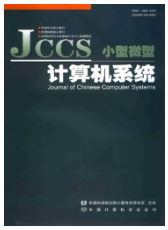

小型微型计算机系统
Journal of Chinese Computer Systems
ISSN 1000-1220,CN 21-1106/TP

《小型微型计算机系统》网络首发论文

题目：一种基于联盟链的兼具授权监管与隐私保护方案
作者：霍鑫磊，龙宇，谷大武
DOI：10.20009/j.cnki.21-1106/TP.2021-0608
收稿日期：2021-07-30
网络首发日期：2022-02-14
引用格式：霍鑫磊，龙宇，谷大武．一种基于联盟链的兼具授权监管与隐私保护方案[J/OL]．小型微型计算机系统．https://doi.org/10.20009/j.cnki.21-1106/TP.2021-0608

DOI：10.20009/j.cnki.21-1106/TP.2021-0608

一种基于联盟链的兼具授权监管与隐私保护方案

霍鑫磊[1]，龙　宇[1]，谷大武[1,2]

[1]（上海交通大学 计算机科学与工程系，上海 200240）

[2]（上海交通大学 网络空间安全学院， 上海 200240）

E-mail：longyu@sjtu.edu.cn

摘　要：区块链技术为推动金融等领域的数据互联互通提供强大助推力. 然而现有区块链研究中仍存在隐私泄露和监管缺失等问题，区块链隐私保护特性及其与监管科技的融合有利于加速区块链应用落地. 本文在联盟链场景下提出了一种兼具授权监管与隐私保护的方案. 一方面，方案在可确保交易正确性的前提下，实现了交易金额和交易者身份地址对交易无关节点的隐私性；另一方面，授权监管方可对任意交易执行审计并对存在违规消息的区块进行修订. 总之，通过对联盟链下成员角色划分及变色龙哈希函数、零知识证明等密码技术，实现了对交易隐私性的全面保障和细粒度的强制监管.

关键词：区块链；联盟链；隐私保护；可监管

中图分类号：TP393

Privacy Protection and Authorization Supervision Scheme based on Consortium Chain

HUO Xin-lei[1]，LONG Yu[1]，GU Da-wu[1,2]

[1]（School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China）

[2]（School of Cyber Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China）

Abstract: Blockchain technology can provide a powerful boost to finance, medicine, and other data interconnection fields. As the saying goes, opportunity comes along with the challenge. There are still issues such as privacy leakage and lack of supervision in existing blockchain research. Accordingly, the research on the characteristics of blockchain privacy protection and its integration with regulatory technology is an urgent need for the implementation of blockchain applications. The application scenario of that scheme is consortium chain. On the one hand, under the premise of ensuring the correctness of the transaction, the scheme realized that the privacy of the transaction amount and the recipient's address in the transaction process to the other nodes except transaction parties and the authorized supervisor; On the other hand, the authorized supervisor can revise the block, which contains violation messages. Concretely speaking, the scheme uses the chameleon hash function instead of the traditional hash function to calculate the block hash, and the authorized supervisor can use the chameleon hash trapdoor key to ensure that the changed target block is not affecting the link status of other blocks. Compared to the state-of-the-art researches, we introduce more fine grained enforced supervision mechanism besides keeping all the privacy properties of Blockchain.

Key words: blockchain; consortium chain; privacy preserving; supervisable

1　引言

区块链技术最初在2008年由Nakamoto作为比特币底层实现技术被提出[1]，是以时间为序的公共的、防篡改的分布式记账技术，是互联网交互中信任问题的一个分布式解决方法. 区块链技术使得其用户在不引入可信第三方的情况下建立一套信任机制，且区块链网络中交易公开透明，一旦上链很难被篡改. 因此，区块链技术被视为解决当前互联网信任机制所导致的一系列问题的突破性技术，目前，具有准入机制的联盟链是应用最为广泛的区块链.

然而，由于区块链使用参与结点共识机制来实现信任，这立足于全网交易的公开可验证性. 但交易的公开可验证性带来了暴露交易相关节点隐私的隐患：如交易双方身份（交易匿名性）及交易的金额（金额隐私性）等. 这引发了关于区块链隐私保护的一系列研究分析[2-3]. 典型工作包括 CoinJoin[4]、CoinShuffle[5]、TumbleBit[6]等使用了混币的思想. 而Cryptonote协议[7]、Zerocoin[8]、Zerocash[9]等则使用了零知

收稿日期：2021-07-30 收修改稿日期：2021-09-11　基金项目：上海市2019年度“科技创新行动计划”项目（19511101403）资助；2020“教育部科学技术研究重点（重大）项目”（2020KJ010201）资助.作者简介：**霍鑫磊，**女，1996年生，硕士研究生，研究方向为区块链技术；**龙 宇（通讯作者），**女，1980年生，博士，副教授，CCF会员，研究方向为区块链、信息安全和密码学；**谷大武，**男，1970年生，博士，特聘教授，博士生导师，CCF会员，研究方向为密码理论与算法、硬件与嵌入式安全、软件与系统安全、区块链与金融安全、智能安全技术、安全测试技术等

识证明、环签名等密码原语.良好的隐私保护机制在一定程度上可以保护区块链网络中节点的隐私,却可能使得对区块链数据的监管较难实现. 具备极强隐私保护机制的区块链网络易为不法分子所用.为此，人们展开了对区块链的监管的研究.

