EdgeChain: An Edge-IoT Framework and Prototype Based on Blockchain and Smart Contracts

EdgeChain： 基于区块链和智能合约的Edge-IoT框架和原型

<https://tongtianta.site/paper/53508>

摘要—新兴的物联网（IoT）面临着重大的可扩展性和安全性挑战。一方面，物联网设备“薄弱”，需要外部帮助。边缘计算为解决集中式云计算在扩展大量设备方面的不足提供了一个有希望的方向。另一方面，由于资源限制，物联网设备也相对容易受到恶意黑客的攻击。新兴的区块链和智能合约技术为物联网和边缘计算带来了一系列新的安全功能。在本文中，为了应对挑战，我们基于区块链和智能合约设计并原型化了一个名为“ EdgeChain”的边缘物联网框架。核心思想是集成许可的区块链和内部货币或“硬币”系统，以将边缘云资源池与每个物联网设备的帐户和资源使用情况以及物联网设备的行为链接在一起。EdgeChain使用基于信用的资源管理系统基于优先级，应用程序类型和过去行为的预定义规则，控制可从边缘服务器获取多少物联网设备资源。智能合约用于以不可否认的自动化方式执行规则和策略，以规范IoT设备的行为。所有物联网活动和交易均记录在区块链中，以进行安全的数据记录和审核。我们实现了EdgeChain原型并进行了广泛的实验以评估这些想法。结果表明，在获得区块链和智能合约的安全利益的同时，将它们集成到EdgeChain中的成本在合理和可接受的范围内。

索引词-边缘计算，雾计算，EdgeChain，物联网，物联网，区块链，智能合约，可扩性，安全性。

1. 引言

预计到2025年，新兴的物联网（IoT）将连接超过500亿个智能设备[1]。它将不可避免地改变我们与智能住宅，工作空间，交通甚至地平线上的城市一起生活和工作的方式。但是，这种趋势带来了重大的可伸缩性和安全性挑战。首先，物联网设备相对“弱”，其大部分数据被发送到远程云进行处理。示例包括大多数智能手机应用程序和智能家居设备，例如Google Home和Amazon Echo。但是，由于生成的大量数据以及物联网设备与云之间的距离相对较长，因此现有的集中式云计算模型很难按计划的大量设备进行扩展。其次，物联网设备相对“易受攻击”，并且可以相对容易地受到恶意黑客的控制，以形成针对各种攻击的“僵尸网络” [2]，[3]。大多数廉价的物联网设备的安全功能非常有限，而且尽管最近却非常差，甚至没有技术升级或维护服务，这一事实使情况更加恶化。

Google的Android Things 1.0 [4]开始推动这一点。边缘计算1 [5]，[6]，[7]，[8]，[9]是为物联网可扩展性问题提供解决方案的新兴方向。它推动了更多的计算，网络，存储和情报资源更靠近IoT设备，并提供各种好处，例如响应速度更快，处理大数据，减少骨干网流量以及提供边缘情报。

受惠的典型物联网应用包括应急响应，增强现实，视频监控，语音识别，计算机视觉和自动驾驶，许多工作也致力于物联网安全性。由于功能限制[32]，传统的通用安全解决方案不适合在IoT设备上运行。典型的折衷方案是使用轻量级的IoT安全协议[13]，[14]，[16]，[17]， [15]，[18]。通过防火墙[19]，[20]进行的基于边界的安全性不需要在IoT设备上运行其他软件，但不能防止内部攻击，并且已被证明无法有效地保护数十亿个弱设备。与基于边界的信任相比，零信任方法[21]，[22]，[23]被证明是更有效的，并且似乎很有希望。直接或间接系统级安全性

这些方法不会在IoT设备上施加大量与安全相关的负担，并且不会假设IoT设备维护得很好，并且如果启用了零信任或不信任功能，则非常需要这种方法。区块链[24]，[25]与智能合约[26]，[33]相结合，实现了不受信任的环境，并且由于其独特的功能（例如数据/事务持久性，防篡改性，有效性，可追溯性和分布式故障）而受到了越来越多的关注。在将它们应用于分散式物联网和边缘计算系统方面所做的努力不大，而Xiong等人则进行了两项典型的工作。[27]，[28]使用博弈论和查佐普洛斯等人。[31]专注于计算卸载。相比之下，我们的研究重点不是共识机制和挖掘，而是使用许可的区块链和智能合约作为运载工具，我们的主要重点是为各种物联网应用程序提供资源，并控制和规范物联网设备的行为。

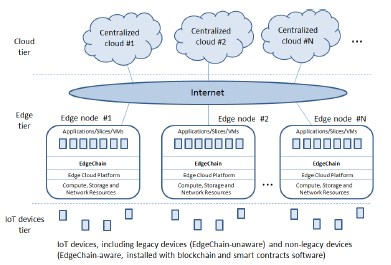


图1：EdgeChain在多层Edge-IoT系统网络拓扑中的位置

在本文中，我们寻求一种根本不同的方法，通过名为EdgeChain的基于区块链和面向资源的边缘IoT框架共同应对这些关键挑战。EdgeChain在多层Edge-IoT系统中的位置如图1所示。我们可以看到EdgeChain位于Edge云平台与在共享基础架构中启动的各种IoT应用之间。这意味着EdgeChain可以在HomeCloud [46]或Cloudlet [9]等不同的边缘云平台上运行。

EdgeChain的核心思想是将许可的区块链与内部货币或“硬币”系统集成在一起，以将边缘云资源池与每个物联网设备的帐户和资源使用情况，以及物联网设备的行为。EdgeChain使用基于信用的资源管理系统，根据有关优先级，应用程序类型和过去行为的预定义规则，控制从边缘服务器获取多少物联网设备。智能合约用于以不可否认的自动化方式执行规则和策略，以规范IoT设备的行为。所有物联网活动和交易均记录在区块链中，以进行安全的数据记录和审核。简而言之，EdgeChain框架的主要贡献包括：

