区块链及其在物联网中的应用

云 霜

物联网可实现物物相连、物人相连、人与人之间任何时间、地点的有效连接。物联网正在快速发展，据预测，到 2020 年物联网设备将会达到 260 亿美元，是 2009 年部署的设备的 30 倍。此外，一些报告预测 M2M 通信将会增长到 3.3 亿，涉及领域，包括：智能家居，交通，国防和公共安全，可穿戴设备或者增强现实。

物联网环境下的主要的访问控制方法有：基于角色的访问控制 RBAC、基于属性的访问控制 ABAC、基于使用控制模型的访问控制 UCON 和基于权能的访问控制 CapABC[1]。上述 RBAC，ABAC 和 UCON 物联网 IOT 解决方案依赖于中心化服务器-客户端架构，通过互联网连接云服务器。为了满足增长，去中心化架构 CapABC 被提出过以创建大型的 P2P 无线传感器网络。CapABC 实现了轻量级的分布式控制、动态性、可扩展性，但 CapABC 不能保证安全性，也无法保证用户的隐私，直到区块链技术的出现。如图 1 所示，从过去的封闭式中心化框架演进到开放式云中心化架构，而下一步是将云功能分布到多节点中，区块链技术可在下一步趋势中起到很大的作用。

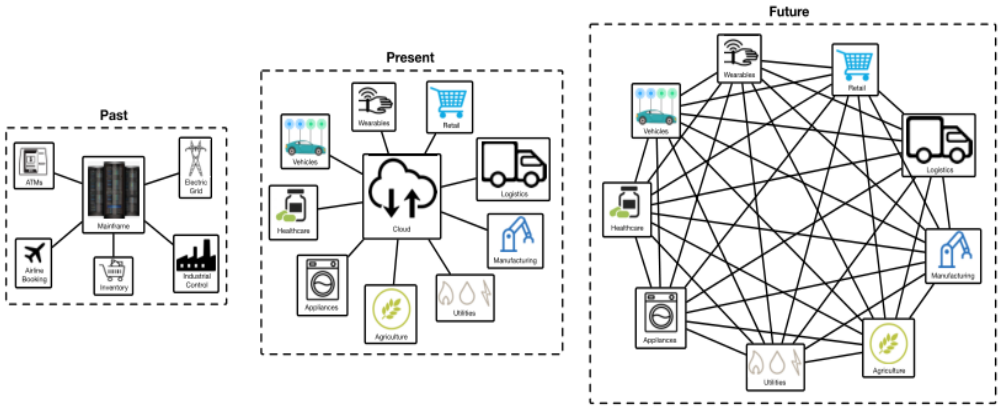

图 1　过去、现在以及未来的物联网架构[2]

一、区块链技术介绍

1、区块链对于物联网应用的优势

区块链是一种去中心化的分布式技术，以密码学算法为基础的点对点分布式账本。区块

链技术基于哈希链以及时间戳机制保证数据能够被追踪，基于共识算法保证节点间数据的一致性，使创建去中心化的应用成为可能。区块链技术可以在大规模IoT系统中解决以下挑战：

大多数IOT解决方法仍然很昂贵，因为部署的和维护中心云和服务器的成本高。当不由供应商来提供上述设施时，这些成本转移至中间商。

维护也是一个大问题，当需要对数以百万计的智能设备定期升级软件时。

在发生斯诺登泄露事件后，对于IOT采用者很难相信其他技术合作伙伴，给予他们权限访问与控制，允许他们收集和分析用户数据。因此，私密和匿名应当是IOT未来发展的核心。

封闭源代码也导致了信任缺失。为了增加信任和安全，透明性很重要，所以当开发下一代IOT解决方案时，开源方案应当被考虑进去。代码仍然容易受到攻击，但是，由于它可以被许多用户长期审视，它不太容易受到第三方的恶意修改。

2、区块链技术基础知识

在过去两年中，区块链技术以令人震惊的速度发展。根据报告，从2013年到2016年，区块链中的投资从9300万美元上升到5.5亿美元。此外，区块链技术的市场预测到2021年增长到2.3亿美元。

区块链起源于一种叫做比特币的加密货币的底层记账系统。区块链具有以下特性[3]:

