Computer Science and Application 计算机科学与应用, 2019, 9(5), 904-911
Published Online May 2019 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2019.95102

Hans汉斯

Data Access Control Framework Based on Blockchain

Zheng Xiong[1], Lei Yao[2], Wenjie Li[1]

[1]Jiangsu Frontier Electric Technology Co., Ltd., Nanjing Jiangsu
[2]Deparment of Software Engineering, Southeast University, Nanjing Jiangsu
Email: 15905166619@139.com, 1173867960@qq.com

Received: May 1st, 2019; accepted: May 13th, 2019; published: May 20th, 2019

Abstract

In the Internet environment, access control of data has become a research hotspot of current information systems. Technologies such as encryption, authentication, intrusion detection, and access control used in traditional security fields cannot meet the requirements for data access in an open environment. Based on this paper, we propose to manage user access rights by using blockchain technology. This effectively achieves controlled access to data by participants in the public environment.

Keywords

Open Environment, Blockchain, Permission, Access Control

基于区块链的数据访问控制框架

熊　政[1]，姚　磊[2]，厉文婕[1]

[1]江苏方天电力技术有限公司，江苏　南京
[2]东南大学软件学院，江苏　南京
Email: 15905166619@139.com, 1173867960@qq.com

收稿日期：2019年5月1日；录用日期：2019年5月13日；发布日期：2019年5月20日

摘　要

在互联网环境下，对数据的访问控制成为当前信息系统的研究热点，传统的安全领域使用的如加密、认证、入侵检测以及访问控制等技术已不能满足在开放环境下对数据访问的要求。基于此本文提出通过采用区块链技术来管理用户的访问权限。这有效地实现了公共环境下各方参与者对数据的控制访问。

文章引用: 熊政, 姚磊, 厉文婕. 基于区块链的数据访问控制框架[J]. 计算机科学与应用, 2019, 9(5): 904-911.
DOI: 10.12677/csa.2019.95102

关键词

开放环境，区块链，权限，访问控制

1. 引言

在开发的互联网环境之下，每个人都可以利用互联网的资源和人脉去做一些有价值的事情，比如个人商品的买卖，网页的设计等等，但这些基本都得在一个中心化的框架内运作，而这与开放的互联网环境又是相悖的。目前现有的框架结构融合了大量具有“所有权”特征的数据[1]，虽然平台也对此做了一定的数据访问安全控制，例如增加多因子安全认证[2]访问控制，采用更强的加密方案等。然而，这也意味着一旦敌手进入了系统，就可以访问到所有数据，存在有单点失败问题。同时，用户必须依赖于第三方，所有的关系数据都集中在中心化服务器中，第三方机构大量收集和控制个人隐私数据已威胁到其信息安全[3]。

区块链作为一个分布式可验证的公共账本，具有匿名性、分布式、去可信等特性，可以作为构建可行计算平台的基础[4]。本文针对在互联网开发环境下如何实现可信的访问，结合当前的区块链技术，提出一个去中心化的访问控制方案。在该方案中，甲方可以通过区块链合约来定义访问控制，而访问者即乙方在满足甲方所设定的条件后，可向区块链申请身份验证，在获得许可之后，便可以访问甲方的数据并作数据进行操作。这有效地实现了用户数据的安全访问和有效使用。

2. 相关工作

2.1. 区块链工作原理

区块链的基本原理理解起来并不复杂。首先，区块链包括三个基本概念：

- 交易(transaction)：一次对账本的操作，导致账本状态的一次改变，如添加一条转账记录；
- 区块(block)：记录一段时间内发生的所有交易和状态结果，是对当前账本状态的一次共识；
- 链(chain)：由区块按照发生顺序串联而成，是整个账本状态变化的日志记录。

如果把区块链作为一个状态机，则每次交易都会改变当前的状态，而每次共识生成的区块，就是参与者对于区块中交易导致状态改变结果的确认。

在实现上，首先假设存在一个分布式的数据记录账本，这个账本只允许添加、不允许删除。账本的底层结构是一个线性的链表，链表由一个个“区块”串联组成(如图 1 所示)，后继区块记录前导区块的

