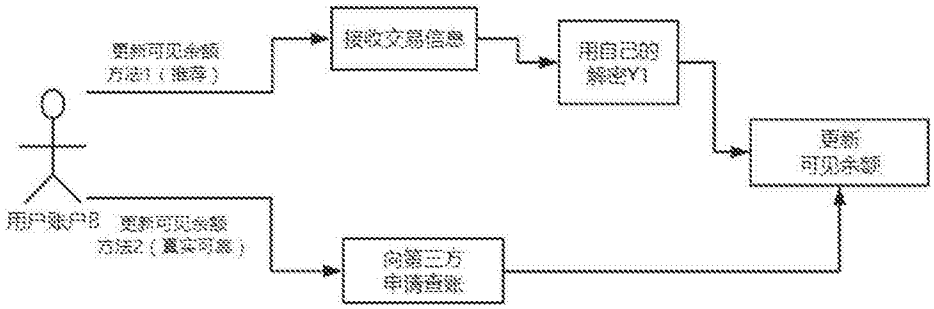
更新可见余额
方法1（推荐）
接收交易信息
用自己的
秘密Y1
更新
可见余额
用户账户B
更新可见余额
方法2（真实可靠）
向第三方
申请查账

图3