1.去中心化。区块链技术不依赖于第三方机构或硬件设施，没有中心管制。

2.开放性。区块链技术是开源的，数据对所有人开放，任何人都可以通过公开接口查询区块链数据和开放相关应用。

3.独立性。基于协商一致的规范和协议，所有节点能够在系统内自动安全地验证、交换数据，不需要任何认为的干预。

4.安全性。只要不能掌控全部数据节点的51%，就无法肆意操控修改网络数据。

5.匿名性。除非有法律规范要求，各节点身份信息无需公开或验证。

基于区块链的加密货币的使用能够对支付起到革命性改革。由于去掉了中间商，商品费用可以降低，用户无需为转账等待多天，可以立即收款。现代加密货币可以分为3个元素：区块链，协议和货币。

对于加密货币，区块链充当一个分类账本，存储所有的已执行货币交易。也就是说，区块链持续性增长，每固定时间间隙增加新的区块。一个完整的节点拥有一份完整区块链的副本，其中包含了用户地址和余额的信息。

因此，区块链的主要贡献在于提供了一个交易不依赖第三方的方式。上述方式要归功于去中心化的旷工，他们审查和验证每一笔交易。这一贡献使得比特币的区块链技术能够为拜占庭将军提供解决方案，因此它能够让不信任的多方就某件事达成一致，交换信息。对于加密货币而言，这个问题就是双重支付，涉及如何在没有信任的第三方验证的情况下，尚未花费并记录在交易和用户余额上的一些金额。

区块链类似于一个不可篡改的分布式账本系统，其中数据共享于对等网络中。如前所述，其被认为是比特币的主要技术，因为它解决了长期存在的金融问题，称为双重支付。比特币提供的解决方案为大多数采矿节点达成共识，将有效交易附加到区块链中。区块链，就如其名而言，其由数据块为单位的交易通过哈希算法连接起来按照时间戳组成的链式数据结构，如图 2 所示，区块分为区块头和区块体，通过区块头中封装的前一个区块的哈希值将区块链接起来形成一个链式结构,具有账本公开、可追踪、不可篡改的性质。

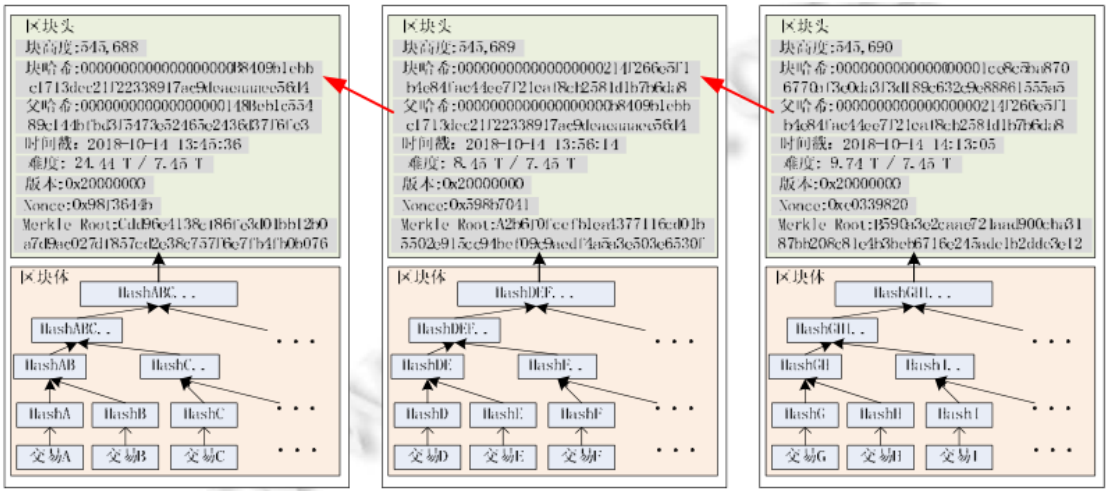

图 2 比特币中区块链的数据结构[1]

为了使用区块链，首先需要建立一个 P2P 网络。网络中的节点接收 2 个密钥：一个用来加密发送信息的公钥，一个用来接收消息的私钥。因此，两个密钥一个用于加密，一个用于解密。实际上，公钥用于签发区块链交易（例如，允许交易），同时公钥就像一个独特的地址，仅当具有正确私钥的用户能够解密对应的加密公钥。我们称这种加密方式为不对称加密。