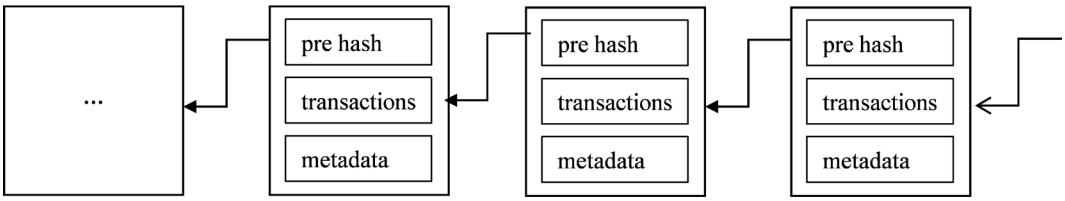

Figure 1. Blockchain ledger structure
图 1. 区块链结构示例

hash 值(pre hash)。新的数据要加入，必须放到一个新的区块中。而这个块(以及块里的交易)是否合法，可以通过计算 hash 的方式快速检验出来。任意维护的节点都可以提议一个新的合法区块，然而必须经过一定的共识机制来对最终选择的区块达成一致。

网络中，所有节点构成了一个点对点的通信网络，通过复制每个节点在同一个区块链上进行操作，其工作过程如下：

1) 交易的生成。当前所有者利用私钥对前一次交易和下一位所有者签署一个数字签名，并将这个签名附加在这枚货币的末尾，制作成交易单。一笔新交易产生时，会先被广播到区块链网络中的其它参与节点。

2) 交易的传播。当前所有者将交易单广播至全网，每个节点会将数笔未验证的交易 Hash 值收集到区块中，每个区块可以包含数百笔或上千笔交易。最快完成 POW 的节点，会将自己的区块传播给其他节点。

3) 工作量证明。每个节点通过相当于解一道数学题的工作量证明机制，从而获得创建新区块的权力，并争取得到数字货币的奖励。各节点进行工作量证明的计算来决定谁可以验证交易，由最快算出结果的节点来验证交易，这就是取得共识的做法。

4) 全节点验证。当一个节点找到截时，它就向全网广播该区块记录的所有盖时间戳的交易，并由全网其他节点核对，其他节点会确认这个区块所包含的交易是否有效，确认没被重复花费且具有效数位签章后，接受该区块，此时区块才正式接上区块链，无法再窜改资料。

5) 区块链记录。全网其他节点核对该区块记账的正确性，没有错误后他们将在该合法区块之后竞争下一个区块，这样就形成了一个合法记账的区块。

2.2. 分布式共识机制

区块链系统的核心是有系统中节点竞争记账，这个竞争的过程称为共识机制，区块链的底层有四部分构成，如图 2 所示，一个分布式的数据库用来存储以往和将来的交易数据，密码学的公私密钥体系用

