基于区块链的物联网域间认证方案

Abstract:

According to the definition of the European Internet of Things Research Group (IERC), the Internet of Things is a global dynamic network infrastructure with self-configuring capabilities. The Internet of Things consists of entities with independent functions and networks that connect them. Objects in the Internet of Things are assigned IP addresses, which can automatically send and receive information from and to the network. Network-based technologies can be used to derive a variety of applications. Early IoT applications usually communicated between objects on a smaller scale, often because of the limitations of equipment and communication technology, and the quality of service is low; Data processing Real-time communication between objects generates and uses massive amounts of data and uses cloud servers for data storage, resulting in cross-domain applications such as smart cities, smart healthcare, and car networking. The functions of IoT applications become more powerful as demand grows, communication between objects becomes more complex, and cross-domain communication becomes the norm. Real-time communication between objects, real-time data access between objects and cloud servers requires secure and reliable signature technology to support mutual recognition. The identity-based encryption system IBC provides a reliable encryption communication and signature technology, but still has its limitations. In the context of big data and cloud data, inter-domain communication requires a more credible and feasible signature technology. In inter-domain communication, the encryption algorithms used in inter-domain communication may have different secret keys, which may result in the failure to complete inter-domain communication. The trusted third-party authentication center CA that distributes certificates is difficult to choose in cross-domain Internet communication. A blockchain can be defined as an unalterable book of recorded transactions that is maintained by multiple nodes that are not trusted by each other in the network. Each node is responsible for maintaining a record of the ledger. These nodes perform a consistent contract to validate the transactions and aggregate them into chunks to build a hash chain of chunks. The blockchain with zone-centricity has the potential to support inter-domain communication, and it is possible to securely store, update, and distribute the materials required for signatures. This paper will discuss the practical value of inter-domain communication and introduce an inter-domain communication signature scheme based on blockchain technology. This blockchain-based cross-domain signature system is transparent to nodes within the domain, and implements signature functions through the materials required for signatures stored on the chain and the hierarchical proxy server.

摘要:

根据欧洲物联网研究集团（IERC）的定义，物联网是有自我配置能力的全球动态网络基础建设。物联网包含具备独立功能的实体和连接它们的网络，物联网中物体被各自分配 IP 地址，可以自动从向网络发送信息和从网络中接受信息。基于联网技术可以衍生出各种应用，早期的物联网应用通常是在较小范围内的物体间通信，往往因为设备和通信技术的局限性高成本而服务质量低下； 新一代的物联网利用大数据处理物体间实时通信产生和使用的海量数据并采取云服务器进行数据存储，产生了诸如智慧城市、智慧医疗、车联网等跨域应用。物联网应用的功能随需求变得愈发强大，物体间的通信也更为复杂，跨域通信成为常态。物体间实时通信，物体和云服务器之间实时的数据存取需要安全可靠的签名技术为相互识别做支撑。基于身份的加密系统 IBC 提供了一种可靠的加密通信和签名技术，但仍然有其局限

性。大数据、云数据的环境下，域间通信需要可信度更高，可行性强的签名技术。域间通信时，各域间通信所采用的加密算法可能不同秘钥不同等问题导致域间通信不能顺利完成；分发证书的可信第三方认证中心 CA 在跨域的互联网通信中难以抉择。区块链可以被定义为不可更改的记录交易的账本，这种账本只要网络中多个相互不信任的节点来维护的。每个节点都负责维护账本的一份记录。这些节点执行一致的契约以验证交易，并把它们聚成区块，建立区块的哈希链。具有区中心化的区块链有支持域间通信的潜能，可以安全地保存、更新、分发签名所需的材料。本文将讨论域间通信的实际价值并对一种基于区块链技术的域间通信签名方案做介绍。这种基于区块链的跨域签名系统对域内的节点透明，通过在链上保存的签名所需材料和分层的代理服务器实现签名功能。

关键词： 物联网 区块链 IBC 跨域认证

第 1 章 介绍

物联网（IoT）指的是在日常生活中围绕人们的物体具有通信，计算，传感和驱动能力的场景。 给与人类生产生活相关的物件安装智能芯片或嵌入式系统，并使成为有通信功能的智能传感器，这些传感器通过专有的网络交换采集的信息，计算和存储数据，从而为人类活动提供高效率的服务，这些联网的智能传感器以及它们通信的网络共同组成了物联网。这些智能的传感器和物体通常被称为“智能对象”，它们能够通过无线技术彼此通信，以便为人和其他智能对象提供具有高价值和合作服务。物联网提供的服务的复杂程度和嵌入了智能芯片的物件的计算能力和处理的数据的。早期的物联网只是简单把两个设备用信号线连接在一起，在大量应用程序中设想和考虑的经典物联网场景是静态的和封闭的。这种情况下物联网中的物件进行简单的计算，涉及的数据较少，因此提供的服务是有限的。由于通信技术和芯片技术的发展，智能芯片的数量和计算能力通信能力和以往不可同日而语，物联网提供的服务也在不断进化。新一代应用程序的特点是数字领域与物理世界的更高程度的集成[1]。 这种趋势在智能物体环境的逐步部署，具有传感和驱动能力的物理器件增加的背景下变得明显。 物联网的应用场景的也从智能城市到智能家居，从工业 4.0 到基础设施监控，从电子健康到汽车，提供的服务多种多样，涉及的设备更加丰富。 除此之外，为个人提供的物联网服务也具有极大商业价值，如通过智能手机或智能平板电脑获取物联网服务，又或是联网的可穿戴设备作为物联网设备为使用者提供有价值的信息，人们与网络的物理系统连续交互的方式变得多样。一个典型的物联网服务实例是：为驾车出行者提供便捷出行方案。驾驶员通过连网的汽车给出该汽车想要抵达的新的城市，以获取规划好的路径和在目的城市的停车地点。为此汽车必须与城市当地服务提供商互动。这整个过程涉及多样数据的处理，例如在此过程中驾驶员可能希望找到一个停车位，该停车位需要靠近他现在的位置并且价格合理。为此，汽车需要与城市运输公司或其他停车场管理人员就位置，价格，车辆类型和停留时间等参数进行协商，以确保得出最令人满意的权衡取舍，并自动达成协议。由于车位的信息和车辆的位

置信息通常是动态变化的，提供通信的网络必须能支撑实时通信。在同一时间可能会有多辆汽车试图访问某个停车场的车位信息，同时如果车辆向第三方寻求数据，第三方可能提供来自不同停车场的数据，为避免不必要的纠纷，这一过程中的所有角色需要能识别彼此身份。同其他任何的数字通信一样，物联网中的域间通信会遭受到攻击，如果通信对象被冒充或消息被劫持、更改，极有可能对交互双方甚至更大范围的对象造成损失。另一方面，汽车也可以向数据中心提供信息，例如它的出发城市和随后的路线，数据中心可以利用这些信息可建立有用的统计数据，用于制定增加来自某些区域的游客数量的战略计划。值得注意的是，当汽车第一次进入城市时，它以前从未见过停车场供应商，甚至不知道如何联系他们。从城市旅游局的角度来看这台汽车同样是陌生的。因此，允许找到合适的服务提供商并确保服务提供商（以及服务消费者）是他声称的人以及谈判技术的机制是该类应用的必要技术基础。汽车和供应商在相互传递数据之前必须先相互识别，这意味着供应商知道这辆汽车的具体身份，通过这个身份判断是否向汽车发送消息和消息的具体内容，同样汽车也需要确认自己获得的消息来自它希望的供应商，否则它可以拒绝这条消息。这正是数字签名将要完成的工作。在通信中 PKI 和由其演化而来的 IBC 系统可以提供有效可靠的签名系统，对于传统的物联网，消息传输范围还在固定域内，IBC 仍然是可行的。一个传统的物联网模型，由于它所提供的服务有限，通常通信可以在某个通信域内完成，但在如上例所提到模型中，仅有域间通信显然不能满足需求。事实上，伴随物联网将提供的服务的复杂化，物联网中的数据交互将更加频繁涉及的对象也会倍增，域间通信将成为必要，不可避免的。例如在上述的例子中，汽车是所去往的城市是不确定的，它所在的通信域和目的城市中的传感器及数据中心所在的域是不同的，当它们之间交换数据，就产生了域间通信。采用 IBC 技术进行域间通信的签名的不安全因素是，IBC 技术依赖于 CA 体系，而 CA 体系静态、树状的特点往往不符合物理世界的需求，因此复杂的管理容易造成错误，同时树状体系中某一节点所覆盖的节点将会受到此节点的影响也对域间签名带来不稳定因素，具体讲在后文介绍。而区块链去中心化的特点能很好地回避以上提及的缺陷，可以作为一种可行的域间通信签名设计方案的基础。本文在第二节将介绍物联网域间签名的相关概念，IBC 作为一种可行的域间签名方法将被着重介绍。在第三小节将介绍针对物联网域间通信的签名已有系统和模型，具体是指双层的 IBC 处理域间签名的方法，将提出现有技术存在的问题和不足。第四部分包含第四、第五节，将提出一种基于区块链的域间通信数字签名技术，并分析这一设想的模型探究其可行性和价值。第五部分将回顾三、四部分，对比不同的方案，对物联网域间通信签名做出总结。

第 2 章 域间通信的数字签名

2.1 域间通信

本文中所提及的“域”是通信域，可看做一个局域网，一个局域网内可以有零到多个通信设备。这种局域网是虚拟局域网，它的划分并不严格按照物理距离和联系进行，考虑到物联网

应用通常是提供某种服务，域的划分更多地参考信息交互对象所扮演的角色和交互需要达成的目的或实现的功能。例如学校内某个校区的教学设备是在同一个域内的，师生通过手机或平板等移动设备访问教学设备，手机和平板却不一定接入校园网，可能采用其他运营商提供的服务，根据运营商的不同，这些移动设备又可以划分在不同的域内。用户通过手机远程遥控智能家电，手机所在的域和智能家电所在的域是不同的，为了使它们能够通信首先需要让它们彼此能够识别对方，否则将难以提供准确实时的信息和存在严重的安全漏洞。在局域网内，通信设备的数量有限，因此设备之间一对一的识别对网络和算法的要求相对容易满足。在物联网的背景下，每个域内都会存在大量的通信设备，域的数量、名称也可能动态的变化。如何识别不同域，如何识别其他域内的通信设备以保障通信安全进行将成为必须探讨的课题。物联网域间通信本质和域内通信相似，但通信设备的数量和种类剧增必然增加处理过程的复杂度会大幅增加。

