基于区块链的数据库访问控制机制设计

付永贵[1]，朱建明[2]
（1. 山西财经大学信息学院，山西 太原 030031；2. 中央财经大学信息学院，北京 100081）

摘 要：针对数据库访问控制中存在的问题，提出将区块链技术应用于数据库访问控制的思想。从区块链层次结构、访问控制过程的逻辑层次结构、访问控制的实现原理、访问控制的共识认证原理以及访问控制区块链体系的构建机制几个方面设计了基于区块链的数据库访问控制实现机制，对基于区块链的数据库访问控制体系的性能进行评价。为区块链应用于数据库访问控制提供了完整的架构，通过对访问者身份、访问权限及访问行为强化认证与监管，有效地提高了数据库访问控制的能力。

关键词：数据库；访问控制；区块链；实现机制
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2020097

Design for database access control mechanism based on blockchain

FU Yonggui[1], ZHU Jianming[2]
1. School of Information, Shanxi University of Finance and Economics, Taiyuan 030031, China
2. School of Information, Central University of Finance and Economics, Beijing 100081, China

Abstract: Aiming at the current problems of database access control, the thought of blockchain technology applied to database access control was proposed. The implementation mechanism of database access control based on blockchain was designed from several aspects as blockchain hierarchical structure, logical hierarchical structure of access control process, implementation principle of access control, consensus authentication principle of access control, and construction mechanism of access control blockchain system. The performance of database access control system based on blockchain was assessed. A complete framework was provided for blockchain applied in database access control. Through strengthening the authentication and supervision of visitor identity, access permission and access behavior, the database access control ability is improved effectively.

Key words: database, access control, blockchain, implementation mechanism

1 引言

数据库是数据的主要存在形式。随着对数据库研究的深入和发展，目前的数据库形式呈现多样化。数据库管理系统负责对数据库进行管理，是用户与系统管理员访问数据库的门户、接口和工具。数据库的最大特点是共享性，随着网络技术的发展，网络数据库成为数据库的主要应用形式，进一步提高了对数据库访问控制的要求。对于数据库的访问控制，通常使用访问控制技术来实现，比如防火墙技术、身份认证技术、权限限制技术等，在具体应用中，数据库是数据库应用系统的一个组成部分，需要根据数据库本身的特点及数据库应用系统的具体要求来运行。

数据库信息泄露与破坏影响着数据库应用系统实施的效率，也是目前数据库应用面临的一个重

收稿日期：2019–12–24；**修回日期**：2020–03–03
通信作者：朱建明，zjm@cufe.edu.cn
基金项目：国家社会科学基金资助项目（No.18BTQ083）
Foundation Item: The National Social Science Fund of China (No.18BTQ083)

要问题。数据库应用系统中信息被破坏表现为黑客入侵、病毒攻击，这种破坏对缺乏备份与恢复的小型和私人数据库影响较大。对数据库的非法操作包括非法访问者访问数据以及合法访问者对数据库非授权对象进行非法访问。造成数据库被攻击的主要原因是数据库访问控制技术不能保障数据库本身的安全防护，具体表现在数据库访问控制过程的中心化管理缺乏对数据库访问者访问行为的认证、记录和监管，对数据库信息泄露事件的责任追溯及控制力不足等。所以，如何加强对数据库访问者身份及访问权限的认证，构建对访问者访问行为的动态、实时监管机制以及访问者身份、访问行为的事后追溯体系，是目前数据库访问控制需要解决的问题。

区块链[1-3]是比特币的技术体系与应用模式，最早于 2008 年 11 月由中本聪提出。区块链的根本特点是去中心化共识认证和分布式记账，由于使用了哈希计算和数字签名技术，区块链从理论上构建了一个完善的、不可伪造的信息或数据记录体系，成功解决了信息或数据的可追溯问题。区块链本身的技术特性使其在实际应用中具备开放性和灵活性，区块链可以根据具体应用环境的特点轻松地进行调整并与应用体系进行融合，而且对应用体系没有额外的硬件设备要求。区块链这一技术体系是多个成熟技术的融合，应用过程中在软件构建方面也不会带来新的问题。因此，区块链在社会生活相关领域得到了迅猛发展。基于此，本文提出将区块链应用于数据库的访问控制过程，在数据库原有访问控制技术的基础上，通过对数据库访问者身份、访问权限及访问者访问行为信息进行共识认证（包括对信息的真实性验证与对访问者身份、权限及访问行为的合理性验证）并分布式存储，构建访问者访问行为过程的可追溯性链条，进一步提高对数据库访问控制的能力。

本文的主要贡献如下。

1) 构建了数据库访问控制体系中区块链的逻辑层次结构，明确了区块链在数据库访问控制体系中的地位；构建了基于区块链的数据库访问控制的逻辑层次结构，明确了基于区块链体系的访问控制的实现过程。

2) 构建了基于区块链的数据库访问控制的实现原理，明确了信息的产生、变化、共识认证及存储的过程，明确了区块链的工作原理及信息的组成，并通过算法模型进行描述。

3) 构建了数据库访问控制的共识认证原理，以访问者访问行为过程为例构建了智能合约的内容、判断逻辑及共识认证算法的实现原理。

4) 构建了数据库访问控制的区块链构建机制，包括区块数据结构、数据的关联关系及基础数据的存储机制。

2　背景知识与相关研究

区块链在生成过程中主要的技术或工作方法有加密技术、数字签名技术、P2P（peer to peer）网络传播技术、哈希计算、去中心化、智能合约、共识认证、时间戳、分布式存储等。这些技术或工作方法在区块链生成的整个时间周期内相互融合，成为一个技术体系。从区块链的结构组成来讲，区块链由不同区块按时间顺序通过哈希函数指针相连，区块由区块头和区块体组成。其中，区块体包含区块链服务的应用体系的基础数据（有些应用体系中基础数据存储于区块链之外的存储体，这主要取决于基础数据的容量及区块的构建方法）及由基础数据哈希计算生成的 Merkel 树的树体；区块头包含本区块的前驱区块的哈希值、本区块基础数据哈希计算生成的 Merkel 树的树根、证明本区块生成时间的时间戳、区块的版本号、共识认证参数值等。区块链的结构如图 1 所示。

