Journal of Computer Applications
计算机应用,2021,41(4):939－944
ISSN 1001-9081
CODEN JYIIDU
2021-04-10
http://www.joca.cn

文章编号:1001-9081(2021)04-0939-06
DOI:10.11772/j.issn.1001-9081.2020111723

基于区块链与可信计算的数据交易方案

张学旺[1,2*],殷梓杰[1],冯家琦[1],叶财金[1],付　康[1]
(1.重庆邮电大学 软件工程学院,重庆 400065;　2.重庆大学 微电子与通信工程学院,重庆 400044)
(*通信作者电子邮箱zhangxw@cqupt.edu.cn)

摘　要:针对当前数据交易过程中数据容易被拷贝的问题以及数据保密的实现,提出一种基于区块链与可信计算的数据交易方案。首先,利用区块链记录数据信息、交易信息以及数据使用记录,这可帮助数据资产确权以及数据溯源;然后,利用可信计算与加密算法来保证交易数据传输安全;最后,用数据主体与数据需求方提供的算法在可信计算环境中完成计算,之后输出结果并加密返回给需求方。所提方案在确保数据主体不泄露数据的情况下,让需求方可以使用数据进行计算,且通过可信加密保证了传输安全。

关键词:数据交易;区块链;数据加密;可信计算;数据溯源
中图分类号:TP309.2　　**文献标志码**:A

Data trading scheme based on blockchain and trusted computing

ZHANG Xuewang[1,2*], YIN Zijie[1], FENG Jiaqi[1], YE Caijin[1], FU Kang[1]
(1. *School of Software Engineering, Chongqing University of Posts and Telecommunications, Chongqing* 400065, *China*;
2. *School of Microelectronics and Communication Engineering, Chongqing University, Chongqing* 400044, *China*)

Abstract: Aiming at the problem of data being easily copied and the realization of data confidentiality in current data trading process, a data trading scheme based on blockchain and trusted computing was proposed. First, the blockchain was applied to record data information, trading information and data usage records, which facilitated to confirm the rights of data assets and data provenance. Then, the trusted computing and encryption algorithms were used to ensure the security of the trading data transmission. Finally, the algorithms provided by the data owners and demanders were applied to complete the calculation in the trusted computing environment, after that, the results were output and encrypted to return to the demanders. In the proposed scheme, the demanders can use the data for calculation without revealing data from the data subjects, and the transmission security is guaranteed through trusted encryption.

Key words: data trading; blockchain; data encryption; trusted computing; data provenance

0　引言

随着大数据相关技术高速发展,大数据[1]相关产业对数据的需求越来越大,但数据往往被少部分人掌握,许多拥有能释放数据价值的人往往拿不到想要的数据。面对这类问题,数据交易的出现可以打破数据孤岛问题,数据的流通能够汇聚高价值数据,满足各类企业、高校团体等对数据的需求,提高数据价值的利用。数据交易对各类大数据产业的创新发展有着深远的意义,大数据的价值可以通过数据交易得以释放[2]。

但由于数据本身的特性——数据的可复制性,加上数据的价值本身就是信息,数据的信息价值可能在数据被"阅读"时便被获取[3],这些特性导致数据交易困难。数据拷贝成本低、维权难,企业并不愿意分享重要数据,且国内数据交易的发展现在正处于初级阶段,交易模式也尚在探索之中,目前还没有一致的标准和规范,数据交易方案需要完善,数据交易缺乏可信、可行的实施方案导致交易无法安全地进行。

目前,主流的数据交易模式为应用程序接口(Application Programming Interface, API)交易[3]和数据包交易,如表1所示。第一种方式解决了数据交易领域中的一部分问题,例如使数据可脱敏以及在一定程度上防止数据被窃取倒卖,但这种模式只能提供部分数据,无法使用完整的数据集,不方便用户对数据进行处理和分析;而第二种数据包交易的模式在实际交易中由于数据的特性导致数据确权难、数据资产容易流失,所以具有较大的争议。

这些交易模式或多或少都存在着一些缺点,无法满足现在数据供应与需求两方之间对数据交易的要求。区块链技术采用一系列密码学算法在非信任节点之间建立信任关系,而不是依赖中心机构的信用背书,这种特殊的安全模型使得区

