基于区块链的物联网设备标识研究

陈美娟，朱晓荣
（南京邮电大学通信与信息工程学院，江苏 南京 210003）

摘　要：将区块链技术与物联网应用相结合，提出了基于区块链标识的物联网体系架构，设计了一种基于区块链的物联网标识编码方法，说明了基于所提架构的物联网设备注册服务流程和查询服务流程，并对该体系的安全性进行了分析。基于所提网络架构和标识方法，给出了智慧家庭场景中的应用，从 2 种典型案例中可以看出，所提方案能够保证物联网各种应用的安全性。

关键词：物联网；区块链；标识；安全
中图分类号：TN915.9
文献标识码：A
doi: 10.11959/j.issn.2096-3750.2018.00048

Research on IoT device identification based on blockchain

CHEN Meijuan, ZHU Xiaorong
College of Telecommunications and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, China

Abstract: Combined blockchain technology with IoT applications, a blockchain-based IoT architecture was proposed, and a blockchain-based IoT identification method was designed. The equipment registration service process and the query service process based on the proposed IoT architecture were illustrated, and the security of the system was analyzed. Finally, based on the proposed network architecture and the identification method, the application in the smart home scenario was given. It can be seen from the two typical cases that the proposed solution can guarantee the security of various applications in the Internet of things.

Key words: Internet of things, blockchain, identification, security

1　引言

国际电信联盟（ITU）对物联网（IoT）的定义是：信息社会全球基础设施（通过物理和虚拟手段）将基于现有和正在出现的、信息互操作和通信技术的物质相互连接，以提供先进的服务[1]。在物联网中，“物”指物理世界（物理装置）或信息世界（虚拟事物）中的对象，可以被标识并整合入通信网。通过使用标识、数据捕获、处理和通信能力，物联网充分利用物体向各项应用提供服务，同时确保满足安全和隐私要求[2]。因此，物联网实现万物互联首先必须对物联网涉及的各种“物”进行高效、唯一的标识，通过物联网标识可以在指定作用域内唯一识别某个物理或逻辑实体对象，还可以实现对实体信息的查询、管理以及控制，为各种物联网应用提供实现的基础[3]。

目前，国内外相关标准化组织都在积极推进物联网的标识相关技术的研究，迄今为止，各标准组织还未形成统一的国际标准[4]。当前的设备编码标准众多[5]，例如，美国 EPCglobal 的电子产品代码（EPC, electric product code）[6-7]、日本泛在识别中心的泛在识别码（uCode, ubiquitous code）[8-9]、韩国的可移动的 RFID 编码（mRFID code, mobile RFID code）[10]、我国商务部的商务产品编码（CPC, commerce product code）[11]。然而，各种设备编码之间相互孤立、没有联系，有的甚至重复交叉，要实现信息的互联互通和系统的有效协同，必须建立统一的物联网标识体系。

收稿日期：2018-02-26；修回日期：2018-03-09

鉴于物联网标识服务对于物联网产业发展的重要性，2013 年，我国开始研发“物联网标识管理公共服务平台（China Internet of Things Name Service Platform）”[12]，该平台兼容多种异构标识，提供解析服务和发现服务，实现所有物联网相关应用信息资源的寻址访问，从而实现物联网中资源信息的获得[4]。但是并没有考虑到隐私与安全问题，而隐私和安全是物联网服务能否被广泛使用的前提[13]，如何保证物联网海量数据的安全和用户的隐私是物联网应用发展必须解决的重要问题。

自从 2008 年出现了比特币和区块链技术[14-15]以来，人类历史上出现了去中心化的电子货币的发行和交易，而且公开部署在区块链上的智能合约使业务逻辑能够不需要人为干预地按照触发条件自动执行。在区块链系统中，数据以区块为单位产生和存储，并按照时间顺序形成链式数据结构。典型的区块链系统具有多方写入共同维护、账本公开、分布式和不可篡改等特点，是一种可追溯历史、多方相互信任的分布式系统。基于区块链技术，PPK 开放小组定义了开放数据索引命名（ODIN, open data Index name）[14]。ODIN 是一种在网络环境下表示和交换数据内容索引的开放性系统，由 ODIN 标识符、解析系统、元数据和规则组成。

物联网中存在着海量的分布式数据，非常适合区块链技术解决物联网的安全问题。区块链的不可篡改特点使各类数据可以进入物联网、区块链中的加密和信任机制，这为家庭或公共环境中大量设备的连接提供了可能[16]，也为机器之间的自动化交易提供了保障机制，采用智能合约可以在设备之间形成更加灵活的交易[17]。因此，本文在借鉴已有标识编码标注的基础上，将区块链技术与物联网应用相结合，提出了基于区块链的物联网设备标识编码方法，给出了采用区块链技术的物联网标识网络架构，说明了基于此架构的物联网设备注册服务流程和查询服务流程，并对该网络架构的安全性进行了分析，最后基于所提标识方法和网络架构，列举了智慧家庭场景中的典型应用案例。

