计算机应用
Journal of Computer Applications
ISSN 1001-9081,CN 51-1307/TP

《计算机应用》网络首发论文

题目：基于改进公证人机制的联盟链跨链隐私保护方案
作者：郭晓涵，姚中原，张勇，郭尚坤，王超，斯雪明
收稿日期：2022-11-02
网络首发日期：2023-05-05
引用格式：郭晓涵，姚中原，张勇，郭尚坤，王超，斯雪明．基于改进公证人机制的联盟链跨链隐私保护方案[J/OL]．计算机应用.
https://kns.cnki.net/kcms/detail/51.1307.TP.20230504.0836.006.html

Journal of Computer Applications ISSN 1001-9081
计算机应用 CODEN JYIIDU http://www.joca.cn

doi:10.11772/j.issn.1001-9081.2022111641

基于改进公证人机制的联盟链跨链隐私保护方案

郭晓涵[1,2,3*]，姚中原[1,2,3]，张勇[1,2,3]，郭尚坤[1,2,3]，王超[1,2,3]，斯雪明[1,3]

(1.中原工学院 前沿信息技术研究院，郑州 450007； 2. 河南省网络密码技术重点实验室，郑州 450007
3. 河南省区块链与数据共享国际联合实验室，郑州 450007)

(*通信作者电子邮箱 thebestguoxh@163.com)

摘 要: 联盟链跨链交互既增强了联盟链应用的功能，又扩展了应用的使用范围，因此对促进联盟链应用推广和产业发展意义重大。然而，目前联盟链跨链交互依然存在着用户身份以及资产交易信息隐私泄露的问题，这已成为阻碍联盟链跨链交互技术应用的一个主要因素。针对以上问题，提出一个改进公证人机制的联盟链资产跨链隐私保护方案。该方案在合约层引入哈希锁定机制改进传统的单签名公证人跨链方式，以降低传统公证人机制中心化作恶的风险；利用同态加密的特性在保证交易合法的前提下实现对交易资产的可用不可见；同时，在网络层利用多密钥生成中心(KGC)模式的标识密码算法实现在网络层的用户身份隐私保护。理论分析和对比实验结果表明，所提方案对联盟链跨链交互时交易中的用户身份信息和资产信息具有良好的隐私保护效果，且相较于其他同类方案在签名和验证方面有更低的开销。

关键词: 区块链；公证人；哈希锁定；同态加密；标识密码；隐私保护

中图分类号:TP309；TP311.13 **文献标志码: A**

Cross-chain privacy protection scheme of consortium chain based on improved notary mechanism

GUO Xiaohan[1,2,3*], YAO Zhongyuan[1,2,3], ZHANG Yong[1,2,3], GUO Shangkun[1,2,3], WANG Chao[1,2,3], SI Xueming[1,3]

(1.The Frontier Information Technology Research Institute,Zhongyuan University of Technology,Zhengzhou,Zhengzhou Henan 450007,China
2. Henan Key Laboratory of Network Cryptography Technology,Zhengzhou Henan 450007,China
3.Henan International Joint Laboratory of Blockchain and Data Sharing, Zhengzhou Henan 450007,China)

Abstract: Cross-chain interaction of the consortium chain not only enhances the function of the application of the consortium chain, but also expands the use scope of the application, so it is of great significance to promote the application promotion and industrial development of the consortium chain. However, the cross-chain interaction of the consortium chain still has the problem of user identity and asset transaction information privacy disclosure at present, which has become a major factor hindering the application of the cross-chain interaction technology of the consortium chain. In view of the above problems, a cross-chain privacy protection scheme for alliance chain assets to improve the notary mechanism was proposed. The scheme introduced a hash locking mechanism at the contract layer to improved the traditional single-signature notary cross-chain method, so as to reduce the risk of the traditional notary mechanism centralizing evil. The characteristics of homomorphic encryption were used to realize the usability and invisibility of transaction assets under the premise of ensuring the legitimacy of transactions. At the same time, the identification cryptography algorithm of Multi-Key Generation Center (KGC) mode was used to protect the user's identity privacy at the network layer. The theoretical analysis and comparative experiment of this scheme show that the scheme has a good privacy protection effect on the user identity information and asset information in the cross-chain interaction of the consortium chain, it also has a lower overhead in signing and verification than other similar schemes.

Keywords: block chain; notary; hash locking; homomorphic encryption; identification password; privacy protection

收稿日期: 2022-11-02; **修回日期**:2022-12-02; **录用日期**: 2022-12-13。

基金项目: 河南省重大公益专项 (201300210300)；河南省网络密码技术重点实验室研究课题（LNCT2021-A14）；河南省科技攻关项目（222102210168）。

作者简介: 郭晓涵(1996—)，男，河南郑州人，硕士研究生，CCF 会员，主要研究方向：区块链；姚中原(1988—)，男，河南固始人，讲师，博士，CCF 会员，主要研究方向：密码学、区块链；张勇(1995—)，男，四川内江人，硕士研究生，CCF 会员，主要研究方向：区块链；郭尚坤(1998—)，男，山东菏泽人，硕士研究生，CCF 会员，主要研究方向：区块链；王超(1998—)，男，河南林州人，硕士研究生，CCF 会员，主要研究方向：区块链；斯雪明(1966—)，男，浙江诸暨人，教授，CCF 会员，主要研究方向：区块链、网络安全。

0 引言

区块链是一种链式数据结构，它将数据以区块的形式保存，每个区块大小相同，以时间顺序连接形成链。区块链具备去中心化、不可篡改、不可伪造等优势[1]，是国内外公认的未来金融服务基础设施[2]。目前，区块链在金融[3]、医疗[4]、物流监管[5]等方面得到了非常广泛的应用。随着区块链行业的不断发展，区块链开始融入更多行业，应用场景日渐丰富，使得不同的联盟链之间数据流通[6]、应用协同等需求也在日益增加，使用区块链跨链技术[7]-[9]成为扩展联盟链应用的功能及其使用范围的主要途径。然而，跨链的过程中也会出现隐私泄露的问题，包括用户的身份信息以及重要交易数据的泄露；这些信息对用户来说至关重要，攻击者能够从用户的交易记录中推出用户账户之间的关联及一系列信息，这将会给用户带来一定的财产损失，严重时可能会威胁到用户的人身安全；而且多种联盟链系统架构及其各自隐私保护方法实现之间的差异性也进一步增加了跨链隐私保护这一问题的困难和复杂程度。

作为当前普遍使用的跨链技术，公证人机制实现简单、执行效率较高。然而，在该机制中，公证人需要独自承担所有业务，包括数据的搜集和验证以及交易的确认，存在过度中心化的风险，故而极易出现诸如单点故障、主观作恶、系统性能受限于中间人能力等一系列问题，而一旦公证人遭受攻击或出现故障变得不可信，公证人手中的用户信息和交易信息将成为一颗炸弹，这些信息的泄露将会给用户带来无穷的隐患与风险，这也给跨链隐私保护带来新的挑战。

针对以上问题，本文面向基于账户模型的联盟链，通过引入标识密码和同态加密技术，结合公证人机制和哈希锁定技术实现跨链交易的隐私保护，实现对用户的身份和交易隐私保护。本文主要工作包括：

1）设计了一个跨链模型。该模型能够通过公证人机制实现跨链资产交易，同时通过哈希锁定技术减少公证人中心化作恶的风险，模型中包含密钥生成中心(Key Generate Center, KGC)联盟、公证人和交易用户三方实体，其中 KGC 联盟负责联盟链的维护和节点的身份审核，公证人负责跨链交易。

2）在该模型下提出一种隐私保护方案，通过结合标识密码和同态加密技术，保护用户交易和身份信息的隐私安全。

3）对方案进行仿真实现，针对其安全性做出分析，并与其他方案模型进行隐私保护能力的对比，最后在其性能方面进行了测试。

1 相关工作

根据祝烈煌等人[10]的研究，区块链的隐私大致可以分为两类，其中一类是身份隐私，指用户身份信息和区块链账户地址之间的关联；另一类是交易隐私，指存储在区块链的交易记录以及相关的信息，包括交易金额和交易双方的信息等。在区块链系统中，这两类隐私的泄露问题一直存在，并且在区块链跨链系统中更加严重。

