基于区块链的智慧城市边缘设备可信管理方法研究

石鹏展[1], 戴 欢[1], 陈 洁[2], 陈儒玉[1]

[1] 苏州科技大学 苏州 中国 215000

[2] 华东师范大学 上海 中国 200241

摘要 由于物联网设备的资源受限, 当前智慧城市相关应用系统, 在抵御以物联网设备为目标的恶意攻击时存在局限性, 难以提供安全可靠的服务。本文设计了基于区块链的智慧城市边缘设备管理架构, 将区块链技术引入智慧城市建设研究中, 利用区块链分布式架构和去中心化的思想, 实现感知数据的可信收集和存储, 并基于该架构提出了一种新的基于信誉的PoW共识算法, 为物联网设备提供信任机制, 该算法极大的增加了由物联网设备端发起的恶意攻击的成本, 有效的预防了设备的恶意攻击行为, 实现了边缘设备行为的可信管理。基于所提方法实现的智慧城市应用案例验证了其可行性, 有效防范了来自节点的恶意攻击, 增强了系统的信息安全性。

关键词 智慧城市; 共识算法; 区块链; 边缘设备

中图法分类号 TP301 DOI 号 10.19363/J.cnki.cn10-1380/tn.2021.07.09

Blockchain-based Approach for Trustworthy Management of Edge Device in Smart City

SHI Pengzhan[1], DAI Huan[1], CHEN Jie[2], CHEN Ruyu[1]

[1] Suzhou University of Science and Technology, Suzhou 215000, China

[2] East China Normal University, Shanghai 200241, China

Abstract Due to the constrained resources of edge device, currently smart city applications with centralized model are vulnerable to malicious attacks from internal, which can hardly provide high-confidence services. This paper designs a blockchain-based smart city framework, which introduces the distributed architecture and decentralization of blockchain into smart city to realize the trustworthy collection and storage of sensor data. Based on the framework, a novel credit-based PoW consensus algorithm is also proposed to provide the trustworthy mechanism for edge device. By increasing the cost of malicious attack, the algorithm can prevent malicious attacks launched by edge devices and implement trustworthy management of the behavior of edge device. The case study of the proposed approaches in smart city scenario shows its feasibility and effectiveness, which can effectively prevent malicious attacks from edge device and enhance the information security of the system.

Key words smart city; consensus mechanism; blockchain; edge device

1 引言

现代信息技术的革新推动了城市向智能化的方向发展, 以物联网[1]、边缘计算[2]、低功耗广域网[3]等技术为支撑的智慧城市不断深入建设。物联网的广泛使用引起了城市云流量的激增, 边缘计算利用将当前集中化的计算模型转变为多层的分布式计算模型的方法, 将计算任务从云计算中心转移到更靠近边缘的位置, 如 Fog[4]和 Cloudlet[5], 极大的提高了在高并发量下其应用系统在响应、带宽和吞吐量等方面的服务质量[6-8]。然而, 由于物联网设备计算资源受限, 当前智慧城市应用系统在面对中心节点故障、内部的恶意攻击时存在安全隐患, 难以提供稳定可靠的服务。并且其数据库、服务器依赖于单一的服务商的维护, 在数据安全性方面也存在信息安全隐患, 如数据的篡改, 数据的可靠性无法得到保障。

区块链技术在电子货币[9]中的成功应用引起了广泛的关注, 其基于数学的方法可以在不可信的环

通讯作者: 戴欢, 博士, 副教授, Email: daihuanjob@163.com。

得到国家自然科学基金(No. 61702354, No. 61876121); 苏州科技大学科研项目(No. XKZ2017004); 江苏省物联网移动互联技术工程重点实验室开放课题(No. JSWLW2017004); 研究生科研创新计划项目(No. SKSJ18_012, No. SJCX19_0963)资助。

收稿日期: 2020-08-22; 修改日期: 2020-11-12; 定稿日期: 2021-06-24

境中构建可信的信息、价值传递通道, 具有去中心化、高可信度等特点, 被认为可以与物联网技术相结合, 解决智慧城市中的信息安全问题[10-12]。文献[13]提出了一种基于智能合约的物联网权限控制架构, 利用智能合约构建一对主客体权限管理实体, 由于物联网设备和边缘服务器在数量上存在较大差距, 该架构并不适用于管理智慧城市中数量巨大的边缘设备。文献[14]构建了一个基于 DAG (Directed Acyclic Graph)结构的区块链系统应用于工业物联网的设备管理, 设计了基于信誉的共识算法, 通过将节点信誉和计算资源相关联, 约束了节点的行为, 但该系统在数据存储方面存在局限性, 会造成大量的数据冗余。文献[15]提出了一种融合区块链与边缘计算的架构 EdgeChain, 利用智能合约构建电子货币系统, 以约束物联网节点的行为, 但其基于智能合约的管理方法会极大的影响系统的效率。综上所述, 区块链技术管理城市中海量的边缘设备, 其主要挑战可以概括为:

1) **适配性**: 边缘节点资源有限难以适配区块链系统中的计算和存储要求, 被排除在区块链系统之外;

2) **安全性**: 当前的共识算法, 例如 PoW[9]、PoS[16], 难以部署在边缘设备上, 并且缺乏约束和管理边缘设备行为的机制, 威胁着系统安全;

