doi:10.6041/j.issn.1000-1298.2023.05.038

面向猕猴桃产业链的联盟链隐私交易方案

景　旭　杨少坤
(西北农林科技大学信息工程学院,陕西杨凌 712100)

摘要:针对猕猴桃产业联盟链交易中金额与身份的双重隐私保护问题,提出一种基于 $^{+}$HomElG 零知识证明($^{+}$HomElG zero knowledge proof,$^{+}$HomElG－ZKProof)和 SM2 的猕猴桃产业联盟链隐私交易方案。首先,转账方利用 $^{+}$HomElG 加密交易金额后将其发送给接收方,接收方基于 SM2 签名确认交易后发送给转账方;其次,转账方基于 $^{+}$HomElG－ZKProof 对交易金额相关密文生成零知识证明证据,基于 SM2 可链接环签名对交易金额相关密文和交易双方身份分别生成环签名,与接收方 SM2 签名一起经系统层 Raft 共识打包上链;然后,由监管节点验证 SM2 签名、两次环签名及链接性后确认交易双方身份,用户节点间在应用层使用 PBFT 共识验证交易金额相关密文、环签名及交易金额相关零知识证明证据后确认交易的有效性;最后,由监管节点将有效交易区块编号经系统层 Raft 共识上链并更新账户余额。分析表明,该文方案具有抗篡改攻击、抗公钥替换攻击、抗假冒攻击以及匿名性,安全性较高;测试结果表明,该文方案可以实现猕猴桃产业联盟链用户交易金额、身份的双重隐私保护;在安全参数为 2 048 bit 时,交易时间为 4.495 s,可以满足猕猴桃产业联盟链交易的实际需要。

关键词:猕猴桃产业链;联盟链;隐私保护;$^{+}$HomElG 零知识证明;SM2
中图分类号:TP391　　**文献标识码**:A　　**文章编号**:1000-1298(2023)05-0369-10　　**OSID**:

Privacy Transaction Scheme of Consortium Blockchain for Kiwifruit Industry Chain

JING Xu　YANG Shaokun
(*College of Information Engineering*, *Northwest A&F University*, *Yangling*, *Shaanxi* 712100, *China*)

Abstract: To meet the privacy protection problem of amount and identity in kiwifruit industry consortium blockchain transactions, a kiwifruit industry chain privacy transaction scheme based on $^{+}$HomElG－ZKProof ($^{+}$HomElG zero knowledge proof) and SM2 was proposed. Firstly, the transaction amount with $^{+}$HomElG was encrypted and sent to the receiver by the transferor, and the signature based on the SM2 to confirm the transaction was generated and sent to the transferor by the receiver. Secondly, zero-knowledge proof evidences for the ciphertext related to the transaction amount based on $^{+}$HomElG－ZKProof, ring signatures for the ciphertext related to the amount and the identity of the transaction based on the SM2 linkable ring signature were generated, with the receiver's SM2 signature was packaged and uploaded to the consortium blockchain through the system layer Raft consensus by the transferor. Then the SM2 signature, the two ring signatures, and the link to confirm the transaction identity were verified by the supervisory node, the PBFT consensus at the application layer was used by verifying the ciphertext related to the transaction amount, ring signature and the zero-knowledge proof evidence related to the transaction amount to confirm the validity of the transaction by the user nodes. Finally, the valid transaction block number through the Raft consensus of the system layer was uploaded and the account balance was updated by the supervisory node. The analysis showed that the proposed scheme had the advantages of anti tamper attack, anti public key substitution attack, anti counterfeiting attack and anonymity, and had higher security. The test results showed that the scheme can realize double privacy protection of transaction amount and identity of users in the kiwifruit industry consortium blockchain. The experimental results showed that when the security parameter was 2 048 bit, the transaction time took about 4.495 s, it can meet the actual needs of kiwifruit industry consortium blockchain transactions.

Key words: kiwifruit industry chain; consortium blockchain; privacy protection; $^{+}$HomElG－ZKProof; SM2

收稿日期:2022－08－16　修回日期:2022－09－21
基金项目:国家重点研发计划项目(2020YFD1100601)、陕西省重点研发计划项目(2021NY－179、2019ZDLNY07－02－01)和上合组织成员国农业技术集成示范与标准化研究项目
作者简介:景旭(1971—),男,副教授,主要从事农业信息化、区块链技术和隐私保护研究,E-mail:jingxu@nwsuaf.edu.cn

0 引言

联盟链由多个机构联盟构成,由联盟指定的成员生成、共识、维护联盟链账本,节点的进入与退出需要满足一定条件并得到许可[1],具有灵活的智能合约定制机制,可以快速处理事务以及可追溯、不可篡改等特性[2],天然满足产业链中各生产环节之间通过交易形成的供应链特性。猕猴桃产业链是以追求高品质、低成本的猕猴桃生产为目的,以地方龙头企业为核心,以资本为纽带,上下游相关企业相互连接形成的链条,可以使相关企业之间利益共享、风险共担,促进企业相互合作以及地方企业由单体优势转化为区域特色产业优势,形成整体核心竞争力[3]。目前,基于联盟链农产品产业链研究大多以质量溯源为主[4-6],尚无关于猕猴桃产业联盟链隐私转账交易的相关研究。在实际应用中,联盟用户企业为了维护自身利益,并不希望其它用户企业通过链上公开的交易数据获取交易金额或确定其身份[7],因此,在保证产业链环境中实现联盟用户企业隐私保护逐渐成为联盟链应用的重要挑战之一。

国内外学者已经开展了一些相关研究[8-13]。这些研究中存在以下问题:现有方案中大多没有采用国密算法,不利于我国建设行业网络安全环境及行业信息系统的安全、自主、可控;没有同时实现交易金额与身份的双重隐私保护;Paillier 零知识证明效率较低。

国家密码管理局在 2010 年发布了 SM2 椭圆曲线公钥密码算法[14],2016 年将其正式发布为中国国家密码标准(GB/T 32918—2016)[15]。与基于有限域上困难问题的数字签名算法相比,在相同的安全强度下,SM2 数字签名具有存储空间小、签名速度快的优势。在基于 SM2 可链接环签名方案[16]中,签名者随机选取无关地址连同签名者构成签名集进行环签名,将真正签名者隐藏到签名集中,在签名集其他成员无感知情况下实现身份匿名,环签名的可链接性可用于帮助追溯签名者身份,可以很好地契合联盟链交易中匿名和可追溯的需求。与常用的加同态 Paillier 算法相比,在相同的安全级别下,$^{+}$HomElG 加同态算法[17]获得了接近 86.7% 的加密加速比和接近 73.4% 的解密加速比。$^{+}$HomElG 零知识证明($^{+}$HomElG zero knowledge proof,$^{+}$HomElG-ZKProof)[18]是基于$^{+}$HomElG 算法,面向联盟链交易的一种非交互式零知识证明,可以在密文状态下验证交易双方交易金额相等、交易金额大于零、交易余额不小于零。