目前针对区块链的隐私保护[10]-[12]研究已经相对成熟，如 Maxwell[14]在 2013 年提出的 Coinjoin 方案，该方案采用混币的方式隐藏了输入输出地址的映射，保证供给者无法获取精确信息，保护用户的隐私；Zerocash[15]为保护交易双方的账户地址以及交易金额，引入了非交互式零知识证明，该方法得到了广泛的认同；2015 年，Maxwell[16]在同态加密中加入盲化因子，提出了机密交易技术。同年，Noether[17]等提出的环机密交易技术，能够做到隐藏区块链账本数据中交易金额的同时隐藏交易的输入输出地址；杨亚涛等[18]提出的基于身份认证的多 KGC 群签名方案，通过改进的 SM9 标识密码方案，实现在节点间进行身份验证的同时保护节点隐私；刁一晴等[19]结合群签名中群的概念和联盟链，加入同态加密，实现对区块链交易和身份隐私保护；郭阳楠等[20]通过结合标识密码和无证书公钥密码体制的优点，从网络层和应用层的双层签名认证，保护了交易和身份隐私安全。但这些方案明显不适用于跨链间的隐私泄露问题。

针对跨链的隐私保护，戴波等[21]提出一种基于多角色节点的区块链跨链方案，该方案通过不同角色的权限控制可以实现节点间的隐私保护，由于该方案需要兼顾区块链扩展、跨链、监管方面的性能，隐私保护方面的功能完全由节点权限控制完成，身份隐私保护效果不佳。郭佳程等[22]针对分布式能源调度等问题，结合区块链，通过侧链技术构建三层网络，设计出一种分布式能源共享网络，提升能源利用率的同时实现隐私保护，但是该方案通过侧链将资产与能源储备信息隔离的方式实现隐私保护的方法并没有保护用户的身份隐私。唐榆程[23]通过设计满足隐私保护需求的交易智能合约，结合相关隐私保护算法实现一个跨链平台，完成了跨链数据的可控共享，完成对交易账户金额的隐私保护，但是该方案没有做到真正的匿名，没有实现用户的身份隐私保护。王宇[24]针对电子健康记录，提出了一种基于跨区块链技术的电子健康记录隐私保护方案，该方案将电子健康记录脱敏处理后生成索引上传至区块链，通过区块链实现对电子健康记录的隐私保护，但是该方案并没有实现医生身份的隐私保护。

以上方案在区块链跨链隐私保护方面做出了一些成果，但是这些方案大都只做数据隐私（交易隐私）保护，而忽视了身份隐私的保护，并不是完善的隐私保护方案。

郑建辉等[25]针对跨链操作难问题提出了一种联盟自治的跨链机制，通过以链治链的方法，解决不同区块链之间的数据共享、价值流通等问题，但是该方案通过通道隔离和私有数据等方法实现的隐私保护虽然实现了身份和交易隐私保护，但是保护性能完全取决于通道，保护效果有限。万哲驿[26]结合零证明技术，通过智能合约来替代交易双方的信息交换，改进了现有的原子交换协议[27][28]，保护跨链原子交换中双方的隐私。但是该方案的实现条件比较苛刻，方案实现难

度较大。这些方案同时做到身份和交易隐私的保护，但是在实现效果或者实现难度方面略有缺陷。

2 基础知识

2.1 区块链

区块链[29]是一种将数据区块按照时间顺序以链的形式组合而成的数据结构，结合了分布式存储、点对点(Peer-to-Peer, P2P)传输、共识机制、智能合约等技术，使得区块链具有防篡改，可追溯，公开透明等特点。区块链系统架构自下而上依次是数据层、网络层、共识层、激励层、合约层和应用层，其架构模型如图 1 所示。

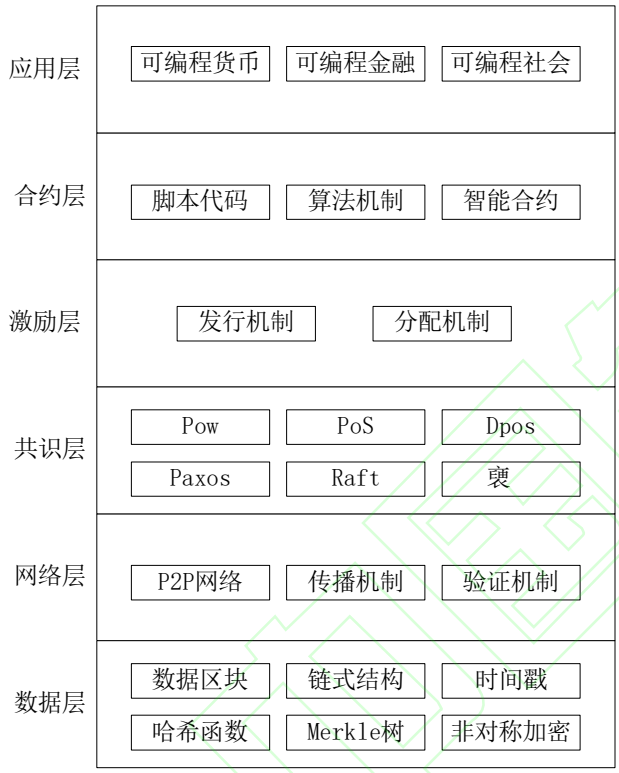

图 1 区块链架构模型

Fig. 1 Blockchain architecture model

其中，数据层包括底层数据区块以及相关的哈希值、随机数、交易信息以及公私钥等，是区块链结构中的最底层数据结构；网络层的 P2P 网络和数据验证机制等保证了数据的传输；共识层则主要封装了区块链核心技术中的共识机制。以上三层结构是区块链底层基础结构。激励层主要是经济激励机制，一般通过挖矿奖励数字资产来维持区块链账本的更新；合约层主要构建了区块链可编程特性的基础，在合约层运行着众多脚本和智能合约；应用层则包含了区块链的应用场景和案例[30]。

总的来说区块链根据其开放程度可以分为三类：公有链，私有链和联盟链。联盟链具有一定的中心化，且区块的产生和交易是可以控制的，具有一定的隐私性。

2.2 Paillier 同态加密

同态加密技术，可以对密文进行计算，并且可以保证计算后的结果经过解密与对应明文数据进行相同计算得到的结果相同。基于此特性，同态加密技术保证在处理密文时操作者无法获知真实的数据，这大幅提高了数据安全性。

根据算法对支持的计算类型的不同，同态加密可以分为全同态加密方案和部分同态加密方案。其中，全同态加密方案功能强大，支持对密文进行任意形式的计算，即同时满足密文加法和乘法的混合且不限制次数的运算。但目前全同态加密仍处于方案探索发展阶段，现有算法存在着一些问题，如密钥过大，效率低等；部分同态加密方案仅支持对密文进行有限地计算，如仅支持加法、仅支持乘法或支持有限次加法和乘法。部分加密方案构造简单、执行效率较高，因此常用于特定场景。

目前较为常见的部分同态加密设计包括 RSA、ElGamal 以及 Paillier。其中，RSA 与 ElGamal 支持乘法同态，Paillier 算法则具备加法同态特性，由于在区块链的交易中，账本金额的变化一般仅通过加减完成，因此 Paillier 算法常用于区块链中验证账本交易金额、账户金额以及交易后余额的合法性等方面。

由 Paillier[31]于 1999 年提出的基于复合剩余类困难问题的 Paillier 同态加密算法。定义 $\gcd(*,*)=1$ 为两个数的最大公约数；$lcm(*,*)$ 为两个数的最小公倍数；$L(u)=(u-1)/n$；$\boldsymbol{Z}_{n^2}^*$ 为不大于 n^2 的自然数构成的乘法群，Paillier 加密算法可由以下四个算法构成：

1) 密钥生成。

任意选取大素数 p 和 q，满足 $\gcd(pq,(p-1)(q-1))=1$。

计算 $n=p\cdot q$ 和 $\lambda=lcm(p-1,q-1)$；任意选取整数 g 且 $g\in\boldsymbol{Z}_{n^2}^*$ 且 $\mu=(L(g^{\lambda}\bmod n^2))^{-1}$ 存在。

则公钥为 $pk_p=(n,g)$，私钥为 $sk_p=(\lambda,\mu)$。

2) 数据加密。

任意选取 $0<r<n$ 其中 $\gcd(r,n)=1$，对于明文 $0\le m<n$，加密密文 $c=g^m r^n \bmod n^2$。

3) 密文解密。

已知密文 c，则经过解密后的明文 $m=L(c^{\lambda}\bmod n^2)\cdot\mu \bmod n$。

4) 密文加法同态。

对于两个明文m_1, m_2，经过 Paillier 同态加密后的密文分别为$c_{m_1} = g^{m_1} r_1^n \bmod n^2$，$c_{m_2} = g^{m_2} r_2^n \bmod n^2$可得$c_{m_1} \cdot c_{m2} = g^{m_1+m_2} (r_1 r_2)^n \bmod n^2 = c_{m_1+m_2}$。

