基于区块链的海洋数据安全共享系统构建

赵运星[1]，赵强[1]，黄超[2]，杨涛[1]，周广军[1]，姜作真[1]，胡丽萍[1]

（1.烟台市海洋经济研究院　烟台　264000；2.烟台市海洋与渔业监督监察支队　烟台　264000）

摘要：在海洋数据体量快速积累和数据技术迅猛发展的时代背景下，海洋数据高效管理和价值挖掘成了重点课题之一。文章结合密码学中非对称加密技术（同态加密）和区块链中智能合约技术，构建“双链并行结合智能合约”的地区海洋数据安全共享系统。该双链系统中，“海洋数据注册链”管理共享节点、“海洋数据匹配链”管理待匹配节点，通过智能合约自动执行供需双方的资源有偿共享。该系统既促进了不同地区间的海洋数据共享流转，又保护了资源供应方的合法控制权，实现了对链上流通海洋数据的有效管理与监控，是区块链技术与传统海洋资源调查数据库相结合的海洋资源创新产物，理论上解决了不同地区间海洋经济发展中的海洋基础数据共享问题。

关键词：区块链技术；同态加密；智能合约；海洋数据

中图分类号：F062.2；P71　　**文献标志码**：A　　**文章编号**：1005－9857(2023)01－0037－07

A Secure Sharing System for Marine Data Based on Blockchain

ZHAO Yunxing[1], ZHAO Qiang[1], HUANG Chao[2], YANG Tao[1], ZHOU Guangjun[1], JIANG Zuozhen[1], HU Liping[1]

(1.Yantai Marine Economic Research Institute, Yantai 264000, China; 2.Yantai Marine and Fishery Supervision Detachment, Yantai 264000, China)

Abstract: Under the background of the rapid accumulation of marine data volume and the rapid development of data technology, the efficient management and value mining of marine data has become one of the key topics. This paper has constructed a regional marine data sharing system, which combined asymmetric encryption technology and smart contract technology in blockchain. In this double-chain system, the marine-data-supply-chain includes the sharing nodes, and the marine-data-demand-chain includes the nodes to be matched. The system achieves decentralization, safe and efficient sharing, voluntary circulation of value, effective growth of marine data resources by smart contracts in blockchain, which not only promotes the sharing and circulation of marine data between different regions, but also protects the legal control rights of resource suppliers. This system is a combination between blockchain technology and traditional marine resources survey database and, will manage to solve the problem of data sharing in the develop-

收稿日期：2022-05-10；**修订日期**：2022-12-22

基金项目：山东省重点研发计划项目“脉红螺种苗规模化生态扩繁技术研究”(2019GHY112022).

作者简介：赵运星，硕士，研究方向为海洋经济学

通信作者：胡丽萍，高级工程师，博士，研究方向为贝类遗传育种和海洋经济学

ment of marine economy in different regions theoretically.

Keywords: Blockchain technology, Homomorphic encryption, Smart contract, Marine data

0 引言

大数据时代的到来,使得各类海洋数据快速累积增长,给海洋领域管理变革带来了新的契机与挑战。目前,我国在海洋领域内具有丰富的数据资源和应用市场优势,因而海洋数据开放共享具有非常大的经济价值和社会价值。中国沿海城市众多,不同城市的海洋产业发展不尽相同。部分城市粗放的海洋经济开发方式阻碍了其海洋经济发展,也有城市因细致的海洋产业布局而实现经济高质量发展。我国在海洋数据应用研究方面起步较晚,仍存在数据资源各自孤立、信息缺乏共享、数据利用率低等问题。实现不同区域间的海洋数据共享,可使不同城市在对海洋资源的管理、保护、开发和利用上能够相互学习,取长补短,对我国沿海城市海洋经济平衡和高质量发展具有重要意义。