收稿日期:2020-11-05;**修回日期**:2020-11-28;**录用日期**:2020-12-04。
基金项目:国家重点研发计划项目(2019YFC1511300);工业和信息化部产业技术基础公共服务平台项目(2019-00894-1-1);重庆市基础研究与前沿探索专项重点项目(cstc2019jcyj-zdxmX0008);渝北区大数据智能化科技专项重点项目(2020-02)。
作者简介:张学旺(1974—),男,湖南祁东人,副教授,博士研究生,CCF高级会员,主要研究方向:区块链与物联网、数据安全与隐私保护、大数据与智能数据处理;　殷梓杰(1996—),男,湖南益阳人,硕士研究生,主要研究方向:区块链、数据资产、可信计算;　冯家琦(1995—),男,河南驻马店人,硕士研究生,主要研究方向:区块链、数据溯源;　叶财金(1994—),男,江西高安人,硕士研究生,主要研究方向:区块链、隐私保护;　付康(1997—),男,重庆人,硕士研究生,主要研究方向:区块链。

块链隐私保护不同于传统的隐私保护。区块链凭借不可篡改性以及可追溯性，使得其在数据资产交易领域能够有所应用，区块链可以构建数据资产交易的索引、帮助数据溯源以及确权。

表1 数据交易方式对比

Tab. 1 Comparison of data trading methods

分类	可追溯性	隐私保护	交易风险	复杂程度
API接口交易	低	中	低	中
数据包交易	一般	低	高	低
区块链数据交易	高	中	中	高

本文以区块链与可信计算为基础，非对称加密技术为辅，针对当前数据交易面对的困难，防止数据交易过程中造成的数据二次转让问题以及数据隐私问题，提出一种有效可行的数据交易方案。本文方案主要目的如下：

1)数据供应方上传数据索引信息，通过区块链存储数据交易索引信息；

2)数据需求方购买数据，通过区块链记录数据交易过程与数据使用记录；

3)基于可信计算技术，保证数据使用环境安全、数据不会被泄露；

4)基于可信计算技术，保证数据使用结果无法被窃取。

1 相关工作

1.1 区块链与数据交易

区块链技术在中本聪的比特币[4]热潮下，引起了众多研究领域的广泛关注。区块链[5-6]技术在没有任何可信机构的维持下，使互不认识、互不信任的人之间可以进行交易。以太坊(Ethereum)区块链平台[7]的提出，首次引入智能合约，为区块链提供了更多数字货币以外的应用场景。而随着Linux基金会发布Hyperledger开源区块链项目，其中Hyperledger Fabric针对企业级商用区块链进行应用设计，引入成员管理服务，为区块链应用提供了良好的解决方案。

区块链发展过程中也诞生了许多与数据交易相关的研究。2016年Christidis等[8]研究了区块链与物联网的特性，描述了区块链与物联网结合发展的前景，提出了在区块链上转移数字资产的方法以及如何利用智能合约转移数字资产。物联网发展的同时也会带来海量数据，区块链与物联网有效结合可以提供更好的隐私保护[9-10]。2017年刘敖迪等[11]从区块链的基本框架、技术特征和应用领域多个方面阐述了区块链基本理论和模型，总结了区块链在认证技术、访问控制技术和数据保护技术方面的研究进展。祝烈煌等[12]分析了区块链技术在隐私保护方面存在的优势与不足，描述了现有研究中针对区块链隐私的攻击方法，详细介绍了针对区块链网络层、交易层和应用层的隐私保护机制。

2018年盛念祖等[13]提出使用区块链来解决物联网系统中数据资产价值转移无法高效完成等问题，通过智能合约技术保障数据的防篡改性，为物联网设备提供全生命周期的设备数据资产化方案，消除数据交易过程中的信任问题。张弛[14]提出构建一种新型的数据资产交易体系，引入区块链技术解决数据资产交易平台缓存、复制、留存交易数据的问题，保护数据的隐私性和安全性，保障数据资产交易者的权益不被数据资产交易平台侵占，实现所有权认证、数据保密等机制，体现数据确权可追溯等特点，但仍无法有效解决数据交易后的拷贝泄露问题。

