



专题：物联网技术与应用

基于区块链的社会物联网可信服务管理框架

赵明慧¹, 张琬², 亓晋¹

(1. 南京邮电大学, 江苏 南京 210003;

2. 中国电信股份有限公司江苏分公司, 江苏 南京 210017)

摘要: 针对当前社会物联网可信服务管理中存在的中心化程度高、交易不透明和易受攻击等问题, 提出了一种基于区块链的社会物联网可信服务管理框架。该框架通过区块链的去中心化特性在服务请求者和服务提供者之间直接建立信任关系, 利用智能合约产生并管理新的交易, 实现交易过程透明化并减少管理维护成本。同时, 区块链的共识机制可用于交易验证并防范恶意攻击和篡改, 减少网络攻击和恶意节点的欺骗。最后, 分析了该框架在实际构建中面临的主要挑战。

关键词: 社会物联网; 可信服务管理; 区块链; 智能合约; 共识机制

中图分类号: TP315

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2017274

A framework of trusted services management based on blockchain in social internet of things

ZHAO Minghui¹, ZHANG Lu², QI Jin¹

1. Nanjing University of Posts and Telecommunications, Nanjing 210003, China

2. Jiangsu Branch of China Telecom Co., Ltd., Nanjing 210017, China

Abstract: To cope with current problems of trusted services management in social internet of things (SIoT), such as high degree of centralization, non-transparent transactions, vulnerability and so on, a framework of trusted services management based on blockchain in SIoT was proposed. This framework established the trusted relationship between service requesters and service providers directly by using decentralization of blockchain, then it produced and managed new transactions through smart contracts to realize transparency and reduce the cost of management. At the same time, the consensus mechanism of blockchain could be used for verifying transactions and preventing malicious attacks in order to reduce network attacks and malicious node spoofing. Finally, the main challenges which the framework would face in actual constructions were analyzed.

Key words: social internet of things, trusted services management, blockchain, smart contract, consensus mechanism

收稿日期: 2017-08-20; 修回日期: 2017-09-25

基金项目: 江苏省自然科学基金资助项目 (No.BK20160910); 江苏省教育厅自然科学研究面上项目 (No.16KJB520034, No.17KJB520026)

Foundation Items: The Natural Science Foundation of Jiangsu Province of China (No.BK20160910), Natural Science Fund for Colleges and Universities in Jiangsu Province (No.16KJB520034, No.17KJB520026)



1 引言

社会物联网^[1] (social internet of things, SIoT) 是将社会网络的概念融入物联网, 使用现有的社会网络模型解决物联网的相关问题, 以更高效的方式支持物联网中新的应用和网络服务。SIoT 中每个设备都扮演着服务提供者或请求者的角色, 并建立自主的社会关系, 从而进行服务交互, 但在 SIoT 中存在着行为不端的设备所有者, 导致其设备会执行恶意攻击从而提供不可信服务。随着服务参与者数量的不断增加, SIoT 对可信服务的需求更加强烈, 因此, 在 SIoT 中提供可信服务管理是十分必要的。

目前, 国内外学者对 SIoT 的可信服务管理做了许多研究工作, 并取得了丰富的研究成果, 大多集中于使用中心化机构收集并管理所有信息。这种解决方案具有高效、便捷以及易控制等特性, 但其建设、管理、维护成本较高, 难以支持 SIoT 中海量设备的存储、传输和分析, 同时这种交易方式不透明且易受攻击和欺骗。针对以上问题, 若采用去中心化的方式进行可信服务管理, 并披露给参与者一些交易信息, 将大大减少管理维护成本并实现交易透明。目前, 区块链以其去中心化、透明化、不可篡改等特性吸引了各个行业的兴趣, 如医疗保健^[2,3]、物联网^[4]、数字资产交易^[5]以及能源互联网^[6,7]等领域, 近年来已成为研究热点。

针对 SIoT 的特征, 对区块链进行二次开发与应用, 是解决 SIoT 中可信服务管理问题的有效途径。因此, 本文利用区块链在 SIoT 中提出一种可信服务管理框架, 使设备之间直接建立可信、自主、透明的交易, 并有效地防范恶意攻击。首先, 该框架利用区块链充当可信的第三方, 使设备在进行服务交易前直接建立信任关系, 将极大地提高效率并降低成本; 其次, 在交易时使用智能合约, 完成供需双方的自动匹配, 实现几乎不需要