2.2 数字签名

为了了解数字签名技术，首先引入几个概念。

非对称加密：非对称加密的原则是通信双方遵从公钥加密，私钥解密，其中一个密钥用于加密，另一个密钥用于解密，公钥和私钥组成钥匙对。因为公钥是公开的，如果用来解密，所有人都可以解密消息，极不安全，因此发送消息采用公钥加密、私钥解密。 签名过程则要求产生一段只有签名者可以产生的独有字符串，而他人能识别字符串是否由签名者产生，采用私钥加密、公钥解密。 同时，私钥也可以认为是个人身份的证明。通信双方想要互相发送消息，需要建立两套非对称加密的机制（即要产生两对公私钥密钥对），发消息的一方使用对方的公钥对消息进行加密生产密文，接收消息的一方则使用自己的私钥解密密文恢复得到明文。 需要注意，通信的成员每增加一，非对称加密机制至少要增加一套，在某些情况下， 多人通信中两两之间可能都有两套加密机制，这可能带来巨大不便和浪费。

消息摘要：消息摘要的功能是将消息通过哈希算法转换成一个拥有固定长度值的唯一的字符串。 值唯一的意思是不同的消息转换的摘要是不同的，如果确定了消息，通过同一哈希算法应当得到相同的哈希值。哈希的过程是单向的、不可逆的，即即使攻击者截获了摘要也不能通过摘要反推明文。 利用这一特性，可以验证消息的完整性。非对称加密算法和消息摘要算法可以完成数字签名。假设现在有通信双方分别为 A 和 B，两者之间使用两套独立的非对称加密机制（A 的公私密钥和 B 的公私密钥），A 向 B 发送消息数字签名的过程如图 1：

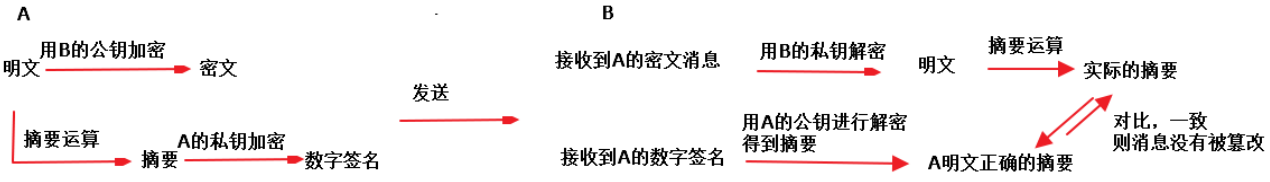


图 1

在通信开始前，A 和 B 应当提前获得了对方的公钥。A 首先用 B 的公钥加密明文 C 获得密文 M，然后通过对 M 采取哈希算法，摘要运算得到一条摘要，这条摘要记为 Z1,A 用自己的私钥加密 Z1，加密得到数字签名。A 将密文和这条密文的数字签名拼接，一并发送给 B。 B 收到 A 加密过的的消息后，先将密文 M 用自己的私钥解密，得到明文 C。 只有拥有私钥的 B 可以正确得获得明文，第三者是无法解密消息的。 对这条明文 B 也用同样的算法进行摘要运算，得到的结果摘要 Z2，由于摘要运算是唯一的，Z2 应当与 Z1 完全相同。 B 将和密文一并发送来的数字签名用 A 的公钥进行解密还原得到摘要 Z3，如果 Z3 和 Z2 比对后一致，说明消息完整性得到保障（消息没有被篡改）。值得注意的是，摘要使用 A 的私钥加密且假设 A 的私钥保存安全没有他人能获取，因为摘要是不可逆推出原文的，如果被拥有 A 的公钥的第三者截获，也不会对安全造成威胁。

2.3 IBC 技术

上文简要介绍了通信网络中两个个体间的数字签名，而实际应用中，通信过程是在多个个体间相互进行的。为了保障通信有序进行，必须对非对称加密机制中的公私钥对有效的系统的管理。

2.3.1 PKI 体系

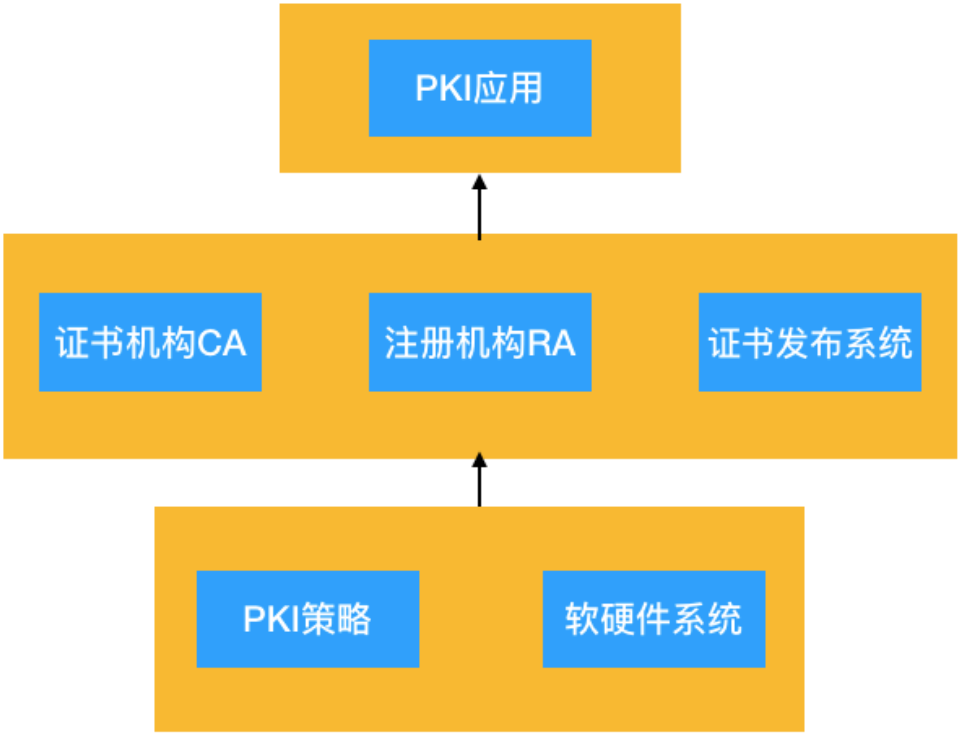


图 2

公开密钥基础设施 PKI(Public Key Infrastructure)是以非对称加密技术为基础的被普遍应用的的安全基础设施，它的目的是数据机密性、完整性、身份认证和行为不可抵赖性。美国学者在 20 世纪 80 年代提出了 PKI 的概念。PKI 提供安全服务包括身份认证、身份识别、数字签名、加密等。PKI 中最基本的元素是数字证书，包括数字签名在内所有安全操作都主要通过证书来实现。 一个典型的 PKI 系统如图 2 所示。

系统的顶层是它所提供的应用。 系统的底层是 PKI 策略和软硬件系统。 软硬件系统是系统内设备的物理设施和搭配的软件的规范。PKI 安全策略是根据应用和通信设施制定的最基本的这个系统信息安全方面的指导方针，同时也将定义密码系统使用的处理方法和原则。策略的内容包括系统怎样密钥对和其他有价值的信息的方法（如密钥对将如何保存），制定风险的级别的判断标准和定义安全控制的级别。

中间层和关键的证书相关，包含认证机构 CA，登记机构 RA 和电子目录，认证机构负责签署证书而登记机构批准证书签署，电子目录中存储这些证书也负责发布这些证书。证书机构 CA 是 PKI 信任的核心，它管理通信使用的公钥，负责产生、发放和销毁这些公钥，它的具体工作是规定证书有效期、发放证书、在有效期后和特殊情况下通过发布证书废除列表（CRL）废除证书。注册机构 RA 向用户提供和 CA 之间的一个接口，它获取并认证用户的身份，向 CA 提出证书请求。注册机构并不能向用户签发证书，只是对用户进行资格审查。它主要完成收集用户信息和确认用户身份的功能，并不是必要的，在用户数量较多的情况下可以分担 CA 的压力。用户可以通过自己或目录服务器请求发放证书。目录服务器可以是一个组织中现存的，也可以由 PKI 方案提供。在通信开始之前的部署阶段，CA 首先产生自身的私钥和公钥（规定密钥长度至少为 1024 位），然后生成数字证书，并且将数字证书传输给安全服务器。 在这一体系下，任何两方之间的身份认证都需要通过 CA，因为 CA 管理着公钥。 如图 3，某个域内的实体 A 有向另一实体 B 发送消息的事务请求。 A 首先向 CA 请求它自己的证书，通过验证 CA 将证书发给 A，之后 A 告知 B 需要获得 A 的公钥， B 向 CA 请求 A 的公钥， CA 在核对证书后发送公钥给 B， B 则可以使用 A 的公钥加密消息了。PKI 体系的部署是一个复杂的过程,通信过程中存在大量证书交换，证书的存储耗费资源。