2　基于区块链的物联网标识解决方案

2.1　基于区块链标识的物联网体系架构

基于区块链标识的物联网架构由 5 层构成，包括设备层、接入层、控制层、内容层和应用层，系统分层结构如图 1 所示。

2.1.1　设备层和接入层

设备层包括物联网的所有设备，即真实的物理设备和虚拟的数字设备。设备层的每个设备都具有全局唯一的标识，多个单一设备可以组合成为一个集合设备，集合设备也具有全局唯一的标识。通过

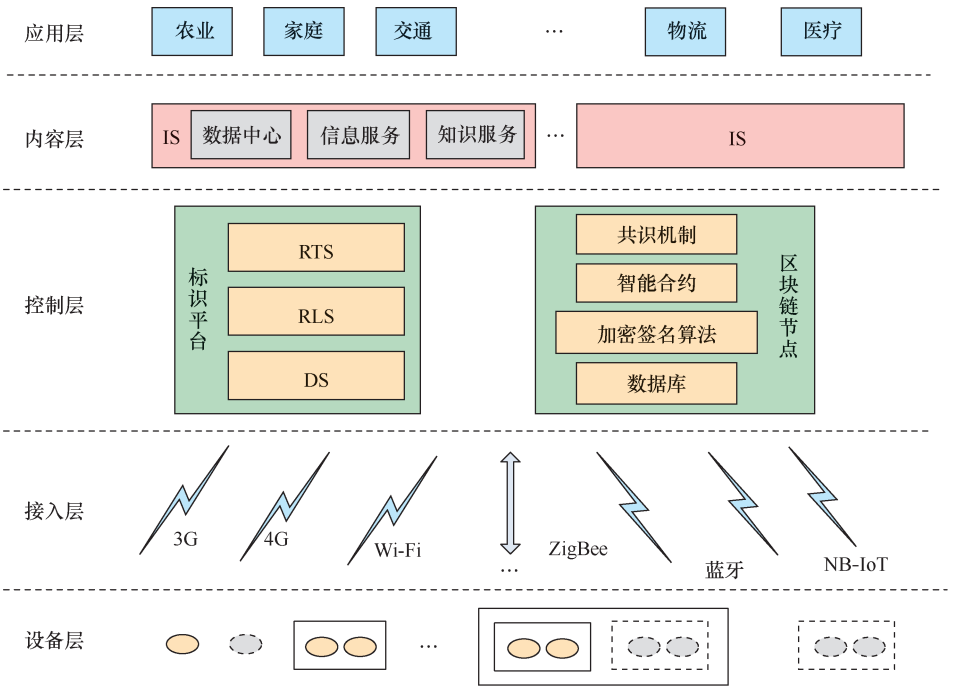

图 1　区块链标识物联网分层结构

标识可以寻找到这些设备。设备层的主要功能是实现数据采集和动作执行，常见的设备有传感器（如温湿度、火焰、浓度、压力等）、摄像头（采集音视频信息）、各种标签（如RFID、一维条形码、二位条形码等）、手机、各种智能的插座、开关、轮胎、冰箱等。

接入层提供了多种连接方式，实现物与物之间、物与人之间、人与人之间等的互联。连接方式包括已有的、未来的各种新方式，如3G、4G、Wi-Fi、蓝牙、NB-IoT、以太网、各种工业总线等多种方式。

2.1.2 控制层

控制层负责向可信的实体提供可信的内容，主要包括物联网标识平台和区块链节点。标识平台包括注册服务器（RTS）、解析服务器（RLS）和发现服务器（DS）。区块链节点包括当前共识算法、智能合约、加密签名算法和数据库等。

注册服务器为设备提供注册功能，所有设备生产厂商必须在注册服务器中注册，注册服务器必须对厂商身份进行认证。注册成功后该厂商就成为物联网标识的拥有者，能够对自己所生产的设备进行自主标识，自行保证标识的唯一性。网络中有一个中央注册服务器，还有许多分布式的厂商注册服务器，它们共同作用为设备提供了全局范围内唯一的标识。

网络中存在大量信息服务器（IS），一台发现服务器对应一组信息服务器，发现服务器将通过设备标识寻址到某台具体的信息服务器。发现服务器相当于云服务中的网络边缘云。解析服务器通过设备标识寻址到设备对应的发现服务器。注册服务器相当于云服务中的核心云。

区块链（BC）节点为物联网提供安全保障，设备的标识写入区块链网络，设备数据信息的数字摘要写入区块链网络，访问设备标识、设备数据信息的实体必须通过区块链网络相应的认证机制。人与人、人与物、物与物之间的交易均可以通过区块链节点中的智能合约来约束和灵活定制，区块链节点的运行机制参考ODIN技术规范来实施。

2.1.3 内容层和应用层

内容层由许多信息服务器构成，信息服务器用于存放设备的数据信息、设备的操作控制信息，通过设备标识可以查找和使用这些信息。信息服务器可放置在生产厂商处，也可以放置在设备使用者所在的地方。信息服务器中的内容必须防篡改，访问信息服务器的对象必须具有合法身份和相应权限。从云服务的观点来理解，信息服务器就是用户边缘云。