2.3 公证人机制

当用户进行跨链交易[32][33]时，交易双方是互不信任且信息是不对称的，最简单的交易方式就是引入一方或多方可信实体做信用背书，由可信实体承担数据收集、交易确认和验证的任务，这样的跨链机制就被称为公证人机制[34][35]。

公证人机制是目前应用最为广泛的一种跨链机制，并且较易实现，其中最大的公证人就是交易所。

公证人机制分为单签名公证人机制以及多签名公证人机制。单签名公证人机制运行处理效率相对较高，但是缺点也明显，中心化严重，公证人的可信是系统正常运行的基础，公证人一旦遭受攻击，系统将非常危险。多签名公证人机制有多个公证人，在每次交易验证时从公证人群体中随机选出一部分公证人，共同完成签名，而这就需要链上支持多重签名机制，因此本文选择在单签名公证人机制上进行改进。

单签名公证人模式下的以太坊和比特币通过交易所进行资产交换的过程如下。

1）用户 A 发起一笔交易，交易金额 1 比特币(Bitcoin, BTC)，输出地址为交易所账户地址；

2）用户 A 向交易所提出用 BTC 兑换以太币(Ether, ETH)的请求，兑换比例 1：10；

3）用户 B 向交易所账户地址转入 10ETH；

4）用户 B 向交易所提出用 ETH 兑换 BTC 的请求，兑换比例 10：1；

5）交易所匹配兑换请求，作为第三方达成交易共识；

6）交易所将相应的 BTC 和 ETH 分别转入 B 和 A 的账户地址，交易结束[7]。

2.4 哈希锁定

哈希锁定[34][35]分为哈希锁和时间锁两部分，通过在交易中锁定部分资产，并设置解锁时间和特定的解锁条件来实现交易。哈希锁定交易与正常的交易类似，只是在交易资金上加一把哈希锁，只有解开哈希锁才能拿到交易资金。例如一个哈希锁定交易$Tx = T(H(s), t)$，其中$H(s)$为随机数s生成的哈希锁，只有交易方使用秘密值s在时间t之前解锁才能完成交易，拿到交易资金，否则交易则取消。

通过哈希锁定完成跨链交易的基本流程如图 2 所示。

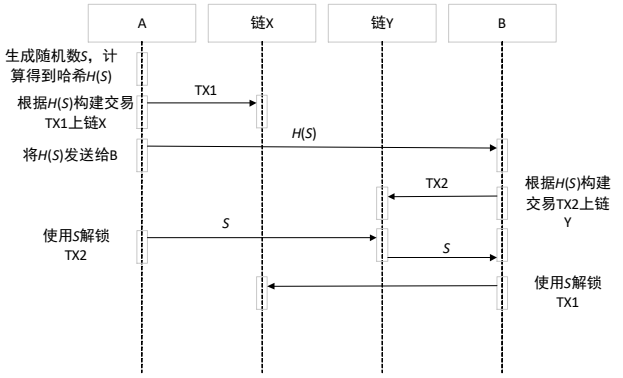

图 2 哈希锁定流程

Fig. 2 Hash locking process

1）用户 A 产生随机数s并计算哈希值$H(s)$，其中，H代表哈希函数；

2）用户 A 使用$H(s)$构造合约交易$Tx_1 = T(H(s), t_1)$并上传至链 X，其中t_1表示一段时间，Tx_1会锁定用户 B 在链 X 上需要的代币 x；

3）用户 A 把$H(s)$发送给用户 B；

4）用户 B 使用$H(s)$构造合约交易$Tx_2 = T(H(s), t_2)$并上传至链 Y，锁定用户 A 需要的链 Y 代币 y，其中$t_2 < t_1$；

5）用户 A 使用s在链 Y 上解锁交易Tx_2，获取该交易锁定的代币 y；

6）用户 B 通过用户 A 解锁交易Tx_2得知随机数s，使用s解锁链 X 上锁定的合约交易Tx_1，获取相应的代币 x。

哈希锁定通过哈希锁和时间锁保障了跨链交易的原子性，是进行原子交易的基本框架。但是，哈希锁定无法完成资产的链间转移，只能实现跨链的资产兑换，即各链资产总量不变，只是将资产转移至对方账户下。对于资产转移，还需要配合其他跨链技术方可实现。

2.5 SM9 标识密码体制

标识密码(Identity-Based Cryptograph, IBC)由 Shamir[36]于 1984 年提出的，其最主要的特点在于不需要由证书授权中心(Certificate Authority, CA)生成公私钥对，公钥的传递也无须使用证书；在 IBC 中，用户使用如网际互连协议(Internet Protocol, IP)地址、手机号、电子邮箱等唯一标识信息作为公钥，私钥则由 KGC 根据系统主密钥和用户标识计算得出。D.Boneh 等[37]以及 R.Sakai 等[38]两个团队都独立提出用椭圆曲线配对构造标识公钥密码。和传统的公钥基础设施(Public Key Infrastructure, PKI)体系比起来，除了上述特点外，IBC 还有成本低和效率高等有点。

SM9 标识密码算法[39]包含总则、数字签名算法、密钥交换协议、密钥封装机制和公钥加密算法几个部分，涉及有限域、椭圆曲线、双线性对及安全曲线、椭圆曲线上双线性对的运算等基本知识和技能。在本文构建的方案中主要使用数字签名算法为消息签名，公钥加密算法为数据加密。

双线性对：设 q 是一个大素数，G_1 和 G_2 是 q 阶的两个椭圆曲线上的加法群，G_T 是 q 阶的乘法群，称映射 $e:G_1\times G_2\to G_T$ 为双线性对，且满足以下条件：

1)双线性性：对于所有的 $g_1\in G_1,g_2\in G_2$ 和 $\forall a,b\in \boldsymbol{Z}_q$，则 $e\left(g_1^a,g_2^b\right)=e\left(g_1,g_2\right)^{ab}$；

2)非退化性：$\exists g_1\in G_1,\exists g_2\in G_2$ 使得 $e\left(g_1,g_2\right)\neq 1$；

3)可计算性：对于 $\forall g_1\in G_1,\forall g_2\in G_2$，存在有效的算法能够计算 $e\left(g_1,g_2\right)$。

系统参数生成：

KGC 选取随机数 s 为主私钥，s 满足 $1\le s\le q-1$；

KGC 计算主公钥 $P_{pub-e}=s\cdot P_1,P_1\in G_1$；

KGC 保存主私钥 s，公开主公钥 P_{pub-e}。

密钥导出函数 KDF、H1、H2 为辅助函数。

3 系统模型

本方案针对跨链资产交易实现身份和交易的隐私保护，在网络层通过 KGC 联盟模式下的标识密码，完成对用户真实信息和链上账户的分离，实现用户身份隐私的保护；在合约层以公证人技术为跨链基础，通过使用哈希锁定机制完成交易，降低公证人机制中心化的作恶风险的同时，为了确保跨链流转时的隐私，使用同态加密技术对哈希锁定交易进行保护，由于 Paillier 同态加密的加同态特性，保证加密后的交易可验证。以此为核心，设计了如图 3 的架构模型。

在本文构建的方案中，两条区块链的基本架构一致，都采用基本的区块链六层架构，且合约层都支持哈希锁定机制。由 KGC 联盟负责两条链区块的生成、维护以及加入区块链的用户审核和后续的用户地址及私钥分配。普通交易节点一般情况下是两个账户属于不同的用户，本文为了方便展示及简化流程，设定本文中的交易需求用户同时拥有两条链上的账户。

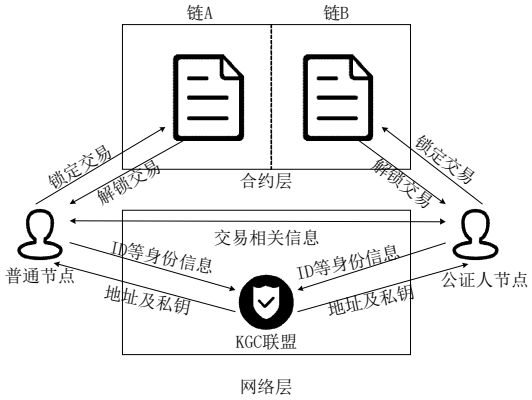

图 3 系统架构模型

Fig. 3 System architecture model

3.1 节点构成

本方案基于联盟链[40]设计，节点主要由 KGC 节点、公证人节点和普通节点构成如图 4 所示。

1）KGC 节点：联盟链的管理者，主要负责维护区块链参数和历史数据以及密钥的生成和发放，根据用户身份标识号(Identity Document, ID)及其身份信息为加入区块链的节点分配地址及对应密钥。