3) **高效性**: 区块链复杂的安全策略, 以及智能合约的高延迟, 会极大降低系统效率和吞吐量。

针对上述问题, 本文提出一种基于区块链的边缘设备可信管理方法, 利用区块链的高安全性机制和去中心化的思想, 实现智慧城市边缘设备的数据和行为的可信管理; 设计了基于区块链的智慧城市边缘设备管理架构, 利用区块链的安全机制, 实现了感知数据的可信收集和分布式存储; 提出了基于信誉的 PoW 共识算法, 为资源受限的边缘设备提供信任机制, 以增加恶意攻击的攻击成本, 实现了对从边缘设备端发起的内部恶意攻击的有效预防, 从而对边缘设备行为的可信管理。基于该方法实现的智慧城市应用案例验证了其可行性, 并可有效规范节点行为, 防范来自内部的恶意攻击, 增强系统的信息安全性。

2 基于区块链的智慧城市边缘设备管理架构

当中心节点故障, 或对物联网设备发起恶意攻击时, 传统基于集中式计算模型的智慧城市边缘设备管理架构存在局限性, 本文将许可链引入智慧城市边缘设备管理当中, 设计了基于区块链的智慧城市边缘设备管理架构, 包括基础设施、网络、区块链和应用层, 如图 1 所示。

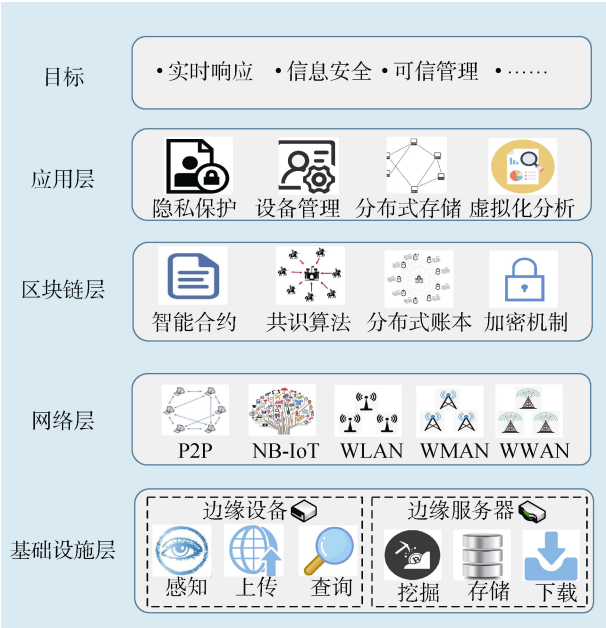

图 1 整体架构

Figure 1 Overall framework

基础设施层: 该层由多类型的边缘设备群和区域化的边缘服务器群组成, 分别担任不同的对等角色, 根据服务区域和服务类型完成预定的工作, 共同参与数据的维护。边缘设备实现对目标的状态监测, 通过向系统提交相关数据参与系统数据的维护。边缘服务器拥有较强的计算能力和大的存储空间, 通过打包和存储数据参与系统数据的维护。边缘设备会同时向服务区域内的若干边缘服务器提交感知数据, 这些数据将会广播在边缘服务器群中。因此, 边缘服务器只能完成对数据的打包和存储, 而无法对数据进行改动。在这种情况下, 边缘设备脱离了与服务器的从属关系, 直接从属于整个系统, 其数据和行为由系统规则约束。

网络层: 整个系统采用分布式的网络模型, 采用 P2P 的连接方式, 节点和服务器、节点和节点、服务器和服务器之间都是对等角色, 整个网络中不存在中心节点。因此, 单一的节点故障既不会影响整个系统的正常运行, 也不会影响系统中数据的安全。并且, 考虑到系统中通讯对象的种类多, 数量大, 网络层为系统中多类型的设备和应用场景提供了不同的通讯方式, 例如使用 NB-IoT 作为边缘设备的通讯方式, 使用 Internet 作为边缘服务器的通讯方式。

区块链层: 以基础设施和网络层为基础, 在边

缘设备和边缘服务器之间搭建许可链, 建立基于 P2P 的分布式网络模型, 实现区块链环境的搭建。该层由 4 个核心模块组成: 智能合约为系统提供去中心化的应用接口; 共识算法为系统节点提供信任机制; 分布式账本为系统数据提供安全的存储方式; 加密机制为系统建立可信的信息、价值传输通道。

应用层: 除了向外界提供应用服务, 例如, 数据的隐私保护、设备的行为管理、数据的分布式存储、虚拟化分析等, 应用层还可为开发者提供去中心化的应用平台, 吸引更多机构的参与, 为智慧城市的发展提供动力。并且, 通过将系统节点的行为和其服务收益相关联, 应用层可以进一步的激励节点的诚实行为, 增加恶意攻击的成本。

3 基于信誉的 PoW 共识算法

由于边缘设备的计算和存储空间受限, 边缘设备和边缘服务器之间存在功能方面的差异性, 当前流行的 PoW、PoS 等共识算法, 缺乏对边缘设备行为的有效约束能力, 并且难以部署在这些边缘设备上。针对上述问题, 本文提出一种新的基于信誉的 PoW 共识算法, 以适配资源受限的边缘设备, 为边缘设备提供信任机制, 增强智慧城市的信息安全性, 实现对边缘设备行为的管理。

