区块链技术的研究现状分析

王莹莹，王咏梅，郑永爱
（苏州高博软件技术职业学院，苏州 215163）

摘要：区块链技术以其去中心化、不可篡改、交易透明、可追溯等优点解决了多方间的信任问题，近几年得到了国内外科研团队及企业的高度重视与研究。本文介绍了区块链技术的典型特点并对区块链的研究现状进行了分析与总结。

关键词：区块链；去中心化；研究现状
doi：10.3969/J.ISSN.1672-7274.2018.12.067
中图分类号：TP3　　**文献标示码：**A　　**文章编码：**1672-7274（2018）12-0089-02

1 引言

区块链（Blockchain）技术是互联网底层多种技术的结合体，是通过多种技术的整合创造出的一种按时间序列和区块来实现数据记录、存储和表达的模式，这种模式的出现有望解决人与人之间的信任危机，让互联网的进化方向从效率转向公平[1]。

区块链能够解决数据的安全与隐私问题，能够对数据进行追溯，解决人类之间的信任危机，它是一个让交易变的透明化、公平化的平台，其必将引起一场新的技术革命和产业革命。

2 技术特点

区块链因其去中心化、公开透明、不可篡改、可追溯等特性，在一定程度上保证了数据的安全性，降低了交易的成本[2]。

（1）分布式存储，去中心化。网络中的任何计算机都可以加入到区块链网络中，通过竞争计算来维护整个网络。网络中没有任何中心化的设备或机构，节点间的交易通过数字签名来进行验证，不需要第三方的介入，节约交易成本，保证交易安全。（2）交易透明，身份匿名。区块链中的每一笔交易数据都是公开的，区块链网络中的每个节点都可以获取完整的交易数据，但是其身份可以选择匿名的，在交易过程中，参与交易的双发可以使用匿名。（3）智能合约，不可抵赖。区块链的智能合约，双方一经签署是自动触发、自动执行的，具有不可抵赖性，不需要担心交易过程中的反悔与欺诈。（4）不可篡改，可追溯。区块链上的数据是只能增加、不可删除的，要修改区块链上的数据需要网络中至少51%节点同时对数据库进行修改，这几乎是一个不可能完成的任务，因此区块链上的数据具有不可篡改性。另外，每一个区块的块头都包含了上一个区块的信息，因此所有交易数据都是可以追溯的。（5）交易成本低。区块链是由集体进行维护的，降低了数据维护的成本。基于区块链的交易，不需要建立信任，不需要第三方的介入，降低了建立信任的成本。区块链的智能合约自动执行，降低维护及履行合约的成本。

3 研究现状分析

3.1 区块链经典应用

以比特币为代表的第一代区块链系统，主要解决货币产生以及交易的去中心化问题。以以太坊为代表的第二代区块链系统，其将智能合约技术引入到区块链中。以Hyperledger为代表的第三代区块链系统，致力于解决区块链平台的可扩展性。

2008年全球金融危机爆发后，一个名为“中本聪”的学者设计出了一种名为比特币的网络虚拟货币。比特币是基于密码编码，通过复杂算法所产生的，其通过电子签名来实现流通，通过分布式记账的方式来保证交易的安全与可靠。比特币九年的稳定运行，充分验证了其底层区块链技术的可行性与安全性[3]。

受比特币的启发，2013年底，程序员Vitalik Buterin提出了以太坊公共区块链平台。以太坊提供了一套图灵完备的脚本语言EVM来编写去中心化的应用程序，并首次将智能合约引入到区块链中，目前已有多个成熟的基于以太坊所创建的项目或应用场景[4]。

Hyperledger[5]是2015年由linux基金发起的一个区块链项目，该项目的目的是打造一个公开、透明、去中心化的超级账本，建立区块链技术的开源规范与标准，使更多的应用轻松地建立的区块链技术之上。目前，全球有200多家的企业与机构已经加入到Hyperledger项目。Hyperledger目前已有多个相对比较成熟的项目，例如Burrow、Fabric、Iroha、Sawtooth、Indy等。其中，Burrow提供了一个模块化的区块链客户端，可以看做是一个支持许可的智能合约机；Faric是专门针对企业级的区块链应用而设计的，其采用模块化的架构作为开发区块链程序的基础，支持身份识别与权限控制，支持多种编程语言，支持共识算法及成员服务的即插即用；Sawtooth是一个创建、部署和运行分布式账本的模块化平台；Indy是为去中心化的身份而建立的一种分布式账本。

