一种应用于工业互联网数据安全的轻量级高通量区块链方法

徐雪松[1,2]，杨胜杰[1]，金泳[1]，陈荣元[1]，曾智[1]

[1](湖南商学院 新零售虚拟现实技术湖南省重点实验室,湖南 长沙 410205)

[2](智能物联网信息安全技术湖南省工程研究中心,湖南 长沙 410205)

通讯作者：杨胜杰, E-mail: daniel613@126.com

摘 要：随着物联网技术的飞速发展，工业互联网应用也呈指数级增长。由于工业互联网分散的拓扑结构和异构设备的资源限制，对传统的数据存储、传输和安全保护提出了新的挑战。区块链技术的分散式信任和分布式帐本等机制，适应于分布式大规模工业互联网，并有可能成为工业互联网安全和数据保护的有效方法。但是，传统区块链的计算通量低、能耗高、可扩展性有限，并且会产生显着的带宽开销和网络延迟，难以直接适应于工业互联网。因此，本文提出了一种满足工控环境要求的安全、私密和轻量级的分层扩展式区块链。该模型由 Overlay 网络下资源受限层、扩展资源层两层区块链构成。设计了轻量级共识算法、分布式信任确权机制和动态高通量管理方法，并通过工业互联网受限资源设备的数据存储请求交易说明了分层区块链具体实现流程。本文主要贡献在于扩展了不同资源能力的设备在整个 Overlay 网络中的高效区块操作，并确保端到端的隐私和安全性。为工业互联网泛在接入建立实体间信任关系和数据安全提供新的思路和方法。

关键词：工业互联网；区块链；数据安全；轻量级

A Lightweight High-throughput Blockchain for Industrial Internet Data Security

XU Xue-song[1,2], Yang Shenjie[1], Jin Yong[1], Chen Rongyuan[1], Zeng Zhi[1]

[1](Key Laboratory of Hunan Province for New Retail Virtual Reality Technology, Hunan University of Commerce, changsha，410205)

[2](Engineering Research Center of Hunan Province for Intelligent Internet of things information security technology , Changsha 410205)

Abstract: With the rapid development of Internet of Things technology, Industrial Internet applications have also grown exponentially. Due to its decentralized topology and resource limitations of heterogeneous devices, traditional data protection methods have been challenged. The basic technologies of decentralized trust and distributed ledger of blockchain technology are suitable for distributed and large-scale Industrial Internet, which aslo becomes an effective method for Industrial Internet security and data protection. However, traditional blockchains have low computational throughput, high power consumption, limited scalability, and significant bandwidth overhead. Therefore, this paper proposes a security, private and lightweight expandable blockchain that meets the requirements of the industrial control environment. The model consists of a restricted resource layer(RRL) and an extended resource layer(ERL) blockchain in the Overlay network. We designed a lightweight consensus algorithm, distributed trust confirmation mechanism and dynamic high-throughput management algorithm. The specific implementation process of the blockchain is illustrated by the local data storage request transaction in the industrial control environment. The main contribution of this paper is to expand the efficient block operation of devices with different resource capabilities in the entire Overlay network and ensure end-to-end privacy and security.

Key words: Industrial Internet; Blockchain; Data security; Lightweight

工业互联网通过构建连接机器、物料、人、信息系统的基础网络，实现了人、机器、产品和服务的泛在互联，为传统工业的发展提供了新的动力，正成为当前研究的前沿热点。然而，由于工业环境中存在大量计算、存储和带宽受限的传感设备，分布式和海量数据流量成为满足所需服务质量（QoS）的瓶颈。与此同时，工业互联网也打破了工业控制系统传统的封闭和高可靠性的格局，使工控系统信息安全问题大量暴露出来。

基金项目：国家自然科学基金重大项目（国家安全管理的决策体系设计：71790615）；湖南省重点实验室开放研究基金项目：18-07

作者简介：徐雪松，博士，教授，硕士生导师，主要研究人工智能、区块链、工业物联网。

区块链技术[1]作为比特币、以太坊等数字加密货币[2]的核心技术，能够通过分布式节点的验证和共识机制解决去中心化系统节点间信任建立的问题，实现了去中心化、分布式的信任建立机制[3]。从而在信息传输的同时完成价值的转移，能够实现当前网络架构由“信息互联网”向“价值互联网“的重大转变。区块链的交易隐私、安全性[4,5]、数据的不变性、可审计性[6,7]、完整性、授权、系统透明性和容错性[8]，使得区块链在除加密货币以外的多个领域中广泛应用，包括身份管理[9]，智能交通[10-14]，供应链管理[15]，物联网[16,17]，工业互联网[18][19]，能源互联网[20-22]等。由于采用了加密技术并且没有集中控制参与者或集中数据存储，并且可以避免控制系统的数据隐私泄露等安全问题，区块链正在通过一个具有匿名和可信交易的分散环境来改变工业互联网应用领域。结合区块链技术，工业控制系统可以从较低的运营成本，分散的资源管理，抵御威胁和攻击的稳健性等方面受益。

