计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.200800123

基于数字承诺的区块链交易金额保密验证方法

张小艳　李秦伟　付福杰
贵州大学计算机科学与技术学院　贵阳 550025
贵州省公共大数据重点实验室　贵阳 550025
(1057879450@qq.com)

摘　要　传统区块链交易中,隐私保护都是在匿名机制下加密用户的敏感信息,引入公正的第三方对交易明文信息进行验证,然而一旦第三方受到攻击,用户的交易信息便会被泄露,且在理性状态下不存在真正公正的第三方。为了能够更好地解决区块链交易中存在的隐私问题,针对交易者非匿名状态下的交易金额保密验证问题,采用PVC数字承诺协议,将交易金额隐藏在承诺中,并构造公开可验证的零知识证明方案,使验证者能在不获取交易敏感信息的情况下对交易的合法性进行保密验证。同时,利用椭圆曲线同态加密特性加密金额,进而解决交易者密文账本的更新问题。对所提出的隐私保护方案的正确性进行验证和分析,结果表明,与已有方案相比,所提方案具有计算复杂度相对较低、安全性强、高效等优点。

关键词:区块链;PVC数字承诺;保密验证;公开可验证;椭圆曲线同态加密
中图法分类号　TP309

Secret Verification Method of Blockchain Transaction Amount Based on Digital Commitment

ZHANG Xiao-yan,LI Qin-wei and FU Fu-jie
College of Computer Science and Technology,Guizhou University,Guiyang 550025,China
Guizhou Provincial Key Laboratory of Public Big Data,Guiyang 550025,China

Abstract　In traditional blockchain transactions,privacy protection is to encrypt users' sensitive information under the anonymity mechanism,and a trusted third party is involved to verify the transaction plaintext information. However,once the third party is attacked,the users' transaction information will be divulged. Furthermore,there is no truly trusted third party in a rational state. To better solve the privacy problems in blockchain transactions,and in view of issues of confidentiality verification of the traders' transaction amount under the non-anonymous state,the PVC digital commitment protocol is adopted to hide the transaction amount in the commitment,and a publicly verifiable zero-knowledge proof scheme is established,so that verifiers are able to confidentially verify the legitimacy of the transaction without obtaining sensitive information from the traders. At the same time,the elliptic curve homomorphic encryption feature is used to encrypt the amount,thereby solving the problem of updating the traders' ciphertext ledger. The correctness of the proposed privacy protection scheme is verified and analyzed,and the results shows that compared with the existing schemes,the proposed scheme has the advantages of relatively low computational complexity,strong security and high efficiency.

Keywords　Blockchain,PVC digital commitment,Confidentiality verification,Publicly verifiable,Elliptic curve homomorphic encryption

1　引言

区块链是一种由多个节点共同维护的分布式公共账本,具有去中心化、去信任化、可追溯、公开透明等特点[1-3]。区块链中所有的交易都是公开的,链中的每个节点均可以读取交易数据,验证交易数据的正确性将导致攻击者很容易从公开透明的交易记录中获取用户的隐私信息。针对基于数据分析的隐私窃取方法,目前已经出现了一些隐私保护机制[4-8],其主要思想是在不影响区块链系统正常工作的情况下,对公开数据中的部分信息进行隐藏,增加数据分析的难度,如混币机制[9]、环签名[10]、零知识证明[11]等。但隐私保护程度的提高会带来另一个问题,即交易难以审计。由于交易时采用匿名的方式,根据链上所记录的交易信息无法识别出关联方,可能会让地下钱庄洗钱、敲诈勒索等非法行为更加泛滥。因此,需

到稿日期:2020-08-19　返修日期:2020-11-18　本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:国家自然科学基金(61802081);贵州省公共大数据重点实验室开放项目(2017BDKFJJ003)
This work was supported by the National Natural Science Foundation of China(61802081) and Key Laboratory Open Project of Public Big Data of Guizhou Province,China(2017BDKFJJ003).
通信作者:李秦伟(1539614676@qq.com)

要研究区块链交易中隐私与可审计性质平衡的方案。而对于具有审计性质的审计方，大多需要建立在对审计方完全信任的前提下，将交易以明文的形式发送给审计方进行审计，但在实际生活中不存在真正公正、值得信赖的审计方，当存在利益诱惑时可能会出现审计方滥用职权的情况，如超出调查范围审计、获取用户敏感信息等。因此，如何在交易过程中既能保护用户的敏感信息，又能对交易的合法性进行验证是目前急需解决的问题。本文研究的主要内容是应用于 B2B，C2M 类电商平台的区块链记账系统交易金额的保密验证和账本更新，与传统区块链隐私保护方法不同的是，本文方案是在交易者不能匿名的前提下，对交易金额密文验证和密文账本进行更新。