根据上述的智慧城市边缘设备管理架构, 系统中的节点可以分为两大类: 边缘服务器和边缘设备。节点的行为记录, 在系统中统称为事务, 事务的格式如表 1 所示。这些事务在执行后都将被广播出去, 添加进各服务器的事务池中。之后, 边缘服务器将事务池中的事务打包成一个区块, 区块的挖掘需要寻找一个合适的 *nonce* 值, 如果将该区块中的相关参数, 例如该区块的哈希值、前一个区块的哈希值、时间戳和 *nonce* 值, 输入到哈希算法(SHA-256[17])当中, 输出的结果小于系统目标值, 则该块可以被系统接受, 最终被存储在分布式账本当中, 作为最新的区块。至此边缘服务器完成了一次打包工作, 并获得相应的工作奖励。网络中只有最快找到 *nonce* 值的区块, 才会被系统所接收, 这保证了区块的唯一性。每个区块都包含前一个区块的哈希值, 使得区块以链式的结构存储在系统之中。由于区块的挖掘需要花费大量算力, 使得区块链在生成后难以篡改, 除非恶意边缘服务器的算力达到系统总算力的 51%, 否则都无法篡改区块中的数据, 破坏系统各边缘服务器中数据的一致性, 威胁系统安全。

表 1 事务格式

Table 1 Format of Transaction

Transaction Header	
Type	事务的类型
From	发送方的地址
Order	该事务的序号
To	接收者的地址
Value	交易的货币数量(交易相关)
Timestamp	该事务的创建时间
Payload(提交数据相关)	
$data_1, data_2, \cdots, data_n$	
Contract Code(智能合约相关)	
$variable_1, variable_2, \cdots, variable_n$	

边缘设备会根据服务区域向附近的若干边缘服务器提交数据, 并且事务在广播的过程中存在时间消耗, 使得距离较近的边缘服务器会首先获取这些事务并着手打包, 相对于距离远的边缘服务器, 其成功打包的概率会增加。这使得拥有相对较低哈希计算能力的边缘服务器有很大机会成功打包自己服务区域内的事务, 获取相应的奖励。如果把一个服务区域内的所有边缘服务器的计算能力看作一个计算池, 当其计算能力溢出时, 随着新的边缘服务器的不断加入, 每个边缘服务器获取奖励的几率就会变小。这使得同一个服务区域内的边缘服务器会因为相互竞争工作奖励, 保持其数量在一个合理的范围内。

基于上述的区块验证方案, 边缘服务器 e 在 n 个边缘服务器中成功打包区块的概率 P_e 可以表示为

$$P_e = \frac{H_e}{\sum_{k=1}^{n} H_k} \cdot D_e \cdot \sigma \tag{1}$$

其中: H_e 和 H_k 分别表边缘服务器 e 和 k 的哈希计算能力, D_e 表示边缘服务器 e 所在区域同类型边缘服务器密度的对打包概率影响因子, σ 表示获取这笔事务所需时间消耗对打包概率的影响因子。

每个边缘设备 r 都有两个属性, 信誉 C_r 和种类 s, 信誉是该边缘设备的基本属性, 并且会根据该边缘设备过去的行为动态变化, 种类定义了其行为准则。当边缘设备提交的数据由边缘服务器打包成块并被系统所接受, 成为最新的区块后, 则该边缘设备完成一次数据提交工作, 并根据信誉获得奖励。边缘设备的正常行为如根据预定义的准则提交数据, 会增加其信誉, 而异常行为则会减少其信誉。系统中边缘设备的异常行为可以概括为以下几种:

1) 为获取更多的奖励, 边缘设备会不正当的增

加获得奖励的机会, 如减少上传数据的周期, 导致系统数据的大量冗余。

2) 边缘设备会出现怠工行为, 即在规定的时间内没有完成对应的工作, 降低系统的服务质量。

3) 恶意的边缘设备会想要破坏系统规则, 牺牲自己的利益阻止系统正常运行, 如以极短的频率上传数据, 阻塞系统网络, 导致系统相关服务停滞。

为了规范上述行为, 边缘设备 r 的信誉 C_r 可以定义为:

$$C_r = \xi_1 \cdot C_r^N + \xi_2 \cdot C_r^M \tag{2}$$

其中, C_r^N 表示正常行为得分, C_r^M 表示异常行为得分, ξ_1 和 ξ_2 为权重系数, 可以根据应用需求调整系统对这两种行为的敏感度。

C_r^N 用于评估边缘设备完成数据提交工作的质量, 与边缘设备提交数据的周期正相关。当周期处于 $(1+\alpha_s)\bar{t}_r$ 和 $\alpha_s \bar{t}_r$ 之间时(α_s 为正常行为的预设值, $\bar{t}_s$ 为 s 类型的边缘设备的预设数据提交周期), 并且数据的格式正确, 则此次数据提交行为被认定为正常行为。C_r^N 可以定义为:

$$C_r^N = \sum_{i=1}^{K_r^N} \frac{1}{\eta^{\left|\bar{t}_r - \Delta t\right|} \cdot (t - t_i)^{\zeta_1}} \quad (1+\alpha_s)\bar{t}_r > \Delta t > \alpha_s \bar{t}_r \tag{3}$$