但是，工业互联网由于缺乏中央控制、设备的异构性以及节点计算能力受限等固有特点，对传统的区块链技术和数据安全保护提出了挑战：如：

（1）资源受限：大多数工业系统设备的资源有限，包括带宽，计算和内存，这与复杂区块链解决方案的要求相悖[23]。

（2）多级中心管理：当前的工业互联网生态系统依赖分级的代理通信模型，其中所有设备都通过各级中控系统或云服务器进行识别，验证和连接。随着工业互联网超大规模设备的连接，集中的云服务器难以满足分散设备的实时交互需求[24][25]。

（3）数据安全：工业生产环境下的关键参数和信息系统的敏感数据，对工业互联网的异构网络结构数据隐私和安全保护提出了更高要求，需要从底层传感、协议通讯及信息处理全流程确保数据的安全防护[26]。

虽然有学者研究提出了基于分布式访问控制方法来控制对敏感信息的访问[27]，但带来了过多的延迟和开销，并且可能潜在地损害用户隐私。文献[28]中使用 IPsec 和 TLS 来提供身份验证和隐私，但由于计算开销太大，不适合许多资源有限的计算设备。文献[29]中提出了一种隐私管理方法用于衡量数据泄露风险，但在某些情况下，工业互联网服务感知收益大于隐私损失的风险。针对以上问题，本文提出了一种轻量级高通量区块链（Lightweight high-throughput blockchain-LHTB）模型，用于工业互联网环境下设备访问控制及数据安全保护。该模型由两个可扩展的分层组成，即受限资源层（Restricted resource layer-RRL) 和扩展资源层(extended resource layer-ERL)。定义了工业互联网资源的基本体系结构，将交易确定为实体间基本通信原语。对分层区域内不同资源能力计算单元设计了相应的区块链操作。为了优化资源消耗，ERL 包括具有一定计算能力的节点，协作管理存储在 Overlay 的公共区块链[18][30]。在 RRL 中为了最大限度保障可扩展性，将受限资源节点聚类为集群，只有集群头节点负责管理公共区块链。为减少网络时延导致区块操作的不同步，设计了一种时间一致性算法；为提高区块链的通量，设计了分布式信任确权算法来提高节点彼此之间存在信任，从而减少需要验证的新区块中的交易数量。提出了一种可扩展的动态高通量管理机制，以动态地确定区块链效率控制参数，以确保公共区块链的交易负载均衡。最后给出了一个本地受限资源设备对数据交易上链的操作实例。从而为工业互联网分布式环境下，对用户、资源、服务、终端的泛在接入建立实体间信任关系和数据安全提供新的思路和方法。

1 背景知识

1.1 区块链工作原理

区块链结构由一系列块组成，这些块通过它们的散列值链接在一起，如图 1 所示。在区块链网络中，公共分类账维护 P2P 网络中用户的数字签名交易。通常，用户有两个密钥：用于加密的其他用户的公钥和用于读取加密消息的私钥，从区块链的角度来看，私钥用于签署区块链交易，公钥代表唯一的身份。非对称密码术用于解密由相应公钥加密的消息。在初始阶段，用户使用其私钥签署交易并将其广播给对方。一旦对等方收到签名的交易，他们就会验证交易并通过网络传播。参与交易的所有各方相互验证交易以达成共识协议。

达到分布式共识后，称为矿工的特殊节点将有效事务包含在带时间戳的块中。矿工包含的块被广播回网络。在验证包含事务的广播块以及将其与区块链中的先前块进行散列匹配之后，将广播块附加到区块链。