然而,海洋数据具有获取难度大、数据流通流程复杂甚至包含隐私性等特点,实现海洋数据的安全共享是解决问题的关键。云计算和云存储的出现解决了大数据存储的问题,Collier 等[1]、Li 等[2]、Haskew 等[3]、Biswas 等[4] 提出将“数据上云”,由“第三方”托管,并实施必要的安全机制保证数据的安全性和隐私性,解决了不同数据的共享问题。对于云上数据的安全问题,Cheng 等[5]和 Shen 等[6]提出一个将数据分割为有序数据列的方案,通过在多个云存储设备上存储相关数据列保证了大数据的安全问题。李新等[7]提出一种可实现发送方在加密前规定访问结构的云存储 CP-ABE 方案,丰富了加密结构的灵活性和用户权限的可描述性。

随着 Nakamoto[8] 提出区块链(blockchain)这一概念,学者在数据隐私和安全性方面的研究有了更多进展。Wang 等[9]提出一个结合身份加密和属性加密的加密方案,不仅通过基于身份的签名实现了数字签名的真实有效性,而且通过区块链技术实现了数据的可追溯性、完整性。董黛莹等[10]提出一个加入改进的拜占庭容错系统共识机制的数据共享模型,可为数据安全和隐私存储提供保障,减少数据周转时间。智能合约作为一个成熟的区块链时代产物,如何通过在区块链上部署智能合约,实现所需功能的自动实现一直是现代学者研究的热点。Dagher 等[11]提出一个在区块链上部署智能合约的隐私保护框架,在节点注册初期设计多个智能合约,确保数据供应方拥有个人数据所有权以及控制权,可实现加入节点、更改权限等多个现实场景的应用。在此基础上,徐文玉等[12]提出一个使用同态加密的隐私保护方案,通过增加“保险公司”节点,保证了数据隐私性的同时,实现了基于智能合约的保险公司自动理赔场景。Culver[13] 提出一个只有数据供应者、政府和数据需求者参与的权限区块链,通过在智能合约上编写三方之间复杂的协议代码,保证了操作透明性。Ekblaw 等[14]提出一个基于区块链的去中心化系统,该系统通过在区块链上存储数据索引的 Hash 值,为数据需求方提供完整的日志,同时通过一系列智能合约提高系统的可操作性。徐健等[15]提出一个包含 3 个智能合约的安全存储访问方案,结合区块不可篡改性和非对称加密技术,有助于解决数据跨域共享、身份跨域验证问题。

梳理现有文献可知,当前基于区块链的数据隐私保护是各国研究的重点问题。因此,为了更好地实现海洋信息在供应方和需求方之间的高效流动,本研究提出一个基于区块链的“海洋数据安全共享系统”,该系统具有以下特点:①海洋数据上链,去中心化、防止篡改。通过合理整合和利用沿海地区海洋资源的调查数据(数据供应方),为其他海洋资源利用率不足、海洋经济发展相对落后的地区(数据需求方)提供数据借鉴、理论资源索引和决策支持。②区块链上部署 4 个智能合约,实现系统上每一次交易的自动执行。③设置访问控制,阻止恶意攻击者对隐私数据的窃取。

1 “海洋数据安全共享系统”方案设计

针对沿海地区数据流通性、共享性较差的问题,结合密码学中非对称加密技术(同态加密)和区

块链中智能合约技术，本研究提出一个基于区块链技术的“海洋数据安全共享系统”。该双链系统通过智能合约自动执行供需双方海洋资源的有偿共享，实现数据共享过程的去中心化、可监管、防篡改、支持多方参与等优良性质。此外，由于该系统具有双链并行的特点，因此运算速度也将大幅提高。

1.1　ElGamal 公钥加密体制

“海洋数据安全共享系统”基于常见的 ElGamal 公钥加密体制，扩大了该系统的应用与理解范围。ElGamal 公钥加密过程包含 3 个阶段。

(1)密钥生成阶段：设 p 是一个大素数，使得 $(Z_{p'}^{*},\cdot)$ 上的离散对数问题难解。令 $\alpha \in Z_p^*$ 是一个本原元，明文集 X 为 Z_p^*，密文集 C 为 $Z_p^* \times Z_p^*$。选择随机数 a，定义密钥数组 K。

$$K=\{(p,\alpha,a,\beta) \mid \beta \equiv \alpha^a (\mathrm{mod}p)\}$$

则公钥 $\mathrm{pk}=(p,\alpha,\beta)$，私钥 $\mathrm{sk}=a$。

(2)加密阶段：对 $K=(p,\alpha,a,\beta)$，以及随机选取的一个(秘密)随机数 $k \overset{R}{\in} Z_{p-1}$，定义密文 C。

$$C=e_K(X,k)=(y_1,y_2)$$

式中：e_K 为加密算法；X 为明文；密文 $C=(y_1,y_2)$，由明文和随机数 k 共同决定，其中，$y_1=\alpha^a \mathrm{mod}p$，$y_2=X\beta^k \mathrm{mod}p$。