本文面向猕猴桃产业链提出一种基于$^{+}$HomElG-ZKProof 和SM2 的联盟链隐私交易方案。方案以猕猴桃产业链相关企业作为用户节点,猕猴桃产业链协会作为监管节点,用户节点之间产生交易,监管节点在交易过程中确认交易双方身份,其他用户节点共识交易的有效性;转账方基于 SM2 和$^{+}$HomElG-ZKProof 生成机密交易信息,经系统层 Raft 共识后打包上链,由监管节点验证两次环签名及链接性确认交易双方身份;用户节点间在应用层使用 PBFT 共识验证环签名及交易金额相关零知识证明确认交易的有效性。

1 预备知识

1.1 $^{+}$HomElG 同态加密

$^{+}$HomElG 算法[17]包含 4 个过程,具体如下:

(1)密钥生成算法

以安全参数 k 为输入,选择两个素数 p 和 p_0,使得对于大素数 q 有 $p=2q+1$,对于小素数 t 和正整数 κ 有 $p_0=2t^{\kappa}+1<p$;选择两个生成元 g 和 g_0,使 g 生成一个 q 阶群 Z_p^*,g_0 生成群 $Z_{p_0}^*$;从 Z_q(Z_p^* 的一个子群)中随机选择一个私钥 x,并计算相应的公钥 $y=g^x \bmod p$;输出系统公共参数(p,q,p_0,g,g_0),返回公私钥对(y,x)。

(2)加密过程

明文空间 $M=\{0,1,\cdots,\lfloor \mathrm{lb}p \rfloor\}$,密文空间$C_p=Z_p^* Z_p^*$。

对于明文 $m\in M$,随机选择 $r\in Z_q$,加密过程为 $c_1=g^r \bmod p$,$c_2=y^r 2^m \bmod p$,得到加密后密文 $C(c_1,c_2)$。

(3)解密过程

对于密文 $C=(c_1,c_2)$,解密过程为 $m=\mathrm{lb}(c_2/c_1^x \bmod p)$。

(4)同态运算

对于给定的明文 m_1、m_2,满足 $m_1,m_2,m_1+m_2\in M$,m_1+m_2 的有效密文表示为 $C(y,m_1)\circ C(y,m_2)=(g^{r_1},y^{r_1}2^{m_1})\circ(g^{r_2},y^{r_2}2^{m_2})=(g^{r_1+r_2},y^{r_1+r_2}2^{m_1+m_2})$。

1.2 零知识证明

(1) 相等性证明

证明者[18]使用交易双方的公钥和系统参数,选择加密过程中的随机数 $r_{0vA}\in Z_q$ 和 $r_{0vB}\in Z_q$,加密交易金额 v 得到密文 $C_{vA}=(c_{1vA},c_{2vA})$、$C_{vB}=(c_{1vB},c_{2vB})$。证明者顺序执行 $v'\xleftarrow{\$}M$,$r_x$、$r'_{0vB}\xleftarrow{\$}Z_q$、$(e_1,f_1)=(g^{r_x},2^{v'}c_{1vA}^{r_x})$、$(e_2,f_2)=(g^{r'_{0vB}},2^{v'}y_B^{r'_{0vB}})$、$\eta=H(c_{1vA},c_{2vA},c_{1vB},c_{2vB},e_1,f_1,e_2,f_2)$后,将$(e_1,f_1,e_2,f_2,Z_v,Z_x,Z_{r_1},\eta)$发送给验证者;验证者验证等式 $\eta=H(c_{1vA},c_{2vA},c_{1vB},c_{2vB},e_1,f_1,e_2,f_2)$,$H$ 表示安全哈希函数,防

止证明者作假，通过后，若等式 $g^{Z_x} \bmod p = y_A^{\eta} e_1 \bmod p$、$2^{Z_v} C_{1vA}^{Z_x} \bmod p = c_{1vA}^{\eta} f_1 \bmod p$、$g^{Z_{r1}} \bmod p = c_{1vB}^{\eta} e_2 \bmod p$、$2^{Z_v} y_B^{Z_{r1}} \bmod p = c_{2vB}^{\eta} f_2 \bmod p$ 均成立则相信密文 C_{vA}、C_{vB} 中隐藏着同一秘密值。

（2）范围证明

Bulletproofs[19] 是最常用的范围零知识证明方法之一，要求有一个离散对数（Discrete logarithm，DL）关系未知的公开承诺密钥 (g,h)。使用相等性证明可将 $^{+}$HomElG 加密后的密文 $C=(c_1,c_2)$ 归约为全局公钥 (g,h) 下的 Pedersen 承诺。根据可证明安全理论，基于 Bulletproofs 证明 Pedersen 承诺的秘密值满足范围证明，从而证明密文 $C=(c_1,c_2)$ 中隐藏的秘密值满足范围证明。

1.3　可链接环签名

文献[20]首次提出环签名的概念，将签名者隐藏到多用户构成的环中，实现签名者的身份隐私。根据不同属性特征，环签名可分为可链接环签名[21]、可否认的环签名[22]、门限环签名[23]、可撤销匿名性环签名[24]等。可链接环签名因可以实现同一签名者所生成签名的链接，而得到了较为广泛的应用。

文献[16]提出基于 SM2 数字签名算法的可链接环签名方案，以环签名概念为基础，基于 SM2 数字签名算法，通过嵌入安全的签名标签，实现了可链接的环签名方案。主要包括 5 个算法：系统初始化算法、密钥生成算法、可链接环签名生成算法、可链接环签名验证算法、链接算法。

1.4　半诚实模型

半诚实模型[25]又称诚实但好奇模型或被动攻击模型，协议参与方均严格执行协议的规程，中途不会强行退出或恶意掺假，但某一参与方可能会保留所有能搜集到的另一方信息，并在协议执行后试图利用这些信息获得更多其他参与者的隐私信息。