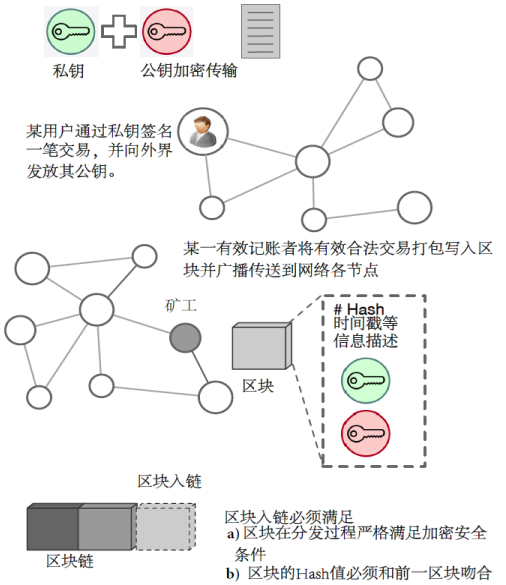

图 1 区块链基本工作原理

因此，区块链维护了一个分布式数字交易总账，并在所有参与节点之间共享[1]。新的交易由参与网络的其他节点进行验证和确认，从而消除了对中央机构的需求。在工业互联网区块链中，添加一个新块需要解决计算要求高、难以求解且易于验证的难题。工业互联网环境下参与共识算法所需的计算资源具有异构、分布、低功耗的特点，这限制了数据采集节点可以挖掘的块的数量。异构网络环境下的节点需要对新挖出区块里所包含交易的正确性以及时序达成一致，否则节点的区块链副本可能不一致，最终导致区块链出现分叉。为此，本文提出了一种基于时间一致性算法来代替资源密集型共识算法来解决这个问题。

1.2 工业互联网分层体系

工业互联网的核心是基于底层的物联网和上层信息互联网而组成的数据驱动型网络。数据、智能、安全是工业和互联网两个视角的共性基础和支撑。通过泛在连接，工业互联网具备对设备、软件、人员和系统等各类生产要素数据的全面采集能力。通过云化服务，实现海量数据存储、管理和计算。根据 IEC62443 标准，我们把工业互联网体系分为现场设备层、现场控制层及管理信息层，其功能包括计算，通信，传感和驱动功能，并且这些功能分布在叠加的 Overlay 网络中，如图 2 所示。

现场设备层：现场设备层包括各类传感器、数据采集器、控制器和执行单元等低功耗嵌入式平台。将该层中的设备定义为具有有限处理和存储能力的节点，称为 0 类设备，归属为受限资源层(Restricted resource layer-RSL)，其设备能耗是重要考虑的因素。

现场控制层：现场控制负责从终端设备收集传感器数据，可由网关、中控器、数据采集器等组成，用于处理与终端设备层的入站和出站通信。此外，来自现场设备层的数据在该层中处理，以满足应用程序的实时需求。在计算和存储能力方面，该层的设备比终端设备层更强大，称为 1 类设备，归属为扩展资源层（Restricted resource layer-ESL）。

管理信息层：管理信息层负责信息处理、存储和可视化功能，归属为核心资源层。该层中的设备具有最大处理和存储容量，由服务器或后端层由最大资源组成。因此，在工业互联网中区块链和协议的设计必须在部署之前考虑不同层的资源容量。

