基于同态加密的区块链交易数据隐私保护方法

刘 琛[1]
LIU Chen

摘 要 因区块链的分布式特性，所有用户均可通过公开的账本，了解到所有交易的细节，导致攻击者可能会通过交易的详细数据来推断出交易双方的身份，并危害到用户的隐私，其中交易额是交易过程中最为重要的交易数据之一。基于此，针对区块链交易过程中的隐私保护问题，基于同态加密技术，实现了交易过程中记账节点能够在不知道双方账户余额和交易额的情况更新账本；同时引入了零知识证明方案，通过区间范围证明，记账节点能够在不知道交易额的情况下验证交易的合法性。通过使用数字签名的方式，验证了交易过程中传输数据时身份的真实性。通过对方案的安全性分析，证明了方案具有隐私安全的特性。

关键词 区块链；同态加密；零知识证明；隐私保护；数字签名

doi：10.3969/j.issn.1672-9528.2023.02.042

0 引言

自比特币诞生以来，区块链技术就由于其去中心化、可溯源、安全性高、保密性好、可信任性等特点受到各行各业的青睐，从以比特币为代表的公有链由此发展出以以太坊为代表的私有链和以超级账本为代表的联盟链分别称为区块链的 1.0 到 3.0。然而在区块链系统中，由于其账本是公开的，在公有链如比特币中，各用户之间的交易公开，可以追踪各用户之间的资金流动，从而推断出多个账号属于同一个用户，或者该用户的身份 [1]；在私有链及联盟链中，各用户的身份并未完全保密，因此链上的其他用户可以通过公开的账本知晓其他用户之间的交易额，从而对区块链上的用户隐私造成了较大的困扰。

针对区块链系统中用户隐私的保护，主要包括两个方面。

（1）交易聚合：为了解除交易之间的耦合性，将多个交易方发起的多比交易混合成单笔交易，从而达到隐藏用户身份的目的。但是将交易聚合只是将用户的身份隐藏起来 [2]，交易额依然公开在账本上。

（2）加密交易：通过密码学技术，将链上的敏感数据进行加密，只有特定用户才能查看。区块链中常用的密码学技术有：群签名等签名技术，如文献 [3] 利用群签名技术实现了链上数据的隐私保护；同态加密技术和零知识证明技术，如文献 [4] 基于 Pedersen 承诺加密和 BulletProof 区间证明实现了公有链进行交易时对交易双方约定的交易额进行隐藏。

本文基于同态加密技术，研究一种实现用户在交易中隐藏交易额的隐私保护方法。本文利用 Paillier 同态加密技术，将交易额隐藏并由其他节点进行加密并签名后以密文形式存入区块中，记账节点将区块上传到区块链网络，并通过 Paillier 加密算法的密文加法同态性在不需要知道真实交易额的情况下更新交易双方的钱包余额。该方法改进了传统区块链中交易数据公开透明的特点，并在不需要第三方可信任机构的情况下保护了用户间交易的交易额的隐私。

1 相关工作

1.1 Paillier 同态加密

同态加密是密码学领域最重要的技术之一，同态加密技术支持在加密后的密文上进行一定的数学运算，运算得到的结果经过解密与明文计算后的结果一致，在隐私保护方面有重大意义。

对于区块链网络中的用户来说，提交到区块链网络中的数据例如交易额，应避免泄露。同态加密技术能够使用户的交易额进行密文运算，而非传统的明文运算。这样的优点是，用户将交易额提交到区块链网络之前，可使用相应的加密算法对交易额进行加密，数据以密文的形式存在，账户余额结算时也不需要知道用户的钱包余额与交易额，同时密文运算结果与明文运算结果一致。由于这种特性，使得同态加密技术经常被引用到区块链技术中 [5]。

Paillier 算法是法国密码学家 Paillier 于 1999 年欧密会上发表 [6]，满足加法同态的半同态加密方案，该密钥系统由密钥生成、加密、解密 3 个部分组成。