1）一个新的EdgeChain框架，集成了许可的区块链和智能合约功能。

2）内部货币或硬币系统，将边缘云资源池与IoT设备帐户和资源使用行为链接在一起。

3）基于信用的资源管理系统，用于控制IoT设备可从边缘服务器获取多少资源。

4）一种基于资源和智能合约的策略执行方法，用于规范IoT设备的行为。

5）验证和评估EdgeChain思想的原型实现和实验。

我们最新的EdgeChain成就已包含在我们最近提交的两项临时专利中[30]，[29]。请注意，EdgeChain仍是一个正在进行的项目，并且一些工作仍在进行中。我们将在以下各节中相应地讨论状态。本文的其余部分安排如下。在第二部分中，我们讨论EdgeChain的几种关键方法和设计。我们在第三节介绍EdgeChain框架和功能模块。第四节介绍关键过程和工作流程。在第五部分中，我们讨论了原型和评估。第六节是相关工作，而结论和未来的工作则在第七节中。

二 边缘链的关键方法和设计

在本节中，我们讨论EdgeChain设计的一些关键注意事项。图2显示了EdgeChain的总体构想，包括问题空间和解决方案空间。

1. 许可的区块链

区块链网络通常可以分为无许可或公共区块链，以及许可或私有区块链[33]。比特币网络等无许可区块链是点对点的去中心化网络。它通常不受任何私有组织的控制，并且整个网络在网络中所有成员的广泛共识下运行。权衡是相对较低的事务处理吞吐量和较高的延迟。但是，许可的区块链并不是纯粹的对等网络。此类区块链的利益相关者（例如应用程序所有者）将拥有更加受控和规范的环境，并且交易吞吐量更高。用于无许可和许可区块链的共识机制也不同。

EdgeChain系统使用许可的区块链，因为主要目标是支持通常具有所有者和客户的各种分布式IoT应用程序。系统涉众需要更多的控制以及更高的吞吐量和性能。不必运行非常耗资源的工作量证明算法来达成共识，并且不会发生sybil攻击。这也消除了对采矿进行经济激励的必要性，而采矿通常在比特币网络中非常消耗资源。可以使用更有效但资源占用较少的共识协议，典型示例是针对此类环境的实用拜占庭容错（PBFT）[34]。

在EdgeChain中，挖掘作仅由资源比IoT设备更多的边缘服务器完成。资源受限的物联网设备永远无法做到这一点。与无许可的区块链网络相比，挖掘的资源密集度要低得多。换句话说，边缘服务器将负责监视事务，并在发生新事务时创建和附加新块。EdgeChain中的IoT设备仅是区块链和智能合约客户端。如果它们是支持EdgeChain的设备并安装了区块链和智能合约软件，则它们可以与边缘服务器进行交互，并通过诸如云卸载之类的程序来获取资源和协助其任务[35]。如果它们是旧设备，并且不需要边缘服务器的资源，那么它们甚至不需要安装区块链和智能合约软件。EdgeChain对他们完全透明，但是仍然可以创建区块链帐户并从后端管理这些IoT设备。

1. 基于信用的资源管理

EdgeChain使用由区块链启用的内部货币或硬币系统将边缘资源池与IoT设备帐户和资源使用行为关联起来。EdgeChain由一个新颖的基于信用的资源管理系统组成，在该系统中，每个物联网设备都创建了一个区块链账户，并获得了初始数量的信用币。信用硬币余额决定了设备从边缘服务器获取资源的能力。一般来说，设备的余额更大，访问速度越来越快。边缘服务器记录贷方和借方，并根据一组规则将IoT设备请求的必要资源提供给用户，这些规则考虑了预定义的优先级，应用程序类型和过去的行为。作为一项持续的研究工作，我们正在边缘云上设计详细的智能资源供应机制，以实现多种应用程序和异构设备的体验质量（QoE）。

实际上，我们观察到这种资源信用管理机制不一定必须由内部货币系统实施。边缘服务器可以维护传统的信用评分系统，并决定如何将资源授予不同的设备。但是，通过利用内部货币系统，EdgeChain可以获得区块链带来的一系列内在安全优势。例如，所有硬币交易都将自动登录到区块链上安全且不可修改的数据库，这对于将来的审计很有用。此外，它启用了智能合约，可以促进边缘物联网系统中调度规则的不可否认和自动化执行以及策略实施。没有区块链和内部货币系统，所有这些新收益都是不可能的。

1. 基于资源、智能合约的策略执行和IoT行为监管

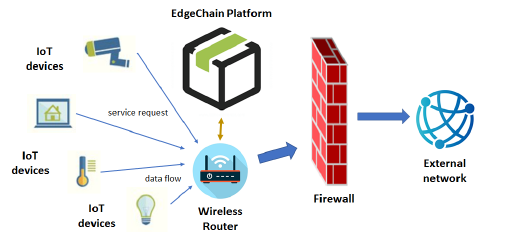


图3：智能家居中独立EdgeChain盒部署的简单示例。

EdgeChain根据其行为和资源使用情况而不是其位置来控制IoT设备，从而实现了更好的安全控制。这克服了现有Edge-IoT解决方案中的限制，这些解决方案通常是基于“外围”的安全性，即在内部和外部网络之间部署防火墙或过滤系统，并且默认情况下信任网络“内部”的用户和节点。如果内部物联网设备被黑客入侵并变为僵尸网络，则很难对其进行控制。

