doi:10.3772/j.issn.2095-915x.2019.04.002

基于轻量级区块链节点的数字电影放映系统设计

杨硕鹏 张延华 杨兆鑫 陈冰容 杨睿哲

北京工业大学信息学部 北京 100124

开放科学（资源服务）标识码（OSID）

摘要：本文基于轻量级区块链节点概念，提出一种新的数字电影放映系统服务框架，利用轻量级区块链节点易维护和运行的特点，在具有嵌入式系统的数字电影放映设备上部署轻节点。该节点设备由完整节点提供服务，不参与高能耗共识运算，仅承担交易发起和部分区块账本存储的功能。应用部署通过轻节点层、全节点层、区块链功能层、服务层以及应用层的划分实现可信服务。实施场景则以数字电影放映管理中的放映机节点需求为例，设计了区块链轻节点放映机功能和工作流程，并采用树莓派实现了一个原型 demo 系统。

关键词：区块链；轻节点；数字电影

中图分类号：N99 G35

IoT Service Architecture Based on Lightweight Blockchain Nodes

YANG Shuopeng ZHANG Yanhua YANG Zhaoxin CHEN Bingrong YANG Ruizhe

Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China

Abstract: A new Digital movie projection system service framework is proposed based on the light blockchain node, which has the character of easy maintenance and operation, and can be deployed on digital projector with embedded CPU. The light node served by the full node, does not participate in the high-consumption consensus operation, while only take part in transaction initiation and partial block book storage. For the application and deployment with different devices, the trusted services are realized through the layers of the light node, the full node, the blockchain function, the service, and the application. Based on this structure, a prototype demo system for the management of digital movie playing is designed, with the details of the functions and workflow of the projector worked as a blockchain light node.

Keywords: Blockchain; light node; digital film

基金项目：国家自然科学基金资助项目（61571021）；北京市博士后科研经费资助项目（2018ZZ029）；北京市博士后朝阳区博士后科研经费资助（2018ZZ017）。

作者简介：杨硕鹏（1995-），硕士研究生，研究方向：区块链技术及智能合约应用；张延华（1960-），教授，研究方向：工业互联网、区块链及智慧无线通信网络研究；杨兆鑫（1993-），博士研究生，研究方向：区块链技术与数据挖掘技术；陈冰容（1995-），硕士研究生，研究方向：区块链技术；杨睿哲（1982-），通讯作者，讲师，研究方向：无线通信技术与移动边缘计算技术，E-mail：yangruizhe@bjut.edu.cn。

doi:10.3772/j.issn.2095-915x.2019.04.002

引言

据估计，未来十年物联网将带动数字企业持续创新，百亿量级的设备互联以及由此生成的大量数据导致的计算开销和数据安全问题已经成为一项巨大的挑战。

在传统的网络应用 C/S（客户端 / 服务器）服务架构中，入网设备将数据或信息上传到中心数据库或者服务器中，缺少相应的容错机制并且容易暴露用户隐私信息；此外，随着联网物理设备（如物联网设备）的持续增加，中心数据库或服务器的运行模式也将面临极大挑战。与集中式存储和运算不同，区块链技术以块链式数据结构验证与存储数据、以分布式节点共识算法保证数据一致性、以自动化脚本代码组成的智能合约来编程和操作数据，是一种去中心化、透明、安全的分布式基础架构。其链上信息的不可篡改性能够保证数据的安全存储与共享，其分布式结构也避免了集中存储数据的设备负担，有效地降低了网络负载，从而成为大规模物联网数据存储和共享的有效解决方案。文献 [1] 中将区块链与工业互联网相结合，提出一种有别于传统区块链链式结构的新型分布式账本技术。文献 [2] 提出一种基于区块链的伴随安全存储和同态计算的物联网系统，利用区块链的特点，服务器可以通过对数据执行同态计算来处理用户的数据。此外，该系统还可以通过吸引外部计算资源加入其中而不断增加系统性能。