目前，区块链隐私保护策略的相关研究已取得一些成果。2013 年，Miers 等[12]基于比特币提出了可匿名的区块链数字货币方案——零币，该方案使用非交互式零知识证明和 RSA 累加器等密码学技术来中断单个交易之间的链接，隐藏交易者的地址，从而达到交易不可追踪、交易信息不被泄露的效果，但是该方案中的节点需要额外维护货币作废列表以保证交易的唯一性，这需要大量的计算工作，且交易验证的时间以分钟为单位，导致实用性不强。2014 年，Sasson 等[13]提出，在 Zerocash 中使用 zk_SNARK 来实现在交易中对用户身份、交易金额和账户余额进行隐藏，理论上每笔交易转账金额可以是任意的正数，且区块链网络中的节点均可以自由验证某笔交易的合法性，但是在验证过程中存在计算量大、交易块传输慢、验证时间过长的问题。2016 年，Noether 等[14]提出了环机密交易的概念，利用门罗币实现了在高度分散的匿名加密货币 Monero 中隐藏交易金额。当用户发起一笔交易时，发起者采用环签名来签署交易，该签名以合理的效率和可验证、不可信任的代币生成，从而达到隐藏交易金额、交易发起点和交易终止点的目的。但是，该签名技术由于在签名的过程中需要其他用户参与以完成签名，因此存在交易信息被泄露的风险。2017 年，Yuan 等[15]提出一个新的环签名方案，旨在保护区块链上的交易隐私。当交易包含多个输入和输出时，此方案能够隐藏交易的金额，但是它仅仅能够保护交易隐私，并不能对交易的合法性进行验证。2018 年，Narula 等[16]提出了第一个保护分类账参与者的隐私并具有快速、可证明特性的审计系统——zkLedger 系统。该系统使用 Schnorr 型非交互式零知识证明方法，向验证方证明用户资金的输出之和不大于用户拥有的资金之和，从而达到保护用户资金敏感信息的目的。针对交易的保护，Li 等[17]采用 Paillier 加密算法加密交易金额，结合零知识证明完成交易金额的保密验证。该方案较简洁，但仅能用于交易验证，且需要诚实可信的第三方获取交易双方的公私钥解密交易输入，来为交易双方的承诺产生相等性证据，安全性不高。文献[18]使用 Paillier 同态加密算法加密交易金额，使加密的交易可以合并、拆分和消费，通过在脚本中隐藏敏感信息来实现交易用户的匿名性，通过承诺证明实现交易密文中金额的验证，从而保证交易的合法性，符合加密交易的理念并可直接解密密文，但是其密文和公钥过长导致效率极低。He 等[19]基于 Pedersen 数字承诺协议，提出了一个公开可验证的承诺方案 PVC，并讨论了其安全性。

综上所述，区块链交易隐私保护的研究方案使用的隐私保护策略如表 1 所列。

表 1 研究方案使用的隐私保护策略

Table 1 Privacy protection strategy used in research project

技术	匿名	可公开验证	保密交易
零币[12]	√	×	√
zk_SNARK[13,16]	√	√	√
门罗币[14]	√	×	√
环签名[15]	√	×	√
Pedersen 承诺[19]	√	×	√

由表 1 可知，几种隐私保护策略方案都能达到保密交易的效果，但都是在交易者匿名的情况下才得以实现，且在以上隐私保护策略中只有 zk_SNARK 能实现交易公开可验证，但是该策略在验证过程中计算量大、验证时间长，导致其应用场景有限。

基于以上研究，针对 C2M，B2B 电商区块链的应用场景，在交易者不匿名的状态下保护交易隐私，实现全网节点均可验证密文交易的合法性，本文基于椭圆曲线同态加密特性，根据 Pedersen 承诺并结合文献[19]提出的公开可验证的 PVC 数字承诺和零知识证明技术，提出了交易金额公开保密验证方法，把交易保密验证问题归约到基于零知识证明的 PVC 数字承诺，利用椭圆曲线高效、密钥短及同态加密的特性，构建了保护交易数据的区块链。本文的主要贡献如下：

(1)为了解决非匿名交易的保密验证问题，利用 PVC 数字承诺方案和零知识证明技术在将交易金额隐藏后公布证据，以供全网节点验证。

(2)利用椭圆曲线同态特性，实现交易者密文账本的更新，从而实现交易验证和账本更新的全程保护。

(3)设计交易保密验证协议，并分析协议的正确性和安全性。

2 准备知识

2.1 同态加密

同态加密最先是由 Rivest 等[20]于 1978 年提出的密文操作技术，利用该加密技术可以在无需对密文解密的情况下直接对密文进行相关操作。设加密操作为 E_K，解密操作为 D_k，明文信息为 $m=\{m_1,m_2,\cdots,m_n\}$，ϕ 和 ω 代表两种运算。如果加解密函数和运算满足同态特性，则下列等式成立：

$$E_K\{\omega(m_1,m_2,\cdots,m_n)\}=\phi\{E_K(m_1),E_K(m_2),\cdots,E_K(m_n)\} \tag{1}$$