其中, K_r^N 表示边缘设备 r 正常行为的总次数, t 表示当前时间, t_i 表示第 i 次行为发生的时间, Δt 表示第 i 次行为和第 $(i-1)$ 次行为的时间间隔, η 表示对行为时间间隔误差的敏感度, ζ_1 表示正常行为得分对时间的敏感度。

从公式(3)可以得出, 正常行为得分和行为周期相关, 行为周期越准确的边缘设备会得到更高的正常行为得分。随着时间的流逝, 过去的行为对正常行为得分的影响随之减少。

C_r^M 则用来评估边缘设备的异常行为, 对行为周期成负相关, 可以定义为:

$$C_r^M = -\sum_{i=1}^{K_r^M} \frac{\left|\bar{t}_r - \Delta t\right|}{(t - t_i)^{\zeta_2} + \kappa} \quad \Delta t \leqslant \alpha_s \bar{t}_r \cup \Delta t \geqslant \alpha_s \bar{t}_r \tag{4}$$

其中, K_r^M 表示边缘设备 r 异常行为的总次数, ζ_2 表示异常行为得分对时间的敏感度参数, κ 用于调整异常行为得分范围的约束参数。

由公式(4)可以得出, 当边缘设备的行为被判定为异常行为时, 通过判断行为时间间隔与预设间隔的误差可以判断此次异常行为的类型, 并且误差越大, 其异常行为得分越低。由公式(2)可以得出, 正常行为可以增加其信誉值, 异常行为会减少其信誉值, 随着时间的推进, 过去的行为对信誉的影响会逐渐减小。

在评估边缘设备的信誉之后, 并且包含此次数据提交行为的区块被系统接受, 该边缘设备会得到相应的工作奖励 P_r, 可以定义为:

$$P_r = \lambda_s \cdot \overline{P} \cdot \left(\frac{\delta^{C_r} - \delta^{-C_r}}{\delta^{C_r} + \delta^{-C_r}} + 1\right) \tag{5}$$

其中, $\overline{P}$ 表示边缘服务器每次完成工作的奖励, δ 表示奖励 P_r 对信誉 C_r 的敏感度, λ_s 表示边缘服务器和种类为 s 的边缘设备的奖励之间的权重系数, 以调整两者之间的奖励比例。以上参数的具体值设定会在第五章进行介绍。

结合公式(2)和公式(5)可以得出, 当正常行为的发生时, 奖励会随着信誉的增加实时的增加, 而当异常行为发生时, 奖励会随着信誉的减少而实时的减少。信誉对奖励的影响也会随着信誉的不断增加或减少而削弱, 奖励不会无限制的增加或减少, 始终在 0 和 $2\lambda_s \overline{P}$ 之间。并且, 通过设定阈值, 将不断进行异常行为的边缘设备判定为恶意攻击者, 剔除系统, 可有效防止恶意攻击的发生。

此外, 所提出的基于信誉的 PoW 共识算法依托许可链环境实现其功能, 允许加入许可链中的每个节点都持有一对公私钥 (Pk, Sk), 取公钥的后 20 字节作为其地址信息, 用于标识其身份。当边缘设备作为发送方, 向服务器提交数据时, 使用其私钥 Sk 将数据签名, 接收方使用发送方的公钥 Pk 解密, 确认发送方的身份。由此防止边缘设备被网络中或网络外的其他节点冒充, 保障边缘设备行为信息的真实性。

4 实验环境搭建和方法实现

4.1 基于以太坊搭建边缘设备管理系统

以太坊[18]是当前最热门的区块链平台之一, 本系统通过利用基于Go实现的以太坊实体在多台边缘服务器之间搭建许可链, 为一些功能模块提供了接口, 如表 2 所示。这些边缘服务器构建了原始的区块链环境, 为系统一致性提供算力, 打包、生产新的区块, 配置如表 3 所示。边缘服务器可以与其他节点进行电子货币交易, 在成功生产新的区块后可以获得

表 2 系统模块

Table 2 System modules

模块	使用技术
RPC	基于 Go 的 RPC APIs
智能合约	基于 JavaScript 的 Web3 APIs
应用	Node.js 框架

表 3 边缘服务器配置

Table 3 Configuration of edge server

参数	配置
处理器	Inter (R) core (TM) i5-3470 3.20GHz
内存空间	4GB
操作系统	Windows 7
硬盘空间	1 TB

电子货币作为工作奖励。边缘服务器将所有的区块信息存储在本地的账本中, 包括区块的头和身体, 通过验证区块的默克尔树, 保证了其本地账本数据与系统中其他边缘服务器的账本数据是一致的。在以太坊中, 由于区块的平均生产间隔为 15s 左右, 以及其每个区块当中事务的存储空间最大为 1024byte, 基于以太坊的边缘设备管理系统在性能方面会有所限制。

考虑到智慧城市中边缘设备的在计算、存储等方面的限制, 以及满足在大规模部署时的连接容量和低延迟需求, 在设计边缘设备时, 选择基于 ARM Cortex-M3 的 32 位芯片 STM32F103VCT6 作为处理器, 选择 SIM7020C 的 NB-IoT 通讯模块作为其网关。通过为边缘设备配备一台笔记本电脑作为其代理节点, 边缘设备可以加入区块链网络, 拥有并管理自己的账户。代理节点只需要存储少量的区块的头部信息, 通过验证区块的默克尔树保证账本数据的一致性。此外, 通过将基于 secp256k1 椭圆曲线算法嵌入到边缘设备中, 与以太坊中一致, 使得边缘设备可以通过 NB-IoT 与代理节点的 RPC 接口进行通讯、提交感知数据。在这种情况下, 边缘设备的工作奖励不会直接发放到自己的账户当中而是会由其代理节点保管。