在区块链监管方面，按照监管者能力，主要划分为区块链数据审计和数据管理两个方向.区块链链上数据审计指监管者判断交易内容是否满足某些特定的格式(如一段时间内的交易总额、纳税比例等）.主要模型有两类：一类主要应用于银行中介模型，通过引入第三方参与交易确认(RSCoin[10]、Solidus协议[11]等)；另一类主要应用于各类隐私货币，使用密码学工具(zkledger[12]、FabZK[13]、PGC[14]等)，通过提供诸如“具有观察权限的审计密钥”等手段实现对部分数据的审计.区块链链上数据管理指通过对区块链上信息的重编辑以删除链上恶意数据，也包括两个模型：一类不需要可信监管方，通过全网投票实现数据管理[15]；另一类则存在可信监管方，监管方通过密码学私钥来修改区块链数据[16-18].

在现有的研究中,对可同时保护交易匿名性及隐私性的区块链下的数据监管问题的研究尚不足够.如 RSCoin 不考虑隐私问题；zkledger 不考虑数据管理问题且需要极大的公开账本以实现公开的交易正确性验证；PGC 既不保护交易用户匿名性也不考虑数据管理问题；文献[15-18]着重于数据管理但均不考虑隐私保护.为此，本文在联盟链场景下，针对以上问题进行了首次全面的综合研究，提出了一个兼具交易匿名性、金额隐私性，且支持强制数据审计和数据管理的监管方案.

具体而言，本文基于联盟链的金融交易场景.在存在可信授权监管方的前提下（如中国银联），多个金融机构共同参与构建联盟链.各参与方的经济活动均在链上进行，经过全网共识的正确交易才能计入公开账本.一方面，联盟链网络中的任一用户所发起的交易将被强制监管,即中国银联可以打开网络中所有交易的具体信息并执行任意审计,还可以针对链上的违规恶意信息进行一定程度的数据修订.另一方面，在每笔金融交易中，除交易双方与中国银联外，其他交易无关用户均不能知道交易金额和交易者身份.

2 基础技术

2.1 联盟链及其账本结构

联盟链是存在准入机制的区块链. 其最大的特点是参与者角色明确,其共识过程只针对某个特定群体的成员和有限的第三方开放,其区块生成仅由预选节点共同决定. 联盟链是目前区块链应用的主要场景，在银行和金融等行业联盟中，拥有天然的可落地基因.

与公有链类似,联盟链也使用 Hash 链和 Merkel 树来实现交易的打包和定序，如图 1 所示.交易本身主要使用两种记账结构：基于交易的 UTXO（Unspent Transaction Output，未花费的交易输出）模型和基于余额的账户模型.前者可以应用在脚本受限的平台上,具有更大的普适性.本文采用这种模型.

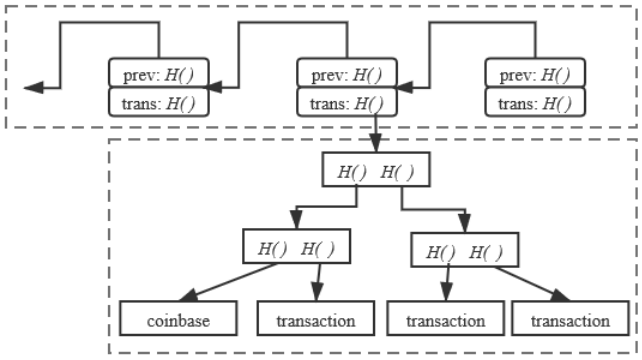

图 1 一般区块链组织结构示意图

Fig. 1 Schematic of general blockchain structure

在 UTXO 模型中，UTXO 不可分割，表示记录在区块中的用户所持有的金额. 在此模型中,交易发起方以其拥有的一笔或多笔 UTXO 作为输入，输出为一笔或多笔属于一个或多个接收方的 UTXO，且每个 UTXO 只能被消费一次，记账方式如图 2 所示.

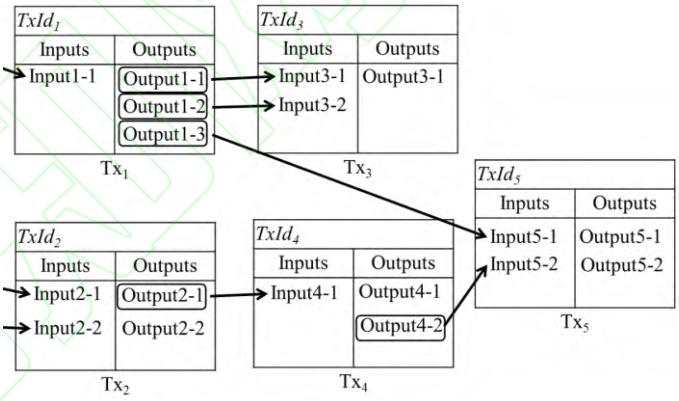

图 2 UTXO 模型下的交易示意图

Fig. 2 Transaction diagram under UTXO model

2.2 非交互零知识证明

非交互零知识证明涉及到的对象被称为证明方和验证方.在证明过程中，给定某个 NP 问题（称为语言L），证明方拥有属于L的实例x及其证据w. 需要向验证方证明$x \in L$且不泄露除此之外的任何信息. 零知识证明具有完备性、健壮性与零知识性. 本文所使用的非交互零知识证明算法简单描述如下：

1) $Setup(1^{k_{NIZK}})$. 以安全参数k_{NIZK}为输入，输出公共参数pp_{NIZK}.