由式(1)可知，如果对明文数据 m 进行 ω 运算后再对其进行 E_K 加密操作，则可以先把明文数据 m 的分量进行 E_K 加密操作后再进行 ϕ 运算，其结果是一样的。将 ϕ 的运算结果进行 D_k 操作即可得到 $\omega(m_1,m_2,\cdots,m_n)$。如果 $\phi=\omega=$“+”，表示加法同态特性，则有：

$$\sum_{i=1}^{n}m_i=D_k\{\sum_{i=1}^{n}(E_K(m_i))\} \tag{2}$$

2.2 椭圆曲线同态特性

使用椭圆曲线加密时，首先需要将明文消息 m 编码到椭圆曲线上得到点 P_m，选取一个随机数 r，利用公钥 K 加密明

文点 P_m，加密结果为：

$$C(P_m)=(C_1,C_2) \tag{3}$$

其中，$C_1=rG$，$C_2=rK+P_m$，(C_1,C_2)即为对 P_m 加密过后的密文。解密时使用私钥 k 解密(C_1,C_2)，即：

$$C_2-kC_1=rK+P_m-krG=rK+P_m-rK=P_m \tag{4}$$

对 P_m 进行解码即可恢复明文信息 m。

椭圆曲线加密算法具有同态加法特性[21]，使用椭圆曲线同态加法时，将对应的明文分量 $m_1,m_2,\cdots,m_n$ 分别映射到椭圆曲线上，得到对应点 $P_{m_1},P_{m_2},\cdots,P_{m_n}$，选取 n 个不同的随机数 $r_1,r_2,\cdots,r_n$，根据 $C_1=rG$ 和 $C_2=rK+P_m$ 可以得到 $C_{1_1},C_{1_2},\cdots,C_{1_n}$ 和 $C_{2_1},C_{2_2},\cdots,C_{2_n}$，其中对点 P_{m_i} 加密得到密文(C_{1_i},C_{2_i})，满足 $C_{1_i}=r_iG,C_{2_i}=r_iK+P_{m_i}$，即对 P_m 的加密结果为：

$$E_K(P_m)=\{(C_{1_1},C_{2_1}),(C_{1_2},C_{2_2}),\cdots,(C_{1_n},C_{2_n})\} \tag{5}$$

对式(5)相应项的密文进行累加即得$(\sum_{i=1}^{n}C_{1_i},\sum_{i=1}^{n}C_{2_i})$，根据式(4)，再结合私钥 k 进行解密计算：

$$\begin{aligned}\sum_{i=1}^{n}C_{2_i}-k\sum_{i=1}^{n}C_{1_i}&=K\sum_{i=1}^{n}r_i+\sum_{i=1}^{n}P_{m_i}-kG\sum_{i=1}^{n}r_i\\&=K\sum_{i=1}^{n}r_i+\sum_{i=1}^{n}P_{m_i}-K\sum_{i=1}^{n}r_i=\sum_{i=1}^{n}P_{m_i}\end{aligned} \tag{6}$$

对$\sum_{i=1}^{n}P_{m_i}$进行解码，即可得到$\sum_{i=1}^{n}m_i=m_1+m_2+\cdots+m_n$。

2.3 公开可验证承诺(Publicly Verifiable Commitment, PVC)

基于 Pedersen 数字承诺协议[22-23]，文献[19]提出了一种公开可验证的 PVC 承诺方案。该承诺方案是基于离散对数困难性假设的，其安全性等价于 Pedersen 承诺的安全性。

数字承诺协议指发送方暂时以隐藏的方式向接收方承诺一个值，发送方承诺后不能再对该值做出任何修改。数字承诺中，Pedersen 数字承诺协议是基于离散对数困难性假设的，其构造包括如下 3 个阶段。

(1)初始化阶段：选择拥有大素数阶 p 的乘法群 G，并选择生成元 g，$f\in G$(假设参与双方无法获知$\log_g f$)，公布(g,f,p)。

(2)承诺阶段：发送者选择随机值 $r\in Z_p$，计算 $C=g^m f^r \bmod p$，然后发送 C 给接收者。

(3)打开阶段：发送者发送(m,r)给接收者，接收者验证 C 是否等于 $g^m f^r \bmod p$，如果等于，则接受。

Pedersen 数字承诺满足隐藏性(hiding)和绑定性(binding)。

2.4 零知识证明协议

零知识证明[24]指证明方能够在不向验证方提供任何有用信息的前提下，也能使验证方相信某个论断是正确的，其本质是一种涉及两方的协议。本文采用基于 PVC 数字承诺的零知识证明协议来证明交易的合法性。

设 t,l,s_1,s_2 为 4 个安全参数，q 和 p 是素数，g_1 是 Z_p^* 中阶最大的元素，g_2,f_1,f_2 是由 g_1 生成的循环群中的元素，Alice 和 Bob 均不能计算$\log_{g_1} f_1$，$\log_{f_1} g_1$，$\log_{g_2} f_2$，$\log_{f_2} g_2$。Alice 有一个随机数 x，$E=E_1(x,r_1)=g_1^x f_1^{r_1} \bmod p$ 和 $F=E_2(x,r_2)=g_2^x f_2^{r_2} \bmod p$ 分别表示以(g_1,f_1)和(g_2,f_2)为基对 x 的承诺。Alice 想向 Bob 证明 E 和 F 隐藏着同一个秘密 x，证明过程如下：