4.2 共识算法实现

智能合约是存储在区块链上的脚本代码, 预置了相应的触发机制, 并采用分布式的形式在区块链系统中执行。边缘服务器会在本地的沙盒(本研究使用 EVM)中执行合约代码, 合约代码根据外部数据源自动判断所处场景是否满足触发条件, 并严格执行预定的规则。在合约代码执行后, 边缘服务器将该合约代码写入区块当中, 并开始挖掘区块。当区块挖掘成功后, 其他边缘服务器会验证该合约的有效性, 验证通过, 则该区块将作为最新的区块被系统接受, 智能合约的运行状态也将存入区块链当中。因此, 智能合约在创建后, 外部无法任意改动其数据内容, 保证了智能合约中数据的安全。

为了在边缘设备间建立信任机制, 规范设备行为, 本系统利用多智能合约实现了基于信誉的 PoW 共识算法为边缘设备提供信任机制, 其中包括一个入口合约和一个判断合约。

入口合约由边缘服务器部署, 是边缘设备向系统上传感知数据的入口。该合约维护了一个边缘设备信息查询表, 负责记录边缘设备的身份信息, 控制边缘设备的访问权限, 如表 4 所示。其中, 每一列包含了以下信息: DecAddress: 边缘设备的地址; AgeAddress: 其代理节点的地址; DecType: 该边缘设备的类型; Order: 该边缘设备上传数据的次数; CreValue: 该边缘设备的信誉值; AccAuthority: 该边缘设备的访问权限; 同时入口合约为维护该查询表提供了以下应用接口:

表 4 边缘设备信息查询表

Table 4 Reporter lookup table

DecAddress	AgeAddress	DecType	Order	CreScore	AccAuthority
0x3c7539cd57b...	0x3aeb636247...	Smoke	1	1/3	True
0x3c7539cd57b...	0x3aeb636247...	Smoke	2	1/5	True
0x3c7539cd57b...	0x3aeb636247...	Smoke	3	–2	False
……	……	……	……	……	……

deviceRegister( ): 为新设备的注册提供接口, 向边缘设备信息查询表添加新的记录。

deviceUpdate( ): 为已注册设备的信息更新提供接口, 修改边缘设备信息查询表中的记录。

deviceDelete( ): 为已注册设备的信息删除提供接口, 删除边缘设备信息查询表中的记录。

accControl( ): 为已注册设备的权限控制提供接口, 更新边缘设备信息查询表中的记录。

只有被授权的地址可以调用相关的应用接口, *accControl* ABI 可以由判断合约直接调用。入口合约同时为边缘设备提供了 *subData* ABI 用于感知数据的提交, 该接口会直接调用判断合约中信誉评估相

关的应用接口。

当边缘设备的上传的感知数据被边缘服务器记录在系统账本中之后, 判断合约实现了对边缘设备行为的信誉评估, 以及奖励分发。判断合约维护了一个时间戳查询表, 记录该合约下所有已注册边缘设备每次行为的时间戳, 并提供 *timUpdate* ABI 更新该查询表, 以及 *timQuery* ABI 查询表中的记录。基于以上记录, 以及所提出的基于信誉的 PoW 共识算法, *creEvaluation* ABI 接口实现了对边缘设备行为的信誉评估, 如算法 1 所示, 输入边缘设备的地址、类型、时间戳、哈希值, 返回对应的信誉值。

系统的工作流程如图 2 所示, 可以分为以下几个步骤:

步骤 1: 基于以太坊平台初始化私链环境, 以及边缘设备、代理节点、边缘服务器的账户地址和信息;

步骤 2: 部署入口、判断合约, 注册边缘设备以及其代理节点信息;

步骤 3: 边缘设备通过代理节点的 RPC 端口调用入口合约的应用接口, 向系统上传感知数据;

步骤 4: 当包含该感知数据的区块被边缘服务器挖掘并且记录在账本当中之后, 该边缘服务器获得相应的工作奖励, 判断合约评估该边缘设备此次行为更新其信誉值, 根据信誉值发放相应的工作奖励。