当节点执行交易时，当前节点会对其进行数字签名，并广播至其他节点。签名交易采用独特的方式（私钥）来验证（当且仅当具有特定私钥的用户能够签名），并且保证完整性（如果数据传输中出现了错误，那么不会对数据解密）。当广播交易的其他节点接收签名的交易，验证交易是否有效，从而促进其通过网络发送。以此方式进行交易，被叫做矿工的节点通过排序和打包至时间戳的链式数据结构中，从而被认为是做有效的方式。矿工的选择以及区块

链中的数据依赖于共识算法。被矿工打包的数据块被广播回到网络中。然后，区块链节点验证广播的数据块是否包含有效的交易，并通过对应的哈希算法来参考之前的数据块。如果上述条件都不满足，则丢弃该数据块。但是，如果条件满足，节点将数据块添加至链中，从而更新交易。

基于管理的数据、数据的可用性、用户操作的方式，区块链可分为不同的类型。即可以区分为公有和私用，许可的和无权的区块链，如图 3 所示。

在公有区块链中，任何人都可以加入区块链（不需要获得第三方的允许），充当一个简单的节点或者矿工。矿工通常被给予奖励在公有区块链中，例如比特币，以太坊或者莱特币。

在私有区块链中，所有者限制网络的访问。很多私有区块链也是许可区块链，以掌控用户交易，实现智能合约或者充当矿工，但是，不是所有的私有区块链都必须许可。

区块链可以区分为基于跟踪数字资产的区块链（比特币）和基于逻辑的区块链（智能合约）。此外，有一些系统采用令牌，其他则不用。

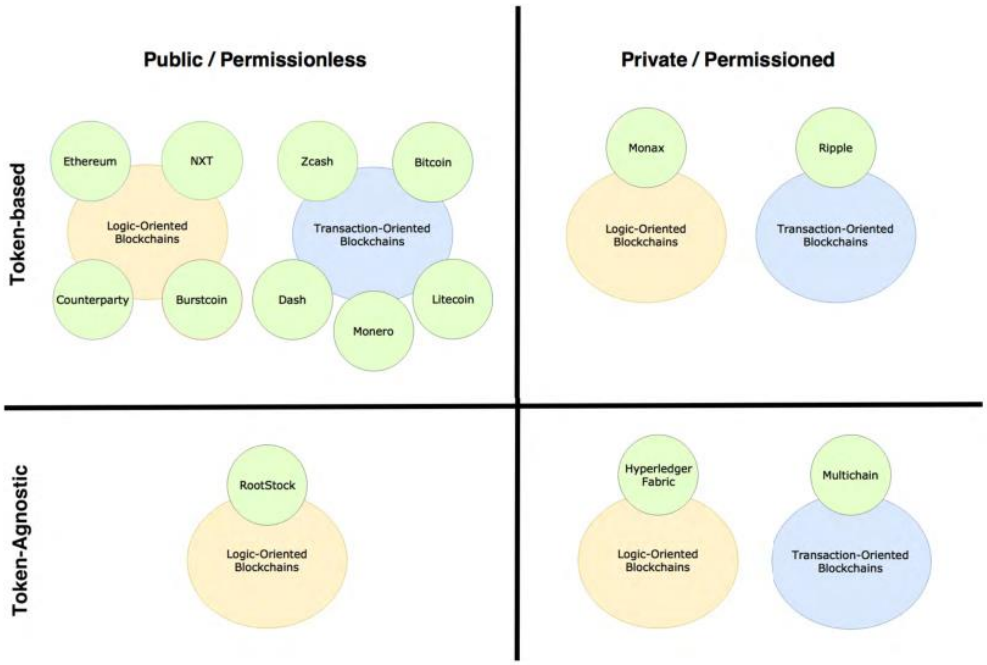

图 3 区块链的分类[2]

3、区块链是否适用于物联网应用的判断因素

需要强调的是，对于每个物联网应用来说，区块链并非最佳解决方案。具体来说，开发者应当从以下的方面考虑区块链是否适用：

1.去中心化。当没有可靠的中心系统时，物联网应用需要去中心化。但是，许多用户仍

然盲目地相信某些公司，政府机构或者银行，所以如有相互的信任，则不需要区块链。

2.对等网络交换。在物联网中，对等节点之间的通信不太常见，除了一些特定的应用，例如智能集群或雾计算系统。

3.交易系统。一些物联网应用需要通过第三方实现金融交易，但是一些不需要。此外，金融交易仍然可以通过传统交易系统实现，尽管他们需要支付手续费以及需要信任银行和中间商。