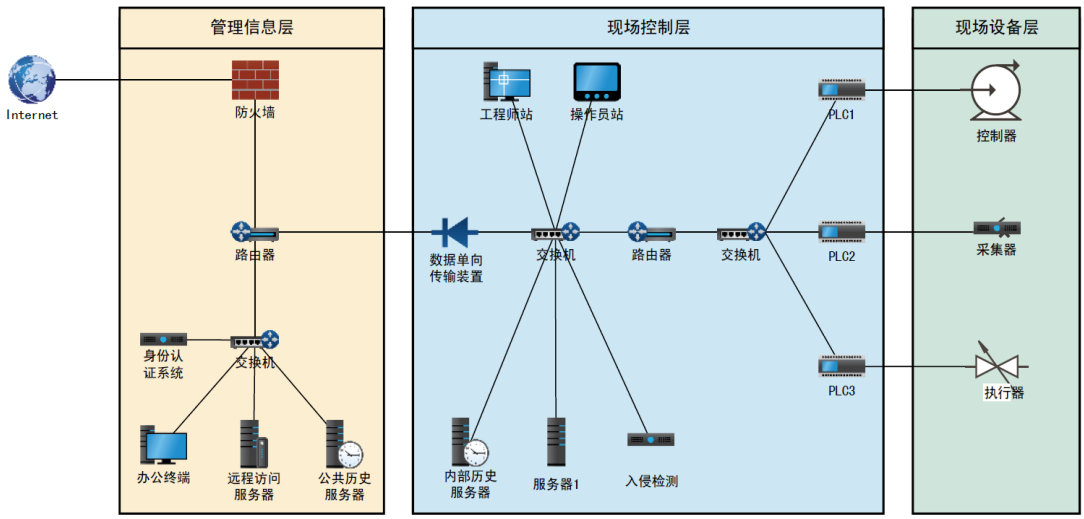

图 2 典型工业互联网分层体系结构

工业互联网现场设备层的数据来源和数据需求可能有成百上千个，为了简化数据交换，一般采取“发布/订阅”模式传递消息。工业互联网体系中，数据采集与交换是系统运作的基底，从微观层每一个零部件信息，到宏观层整个生产流水线信息，如何基于各种网络链接实现数据从微观层到宏观层的流动，形成各个层、全方位数据链条，并保证多源数据在语义层面能够互通，降低数据交换的时延，以实现有效数据交换，技术上是一个比较大的挑战。

2 分层的轻量级高通量区块链设计

根据上一节的工业互联网结构，我们将受限资源层（RRL）和扩展资源层（ERL）构建在 Overlay Network（ON）上，并由此来设计一种轻量级高通量区块链模型（LHTB），如图 3 所示。ON 由各种设备实体组成，称为资源节点，包括传感设备、采集设备、执行单元、集控器、网络设备和服务器等。为了确保区块链可伸缩性和减少网络开销延迟，把 ON 中的设备或计算单元节点按聚类分组，每个聚类选择簇头（Cluster Head-CH），并负责相对应区块链的管理，如 RRL Overlay Block。如果工业互联网环境中存在部分节点 CH 过度延迟，则节点可以重新聚类并自由更改其集群。此外，CH 还处理从其集群成员设备的生成或注销事务。一般情况选择较长时间内保持在线的 CH 节点，并处理集群内基本任务。因此受限资源层区块链不受设备动态变化的影响。节点内使用非对称加密、数字签名和加密散列函数（例如 SHA256）来保护由 ON 节点生成的各类事务。

与比特币挖掘不同，每个 CH 根据接送收到交易参与者的通信，独立决定是保留新块还是丢弃它。这可能导致每个 CH 中不同版本的区块。由于不需要实时协调区块一致性，所以减少了同步开销。但是，在一定时间等待周期内，由 ERL 中的扩展资源节点进行区块一致性校验功能。ON 结构中将数据流与业务分离，因此，对于工业互联网中访问请求或监控类事务，被访问设备在确权后，通过单独的数据包将数据发送给请求者。类似的，对于数据采集或存储类事务，由请求者创建直接发送数据。Overlay 事务存储在对应 CH 管理的公共区块中。该区块中的每个块由两个主要部分组成，即交易和块头。块头包含以下内容：前一个区块的 hash，区块生成者 ID 和验签者的签名。公共区块中前一个块的散列确保了不变性，如果攻击者试图改变先前存储的交易，那么相应块的哈希值将保留在本块上并出现不一致性，从而暴露出这种攻击。