2) $CRSGen(pp_{NIZK})$. 以零知识证明公共参数pp_{NIZK}为输入，输出公共参考串crs.

3) $Prove(crs,x,w)$. 以公共参考串crs、实例-证据对$(x,w) \in L$为输入，输出$\Pi = Prove(crs,x,w)$.

4) $Verify(crs,x,\Pi)$. 以公共参考串crs、实例x、证明Π为输入，若通过验证，输出为 1，反之则输出为 0.

2.3 变色龙哈希函数

变色龙哈希函数是一种带有“陷门”的密码学哈希函数.在变色龙哈希函数中，可以人为设下一个“私钥”，通过使用此“私钥”易找到碰撞. 其算法简单描述如下：

1) $HGen(1^{k_{CH}})$. 选取安全参数k_{CH}作为输入，输出哈希

密钥hk，陷门密钥tk.

2) $CHash(hk,m,\xi)$. 哈希密钥hk的持有者输入哈希密钥hk、消息m、随机数ξ(检查字符串)，输出哈希值$h=CHash(hk,m,\xi)$；

3) $CHVer\big(hk,m,(h,\xi)\big)$. 哈希密钥$hk$持有者输入哈希密钥$hk$、消息$m$、哈希值$h$与随机数$\xi$(检查字符串)，若$h=CHash(hk,m,\xi)$，输出为1，反之输出为0；

4) $CHCol(tk,(h,m,\xi),m')$. 陷门密钥tk持有者输入陷门密钥tk、原消息m、哈希值h、原随机数ξ与修改后消息m'. 输出新检查字符串$\xi'=CHCol(tk,(h,m,\xi),m')$. 新的检查字符串$\xi'$满足$CHVer\big(hk,m',(h,\xi')\big)=1$.

2.4 数字签名算法

数字签名算法涉及到的对象称为签名方与验证方. 数字签名具有不可伪造性与不可抵赖性. 算法简单描述如下：

1) $Setup\big(1^{k_{Sig}}\big)$. 以安全参数$k_{Sig}$为输入，输出公共参数$pp_{Sig}$.

1) $KeyGen\big(pp_{Sig}\big)$. 以公共参数pp_{Sig}为输入，输出签名密钥对(pk,sk).

3) $Sign(sk,m)$. 签名方存在数字签名公私钥对(pk,sk). 签名方以数字签名私钥sk与消息m为输入，得到数字签名$\sigma=Sign(sk,m)$.

4) $VerSig(pk,m,\sigma)$：接收方以签名方数字签名公钥pk，及其原消息内容m和对应的数字签名σ为输入，若通过验证，输出为1，反之输出为0.

2.5 公钥加密算法

公钥加密算法简单描述如下：

1) $Setup(1^{k_{PKE}})$. 以安全参数k_{PKE}为输入，输出公共参数pp_{PKE}.

2) $KeyGen(pp_{PKE})$. 以公共参数pp_{PKE}为输入，输出公私钥对(PK,SK)

3) $Enc_{PK}(m,r)$：消息加密方以消息接收方公钥PK、消息m及随机数r接为输入，生成密文$c=Enc_{PK}(m,r)$.

4) $Dec_{SK}(c)$：消息接收方以自身私钥SK与密文c为输入，若SK与加密时使用的PK对应同一对公私钥对，输出消息m，反之则输出不可读消息.

3 方案设计

3.1 方案参与方及基本思路

本文所提出的基于联盟链的方案旨在协调交易过程中交易隐私保护与监管粒度. 方案参与角色包括：证书签发机构、授权监管方、记账节点、普通交易节点. 方案模型如图3所示.

1）证书签发机构：可信第三方，负责成员身份管理. 在方案初始化之前，联盟链各成员节点从证书签发机构获得自己数字证书.

2）授权监管方：联盟链交易的可信监管者，负责交易审计和链上数据管理. 在此方案中授权监管方默认已知各普通用户在联盟链中普通用户的初始UTXO持有情况.

3）记账节点：联盟链中预先选定的多个节点，负责收集交易并通过安全共识算法形成公开账本.

4）普通交易节点：参与联盟链中的交易节点，包括交易发起方和接收方. 普通交易节点生成交易并将交易提交给记账节点，不参与记账行为与区块生成.

为实现交易隐私性，本方案中交易发起方使用交易接受方公钥来加密交易，从而保护交易金额及接收方地址的隐私性；为保证交易的可审计性，本方案同时使用监管者公钥来加密交易；为保证交易/审计的正确性及审计的强制性，本方案使用非交互零知识证明来确保交易的正确性和有效性. 此外，为实现监管方的链上数据管理，方案中使用了变色龙哈希函数，使得授权监管方可以对承载恶意信息的区块进行修订而保持所修订的区块原哈希值不变，从而保持了链结构.