4.公共顺序支付登录。许多 IOT 网络收集数据，这些数据被打上时间戳和按照顺序存储。但是，传统数据库能够简单地实现上述需求，特别是安全或者攻击很少的情况下。

5.分布式系统。分布式系统可以构建在云端上、服务器上或者其他传统的分布式计算系统上。分布式系统不应当作为采用区块链的一个充分理由，除非在分布式计算系统中缺乏信任。

6.微交易收集。一些物联网应用，需要记录每一个交易，以在审计方面或者大数据应用情况下维持可追溯性。在这些应用场景下，可以适用侧链。但是，其他应用场景不需要存储每一个收集的数据。例如，在远程农场监控中，其中通信费用昂贵，通常将物联网设备每小时唤醒以获取环境信息，可以将一段时间内的交易存储在本地，再一次性上传。

图 4 具体描述了是否需要采用区块链的流程图。

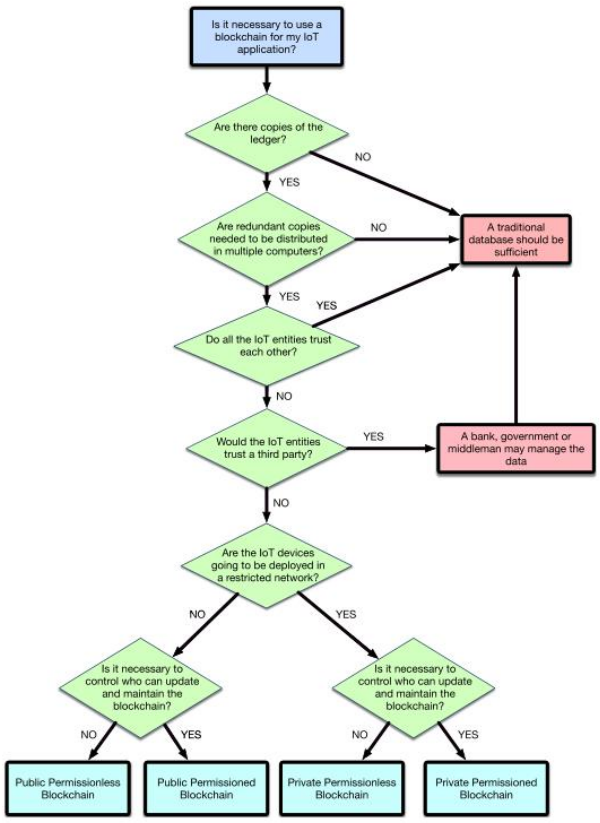

图 4　采用区块链的流程图[2]

二、物联网区块链应用现状

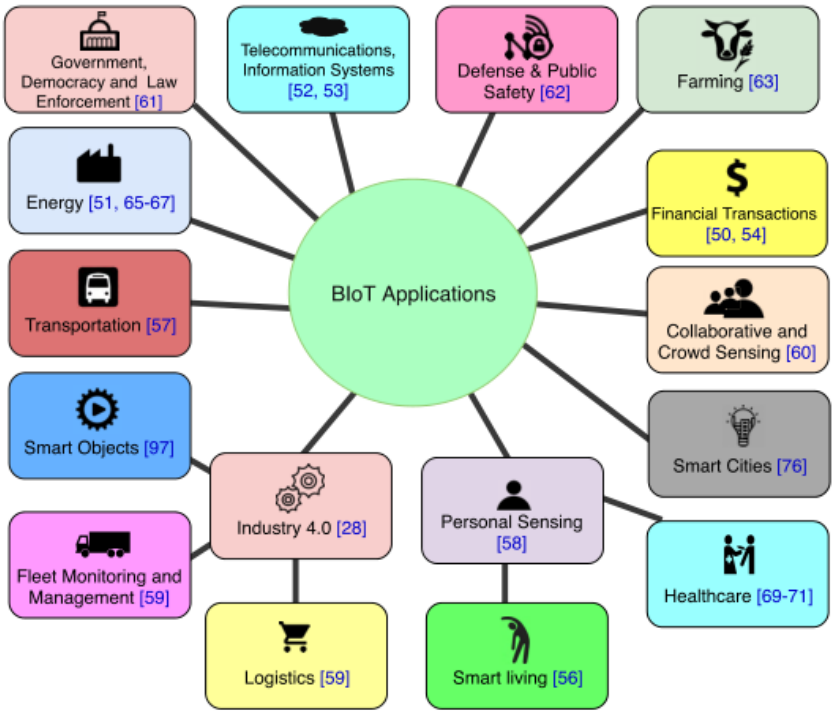

图 5 物联网区块链应用领域[2]