2）公证人节点：公证人节点加入区块链时需要经过 KGC 联盟的认证，检查其是否具有公证人资质后根据其 ID 为其分配交易地址以及私钥。主要负责与普通节点进行交易，收到普通节点的交易请求后发起哈希锁定合约并验证普通节点的合约是否正确。

3）普通节点：参与交易的普通用户，交易过程中需要向公证人节点发起交易请求，并验证公证人发起的哈希锁定合约以完成交易。普通节点加入区块链时需要向 KGC 联盟提供其 ID 等身份信息[41]，KGC 联盟验证身份信息后为使用哈希函数为其生成交易地址，再根据 SM9 标识密码算法生成对应私钥，地址作为公钥使用。其身份信息只有 KGC 联盟知道，其余用户无法查看，在网络层面隐藏其身份信息和交易地址的联系。

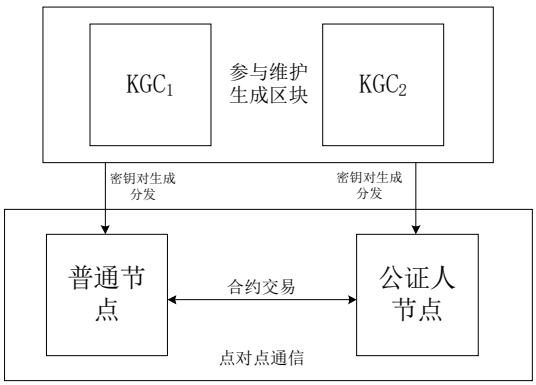

图 4 方案节点构成

Fig. 4 Solution node Composition

3.2 账户分配及私钥

本文借鉴杨亚涛等[18]的基于 SM9 的可证明安全的隐私保护方案，该方案通过多 KGC 群签名机制隐藏了交易双方的身份信息。在本文的方案中，同样使用多 KGC 的模式，采用多 KGC 的模式可以降低单一 KGC 被攻击后中心化的风险，通过 KGC 联盟使用哈希函数为用户 ID 等身份信息生成链上账户地址，再根据主私钥和链上账户地址其生成与账户地址配套的私钥，私钥生成过程如图 5 所示，实现用户 ID 与账户的分离，保护用户隐私。

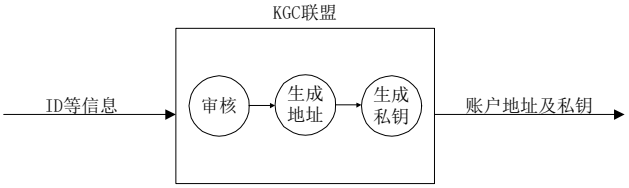

图 5 KGC 联盟分配账户地址及私钥

Fig. 5 KGC consortium assigns account addresses and private keys

用户私钥生成：

KGC 根据用户 ID 通过哈希函数计算出用户账户地址：$ID \xrightarrow{hash} Address_{ID}$；

用户选取主私钥 ks，ks 满足条件 $1 \le ks \le q-1$；

计算用户签名私钥，$ID\_sk_v = ks \cdot P_1 / H_1\left(Address_{ID} \| hid, q\right)$，其中 hid 为函数识别符，$P_1 \in G_1$。

计算用户加解密私钥，$ID\_sk_v = ks \cdot P_2 / H_1\left(Address_{ID} \| hid, q\right)$，其中 hid 为函数识别符，$P_2 \in G_2$。

3.3 基于哈希锁定的公证人机制

本方案基于原始的单签公证人机制，在公证人接收验证消息的过程中引入哈希时间锁定机制，使得公证人想要完成某笔跨链交易时，需要先将交易中需要交易的资产锁定在目标链上，待与公证人交易的用户对锁定的资产金额验证成功后，公证人才能从原链上的哈希锁定交易中拿到自己应得的那份资产。通过这样的机制，降低单签公证人的中心化的风险。

如图 6 所示，具体的公证人哈希锁定机制如下：

1）公证人使用 s 的哈希 $H(s)$ 将交易资金在链 A 中通过哈希锁定交易中锁定；

2）用户验证链 A 的哈希锁定交易金额，若验证通过，则继续执行下一步；若验证未通过，则交易结束；

3）用户使用 $H(s)$ 将交易资金在链 B 中通过哈希锁定交易锁定；

4）公证人验证链 B 的哈希锁定交易金额，若验证通过，则继续执行下一步；若验证未通过，则交易结束；

5）公证人使用 s 解锁链 B 的哈希锁定交易，获取资金；

6）用户获得 s，使用 s 解锁链 A 的哈希锁定交易，获取资金，交易结束。

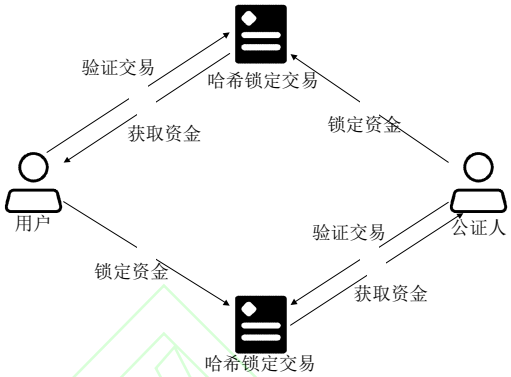

图 6 基于哈希锁定的公证人机制

Fig. 6 Notary mechanism based on hash locking

与原有公证人机制相比，本方案通过结合哈希锁定机制来完成交易，需要公证人事先在两条链上都有账户，并且账户中需要有一定的资金，而不是单纯地匹配两条链上的交易促使交易的完成。本方案的公证人需要切实地参与交易，成为交易方，并且按照规则需要先支付一定的资金将其锁定，可以有效地降低公证人中心化的风险。

4 方案设计

本文面向联盟链跨链交易，通过哈希锁定机制限制公证人的行动，降低中心化的风险，再加上同态加密和 KGC 联盟下的标识密码，实现对用户的隐私保护。方案流程如图 7 所示，大致可分为以下 3 个过程：

1）信息生成阶段：在这个阶段会生成交易阶段需要用到的信息，其中包括 KGC 联盟需要的主密钥和系统参数以及用户的账户地址和私钥等。

2）交易阶段：这是交易的主体阶段，在这个阶段会完成整个交易。其中包括用户和公证人的信息交换以及合约交易等。

3）验证阶段：这个阶段需要对交易阶段的一些数据进行验证，以保证交易的正常进行。

4.1 信息生成阶段

在本方案中一共需要用到以下密钥：

KGC 联盟初始化时生成的系统参数 k 主密钥对 (P_{KGC}, S_{KGC})，其中系统参数 k 公开。

需求用户 U 向 KGC 联盟申请加入区块链，KGC 根据其提供的 ID 等身份信息为其生成 Ua，Ub 的账户地址 $Address_{\mathrm{Ua}}$，$Address_{\mathrm{Ub}}$ 作为公钥并生成对应的数字签名

私钥Ua_sk_v，Ub_sk_v和用户加解密私钥Ua_sk_e，Ub_sk_e。

公证人 N 向 KGC 联盟申请加入区块链，KGC 根据其提供的信息为其生成 Na，Nb 的账户地址$Address_{\mathrm{Na}}$，$Address_{\mathrm{Nb}}$作为公钥并生成对应的数字签名私钥Na_sk_v,Nb_sk_v和加解密私钥Na_sk_e，Nb_sk_e，在 KGC 联盟审核其资质后向网络中公开其账户地址。