Alice 随机选取数 $\omega\in[0,2^{t+1}q-1]$，$\eta_1\in[1,-2^{t+l+s_1}q-1]$，$\eta_2\in[1,2^{t+1}q-1]$，然后计算 $W_1=g_1^{\omega}f_1^{\eta_1} \bmod p$，$W_2=g_2^{\omega}f_2^{\eta_2} \bmod p$，$c=H(W_1\parallel W_2)$，$D=\omega+cx$，$D_1=\eta_1+cr_1$，$D_2=\eta_2+cr_2$，Alice 向 Bob 发送证据$(c,D,D_1,D_2)$。

Bob 验证 $c=H(g_1^D f_1^{D_1}E^{-c} \bmod p \parallel g_2^D f_2^{D_2}F^{-c} \bmod p)$。记上述协议 $ZPK\{x,r_1,r_2 \mid E=g_1^x f_1^{r_1} \bmod p \wedge F=g_2^x f_2^{r_2} \bmod p\}$是一个完全零知识证明协议，即使攻击者的计算能力是无限的，其也不能提取 x 的任何信息。

2.5 离散对数问题

椭圆曲线离散对数问题(ECCDLP)指：设 E 为定义在有限域 $GF(p)$ 上的椭圆曲线，对于给定的 E 上的两点 G 和 K，求满足 $K=kG$ 的 k 在计算上是非常困难的。

对于大素数 p 阶的乘法群 G 来说，使用目前已知的最好的求解离散对数的算法来求解 G 上的离散对数，仍然需要大约 $O(\sqrt{p-1})$次群运算，因此本承诺方案采用离散对数知识证明，例如：

$$\begin{aligned}PK(y_1,y_2,p)=\{\exists\, x,\gamma_1,\gamma_2 : y_1=g^x f^{\gamma_1} \bmod p \wedge y_2=\\ g^x f^{\gamma_2} \bmod p\}\end{aligned} \tag{7}$$

式(7)表示用户想要证明承诺 y_1 和 y_2 是对同一个秘密的承诺值，使用上述公式可以简化表示不同的离散对数知识证明，而不必写出具体的证明过程。

3 区块链交易数据保密验证

3.1 问题描述

本文针对区块链交易保密验证问题的应用场景如图 1 所示。存在这样一笔交易，交易发起者 Alice 需要转出 $S_{A\to B}$ 的交易金额给交易接收方 Bob，Bob 接收到转入的交易金额 $S'_{A\to B}$后，Alice 和 Bob 线下协商达成交易，将交易发给全功能记账节点验证该笔交易的合法性。全功能记账节点对 Alice 转出金额 $S_{A\to B}$ 与 Bob 转入金额 $S'_{A\to B}$ 的一致性进行验证。若 $S_{A\to B}=S'_{A\to B}$，则输出 1 返回给交易双方，表明交易合法，同意该笔交易，并更新 Alice 和 Bob 本地数据库临时存储的账本，否则输出 0，拒绝该笔交易。在验证交易金额的一致性和更新账本时，为了防止全功能记账节点滥用职权来获取交易双方的交易金额敏感信息，本文中交易双方将交易信息加密后以密文的形式发送给全功能记账节点以进行验证，同时交易双方的余额也是加密后存放在全功能记账节点临时创建的本地数据库中，交易双方完成该笔交易后全功能记账节点对交易双方的密文账本进行更新。

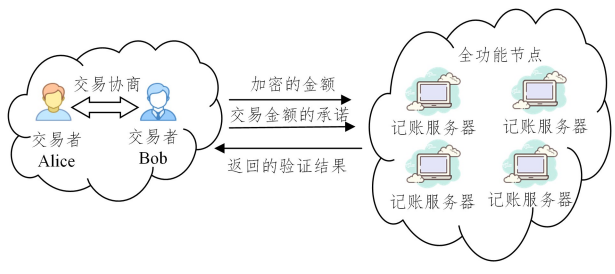

图 1 应用场景图

Fig. 1 Application scene graph

3.2 协议设计

交易双方将自己的账户余额和本次交易金额加密后发送

给全功能记账节点进行存储，以便交易双方完成交易后全功能记账节点对交易者的账本进行更新。

3.2.1 协议前置条件

(1)Alice 的公、私钥为 K_A，k_A；Bob 的公、私钥为 K_B，k_B。

(2)Alice 选取随机数 r_A，r_A'，结合公钥 K_A，利用椭圆曲线同态加密分别对账户余额和交易金额进行加密，得到账户余额密文 $C_A=(C_{A1},C_{A2})$和交易金额密文 $C_A'=(C'_{A1},C'_{A2})$，将 C_A，C_A'发送给全功能记账节点；同理，Bob 选取随机数 r_A，r_A'，结合公钥 K_B 分别对账户余额和交易金额进行加密，得到账户余额密文 $C_B=(C_{B1},C_{B2})$和交易金额密文 $C_B'=(C'_{B1},C'_{B2})$，并将密文 C_B 和 C_B'发送给全功能记账节点。