每个信息服务器由3部分组成：数据中心、信息服务和知识服务，这3部分的功能可以按照应用进行设置，如农业服务、物流服务和医疗服务等。数据中心是设备层的设备感知到的原始信息数据，通过设备标识可以查找到该设备的所有数据，例如，可以根据摄像头的标识，查找到该摄像头拍摄的视频内容。数据中心的物理位置可以在距离较近的地方，例如，设备接入网络的接入点（AP, access point）。信息服务是在数据中心的基础上，通过数据分析得出的信息，例如，从相关的火焰、温度、视频感知设备可以得知某个地方发生了火灾，或从某人的多个穿戴传感器得知他血压高了。知识服务器是在信息服务的基础上进一步对数据进行挖掘分析得出来的一些普适的结论，例如，对某类病人长期用药效果进行分析，得出相应的医疗处方，可以为网上医疗提供参考。

应用层是物联网面向各行业提供的智慧服务，例如，对于农业，可以提供农产品溯源、智能浇灌；对于医疗行业，可以提供药品溯源、网上医疗等。

2.2 基于区块链的物联网标识编码

2.2.1 物联网标识编码的需求

兼容性是对物联网标识编码的主要要求[18]。当前物联网中设备编码标准存在多样性，如EPC、uCode或其他自定义编码，形成了异构的设备编码标准，这些异构的编码标准可能导致物联网标识服务发生冲突。在物联网场景中，有可能为了描述一个事件，需要多种具有不同感知功能的设备，而且这些设备所感知到的数据的存放格式也不尽相同。例如，判断火灾事件是通过温度、烟雾浓度、火焰等传感器和视频摄像头采集到的信息共同决策后得出的结论。因此，物联网标识必须兼容已有的异构编码标准，使设备的标识具有全球唯一性。

有效性是物联网标识服务的重要特点[19]。物联网中拥有海量设备，这些设备具有高度的动态性[20]，能够在陆、海、空范围内频繁移动，设备的属性也随时间不断发生变化，相应的网络中描述这些设备的数据信息也需要不断更新，这将导致设备名字与物理地址的映射发生频繁变化。由于映射的频繁更新，物联网中标识服务的查询数量将远远超出互联网中的DNS服务，因此，要求物联网对标识服务的访问具有有效性保证。

隐私与安全是物联网进一步发展的难题，设备名字和地址的映射关系可能导致隐私泄露，在一些设备标识的映射中应注意隐私的保护，例如，有些用户并不想让别人知道自己用了什么药物。设备的数据信息不能篡改，如果通过设备标识进一步篡改设备的数据信息会带来安全问题，例如，居民电表读数的篡改将导致用户对供电公司的不信任。另一方面，没有授权的人或机器读取设备的数据信息或操作设备也将导致安全隐患。因此，隐私和安全是物联网标识体系设计时必须考虑的问题。

标识用于在设备流通过程中唯一标识设备身份的编码，通过标识可以在网络中查找到该设备，也可以获得对该设备的控制信息。鉴于以上需求，本文提出一种基于区块链的物联网标识编码方法，简记为 BCNS，BCNS 分为基础标识编码和扩展标识编码 2 种类型。

2.2.2　基础标识编码

基础标识编码包括区块链域和设备域 2 部分，该标识编码结构如图 2 所示。

区块链域包括 2 个部分：[区块号].[位置号]。[区块号]由区块链网络决定，表示该标识编码在区块链网络上登记时所在的区块的流水号（由区块链网络给出）。[位置号]表示该标识编码在该区块内的位置（从 0 开始编号），也就是在该区块内的哪个条目。设备域与区块链域之间以符号“/”分隔。通过注册方式获得区块链域编码的厂商，称为物联网标识拥有者。

设备域也包括 2 个部分：[标准标识]#[资源标识]。[标准标识]表示某种物联网编码标准，已有的各类异构编码均可以成为这个地方的内容，没有采用已有编码标准的设备，按照 BCNS 编码标准对待，由 BCNS 平台统一分配。[资源标识]对应某种编码标准下的某个设备的标识编码，由该编码标准机构统一编码并保证唯一性。

例如，标识编码为：345678.111/ EPC-96I#01.0371002.010101.0001600A2，表示该标识编码在第 345 678 区块的第 111 个条目，是采用 EPC-96I 编码标准的某个资源的标识。该 BCNS 标识串将被映射到该资源的元数据和可能的一些 URL 上，此时，BCNS 就成为该资源的一部分，始终与该资源同时存在。该资源的 BCNS 信息、元数据和 URL 等信息保存在 BCNS 拥有者的数据库内，该数据库本文称为信息服务器。

2.2.3　扩展标识编码

上述基于区块链的物联网标识编码称为基础标识编码，在此基础上，可以定义扩展的区块链物联网标识编码。物联网标识拥有者可以利用已有的区块链编码来自定义扩展的 BCNS 标识编码，这样可以方便标识拥有者为自己的设备定义标识。物联网标识拥有者将二级 BCNS 标识记录批量打包后形成新区块的散列关键字写入上一级的基础区块链。以此类推，可以形成更多级的基于区块链的物联网标识。

