Integrated Blockchain and Edge Computing Systems: A Survey, Some Research Issues and Challenges

集成区块链和边缘计算系统：调查，一些研究问题和挑战

摘要-Blockchain作为加密货币的基础技术，引起了人们的极大关注。它已被许多应用所采用，例如智能电网和互联网。但是，区块链存在显着的可扩展性障碍，这限制了其支持频繁交易的服务的能力。另一方面，引入边缘计算以扩展在网络边缘分布的云资源和服务，但目前在其分散管理和安全性方面面临挑战。将区块链和边缘计算集成到一个系统中可以实现对边缘分布的网络，存储和计算的可靠访问和控制，从而以安全的方式提供大规模的网络服务器，数据存储和有效性计算。尽管集成区块链和边缘计算系统具有前景，但在广泛部署之前，其可扩展性增强，自组织，功能集成，资源管理和新安全问题仍有待解决。在本次调查中，我们研究了为实现集成区块链和边缘计算系统所做的一些工作，并讨论了研究挑战。我们确定了区块链和边缘计算集成的几个重要方面：动机，框架，支持功能和挑战。最后，探讨了一些更广泛的观点。

索引术语 - 区块链，边缘计算，网络，存储，计算。

1. **导言**

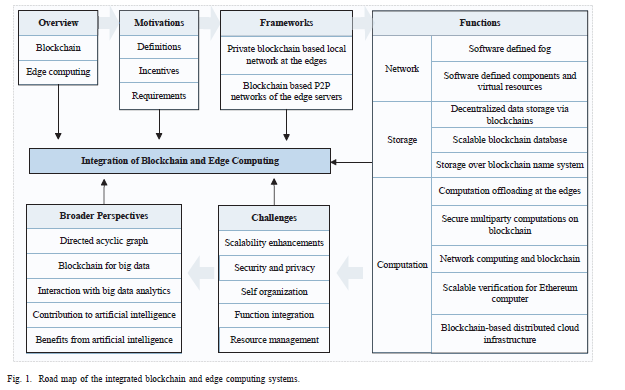
随着数字加密货币的基础技术最近引起了技术巨头对制造商的高度关注，出现了区块链[1]。 根据市场情报公司Tractica的数据，到2025年，区块链企业应用的年收入将达到199亿美元，市场将由涉及至少19个不同行业的29个关键用例组成。

与集中式数字分类帐方法不同，区块链使用社区验证来同步跨多个用户复制的分布式分类帐。 它与比特币[2]一起引入，以解决双重支出问题。除了其最初的设计和应用之外，区块链已成为一种基础技术，导致了从集中控制到分散控制的范式转变。 从信息和通信技术的角度来看，资产的所有权和协议产生的权利和义务可以记录在区块链上，以实现分散，透明，安全，不变和自动化。 但是仍然存在一个严重的缺陷，使我们无法看到这些应用程序得以实现：可扩展性。当今的区块链在扩展能力上受到限制[3]。

另一方面，计算技术的飞速发展已经实现了广泛的应用。在这种情况下，引入了边缘计算[4]作为云的扩展。边缘计算可能具有其他名称，例如雾计算，虚拟小云和移动云。尽管有这些技术的相似性和相异性的争论，但就目标而言，它们几乎是相同的，以使数十亿个设备能够在网络边缘运行应用程序。与云类似，边缘计算通过提供计算能力，数据存储和应用程序服务来协助用户，以具有位置感知能力，保持低延迟，支持异构性并改善应用程序的服务质量（QoS），特别是计算密集型和延迟敏感的。边缘计算的分布式结构具有许多好处。但是，由于异构边缘节点的相互作用以及边缘节点之间的服务迁移，其安全性和隐私性仍然是一个巨大的挑战[5]。

因此，将区块链和边缘计算集成到一个系统中成为自然趋势[6] – [8]。 通过将区块链合并到边缘计算网络中，系统可以在大量分布式边缘节点上提供对网络，存储和计算的可靠访问和控制。 因此，可以大大提高系统的网络安全性，数据完整性和计算有效性。 另一方面，边缘计算的结合使系统拥有大量计算资源和分布在网络边缘的存储资源，从而有效地减轻了功率限制设备的区块链存储和挖掘计算负担。 此外，边缘的链外存储和链外计算可在区块链上实现可扩展的存储和计算[9]。

尽管有集成区块链和边缘计算系统的潜在愿景，但在其广泛应用之前，仍需应对研究挑战。特别地，为了增强可伸缩性，似乎最终将使用不同级别的方法的组合。同时，需要进一步研究由于边缘服务大量外包而导致的新安全问题。此外，自组织通过添加自治机制有效地降低了管理的复杂性，还引发了新的安全问题。此外，基于区块链和边缘计算的网络，存储和计算功能应从多角度，灵活和稳定的角度深度集成。因此，需要通过全面的研究工作来广泛解决涵盖不同方面的资源管理问题。最后，从更广泛的角度来看，有向无环图，大数据和人工智能提供了与区块链和边缘计算的促进关系。



在本次调查中，我们调查了已经完成的使区块链和边缘计算系统集成的工作，并探讨了相关的研究挑战。 图1.展示了设计集成区块链和边缘计算系统的方法，其中我们重点介绍概述，动机，框架，支持功能，挑战和更广阔的视野。

本文的其余部分结构如下。 第二部分概述了区块链和边缘计算技术。 第三节讨论了区块链和边缘计算集成的动机和要求。 在第四部分中，我们探讨了集成区块链和边缘计算的一些典型框架。 第五节详细介绍了网络，存储和计算的集成工作。 第六节讨论了研究挑战和更广阔的前景。 最后，我们在第七节结束本文。