如图 4 所示，除了加密货币和智能合约，区块链技术可以应用到涉及物联网应用的不同领域，如传感、数据存储、身份管理、时间戳服务，智能生活应用，智能交通系统，穿戴式设备，供应链管理系统，移动人群感知等。

区块链还可以用于物联网农业的应用。例如，农产品供应的溯源，基于 RFID 和区块链，用以增强食品安全和质量，并减少物流方面的损失。

通过区块链管理 IOT 设备。例如，一个远程管理和配置物联网设备的系统。该系统存储公钥在以太坊中，但将私钥存储于每一个 IOT 设备中。

能源部门也可以从区块链应用或能源互联网中受益。一个基于区块链的系统允许 IOT 设备相互支付，在没有人工介入的情况下。

基于区块链的物联网可应用于医疗领域中。利用物联网传感器和区块链技术验证数据完整性和访问药品供应链的温度记录。验证对医疗产品的运输至关重要，以保证产品的质量和环境条件。因此，每一个传输的包裹包含一个传感器，该传感器传输收集的数据至区块链中，其中智能合约判断接收的数据是否保持在允许的范围中。

区块链还可以增强物联网底层设备的安全性。特别地，区块链能够改进远程认证，远程

认证用于验证一个设备是否值得信任。

最后，大数据可以应用区块链技术，来采集和控制来自 IOT 网络中大批量数据。

三、区块链在 IOT 应用的关键技术

1、架构

对于一个云架构，由云来实现大多数处理。因此，对于传统云中心的 IOT 架构存在漏洞：云是一个失败点，这是因为如果网络攻击、维护、软件问题导致云故障，整个系统将停止运行。此外，需要强调的是，通过 DOS 攻击能够导致整个网络破坏，窃听私人数据，篡改收集的数据或者误导其他系统。因此，一旦连接的云或者其他中心服务被破坏，物联网上的其他节点可能被泄露。相反地，区块链并不依赖任何中心服务器或者云，此外，当检测到故障设备的恶意行为，整个系统可以拒绝更新。

雾计算基于一组本地网关，通过特定服务快速响应 IoT 节点请求。这样的节点可以相互交互，如果需要的话，也与云交互。在图 5 中，雾本地网关由 SBCs 标识，SBCs 是低成本和低能耗的计算机。雾计算实际上被认为是边缘计算的子集，其最近几年被认为是支持区块链以及 DAGIOT 应用的最有效的架构。如图 5 所述，在边缘计算层，除了网关之外还具有一微云计算，其实际上包括一个或者多个低配置云的计算机。微云计算的主要优势在于：当应用雾计算网关时则不能有效传送时，对节点层深度计算任务作出高速反应，。

IBM’S ADEPT 提升了 IOT 系统的去中心化能力。ADEPT 安全、可扩展且能实现自主的点对多点传输。ADEPT 指出 IOT 设备应当能够实现自我认证和自我维护。此外，IBM 认为采矿限制了可扩展性并且导致了计算开销大。因此，ADEPT 采用 P0S 和 POW，来保证网络的完整以及安全。

有作者提出了一个理论上的轻量级模型，其考虑到安全和隐私，并通过采用区块链的方式减少了通信开销。所提出的系统面向家庭自动化，且其体系结构分为三部分层:具有传感器、执行器和本地存储器的智能家居层;一个由对等节点和共享存储组成的覆盖网络;还有云，其提供远程存储服务。在低层(智能家居和覆盖层)，存储器由传统的存储服务器以及区块链组成，无论是公共的还是私有的。通过消除 PoW 共识来实现减少开销，因此每个块都被挖掘并附加到没有额外交付的区块链。这种方式简化了区块链。