(3)解密阶段：解密方接收到密文 C 后，计算明文 X。

$$X=d_K(y_1,y_2)=y_2(y_1^a)^{-1}\mathrm{mod}p$$

式中：d_K 为解密算法。

同时，ElGamal 公钥加密体制为乘法同态。

设明文空间元素 x、y，$k_1,k_2 \overset{R}{\in} Z_{p-1}$ 通过 ElGamal 公钥加密体制进行加密，分别得到密文：

$$E(x,k_1)=x\beta^{k1}(\alpha^{k1})^{-1}$$

$$E(y,k_2)=y\beta^{k2}(\alpha^{k2})^{-1}$$

式中：$x\beta^{k1}(\alpha^{k1})^{-1}$ 和 $y\beta^{k2}(\alpha^{k2})^{-1}$ 分别是对明文 x 和 y 加密后得到的密文。则：

$$E(x,k_1,y,k_2)=x\beta^{k1}(\alpha^{k1})^{-1}\cdot y\beta^{k2}(\alpha^{k2})^{-1}=$$
$$(xy)\beta^{k1+k2}(\alpha^{k1+k2})^{-1}=E(xy,k_1+k_2)$$

满足乘法同态性质。

1.2　“海洋数据安全共享系统”流程设计

基于区块链，通过依次部署的 4 个智能合约(海洋数据共识智能合约、注册分类智能合约、自动合同执行智能合约及自动合同签订智能合约)，分步实现一种全新的海洋数据共享系统新模式。该系统通过两链并行结构(海洋数据注册链－海洋数据共享链)，可以自动进行“海洋数据供应地区”与“海洋数据需求地区”的资源共享，实现海洋调查数据在地区间的自主价值流通。表 1 是本研究出现的缩写及其定义，图 1 是本研究构建的“海洋数据安全共享系统”模式图。

表 1　缩写及定义

Table 1　Abbreviation and definition

缩写	变量定义
OD	海洋数据(ocean-data)
MS	海洋数据共享供应方(marine data supplier)
MD	海洋数据共享需求方(marine data demander)
MN	矿工(minor)
SA	监督机构(supervisor agent)
CSG	联盟服务群组(coalition service group)

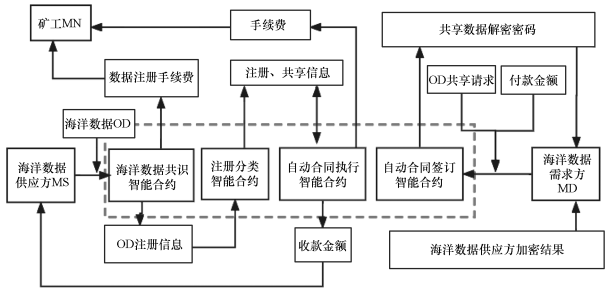

图 1　“海洋数据安全共享系统”模式

Fig.1　Pattern of the secure sharing system for marine data

如图 1 所示，“海洋数据安全共享系统”中包含 3 类主体：“海洋数据供应方 MS”“海洋数据需求方 MD”以及“矿工 MN”。新模式具有如下特点。

(1)系统去中心化，自发运行、高度自治。“匹配需求方”通过支付预先约定好的金额，满足相应智能合约触发条件后，进入匹配系统。当矿工获得一定经济激励(手续费)将自动执行计算任务，保证系统正常运行、去中心化，高度自治。

