用区块链技术保障物联网安全

由区域链分布式账本工作组提供

cloud security alliance®

关于 CSA

云安全联盟是一个非营利组织，其使命是促进在云计算中提供安全保证的最佳实践，并提供关于云计算用途的教育，以帮助确保所有其他形式的计算。云安全联盟是由行业从业者、公司、协会和其他关键利益相关者组成的广泛联盟。如需进一步信息，请访问我们的 www.cloudsecurityalliance.org 或在推特@ cloudsa 上关注我们。

目录

致谢

主导者

Sabri Khemissa

主 要 贡 献 者

Alex Brown
Giuliana Carullo
Elier Cruz Kevin
Fielder Doug
Gardner Jas
Khehra Imre
Kocsis Paul
Lanois Ashish
Mehta Matt
Murphy Todd
Nelson Denis
Nwanshi Luc
Poulin Michael
Roza
Brian Russell Srinivas Tatipamula
Udo Gustavo von Blücher

CSA Staff: CSA 员工

Hillary Baron
Kendall Scoboria
John Yeoh

中文翻译

北京老李

序言

2016年10月份，攻击者利用15万个安全性不够的物联网终端设备对美国主要域名服务器提供商DYN的服务器发起DDOS恶意攻击，导致美国大规模互联网瘫痪，受害企业横跨支付、餐饮、网络社交、财经媒体等多个不同领域，包括PayPal、星巴克、Twitter、《华尔街日报》在内的众多网站都无法访问。

物联网安全威胁真正引起了人们的关注，但是，保障物联网设备的安全具有极度的挑战性，各设备之间的通信互信是物联网安全的基石，由于大多IoT设备成本很低算力不足，传统的安全技术在物联网设备上过重而很难实施，区块链技术有着先天的分布式可信模式，采用轻量级区块链技术保障物联网设备的可信与安全成为云安全联盟的独特研究思路。本白皮书是物联网与区块链结合的投石问路之作，CSA全球与大中华区的专家们给广大读者又一专业奉献。

中国云安全与新兴技术安全创新联盟常务副理事长
CSA云安全联盟大中华区主席
李雨航 Yale Li

简介

在过去的四年中，技术专家、首席数字官、营销经理、记者、博客作者和研究机构讨论 并推广了一种新的分布式模型，将区块链技术应用于安全事务处理和存储。国际数据公司 IDC FutureScape 预测，到 2020 年，全球 20%的贸易融资将纳入区块链。

1、Coindesk 报告说，过去几年，风险投资在区块链的创业公司投资超过 18 亿美元。

2、区域链的财团和联盟已经涌现，例如企业以太坊联盟，它是致力于识别跨部门的区块 链技术的新用例。

区块链是一种公共的和分布式的交易分类账簿，它能够承诺：

1.提高数字资产所有权转让的速度、效率和安全性。

2.消除中央主管（权利）机构认证所有权和清算交易的需要。

3.通过提供透明和公开的审计的分类账目来减少欺诈和腐败。

4.使用可根据特定条件自动激活、保护和验证可信操作(“智能合约”)的协议降低管理 成本。

与采用区块链相关的一个关键挑战是需要确定相关的用例，这些用例将从区块链技术的集成中获益。物联网(IoT)长期以来一直与安全漏洞（脆弱性）和挑战联系在一起，专家和组 织已经开始探索利用区块链来保护物联网的安全。像 IOTA 和可信物联网联盟这样的组织已经开始通过应用区块链来关注物联网的安全性。

物联网本身正在改变消费者的行为和业务流程。分布式边缘物联网设备采集和传输数据进行处理。物联网系统依靠这些数据向最终用户提供先进的服务、自动化的特性和定制体验。 物联网系统是动态和分布式的。它们包括设备、移动应用程序、网关、云服务、分析和机器学习过程、网络基础设施、网络（WEB）服务、存储系统、雾层和用户。所有这些系统都可以写入和读取数据，这些数据可以被记录为分类帐簿上的事务。

自 2014 年以来，云安全联盟物联网工作组(IoT WG)一直致力于物联网安全的最佳实践的文档化。鉴于将区块链技术应用于物联网安全问题的潜在好处，物联网工作组与 CSA 区块链/分布式分类账技术工作组合作研究并记录了区块链可以开始帮助确保物联网系统安全的一些方法。因此，本文讨论了两种不同成熟度级别的技术：

区块链：通过支持快速发展的加密货币如比特币、以太坊、莱特币和达世币，推动了数字经济的彻底变革和颠覆的技术推动。区块链作为加密货币基础的成功案例，在业界催生 了新的研究，旨在是利用分布式分类账目技术来保障系统和技术的安全。在 2017 年，许多商业计划的重点是创建有限的原型和概念证明，这些概念主要是为了掌握这一复杂技术的的 复杂之处。

物联网：一套快速成熟的技术，支持业务和任务流程的转换。物联网在消费者、交通运输、能源、医疗、制造业、零售和金融等行业已经达到了不同程度的成熟度。物联网是物理设备之间的互联互通。作为连接的车辆、智能建筑、工业控制系统、无人机和机器人系统以及其他嵌入电子、软件、传感器、执行器和网络连接的物品，这些东西能够使这些物体交换数据。

本文描述了区块链技术的顶层概述，并描绘了一套架构模式，这些模型使区块链能够作为一种技术来保护物联网的能力。此外，本文还探讨了用于物联网安全的具体用例示例，尽管这些用例的技术实现将因公司而异.