EdgeChain使用面向资源，基于智能合约的间接安全方案来进行IoT行为监管和审核。EdgeChain采用间接系统级安全性方法，这意味着我们不需要IoT设备运行资源密集型安全性软件。相反，EdgeChain根据其资源使用情况和活动​​来监视，控制和调节IoT设备的行为。根据应用程序类型，优先级，设备的过去行为，预编程的智能合约会自动执行资源策略。这意味着，如果某些物联网设备因黑客的恶意活动而受到入侵和控制，由于行为不正常，连续不断地提出与其配置文件或应用程序意图不符的资源请求，或者发起了拒绝服务（DoS）攻击，因此智能合约将根据预编程的策略自动执行。很快，该设备的货币帐户就会用光，EdgeChain可以通过它快速识别，控制和包含网络中的恶意节点或设备，而无需它们实际参与特定的安全程序。EdgeChain可以轻松采取进一步措施，例如将设备列入黑名单或阻止特定设备采取进一步行动。由于智能合约基于区块链，因此所有活动都记录在区块链中。因此，任何恶意节点都很难造成持续的损坏或无痕迹地逃跑。作为一项持续不断的研究工作，我们正在设计智能方法，根据区块链中记录的数据来学习设备的历史行为模式，以更准确地识别和识别潜在的恶意行为。

1. 进化和向后兼容方法

我们意识到，有很多廉价的物联网设备，其安全功能可能非常有限，或者维护和维护都很差，几乎没有升级。尽管Google的Android Things 1.0 [4]刚刚发布，试图解决这一问题， 它还有很长的路要走。有一些极其无法使用的物联网设备，例如窄带物联网（NB-IoT）设备。即使运行最轻量级的区块链客户端软件也可能不可行。我们将这些设备归类为EdgeChainunaware的传统设备。另一种类型的设备相对足够有能力安装区块链和智能合约软件并充当区块链客户端。我们将它们归类为非传统设备。非旧式设备能够直接与EdgeChain交互，并从边缘服务器请求资源和协助。传统节点不知道边缘服务器的存在并且无法使用边缘服务器。

EdgeChain框架采用了一种演进性的，向后兼容的方法，使旧的或功能极其强大的IoT设备可以在新的范式下工作，而无需假定它们安装新的区块链软件或定期进行更新。EdgeChain系统级功能可测量，监视和控制当前和以前安装的IoT设备的资源使用情况。该目标是通过在旧式物联网设备与区块链和智能合约模块之间工作的代理来实现的，通过该代理，区块链和智能合约对旧式设备透明地运行。代理嗅探旧节点的活动，并为非旧节点创建区块链帐户。在这种情况下，EdgeChain仅监视行为并在检测到恶意活动时采取必要的措施。它不会涉及为设备分配边缘服务器资源。通过代理，旧式IoT设备无需了解任何有关区块链和智能合约的信息，但仍可以通过新的Edge-IoT框架进行监视，管理和控制。即使它们受到黑客的攻击，也可以识别其恶意行为并控制损害。

1. 独立部署与分布式部署

EdgeChain的另一个重要优点是能够根据预期应用程序的需求进行量身定制。这使得它既可以部署在智能家居等独立模式中，又可以部署在智能校园或智能城市场景中的分布式模式中。图3显示了部署在智能家居中的独立EdgeChain框的简单示例。在诸如智能校园和智能城市之类的大规模使用案例和应用中，多个此类EdgeChain框可以在完全分布式的环境中工作，在这种情况下，分布式框可以协同工作并共享区块链和智能合约数据。边缘服务器还能够在繁忙情况下彼此分担工作负载并进行交接。边缘服务器还可以运行与其资源池和区块链代币帐户相关的适当激励或游戏算法，以优化收入，成本或服务延迟方面的特定目标 。

三， 边缘链框架和功能模块

在本节中，我们讨论整个EdgeChain框架和功能模块。整个系统框架如图4所示。我们可以看到EdgeChain位于IoT设备和边缘服务器之间，它们侦听消息并执行相应的任务，包括设备注册和设备请求处理。沿着消息路径，EdgeChain的关键模块包括IoT代理，智能合约界面，智能合约，区块链服务器和应用程序界面。我们将更详细地讨论这些模块。

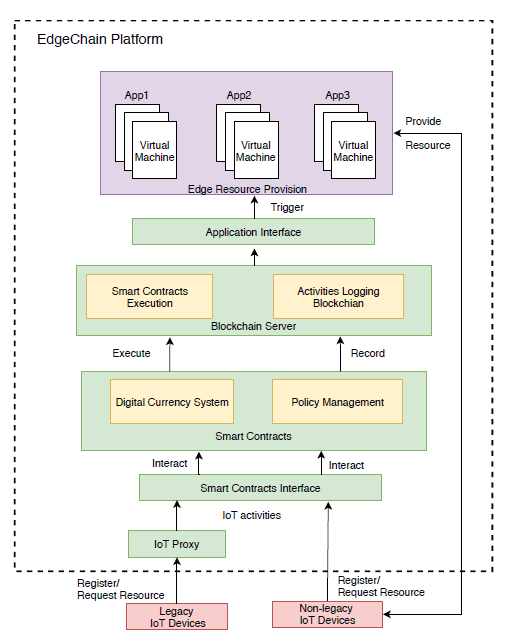


图4：EdgeChain框架和功能模块。

1. 物联网代理

正如我们在第II-D小节中讨论的那样，IoT代理模块的主要功能是容纳旧设备并促进其与区块链和智能合约模块的交互。代理监听并嗅探旧节点的活动，并为其创建区块链帐户。它们以与非传统节点相同的方式为它们完成注册，因此IoT行为监管和审核功能也适用于它们。因此，它们的所有活动都作为非遗留节点记录在区块链中。相比之下，非遗留设备可以直接与智能合约进行交互，并且可以通过智能合约界面获取自己创建的账户。要实现此代理服务器功能，需要适当的嗅探软件，并且我们目前正在研究针对EdgeChain项目目的最有效的开源工具。