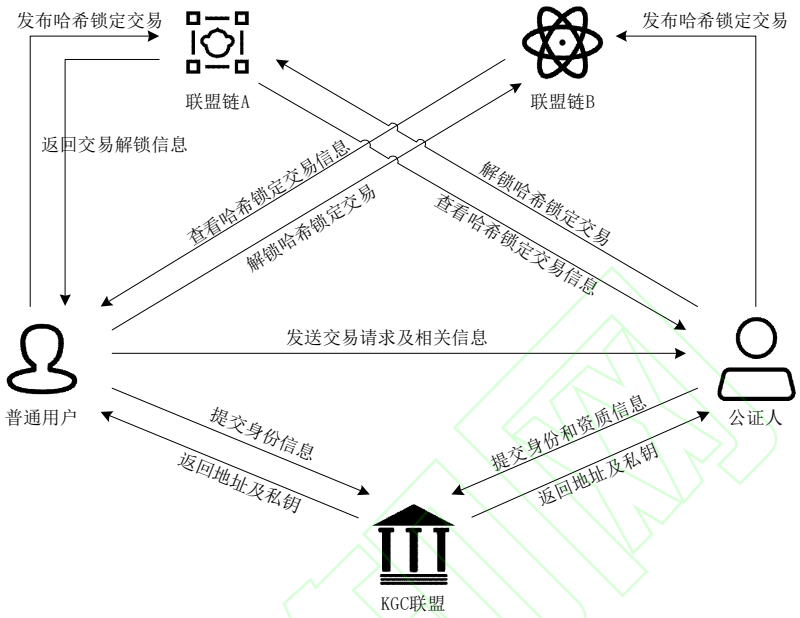

图 7 方案具体过程

Fig. 7 Specific process of the scheme

该方案中算法使用函数符号含义如表 1 所示。

表 1 函数符号说明

Tab. 1 Function symbol description

符号	含义
$Key\_Generate(\mathrm{size})$	Paillier 同态加密密钥生成算法，生成 size bit 大小的密钥
$Enc_{Add}(k,\mathrm{M})$	利用公共参数 k 和地址 $Address$ 对消息 M 进行加密
$Dec_{Add}(k,CT)$	利用公共参数 k 解密消息 CT
$Sig_{sk}(\mathrm{M})$	利用地址对应私钥 sk 对消息 M 进行签名
$Verify(k,M)$	签名验证函数，验证成功返回 1，验证失败返回 0
Enc_p	利用 Paillier 算法公钥加密消息
$Hash(s)$	SHA-256 哈希函数
$Get\_Balance$	获取当前账户余额

4.2 交易阶段

在交易阶段，需求用户需要和公证人产生信息交流，该部分信息包括两个部分，第一部分是交易需求部分，这部分需要用户和公证人之间点对点的网络层交流，这时需要对这部分信息使用标识密码进行加密，保护用户的隐私；第二部分是交易阶段的金额等信息，体现在哈希锁定交易中，由于这部分信息在验证过程中需要使用，所以需要对这部分信息使用同态加密进行保护，同时便于后续验证。

1）用户 U 在联盟链 A 中使用公证人 N 在链 A 上的账户地址$Address_{\mathrm{Na}}$加密消息发送给公证人。该消息包括用户 U 跨链资产交换所需要的链 B 上的代币金额$amount$，用户 U 在链 B 上的账户地址$Address_{\mathrm{Ub}}$，即消息$\mathrm{M}=(Address_{\mathrm{Ub}},amount)$，将消息执行消息传递算法 Transmit，该算法根据系统参数k，将消息 M、同态公钥pk_p和随机数r签名并加密成密文 CT 传递给公证人 N。

2）公证人 N 收到消息 CT 后，使用 Na 对应的解密私钥Na_sk_e解密，并对 Ua 的签名进行验证，若验证未通过，则交易结束；若验证通过，则查看消息 M 的内容并执行 3）；

算法 1　消息传递 Transmit

输入：系统参数 k，公证人 N 在链 A 上的账户地址 $Address_{\mathrm{Na}}$，用户 U 链 A 上的对应签名私钥 Ua_sk_v，消息 M。

步骤 1：使用函数 $Key\_Generate(\mathrm{size})$ 生成同态加密密钥对 pk_p, sk_p 和随机数 r。

步骤 2：使用 $Sig_{sk}()$ 函数借助签名私钥 Ua_sk_v 对消息 M 和同态加密公钥 pk_p 及随机数 r 进行签名。

步骤 3：使用 $Enc_{Add}()$ 函数借助公证人账户地址 $Address_{\mathrm{Na}}$ 和参数 k 对签名后的消息进行加密，生成密文 CT。

输出：密文 CT。

3）公证人 N 执行哈希传递算法 HTransmit 生成随机数 S 并生成对应哈希 $H(S)$，将生成的 $H(S)$ 签名后使用 Ub 地址加密，得到密文 CT_1，之后发布一条哈希锁定交易 $Tx_1 = T(H(S), Enc_p(amount_{\mathrm{B}}), t_1)$ 至联盟链 B 中，并将密文 CT_1 发送给用户 U。

算法 2　哈希传递 HTransmit

输入：系统参数 k，用户 U 在链 B 上的账户地址 $Address_{\mathrm{Ub}}$，公证人 N 链 A 上的对应签名私钥 Na_sk_v。

步骤 1：产生随机数 S 并生成对应哈希 $H(S)$。

步骤 2：使用 $Sig_{sk}()$ 函数签名私钥 Na_sk_v 对哈希 $H(S)$ 进行签名。

步骤 3：使用用户 U 在链 B 的账户地址 $Address_{\mathrm{Ub}}$ 和参数 k 调用函数 $Enc_{Add}()$ 对签名后的消息进行加密，生成密文 CT_1。

输出：密文 CT_1。

4）用户 U 在链 B 上查看哈希锁定交易 Tx_1，获取其中的信息 $Enc_p(amount_{\mathrm{B}})$ 进行验证，查看该金额是否是自己所需要的金额。即下式中 c_1 和 $c_1^{'}$ 是否相等：

$$\begin{aligned} &Enc_p(amount_{\mathrm{B}}) \cdot Enc_p(Sum_{\mathrm{Ub}}) = c_1 \\ &Enc_p(Sum_{\mathrm{Ub}}^{'}) = c_1^{'} \end{aligned} \tag{1}$$

其中 Sum_{Ub} 为当前账户余额，$amount_{\mathrm{B}}$ 为交易金额，$Sum_{\mathrm{Ub}}^{'}$ 为用户在账户余额上加上交易金额自己预先计算出的交易后的应有金额，$amount_{\mathrm{B}}$ 和 Sum_{Ub} 使用随机数 r 和 pk_p 加密，$Sum_{\mathrm{Ub}}^{'}$ 使用 $r' = r * r$ 和 pk_p 加密。

5）验证成功后，用户 U 将 CT_1 解密并验证，若验证未通过，则交易结束；若验证通过，则使用账户 Ua 发布交易 $Tx_2 = T(H(S), Enc_p(amount_{\mathrm{A}}), t_2)$ 至链 A 上。

6）公证人 N 在链 A 上查看哈希锁定交易 Tx_2，获取其中的信息 $Enc_p(amount_A)$ 进行验证，查看该交易金额是否满足自己所需要的交易金额。即下式中 c_2 和 $c_2^{'}$ 是否相等：

$$\begin{aligned} &Enc_p(amount_{\mathrm{A}}) \cdot Enc_p(Sum_{\mathrm{Na}}) = c_2 \\ &Enc_p(Sum_{\mathrm{Na}}^{'}) = c_2^{'} \end{aligned} \tag{2}$$

其中 Sum_{Na} 为当前账户余额，$amount_{\mathrm{A}}$ 为交易金额，$Sum_{\mathrm{Na}}^{'}$ 为交易后的应有金额，$amount_{\mathrm{A}}$ 和 Sum_{Na} 使用随机数 r 和 pk_p 加密，$Sum_{\mathrm{Na}}^{'}$ 使用 $r' = r * r$ 和 pk_p 加密。

7）若验证失败，则交易结束；若验证成功后，使用生成的随机数 S 解锁交易 Tx_2，获取资金 $amount_{\mathrm{A}}$；

8）用户 U 在在公证人 N 解锁交易 Tx_2 后获得随机数 S，在链 B 中通过账户 Ub 使用 S 解锁交易 Tx_1，获取资金 $amount_{\mathrm{B}}$，交易完成。