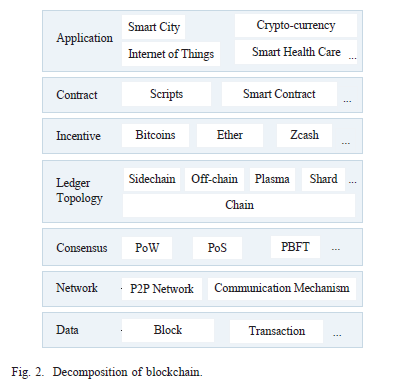
1. **区块链和边缘计算概述**

在本节中，将简要介绍区块链和边缘计算。

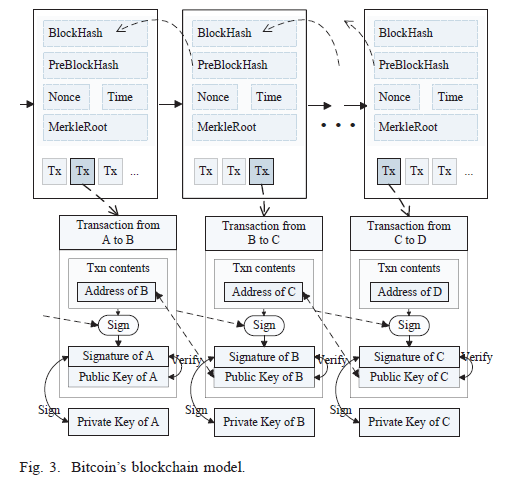
A.区块链

区块链是点对点（P2P）网络中的分散式数字分类帐，每个参与者都维护数字签名和加密交易的仅附加分类帐的副本。 尽管它起源于早期的技术，但区块链已在比特币上获得了巨大的普及，比特币是一个始于2009年的全球电子支付系统[10]。 随着人们逐渐加深对区块链的了解，其技术范围和应用范围也在不断扩大。

1. 层：基于[11] [12]，[13]中的研究，为了更好，更清楚地了解已完成的技术贡献和性能改进，介绍了将区块链系统分解为单独的层 ，从下至上依次是数据，网络，共识，分类帐拓扑，激励，合同和应用，如图2所示。



数据层封装通过事务和块从不同应用程序生成的数据。 验证了两方之间的事务并将其打包到一个带有块头的块中，以“链接”回前一个块，从而得到一个有序的块列表，请参见图3。块头指定元数据，包括前一个的哈希 区块，当前区块的哈希，区块创建时间的时间戳，与上层挖掘竞争有关的Nonce和Merkle根源于区块主体中所有交易的哈希树。



网络层定义了区块链中使用的网络机制。 该层的目标是传播从数据层生成的数据。 通常可以将网络建模为P2P网络，其中对等方是参与者。 使用网络机制，一旦生成交易，它将被分发给邻居，并且仅转发有效的交易。

共识层由共识算法组成，以在分散环境中的不可信节点之间达成共识。在现有系统中，存在三种主要的共识机制：工作量证明（PoW）[10]，权益证明（PoS）[14]，[15]和实用拜占庭容错（PBFT）[16] ]。在向比特币区块链中添加区块以获取奖励的竞争中，每个竞争对手（矿工）都需要通过重复运行哈希函数来查找Nonce值来进行PoW，该值很难生成但易于他人验证。由于PoW的计算需求，可防止来自恶意节点的攻击，因为与总网络计算能力相比，恶意节点的计算能力受到限制（小于51％）。在以太坊中使用的PoS [17]中，哈希目标是每个币龄，可以简单地定义为币种数量乘以持有期，因此选择总币龄最高的区块链作为主链。它消除了PoW中的高能耗，但通过增加控制大量股权的成本来防止攻击。与公共区块链中应用的PoW和PoS不同，PBFT由许可的Hyperledger Fabric中的验证对等方运行以验证交易。 PBFT的工作原理是假设少于三分之一的节点有故障，而其他所有节点均正确执行。一些变体[18]，例如委派的PoS（DPoS），事务处理的PoS（TaPoS），PoS速度（PoSV），委派的拜占庭容错（DBFT）和Bitcoin-NG，请选择一些变体来生成并验证块以进行改进可扩展性，吞吐量和延迟。同样，许多其他共识机制，例如服务证明[19]，存储证明[20]，贡献证明（PoC）[21]，[22]等，也针对不同的特定应用程序而设计。

分类账拓扑层定义了分类账拓扑，用于存储由共识层产生的认证数据。它包含存储系统分类帐的区块链，以及由共识产生的其他一些状态。除了图3所示的传统区块链（主链）结构外，我们还特别关注在可伸缩性改进工作中产生的一些新的链拓扑。例如，[23]中首先提出的侧链是较低层的层次结构“共识实例”的分散程度可能低于顶层链，并允许通过交易在链之间转移资金。脱链允许活动不会在区块链上发生。例如，闪电网络[24]提出了小额支付渠道来发送交易，交易的价值转移发生在区块链之外。树状层次结构组成的等离子链[25]使用综合化证明来强制执行子链，以最大程度地降低成本效率并净赚钱。交易结算。以太坊分片[26]中的分片链使用链上状态分区来获得更高的吞吐量，其中交易被包装在“排序规则”中，类似于区块的排序规则则使用哈希值。

激励层集成了经济激励措施，以激励节点做出自己的努力来验证数据。 这对于保持分散的区块链系统在没有中央授权的情况下整体运作至关重要。 在比特币和以太坊中，比特币和以太币将作为奖励，向在链中添加区块的节点进行奖励。 除奖励外，存款和罚款都被引入到区块链中以保护外包计算。

合约层将可编程特性带入区块链。 比特币脚本提供了多种花费硬币的方式。 基本上，事务的每个输入都连接到先前的输出，并且在输入的输入给出给定签名的情况下，当输出的脚本评估为true时，该连接才有效。 在以太坊中，作为功能强大的脚本的智能合约是一组状态响应规则，用于在用户之间自动转移数字资产，而不仅仅是货币。

区块链的最高层是应用程序，包括加密货币，物联网（IoT），智能城市等，这些应用程序可能会革新金融，管理和制造业等许多领域。 然而，区块链仍处于起步阶段，学术界和行业都在尝试深化该技术，特别是从信息和通信技术的角度来看，以支持这些高级应用程序。

2）表征：区块链技术范围和应用的扩展仍在进行中。 但是，核心机制可以概括如下。

•分散和透明：区块链网络中有许多验证对等节点无需集中权限即可访问信息。 因此，事务（记录）是透明且可追溯的。

•通过共识同步：共识协议可确保一定数量的节点就有序追加到共享分类账的新交易块达成协议，参与者共享副本的副本保持同步。

•安全性和不变性：共享的，防篡改的复制分类帐通过单向加密哈希函数确保不变性和不可否认性。 对手很难篡改

有这样的记录，除非他们控制了大多数矿工。...