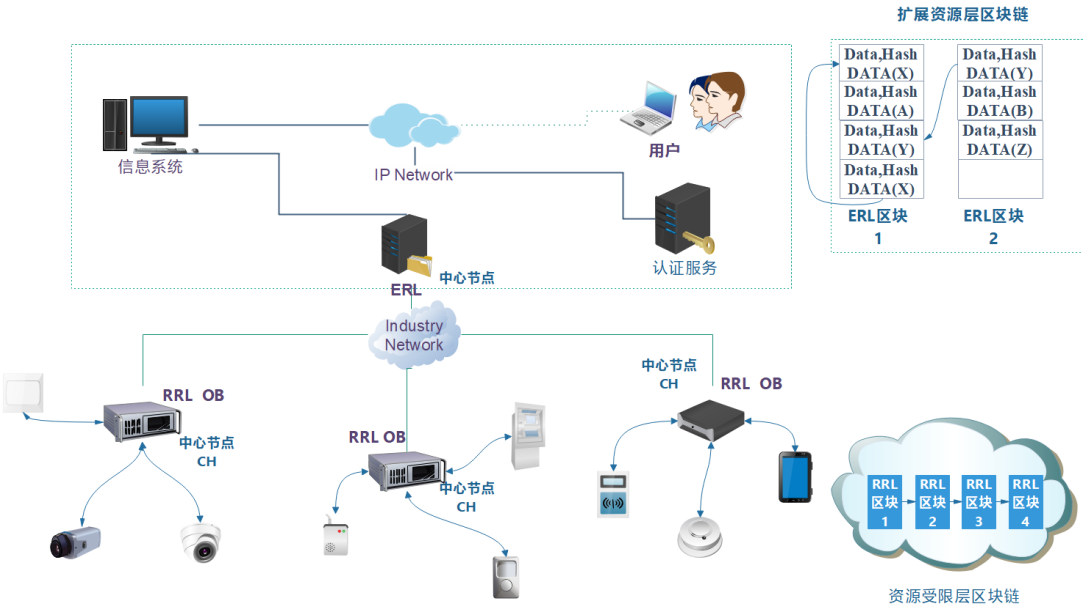

图 3 分层可扩展工业互联网区块链模型

2.1 改进的轻量级共识算法

在 LHTB 中，我们提出了一种基于时间一致性算法来代替资源密集型算法。该时间一致性算法必须确保在节点之间随机选择块生成器，并且限制它可以生成的块的数量。为了在块生成器之间引入随机性，每个 Overlay 区块的 CH 必须在生成新块之前等待一个随机周期 *T*。由于每个 CH 的等待时间段不同，该 CH 可能会收到由另一个 CH 创建的新块，其中可能包含当前在 Overlay 交易池中的部分或全部交易。在这种情况下，该 CH 必须从它的区块中删除这些交易，并且请求其他 CH 等待一定时间以求达到同步。最大等待时间的上限是 Overlay 中最大端到端延迟的两倍。为了保护整个 Overlay 免受非法恶意节点的攻击，Overlay 的 CH 可以允许只有一个块是在由共识周期区间内生成。共识期的默认（和最大）值为 2 分钟。共识周期的最小值等于覆盖中最大端到端延迟的两倍，以确保有足够的时间来传播由其他 CH 生成的新块。为了防止 CH 始终声称等待时间较短，邻居节点会经常监视其在等待期间生成新块的频率。这些块的数量超过阈值（根据网络环境和性能需要设定），CH 会丢弃他们邻居节点生成的块。区块链上每一个 CH 节点必须验证从其他节点接收的新块，然后再将其附加到链上。为了验证块，CH 首先验证块生成器的签名。算法 1 概述了验证单个交易（X）的过程。

算法 1 交易共识.

输入: Overlay 交易(X)

输出: True 或 False

请求者验证:

1: 如果当前请求验证 Hash 值与前一块尾 Hash 值不同，则返回 False

2: 如果当前请求验证的签名不通过，则返回 False

输出验证:

3: 如果交易(X.output[0] - X−1.output[0]) + (X.output[1] - X−1.output[1])> 1) 表明区块链接受的成功交易具有重复区块，则返回 False

被请求者验证:

4: 如果被请求者当前交易签名验证不通过，则返回 Flase
否则，该交易达成共识，验证通过。

2.2 分布式信任确权机制

验证所有交易和区块会耗费很高的算力，特别是当 Overlay network 中的节点数量增加时。在工业互联网环境中，人们很难预期节点的扩展性问题，因为节点变化数量会非常大。为了解决这个问题，LHTB 使用分布式信任确权机制，在 CH 节点建立相互建立信任，逐渐减少每个新块中需要验证的交易数量。该机制引入直接和间接信任模式。（1）直接信任：如果先期有一块区块是由 CH#1 生成，则 CH#x 则对 CH#1 信任。间接信任：如果 CH#2 没有对 CH#1 的信任证据，但是如果有其他任意一 CH#x 节点确认 CH#1 生成的块是有效的，那么 CH#2 就有 CH#1 的间接证据。因此，每个 CH 维护一动态列表，记录相关信息以建立直接证据。CH 节点通过信任机制降低对其他不合规节点的信任评级。分布式信任算法背后的核心思想是 CH 收集的有关其他节点生成新块的信任越强，该该块内需要验证成本越少，从而提升区块链共识和确权效率。