还有作者提出了一种基于区块链的理论体系结构，该体系结构关注于提供物联网服务和

连接异构设备。该体系结构利用分层和多层区块链，实现了一个叫做 CONNCET 的上下文服务发现系统。

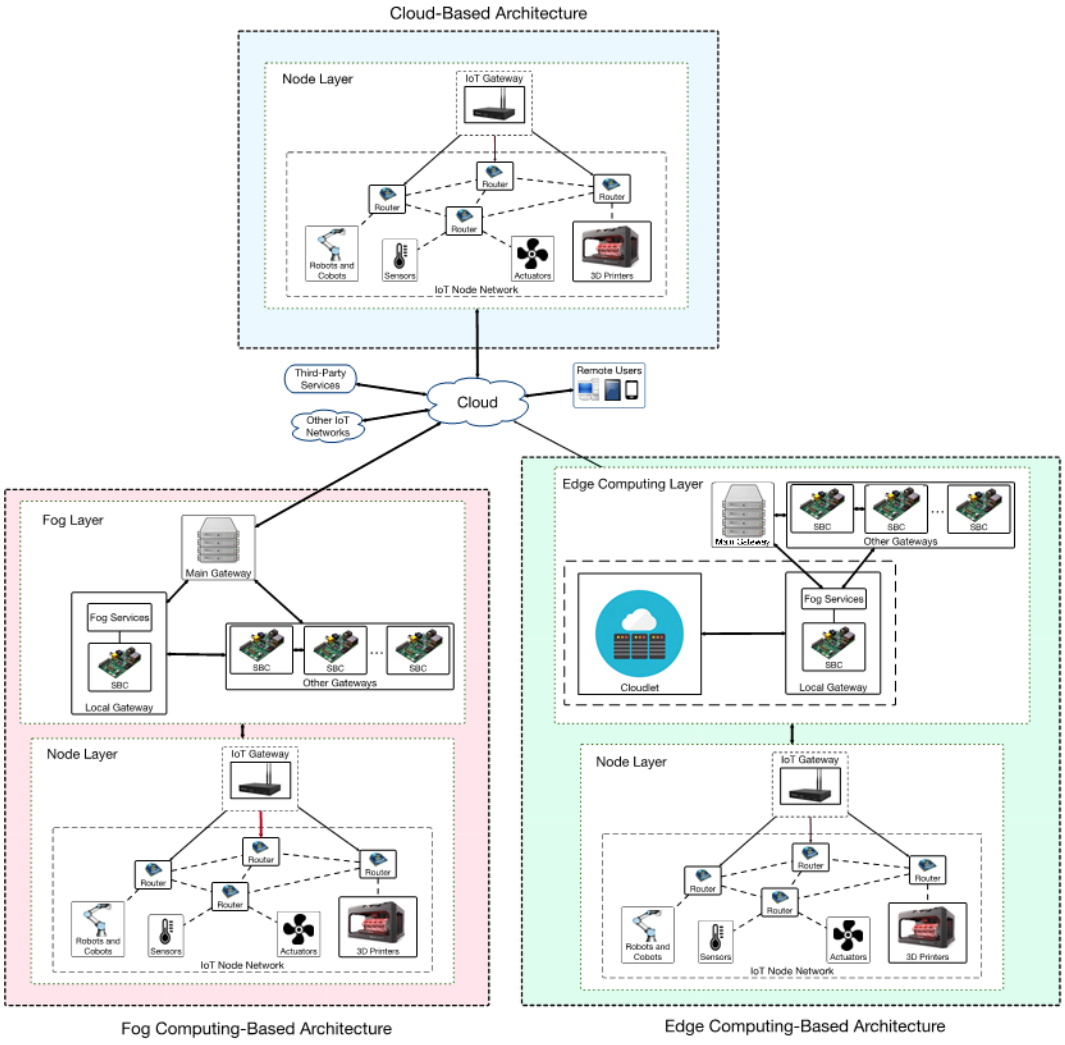

图 6 传统的物联网架构演进[2]

此外，可基于区块链技术实现多层物联网架构。该架构通过将物联网生态系统划分为多个层次，并在每个层次上利用区块链，来降低了部署区块的复杂性。该架构既利用了云的强大功能，又利用了区块链的安全性和可靠性。

还有一种稍微不同的方法，评估了使用云和雾计算架构来提供 BIoT 应用程序。该系统，在大量交易的负载下，雾计算系统的延迟响应明显快于基于云的系统。

另一种基于边缘计算，它是基于 IEC61499 标准的分层分布式平台，该平台支持分布式自动化控制系统。这样的系统可以分为两层:控制设备及过程的底层和管理底层的顶层。