3.2 BAT布局区块链

由于区块链能够减少交易成本，提高经济效率，助力经济发展，越来越多的企业将区块链作为转型方向，截至2018年3月底，我国以区块链业务为主营业务的区块链公司数量已经达到了456家。截止到6月份以区块链概念上市的公司就已经达到了67家，区块链产业已经初步形成规模。国内众多互联网公司积极布局区块链，百度、阿里巴巴、腾讯、京东、网易、苏宁等都已经展开了对区块链的研究，并取得了初步的成效。腾讯区块链主要提供共享账本与数字资产服务，于2017年6月发布企业级区块链数据库——TrustSQL，次年5月份发布首款基于该平台的区块链游戏。TrustSQL有两个优点：一是支持SQL接口访问，用户可以沿用以前的开发习惯；二是独创内置智能合约，执行起来更加的安全、高效。百度2017年7月推出了商业级区块链开放平台BaaS；2018年3月发布图腾项目解决版权保护问题；2018年6月份发布新一代区块链网络操作系统—超级链。阿里巴巴2016年7月将区块链技术引入到支付宝爱心捐助平台，实现捐款信息可溯源；之后又将区块链技术引入到商品溯源中，实现对物品的跟踪，防止造假。

3.3 研究热点

在学术界，国内外众多学者也纷纷展开了对区块链的研究。Boyd[6]提出引入区块链来解决服务器的公平使用问题；Herber[7]提出引入区块链来解决版权保护问题；Zyskind[5]提出引入区块链技术来保护人隐私数据；Azaria[8]等人提出将区块链技术用在医疗数据访问和权限管理中。另外众多学者针对区块链的安全问题、交易效率、共识算法、加密算法、资源问题、博弈问题、容量扩展问题等方面都做了深入研究与探索。

4 结束语

区块链技术能够较好的解决数据的安全与隐私问题，因此迅速得到了国内外企业及机构的重视与研究。各企业纷纷布局区块链，旨在使用区块链技术来解决数据安全问题。本文主要从区块链的基本特点，区块链发展现状及研究热点等几个方面对区块链进行了研究与探索。

参考文献

[1] 沈鑫，裴庆祺，刘雪峰.区块链技术综述[J].网络与信息安全学报，2016，2(11).
[2] King S，Nadal S.PPCoin：Peer-to-Peer Crypto-Currency with Proof-of-Stake[J].2012.
[3] 邵奇峰，金澈清.区块链技术：架构及进展.计算机学报，2017（转下页）

作者简介：王莹莹，讲师，主要研究领域为无线传感器网络，区块链技术。

面向物联网的轻量级语义模型设计

张普钊[1]，胡燕飞[2]
（1. 中国移动通信集团重庆有限公司，重庆 401147；2. 中国电信股份有限公司重庆分公司，重庆 401121）

摘要：不同物联网平台之间的异构性，使得物联网系统的跨平台互操作面临严峻挑战。对传感器进行轻量级语义描述，可有效提高物联网异构平台之间的互操作性。本文提出了一个适用于物联网的轻量级语义模型，可适用于实时的传感器资源发现，并为提高物联网感知资源搜索的效率奠定了理论基础。

关键词：物联网；语义模型；轻量级
doi：10.3969/J.ISSN.1672-7274.2018.12.068
中图分类号：TN92，TP3　　**文献标示码：**A　　**文章编码：**1672-7274（2018）12-0090-01

1 引言

随着机器对机器通信和物联网应用场景的不断深入，不同物联网平台之间的互操作性已成为创建大型物联网框架的关键问题。物联网测试平台提供商最近开始将语义添加到物联网的框架中，通过创建具有明确语义的传感器 Web，使得机器对机器通信，人员和设备之间的交互更便捷。语义技术通过共享通用词汇表提供了一种适用于互操作的方法，并且还实现了数据的推理能力。物联网模型应该针对物联网环境的约束进行动态设计，尤其是要认识到将语义处理集成到受限设备的新趋势。

对传感器进行轻量级描述以有效管理传感器数据的注释和发现至关重要。本文基于语义传感器网络，提出一个轻量级的语义模型 -IoT-LSM，致力于实现实时传感器数据松散耦合发现，并寻求能够为大多数用户查询提供最佳答案的方法，以提高物联网感知资源搜索的效率。

