第31课：区块链...

大家好，我是丹华。本节我们讨论区块链在物联网 IoT 中的应用。

- 物联网简述
- 从车联网看物联网的痛点
- 区块链+物联网的机会
- 区块链+物联网的挑战
- 应用案例
- 了解更多

物联网简述

大家知道，物联网（Intrernet of Things，简称 IoT）代表一个新的庞大的技术和产业方向。概念上，物联网是指将所有物理设备连接起来形成网络。

物联网是传统互联网的深化和扩展，从原来的电脑、智能手机和平板，扩展到任意的物理设备，是设备信息化和智能化的必然趋势。据称，2017年全球接入 IoT 网络的设备数量超过84亿台。2020年将达到300亿台。目前主要应用领域包括生产线监测、智能设备、智能建筑、智慧城市、智能家庭、车联网、智能电网、环保监测、供应链管理等。

物联网更严格的定义是，即通过射频识别（RFID）(RFID+互联网）、红外感应器、全球定位系统、激光扫描器、气体感应器等信息传感设备，按约定的协议，把任何物品与互联网连接起来，进行信息交换和通讯，以实现智能化识别、定位、跟踪、监控和管理的一种网络。

物联网的一个核心特征是，接入网络的设备异质化程度高（种类多样、各不相同），设备自身资源有限（计算能力、联网能力、电能等）。任何基于物联网的应用和协议都必须考虑设备的异质性和资源禀赋。

从车联网看物联网的痛点

车联网是物联网的一个子技术方向，目标是实现以车辆为中心、用无线网络将车上的多种传感器连接起来。车联网实现了车辆数据的信息化和互联网化，将催生全新的车辆经营维护、智慧城市管理、保险等模式。

车联网也是一个典型的多方参与、多方合作的产业网络。具体来说，车联网存在如下特点：

- 多个数据来源：大量的车载传感器、网络连接、云端服务、第三方数据。
- 多方参与，弱信任：涉及用户、整车厂、4S 店、修理店、保险、二手市场、车辆管理部门、交警与执法部门、汽车共享平台、汽车后市场应用平台等；各环节之间都有一定的利益冲突和信息不对称，信任程度较低；
- 各方均要求信息的客观真实性：如行驶记录、事故记录、维修历史等。

- 往往一次事件引发多方交互：如一次交通事故、一次车辆交易、一次维修和赔付请求，往往都涉及多方。

结合区块链的技术特征可知，区块链技术所适用的场景和车联网的特征相当匹配。利用区块链，可以通过数据防篡改和可追溯的统一账本来记录车辆整个生命周期的信息，该账本在各参与方之间共享，实现去中心化的信息互通。

同时，利用智能合约，可以驱动以事件处理为中心、多方合作的各类事件性流程，如车辆报修、保养、事故处理等。智能合约和区块链能够实现整个汽车价值链上几乎所有流程的自动化，提升效率。例如基于车辆的生命周期信息，可以将区块链用于出厂/维修/改装/维护/租用、事故处理、保险理赔、车况取证等场景。

目前的物联网生态，依赖中心化的网络管理架构，所有设备都是通过云服务器连接。随着网络规模的扩大，中心化云服务器、大型服务器和网络设备的基础设施和维护方面将产生高昂成本。在去中心化的物联网中，区块链是设备间交互和协作的框架和平台，是核心的神经系统，每个设备都可作为一个独立、微型的商业主体运行，最终推动网络向自洽、自治的方向进化。

区块链+物联网的机会

- 隐私和匿名性：

  区块链中的交易都使用公钥加密和哈希算法产生的数字身份。IoT 应用如果有敏感信息，可以借助这一机制隐藏设备的真实网络身份。

- 货币激励机制：

  区块链中有内生的代币，可以作为费用和奖励机制，来激励节点分享数据、参与验证交易、提供服务、共享带宽存储空间或算力等。

- 可信的交易记录：

  区块链提供关于全网的去中心化的、完整可信的交易记录，便于查询、追踪和审计，有助于提高设备管理和数据管理的效率。

- 智能合约：

  设备间的交互作业（业务逻辑）可以固化为智能合约，自主决策，自动执行。甚至可以支持在不同的参与节点之间，实现数据的货币化交易功能。

区块链+物联网的挑战

物联网的特性也决定了应用区块链会遇到一些技术上的挑战，包括：

- 设备的资源限制：

  IoT 平台往往都只有有限的计算、通信和存储资源，而区块链作为一种去中心化的数据库，需要消耗大量的资源。IoT 网络中包含着大量的低功率器件，拥有不到 10KB 的数据内存和不到100KB的程序内存。作为对比，主流的区块链节点都需要上百 GB 的空间。采