然而，区块链技术应用于物联网 [3]，在设备管理及数据传输交换方面将存在低功耗物联网终端设备没有足够的资源运行区块链客户端并且进行密集的区块链计算的问题 [4]。本文提出一种基于轻量级区块链节点的物联网服务架构，通过轻节点层、全节点层、区块链功能层、服务层以及应用层的划分完成可信的服务。其中，轻量级区块链节点部署在物联网中具有嵌入式系统的设备上，承担交易发起和部分区块账本存储的功能，但避免参与高消耗的共识，以其有限资源提高系统的可靠性 [5]。本文基于区块链轻节点架构，研究了轻节点功能和工作流程，并采用树莓派设计实现了一个原型区块链数字电影放映系统。

1 轻节点区块链系统部署

轻量级区块链节点物联网服务架构由轻节点层、全节点层、区块链功能层、服务层以及应用层组成，如图 1 所示。

（1）轻节点层

轻节点层包括可部署和运行区块链客户端的各类设备。由于计算和存储性能的约束，这类设备在系统架构中作为轻量级区块链节点，一方面，其本身并不具有足够的算力执行共识算法（挖矿命令），而是转发交易到系统架构上一层的全节点层进行共识上链，另一方面，由于节点受限于存储容量，故节点存储区块链副本且只存储区块头而不存储包含大量交易数据的区块体。

在物联网环境中，轻节点特性与网络边缘设备的物理特性以及通信特点相匹配，特别是采用 M2M 的物联网终端设备间的 P2P 通信与区块链网络层 P2P 结构的一致性，能够有效支撑轻量级的区块信息传播。

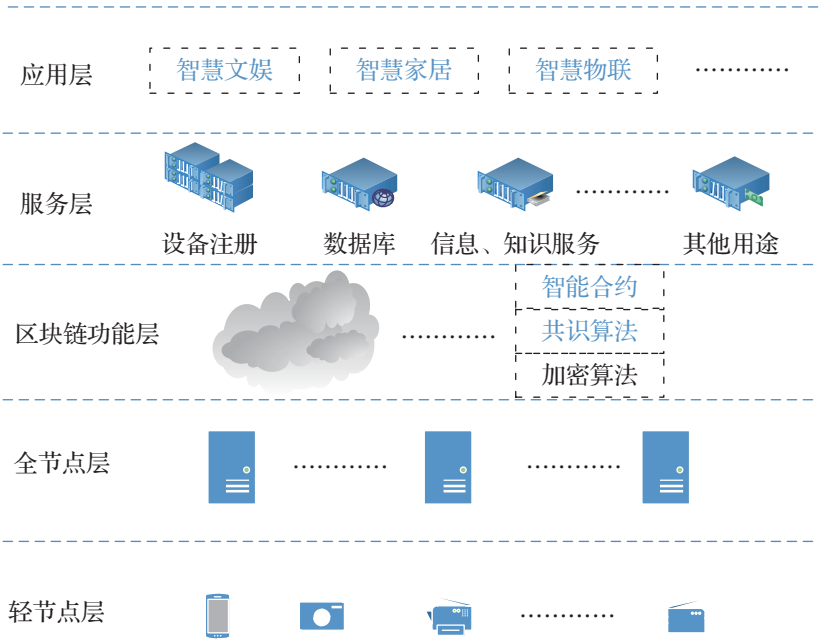

图 1　轻量级区块链节点物联网服务架构

（2）全节点层

全节点层包括负责维护整个区块链系统正常运转的全节点，处理由下一层的物联网设备、轻量级节点提交到区块链网络中的交易请求。全节点通过共识机制将设备信息、数据信息写入区块链网络中 [6]。

作为区块链节点的设备，不论是轻节点还是全节点，都需要拥有区块链账户地址作为接收该设备产生的数据信息提交的目标地址 [7]。设备在加入区块链系统前需伴随密码参数向区块链系统发送请求，使用该密码作为私钥来申请账户地址。私钥经过区块链加密算法生成公钥，作为该节点设备的唯一标识。各设备在上传信息时需要将公钥、私钥与数据信息共同提交给区块链账户。

（3）区块链功能层

区块链功能层包括共识算法、加密算法、智能合约。该层由区块链全节点层的节点共同维护。数据由物联网 [8] 轻节点设备加密后上传到全节点进行共识，通过共识后上传至区块链账本并根据智能合约触发相应的服务层及应用层 [14]。