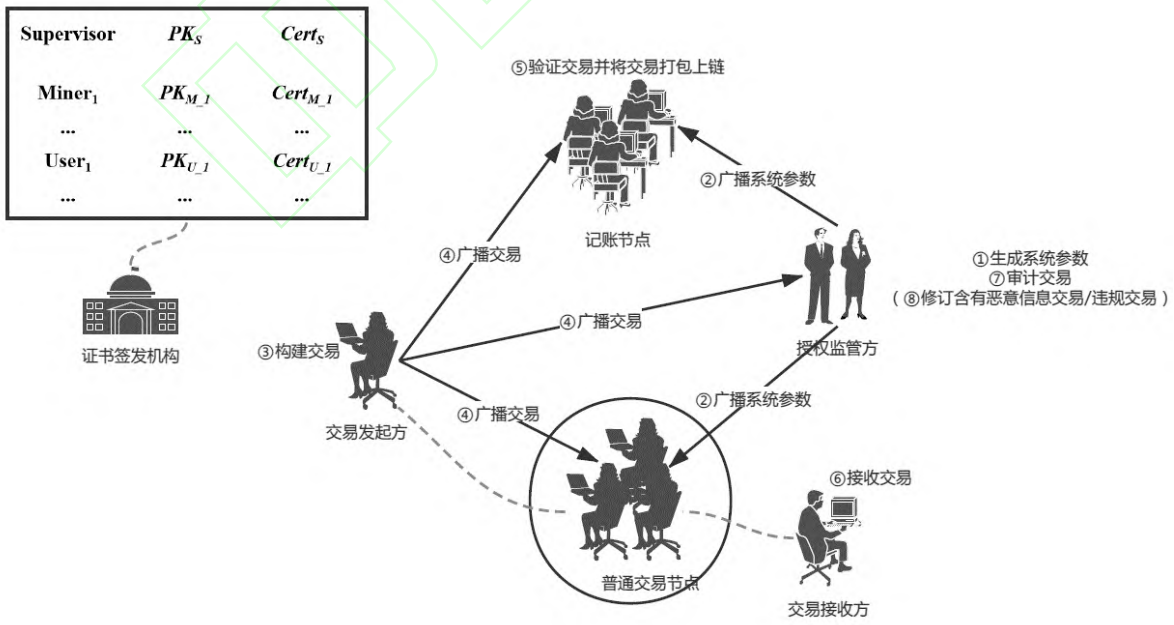

图3 方案模型

Fig. 3 Scheme model

3.2 方案 UTXO 交易及区块结构

本文所基于的 UTXO 模型的交易信息结构如图 4(a)所示. 此方案针对交易金额与交易输出地址字段进行隐私保护，涉及到的交易均非区块生成交易.

其中，Sig为交易发起方使用数字签名方案对交易的输入输出部分的签名，以保证交易的完整性与不可抵赖性，并参与交易发起方对于作为输入的 UTXO 的所有权的验证；$Witness_{add}$用于验证交易发起方对于作为输入的UTXO具有使用权；$Witness_{out}$用于验证交易可被监管者监管；$Witness_a$用于验证整个交易金额的平衡性. 值得注意的是，交易无关的其他节点均不能从$Witness_{add}$、$Witness_{out}$、$Witness_a$中读取任何交易隐私相关信息.

一个$Input$字段，即为此交易的一个$PreUTXO$，$PreUTXO$表示为其所在的交易标识$PreTxId$与其对应的偏移量$Index$，则$Input=(PreTxId,Index)$. 例如，图 2 中$Input5-2=(TxId_4,2).TxId$为该交易的输入输出的哈希值，$TxId=H(Inputs||Outputs)$；一个$Output$字段表示的即使一个新的UTXO，包括交易输出的交易金额$Amount$与交易的接收方地址$LockAddress$，$Output=(Amount,LockAddress).Amount$与$LockAddress$字段均以密文形式出现在交易中，交易无关用户不可读取.

此方案中所使用的区块结构包括前一区块的哈希值HashPrev；区块生成的相关参数Nonce；当前区块所包含交易的默克尔树的根Merkel Root；变色龙哈希函数的检查字符串Check string，具体如图 4(b)所示. 此区块结构中，区块的哈希值的计算方式为：$H(n,S,CHash(hk,x,\xi))$.

图 4 本方案所使用的交易结构与区块结构

Fig. 4 Transaction structure and block structure used in this scheme

4 方案构造

此方案由 6 个算法组成：初始化算法、交易生成算法、交易验证算法、交易接收算法、审计算法、区块信息修订算法. 以下算法描述中，发送方的公私钥对表示为(PK_U^S,SK_U^S)，数字签名公私钥对(pk_U^S,sk_U^S)；接收方的公私钥对表示为(PK_U^R,SK_U^R)，数字签名公私钥对(pk_U^R,sk_U^R)；授权监管方的公私钥对表示为(PK_S,SK_S)，数字签名公私钥对(pk_S,sk_S).

算法 1. 初始化算法.

初始化算法的主要功能是生成此方案所需参数.

输入：一系列安全参数；

输出：公共参数$para_{pub}$与私有参数$para_{sec}$.

1) 生成变色龙哈希函数的公私钥对(hk,tk).

2) 生成签名方案的公共参数pp_{Sig}.

3) 生成公钥加密算法的公共参数pp_{PKE}.

4) 生成非交互式零知识证明的公共参数pp_{NIZK}与crs.

5) 规定零知识证明语言L_{add}.

$$L_{add}=\{(Sig,PreUTXO,TxId)|\exists(PK_U^S,SK_U^S,pk_U^S,sk_U^S)\ s.t.\ PK_U^S=Dec_{SK_U^S}(LockAddress_{PreUTXO})\wedge Sign(sk_U^S,TxId)=Sig\},$$

借助证据$w_{add}=(PK_U^S,SK_U^S,pk_U^S,sk_U^S)$，为实例$x_{add}=(Sig,PreUTXO,TxId)$，生成证明，记为$\Pi_{add}$.