扩展物联网标识编码结构包括 3 个部分：[父链域]/[扩展域]#[设备域]。[父链域]对应基础标识编码的[区块链域]。[扩展域]是基础标识在子级区块链上

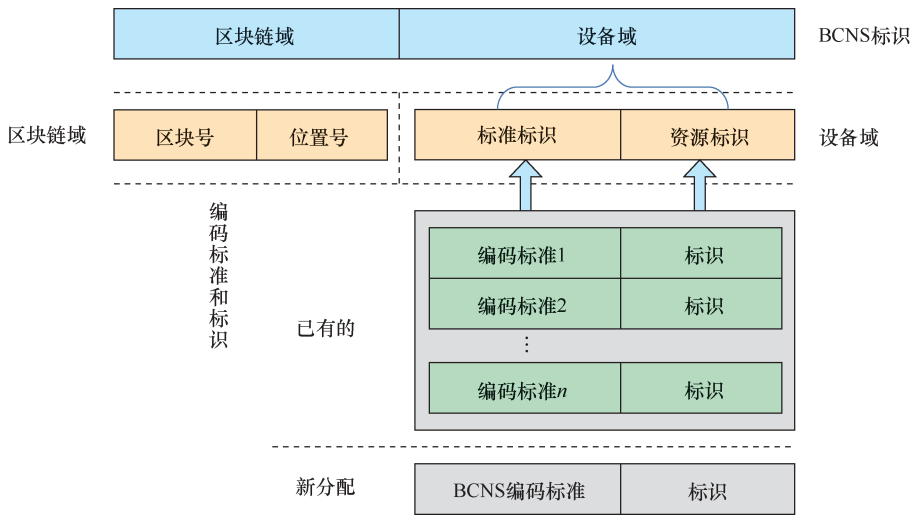

图 2　基于区块链的物联网标识编码

的唯一标识，由 BCNS 拥有者来定义，可以是流水号或取值唯一的字符串。[设备域]与基础编码中的[设备域]含义相同。例如：345678.111/22/EPC-96I#01.0371002.010101.0001600A2。

2.3 基于区块链的物联网标识服务流程

2.3.1 注册服务

基于区块链的物联网标识注册服务关键过程有：厂商向标识平台注册设备标识；设备信息向信息服务器的注册；标识关联性的注册；设备数据信息的数字摘要进入区块链。如果不存在多个物联网标识的嵌套，就不需要关联性注册过程。基于区块链标识的物联网设备注册服务流程如图 3 所示。

Step1 每个厂商通过注册客户端向标识平台的注册服务器进行注册，注册服务器结合区块链标识和该设备，为该设备分配标识编码{BCNS_ID}。注册服务器将该标识与厂商的对应关系告诉解析服务器，解析服务器记录该厂商的 BCSN_ID 号并分配合适的发现服务器给该厂商，记录的主要内容为 RecordDS={BCNS_ID,DSa}。然后转发注册请求给发现服务器。

Step2 发现服务器找到该厂商的信息服务器，记录标识编码规则和信息服务器之间的映射关系，在发现服务器中增加记录 RecordIS= {BCNS_ID, ISa}，之后向该厂商返回注册成功的响应消息，消息中带有发现服务器的号码{BCNS_ID, DSa}，同时把该设备的标识编码写入区块链网络。

Step3 当该设备采集到数据需要上报时，该设备发送注册请求给相应的信息服务器，消息中包含标识编码和采集到的数据{BCNS_ID1, Data}等信息；信息服务器记录该设备的物联网区块链标识与设备上报的元数据、URL 等的对应关系，主要内容为 RecordData={BCNS_ID1,ISa,Data,URL}。然后，信息服务器把 RecordData 的数字摘要写入区块链节点、把注册请求消息转发给相应的发现服务器。发现服务器更新该设备标识的内容为 RecordIS={BCNS_ID1, ISa}等，并向用户返回设备注册成功的响应。