总的来说，在数据交易中利用区块链的特性，能够为交易提供安全与隐私保证，智能合约引入可以支持更多的业务逻辑。但由于智能合约作为区块链的一部分，需要覆盖全部节点，这也决定了智能合约体量不易过大，逻辑不能过分复杂以免出现漏洞。这就意味着需要更好的链下协同解决方案来保证业务逻辑实现。

1.2 可信计算技术

随着互联网时代的飞速发展以及移动互联网的普及，各类计算平台[15]以及云平台安全问题也随之增长，各类恶意攻击威胁着信息安全，也导致许多企业、个人遭受着隐私与财产被侵害的危险。单纯通过使用软件的形式难以解决这些问题，而以硬件安全芯片为信任根的可信计算[16-18]环境为此提供了一种新的解决思路。

2015年，可信计算组织(Trusted Computing Group，TCG)发布了可信平台模块(Trusted Platform Module，TPM) 2.0[19]规范，成为ISO/IEC标准；以CPU作为信任根，建立从信任根到应用程序的信用链。目前我国可信计算技术走在世界前沿，已经进入了可信3.0[20]发展阶段，其核心思想是建立一套主动免疫的计算机安全体系。

随着云计算、5G、物联网、区块链、人工智能等新技术与应用场景的出现[21]，也为可信计算提供了许多融合发展的“温床”，当前可信计算主要的融合创新包括移动可信计算、抗量子可信计算、可信物联网、可信区块链[21]等应用场景。其中可信区块链中有许多成功的案例，例如阿里云旗下的蚂蚁区块链的可信计算服务，以自研虚拟机内嵌可信执行环境(Trusted Execution Environment，TEE)为基础，实现了通用链下智能合约为数据提供保密服务，为解决区块链链上链下数据协同问题提供了一种解决方法。

可信计算的主要方法是以一个可信根为基础，建立一条可信链，然后自底向上，从底层硬件一直扩展到应用，通过对硬件、软件的全面把控，增强整个计算系统的安全性。信任根可以由TPM/TCM/TPCM的形式实现，其安全假设不完全适用于实际网络环境，但可以设计为协同工作的模块化组件，负责独立地实现业务功能。

图1 TCM基本结构

Fig. 1 Basic structure of TCM

2 数据交易模型

2.1 交易索引链数据结构

为了防止数据信息被篡改，区块链是以区块为最小单位的链式存储结构。区块的组成结构通常分为区块头与区块体两部分。在该交易方案区块链结构设计中，区块头负责存放当前区块Hash值(CurHash)、上一个区块的Hash值(PreHash)、时间戳(Timestamp)、区块体中包含的数据记录数

(DataRecord),详见表2。

表2　区块头结构

Tab. 2　Block header structure

字段	大小/B	描述
CurHash	32	当前区块Hash值
PreHash	32	上一个区块的Hash值
Timestamp	4	该区块产生的时间
DataRecord	4	区块体中数据记录的数量

区块体中记录数据索引信息,包括记录编号、主体数据描述、数据内容的Hash值、数据提供方公钥、数据记录时间、数据标价、数据交易记录以及数据使用记录。

区块链的数据结构是一种基于哈希指针的有序单向链表结构,通过哈希指针的方式确保区块链的不可篡改性和可追溯性。不可篡改性是通过哈希指针来实现的,区块链的初始化生成一个创世区块;由创世区块开始,每个区块打包时都会在区块头生成一个CurHash和一个PreHash,新生成的区块PreHash值会指向前一个区块的CurHash,这种链式结构确保区块链信息难以被更改;当攻击者对某个区块进行修改时,该区块的后一个区块PreHash值就不再正确,当攻击者对后一个区块进行修改时,继续往后的区块也会不再正确。链式结构维护了区块链的稳定,确保区块链无法被篡改。具体结构如图2所示。