B.边缘计算

在过去的十年中，云计算提供的无限可用的计算，存储和网络管理资源导致了许多新的基于云的应用程序以及许多互联网公司（例如亚马逊）的快速增长。 然而，近年来，一种新趋势正逐渐从云的功能向网络边缘转移[27] [4]。 主要由某些对延迟敏感的应用程序（例如虚拟现实）需要，这些应用程序对延迟有严格的要求。 因此，通过将云资源和服务推向边缘的边缘计算范式可实现移动性支持，位置感知和低延迟。 这些有望实现的成果使其成为实现下一代互联网（如IoT [5]和触觉互联网（毫秒级反应时间）[28]）的各种愿景的关键技术。

1）体系结构：一般来说，边缘计算的结构可分为三个级别：终端设备（前端），边缘服务器（近端）和核心云（远端）。此层次结构表示边缘计算元素的计算能力及其特征。前端的终端设备（例如传感器，执行器）为用户提供了更多的交互性和更好的响应能力。但是，由于容量有限，必须将资源要求转发到服务器。近端的边缘服务器可以支持网络中的大多数流量以及大量资源需求，例如实时数据处理，数据缓存和计算分流。因此，边缘服务器为延迟时间稍有增加的最终用户提供了更好的性能。远端的云端伺服器提供更强大的运算能力（例如大数据处理）和更多资料储存空间，并具有传输延迟。此体系结构的目标是执行边缘网络中应用程序的计算密集型和延迟敏感部分，并且边缘服务器中的某些应用程序与核心云通信以进行数据同步。

2）表征：边缘计算的分层体系结构包含以下属性。

•邻近性和低延迟：在物理和逻辑意义上，接近边缘计算的末端都比远程集中式云支持更有效的通信和信息分发。对于密集的小型蜂窝网络或机器到机器的传输，它通常具有数十米的传播距离，并且在回程网络和Internet传输中没有过多的延迟。由于传播距离短，边缘计算有潜力在许多可能需要触觉速度且等待时间接近1ms的关键等待时间应用中实现触觉级等待时间[29]。

•智能和控制：现代边缘节点的性能足以满足一组本地用户的高速率传输，大数据存储和复杂的计算程序的需求。这为应用程序的自治管理和边缘协调开辟了道路，从而可以将本地设备的计算和存储卸载到本地，或有选择地委派给其他节点或核心。

•更少的集中度和隐私性：许多边缘计算服务器可能是私有的Cloudlet，而这些较少的信息集中度将减轻因所有权和数据管理分离而导致的云计算中信息泄漏的担忧。 例如，边缘计算设施的企业部署在其自己的管理内会敏感地交换信息，因此具有增强隐私的潜力。

•异构和可扩展性：扩展到大量站点的边缘计算是实现可扩展性的一种较便宜的方法，而不是在企业中心安装服务器。 此外，可以是异构平台的边缘节点通过考虑设备的异构性来提供效率。

1. **区块链和边缘计算集成的动力和要求**

在本节中，我们首先定义了区块链和边缘计算的集成系统，然后讨论了集成的动机，然后讨论了区块链和边缘计算的集成需求。

A.什么是区块链和边缘计算的集成

为了清楚地描述集成的区块链和边缘计算系统，我们首先在本文中分别展示了我们专注于区块链和边缘计算的内容。

这里涉及的区块链涉及其允许网络参与者将系统记录在分布式共享账本中的能力。图2中对其共识协议，分类帐拓扑，激励和契约给予了更多关注，它们将在集成系统中扩展以适应边缘计算系统及其组合的不同层次。区块链的关键点是安全性和隐私性的优势以及对可扩展性的需求。

这里考虑的边缘计算与其在分布式网络边缘中执行联网，存储和计算的能力有关。集中是服务的支持和管理。边缘计算的关键点在于以分布式方式实现可伸缩性的优点以及以安全方式进行有效控制的需求。

因此，这里基于区块链和边缘计算的系统的集成框架和功能旨在通过考虑网络，存储和计算来提供安全服务以满足应用需求，这些安全，服务涵盖了区块链的核心层和边缘的主要功能。计算。集成的可能性来自于相同的分散式网络基础设施以及相同的存储和计算功能，而集成的必要性在于区块链和边缘计算的不同优势以及相应的互补作用。接下来，我们将介绍细节。

B.我们为什么需要区块链和边缘计算的集成

1）边缘计算的安全性受到挑战：边缘计算的分布式结构具有许多好处。尽管如此，其安全性还是一个重大挑战[5]，[30]，[31]。 在下一代互联网中，边缘计算处于多种不同技术（例如P2P系统，无线网络，可视化等）的复杂交织中。 异构设备以及边缘服务器的相互作用以及跨全球和本地规模的服务迁移，都可能产生恶意行为。

在邮件传输期间，可能会发起某些攻击（例如，干扰攻击，嗅探器攻击等），以通过阻塞网络来禁用链接或监视网络数据流。 因此，网络管理员输入的配置必须是值得信任和验证的，这实际上由于边缘计算环境的高动态性和开放性而受到挑战。 此外，在管理异构边缘网络时，很难将管理流量与常规数据流量隔离开来，这使得对手更容易控制网络。 此外，Internet边缘的分散控制可能给网络管理带来沉重负担。

在边缘计算网络中，数据被分成许多部分并存储在不同的存储位置，这使得丢失数据包或错误存储变得更加容易。因此，很难保证数据的完整性。此外，当涉及多个边缘节点的上传数据可能被未经授权的对手修改或滥用时，可能会发生数据泄漏和其他隐私问题。存储的另一个挑战是确保数据的可靠性，因为使用擦除码或网络编码来检测和修复损坏的数据的传统方法会导致边缘计算系统中沉重的存储开销。

边缘计算网络中的另一个重要安全挑战是在将计算任务上载到边缘计算节点时保持安全性和私密性。引入了一些可验证的计算方案，其中将计算与计算功能或公钥一起外包给一个或多个服务器，这些服务器返回计算结果以及验证计算的证明。