Step4 当用户 b 对该设备做了相关的操作并产生了新的标识 BCNS_ID2 时，则设备的新标识注册请求被发送至与用户 b 相关的信息服务器，注册请

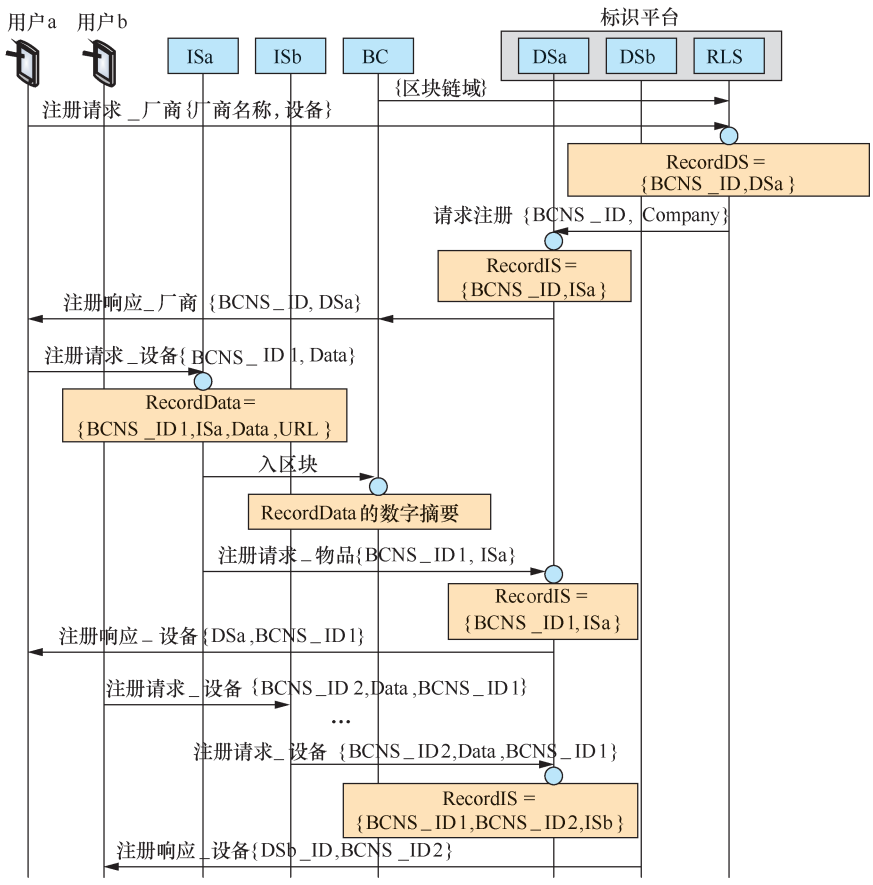

图 3 注册服务流程

求消息中同时含有该设备当前的标识和之前的标识。信息服务器记录该设备的物联网区块链标识与设备上报的元数据、URL 等的对应关系，信息服务器中记录的主要内容为 RecordData={BCNS_ID2, ISb, Data, URL}。信息服务器把 RecordData 的数字摘要值送入区块链节点。

Step5　信息服务器转发新设备的注册请求给相应的发现服务器，注册请求消息中包含了该设备的本次标识 BCNS_ID2 和上次标识 BCNS_ID1 等信息。发现服务器记录该设备标识 BCNS_ID2 与信息服务器 ISb 之间的对应关系，同时记录了上次标识 BCNS_ID1，并向用户 b 返回设备注册成功的响应。发现服务器记录的主要内容为 RecordIS={BCNS_ID1, BCNS_ID2,ISb}。

2.3.2　查询服务

当某用户使用物联网设备并通过手机中的客户端扫描该设备上的条形码或二维码时，可以获得该设备的物联网标识，用此标识可以查询到与该设备相关的信息。查询过程需要对查询者的身份进行认证，有权限的用户才可以访问相关的信息服务器器。查询服务流程如图 4 所示。

Step1　客户端发送物联网标识编码的解析请求消息给解析服务器，消息的主要参数是该设备的标识{BCNS_ID2}。解析服务器接收到解析请求消息后，查询记录后得出该标识的发现服务器是 DSb，于是，解析服务器器转发解析请求消息给 DSb。

Step2　发现服务器 DSb 接收到解析请求消息{BCNS_ID2}后，查询记录后得出该标识对应的信息服务器是 ISb，同时发现有上级标识{BCNS_ID1}。DSb 一方面发送解析请求消息{BCNS_ID1}给解析服务器，另一方面 DSb 请求区块链网络对用户 a 接入信息服务器 ISb 进行认证。