区块链概述

一个区块链服务，或者简称为区块链，是一个事务存储库，将事务分组到块中。“每个 块都包含上一个块的散列。就产生了创建从成因块到当前块的一系列块的效果。对每个块的 内容进行数字签名，以确保记录的事务的数据完整性。

区块链服务包括三个主要组件:

(1) 自治节点网络

独立节点自动生成并将合法的事务注册到分布式账本中。对于验证事务，不需要中央主 管（权利）机构或可信的第三方。区块链服务的所有节点(也称为区块链平台)协作以保持分 类帐簿的一致性。

每个节点都运行一个被称为协商一致的程序机制。协商一致意见是节点在一组事务中如 何更新区块链的过程。达成共识确保网络中的大多数节点都验证了相同的事务集。

分布式协商一致的目标是保持系统中足够多数的分类账本是正确和最新的(在一个粗略 的时间尺度上)。协商一致机制防止恶意的同行通过(a)追溯修改交易来破坏账簿的完整性;(b)执行语义未经许可的交易(例如:“双支出”和在加密货币设置中转让非自有资产);或(c)阻止对正确事务请求的接受和预订。

在开发区块链服务防范特定攻击时所选择协商一致的方法，这些攻击缓解措施并不完全 是技术性的。以比特币的“工作量证明”为例，要想在网络中获得 51%的哈希计算力，有一定的经济抑制因素。即获得 51%的采矿哈希计算力，将有可能使攻击者花费双倍花费的硬币或改变近期的交易历史。

此外，获得 51%的哈希率和传播恶意交易将迅速破坏对加密货币的信心，并显著降低恶意方的利益风险价值。此外，恶意方可以简单地利用他们的哈希计算力在挖掘（mining）过 程中为自己创造收益。

在一个被许可的(封闭的)系统中，经济不利因素可能不存在。许可系统还往往采用减少开采困难，允许在网络中进行更快的事务。这些许可系统必须要符合传统的网络安全控制， 包括弹性防护、基于硬件的钱包、网络矿工限制访问控制、身份管理和强大的审计能力，以确保潜在的监管介入、诉讼和刑事调查系统在内的不当行为。

三种在区块链中的主要共识的机制:

拜占庭容错（BFT）：拜占庭式容错(BFT)算法的设计是为了避免攻击和软件错误引起的故障节点表现出任意的行为(拜占庭式的错误)。BFT[4]在参与的情况下提供了一致意见：恶 意行为不当(拜占庭将军问题)节点。然而，这种方法的缺点是，在形成区块链网络的节点数 量上，可伸缩性限制。已经提出了 BFT 的替代方法，包括实用的拜占庭式容错。目前使用 PBFT 的区块链实现的例子是 Linux 基金会 Hyperledger fabric (0.6)和瑞波币.

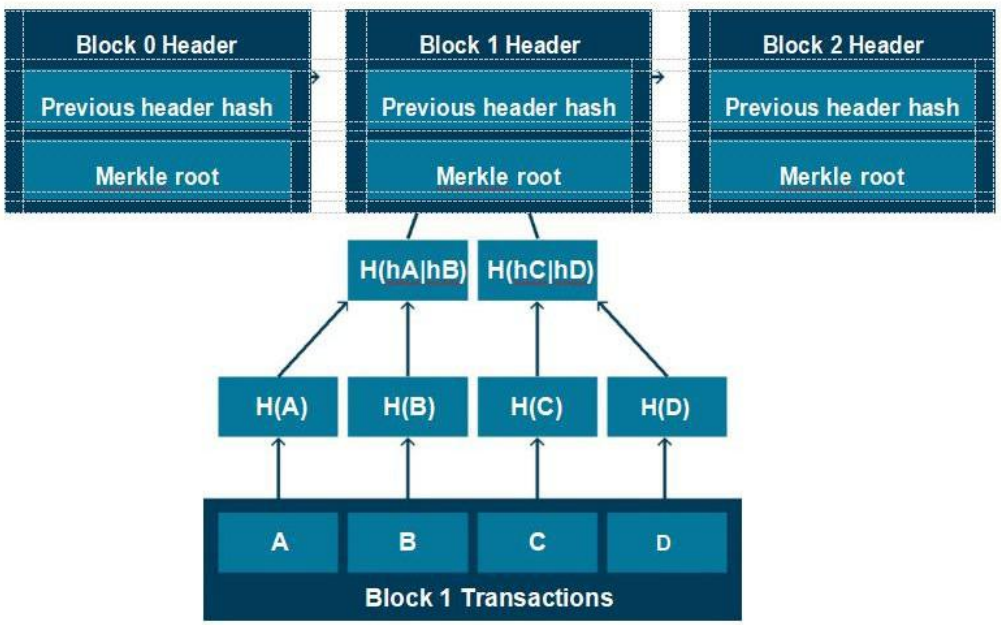
由比特币和以太坊(Ethereum)使用的“工作量证明”(POW)是一种广为人知的建立共识的机制：在工作量证明（POW）一个单独的节点可以向其他节点提供其结论，该节点可以由网络中的其他节点进行验证。提交一个生成的块的节点，为了能够达成共识，还必须提供它 执行的工作的证明，这是一个计算困难的任务(基于哈希函数的“密码难题”)。工作量证明（POW）提供了良好的网络稳定性。然而，工作量证明（POW）的成本特别高。计算资源消耗。 被授予作为成功的块生成的回报，“矿工”被激励参与获得一个秘密奖励。

权益证明(POS)与 POW 类似:节点在生成块时获得奖励。然而，只有几个节点可以参与到这个阶段。实际上，下一个生成节点是基于累积的财富(即，即:“权益”)。基于 POS 的区块链的挖掘（mining）过程通常称为“伪造”或“铸造”。推出 PoS 的技术就是点点币（PeerCoin）。

(2) 交易分类帐

数据库由块组成，因此叫“区块链”。每个块包含一个有效的事务列表、一个时间戳和 将当前块链接到上一个块的信息。通过每个块的链接到前面的块的链接创建分类账。

分类账的核心是哈希加密，这是一种数学算法，它将可变大小的数据映射到一个固定大 小的字符串。所有的交易——A, B, C, D -都是散列- H(A)， H(B)， H(C)， H(D) -然后汇总成连续的哈希- H(hA|hB)， H(hC|hD) -构成一棵 Merkle 树。顶部散列，或 Merkle 树根，是集成块头部。