2.3 动态高通量管理算法

在 LHTB 中，我们提出了一种动态高通量管理（Dynamic high throughput management-DHM）机制，以主动监视区块链吞吐量利用率并且适当地调整以确保它保持在可接受的范围。在某个共识期结束时，每个 CH 计算利用率 $\theta=(\theta_{\min},\theta_{\max})$ 作为生成的新交易总数与添加到区块链交易总数的比率。假设网络具有 N 个节点，C 为共识效率，其中 M 是聚类后的 CH 数量，S 表示节点每秒产生交易的平均速率，T 为 2.1 节所述的等待周期。则区块链利用率 θ 表示如下：

$$\theta=\frac{N*S*C-T}{M*T_{\max}} \tag{1}$$

上述等式表明，有两种方法可以调整利用率：（1）改变共识周期 T，该值会根据相应工业互联网络延时及区块链区块生成频率确定；（2）改变 M。由于每个 CH 可以在共识期内产生一个块，如果重新调整 Overlay 节点聚类状态，则会产生更大的开销。因此，如果 θ 超过 $\theta_{\max}$，采用第一种模式，DHM 检查是否可以减少共识周期，并确保 θ 在期望范围的中值附件。相反，如果不能减少共识周期，则重新对 Overlay 网络进行聚类调整 CH 及节点的集群关系，从而实现 LHTB 的扩展。我们将共识周期重置为默认值，否则它将保持在最小阈值不变，因此如果利用率增加到其阈值以上，则启动网络重新配置，其中参与节点数量的增加可提供更高的吞吐量。当利用率下降到 $\theta_{\min}$ 以下的情况下，采用反向操作。根据以上操作可以实现对不同网络状态情况下区块链通量的动态管理。

3 工业互联网区块链交易实现

工业互联网各种异构设备由本地 CH（LCH）管理。由于现场设备通常受资源限制，使用对称加密方法对本地交易进行加密，在双方之间建立共享密钥，并使用轻量级加密哈希函数。LCH 集中管理一份本地不可变登记表（LIB），其结构类似于区块链表。所有交易日志都存储在 LIB 表中交易部分中以供日后审计。