Step3　解析服务器解析{BCNS_ID1}，得到对应的发现服务器是 DSa，于是转发解析请求消息

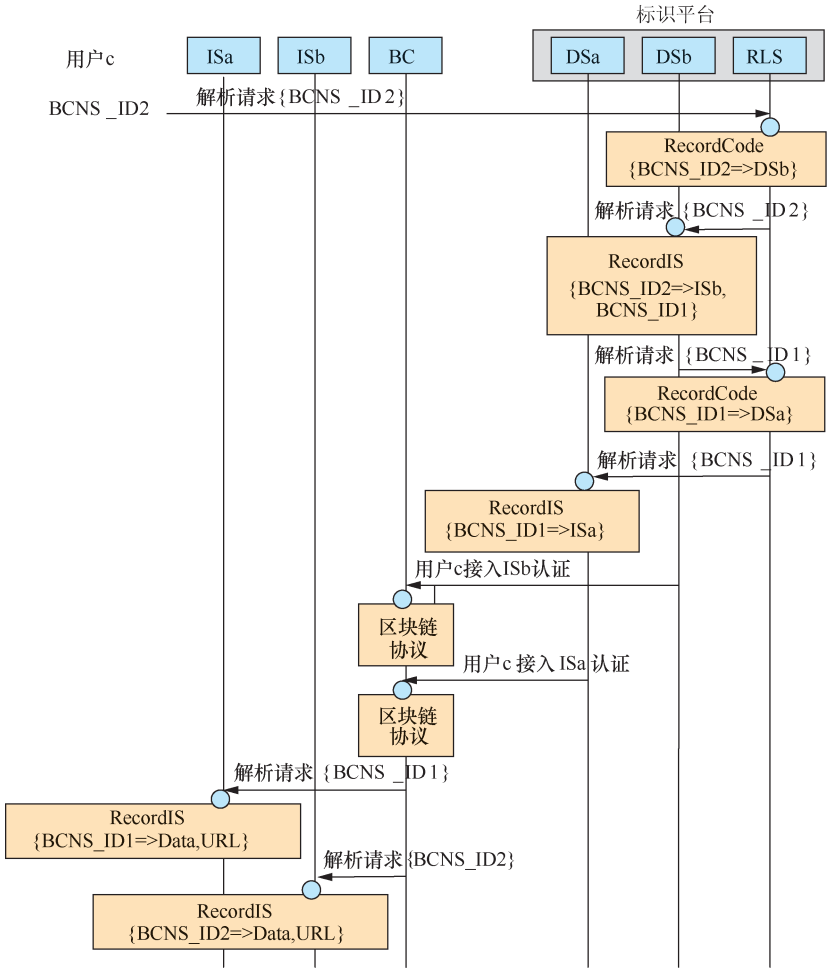

图 4　查询服务流程

{BCNS_ID1}给 DSa。DSa 解析{BCNS_ID1}，得出对应的信息服务器是 ISa。于是 DSa 请求区块链网络对用户 a 接入信息服务器 ISa 进行认证。

Step4 区块链网络对用户 a 接入信息服务器 ISa 和 ISb 认证通过后，分别发送解析请求消息{BCNS_ID1}和{BCNS_ID2}给 ISa 和 ISb。

Step5 信息服务器 ISa 和 ISb 分别向用户返回标识所对应的数据信息或 URL 信息。

当设备处于流通过程中时，它会在多个地方注册。此时，标识平台会返回多个信息服务器地址，用户可以查询到多个信息服务器中的数据，实现设备追踪、溯源等功能。

基于区块链的物联网标识拥有者可以完全开放数据资源访问权，也可以通过适当的自定义机制使用户获取相应的数据资源的访问权，用户也可以通过智能合约的方式，在智能合约的控制下由网络推送与某标识相关的数据给用户。

2.4 安全性分析

2.4.1 基于区块链技术的物联网安全保障

基于区块链的物联网设备标识是生产厂商在公共标识平台通过注册得到的，只有合格的厂商才是区块链物联网标识的拥有者，会得到平台分配的物联网标识 BCNS_ID，BCNS_ID 写入区块链网络后将不会被篡改。大量物联网设备的数据虽然短小但量很大，例如，智能电表会周期性读取很多用户的电表读数。把大量的数据写入区块链是不可取的，因此，本文采用把这些数据的数字摘要存入区块链网络，区块链采用密码学散列算法技术，能够保证物联网设备数据信息的完整性（防篡改性）。区块链在网络传输过程中，采用了数字签名技术，即加密算法，包括非对称加密和对称加密算法。非对称加密算法在通信双方不需要交换密钥的情况下就可以建立保密通信，而对称加密算法具有运算速度快的特点，因此，结合 2 种加密算法的数字签名技术保证了物联网设备数据信息在传输过程中的机密性。

散列算法保证了区块链中区块的数据不被篡改，数字签名保证了区块链数据传输过程中的安全性，但是这些都不能保证通信对端的可信任性。区块链中使用的数字证书机制可以用来检验通信对端的身份。网络中的权威机构（CA，certification authority）为厂商签发数字证书，任何人都能够很方便地找到权威机构的公钥，使用权威机构的公钥可以得到通信对端的公钥，然后可以验证对端的数字签名。这种方式确认了通信对端的身份，能够保证物联网应用中可信的人有权限看到可信的数据，或可信的实体有权限操控其他实体。

2.4.2 违规设备的监管

一个物联网设备的标识关联了这个设备在运输和使用过程中的许多环节，通过标识可以查询到与该设备相关的所有信息，这正是利用了区块链的可追溯性，实现了物联网中的溯源问题，如食品溯源、药品溯源。另一方面，如果一个设备是由多个小设备组合而成的，则这些设备标识之间就会存在着关联性，当查询任意一个设备的标识时，就可以得到其他相关联设备的信息以及它们之间的关联过程。基于这种特点，可以防止和发现物联网中伪设备的存在。这里的伪设备是指没有在物联网标识平台注册的设备，或已经注册但是在使用过程中超出注册时约定权限的设备。

以无人机为例，一个厂商生产的无人机，组合了多个零部件，这个厂商在物联网标识平台注册时，这些部件都得到了唯一的标识，而且这些标识之间具有关联性。如果是假冒无人机，则零部件的组合与正规厂商不一样，通过对零部件的查询，就得不到标识之间的关联性，从而可以发现是假冒无人机。另一方面，当一台合法的无人机在物联网平台注册后，该无人机的飞行区域、速度等参数也会被约定下来，这些约定被写入智能合约中，当无人机违背合约时，会按照智能合约中的规定做相应的处理。因此，基于区块链的物联网标识可以规范物联网设备的使用。

3 应用场景分析

智慧家庭中包括多种行业的应用，例如，智能家电、智能能源、智慧安防、智能家居等，为用户提供智慧家庭服务就是把家庭中各种设备/环境数据和人们生活经验数据有机地结合起来。为解决该应用中存在的不同厂商、不同标识体系设备之间的互联互通，下面，将采用基于区块链的物联网标识映射模型建立智慧家庭应用原型，系统模型如图 5 所示。