2　基于 $^{+}$HomElG－ZKProof 和 SM2 的联盟链隐私交易方案

2.1　基于联盟链的猕猴桃产业链交易架构

猕猴桃产业链一般包含农资供应、田间生产、企业加工和产品销售等环节，由农资电商、农业合作社、加工企业、电商平台等单元承担对应的环节，每个单元又可能包含众多企业实体。产业链的企业实体间在现实中既存在竞争关系，也有一定合作信任关系，构成天然的联盟组织链条[26]。猕猴桃产业链企业实体在交易时，希望交易公开可追溯，但为了维护自身利益可能不希望竞争对手知道交易金额以及交易双方的身份。因此，设计了基于联盟链的猕猴桃产业链交易架构，如图 1 所示。

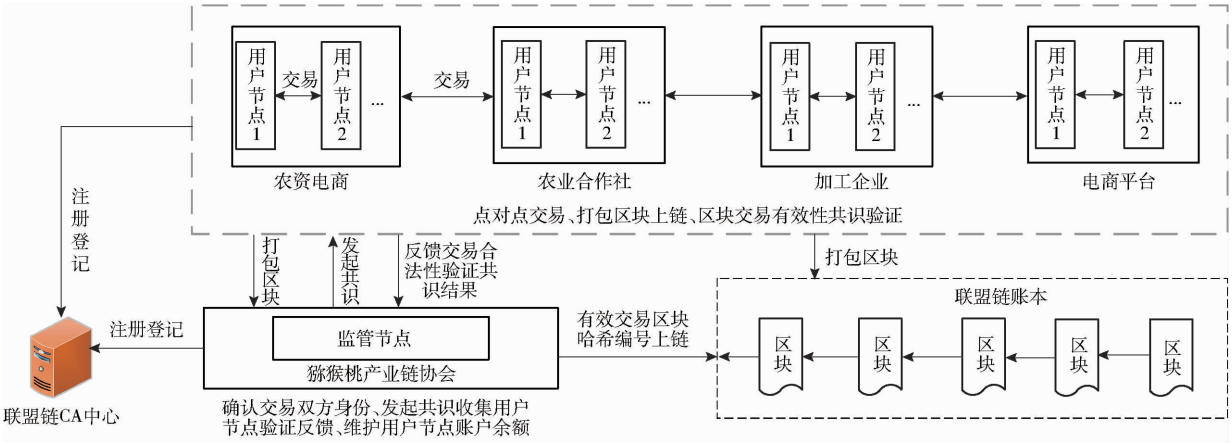


图 1　基于联盟链的猕猴桃产业链交易架构

Fig. 1　Transaction structure diagram of kiwifruit industry chain based on consortium blockchain

在图 1 中，以不参与联盟链具体交易的猕猴桃产业链协会作为监管节点，以产业链各环节不同的企业实体作为用户节点，在用户节点间发生交易，监管节点和用户节点均向联盟链 CA 中心登记注册，由 CA 中心生成并颁布节点证书。系统初始化时，用户节点将其受猕猴桃产业链协会监管的账户余额加密后，发送给监管节点，监管节点在本地数据库存储用户节点的账户余额密文。作为猕猴桃产业链协会的监管节点是半诚实的，联盟链交易在用户节点间匿名，对监管节点不匿名，但交易过程中监管节点无法得知具体的交易金额。当用户节点间发生交易时，转账方用户节点利用 SM2 签名、SM2 环签名、同态加密、$^{+}$HomElG－ZKProof 等技术生成机密交易信息并经系统层 Raft 共识打包上链；监管节点在验证交易双方身份通过后，向其他用户节点发起交易有效性验证；由其他用户节点在应用层使用 PBFT 共识算法[27]验证区块交易有效性并向监管节点反馈共识结果；监管节点收到共识反馈结果为验证通过

(有效交易)后,将交易双方交易余额密文经监管节点公钥加密后和区块哈希编号一起经系统层 Raft 共识打包上链,更新本地数据库中交易双方的账户余额密文,交易完成。

2.2 交易协议

2.2.1 初始化

(1)系统参数生成

由联盟链 CA 中心根据$^+$HomElG 算法的参数生成算法,输入安全参数 κ,生成系统公共参数 Bparams;根据基于 SM2 可链接环签名算法的系统初始化算法,输入安全参数 λ,生成系统公共参数 Aparams;将 Bparams 和 Aparams 写入 CA 中心的证书,其中,Bparams 用于用户节点的账户余额加解密和生成交易相关零知识证明证据,Aparams 用于用户节点账户地址的加解密以及生成和验证签名和环签名。通过 CA 中心证书公开发布,实现 CA 中心公钥及系统公共参数的分发。

(2)节点密钥生成与分发

用户节点通过 CA 中心的证书获得系统公共参数,根据 Bparams 生成自身账户公私钥对(sk,h),根据 Aparams 生成自身地址公私钥对(x,y)。以安全的方式将用户节点的账户公钥 h、地址公钥 y 提交给 CA 中心。CA 中心将用户节点的账户公钥 h、地址公钥 y 写入用户节点的证书,实现公钥的安全分发。账户私钥 sk、地址私钥 x 由用户节点安全保存。

监管节点只需生成地址公私钥对(x_S,y_S),管理方式与用户节点相似。

(3)用户节点账户初始化

联盟链用户节点分别使用其账户公钥加密自身受猕猴桃产业链协会监管的账户余额,发送给监管节点。监管节点以用户节点的地址公钥作为联盟链用户节点身份,在本地数据库中存储用户节点的账户余额密文。

2.2.2 交易协议过程

本方案基于$^+$HomElG - ZKProof 实现交易金额的隐私,基于环签名实现用户节点之间的身份隐私。用户节点之间发生交易,交易对监管节点不匿名,监管节点负责确认交易双方身份、发起交易有效性共识验证以及维护双方交易余额密文,用户节点在应用层经 PBFT 算法共识交易有效性,交易协议过程如图 2 所示。

(1)符号说明

符号说明如表 1 所示。

(2)转账方发起交易

假设联盟链用户节点 Alice 因订单编号为 OrderNum 的订单需要向 Bob 支付的交易金额为 m。Alice 通过 CA_{Bob} 获得 Bob 的账户公钥 h_B,使用$^+$HomElG 算法加密交易金额 m 得到 $BEnc_B(m)$,公式为 $BEnc_B(m)=(g^r,2^m h_B^r)$;将 $BEnc_B(m)$ 和 OrderNum 发送给 Bob 确认,如图 2 中步骤①所示。