Merkle tree connecting block transactions to block header Merkle root

(3) 分布式数据库

当添加新的事务时，会生成一个分类账，并且可以在系统的节点上进行复制，这就是分 布式账簿。网络上的每个节点都有自己的数据库副本，可以访问任何数据库的历史事务。

特定的加密货币的区块链容量将驱动特联网和其他主机的存储容量需求。下表为流行的 加密货币在 2017 年 8 月 14 日提供区块链容积。

加密货币	区块链容积（截止于 8/14/17
比特币	151.74GB
以太币	98.94GB
以太坊经典	20.12GB
莱特币	8.62GB

达世币	3.69GB

事务传播和区块链建设

下面是区块链事务的通用处理流程。当一个事务被提交到一个节点时，一个区块链服务 通常运行如下:

1、将新事务广播到所有节点。

2、每个节点将新事务收集到块中。

3、每个节点工作在块的一致性算法上（一般来说，这个任务在节点处理和耗电方面是昂贵的）。

4、当节点完成协商一致性算法处理时，它将该块和处理结果广播给所有节点，然后接收该工作的补偿。（在比特币的情况下，补偿是由比特币矿工处理和接收的交易费用。）

5、节点仅在其所有事务有效时才接受该块。

6、通过使用已接受块的散列作为前一个散列，通过在链中创建下一个块来表示对块的接受。

这种技术并不新鲜：它涉及数字签名、密码哈希算法、对等连接、分布式数据库等等。 在当前的形势下，有效结合这些离散技术的区块链技术是必要的，因为提高计算能力和互联网速度可以实现分布式计算。

智能合约

智能合约是在分类帐上执行的自执行代码。使用智能合约，双方进行交易。例如，一方 可以提供服务，而另一方为该服务提供支付。智能合约强制执行交易规则，也可以执行与违 约相关的惩罚。

在物联网的背景下，设备可以预先配置为基于区块链上的契约地址与智能合约进行交互。 这些设备随后可以进入彼此之间的事务处理。智能合约监视事务流程，并验证在发布资金或 允许操作之前遵循了规则。

使用智能合约的物联网系统的实现者必须考虑潜在的误用案例，并安装规则在合约中。 例如，一个智能合约开发人员可能会强制执行托管（保留资金）要求，直到完成智能合约条款的验证。与智能合约一起工作时，考虑其他安全要求，包括需要避免在第一次合约交易完成之前再次执行合约的竞争条件（即第一笔合约交易完成之前，合同可以再次执行），验证合约的发送方和接收方不使用相同的地址。确保只有授权的设备才能使用智能合约。您可以学习更多关于智能合约的安全知识。

https://consensys.github.io/smart-contract-best-practices/。

链下存储解决方案

负责实施区块链技术的解决方案开发人员应该认识到，没有与使用公共区块链网络相关的机密性保护。即使是私有/许可的网络也缺乏足够的保密工具来支持在链上存储敏感数据。

相反，许多组织需要建立起来“链下”存储解决方案，这些解决方案可以用来存储数据产品， 而区块链将这些产品的散列记录为事务。这些链下存储解决方案应该根据任何法规要求或行业最佳实践进行加密。

部署选项

区块链可以在三个区域内部署:

- 未经许可的区域(public):每个节点都可以读取和发送事务，也可以参与协商一致的过程。POW 一致性算法最适合于不受约束的区域。
- 联盟区域(例如部分许可):定义节点可以参与协商一致过程。读取和发送交易可能是公 开的或受限制的。拜占庭容错（BFT）最好应用于联盟部署，比如 Hyperledger——一个由 Linux 基金会管理的开源项目。
- 许可区域(private):受信任的组织可以将事务写入区块链，而协商一致机制则无关紧要。这种部署对受监管的行业或属于同一法律实体的组织最有效。例如由项目 R3 和金融机构的链核心所提议的垂直项目，很可能是由中央权威管理的私人区块链。

比特币和以太坊是不受许可的区块链实现，它们在支持分布式应用程序(DAP)方面获得了广泛的支持。以太坊包括可以使用的 Solidity 编程语言。轻松构建智能合约，实现物联网设备之间的自主点对点交易。解决方案，如 BTC 中继，提供了在以太坊中解决智能合约的能力，并通过比特币进行支付。

区块链实现是在区块链网络上构建服务的框架，例如加密 货币、分布式应用程序和智能合约。该框架描述了要使用的理 论概念以及它们如何组合(例如，协商一致机制，数字签名、密码方法和通信属性等内容)。由实现者指定并详细说明实现框架的技术组件。右边的图提供了在设计基于块的物联网的安 全解决方案时要考虑的技术组件。