（1）密钥生成，首先随机选择大素数 p、q，且满足 $gcd(pq,(p\text{-}1)(q\text{-}1))=1$，$gcd()$ 函数是求最大公因数。然后计算 $n=pq$，$\lambda=lcm(p\text{-}1,q\text{-}1)$，$lcm()$ 函数是求最小公倍数，随机选取 $g\in\mathbb{Z}_{n^2}^*$，得到公钥 $pk_p=(n,g)$，密钥 $sk_p=(\lambda,u)$。

（2）加密 $Enc()$，若要加密明文 m 随机选择 $r\in\mathbb{Z}_{n^2}^*$，计

1. 三峡大学 湖北宜昌 443000

算密文 $c=g^m r^n \bmod n^2$。其加法同态性表现为：

$$\begin{aligned} &Enc(m_1)\times Enc(m_2)\\ &=(g^{m_1}r_1^n \bmod n^2)\times(g^{m_2}r_2^n \bmod n^2)\\ &=g^{m_1+m_2}(r_1\times r_2)^n \bmod n^2\\ &=Enc(m_1+m_2)\end{aligned} \quad (1)$$

即密文的数乘解密后为明文相加。

（3）解密 $Dec(c)$，令函数 $L(x)=\frac{x-1}{n}$，得到明文：

$$m=\frac{L(c^\lambda \bmod n^2)}{L(g^\lambda \bmod n^2)} \bmod n \quad (2)$$

1.2 Elgamal 签名算法

ElGamal 公钥密码体制是由 T.ElGamal 于 1985 年提出的[7]，其安全性依赖于计算有限域上离散对数这一难题，既能用于数据加密也能用于数字签名。本文只用其进行数字签名，数字签名系统分为密钥生成、数字签名、签名认证 3 个部分组成。

（1）密钥生成，选择一个大素数 p，和一个 p 的本原根 g。随机选择一个 x，使得 $1<x<q-1$，计算 $y=g^x \bmod p$，得到公钥 pk_e 为 $\{p, g, y\}$，私钥 sk_e 为 x。

（2）数字签名 $Sign()$，若要签名信息 m，首先选择一个随机数 k，满足 $gcd(k, p-1)=1$，$gcd()$ 函数是求最大公因数。然后计算 $r=g^k \bmod p$，计算 $s=k^{-1}(m-xr) \bmod (p-1)$，得到签名后的消息 $Sign(m)$ 为 $\{m, r, s\}$。

（3）签名认证 $Auth()$，对数字签名 $Sign(m)$ 进行认证，计算 $v_1=y^r r^s \bmod p$ 和 $v_2=g^m \bmod p$，若 $v_1=v_2 \bmod p$，则 $Auth(m, r, s)$ 认证成功，签名有效。

1.3 零知识证明

1.3.1 Fujisak-i Okamoto 承诺

假设 n 作为大合数，$g\in\mathbb{Z}_{n^2}^*$，h 是 g 循环群中的元素，r 为随机整数，$E(x, r)=g^x h^r \bmod n$ 表示对 x 的承诺，该承诺能防止验证者通过该承诺获得关于 x 的任何信息，该协议是统计安全的，以下称该承诺为 FO 承诺，详细的分析见文献 [8]。

1.3.2 区间范围证明

在交易过程中，交易额与账户余额以密文形式进行存储和运算，通常需要满足账户余额大于交易额时，交易成立。为了证明一个承诺是在一个范围区间内，本文引用一种区间范围证明方法[9]，其相比 Fabrice Boudot 协议计算效率更高，协议更简便。简要证明过程如下：

（1）设 $E(x, r)=g^x h^r \bmod n$ 是一个 FO 承诺，t、l、s 为安全参数，T 为一个大合数，若想证明 $x\in(a,b)$，令 $y=x-a$，证明者随机选择整数 $\alpha\neq 0$，$0<\omega<2^{s+T}$，使 $u=\alpha^2 y+\omega>2^{l+t+s+T}$。