（4）服务层

服务层由多种服务器构成，不同的服务器用于执行不同的服务，包括注册服务器、信息服务器、知识服务器等 [9]。

注册服务器负责处理轻量级节点设备注册、用户注册等服务。每个轻量级节点设备都需要经过注册服务器在区块链系统中完成注册（详见图 2）。区块链系统会根据设备厂商为设备设置的私钥经过特定公钥 / 私钥算法计算出一个公钥 [10]，并将该设备的信息与公钥、私钥共同作为设备属性存储在智能合约中。该公钥在区块链系统中唯一且有效，公钥再经过注册服务器返回给设备。由此，设备被允许作为轻量级节点 / 全节点接入区块链网络中参与交易 [11]。

doi:10.3772/j.issn.2095-915x.2019.04.002

信息服务器存储每个轻量级节点上传的信息[12]。在验证通过的情况下，信息除了通过轻量级设备节点被提交到区块链系统中储存外，还能够直接向信息服务器发送数据，包括轻量级设备节点公钥、URL、数据字段等信息。信息服务器保存之后同时将数据上传至区块链系统，交易完成后区块链系统会返回交易哈希、交易所在区块等信息，再由信息服务器对应信息将交易信息完成保存，与数据信息构成映射对，以方便后续用户对数据的使用。

知识服务器对应信息服务器，在信息服务器的数据基础上，通过大数据分析得出的信息获得普遍适用的结论，并进行信息预测，为进一步规划等做出指导意见。

（5）应用层

应用层包括手机 APP、信息监管平台等，为各行业提供智慧服务。亦可由上到下指导物联网设备的信息采集动作，下发命令管理等。适用于不同领域，包括农业、交通、物流、医疗等。

2 树莓派轻节点系统设计

基于图 1 的系统架构，本文采用树莓派设计并实现了一个轻量级区块链节点原型系统，采用 go 语言构建了以太坊客户端的私有链测试环境，使用 python 语言的 web 开发框架 django 处理轻量级节点设备发起的请求，具体操作流程如下。

