基于双默克尔树区块结构的交易粒度联盟链修改方案

王冬, 李笑若, 祝丙南

引用本文

王冬, 李笑若, 祝丙南. 基于双默克尔树区块结构的交易粒度联盟链修改方案[J]. 计算机科学, 2024, 51(9): 408-415.

WANG Dong, LI Xiaoruo, ZHU Bingnan. Transaction Granularity Modifiable Consortium Blockchain Scheme Based on Dual Merkel Trees Block Structure [J]. Computer Science, 2024, 51(9): 408-415.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.231000054

基于双默克尔树区块结构的交易粒度联盟链修改方案

王 冬 李笑若 祝丙南
河南大学软件学院 河南 开封 475001
河南省智能网络理论与关键技术国际联合实验室 河南 开封 475001
(juliawdd@henu.edu.cn)

摘 要 随着区块链技术的蓬勃发展,以区块链为底层架构的信息系统已应用于包括数字货币、供应链等众多领域。在监管和实际应用双重需求的驱动下,可修改区块链技术因能够进行安全且权责分明的数据治理而成为当前研究的热点。然而,目前的修改方案中仍然存在修改权限过度中心化、修改效率不高等问题。针对上述问题,提出了一种交易粒度联盟链账本修改方案,构建了双默克尔树区块结构,利用椭圆曲线加密和迪菲-赫尔曼秘钥交换技术将变色龙哈希陷门信息(即变色龙哈希私钥)加密存储在区块中,降低密钥分发的系统通信开销。在此基础之上,通过默克尔树将修改权与用户绑定,修改提案受权限节点投票审查,有效防止了修改权的滥用,进一步提高了区块链系统的监管问责能力。实验表明,该联盟链账本修改方案的算法执行速率整体达到毫秒级,并大幅降低了链上数据修改操作的额外开销。

关键词:联盟链;变色龙哈希;可修改区块链;椭圆曲线加密;数据治理
中图分类号 TP309

Transaction Granularity Modifiable Consortium Blockchain Scheme Based on Dual Merkel Trees Block Structure

WANG Dong,LI Xiaoruo and ZHU Bingnan
School of Software,Henan University,Kaifeng,Henan 475001,China
Henan International Joint Laboratory of Intelligent Network Theory and Key Technology,Kaifeng,Henan 475001,China

Abstract With the vigorous development of blockchain technology,information systems based on blockchain have been applied in many fields,including digital currency,supply chain and other fields. Driven by the dual needs of supervision and practical application,modifiable blockchain technology has been developed. However,the current modification scheme still has problems such as excessive centralization of modification authority and low modification efficiency. In response to the aforementioned problems,a transaction-granularity consortium blockchain ledger modification approach is proposed. It constructs a dual Merkle tree block structure,utilizing elliptic curve encryption and Diffie-Hellman key exchange technology to encrypt and store the chameleon hash trapdoor information(i.e.,chameleon hash private key) in the blockchain,reducing the system communication overhead for key distribution. On this basis,the modification right is bound to the user through the Merkle tree,and the proposal is subject to voting review by authorized nodes,which effectively prevents the mining of modification rights and further improves the regulatory warehouse capabilities of the blockchain system. Modification experiments show that the overall algorithm execution speed of this consortium blockchain ledger solution reaches the millisecond level,and significantly reduces the additional overhead of data operations on the chain.

Keywords Consortium blockchain,Chameleon hash,Modifiable blockchain,Elliptic curve cryptography,Data governance

到稿日期:2023-10-10 返修日期:2024-03-14
基金项目:国家自然科学基金面上项目(61872125);河南省高等学校重点科研项目(23A520035);南京大学计算机软件新技术国家重点实验室开放课题(KFKT2022B08);河南省科技攻关项目(232102210192)
This work was supported by the General Program of the National Natural Science Foundation of China(61872125),Colleges and Universities Key Research Project of Henan Province(23A520035),Foundation of National Key Laboratory for Novel Software Technology,Nanjing University(KFKT2022B08) and Henan Province Science and Technology Research Project(232102210192).
通信作者:李笑若(lixiaoruo@henu.edu.cn)

1　引言

区块链是近十几年来最具革命性的新兴技术之一，其本质是利用密码学原理、点对点网络、分布式存储、共识机制等技术所构建的去中心化、不可篡改、可溯源的分布式账本[1]。

依据准入机制，区块链可分为公有链、联盟链和私有链。完全去中心化且不可篡改的公有链使得监管异常困难，区块链容易成为滋生违法犯罪行为的温床[2]；非法、错误或失效数据永久存储于链上，不利于数据治理。私有链是一种只面向特定组织或个人的区块链网络，难以实现大规模分布式计算，无法满足信息系统的应用需求。联盟链兼顾了公有链的去中心化和私有链的高效性，采用部分去中心化，存在部分权限节点，内部指定多个预选的记账节点，可控性较强，交易速度快，成为可修改区块链的首选。目前在联盟链的编辑修改中，变色龙哈希技术应用相对较为广泛，能够在不影响区块链完整性验证的情况下直接修改账本[3]。然而，目前基于变色龙哈希技术的修改方案中分发私钥以及恢复陷门都需要付出高额的通信代价和计算开销，系统效率有待进一步提高。

本文提出基于双默克尔树的交易粒度联盟链修改方案。该方案根据联盟链交易中各交易用户平等地拥有对交易修改的投票权的特点，以变色龙哈希函数为主要工具，实现链上数据的编辑修改，避免了权限节点滥用修改权限，有效抵抗了中心化攻击；该方案将陷门信息直接加密存储在联盟链上，有效降低了分发陷门信息时所必须的链上链下通信代价，提高了系统交互效率；该方案提出的双默克尔树区块结构，在适用区块链账本可修改功能的同时，还保证了交易用户的修改投票权不被破坏和剥夺，从而保护了交易用户的权益。