（2）证明者随机选择整数 $r_1, r_2, r_3\in[-2^s n+1, 2^s n-1]$，使得 $r_3-r\alpha^2-r_1\alpha-r_2\in[-2^s n+1, 2^2 n-1]$，并计算：

$$E_1=E^\alpha h^{r_1} \bmod n \quad (3)$$

$$E_2=E_1^\alpha h^{r_2} \bmod n \quad (4)$$

$$F=g^\omega h^{r_3} \bmod n \quad (5)$$

$$U=g^{u/E_2}=g^\omega h^{r_3-r\alpha^2-r_1\alpha-r_2} \bmod n \quad (6)$$

（3）证明者向验证者发送 (u, E_1, E_2, F)，并执行：

$$PK\{\alpha, r_1, r_2: E_1=E^\alpha h \bmod n \wedge E_2=E_1^\alpha h^r \bmod n\} \quad (7)$$

$$PK\{\omega, r_3, r_3-r\alpha^2-r_1\alpha-r_2: F=g^\omega h^{r_3}\wedge U=g^\omega h^{r_3-r\alpha^2-r_1\alpha-r_2} \bmod n\} \quad (8)$$

$$PK\{\omega, r_3: F=g^\omega h^{r_3}\wedge -2^{t+l+s+T}\le\omega\le 2^{t+l+s+T}\} \quad (9)$$

（4）验证者计算 $E=g^{x-a+1}h^r=E(x, r)g^{a+1}=g^y h^r \bmod n$ 和 $U=g^{u/E_2}=g^\omega h^{r_3-r\alpha^2-r_1\alpha-r_2} \bmod n$ 并验证式 (7)、(8)、(9) 和 $u=\alpha^2 y+\omega>2^{l+s+t+T}$ 即可确信 x 大于等于 a。

2 基于同态加密的区块链交易数据隐私保护协议设计

2.1 初始化

区块链中所有节点基于 Paillier 同态加密技术与 Elgamal 数字签名算法通过 1.1 与 1.2 的方法分别生成自己的公私钥对，pk_p、sk_p 和 pk_e、sk_e。

2.2 协议设计

步骤一，交易发起方 A 使用记账节点 C 的公钥 pk_{pC} 加密数字 1 得到 $Enc_c(1)$ 作为判定位，然后将真实交易额明文 m 与判定位使用自己的私钥 sk_{eA} 签名后，得到 $Sign_A(m, Enc_c(1))$ 发送给区块链上除记账节点和交易接受方 B 外任一节点 I_1；同时，交易发起方 A 生成 n 个虚假交易额 m_0，$n\geqslant 2$，并使用记账节点 C 的公钥 pk_{pC} 加密数字 2 得到 $Enc_c(2)$ 作为判定位，将虚假交易额 m_0 与判定位 $Enc_c(2)$ 使用自己的私钥 sk_{eA} 签名后，得到 $Sign_A(m_0, Enc_c(2))$ 发送给区块链上除记账节点和交易接受方 B 和 I_1 外的 n 个节点。

步骤二，在其他节点收到包含交易发起方 A 的签名的数据后，以获得真实交易额的节点 I_1 为例，在收到交易额数据 $Sign_A(m, Enc_c(1))$ 后，首先使用交易发起方 A 的公钥 pk_{eA} 进行签名认证，验证交易发起方 A 身份的真实性。然后将交易额明文 m 分别使用交易发起方 A 与交易接收方 B 的公钥 pk_{pA} 和 pk_{pB} 进行加密，得到密文 Enc_A(m) 与 Enc_B(m)，与 $Enc_c(1)$ 进行拼接后，使用节点 I_1 的私钥 $sk_{e_{I_1}}$ 进行签名得到 $Sign_{I_1}(Enc_A(m), Enc_B(m), Enc_C(1))$，发送给交易申请方 A。其他收到交易额的节点进行与 I_1 节点相同的操作。