6) 规定零知识证明语言L_{out}.

$$L_{out}=\{(y_S,C_A,C_P)|\exists(a,PK_U^R,r_a,r_p,PK_S,r_S)\ s.t.\ Enc_{PK_U^R}(a,r_a)=C_A\wedge Enc_{PK_U^R}(PK_U^R,r_p)=C_P\wedge Enc_{PK_S}(a||PK_U^R||r_a||r_p,r_S)=y_S\}$$

借助证据$w_{out}=(a,PK_U^R,r_a,r_p,PK_S,r_s)$，为实例$x_{out}=(y_S,C_A,C_P)$生成证明，记为$\Pi_{out}$.

7) 规定零知识证明语言L_a.

$$L_a=\{(C_{B_1},\dots,C_{B_n},C_{A_1},\dots,C_{A_m})|\exists(b_1,\dots,b_n,a_1,\dots,a_m,r_{a_1},\dots,r_{a_m},PK_U^S,SK_U^S,PK_U^{R_1},\dots,PK_U^{R_m})\ s.t.\ Dec_{SK_U^S}(C_{B_i})=b_i,i\in\{1,\dots,n\}\wedge Enc_{PK_U^{R_j}}(a_j,r_{a_j})=C_{A_j},j\in\{1,\dots,m\}\wedge\sum_{i=1}^{n}b_i=\sum_{j=1}^{m}a_j\}$$

借助证据$w_a=(b_1,\dots,b_n,a_1,\dots,a_m,r_{a_1},\dots,r_{a_m},PK_U^S,SK_U^S,PK_U^{R_1},\dots PK_U^{R_m})$，为实例$x_a=(C_{B_1},\dots,C_{B_n},C_{A_1},\dots,C_{A_m})$生成证明，记为$\Pi_a$.

8) 私有参数$para_{sec}=(tk)$发至授权监管方，公共参数$para_{pub}=(hk,pp_{Sig},pp_{PKE},pp_{NIZK},crs)$广播给网络中节点.

算法 2. 交易生成算法.

交易生成算法的主要功能是生成符合此方案的交易规则的交易并广播到区块链网络中.

输入：公共参数$para_{pub}$、交易信息meg、交易发送方公私钥对(PK_U^S,SK_U^S)、交易发送方数字签名公私钥对(pk_U^S,sk_U^S)、交易接收方公钥PK_U^R、授权监管方公钥PK_S.

输出：交易输入$Inputs$、交易输出$Outputs$、交易见证$Witness$.

交易信息meg包含作为输入的 UTXO 的集合与新生成的UTXO的集合. 输入的UTXO的集合即为$Inputs$. 新生成的UTXO集合即为$Outputs$. 网络中的交易可包含多个输入与多个输出，以下以仅包含一个输入一个输出的情况进行说明.

交易见证$Witness=(Sig,Witness_{add},Witness_{out},Witness_a)$. 在此交易中，$Witness_{add}$即为$\Pi_{add}$，$Witness_{out}$即为$(y_S,C_A,C_P,\Pi_{out})$，$Witness_a$即为$\Pi_a$.

1) 选择随机数r_a,r_p，使用交易接收方公钥对交易金额a及接收方地址PK_U^R加密，得到密文C_A,C_P. 则$Output=(C_A,C_P)$；其中$C_A=Enc_{PK_U^R}(a,r_a)$；$C_P=Enc_{PK_U^R}(PK_U^R,r_p)$；

2) 表示此交易的$Inputs$，即此交易所使用的$PreUTXO.PreTxId$为交易发起方使用的$PreUTXO$所在的交易的标识；$Index$表示作为输入的$PreUTXO$在$PreTxId$交易输出中的偏移量，则$Input=(PreTxId,Index)$；

3) 计算交易标识$TxId=H(Input||Output)$；

4）为此交易的输入输出部分生成数字签名$Sig = Sign(sk_U^S, TxId)$；

5）利用证据$w_{add} = (PK_U^S, SK_U^S, pk_U^S, sk_U^S)$，通过零知识证明的证明生成算法$Prove(crs, w_{add}, x_{add})$计算关于实例$x_{add} = (Sig, PreUTXO, TxId) \in L_{add}$的证明$\Pi_{add}$，用于其他节点使用非交互式零知识证明的验证算法对交易完整性与$PreUTXO$的所有权进行验证；

6）选择随机数r_S，使用授权监管方公钥加密交易金额a与交易接收方地址PK_U^R及$Output$字段公钥加密所使用的随机数，得到密文$y_S = Enc_{PK_S}(a||PK_U^R||r_a||r_p, r_S)$.

7）利用证据$w_{out} = (a, PK_U^R, r_a, r_p, PK_S, r_S)$，通过零知识证明的证明生成算法$Prove(crs, w_{out}, x_{out})$计算关于实例$x_{out} = (y_S, C_A, C_P) \in L_{out}$的证据$\Pi_{out}$. $(y_S, C_A, C_P, \Pi_{out})$用于其他节点使用非交互式零知识证明的验证算法验证当前交易方提供的监管信息的正确性.

8）假定$PreUTXO$的金额的密文表示为C_B，对应的金额为b. 交易发起方利用证据$w_a = (b, a, r_a, PK_U^S, SK_U^S, PK_U^R)$，通过零知识证明的证明生成算法$Prove(crs, w_a, x_a)$计算关于实例$x_a = (C_B, C_A) \in L_a$的证明$\Pi_a$. Π_a用于其他节点使用非交互式零知识证明的验证算法对此交易金额的平衡性进行验证.

算法 3．交易验证算法.

交易验证算法的主要功能是验证交易的有效性与正确性.