以分层区块链的 RSL 层数据存储交易为例，图 4 描述了某一 0 号设备(温控器)的采集数据请求区块生成及交易确权过程。其流程说明如下：

① 本地数据请求设备（温控器）向 CH 节点的控制设备发起数据交互请求，两个实体之间的共享密钥

加密，同时请求设备在本地创建 LIB 账本。

② 控制设备查询本地区块确权请求设备是否具有相应权限。

③ 在区块表中的执行策略部分加密存储了 RRL 集群设备的所有策略定义，并执行相应的策略。

④ 根据相应区块及 Hash 值检查交易请求的有效性，并确认区块的可用空间。

⑤ 通过计算接收数据包的散列并将其与接收的散列进行比较，如果两个哈希匹配，则运行将请求设备数据交易进行存储。

⑥ 将产生的新的区块号用共享密钥加密，并发送给 ERL 控制设备进行区块确权操作。

⑦ 将新区块进行 Hash 运算并发送回给 Overlay 网络，以更新 RRL 各 CH 节点的区块信息。

⑧ ⑨ 返回新区块号并通过 CH 设备更新 RRL 本地区块链，完成分层区块链的交易流程。

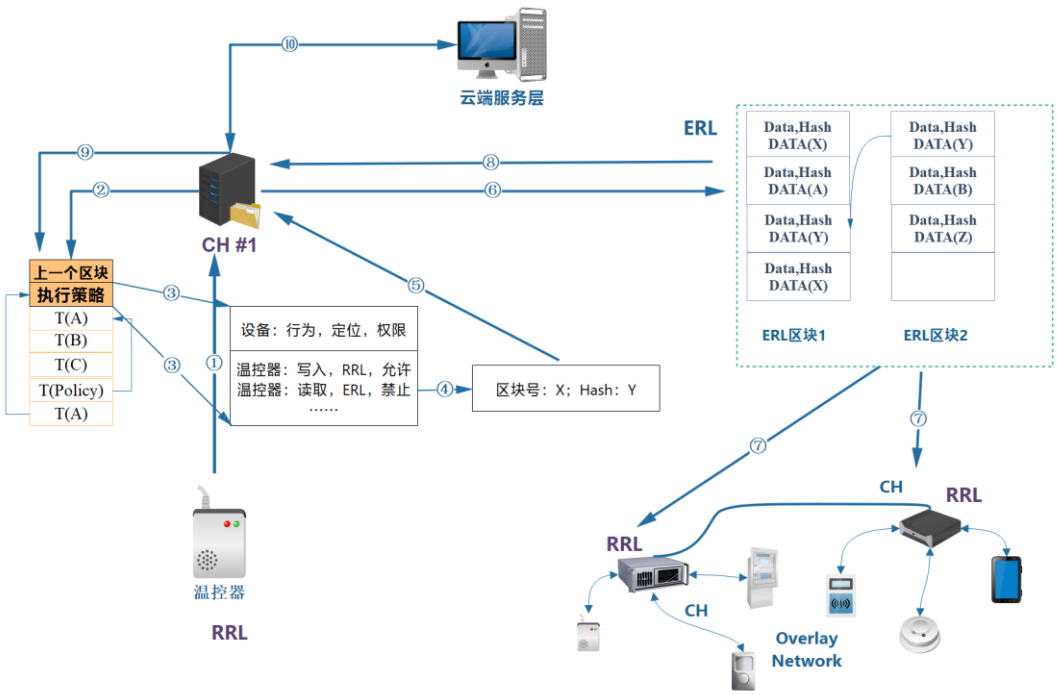

图 4 工业物联网受限资源层区块链生成流程

在这个过程中，所有 Overlay 网络已转发交易的 CH 节点必须将 Hash 值其保留在 RRL 区块链中。 此外，请求者和被请求者的 CH 也记录该事务。 其他节点决定基于它们是否涉及与该事务相关的任何中间通信来存储事务，从而降低了整个网络的通讯量，提高了区块链的处理效率。

4 总结

工业互联网由大多数资源受限的设备组成，具有分散化的拓扑结构，传统的集中式访问控制模型在工业互联网应用中面临巨大的挑战。新兴的区块链技术具有和工业互联网相似的分散化拓扑结构，具有去信任中心、防篡改等特性。区块链提供了工业互联网中有效的数据安全和隐私保护技术，但同时也面临了诸多挑战，包括：复杂性、带宽和延迟开销以及可扩展性等。为了应对这些挑战，本文提出了一种用于工业互联网的轻量级高通量区块模型（LHTB），用于工业网络环境下设备访问控制及数据安全保护。将工业互联网的 Overlay 网络分层为受限资源层和扩展资源层，对分层区域内不同资源能力的设备设计了相应的区块链操作。在受限资源层，为了最大能力保障可扩展性，将受限资源节点组织为集群，只有集群头节点 CH 负责管理公共区块

链。为建设网络时延的区块操作不同步，设计了一种时间一致性算法，该算法限制了节点在共识周期内生成的新块的数量，可减少验证和添加到新区块的计算开销。为提高区块链的通量，设计了分布式信任确权算法，每个节点基于它们生成的新块的有效性累积关于其他节点的证据。由于节点彼此之间存在信任，因此需要验证的新区块中的交易数量逐渐减少。提出了一种可扩展的动态高通量管理机制，以动态地确定区块链效率控制参数，以确保公共区块链的交易不会显着偏离网络中的事务负载。最后给出了一个本地受限资源设备对数据交易上链的操作实例。未来我们将拓展探讨受限资源层、扩展资源层及中心资源层相互的区块链实现机制，以扩展其应用领域，并对其运行效率进行定量研究与分析

References:

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

[2] Mukhopadhyay U, Skjellum A, Hambolu O, Oakley J, Yu L, Brooks R. A brief survey of Cryptocurrency systems. In: Privacy, Security and Trust. 2017. 745–752.

[3] Antonopoulos AM. Mastering Bitcoin: Unlocking Digital Crypto-Currencies. O’Reilly Media, Inc., 2014.

[4] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, “Everything you wanted to know about the blockchain: Its promise, components, processes, and problems,” IEEE Consumer Electronics Mag, 2018.7(4):6-14

[5] M. Mukherjee, R. Matam, L. Shu, L. Maglaras, M. A. Ferrag, N. Choudhury, and V. Kumar, “Security and privacy in fog computing: Challenges,” IEEE Access, 2017. (5):19293-19304

[6] M. Swan, Blockchain: blueprint for a new economy, 1st ed. ÓReilly Media, Jan. 2015.

[7] F. Tschorsch and B. Scheuermann, “Bitcoin and beyond: A technical survey on decentralized digital currencies,” IEEE Commun. Surveys & Tut., 2016.3(18):2084-2123

[8] 袁勇,王飞跃.区块链技术发展现状与展望.自动化学报,2016,42(04):481-494

[9] D. Wilson and G. Ateniese, “From pretty good to great: Enhancing PGP using bitcoin and the blockchain,” in Network and System Security. Springer International Publishing, 2015: 368–375.