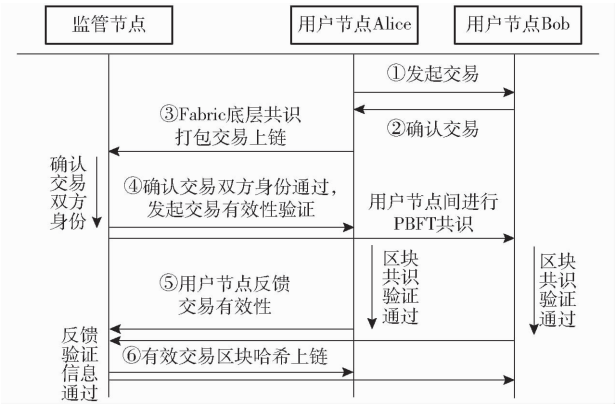


图 2 交易协议过程

Fig. 2 Transaction agreement process

表 1 符号说明

Tab. 1 Description of symbols

符号	含意
G	SM2 椭圆曲线算法的基点
H	安全哈希函数
$BEnc(\ )$	使用账户公钥加密($^+$HomElG 算法加密)
$AEnc(\ )$	使用地址公钥加密(SM2 算法加密)
$OrderNum$	订单编号
$Sign(\ )$	使用 SM2 数字签名算法进行签名
$EP(m)$	交易双方交易金额相等的零知识证明证据
$RP(m)$	交易金额大于零的零知识证明证据
$RP(b)$	转账方交易余额大于零的零知识证明证据
Q	SM2 可链接环签名的链接标签
L	SM2 可链接环签名的环成员
$\sigma(a)$	消息 a 的 SM2 可链接环签名

(3)接收方确认交易

Bob 接收到 $BEnc_B(m)$ 和 OrderNum 后,使用账户私钥 sk_B 解密 $BEnc_B(m)$,确认双方交易金额;交易金额确认后,Bob 查询自己的账户余额密文,经同态计算后,得到交易后账户余额密文 $BEnc_B(b)$,即 $BEnc_B(b)=BEnc_B(b')\circ BEnc_B(m)$;Bob 用地址私钥 x_B 对 $BEnc_B(m)\parallel BEnc_B(b)\parallel OrderNum\parallel y_A$ 签名,将签名 $Sign_B(BEnc_B(m)\parallel BEnc_B(b)\parallel OrderNum\parallel y_A)$ 发送给 Alice,如图 2 中步骤②所示。

(4)转账方提交交易

Alice 使用账户公钥 h_A 加密交易金额得到 $BEnc_A(m)$,即 $BEnc_A(m)=(g^r,2^m h_A^r)$;通过$^+$HomElG同态运算得到交易余额密文 $BEnc_A(b)$,即 $BEnc_A(b)=BEnc_A(b')\circ BEnc_A(m)^{-1}$;根据 $BEnc_A(m)$和$BEnc_B(m)$生成交易双方交易金额相等

的零知识证明证据 $EP(m)$，根据$BEnc_A(m)$生成交易金额大于零的零知识证明证据 $RP(m)$，根据 $BEnc_A(b)$生成转账方交易余额不小于零的零知识证明证据 $RP(b)$；随机选取其他用户节点的地址公钥，结合自身地址公私钥对，对消息 $BEnc_A(m)$、$BEnc_B(m)$、$BEnc_A(b)$使用 $L=\{y_1,y_2,\cdots,y_n\}$ 和 x_A 生成可链接环签名 $Q,\sigma(a)=(c_1,s_1,s_2,\cdots,s_n)$；得到最终交易金额相关信息为 $BEnc_B(m)\parallel BEnc_A(m)\parallel BEnc_A(b)\parallel L\parallel Q\parallel\sigma(a)\parallel EP(m)\parallel RP(m)\parallel RP(b)$。

Alice 对 y_A、y_B、OrderNum 和 $Sign_B(BEnc_B(m)\parallel BEnc_B(b)\parallel OrderNum\parallel y_A)$使用相同环成员再次生成可链接环签名 $Q',\sigma(a')=(c_1',s_1',s_2',\cdots,s_n')$；通过 CAs 获得监管节点的公钥 y_S 分别加密 y_A、y_B、Q' 以及 OrderNum，与再次生成的可链接环签名$\sigma(a')$、接收自 Bob 的签名 $Sign_B()$一起构成了此次交易的身份证明相关信息，即 $AEnc_S(y_A)\parallel AEnc_S(y_B)\parallel AEnc_S(Q')\parallel AEnc_S(OrderNum)\parallel\sigma(a')\parallel Sign_B()$。

Alice 将交易金额相关信息和身份证明相关信息经系统层 Raft 共识后打包成区块上链，如图 2 中步骤③所示。

(5)监管节点确认交易双方身份

监管节点在联盟链上获取用户节点 Alice 提交的交易信息后，首先，使用私钥 x_s 解密 $AEnc_S(y_A)\parallel AEnc_S(y_B)\parallel AEnc_S(Q')\parallel AEnc_S(OrderNum)$；其次，对交易金额相关信息和身份证明相关信息中的环签名进行验证和链接验证，通过后查询本地数据库中 Alice 的账户余额密文，并与交易金额相关信息中的交易金额密文进行同态运算，得到结果与交易金额相关信息中的账户余额密文进行比较，若相等，则 Alice 身份确认；然后，通过后查询本地数据库中 Bob 的账户余额密文 $BEnc_B(b')$，并与交易金额相关信息中的交易金额密文 $BEnc_B(m)$进行同态运算得到 $BEnc_B(b)$，利用 y_A、y_B、$BEnc_B(m)$、$BEnc_B(b)$以及 OrderNum 对 Bob 确认交易的签名 $Sign_B(BEnc_B(m)\parallel BEnc_B(b)\parallel OrderNum\parallel y_A)$进行验证，若通过，Bob 身份确认；最后，由监管节点发起交易有效性共识验证并等待用户节点反馈，如图 2 中步骤④所示。

(6)用户节点共识交易有效性

用户节点根据新生区块中交易双方的交易金额密文 $BEnc_B(m)\parallel BEnc_A(m)$和交易金额相等的零知识证明证据$EP(m)$验证交易金额相等；根据 $BEnc_A(m)$和交易金额大于零的零知识证明证据 $RP(m)$验证交易金额大于零；根据转账方交易余额 $BEnc_A(b)$和交易余额不小于零的零知识证明证据 $RP(b)$验证转账方交易余额不小于零；根据 L 和 $\sigma(a)$验证环签名。用户节点之间利用 PBFT 共识算法对交易有效性验证结果进行共识，向监管节点反馈验证交易有效性共识结果，如图 2 中步骤⑤所示。

(7)更新账本

当监管节点至少收到 $2f+1$(f 为系统允许最大拜占庭节点数)个用户节点发送的交易有效性共识验证结果为通过的反馈信息后，将交易双方交易余额密文经监管节点公钥加密后和区块哈希编号一起经系统层 Raft 共识后打包上链，更新监管节点本地数据库中 Alice 和 Bob 的账户余额密文，如图 2 中步骤⑥所示，交易结束。