因此，可以看出诸如边缘安全控制，安全数据存储，安全计算和安全网络之类的安全问题可能需要新的思想来适应边缘计算的去中心化，协调性，异构性和移动性，尤其是可伸缩性的结合 如此庞大的覆盖范围内具有安全性，但避免了过多的加密开销。

2）区块链的技术挑战和局限性：尽管区块链具有巨大的潜力，但它面临着众多挑战，可能会限制其广泛使用。 存在某种困境，区块链系统最多只能具有去中心化，可扩展性和安全性两个方面[26]。 具体地说，分散化使网络成为无权且不受审查的限制，安全性与不变性和一般的攻击抵制有关，而可伸缩性则分别与处理事务的能力有关。 当前，可伸缩性问题，特别是低吞吐量，高延迟和资源耗尽的局限性阻碍了任何基于区块链的解决方案的实际可行性。

随着交易数量的增加，区块链需要增加存储空间。 2017年9月，比特币的区块链大小约为158 GB，对于新节点参与，其引导时间大约为四天。以太坊似乎遭受了类似的应用增长，这一事实得到了改善，因为仅州而不是州 整个区块链历史需要存储在整个节点上。 尽管互联网已经非常庞大，但它仍然显示出此类分散网络的扩展限制。 此外，如果只有一小群大型企业能够运行完整的节点并且可能在轻节点无法立即检测到这种情况的情况下作弊，那么这么大的区块链规模就是集中化风险[14]。

此外，受最大区块大小和用于生成新区块的区块间时间的限制，公共区块链（例如比特币（每个区块的区块链大小限制为1 MB）和以太坊）平均每秒只能处理7-20笔交易 ，远远低于主流支付处理器，例如Visa信用卡平均每秒处理2000次交易[11]。

此外，从用户的角度来看，交易费用可能会有所不同，因为服务和矿工对交易验证的费用率有所不同。 但是，挖掘过程的硬件成本是不可忽略的，与执行CPU演算所需的功耗有关[32]。

由于安全成本和集中风险，人们批评使用许多不同的山寨币或增加区块大小。 最近，可以说链上扩展（分片）和链外扩展（状态通道）既必要又互补。 但是，所有这些技术仍处于起步阶段，并且需要其他技术来支持执行脱链人员的工作。

因此，研究的主要目标集中在增加事务吞吐量和减少对节点的带宽，存储和处理能力的要求，同时最小化安全性。

3）区块链和边缘计算的集成带来的好处：构建在计算，数据存储，网络以及它们不同互补重点上的区块链和边缘计算的相同去中心化机制注定要结合在一起。 我们给出了从组合中获得的收益[33]。

将区块链并入边缘计算可增强安全性，隐私性和自动资源使用率。

•使用区块链技术，可以在数十个边缘节点上构建分布式控件。由于挖掘过程和在大量节点上的复制，区块链以透明的方式在其生命周期内保护数据和规则的准确性，一致性和有效性。因此，这是一种有效的解决方案，适用于分配在分离的物理边缘处或在分离的物理边缘之间移动的大量异构用户。

•边缘存储中的隐私保护优势是通过在本地存储数据或在多方之间存储数据的小片段来协调边缘活动的挑战。使用区块链技术，每个用户都可以管理自己的可变密钥，从而无需第三方即可访问和控制数据，其匿名性质允许在对等基础上进行协调，而无需透露元数据（源，目的地，内容）给任何人。因此，可以实现完全的隐私。

•雾节点之间的动态协调涉及资源借用和借出。 区块链的智能合约可通过自动运行所请求服务的按需资源算法来促进按需使用资源。 此外，还提供了资源使用情况的可追溯性，以正确地验证客户端和服务提供者的服务级别协议。 因此，通过区块链和智能合约，边缘计算中的资源使用实现了可靠，自动和高效的执行，并显着降低了运营成本。...

另一方面，将边缘计算并入区块链带来了强大的分散网络以及网络边缘中丰富的计算和存储资源。

•区块链共识依赖于P2P网络层传输的数据，而边缘计算范式源自P2P，但将对等对象扩展到边缘的设备，并将P2P计算与云融合在一起。这种层次结构使信息在区块链中的传播变得容易，并且在物理上支持某些区块链扩展方法，例如边缘的侧链。

•从终端设备到边缘服务器的计算分流使资源受限的最终用户可以参与区块链。例如，比特币的区块链作为一种最受信任的不变技术，但几乎没有在移动设备或传感器上运行，可以通过利用边缘为用户处理电量耗尽的PoW难题来实现。此外，强大的优势为区块链计算资源管理引入了更经济的方法。

•边缘服务器为庞大的公共区块链提供了强大的存储容量，为私有区块链提供了独立而机密的环境。此外，由于区块链提供的数据存储空间有限，某些多媒体应用需要链下数据存储。将原始数据外包到边缘服务器可以在区块链上利用尖端的多媒体技术。

C.区块链与边缘计算整合的要求

要实现区块链和边缘计算的集成，需要满足一些要求[34]-[37]。

•身份验证：在具有多个交互服务提供商，基础架构和服务的边缘计算环境中，至关重要的是验证这些实体的身份验证，这些实体通过各自的接口进行协作以通过签署智能合约来达成协议。 实体的权利和要求在合同建立过程中由区块链记录。 这对于在边缘生态系统的元素之间建立安全的通信通道是必要的，即使它们属于不同的安全域。

•适应性：随着时间的流逝，设备的数量和应用程序的复杂性，特别是有限资源设备上应用的区块链，正在增加。因此，区块链和边缘计算的集成系统应具有支持数量不断变化的复杂性不同的最终用户和任务的能力，并具有适应不断变化的环境的灵活性，以允许对象或节点自由连接或离开网络。

•网络安全：由于异构性和攻击漏洞，网络安全是边缘计算网络的主要关注点。需要将区块链集成到边缘计算网络中，以替换某些通信协议中的重密钥管理，为维护大规模分布式边缘服务器提供方便的访问，并在控制平面中进行更有效的监控以防止恶意行为（例如DDoS）攻击，封包饱和）。