协议 1　基于 PVC 数字承诺协议交易金额保密验证方法。

本文基于 PVC 数字承诺协议，结合零知识证明，验证交易双方的交易金额是否具有一致性。交易双方将交易金额明文隐藏在承诺中，并把承诺放入一个零知识证明中以获取交易金额相等性的证据。全功能记账节点验证两个承诺是否隐藏同一个秘密，验证结束后全功能记账节点除了知道两个承诺是对同一个交易金额的承诺以外，并不能从中得到额外的交易信息。验证通过后，对交易双方的密文账本进行更新。

(1)参数生成。PVC 数字承诺协议中承诺者选取大素数 q，$p=2q+1$ 也是素数。$H(\cdot)$为安全哈希函数，对于任意的 $x\in Z_p^*$，$|H(x)|+1=|p|$，并且 $H(x)\in Z_p^*$。为了保证承诺值无条件隐藏且承诺公开可验证，本文的生成元是单哈希函数值。选择随机数 $u_1,u_2\in Z_p^*$，令：

$$g_1=H(u_1)^{\frac{p-1}{q}}=H(u_1)^2 \bmod p$$

$$g_2=H(u_2)^{\frac{p-1}{q}}=H(u_2)^2 \bmod p$$

$$f_1=H(g_1)^2 \bmod p,\ f_2=H(g_2)^2 \bmod p$$

其中，$g_1,g_2\neq 1$，$f_1,f_2\neq 1$，且 g_1,g_2,f_1,f_2 的阶均为 q。随机选取 l,t,s_1,s_2 作为安全参数，公开参数 $(g_1,g_2,f_1,f_2,p,q,l,t,s_1,s_2)$。

(2)承诺阶段。Alice 选取 $\omega\in[1,2^{l+t}q-1]$，$\eta_1\in[1,2^{l+t+s_1}q-1]$，$\eta_2\in[1,2^{l+t+s_2}q-1]$，计算 $W_1=g_1^{\omega}f_1^{\eta_1} \bmod p$，$W_2=g_2^{\omega}f_2^{\eta_2} \bmod p$，$c=H(W_1\parallel W_2)$，并用 Bob 的公钥加密参数 c 和 η_2，从而得到 $\phi=E_{K_B}(c,\eta_2)$，将 ϕ 发给 Bob。

Alice 选择随机数 $r_{A_1}\in[-2^{s_1}q+1,2^{s_1}q-1]$，结合参数 g_1，f_1 和 p，将交易金额 $S_{A\to B}$ 隐藏在承诺 y_A 中，得到式(8)：

$$y_A=y_A(S_{A\to B},r_{A_1})=g_1^{S_{A\to B}}f_1^{r_{A_1}} \bmod p \tag{8}$$

同理，Bob 选取随机数 $r_{B_1}\in[-2^{s_2}q+1,2^{s_2}q-1]$，结合参数 g_2，f_2 和 p，将交易金额 $S_{A\to B}$ 隐藏在承诺 y_B 中，得到式(9)：

$$y_B=y_B(S_{A\to B},r_{B_1})=g_2^{S_{A\to B}}f_2^{r_{B_1}} \bmod p \tag{9}$$

同时，Bob 用自己的私钥 k_B 解密密文 ϕ，即 $D_{k_B}(\phi)=D_{k_B}(E_{K_B}(c,\eta_2))$，得到参数 c 和 η_2。Bob 计算 $D_2=cr_{B_1}+\eta_2$，并将承诺 y_B 和 D_2 发送给 Alice。

(3)生成零知识证明阶段。Alice 收到 Bob 发送的承诺 y_B 和 D_2 后，计算 $D=cS_{A\to B}+\omega$，$D_1=cr_{A_1}+\eta_1$，并为两个承诺 y_A 和 y_B 产生隐藏同一个秘密 $S_{A\to B}$ 的相等性证据 π，即 $\pi=(c,D,D_1,D_2)$，Alice 构造如下零知识证明：

$$PK\{S_{A\to B},r_{A_1},r_{B_1}:y_A=g_1^{S_{A\to B}}f_1^{r_{A_1}} \bmod p \wedge y_B=g_2^{S_{A\to B}}f_2^{r_{B_1}} \bmod p\} \tag{10}$$

Alice 将式(10)和相等性证据 π 发给全功能记账节点以进行验证。

(4)验证阶段。全功能记账节点收到 Alice 发来的交易验证请求后，结合相等性证据 π 和零知识证明式(10)对交易进行验证，即计算 c'。

$$c'=H(g_1^Df_1^{D_1}y_A^{-c} \bmod p\parallel g_2^Df_2^{D_1}y_B^{-c} \bmod p) \tag{11}$$