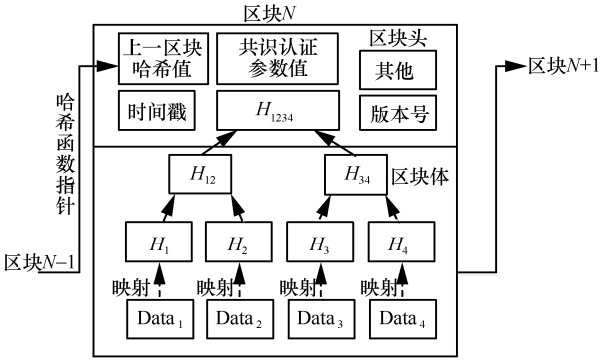

图 1　区块链的结构

图 1 中，Data 表示区块记录的基础数据，包括业务数据及与业务相关的其他数据、智能合约等，这些数据的记录内容在区块记录中进行了规定；*H* 表示其下层进行哈希运算后生成的 hash 值。

区块链产生之初，人们对区块链的认识是与数字货币作为一个整体的，之后逐渐将区块链与数字货币分离而开始研究其在不同场景的应用。纵观区

块链的发展，区块链经历了数字货币→智能合约→去中心化信任网络几个阶段的发展，目前区块链信任网络的构建还处于初级阶段，但总体呈快速发展的势头。

目前，区块链在产业界的应用场景涉及物联网体系管理[4-5]、健康记录[6-7]、契约订立[8-9]、投票选举[10-11]等不同的领域，虽然目前区块链的应用还处于探索阶段，相关的产品也主要处于局部小范围的应用，但区块链对应用体系强大的适应能力和人们对网络信用的需求将促进区块链在不同应用场景的快速发展，具体应用场景区块链的互相链接、信用信息的相互认证和交互记录将会使信用记录能力快速叠加，未来基于区块链的互联网络将是区块链发展的根本方向。

基于区块链作为产品的特性，与产业界的发展相比，区块链在学术界的发展相对滞后，具体表现为学术研究成果不能起到引领产品研发的作用。2019 年 7 月 26 日，本文通过中国知网设定检索范围为“文献”，对“主题”为“区块链”的研究成果进行搜索，搜索结果中 2015 年的文献数量为 38 个，2016 年的文献数量为 760 个，2017 年的文献数量为 1 776 个，2018 年的文献数量为 4 387 个。对这些文献进行分析可知，目前区块链的研究呈逐渐高涨的趋势，其研究成果包括区块链工作原理分析[12-13]、价值及社会影响分析[14-15]、区块链技术架构设计、应用模式设计、应用系统介绍等。国外关于区块链的研究成果与国内关于区块链的研究成果具有相似的内容及数量变化特点。

下面，从区块链技术架构设计、应用模式设计及应用系统介绍介绍几方面介绍区块链的研究进展情况。

1) 区块链技术架构设计方面的研究成果。闵新平等[16]对许可链多中心动态共识验证的实现机制进行了研究；马晓婷等[17]设计了一种区块链环境下跨越异构域的认证协议；Fu 等[18]构建了基于区块链和大数据的 CPS（cyber physical system）信息安全风险评估体系，并构建了区块链应用于 CPS 的分层模型结构；Gao[19]提出了一种电子商务平台基于区块链的数据加密算法，并进行了分析和安全测试；Muneeb 等[20]从不同角度讨论了物联网环境下区块链隐私保护策略问题。

2) 应用模式设计方面的研究成果。蔡维德等[21]通过实例设计了区块链系统的模型结构并研究了区块链系统的开发方法；朱建明等[22]设计了基于区块链的 SWIFT（society for worldwide interbank financial telecommunications）系统模型结构及运行机制；Memon 等[23]构建了一个基于排队论的区块链系统仿真模型；She 等[24]提出了一个无线传感器网络中用于恶意节点检测的区块链信任模型。

3) 应用系统介绍方面的研究成果。Toyoda 等[25]提出了一个区块链应用于供应链体系的系统；Mao 等[26]提出了一个基于联盟区块链的新型自动化食品交易系统；Zhong 等[27]提出了一个基于区块链的支付系统；Tao 等[28]提出了一个基于分层多域区块链网络的食品安全监管系统；Liao 等[29]提出了一个基于区块链的可信数据发布系统。

对区块链的研究成果分析可知，目前区块链的研究主要集中于如何对区块链技术架构进行设计以适应具体的应用场景，并提出相应的应用模式，属于未来基于区块链的信用网络的底层技术分析与应用方案设计阶段。目前，区块链应用研究的不足主要表现在学术研究的不足、体系标准的缺失导致尚未形成全社会的、整体的、完善的区块链发展规划和图景，这也在一定程度上影响了区块链应用及价值实现速度。

目前，区块链在访问控制方面取得了一定的研究成果。Wang 等[30]研究了基于区块链的分布式存储系统中细粒度访问控制问题；Ma 等[31]将区块链应用于物联网场景中的分层访问控制；Ding 等[32]提出了一个将区块链应用于物联网的基于属性的访问控制方案；刘敖迪等[33]提出了基于区块链的大数据访问控制机制；王秀利等[34]提出了一个基于区块链的访问控制模型与算法；Zhang 等[35]设计了一个区块链应用于物联网环境的访问控制方案，主要使用的技术方法包括密文属性认证与门限策略；Zhang 等[36]提出了一个区块链应用于电子病历访问控制的方案。对目前基于区块链的访问控制研究成果进行分析可知，这些成果只是从某一个角度研究了基于区块链的访问控制，例如，限定于某一个场景（如物联网、医疗健康等）的应用研究、实现技术或条件的算法分析，或仅限于应用体系的某一部分（智能合约、共识方法、数据存储等）的研究。尚未查到区块链应用于数据库访问控制的完整的架构体系，并阐述访问控制的实现方法、数据记录与关联关系的研究成果。基于此，本文提出了基于区块链的数据库访问控制机制，从访问者行为过程

出发研究区块链技术体系下对访问者行为的安全监管和对访问者行为数据及其相关数据的不可否认记录。本文研究可以为区块链应用于数据库访问控制提供完整的思路，促进区块链在各类数据库中的应用与研究发展。

3　实现机制

3.1　区块链逻辑结构

在基于区块链的数据库访问控制体系中，区块链的逻辑结构如图 2 所示。

如图 2 所示，区块链的逻辑结构共分为四层，分别为数据库管理层、应用系统数据管理层、区块链管理层、信息应用层。区块链不对数据库管理层的数据进行记录和管理，只对应用系统数据管理层的数据进行记录、认证和分析，即数据库数据并不在区块链中运行，区块链体系中运行的是对数据库数据进行操作的相关行为数据及行为主体的数据，行为主体对数据库访问的数据以标识符号的形式记录。