当交易发生纠纷需要追责时，所有用户节点均可对区块信息进行溯源；当追溯到某一交易时，由监管节点负责解密身份证明信息中的相关密文，得到可以证明交易双方身份的信息 $y_A\parallel y_B\parallel OrderNum\parallel Q'\parallel BEnc_B(b)$；纠纷各方均可根据此信息对区块中的交易金额信息和身份证明信息中的环签名进行验证和链接验证，对身份证明信息中 Bob 的签名进行验证，确定交易双方的身份，完成追责。

2.3　方案分析

本文方案由用户节点经系统层 Raft 共识将交易信息打包上链，监管节点通过链上信息确认交易双方身份通过后，在应用层向用户节点发起 PBFT 共识请求；当用户节点共识交易有效性后，向监管节点反馈共识结果；当监管节点至少收到 $2f+1$ 个用户节点反馈的共识验证结果为通过时，将交易双方交易余额密文经监管节点公钥加密后和区块哈希编号一起经系统层 Raft 共识后打包上链，更新本地数据库中交易双方的账户余额密文。

2.3.1　安全性分析

本文方案基于 $^+$HomElG－ZKProof、SM2 椭圆曲线算法(SM2 加解密、SM2 数字签名、SM2 可链接环签名)。$^+$HomElG－ZKProof 中的 $^+$HomElG 同态加密算法基于离散对数困难问题，在私钥未知条件下，攻击者从密文推测出明文是困难的。SM2 椭圆曲线算法基于椭圆曲线上的离散对数困难问题，加解密算法在私钥未知条件下，攻击者从密文推测出明文是困难的；SM2 数字签名算法具有正确性、独特性、可验证性和不可伪造性；SM2 可链接环签名算法具有正确性、不可伪造性、无条件匿名性以及可链接性。

(1)篡改攻击

本文方案由 Alice 向 Bob 发起交易。Alice 如果在交易发起时篡改了交易金额，Bob 在确认交易时

解密 Alice 发送的交易金额后就会发现交易金额被篡改;Alice 如果在交易提交时篡改了自己账户公钥加密的交易金额或者自己的交易余额,监管节点在确认 Alice 身份时,会查询本地数据库中 Alice 的账户余额,通过同态计算得到交易余额密文,再与 Alice 提交的交易余额密文比对会失败,确认 Alice 的身份失败;Alice 如果在交易提交时同时篡改自己账户公钥加密的交易金额和自己的交易余额,虽然监管节点会确认身份通过,但用户节点根据零知识证明在验证交易双方交易金额相等时,将无法通过;监管节点是半诚实的,不会篡改交易双方的账户余额密文,且链上数据包含交易双方对自己交易余额密文的签名,假如监管节点篡改交易双方交易余额,该攻击依然可以被发现。因此,本文方案可以抵抗篡改攻击。

(2)公钥替换攻击

公钥替换攻击,即攻击者用自己选定的假公钥替换公钥目录中真实的公钥,当用户使用假公钥加密一个消息时,攻击者就可以截获消息并正确解密。

本文方案选取的 CA 身份认证服务依赖于 PKI(Public key infrastructure)体系,联盟链中的任何成员都可以验证 CA 证书的合法性来认证公钥,因此攻击者无法实施公钥替换。因此,本文方案可有效抵抗公钥替换攻击。

(3)假冒攻击

对于本文方案的签名算法,当攻击者截获 Alice 交易发起阶段向 Bob 发送的信息,可能伪造签名消息假冒 Bob 向 Alice 发送确认交易的虚假签名,监管节点在确认接收方身份时,会使用 Bob 的地址公钥验证 Bob 确认交易的签名,伪造签名消息的验证将不会通过;当攻击者截获 Alice 向监管节点发送的交易提交信息,伪造关于接收方的相关信息,假冒 Alice 向监管节点提交交易,若攻击者将接收方信息完全修改,监管节点确认交易双方身份可能会通过,但由于交易金额是密文,攻击者直接猜中交易金额可规约为离散对数困难问题,在用户节点共识交易有效性,对双方交易金额相等进行验证时,将不会通过。因此,本文方案可抵抗假冒攻击。

2.3.2 匿名性分析

本文方案在用户节点之间发生交易,由监管节点确认交易双方身份和维护用户节点的账户余额密文,因此,交易对于用户节点是匿名的,对于监管节点不匿名。交易发起节点 Alice 将交易金额相关信息和身份证明等相关信息打包生成新生区块,在监管节点确认交易双方身份后,由用户节点共识交易有效性。身份证明相关信息中的 $AEnc_S(y_A) \parallel AEnc_S(y_B) \parallel AEnc_S(Q') \parallel AEnc_S(OrderNum)$ 是经监管节点公钥加密后的密文,用户节点无法从身份证明相关信息获取交易双方身份的有用信息;由于用户节点无法得知身份证明相关信息中 Bob 确认交易签名 $Sign_B(BEnc_B(m) \parallel BEnc_B(b) \parallel OrderNum \parallel y_A)$ 中的消息,无法获取交易双方身份的有用信息;同理,用户节点无法得知 $\sigma(a')$ 中的消息无法验证 $\sigma(a')$,同样无法获取交易双方身份的有用信息。在交易金额相关信息中,用户节点可以验证信息中的环签名,可以确定转账方为环中成员,但无法确定具体成员;信息中的交易金额、交易余额均为经 $^{+}$HomElG 加密后的密文,确保了交易金额的隐私,由于交易余额密文随着交易在不断动态变化,用户节点无法根据信息中的账户余额密文推断转账方的身份。因此,本文方案可以在用户节点间实现匿名交易。

2.3.3 共识分析

Raft 共识属于强领导者型共识机制,即使在节点规模扩大的情况下仍能保持算法的高共识效率,但不具备拜占庭容错能力。PBFT 共识算法提供 $(n-1)/3$(n 是系统参与共识的节点数)的拜占庭容错性,但是 $O(n^2)$ 消息复杂度使得随着节点的增加,交易性能大幅下降。联盟链应用中的共识机制需要兼顾高效、安全与可拓展性,尤其是在大规模网络环境下仍需保持高吞吐量和低时延。

在本项目整体研究中,对于一般业务采用 Fabric 联盟链系统自带的崩溃容错共识算法[28-29],以提高系统的性能。作为整体研究的一部分,本文方案在系统层仍然使用 Fabric 联盟链自带的 Raft 共识。但本文主要研究用户之间的资金交易信息,属于需要公开验证的敏感业务,因此,在应用层添加了能够抵抗拜占庭问题的 PBFT 共识,即本文方案使用 Fabric 底层 Raft 共识将相关交易信息打包上链,在应用层使用 PBFT 共识由用户节点公开验证交易有效性。