•数据完整性：数据完整性是数据在整个生命周期中的维护和保证。通过充分利用边缘计算的分布式存储资源，可以在完全分散的环境中通过一组边缘服务器以及基于区块链的框架来为数据完整性服务复制数据，从而极大地阻止了对数据完整性的侵犯（外包的丢失或错误修改）数据和滥用的上传）。因此，需要对数据所有者和数据使用者都进行更可靠的数据完整性验证。

•可验证的计算：可验证的计算使计算工作可以卸载到某些不受信任的客户端，同时保持正确的结果。边缘计算中的外包计算可以扩展到大量计算，而不受区块链的可扩展性的限制，而以太坊区块链中智能合约的激励和自主性应保证有效的计算调度和返回解决方案的正确性。

•低延迟：通常来说，应用程序的延迟是两个组件的乘积：传输延迟和计算延迟。计算等待时间表示花费在数据处理和区块链挖掘上的时间，这取决于系统的计算能力。从终端用户到云服务器，提供快速计算的能力不断增加，但同时也导致传输延迟显着增加。因此，区块链与边缘计算的集成是确定哪种计算与执行位置之间的映射，从而实现传输等待时间与计算等待时间之间的理想折衷。

1. **集成区块链和边缘计算系统的框架**

在本节中，我们将详细讨论集成的区块链和边缘计算系统如何满足网络，存储和计算的需求。 在每个方向上，都会介绍一些使能技术。

A.网络

确保传输过程中的安全性是基于区块链的边缘计算网络的成就之一。 在这个集成系统中，通过边缘层中的中央节点连接的两个设备之间存在典型的数据通信。 此外，在两个边缘之间设置了数据通信中的规则的区块链（智能合约）通信[38]，例如寻址，加密，权益，有效期等。 因此，数据通信与区块链通信相结合，确保了网络的高效可靠合作。

在数据传输过程中，可以发起不同级别的几种攻击（干扰攻击，Sybil攻击，泛洪攻击，资源消耗拒绝服务，以及其他[47]），以通过阻塞网络来禁用链路或监视网络数据流。而且，部署了边缘计算以提供到下级（物理设备和通信）和上层（网络和传输）的接口，以及这些各种类型的网络和通信协议，例如移动无线网络，Wi-Fi，ZigBee和M2M，显然将是管理网络的挑战。 SDN及其对软件定义网络组件（SDNC）的扩展[19]是缓解上述问题的有效措施。通过将控制平面与数据平面分离，软件定义的特性可提供更好的网络可见性，并且OpenFlow协议通过提供可编程和标准化的接口来利用网络管理和智能合约[48] – [50]。此外，随着SDN的出现，网络虚拟化（NV）有了新的发展[51]。起源于90年代的网络虚拟化使用户之间可以共享和隔离大量资源，并可以用小资源构建大型虚拟资源。这种动态的网络虚拟资源简化了SDN上下文中的网络管理，并有助于通过区块链[8]，[37]，[49]，[52]实现网络安全性和隐私性。

1）软件定义的雾：软件定义的雾[19]由分布式SDN控制器组成，网络中的所有控制器都使用区块链技术以分布式方式互连，从而使通信可靠高效。 。 每个SDN控制器都包括一个流控制分析器（解析器，图形生成器和验证器）和数据包迁移组件（迁移代理和数据平面缓存）。

分析器是控制平面上的应用程序，它执行网络基础结构的主要功能以抵抗饱和攻击。

•当攻击者试图通过一部分OpenFlow消息扭曲控制器的网络视图时，解析器监视器将解析传入的数据包以提取重要的元数据。

•图形构建器基于对解析的数据集的分析来构造和更改连接到网络流量的流程图，以便可以识别流程图中反映的安全策略中的攻击以及拓扑交换元数据。

•在验证程序中，通过导航所有可能的路径并收集所有路径条件来生成脱机路径条件，而在线反应规则是通过监视全局变量的值并将其分配给状态路径然后解析路径来建立的 生成状态消息。

迁移组件是控制平面和数据平面之间的应用程序，它在攻击中将良性网络流发送到OpenFlow控制器。

•迁移代理检测攻击并做出不同的决定。 针对饱和攻击，它会触发解析器的流规则以生成新规则并在数据缓存中迁移丢失的表数据包。

•数据平面缓存用于在发生饱和攻击时临时缓存丢失的数据包，并在洪泛攻击期间缓存洪泛包。

在这里，[7]中提出的区块链技术可以直接用于边缘计算环境中的流规则表的更新，其中软件定义的雾保持其数据库中更新的流规则表的记录，而设备没有 数据库，但按以下步骤将其流规则表更新到区块链中。

•请求设备首先通过广播版本验证的请求数据包来更新流规则表，这需要来自响应设备的答复和所有的迷雾。

•雾检查收到的请求数据包中流规则表的版本。 如果它是最新版本，则fog将进一步检查其完整性，否则会将流规则表的最新版本打包到响应数据包中，以转发到请求设备。

•响应设备还检查请求数据包及其自身记录中流规则表的版本一致性。

（1）如果两者具有相同的版本，则响应设备将让区块链网络中的其他节点验证流规则表的哈希值，并且除非收到其他节点的确认（即PoW），否则无法将响应数据包发送到请求设备 ），使其相信此流量规则表的正确性。

（2）当流规则表的版本不同时，响应节点必须签出最新版本。 如果响应节点的流规则表是最新的，则将其打包到响应数据包中并发送到请求节点，否则必须更新较低版本的响应节点的流规则表。

2）软件定义的组件和虚拟资源：为了在云，雾和边缘主机之间提供服务，[8]，[49]中使用了虚拟资源形式的软件定义的组件。 网络虚拟化的虚拟资源在概念上可以与SDN共享许多共同的元素[53]。 该视图由虚拟资源提供，因此，将创建物理系统之上的虚拟系统。 每个虚拟系统的独立配置将工作负载分配给雾气而不是受约束的设备（在能源，通信和计算能力方面受到严重约束），可以执行实时处理或任务，并提供对物理设备的受控且低延迟访问。 资源虚拟化分为两层：