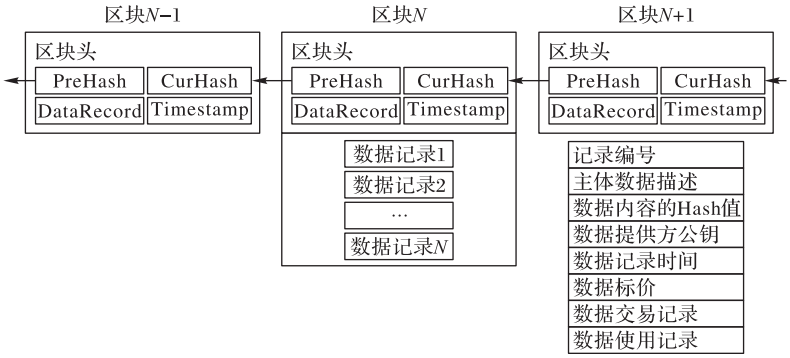


图2　交易索引链结构

Fig. 2　Trading index chain structure

区块体主要作为数据主体信息的记录,主要目的是实现数据可追溯、数据主体可验证和数据交易可追溯。数据可追溯主要体现为:数据主体可以在更迭中产生更新,可以将新的数据信息索引进行上链,后续产生的数据索引信息可以指向上一个版本的数据内容Hash值;数据主体可验证主要体现为:为了保证数据安全,数据主体不存放在任何第三方设备而由数据提供者保存,只有在交易完成后的使用阶段才传输数据进入可信计算环境,通过数据内容Hash可以对数据主体进行验证;数据交易可追溯主要体现为:对数据的交易操作存储在区块链中,由于区块链本身具有不可篡改的特性,可以保证数据交易记录的可追溯性,可信计算环境也可通过交易记录来验证交易双方身份。

2.2　可信计算环境

引入可信计算环境,主要解决下列两个问题:

1)使链上链下进行协同,在保证数据隐私安全的前提下对链上业务进行扩展。链上数据主要记录数据主体信息同时保证数据、交易的可追溯性,而可信计算则为方案中所涉及到的业务需求提供一个可信执行环境。

2)数据流转中会涉及到隐私保护需求,需要在不暴露用户数据的情况下对数据进行计算分析,并对结果进行加密传输,解决数据的隐私泄露问题。

2.3　数据交易模型

在现有的数据交易模式中,通常需要中间平台来集结数据供应方和数据,然后以接口的形式提供数据;或者是直接交易数据集。这些方式都容易造成数据泄露,难以防范数据被拷贝和二次销售。基于区块链与可信计算技术,本文设计了一种数据交易模型,如图3所示。根据数据交易的需求将交易双方抽象成两个对象:

数据供应方——拥有数据这一生产资料,希望将数据资产变现,但又担心数据资产可复制性导致交易出去的数据可能被二次转让,使自己会失去数据的主导权。例如工业物联网中产生的工业数据。

数据需求方——拥有转换、加工数据这一生产资料的能力,但缺乏数据,需要从其他拥有数据的数据供应方手中购买数据来挖掘数据的潜在价值,但又担心泄露技术机密。

完整的交易流程包括:

数据供应方上传数据索引信息,系统通过各节点共识后将数据索引信息上传到数据索引区块链中;数据需求方购买数据后,将交易流程记录到区块链中,数据需求方获得数据的使用权,无法下载数据,或查看完整数据,断绝数据的二次转让。

当数据需求方需要使用数据时,将算法代码输出描述以及算法代码Hash值上传,发送数据调用请求;可信计算环境生成一个公私钥对,将公钥发送给数据供应方和数据需求方,数据供应方与需求方加密数据与算法、用个人私钥签名后上传至可信计算环境;可信计算环境获取数据与算法后,用可信私钥解锁后验证数据主体与算法的Hash值是否正确,在确定数据与算法的Hash值无误后进行运算。

运算完成后,可信计算环境将运算结果用数据需求方的公钥进行加密、用可信计算环境的私钥进行签名后,将加密后算法结果返回给数据需求方;同时销毁可信计算环境内数据、算法以及算法结果。