软件定义网络(SDN)也被建议用于实现 BIoT 架构。例如，一种基于区块链的架构，利用

SDN 来控制物联网的雾节点。该系统利用云来执行计算密集型任务，同时通过雾计算来提供低延迟的数据访问。雾节点是分布式的，提供服务，并与区块链交互。该体系结构降低了时延，提高了吞吐量，能够检测到对物联网网络进行的实时攻击。由于使用了区块链和 SDN 算法，该架构能够平衡雾节点之间的负载。

2、加密算法

公钥的加密对于提供区块链中的加密安全性以及隐私性至关重要。然而，资源受限的物联网设备难以满足现代安全加密方案的计算需求。因此，在选择正确的加密算法时，不仅要考虑计算负载和内存需求，还要考虑能耗。

最常见的公钥密码套件是 RSA 算法以及 ECDHE 算法，其是 NIST 推荐的传输层算法。

哈希函数是区块链中的关键，因此，他们需要对交易签名。因此，哈希函数需要保密性好，快速且能耗低。最常用的区块链哈希函数是 SHA-256D 和 Scrypt。SHA-256 已经在不同的物联网设备上进行了评估，比如，可穿戴设备。

为了追踪区块链上的修改，交易必须被签名和打上时间戳。可以使用不同的时间戳机制。传统的方案依赖于服务器的可靠性，服务器使用自己的私钥对交易进行签名和时间戳。尽管如此，仍然不能阻止服务器签名过去的交易。因此，不同安全机制被提出。例如,比特币中,其中每个时间戳的包括一个之前的时间戳的哈希值,以维护交易的顺序,并让插入虚假交易难以实现。此外，可以分布时间戳，从而避免了单点故障的问题。虽然这样的分布式系统容易受到攻击，但比特币使用 PoW 机制来解决这些问题。

3、共识机制，采矿以及信息验证

区块链中的共识机制解决了区块分布式存储的一致性问题，也就是拜占庭将军问题。比特币采用的是 PoW 共识机制，粗暴地通过算力证明解决了女巫攻击(Sybil attacks).

其他的一些共识算法包括如下：

PoS：它比 PoW 需要更少的计算能力，因此它消耗的能量更少。在基于 pos 的区块链中，假设网络上参与度较高的实体被攻击的可能性越小。因此，矿工们需要周期性证明他们持有一定数量的货币。该机制看似不公平，因为最富有的参与者能够掌控整个区块链，所以对该算法进行了改进。例如，具有最大年龄和最多货币的实体更可能挖掘出区块。

DPOS 和 POS 很相似，其选举出代表来生成和验证区块。由于更少的节点参与在区块的

验证中，因此，相比于其他机制，交易能够更快速的完成。其外，选举出来的节点能够适应区块大小和间隔，如果他们存在欺骗行为，则很容易被替换。

TaPos 是 PoS 的变种。在 POS 系统中只有一些节点参与到共识中，但 TAPOS 中所有参与区块生成的节点都会负责维护网络的安全。

PoA 共识算法被提供，由于 PoS 系统的限制：即使节点没有连接到网络，持币的年龄依旧在累积增长。因此，PoA 系统中同时考虑鼓励货币持有和节点的活动。

PBFT 共识算法，解决了异步环境下拜占庭将军问题。PBFT 假定只有不到三分之一的节点是敌对的。对于要添加到链中的每个区块，将选择一个领导节点负责对交易进行排序。选择的节点必须得到至少 2/3 的节点的支持。

Ripple 共识算法，在共识判定时，Ripple 服务器依赖于一些可信的节点使用同步的通信方式，从而减少了延迟。

SCP 和 PBFT 类似，但 PBTF 中每个节点查询其他节点并等待大多数同意。在 SCP 中节点只需等待它们认为重要的节点的同意。

BFT 共识算法基于 raft 算法，其目标在于浅显易懂，但导致实际中很少采用，例如，节点只有停止才会失败。因此，BFTRaft 增强了容错能力，并提高了其对各种威胁的安全性。

Sieve 共识算法由 IBM 出，并在超级账本中已经实现。它通过 BFT 复制在认可的区块链上运行非确定性智能合约。在这种情况下，Sieve 复制与非确定性智能契约相关的流程，然后比较结果。