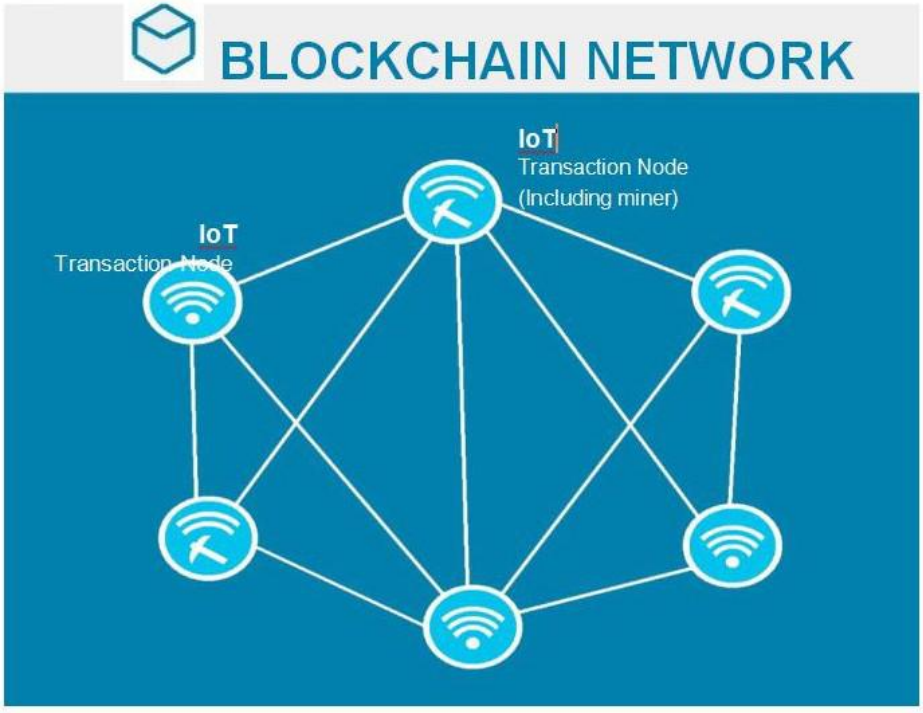
多个区块链实现是可能的，并且每一个都提出了不同用法和服务的建议。在这些网络之间的“无信任交换”将可能使用一个名为双向挂钩”的中继，允许访问另一个区块链的功能。Rootstock 是一个开放源代码的智能合约平台，采用双向绑定的比特币。

基于区块链技术的物联网架构

将区块链技术应用到物联网中，需要对物联网的体系结构模式进行测试。区块链服务，定义 的模式应该包括以下三个部分:

通信模型

通信模型描述了直接在物联网节点上安装区块链软件，或者将应用程序编程接口(api)安装到物联网（IoT）节点上。下图展示了一个通用的、接受的模型，结合了区块链技术和物联网（IoT），当 IoT edge 设备具有强大的功能，使它们能够承载事务节点软件，存储分类账，并通过节点网络维护通信。



Each IoT node acts as a blockchain transaction node

物联网事务节点

在前面的图中，每个物联网设备都承载了分类账，并且能够参与包括挖掘（mining）在 内的区块链事务。每个设备都配置了一个私有密钥，或者包含了内部自生成的私有密钥来参 与网络事务。这个最终状态模型提供了三个基本功能，可以启动使用区块链服务:

- 自主的物联网设备网络，包括自主协调(如：协商一致和点对点信息)
- 任何物联网的设备都可以创建运行加密特性的事务分类账簿。
- 一个分布式数据库，其中任何物联网设备都有最新版本的分类账簿。

硬件的限制使得采用这个模型在当前的时间内很难实现。具有如下挑战:

1、低处理:区块链服务的计算需要较高的 CPU、内存和电源能力。在区块链平台上，主要的潜在硬件是挖掘（mining）POW;智能合约的执行和加密原始执行。

2、小存储:在分类帐簿中添加的事务量会增加，即使处理小的事务数据也会变得很麻烦。

3、有限的连通性:一个物联网设备可以利用低带宽的互联网或无线电访问，这在下载期 间的性能问题并与分类账同步时都会引入性能问题。

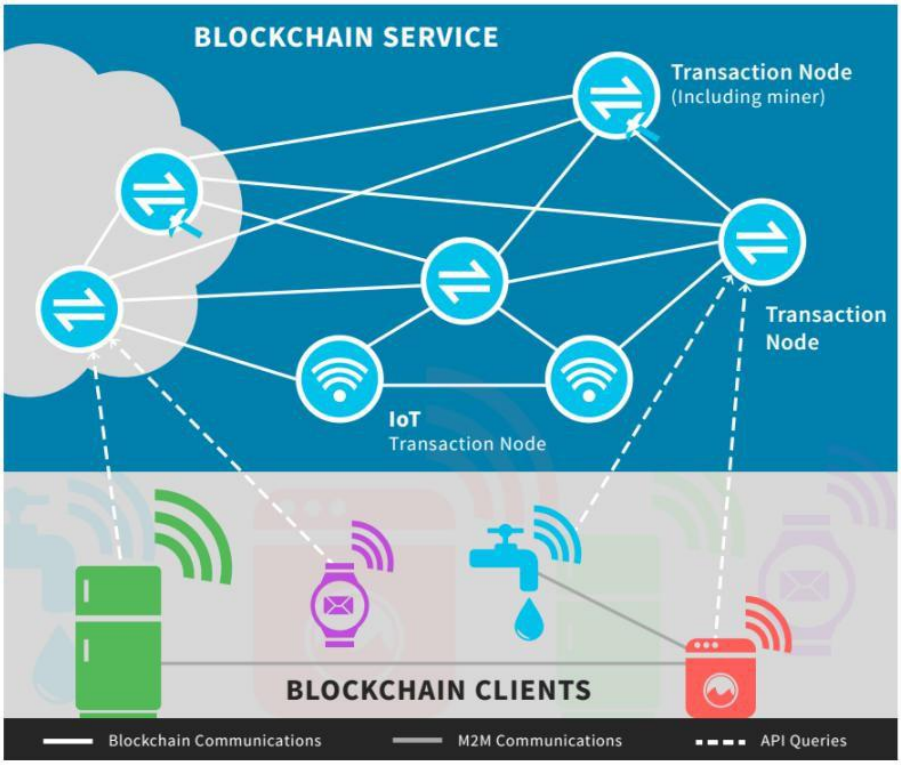
一些公司，如 IOTA，提出了“区块链”微型传感器的新方法，包括以下内容及解决方案:

- 简化挖矿（mining）处理过程，减少硬件需求。

- 实现与物联网交互相关的微事务。
- 保持轻量级的帐簿

基于云计算的物联网区块链网络

在启用云的区块链网络中，事务和挖矿（mining）节点都位于云和预置环境。根据实现 的不同，节点可能是企业服务器、企业/个人电脑或智能设备。基于云的虚拟机和物联网设备（手机或平板电脑），需要拥有足够的硬件资源(CPU、RAM、存储等)。