交易流程如图 8 图 9 所示。

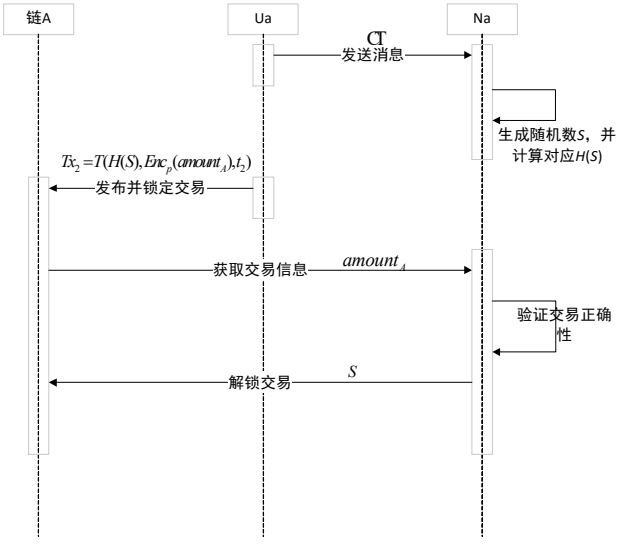

图 8 链 A 中交易流程

Fig. 8 Transaction flow in chain A

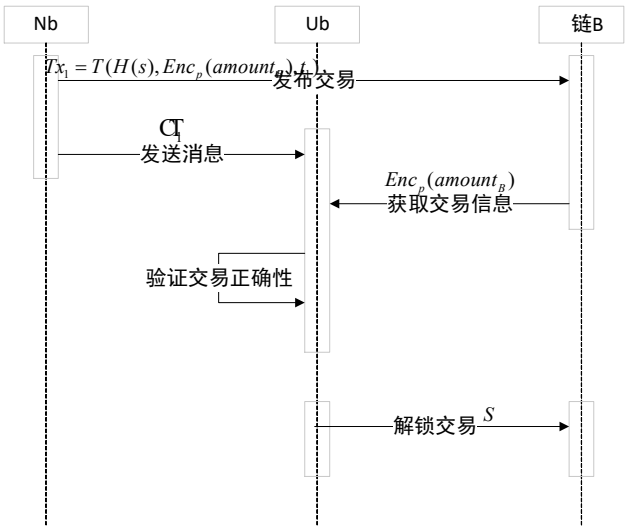

图 9 链 B 中交易流程

Fig. 9 Transaction flow in chain B

4.3 验证阶段

在整个交易阶段，一共需要进行如下验证：

1）验证签名。收到信息的用户先使用本人加解密私钥对消息进行解密，之后对消息签名进行验证，验证通过后方可进行下一步操作。

签名验证算法 Verify_sign（以公证人验证用户消息为例）：

公证人收到消息 CT 后，先将消息解密，后使用数字签名私钥 Na_sk_v 对消息进行验证。

算法 3　签名验证算法 Verify_sign

输入：系统参数 k，用户 U 在链 A 上的账户地址 $Address_{\mathrm{Ua}}$，密文 CT。

步骤 1：调用函数 $Dec_{Add}()$ 使用解密密钥解密 CT 得到消息 M。

步骤 2：调用函数 $Verify()$ 使用用户 U 账户地址 $Address_{\mathrm{Ua}}$ 和参数 k 对消息 M 进行验证，得到返回结果。

输出：消息验证结果

2）验证交易正确性。对与用户相关的哈希锁定交易，用户需要获取其中的使用同态加密之后的交易金额，与自己的账户余额做相关运算，检验该交易是否正确。验证通过则表明该交易是正确的，符合自己预期的交易，之后进行下一步操作。

交易正确性验证算法 Verify_trx（以需用户验证链 B 哈希交易为例）：

用户通过交易正确性验证算法验证交易正确性。其中 $c_{m1} = Enc_p(amount_{\mathrm{B}})$ 是加密后的交易金额。

算法 4　交易正确性验证算法 Verify_trx

输入：加密后的交易金额 c_{m1}，根据账户余额算出的交易成功后应有金额 Sum'_{Ub}。

步骤 1：调用函数 $Get\_Balance$ 获取当前账户余额 Sum_{Ub}，并判断余额是否能够保证交易进行，若不能，则交易取消。

步骤 2：调用函数 Enc_p 将 Sum_{Ub} 使用随机数 r 和同态加密公钥 pk_p 加密得到加密后的金额 c_{m2}。

步骤 3：将 c_{m1} 和 c_{m2} 数乘的结果 c 和 Sum'_{Ub} 经过 $r' = r * r$ 和 pk_p 加密后的结果 c' 进行比对，得到判断结果。

输出：判断结果

在整个交易阶段，用户与公证人之间的交流信息分为两个方面，一是在链上网络层进行传递的非交易信息，这些是用来传递用户的交易意愿或者与哈希锁定交易相关的重要信息，由于区块链链上账本公开透明的特性，所有的链上消息都可能被攻击者获取，为了防止被攻击者获取与用户相关的信息，本方案中使用标识密码对这些消息进行加密，保护用户的身份隐私。

二是在链上交易层的哈希锁定交易，对于哈希锁定交易来说，除了拥有 $H(S)$ 对应的 S 的用户可以解锁该笔交易，其他用户只能查看到来链上存在一个哈希锁定交易，并不能对其进行有效操作，并且在本方案中对哈希锁定交易进行改进，对其锁定的代币金额进行同态加密，攻击者便无法得知交易的金额，保护用户的交易隐私。

5　方案分析

本方案在网络层采用多 KGC 的 SM9 标识密码算法，通过多个 KGC 节点共同生成维护整个区块链，区块链中的用户也都由 KGC 联盟审核后方可加入区块链，根据标识密码的特性及性质，对用户在网络层的身份信息通过 KGC 联盟使用哈希函数转换为链上账户地址，达到用户的身份信息和链上账号的不可逆转换，从而保护用户的身份隐私；在合约层使用改进后的公证人机制，通过引入哈希锁定交易，使用 Paillier 同态加密对交易金额进行加密，从而保护用户的交易隐私。

本小节对方案进行安全性和效率分析，并与其他类似方案进行对比，论证本方案隐私保护的正确与安全。

5.1 安全性分析

攻击者类型 1：普通攻击者通过伪装成被攻击者（需求用户）U 获取信息或私钥。

对于攻击类型 1 的普通攻击者 A，根据本文的模型，攻击者能够伪装成需求用户只需要攻击者能够使用需求用户对应的私钥签名信息即可，即攻击者能够计算出用户私钥，而用户的私钥由 KGC 联盟使用标识密码主密钥对计算得出，即攻击者要在多项式时间内求解椭圆曲线上的离散对数问题。显然离散对数问题是困难问题，故本方案被普通攻击者获取信息或者私钥的概率可以忽略不计。

攻击者类型 2：攻击者为 KGC 联盟中的某个恶意节点，通过其生成的(P_{KGC},S_{KGC})获取被攻击者的私钥，即恶意 KGC 冒充被攻击者进行交易。

对本方案来说，单一的恶意节点无法获取攻击者私钥，而能够获取用户私钥的情况需要攻击者掌握超过一半的 KGC 节点，代价较高且该问题存在于所有同结构的去中心化机构中；而且由于本方案采用哈希锁定进行交易，恶意节点需要自己先付出代价锁定部分代币，风险较高，一旦进入哈希交易步骤，便无法作恶。因此本方案可以抵抗恶意 KGC 的攻击。

5.2 匿名性分析

本方案中使用的标识密码由 KGC 联盟生成，可以很好地避免中心化 CA 机构遭到攻击或者信息泄露而带来的安全隐患。若存在攻击者想要获取用户的身份信息，则存在如下博弈：

类型Ⅰ博弈：此类攻击者为区块链上某个普通节点。试图通过链上公开的账户地址获取用户的真实 ID 或其关联信息。

由于网络层使用的账户地址是由 KGC 联盟根据用户的 ID 等身份信息使用哈希生成的，所以如果该攻击者想要获取用户的身份信息就必须攻击 KGC 联盟，直至攻击者拥有超过一半的节点；或者通过账户地址逆推出其身份信息，则 KGC 联盟使用的哈希函数将不具备单向性，与哈希函数的定义不符。因此，在此类博弈中，攻击者优势极小，换言之，本方案能后保证此类博弈下的用户身份隐私。

类型Ⅱ博弈：此类攻击者为 KGC 联盟中某个恶意节点。

由于本方案使用的 KGC 联盟具有去中心化的特性，因此，此类攻击者在掌握单一节点的情况下无法获取用户身份信息，而能够获取用户身份信息则需要掌握超过一半的 KGC 节点，需要消耗巨大的代价，并且此类问题存在于同结构的所有去中心化机构中。因此，在此类博弈中，攻击者优势极小，换言之，本方案能后保证此类博弈下的用户身份隐私。

5.3 性能与功能理论分析

基于上述方案，定义符号T_E表示模幂运算时间开销，T_M表示模乘运算时间开销，H为哈希运算开销，T_B为双线性对运算开销，T_m表示群中元素点乘运算，T_A为指数运算。本方案与其他方案对比情况如表 2 所示。

从表 2 可以看出，从方案开销方面来看，与其他方案相比，本方案的签名开销要低于方案[20]，而验证开销要低于方案[19]，略高于方案[18]和方案[20]的模型，相比于方案[18]和[20]，本方案在加密方面做出了尝试，开销稍高，并且相比于方案[18]，本方案能够做到交易隐私的保护。

综上所述，本方案通过使用同态加密以及标识密码在公证人哈希锁定机制中实现了跨链交易的隐私保护，并且根据 Paillier 同态加密的加同态特性，可以实现交易的正确性验证；在保证交易的安全性的同时，又在一定程度上保证了效率，满足区块链跨链交易时的隐私保护需求。