人参与就可以自主完成并记录交易信息, 且过程透明化; 最后, 恶意节点无法通过共识机制将数据写入区块链, 且保存在区块链中的数据也无法被篡改, 保证了内容的可信性, 解决了管理过程中易受攻击的问题。

2 社会物联网中的可信服务管理

与其他网络如 P2P 网络、传感器网络相比, SIoT 是具有异构互联、智能感知以及多领域应用特征的更加复杂的新型网络, 通常伴随着大量的服务且管理难度较大。目前, 大多数研究主要利用中心化的管理控制平台完成一系列的服务管理, 参考文献[8]提出了一个分层物联网架构下的量化信任管理模型, 计算智能物品追踪场景中合作节点和网络的可信性, 从而选择合适的节点执行任务。参考文献[9]提出了基于云计算的物联网部署应用平台 Lysis, 在 SIoT 中根据设备所有者使设备自主地建立社会关系, 提高了网络的可扩展性和信息发现的效率。参考文献[10]指出第三方代理是物联网中建立信任的一个至关重要的因素, 在构建信任关系时, 代理作为一个驱动程序嵌入数字系统。以上研究主要集中于对 SIoT 中的节点进行可信评估, 使节点间建立可信关系从而进行可信交互, 然而这些评估大多来自第三方机构, 过度依赖信任背书会造成权力集中且大大增加管理维护成本。同时, SIoT 体系庞大, 利用中心化管理平台进行的服务交易具有不透明性, 社会认同度和可信度不高。

在 SIoT 中, 数据集中在管理平台上很容易受到攻击和滥用, 安全风险迅速增加, 许多研究主要使用访问控制和防范措施应对恶意攻击。参考文献[11]在资源受限的设备上利用基于 CoAP 框架对服务进行级别访问控制。参考文献[12]在物联网中提出一种自适应推理发现服务 (adaptive inference discovery service, AID-S), 将其集成到个人数据管理器中, 防止个人信息泄露。参考文献[13]

讨论了一些证明操作策略、风险管理方法和识别方法来减轻安全风险和隐私威胁。然而,由于 SIoT 的开放性,传统的访问控制策略和防范措施将不再适用于解决分布式系统的安全问题。

综上所述,国内外对于社会物联网可信服务管理的研究主要存在中心化程度高、交易不透明和易受攻击等问题。针对这些问题,本文首次将区块链技术应用于社会物联网的可信服务管理,提出了一种基于区块链的 SIoT 可信服务管理框架,实现去中心化、透明、安全的可信服务管理模式。

3 基于区块链的 SIoT 可信服务管理框架

本文提出的基于区块链的社会物联网可信服务管理框架如图 1 所示,在无需信任单个节点的同时创建整个网络的信任共识,让物与物之间不仅相连起来,而且能自发进行一些活动。在该框架中,服务请求者和服务提供者通过区块链建立信任关系,两者之间利用智能合约产生并管理新的交易,并将交易信息对全网进行广播,接收到信息的节点通过共识机制对交易进行验证并防范恶意攻击,验证通过后的交易将写入区块链中。

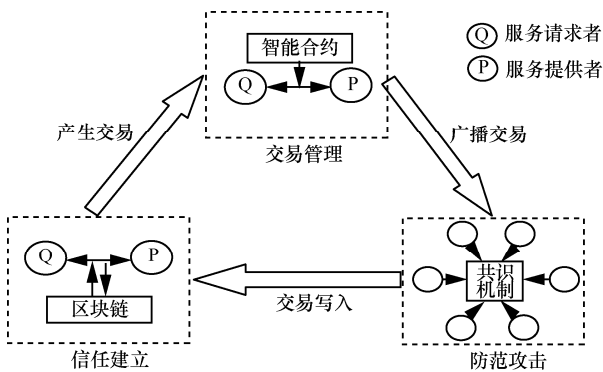


图1 基于区块链的社会物联网可信服务管理框架

3.1 信任建立

在社会物联网中,对象之间建立的信任关系是一种依赖关系,且信任难以在短时间内建立,因此,本文考虑对象间无需建立信任关系是否可以直接进行交互行为并提供服务。在不需要信任

