DOI:10.13718/j.cnki.xsxb.2020.09.017

基于可扩展区块链的智慧城市框架①

陈 立[1], 朱丙丽[2]

1. 重庆幼儿师范高等专科学校 初等教育与应用技术系,重庆 万州 404047;
2. 重庆三峡学院 计算机科学与工程学院,重庆 万州 404100

摘要:为解决智慧城市中的大数据相关隐私和安全问题,提出一种基于多链和分片技术的异构多链可扩展区块链结构,使高效的跨链事务具有高可伸缩性和可扩展性.并设计了基于可扩展区块链的智慧城市框架,该框架由物理层、通信层、平台层和应用层组成,其中通信层与可扩展区块链集成,通过内容分发协议和智能合约等区块链技术保证传输数据的安全性和隐私性.平台层中区块链分布式分类帐本数据库,安全存储交易记录.通过可扩展区块链智慧城市框架,更好地支持大规模业务应用,实现智慧城市的建设和发展.

关 键 词:区块链;分片技术;可扩展区块链;智慧城市;安全性

中图分类号:TP391 **文献标志码**:A **文章编号**:1000-5471(2020)09-0112-06

近几十年来,由于人口增长、气候变化、经济发展和资源整合,世界上城市数量增长迅速,城市人口占总人口的 54%,到 2050 年将达到 68%[1].但城市在高速发展的同时,面临环境、交通和资源配置等问题,为了解决这些问题,现代技术被广泛运用,旨在降低成本、优化资源,创造更宜居的城市环境[2].物联网和无线通信的快速进步使得连接各种设备变得容易,并使它们可以从远程位置传输数据,但是这些系统更多地使用位置、个人和财务信息等开放数据,因此必须能够抵御安全攻击[3].

随着物联网(Internet of Things,IOT)、云计算和互联网络等技术的发展,智慧城市可以提供创新的信息通信技术(Information Communications Technology,ICT)来整合和管理各种事务,以便为居民提供更好的服务,同时确保有效地利用可用资源[4].解决方案可以方便居民与当地政府之间更直接的互动和协作.尽管智慧城市存在许多优点,但数字中断带来了许多与信息安全和隐私相关的挑战[5].目前城市中智能终端如租车客户端、自助服务机和信息亭等存在许多安全漏洞,网络犯罪分子利用这些设备可访问用户个人信息和财务信息,传统的安全机制不能全面解决智能化的智慧城市中的安全问题,因此必须开发新解决方案,为智慧城市智能设备和用户数据提供安全的隐私保护[6].

区块链是一个分布式数据库(或称为共享分类账)[7],分布式体现在数据分布式存储和记录上,区块链由包含事务的、带时间戳的区块组成,通过链的形式把区块组合起来,将有关系的、能在系统内验证的数据进行永久性存储和记录,通过密码学保证数据不可伪造和篡改,智能合约使得参与者对全网交易记录事件的顺序和当前状态建立共识[8].区块链提供了一个完美的解决方案,用于开发智慧城市的智能网络,其中所有交易都是透明的(公共分类账可供网络中的相关方使用),民主的(必须达成共识以接受交易)和安全

① 收稿日期:2019-11-04
基金项目:国家自然科学基金项目(61602072);重庆市基础研究与前沿探索项目(cstc2016jcyjA0063,cstc2018jcyjAX0502);重庆市教委科技项目(KJ1710248).
作者简介:陈 立(1975-),男,讲师,主要从事计算机软件与应用研究.