(2)海洋数据注册链－海洋数据共享链，两链并行结构。系统通过筛选、审查“供应方”提供的海洋数据资源，满足一定要求的数据构成海洋数据注

册链;“需求方”将对供应方感兴趣的待共享信息构成海洋数据共享链。

(3)经济激励保证资源自增长,权益有保障。由于供需关系,使得海洋数据需求方需要支付一定报酬才能使得矿工“挖矿”,完成大量计算工作;而海洋数据供应方也得到数据流通中的价值变现,因此不同种类有效记录资源将实现自增长。

为了成功执行并监管各主体间产生的交易或其他行为,本系统由以下智能合约构成。

(1)供应方角度:海洋数据共识智能合约、注册分类智能合约和自动合同执行智能合约。①供应方将加密后的海洋数据发送至系统,系统自动执行海洋数据共识智能合约,判断数据集是否满足 CSG 等其他共识要求,并在全网公示。②公示期间无异议的海洋数据将通过注册分类智能合约,自动生成合法注册记录供矿工打包成资源区块,并依据不同海洋数据类型自动分类。③匹配方得到矿工发送的有序数组,若通过私钥求解后值为 1,系统运行自动合同执行智能合约,即向供应方支付需求方预付资金,同时也将得到的匹配记录对应对称密钥加密的海洋数据密钥发给需求方,完成共享。

(2)需求方角度:自动合同签订智能合约。自动合同签订智能合约收到海洋数据供应方提供的地区加密待共享海洋数据,通过矿工对链上相关数据库计算,形成对应有序数组并发送至需求方,等待需求方判断有无共享数据。

(3)监管方角度:申诉智能合约和处罚智能合约。①若出现虚假海洋数据、共享结果有误、交易金额异常等情况,供应方或需求方有权提出申诉,自动执行申诉智能合约。②申诉方申诉成功后,自动执行处罚智能合约。

2 “海洋数据安全共享系统”方案实现

2.1 “海洋数据安全共享系统”初始化

(1)系统初始化:“海洋数据安全共享系统”由一个开源社区或一家公司初始发起与构建,即生成两条区块链(海洋数据注册链-海洋数据共享链)各自第一个区块,创世区块。第一个区块中不含交易、流通信息,只记录系统构建时间等其他设计信息;生成各自创世区块后,采用多种方案对“海洋数据安全共享系统”进行宣传推广,让沿海地区海洋管理部门了解此类新模式,并愿意进行尝试,启动系统。

(2)参与主体初始化:新模式中主要主体,“海洋数据供应方 MS”“海洋数据需求方 MD”“矿工 MN”以及“监督机构 SA”。通过向发起方发送各自数字证书(用自己的私钥对用户的身份信息进行签名,该签名和用户的身份信息共同形成证书,如 MAC 码)申请加入系统,参与流通。数字证书作为各主体系统中流通时客户端账号,与真实身份对应,参与主体通过客户端进行各自需求活动。

2.2 “海洋数据安全共享系统”注册流程

“海洋数据安全共享系统”注册流程由以下 4 个步骤完成。

(1)海洋数据供应方申请注册。在私有链上每个节点加入与退出网络需要共识,因此海洋数据供应方需要首先向系统申请注册,发送海洋数据、海洋数据属性集,后续节点进行“共识”投票时依据的判断属性,如地区、经度、纬度、所需海洋数据等,并交付一定的注册手续费用,用于支付矿工算力,同时防止恶意节点注册。

(2)共识审核。系统启动海洋数据共识智能合约,首先对供应方进行联盟群组检验,即通过海洋数据属性集判断此类海洋数据是否满足上链条件,并决定是否进行唯一性检验。其次进行唯一性检验。通过供应方提供的非对称加密后的身份 ID [SHA256(pk,ODdata)=Hash(ID)]判断是否为初次注册节点。这一过程中将注册手续费部分支付给付出审核共识算力的矿工。

(3)分类注册。通过共识审核后的海洋数据将启动注册分类智能合约,根据 CSG 群组分成二级类别(如海洋水温数据、海洋气象数据、海洋化学数据以及海洋生物数据等),在全网公示,经过公示期后智能合约将对其生成合法注册记录并打上注册生效时间戳。

(4)发送最新注册链信息。矿工经过一个固定时间段将各自“挖矿”通过第(2)和第(3)步骤的合法注册记录打包形成区块,广播到全面所有节点进行审核与共识,获得最终共识通过的区块将最终上