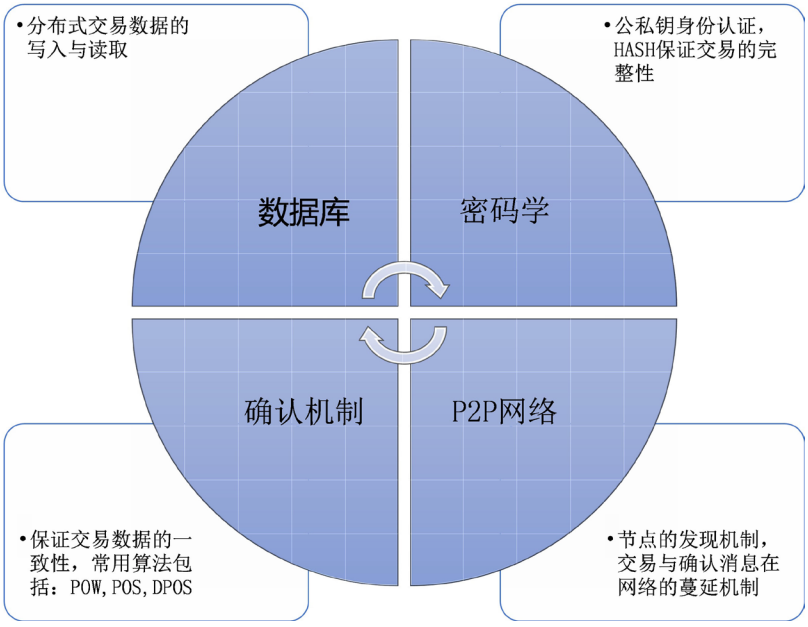

Figure 2. Distributed consensus mechanism
图 2. 分布式共识机制

来确认交易双方的身份，P2P 网络用来广播和蔓延各类消息(如节点加入消息，节点失效消息，得到挖矿数据的消息)和用来决定节点记账权利的共识机制。

2.3. 区块链技术特点

特点一：分布式数据库

区块链上的每一方都可以访问整个数据库及其完整的历史记录。没有单一方控制数据或信息。每一方都可以直接验证其交易合作伙伴的记录，而无需中间人。

特点二：对等传输

通信直接在对等体之间发生，而不是通过中心节点。每个节点存储并转发信息到所有其他节点。

特点三：透明的匿名性

任何有权访问系统的用户都可以看到每个事务及其关联值。区块链上的每个节点或用户都有一个唯一的 30 以上的字母、数字组成的地址，用于标识自身。用户可以选择保持匿名或向他人提供其身份证明。

特点四：记录的不可逆性

一旦在数据库中输入事务并更新了帐户，则不能更改记录，因为它们链接到它们之前的每个交易记录(因此称为“链”)。采用各种不同的算法以确保数据库中的记录是永久的、按时间顺序排序的，并且对于网络上的所有其他节点都是可以访问的。

特点五：计算逻辑

分类帐本的数字性质意味着区块链交易可以关联到计算逻辑、本质上是可编程的。因此，用户可以设置自动触发节点之间交易的算法和规则。

3. 基于区块链的访问控制框架

区块链的技术特点避免了现有的中心化所带来的安全问题，在开发的互联网环境中，任何参与方都可以在此框架之下进行价值的互换。如图 3 所示，企业或者个人可以在平台上发布任务，然后交由平台去推广，接单者可在业余时间，在具备一定条件之后便可以去接受任务，完成之后，结果交由区块链中的智能合约来验证，通过合约中设置的条件，即可获得任务奖励。