的(区块链很难篡改网络)[9]. 区块链的优势将对社会产生大的影响，包括金融、医疗保健、汽车、能源、公共部门和农业等. López 等[10]提出一种智慧移动数据的区块链框架，每个参与者将其加密数据共享到区块链网络，并且只要双方同意数据所有者发布的交易规则，就可以与其他参与者进行信息交易. Pham 等[11]将区块链应用于智慧医疗，通过传感器测量患者的健康状况，并将这些信息自动写入区块链，可以根据患者的健康状况有效地保存医疗设备信息. Mengelkamp 等[12]和 Pop 等[13]都研究了基于区块链的智慧电网框架. 目前，对于智慧城市的研究较少，唐新宇等[14]研究了区块链和智慧城市，从理论上研究了区块链在智慧城市应用的可行性和必要性. 但是以上研究存在两个问题，①给出的区块链研究没有应用在大规模业务的智慧城市上；②对于区块链和智慧城市的研究，只给出了可行性和必要性内容.

在前人研究了区块链与智慧城市的基础上，针对以上研究的问题，本文提出一种基于可扩展区块链技术的智慧城市安全框架，该框架允许在智能城市中实现通信，而不会影响隐私和安全. 可扩展区块链中，服务被分配给不同的子链，不仅保证了服务之间的隐私，还增加了整个系统的可扩展性，从而增强了区块链智慧城市框架的可扩展性，便于处理更大规模的智慧城市事务.

1　可扩展区块链

1.1　多链分片可扩展区块链

目前大多数区块链系统都是单链架构，其中每个节点都是单片全功能节点，因此每个节点必须执行许多重复的计算任务，这导致能量浪费. 此外，如果遇到流量峰值，其性能明显下降，因此单链架构无法满足不断增长的需求. 另外，考虑到越来越多不同类型的服务将连接到区块链系统，单链架构很难支持复杂的需求. 针对以上问题，本文提出一种多链异构区块链结果，将服务分配给不同的子链，在保证隐私的前提下，提高区块链的扩展性.

多链结构由单个主链和一组子链组成，利用价值交换层将子链和主链连接起来，并实现了子链之间的相互作用. 与创建具有全局交易分类帐的单个区块链的现有结构相比，该结构允许一组区块链在保持互操作性的同时与另一条区块链并行运行. 图 1 所示为多链体系结构的层次结构. 在体系结构的核心是主链，它管理着许多半独立的子链. 主链的设计原则是利用最小的数据量、最小的计算资源和最小的网络带宽来提供可信的主网. 主链将子链中的事务元数据持久化保持，为了提高性能，不会包含详细信息.

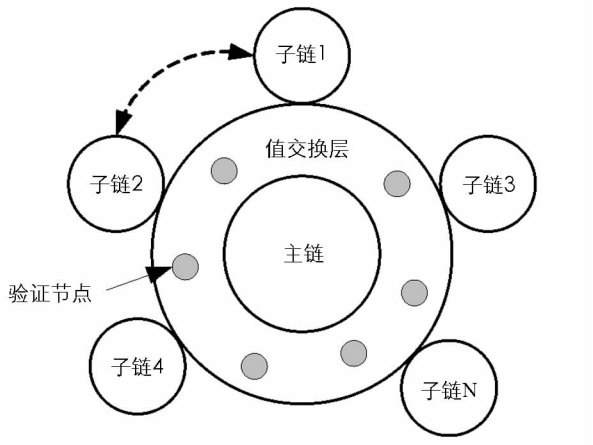

图 1　多链体系结构

值交换层旨在使资产在不同链之间流通，此层中有大量验证节点，每当发生跨越链的事务时，数据将在验证节点中进行验证. 为了确保数据的一致性，不同子链之间的数据以 Merkle 为证据，证明信息已被成功发送和接收，以便于检查.

子链独立于主链运行，当创建主链以后，子链被合并回主链. 在子链信息合并后，这些子链的最终结果被提交给主链，以便使主链保持最新. 当创建一个子链时，相关信息将从主链镜像到相应的子链，以便子链跟上主链的状态.