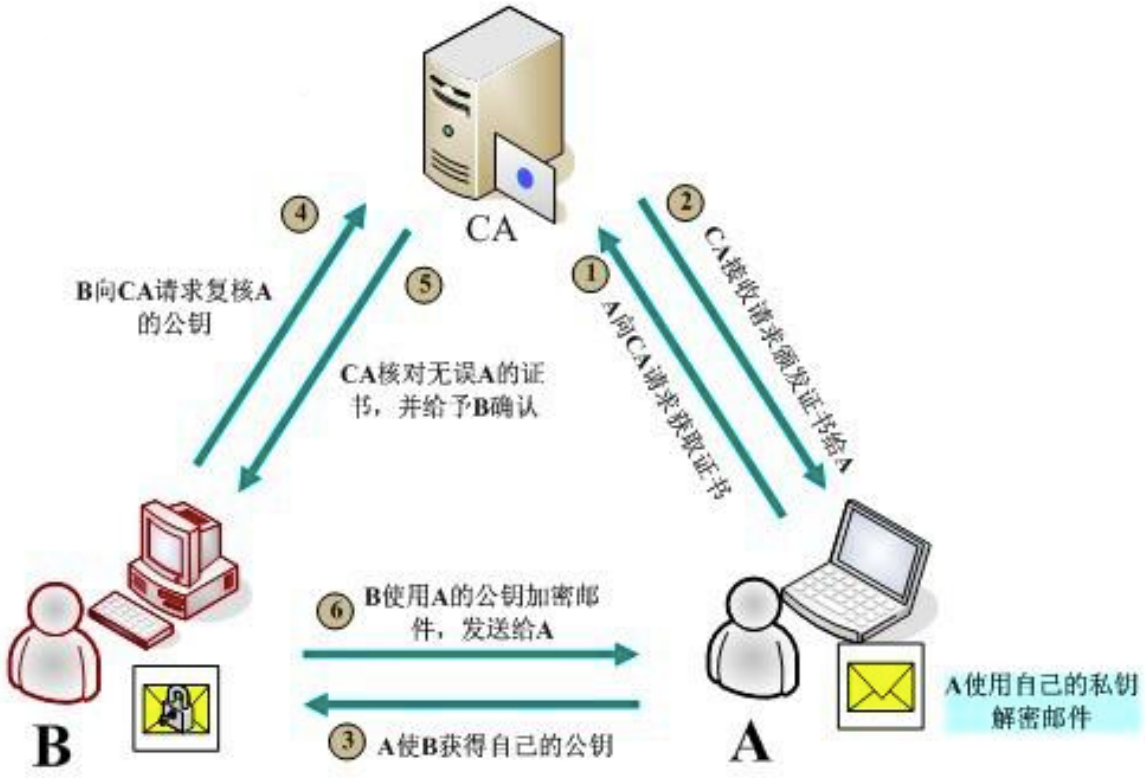


图 3

2.3.2 IBC 体系

现在广泛应用的加密方案和签名方案是基于身份的[1, 2]。基于标识的密码技术 IBC(Identity- Based Cryptograph)是在传统的 PKI(公开密钥基础设施)基础上发展而来，它的主要成就第降低了 PKI 安全应用在部署和使用上的复杂度，避免了安全应用中产生的大量数字证书交换。而在 IBC 中，每个人的公钥就是他的身份标识，常见的身份标识有 email 地址，电话号码等，用户自己掌握私钥，因此密钥管理相当简单，可以很方便的对数据信息进行加解密。 IBC 方案中的随机数和密钥的安全性均是基于椭圆曲线上的离散对数难题， 因此基于 IBC 模型的方案都是可计算安全的。在物联网系统中，也可以给每个传感器分配一个专有的名称作为其身份标识。先是 Shamir[3] 提出基于身份的密码体制的思想，直到 2001 年 Boneh 和 Franklin 提出了一个实用的基于身份的加密方安 IBC[4] 。 这一方案的特点是让身份信息充当标识符，简化了存储和计算。

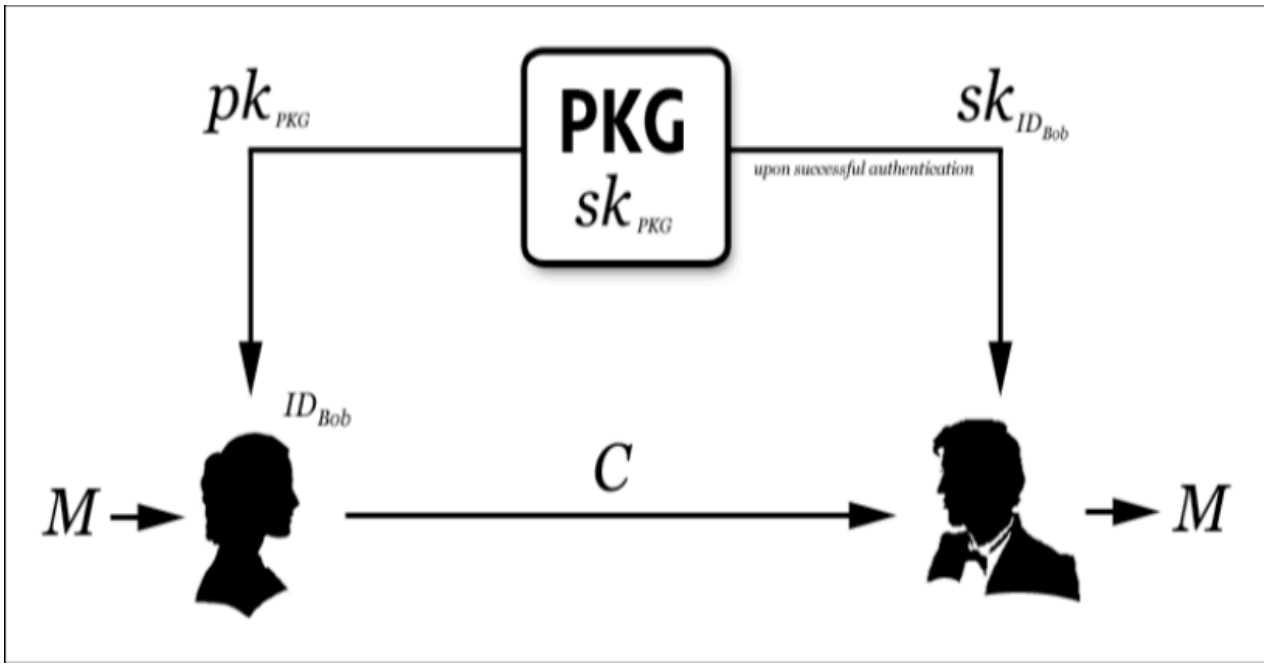
基于 IBC 的加密和解密过程如下:

1）Alice 为鲍勃准备明文消息 M。她使用 Bob 的身份 IDBob 和 PKG 公钥 pkPKG 加密 M，得到密文消息 C。然后 Alice 将 C 发送给 Bob。请注意，在开始加密之前，Alice 已经知道 IDBob 和 pkPKG，因此，她不需要事先协调或准备 Bob 的部分来加密给他留言。

2）Bob 从 Alice 那里收到 C。 Bob 通过 PKG 进行身份验证，基本上向其发送 IDBob 属于他的足够证据，PKG 通过安全通道将 Bob 的私钥 skIDBob 传送给他。例如，如果 IDBob 基于

电子邮件地址，PKG 可以向该电子邮件地址发送一个没有内容的消息，成功返回该 ID 可能提供可接受的证明，即 IDBob 的所有者是与 PKG 联系的人。该随机数可以通过 SSL 超文本链接返回，该链接向 Bob 提供用于下载其私钥的安全链接。

3）Bob 使用他的私钥 skIDBob 解密 C 以恢复明文消息 M。



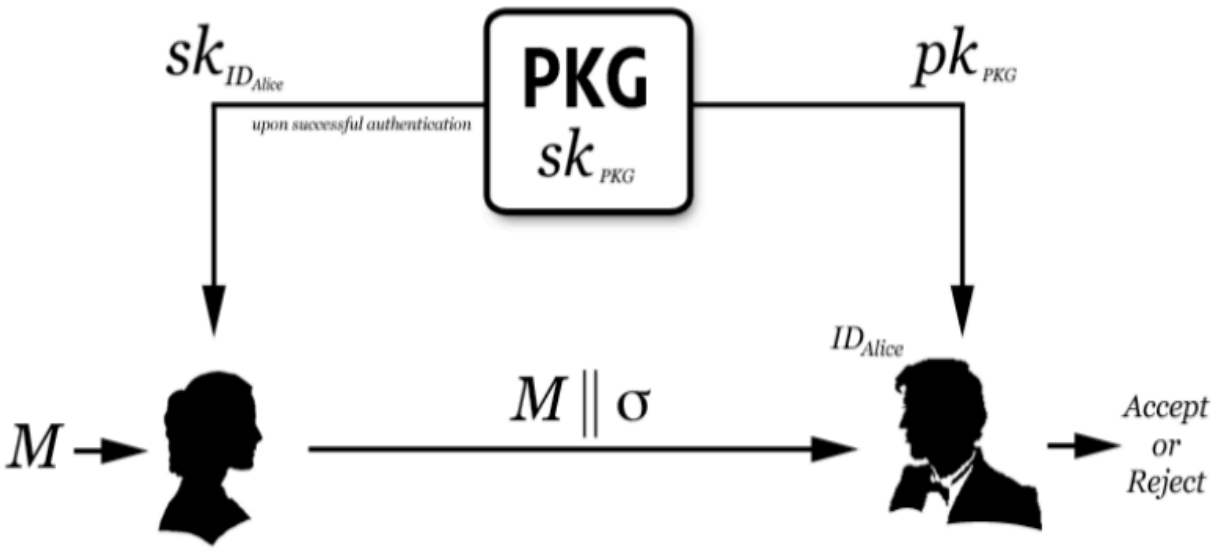
基于身份的签名（IBS）本质上是加密过程的镜像：

1）Alice 使用 PKG 进行身份验证并接收她的私钥 skIDAlice。

2）使用她的私钥 skIDAlice，Alice 为 M 生成签名 σ 并将其发送给 Bob，有时还有上面加密的消息 C。

3）在从 Alice 收到 M 和 σ 后，Bob 检查 σ 是否是 M 使用的真实签名

Alice 的身份 IDBob 和 PKG 的公钥 pkPKG。 如果是，他返回“接受”。 否则，他返回“拒绝”。 注意，Bob 不需要为 Alice 提供任何类型的证书。