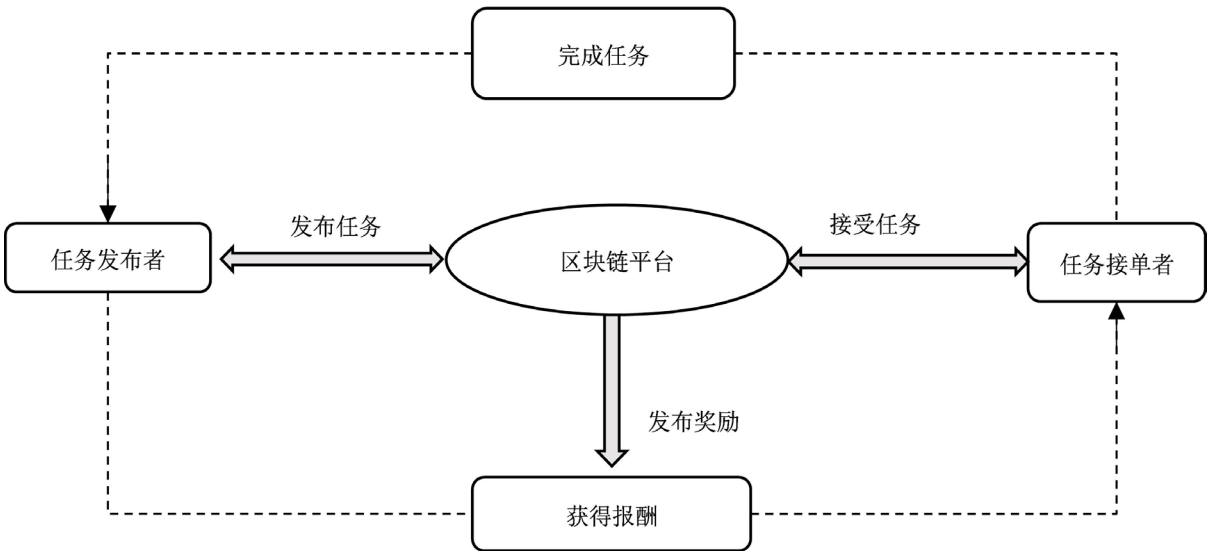

Figure 3. Value network interconnection under the blockchain platform
图 3. 区块链平台下的价值网络互联

在实际应用过程中，无论是对于任务发布者而言还是针对任务接单者，在访问这个基础平台之前，都会先进行拦截，利用区块链的可信的技术特点，判断当前的用户是否有这个权限去访问，只有通过身份验证和达到合约访问控制条件之后，才能进行后续的操作。

在该平台上，我们可以将发布的任务用数据来清晰的表示，任务的发布者可以定义为数据的拥有者，他可以根据自己的需求去定义数据的访问规则。任务接单者可以被当作数据的访问者来看待，需要满足一定的条件才可以访问以及操作拥有者的数据。