本文的研究内容和创新成果主要有以下 4 个方面。

1）设计了一种变色龙哈希陷门信息链上加密存储方法，既避免了分发秘钥所需的系统开销，又提高了交易用户获取其陷门信息碎片的效率。

2）提出了双默克尔树可修改区块链结构，用于保存变色龙哈希私钥密文。通过对默克尔根的一致性验证，保证交易用户对修改方案的投票权不受破坏。

3）面向联盟链，在双默克尔树区块结构基础上设计了一种交易粒度的账本修改方案，采用交易用户共同决策的方法，实现链上数据的编辑操控，避免了权限节点滥用修改权。

4）对提出的账本修改方案进行了性能测试，主要分析并测试了关键算法的执行速率、额外存储空间以及安全性。其中，关键算法执行速率整体达到毫秒级。

2　相关工作

当前编辑修改区块链账本的技术方法主要分为两大类[3]：逻辑编辑和物理编辑。2020 年，Yuan 等[4]在其可编辑区块链的综述文章中系统地梳理了可编辑区块链的技术及方法，并讨论了该领域亟待解决的关键问题。

逻辑编辑的核心思路是在不对原始数据进行操作的情况下，使用诸如单链追加[5-6]、双区块链[7]等技术手段实现区块链编辑。但是，逻辑编辑难以有效清除、修改或隐藏被编辑信息。

物理编辑则是在不破坏区块链哈希链路完整性的前提下，直接编辑区块数据。Ren 等[8]基于抗碰撞哈希函数，利用安全的门限环签名方案提出了可删除区块链系统；而后，Ren 等[9]又使用抗碰撞哈希函数，基于 POSpace 共识机制实现可修改的区块链方案。该修改方案适用于交易粒度修改，但通用性较差。

Krawczky 和 Rabin 首先提出了变色龙哈希方案[10]，人为地设下“后门”，进而利用该陷门信息获得哈希碰撞。利用变色龙哈希技术的“可修改区块链”在赋予了区块链修正功能的同时，也最大程度地维护了区块链的基本特性。2017 年，Atenise 等[11]率先提出利用变色龙哈希函数替换区块数据的方案，在改变区块内容的同时保持区块头部哈希不变，维持哈希链路的完整性，实现对区块链的编辑。Li 等[12]、Ashritha 等[13]、Zhao 等[14]引入秘密共享技术，实现对修改权的合理控制。Xue 等[15]使用加法同态的主私钥合成算法和匹配机制，减少了私钥合成过程中的通信量。Lv 等[16]利用改进的变色龙哈希算法，分别提出了多种粒度的修改方案。上述方案中分发私钥以及合并陷门都需要付出高额的通信代价及计算开销，系统效率有待提高[17]。Xu 等[18]通过变色龙哈希和更改传统区块链链式结构的方式实现区块链的可修改，但通用性不强。Shen 等[19]基于双陷门的变色龙哈希构建可修改区块链，并结合无陷门通用累加器和最大序号原则提高区块链系统的安全性。Xu 等[20]基于一次性哈希函数设计可修改区块链系统，将系统维护复杂度降低，但后续修改操作仍面临诸多难题。而后，诸多研究基于物联网轻量级设备进行可修改区块链的优化[21-22]。

本文提出基于椭圆曲线迪菲-赫尔曼秘钥交换[23]（Elliptic Curve Diffie-Hellman key Exchange，ECDH）的主密钥加密方案，将交易数据修改权限平等地赋予交易参与者，修改操作需通过所有交易用户投票，并由权限节点审核，避免了私钥管理的中心化；通过陷门信息链上存储，避免了分发私钥的通信步骤，提高了陷门信息的获取效率。

3　预备知识

3.1　椭圆曲线加密算法

用于加密的有限阈椭圆曲线方程如下：

$$\begin{cases} E_p: y^2 = x^3 + ax + b (\mathrm{mod}\ p) \\ 4a^3 + 27b^2 \neq 0 \end{cases} \tag{1}$$

椭圆曲线 $E_p(a,b)$ 需满足式(1)，即魏尔斯特拉斯标准型。本文加密算法的数学依据如下：

1）公钥加密

$$PK = sk \cdot G \tag{2}$$

Gn 是 G 的阶（$n \cdot G = 0_\infty$），私钥 sk 为小于 n 的整数。式(2)中，PK 为公钥，G 为基点，PK 和 G 均为椭圆曲线上的点。根据椭圆曲线加法法则，已知私钥 sk 和基点 G，求得 PK 是容易的；反之，已知 PK 和 G，求得 sk 是非常困难的。

2）椭圆曲线迪菲-赫尔曼秘钥交换

ECDH 是一种匿名的密钥协商协议，通过该算法，利用由椭圆曲线加密建立的公钥与私钥对，在一个不安全的通道中建立起安全的共有加密资料。加密函数 $Encrypt(m,r) \rightarrow C$ 构成如下所示：

$$C=(c_1,c_2)=(m+r\cdot PK,r\cdot G) \tag{3}$$

其中，r 为随机数，m 为明文，经过椭圆曲线加密计算最终获得密文 C。

解密 $m=c_1-sk\cdot c_2$ 方法如下：

$$m=c_1-sk\cdot c_2 \tag{4}$$

本文的变色龙哈希私钥加解密算法将以 ECDH 为基础进行修改实现。

3.2 变色龙哈希算法

Krawczky 提出的变色龙哈希方案由 4 个算法构成。在变色龙哈希方案中有一个人为设下的陷门，未知陷门信息时，方案满足抗碰撞性；而已知陷门时，找到哈希碰撞[15]则非常容易。