IBC 淘汰了 PKI 体系中的数字证书也无需证书颁发机构 CA，使用简单，部署方便，是在用户数量巨大的情况下能更好的适应尤的安全系统；又由于无需 PKI 中证书验证等计算过程，具备较低的计算代价，适用于手机终端等小型设备或嵌入式系统；部署方便计算简单的特点使得 IBC 是适应物联网通信。在域内通信中 IBC 可以满足安全需要，域间通信可以采用二级 IBC 的系统（即域内实体用 IBC 进行认证，域之间的认证也采用 IBC），这种方案可行但存在较大安全隐患。

第 3 章　物联网域间通信

3.1 物联网安全需求

物联网引入有计算和存储功能的设备和连接它们的网络使得物与物通信，人与智能设备间交互成为可能。多年来，连接到互联网的设备数量呈指数增长。2015 年，在超过 150 亿台设备中，超过 230 亿台设备连接在一起。据估计，到 2020 年这一数字将超过 300 亿大关，预计到 2025 年将有超过 750 亿台设备连接到互联网[5]。 这一增长使许多物联网服务成为可能，也对物联网通信的安全作出考验。 为保障消息传输和计算按照使用者所期待的方式进行，物联网的搭建有基本的安全需求。物联网安全体系按照普遍认同的架构分为以下三层 : 感知层，即由二维码、智能传感器、GPS 设备等设备组成用于数据采集、物体识别的物理层。网络层，该层主要是结合通信技术通过传感器将信息通过互联网传送到上一层，网络层的主要工作是将感知层感知到的信息传递给远端如云计算存储器和大数据中心进行应用。

3.2 跨域认证方法

终端节点是物联网的重要组成部分，所以传感网络中的信息加密和数据传输安全，是物联网体系的发展中很受关注的内容。在物联网的服务中，终端设备不一定是有足够容量和电量的设备，同时可能还要承担其他的计算任务，比如智能手环，它的主要芯片将和传感器通常用于测量身体和运动的数据，网络功能不能占用过多的资源。为满足无线传感网络的低功率传输要求，利用终端节点将 无线传感器网络集成到网络中的常见的方法有基于云的集成[6，7]、前段代理的集成和通过因特网通信协议的集成[8，9]。满足传输要求的基础上，跨域认证的安全由域内认证安全和域间认证安全两部分组成。

网格环境下，资源的管理以虚拟组织为基本单位，同一个虚拟组织中的网格资源遵守一组共同的管理规范和共享策略。每个虚拟组织形成独立的信任域，资源主体在加入信任域时必须通过域中认证 中心的身份认证，同时也要遵守相同的本地安全管理策略。在域内采用基于身份的认证方案，域内认证机制如图 4 所示。

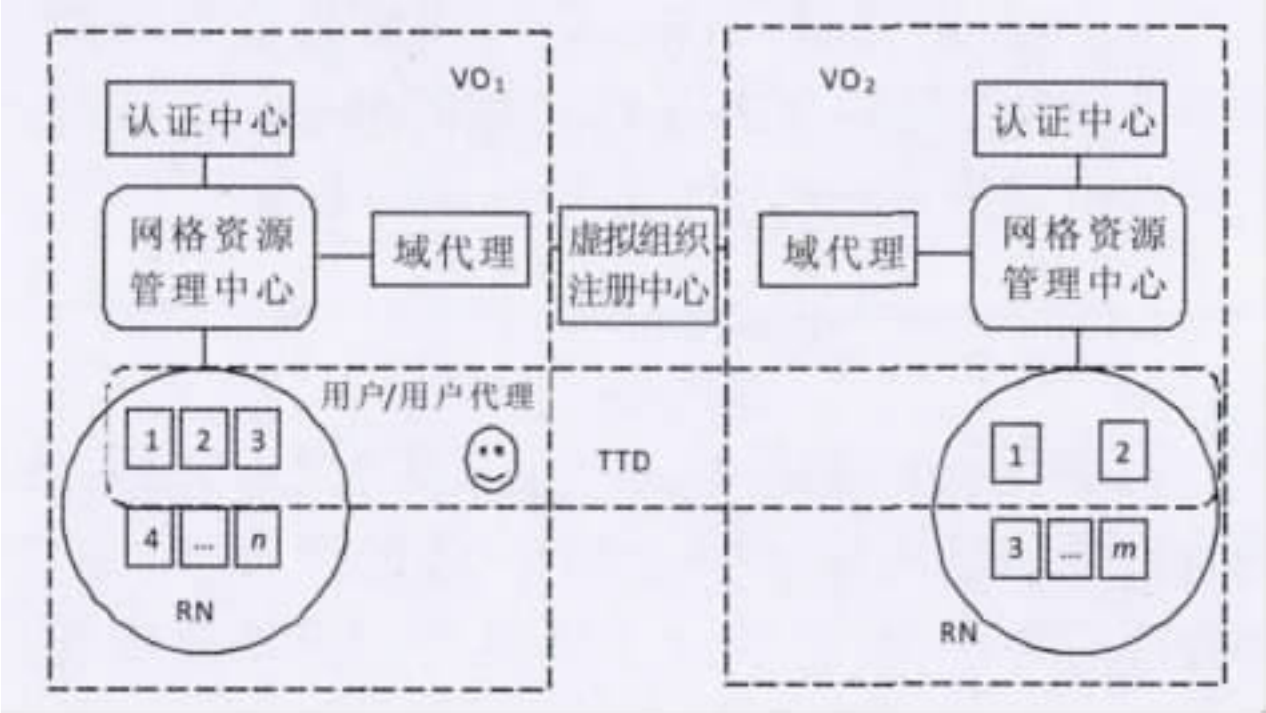


图 3

域内认证过程如下:

1）用户实体向认证中心注册。例如在 PKI 体系中，注册中心 RA 担任这一职能。

2）认证中心产生用户公钥及部分用户私钥，用户私钥最终由用户按照文献[6]的算法得出。在 IBC 系统中用户的标识信息就是公钥，但为了使其他用户能够使用公钥，需要一个可信任的第三方进行公钥的存储和分发。

3）域内用户实体进行双向认证。无论是 PKI 还是 IBC 都可以完成这一过程。

通常情况下，物联网应用中的许多任务需要多个域内的多个实体共同协作才能完成， 例如一次导航过程需要汽车、地图、监控中心等多个角度的器件共同作业，而不同域中的实体之间通信时也必须进行相互认证。 针对这种情况域间认证基于 IBC 的认证方案。域间利用

证书来交换各域的系统参数。使用上述域内和域间认证机制，在网格中，任意 2 个实体在通信前能够进行安全的身份认证，但通常网格中任务规模大且动态变化，需跨越多个自治域的资源间密切协作，并且执行同一任务的多个资源主体之间需要频繁通信，从而使得实体之间的认证过于频繁和复杂，认证效率不高。

为了解决这个问题，引入时信任域 TTD(temp trust-domain) 的概念。TTD 包括用户或用户代理、执行该任务的所有网格资源主体。 用户所在虚拟组织的网格资源调度管理中心负责对 TTD 和其中的资源进行管理。临时信任域的构建图 5 所示.。

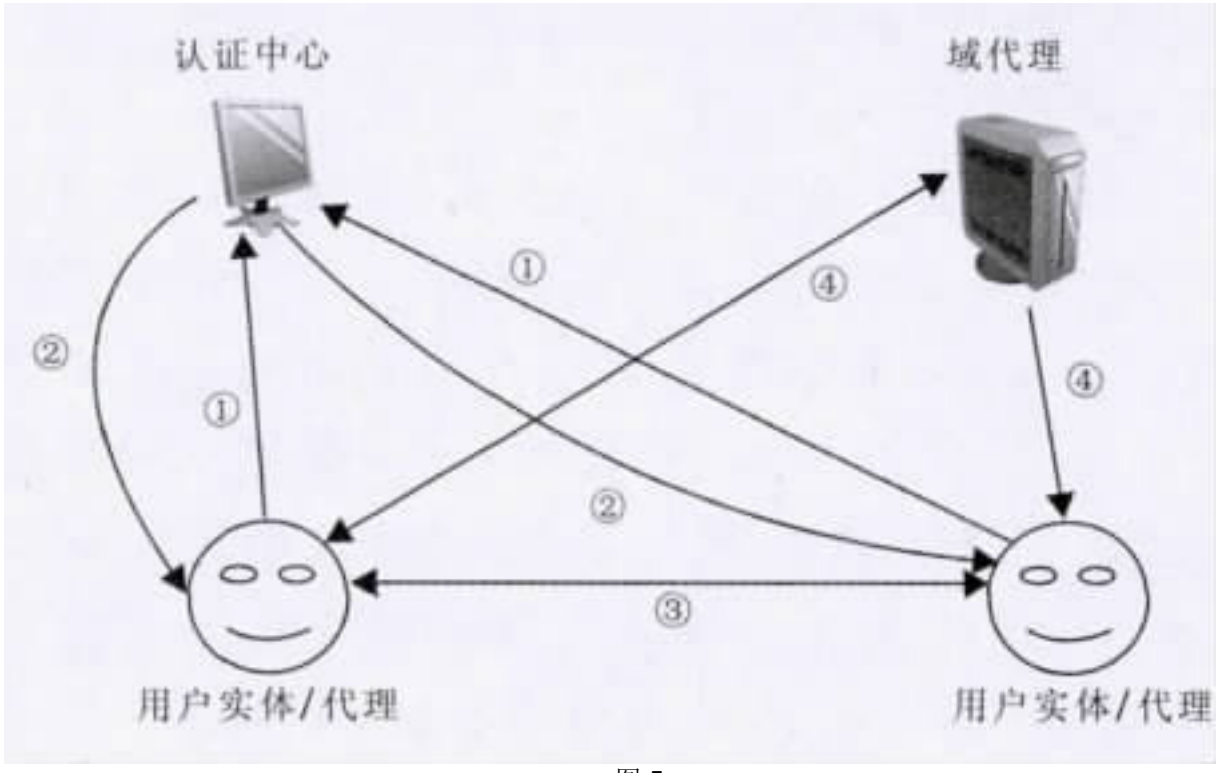


图 5

以手机控制教室内空调为例，TTD 的认证步骤如下:

1) 假设一个虚拟组织，这个虚拟组织中的用户或用户代理利用上文描述的域内认证机制进行身份认证。手机 P 通过运营商提供的虚拟域 VO1 进行认证，VO1 认证 P 的身份。

2) 认证通过后，本地虚拟组织中的用户或用户代理，此处为 P,向 VO1 中的网格资源管理中心提出任务请求，该中心负责查找合适的资源给该任务，如果该中心发现有 n 个资源 $RN=\{R_1...R_n\}$，但依然无法满足该任务需求，就向虚拟组织注册中心查询其他虚拟组织中的资源，假设获得虚拟组织,在此处为校园的局域网， VO_2 中的 m 个资源 $RN=\{R_1\cdots R_m\}$，需要访问的空调是其中一个资源。

3) 利用域间认证机制对用户或用户代理和 VO_2 进行双向实体认证。

4) VO_1 的网格资源调度管理中心在认证通过后，根据资源调度算法对任务进行分配，根据资源分配的结果，用户与本地资源使用域内认证机制进行身份鉴别，对远程资源则运用域间认证机制逐一进行身份认证。

5) 认证通过后，用户用过 VO_1 ，VO_2 域代理获取该资源的声誉，声誉超过规定的门限值，则批准相应资源加入临时信任域· 网格资源调 度管理中心将子任务分配给相应资源并在其上创建相应进程。

6) 根据任务情况，各进程间进行通信时，运行进程的各资源主体，如果在临时信任域内，那么运行进程的各资源主体双方不再进行身份认证。 在任务执行过程中，临时信任域的资源可以随 时增加或离开。

7) 任务执行完成后，临时信任域、撤销。

3.3 采用 CA 体系的域间通信的缺点

如 3.2 中描述，使用 IBC 技术进行跨域认证，认证中心的存在不可跨过。CA 体系的身份标志就就是“数字证书”。CA 体系从根证书开始，逐级签发各级证书，从而形成树状信任体系。在树状体系中，对叶子节点的末端证书追溯，可以很容易地确定用户的唯一身份。但在实际应用中，比起用户身份，他所担任的职能更为重要，这决定了他拥有怎样的操纵数据的权限，而同一个用户可能担任不同的身份。例如，作为终端设备的某台手机，它所绑定的用户可能是某套智能家居的第一用户，可以操控家居中所有的电器和设备，同时他还可以作为某间教室的空调的遥控器，它可以开关空调和调节温度但对一些其他的设置没有访问权限。由于实际应用中的逻辑关系并不像 CA 体系的树状结构，是更为复杂且具有较强动态性的特点，用 CA 系统实现这种真实结构，管理复杂。

假如签名私钥处于永久、绝对安全的状态，数字签名的有效性将是完美的。但实际情况是，用户的私钥可能由于各种各样的原因而失效，甚至是人为让它失效。理论上来说，一旦私钥失效，与之相关的签名都不再具有不可否认性。如果使用时间戳技术，签名私钥失效的问题可以得到解决，但时间戳要求用户永久在线，又造成资源浪费和使用不便.

随着结构体系的扩充，CA 的管理难度和应用风险将进一步增大。之前已经说明，CA 体系是一种静态的树状体系。CA 以静态、长期的方式使用签名私钥，下级节点的安全性直接依赖于上级节点，如果某个节点的私钥失效则意味着它所覆盖的所有下级节点的安全性无法保障，如果根节点失效则整个信任体系崩溃。且 CA 体系扩充用户容量困难。从管理成本及安全风险的方面考虑，一个 CA 体系的层次结构应该尽可能简单，最好只用一个 CA。但从扩充用户容量的角度而言，CA 应该设置尽可能多的下级机构。短时间内 IBC 用于跨域通信设立的 CA 数量有限，用少量 CA 吸纳大量用户将是个漫长的过程。注册机构 RA 虽可以一定程度上缓解成本和扩容之间的矛盾，但也仅仅是线性地增大容量，不能满足物联网应用中网

络用户和设备的急速增长。IBC 虽然通过实体认证的方法消除了 CA 这一部门的存在，但公钥的分发存储仍然是由有安全隐患的第三方完成的。

因此，有必要寻找一种新的方案来为物联网域间通信服务。这种方案应当安全且能够适应物联网接入点数量巨大且变化的特点，也应当是容易部署的。区块链具有去中心化的特点，能够很好地解决 IBC 赖以需要的 CA 隐藏的安全问题。本文提出一种基于区块链的对底层透明的域间通信方案。

第 4 章 基于区块链的域间通信

4.1 区块链基础技术

区块链是由多独立节点参与的分布式数据库系统[11]，记录节点上发生的所有交易信息，过程高度透明，数据高度安全，凡是需要公平、公正、诚实的领域，都可应用区块链技术[11]。区块链的数据结构可以从三个层次来描述: 链、区块和交易，同一个时间周期中所有交易组成区块，区块按时间顺序链接起来就形成了区块链，区块体内交易采用 Merkle 树结构组织，内部任何一 个数据改动都会引起交易总哈希值的变化，导致区块链从该区块断开，因此可保证数据不易篡改、很难伪造、可追溯。根据中心化的不同，区块链可分为公有链、私有链 和联盟链。联盟链介于公有链和私有链之间，节点少，交易速度较快，交易成本低，且保留了区块链其他特性，逐 步成为商业应用领域的主流。下面对区块链做基本的介绍。

4.1.1 哈 希 算 法

哈希(也称为散列)算法将任意长度的输入值映射为较短的固定长度的二进制值。例如，SHA 256 算法 [12] 就 是 将 任 意 长度的输入映射为长度为 256 位的固定长度输出，这个二进制值称为哈希值(也称为散列值)。在第二节中已经介绍，哈希值是唯一的，因此数据的哈希值可以检验数据的完整性，一般用于快速查找和加密算法。哈希算法广泛应用于区块链中，区块链通常不保存原始数据 ，而是保存该数据的哈希值 ，Merkle 树中的节点信息是两次 SHA256 哈希运算得到的。

4.1.2 Merkle 树

Merkle 树 [13-15]是由 Ralph Merkle 发明的一种基于数据哈希构建的树。其数据结构是一棵树，一般为二叉树，也可以为多叉树；图中虚线框内是节点，叶子节点是文本或文件的哈希值，非叶子节点是所有子节点的哈希值。

Merkle 树在验证、文件对比中应用较多，特别是在分布式环境下 ，Merkle 树会大大减小数据的传输量和计算的复杂度。区块链中的每个区块都包含了记录于该区块的所有交易，区块链系统采用二叉树型的 Merkle 树对这些交易进行归纳表示，同时生成该交易集合的数字签名，如图 6 所示。Merkle 树支持快速地归纳和校验区块中交易的完整性与存在性。

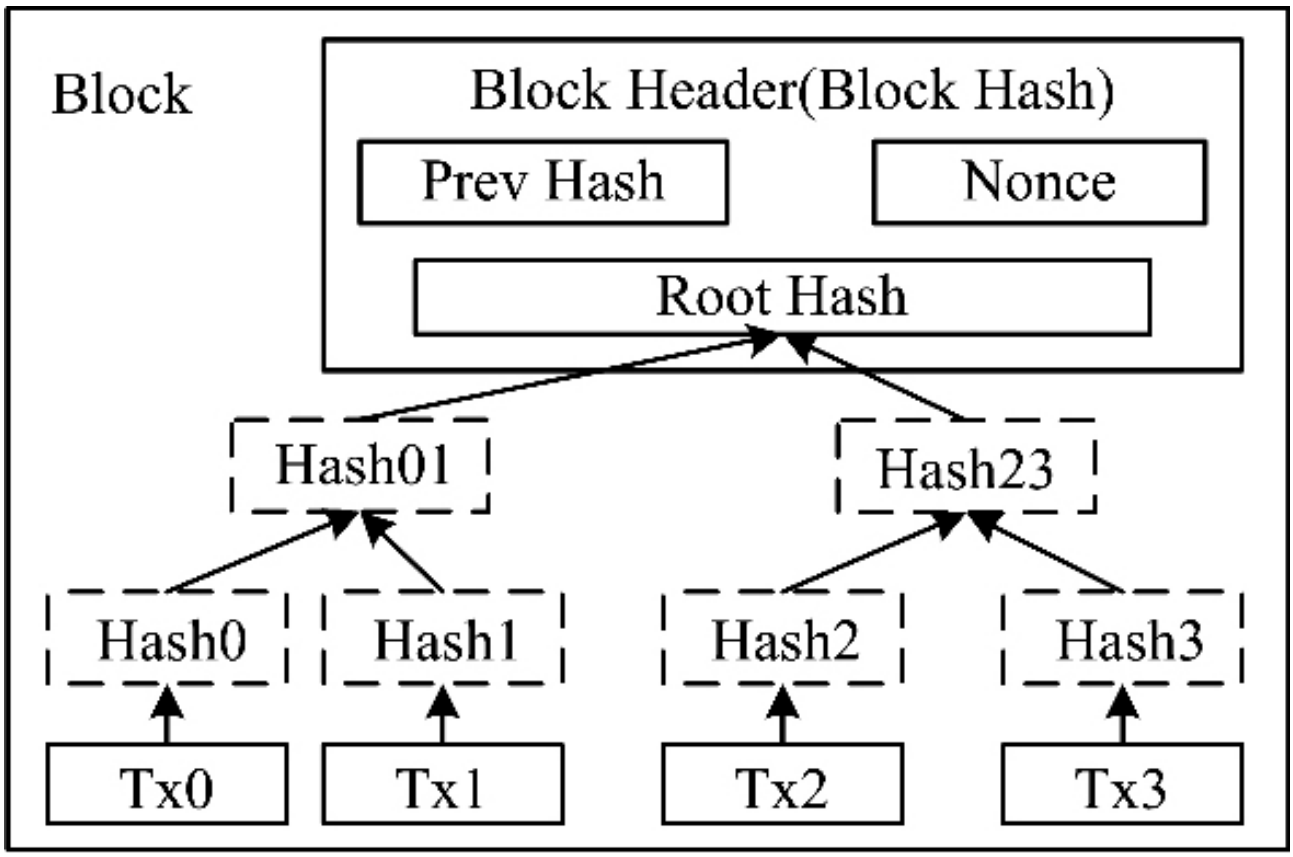


图 6

4.1.3 时间戳服务

区块链技术的发展受到比特币应用需求的推动。比特币作为数字货币，首先需要解决“重复支付 (doublespending)”问题，即一笔货币不能被花费两次或者一笔资金不能出现在两个交易中。中心化的信用系统(例如银行)依靠国家机器的强制力来防止伪钞，而区块链系统完全依靠技术来解决“重复支付 ”问题 。系统给每一笔交易盖上正确的时间戳 [16]，以此证明在这个时刻这笔交易确实发生，交易中资金的所属权已经转移，之前资金所有者再次使用这笔资金时就会报错，从而解决重复支付问题。另外每一个区块也会盖上正确的时间戳，区块链是一种分布式数据库，起从而形成一个按时间顺序发展的正确链表。