用工作量证明 POW 机制的区块链，还需要消耗大量 CPU 资源。如果要应用区块链技术，只能将 IoT 网络中的高性能服务器设置为计算节点。

- 带宽限制：

  区块链中的节点需要时时刻刻连接入区块链网络，以参与到共识过程中。基于去中心化的本质，节点需要不断与其他节点交换数据、验证交易和区块、发送接收新交易和新区块等。这对网络接入和带宽提出了很高的要求。物联网中的大多数设备都不具备这一条件。对于当前大多数的主流区块链协议而言，带宽要求甚至会超过了物联网应用本身。因此，一方面应寻求更轻量级的区块链网络协议，另一方面，如果选择服务器作为节点，也需要提升服务器的性能以应对网络设备增加带来的网络压力。

- 安全问题：

  区块链网络要求设备节点时刻在线，这种时刻在线的特征使得设备更容易面临安全攻击和数据泄露等风险。

- 网络延迟

  IoT 网络中有的设备是数据生产者，有些设备需要这些数据、事件以做出决策、生成响应或产生新的数据。处在区块链网络中的设备，可能需要等待共识过程的最终完成，才能使用这些被全网接受的“共识数据”“真相数据”，从而对一个事件作出响应。毫无疑问，这种延迟如果不得到改善，将大大阻碍区块链在多数“时间敏感”的物联网场景中的应用。

- 交易费用

  含有内生代币的区块链，交易中多数会以代币作为交易费用，以激励参与共识、验证交易的节点，同时也使得代币具有价值基础而吸引更多参与者。物联网中，设备间有大量频繁的交互，不太可能都为交互支付代币费用。而无币区块链如联盟链，又可能遇到激励不足、不愿分享设备和数据的情况。

- 公链 or 联盟链

  物联网应用区块链技术，不可回避的问题是，你选择公有链还是联盟链？考虑你的应用，如果参与者之间需要足够的相互信任，需要控制新节点加入的，则应选择联盟链模式。

- 分区容错性

  物联网中的设备可能随时会主动或被动断开网络连接，或断续连接。有些依赖电池的设备仅有有限的持续工作时间。这时，节点服务器无法与设备取得联系并获取最新信息，就无法将最新信息写入区块链中。新的区块链架构如 IOTA 就允许一定程度的分区容错。

- 交易性能瓶颈

  主要的公链面临着严重的交易性能不足和网络拥堵的困扰。

- 物理设备特性

物理设备本身不稳定，会给出错误的数据，服务器根据错误数据可能得出错误结论和行为。而数据一旦记入区块链，就很难更改和删除。

应用案例

区块链+物联网的发展空间非常大，传统的技术巨头们都没有缺席这场盛宴：阿里、腾讯、IBM、微软、亚马逊、Cisco等。各垂直领域的创业探索也都遍地开花。

公链领域最出名的物联网项目就是 IOTA 了。IOTA 是一个专为 IoT 打造的公有链项目。IOTA 使用有向非循环图（DAG），即 Tangle 网络，而不是"线性"区块链。IOTA 里没有区块的概念，也没有挖矿和矿工的概念。在 Tangle 这个由交易组成的有向无环图里，节点要发起一笔新的交易时，需要在 Tangle 中找另外2笔交易完成验证，做一个 POW 计算，并且将自己新发起的交易指向这两笔交易，整个 Tangle 就是这样逐步扩展出去的。由此，网络中验证交易的功能从传统的矿工转移到了每个用户身上——你要发起一笔交易，就必须帮忙验证网络中的其他交易。

目前 IOTA 的主要功能是无偿小额支付和安全的数据传输和数据锚定。有了这两个特性，再加上 IOTA 的可扩展性和分区容错性，可以派生出大量的用例。

IOTA 官网
https://www.iota.org/

IOTA 白皮书
https://iota.readme.io/docs/whitepaper

了解更多

1. Blockchain Enabled Enhanced IoT Ecosystem Security，Mahdi H. Miraz and Maaruf Ali，2018-6
2. Blockchain for the IoT: Opportunities and Challenges，Gowri Sankar Ramachandran，2018-5
3. Incentivized Delivery Network of IoT Software Updates Based on Trustless Proof-of-Distribution，2018-5
4. IoT Security: Review, Blockchain Solutions, and Open Challenges，Minhaj Ahmad Khana, Khaled Salahb，2017-11
5. IoTChain: A Three-Tier Blockchain-based IoT Security Architecture，Zijian Baoa,b, Wenbo Shi，2018-6