B．智能合约接口

当发生IoT活动（例如注册，IoT设备之间的通信，请求边缘服务器资源或将数据发送到Internet上的外部服务器）时，将触发预编程和部署的智能合约，以自动执行相应的操作并执行预定义的管理规则或策略 。智能合约接口在IoT应用程序和智能合约之间架起了一座桥梁。在我们的实现中，我们利用名为Web3协议的基于Javascript的API为IoT设备创建智能合约实例。智能合约实例可以代表特定的IoT设备调用功能并执行在合约中编码的规则。

C．智能合约

智能合约作为所有规则和策略的容器，由EdgeChain系统中的两个主要模块组成。首先，我们建立一个数字货币系统，其令牌为虚拟硬币，代表物联网设备的信任级别或它们可获得的边缘资源配额。由于每个物联网设备都绑定有一个区块链帐户，因此将根据其历史行为和资源类型为其分配一定数量的硬币。例如，如果设备在没有任何恶意行为的情况下保持良好状态，则它将收到更多硬币以支付更多服务资源。否则，可能会向该设备收取更多金币以接收相同服务而受到惩罚，或者永远不会得到奖励。其次，策略管理模块维护在创建时确定的所有规则。这些策略可以分为两种类型：（1）用于分析IoT设备行为并处理有害设备的规则； （2）资源分配策略，以动态分配资源给请求和计划任务。

D.区块链服务

在我们的实施中，智能合约被部署并分布在区块链上。区块链服务器提供区块链服务，其中IoT设备作为客户端连接到它。在区块链服务器上执行两项功能：首先，服务器通过收集设备之间的交易并生成新的区块来运行智能合约，以运行合约中嵌入的代码。其次，通过自动在块上记录设备信息，请求和其他活动，将我们系统中的所有活动记录在区块链上。在无许可的区块链中，此过程也称为“挖掘”。但是，如第II-A小节所述，由于可以使用更有效的共识机制（例如PBFT [34]），并且不需要工作量证明机制，因此EdgeChain挖掘过程的资源密集度大大降低。

E.应用接口

在与智能合约和区块链进行交互之后，有两种可能的结果：由于账户余额有限或识别出的恶意行为而拒绝了请求，或者接受并授予了请求以允许从边缘服务器接收额外边缘资源的请求 。如果请求被批准，则IoT设备可以直接与边缘服务器IoT应用程序进行交互，例如可以将资源密集型工作（例如来自视频流的面部识别）卸载到边缘服务器以进行更快的处理。在这种情况下，应用程序接口会打开智能合约和边缘云之间的通道，以根据智能合约的执行结果触发资源供应。我们使用Node.js框架实现此功能，以监听频道上的事件并相应地为IoT设备和边缘云建立通信。

请注意，就延迟和时间成本而言，智能合约和区块链操作并非免费的，这可能需要一定的时间才能完成。好消息是，注册通常是特定设备的一次性操作。对于与边缘服务器的资源请求，在授予初始请求后，资源供应和交互直接发生在IoT设备和边缘服务器之间，不会造成进一步的延迟。我们在第五节中进行了非常详细的评估和实验。

F.边缘资源

一旦物联网设备获得了资源许可，并且其帐户具有足够的余额来满足所请求的资源，边缘云将相应地在计算，内存，存储，网络和智能中提供资源。由于该应用程序可能对计算机功能，带宽，延迟和隐私具有各种要求，因此各个虚拟机将作为满足特定资源请求的基本单元。例如，对于我们提到的基于视频流的面部识别应用示例，边缘服务器可以生成并启动其他虚拟机来处理视频流并获得面部识别。如果此边缘服务器没有足够的可用资源，则EdgeChain可以与邻居边缘服务器协调以获取其他资源。使用博弈论或拍卖的其他激励机制和动态定价方案可用于优化收入或成本中的某些目标。IoT设备帐户将根据其收到的服务数量和质量相应收费。

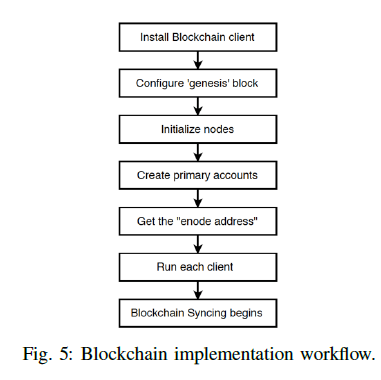
IV。边缘链的关键过程和工作流程

使用所有EdgeChain框架和模块，我们将在本节中讨论关键的流程和工作流程。

1. 区块链部署

可以在边缘服务器和用户设备上以分布式方式执行区块链实现，并在这些节点之间实现同步。我们首先在边缘服务器，非旧版设备和IoT代理上安装区块链软件。我们的区块链建立在以太坊平台[47]上，该平台默认进行初始化以与实时公共网络同步。但是，我们的EdgeChain系统当前是为实验目的而开发的，因此我们将其配置为在校园专用网络上使用。