4.1.4 工作量证明机制

工作证明 (Proof Of Work，POW)，也称为工作量的证明[17]。比特币系统利用 POW 机制使系统各节点最终达成共识，进而得到最终区块。这里的工作是指找到一个合理的区块哈希值，它需要不断地进行大量的计算，计算时间取决于当前目标的难度和机器的运算速度。当一个节点找到这个值之后，就说明该节点确实经过了大量的计算，这就是工作量证明。由于验证只需对结果值进行一次哈希运算，因此 POW 的验证效率很高。

4.1.5 权益证明机制

相比 POW 浪费大量的算力，点权益证明(Proof Of Stake，POS)仅仅需要少量的计算就能维持区块链的正常运转。这种机制根据货币持有量和时间来分配相应的利息。但是

这种机制存在一点不足，即区块的产生没有消耗大量算力， 导致这种机制下的货币价值来源难以确定，因为任何区块链系统都可以实现。

4.1.6 P2P 网络技术

P2P 网络技术又称为点对点技术，它是一个没有中心服务器、依靠用户群交换信息的互联网体系。P2P 网络由于没有中心化服务器，使得它天生具有耐攻击、高容错的优点;并且各个节点地位平等，服务分散在各个节点上进行，因此部分 节点或网络遭到攻击对整个系统几乎没有影响。比特币系统 应用 P2P 技术，使各个节点独立地参与系统，每个节点都是 一个独立的个体，单独节点宕机或者遭到攻击都不会对系统造成影响。

4.1.7 非对称加密技术

私钥保密，私钥加密的信息只有对应的公钥才能解开，公钥加密的信息只有对应的私钥才能解密，即公钥加密，私钥解密;私钥签名，公钥验证。 非对称加密需要密钥对即公钥和私钥成对出现。公钥公开、私钥保密，私钥加密的信息只有对应的公钥才能解开，公钥加密的信息只有对应的私钥才能解密，即公钥加密，私钥解 密;私钥签名，公钥验证。在比特币系统中，公钥由私钥通过 椭圆曲线加密算法生成;交易信息中必须要有正确的数字签 名才能验证交易有效。

4.2 区块链特点

4.2.1 可靠开放性

区块链的设计使它能够有效预防故障与攻击 。所有参与系统的用户共 享一个公共区块链，不会存在因为单点失效而导致系统故障的情况，从而保证了系统的可靠性和数据的可获得性。 但它仍然遭受 5 1 % 攻击。假设某个用户拥有大幅度超越其他用户的计算能力，计算出更多的节点，当攻击者拥有网络中 5 1 % 的算力，他就可以对区块进行伪造，然后自己又最快地计算出正确的解， 造成区块链分叉，达到攻击的目的。这是规模较小的区块链容易遭受的攻击，如果链上的节点数量足够多这种攻击就相对难度增大了。

4.2.2 信息透明性

网络上的任何节点都可以查看整个账本，这保障了信息的透明公开。在物联网域间通信的应用中，公钥的保存也应当是数据透明的，这一特点也正好满足通信需求。

4.2.3 不可更改性

区块链系统采取的是完全冗余的策略， 所有完整节点都有一份完整数据，因为哈希值是根据以往的信息产生的，要想更改某一区块的数据， 必须保证所有完整节点数据被修改，这个情况几乎不可能发生，因此降低了欺诈的风险。

4.2.4 不可逆转性

交易不存在撤销操作，由于哈希不存在逆运算，交易一旦被验证认可就不可再逆转。

4.3 区块链的去中心化

去中心化的概念具有三个相互独立又相互依赖的维度：架构层面的去中心化，系统中物理计算机的数量，系统可以承受的物理计算机同时崩溃的数量； 控制权层面的去中心化，有多少个体或者组织拥有系统的实际控制权； 逻辑层面的去中心化：系统呈现和维护的接口和数据结构看起来更像一个整体，还是非晶群？如果将系统分为提供者和用户两部分，那么这两个部分是否作为独立单元继续正常运行。区块链在控制权上是去中心化的，架构层面是去中心化的，没有单一节点能够完全控制，也没有系统架构上的故障引发点。但是逻辑上是中心化的（群体达成的共识状态与单一节点的行为无异。

4.4 功能分析

本套系统采用联盟链 Hyperledger Fabric 实现。联盟链指定的节点可拥有交易权限，节点数远小于公有链 。采 用 文 献 [25]中 对 A B C / T B C 双链架构分析的举例假设分析方法，认证凭证大小为 128bit，假设每 10 分钟生成一个区块，每分钟 50% 用户请求外域访问，其中的 10% 申请访问未认证或认证凭证失效的 ISE，对一台节点服务器生成认证凭证的理论 数据值计算如下表。 可以看出，24 小时内用户之间访问不重复，若区块上限为 1M，联盟链可允许 1312 个(代 理 100 个用户) 或者 131 个(代理 1000 个用户) 服务器 节点同时以上述假设访问强度的工作. 联盟链与公有 链类似，可由通信能力强的完全节点同步所有数据. 因 访问信息服务具有持续性和重复性，实际访问量密集 度会降低，且信息服务实体数量有限，实际生成认证证值的大小比表中理论分析值更小。

代理用户数量	**100**	**1000**
10min 生成认证凭证大小	0.78kb	7.8kb
一年生成认证凭证大小	0.04G	0.4G
24 小时认证 ISE 总量	7200 个	72000 个
联盟可容纳节点上限	1312 个	131 个

因此认为将所有的通信节点是不现实的。同时物联网中每个域内的通信有各自的特点和安全需求，不便统一，采用对域内实体透明的跨域认证更为可行。因此该设计将满足以下特点：

（1）域内通信采用 IBC，使用各自的算法和公钥，域之间互不影响。

（2）跨域认证对域内实体透明，即是说对域 A 内某个实体 a 来说，与域 B 内某个实体 b 的通信看起来和与域 A 内另一实体 c 的通信是一样的。

（3）区块链上将存储各个域的域间通信使用的算法名称和公钥，任何链上的域可以访问链上其他域的算法名称和公钥，当两域间发生通信时，用链上的信息进行签名。

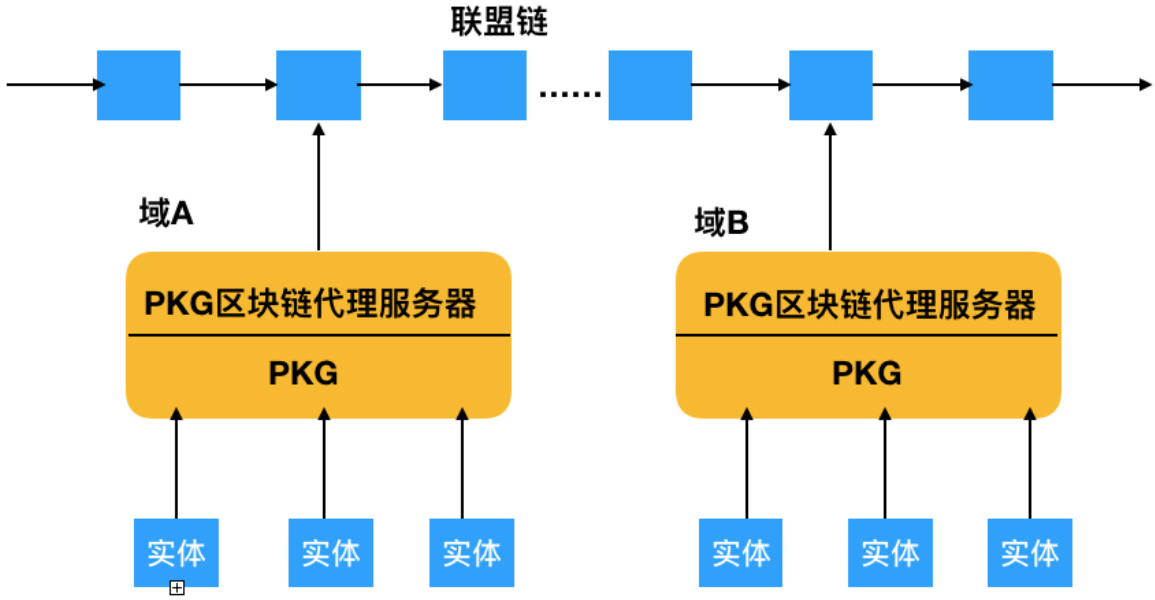
4.5 具体方案描述

4.5.1 对实体透明

对于系统内任意两实体间通信的认证过程，实体所看到的过程和实际过程是不完全相同的。如果 A 向 B 发送消息，无论是域间认证还是域内认证，A 看到的过程都是向认证中心请求私钥并获得私钥，B 看到的过程是认证中心发给自己公钥和附有签名的消息，A 和 B 并不关心私钥和公钥具体是怎么分发的，这一过程对他们来说是透明的。对认证做出不同决策的部门是认证中心，它需要选择合适的算法和加密方法。