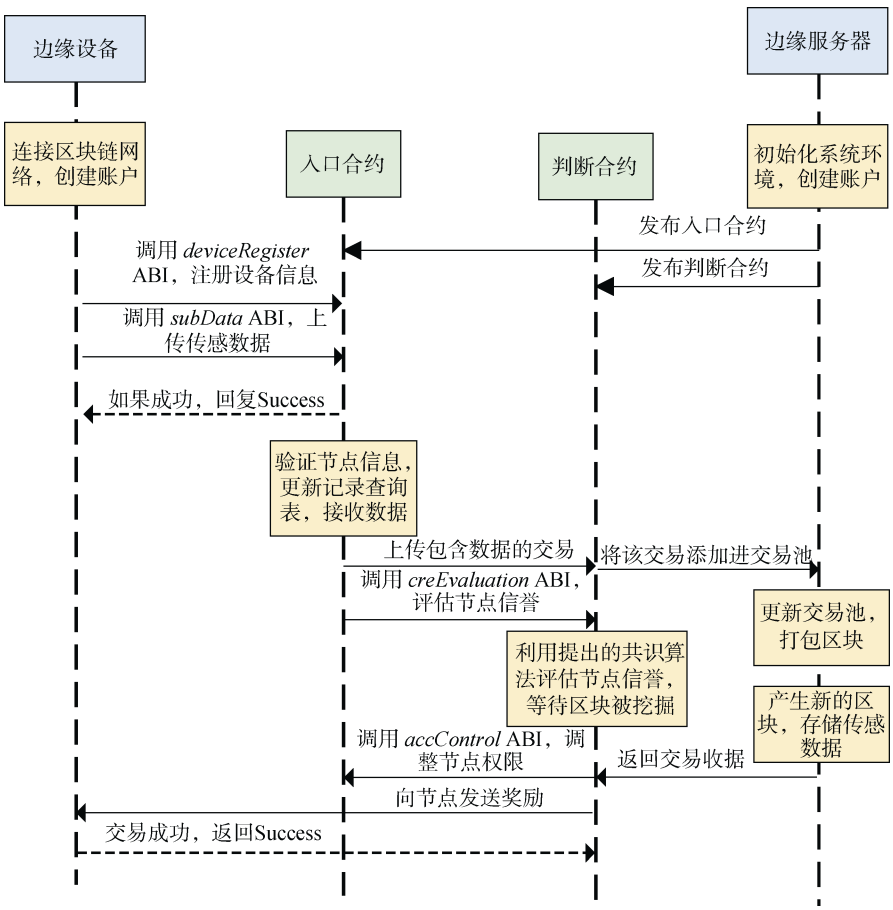

图 2 系统工作流程

Fig.2 System workflow

Algorithm 1: *creEvaluation* ABI

Input: *address, type, timestamp, hash.*

Output: *result(update,reward).*

Require: *result.update* ← False, *result.reward* ← False,

timUpdate( ) and *timQuery( )* of timestamp list ABIs.

1: Create a timestamp array *timestampArray[ ]*.

2: *timUpdate(address,timestamp).*

3: *timestampArray* ← *timQuery(address).*

4: get C_r *(address, timestampArray)* using (2).

5: create an Entry Contract instance *entry.*

6: **if** *entry.accControl(address,* C_r*)* is captured **then**

7: *result.update* ← True.

8: **end if**

9: **while** true **do**
10: check the block containing the report.
11: **if** the block containing the report is generated **then**
12: get P_r (C_r) using (5).
13: create a *transaction*(*address*, P_r).
14: send the *transaction* to the agent of the reporter.
15: *result.reward* ← True.
16: break.
17: **end if**
18: **end while**
19: **return** *result*(*update*,*reward*).

5 实验结果与分析

5.1 实验参数设置

表 5 实验参数设置
Table 5 Parameter setting

参数	参数说明	初始值
ξ_1, ξ_2	正常行为和异常行为的权重	$\xi_1 : \xi_2$ =1∶1
ζ_1, ζ_2	行为对时间的敏感度	$\zeta_1 = \zeta_2$ =1/2
$\bar{t}_r$	预定数据上传周期	30s
η	对周期误差的敏感度	2
α_s	对周期误差的最大容忍度	2/3
κ	调整异常行为得分范围的约束参数	2
$\overline{P}$	边缘服务器每次完成工作的奖励	5 Eth
λ_s	奖励的调整系数	1/2
δ	奖励对信誉的敏感度	2

5.2 实验结果分析

如图 3 所示, 边缘设备数据预设的数据上传周期为 30s, 异常的数据上传周期为 10s, 边缘设备的信誉值会随着其行为动作而动态的变化。当数据的上传周期满足正常行为范围时, 该设备的此次行为被认定为正常行为, 并且数据上传周期与预设周期的误差越低, 此次数据上传工作完成的质量就越高, 信誉值也就会越高。而当设备以 10s 为周期上传数据时, 此次行为就会被认定为异常行为, 异常行为会使设备的信誉值下降, 并且不会获得工作奖励。设备的异常行为会一直影响它的信誉值, 并且在异常行为发生之后, 其平均信誉值会相对低于异常行为发生之前的平均信誉值。设备信誉的变化会直接影响设备每次完成工作的奖励, 信誉值越高, 其工作奖励 P_r 也就越高, 不会高于 $\overline{P}$, 但也不会低于 0。