任何实体的情况下,区块链技术为服务交互提供了一个值得信赖的环境。相比中心化模式中的服务交互过程,服务请求者和服务提供者可以直接相互信任而不需要通过可信的第三方来达成一致进行交互,区块链可以取代这个可信的第三方^[14],负责对象之间的信任问题,具体去中心化的信任建立过程如图2所示。

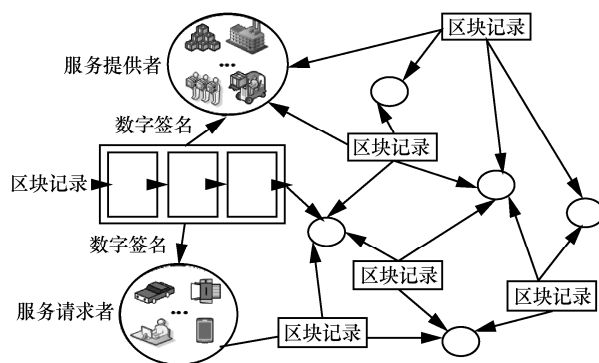


图2 去中心化的信任建立过程

区块链通过算法建立一个公开透明的规则,重新定义了网络中信用的生成方式,以此来创建一个信任网络。在该网络中,所有的规则事先都以算法的形式表述出来,服务参与者无需了解其他节点的相关信息,也能确保点对点之间的信任与交易的安全,这就摒弃了传统的中心化的第三方机构的信任背书,而只需要信任算法就可以建立互信,也省去了统一的账簿更新和验证环节,同时保障了对服务交易的活动进行记录、传输和存储。区块链技术消除了第三方机构,并提供了一种可行的替代方案,从而降低运营成本和提高共享服务的效率。因此,在社会物联网中使用区块链可以提供一种不需要建立信任关系来进行可信服务交互的方法。

3.2 交易管理

在给定的区块链中,根据设定的一系列规则,正当的交易定义了如何改变状态,从该状态中可以获得什么意义。因此,交易被视为区块链中业务逻辑的应用程序,这样复杂的应用程序通常被称为智能合约。智能合约通过赋予资产一些代码

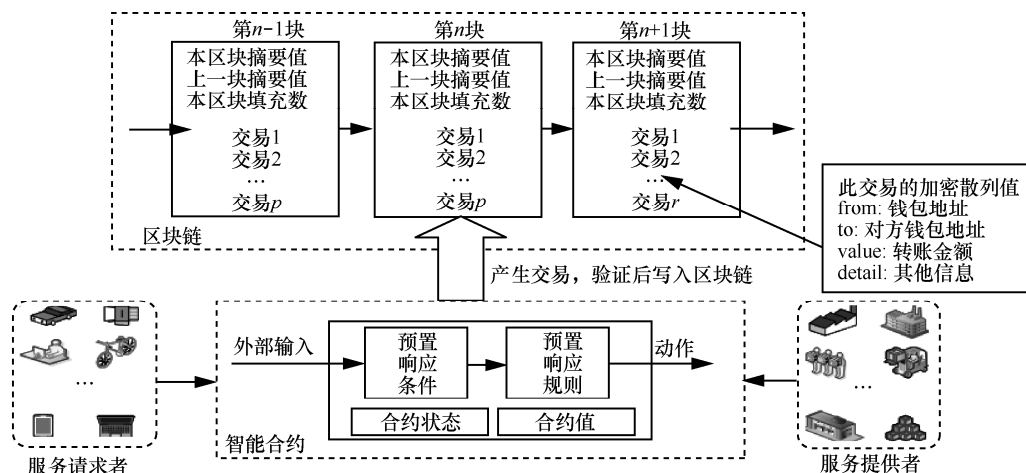


图3 融合区块链和智能合约的SIoT中的交易管理

并在区块链上运行，成为全网共享资源和共识算法，再通过外部数据触发合约执行，决定网络中智能资产分配或转移。在以太坊区块链中，智能合约符合图灵完备的虚拟机语言，为创建复杂的分布式应用程序提供了可能性^[15,16]。