输入：公共参数$para_{pub}$、交易输入$Inputs$、交易输出$Outputs$、交易见证$Witness$；

输出：1 或 0.

1）通过非交互式零知识证明的验证算法$Verify(crs, x_{add}, \Pi_{add})$验证交易的完整性与交易发起方对$PreUTXO$的所有权；

2）通过非交互式零知识证明的验证算法$Verify(crs, x_{out}, \Pi_{out})$验证交易发起方以密文形式发送给授权监管方的监管信息的正确性；

3）通过非交互式零知识证明的验证算法$Verify(crs, x_a, \Pi_a)$验证交易金额的平衡性.

若输出为 1，则表示该交易有效且正确；若输出为 0，则表示该交易无效，丢弃此交易.

算法 4．交易接收算法.

交易接收算法的主要功能是使得交易接收方获知交易具体金额，并更新自身资产列表.

输入：公共参数$para_{pub}$、交易输出$Outputs$、交易接收方私钥SK_U^R；

输出：交易金额a

对于已经上链的交易，交易接收方使用自身私钥解密C_A，得到交易金额，并更新自身资产列表.

算法 5．审计算法.

审计算法的主要功能是使得授权监管方获知网络中交易的流动.

输入：公共参数$para_{pub}$、交易输入$Inputs$、交易输出$Outputs$、交易见证$Witness$、授权监管方私钥SK_S；

输出：全部交易接收方公钥地址与对应输出的金额的集合.

对于使用交易验证算法验证后输出为 1 的交易，针对其每一个输出授权监管方均使用自身私钥解密y_S，得到当前交易的金额与接收方的公钥地址及相关参数.

算法 6．区块信息修订算法.

区块信息修订算法的主要功能是使得授权监管方可针对存储在区块中的交易无关的恶意信息修订.

记账节点利用安全共识协议将交易信息打包成区块，区块间关系如图 5 所示. 区块S_{j-1}, S_j, S_{j+1}为相邻的三个区块. 假设其中区块S_j包含了恶意内容. 授权监管方需要在保证整个区块链的区块间链接信息不变的前提下，完成对区块S_j的修订，即删除区块S_j的恶意内容，且保证区块S_j的区块哈希值不变.

输入：私有参数$para_{sec}$、需修改区块S_j；对目标区块进行的修订操作op；

输出：修改后的区块S_j'

1）授权监管方删除恶意信息，并利用剩余数据重新计算区块S_j的 Merkel Root 的值，得到x_j'.

2）授权监管方利用自己所掌握的变色龙哈希函数的哈希私钥tk针对新的 Merkel Root x_j'，计算$\xi_j' = CHCol(tk, (h_j, x_j, \xi_j), x_j')$，得到新的检查字符串，其中$h_j = CHash(hk, x_j, \xi_j)$，即区块$S_j$的原变色龙哈希值. 新检查字符串$\xi_j'$满足:$CHVer\left(hk, x_j', (h_j, \xi_j')\right) = 1$.

3）$CHash(hk, x_j', \xi_j')$更新区块S_jMerkel Root 字段为x_j'，Check String 部分为ξ_j'，完成区块S_j的修订.

区块间的变化如图 5 所示. 由此，在不影响其他区块正确性的前提下授权监管方实现了对包含恶意内容的区块的修订.

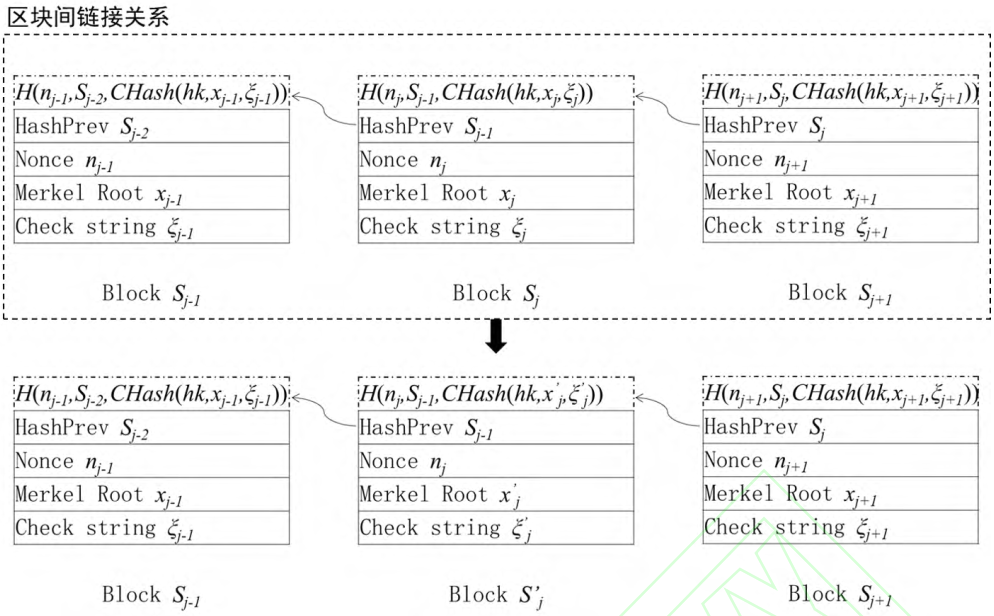

图 5　区块间的链接关系与区块信息修订

Fig. 5 The relationship of links between blocks and revision of block information

5 方案分析

5.1 安全性定义及分析

本文试图缓解基于联盟链的金融交易场景中交易信息的隐私保护与监管间的冲突，可能遭遇两类不良行为：逃避监管及隐私攻击. 前者是指交易参与方试图构造“看似”合法的交易以通过共识节点的认可，但交易中并不包含审计信息或试图产生错误的审计信息. 后者是指与交易无关的非监管节点试图从交易中读取交易相关金额、身份等信息.