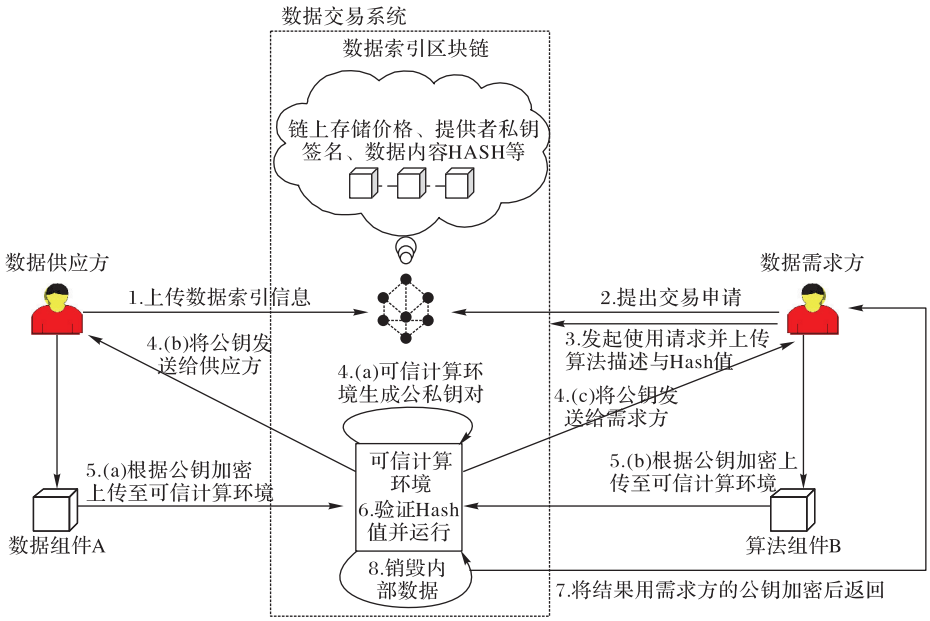


图3 数据交易模型

Fig. 3 Model of data trading

3 数据交易方案设计

3.1 可信计算框架设计

基于可信芯片为核心、结合可信硬件构建可信链，构建可信操作系统内核提供可信核心服务，内核启动后由可信应用处理业务服务。本文提出一种可信计算框架，如图4所示，根据功能结构自底向上分为物理层、中间层和应用层。

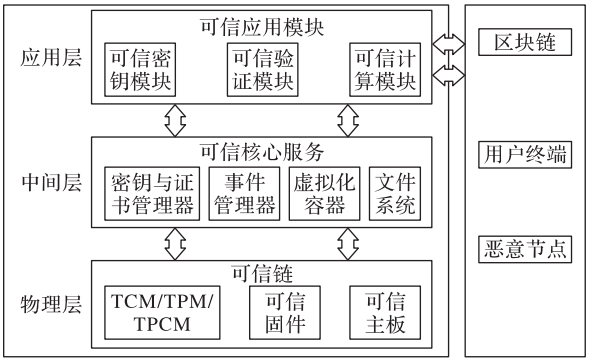


图4 可信计算框架

Fig. 4 Framework of trusted computing

物理层由可信硬件与可信芯片组成，负责可信计算环境的安全控制与运算功能，本质上是由存储器、输入/输出(Input/Output，I/O)、密码处理引擎、随机数生成器与执行控制引擎组成。可信平台模块(TPM)由可信计算组织(Trusted Computing Group，TCG)提出，使用哈希消息认证码(Hash-based Message Authentication Code，HMAC)引擎提供Hash验证，运用密钥生成器与密钥协处理器提供密钥生成检验功能，执行引擎负责执行程序代码；可信密码模块(Trusted Cryptography Module，TCM)是由我国自主研发的基于国密算法的安全芯片，该芯片以TPM 1.2框架为基础、国密算法为核心，更加符合我国安全管理策略要求；可信平台控制模块(Trusted Platform Control Module，TPCM)则是以可信密码模块为基础，新增主动控制模块。

中间层以底层可信硬件为基础为应用层提供服务，是应用层调用底层功能的接口，主要负责密钥与证书管理、事件管理器、文件系统以及虚拟化容器管理。

应用层为主要业务功能实现，分为可信密钥模块、可信验证模块和可信计算模块。可信密钥模块使用非对称加密算法生成可信的公私钥对，可信私钥存于可信存储环境，用于验证。可信公钥则发送给用户用于加密数据与算法，保证数据传输安全；可信验证模块通过哈希算法与非对称加密算法，对加密数据进行解密，并结合链上信息验证链下数据、算法以及用户签名，保证链上信息与链下数据能够对应；可信计算模块采用虚拟化容器技术，为计算提供可信的执行环境，数据与算法在通过验证模块后，转入可信计算模块中进行运算，最后将运算结果返回给数据需求方，将交易过程记录到链上后，销毁内部数据。