结合以上在区块链网络中如何实现在开放环境下的商业运作，提出基于区块链的数据访问控制框架，如图 4 所示。

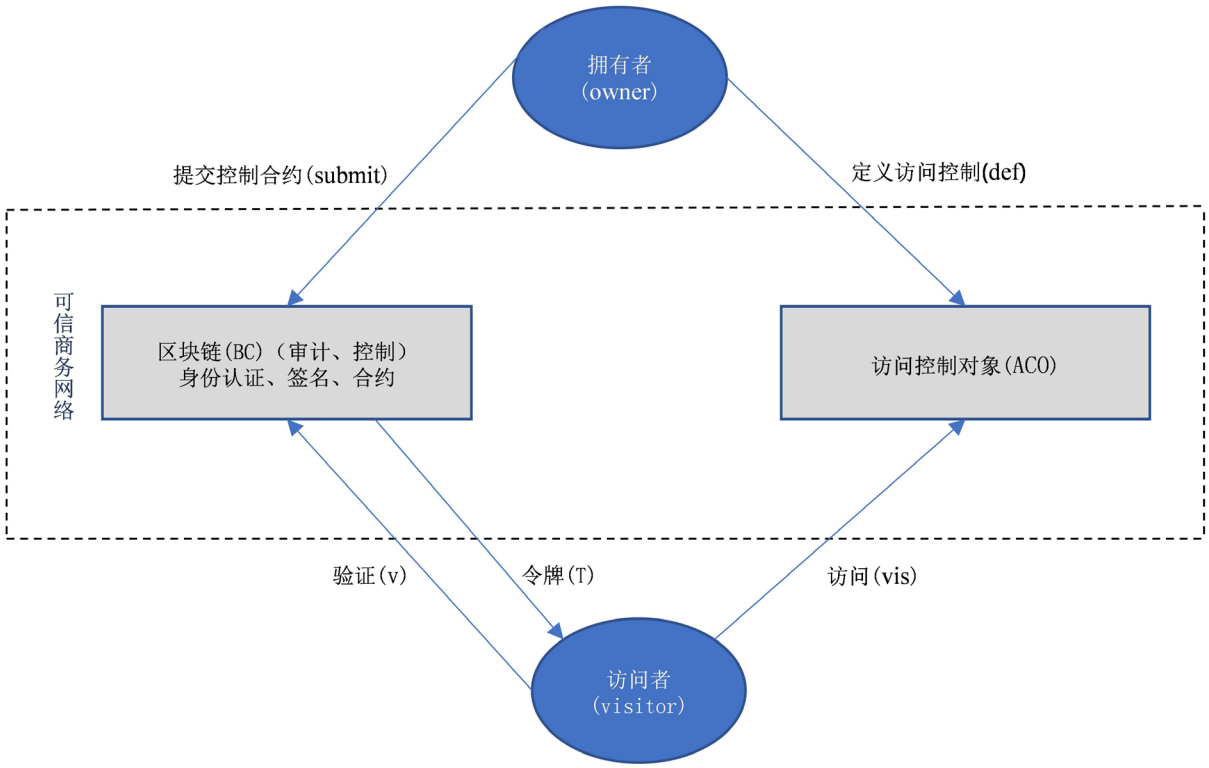

Figure 4. Blockchain access control framework
图 4. 区块链访问控制框架

在开放的环境当中，数据拥有者 owner 会根据数据的敏感程度来定义数据访问控制规则 def(data)，并将访问规则表示成智能合约的形式，部署到区块链网络之中 submit(contract)。访问者 visitor 在访问数据的时候，首先需要进行身份验证 V(ID)，如果通过身份验证并且符合合约条件 C(condition)便可以获取到身份令牌 T，例如 T= {V(ID) AND C(condition)}，数据访问者可以拿着这个令牌访问数据对象。

在该框架中，任何人都可以发布任务，也可以接收任务，没有所谓的中心化的思想束缚。在一个可信的去中心化环境中，数据的拥有者可以自定义数据访问权限，即任务的要求，访问者根据自身的条件，觉得可以胜任，就可以去申请，通过复杂的区块链验证之后，便可以去访问执行数据(任务)。没有第三方的干预，双方可在自由的环境中完成对等的交易。

3.1. 智能合约设计

数据拥有者根据访问规则制定合约，区块链的智能合约赋予账本可编程的特性，也是实现用户数据

交易的基础通道。

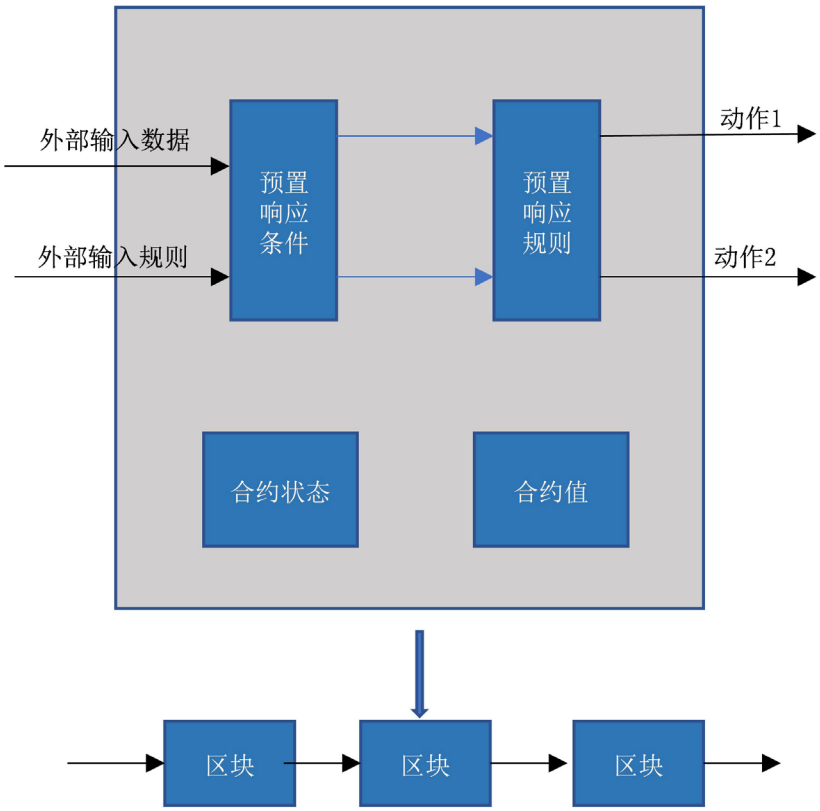

Figure 5. Smart contract conceptual model
图 5. 智能合约概念模型

智能合约的概念模式图如图 5 所示。一般而言，智能合约封装定义的若干状态、转换规则、触发条件以及应对操作等，经各方签署后以程序代码的形式附着在区块链数据上，经过对等计算机网络传播和节点验证后记入各个节点的分布式账本中，区块链可以实时监督整个智能合约的状态，在核查外部数据源确认满足特定的触发条件后激活并执行合约[5]。