具有有限硬件资源的物联网设备作为区块链客户端。他们不存储分布式账本。这些客户 机通过 api 与上游的基于云的区块链事务节点交互。api 可能是 HTTP REST 或 JSON RPC。

物联网设备收集数据转发到事务节点以进行区块链服务的处理，或者通过指向在云中运 行的区块链节点参与智能合约事务。在这种情况下，特联网设备仍然配置了私有密匙来签署 它们的数据。然后将已签名的数据发送到事务节点进行处理。为了安全地发送数据，特联网 设备和事务节点之间必须有一个单独的信任协议。例如，一对一的关系可以在两个设备(一个物联网设备和一个事务节点)之间使用白名单和双向身份验证功能。还应该使用硬件安全性来安全地存储私有（签名）密钥。

对于许可区域(私有区块链服务)，对挖矿（mining）节点的访问可能仅限于授权的操作人员。在一个联合区域(部分许可的区块链服务)或许可区域(私人区块链服务)，成员可以决 定实现该体系结构模式以提高安全性或用于法规遵从性目的。

比特币的实现使用“瘦客户端”来提出这种功能，也叫简化支付验证(SPV)，它不存储所有分类账的完整副本。这些“瘦客户机”与使用比特币客户端 API (BCCAPI)的节点通信。

可以在多个特联网设备之间交换消息。这些消息包含的数据被集成到参与交换到事务节点的特联网设备的事务中。物联网设备之间的通信协议和消息格式超出了区块链实现的范围: 这些通信是指机器对机器的通信，如消息队列遥测传输(MQTT)。

一个利用互操作性能力的丰富生态系统离利用互操作能力

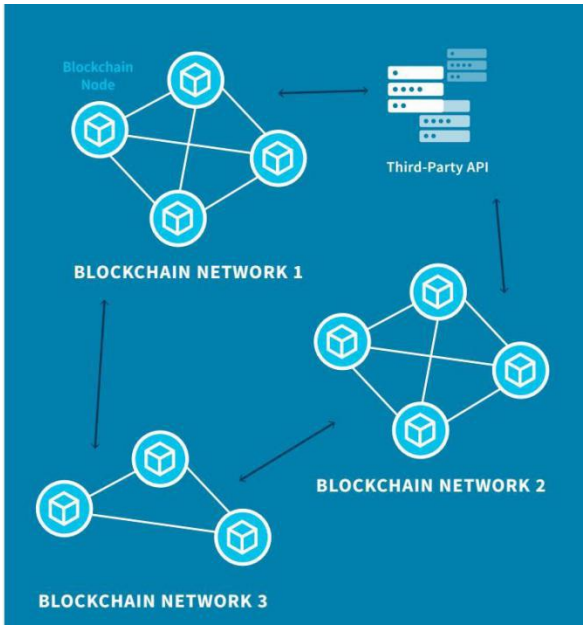
围绕区块链技术开发一个生态系统将是一个加速其采用的机会。这个潜在的生态系统将 提供简化物联网集成到区块链服务的功能。

服务提供商，如块密码，提供 API 功能，简化物联网与区块链服务客户和服务之间的交互。API 中间层允许开发物联网上与不同区块链服务通信的特性，方法是关注服务的价值而不是区块链技术的技术实现。

解决方案提供商，例如信用，提供了快速构建私有区块链服务的框架。这些框架在事务 节点上运行每个节点都由客户端通过 API 访问。这些框架还提供了与其他块链服务交互的功能。

多个区块链服务之间的共存

如下图所示，另一个概念集中于多个区块链服务，每个服务提供不同的特性和货币，它 们的数量将增长。这些区块链服务将提出互补的功能。每个区块链服务都可以与其他服务进 行绑定，或者使用第三方提供的 api。

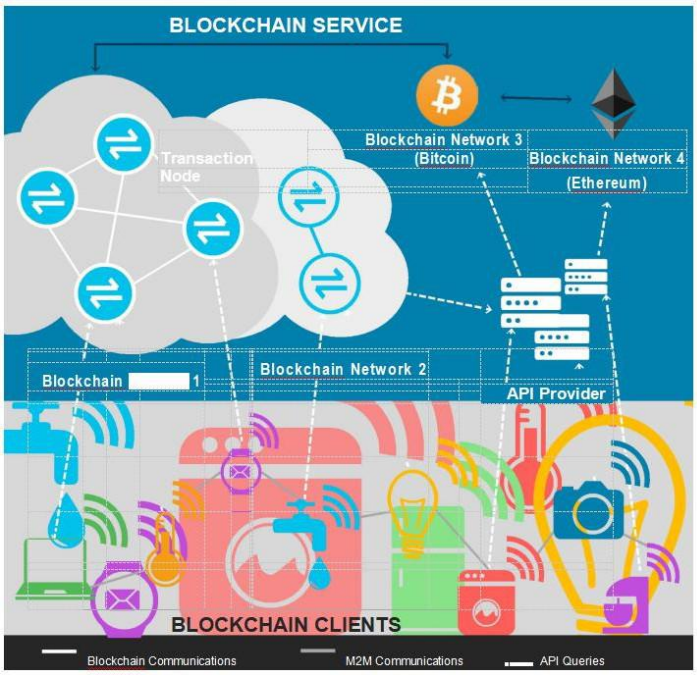


Each blockchain service can run in different contexts, such as personal home network, enterprise and the Internet.