1) 初始化函数 $Setup(\lambda)\rightarrow pp$

通过输入安全参数 λ，构造满足安全参数的大素数 p,q，其中 p,q 满足 $p=kq+1$。选取乘法循环群 $\mathbb{Z}_p^*$ 中阶为 q 的元素 g，输出公共参数 $pp=(p,q,g)$。

2) 秘钥生成函数 $KeyGen(pp)\rightarrow Hsk,Hpk$

输入公共参数，在乘法循环群 $\mathbb{Z}_q^*$ 中随机选择指数 x，计算 $h=g^x$。最后得到变色龙哈希私钥 $Hsk=x$，变色龙哈希公钥 $Hpk=h$。

3) 哈希函数 $Hash(Hpk,m,\tau)\rightarrow CH$

输入公钥 Hpk、原文 m 和可变参数 τ，其中 m 和 τ 均为 $\mathbb{Z}_q^*$ 中的元素，计算哈希值 $CH=g^m h^\tau \bmod p$。

4) 可变参数锻造函数 $Forge(Hsk,m,\tau,m')\rightarrow\tau'$

输入私钥 Hsk、原文 m、可变参数 τ 和新明文 m'，其中 m,τ,m' 均为 $\mathbb{Z}_q^*$ 中的元素。计算过程如下：

(1) $CH=g^m h^\tau=g^{m'}h^{\tau'} \bmod p$

(2) $m+x\tau=m'+x\tau' \bmod q$

(3) $\tau'=(m-m'+x\tau)\cdot x^{-1} \bmod q$

计算出新的可变参数 τ'，使得原文修改后哈希值不变。

4 联盟链账本修改方案设计

4.1 方案概述

在本文的交易粒度区块链可修改方案中，实现交易数据修改时，只需要通过变色龙哈希陷门计算该交易哈希相关的新可变参数，从而在交易数据改变后，使得交易的哈希值不发生改变。修改流程如图 1 所示。

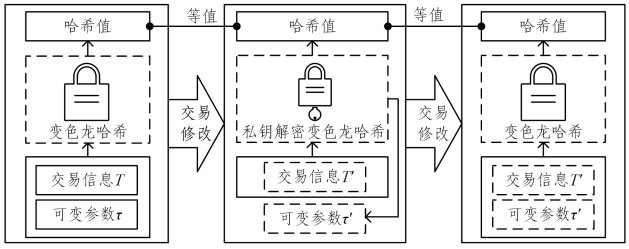


图 1 替换交易哈希方案的流程

Fig. 1 Flow of replaceing transaction hash program

为保障区块链系统的安全性并避免修改权限的滥用，在本文的可修改联盟链方案中，每笔交易都会随机产生一个对应该交易的变色龙哈希私钥，且私钥通过改进后的 ECDH 算法生成变色龙哈希私钥密文(Chameleon Hash Secret key Ciphertext，CHSC)并记录在区块链上，只有交易用户可使用用户私钥解密该交易对应的部分密文信息，当所有交易用户共同解密密文后才能获取变色龙哈希陷门信息。

该变色龙哈希函数对于没有陷门信息的用户而言，仍然满足抗碰撞性；当拥有陷门信息时，可以运行可变参数锻造函数 $Forge(Hsk,m,\tau,m')$ 找到碰撞，使得修改前后哈希值不变，从而满足区块的可验证性。可变参数锻造函数已在本文第 3 章中阐述。

对区块链交易的变色龙哈希陷门信息采用与产生用户公、私钥相同的椭圆曲线加密标准，完成加密上链，使得用户无需承担区块链可修改操作引入的额外密钥管理问题；区块链系统中的全节点将存储包括 CHSC 的所有链上数据。在本文提出的可修改区块链中，某笔交易中包含的所有用户被称为交易用户 T_{users}，它们拥有对于该笔交易的修改方案投票权和部分变色龙哈希陷门信息解密能力。

4.2 双默克尔树区块结构

秘密分享交易粒度修改所产生的大量变色龙哈希私钥，将产生巨大的系统通信开销。为解决上述问题，本文构建了适用于可修改区块链的双默克尔树区块结构，并提出了一种变色龙哈希陷门信息存储方法。新区块结构如图 2 所示。

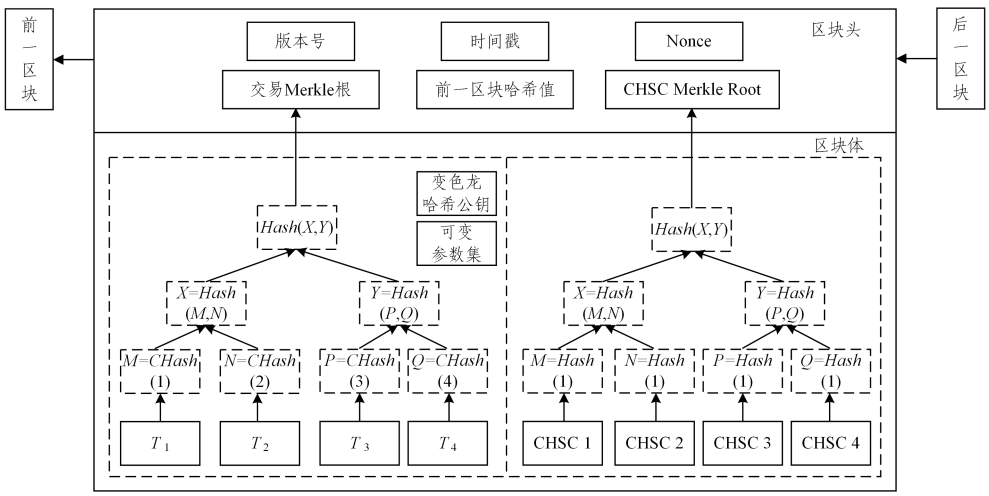


图 2 双默克尔树区块结构图

Fig. 2 Structure of double Merkel tree block

在该区块结构中，区块体由两部分构成，一部分是交易数据，另一部分是 CHSC 数据。在区块中，变色龙哈希私钥密文、变色龙哈希可变参数、变色龙哈希公钥与区块中的交易一一对应。通过二叉树可以快速归纳和校验区块数据的存在性和完整性[24]，区块前后向链接仍通过传统交易 Merkle 根实现，区块唯一性由两个 Merkle 根共同保证。