若 $c'=c$，则全功能记账节点返回 1 给交易双方，表示承诺 y_A 和 y_B 隐藏同一个秘密，即交易发起方 Alice 减少的金额与交易接收方 Bob 增加的金额一致，交易合法且接受此交易。否则，全功能记账节点返回 0 给交易双方，拒绝该笔交易。

(5)账本更新。利用椭圆曲线加同态算法直接对密文进行处理，即在不需要解密的情况下直接对密文账本进行更新，有效地提高了交易数据的安全性。密文账本的更新过程如下。

全功能记账节点利用椭圆曲线加同态算法，对交易发起者 Alice 的密文账本进行更新，把本次交易金额密文 $C_A'=(C'_{A1},C'_{A2})$作为要更新的内容，并与原余额密文账本 $C_A=(C_{A1},C_{A2})$做加同态运算，即：

$$\begin{aligned}C''_{A1}&=C_{A1}-C'_{A1}\\C''_{A2}&=C_{A2}-C'_{A2}\end{aligned} \tag{12}$$

在得到交易后，Alice 的余额密文 $C_A''=(C''_{A1},C''_{A2})$，该密文即为 Alice 更新后的密文账本，将该密文账本存储在本地数据库中。同理，对 Bob 的账本进行更新，得到交易后 Bob 的余额密文 $C_B''=(C''_{B1},C''_{B2})$，该密文即为 Bob 更新后的密文账本，将该密文账本存储在本地数据库中。

4　协议分析

4.1　协议正确性分析

定理 1　协议 1 能保证 y_A 和 y_B 是对同一笔交易金额 $S_{A\to B}$ 的承诺。

证明：由于 Alice 向记账节点出示了式(10)，使记账节点相信 $y_A=g_1^{S_{A\to B}}f_1^{r_{A_1}} \bmod p$ 和 $y_B=g_2^{S_{A\to B}}f_2^{r_{B_1}} \bmod p$，同时若承诺 y_A 和 y_B 不是对同一秘密 $S_{A\to B}$ 的承诺，则全功能记账节点执行 $c=H(g_1^Df_1^{D_1}y_A^{-c} \bmod p\parallel g_2^Df_2^{D_1}y_B^{-c} \bmod p)$时，有 $c'\neq c$，验证失败，拒绝本次交易。若 Alice 和 Bob 诚实地执行协议，则协议失败的概率是零知识证明式(10)失败的概率。由于零知识证明的协议是完备的，因此交易者诚实地执行式(10)就一定能通过验证。验证交易时，全功能记账节点总能得到正确的结果，即：

$$\Pr[\exists(S_{A\to B},r_{A_1}),(S'_{A\to B},r_{B_1}):S_{A\to B}\neq S'_{A\to B}\wedge y_A(S_{A\to B},r_{A_1})=y_B(S'_{A\to B},r_{B_1})]=0$$

$$\Pr[\exists(S_{A\to B},r_{A_1}),(S'_{A\to B},r_{B_1}):S_{A\to B}=S'_{A\to B}\wedge y_A(S_{A\to B},r_{A_1})=y_B(S'_{A\to B},r_{B_1})]=1$$

定理 2　协议 1 能保证 ECC 同态加密后的密文能被正确解密。

证明：更新交易者的账本时，利用 ECC 同态加密算法将 Alice 要更新的内容和原账本直接相加，得到更新后的密文

$C_A''=(C''_{A1},C''_{A2})$，将更新后的密文用私钥 k_A 解密，即：

$$\begin{aligned}C''_{A2}-k_AC''_{A1}&=\{(r_AK_A+P_A)-(r_A'K_A+P_{mA})\}-k_A(r_AG-r_A'G)\\&=r_AK_A+P_A-r_A'K_A-P_{mA}-k_Ar_AG+k_Ar_A'G\\&=r_AK_A+P_A-r_A'K_A-P_{mA}-r_AK_A+r_A'K_A\\&=P_A-P_{mA}\end{aligned}$$

对 P_A-P_{mA} 解密即可恢复明文信息。由解密后的明文可知，即使加密时使用的随机数不一样，对密文进行同态加密操作以后仍然可以被正确解密。

4.2 协议安全性分析

协议 1 的安全性主要以 ECC 同态加密算法和 PVC 数字承诺协议的安全性为基础，二者都是基于离散对数难题(ECCDLP)的。

定理 3 若 ECCDLP 是求解困难的，则协议 1 是安全协议。证明：本文中，椭圆曲线同态加密算法是基于 ECCDLP 求解困难，主要体现为不能由公钥 K 求出私钥 k。交易双方将金额加密后发给全功能记账节点，若全功能记账节点由交易双方公布的基点 G 和公钥 K 求解出私钥 k，这相当于它攻破了 ECDLP 难题。迄今为止，还没有发现在有效的多项式时间里能攻破椭圆曲线离散对数难题的研究，因此全功能记账节点无法通过密文获取交易双方的交易信息。