1.2　多层分片

与单一链结构不同，在多链结构中不同组织、机构和企业的业务根据不同的需求被定位到子链中，例如，一个业务实体在其独立的子链中运行自己的业务，不同的子链可以有不同的节点数量、块生成时间和策略. 如图 2 所示子链经营业务，这是保证不同组织之间数据安全和隐私的自然方式，也是一种分割计算

任务的方法. 对于这种结构，子链的共识算法不受限制，现有的共识算法有拜占庭容错技术(Byzantine Fault Tolerance，BFT)、实用拜占庭容错算法(Practical Byzantine Fault Tolerance，PBFT)、工作证明(Proof of Work，POW)，股权证明(Proof of Stake，POS)和委任权益证明(Delegated Proof of Stake，DPOS). 在一些可信环境中子链共识算法可以是其他算法，如分布式一致性RAFT协议等，可以大大提高子链的性能和可扩展性.

在复杂的业务场景中某个组织或企业的业务可能特别大，如果一家大型企业将其供应链迁移到区块链上，那么该子链的需求和交互将会相当大，单一的子链解决方案显然不能满足这一要求. 每个部门的业务可以通过多层次分片的方式划分为主链和多个子链，公司的每个部门都可以运行在子链中，当跨部门的数据需要交互时，就会在主链和多个子链中进行处理.

1.3 多链交易

在大多数情况下一个子链节点承载大量的服务，如交换交易、电子商务、供应链等等，从系统的角度来看，子链必须将关联交易与主链同步以增加其信用. 主链起见证作用，子链可以定期向主链提交自己块中的信息，该机制保证了子链和主链之间的一致性，子链证人工作流程如图3所示.

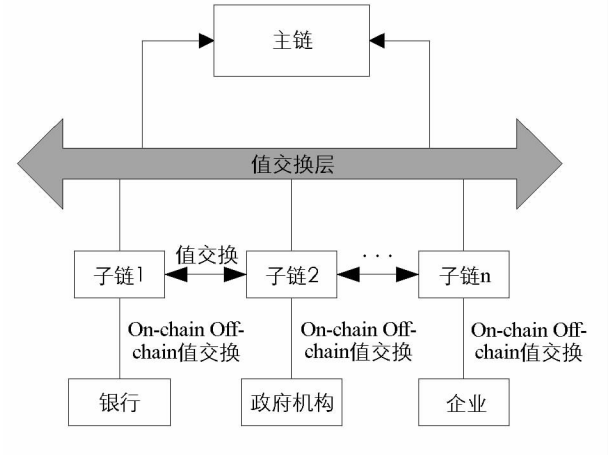

图2 不组织的业务分片

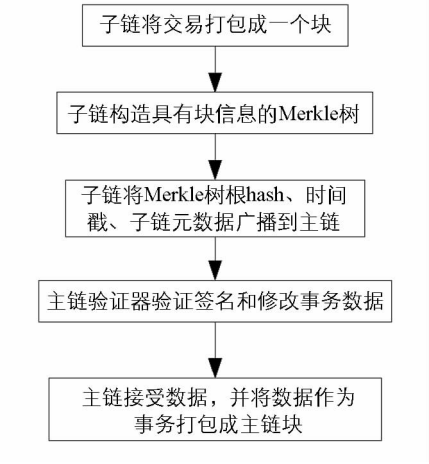

图3 子链证人工作流程

当资产需要从一个组织流向另一个组织，并且需要一个可信任的机制来确保事务是原始的和安全的，交叉链交易机制能够满足这些要求.

对于两个子链 SC_1 和 SC_2 不能直接进行支付交易，但两个子链可以通过主链MC进行支付，SC_1 向 SC_2 支付X令牌T. 子链 SC_1 生成具有其私钥的随机数N，SC_2 生成具有hash函数hash(N)的hash H，子链 SC_2 向子链 SC_1 发送hash H. 子链 SC_1 以X令牌T对主链MC进行 T_1 交易，MC要求满足两个条件的支付.

MC必须提供 N'，满足 $hash(N')=H$；

MC必须在 P_1 秒内提供 N'.