第一层，数据库管理层。这一层负责对数据库及其管理逻辑进行定义，与区块链运行体系无关。

第二层，应用系统数据管理层。这一层对访问者身份信息、系统管理员授权给访问者的权限信息、访问者行为信息、访问者访问对象信息进行规定，并定义记录这些信息的具体格式。

第三层，区块链管理层。这一层按照区块链工作原理分成 4 个部分，即区块链定义、信息生成与网络广播、共识认证、区块链构建与存储管理。区块链定义部分对区块及区块链结构、区块链运行涉及的技术进行定义；信息生成与网络广播部分对访问者相关信息的生成机制、网络广播机制、网络体系结构、验证者对信息接收与验证的网络逻辑进行规定；共识认证部分对认证主体的规定与选择、智能合约的定义、共识认证的实现原理、认证主体的激励机制进行规定；区块链构建与存储管理对区块链的构建、区块链内信息的关联模式、信息的存储模式以及分布式存储的存储体进行规定。

第四层，信息应用层。这一层对如何通过对区块链记录信息进行检索、分析来实现对访问者行为链条进行追溯，对访问者身份进行验证，对访问者的访问行为合理性进行评价，对数据操作的访问者进行责任认定等进行规定。

3.2　数据库访问控制逻辑层次结构

基于区块链的数据库访问控制逻辑层次结构如图 3 所示。

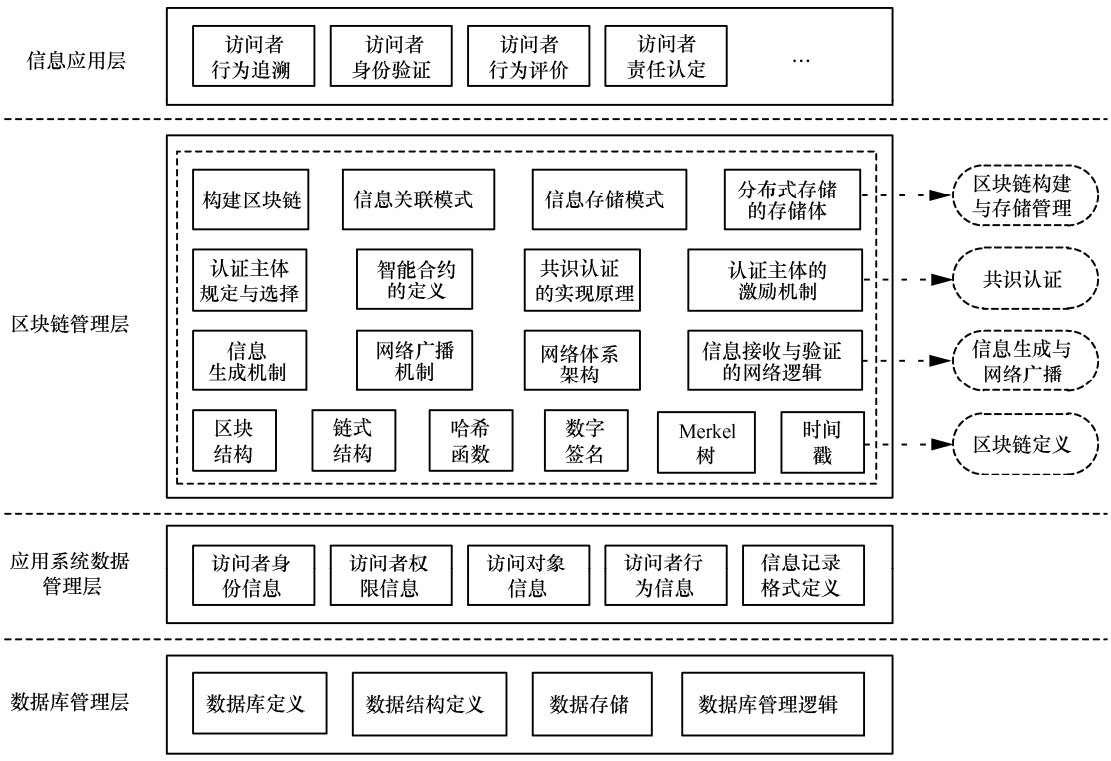

图 2　数据库访问控制体系中区块链的逻辑结构

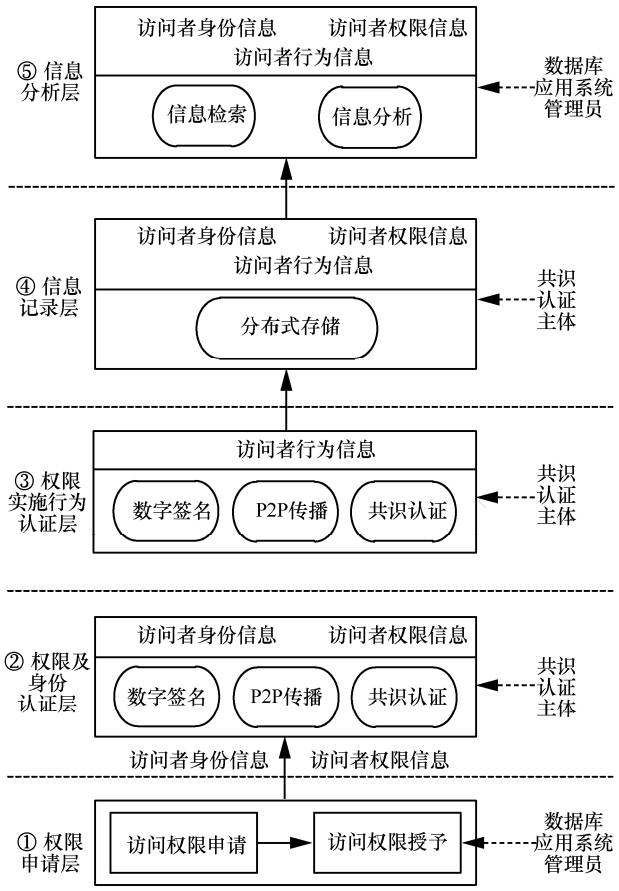

图 3　基于区块链的数据库访问控制逻辑层次结构

通常访问者对数据库的访问权限包括读、修改、增加、删除等操作权限。由图 3 可知，在基于区块链的数据库访问控制体系中，数据库应用系统管理员对访问者授权后，增加了由共识认证主体对访问者身份、访问权限及访问行为的认证。图 3 共分为 5 个逻辑层次，第一层为权限申请层，用于对访问者对数据库访问权限的申请和授权过程进行规定；第二层为权限及身份认证层，数据库应用系统管理员对访问者访问权限进行授权以后，共识认证主体需要对数据库应用系统管理员对访问者的访问授权是否合理进行认证，以及对所授予的访问权限的合理性进行认证，权限及身份认证层就是用于实现这一功能的；第三层为权限实施行为认证层，这一层对访问者的访问行为进行认证和记录，确保访问者的访问行为是在数据库应用系统管理员授权范围内的权限的实施；第四层为信息记录层，这一层对访问者身份信息、权限信息以及访问者行为信息进行存储规定，也就是构建区块并形成区块链的过程；第五层为信息分析层，用于数据库应用系统管理员对访问者身份信息、权限信息以及访问者行为信息进行检索并分析，形成对其访问过程合理性的事后监管。