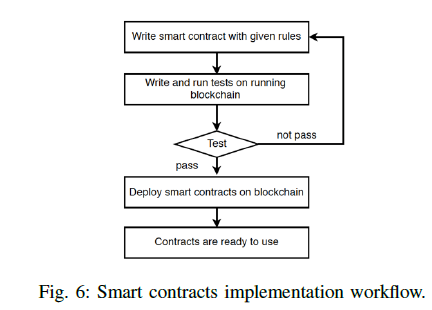
图5显示了区块链部署的工作流程。区块链首先创建一个“创世”区块，其中包含配置信息，例如区块头的哈希值，时间戳和区块挖掘的难度。值得注意的是，由于通过解决具有一定难度的工作量证明（PoW）问题来实现采矿过程，因此难度的高低会对采矿速度以及随后的全局系统性能产生重大影响。假设只允许边缘服务器执行挖掘工作，则无需严格的PoW机制即可解决共识问题。因此，我们的EdgeChain系统将难度设置在合理的较低水平，以在快速开采以避免储藏浪费和包装交易效率之间取得平衡。为了进一步减少边缘服务器的资源消耗，我们实现了仅在存在未确认交易时才发生的自动挖掘功能。



为了彼此同步，所有设备必须具有相同的创世块。初始化过程将为每个节点提供相同的创始配置。接下来，必须为每个节点创建一个主帐户，并分配公钥以进行唯一标识。该账户为每个节点提供了一个区块链地址，可以与其他节点和智能合约进行交互。为了将我们的系统与其他公共或私人区块链隔离，所有节点均设置为“未发现”，因此，如果没有显式地址，它们将无法连接到其他对等节点。这样的隔离可确保设备免受外部攻击者的攻击。因此，每个节点维护一个称为“ enode地址”的特定白名单，该白名单包含边缘服务器和某些从属IoT设备的公钥，IP地址和网络端口。将enode地址添加到每个节点的配置中将允许进行同步。完成上述步骤后，每个节点即可启动。他们将开始寻找朋友节点，进行同步并准备使用。

1. 开发和部署智能合约

正确开发智能合约可确保正确执行管理规则。在我们的EdgeChain系统中，关键功能操作（包括设备注册和边缘资源分配）由相应的合同强制执行。我们按照图6中的工作流程部署智能合约。在区块链上开发智能合约时，进行彻底的测试很重要，因为一旦部署，合约只能重新部署，并且会丢失与先前版本相关的任何数据。这样的重新部署会将合同迁移到新位置，并且用户可能会因为不支持的合同而过时。部署后，将为智能合约分配地址，并将其视为区块链上的普通帐户。为了与他们进行交互，用户必须具有正确地址的副本才能使用远程过程调用（RPC）协议将实例创建为接口。当物联网设备是触发合同功能的发起者时，边缘服务器就是执行合同中功能的执行者。



智能合约为不同的设备指定了各种权限，其中边缘服务器拥有更高的访问所有功能的权限，但是物联网设备仅限于某些基本功能。即使某些弱小的设备被黑以执行恶意活动，这种设置也可以减少影响。为了帮助遗留节点进入系统，部署了代理来满足它们的交互请求。除了由节点发起的直接交互之外，智能合约还能够通过触发“事件”来间接与外界交互 由边缘服务器或网络上其他节点上运行的应用程序接口监视。注意到应用程序的事件后，可以自动触发一些智能合约以执行预定义的任务。例如，边缘服务器完成一个用户请求的服务后，将通过执行特定合同将相关服务数据（如服务时间）记录在区块链上。

1. 区块链上的设备注册

注册是使EdgeChain系统中要管理和监视的IoT设备参与的第一步。如图7所示，注册从确定设备的类型开始。如果存在遗留设备缺乏运行区块链的能力，则代理可以为每个设备创建帐户并注册存储在注册智能合约中的设备规格。如果存在非旧版设备，它们可以直接与合同进行交互以通过发送交易来保存其属性。

注册的信息对下一节介绍的请求接受具有决定性的作用。具体来说，设备规范部分引用了制造商使用说明（MUD）[48]文件，该文件列出了IoT设备允许的活动和通信。这些规范包含输入/输出数据类型，边缘资源请求，MAC地址，IP地址，网络端口，通信协议和指示标志。此外，每个设备都注册一个唯一的帐户地址以加入区块链。注册后，边缘服务器将验证上述信息，并控制注册数据的修改权限。将附加更多参数，例如优先级，硬币余额，信用和请求时间戳，以使设备管理受益。概括而言，表I表示我们在注册数据库中定义的关键设备属性，其中包括所有设备关键信息，价值单位和示例。边缘服务器和IoT设备具有不同的权限来修改注册表。标有“ \*”的属性只能由边缘服务器更新。其他基本属性在物联网设备初始化的第一次注册过程中被填写。

1. 物联网行为法规和活动管理

IoT行为法规和活动管理是EdgeChain系统的核心功能，可实现IoT可扩展性和安全性。在本小节中，我们按以下顺序解释关键设计：详细的工作流程，边缘资源分配算法和行为管理方案。

1. IoT行为监管工作流：EdgeChain不仅可以监管IoT设备之间的活动，还可以提供额外的边缘计算服务来提升资源密集型应用程序。收到IoT设备的活动或请求后，会根据设备类型（旧设备或非旧设备）对它们进行不同的处理。传统设备不需要支持边缘云来处理额外的工作负载。非旧版设备可以根据智能合约的强制规则请求获取边缘资源和服务。详细的工作流程如图7所示，下面进行讨论。