MC通过智能合同，与 SC_2 进行具有X令牌T的 T_2 交易. SC_2 必须提供 N''，满足 $hash(N'')=H$，SC_2 必须在 P_2 秒内提供 N''. SC_2 的原始编号为N，SC_2 在 P_1 秒内完成交易 T_2，并完全接收来自MC的X令牌T，MC使用 N' 从 SC_1 完成交易 T_1.

2 基于可扩展区块链的智慧城市框架

本文提出了一种基于可扩展区块链的智慧城市框架，以实现智慧城市的安全数据通信. 新型智慧城市解决方案由一个智慧城市各维度大数据中心，智慧政务、城管、民生和经济综合服务4个平台，多个智慧应用，以及可扩展多链区块链多维框架组成. 可扩展区块链的智慧城市多维结构如图4所示.

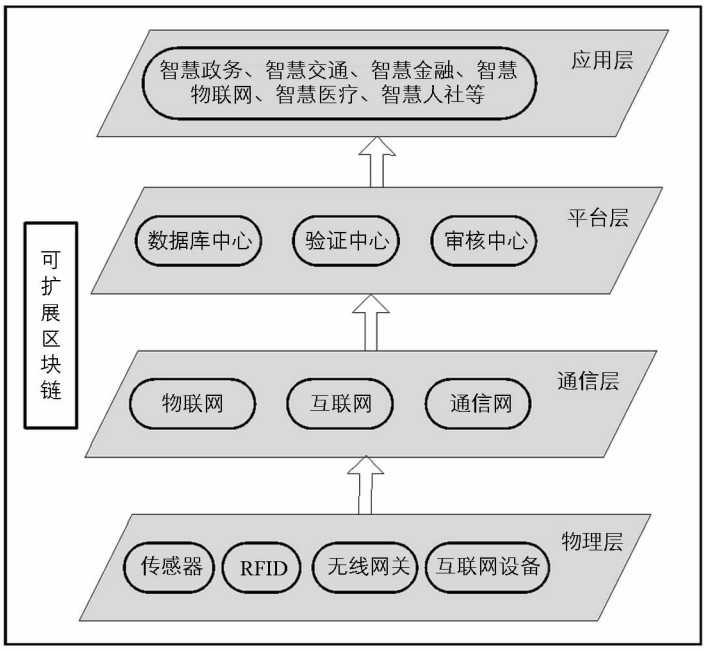

图 4　可扩展区块链的智慧城市多维结构

物理层：智慧城市设备配备有传感器和执行器，另外还有 RFID(Radio Frequency Identification)电子标签、硬件网关设备和互联网设备，用于收集数据并将数据转发到上层协议. 其中一些设备如恒温器 Nest 和 Acer Fitbit 由于加密和访问控制机制松懈，容易受到安全攻击. 此外，智能设备没有单一标准，因此可以共享和集成由它们生成的数据以提供交叉功能. 供应商需要商定一致同意的通信标准来解决智能设备中的这些问题.

2) 通信层：在这一层，智慧城市网络使用蓝牙、6LoWPAN、WiFi、以太网、3G 和 4G 等不同的通信机制在不同的系统之间进行信息交换. 区块链协议需要与该层集成，以提供传输数据的安全性和隐私性. 可以在网络中广播的网络上以 P2P 的方式，通过重叠网络传输协议将交易记录转换成块，将区块链中的分发协议比特流(BitTorrent)用于点对点通信，然后以太坊提供智能合约功能，通过部署智能合约，实现自我执行和自我验证. 然而，现有通信协议与区块链的集成是一项重大挑战，因为不同的应用程序要求不同，本文的多链区块链提供特定于应用程序的功能.