表 2 效率与相关隐私保护情况对比

Tab. 2 Comparison of efficiency and related privacy protection

方案	签名开销	加密开销	验证开销	身份隐私保护	交易隐私保护
方案[18]	$2T_m+T_A$	无	T_m+3T_B	有	无
方案[19]	T_E+H	$2T_E+T_M$	$19T_E+8T_M+H$	有	有
方案[20]	$2T_M+T_B+T_E$	无	$T_M+3T_B+2T_E$	有	有
本方案	$2T_m+T_A$	$6T_A+2T_B+3T_M+3H$	$4T_E+3T_B+2T_M+T_m$	有	有

6 仿真实验

本方案的仿真实验环境主机为 Intel(R) Core(TM) i7-5500U CPU @ 2.40GHz 处理器，8G 内存的 windows10 系统，主机系统下的 IntelliJ IDEA 做链下 Paillier 同态加密及解密，区块链搭建在 Ubuntu on windows 中的 Ubuntu 20.04.4 LTS，配置和主机一致，搭建的区块链为 Fisco Bcos 单群组四节点

联盟链，版本 2.8.0，两条区块链同样的配置，在区块链上通过智能合约进行同态运算验证交易金额的正确性。

本次实验测试用户 ID 为 201508020116，通过 KGC 联盟验证后为其分配链上地址及对应私钥如表 3 所示。

表 3 账户信息

Tab. 3 Account Information

用户 ID	201508020116
链上账户地址	13de33c9f3246dc51efc345fd6a8780b1ced68e73c81115ebb8b2c715d7b853c
用户签名私钥	03420004512865bf1280168a8a4fee7393f22a95c19b68aa2d5c07378ca65fd485f324a61ef981952e807cb93202c789e04b1aa4690d3693df780c00801fd0f73912abce
用户加密私钥	03818200040f7884b3ff527f06ffc493299bcf46adbf5dac3634e5098dd14baa21c93d6ed5178595379515 58b296aacdde6507f3508f5254056fa3601a63b1327 4ab9691780b2f4a650b40d2a800fc39a2bde09266d 4028ae0e92a725d6bd8e891c7a32a076fa2064cc59 1811c0015db46f93d8f9de8c60e70993c1462aee11 3c9df314638

本方案的模型中包括 SM9 的加密(SM9_Encrypt)，解密(SM9_Decrypt)，签名(SM9_Sign)，验签(SM9_Verify)以及 Paillier 同态加密的加密(Paillier_Encrypt)和解密(Paillier_Decrypt)。经过对各算法测试多次测试，测试结果及平均消耗时间如图 10，图 11，表 4 所示。

从算法的各个功能平均耗时来看，在本方案中，SM9 部分算法占据大部分的时间，与其相比，同态加密的耗时很短，也就是说，在本方案中交易的正确性验证可以很流畅地进行，但是在用户和公证人做验证及加解密信息的过程将占据交易的大部分时间。

本次实验还对交易的正确性做出验证，在同态加密交易金额和用户当前账户余额，并且将加密后的金额在智能合约中运行，得出的结果图 12 所示。

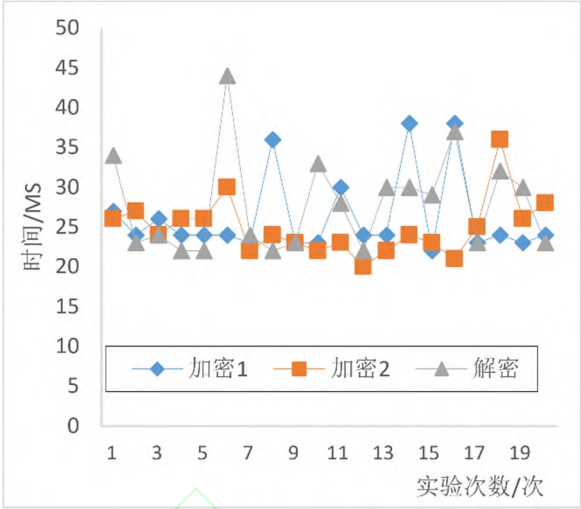

图 10 同态加密耗时

Fig. 10 Homomorphic encryption time-consuming

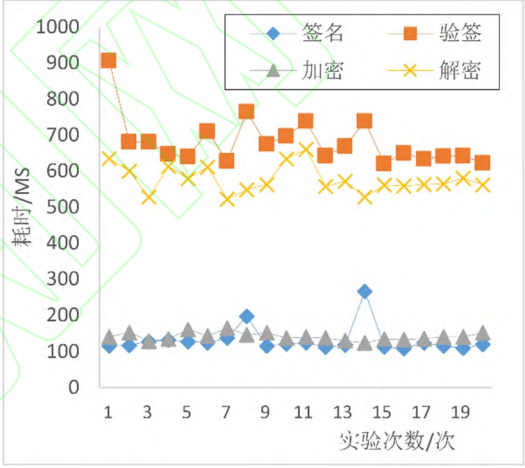

图 11 SM9 算法耗时

Fig. 11 SM9 algorithm time-consuming

表 4 各算法平均耗时

Tab. 4 Algorithm average time consumed

算法	平均耗时/ms
SM9_Encrypt	141.45
SM9_Decrypt	577.33
SM9_Sign	131.48
SM9_Verify	681.50
Paillier_Encrypt	25.55
Paillier_Decrypt	27.75

图 12 同态加密结果

Fig. 12 Result of homomorphic encryption

链上调用智能合约计算同态加密后结果与链下计算结果对比如图 13 所示。

图 13 链上链下结果对比

Fig. 13 Results comparison

对比结果显示结果一致，表明哈希锁定交易中确为目标金额，交易的正确性得到验证，表明本方案确实可以保证交易的正确性。同时因为该消息是使用 Paillier 同态加密算法加密的，消息的隐私性得到算法的保护，也就是说，保护了用户的交易隐私。

7 结语

本文提出一种基于哈希锁定的公证人机制跨链资产交换隐私保护方案。方案对公证人机制进行改进，通过结合哈希锁定机制加大公证人中心化作恶的难度，降低隐私泄露的风险。在网络层中通过哈希函数切断用户身份与区块链的联系，保护用户的身份隐私；在合约层交易时实现交易信息的加密可验证，对用户交易隐私进行保护。对比实验结果表明，本文模型兼顾身份隐私保护和交易隐私保护的同时在效率上并没有太多的降低，并且在保护隐私的同时能够保证交易的正确性，在跨链隐私保护方面有一定优势，但是具有一定的限制，未来的工作将会在本方案的基础上进一步研究减少限制。

参考文献

[1] 邵奇峰,金澈清,张召,等.区块链技术:架构及进展[J]. 计算机学报, 2018,41(05): 969-988. (SHAO Q F, JIN C Q, ZHANG Z, et al. Blockchain: architecture and research progress[J]. Chinese Journal of Computers, 2018, 41(05): 969-988.)

[2] 黄征,李祥学,来学嘉,等.区块链技术及其应用[J].信息安全研究, 2017,3(3):237-245. (HUANG Z, LI X X, LAI X J, et al. Blockchain technology and its application[J]. Journal of Information Security Research, 2017,3(3):237-245.)

[3] TRELEAVEN PHILIP, GENDAL BROWN RICHARD, YANG DANNY. Blockchain Technology in Finance[J]. Computer, 2017,50(9):14-17.

[4] SHAHNAZ A, QAMAR U, KHALID A. Using blockchain for electronic health records[J]. IEEE Access, 2019, 7:147782-147795.

[5] PAL A, KANT K. Using blockchain for provenance and traceability in internet of things-integrated food logistics[J]. Computer, 2019, 52(12): 94-98.

[6] 张志威,王国仁,徐建良,等.区块链的数据管理技术综述[J].软件学报,2020,31(09):2903-2925. (ZHANG Z W, WANG G R, XU J L, et al. Survey on data management in blockchain systems[J]. Journal of Software, 2020,31(09):2903-2925.)

[7] 何帅,黄襄念,陈晓亮.区块链跨链技术发展及应用研究综述[J].西华大学学报(自然科学版),2021,40(03):1-14. (HE S, HUANG X N, CHEN X L. The research summary of the development and application of blockchain cross-chain technology[J]. Journal of Xihua University (Natural Science Edition), 2021,40(03):1-14.)

[8] 李芳,李卓然,赵赫.区块链跨链技术进展研究[J].软件学报,2019,30(06):1649-1660. (LI F, LI Z R, ZHAO H. Research on the progress in cross-chain technology of blockchains[J]. Journal of Software, 2019,30(06):1649-1660.)