步骤三，交易申请方 A 在收到其他节点的数据块后，使用在步骤一中加密判定位 1 时相同的随机数 r 加密数字 1，与收到的所有数据块中的判定位相对比，找出正确的交易额所处的数据块，然后使用节点 I_1 的公钥 $pk_{e_{I_1}}$ 对收到的数据块 $Sign_{I_1}(Enc_A(m), Enc_B(m), Enc_C(1))$ 进行签名认证，确认节点 I_1 身份的真实性；然后对 Enc_A(m) 使用自己的私钥 sk_{pA} 进行解密，若与真实交易额相符合，将该数据块使用自己的私钥 sk_{eA} 进行签名，并将得到 $Sign_A(Sign_{I_1}(Enc_A(m), Enc_B(m), Enc_C(1)))$，发送给交易接收方 B。

步骤四，交易接受方 B 收到数据块后，分别使用 A 的公钥 pk_{eA} 与 I_1 的公钥 $pk_{e_{I_1}}$ 进行签名认证，检验交易申请方 A 与节点 I_1 身份的真实性，若身份无误，则对数据块中的 Enc_B(m) 使用自己的私钥 sk_{pB} 进行解密，若交易额无误，则将收到的数据块使用自己的私钥 sk_{eB} 进行签名，得到

$Sign_B(Sign_A(Sign_{I_1}(Enc_A(m),Enc_B(m),Enc_C(1))))$，发送给交易申请方 A。

步骤五，交易申请方 A 收到来自交易接受方 B 的数据块后，使用 B 的公钥 pk_{eB} 进行签名认证，确认交易接收方 B 的身份的真实性，然后将账户余额 T 与交易额 m 的密文作同态减法，得到模拟交易后余额的密文，由于交易在最后上传至区块链时需要验证交易的合法性，即验证交易申请方 A 的余额是否大于交易额，即证明模拟交易后的余额密文 T`>0。根据 1.3.2 中区间范围证明的方法，作为证明者，交易申请方 A 将证明 $T$`>0 得到的 (u, E_1, E_2, F) 作为零知识证明 π，然后将步骤三中收到的所有数据块进行打包并使用自己的私钥 sk_{eA} 进行签名，得到 $Sign_A(Sign_{I_1}(Enc_A(m),Enc_B(m),Enc_C(1)),...,\pi)$，并发送给记账节点 C。

步骤六，在记账节点 C 收到来自交易申请方 A 的数据块时，首先使用 A 的公钥 pk_{eA} 进行签名认证，在确认 A 的身份的正确性后，在其他节点进行签名的数据块中对判定位 $Enc_c(1)$ 或 $Enc_c(2)$ 进行解密，在找到判定位为 1 的数据块后，根据 1.3.2 中区间范围证明的方法，作为验证方，确信交易申请方 A 的交易的合法性，最后将使用该数据块中的密文 Enc_A(m) 与 Enc_B(m) 分别对 A 与 B 的账户余额进行更新，并将 A 传入的数据块 $Sign_A(Sign_{I_1}(Enc_A(m),Enc_B(m),Enc_C(1)),...)$ 打包写入区块链中。

3 方案评估

3.1 方案安全性评估

Paillier 同态加密和 Elgamal 数字签名均基于大数的因式分解困难来保证其安全性，文献 [6-7] 具体的分析了这两种方案的安全性，并证明其是安全的。基于同态加密的特点，使该方案在交易过程中与数据上链时，除交易双方外，在其他节点不知道具体交易额与双方账户余额的情况下能够完成交易，并通过使第三方节点进行加密，有效防止交易双方在交易中通过约定与真实交易额不同的交易额，在其他节点无法知道交易额与账户余额的真实信息的情况下，使交易双方账户余额的变化不相等。在节点通信中采取数字签名的方式也有效保证了区块链中用户身份的不可伪造。本方案还采用伪造多个虚假交易额的方法，使第三方节点进行加密并签名时无法知道自己加密的是否为真实交易额，若选中的第三方节点中有作恶节点，使其作恶成功率下降为 1/n，n 为第三方节点参与加密的数量。通过零知识证明，使得该方案在交易过程中无需知道交易申请方的账户余额与交易的交易额就能够判断交易申请方的账户余额是否充足，无法在账户余额不足的情况下进行非法交易。