依据攻击者的攻击目标，定义本方案所需满足的安全性质分别为：强制审计性、审计可靠性、交易金额与地址隐私性. 若方案满足强制审计性、审计可靠性与交易金额与地址隐私性，则称此交易方案是安全的.

性质 1. 强制审计性. 该性质要求：若不诚实用户发布缺失审计信息的交易，则此交易被纳入区块链的概率为 0.

性质 1 分析：强制审计性保证网络中每一笔交易都强制接受授权监管方的审计，由此，授权监管方可监察整个网络的交易流动. 方案要求交易发起方将审计信息作为方案中交易内容的一部分，即只有完整、正确的交易才有机会通过共识节点的验证机制并被纳入区块链. 假设存在不诚实的普通交易节点想要逃避授权监管方的审计进行交易，并使得该交易通过共识节点的验证机制并最终被区块链接收. 在此情况下，不诚实节点发布的交易缺失$Witness_{out}$字段，导致交易信息不符合方案完整交易内容的需求. 此时，该不诚实节点发布的交易消息不合法，即无法通过共识节点的验证机制并被纳入区块链. 共识协议的安全性保障了方案的强制审计性.

性质 2. 审计可靠性. 该性质要求：在交易过程中，若授权监管方接收到不诚实节点的交易，该交易中包含与原交易信息不一致的虚假审计信息，则该交易通过验证算法的概率是可忽略的.

性质 2 分析：审计可靠性主要针对授权监管方而言. 网络中每一笔交易输出的真实金额与接收方的公钥地址均使用授权监管方的公钥，以公钥加密的形式发送给授权监管方. 假设存在不诚实的普通交易节点想要逃避授权监管方审计进行交易. 为了使得交易信息满足方案交易内容完整的需求，该不诚实节点伪造审计信息数据为$Witness'_{out}=(x'_{out},\Pi'_{out})$或使用其掌握的其他交易中有效审计信息数据$Witness''_{out}=(x''_{out},\Pi''_{out})$作为当前交易审计信息字段数据使用. 假设当前交易正确的实例证据对为(x_{out},w_{out}). 对于伪造的实例证据对$(x'_{out},w'_{out})\neq(x_{out},w_{out})$；对于非当前交易的实力证据对$(x''_{out},w''_{out})\neq(x_{out},w_{out})$. 若在以上两种情况，不诚实节点可以达到目的，则需要使得$\Pr\{Verify(crs,x'_{out},\Pi'_{out})=1\}\geq 1-f(\lambda)$；$\Pr\{Verify(crs,x''_{out},\Pi''_{out})=1\}\geq 1-f(\lambda)$. 其中，$f(\lambda)$为可忽略函数. 这与零知识证明的健壮性相违背，所以不诚实的普通交易节点无法欺骗监管方. 零知识证明的完整性与健壮性保障了方案的审计可靠性.

性质 3. 交易金额与地址隐私性. 该性质要求：在交易过程中交易金额与地址泄露给除交易接收方与授权监管方以外的交易无关节点的概率是可忽略的.

性质 3 分析：交易金额与地址隐私性主要针对用户而言. 网络中的每笔交易的交易金额与交易接收方地址以密文或零知识证明的隐私输入的形式出现在交易中. 在交易的$Outputs$字段，交易发起方以交易接收方公钥分别对交易金额与交易地址进行公钥加密；在交易的$Witness_{out}$字段，交易发起方以授权监管方的公钥对交易金额与交易地址进行公钥加密. 此外，交易金额与交易接收方地址还作为零知识证明的隐私输入参与交易$Witness$字段证据的生成. 对于密文形式数据而言，只有持有正确的私钥的节点才能解密密文得到交易的交易金额与交易地址信息，其他节点无法从密文中获取任何信息. 公钥加密体制的安全性保证密文的 CCA2 安全；对于零知识证明隐私输入而言，假设存在不诚实节点通过收集学习网络中交易的零知识证明生成的证据部分获得某交易的交易金额、交易接收

地址信息.这与零知识证明的零知识性相违背，因此，网络中其他成员节点无法从零知识证明生成的证据中得到任何交易金额与交易地址的信息. 综上,公钥加密体制与零知识证明的零知识性保证了方案的交易金额与地址隐私性.

5.2 特性分析

本小节将此方案与部分具有代表性的适用于区块链的隐私保护与监管的方案进行对比，结果如表 1 所示. 综合来看，本文方案兼具交易金额与交易地址的隐私,且不需要授权监管方参与交易确认. 交易上链即在授权监管方的可控范围内,监管粒度细致到每个交易的每一个输入输出. 此外,较于其他方案，本文方案提供了强制监管与区块链修订功能，使授权监管方能执行审计和数据管理.