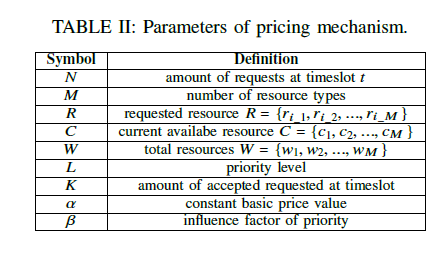
对于旧设备，区块链服务器通过部署在IoT网关（例如WiFi路由器）上的嗅探器监视其数据流向其他IoT设备或外部网络的流量，在工作过程中，其活动或行为（例如网络端口和数据目的地） 记录在区块链上，然后智能合约通过将上述观察结果与注册的属性进行匹配来开始分析设备的行为。根据分析结果，区块链服务器将选择继续监视正常行为。否则它将触发智能合约以阻止任何恶意的旧设备并更新其注册文件中的标志。他们的未来活动将被自动检测和阻止，而无需再次执行行为分析。最后，相关智能合约的执行结果将自动存储在区块链中。

对于非旧版设备，它们可能会发送针对资源密集型应用程序（例如虚拟现实（VR）游戏）的其他资源的服务请求。收到请求后，请求将以交易形式记录在区块链上。接下来，边缘服务器执行资源分配合同，以检索设备的属性并分析服务请求中的资源需求。如果发现设备尝试进行恶意行为，则会通过减少其硬币余额，降低信用点甚至阻止所有未来请求的服务而受到处罚。如果设备运行正常，则边缘云将首先检查剩余的可用资源，然后再进一步处理请求。如果资源池已用尽，则请求将被拒绝并记录。否则，智能合约将根据设备类型，请求明细和应付代币执行资源分配策略。在获得决策之后，边缘服务器开始立即为设备安排服务。同时，边缘服务启动时将从设备的帐户中收取硬币费用。同样，决策和硬币交换都记录在区块链上。

1. 基于定价机制的资源分配：在这种特定情况下，我们的资源分配优化目标是最大化用户请求的接受率，在这种情况下，货币系统充当边缘服务器，物联网设备和区块链之间的连接器 将边缘资源与硬币联系起来。我们提议的货币系统建立在定价机制的基础上，以决定：（a）可以满足要求的顺序； （b）具体服务费。资源请求的价格根据以下环境参数动态变化：

* 边缘资源总量
* 当前可用的边缘资源
* 请求的边缘资源
* 申请优先权

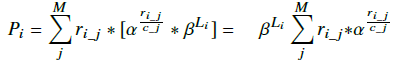
考虑到QoE要求，我们将物联网应用程序的优先级从最高到最低分为4个级别：（1）紧急监控：患者监控，人群感知;（2）延迟敏感任务：虚拟现实（VR），增强现实（ AR）; （3）可靠的数据传输：银行交易，隐私转移； （4）宽容的任务：灯光控制，基于传感器的被动监控。



表II显示了用于计算价格的符号符号。我们首先为请求i定义资源j的单价：



然后，将请求i的总价格定义为，其中cj 2»0; wj¼：



使用动态定价，我们提出了一种启发式请求接纳算法，如算法1所示。提出的算法进行如下。在时隙t的开始处，请求数为N，资源类型数为M。对于每个请求ri\_j 2 R，判断是否有任何一种左边缘资源ri\_j小于cj。如果是，则此时隙中的请求将被拒绝，无需考虑。如果仍然有足够的资源，请计算请求的总价。估计所有请求后，将接受价格最低的请求并将其添加到接受队列。然后，可用资源量C被更新。其余请求将在下一次迭代中重新估算。该算法将持续进行，直到无法接受任何请求为止。假设请求的最终接受数为K，则可以得出时间复杂度为O»¹NM +1 +MºK¼=O¹NMKº，其中K <N。因此，该算法可以在多项式时间内求解 。

1. 基于信用系统的行为管理：行为管理旨在检测潜在的恶意活动或请求，并采取措施避免对系统造成进一步的损害。我们建议实行学分制来进行行为管理。我们的信用体系与物联网环境中的其他类似方案不同，因为信用会影响边缘服务器上的资源分配，而不是物联网设备之间的协作。另一方面，信用并不与边缘服务的价格策略直接相关，而是构成限制请求活动的激励或惩罚方案。在本文中，我们将介绍正在进行的设计和主要模型，以说明学分制的工作原理。我们考虑以下功能：

价格阈值：假设每个设备仅运行一种应用程序并发送一种资源请求，则为此设备i设置一个特定的阈值Pthres。如果Ptotal超过Pthres，则该请求被视为潜在的不良行为，因此降低了设备信用。否则，该请求被视为良好行为，并且信誉增加。

请求频率：如果设备以超高频率连续发送请求，则它倾向于占用比通常用途更多的资源。因此，我们减少了信用。

网络端口：设备应使用MUD文件中预定义的网络端口与边缘服务器通信。否则，会发生一些异常行为。

数据流量目的地：设备通常具有固定的通信目标，因此陌生的目的地表明该设备被黑客入侵或受到控制的可能性。

每个新注册的设备都拥有相同的初始信用。随着实时信用额度的变化，我们提出了两种管理措施：（1）如果设备的信用额已经减少到0，则它将在以后的任何活动中被阻止； （2）否则，设备将根据信用额度更改返回各种硬币。该方程定义如下：



其中Credit是信用价值的变化，是变化的影响因素。

我们可以得出结论，支付边缘服务的能力是受信用体系控制的。更好的方式会获得更多资源的机会更大。

五，原型与评估

在本节中，我们首先介绍作为EdgeChain原型构建的实验性测试平台。然后，我们实现关键功能以验证是否可行并且可接受的性能开销。第三部分，在EdgeChain系统上部署了两个具有不同服务优先级的典型物联网应用程序，以展示区块链与应用程序之间的兼容性。最后，我们测试了基于定价的资源分配系统的性能。