[9] ROBINSON PETER. Survey of crosschain communications protocols[J]. Computer Networks,2021,200.

[10] 祝烈煌,高峰,沈蒙,等.区块链隐私保护研究综述[J].计算机研究与发展,2017,54(10):2170-2186. (ZHU L H,GAO F, SHEN M, et al. Survey on privacy preserving techniques for blockchain technology[J]. Journal of Computer Research and Development, 2017,54(10): 2170-2186.)

[11] 王晨旭,程加成,桑新欣,等.区块链数据隐私保护:研究现状与展望[J].计算机研究与发展,2021,58(10):2099-2119. (WANG C X, CHENG J C, SANG X X, et al. Data privacy-preserving for blockchain: state of the art and trends[J]. Journal of Computer Research and Development, 2021,58(10):2099-2119.)

[12] 张奥,白晓颖.区块链隐私保护研究与实践综述[J].软件学报, 2020,31(05):1406-1434. (ZHANG A, BAI X Y. Survey of research and practices on blockchain privacy protection[J]. Journal of Software, 2020,31(05):1406-1434.)

[13] 刘彦松,夏琦,李柱,等.基于区块链的链上数据安全共享体系研究[J].大数据,2020,6(05):92-105. (LIU Y S, XIA Q, LI Z, et al. Research on secure data sharing system based on blockchain[J]. Big Data Research, 2020,6(05):92-105.)

[14] MAXWELL G. Coinjoin: Bitcoin privacy for the real world[EB/OL]. (2013 -08-22)[2021-05-03]. https://bitcointalk.org/?topic=279249.

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

[16] MAXWELL G. Confidential transactions[EB/OL]. 2015 (2016-09-05) [2021-09-15]. https://people.xiph.org/～greg /confidential_values.txt

[17] SHEN N, MACKENZIE A, LAB T M. Ring confidential transactions[J]. Research Bulletin, 2016.1:1-18.

[18] 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(06):1692-1704. (Yang Y T, CAI J L, ZHANG X W, et al. Privacy preserving scheme in block chain with provably secure based on SM9 algorithm[J]. Journal of Software, 2019,30(06): 1692-1704.)

[19] 刁一晴,叶阿勇,张妍美,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(01):172-181. (DIAO Y Q, YE A Y, ZHANG J M, 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(01):172-181.)
[20] 郭阳楠,蒋文保,叶帅.可监管的区块链匿名交易系统模型[J].计算机应用,2022,42(09):2757-2764. (GUO Y N, JIANG W B, YE S. Supervisable blockchain anonymous transaction system model[J]. Journal of Computer Applications, 2022,42(09):2757-2764.)
[21] 戴波,赖旬阳,胡凯,等.基于多角色节点的区块链可扩展方案研究与设计[J].浙江工业大学学报, 2021,49(05):487-493. (DAI B, LAI X Y, HU K, et al. Research and design of scalable blockchain scheme based on multi-role nodes[J]. Journal of Zhejiang University of Technology, 2021,49(05):487-493.)
[22] 郭佳程,宁德军,李泱丞,等.基于区块链的可信分布式能源共享网络研究[J].计算机工程,2021,47(03):17-28. (GUO J C, NING D J, LI Y C, et al. Research on trusted distributed energy sharing network based on blockchain[J]. Computer Engineering, 2021,47(03):17-28.)
[23] 唐榆程. 基于区块链的隐私保护技术的研究与应用[D].电子科技大学,2021:15-41. (TANG Y C. Research and application of privacy protection technology based on blockchain[D]. University of Electronic Science and Technology of China, 2021:15-41.)
[24] 王宇. 基于跨区块链的电子健康记录隐私保护方案研究[D].西华大学,2021:15-40. (WANG Y. Research on privacy-preserving scheme of electronic health records based on cross-blockchain[D]. Xihua University, 2021:15-40.)
[25] 郑建辉,林飞龙,陈中育,等.基于联盟自治的区块链跨链机制[J].计算机应用,2022,42(11):3444-3457.(ZHENG J H, LIN F L, CHEN Z Y, et al. Federated-autonomy-based cross-chain scheme for blockchain[J]. Journal of Computer Applications,2022,42(11):3444-3457.)
[26] 万哲驿.基于零知识证明的区块链数据隐私保护方法研究[D].重庆邮电大学,2020:17-41. (WAN Z Y. Research on blockchain data privacy protection method based on zero[D]. Chongqing University of Posts and Telecommunications, 2020:17-41.)
[27] SOICHIRO IMOTO, YUICHI SUDO, HIROTSUGU KAKUGAWA, TOSHIMITSU MASUZAWA. Atomic cross-chain swaps with improved space and local time complexity[A]. International Symposium on Stabilization, Safety, and Security of Distributed Systems. Pisa, Italy, 2019:194-208.
[28] MAURICE HERLIHY. Atomic cross-chain swaps[C]//Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing.RI: Brown University,2018:245-254.
[29] 蔡晓晴,邓尧,张亮,等.区块链原理及其核心技术[J].计算机学报,2021,44(01):84-131. (CAI X Q, DENG Y, ZHANG L, et al. The principle and core technology of blockchain[J]. Chinese Journal of Computers, 2021,44(01):84-131.)
[30] 袁勇,王飞跃.区块链技术发展现状与展望[J].自动化学报, 2016,42(04):481-494. (YUAN Y, WANG F Y. Blockchain: The state of the art and future trends[J]. ACTA AUTOMATICA SINICA, 2016,42(04):481-494.)
[31] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes[J]. Advances in Cryptology Leurocrypt, 2004: 223-238.
[32] HERLIHY, MAURICE, LISKOV, et al. Cross-chain deals and adversarial commerce[J]. The VLDB Journal,2021:1291-1039.
[33] PETER ROBINSON, RAGHAVENDRA RAMESH, SANDRA JOHNSON. Atomic cross-chain transactions for ethereum private sidechains[J]. IET Blockchain, 2022,003(001):23-39.
[34] 郭朝,郭帅印,张胜利,等.区块链跨链技术分析[J].物联网学报,2020,4(02):35-48. (GUO Z, GUO S Y, ZHANG S L, et al. Analysis of cross-chain technology of blockchain[J]. Chinese Journal on Internet of Things, 2020,4(02):35-48.)
[35] 路爱同,赵阔,杨晶莹,等.区块链跨链技术研究[J].信息网络安全,2019(08):83-90. (LU A T, ZHAO K, YANG J Y, et al. Research on cross-chain technology of blockchain[J]. Netinfo Security, 2019(08):83-90.)
[36] ADISHAMIR. Identity-based cryptosystems and signature schemes[J]. Lecture Notes in Computer Science,1985,196(1):47-53.
[37] DAN B, FRANKLIN M. Identity-based encryption from the weil pairing[C]// Annual International Cryptology Conference. Springer, Berlin, Heidelberg, 2001,2139:213-229.
[38] SAKAI R. Cryptosystems based on pairing[C]// Symposium on Cryptography & Information Security. Okinawa, Japan, 2000:26-28.
[39] 袁峰,程朝辉.SM9 标识密码算法综述[J].信息安全研究, 2016,2(11):1008-1027. (YUAN F, CHENG Z H. Overview on SM9 identity-based cryptographic algorithm[J]. Journal of Information Security Research, 2016,2(11):1008-1027.)
[40] QIANWEN WANG, SHEN WANG, PAN ZHANG, et al. An achieving data exchange cross-chain alliance protocol[J]. Journal of Physics: Conference Series,2019,1213(4).
[41] HUI WANG,YUANYUAN CEN,XUEFENG LI.Blockchain Router: A Cross-Chain Communication Protocol[C]//Proceedings of the 6th International Conference on Informatics, Environment, Energy and Applications.New York: Association for Computing Machinery,2017:94-97.

This work was supported by Major Public Welfare Project of Henan Province (201300210300), Henan Key Laboratory of Network Cryptography Technology (LNCT2021-A14), Key science and technology Project of Henan Province (222102210168).

GUO Xiaohan, born in 1996, M. S. candidate.His research interests include blockchain technology.
YAO Zhongyuan, born in 1988, Ph. D., lecturer. His research interests include cryptology, blockchain technology.
ZHANG Yong, born in 1995, M. S. candidate. His research interests include blockchain technology.
GUO Shangkun, born in 1998, M. S. candidate. His research interests include blockchain technology.
WANG Chao, born in 1998, M. S. candidate. His research interests include blockchain technology.
SI Xueming, born in 1966, professor. His research interests include blockchain and cybersecurity.