3.2 相关研究

保护交易数据的隐私，通常使用对交易数据进行加密来进行交易。

在区块链网络中使用同态加密技术，可以对数据进行聚合，通过将大量数据集合达到隐藏用户身份的目的，如文献 [10] 基于 Hyperledger Fabric 联盟链，使用 Paillier 同态加密进行聚合数据，隐藏了用户的身份；文献 [11] 利用同态 Paillier 密码技术加密结构化数据将用户数据与管理平台之间的数据进行聚合，实现用户身份的匿名性。这些方案一定程度上实现了区块链中用户身份的匿名性，但无法完成对交易额的隐私保护，交易额依然暴露在公开的账本中。

针对交易额的隐私保护，文献 [12] 基于 Elgamal 的强盲签名算法，对投票内容进行加密，通过智能合约取代第三方可信平台，实现了对交易内容的隐私保护，但并未对用户的钱包账户进行保护。为了同时隐藏具体交易额与用户的账户，将同态加密技术引入到加密交易额与用户钱包账户中。如文献 [4] 构建了一个区块链网络，节点通过可信平台的公钥加密交易额和钱包余额，实现了平台中用户间交易的交易额隐藏，但是，对于公有链的情况，由于公有链中用户身份的混乱性，不可能产生一个令所有用户信任的第三方平台。文献 [13] 通过同态加密和轻量级的零知识证明，不需要一个可信的第三方机构来验证交易的合法性，但最后将交易数据上传至区块链网络的矿工节点总能够知道具体的交易额，并不能完全隐藏住真实的交易额。本方案与上述研究对比如表 1。

表 1 相关隐私区块链的功能对比

方案	匿名性	是否隐藏钱包	是否隐藏交易额	是否有第三方知道交易额
文献 [4]	否	是	是	是
文献 [10]	是	否	否	是
文献 [12]	是	否	是	否
文献 [13]	是	是	是	否

4 结语

本文提出了基于同态加密的区块链交易数据隐私保护方法，将区块链交易过程中的交易额隐藏并同时隐藏用户的钱包账户，使交易可以在其他节点不知道交易额和交易用户的钱包余额的情况下进行，同时引入零知识证明，使其他节点能够验证交易合法并有效，采用数字签名使节点在通信过程中能够验证其他用户身份的可靠性。本方案相比其他使用同态加密的方案，无需依赖可信的第三方平台或记账节点，同时保证安全性。后续将在此基础上进一步研究安全性，并实现全匿名区块链。

参考文献：

[1] BONNEAU J, MILLER A, CLARK J, et al. Sok: research perspectives and challenges for bitcoin and cryptocurrencies[C]//2015 IEEE Symposium on Security and Privacy. San Francisco, CA, USA: IEEE, 2015: 104-121.

（下转第 178 页）

机构签订保密协议。系统管理员、网络管理员、安全管理员对所有评测实施过程中用过的账户口令做集中管理，测评实施结束后，集中修改口令与安全访问策略。

3 结束语

学校的安全网络建设对中小学信息化的发展起着至关重要的作用[10]。本文研究了等保 2.0 的特点与变化，以等保 2.0 为切入点，从安全管理和技术应用两方面落实等级保护 2.0 的建设；根据中小学目前的网络安全现状，建立了基于等级保护 2.0 标准下网络安全的防御模型，以及新标准下校园网络安全的风险评估与策略，为优化中小学网络提供保障，提升了校园的安全防护能力。

参考文献：

[1] 林锐 . 加快推进网络安全保障体系建设 [J]. 中国党政干部论坛 , 2020(1):38-43.

[2] 夏冬梅 . 基于智慧校园的网络安全保障体系建设 [J]. 智能城市 , 2019,5(19):13-14.

[3] 信息安全等级保护制度在信息系统建设中的应用分析 [J]. 郑绍林 . 电子元器件与信息技术 ,2022(1):25-28.