链，链接到“海洋数据注册链”末端，矿工也将获得最终上链数据的全部“挖矿”费用。

步骤(1)至步骤(4)完成“海洋数据安全共享系统”注册流程，系统每经过一个固定时间段向客户端发送当前最新海洋数据注册链信息。

“海洋数据注册链”具有如下性质：①“海洋数据注册链”经过固定时间段汇总供应方申请，生成各自身份 ID、记录登记时间并进行“共识”审核，审核通过后生成区块广播至全网、上链。②链上记录一经共识，无法更改。即区块只能新增，无法删减或更改。

2.3 “海洋数据安全共享系统”共享流程

“海洋数据安全共享系统”共享流程由以下 5 个步骤完成。

(1)链上记录预处理。“海洋数据供应方”预先对共享系统中需求方感兴趣的“待咨询”数据进行登记注册(仅注册一次)，进入共享系统。并启动处罚智能合约，保证数据需求方利益。“海洋数据需求方”完成共享系统用户注册。系统自动执行自动合同签订智能合约，需求方开通个人电子钱包，支付相应费用。

(2)海洋数据需求方发出海洋数据查看请求。系统收到需求方公钥($pk_{\_MD}$)和地区加密待共享记录(根据 CSG 群组类别首先进行分类，简化后续计算)，并等待通过矿工对链上相关数据库计算。

(3)系统启动自动合同签订智能合约，生成共享电子合同。海洋数据需求方“电子钱包”中的预付款将被冻结，同时矿工将进行如下操作。

首先，通过强大计算能力使用需求方的公钥($pk_{\_MD}$)，对 CSG 中的加密海洋数据(已通过对称加密)进行运算，记作：

$E_{pk\_MD}(\mathrm{P}_1)$，$E_{pk\_MD}(\mathrm{P}_2)$，$E_{pk\_MD}(\mathrm{P}_3)$，…，严格保持原始顺序。

式中：P_i 为供应方共享海洋数据，$E_{pk\_MD}(P_i)$ 为加密共享海洋数据。

其次，与需求方的地区加密待共享记录记作 $E_{pk\_MD}(M)$ 共同执行第二次计算：

$E_{pk\_MD}(P_1)\times E_{pk\_MD}(M)^{-1}$，$E_{pk\_MD}(P_2)\times E_{pk\_MD}(M)^{-1}$，$E_{pk\_MD}(P_3)\times E_{pk\_MD}(M)^{-1}$，……。

由同态乘法性质有：

$E_{pk\_MD}(P_1\times M^{-1})=E_{pk\_MD}(P_1)\times E_{pk\_MD}(M)^{-1}$，

$E_{pk\_MD}(P_2\times M^{-1})=E_{pk\_MD}(P_2)\times E_{pk\_MD}(M)^{-1}$，

$E_{pk\_MD}(P_3\times M^{-1})=E_{pk\_MD}(P_3)\times E_{pk\_MD}(M)^{-1}$，……。

将加密数值保存在有序数组 $A[M]$ 中，将有序数组 $A[M]$ 和对其数字签名发送给海洋数据需求方。

海洋数据需求方得到有序数组 $A[M]$ 和对其签名，首先，根据公钥验证矿工计算结果的真实性。其次，根据私钥($sk_{\_MD}$)解密数组 $A[M]$ 中数据，若 $P_i=M$，则解密值

$$D_{sk\_MD}[E_{pk\_MD}(P_i\times M^{-1})]=1$$

即海洋数据需求方得到“待咨询”海洋数据，完成数据共享；否则，若：

$$D_{sk\_MD}[E_{pk\_MD}(P_i\times M^{-1})]\neq 1$$

即未找到相关海洋数据共享结果。

(4)系统定时广播新区块待全网审核，只有经过系统审核的区块视为合法流通。需求方通过私钥($sk_{\_MD}$)解密数组 $A[M]$ 中数据，触发自动合同执行智能合约，自动完成“供需双方钱货两清”过程，即供应方发送解密海洋数据，需求方向供应方支付预付款。需要注意的是，当需求方未找到共享数据时，将仅支付 30% 的预付款，目的在于挽回其一定损失。