由图 3 可以看出，基于区块链的数据库访问控制逻辑层次结构在原有数据库访问控制过程逻辑结构的基础上，增加了权限及身份认证层、权限实施行为认证层、信息记录层，实现了对访问者访问控制过程的强化及数据库应用系统权威组（个人或组织组成的共识认证主体）对数据库被访问过程的实时跟踪和监管。对访问者身份、操作权限的共识认证过程以及对访问者访问行为的共识认证过程，需要通过构建智能合约来实现。

3.3　数据库访问控制实现原理

基于区块链的数据库访问控制实现过程如图 4 所示。

对访问者身份信息、访问权限信息的共识认证过程（如步骤 5)所示）不仅要验证信息传输的正确性，还要进一步验证信息的合理性，所以需要运行智能合约 1 来实现；同样，在对访问者访问行为进行验证（如步骤 8)所示）时，需要运行智能合约 2 来实现。

为了描述简洁清晰，定义如下。Adm 表示系统管理员，Visitor 表示访问者，Vis_id 表示访问者身份信息，Vis_per 表示访问者权限信息，Vis_beh 表示访问者行为信息，Vis_obj 表示访问对象信息，apply 表示申请，grant 表示授权，sig 表示数字签名，P2P 表示 P2P 广播，$\text{Visitor}_{\text{pub}}$(Key)表示访问者公钥，Authen_sub 表示共识认证主体，all 表示所有，auth 表示共识认证，smart_con1 表示智能合约 1，smart_con2 表示智能合约 2，blockchain 表示区块链，exe 表示实施，storage 表示存储；则基于区块链的数据库访问控制实现过程可以描述如下。

步骤 1) $\text{Visitor}_{\text{apply}}$(Vis_per)→ Adm and $\text{Visitor}_{\text{apply}}$(加入区块链系统)→Adm

//访问者申请权限

步骤 2) Visitor←$\text{Adm}_{\text{grant}}$(Vis_per) and Visitor←$\text{Adm}_{\text{grant}}$(加入区块链系统)

//管理员授予权限

步骤 3) $\text{Visitor}_{\text{sig}}$ (Vis_per, Vis_id)

//访问者对权限数字签名

步骤 4) $\text{Visitor}_{\text{P2P}}$($\text{Visitor}_{\text{sig}}$ (Vis_per, Vis_id), Vis_per, Vis_id,$\text{Visitor}_{\text{pub}}$(Key))

//访问者广播

步骤 5) $\text{Authen\_sub}_{\text{all, auth}}$(Vis_per, Vis_id) and

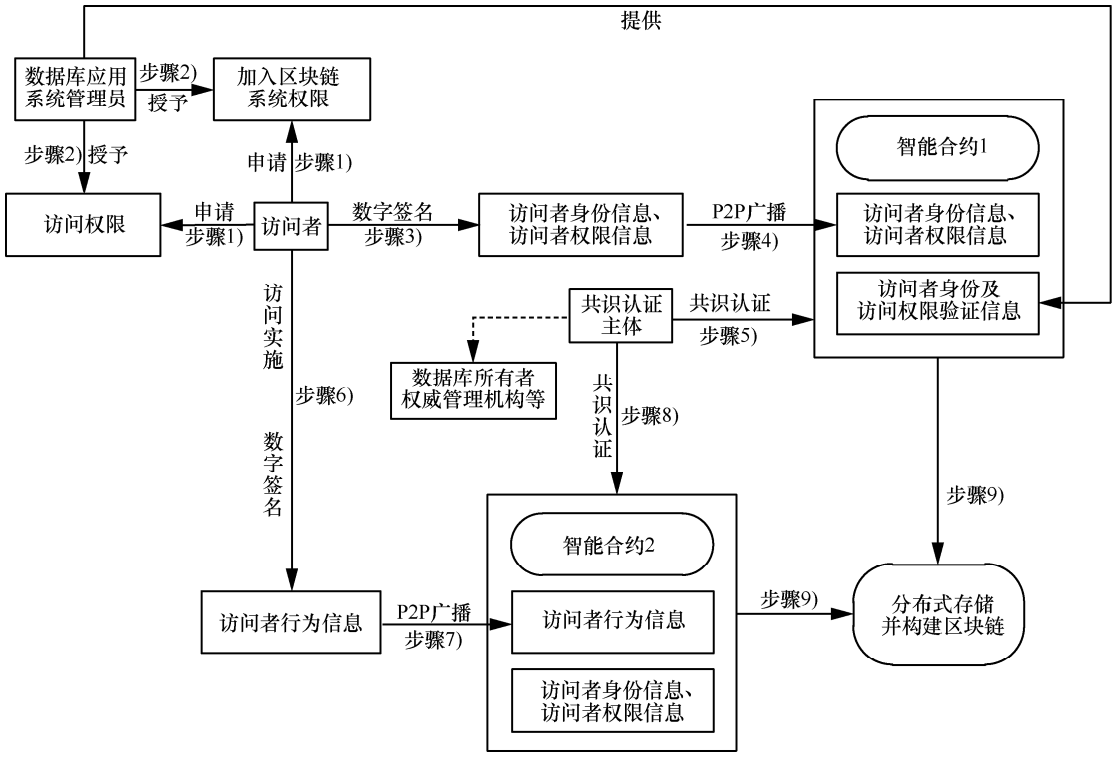

图 4　基于区块链的数据库访问控制实现过程

$Authen\_sub_{all,\ smart\_con1}(Vis\_per, Vis\_id)$

//共识认证，启用智能合约 1

步骤 6) $Visitor_{exe}(Vis\_per, Vis\_obj) \rightarrow Visitor(Vis\_beh)$ and $Visitor_{sig}(Vis\_obj, Vis\_beh)$

//访问者执行权限，并数字签名

步骤 7) $Visitor_{P2P}(Visitor_{sig}(Vis\_obj, Vis\_beh), Vis\_obj, Vis\_beh, Visitor_{pub}(Key))$

//访问者广播

步骤 8) $Authen\_sub_{all,\ auth}(Vis\_obj, Vis\_beh)$ and $Authen\_sub_{all,\ smart\_con2}(Vis\_per, Vis\_id, Vis\_obj, Vis\_beh)$

//共识认证，启用智能合约 2

步骤 9) $Authen\_sub_{all}(blockchain(Vis\_per, Vis\_id, Vis\_obj, Vis\_beh))$ and $Authen\_sub_{all,\ storage}(blockchain)$