3.2 可信计算支撑的加密设计

交易完成后，在请求数据使用时，本文方案使用哈希算法、非对称加密算法与可信计算来保证机密性与完整性。为了保证数据传输过程安全可靠，基于可信计算环境生成的公私钥对，建立如图5所示的加密传输。以图5所示的数据需求方数据加密流程为例，具体步骤描述如下：

步骤1 数据需求方发出数据使用请求后，可信计算环境生成公私钥对($PK_{可信}$，$SK_{可信}$)，并将$PK_{可信}$发送给数据供应方与数据需求方。

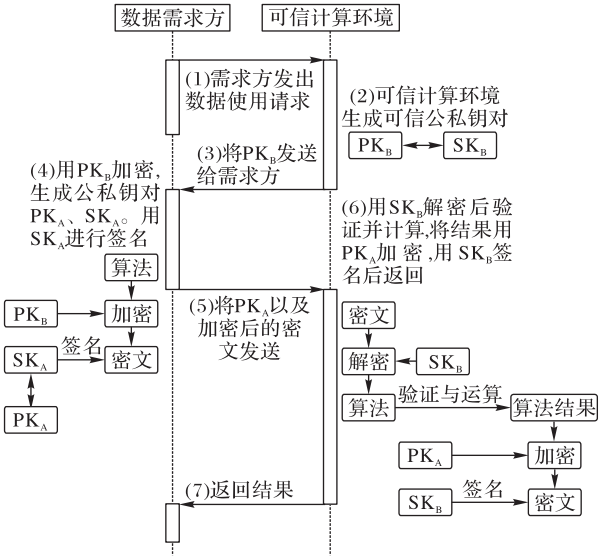
步骤2 收到$PK_{可信}$后，使用$PK_{可信}$对原始数据Data进行加密，encry = encrypt(Data，$PK_{可信}$)，然后使用自身私钥进行签名，sigEncry=sign($SK_{提供方}$，encry)。

步骤3 可信计算环境收到加密数据sigEncry后，使用链

上的数据提供方公钥验证签名并用可信私钥进行解密，decrData= decrypt(sigEncry, $PK_{提供方}$, $SK_{可信}$)。

步骤 4　计算解密后的数据 decrData 的 Hash 值，与链上数据主体 Hash 值进行对比，valid=verify(Hash(decrData), $Hash_{提供者}$)，检验数据完整性，验证成功后进行计算。

步骤 5　计算完成后，对计算结果 result 进行加密，res= encrypt(result, $PK_{提供者}$)，将加密后的 res 返回给数据需求方。



注：PK_A(提供方公钥), PK_B(可信公钥), SK_A(提供方私钥), SK_B(可信私钥)。

图5　可信计算环境支撑的加密传输

Fig. 5　Encryption process supported by trusted computing environment

3.3　数据交易验证设计

数据交易验证的主要功能是保证可信计算环境接收到的数据与算法代码与交易时协商的一致。在请求数据使用前，数据使用的申请会被记录在交易索引链中，包括算法的 Hash 值、算法的使用描述以及算法的输出描述，保证计算结果不牵涉数据隐私。

在数据使用过程中，可信计算环境对解密后的数据以及算法进行验证，与链上信息进行比对，确认数据一致性；并且将计算结果使用数据需求方公钥进行加密留存，将数据使用结果 Hash 值记录在区块链中，以便于出现数据使用纠纷时为数据使用过程提供证明。数据交易验证过程如图 6 所示，具体步骤如下：

步骤 1　数据需求方发出数据使用请求时，上传算法代码相关信息，验证信息包括：$Hash_{算法}$、算法描述 $desc_{算法}$、算法结果描述 $desc_{结果}$。