(5)若出现共享数据不符、交易金额异常等纠纷时，可随时向监管机构申诉，请求处罚，双链系统将无偿提供记录支持。

“海洋数据共享链”主要具有如下性质：①由于每一个区块都有数字签名、时间戳、Merkle 值等数据，“海洋数据共享链”保证了共享数据安全性与公平性。②由于共享数据计算量巨大以及相应信息存储在区块链网络上，因此“海洋数据共享链”实现了分布式记账功能，安全性较高。③参与主体随时申诉、得到监管保障。

3 系统性能分析

3.1 正确性分析

定理：数据需求方利用自身私钥($sk_{\_MD}$)可从有序数组 $A[M]$中得到匹配结果。

证明：设明文空间元素 $x,y,k_1,k_2\in Z_{p-1}$，通

过 ElGamal 公钥加密体制进行加密，分别得到密文：

$$E(P_i)=P_i\,\beta^{k1}(\alpha^{k1})^{-1} \tag{1}$$

$$E(M)=M\,\beta^{k2}(\alpha^{k2})^{-1} \tag{2}$$

则：

$$E(P_i)\times E(M)=P_i\beta^{k1}(\alpha^{k1})^{-1}\times M\beta^{k2}(\alpha^{k2})^{-1}=(P_iM)\,\beta^{k1+k2}(\alpha^{k1+k2})^{-1}=E(P_iM) \tag{3}$$

需求方得到有序数组 $A[M]$，根据私钥($sk_{\_MD}$)解密数组 $A[M]$中数据，若 $P_i=M$，则解密值

$$D_{sk\_MD}[E(P_i)\times E(M)^{-1}]=D_{sk\_MD}[E(P_iM^{-1})]=1 \tag{4}$$

即得到需求方得到“待咨询”海洋数据结果。否则，若：

$$D_{sk\_MD}[E(P_i)\times E(M)^{-1}]=D_{sk\_MD}[E(P_i\,M^{-1})]\neq 1 \tag{5}$$

即需求方未得相关海洋数据结果，完成目标搜索匹配。

3.2 安全分析

(1)若存在恶意供应方提供篡改、无用数据旨在获得非法利益，必须进行供应方认证审核，审核通过方可提供数据，因此供应方完成非法获利行为的概率很低；同时需求方若想要恶意获得隐私数据，首先也需进行节点审核，通过后才可获得矿工计算数据，进行下一步匹配访问，如此多重认证防止非法或恶意节点访问敏感隐私数据。

(2)在所有交互中，只有经过审核认证通过的需求方可获得明文消息。后期若发生申诉等赔偿事故时，区块链将提供交易记录，自动启动申诉、处罚智能合约，保障各方合理权益。

3.3 隐私分析

(1)由初始系统设置，供应方提供记录为对称加密后记录，并默认矿工为“诚实的(即诚实地执行加密协议)”，供应方与矿工之间进行约定在安全信道进行加密运算过程，因此矿工的第一轮加密计算，形成有序加密数组 $A[M]$，并将其发送给匹配方，由匹配方进行解密操作，这在一定程度上保护了双方隐私。

(2)由于匹配方和供应方都在进入系统前进行审核，通过后才能进入私有链上进行数据流通，即任何节点注册时都要认证自身合法性，这也降低了未授权节点访问敏感信息的可能。

(3)本系统中共 4 个主要匹配智能合约和两个后期服务保障智能合约。海洋数据共识智能合约、注册分类智能合约、自动匹配合同执行智能合约为供应方进行数据上链、分类，以及匹配功能，每个合约存储内容相关且有顺序关联，若想跳步进行某一合约无法实现；自动匹配合同签订智能合约为匹配需求方完成自身节点数据认证，进行记录自动匹配合约，只有需求方和供应方同时满足访问条件才能进行系统访问。