//构建区块，分布式存储

3.4　数据库访问控制的共识认证原理

区块链通过共识认证实现了对业务内容的监管。对于数据库应用系统来说，通常基于数据的保密性及其管理的专有性需求，只有经过授权的个人或组织才能对数据库应用系统进行管理。因此，在基于区块链的数据库应用系统中，只能由数据库应用系统的所有者及其管理机构组成共识认证主体实现对访问者身份、权限的认证，实现对访问者访问行为的认证和监管。这样，在基于区块链的数据库应用系统中的认证主体不会是一个庞大的群体，而是成员数量较为有限的集合。这与共识认证由大量主体组合实施以防共谋的思想是有差别的。但如果将认证主体限定为应用系统的所有者、受到监管的管理者及权威管理机构，加强共识认证的逻辑能力，同时阻断认证主体共谋的主观驱动和实现条件，则由少量共识认证主体对数据库访问者的身份、权限及访问行为实施共识认证是可行的。与传统的中心化认证体系相比，本文提出的由有限数量的主体组成的“多中心”认证体系具备区块链的工作特点，实现了本文对认证数据或信息分布式存储的需求。由于共识认证主体的权威性及其认证的主动性，因此区块链的记账可以指定任一认证主体实施，并且不需要建立相应的激励机制，因此本节不再讨论激励机制构建问题。

3.4.1　智能合约

基于区块链的数据库访问控制智能合约用于判断访问者身份、访问权限或访问者访问行为的合理性，智能合约 1 需要根据数据库应用系统管理员提供的访问者身份信息或授权信息来判断访问者在区块链体系中发布的身份信息或访问权限信息的正确性，还需要通过引入与访问者身份相关的数

据库管理系统内、外部多源数据以判断访问者身份的合法性（是合法用户还是非法用户），智能合约 2 需要根据得到验证的访问者身份信息或授权信息判断访问者访问行为的合理性。

用基于角色的权限访问控制（RBAC, role-based access control）描述对访问者访问行为的判断逻辑，用户是访问者，用户的角色为数据库应用系统管理员授予用户的角色，角色对应的权限是数据库应用系统管理员授予对应角色的权限，操作的对象是数据库的具体字段或记录。对应于智能合约 2，基于区块链的数据库访问控制用户行为过程判断原理如图 5 所示。

对应时间 T_1 的访问者访问行为，智能合约 2 的逻辑判断过程如图 6 所示。

对应其他时间（如 T_2、T_3）的访问者访问行为，可以参照图 4 过程实现其合理性判断。由于所有共识认证主体使用相同的共识认证算法并执行相应的程序，因此通常其共识认证结果是一致的。如果在共识认证过程中出现共识认证结果不一致的情况，系统会重新启动智能合约并进行认证分析；对于无法通过智能合约得到一致性判断结果的访问者访问行为，区块链系统会将其所有共识认证主体的判断结果提交给数据库应用系统管理员，由数据库应用系统管理员重新组织其他的共识认证主体集合对访问者访问行为进行检验和认证。对于所有认证主体认为合理的访问行为，区块链系统会进行记录并由认证主体分别构建区块；对于所有认证主体认为不合理的访问行为，区块链系统会终止访问者下一步的访问行为，并由数据库应用系统管理员对访问者的访问权限进行裁定和处理。

3.4.2 共识认证算法

为了便于算法描述，参照 3.3 节的相应符号说明，并用 Vistor_role 表示系统管理员授予访问者的角色，则智能合约 2 共识认证的算法（Smart_con2 算法）如算法 1 所示，系统管理员决策判定如算法 2（Adm( ) 算法）所示。

算法 1 Smart_con2 算法

输入 Vis_id, Vis_per, Vistor_role, Vis_obj

输出 Vis_beh 判定结果

1) 每一个 Authen_sub 认证 Visitor 的 Vis_id

if 所有 Authen_sub 的认证结果都是 true，做以下判断

2) 每一个 Authen_sub 认证 Adm 授予 Visitor 的 Vistor_role

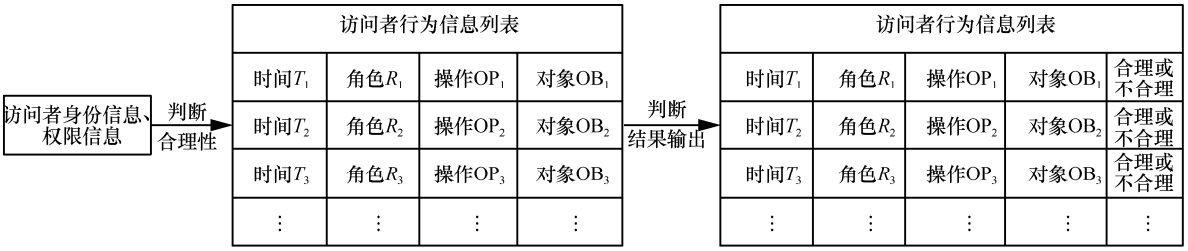

图 5 基于区块链的数据库访问控制用户行为过程判断原理

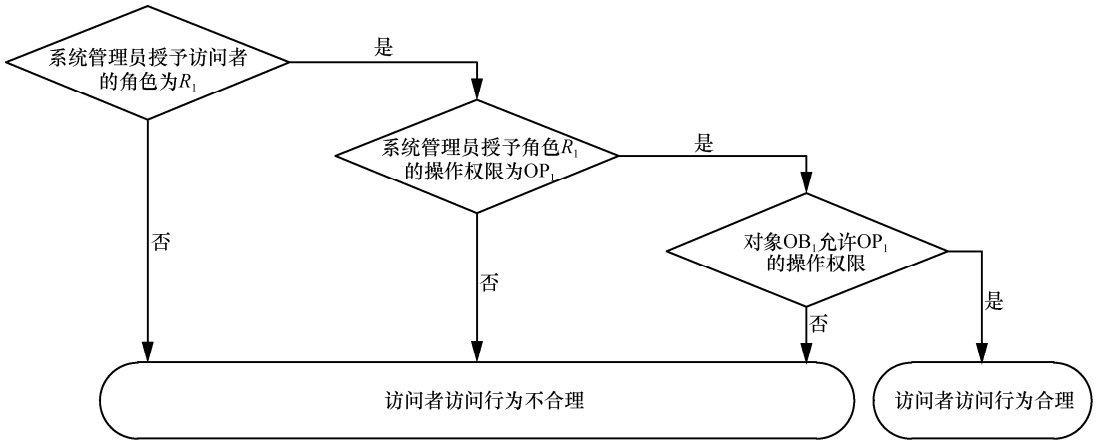

图 6 智能合约 2 的逻辑判断过程

if 所有 Authen_sub 的认证结果都是 true，做以下判断

3)　每一个 Authen_sub 认证 Adm 授予 Visitor_role 的 Vistor_per

if所有 Authen_sub 的认证结果都是 true，做以下判断

4)　每一个 Authen_sub 认证 Vis_obj 授予 Visitor 的 Vistor_per

if所有 Authen_sub 的认证结果都是 true

Visitor 的 Visitor_beh 合格

else if 所有 Authen_sub 的认证结果都是 false

Visitor 的 Visitor_obj 不合格

else if Authen_sub 的认证结果 inconsistent 并且是第一次判断

goto 4)，重新判断一次

else goto Adm( )