双默克尔树区块结构由引入变色龙哈希的默克尔树和哈希默克尔树构成。图 2 中区块体部分，左树通过变色龙哈希的性质，使得区块链历史交易可修改；右树（密文默克尔树）实现密文链上存储，同时使得密文中蕴含的修改密钥与权益用户绑定，无法篡改，从而实现交易用户修改权限不受恶意用户破坏，有效保证交易用户的权益。

因此，本文在区块头中加入了 CHSC 的 Merkle 根，通过 CHSC Merkle 根将每笔交易与其初始交易用户进行绑定，有效保证了账本交易修改前后，交易用户及其部分陷门信息解密能力不发生改变。若权限节点在修改账本时作恶，将陷门信息解密权限赋予非初始交易用户，则会使 CHSC Merkle 根改变，区块便无法通过完整性验证。

通过变色龙哈希私钥密文上链，减少了系统的通信开销，保证了交易用户直接从链上解密获取相关陷门信息碎片的效率。

4.3　变色龙哈希私钥生成

在方案中，变色龙哈希私钥由联盟链中预选的记账节点生成，通过 $Setup(\lambda)$ 和 $KeyGen(pp)$ 函数由联盟链记账节点对各项交易生成一一对应的变色龙哈希公私钥对和可变参数，并对变色龙哈希私钥进行加密，生成变色龙哈希私钥密文；将生成的密文写入区块，实现链上存储。

4.4　变色龙哈希私钥加密与还原算法

本节将详细阐述变色龙哈希私钥密文的生成方法和变色龙哈希私钥的还原方法。

4.4.1　基于 ECDH 的陷门信息加密算法

将 ECDH 算法扩展到多用户，秘密信息被多用户的公钥加密，聚合生成 CHSC，从而实现修改权的多用户共同管理。方法如下。

$$\begin{aligned} CHSC &= Encrypt(Hsk, r, PK_{[n]}) \\ &= (Hsk + rPK_1 + rPK_2 + \cdots + rPK_n, rG) \\ &= (Hsk + \sum_{n}^{i=1} r \cdot PK_i, rG) \end{aligned} \tag{5}$$

输入变色龙哈希私钥 Hsk、随机数 r 和交易用户公钥 $CHSC \leftarrow (C_1, C_2)$ 集合，通过运算获得 $CHSC \leftarrow (C_1, C_2)$。其中，$CHSC$ 由 C_1 和 C_2 构成。

$$C_1 = Hsk + \sum_{n}^{i=1}(r \cdot PK_i) \tag{6}$$

$$C_2 = r \cdot G \tag{7}$$

变色龙哈希私钥密文生成伪代码如算法 1 所示。

算法 1　算法 1 变色龙哈希私钥密文生成 $GenerateCHSC(Hsk, PK_{[n]}, r)$

输入：变色龙哈希私钥 Hsk，交易用户公钥集合 $PK_{[n]}$，伪随机数 r

输出：变色龙哈希密文 CHSC

```
1. FOR i 1 TO n STEP 1
2. DO medium←ECC[Hpk[i]+medium] /* ECC[]为椭圆曲线上运算，medium 初始值为空 */
3. END
4. Hsk_ec←Embed[Hsk] /* Embed[]为明文嵌入[25]，将转为椭圆曲线上一点 Hsk_ec */
5. C1←ECC[Hsk_ec+r·medium]
6. C2←r·G //G 为输入椭圆曲线的基点
7. RETURN CHSC←(C1,C2)
```

算法时间复杂度为 $O(n)$。

4.4.2　私钥还原算法

输入 CHSC 和用户私钥集合 $sk_{[n]}$，通过代入式（6）、式（7），通过椭圆曲线运算求得 Hsk，如式（8）所示：

$$\begin{aligned} Decrypt(CHSC, sk_{[n]}) &= \sum_{n}^{i=1}(C_1 - sk_i \cdot C_2) - (n-1) \cdot C_1 \\ &= C_1 - r \cdot (\sum_{n}^{i=1} PK_i) = Hsk \end{aligned} \tag{8}$$

在原算法基础上通过引入多用户，将获取陷门信息的能力赋予交易用户，计算方法在第 3 章中已详细阐述。

1）在区块链系统中进行通信直接传递私钥是不安全的，因此用户将通过用户私钥 sk_T 解密部分 CHSC 获得变色龙哈希陷门信息碎片 Hsk_{piece}，并将该碎片传递给联盟链中的权限节点。$DecodeCHSC(sk, CHSC) \rightarrow Hsk_{piece}$ 计算过程如下所示：

$$Hsk_{piece} = C_1 - r \cdot PK_T = C_1 - sk_T \cdot C_2 \tag{9}$$

2）当权限节点获取交易中全部交易用户的变色龙哈希陷门碎片 Hsk_{piece} 后，可以恢复变色龙哈希私钥。变色龙哈希私钥恢复如图 3 所示，伪代码如算法 2 所示。

算法 2　变色龙哈希私钥恢复 $RecoveryHsk(Hsk_{piece[n]}, CHSC)$

输入：陷门碎片集合 $Hsk_{piece[n]}$，变色龙哈希密文 CHSC

输出：变色龙哈希私钥 Hsk

```
1. IF n==交易用户数 THEN /* 需要获取所有交易用户的陷门碎片 */
2. FOR i 1 TO n STEP 1
3. DO Medium←ECC[Hsk_piece[i]+medium]/* 为椭圆曲线上运算，初始 medium 值为空 */
4. END
5. Hsk_ec←ECC[medium-(n-1)·C1]/* (n-1)为常数运算 */
6. Hsk←Inverse[Hsk_ec] /* Inverse[]为椭圆曲线逆明文嵌入方法 */
7. RETURN Hsk
```