（1）轻量级节点的设备注册

轻量级节点设备注册步骤，如图 2 所示。

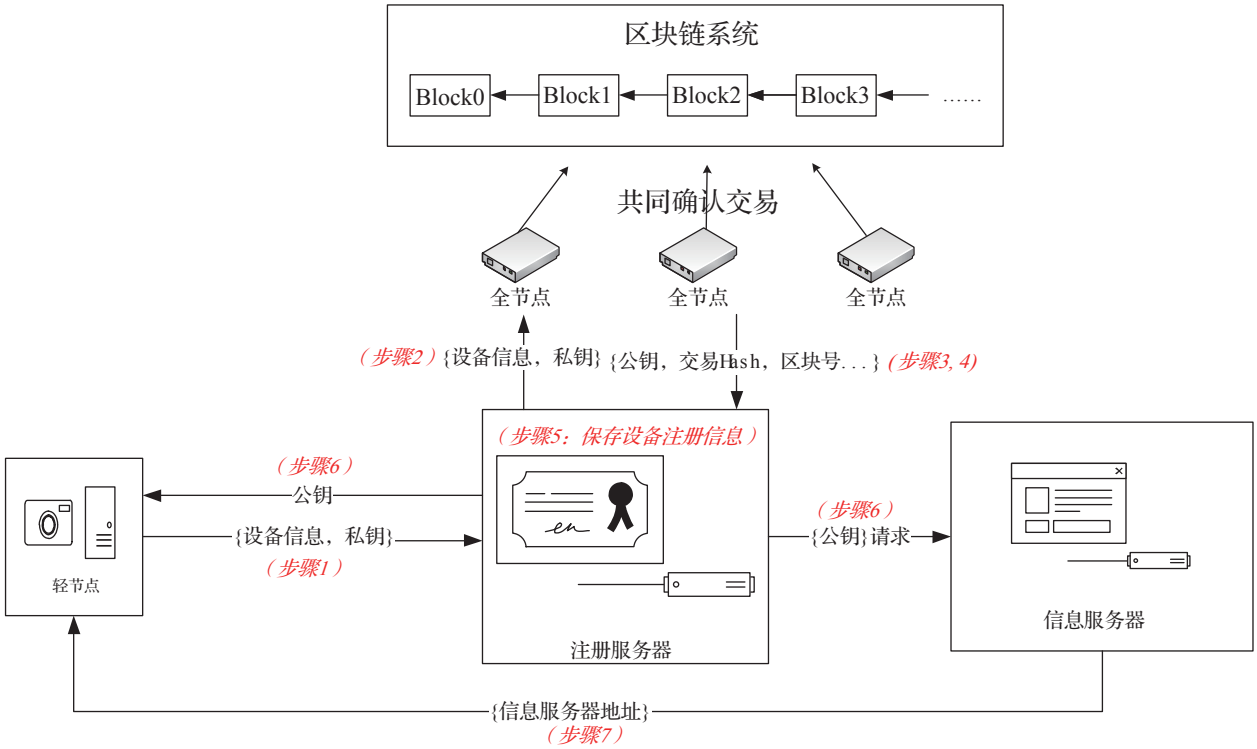

图 2 轻量级节点设备注册过程

步骤 1：当一个设备作为轻量级区块链节点接入区块链系统之前，轻量级节点设备需向注册服务器发送请求，请求参数包括设备信息（例如生产时间、设备型号、设备细节参数等）和属于设备的私钥信息。该私钥作为后续使用设备服务的密码。即轻量级节点设备需向注册服务器发送一个带有设备信息和私钥字符串的请求。

步骤 2：注册服务器接收到来自轻量级区块链节点设备的请求之后，获得请求参数，包括设备信息和私钥信息并将其保存在本地数据库，同时将设备信息和私钥作为参数向区块链系统发送。

步骤 3：区块链系统接收到轻量级区块链节点设备信息和私钥后，通过加密算法根据设备的请求私钥计算出一串唯一的十六进制字符串，作为该请求设备的公钥，即该设备的唯一标识。

步骤 4：区块链系统根据私钥计算出公钥之后，将设备信息、私钥、公钥对应该设备存入关于设备注册的智能合约中，成功存入之后会返回交易 Hash 值、区块号等交易数据，区块链系统将公钥、交易 Hash、区块号返回给注册服务器。

步骤 5：注册服务器将接收到的公钥、交易 Hash、区块号对应步骤 2 中保存在本地的设备信息和私钥信息一并保存，作为后续查询区块链系统的索引，方便了设备注册信息的查询。

步骤 6：注册服务器一方面将公钥信息返回给轻量级区块链节点设备，另一方面将公钥作为参数向信息服务器发出请求，使用公钥作为主键为该设备请求一个信息服务器，存储该设备后续可能上传的信息。

步骤 7：信息服务器接收到注册服务器的请求之后，将信息服务器地址返回给轻量级节点设备，轻量级节点将信息服务器地址对应本设备的公钥信息存储在设备本地。

至此，轻量级区块链节点设备完成设备注册。设备注册信息分别存储在区块链系统的智能合约和注册服务器中，另外注册服务器中还存储着设备注册信息在区块链系统中对应存储的区块号（位置）以及交易 Hash 值，便于后续查询以及验证。

（2）轻量级节点的数据上传

数据上传步骤如图 3 所示。

步骤 1：轻量级区块链节点首先检查内部是否存有一部信息服务器的地址，若没有，则代表该设备未在区块链系统中进行注册；若有，则将｛公钥、私钥、要上传的数据 Data｝作为请求参数向信息服务器发送请求。

步骤 2：信息服务器接收到请求后，一方面将数据保存在本地，另一方面将数据上传到区块链系统，同时将数据发送给知识服务器。

步骤 3：区块链系统接收到从信息服务器发送过来的新信息记录之后，存入记录数据的智能合约，成功保存之后将｛交易 Hash，区块号｝返回给信息服务器。

步骤 4：信息服务器接收到｛交易 Hash，区块号｝后，对应该条记录保存，即完成数据 - 交易的映射，例如｛设备公钥，所上传数据，URL｝-｛交易 Hash，区块号｝。