智能合约以程序代码的形式预置在智能设备中，并完成对区块链数据的操作，在社会物联网中不同类型的设备内置实现不同操作的智能合约，实现设备之间点对点的自动化交易，将通过验证后的交易记录存入区块链。利用区块链和智能合约实现服务提供者和服务请求者间交易数据的验证、记账、存储、维护和传输等过程，融合区块链和智能合约的社会物联网中的交易管理，如图3所示。利用区块链技术在社会物联网中实现了信息高度透明、信息不可篡改、高度匿名性，从而实现几乎不需要人员参与就可以管理记录交易。

社会物联网连接了海量分布式设备、大规模用户及融合各种网络，本文基于智能合约使交易双方之间建立快速、可信、自动的交易模式，帮助交易双方高效地建立和完成交易。因此，基于智能合约和区块链，社会物联网将实现真正点对点、端到端、个人对个人的透明化服务交易，促进服务综合提供率的提高。

3.3 防范攻击

社会物联网的欺骗行为主要在服务交易过程中发生，区块链可以采用非对称密码学原理对数据进行加密，同时借助去中心化中各节点的工作量证明等共识算法来抵御外部攻击。共识机制是区块链中实现不同节点之间建立信任、获取权益的数学算法，能保证分布式系统中所有节点均可参与区块的验证过程，并通过共识算法选择特定的节点，将新数据添加到区块链中。因此，本文在社会物联网中利用区块链的共识机制验证并防范恶意攻击，如图4所示。

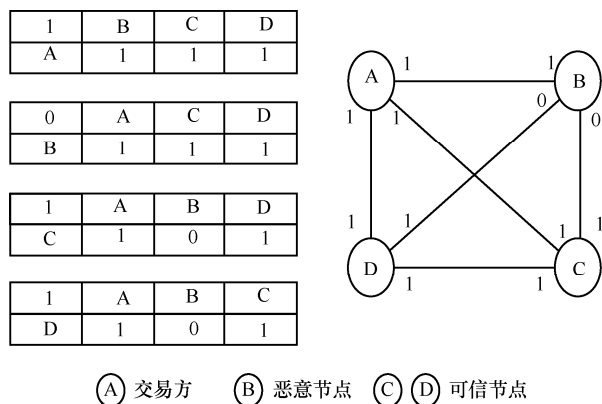


图4 共识机制防范恶意攻击的过程

A、B、C、D 是社会物联网中 4 个节点，其中，A 是交易方，B 是恶意节点，试图破坏该交易，C 和 D 是可信节点。A 将交易信息广播给其

他节点, 命令为“1”, B、C、D 都会收到 A 发来的命令“1”, 每个节点把收到的命令签名再发给其他节点。恶意节点 B 为了混淆视听, 转发给 C 和 D 的不是“1”, 而是“0”, 但为了不暴露自己, 发给 A 的仍然是“1”。可信节点 C 和 D 收到命令后签名并按照原样发出去。各节点收到的命令如图 4 中表格所示, C 和 D 收到的是“101”, 但是根据共识算法, 按“多数裁决”方式确定正确的命令, 即 C 和 D 同意命令“1”。因此, 尽管有恶意节点 B, 但 A 仍然可以和 C、D 一起确定命令, 将交易写入区块链中。

只有当全网大部分节点都认为这个记录正确时, 记录的真实性才能得到全网认可, 从而被允许写入区块链中, 恶意欺骗行为与数据无法通过共识机制写入区块链中, 且无法篡改区块链中的数据。因此, 本文在社会物联网中利用区块链的共识机制防范网络的攻击和恶意节点的欺骗, 保证了内容的可信性且具有较高的安全性。

4 主要挑战

区块链技术以其独特的优势和特点吸引了众多研究者进行开发与探索, 具有较高的价值和良好的应用前景, 提供了更安全、高效和低成本解决方案来完成社会物联网的可信服务管理过程。然而, 在实践运用中却存在一些挑战, 主要集中于落实到应用时的技术细节问题。