算法 2 时间复杂度为 $O(n)$。

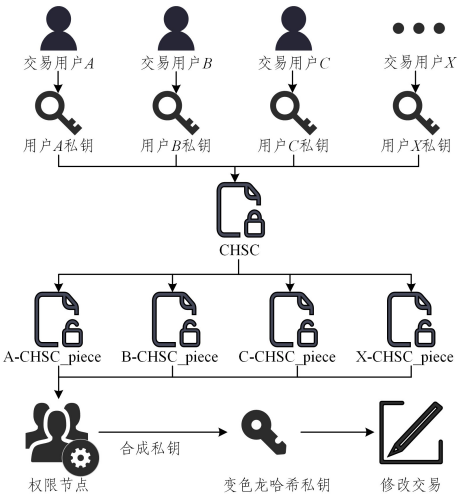


图 3　变色龙哈希私钥恢复流程图

Fig. 3　Flowchart of chameleon hash private key recovery

当权限节点恢复变色龙哈希私钥后，通过 $Forge(Hsk, m, \tau, m') \rightarrow \tau'$ 实现哈希碰撞，重写区块交易数据，修改历史交易。

4.5 联盟链账本修改流程

当需要对历史某一区块交易信息进行更改时，方案包含3个阶段：投票阶段、权限节点审核修改阶段和更改确认阶段。具体流程如下：

1)投票阶段

(1)联盟链用户 P_u 发起针对某笔历史交易 T_i 并将其交易内容 m 修改为 m' 的修改请求 R_u，并对请求 R_u 签名得到 σ_u，广播(R_u，σ_u)给联盟链中交易 T_i 的交易用户 T_{users}，开启投票阶段。

(2) T_{users} 收到请求后，若同意修改，则对用户 P_u 的请求 R_u 签名并广播。

(3)用户 P_u 收集到交易 T_i 中全部交易用户 T_{users} 的签名后，向权限节点发送所有对于 R_u 请求的签名 σ_u。

2)权限节点审核修改阶段

(1)权限节点收到交易 T_i 修改请求 R_u 和 T_i 中全部交易用户 T_{users} 的签名 σ_u 后，对请求 R_u 和交易用户 T_{users} 的签名 σ_u 进行审核验证。若同意请求，则开始修改阶段。

(2)权限节点将广播对请求 R_u 和交易用户 T_{users} 的签名，交易 T_i 的交易用户 T_{users} 收到签名后，通过秘钥交换发送变色龙哈希私钥碎片 Hsk_{piece} 至权限节点。

(3)收集到全部 T_{users} 的 Hsk_{piece} 后，权限节点合成变色龙哈希私钥，完成哈希碰撞，将交易内容 m 修改为 m'，可变参数 τ 更改为 τ'，完成历史交易的修改，广播用户 P_u 对请求 R_u 的签名、交易 T_i 的全部交易用户 T_{users} 的投票(T_{users} 针对请求 R_u 的签名)，并完成交易修改后的交易内容签名。

3)更改确认阶段

联盟链中用户收到权限节点的历史交易修改广播后，验证交易用户 T_{users} 的投票、R_u 与修改后内容是否相同、交易修改前后哈希值是否相同，若验证通过，则更新历史区块交易信息并广播。

5 性能分析与实验结果

本章将从方案额外区块空间占用、关键算法执行速率和安全性能方面进行分析和测试，并对比相关的研究方案。为了具体评估方案的性能，本文方案关键算法执行速率实验使用 OpenSSL3.0 密码学库，选用 secp256k1 椭圆曲线标准完成实验代码编写，时间测试采用 C 语言 windows.h 库，通过 CPU 频率计算时间开销。区块链系统对比实验使用 Substrate 区块链框架，通过 pallet 托盘及 runtime 模块开发相应区块链功能，时间测试采用系统时间戳输出计算。

在配置为 Intel(R) Core(TM) i7-12650 CPU、8GB 内存、1TB 硬盘的主机上进行实验。

5.1 方案额外空间占用

本文的方案中，为了减小通信代价，提高秘钥获取效率，提出了双默克尔树的区块结构，并引入了变色龙哈希私钥密文这一概念，因此需要占用额外的区块空间。

相比传统区块结构空间大小 $size_{Block}$，新区块结构空间大小 $size_{NewBlock}$ 新增了变色龙哈希私钥密文空间 $size_{CHSC}$、变色龙哈希私钥密文散列空间 $size_{CHSC\ Hash}$、变色龙哈希公钥空间 $size_{HPK\ set}$ 和可变参数空间 $size_{\tau\ set}$。

改进后的区块头新增了 CHSC Merkle 根，区块体中新增了 CHSC 及变色龙哈希私钥密文散列，其中每笔交易都会产生一个 CHSC。因此，每个区块新增空间大小为：

$$size_{changes} = size_{CHSC} + size_{CHSC\ Merkle} + size_{\tau\ set} + size_{HPK\ set}$$

区块的新增空间大小与区块内所包含的交易数成正相关。由于 CHSC 通过椭圆曲线运算求出，因此长度固定。

在节点链下存储密钥的方案中，密钥空间占用会随着区块链的节点数增多或区块链的运行而不断膨胀，用户需要构建新的数据关系来管理密钥，造成密钥管理难题。而本文的链上加密存储方案，对于用户来说，简单支付验证(Simplified Payment Verification，SPV)节点仅保存区块头以实现验证，而变色龙哈希私钥密文保存在区块体中，因此在 SPV 节点中新型区块结构仅新增 $size_{CHSC\ Hash}$ 这一额外空间占用。表 1 对文献[12,14,16]方案进行了 SPV 节点新增空间的对比。