步骤 2　可信计算环境对数据和算法进行验证，保证数据与算法 Hash 值与链上一致。

步骤 3　将计算结果 result 采用需求方公钥 $PK_{需求方}$ 进行加密，encry = encrypt(result, $PK_{需求方}$)，并在可信计算存储留存。

步骤 4　将计算结果 Hash 上传至交易索引链，记录交易流程。

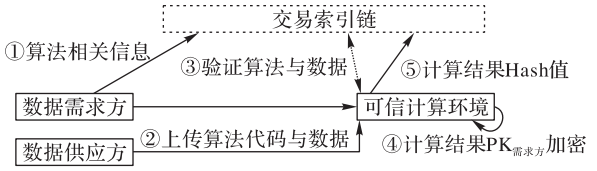


图6　数据交易验证过程

Fig. 6　Data trading verification process

4　结语

鉴于现有数据交易方案中存在的问题，提出一种数据交易方案，引入区块链与可信计算技术结合业务需求，构建了一种新的数据交易渠道。相较于传统的数据交易模式，通过区块链和可信计算环境的构建，能够有效保证数据传输安全。在不暴露用户数据的情况下，将交易数据的使用权提供给数据需求方来进行计算和分析，以保证数据的隐私性和安全性。

本文方案具有以下特点：

1)采用非中心化的模式，对数据索引信息、交易过程以及数据使用记录进行存储。链上数据主要作为交易索引与链下数据协同，将链上无法实现的复杂业务逻辑转移到链下可信计算环境进行，在保证数据隐私安全的前提下对链上业务进行扩展。同时可采用联盟链的形式，提供准入机制，对节点成员进行把控。

2)与现有的数据交易方式相比，本文方案中数据主体不在任何一方留存，数据提供方在保证数据所有权不被危害的前提下交易“数据中所包含的信息”，且不会泄露数据隐私。攻击者如果在传输过程截获数据，必须计算出对应私钥或者攻击可信计算环境来获得私钥。相较于传统的数据交易方式，本文方案所交易的数据无法被窃取或者泄露。

参考文献(References)

[1] 孟小峰，李勇，祝建华. 社会计算：大数据时代的机遇与挑战[J]. 计算机研究与发展，2013，50(12)：2483-2491.(MENG X F, LI Y, ZHU J H. Social computing in the era of big data: opportunities and challenges [J]. Journal of Computer Research and Development, 2013, 50(12): 2483-2491.)

[2] 叶雅珍，刘国华，朱扬勇. 数据资产相关概念综述[J]. 计算机科学，2019，46(11)：20-24.(YE Y Z, LIU G H, ZHU Y Y. Survey of concepts related to data assets[J]. Computer Science, 2019, 46(11): 20-24.)

[3] 贵阳大数据交易所. 2016年中国大数据交易产业白皮书[R/OL]. [2019-11-21]. http://www.cbdio.com/BigData/2016-06/02/content_4965656_all.htm.(GBDEx. 2016 white paper on China big data exchange[R/OL]. [2019-11-21]. http://www.cbdio.com/BigData/2016-06/02/content_4965656_all.htm.)

[4] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[EB/OL]. [2019-06-21]. https://bitcoin.org/bitcoin.pdf.

[5] 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(4)：481-494.(YUAN Y, WANG F Y. Blockchain: the state of the art and future trends [J]. Acta Automatica Sinica, 2016, 42(4): 481-494.)

[6] 蔡维德，郁莲，王荣，等. 基于区块链的应用系统开发方法研究[J]. 软件学报，2017，28(6)：1474-1487.(CAI W D, YU L,

WANG R, et al. Blockchain application development techniques [J]. Journal of Software, 2017, 28(6): 1474-1487.)

[7] Ethereum White Paper. A next-generation smart contract and decentralized application platform[EB/OL]. [2020-02-10]. https://github.com/ethereum/wiki/wiki/White-Paper.

[8] CHRISTIDIS K, DEVETSIKIOTIS M. Blockchains and smart contracts for the internet of things[J]. IEEE Access, 2016, 4: 2292-2303.

[9] 王云,何明久. 区块链与物联网的应用案例分析[J]. 集成电路应用, 2018, 35(3): 70-74. (WANG Y, HE M J. The case study on the application of the block chain and the internet of things[J]. Journal of Applications of IC, 2018, 35(3): 70-74.)