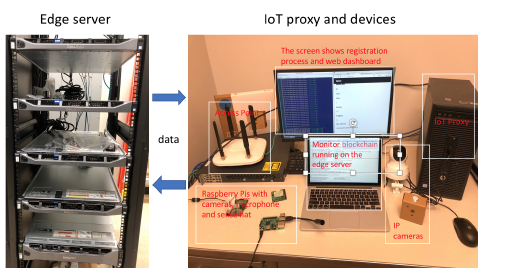


图9：EdgeChain测试平台

1. EdgeChain原型环境设置

测试平台包括后端边缘云集群和前端IoT设备，代理和访问点。边缘云集群是一个OpenStack部署，包括4台高性能Dell PowerEdge R630机架服务器，1台高性能Dell PowerEdge C730x机架服务器和1台高性能Cisco 3850交换机。前端包括多台Raspberry Pi 3 Model B单板计算机，一个Google AIY语音工具包，一个Google AIY视觉工具包和一台笔记本电脑。如图9所示，一个台式机被配置为旧物联网设备的代理，以及一个高性能的Cisco WiFi接入点。

详细的硬件和软件配置如下。从硬件方面来看，每台OpenStack计算节点机架服务器均配备18个独立的CPU内核和256GB RAM。挖掘环境是使用一个内核设置的，其余处理器内核则保留用于边缘计算服务。该矿机最多可提升3.5GHz CPU，8GB RAM和1TB存储空间。作为物联网设备，Raspberry Pi具有1.2GHz CPU，1 GB RAM和32GB存储空间，并具有多个附件模块，包括相机，感应帽，麦克风和Google引擎盖。笔记本电脑具有2.2GHz CPU，4GB RAM和256GB存储空间。至于桌面代理，已安装3.2 GHz CPU，16GB RAM和1TB存储设备以管理IoT设备的多个区块链帐户。

关于软件，边缘服务器安装了CentOS 7作为操作系统，Go-ethereum作为区块链运行框架，Solidity作为智能合约开发语言，Truffle作为合约部署工具，Node.js作为交互界面 物联网应用程序和区块链之间。除区块链部分外，边缘计算资源均使用OpenStack云平台进行虚拟化，有助于灵活地扩展或缩小资源池。边缘服务以虚拟机的形式提供，以适应用户请求的各种规格。Raspberry Pis已经安装了Raspbian操作系统和Go-ethereum，可以在轻量模式下工作，而没有块挖掘功能。笔记本电脑装有MacOS，台式机装有Ubuntu 16。

在测试平台中，机架服务器充当边缘服务提供商，而块矿工则充当工作量证明（PoW）难题。Raspberry Pis和便携式计算机充当区块链客户端，生成资源请求的事务并将其发送到边缘服务器。桌面在旧设备上代表代理与区块链进行交互。在完成上述安装后，边缘服务器将充当“完整”区块链节点，存储所有交易，执行预定义的智能合约并挖掘新区块。物联网设备充当“轻型”区块链节点，仅存储交易数据。图10显示了必备软件模块的存储要求，其中Ethash是用于挖掘区块的PoW系统。我们将发生在区块链上的大部分计算工作放到整个节点上，以减少轻节点上的开销。

1. 区块链和智能合约运营的开销

我们基于以下两个主要功能评估区块链的运行：IoT设备注册和边缘服务器资源分配，以说明由区块挖掘和智能合约的交互所造成的额外开销。开销的来源可以分为三个方面：计算，通信和存储。

1. 边缘服务器上的挖掘过程的计算成本：我们首先评估设备注册的开销，在该过程中，将设备规范加载到由其生成器签名的事务中。然后，交易将广播到我们系统中使用的所有其他设备。最后，这些新交易被打包在区块中并由矿工进行验证。我们观察到挖掘期间和不挖掘期间边缘服务器上计算资源的平均使用情况，如图11a所示。在块挖掘期间，边缘服务器会消耗更多的CPU和内存资源来进行提交并将事务打包到新的块中。相反，在空闲状态下，它仅侦听即将到来的事务，例如挖掘由新事务引起的新块，因此消耗的CPU和内存资源要少得多。
2. 块同步的通信和存储成本：鉴于区块链是完全分布式的，因此需要将每个设备与主流链同步。同步机制依赖于自动更新，并导致系统的通信和存储开销，其中前者来自数据传输，而后者则来自写入本地磁盘。在我们的系统中，边缘服务器维护着主流区块链，而其他设备则从中下载链数据。为了直观地评估同步延迟，我们将物联网设备与边缘服务器进行了比较。由于作为矿工的边缘服务器比物联网设备具有更多的计算和带宽资源，因此它可以更快地完成新块的验证和传输。如图11b所示，我们发现同步新块的平均时间对于边缘服务器为4.09 ms，对于IoT设备为35.9 ms。有了更高的延迟，即使对于响应时间小于100ms的实时应用程序，IoT设备仍然可以满足延迟要求。

一个块的平均大小为128.78 KB，每个块最多可以存储208个设备注册。图11c展示了一个50个块的样本，其大小从108 KB到223 KB不等。因此，该系统平均将为1,000个设备的注册生成约1.8 MB的区块链数据。

1. 智能合约交易的计算和通信成本：除了区块挖掘和同步外，区块链操作还依赖于智能合约触发的交易。以资源请求交易为例，我们评估了智能合约的计算成本和交互延迟。如图11d所示，比较边缘服务器和IoT设备之间的CPU和内存使用情况。我们观察到，常规交易占用的CPU资源百分比非常低，而内存使用率却更高，因为即使在闲置时间内，区块链客户端也占据了8％的比例。我们还评估了智能合约的交互延迟，这对于保证系统效率非常重要。图11e示出了小于50毫秒的一个事务的完成。这样的延迟应满足实时应用程序的延迟要求。
2. 两种典型物联网应用的开销比较