其中合约对这些关系数据的定义以及描述是整个系统的关键，在设计时需要明确合约的表示能满足开放环境下读写规则的表达。

基本表示为：

1) 合约的自定义数据模型对应着网络中的具体关系。

2) 合约的函数方法对应着网络数据的读、写和更新操作。

3) 合约当中的逻辑设计对应着网络数据中存在的规则。

数据拥有者可根据自己的意愿来灵活的定义智能合约，以满足自身的业务需求。

3.2. 参与者权限管理

利用区块链的技术特性，可以很容易的处理个人身份验证和协调问题。它可以让个人自由地创建加密的数字身份，取代多个用户名和密码，同时提供更全面的安全功能，能够节省客户和机构宝贵的时间和资源。同时区块链本身就有基于 PKI 体系[6]，生成数字证书以标识用户身份的能力，所以自带用户身份认证的功能。

访问者在获得区块链身份认证之后，便可以调用智能合约，如果满足数据拥有者所制定的合约规则，便能获得 Token 令牌，进而拿着令牌去访问数据对象。

4. 对比分析

本文主要从数据安全、去信任和数据存储 3 个方面进行对比分析。

4.1. 数据安全

常用的四种访问模型，其中基于 RBAC [7] [8]、ABAC [9]和 UCON [10] [11]的访问控制模型都需要一个集中式的服务器来完成授权决策[12]而基于 CapBAC [13] [14]的物联网访问控制模型实现了分布式的架构，但是将访问控制决策放在较弱的物联网设备上并不安全，容易受到黑客的单点攻击，无法满足开放环境下的应用需求。而去中心化的区块链技术很好的解决了中心化所带来的数据安全问题，它不仅保证链上信息的安全可靠，而且也为互联网开发环境下的访问控制带来了新的生机。

4.2. 信任机制

在目前的互联网环境里，数据拥有者一般都是由第三方机构扮演这个角色，因为他们有能力提供足够的计算和存储资源。但是将数据访问控制权力全都交由第三方机构来掌控，又会带来信任危机，诸如数据被篡改、规则一家制定、数据泄露等等问题。区块链技术的目的就是要解决互联网的信任问题，它从技术角度就解决了基于信任的中心化垄断统治的弊端。

4.3. 数据存储

区块链拥有高冗余存储(每个节点存储一份数据)，去中心化、高安全性和隐私保护等特点使其特别适合存储和保护重要隐私数据，以避免因中心化机构遭受攻击或权限管理不当而造成的大规模数据丢失或泄露。任意数据均可通过哈希运算生成相应的 Merkle 树[15]并打包记入区块链，通过系统内共识节点的算力和非对称加密技术来保证安全性[16]。区块链上记录了每个数据拥有者所定义的访问控制策略，由于区块链的去中心化、防篡改等特点，所以更加安全可靠。访问者在身份验证之后，如果通过合约的访问控制，便能安全访问数据。

采用区块链的访问控制方式可以保证参与方在开放环境下数据访问的安全性但在效率方面欠佳，中心化系统一般每秒交易量(tps)可达到百万级以上，而区块链目前的 tps 只达到还远远没有达到理想的数量级。

表 1 是中心化和去中心访问控制的综合比较：

Table 1. Centralized and decentralized access control comparison
表 1. 中心化和去中心化的访问控制比较

	数据安全	信任机制	数据存储	效率
中心化	易受攻击	第三方	中心化数据库	tps 高
去中心化	相对安全	Pow、Pos…	分布式多方存储	tps 低

5. 总结

区块链技术已被证明是廉洁和高度透明的。由于分散，它提供了端到端的安全性和加密。由于其分布式特性，区块链消除了人为错误和防范黑客攻击的风险。所有这些对于访问控制尤其是访问控制即服务来说都是至关重要的。毋庸置疑，未来区块链技术将会让人类社会真正实现“万物互联”。越来越多