表 1 SPV 节点新增空间占用的对比

Table 1 Comparison of added space for SPV nodes

方案	SPV 额外空间占用
Li 等[12]	$size_{HPK\ set} + size_{\tau\ set} + size_{HPK\ set}$
Zhao 等[14]	$size_{HPK\ set} + size_{\tau\ set} + size_{HPK\ set}$
Lv 等[16]	$size_{HPK\ set} + size_{\tau\ set} + size_{HPK\ set}$
Ours	$size_{CHSC}$

文献[12,14,16]的方案均通过用户链下存储节点相关的变色龙哈希子密钥，引入了密钥管理问题及密钥膨胀问题。Zhao 等[14]的方案中引入追责功能，此处对比不计入因该功能产生的额外空间占用。通过对比可得出，随着区块用户 SPV 节点运行，新增空间小于其他对比方案。但区块链系统中全节点需要额外存储链上密文，以确保可修改区块链系统的可靠性，因此全节点的空间占用将大于其他方案。

5.2 关键算法的执行效率

关键算法的执行效率影响联盟链修改行为的运行效率，且与算法安全参数的选取有直接联系。本文算法中选取的安全参数为 256，即变色龙哈希算法和椭圆曲线加密算法的私钥比特位为 256 位。

模拟执行算法，在 CHSC 生成算法中默认权限节点已获取并存储交易用户公钥；Hsk 恢复算法默认权限节点已获取并存储交易用户传递的 Hsk_{piece}，直接从内存储获取数据并执行相关计算任务，并记录算法运行开始至结束的执行时长。分别模拟不同交易用户个数的场景，进行 200 次实验，结果如表 2 和表 3 所列。

表 2 CHSC 生成算法的执行效率

Table 2 CHSC generation algorithm execution efficiency

交易用户数	运行次数	最大值/ms	最小值/ms	平均值/ms	方差/ms^2
2	200	14.466	6.355	7.433	1.438
5	200	16.864	6.389	7.452	1.063
10	200	17.148	6.467	7.552	0.948
15	200	19.354	6.546	7.669	1.481
20	200	20.513	6.669	7.736	1.716

表 3　Hsk 恢复算法的执行效率

Table 3　Hsk recovery algorithm execution efficiency

交易用户数	运行次数	最大值/ms	最小值/ms	平均值/ms	方差/ms^2
2	200	0.1324	0.0377	0.0441	0.0001
5	200	0.2698	0.0873	0.1041	0.0004
10	200	0.4896	0.1631	0.1952	0.0024
15	200	0.5749	0.2382	0.2705	0.0014
20	200	0.8961	0.3162	0.3825	0.0072

由于 CHSC 生成算法和变色龙哈希私钥恢复算法需要用到椭圆曲线标量乘法和与交易用数相同次数的椭圆曲线加法，因此理论上两个关键算法的运行速度与交易用户个数呈正相关。如图 4 所示，关键算法执行速率较快，达到毫秒级，交易用户个数对其影响较小，几乎不会对区块链系统运行效率产生影响。

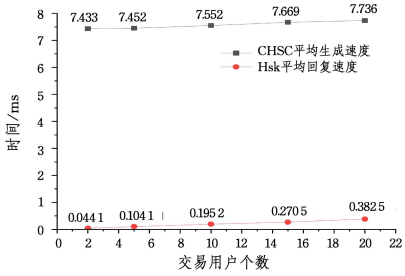


图 4　关键算法的平均执行速度

Fig. 4　Average execution speed of key algorithms

5.3　可修改区块链安全性分析

1）本文的可修改联盟链方案没有指定某种共识算法，当采用工作量证明（Proof of Work，PoW）共识机制时，共识节点或联盟链预选记账节点计算区块 Nonce 值时需将区块头中的 CHSC Merkle 根引入计算；采用 PoS 共识机制时，使用质押代替计算能力，因此最终的挖矿能力受到网络速度的影响。共识节点提供它们的 Token 作为抵押品，以获得验证新区块并成为“验证者”的能力。操作正确，会完成出块。若故意作恶，则会失去一些质押的 Token 作为惩罚。本文提出的新区块结构由于区块体中内容增多，共识节点工作量变大，即每产生一个新区块，需要进行与交易数量相同的 CHSC 生成算法的执行次数，因此联盟链预选记账节点会产生额外的计算开销，但通过表 2 可以看出额外时间开销整体可以接受。因此，本方案可以适应 PoW，PoS 和 PBFT 等现有的共识算法，使得系统在不可信的环境中实现节点之间的相互信任。值得注意的是，共识算法的选择会对区块链系统的可扩展性、安全性和去中心化产生影响。

2）在本文方案中，变色龙哈希私钥被加密存储在区块体中，即链上存储的 CHSC。变色龙哈希函数私钥的安全性保障由离散对数问题（Discrete logarithm Problem，DLP）和椭圆曲线离散对数问题（Elliptic Curve Discrete Logarithm Problem，ECDLP）保证。Secp256k1 椭圆曲线满足当前区块链的安全需求，因此选择合适的安全参数即可保护可修改联盟链系统免受离线攻击。

攻击者需要计算出在椭圆曲线上的离散对数，这在目前的计算资源下是非常困难的，无法在概率多项式时间内完成。更长的密钥提供更高的安全性，但也增加了计算负担。因此，可以根据预计的攻击威胁和性能要求选择合适的密钥长度。

3）变色龙哈希私钥密文碎片的传递对于本文提出的账本修改方案十分关键，掌握了全部密文碎片的节点就可以修改交易内容，因此必须保证密文碎片在同步过程中的保密性，防止其他节点获得正确的密文碎片。若作恶节点非法拦截了关于某笔交易的 n 个密文碎片，只要 n 不等于交易用户个数，根据 ECDH 算法的性质，攻击者就不能通过变色龙哈希私钥密文计算出变色龙哈希私钥。