3) 平台层：在区块链中分布式分类帐是一种分散式数据库，可以一个接一个地存储记录，分类帐中的每条记录都包含时间戳和唯一的加密签名. 分类帐的完整交易历史记录可由任何合法用户验证和审核. 有两种不同类型的分布式分类帐：无许可的分布式分类帐和许可的分布式分类帐. 无许可分类帐的主要好处是可以抵抗审查制度，而且是透明的，但是公共分类帐必须维护复杂的共享记录，与私有分类帐相比，它需要更多时间才能达成共识. 此外，公共分类账也可能遭到匿名攻击. 因此，建议使用私有分类帐以确保实时应用程序的可扩展性和安全性.

4) 应用层：该层包含许多智能应用程序，涉及到方方面面的专项服务，如智慧政务、智慧交通、智慧金融、智慧物联网、智慧医疗、智慧人社和智能家居等，它们相互协作做出有效决策. 如智能电话应用程序可以向智能家居系统提供位置信息，以便在到达家中之前 5 min 打开空调. 但是，应该仔细集成应用程序，因为一个应用程序中的漏洞可能会让入侵者访问其他依赖进程.

在智慧城市分领域解决方案中，热点研究领域是智慧医疗，主要集中在医疗数据安全存储与共享、医疗流程改革和药品供应链的监管与药品鉴别方面. 对于医疗数据安全存储与共享，基于区块链的智慧医疗，通过无钥签名基础设施区块链技术与 Oracle 数据引擎，可以安全、实时查看病人病例. 对于医疗流程改革，利用区块链技术进行用户身份确认，对消费者与服务提供商进行识别，在自动识别交易参与方的基

础上，利用智能合约实现医疗保险的快速赔付. 对于药品供应链的监管与药品鉴别，所有参与药品冷链的参与者，通过智能物联设备所采集的数据串联起来，链接了药品生产者、经销商、承运商、医院和监管机构，利用区块链技术将数据上链，杜绝了人为篡改的可能，确保了数据的安全与可回溯；同时智能合约在采集数据出现异常时自动报警，避免出现更大损失.

在智慧城市分领域解决方案中，区块链物联网具有以下优势：①保护用户隐私，重塑信任机制. 区块链重塑物联网设备的连接方式，采用分布式网络结构，使得设备之间保持共识；去中心化验证方式，使得一个或者少量节点被攻破之后整个网络的体系依然是稳定的，避免了批量用户信息泄露的问题. ②降低运营成本，普及物联设备. 区块链技术传输数据的方式为点对点通信，分布式的计算可以处理数以亿计的交易，充分利用闲置计算力、存储容量和带宽，用于交易处理，大幅度降低存储成本.

区块链对智慧城市安全保护体现在多个方面，如共识机制和智能合约安全保障，就是在维护区块链数据时，每一个区块上的每一个修改都需要共识确认，从而保障数据安全；智能合约具有去人为干预性的特征，通过程序算法替代人仲裁和执行合同，排除了人为参与带来的风险. 另外，还有身份匿名安全保障，区块链具有匿名性，攻击者无法对账户主体信息进行匹配. 最后，区块链具有加密算法安全保障，区块链中多种加密算法在智慧城市框架中，可通过比特币加密和数字签名加密方法，保护智慧城市中的数据安全.

基于区块链的智慧城市建设，使民众参与度更高和选择性更多，使城市服务更加便捷，能够创造出更多效益. 城市管理模式转变为全民参与、政府监管，提高了工作效率、提升了服务水平，更降低了服务成本，让大数据更好地服务民众，进一步推动城市建设.

3 结　　语

本文提出一种区块链智慧城市框架，设计了可扩展分片多链的区块链架构，由并行子链和主链构成. 在架构中提出了可扩展的多级分片模型，多链体系结构具有子链事务见证功能，并且在可伸缩性和可扩展性方面实现了高效的交叉链事务. 将多链可扩展区块链技术与智慧城市中的设备集成创建一个通用平台，其中所有设备都能够在分布式环境中安全地通信，同时本文区块链智慧城市多维结构提高了智慧城市的可扩展性，能够高效率处理海量设备数据. 未来的工作旨在设计系统级模型，以研究智能城市中使用不同平台的互操作性.