3.1 煤气查询

假设小明在家里用手机上的物联网设备客户端软件扫描智能煤气表上的物联网设备标识，于是一个解析请求消息通过家庭网关发送给物联网标

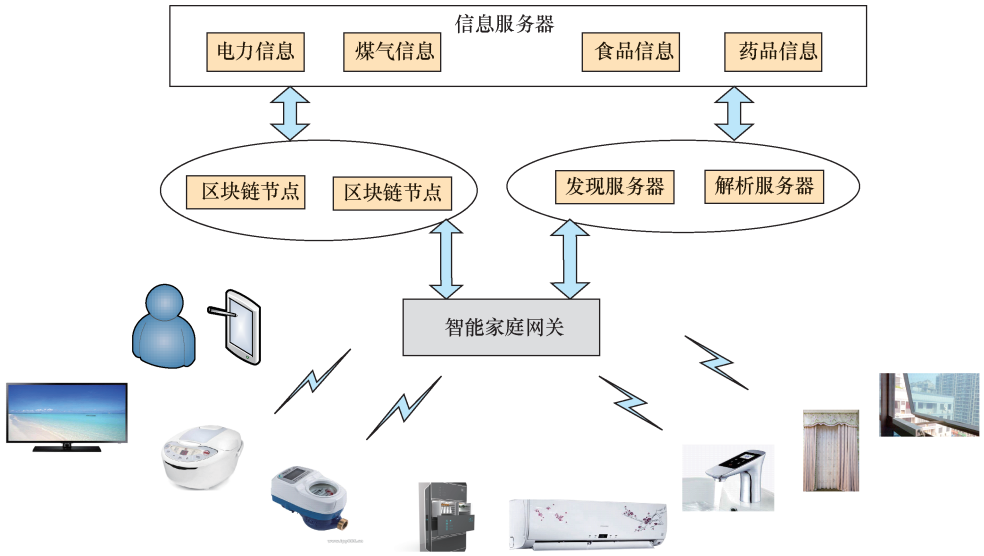

图 5　智慧家庭应用

识平台的解析服务器，请求解析该智能煤气表的标识号码{BCNS_ID$_{gas}$}。解析服务器收到该解析请求后，查找到与该标识对应的发现服务器的地址，于是转发该请求给发现服务器。发现服务器接收到该解析请求消息后，查找到与该标识对应的信息服务器的地址。然后，发现服务器发送请求给区块链网络，要求对小明和信息服务器的身份进行认证，认证通过后，区块链网络发送解析请求消息给刚才的信息服务器。信息服务器用{BCNS_ID$_{gas}$}查找记录，找到了该智能煤气表的读数等信息并返回给小明。

以上信息查询过程可以简化，例如，小明扫描过几次煤气表的标识后，家庭网关可存储下该煤气表的信息服务器的地址，解析请求消息不必再送到物联网标识平台，但是对于小明和信息服务器身份的认证依然要去区块链网络进行。当小明订购了煤气表信息推送业务时，煤气公司的信息服务器会在规定的时间经区块链网络认证后，将小明家煤气相关的信息推送给小明。

以上信息查询过程可以推广到家庭中对于智能设备的控制，例如，远程控制电视机、远程控制电饭锅。与以上过程的区别是，不在家里的小明，在手机客户端上点击家里的电视机/电饭锅后，启动类似以上的解析过程；当从信息服务器器获取到{BCNS_ID}的信息时，信息是该设备的控制功能菜单界面，小明可以在这个界面中远程控制家里的电器。当然，家里电器的控制功能需要在注册这个电器时，使用前文所述的注册过程，将这些功能写入信息服务器，相应的数字摘要写入区块链节点中。

3.2　物联网设备间互动

家里各种物联网设备都有标识，包括家里的烟雾、煤气、温湿度传感器、智能窗户、家庭网关等，这些设备的标识都通过厂商在物联网标识平台注册，而且这些传感器采集到的信息或执行的动作等情况也会写入信息服务器，相应的数字摘要写入区块链网络中。

当厨房的煤气浓度超标时，数据上报给智能网关，智能网关会通过注册流程把信息保存在信息服务器和区块链节点中。同时，智能网关会判断出煤气浓度超标这个事件，接下来会启动打开厨房窗户的操作，这个操作需要智能网关取得厨房智能窗口的控制功能，然后进行操作。于是，智能网关向标识平台发送请求对智能窗户标识{BCNS_ID$_{kitchen_window}$}进行解析，该智能网关和智能窗户经过区块链网络进行认证后，智能网关获得了智能窗口的信息，包括对窗口可以进行的操作。于是智能网关控制窗口打开，解除了家庭煤气中毒的隐患。

以上流程也可以简化，例如，智能网关就是信息服务器，经过身份认证的物联网设备在一段时间内不需要重复到区块链进行网络认证，相应的信息在智能网关中缓存。这种情况下，家庭设备间互操作的实时性大大提高，可以实现本地服务的快速发现和提供。

4　结束语

物联网的安全涉及多个方面，本文从物联网标识角度出发，首先提出了基于区块链标识的物联网

体系架构，包括设备层、接入层、控制层、内容层和应用层，区块链技术和标识相关服务器主要位于控制层；然后给出了一种基于区块链的物联网标识编码方法，该标识方法兼容已有异构物联网编码标准，将设备标识保存在区块链上，保证了标识的唯一性和完整性。本文所提各功能模块在具体实现过程中，可以根据需要设置在网络的不同位置。本标识在使用过程中，通过区块链网络的身份认证、数据安全传输、数据的完整性以及智能合约技术，实现了设备可信的人或实体可以获得可信设备的信息或操作权限，加强了物联网的隐私与安全保护。

参考文献：

[1] ITU-T-REC-Y. Overview of the Internet of things[S]. 2012.