定理 4 验证者无法根据承诺和已知的参数获取秘密值。

证明：协议 1 在随机预言机模式下是基于离散对数困难性假设且是统计零知识证明的，验证者即使具有无限的计算能力也不能求解出相应的离散对数，也无法根据承诺和已知参数获取秘密值。验证者随机选取秘密值和随机数($S'_{A\to B}$，r'_{A_1})，若对于承诺 y_A 有两种不同的打开值，分别为($S_{A\to B}$，r_{A_1})和($S'_{A\to B}$，r'_{A_1})，于是有：

$$\begin{aligned}y_A&=(g_1)^{S_{A\to B}}(f_1)^{r_{A_1}}\bmod p\\&=(g_1)^{S'_{A\to B}}(f_1)^{r'_{A_1}}\bmod p\\\Rightarrow(f_1)^{r'_{A_1}-r_{A_1}}&=(g_1)^{S_{A\to B}-S'_{A\to B}}\bmod p\\\Rightarrow(f_1)&=(g_1)^{(S_{A\to B}-S'_{A\to B})/(r'_{A_1}-r_{A_1})}\bmod p\end{aligned}$$

以上说明式 $\log_{g_1}(f_1)$ 可以计算，这与离散对数困难问题相悖，因此，验证者无法根据承诺和已知参数猜测出承诺隐藏的秘密值。在多项式时间算法中，验证者根据获得的公开数据来求解离散对数大约需要 $O(\sqrt{p-1})$ 次运算(p 是大素数)，故验证者想要根据承诺求解秘密值是困难的，验证者不可能从证明中获取交易秘密信息。

4.3 协议性能分析

本文方案的复杂性主要与文献[17-18]中的方案进行对比分析，从协议复杂度、困难性假设、是否同态和运行时间入手。文献[17-18]基于 Paillier 加密算法结合零知识证明来解决交易保密验证问题，而本文基于椭圆曲线同态加密算法和零知识证明来解决交易保密验证和账本更新问题。文献[17-18]和本文的方案除了困难性假设相同外都使用了同态加密特性。文献[17]中的方案需要做 7 次加密运算和 2 次解密运算，而 Paillier 加密、解密运算的计算复杂度均为 $\log^3 p$，因此文献[17]中的方法的总计算开销为 $9\log^3 p$。文献[18]中的方案需要做 2 次加密运算和 1 次解密运算，根据 Paillier 算法的计算复杂度可知文献[18]中的方法的总计算开销为 $3\log^3 p$。在本文方案中，验证阶段需要做 1 次加密运算和 1 次解密运算，更新账本阶段需要做 4 次加密运算和 2 次同态加运算。由 $E_K(m_i)=(C_1,C_2)$ 可知，基于椭圆曲线同态加密算法加密一个明文会有两个密文分量产生，分量 C_1 的计算开销为 $6\log p$，分量 C_2 的计算开销为 $6(1+\log p)$，因此对 m_i 加密 1 次的总开销为 $6(1+2\log p)$，解密 1 次的计算开销为 $6(1+\log p)$，故本方案的总计算开销为 $36+66\log p$，而全功能记账节点只需要做 1 次同态计算。在忽略参数生成及密钥生成开销的情况下，具体的计算复杂性比较结果如表 2 所列。

表 2 本文方案与其他方案的性能对比

Table 2 Performance comparison

协议	计算复杂度	困难性假设	是否同态
文献[17]中的方案	$9\log^3 p$	离散对数	√
文献[18]中的方案	$3\log^3 p$	离散对数	√
本文方案	$36+66\log p$	离散对数	√

由表 2 可知，与文献[17-18]中的方案相比，本文提出的方案在计算复杂度方面具有相对的优势。

本文隐私保护方案的效率主要与文献[17-18]中的隐私保护方案的效率进行对比。由于本文的研究方案是完整的区块链交易流程，除了研究交易的保密验证外，还有密文账本的更新，而文献[17-18]只对交易的保密验证展开了研究，因此在效率对比时不再对账本的更新进行测试。为了方便比较，这里的密钥长度统一为 3072 bit。本文方案与文献[17-18]中的方案在相同密钥长度下交易保密验证算法的效率测试结果如表 3 所列。本次测试的环境如下：操作系统为 Windows7 旗舰版 64 bit，处理器为 Intel(R) Core(TM) i7-4770 CPU@3.40 GHz，内存为 8.0 GB。

表 3 相同密钥长度下的效率对比

Table 3 Comparison of efficiency under the same key length

协议	密钥长度/bit	时间/ms
文献[17]中的方案	3072	1548.36
文献[18]中的方案	3072	1900.26
本文方案	3072	844.56

由表 3 可知，与文献[17-18]中的方案相比，在同等密钥长度下，本文方案能在相对较短的时间内完成交易的保密验证。

结束语 本文基于椭圆曲线同态加密算法，结合公开可验证的承诺和零知识证明密码学技术，针对现有区块链交易存在的隐私泄露问题，提出了一种区块链交易金额保密验证的方案，该方案不仅能对交易者的密文账本进行实时更新，而且能在不泄露交易者隐私信息的情况下实现全网节点均可对交易进行保密验证。与现有的隐私保护方案相比，该方案具有高效、密钥短、安全性较强等优点。本文方案虽优于现有的一些隐私保护方案，但是其交易双方的通信量大，从而导致在实际应用中每完成一笔交易所耗费的时间较长，因此在性能方面还有待完善，另外在实际应用中可能还需考虑权威第三方在特殊情况下可对某段时间内提交的交易密文进行验证和追溯。

参 考 文 献

[1] YUAN Y,WANG F Y. Blockchain:The state of the art and future trends[J]. Acta Automatica Sinica,2016,42(4):481-494.