为了评估所提出系统的可行性和兼容性，我们比较了两个典型Edge-IoT应用程序的区块链开销。我们通过测试计算和通信成本来评估人脸识别和自然语言处理应用程序。人脸识别已广泛用于安全监控应用中，例如城市监控，人群控制和门禁，它们对时延敏感，可以实现快速反应。自然语言处理或语音识别的典型应用是智能家居助手，例如Google Home和Amazon echo。

为了进行人脸识别，Raspberry Pi使用具有1080p分辨率和60Hz频率的摄像头模块捕获视频帧，并将其上传到边缘服务器进行图像处理，并以检测到的人脸的位置坐标形式等待检测结果。关于自然语言处理，Raspberry Pi用USB麦克风记录人的语音，将其传输到边缘服务器，然后返回翻译后的文本。

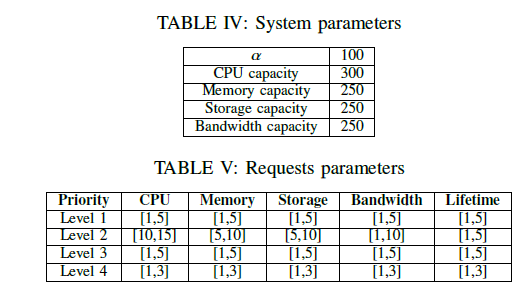
我们首先将区块链的计算成本与两个应用程序进行比较。图12a显示，与两个应用程序相比，区块链的CPU使用率最低。另外，图12b显示了区块链具有最高的内存使用率，但与其他应用程序并行工作时仍处于较低的百分比。因此，物联网设备将不会遭受过载问题。其次，我们评估了在树莓派上发送区块链交易，视频和音频数据之间的通信数据速率差异，如表III所示。我们观察到资源请求的常规事务为I / O性能和整个网络带宽带来了非常低的开销。

总而言之，我们观察到区块链可以以分布式和安全的方式支持IoT应用程序并与之协作。开销在合理且可接受的范围内，并且该系统可行，可以满足构建满足未来需求的多应用EdgeChain平台的要求。

1. 定价方案的资源分配绩效

最后，我们评估了提议的定价方案的资源分配性能。资源分配的目标是提高使用请求的接受率，这主要取决于提议的定价机制。

我们首先评估和的影响。对性能没有影响，因为它确定ri\_j c\_j的范围位于»1； ¼。相反，在更可能满足高优先级请求的地方，调整应用程序优先级的影响。我们进行了三个随机模拟，每个模拟包含2000次随机迭代的具有不同资源需求的用户请求。系统参数在表IV中设置，请求参数在表V中设置。图13a显示Beta的最佳范围在[1.3，1.4]中，并且太大的beta会导致接受率降低，因为简单地允许请求接纳 取决于优先级。



其次，我们比较定价机制，先到先得（FCFS）和基于优先级的多层次调度之间的接受率，其中= 1:35。图13b显示了我们提出的算法性能最佳。然后，如图13c所示，随着总边缘资源的变化，我们评估了性能。从表IV中的配置开始，资源量逐渐减少到较低的百分比。我们的定价算法性能更好。

**VI 相关工作**

由于EdgeChain的跨学科本质，相关工作来自物联网，边缘计算，区块链和智能合约等不同方面。针对这些主题进行了大量的工作，因此，由于篇幅所限，我们不会列举所有单独的工作，而是将重点放在那些直接或密切相关的工作上。

最密切相关的工作是Xiong等。[27]，[28]使用博弈论和定价机制来优化边缘服务器上矿工的利润。它着重于区块链的运行成本。Chatzopoulos等。[31]通过使用一些激励机制和信誉机制，专注于设备自身之间的计算分流。Sharma等。[36]提出了一种使用多层区块链的概念性软件定义边缘节点方案。与这些工作不同，我们的研究重点不是区块链本身。取而代之的是，我们使用区块链作为运载工具，为各种物联网应用配置资源，并控制和规范物联网设备的行为。更多评论文章[33]，[45]，[37]，[38]，[40]提出了结合区块链和物联网的整体未来前景。

区块链和智能合约已用于保护许多不同的领域，在这里我们不做枚举，但是一些示例性的工作包括保护智能家居[39]，保护5G雾网络切换[41]，保护虚拟机编排[42]，确保物联网中的访问控制[43]和安全的数据来源管理[44]。

相关工作的另一个重点是边缘计算研究。大量现有工作要么针对视频分析，车载网络，认知帮助和紧急响应等特定应用，要么非常专注于优化特定目标（例如与收入相关的成本，成本，延迟或能耗），例如 移动边缘卸载，服务迁移，虚拟机链接，放置和编排。我们不会列出所有这些作品，其中[5]，[6]是两个不错的研究点。

**七 结论与未来工作**

在本文中，我们讨论了EdgeChain框架的设计和原型，该框架是一种基于区块链和智能合约的新型Edge-IoT框架。EdgeChain集成了一个许可的区块链，以将边缘云资源与每个IoT设备的帐户，资源使用情况以及IoT设备的行为链接在一起。EdgeChain使用基于信用的资源管理系统来控制可从边缘服务器获取的IoT设备资源。智能合约用于规范物联网设备的行为并执行政策。我们实施了EdgeChain原型并进行了广泛的实验，表明EdgeChain整合区块链和智能合约的成本在合理范围内，同时从区块链和智能合约中获得了各种内在收益。EdgeChain仍是一个正在进行的项目，我们目前正在框架内处理各种问题，例如IoT代理，针对多个异构应用程序的智能资源配置以及更好的IoT设备行为法规。