2 语义模型设计

本文中轻量级语义模型 -IoT-LSM 的设计遵循以下原则：

（1）便于大规模推广应用。
（2）考虑语义模型使用者的需求。
（3）提供更新和更改语义注释的方法。
（4）创建用于验证和互操作性测试的工具。
（5）创建分类法和词汇表。
（6）现有模型的高重用性。
（7）将数据和描述链接到其他现有资源。
（8）创建有效的方法、工具和 API 来处理语义。

尽管大多数语义模型倾向于详细描述概念并表示物联网系统中的各种链接，但 IoT-LSM 仅代表物联网应用程序中数据分析的最常用概念，例如传感数据，位置和类型。这为创建可扩展的系统铺平了道路，并降低了大型物联网应用中查询处理的内存和计算成本。

（1）本体的简单性：本文所设计的 IoT-LSM 参见图2，其目的是在数据分析环境中搜索物联网概念时，只定义最常用的术语。根据数据分析应用程序使用的其他物联网本体的经验，研究物联网本体的最常见用途。

（2）互操作性：语义模型的另一个重要方面是互操作性。在 IoT-LSM 的设计中，遵循链接数据的基本要求。IoT-LSM 的本体与其他本体链接在一起，使用统一的词汇表来表示不同来源的数据，以提高异构平台之间的互操作性。

IoT-LSM 并非物联网的完整本体集，其目标是创建一个核心轻量级本体，保障物联网系统相对较快的注释和处理时间。IoT-LSM 可以成为语义模型的核心部分，根据应用程序的不同，可以添加不同的语义模块来为额外的应用程序定义概念和关系。从这个意义上说，已经将 IoT-LSM 与流注释本体相关联，以允许聚合数据流的注释。

最后，IoT-LSM 使用动态语义，以用来推断传感器数据语义的缺失值。通过遵循 IoT-LSM 的设计原则，动态语义减少了三元组存储的大小，并为查询提供了快速的响应时间。与其他解决方案（例如使用 RESTful 服务器推断传感器数据语义的缺失值）不同，IoT-LSM 将所有关于流数据的信息一起存储在三元组中。

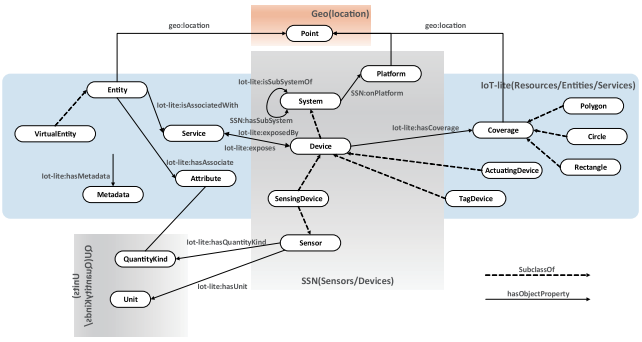

图1 IoT-LSM语义模型

3 结束语

对物联网中的感知资源进行轻量级描述，可有效提高异构物联网平台之间的互操作性。本文设计了一个适用于物联网的轻量级语义模型，提出了语义模型设计所要遵循的设计原则，给出了所提语义模型的设计框架。本文所作研究为后续物联网感知资源的高效搜索奠定了理论基础。

参考文献

[1] 于海宁，张宏莉，方滨兴等 . 物联网中物理实体搜索服务的研究 [J]. 电信科学，2012，28（10）：111-119.
[2] 袁凌云，王兴超 . 语义技术在物联网中的应用研究综述 [J]. 计算机科学，2014，41（S1）：239-246.
[3] 施昭，刘阳，曾鹏等 . 面向物联网的传感数据属性语义化标注方法 [J]. 中国科学：信息科学，2015，45（6）：739-751.

（接上页）Online.
[4] Buterin V.A next-generation smart contract and decentralized application platform.White Paper，2014.
[5] Cachin C.Architecture of the hyperledger blockchain fabric//Proceedings of the Workshop on Distributed Cryptocurrencies and Consensus Ledgers（DCCL）. Chicago，USA，2016.
[6] Boyd C，Carr C.Fair Client Puzzles from the Bitcoin Blockchain[M]//Information Security and Privacy.Springer International Publishing，2016：161-177.
[7] Herbert J，Litchfield A.A Novel Method for Decentralised Peer-to-Peer Software License Validation Using Cryptocurrency Blockchain Technology[C]// Australasian Computer Science Conference.2015.
[8] Zyskind G，Nathan O，Alex.Decentralizing Privacy：Using Blockchain to Protect Personal Data[C]//IEEE Security and Privacy Workshops.IEEE Computer Society，2015：180-184.