的参与者会将区块链技术作为一种工具，借助区块链技术解决行业中存在的信任问题。

当然，市场瞬息万变，区块链技术在数据存储上的应用需要一段时间的检验。在大数据时代，区块链技术的去中心化存储为人们提供了一种更安全、高效、可扩展的解决方案，更好地服务于未来社会。

参考文献

[1] 房梁, 殷丽华, 郭云川, 方滨兴. 基于属性的访问控制关键技术研究综述[J]. 计算机学报, 2017, 40(7): 1680-1698.

[2] Mahnken, S. (2014) Today's Authentication Options: The Need for Adaptive Multifactor Authentication. *Biometric Technology Today*, **2014**, 8-10. https://doi.org/10.1016/S0969-4765(14)70126-2

[3] 刘帝, 吴鹏. 一种基于区块链的个人数据保护模型[J]. 信息与电脑(理论版), 2018(21): 140-142.

[4] Zyskind, G., Nathan, O. and Pentland, A. (2015) Decentralizing Privacy: Using Blockchain to Protect Personal Data. 2015 *IEEE Security and Privacy Workshops*, San Jose, CA, 21-22 May 2015, 180-184. https://doi.org/10.1109/SPW.2015.27

[5] 贺海武, 延安, 陈泽华. 基于区块链的智能合约技术与应用综述[J]. 计算机研究与发展, 2018, 55(11): 2452-2466.

[6] 关振胜. 公钥基础设施 PKI 与认证机构 CA[M]. 北京: 电子工业出版社, 2002.

[7] 赵明斌, 姚志强. 基于 RBAC 的云计算访问控制模型[J]. 计算机应用, 2013, 32(S2): 267-270.

[8] 李凤华, 苏铓, 史国振, 马建峰. 访问控制模型研究进展及发展趋势[J]. 电子学报, 2012, 40(4): 805-813.

[9] Yuan, E. and Tong, J. (2005) Attributed Based Access Control (ABAC) for Web Services. *IEEE International Conference on Web Services*, Orlando, FL, 11-15 July 2005, 569. https://doi.org/10.1109/ICWS.2005.25

[10] Park, J. and Sandhu, R. (2002) Towards Usage Control Models: Beyond Traditional Access Control. In: *Proceedings of ACM Symposium on Access Control Models and Technologies*, ACM, New York, 57-64. https://doi.org/10.1145/507711.507722

[11] Zhang, G. and Gong, W. (2011) The Research of Access Control Based on UCON in the Internet of Things. *Journal of Software*, **6**, 724-731. https://doi.org/10.4304/jsw.6.4.724-731

[12] 史锦山, 李茹. 物联网下的区块链访问控制综述[J/OL]. 软件学报: 1-17, 2019-04-03.

[13] Shen, H.-B. and Liu, S.-B. (2014) A Context-Aware Capability-Based Access Control Framework for the Internet of Things. *Journal of Wuhan University*, **60**, 424-428.

[14] Gusmeroli, S., Piccione, S. and Rotondi, D. (2013) A Capability-Based Security Approach to Manage Access Control in the Internet of Things. *Mathematical & Computer Modelling*, **58**, 1189-1205. https://doi.org/10.1016/j.mcm.2013.02.006

[15] Merkle, R.C. (1987) A Digital Signature Based on a Conventional Encryption Function. In: Pomerance, C., Eds., *Advances in Cryptology—CRYPTO*' 87. *CRYPTO* 1987. *Lecture Notes in Computer Science*, Springer, Berlin, Heidelberg, 369-378. https://doi.org/10.1007/3-540-48184-2_32

[16] 韩璇, 袁勇, 王飞跃. 区块链安全问题: 研究现状与展望[J]. 自动化学报, 2019, 45(1): 206-225.