[2] VERMESAN O, FRIESS P, GUILLEMIN P, et al. Internet of things strategic research roadmap[J]. Information Security & Technology. 2014, 29(16): 300-304.

[3] 王平泉, 罗红, 孙岩. 面向物联网的多元标识映射模型[J]. 中国科学: 信息科学, 2013, 43(10): 12440-1264.
WANG P Q, LUO H, SUN Y. Mapping model of multi-identifers oriented to Internet of things[J]. Scientia Sinica Informationis, 2013, 43(10): 1244-1264.

[4] 刘阳, 李馨迟, 田野, 等. 物联网名字服务关键技术研究[J]. 电子学报, 2014, 42(10):2032-2039.
LIU Y, LI X C, TIAN Y, et al. Research on key technology of name service for the Internet of things[J]. Acta Electronic Sinica, 2014, 42(10): 2032-2039.

[5] 高云全, 李小勇, 方滨兴. 物联网检索技术综述[J]. 通信学报, 2015, 36(12): 57-76.
GAO Y Q, LI X Y, FANG B X. Survey on the search of Internet of things[J]. Journal on Communications, 2015, 36(12): 57-76.

[6] EPCglobal. The EPCglobal architecture framework[S]. The EPCglobal Standards Development Process, 2007.

[7] EPCglobal. EPCglobal object name service (ONS) 2.0.1[S]. The EPCglobal Standards Development Process, 2013.

[8] KOSHIZUKA N, SAKAMURA K. Ubiquitous ID: standards for ubiquitous computing and the Internet of things[J].IEEE Pervasive Computing, 2010, 9(4): 98-101.

[9] POETER E P, HILL M C, BANTA E. R, et al. Ucode 2005 and three post- processors computer codes for universal sensitivity analysis, inverse modeling, and uncertainty evaluation[R]. US Geological Survey Techniques and Methods Report TM, 2005:6-11.

[10] NIDA. Mobile RFID code architecture[S]. 2013.

[11] 中华人民共和国商务部. 商务领域射频识别标签数据格式[S]. 2010.
Ministry of Commerce of The People's Republic of China. Commercial radio-frequency identification tag data format[S]. 2010.

[12] 中国互联网络信息中心. 物联网标识管理公共服务平台接入说明[S]. 2012.
China Internet Network Information Center (CNNIC). The access description for the management public service platform of the Internet of things logo[S]. 2012.

[13] FABIANO N. The Internet of things ecosystem: the blockchain and privacy issues. the challenge for a global privacy standard[C]//2017 International Conference on Internet of Things for the Global Community (IoTGC). 2017: 1-7.

[14] 邹均, 张海宁, 唐屹, 等. 区块链技术指南[M]. 北京: 机械工业出版社, 2016.
ZOU J, ZHANG H N, TANG Y, et al. Blockchain technology guide[M]. Beijing: Machinery Industry Press, 2016.

[15] 田野, 袁博, 李廷力. 物联网海量异构数据存储与共享策略研究[J]. 电子学报, 2016, 44(2):37-46.
TIAN Y, YUAN B, LI T L. A massive and heterogeneous data storage and sharing strategy for Internet of things[J]. Acta Electronic Sinica, 2016, 44(2): 37-46.

[16] 王继业, 高灵超, 董爱强. 基于区块链的数据安全共享网络体系研究[J]. 计算机研究与发展, 2017(4):742-749.
WANG J Y, GAO L C, DONG A Q. Block chain based data security sharing network architecture research[J]. Journal of computer research and development, 2017(4): 742-749.

[17] POLYZOS G C, FOTIOU N. Blockchain-assisted information distribution for the Internet of things[C]//2017 IEEE International Conference on Information Reuse and Integration (IRI). 2017: 65-78.

[18] CHA S C, CHEN J F, SU C H, et al. A blockchain connected gateway for BLE-based devices in the Internet of things[J]. IEEE Access, 2018(1): 1-10.

[19] SAMANIEGO M, DETERS R. Internet of smart things-IoST: using blockchain and CLIPS to make things autonomous[C]//2017 IEEE International Conference on Cognitive Computing (ICCC). 2017: 9-16.

[20] LI C, ZHANG L J. A blockchain based new secure multi-layer network model for Internet of things[C]//2017 IEEE International Congress on Internet of Things (ICIOT). 2017: 33-41.

[作者简介]

陈美娟（1971-），女，博士，南京邮电大学副教授，主要研究方向为异构无线网络资源管理、区块链技术、SDN/NFV 技术等。

朱晓荣（1977-），女，南京邮电大学教授、博士生导师，主要研究方向为下一代无线网络、物联网等。