每次区块链服务可以运行在不同的语境中，如个人的家庭网络，企业和互联网。

基于区块链技术的物联网架构模式

CSA 物联网和区块链/分布式分类技术工作组提出了以下系统，在多区块链服务中，物联网客户端可以进行协作。



区块链服务 1 是一个专注的企业实施:

•事务节点是托管在云中的企业计算机或服务器。

•物联网区块链客户是部署在企业地区区块链服务 2 的传感器和智能设备，是一个消费智能家居:

•事务节点是个人计算机和其他设备或云订阅。

•物联网区块链客户是智能设备，如冰箱、温度传感器和安全摄像头。

物联网设备是区块链服务的客户端的架构，主要是由当前业界的努力所采用的实现区块 链技术。

用于物联网安全的区块链技术的选择

区块链技术可以帮助保护物联网设备。物联网设备可以配置为利用公共区块链服务或通 过安全 API 与云中的私有区块链节点通信。将区块链技术纳入物联网系统的安全框架中，使物联网设备能够安全地发现彼此，使用分布式密钥管理技术对那些机器对机器的事务进行加 密，并验证软件映像更新的完整性和真实性，以及策略更新。

基于本报告中详细描述的潜在架构模式，物联网设备将通过 API 与区块链事务节点进行通信，甚至允许受限设备参与区块链服务。

为了确保安全性，在将物联网设备引导到特定的区块链服务时应该注意。下面是物联网 发现的一个用例，它支持将一个物联网设备注册到一个事务节点中。物联网设备必须首先配 置凭据，可以用来证明授权，以便将其添加到事务节点。必须在安全的环境中进行这种凭据 供应，以防范特定物联网设备生态系统的威胁。

我们对区块链技术的回顾和市场计划的发展，突出了五个需要考虑的特点。使用区块链 技术保护物联网时:

1、物联网发现可伸缩

2、信任的沟通

3、消息身份验证/签名(事件链)

4、物联网配置和更新

5、安全固件映像的发布和更新。

1. 物联网发现可伸缩

智能城市和大型企业物联网的部署将导致数千或数万个必须协同工作的物联网设备[28] 的激活。通常，这些设备将在自主机器对机器的事务中相互协调。这些设备还必须能够发现合法的对等点和服务进行交互。物联网系统可以利用公共和私有的区块链实现来利用可扩展的物联网发现。

例如，在比特币内部，一组硬编码的 DNS 种子为新用户和设备提供了引导服务。这些 DNS 种子可以在物联网设备中预先配置。物联网设备查询这些地址，并提供完整节点的 IP 地址。然后物联网设备将自己注册到一个节点，并请求网络上的其他物联网设备列表。当供 应时，物联网设备可以开始点对点通信，同时向网络中邻居传播同伴发现信息。

命名 DNS 种子地址的预配置(硬编码)降低了执行中间人攻击的能力。物联网设备在选择一个节点注册之前，从多个 DNS 种子接收信息。必须使用 DNS 安全来确保根服务器的名称解析，并减轻 DNS 欺骗攻击。

命名 DNS 种子地址应该硬编码到固件中;案例 5 提供了一种保护固件映像分布和更新的方法。

一个私有的区块链服务也可以支持引导和注册物联网设备到网络上。事务节点将在提供 可信节点列表之前对物联网设备进行身份验证，物联网设备的注册。

可以包括以下内容的凭证:

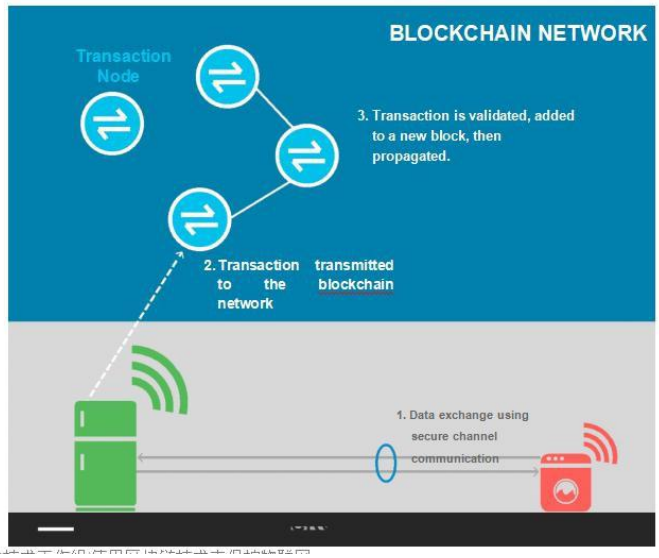
在安装过程中安装的物联网设备上安装的安全凭据必须被生成，并提供一个安全的过程， 这可能是区块链实现的一部分。