变色龙哈希私钥密文碎片在传输的过程中可能受到侧信道攻击的威胁，如时钟攻击、功耗分析等。为了抵御这些攻击，可以采取额外的防护措施，引入随机化计算过程和可信执行环境等物理层面的安全措施。

4）本文提出的方案中，变色龙哈希函数替换的是内层的交易哈希函数，区块链系统最大限度地保证了可修改特性对系统安全性的影响，提出的新型区块结构中 CHSC Merkle 根与密文合成算法共同保证了交易用户的区块链交易修改权不被破坏和剥夺。合法的账本修改操作不会导致区块的两个 Merkle 根产生改变，可以实现对数据完整性的验证。

5.4　不同方案的对比

现有的以变色龙哈希函数为主要工具的可修改区块链的研究非常重视修改权的限制，但我们主要是通过在多个用户间分享修正权来避免特权滥用。相比之下，本文方案虽然也注重修改权限的限制，但我们从交易用户利益出发，将修改权限设定为交易粒度，并将交易的修改权限赋予该交易所涉及的交易用户，利用联盟链权限节点的优势，对修改特权进行了最大程度的限制，从而更好地提升可修改区块链的用户信任度。本文从秘钥生成粒度、变色龙哈希私钥存储方式、系统通信时间代价、修改权限去中心化程度及面向场景这 5 个方面进行比较，符号表示如表 4 所列，对比结果如表 5 所列。

表 4　时间开销符号对照

Table 4　Time overhead symbol comparison

符号	符号名称
n	平等修改权用户数
SS	秘密共享成本
CH	变色龙哈希函数成本
SD	秘密分发通信成本
SP	秘密传递通信成本

表 5　可修改区块链方案对比

Table 5　Comparison of modifiable blockchain solutions

方案	秘钥生成粒度	变色龙哈希私钥存储方式	额外时间开销	修改权限去中心化程度	面向场景
文献[12]	联盟链	全体节点存储	$n(SS+SD+SP)+CH$	半去中心化	联盟链
文献[14]	区块	全体节点存储	$n(SS+SD+SP)+CH$	半去中心化	联盟链
文献[16]	多粒度	权限节点存储	$n(SS+SD+SP)+CH$	多中心化	联盟链
本文方案	交易	链上加密存储	$n(SS+SP)+CH$	多中心化	联盟链

为了讨论可修改操作引入的区块链额外开销，分别就密钥合成、账本修改过程的运行时间与文献[12,14,16]进行对比。系统由10个本地运行的节点构成，其中文献[12,14]方案中秘密共享的阈值为5人，权限节点数为2。使用Substrate区块链框架进行系统中部分模块的运行测试，密码学工具均选择相同系统参数，根据不同方案进行算法编码修改。修改操作的系统额外时间开销对比如图5所示。

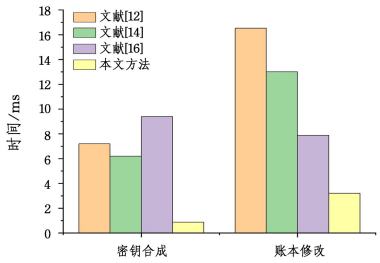


图5 修改操作的额外系统开销对比

Fig. 5 Comparison of additional system overhead for modification operations

由图5可以明显看出，链上存储密文显著降低了修改操作产生的额外开销。

文献[12]的方案改进了变色龙哈希算法，将私钥分配至全部节点，采用随机数生成协议与秘密分享技术随机挑选修改者对区块进行修改，关于私钥的秘密信息由参与秘密共享的所有节点存储。该方案的通信代价会随着链上节点的增多而提高。

文献[14]的方案结合公开可验证秘密共享、零知识证明等工具，实现了编辑权的去中心化和编辑者的随机化，以及已编辑块不能通过验证时的可追责性，且在陷门值分发时不需要秘密通道，从而减少了部分通信开销。

文献[16]详述了多粒度的修改方案，可根据联盟链的需求进行选用。方案由多个节点生成变色龙哈希子私钥，最后通过广播的方式合成主私钥。系统中节点数越多，通信代价就越高。

本文方案将陷门信息加密后进行链上存储，相较于文献[12,14,16]，避免了完成秘钥分发所需的高额通信代价，降低了额外引入的系统开销；而且加密后的陷门信息数据大小固定，并未随着交易用户数量的增加而增大。把交易修改权限分配到交易用户，使修改权限分配更加合理，修改操作受权限节点审核监管，更适用于联盟链系统的各种应用。

结束语 针对可修改联盟链的修改效率和交易粒度修改产生的大量私钥管理问题，本文提出了一种基于双默克尔树区块结构的账本修改方案，通过变色龙哈希陷门信息加密上链的方式，降低了现有研究中修改操作的通信代价；采用交易用户平等享有修改方案投票权的方法，有力保证了交易用户的权益，并且保证了可修改区块链的数据安全性。

进一步工作如下：

1)通过改进预选联盟链记账节点的共识机制，提高可修改区块链系统抗中心节点作恶能力；

2)优化变色龙哈希算法，进一步提高修改效率和系统安全性；

3)优化链上存储私钥密文的方案，减少全节点的额外存储空间占用。

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] CHEN C. Key Technology in Alliance Chain and Challenges in Monitoring Blockchain[J]. Electric Power Equipment Management, 2019(11): 20-21.

[3] PANG J, LIU C, HAO K, et al. Research on Editable Blockchain Model Based on Temporal Index[J]. Journal of Frontiers of Computer Science and Technology, 2023, 17(5): 1180-1188.