Tendermint 共识算法中，即使有多达 1/3 的机器出现任意故障的情况下，Tendermint 仍然能够正常工作。称作“验证人”的区块链参与者对交易进行提议并投票。一个区块的验证分为 2 个步骤：预投票和预提交。只有超过 2/3 的验证人在一轮中预提交，才会提交成功。

Bitcoin-NG 共识算法，目标在于提高可伸缩性，吞吐量和延迟。开发人员对 1000 个节点进行了实验，实验结论是，Bitcoin-NG 具有良好的伸缩性，受节点带宽限制，延迟和网络传输时间有关。

PoB 共识算法需要矿工燃烧一些加密货币，以证明他们挖矿的决心。POB 背后的思想是，用燃烧货币代替 POW 中的燃烧计算力，因为货币和算力一样都需要代价。

PoP 共识算法采用环状签名和集体签名，从而将物理身份绑定到虚拟实体，并保持匿名。PoI 和 PoP 相似，其在以太坊中开发。

4、区块链升级/维护以及协议堆栈

物联网网络的建设需要部署大量的设备。这些设备嵌入了某些固件，这些固件通常会被更新以纠正错误、防止攻击或仅仅是为了改进某些功能。传统上，物联网设备必须手动或使用无线更新。这些更新可以通过使用区块链来执行，这使得物联网设备能够安全地传输新版本。

关于协议栈，一些作者建议对传统 OSI 栈进行修改，使其适应区块链技术。最相关的就运行在 TCP/IP 上的五层(如图 6 所示)。这五层包括:

•创建分类账并发行资产的分类账层。

•支付和交换层。

•寻路层，计算出最优的集合，以自动执行最佳转账或交换金额。

•契约层，运行代码控制平衡。

•应用层，允许开发应用程序和用户界面。

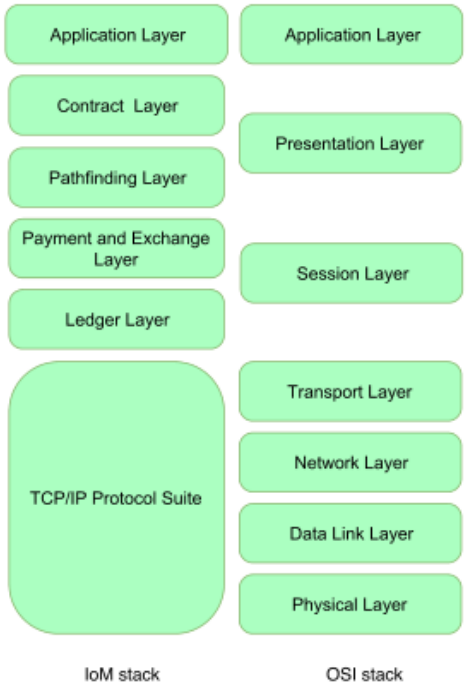

图 7 区块链与传统 OSI 协议栈[2]

四、区块链技术在物联网应用的发展挑战

尽管 BIoT 具有良好的前景，在开发和部署现有和未来的系统时，仍然存在以下挑战：

•复杂的技术挑战:需要解决关于 BIoT 应用程序的可伸缩性、安全性、加密开发和稳定性需求。此外，区块链技术在交易能力、失效协议或智能契约实现方面面临设计限制。

•互操作性和标准化:采用 BIoT 需要所有利益相关者的妥协，以实现完全的互操作性(即，从数据到策略互操作性)以及与系统的集成。

•区块链基础设施:需要创建一个全面的信任框架或基础设施，以满足在物联网中使用区块链的所有要求。

•组织、治理、监管和法律方面:除了技术挑战，还要塑造监管环境。

•快速测试机制:在不久的将来，需要为不同的应用程序提供不同的区块链并进行优化。

参考文献

[1] 史锦山,李茹, 物联网下的区块链访问控制综述, 软件学报, 2019,30(6):1632−1648

[2] TIAGO M,PAULA FRAGA,A Review on the use of Blockchain for the Internet of Things,IEEE Access,2018, 6,32979-33000

[3]姚忠将，葛敬国，关于区块链原理及应用的综述，科研信息化技术与应用，2017,8（2）：3-17

临菲信息技术港

临菲信息技术港 公众号

临菲学堂