[2] HALPIN H,PIEKARSKA M. Introduction to Security and Privacy on the Blockchain[C]// 2017 IEEE European Symposium on Security and Privacy Workshops(EuroS&PW). IEEE,2017:1-3.

[3] CAO B,LIN L,LI Y,et al. Review of blockchain research[J]. Journal of Chongqing University of Posts and Telecommunications(Natural Science Edition),2020,32(1):1-14.

[4] XU C J,LI X F. Blockchain transaction data privacy protection method[J]. Computer Science,2019,47(3):281-286.

[5] FENG Q,HE D,ZEADALLY S,et al. A survey on privacy protection in blockchain system[J]. Journal of Network and Computer Applications,2019,126:45-58.

[6] LI X,MEI Y,GONG J,et al. A Blockchain Privacy Protection Scheme Based on Ring Signature[J]. IEEE Access,2020,8:76765-76772.

[7] SONG S,PENG W. BLOCCE+:An Improved Covert Communication Method Based on Blockchain[J]. Journal of Chongqing University of Technology(Natural Science),2020,34(9):238-244.

[8] GONG Y X,LV J K. A Kinds of Design of Data Storage System Based on Blockchain[J]. Journal of Chongqing University of Technology(Natural Science),2019,33(9):190-195.

[9] ZHU L H,GAO F,SHEN M,et al. Survey on Privacy Preserving Techniques for Blockchain Technology[J]. Computer Engineering and Application,2017,54(10):2170-2186.

[10] RIVEST R L,SHAMIR A,TAUMAN Y. How to leak a secret [C]// International Conference on the Theory and Application of Cryptology and Information Security. Berlin, Heidelberg: Springer,2001:552-565.

[11] GOLDWASSER S,MICALI S,RACKOFF C. The knowledge complexity of interactive proof systems[J]. SIAM Journal on Computing,1989,18(1):186-208.

[12] MIERS I,GARMAN C,GREEN M,et al. Zerocoin:Anonymous distributed e-cash from bitcoin[C]// 2013 IEEE Symposium on Security and Privacy. IEEE,2013:397-411.

[13] SASSON E B,CHIESA A,GARMAN C,et al. Zerocash:Decentralized anonymous payments from bitcoin[C]// 2014 IEEE Symposium on Security and Privacy. IEEE,2014:459-474.

[14] NOETHER S,MACKENZIE A. Ring confidential transactions [J]. Ledger,2016,1:1-18.

[15] YUAN C,XU M,SI X. Research on a new signature scheme on blockchain[J]. Security and Communication Networks,2017,2017:1-10.

[16] NARULA N,VASQUEZ W,VIRZA M. zkledger:Privacy-preserving auditing for distributed ledgers[C]// 15th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 18). 2018:65-80.

[17] LI G L,HE D B,GUO B,et al. Blockchain Privacy Protection Algorithm Based on Zero-knowledge Proof[J]. Journal of Huazhong University of Science and Technology(Natural Science Edition),2020,48(7):112-116.

[18] WANG Q,QIN B,HU J,et al. Preserving transaction privacy in bitcoin[J]. Future Generation Computer Systems,2017,8(26):793-804.

[19] HE Y Z,WU C K,FENG D G. Publicly Verifiable Zero-knowledge Watermark Detection[J]. Journal of Software,2005,16(9):1606-1616.

[20] RIVEST R L,ADLEMAN L,DERTOUZOS M L. On data banks and privacy homomorphisms[J]. Foundations of Secure Computation,1978,4(11):169-180.

[21] QIAN P,WU M,LIU Z. Homomorphic Encryption Privacy Protection Method towards Cloud Computing[J]. Small Micro-computer System,2015,36(4):840-844.

[22] PEDERSEN T P. Non-interactive and information-theoretic secure verifiable secret sharing[C]// Annual International Cryptology Conference. Berlin,Heidelberg:Springer,1991:129-140.

[23] DONG G S,CHEN Y X,FAN J,et al. Research on Privacy Protection Strategy in Blockchain Application[J]. Computer Science,2019,46(5):29-35.

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

ZHANG Xiao-yan, born in 1996, postgraduate. Her main research interests include information security and blockchain technology.

LI Qin-wei, born in 1961, professor, master supervisor. His main research interests include information security, blockchain and privacy protection.