4.5.2 设计基本描述

设计一种基于联盟链的双代理跨域认证架构。跨域认证过程对于 IBC 域内实体来说是透明的，实体和其它域内实体之间的认证过程和与本域内实体相互认证过程并没有区别，都是基于 PKG 跨域认证代理服务器来实现。实体本身所需承担的计算开销很小，只是消息的发送和接收。使用联盟链作为底层区块链：可将每个 IBC 域逻辑上可视为一个组织或者机构，联盟链内节点各自代表者一个 IBC 域。联盟链具有高吞吐量、交易速度快等特点，能够获得更高的性能，更符合物联网场景下的应用。



PKG 区块链代理服务器(Blockchain Agent Server，BCAS)：每个 PKG 设一个区块链代理服务器，区块链代理服务器作为联盟链节点。PKG 将本 IBC 域内使用的系统公钥 pk_{PKG}、签名算法 Signature、域内实体标识符 ID_{Entity} 传给区块链代理服务器。区块链代理服务器将这些信息统一写入区块链。PKG 区块链代理服务器同样需要负责更新节点区块内容。

PKG 跨域认证代理服务器(Authentication Agent Server，AAS)：PKG 跨域认证代理服务器本身并不属于区块链节点，但对其它域实体的认证信息来源于域内的 PKG 区块链代理服务器和 PKG，而 PKG 区块链代理服务器的认证信息来自于区块链。

Alice 给 David 发送签名消息：

1.Alice 将明文消息 M、目标实体标识 ID_{David}、签名请求发送给 IBC_1 域的代理服务器 $BCAS_{PKG1}$；

2.代理服务器 $BCAS_{PKG1}$ 将 Alice 的私钥 sk_{Alice} 作为参数，使用签名算法 $Sigenature_1$ 对 M 进行签名，产生签名 sig_{Alice}，将消息 M 和签名 sig_{Alice} 一起发给 IBC_2 域的代理服务器 $BCAS_{PKG2}$；

3.代理服务器 $BCAS_{PKG2}$ 根据收到的实体 ID_{Alice} 查询其对应的 PKG 标识 ID_{PKG1}，基于标识 ID_{PKG1} 查询使用的签名算法 $Signature_1$、公钥参数 pk_{PKG1}；

4.代理服务器 $BCAS_{PKG2}$ 以 ID_{Alice} 和 pk_{PKG1} 作为参数，使用签名算法 $Signature_1$ 对接收到的 M 进行签名，产生签名 $sig_{Alice'}$；

$BCAS_{PKG2}$ 对比接收到的签名 sig_{Alice} 和自己产生的签名 $sig_{Alice'}$。如果相同，则将消息 M 发送给 David；否则，丢弃该消息；

第 5 章 智能合约的实现

5.1 联盟链 Hyperledger Fabric

区块链可以被定义为用于记录事务的不可变分类帐，其在相互不信任的对等体的分布式网络内维护。 每个对等方都维护着分类帐的副本。 对等体执行共识协议以验证事务，将它们分组为块，并在块上构建哈希链。 此过程通过对事务进行排序来形成分类帐，这是一致性的必要条件。 区块链已经出现了比特币，并被广泛认为是在数字世界中运行可信交换的有前途的技术。

区块链分为 3 类[17]: 公有、私有及行业区块链。在公有区块链(简称公有链)中，指任何接入此链的个体或团体都可以在上面发送能够获得该区块链有效认证的交易。公有区块链是最先出现的区块链，也是目前应 用最为广泛的区块链，这类区块链被认为是“完全去中心化”的。在物联网域间认证中公有链并不适合用于物联网域间认证。中行业区块链(简称行业链)指共识过程受到某些预选节点 控制的区块链。由该行业集体内部首先指定多个预选节点为记账人，每个区块的生成是由所有的预选节点共同决定的预选节点决定区块链的共识，其他节点只能接入区块链负责交易，但不参与共识过程，任何人都可以通过此区块链对外开放的 API 进行有限查询。这类区块链被认为是“部分去中心化 ”的 。私有区块链(简称私有链)指仅仅使用区块链这一技术进 行记账操作，但它不对外公开。它的对象可以是一个公司也 可以是个人，单独拥有此区块链的写入权限，或许会对外开放 有高度限制的读取权限。目前金融巨头都在探索自己的私有 区块链，既应用到区块链的特性，又能保证安全。 行业链结合了公有链的完全开放和私有链的高度集中， 提供了一种混合折中的模式;而私有链由于完全限制的写入 权限和高度受限的读取权限，对于保护个人隐私非常合适。区块链的发展过程中，一般 1.0 时代就是数字货币时代，代表是比特币，而 2.0 时代就是智能合约（现在是 3.0 时代， 各种联盟链即为代表）。

Hyperledger Fabric 是一种被广泛认可的分类账平台，旨在实现区块链的高度模块化和可扩展性，为企业提供具有机密性，隐私性和可扩展性的区块链。 根据 Fabric 在 2017 年中期的生产等级，各企业正在尝试使用 Fabric 来构建真实的区块链应用程序。Fabric 使联盟内的参与组织能够构建和部署区块链应用程序。区块链网络由托管区块链的多个节点（或对等方）组成，执行智能合约（称为链码）并共同维护分类账的状态。链接可以由联盟内的所有实体共享，也可以私下部署以供实体子集访问。私有链代码仅在与其共享链代码并且其他人无法访问的对等方上运行。这是通过 Fabric 中的通道概念实现的，其中通道上的所有链代码和数据仅可由作为通道一部分的实体访问。在设置阶段，对等体需要生成的加密材料以识别和验证区块链网络的对等体。以这种方式，可以确定给定对等体是否属于特定频道。除了对等体之外，Fabric 网络还需要订购服务/订购者。订购服务在每个通道的基础上执行 Fabric 网络接受的事务的总排序。当前的生产版本不支持任何形式的订购一致性算法。预计将在未来版本中加入。。

Fabric 中的事务是对链代码方法的调用。 链代码本身在 Docker 容器中运行，从而将自身与 Fabric 代码以及在同一对等机器上运行的其他链代码隔离开来。 每个链代码都有一个称为键值存储的持久状态。 Chaincode 方法使用 put 和 get 方法操作键值存储的值，这些方法基本上允许它从键值存储中写入和读取。 键值存储在同一节点上的 LevelDB 数据库[19]内部。 Fabric 还支持 CouchDB [20]作为可用于存储键值对的备用数据库实现。

Hyperledger Fabric 按以下步骤执行：

1）客户端产生交易：一个客户端要求调用链代码功能。请求由客户端签名，并在部署链代码的通道上发送。它期望获得的认可数量符合链码的认可政策。

2）支持对等方验证签名并执行交易：支持对等方执行所有有效性检查，以确保格式良好，真实性，重放保护和客户端授权。如果成功通过了所有检查，则对等体针对其自己的键值存储执行事务，并生成包含由于链代码执行而生成的读写集的响应。由对等方签署的这些值将作为提议响应或认可发送回客户端。此时不会对分类帐进行任何更改。

3）客户收集认可并发送给订购服务：客户检查并比较所有认可并验证其是否符合链码的认可政策要求。如果请求是读取请求，则它不会向订购服务发送请求。如果请求是一个链代码调用（或写入），它会将代言组合到一个事务中并将其发送到订购服务以包含在区块链中。订购服务验证交易并按渠道对其进行订购。

4）验证和提交事务：块内的有序事务通过订购服务传递给信道上的所有对等体。同行验证交易和认可政策履行情况;如果所有检查都通过，则对等方将块添加到分类帐。请注意，所有对等体都必须提交事务（因此扮演提交对等体的角色），而认可可以仅委托给通道上的对等体的子集，并且被称为支持对等体（EP），如图「21」。

5.2 智能合约

智能合约[22]这一理念最早是在1994年出现的，这个术语是由密码学家Nick Szabo提出的。智能合约的定义定义是[23]以信息化方式传播、验证或执行合同的计算机协议。智能合约可以看做一系列流程，这些智能合约的工作原理与编程语言中的条件语句类似，即当满足一个预先设定的条件时，智能合约就被触发执行相应的条款。区块链技术的出现，使得智能合约再次活跃起来，并且重新定义了智能合约[24]：智能合约是一份运行在账本上的程序，程序由事件驱动，具有状态，账本可复制和共享、程序能够保管账本上资产。智能合约是运行在区块链上的模块化、可重用的自动执行脚本。一个区块链上可以有多份合约以完成复杂的业务逻辑，每份合约可以约束不同的参与者，规定不同的事务的执行方法。可以利用智能合约规定物联网通信中的认证流程。

在fabric中，智能合约叫做chaincode，它有6个状态，如下所示：

Install → Instantiate → invocable → Upgrade → Deinstantiate → Uninstall.