步骤 5：知识服务器获得由信息服务器发送来的数据后，根据设备公钥、数据等信息提取深层次的数据价值，利用数据挖掘、大数据分析技术提炼出普遍适用的结论或是预测数据等，供应用层使用，提高用户体验。

doi:10.3772/j.issn.2095-915x.2019.04.002

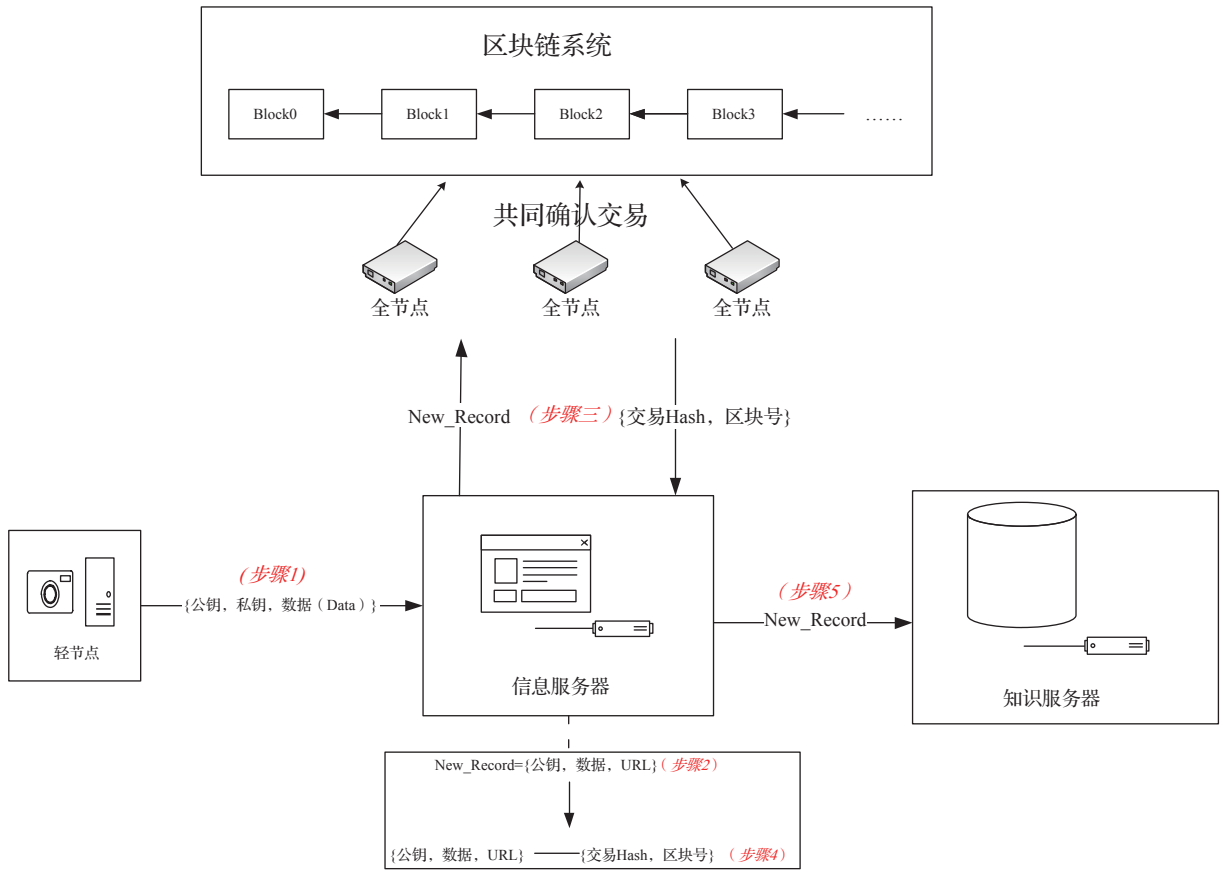

图 3 轻量级节点的数据上传

至此，轻量级区块链节点设备完成了数据的上传。设备经过验证后将信息上传到信息服务器，信息服务器将数据分别发送给区块链系统和知识服务器，并将数据以及区块链系统返回的交易 Hash 和区块号映射保存，方便后续对数据的查询与使用。

3 数字电影应用场景设计

院线制数字电影放映一直以来存在着放映信息难以实时采集和监管的难题。针对这一需求，本文基于区块链轻节点架构，采用树莓派设计并实现了一个数字电影放映信息采集和监管系统，部署区块链轻节点放映机作为区块链节点，将放映机产生放映数据直接写入区块链。