参考文献：

[1] CARDULLO P, KITCHIN R. Being a 'Citizen' in the Smart City: Up and down the Scaffold of Smart Citizen Participation in Dublin, Ireland [J]. GeoJournal, 2019, 84(1): 1-13.

[2] COWLEY R, JOSS S, DAYOT Y. The Smart City and Its Publics: Insights from across Six UK Cities [J]. Urban Research & Practice, 2018, 11(1): 53-77.

[3] 杨　伟，何　杰，万亚东，等. 物联网通信协议的安全研究综述 [J]. 计算机科学，2018，45(12)：32-41.

[4] MEMOS V A, PSANNIS K E, ISHIBASHI Y, et al. An Efficient Algorithm for Media-based Surveillance System (EAMSuS) in IoT Smart City Framework [J]. Future Generation Computer Systems, 2018, 83: 619-628.

[5] SHOLLA S, MIR R N, CHISHTI M A. Docile Smart City Architecture: Moving Toward an Ethical Smart City [J]. International Journal of Computing and Digital Systems, 2018, 7(3): 167-174.

[6] 安　达，梁智昊，许守任. 基于大数据的智慧城市安全建设研究[J]. 中国电子科学研究院学报，2016，11(3)：229-232.

[7] 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.

[8] CONG L W, HE Z G. Blockchain Disruption and Smart Contracts [J]. The Review of Financial Studies, 2019, 32(5): 1754-1797.

[9] DINH T T A, LIU R, ZHANG M H, et al. Untangling Blockchain: a Data Processing View of Blockchain Systems [J].

IEEE Transaction on Knowledge and Data Engineering, 2018, 30(7): 1366-1385.

[10] LÓPEZ D, FAROOQ B. A Blockchain Framework for Smart Mobility [C]// 2018 IEEE International Smart Cities Conference (ISC2). Kansas City: IEEE, 2018.

[11] PHAM H L, TRAN T H, NAKASHIMA Y. A Secure Remote Healthcare System for Hospital Using Blockchain Smart Contract [C]//2018 IEEE Globecom Workshops (GC Wkshps). Abu Dhabi: IEEE, 2018.

[12] MENGELKAMP E, NOTHEISEN B, BEER C, et al. A Blockchain-based Smart Grid: Towards Sustainable Local Energy Markets [J]. Computer Science-Research and Development, 2018, 33(1): 207-214.

[13] POP C, CIOARA T, ANTAL M, et al. Blockchain Based Decentralized Management of Demand Response Programs in Smart Energy Grids [J]. Sensors, 2018, 18(1): 162.

[14] 唐新宇，张新政，赵月爱. 云计算中基于群体智能算法的大数据聚类挖掘 [J]. 重庆理工大学学报(自然科学版)，2019，33(4)：128-133，167.

Smart City Framework Based on Scalable Blockchain

CHEN　Li[1]，　ZHU Bing-li[2]

1. *Department of Primary Education and Applied Technology, Chongqing Preschool Teachers College, Wanzhou Chongqing 404047, China;*

2. *Computer Science and Engineering College, Chongqing Three Gorges University, Wanzhou Chongqing 404100, China*

Abstract: In order to solve the privacy and security problems related to big data in smart cities, an extensible blockchain intelligent city structure has been proposed. Firstly, a heterogeneous multi-chain extensible block chain structure based on multi-chain and fragmentation technology has been proposed, which makes efficient cross-chain transactions highly scalable and scalable. Secondly, the communication layer has been integrated with the scalable blockchain to ensure the security and privacy of the transmitted data through blockchain technologies such as content distribution protocols and smart contracts. And lastly, the blockchain distributed ledger database in the platform layer securely stores transaction records. Through the extensible blockchain smart city framework, better support large-scale business applications, to achieve the construction and development of smart cities.

Key words: blockchain; partition technology; extensible blockchain; smart city; security

责任编辑　夏　娟