•原子抽象层（A2L）管理其原子虚拟资源（AVR）与物理组件（传感器，执行器）之间的一对一配置关系。 AVR公开了约束应用协议（CoAP）方法定义：获取，发布，放置和删除。

•A2L顶部的视图抽象层（VAL）管理其视图虚拟资源（VVR）与较低的AVR之间的一对多关系以及VVR之间的多对多关系。 在这一层中，使用约束的RESTful环境（CoRE）链接格式（RESTful表示表示状态传输（REST）体系结构）通过CoAP进行服务发现和状态检索的工作。

在多个虚拟系统属于不同租户的情况下，将基于权限的区块链部署在每个系统中，以处理虚拟资源的供应并以安全的方式控制对网络的访问。 系统测试展示了在雾层中托管的具有多链区块链集群的，连接到Wi-Fi网络的Edison模块的实施中，响应时间更快。

B.储存

边缘计算通过将数据外包到网络边缘来保持数据与用户的距离，与集中式云计算相比，它提高了可用性并减少了延迟[54]。 但是，由于存储位置不同，通常会批评其数据安全性，尤其是数据完整性[30]。 幸运的是，将区块链集成到边缘计算中极大地利用了边缘计算中的P2P数据存储机制与区块链的P2P去中心化数据有效性之间的相同性，以及它们在存储容量和安全性提供方面的互补性。

关于将区块链和边缘计算结合用于数据存储，首先应解决两者之间的差异，因为两者通常都指同一术语“数据库”。在分类账的意义上，有时区块链被称为分布式数据库[54]。但是，它只能处理简单的事务日志，而不能处理大量数据。即使有这些简单日志的负担，区块链的可扩展性仍在账本大小，吞吐量和延迟方面受到严重挑战。因此，将数据直接存储在区块链中是不可行的[55]。 [56]中的解决方案使用区块链中的分布式哈希表（DHT）设计链下存储，该分布式哈希表使用DHT中的（键，值）对提供数据引用，从而使区块链变成自动化访问控制管理器。开发到Enigma [57]中的脱链网络克服了数据完整性问题。随着PB级数据新时代的到来，将区块链连接到能够分散存储大量数据链的现有分散式存储或数据库变得更加可行。

1）通过区块链进行分散式数据存储：分散式存储系统利用对等网络的组合存储容量来存储和共享内容，已经在文件系统和数据库社区中进行了性能，可用性和持久性方面的广泛研究。在近年来流行的系统中，行星际文件系统（IPFS）是最强大的，经过深思熟虑的分布式存储解决方案。它综合了迄今为止最成功的系统中的许多最佳创意，并提出了一种用于数据交换的新颖协议BitSwap。 [58] [59]中的IPFS设计自下而上地经历了以下几层：网络，路由，交换，消息，命名和应用程序，这些进一步可视化为libp2p，IPNS（名称服务）和IPFS堆栈以分别移动，定义和使用数据。从其基础技术中可以找到更深刻的理解，包括DHT，块交换-BitSwap，版本控制系统-Git，自认证文件（SFS）系统。对于路由，DHT用于向网络通告添加的数据，并帮助定位所请求的数据。特别是为了提高效率，IPFS DHT根据存储的值来区分存储的值，该值直接存储较小的值，但仅存储较大值的引用。受BitTorrent启发的BitSwap通过添加具有BitSwap信用和策略的新功能，使IPFS能够快速，稳健地分发块。 Git中的Merkle DAG对象模型提供了以分布式方式捕获随时间推移文件系统树的更改的功能。 SFS是用于实现IPNS名称系统，该系统生成并验证远程文件系统的地址。

IPFS所做的创新将功能扩展到了分散数据存储的更广泛使用。在IPFS之上，类似于比特币的Filecoin [20]用作激励层，以形成一个完全分布式的文件存储系统。与比特币的仅用于计算的PoW不同，它引入了一类存储证明，其中复制证明（PoRep）允许证明者说服验证者某些数据已复制到其自己的专用物理存储和证明中。 -Spacetime（PoSt）使证明者可以说服验证者存储数据的时间。借助这些新颖的共识协议，Filecoin激发了强大的动力，促使矿工积累尽可能多的存储并将其出租给客户。另一方面，在文献[9]中提出了一种完全分散的基于区块链的数据完整性服务（DIS），该协议具有用于数据完整性验证的协议，其中以太坊智能合约和IPFS组合在一起以促进数据验证。同样基于以太坊和IPFS，提出了一种称为Desema的去中心化服务市场系统[60]，其中IPFS用于链下服务元数据以提供链上标识符，以便可以通过计算标识符来检查数据完整性。智能合约中的数据并将其与参考进行比较。

但是，还有其他值得注意的竞争者[61]，例如以太坊Swarm，StorJ和Maidsafe。 Swarm的主要目标是为以太坊的公共记录提供足够分散和冗余的存储，并且它似乎是通过智能合约强制执行的激励平台。 StorJ创建了一个使用区块链在网络上购买或出租磁盘空间的市场。 Maidsafe实施了以太坊等下一代分散，安全的网络“ SAFE Network”，并为StorJ提供了类似的服务。 在[62]中，Viktor Tron对Swarm和IPFS进行了全面的比较。 它表明，作为集成许多现有协议的统一解决方案，IPFS在代码成熟度，可伸缩性，采用，社区参与以及与专用开发人员社区的交互方面走得更远。 因此，对于某些项目，目前IPFS似乎是一个不错的选择。

2）可扩展的区块链数据库：由于区块链无法扩展以其当前形式处理大量数据，因此名为BigchainDB的可扩展区块链数据库通过将区块链特征添加到经过验证的可扩展大数据数据库中，解决了扩展问题[63][64]。 它避免了完全复制和困扰比特币的其他技术，但同时利用了现代分布式数据库和区块链的优势。 BigchainDB建立在大数据分布式数据库上，具有以下基本功能：NoSQL查询语言，高效的查询，许可以及高吞吐量和容量，可以通过添加节点来进一步增加。 包含区块链带来了分散控制，数字资产不变性和转移的能力。 在这里，我们列出了BigchainDB的一些关键点，如下所示。