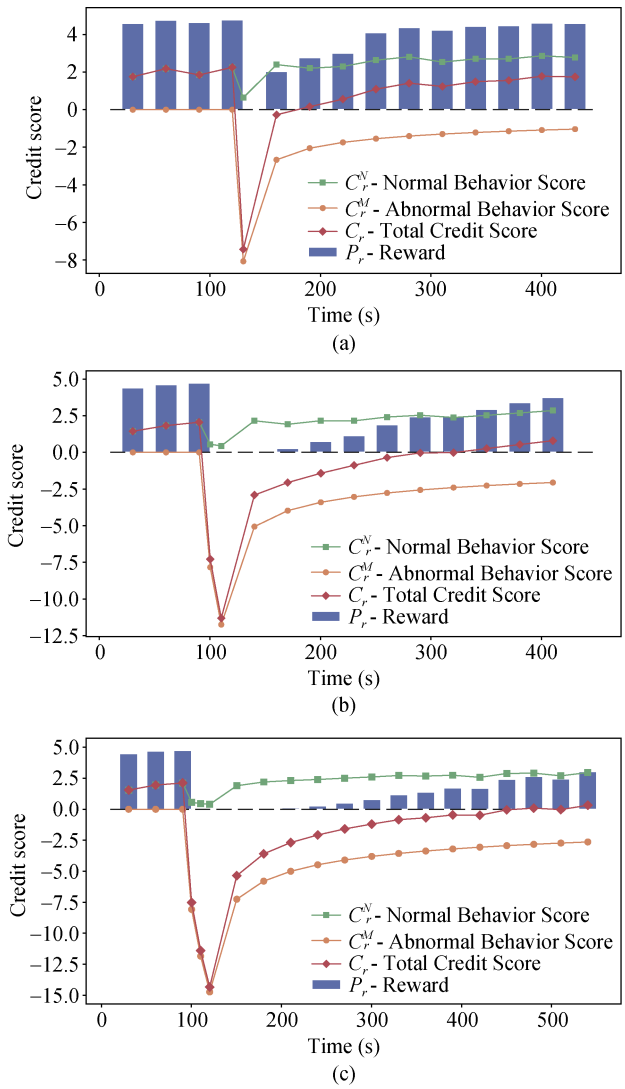

图 3 边缘设备信誉和行为之间的变化关系; (a)发生一次异常行为; (b)发生两次异常行为; (c)发生三次异常行为

Figure 3 Credit score changes based on behaviors of edge device. (a) When once abnormal behavior happens. (b) When twice abnormal behaviors happen. (c) When three times abnormal behaviors happen.

如图 3(a)所示, 在系统时间 110s 时, 该边缘设备发生了一次上传周期为 10s 的异常行为, 可以看出边缘设备的信誉值随着其异常行为的发生而骤降, 该次工作奖励也降低到了 0 之后, 该设备继续以 30s 为周期正常进行上传, 随着正常行为次数增加, 其信誉值在慢慢的回升, 奖励也慢慢回升。但以同样的质量完成工作, 该设备获得的信誉值和奖励都低于异常行为发生之前的水平。

在图 3(b)中, 该边缘设备连续两次发生了异常行为, 可以看出该设备的信誉值比发生一次异常行为时下降的更快更低了, 这两次工作的奖励同样也降低到了 0。在这两次异常行为之后, 虽然该设备的

平均数据上传周期和发生一次异常行为时大致相同，以同样的质量完成工作，但平均奖励比发生一次异常行为时低很多，该设备通过正常行为恢复其信誉值的周期也更长。

同样，在图 3(c)当中，该边缘设备连续三次发生了异常行为，相比于前两次实验，此次实验该设备的信誉值同样发生了骤降，信誉和奖励也都需要更长的恢复周期。除以之外，该设备还受到了更严重的惩罚，这三次异常行为将不会获得工作奖励，其之后的数次正常行为也没有获得工作奖励。

对比图 3 中的三次实验结果可以得出，在基于信誉的PoW共识算法的约束下，边缘设备发生异常行为会极大的降低其信誉，从而减少其工作奖励。随着异常行为发生次数的增加，边缘设备的平均工作奖励逐渐减少，恢复信誉所需要的周期也越长。因此，对于持续发生异常行为的边缘设备，可以通过在系统中设定信誉阈值，将信誉低于阈值的设备加入系统黑名单，从系统网络中剔除。并且，通过将设备工作奖励和订购相关服务的费用相关联，可以在智慧城市系统中构建一个货币体系，使得边缘设备的经济收益和其行为相关联，可有效约束边缘设备的行为，鼓励设备更加诚实，增加恶意攻击的攻击成本。

边缘设备的平均工作奖励和信誉与其数据上传周期之间的关系如图 4 所示。随着实际数据上传周期和预设周期误差的增加，边缘设备的平均工作奖励和信誉逐渐的减少。并且，随着边缘设备数据上传周期与预设周期之间误差的增加，其平均奖励的下降速度比其信誉值更快。这使得边缘设备不能通过减少其数据上传周期获得更多的奖励，鼓励设备更加诚实、准确的完成相应的工作。

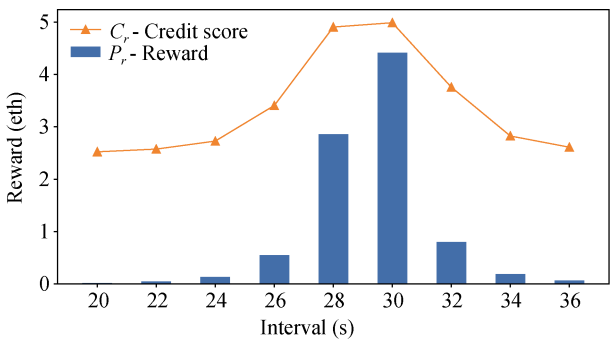

图 4　边缘设备的平均信誉和奖励与其数据上传周期之间的关系

Figure 4　Relationship between reward and data upload periods of edge device

6　结束语

本文提出的基于区块链的智慧城市边缘设备可信管理方法，将区块链引入边缘计算当中，旨在解决智慧城市相关应用系统中的信息安全问题。基于信誉的 PoW 共识算法为边缘设备提供了信任机制，解决了资源受限的边缘设备难以适配区块链中相对高的计算和存储要求，实现了对边缘设备行为的可信管理。基于区块链的智慧城市边缘设备管理架构，将许可链引入智慧城市，利用其安全机制和分布式架构，实现了感知数据的可信收集和安全存储。以智慧城市为背景的案例研究验证了该方法可有效约束边缘设备行为，增强系统的信息安全性，并有望扩展到更多的智慧城市相关应用服务中。