智能合约实质上就是一段代码，我使用的是JAVA语音编写。具体使用方法是首先将合约代码上传到区块链上Install。接着，需要做初始化操作。比如数据的迁移，当前数据是存放在mysql中的，那么上线时需要用Instantiate把数据迁移至链上。初始化后，chaincode就进入invocable可调用状态了。通用我们可以通过CLI命令行或者程序里用SDK调用合约。根据服务需求变化，智能合约版本升级时，就是Upgrade状态。最后两个状态对应着合约下链。

5.3 用JAVA实现智能合约

5.3.1 搭建环境

网络环境: Docker 18.09.2

```
Last login: Wed May  8 09:04:52 on console
cicideMacBook-Air:~ cici$ docker -v
Docker version 18.09.2, build 6247962
```

构建软件：Gradle 3.3

```
cicideMacBook-Air:~ cici$ gradle -v

------------------------------------------------------------
Gradle 3.3
------------------------------------------------------------

Build time:   2017-01-03 15:31:04 UTC
Revision:     075893a3d0798c0c1f322899b41ceca82e4e134b

Groovy:       2.4.7
Ant:          Apache Ant(TM) version 1.9.6 compiled on June 29 2015
JVM:          1.8.0_191 (Oracle Corporation 25.191-b12)
OS:           Mac OS X 10.14.2 x86_64
```

HTTP 客户端： postman

开发环境及插件： eclipse + buildship

5.3.2 功能代码

（1）首先，需要实现 getChaincodeID()。它的合约要求返回链代码的唯一标识符。

```
public String getChaincodeID()
        {
                return CONTRACT_ID;
        }
```

（2）接下来将实现 handleInit() 方法。它的合约要求处理链代码程序的初始化，它将向账本添加一条指定的消息，并在调用成功时将该消息返回给调用方。public String handleInit(ChaincodeStub stub, String[] args)

```
        {
                String ret;
                ret = handleLog(stub, args);
                return ret;
        }
```

（3）接下来将实现 handleQuery() 方法。它的合约要求查询账本，为此，它会获取指定的键，在账本中查询与这个（这些）键匹配的值，然后将该（这些）值返回给调用方。如果指定了多个键，应该使用逗号分隔返回的值。

```
public String handleQuery(ChaincodeStub stub, String[] args)
        {
                StringBuilder sb = new StringBuilder();
           int aa = 0;
           for (String key : args) {//将输入的值依次给 key，当查询数目大于 1 时用逗号隔开
             String logKey = KEY_PREFIX + key;
             if (aa++ > 0) {
               sb.append(",");
             }
             String value = stub.getState(logKey);
             log.info("*** Query: For key '" + logKey + ", value is '" + value + "' ***");
             sb.append(value);
           }
           return sb.toString();
```

（4）接下来实现 handleLog()方法。它的合约要求是写入账本。写入的消息的格式是 json 的，应答包含域的标识符，域内通信使用的算法，域内通信使用的公钥。这些信息将可以被链上的其他域服务器访问。

```
private String handleLog(ChaincodeStub stub, String[] args) {
        String ret = null;
        String logKey = args[0]; //第一个输入的值是钥匙
        String  logMessage = args[1];
        log.info("*** Storing log message (K,V) -> (" + KEY_PREFIX + logKey + "," +
logMessage + ") ***");//向用户显示输入的键值
        stub.putState(KEY_PREFIX + logKey, logMessage);//写入账本
        ret = logKey;
        return ret;
       }
```

（5）接下来实现 handleDelet()方法。它的合约要求是删除账本中的某一条。当物联网中某个域不再存在时可以进行此操作。

```
public String handleDelet(ChaincodeStub stub, String[] args) {
            StringBuilder sb = new StringBuilder();
        for (String key : args) {//将输入的值依次给 key，当查询数目大于 1 时用逗号隔开
          String logKey = KEY_PREFIX + key;
          String value = stub.getState(logKey);
          stub.delState(logKey);
          log.info("*** Delet: For key '" + logKey + ", value is '" + value + "' ***");
          sb.append(value);
        }
        return sb.toString();
      }
```

（6）接下来实现 handleChange()方法。它的合约要求是改变账本中的某一条记录。当物联网内某个域进行升级而改变域内算法或定时更新钥匙对，可以通过这个方法及时地将链上的消息更新。

```
public String handleChange(ChaincodeStub stub, String[] args)
      {
            String key = args[0];
            String value = args[1];
```

```
        String logkey = KEY_PREFIX + key;
        stub.delState(logkey);
        stub.putState(logkey, value);
        return  value;
}
```

总结

根据中国物联网校企联盟的定义，物联网是当下几乎所有技术与计算机、互联网技术的结合，实现物体与物体之间环境以及状态信息实时共享以及智能化的收集、传递、处理、执行。随着物联网技术的快速发展，各种各样的传感器、智能终端等被广泛地应用在家居、校园、医院等生活场景。通常情况下，各个域内的传感器都是被隔离在各个域内的（比如医院和校园通常是相互隔离的）。域内的传感器间的通信通常基于 IBC(Identity Based Cryptography)的认证技术。IBC 是基于标识的密码系统，比起传统的 PKI，它易于部署和使用，简化了大量证书交换的问题。目前，IBC 安全性模型已经获得国际密码学界的证明，在国际上，IBC 密码技术已经获得了广泛的应用。在智慧校区、智慧医院、智慧城市等概念的提出后，IBC 域间通信的需求变得越来越迫切。传统的域间通信通常采用 PKI 和 IBC 结合或者 IBC 分级的方案，但都不可避免的存在一个可信第三方的中心化节点。存在单点故障问题，认证不透明等弊端。随着区块链技术的出现和快速发展，为解决这类问题提供了思路。区块链技术由于其去中心化、公开透明、数据不可篡改等特性，能够保证认证信息和认证过程的真实性，为 IBC 跨域通信提供可靠性保证。认证信息的共享是 IBC 域间实体相互认证过程中的关键一环。但是区块链的更新账本的速度是有限的，将所有的实体全部上链不是高效的做法。本方案采用双代理服务器，分别用于获取链上信息和签名实现对实体的域间通信透明。采用这种策略联盟链中的节点是各个域产生的，由于域的数量有限，区块链的规模较小，假设各个域的区块链代理服务器的计算能力相近，否则区块链易遭受 51%攻击。

引用：

[1]D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. Advances in Cryptology — CRYPTO ’01, LNCS 2139, pp. 213 – 229, Springer- Verlag, 2001.

[2]D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. Siam Journal of Computing, Vol. 32, pp. 586 – 615, 2003. Updated version of [4].

[3]Adi Shamlr. Identity-based crypto systems and signature schemes [C] .In G. BIakley and David Chaum, editors, Procedings of Cryp to 1 9 8 4 , volume 1 9 6 of L N C S . S p ring er - Ver lag , 1 9 8 4 . 4 7 - 53.

[4]Dan Boneh, Mat Franklin. Identity-based encryption from the Wel pairing [C] .JoeKilian, editor, Procedings of Crypto2001, LNCSS pringer- Ver lag, 2001, 2139:213-229.

[5] https://baijiahao.baidu.com/s?id=1617277692902763343&wfr=spider&for=pc

[6] Kumarage H, Khalil I, Alabdulatif A, et al. Secure data analytics for cloud-integrated internet of things applications[J]. IEEE Cloud Computing, 2016, 3(2): 46-56.

[7] Botta A, De Donato W, Persico V, et al. Integration of cloud computing and internet of

things: a survey[J]. Future Generation Computer Systems, 2016, 56: 684-700.

[8] Thang V C, Van Tao N. A Performance Evaluation of Improved IPv6 Routing Protocol for Wireless Sensor Networks[J]. International Journal of Intelligent Systems and Applications, 2016, 8(12): 18.

[9] Raza S, Seitz L, Sitenkov D, et al. S3k: Scalable security with symmetric keys—dtls key establishment for the internet of things[J]. IEEE Transactions on Automation Science and Engineering, 2016, 13(3): 1270-1280.

[10] Farash M S, Turkanović M, Kumari S, et al. An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment[J]. Ad Hoc Networks, 2016, 36: 152-176.

[11] Kosba A， Miller A， et al. Hawk: the blockchain model of cryptography and privacy-preserving smart contracts[A]. IEEE Symposium on Security and Privacy (SP) [C]. 2016， San Jose， CA， USA: IEEE Press， 2016. 839 - 858.

[12] WOLRICH G M， YAP K S， GuilfordJ D， et al.Instruction set for mes sage scheduling of SH A256 algorithm :US， 8838997B2 [P].2012-09-28.

[13]SZYDLO M.Merkle tre traversal in log space and time [J].

Lecture Notes in Computer Science， 2004， 3027:541-554.

[14] MERKLE R C.Protocols for public key cryptosystems [C] // Proc.1980 Symposium on Security and Privacy.New York: IEEE Computer Society，1980:122-133.

[15] MERKLE R C.A digital signature based on a conventional en- cryption function[J].Conference on Advances in Cryptology- crypto，1987，293(1):369-378.

[16]BAYER D，HABER D，STORNETTA W S.Improving the efi- ciency and reliability of digital time-stamping[M].New York:

Springer New York.1993:329-334.

[17] ROY C K，CORDY J R，KOSCHKE R.Comparison and evalua- tion of code clone detection techniques and tools:A qualitative approach[J].Science of Computer Programming，2009，74(7): 470-495.

[18]ANTONOPOULOS A M.Mastering Bitcoin[M].USA:O'Reil- ly Media，2014.

[19] Level DB. Level DB Database. http://leveldb.org/, 2018.

[20] Couch DB. Couch DB Database. http://couchdb.apache.org/, 2018.

[21]Performance Characterization of Hyperledger Fabric

Arati Baliga, Nitesh Solanki, Shubham Verekar, Amol Pednekar, Pandurang Kamat and Siddhartha Chatterjee

[22] WIKIPEDIA.Smart contract[EB/OL].htps://en.wikipedia. org/wiki/Smart_contract.

[23]CASSANO J.What are smart contracts?cryptocurency's kiler app[N/OL].Fastcompany，2014-09-17 [2016-10-23].htps:// www.fastcompany.com/3035723/app-economy/smart-con-tracts-could-be-cryptocurencys-kiler-app.

[24]BROWN A R.A simple model for smart contracts[EB/OL].https://gendal.me/2015/02/10/a-simple-model-for-smart-contr- acts.

[25]Tsai W T，Yu L，et al. Blockchain application development techniques[J].Journal of Software，2017，28(6):1474-1487. (in Chinese)

[26 Matsumoto S, Reischuk R M. IKP: Turning a PKI around with decentralized automated incentives[C]//Security and Privacy (SP), 2017 IEEE Symposium on. IEEE, 2017:410-426.

[27] Ali M, Nelson J C, Shea R, et al. Blockstack: A Global Naming and Storage System Secured by Blockchains[C]//USENIX Annual Technical Conference. 2016: 181-194.

[28] Francesco Marinoa,, Corrado Moisob, Matteo Petraccaa Automatic contract negotiation, service discovery and mutual authentication solutions: A survey on the enabling technologies of the forthcoming IoT ecosystems //Computer Networks 148 (2019) 176－195

[29] Mohammad Wazid a, Ashok Kumar Das b, Rasheed Hussain c, Giancarlo Succi d, Joel J. P. C. Rodrigues e, Authentication in cloud-driven IoT-

based big data environment:survey and outlook //Journal of Systems Architecture(2018),doi: https://doi.org/10.1016/j.sysarc.2018.12.005