相比于独立采用系统层 Raft 共识,本文双共识方案虽然弱化了部分性能,但提高了敏感业务的安全性,实现了交易金额和交易身份的双重隐私保护。相对于独立采用系统层 PBFT 共识,本文方案从项目总体上提高了系统整体性能,特别是当敏感业务在总体业务中占比较少的时候,使得系统的总体性能接近于独立采用 Raft 共识。因此,在平衡系统性能和安全性基础上,本研究采用了系统层 Raft 共识和应用层 PBFT 的双共识方案。

3　测试与分析

3.1　测试环境

（1）系统环境：Ubuntu 虚拟机 18.04，8 GB 内存，50 GB 存储磁盘，处理器内核总数为 4，带宽为 1 000 Mb/s。

（2）联盟链网络：使用 Hyperledger Fabric 1.4.0 搭建；部署 NZ.itcast.cn、HZS.itcast.cn、JGC.itcast.cn、DS.itcast.cn 等 4 个组织，每个组织部署节点 peer0、peer1、peer2 充当记账节点，部署 4 个 Orderer 节点作为排序节点，部署节点 SV.itcast.cn 为监管节点；系统层共识采用 Raft；状态数据库采用 levelDB；区块的最大交易数为 10 笔，最大打包时间间隔为 2 s，最大字节为 10 MB。

（3）初始化：系统初始化过程中，CA 中心选择合适的安全参数生成系统公共参数后，写入 CA 中心证书；用户节点及监管节点选取合适的私钥生成公钥，将公钥发送给 CA 中心生成各节点证书；账户初始化过程中，各用户节点将自身账户余额使用自身账户公钥经 $^+$HomElG 加密后，发送给监管节点。

（4）应用层共识：采用 corgi-kx 的 PBFT 算法（https://github.com/corgikx/blockchain_consensus_algorithm，2019－12－01），由 12 个用户节点共识验证，最大拜占庭节点数 f 为 3 个。

（5）环签名：环签名集公钥个数 12 个。

3.2　功能测试

联盟链用户 Alice（加工厂用户节点）向联盟链用户 Bob（合作社用户节点）购买了 16 t 中华猕猴桃，Alice 因订单 O14271375ffe71bf86b4（订单生成过程详见文献[28]）需向 Bob 转账 40 万元，订单如图 3 所示。

图 3　订单详情

Fig. 3　Transaction order details

订单 O14271375ffe71bf86b4 的交易流程如下：

（1）转账方 Alice 向 Bob 发起交易，Alice 使用 Bob 的账户公钥加密交易金额，将交易金额密文以及订单号 OrderNum 发送给 Bob，如图 4 所示。

图 4　发起交易

Fig. 4　Initiate transaction

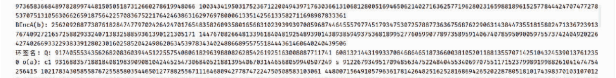
（2）Bob 使用其账户私钥解密确认交易金额通过后，查询其账户余额密文并计算交易后的账户余额，基于 SM2 对 $BEnc_B(m)$、$BEnc_B(b)$、y_A 和 OrderNum 签名，将签名发送给 Alice，如图 5 所示。

图 5　确认交易

Fig. 5　Confirm transaction

（3）Alice 收到交易金额信息后，首先，生成交易金额相关密文及环签名，如图 6a 所示；其次，生成交易金额相关零知识证明过程，如图 6b 所示；然后，生成交易的身份证明相关信息，如图 6c 所示；最后，经系统层 Raft 共识后打包交易上链，如图 6d 所示。

（a）生成交易金额相关密文及环签名



（b）生成交易金额相关零知识证明

（c）生成交易的身份证明相关信息

（d）打包区块信息

图 6　生成交易信息并打包上链

Fig. 6　Generate transaction information and package it on consortium blockchain

（4）监管节点从链上“8ce9741829cd82b5759b338be842fda4ec9999d983a23f395a27b1198e4196f6”获取 Alice 交易信息，如图 7a 所示；监管节点确认交易双方身份通过后，向用户节点发起相关的验证共识验证，等待用户节点反馈，如图 7b 所示。

（5）用户节点根据零知识证明过程和环签名验证交易的有效性，使用 PBFT 算法达成共识，向监管节点反馈共识结果。用户节点验证交易有效性时包

(a) 获取交易信息

(b) 确认交易双方身份

图 7 监管节点确认交易并发起共识验证

Fig. 7 Confirm transaction and initiate consensus verification

括 4 个部分,分别为 VerifyEp(m)(交易双方交易金额相等验证)、VerifyRp(m)(交易金额大于零验证)、VerifyRp(b)(交易余额不小于零验证)以及环签名验证。每个部分验证通过返回 1,验证失败返回 0。用户节点间在应用层使用 PBFT 共识算法共识交易的有效性并向监管节点反馈共识结果,如图 8 所示。

图 8 共识验证区块

Fig. 8 Consensus verification block

(6)当监管节点至少收到 $2f+1$ 个($f=3$)用户节点发送的反馈共识结果为“1111”时,该区块交易有效,将交易双方交易余额密文经监管节点公钥加密后和区块哈希编号一起经系统层 Raft 共识后打包上链,更新本地数据库中交易双方的账户余额密文,完成交易,如图 9 所示。

图 9 有效交易区块哈希编号上链

Fig. 9 Valid transaction block Hash number on chain

3.3 方案效率分析

本文方案中将交易分为发起交易、确认交易、提交交易、生成区块、确认交易双方身份以及确认交易有效性等阶段,使用不同的安全参数 κ 测试各个阶段的效率,如表 2 所示。

表 2 不同安全参数交易各阶段效率

Tab. 2 Efficiency in different stages of transaction with different security parameters

安全参数大小/bit	发起交易时间/ms	确认交易时间/ms	提交交易时间/ms	生成区块时间/s	确认身份时间/ms	PBFT 共识时间/ms
1 024	2.3	2.1	190.0	4	113.9	161.1
2 048	2.7	2.2	208.2	4	115.6	166.5
4 096	5.1	2.4	217.5	4	119.4	190.9
8 192	15.2	2.6	265.4	4	122.9	322.1
16 384	45.3	2.9	367.6	4	128.8	743.6