[4] 朱圣才 . 等保 2.0 框架下高校网络安全体系建设 [J]. 网络空间安全 , 2020,11(4):14-18.

[5] 国家市场监督管理总局 , 中国国家标准化管理委员会 . GBT36342—2018 智慧校园总体框架 [S]. 北京 : 中国标准出版社 , 2018:1-4.

[6] 许子明 , 田杨锋 . 云计算的发展历史及其应用 [J]. 信息记录材料 , 2018,19(8):66-67.

[7] 万波 , 辛建平 . 移动互联网环境下高校智慧校园的构建分析 [J]. 信息与电脑 (理论版), 2017(15): 171-175.

[8] 姜琪 , 李亚龙 , 张洁 , 等 . 新形势下的电子政务网络安全保障体系蓝图设计 [J]. 网络安全技术与应用 ,2019(5):113-115.

[9] ACKOFF R L. From data to wisdom[J]. Journal of applied systems analysis, 1989(15): 3-9.

[10] LI Y, ZHANG Z, CHEN Z, et al. Study and analysis of collaborative management system of network security in universities (CMSNSU) under the background of 2.0 criteria of classified protection of network security[C]//2021 2nd International Conference on Computing and Data Science (CDS). New York: IEEE, 2021: 398-401.

【作者简介】

孔志业（1979—），男，江苏泰州人，大学本科，泰州市姜堰区教师发展中心高级工程师，研究方向：计算机设备、中小学信息装备配备、网络安全、教育城域网等信息化工作。

（收稿日期：2022-10-16 修回日期：2022-11-28）

（上接第 174 页）

[2] 陈思光 , 杨熠 , 黄黎明 , 等 . 基于雾计算的智能电网安全与隐私保护数据聚合研究 [J]. 南京邮电大学学报 (自然科学版), 2019, 39(6):62-72.

[3] 李莉 , 杜慧娜 , 李涛 . 基于群签名与属性加密的区块链可监管隐私保护方案 [J]. 计算机工程 ,2022,48(6):132-138.

[4] 王子钰 , 刘建伟 , 张宗洋 , 等 . 基于聚合签名与加密交易的全匿名区块链 [J]. 计算机研究与发展 ,2018,55(10):2185-2198.

[5] MAHESH K M, PRASAD M V N K, RAJU U S N. BMIAE: blockchain - based multi - instance iris authentication using additive ElGamal homomorphic encryption[J]. IET biometrics, 2020, 9(4): 165-177.

[6] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes[C]//International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Heidelberg: Springer, 1999: 223-238.

[7] ELGAMAL T. A public key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE transactions on information theory, 1985, 31(4): 469-472.

[8] FUJISAKI E, OKAMOTO T. Statistical zero knowledge protocols to prove modular polynomial relations[C]//Annual International Cryptology Conference. Berlin, Heidelberg: Springer, 1997: 16-30.

[9] 伍前红 , 张键红 , 王育民 . 简单证明一个承诺值在特定区间内 [J]. 电子学报 , 2004(7):1071-1073.

[10] 胡柏吉 , 李元诚 , 房方 , 等 . 基于轻量级区块链的隐私保护传染病监测数据聚合 [J]. 中国科学 : 信息科学 , 2021, 51(11): 1885-1899.

[11] 朱嵩 , 王化群 . 基于 Paillier 算法的智能电网数据聚合与激励方案 [J]. 计算机工程 ,2021,47(11):166-174.

[12] 邵清 , 洪皓洁 , 李斌 . 基于 Elgamal 强盲签名的区块链电子投票方案研究 [J]. 小型微型计算机系统 , 2021,42(11):2400-2406.

[13] 王瑞锦 , 唐榆程 , 裴锡凯 , 等 . 基于轻量级同态加密和零知识证明的区块链隐私保护方案 [J]. 计算机科学 , 2021, 48(S2):547-551.

【作者简介】

刘琛（1997—），男，湖北黄石人，三峡大学硕士，研究方向：区块链。

（收稿日期：2022-08-27 修回日期：2022-10-08）