end if

else if 所有 Authen_sub 的认证结果都是 false

Visitor_role 的 Vistor_per 不合格

else if Authen_sub 的认证结果 inconsistent 并且是第一次判断

goto 3)，重新判断一次

else goto Adm( )

end if

else if 所有 Authen_sub 的认证结果都是 false

Visitor 的 Vistor_role 不合格

else if Authen_sub 的认证结果 inconsistent 并且是第一次判断

goto 2)，重新判断一次

else goto Adm( )

end if

else if 所有 Authen_sub 的认证结果都是 false

Visitor 的 Vis_id 不合格

else if Authen_sub 的认证结果 inconsistent 并且是第一次判断

goto 1)，重新判断一次

else goto Adm( )

end if

其中，Adm()算法为系统管理员决策判定算法，如算法 2 所示。

算法 2　Adm( )算法

输入　Authen_sub 判定 Vis_beh 的判定结果

输出　Adm 的决策判定

for Authen_sub 对 Vis_id or Vistor_role or Visitor_per or Vis_obj 认证结果 inconsistent

Adm 重新组织 Authen_sub 执行 Smart_con2 算法，并且 Adm 通过系统数据进行判定

Adm 给出最终决策判定结果

end for

对于访问者身份信息、访问行为信息共识认证的智能合约 1，可以参照智能合约 2 的判定原理、判定过程及共识认证算法进行实现。

3.5　数据库访问控制区块链构建机制

在构建区块时，区块包含的主要信息有访问者身份信息、访问权限信息、访问者访问行为信息、访问对象（数据库的字段或记录）信息，这些信息彼此记录，互为一个整体，形成了对访问者访问行为进行追溯的证据链条，也是对访问者访问行为合理性进行验证的依据。由于区块链本身是一个分布式存储的数据库，并且数据库管理员保存了访问者的身份信息、访问权限信息，访问者访问行为信息又是按数据库应用系统设定的标准信息格式形成的，因此在区块生成时，可以由访问者的身份信息、访问权限信息、访问者访问行为信息、访问对象（数据库的字段或记录）信息内容的相应标识（如编码、符号等）进行记录，以避免区块信息记录的冗余与造成整个存储体系负担过重的问题。

因此，在区块链运行体系外，对访问者身份、访问权限（读、修改、增加、删除等）、访问行为（与访问权限对应）建立对应的标识字典，对相应的数据库的记录内容也建立对应的标识字典，这样会大大缩减区块链的记录空间。标识字典由标识及其对应的访问者身份信息、访问权限信息及访问对象信息组成。

基于以上分析，本文提出数据库访问控制区块链结构如图 7 所示。

图 7 反映了区块链体系的结构、内容及不同部分相应的存储与管理关系。区块链体系主要分为 4 个部分：数据库应用系统管理员、标识字典、区块链（基础记账数据与区块对应）、认证体系（由数据库所有者与权威机构等组成，其中权威机构与数据库所属的业务体系对应）。在图 7 中，标识字典

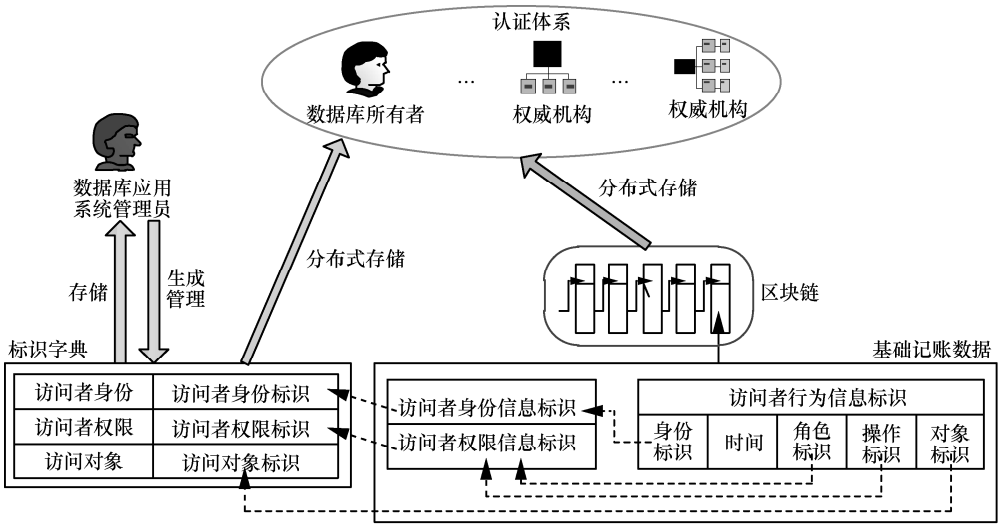

图 7　数据库访问控制区块链结构

由数据库应用系统管理员生成、管理，并由认证主体分布式存储，标识字典与区块链中基础记账数据建立相应的对应关系。在区块链生成过程中，认证体系只需要对访问者的身份信息标识、权限信息标识及访问对象信息标识等进行认证、记录。由图 7 可知，数据库访问控制区块链不仅可以实现对访问者访问行为相关信息的记录，而且相应的访问行为信息也会按访问时间序列形成访问行为路径，有利于对其访问行为进行动态跟踪追溯。

对于区块链的存储问题，由于每个访问者的身份信息与访问行为信息在区块链中是通过标识进行记录的，因此可以由共识认证主体分别进行区块链及其基础数据的存储。对于保密性要求比较高的访问控制系统，也可以由认证主体仅存储区块链，而基于区块链运行的基础数据可以由一些专门的存储体进行存储管理。

在本文构建的访问控制机制中，区块链体系起到了由数据库所有者与权威机构共同验证访问者身份信息、访问权限信息及其访问行为信息合法性并进行分布式存储的作用，实现了对访问者访问过程的监管（对不合法访问的筛查），并确保访问相关信息的可追溯性。与传统数据库访问控制机制相比，本文构建的区块链体系强化了数据库访问控制的力度，确保了访问者对数据库访问的过程形成证据记录，提高了对数据库访问的安全性、可靠性。