•BigchainDB具有两个分布式数据库：将事务设置为待办事项的数据库S和具有形成区块链的块的数据库C。 每个数据库中都有一个内置的共识算法（例如Paxos解决一组可能有故障的不可靠处理器之间的共识），数据库之间有一个BigchainDB共识算法，通过该算法，在S中排序和收集的事务将被组装成一个块 在数据库C中。

•分散控制是通过类似于域名系统（DNS）的节点（签名节点）联合对区块中的交易进行表决来实现的，这些联合在数据库的内置共识之上运行。

•与直接引用典型区块链中的上一个区块不同，BigchainDB使用投票列表提供对上一个区块的引用，所有投票都应引用相同的区块，只有当节点发生故障时，例外情况才会发生。

使用不同的许可，该系统可以是从私有企业区块链数据库到开放式公共区块链数据库的配置。 新发布的版本包含许多修复程序和测试，可以更自信地谈论BigchainDB在极端情况下的行为[65]。

3）通过区块链名称系统存储：由于DNS是Internet的基本组成部分，因此Namecoin首先关注一些DNS缺陷，并使用PoW协议使用区块链创建去中心化DNS系统。 此后，吸取了Namecoin的许多经验教训，提出了一种由名为Blockstack [66]的区块链保护的全球命名和存储系统，作为去中心化应用程序的新Internet。 它在区块链分层，存储模型，名称定价模型，矿工激励方面做出了巨大努力。 与其他面向存储的加密货币区块链不同，Blockstack将托管数据与基础区块链的操作分离，从而可以更正确地使用存储系统。

Blockstack中有三层：控制平面中的区块链层，以及数据平面中对等网络层之上的数据存储层[67]。

•控制平面中的区块链为操作提供存储介质，并就操作顺序达成共识。 这些操作由基础区块链顶部的特殊虚拟链编码，该虚拟链基于基础区块链提供的抽象运行，其复杂性隐藏在其下。 在虚拟链中，定义了一些新操作，例如接受或拒绝虚拟链的规则，但是，这些定义未对基础区块链进行任何更改。

•在数据平面中，对等网络通过将路由信息存储到区域文件中来为发现信息提供全局索引，该区域文件的格式与DNS区域文件相同。 实际数据值以高性能托管在外部数据存储中，从而构成了存储层。 这种从实际数据到发现数据的分离存储允许多个存储提供商共存，包括云存储（S3）和P2P系统（IPFS）。

通过虚拟链中新定义的操作以及对等网络中所有区域文件的完整副本，构建了将人类可读名称绑定到发现数据的区块链名称系统（BNS）。 这种具有分布式控制的分散命名系统摆脱了故障的中心点。 在BNS中，查找名称的数据摘要如下：

•通过virtualchain搜索与给定名称配对的哈希。

•通过搜索此哈希在对等网络中获取相应的区域文件。

•从区域文件中获取存储后端URI，以链接到存储后端。

•读取具有访问权限的数据，并验证各自的签名或哈希。

得益于具有分层架构的分散式命名系统，Blockstack增强了Internet服务的安全性和可靠性，而没有任何性能损失。

我们只是从分布式存储，数据库和DNS以及代表性系统的角度介绍了基于区块链的存储。 它们的分散功能都非常适合边缘计算的地理结构。 但是，从技术和目标的角度来看，基于区块链的分散数据存储是基本功能，而基于区块链的数据库是存储的补充，可以与更高级别的计算应用程序并用，并与第三方存储和 Internet对Blockstack的支持似乎提供了服务器支持。

4）在雾/边缘计算基础架构中的使用：由于IPFS当前的成熟，已经完成了一些基于IPFS的边缘计算中数据存储的工作。在[68]中，作者基于IPFS的不可变对象（名称取决于内容）和由Kademlia DHT定位对象的专用机制来分析IPFS对雾的支持。详细而言，它通过在本地存储对象来支持数据局部性，当可以在Kademlia DHT中找到该位置并且存储节点可访问时，部分以断开模式工作，从而自然地通过透明地重新定位数据来实现移动性并扩展到大量网站。通过Yahoo Cloud System Benchmark（YCSB）在网络边缘对IPFS进行的测试表明，IPFS在访问时间和站点之间的网络交换容量方面的提升，明显优于Rados，开源对象存储服务和Cassandra，一个开源的分布式NoSQL数据库。 IPFS在边缘计算中的主要缺点是需要访问全局DHT，因此需要站点之间的大量网络流量以及增加本地读取的访问时间。为了解决这个问题，在[68]中提出了与横向扩展NAS系统耦合的IPFS。本地且独立地部署在每个雾站点上的横向扩展NAS在该站点内的所有IPFS节点之间共享对象，并且在本地存储要读取的对象时避免访问DHT。为了实现物联网数据的安全性和私密性，在[69]中提出了在区块链和IPFS的软件堆栈之上的模块化联盟架构，包括两个部分：私有侧链和联盟区块链。专用区块链由边缘服务器（验证器）为本地网络中的设备维护，全球联盟区块链连接边缘服务器。

本地区块链和数据存储：在本地私有侧链中，设备使用其自己的唯一公共和私有密钥对数据进行加密，然后将加密的数据发送到边缘服务器。 边缘服务器在计算和存储方面具有更大的功能，它扮演验证器的角色，并对尝试加入侧链的任何身份进行身份验证。 为此，智能合约必须具有以下功能：

•存储授权设备的公钥及其IPFS文件的哈希。

•控制访问，以便仅允许来自授权设备的数据连接验证器。

身份验证成功后，边缘服务器将在新区块中记录“数据创建”交易，然后更新IPFS文件及其存储在智能合约中的哈希。

财团区块链和数据请求：具有边缘服务器（验证器）的分散财团网络负责外部请求者对特定侧链中特定数据的访问控制。 通过联合体区块链和侧链中访问策略的组合对访问进行身份验证，包括以下步骤：

•请求者使用其私钥签署访问请求事务。

•验证者节点使用密钥对联合体区块链中的请求者进行身份验证。 如果请求者未经授权，则该交易将被丢弃。

•根据财团区块链中的授权请求者，将验证所请求侧链中的身份验证。

•通过两个认证后，请求者将收到目标IPFS文件的加密哈希，可以使用私钥对其进行解密，从而访问目标数据。

为了实现数据隐私和安全性，联盟区块链中的智能合约必须能够修改访问策略和授权请求者列表，例如从授权列表中删除请求者以防止其连续出现的数量泛滥 不成功的请求超出了许可。