基于以太坊实现的边缘设备管理系统是该方法的一个应用雏形，还存在一些不足，需要持续的更新和完善，例如智能合约引起的并发量低，边缘设备功能性不足等问题。在未来工作中，我们将继续探究基于区块链的边缘设备可信管理的实现途径和方法，例如可插拔共识算法的区块链架构、跨链间的通讯等以提高系统可扩展性和纯粹性。

参考文献

[1] Zanella A, Bui N, Castellani A, et al. Internet of Things for Smart Cities[J]. *IEEE Internet of Things Journal*, 2014, 1(1): 22-32.

[2] Wang T, Ke H X, Zheng X, et al. Big Data Cleaning Based on Mobile Edge Computing in Industrial Sensor-Cloud[J]. *IEEE Transactions on Industrial Informatics*, 2020, 16(2): 1321-1329.

[3] Wang X K, Chen X, Li Z, et al. Access Delay Analysis and Optimization of NB-IoT Based on Stochastic Network Calculus[C]. *2018 IEEE International Conference on Smart Internet of Things*, 2018: 23-28.

[4] Salaht F A, Desprez F, Lebre A. An Overview of Service Placement Problem in Fog and Edge Computing[J]. *ACM Computing Surveys*, 2020, 53(3): 1-35.

[5] Chatzopoulos D, Bermejo C, Kosta S, et al. Offloading Computations to Mobile Devices and Cloudlets via an Upgraded NFC Communication Protocol[J]. *IEEE Transactions on Mobile Computing*, 2020, 19(3): 640-653.

[6] Pan J L, McElhannon J. Future Edge Cloud and Edge Computing for Internet of Things Applications[J]. *IEEE Internet of Things Journal*, 2018, 5(1): 439-449.

[7] Jia G Y, Han G J, Rao H L, et al. Edge Computing-Based Intelligent Manhole Cover Management System for Smart Cities[J]. *IEEE Internet of Things Journal*, 2018, 5(3): 1648-1656.

[8] Muhammed T, Mehmood R, Albeshri A, et al. UbeHealth: A Per-

sonalized Ubiquitous Cloud and Edge-Enabled Networked Healthcare System for Smart Cities[J]. *IEEE Access*, 2018, 6: 32258-32285.

[9] Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System[EB/OL]. [2020-08-20]. https://bitcoin.org/bitcoin.pdf.

[10] Yu H Y, Yang Z, Sinnott R O. Decentralized Big Data Auditing for Smart City Environments Leveraging Blockchain Technology[J]. *IEEE Access*, 2019, 7: 6288-6296.

[11] Chen R N, Li Y N, Yu Y, et al. Blockchain-Based Dynamic Provable Data Possession for Smart Cities[J]. *IEEE Internet of Things Journal*, 2020, 7(5): 4143-4154.

[12] Lin X, Wu J, Mumtaz S, et al. Blockchain-based On-Demand Computing Resource Trading in IoV-Assisted Smart City[J]. *IEEE Transactions on Emerging Topics in Computing*, 2020.

[13] Zhang Y, Kasahara S, Shen Y L, et al. Smart Contract-Based Access Control for the Internet of Things[J]. *IEEE Internet of Things Journal*, 2019, 6(2): 1594-1605.

[14] Huang J Q, Kong L H, Chen G H, et al. Towards Secure Industrial IoT: Blockchain System with Credit-Based Consensus Mechanism[J]. *IEEE Transactions on Industrial Informatics*, 2019, 15(6): 3680-3689.

[15] Pan J L, Wang J Y, Hester A, et al. EdgeChain: An Edge-IoT Framework and Prototype Based on Blockchain and Smart Contracts[J]. *IEEE Internet of Things Journal*, 2019, 6(3): 4719-4732.

[16] Kiayias A, Russell A, David B, et al. Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol[C]. *Annual International Cryptology Conference*, 2017: 357-388.

[17] Martino R, Cilardo A. Designing a SHA-256 Processor for Blockchain-Based IoT Applications[J]. *Internet of Things*, 2020, 11: 100254.

[18] Wood G. Ethereum: A Secure Decentralised Generalised Transaction Ledger[EB/OL]. [2020-06-08]. http://gavwood.com/Paper.pdf.

石鹏展 2018 年获学士学位。现在苏州科技大学电子与信息工程学院攻读硕士学位。主要研究领域为物联网、区块链。Email: spiriz@126.com

戴欢 2012 年获博士学位。现任苏州科技大学电子与信息工程学院副教授，研究生导师。主要研究领域为区块链、物联网、无线感知。Email: daihuanjob@163.com

陈洁 2012 年获博士学位。现任华东师范大学软件工程学院教授，博士生导师。主要研究领域为信息安全、人工智能。Email: jchen@cs.ecnu.edu.cn

陈儒玉 2019 年获学士学位。现在苏州科技大学电子与信息工程学院攻读硕士学位。主要研究领域为物联网、区块链。Email: chenruyu815@163.com