(1) 存储空间

区块链记录了从网络创建发生的每一笔交易与信息, 网络中的每个节点都有一份完整账本, 每一个想参与进来的节点都必须下载存储并实时更新一份从创块到至今的数据, 即第一次使用需要下载历史上所有交易记录才能正常工作, 每次交易为了验证节点确实拥有足够的钱而需要追溯历史每一笔交易来计算余额。随着时间的推进, 海量的数据存储需要更大的存储空间, 当交易数据超大的时候, 区块链就会出

现性能问题。虽然可以通过一些技术手段来缓解性能问题, 但问题还是明显存在的, 因此, 区块链数据的存储空间容量要求是一个制约其发展的关键问题。

(2) 智能合约

当前, 智能合约的标准主要是由分散的区块链应用联盟建立, 缺乏统一的技术开发标准, 在实际部署时将面临兼容性等方面的限制。由于智能合约出现时间不长, 缺失大量、可靠的实践应用进行验证测试, 从而缺少发现潜在风险漏洞的机会。尽管数字货币运行较为良好, 但若利用智能合约运行每天近万亿美元交易行为, 尚需更多的实践应用对其实用性和稳定性等进行测试, 以发现潜在的漏洞。在现实世界中对于有失公平的交易可以采用取消或暂缓等措施, 而智能合约中程序依旧会得到严格执行, 直至运行结束或出错。因此, 其灵活性不足也会导致参与者交易时存在风险, 且在风险管理方面的技术手段缺失。

(3) 共识机制

由于使用挖矿算法, 区块链的共识机制限制了交易速率, 不能像已有的云计算支付系统进行快速高效的运算。虽然共识机制解决了比特币发行、交易和验证的功能, 一定程度上保证了网络的安全性, 但其高度依赖网络节点贡献的算力。各节点的算力用于解决 SHA256 散列和随机数搜索, 即一个没有实际意义的纯数学问题, 且每次只有一个矿工获得记账权而其他矿工的计算能力都被浪费, 也消耗了大量的电力资源。为实现全网达成共识, 区块链要将消息的广播到所有节点中, 易引起广播风暴, 大量消耗底层网络的带宽, 导致网络性能下降甚至瘫痪。因此, 如何能有效利用分布式节点的网络算力解决大规模的实际问题, 是区块链技术需要解决的重要问题。

随着人们对区块链技术优势的认识越来越深



刻, 本文认为区块链技术不会因为上述问题而停滞不前。越来越多的人和资源正在不断地投入相关技术的研究中, 区块链技术的上述缺陷得到解决只是时间问题。

5 结束语

本文提出的基于区块链的社会物联网可信服务管理框架, 利用区块链、智能合约和共识机制解决了 SIoT 可信服务管理存在的中心化程度高、交易不透明和易受攻击等问题, 实现了去中心化、交易透明以及安全的可信服务管理, 有效降低了管理成本, 提高了系统整体运行效率, 减少了恶意攻击和欺骗, 使社会物联网成为一个真正的自组织、自调节的系统。

虽然区块链技术在各个领域有着不同程度的应用研究, 但总体上处于研究初期阶段, 仍面临着一些挑战而导致尚未被广泛应用。对此, 本文分析了该框架在实际构建应用过程中将要面临的主要挑战, 包括存储空间容量的限制、智能合约的灵活性不足以及共识机制的效率过低等, 为未来相关研究提供有益的启发与借鉴。

参考文献:

- [1] ATZORI L, IERA A, MORABITO G, et al. The social internet of things (SIoT)—when social networks meet the internet of things: concept, architecture and network characterization[J]. *Computer Networks*, 2012, 56(16): 3594-3608.
- [2] AZARIA A, EKBLAW A, VIEIRA T, et al. MedRec: using blockchain for medical data access and permission management[C]//2016 2nd International Conference on Open and Big Data (OBD), Aug 22-24, 2016, Vienna, Austria. New Jersey: IEEE Press, 2016: 25-30.
- [3] ZHANG J, XUE N, HUANG X. A secure system for pervasive social network-based healthcare[J]. *IEEE Access*, 2016(4): 9239-9250.
- [4] 李董, 魏进武. 区块链技术原理、应用领域及挑战[J]. *电信科学*, 2016, 32(12): 20-25.
LI D, WEI J W. Theory, application fields and challenge of the blockchain technology[J]. *Telecommunications Science*, 2016, 32(12): 20-25.
- [5] ZHANG Y, WEN J. An IoT electric business model based on the protocol of bitcoin[C]//2015 18th International Conference on Intelligence in Next Generation Networks, Feb 17-19, 2015, Paris, France. New Jersey: IEEE Press, 2015: 184-191.
- [6] 周国亮, 吕凛杰. 区块链技术在能源互联网中的应用[C]//2016 电力行业信息化年会, 2016 年 9 月 24 日, 天津, 中国. 北京: 人民邮电出版社, 2016.
ZHOU G L, LV L J. Application of blockchain technology in energy internet[C]//2016 Annual Conference on Informatization of Power Industry, February 24, 2016, Tianjin, China. Beijing: Posts&Telecom Press, 2016.
- [7] 颜拥, 赵俊华, 文福拴, 等. 能源系统中的区块链: 概念、应用与展望[J]. *电力建设*, 2017, 38(2): 12-20.
YAN Y, ZHAO J H, WEN F S, et al. Blockchain in energy systems: concept, application and prospect[J]. *Electric Power Construction*, 2017, 38(2): 12-20.
- [8] 汪京培. 物联网量化信任管理模型研究[J]. *网络安全技术与应用*, 2014(12): 89-90, 92.
WANG J P. Study of quantitative trust management model for the internet of things[J]. *Network Security Technology & Application*, 2014(12): 89-90, 92.
- [9] GIRAU R, MARTIS S, ATZORI L. Lysis: a platform for IoT distributed applications over socially connected objects[J]. *IEEE Internet of Things Journal*, 2017, 4(1): 40-51.
- [10] KOUNELIS I, BALDINI G, NEISSE R, et al. Building trust in the human? internet of things relationship[J]. *IEEE Technology and Society Magazine*, 2014, 33(4): 73-80.
- [11] TAMBOLI M B, DAMBAWADE D. Secure and efficient CoAP based authentication and access control for internet of things (IoT)[C]//2016 IEEE International Conference on Recent Trends in Electronics, Information Communication Technology (RTEICT), May 20-21, 2016, Bangalore, India. New Jersey: IEEE Press, 2016: 1245-1250.
- [12] TORRE I, ADORNI G, KOCEVA F, et al. Preventing disclosure of personal data in IoT networks[C]//2016 12th International Conference on Signal-Image Technology Internet-Based Systems (SITIS), Nov 28-Dec 1, 2016, Naples, Italy. New Jersey: IEEE Press, 2016: 389-396.
- [13] SUPRIYA S, PADAKI S. Data security and privacy challenges in adopting solutions for IoT[C]//2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Dec 15-18, 2016, Chengdu, China. New Jersey: IEEE Press, 2016: 410-415.
- [14] The Economist. The promise of the blockchain: the trust machine[EB/OL]. (2015-10-31)[2017-08-20]. <http://www.economist.com/news/leaders/21677198-technologybehind-bitcoin-could-transform-how-economy-works-trust-machine>.
- [15] White paper[EB/OL]. (2017-01-13)[2017-08-20]. <https://github.com/ethereum/wiki/wiki/White-Paper>.

- [16] 梅海涛, 刘洁. 区块链的产业现状、存在问题和政策建议[J]. 电信科学, 2016, 32(11): 134-138.

MEI H T, LIU J. Industry present situation, existing problems and strategy suggestion of blockchain[J]. Telecommunications Science, 2016, 32(11): 134-138.

[作者简介]



赵明慧（1993-），女，南京邮电大学硕士生，主要研究方向为社会物联网、可信计算。



张琨（1982-），男，中国电信股份有限公司江苏分公司操作维护中心客户工程师，主要从事省级大客户的技术支撑、新兴业务的支撑和维护工作。



元晋（1983-），男，博士，南京邮电大学物联网学院网络工程系主任、副教授，主要研究方向为新一代网络与数据通信理论及技术、人工智能算法在工业互联网及能源互联网中的应用。