为了降低实验偶然性,表 2 中数据均为 50 次测试的平均值。安全参数 κ 越大,表明方案安全性越高。由表 2 可以看出,随着安全参数 κ 的增大,方案各阶段除新生区块生成外,效率都会降低,但总体交易时间均在毫秒级,可根据具体情况选择合适的安全参数,一般情况下设置 κ 为 2 048 bit,交易时间为 4.495 s,可以满足猕猴桃产业联盟链交易的实际需要。

3.4 方案特性分析

文献[8]面向联盟链使用 SM9 算法和群签名技术实现了身份匿名,但未实现交易金额的隐私保护;文献[9]和文献[10]面向联盟链使用同态加密和零知识证明技术实现了交易金额的隐私保护,但未实现身份匿名;文献[11]使用环签名和 Pedersen 承诺实现了全匿名,但因切断了交易关联性导致可追溯性较差;文献[12]使用聚合签名实现了全匿名,但面向比特币基于交易的区块链模型,不适用于联盟链。本文方案与其它相关研究的特性对比如表 3 所示。

表 3 本文方案与其它方案的特性对比

Tab. 3 Feature comparison

方案	交易金额隐私	身份隐私	可追溯性	数据模型	应用范围
文献[8]	No	Yes	Yes	UTXO	联盟链
文献[9]	Yes	No	Yes	账户模型	联盟链
文献[10]	Yes	No	Yes	账户模型	联盟链
文献[11]	Yes	Yes	No	UTXO	公有链
文献[12]	Yes	Yes	Yes	UTXO	公有链
本文	Yes	Yes	Yes	账户模型	联盟链

由表 3 可以看出,相较于只实现单一隐私方向的方案,本文方案提升了对用户以及交易整体的隐私保护程度,满足了面向猕猴桃产业联盟链交易时企业实体对身份隐私和交易金额的隐私保护需要;相较于面向公有链的方案,本文方案有更快的区块生成及事务处理速度,可以提高交易效率;且本文方案具有可追溯性,更加满足猕猴桃产业联盟链交易

的实际需求。

4　结束语

本文面向猕猴桃产业链隐私交易的需求，利用$^{+}$HomElG－ZKProof 和 SM2 的特性，提出了一种联盟链隐私交易方案。以猕猴桃产业链相关企业作为用户节点，以猕猴桃产业链协会作为监管节点，设计了基于联盟链的猕猴桃产业链交易架构。根据产业链企业实体在交易时希望交易金额和身份的双重隐私需求，设计了具体的交易协议。当用户节点间发生交易时，转账方利用$^{+}$HomElG 加密交易金额后发送给接收方，接收方基于 SM2 签名确认交易后发送给转账方；转账方利用 SM2 加密、SM2 可链接环签名、同态加密、零知识证明等技术生成机密交易信息和接收方 SM2 签名一起经系统层 Raft 共识后打包上链；监管节点在解密相关密文后，通过验证 SM2 签名、两次环签名及链接性确认交易双方身份后，向其他用户节点发起交易有效性验证；由其他用户节点在应用层使用 PBFT 共识算法，通过验证交易金额相关密文的环签名及交易金额相关零知识证明证据确认区块交易有效性并向监管节点反馈共识结果；监管节点收到共识反馈结果为验证通过后，将交易双方交易余额密文经监管节点公钥加密后和区块哈希编号一起经系统层 Raft 共识后打包上链，更新本地数据库中交易双方的账户余额密文，完成交易。基于 Hyperledger Fabric 实现了一个面向猕猴桃产业链隐私交易原型系统，对方案进行了分析与测试。分析表明，本文方案具有抗篡改攻击、抗公钥替换攻击、抗假冒攻击以及匿名性，安全性较高；测试结果表明，本文方案可以实现猕猴桃产业联盟链用户交易金额和身份双重隐私保护，且交易时间相对较短，可以满足猕猴桃产业联盟链交易的实际需要。

参　考　文　献

[1] 曾诗钦，霍如，黄韬，等. 区块链技术研究综述：原理、进展与应用[J]. 通信学报，2020，41(1)：134－151.
ZENG Shiqin，HUO Ru，HUANG Tao，et al. Survey of blockchain：principle，progress and application[J]. Journal on Communications，2020，41(1)：134－151.（in Chinese）

[2] 赵辉，李星，谭嘉诚，等. 智能合约安全问题与研究现状[J]. 信息技术与网络安全，2021，40(5)：1－6，19.
ZHAO Hui，LI Xing，TAN Jiacheng，et al. Research status of smart contract security[J]. Information Technology and Network Secutity，2021，40(5)：1－6，19.（in Chinese）

[3] 朱绪荣，李靖，付海英. 现代农业示范区总体规划理论与实践[J]. 农业工程学报，2013，29(6)：223－231.
ZHU Xurong，LI Jing，FU Haiying，et al. Integrative planning theory and practice of modern agriculture demonstration zone[J]. Transactions of the CSAE，2013，29(6)：223－231.（in Chinese）

[4] 许继平，孙鹏程，张新，等. 基于区块链的粮油食品全供应链信息安全管理原型系统[J]. 农业机械学报，2020，51(2)：341－349.
XU Jiping，SUN Pengcheng，ZHANG Xin，et al. Prototype system of information security management of cereal and oil food whole supply chain based on blockchain[J]. Transactions of the Chinese Society for Agricultural Machinery，2020，51(2)：341－349.（in Chinese）

[5] 葛艳，黄朝良，陈明，等. 基于区块链的 HACCP 质量溯源模型及系统实现[J]. 农业机械学报，2021，52(6)：369－375.
GE Yan，HUANG Chaoliang，CHEN Ming，et al. HACCP quality traceability model and system implementation based on blockchain[J]. Transactions of the Chinese Society for Agricultural Machinery，2021，52(6)：369－375.（in Chinese）

[6] 任守纲，何自明，周正己，等. 基于 CSBFT 区块链的农作物全产业链信息溯源平台设计[J]. 农业工程学报，2020，36(3)：279－286.
REN Shougang，HE Ziming，ZHOU Zhengji，et al. Design and implementation of information tracing platform for crop whole industry chain based on CSBFT－blockchain[J]. Transactions of the CSAE，2020，36(3)：279－286.（in Chinese）

[7] 王皓，宋祥福，柯俊明，等. 数字货币中的区块链及其隐私保护机制[J]. 信息网络安全，2017(7)：3239.
WANG Hao，SONG Xiangfu，KE Junming，et al. Blockchain and privacy preserving mechanisms in cryptocurrency[J]. Netinfo Security，2017(7)：3239.（in Chinese）