[4] YUAN Y, WANG F Y. Editable blockchain: models, techniques and methods[J]. Acta Automatica Sinica, 2020, 46(5): 831-846.

[5] PUDDU I, DMITRIENKO A, CAPKUN S. μchain: How to Forget without Hard Forks[J/OL]. http://eprint.iacr.org/2017/106.pdf.

[6] POLITOU E, CASINO F, ALEPIS E, et al. Blockchain mutability: Challenges and proposed solutions[J]. IEEE Transactions on Emerging Topics in Computing, 2019, 9(4): 1972-1986.

[7] MARSALEK A, ZEFFERER T. A correctable public blockchain [C]// 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). IEEE, 2019: 554-561.

[8] REN Y L, XU D T, ZHANG X P, et al. Deletable blockchain based on threshold ring signature[J]. Journal on Communications, 2019, 40(4): 71-82.

[9] REN Y L, XU D T, ZHANGX P, et al. Scheme of revisable blockchain[J]. Journal of Software, 2020, 12: 3909-3922.

[10] KRAWCZYK H M, RABIN T D. Chameleon hashing and signatures: U. S. Patent 6, 108, 783[P]. [2000-08-22].

[11] ATENIESE G, MAGRI B, VENTURID, et al. Redactable blockchain-or-rewriting history in bitcoin and friends[C]// 2017 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, 2017: 111-126.

[12] LI P, XU H, MA T, et al. Research on fault-correcting blockchain technology[J]. Journal of Cryptologic Research, 2018, 5(5): 501-509.

[13] ASHRITHA K, SINDHU M, LAKSHMY K V. Redactable blockchain using enhanced chameleon hash function[C]// 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS). IEEE, 2019: 323-328.

[14] ZHAO X, ZHANG Z, LI Y. An Editable and Accountable Blockchain Scheme[J]. Journal of Cyber Security, 2022, 7(5): 19-28.

[15] XUE Q, XUE Z, WANG C, et al. One modifiable blockchain scheme based on additive homomorphic encryption algorithm[J]. Application Research of Computers, 2022, 39(11): 3232-3237.

[16] LV W, WEI S J, YU M H, et al. Research on Verifiable Blockchain Ledger Redaction Method for Trusted Consortium[J]. Chineses Journal of Computers, 2021, 44(10): 2016-2032.

[17] WANG R M, WU J Y, ZHANG J H. Blockchain secure data sharing model based on secret sharing [J]. JoCQUPT, Natural

Science Edition，2023，35(6)：1145-1153.

[18] XU G，SUN H. Modifiable Blockchain Based on Chebyshev Polynomial and Chameleon Hash Function[C]// International Conference on Web Information Systems and Applications. Cham：Springer International Publishing，2022：732-739.

[19] SHEN J，CHEN X，LIU Z，et al. Verifiable and Redactable Blockchains With Fully Editing Operations[J]. IEEE Transactions on Information Forensics and Security，2023，18：3787-3802.

[20] XU Y，XIAO S，WANG H，et al. Redactable blockchain-based secure and accountable data management[J]. IEEE Transactions on Network and Service Management，2024，21(2)：1764-1776.

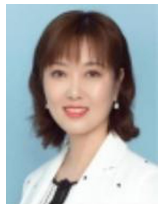
[21] LI F，XU H，SONG Q，et al. BLMA：Editable Blockchain-Based Lightweight Massive IIoT Device Authentication Protocol[J]. IEEE Internet of Things Journal，2023，10(24)：21633-21646.

[22] SHAO W，WANG J，WANG L，et al. Auditable Blockchain Rewriting in Permissioned Setting with Mandatory Revocability for IoT[J]. IEEE Internet of Things Journal，2023，10(24)：21322-21336.

[23] HAAKEGAARD R，LANG J. The elliptic curve diffie-hellman (ecdh)[J/OL]. https://koclab. cs. ucsb. edu/teaching/ecc/project/2015Projects/HaakegaardLang. pdf，2015.

[24] MERKLER C. Protocols for public key cryptosystems [C]// Proceedings of the 1980 IEEE Symposium on Security and Privacy. Oakland，CA，USA：IEEE，1980.

[25] ZHANG X，TONG W，WANG T，et al. Cipher texts generation method in elliptic curve cryptography based on plaintext length [J]. Journal of Computer Applications，2015，35(10)：2863-2866，2876.



WANG Dong，born in 1977，Ph.D，professor，is a member of CCF (No. 22542S). Her main research interests include blockchain and its applications，and so on.

LI Xiaoruo，born in 1999，postgraduate. His main research interests include cryptography and blockchain.

（责任编辑：柯颖）

启动申报 | 2024 年 CCF-绿盟科技“鲲鹏”科研基金正式发布

CCF-绿盟科技“鲲鹏”科研基金项目由 CCF 和绿盟科技于 2017 年共同发起成立，主要面向国内高校、科研机构的全职教师和研究人员，旨在以小微课题的方式支持科研人员的研究与创新，推动科研技术成果转化的同时，促进外部科研机构优秀研发能力与绿盟科技产品价值的深度融合，从而进一步构建互动合作与创新发展的生态圈。

2024 年，CCF-绿盟科技“鲲鹏”科研基金将重点聚焦于数据安全、人工智能安全、云计算安全与安全对抗 4 个方向，计划资助不少于 10 个项目，项目实施期为 1 年，单项资助额度原则上不低于 8 万元。

欢迎广大学者关注并申报本年度鲲鹏基金，申报截止时间为 2024 年 9 月 22 日 24：00(北京时间)，申报人请点击阅读原文、完整填写《项目申报表》并发送至 kunpeng2024@nsfocus. com。逾期将不再接受申报。

申报咨询：尤老师 (010)68438880-5485

技术答疑：kunpeng2024@nsfocus. com

据 CCF 微信公众号