物联网设备的所有者或安装技术人员提供的凭据将初始化设备注册到安全服务器，以获 得物联网的特定凭证。

在这两种情况下，必须强制执行注册过程，以确保只有合法的物联网设备才能添加到区 块链服务中。必须对所描述的所有通信进行身份验证和加密，以确保机密完整性。

有关在区块链上注册设备标识的能力的进一步信息，请访问受信任的物联网联盟，以查阅 在区块链中注册身份标识而开发的区块链 api。

2、信任的沟通

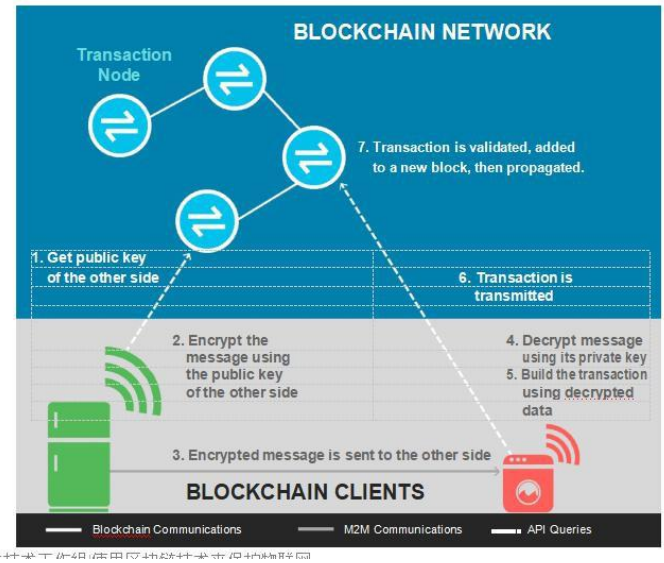


在某些情况下，例如公共部署，物联网设备需要使用安全通信通道来交换构建事务所需 的数据，以便存储到分类帐簿中。这个分类账也可以用来存储公共加密密钥。

如果交换必须保密，物联网设备(发送方)将加密消息发送到对等物联网设备(接收方)　使用接收器物联网设备的公钥，该设备存储在区块链服务中。

为了方便这个安全的事务，物联网发送者请求它的事务节点从物联网接收器的公钥到区　块链分类。物联网发送者使用物联网接收器的公钥对消息进行加密。

只有接收者可以用他们的私钥解密消息。关键的协议算法，如基于椭圆曲线密码学算法(ECDH)，应该用来创建密钥来保护诸如内容加密密钥(CEK)和/或通信加密密钥(TEKs)之类的事务。



在这个用例中，区块链服务充当分布式公共密钥基础结构[29]。公共密钥存储在事务中:　当一个新的物联网设备注册到一个私有或公共的区块链服务(见上一节)时，将创建一个新的　事务。该事务由物联网属性(包括其公钥)组成。如果物联网设备必须更新其证书，则重新注　册。被撤销的证书也可以作为事务添加到区块链服务中。在分类帐簿中记录的有担保的交易　记录提供了在他们的一生中物联网设备键的一致性。

在区块链中实现了使用多种类型的加密密钥。用于确保区块链交易的密钥通常被称为钱　包参数。在这个用例中讨论的参数代表了身份密钥，可以用来生成加密密钥(TEKs)或内容加　密密钥(CEKs)进行通信，来保护物联网设备点对点之间的通信。

物联网身份密钥（参数）:用于生成密钥材料的非对称密钥，可用于加密物联网设备之　间的消息内容和流量。

钱包钥匙（参数）:用于存储在分类帐簿中的交易;可能包括物联网身份密钥。

3、半自治机器对机器的操作

物联网技术的一个关键驱动力是机器能够以半自治的方式协同工作以实现特定目标的　能力。区块链可以使用智能合约功能作为这些自治事务的安全助推器。

智能合约可以写下来，包括合同的规则、处罚和条件。物联网相关设备可以配置一个API 来与智能合约进行交互，从而与对等设备或服务签订协议。每个事务必须在执行之前满足协定的条件，并且所有的事务都被写入到区块链。

智能合约可以强制执行访问限制，比如谁(物联网设备)可以进入事务。每个事务都与物　联网节点的钱包参数签名，钱包应该存储在硬件安全容器中。在区块链上的事务记录确保了　事务不能被拒绝(例如，当一个服务提供者的物联网设备与一个消费者的物联网设备进行交易时)。

4、物联网配置和更新控制

随着更多的物联网设备的诞生，区块链技术在可信的安全配置领域是有希望连接到云 服务。**以下是三种安全措施:**

1、分类账簿可以托管物联网属性，例如最后一个版本的验证的固件和配置细节。在引导过程中，特联网设备要求事务节点从分类帐簿中获取配置。通过对公共分类账簿的内容进 行分析，可以在分类账簿中对配置进行加密，以避免物联网的网络拓扑的发现。

2、分类账簿可以为每个特联网设备托管最新配置文件的哈希值。物联网设备从云服务下载最新的可信配置文件(或设置时间)，然后利用事务节点 API 来检索和匹配存储在区块链上的哈希值。这允许管理员定期刷错误的配置，并在其网络中重新启动物联网设备，并加载 新的配置。

3、上述第 2 条所讨论的过程可以应用于物联网设备的固件映像，尽管这可能，在物联网设备上需要额外的带宽容量。

5、安全固件映像的发布和更新

类似于支持从云服务提供商下载可信配置，区块链技术也可以支持物联网设备的可信存 档（固件）的过程。物联网设备开发人员也可以实现他们自己的区块链或使用公共区块链。开发人员可以将最新已知的可信映像的哈希用于其设备家族，并将这些哈希加载到区块链中。 该方法通过三种方式支持增强物联网设备的安全性:

1、物联网设备可以通过 API 进行配置，在重复的基础上下载新的固件映像。因为大多数物联网设备不需要内存中保存或存储数据，所以它们可以在需要时被覆盖。例如，可以通 过在供应商的区块链上验证映像哈希来启用每日或每周的映像更新过程。

2、物联网设备可以使用基于块的映像更新过程来验证供应商提供的所有更新。

3、物联网设备可以使用上面的方法 1 或2 来验证所有更新，此外还需要设备所有者批准固件的更新(使用安全的方法)

物联网企业应加强在总账中固件的数字答名，提高当前标准软件签名的方法，而不是在应用更新之前将其发布在其网站上，物联网设备从分类账簿中获得新固件的数字签名，然后使用维护公钥验证它。此维护公钥可以在 fabric 和硬件级别进行融合（无更改/更新功能）

警告:必须确保制造商维护私钥，以避免损害所有固件。获取私钥的攻击者可以使用看 似“有效”的数字签名来提供可用的恶意固件。

在所有设备上改变制造商的公钥的过程需要付出巨大的努力。 **基于固件信誉的更新(事物链):**

分类帐簿的事务历史交易能力可以聚合新固件的符号，避免被安装恶意软件和后门固件， 为社区专家提高固件安全固件的信任力.