[10] 任鹏,徐晶晶,王意,等. 基于区块链和车联网的汽车租赁联盟的研究与实现[J]. 应用科学学报, 2019, 37(6): 851-858. (REN P, XU J J, WANG Y, et al. Research and implementation of car rental alliance based on blockchain and internet of vehicles [J]. Journal of Applied Sciences, 2019, 37(6): 851-858.)

[11] 刘敖迪,杜学绘,王娜,等. 区块链技术及其在信息安全领域的研究进展[J]. 软件学报, 2018, 29(7): 2092-2115. (LIU A D, DU X H, WANG N, et al. Research progress of blockchain technology and its application in information security[J]. Journal of Software, 2018, 29(7): 2092-2115.)

[12] 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.)

[13] 盛念祖,李芳,李晓风,等. 基于区块链智能合约的物联网数据资产化方法[J]. 浙江大学学报(工学版), 2018, 52(11): 2150-2158. (SHENG N Z, LI F, LI X F, et al. Data capitalization method based on blockchain smart contract for internet of things [J]. Journal of Zhejiang University (Engineering Science), 2018, 52(11): 2150-2158.)

[14] 张弛. 数据资产价值分析模型与交易体系研究[D]. 北京:北京交通大学, 2018: 92-98. (ZHANG C. Research on value analysis model and transaction system of data assets[D]. Beijing: Beijing Jiaotong University, 2018: 92-98.)

[15] BUYYA R, YEO C S, VENUGOPAL S, et al. Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility[J]. Future Generation Computer Systems, 2009, 25(6): 599-616.

[16] SHEN C, ZHANG H, WANG H, et al. Research on trusted computing and its development[J]. Science China Information Sciences, 2010, 53(3): 405-433.

[17] 冯登国,秦宇,汪丹,等. 可信计算技术研究[J]. 计算机研究与发展, 2011, 48(8): 1332-1349. (FENG D G, QIN Y, WANG D, et al. Research on trusted computing technology[J]. Journal of Computer Research and Development, 2011, 48(8): 1332-1349.)

[18] 宋成. 可信计算平台中若干关键技术研究[D]. 北京:北京邮电大学, 2011: 19-24. (SONG C. Research on some key technologies of trusted computing platform[D]. Beijing: Beijing University of Posts and Telecommunications, 2011: 19-24.)

[19] CHEN L, LI J. Flexible and scalable digital signatures in TPM 2.0 [C]// Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2013: 37-48.

[20] 沈昌祥,张大伟,刘吉强,等. 可信3.0战略:可信计算的革命性演变[J]. 中国工程科学, 2016, 18(6): 53-57. (SHEN C X, ZHANG D W, LIU J Q, et al. The strategy of TC 3.0: a revolutionary evolution in trusted computing[J]. Strategic Study of CAE, 2016, 18(6): 53-57.)

[21] 刘明达,拾以娟,陈左宁. 基于区块链的分布式可信网络连接架构[J]. 软件学报, 2019, 30(8): 2314-2336. (LIU M D, SHI Y J, CHEN Z N. Distributed trusted network connection architecture based on blockchain[J]. Journal of Software, 2019, 30(8): 2314-2336.)

This work is partially supported by the National Key Research and Development Program of China (2019YFC1511300), the Industrial Technology Foundation Public Service Platform of Ministry of Industry and Information Technology (2019-00894-1-1), the Key Program of Chongqing Basic Research and Frontier Exploration Project (cstc2019jcyj-zdxmX0008), the Key Program of Big Data and Intelligent Science and Technology Project of Yubei District (2020-02).

ZHANG Xuewang, born in 1974, Ph. D. candidate, associate professor. His research interests include blockchain and internet of things, data security and privacy protection, big data and intelligent data processing.

YIN Zijie, born in 1996, M. S. candidate. His research interests include blockchain, data asset, trusted computing.

FENG Jiaqi, born in 1995, M. S. candidate. His research interests include blockchain, data provenance.

YE Caijin, born in 1994, M. S. candidate. His research interests include blockchain, privacy protection.

FU Kang, born in 1997, M. S. candidate. His research interests include blockchain.