[10] X. Huang, C. Xu, P. Wang, and H. Liu, “LNSC: A security model for electric vehicle and charging pile management based on blockchain ecosystem,” IEEE Access,2018(6)13565-13574

[11] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, “BlockChain: A Distributed Solution to Automotive Security and Privacy,” IEEE Commun. Mag, 2017,12(55):119-125

[12] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, “Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems,” IEEE Internet Things, 2017.6(4):1832-1843

[13] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, “Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains,” IEEE Trans. Ind. Informatics, 2017.6(13):3154-3164

[14] L. Li, J. Liu, L. Cheng, S. Qiu, W. Wang, X. Zhang, and Z. Zhang, “CreditCoin: A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles,” IEEE Trans. Intell. Transp. Syst., 2018.1-17

[15] Z. Yang, K. Zheng, K. Yang, and V. C. M. Leung, “A blockchain-based reputation system for data credibility assessment in vehicular networks,” in 2017 IEEE 28th Annu. Int. Symp. Pers. Indoor, Mob. Radio Commun. IEEE, oct 2017, 1–5.

[16] J. Wang, M. Li, Y. He, H. Li, K. Xiao, and C. Wang, “A Blockchain Based Privacy-Preserving Incentive Mechanism in Crowdsensing Applications,” IEEE Access, 2018.(6): 17545–17556

[17] F. Tian, “An agri-food supply chain traceability system for China based on RFID & blockchain technology,” in Proc. IEEE 13th Int. Conf. on Service Systems and Service Management (ICSSSM), June 2016.

[18] A.Dorri,S.S.Kanhere,R.Jurdak,andP.Gauravaram.Blockchain for iot security and privacy: The case study of a smart home, in IEEE Percom workshop on security privacy and trust in the Internet of Things. IEEE, 2017.

[19] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, “Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things,” IEEE Trans. Ind. Informatics, 2017.1-10

[20] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, and B. Amaba, “Blockchain technology innovations,” in Proc. IEEE Technology & Engineering Management Conference (TEMSCON), 2017.

[21] J. Gao, K. O. Asamoah, E. B. Sifah, A. Smahi, Q. Xia, H. Xia, X. Zhang, and G. Dong, “GridMonitoring: Secured sovereign blockchain based monitoring on smart grid,” IEEE Access, vol. 6, pp. 2018.(6):9917–9925,

[22] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, “Distributed Blockchain-Based Data Protection Framework for Modern Power Systems against Cyber Attacks,” IEEE Trans. Smart Grid, 2018.

[23] 唐长兵,杨珍,郑忠龙. PoW共识算法中的博弈困境分析与优化.自动化学报，2017, 43 (9) :1520-1531

[24] 丁庆洋，王秀利，朱建明,等. 基于区块链的信息物理融合系统的信息安全保护框架. 计算机科学, 2018, 45(2):32-39.

[25] 祝烈煌,高峰,沈蒙. 区块链隐私保护研究综述.计算机研究与发展，2017, 54(10):2170 -2186.

[26] N. Zhumabekuly Aitzhan and D. Svetinovic, “Security and Privacy in Decentralized Energy Trading through Multi-signatures, Blockchain and Anonymous Messaging Streams,” IEEE Trans. Dependable Secur. Comput., 2016.

[27] N. Kshetri, “Blockchain’s roles in strengthening cybersecurity and protecting privacy,” Telecommunications Policy, vol. 41, no. 10, pp. 1027–1038, Nov. 2017. A. Dorri, S. S. Kanhere, and R. Jurdak, “Towards an optimized blockchain for iot,” in IEEE/ACM International conference on Internet-of-Things Design and Implementation (IoTDI), 2017.

[28] Skarmeta, Antonio F., Jose L. Hernandez-Ramos, and M. Moreno., "A decentralized approach for security and privacy challenges in the internet of things," in nternet of Things (WF-IoT), 2014 IEEE World Forum on, 2014.

[29] H. Gross; M. Holbl, D. Slamanig, and R. Spreitzer, "Privacy-Aware Authentication in the Internet of Things," Cryptology and Network Security. Springer International Publishing, 2015. 32-39

[30] Ali Dorri, Salil S. Kanhere, Raja Jurdak.Blockchain in internet of things: Challenges and Solutions. arXiv:1608.05187