4　性能评价

与传统的数据库访问控制体系相比，由于区块链本身的特点及本文构建的架构体系的特点，基于区块链的数据库访问控制体系在实现过程中会在运行时间、资源消耗方面产生变化，具体体现在数据上传区块链时间、共识完成时间、认证过程资源消耗、相关数据存储资源消耗几个方面。对于不同的基于区块链的数据库访问控制体系，由于系统物理架构、区块构建方法、共识认证机制、认证主体特性的不同，区块链运行时间与资源消耗是不同的。数据上传区块链时间及共识完成时间主要体现在与传统访问控制时间及访问者访问时间的对比；认证过程资源消耗及相关数据存储资源消耗体现在与传统数据库访问控制及管理资源消耗的对比。$T_{\text{tra\_con}}$ 表示传统访问控制时间，$T_{\text{tra\_acc}}$ 表示传统访问者访问时间，$T_{\text{data\_bc}}$ 表示数据上传区块链时间，$T_{\text{con\_au}}$ 表示共识完成时间；$R_{\text{tra\_acc}}$ 表示传统数据库访问控制资源消耗，$R_{\text{tra\_man}}$ 表示传统数据库管理资源消耗，$R_{\text{au\_bc}}$ 表示认证过程资源消耗，$R_{\text{sto\_bc}}$ 表示区块链及相关基础数据（标识）分布式存储所消耗的资源。本节从理论方面进行分析和证明。

1) 数据上传区块链时间

在区块链中，数据是以 hash 值的形式以 Merkel 树的结构在区块中进行记录的，由于在基于区块链的数据库访问控制体系中，与区块链构建对应的基础数据包括访问者身份信息、访问者权限信息、访问者访问行为信息、智能合约等，这些数据容量较小，而对于每一个认证主体，其区块的构建是系统自动完成的，因此，基础数据上传区块链的时间远小于传统数据库访问控制过程的时间，即

T_{data_bc}<<T_{tra_con}，T_{data_bc}<<T_{tra_acc}。

2) 共识完成时间

对于不同认证主体验证区块链对应基础数据的真实性或通过智能合约共识形成合理性验证结果来说，整个过程是自动完成的，由于数据真实性判断逻辑或智能合约结构相对简单，进行合理性验证所依据的数据源固定，因此，整个共识认证过程所需要的时间远小于传统数据库访问控制过程的时间，即 T_{con_au}<<T_{tra_con},T_{con_au}<<T_{tra_acc}。

3) 认证过程资源消耗

根据区块链的工作原理，认证主体对数据真实性的验证或对智能合约的运行需要消耗访问控制体系的算力，但由于认证主体数量有限，共识认证逻辑简单，基础数据容量较小，认证主体的认证过程不需要相应的激励机制，因此，认证过程所消耗的资源量远小于传统数据库访问控制体系所消耗的资源量，即 R_{au_bc}<<R_{tra_acc}，R_{au_bc}<<R_{tra_man}。

4) 相关数据存储资源消耗

数据库访问控制相关信息以标识的形式在区块链体系中分布式进行存储，会消耗相应的存储空间，但由于认证主体数量有限，区块链及相关基础数据容量较小，因此，区块链及相关基础数据（标识）分布式存储所消耗的存储资源量远小于传统数据库访问控制体系所消耗的资源量，即 R_{sto_bc}<<R_{tra_acc}，R_{sto_bc}<<R_{tra_man}。

综合以上分析与证明，与传统的数据库访问控制体系相比，基于区块链的数据库访问控制体系在运行时间、资源消耗方面的投入量是可以忽略不计的。

5　结束语

目前，数据库访问控制体系存在着明显的不足，所以在应用中数据库信息泄露的案例较多，包括一些大型公司的数据库以及政府机构的数据库，其根本原因是在访问者对数据库进行访问的过程中访问者身份、访问者权限合理性没有得到进一步的认证，访问者行为的合法性没有得到动态监管和验证，数据库信息泄露后不能有效地追溯责任人的身份与行为过程，不能及时制止损失的扩散。区块链是一个去中心化的分布式数据库，使用共识认证机制对信息的运行过程进行记录，有效地解决了区块链体系内行为过程的可追溯问题，是目前严密解决信用问题的技术体系。

本文将区块链技术应用于数据库访问控制中，通过对访问者身份、访问权限以及访问行为去中心化智能认证和监管，实现了对数据库访问控制的强化，解决了目前数据库访问控制能力弱、访问控制过程追溯性差、责任认定不足的现实问题。本文构建了数据库访问控制体系中区块链的逻辑层次模型及基于区块链的数据库访问控制模型，构建了基于区块链的数据库访问控制过程原理并通过算法进行了流程分析，构建了基于区块链数据库访问控制的共识认证原理，包括智能合约的内容、判断逻辑及实现算法，构建了访问控制过程中区块构建的方法及数据之间的关联关系，对基于区块链的数据库访问控制体系的性能进行了分析与证明。本文的研究在保持数据库应用系统原有访问控制模式的基础上应用区块链技术，可以确保其应用的可行性，其研究具有很大的前瞻性和现实性，对同类其他研究具有很大的参考价值和借鉴意义。

下一步的研究将致力于将本文的研究架构和模式在具体的数据库应用系统中进行应用，确保本文的研究成果落地和运行，并在实际应用中不断地进行测试和评估，针对具体的应用环境对架构和模型进行改进和具体化，提高现有数据库应用系统访问控制的能力。

参考文献：

[1] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[R]. Bitcoin Whitepaper, (2008-11)[2019-12-24].

[2] 张健. 区块链: 定义未来金融与经济新格局[M]. 北京: 机械工业出版社, 2016.
ZHANG J. Blockchain: defining new patterns for finance and economics in future[M]. Beijing: China Machine Press, 2016.

[3] 朱建明, 高胜, 段美姣, 等. 区块链技术与应用[M]. 北京: 机械工业社, 2018.
ZHU J M, GAO S, DUAN M J, et al. Blockchain technology and applications[M]. Beijing: China Machine Press, 2018.

[4] 任彦冰, 李兴华, 刘海, 等. 基于区块链的分布式物联网信任管理方法研究[J]. 计算机研究与发展, 2018, 55(7): 1462-1478.
REN Y B, LI X H, LIU H, et al. Blockchain-based trust management framework for distributed Internet of things[J]. Journal of Computer Research and Development, 2018, 55(7):1462-1478.

[5] DWIVEDI A D, SRIVASTAVA G, DHAR S, et al. A decentralized privacy-preserving healthcare blockchain for IoT[J]. Sensors, 2019(19): 326.