4 结论

针对沿海地区海洋数据利用率低、共享性较差的问题，本研究结合密码学中非对称加密技术(同态加密)和区块链中智能合约技术，创新性地提出一个基于区块链技术的“海洋数据安全共享系统”。该双链系统通过智能合约自动执行供需双方海洋资源的有偿共享，实现数据共享过程的去中心化、可监管、防篡改、支持多方参与等优良性质。该系统既促进了不同地区间的海洋数据共享流转，又保护了资源供应方的合法控制权，实现了对链上流通海洋数据的有效管理与监控，是区块链技术与传统海洋资源调查数据库相结合的海洋资源创新产物，理论上解决了不同地区间海洋经济发展中海洋基础数据的共享问题。

参考文献(References)：

[1] COLLIER D S, GRANT R W, ESTEY G, et al. Physician ability to assess Rheumatoid Arthritis disease activity using an electronic medical record-based disease activity calculator[J]. Arthritis Care & Research, 2010,61(4):495－500.

[2] LI Z R, CHANG E C, HUANG K H, et al. A secure electronic medical record sharing mechanism in the cloud computing platform[C]// 2011 IEEE 15th International Symposium on Consumer Electronics (ISCE), Singapore, IEEE, 2011:98－103.

[3] HASKEW J, SAITO K. Implementation of a cloud-based electronic medical record for maternal and child health in rural Kenya[J]. International Journal of Medical Informatics, 2015, 84(5):349－354.

[4] BISWAS S, BABLA A, AKHTER T, et al. Cloud based healthcare application architecture and electronic medical record mining: An integrated approach to improve healthcare system[C]//2014 17th International Conference on Computer and Information Technology (ICCIT), Dhaka, IEEE, 2015:286－291.

[5] CHENG H, RONG C, HWANG K, et al. Secure big data storage and sharing scheme for cloud tenants[J]. China Communications, 2015, 12(6):106－115.

[6] SHEN M, MA B, ZHU L, et al. Cloud-based approximate constrained shortest distance queries over encrypted graphs with privacy protection[J]. IEEE Transactions on Information Forensics & Security, 2018, 13(4):940－953.

[7] 李新，彭长根，牛翠翠.隐藏树型访问结构的属性加密方案[J].密码学报，2016，3(5)：471－479.
LI Xing, PENG Changgen, NIU Cuicui. Attribute-based encryption scheme with hidden tree access structures[J]. Journal of Cryptologic Research, 2016, 3(5):471－479.

[8] NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash system [EB/OL]. [2022－12－12]. https://bitcoin.org/bitcoin.pdf.

[9] WANG H, SONG Y. Secure cloud-based EHR system using attribute-based cryptosystem and blockchain[J]. Journal of Medical Systems, 2018, 42(8):152.

[10] 董黛莹，汪学明.基于区块链的电子医疗记录共享[J].计算机技术与发展，2019，(29)：121－125.
DONG Daiying, WANG Xueming. Research on electronic medical record sharing model based on blockchain[J]. Computer Technology and Development, 2019, (29):121－125.

[11] DAGHER G G, MOHLER J, MILOJKOVIC M, et al. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology[J]. Sustainable Cities and Society, 2018, 39(4):283－297.

[12] 徐文玉，吴磊，阎允雪.基于区块链和同态加密的电子健康记录隐私保护方案[J].计算机研究与发展，2018(55)：2233－2243.
XU Wenyu, WU Lei, YAN Yunxue. Privacy-preserving scheme of electronic health records based on blockchain and homorphic encryption[J]. 2018(55): 2233－2243.

[13] CULVER K. Blockchain Technologies: A whitepaper discussing how the claims process can be improved [EB/OL]. [2022－12－12]. https://www. healthit. gov/sites/default/files/3 － 47 － whitepaperblockchainforclaims_v10.pdf.

[14] EKBLAW A, AZARIA A, HALAMKA J D, et al. A case study for blockchain in healthcare: MedRec prototype for electronic health records and medical research data[J]. Computer Science, 2016.

[15] 徐健，陈志德，龚平，等.基于区块链网络的医疗记录安全存储访问方案[J].计算机应用，2019(39)：1500－1506.
XU Jiang, CHEN Zhide, GONG Ping, et al. Secure storage and access scheme for medical records based on blockchain [J]. Journal of Computer Applications, 2019(39): 1500－1506.