根据图 1 所示的区块链应用架构，图 4 的轻量级区块链流动电影应用平台将放映机作为轻量级区块链节点设备。放映机在作为轻量级节点使用前，需要将放映机信息（包括厂商信息、放映机型号、生产信息等）、私钥作为参数向图 4 服务层的注册服务器发出请求，注册服务器接收请求后会将该放映机信息、私钥写入区块链的智能合约中，同时保存该条交易的交易 Hash 值、区块号等关键信息。此外，注册服务器向信息服务器注册该放映机上传数据的路径，信息服务器返回给放映机一个地址供其上传数据，完成放映机的注册。此时，该放映机作为轻量级区块链节点接入区块链系统。

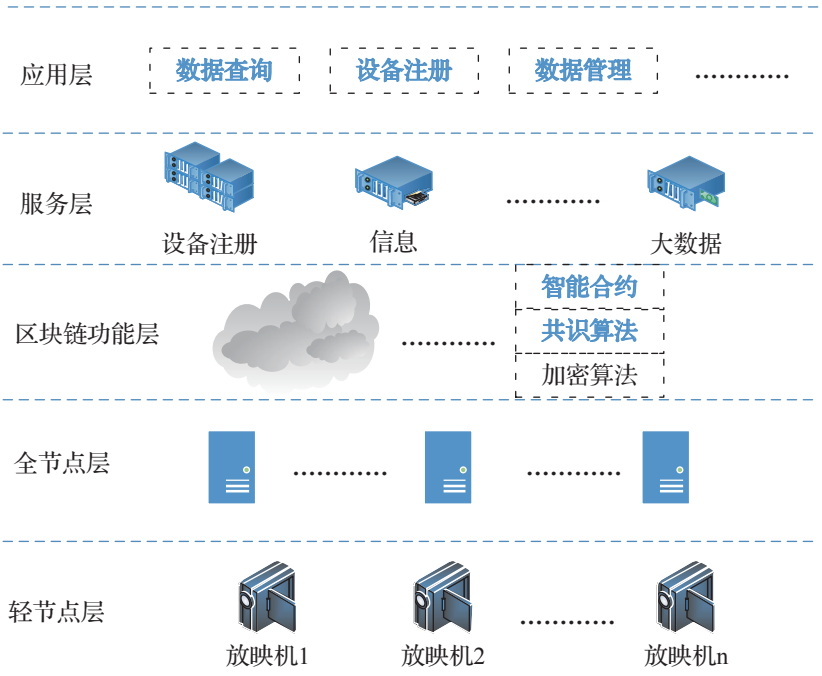

图 4 轻量级区块链节点数字电影放映应用架构

在放映机播放电影并产生放映数据（包括放映员 ID、播放影片信息、开始 / 结束时间、地点等）之后，作为轻节点的放映机可将信息直接写入区块链功能层的智能合约中，同时该放映机向保存在本地的信息服务器路径发送 { 公钥，私钥，放映数据 }，信息服务器接收数据之后保存该条交易返回的交易 Hash 值和区块号，并将该条放映数据发送给知识服务器。

监管人员查询、管理放映数据，需要在区块链系统中注册权限，注册方法类似于放映机的注册，该注册信息同样保存在智能合约中和注册服务器中。

4 结论

基于轻量级区块链节点的物联网服务架构，具备区块链数据的不可篡改性、可追溯性以及分布式特点的数据传输可信的特征，其轻量级节点放映机的引入提供了边缘设备数据到区块链的快速通道，不仅保证了电影放映数据传输安全和可信，还为进一步增强区块链账本及其共识的应用便利性提供了新的途径。

参考文献

[1] Eris Industries. Eris Industries Documentation—Blockchains[EB/OL]. [2016-03-15]. https://docs.erisindustries.com/explainers/ blockchains/

[2] Buterin V. Slasher Ghost, and Other Developments in Proof of Stake [EB/OL]. [2014-10-03]. https://blog.ethereum.org/2014/10/03/slasherghost-developments-proof-stake/

[3] Drdobbs. The Byzantine General's problem[J]. Acm Transactions on Programming Languages & Systems, 1982, 4(3):382-401.