[6] KSHETRI N. Blockchain and electronic healthcare records[J]. Computer, 2018, 51(12): 59-63.

[7] CLAUDE P, JESSE E. Blockchain for healthcare: the next generation of medical records?[J]. Journal of Medical Systems, 2018, 42(9): 1-3.

[8] DOLGUI A, IVANOV D, POTRYASAEV S, et al. Blockchain-oriented dynamic modelling of smart contract design and execution in the supply chain[J]. International Journal of Production Research, 2019, 58(7): 2184-2199.

[9] CHRISTOPH V D E, LAFARRE A. Blockchain and smart contracting for the shareholder community[J]. European Business Organization

Law Review, 2019, 20(1): 111-137.
[10] SUN X, WANG Q, KULICKI P, et al. A simple voting protocol on quantum blockchain[J]. International Journal of Theoretical Physics, 2019, 58(1): 275-281.
[11] KSHETRI N, VOAS J. Blockchain-enabled e-voting[J]. IEEE Software, 2018, 35(4): 95-99.
[12] 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(5): 969-988.
SHAO Q F, JIN C Q, ZHANG Z, et al. Blockchain: architecture and research progress[J]. Chinese Journal of Computers, 2018, 41(5): 969-988.
[13] 朱建明, 付永贵. 基于区块链的供应链动态多中心协同认证模型[J]. 网络与信息安全学报, 2016, 2(1): 27-33.
ZHU J M, FU Y G. Supply chain dynamic multi-center coordination authentication model based on blockchain[J]. Chinese Journal of Network and Information Security, 2016, 2(1): 27-33.
[14] ASTE T, TASCA P, DI MATTEO T. Blockchain technologies: the foreseeable impact on society and industry[J]. Computer, 2017, 50(9): 18-28.
[15] ROMAN-BELMONTE J M, HORTENSIA C R, RODRIGUEZ-MERCHAN E. C. How blockchain technology can change medicine[J]. Postgraduate Medicine, 2018,130(4): 420-427.
[16] 闵新平, 李庆忠, 孔兰菊, 等. 许可链多中心动态共识机制[J]. 计算机学报, 2018, 41(5): 1005-1020.
MIN X P, LI Q Z, KONG L J, et al. Permissioned blockchain dynamic consensus mechanism based multi-centers[J]. Chinese Journal of Computers, 2018, 41(5): 1005-1020.
[17] 马晓婷, 马文平, 刘小雪. 基于区块链技术的跨域认证方案[J]. 电子学报, 2018, 46(11): 2571-2579.
MA X T, MA W P, LIU X X. Cross domain authentication scheme based on blockchain technology[J]. Acta Electronica Sinica, 2018, 46(11): 2571-2579.
[18] FU Y G, ZHU J M, GAO S. CPS information security risk evaluation based on blockchain and big data[J]. Tehnički Vjesnik, 2018, 25(6): 1843-1850.
[19] GAO F. Data encryption algorithm for e-commerce platform based on blockchain technology[J]. Discrete and Continuous Dynamical Systems-Series S, 2019, 12(4-5): 1457-1470.
[20] MUNEEB U H, MUBASHIR H R, CHEN J. Privacy preservation in blockchain based IoT systems: integration issues, prospects, challenges, and future research directions[J]. Future Generation Computer Systems-the International Journal of eScience, 2019, 97(3): 512-529.
[21] 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.
[22] 朱建明, 丁庆洋, 高胜. 基于许可链的 SWIFT 系统分布式架构[J]. 软件学报, 2019,30(6): 1594-1613.
ZHU J M, DING Q Y, GAO S. Distributed framework of SWIFT system based on permissioned blockchain[J]. Journal of Software, 2019, 30(6): 1594-1613.
[23] MEMON R A, LI J P, AHMED J. Simulation model for blockchain systems using queuing theory[J]. Electronics, 2019, 8: 234.
[24] SHE W, LIU Q, TIAN Z, et al. Blockchain trust model for malicious node detection in wireless sensor networks[J]. IEEE Access, 2019(7): 38947-38956.
[25] TOYODA K, MATHIOPOULOS P T, SASASE I, et al. A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain[J]. IEEE Access, 2017(5): 17465-17477.
[26] MAO D, HAO Z, WANG F, et al. Novel automatic food trading system using consortium blockchain[J]. Arabian Journal for Science and Engineering, 2019, 44(4): 3439-3455.
[27] ZHONG L, WU Q, XIE H, et al. A secure versatile light payment system based on blockchain[J]. Future Generation Computer Systems-The International Journal of eScience, 2019, 93(4): 327-337.
[28] TAO Q, CUI X, HUANG X, et al. Food safety supervision system based on hierarchical multi-domain blockchain network[J]. IEEE Access, 2017(7): 51817-51826.
[29] LIAO F Q, WANG J F, SHEN J. BCDP: a blockchain-based credible data publishing system[J]. Journal of Internet Technology, 2019, 20(2): 323-331.
[30] WANG S, ZHANG Y, ZHANG Y. A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems[J]. IEEE Access, 2018(6): 38437-38450.
[31] MA M, SHI G, LI F. Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the IoT scenario[J]. IEEE Access, 2019(7): 34045-34059.
[32] DING S, CAO J, LI C, et al. A novel attribute-based access control scheme using blockchain for IoT[J]. IEEE Access, 2019(7): 38431-38441.
[33] 刘敖迪, 杜学绘, 王娜, 等. 基于区块链的大数据访问控制机制[J]. 软件学报, 2019, 30(9): 2636-2654.
LIU AD, DU XH, WANG N, et al. A blockchain-based access control mechanism for big data[J]. Journal of Software, 2019, 30(9): 2636-2654.
[34] 王秀利, 江晓舟, 李洋.应用区块链的数据访问控制与共享模型[J]. 软件学报, 2019,30(6): 1661-1669.
WANG X L, JIANG X Z, LI Y. Model for data access control and sharing based on blockchain[J]. Journal of Software, 2019, 30(6): 1661-1669.
[35] ZHANG Q, LI Y, LI Z, et al. Access control based on ciphertext attribute authentication and threshold policy for the Internet of things[J]. Sensors, 2019(19): 5237.
[36] ZHANG Y B, CUI M, ZHENG L J, et al. Research on electronic medical record access control based on blockchain[J]. International Journal of Distributed Sensor Networks, 2019, 15(11): 1-13.

[作者简介]

付永贵（1976– ），男，山西广灵人，博士，山西财经大学副教授，主要研究方向为区块链、信息安全等。

朱建明（1965– ），男，山西太原人，中央财经大学教授、博士生导师，主要研究方向为网络与信息安全、区块链等。