C.计算

除了网络控制和存储外，边缘计算的关键作用还在于将计算密集型任务的计算任务从能力较弱的设备转移到功能强大的边缘服务器，这可以延长设备的电池寿命并加快计算过程。

1）边缘的计算卸载：在边缘的本地网络中，移动设备或IoT设备通常计算能力较低且功耗较低。 这个限制对于区块链的应用变得至关重要，特别是在PoW的挖掘过程中[70]。 作为解决方案，将具有足够资源用于区块链计算的接近末端的边缘服务器用于从相邻设备上卸载作业，以便使用支持哈希，加密算法以及可能的共识（如PoW）的本地计算功能来在设备上部署区块链。

为了对区块链进行高效的边缘计算资源管理，提出了一些优化模型。 [71]中的作者研究了移动区块链的边缘资源分配，并开发了一种基于深度学习的拍卖方案，其中基于分析解决方案构建了多层神经网络架构。 使用矿工的评估值训练神经网络，并通过随机梯度下降（SGD）求解器优化网络参数，以最大程度地减少损失函数，该损失函数是计算提供商的预期负收益。

在[72]中，基于区块链挖掘实验的结果，定义了一个哈希功率函数，该函数表征了每资源量成功挖掘一个区块的概率。 考虑到设备之间对计算资源的竞争，在模型中考虑了分配外部性。 在拍卖机制中，社会福利最大化，同时又保证了真实性，个体合理性和计算效率。

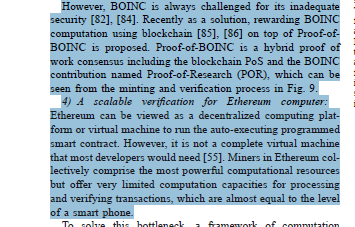
提出了一个两阶段的Stackelberg游戏来模拟计算提供商与矿工之间的互动[73]。具有计算资源的边缘服务器在游戏中扮演领导者的角色，设定了每个计算单元的服务价格，以最大化其利润。 根据提供者设置的价格，需要挖掘块的设备（即较低阶段的追随者）为卸载采矿任务确定最佳计算服务量。

另一方面，由于与云计算相比单个边缘节点的计算能力较低，因此通常需要将计算任务分配给多个边缘节点。 在这种分散式计算中，效率和安全性都是关键问题。 因此，在区块链上运行的分布式计算成为最有前途的方法，其中区块链既可作为激励又可作为验证。

2）在区块链上进行安全的多方计算：[74]中有关区块链与计算的集成的早期工作研究了如何在比特币上进行多方计算（MPC）。SecureMPC是密码学的一个子领域，允许一组互不信任的各方进行加密。共同根据其私有输入计算功能，然后使用比特币为MPC构造一个定时承诺版本。提交者负责以一个秘密值启动MPC，但是如果在指定时间内未完成秘密的披露，还必须强制退还保证金并从押金中扣除。因此，可以获得某些多方协议的公平性。同时，[36]中的作者使用比特币来激励正确的计算。在其可验证的计算方案中，求解程序可以提交正确性证明以及答案，答案将由矿工或指定的验证者进行检查。 [75]提出了一种安全的带补偿的MPC协议，如果对手发起拒绝服务攻击而诚实的人收取补偿，则对手必须遭受金钱罚款，因此，不仅可以保证公平性，而且还可以保证鲁棒性。稍后在[76]中，使用罚分来提高效率，其中非反应性设置和反应性设置中的脚本复杂性均得到有效降低。最近在[77]中提出了一种有效的协议，用于对带有罚款和安全现金分配的安全MPC进行摊销。在加密货币的初始阶段之后，各方可以在玩很多扑克游戏的过程中仅在彼此之间进行交互，在其中货币易手。在特定应用中，MPC用于Enigma [57]中的数据查询，Enigma是一个使用区块链存储和计算数据的平台。为了降低通信复杂度，提出了分层安全的MPC，其代价是增加了并行化计算的复杂度。在这一研究领域中，由于MPC的原始安全性和可验证性，区块链主要解决了公平性和隐私性问题。

3）网络计算和区块链：伯克利开放式网络计算基础架构（BOINC）[81]是由美国联合王国开发的网络计算平台。伯克利太空科学实验室。它是SETI @ home闻名的客户端-服务器Internet规模模型的通用实现。请注意，SETI @ home利用位于Internet边缘的机器，以边缘为中心的计算云从中获得灵感。它首先是一种用于志愿者计算的开源软件，其中每个项目都运行自己的服务器和参与者（客户端），范围从通用GPU，多个强大的CPU到具有应用程序编程接口（API）的无处不在的智能手机。和工具。为了提高系统响应时间，BOINC与云的结合引入了虚拟化技术，以创建志愿者云系统[82]。为了突破志愿者的固有局限性，可伸缩的云资源用于按需短缺项目[83]，其中客户端从志愿者计算架构更改为基于云计算的服务即基础架构。在开发基于BOINC的大数据挖掘应用程序[84]的过程中，需要一个高速本地网络来连接计算资源并释放要在客户端之间传输的海量数据集。可以看出，BOINC平台正从P2P科学计算发展到P2P云计算/边缘计算，以实现高计算任务，特别是大数据应用。

P15



However, BOINC is always challenged for its inadequate

security [82], [84]. Recently as a solution, rewarding BOINC

computation using blockchain [85], [86] on top of Proof-of-

BOINC is proposed. Proof-of-BOINC is a hybrid proof of

work consensus including the blockchain PoS and the BOINC

contribution named Proof-of-Research (POR), which can be

seen from the minting and verification process in Fig. 9.

*4) A scalable verification for Ethereum computer:*

Ethereum can be viewed as a decentralized computing platform

or virtual machine to run the auto-executing programmed

smart contract. However, it is not a complete virtual machine

that most developers would need [55]. Miners in Ethereum collectively

comprise the most powerful computational resources

but offer very limited computation capacities for processing

and verifying transactions, which are almost equal to the level

of a smart phone.