[8] 杨亚涛，蔡居良，张筱薇，等. 基于 SM9 算法可证明安全的区块链隐私保护方案[J]. 软件学报，2019，30(6)：1692－1704.
YANG Yatao，CAI Juliang，ZHANG Xiaowei，et al. Privacy preserving scheme in block chain with provably secure based on SM9 algorithem[J]. Journal of Software，2019，30(6)：1692－1704.（in Chinese）

[9] 张小艳，李秦伟，付福杰. 基于数字承诺的区块链交易金额保密验证方法[J]. 计算机科学，2021，48(9)：324－329.
ZHANG Xiaoyan，LI Qinwei，FU Fujie. Secret verification method of blockchain transcation amount based on digital commitment[J]. Computer Science，2021，48(9)：324－329.（in Chinese）

[10] 李龚亮，贺东博，郭兵，等. 基于零知识证明的区块链隐私保护算法[J]. 华中科技大学学报(自然科学版)，2020，48(7)：112－116.
LI Gongliang，HE Dongbo，GUO Bing，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. (in Chinese)
[11] SHEN N, ADAM M. Ring confidential transactions[J]. Ledger,2016,1(1):1 - 18.
[12] 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.
WANG Ziyu, LIU Jianwei, ZHANG Zongyang, et al. Full anonymous blockchain based on aggregate signature and confidential transaction[J]. Journal of Computer Research and Development, 2018, 55(10): 2185 - 2198. (in Chinese)
[13] 刁一晴, 叶阿勇, 张娇美, 等. 基于群签名和同态加密的联盟链双重隐私保护方法[J]. 计算机研究与发展, 2022, 59(1):172 - 181
DIAO Yiqing, YE Ayong, ZHANG Jiaomei, et al. A dual privacy protection method based on group signature and homomorphic encryption for alliance blockchain[J]. Journal of Computer Research and Development, 2022,59(1):172 - 181. (in Chinese)
[14] 国家密码管理局. SM2 椭圆曲线公钥密码算法[S/OL]. [2022 - 06 - 24]. https://sca.gov.cn/sca/xwdt/2012 - 11/22/content_1002397.shtml.
[15] 国家密码管理局. 信息安全技术 SM2 椭圆曲线公钥密码算法[EB/OL]. [2022 - 06 - 24]. http://www.gb688.cn/bzgk/gb/std_list? p.p1 = 0&p.p90 = circulation_date&p.p91 = desc&p.p2 = 32918.
[16] 范青, 何德彪, 罗敏, 等. 基于 SM2 数字签名算法的环签名方案[J]. 密码学报, 2021, 8(4): 710 - 723.
FAN Qing, HE Debiao, LUO Min, et al. Ring signature schemes based on SM2 digital signature algorithm[J]. Journal of Cryptologic Research, 2021, 8(4): 710 - 723. (in Chinese)
[17] WANG Licheng, WANG Lihua, YANG Yixian, et al. Discrete logarithm based additively homomorphic encryption and secure data aggregation[J]. Information Sciences, 2011, 181(16): 3308 - 3322.
[18] 景旭,杨少坤. 面向联盟链转账隐私保护的 + HomElG 零知识证明协议[J/OL]. 工程科学与技术:1 - 11[2023 - 03 - 16]. https://doi.org/10.15961/j.jsuese.202200409.
JING Xu, YANG Shaokun. + HomElG zero-knowledge proof protocol for privacy protection of consortium blockchain transfer [J/OL]. Advanced Engineering Sciences: 1 - 11[2023 - 03 - 16]. https://doi.org/10.15961/j.jsuese.202200409. (in Chinese)
[19] BÜNZ B, BOOTLE J, BONEH D, et al. Bulletproofs: short proofs for confidential transactions and more[C]// 2018 IEEE Symposium on Security and Privacy (SP), SanFrancisco, USA,2018: 315 - 334.
[20] RIVEST R L, SHAMIR A, TAUMAN Y, et al. How to leak a secret[C]// Advances in Cryptology ASIACRYPT 2001. Springer Berlin Heidelberg, 2001: 552 - 565.
[21] LIU Jiakai, WEI Wei, HUANG Dashen. Linkable spontaneous anonymous group signature for ad hoc groups[C]// Information Security and Privacy ACISP 2004. Springer Berlin Heidelberg, 2004: 325 - 355.
[22] NAOR M. Deniable ring authentication[C]// Advances in Cryptology CRYPTO 2002. Springer Berlin Heidelberg, 2002: 481 - 498.
[23] BRESSON E, STERN J, SZYDLO M, et al. Threshold ring signatures and applications to ad hoc groups[C]// Advances in Cryptology CRYPTO 2002. Springer Berlin Heidelberg, 2002: 465 - 480.
[24] LV Jianqiang, WANG Xinmin. Verifiable ring signature[C/OL]// Proceedings of Third International Works-hop on Cryptology and Network Security (CANS' 03), 2003: 663 - 665. https://www.researchgate.net/p-ublication/265929579.
[25] 李顺东, 徐雯婷, 王文丽, 等. 恶意模型下的最大(小)值保密计算[J]. 计算机学报,2021,44(10):2076 - 2089.
LI Shundong, XU Wenting, WANG Wenli, et al. Secure maximum (minimum) computation in malicious model[J]. Chinese Journal of Computers, 2021,44(10):2076 - 2089. (in Chinese)
[26] BAI Chao, ZHU Qiong, SARKIS J. Joint blockchain service vendor-platform selection using social network relationships: a multi-provider multi-user decision perspective[J]. International Journal of Production Economics, 2021, 238: 108165 - 108180.
[27] WAN Shaohua, LI Meijun, LIU Gaoyang, et al. Recent advances in consensus protocols for blockchain: a survey[J]. Wireless Networks, 2020, 26(8): 5579 - 5593.
[28] 景旭, 秦源泽. 面向猕猴桃质量溯源的联盟链跨组织链上合同交易机制[J]. 农业机械学报, 2022, 53(5): 282 - 290.
JING Xu, QIN Yuanze. Consortium blockchain inter-organizational contract transaction mechanism for kiwifruit quality traceability[J]. Transactions of the Chinese Society for Agricultural Machinery, 2022, 53(5): 282 - 290. (in Chinese)
[29] 景旭,刘滋雨,秦源泽. 基于区块链中继技术的集群式农产品供应链溯源模型[J]. 农业工程学报,2022,38(11):299 - 308.
JING Xu, LIU Ziyu, QIN Yuanze. Traceability model of cluster agricultural product supply chains based on blockchain relay technology[J]. Transactions of the CSAE, 2022, 38(11): 299 - 308. (in Chinese)