表 1 适用于区块链的授权监管方案的特性对比

Table 1 Characters of Supervision Scheme

方案	交易数据的隐私保护范围	授权监管方不参与交易确认	交易监管周期	交易监管粒度	强制监管	区块数据管理
CoinJoin[4]	交易间关联	——	——	——	×	×
Monero[7]	交易金额、交易地址	√	交易发起方决定	可提供审计密钥	×	×
ZeroCash[9]	交易金额、交易地址	√	交易发起方决定	可提供审计密钥	×	×
RSCoin[10]	---	×	周期性	下属银行的分帐本	×	×
Solidus[11]	交易金额、交易地址；但无法隐藏银行间交易	×	授权监管方主动发起询问时	银行享有账户私钥	×	×
Zkledger[12]	交易金额、交易地址	√	授权监管方主动发起询问时	包括某时刻账户余额等交易信息	×	×
FavZK[13]	交易金额、交易地址	√	授权监管方主动发起询问时	交易的某些统计结果	×	×
PGC[14]	交易金额	√	交易发起方决定	发起方参与的一连串交易	×	×
本文	交易金额、交易地址	√	交易上链时	每笔交易的每个输出	√	√

6 总 结

本文提出了一种适用于联盟链的兼具隐私保护与授权监管的方案. 首先,本方案结合公钥加密方案与零知识证明技术使得普通用户的交易信息隐私得到保障,解决了普通用户在交易过程中隐私信息保护的基本诉求. 其次,在本方案中授权监管方兼具审计与修订区块的能力. 授权监管方可审计网络中全部交易，在一定程度上可溯源，实现对洗钱、违规融资等违规行为的监管. 最后,授权监管方可以使用变色龙哈希函数的陷门密钥可实现对区块上违规信息的修订,阻断了交易不相关的违规消息的进一步传播，及时消除不良影响. 此外，就效率方面，在此方案中，零知识证明的证据的个数与交易输出的个数呈正相关,使用非交互式零知识证明方案证明生成时开销较大,因此提高隐私保护与授权监管方案的效率是下一步研究中应重点考虑的问题.

References:

[1] Nakamoto S. Bitcoin:a peer-to-peer electronic cash system[EB/OL]. https://bitcoin.org/bitcoin.pdf,2021.

[2] 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.

[3] Zhang A, Bai X Y. Survey of research and practices on blockchain privacy protection[J]. Journal of Software, 2020, 31(5):1406-1434.

[4] Maxwell G. CoinJoin: Bitcoin privacy for the real world[EB / OL]. https://bitcointalk.org/index.php?topic=279249 [1].

[5] Ruffing T, Moreno-Sanchez P, Kate A. CoinShuffle: practical decentralized coin mixing for bitcoin[C]//Proceeding of the 19th European Symposium on Research in Computer Security, Springer-Verlag Press, 2014: 345-365.

[6] Heilman E, AlShenibr L, Baldimtsi F, et al. TumbleBit: an untrusted Bitcoin-compatible anonymous payment hub[C]//Proceedings of the Network and Distributed System Security Symposium, Internet Society, 2017:1-15.

[7] Saberhagen N. Cryptonote v 2.0[EB / OL]. https://cryptonote.org/whitepaper.pdf [2].

[8] Miers I, Garman C, Green M, et al. Zerocoin: anonymous Distributed E-Cash from Bitcoin[C]//IEEE Symposium on Security and Privacy, IEEE Press, 2013: 397-411.

[9] Ben-sasson E, Chiesa A, Garman C, et al. Zerocash: Decentralized anonymous payments from bitcoin[C]//IEEE Symposium on Security and Privacy, IEEE, 2014:459 - 474.

[1] https://bitcointalk.org/index.php?topic=279249

[2] https://cryptonote.org/whitepaper.pdf

[10] Danezis G,Meiklejohn S.Centrally banked cryptocurrencies[C]//Proceedings of the 23th Network and Distributed System Security Symposium,Internet Society,2016:1-14.

[11] Cecchetti E,Zhang F,Yan J,et al.Solidus: confidential distributed ledger transactions via PVORM[C]//Proceedings of the ACM SIGSAC Conference on Computer and Communications Security，2017:701-717.

[12] Narula N,Vasquez W, Virza M.ZKLedger: privacy-preserving auditing for distributed ledgers[C] // Proceedings of the 15th USENIX Symposium on Networked System Design and Implementation,USENIX,2018:65-80.

[13] Kang H,Dai T,Jean-Louis N,et al.FabZK: supporting privacy-preserving, auditable smart contracts in hyperledger fabric[C]//Proceedings of 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks,2019:543-555.

[14] Chen Y,Ma X,Tang C,et al. PGC: decentralized confidential payment system with auditability[C]// Proceedings of European Symposium on Research in Computer Security,Springer,2020:591-610.

[15] Deuber D,Magri B,Thyagarajan S. Redactable Blockchain in the Permissionless Setting[C]//Symposium on Security and Privacy,IEEE,2019:645-659.

[16] Ateniese G,Magri B,Venturi D,et al.Redactable blockchain-or－rewriting history in bitcoin and friends[C]//EEE European Symposium on Security and Privacy，2017：111－126.

[17] Derler D,Samelin K,Slamanig D, et al. Fine-grained and controlled rewriting in blockchains: chameleon-hashing gone attribute-based[C]//Proceedings of the 26th Network and Distributed System Security Symposium, Internet Society, 2019: 1-15.

[18]Li S,Zhao P P,Yu J G,et al. Research and design of data trading platform based on blockchain[J], Journal of Chinese Computer Systems,2021,42(5):1109-1114.

附中文参考文献：

[2] 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.

[3] 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(5):1406-1434.

[18] 李 姝，赵培培，于金刚，等.基于区块链的数据交易平台的研究与设计[J].小型微型计算机系统，2021，42(5):1109-1114.