[4] Walport M. Distributed ledger technology: beyond block chain [EB/OL]. [2016-05-01]. https://www.

doi:10.3772/j.issn.2095-915x.2019.04.002

gov.uk/government/publications/ distributed-ledger-technology-blackett-review

[5] 张正，杨睿哲，金凯，等．面向工业互联网场景的新型分布式账本技术 [J]. 情报工程，2018, 4(3):21-28.

[6] Zhou L J, Wang L C, Sun Y R, et al. BeeKeeper: A Blockchain-based IoT System with Secure Storage and Homomorphic Computation[J]. IEEE Access, 2018: 43472-43488.

[7] 王子娇．物联网与区块链相结合，新技术下供应链金融模式探讨 [J]. 金融视线，2019: 74-77.

[8] Huh S Y, Cho C G, Kim S H. Managing IoT Devices using BlockChain Platform[C]. ICACT2017 February 19~22. 2017:464-467.

[9] Nakamoto S. Bitcoin:Peer-to-Peer Electronic Cash System[EB/OL]. [2008-11-01]. https://bitcoin.org/en/bitcoin-paper 2008.

[10] Device Democracy: Saving the Future of the Internet of Things, IBM, New York, NY, USA, 2015.E. C. Ferrer, "The blockchain: a new framework for robotic swarmsystems," arXiv preprint arXiv:1608.00695, 2016.

[11] Microsoft. Understanding Public Key Cryptography [EB/OL]. [2014-07-29]. https://technet.microsoft.com/en-us/library/aa998077(v=exchg.65).aspx.

[12] Johnson D, Menezes A, Vanstone S. The elliptic curve digital signature algorithm (ECDSA)[J]. International Journal of Information Security, 2001, 1(1): 36-63.

[13] Szabo N. "Smart contracts." Unpublished manuscript, 1994.

[14] 李赫．区块链开发（三）编写调试第一个以太坊智能合约 [EB/OL]. [2016-09-10]. http://blog.csdn.net/sportshark/article/details/52497176,2016-09-10.

[15] 张鑫，杨晓元，朱率率，等．物联网环境下移动节点可信接入认证协议 [J]. 计算机应用，2016(11):3108-3112.

[16] Rahulamathavan Y, Phan R C W, Misra S, et al. Privacy-preserving Blockchain based IoT Ecosystem using Attribute-based Encryption.2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS). 2017.

[17] Krishnan M A, Shankar C G, Raj S A, et al. Peer to Peer File Sharing by Blockchain Using IOT[EB/OL]. [2017-11-12]. http://ijsrset.com/paper/2349.pdf.

[18] Sasson E B, Chiesa A, Garman C, et al. Zerocash: Decentralized Anonymous Payments from Bitcoin[C]. 2014 IEEE Symposium on Security and Privacy (SP). IEEE, 2014: 459-474.

[19] Wu L, Du X, Wang W, et al. An Out-of-band Authentication Scheme for Internet of Things Using Blockchain Technology[C]. International Conference on Computing, Networking and Communications 2018. 2018.

[20] Sharma P K, Chen M Y, Park J H. A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT[J]. IEEE Access, 2018(6):115-124.

[21] Announcing the Secure Hash Standard [EB/OL]. [2002-08-01]. http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf.

[22] Block Hashing Algorithm—Litecoin WiKi, accessed on[EB/OL]. [2016-03-15]. https://litecoin.info/Block_hashing_algorithm.

[23] Kelly J, Williams A. Forty Big Banks Test Blockchain-Based Bond Trading System [EB/OL]. [2016-03-02]. http://www.nytimes.com/reuters/2016/03/02/business/02reuters-bankingblockchain-bonds.html.

[24] Kar I. Estonian Citizens Will Soon Have the World's Most Hack-Proof Health-Care Records[EB/OL]. [2019-03-22]. Available: http://qz.com/628889/this-eastern-european-country-is-moving-its-health-recordsto-the-blockchain/.

[25] Suberg W. Factom's Latest Partnership Takes on US Healthcare[EB/OL]. [2018-11-03]. http://cointelegraph.com/news/factoms-latestpartnership-takes-on-us-healthcare