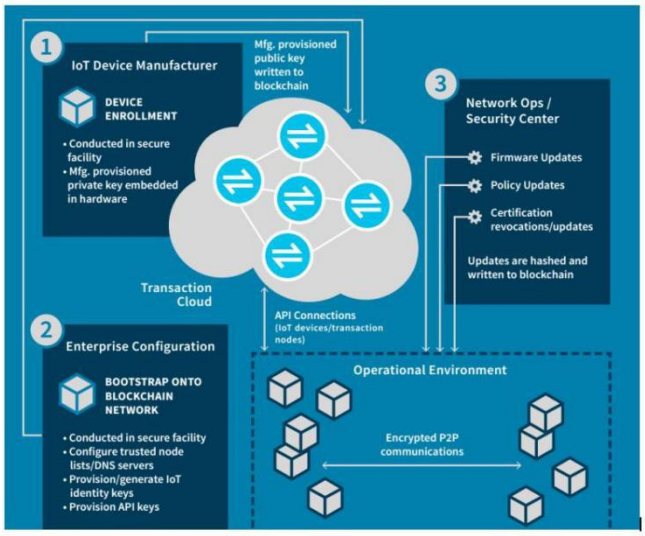
当固件信誉在分类帐簿中达到特定的选票级别的分类账簿，物联网设备的所有者/管理员还应该配置物联网的自动更新。这种在区块链服务中对物联网设备的“接受”可能基于设 备在分类帐簿中的固件信誉，这将产生以下好处:

1、避免使用与区块链服务相连接脆弱的设备。

2、在物联网设备上执行安全更新流程。

3、在区块链服务中定义最低要求的安全要求。

物联网的区块链安全服务总结



结论

实施物联网解决方案的组织，继续面临着识别安全技术和方法的挑战，确定能够减轻对物联网（IoTs）的独特威胁。区块链技术有望在应对这些挑战中发挥重要作用。利基（Niche） 安全厂商将开始提供这些服务，可以立即利用区块链实现提供的完整性和真实性服务。

在本文中，我们强调了在使用区块链技术保护连接设备时需要考虑的特性。然而，由于 物联网的硬件限制，我们得出结论：在几十万或更多的物联网设备的背景下，这些设备中有 许多不能作为事务节点(生成事务、提供协商一致性等)，因此不属于安全区块链。许多设备 将受益于安全性。许多设备将受益于区块链服务提供的安全性和其他功能，这些服务通过网 络的上游事务节点或专门的中间商提供。这些上游功能可用于保护物联网设备(配置和更新控制、安全固件更新)和通信(物联网发现、可信通信、消息认证/签名)。

我们希望这个文件能够鼓励商业领袖和开发人员拥抱区块链这个机会，来扩展这项技术 的能力以确保物联网的安全。

参考文献

[1] IDCF utureScape https://www.idc.com/url.do?url=/getfile.dyn?containerId=US42259417&attachmentId=47254824&elementId=54425583&term=&position=1&page=1&perPage=50&id=b28d2b1c-ddd5-4e60-a2c2-de3a4f7ee253

[2] Bitcoin Venture Capital https://www.coindesk.com/bitcoin-venture-capital/

[3] Blockchain https://en.bitcoin.it/wiki/Block_chain

[4] Leslie Lamport, Robert Shostak, and Marshall Pease. The Byzantine generals problem. ACMTrans. Program. Lang. Syst., 4:382–401,July 1982. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.126.9525&rep=rep1&type=pdf

[5] Miguel Castro and Barbara Liskov. Practical Byzantine fault tolerance and proactive recovery. ACM Trans. Comput. Syst., 20(4):398–461, November 2002.

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.84.6725&rep=rep1&type=pdf

[6] Nakamoto, Satoshi. “Bitcoin: A peer-to-peer electronic cash system.” (2008): 28. https://bitcoin.org/bitcoin.pdf

[7] Vasin, Pavel. “Blackcoin’s proof-of-stake protocol v2.” (2014) https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf

[8] What is IOTA? https://iota.readme.io/v1.1.0/docs

[9] Trustless exchange and pegging of BTC in Ethereum https://medium.com/@ConsenSys/taking-stock-bitcoin-and-ethereum-4382f0a2f17#.h6nhib6ql

[10] Rootstock http://www.rsk.co/

[11] On Public and Private Blockchains https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

[12] Bitcoin https://bitcoin.org/

[13] The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication http://vukolic.com/iNetSec_2015.pdf

[14] Ethereum https://www.ethereum.org/

[15] BTC Relay http://btcrelay.org/

[16] Ethereum Blockchain as a Service now on Azure https://azure.microsoft.com/fr-fr/blog/ethereum-blockchain-as-a-service-now-on-azure/

[17] Hyperledger https://www.hyperledger.org/

[18] IBM Blockchain on Bluemix https://www.ibm.com/blockchain/offerings.html

[19] Project R3 https://r3cev.com/

[20] Chain Core https://chain.com/technology/

[21] Thin Client Security https://en.bitcoin.it/wiki/Thin_Client_Security

[22] BCCAPI (Bitcoin Client API) https://en.bitcoin.it/wiki/BCCAPI

[23] Machine-to-Machine https://en.wikipedia.org/wiki/Machine_to_machine

[24] Blockcypher https://www.blockcypher.com/

[25] Credits http://credits.vision/

[26] Drivechains sidechains and hybrid 2-way peg designs http://www.the-blockchain.com/docs/Drivechains%20sidechains%20and%20hybrid%202-way%20peg%20designs%20-%20Sergio%20Lerner%20-%202016.pdf

[27] Chain of Things http://www.chainofthings.com/

[28] Gartner Says 8.4 Billion Connected “Things” Will Be in Use in 2017, Up 31 Percent From 2016 http://www.gartner.com/ newsroom/id/3598917

[29] Decentralized Public Key Infrastructure http://www.weboftrust.info/downloads/dpki.pdf

[30] Cryptocurrency Statistics https://bitinfocharts.com/